Universität Rostock

Traditio et Innovatio

Representation Theory and Polytopes

Habilitationsschrift
zur Erlangung des akademischen Grades
doctor rerum naturalium habilitatus (Dr. rer. nat. habil.)
der Mathematisch-Naturwissenschaftlichen Fakultät
der Universität Rostock.

vorgelegt von
Frieder Ladisch,
geboren am 25. März 1977 in Karlsruhe,
aus Rostock.

Eingereicht: 1. Juni 2017
Verteidigt: 18. Januar 2018

urn:nbn:de:gbv:28-diss2018-0026-2

Frieder Ladisch
Universität Rostock
Institut für Mathematik
18051 Rostock (Germany)
frieder.ladisch@uni-rostock.de

Research supported by the Deutsche Forschungsgemeinschaft (DFG),
Project: SCHU 1503/6-1.

Gutachter:

Prof. Dr. rer. nat. habil. Achill Schürmann
Institut für Mathematik, Universität Rostock.

Peter McMullen, Emeritus Professor, Ph.D., D.Sc.
University College London.

Prof. Dr. rer. nat. habil. Rudolf Scharlau
Fakultät für Mathematik, Technische Universität Dortmund.

Eingereicht: 01. Juni 2017
Probevorlesung: 21. Dezember 2017
Kolloquium: 18. Januar 2018

2010 Mathematics Subject Classification:

52B15	Symmetry properties of polytopes
05E18	Group actions on combinatorial structures
20B25	Finite automorphism groups of algebraic, geometric, or combinatorial structures
20C10	Integral representations of finite groups
20C15	Ordinary representations and characters
52B05	Combinatorial properties of polytopes and polyhedra
52B20	Lattice polytopes
90C10	Integer programming

Keywords and Phrases:
Orbit polytope, group representation, affine symmetry, generic symmetry, representation polytope, permutation polytope, character, core point, lattice polytope, integer linear programming, Birkhoff polytope, abstract regular polytope

Preface

The present habilitation thesis concerns applications of the representation theory of finite groups to polytopes and their symmetries, and in particular, *orbit polytopes*. This is a cumulative thesis, and so the main part of this thesis consists of papers (listed on Page 23) which are already published, or submitted for publication. All papers are also available from the preprint server arXiv.

The papers contained in this thesis have been written at the Institute for Mathematics of the University of Rostock between 2014 and 2017. I wish to thank the members of the Geometry group in Rostock for their collegiality and for stimulating discussions. In particular, I wish to thank Achill Schürmann for his steady support and encouragement during the writing of this thesis, and Erik Friese for the many discussions that led to our two joint papers.

Since 2015, the author is supported by the Deutsche Forschungsgemeinschaft (DFG), Project SCHU 1503/6-1.

Frieder Ladisch
Rostock
May 2017.

For the publication of this thesis, the references were updated, and the comments of the referees of the corresponding papers have been incorporated (in Chapters II, IV and VI).

F. L.
January 2018

Contents

Chapter I.

Introduction

The character theory of finite groups was invented by Ferdinand Georg Frobenius on April 12, 1896 in a letter to Richard Dedekind[1], motivated by finding the factorization of the *group determinant*. Soon thereafter, Frobenius introduced the general notion of a *representation* of an abstract group. The theory was further developed and simplified by William Burnside, Issai Schur, Emmy Noether, and Richard Brauer, to name only a few.

On the one hand, the representation theory of finite groups is a beautiful subject in its own right. On the other hand, it was soon realized that this theory provides a powerful tool to prove theorems about finite groups. For example, Burnside used character theory to prove that groups of order $p^a q^b$ (p and q primes) are solvable, or that a transitive permutation group of prime degree p is either doubly transitive, or permutation isomorphic to a proper subgroup of $\mathrm{AGL}(1, \mathbb{F}_p)$, the group of affine transformations $\mathbb{F}_p \to \mathbb{F}_p$. But the range of applications of representation theory is not limited to pure mathematics, and includes subjects such as physics, chemistry, engineering and statistics. Indeed, whenever some object is given, which is or can be embedded into a linear space, and when this object has symmetries, then representation theory can usually be applied in profitable ways.

In this thesis, we apply this philosophy to the study of symmetry properties of polytopes. Symmetric polytopes in dimension 3 have fascinated mathematicians since antiquity, the most famous examples being the five Platonic solids. The Platonic solids are polytopes that are "as symmetric as possible". Making precise this statement leads to the definition of *regular* polytopes in arbitrary dimension [26].

In the papers contained in this thesis, we are mostly concerned with a larger class of symmetric polytopes, namely *orbit polytopes*. These can be characterized as polytopes whose (linear) symmetry group acts transitively on their vertices. Equivalently, an orbit polytope is the convex hull of an orbit of a point $v \in \mathbb{R}^d$ under a finite group $G \subset \mathrm{AGL}(d, \mathbb{R})$.

Of course, all of the well known regular polytopes are orbit polytopes. By (one) definition, the *Archimedean solids* are orbit polytopes in dimension 3 such that all faces are regular polygons (By another definition, the pseudo-rhombicuboctahedron

[1] This is one of the few instances where one can assign a specific date to the birthday of a whole mathematical theory.

is also an Archimedean solid, which is not vertex transitive. Indeed, many authors do not clearly distinguish these definitions [35].) Another classical example is the permutahedron [17], which is an orbit polytope of the symmetric group S_n in its standard representation (permuting coordinates of $\mathbb{R}^n$). Other permutation groups yield orbit polytopes which are important in combinatorial optimization, for example the (symmetric or asymmetric) *traveling salesman polytope* [6, 68].

A particularly interesting case are orbit polytopes of finite reflection groups, which are often called generalized permutahedra, or simply permutahedra [17, 43, 44, 58, 78]. The classical *Wythoff construction* [25, 26, 27] basically consists in taking orbits under a reflection group to construct polytopes or tessellations of a sphere. In particular, Coxeter [25] has shown that several uniform polytopes can be obtained as orbit polytopes of (finite) reflection groups by choosing a suitable starting point v (see also [65]). In the language of Sanyal, Sottile and Sturmfels [73], orbit polytopes are polytopal *orbitopes*. (An orbitope is the convex hull of an orbit of a compact group, not necessarily finite. Convex hulls of orbits of compact groups were also studied by Barvinok and Blekherman [7].)

Ellis, Harris and Sköldberg [31] used orbit polytopes to compute free resolutions for finite groups (in the context of group homology).

An interesting class of orbit polytopes is formed by representation polytopes. A representation polytope is defined as the convex hull of $D(G)$, where $D\colon G \to \mathrm{GL}(d, \mathbb{R})$ is a representation of an abstract finite group G. If the image group consists of permutation matrices, the polytope is called a permutation polytope. A well-known example is the celebrated Birkhoff polytope of doubly stochastic matrices (also known as assignment polytope), which is the convex hull of *all* permutation matrices of a fixed dimension. Permutation polytopes and some other special classes of representation polytopes have also been studied by a number of people [8, 36, 42, 57].

In the papers included in this thesis, we study several special aspects of orbit polytopes, including a special property of the Birkhoff polytope. In the following, we give a more detailed summary of these papers and their relations to each other. We will recall the relevant definitions as we go along.

1. Polytopes and their different symmetries

Recall that a **polytope** P is the convex hull of a finite number of points $v_1, \ldots, v_n$ in some euclidean space V, without loss of generality $V = \mathbb{R}^d$:

$$P = \operatorname{conv}\{v_1, \ldots, v_n\} := \left\{ \sum_{i=1}^{n} \lambda_i v_i \;\middle|\; \sum_{i=1}^{n} \lambda_i = 1,\ \lambda_i \geqslant 0 \right\}.$$

The **dimension** $\dim(P)$ of a polytope P (or any subset $P \subseteq V$) is by definition the dimension of its affine hull $\mathrm{Aff}(P)$ (the smallest affine subspace of V containing P).

A linear inequality $a^t x \leqslant b$ is **valid** for the polytope P if $a^t x \leqslant b$ for all $x \in P$. A **face** of P is a set F of the form

$$F = P \cap \{x \in V \mid a^t x = b\},$$

where $a^t x \leqslant b$ is valid for P. The **vertices** of P are the points $v \in V$ such that $\{v\}$ is a face of P. Thus the vertices correspond to the faces of P of dimension 0. We write $\mathrm{Vert}(P)$ for the set of vertices of a polytope P. The faces of dimensions 1 and $\dim(P) - 1$ are called **edges** and **facets**, respectively.

By the Farkas-Minkowski-Weyl theorem, a polytope can equivalently be defined as a bounded subset of $\mathbb{R}^d$ which is the intersection of finitely many half-spaces. This is the dual description of the polytope. Another important fact is that each face of a polytope is the convex hull of the vertices of the polytope that are contained in the face in question. Thus we can (and often do) identify a face of P with the set of vertices of P contained in it. The aforementioned facts can be found in any text on polytopes, for example in the first few lectures of Ziegler's book on polytopes [77].

Now we recall the definitions of the different types of symmetries of polytopes. More generally, we consider isomorphisms between two polytopes $P \subset V$ and $Q \subset W$, where V and W are two euclidean spaces.

1.1 Definition. Let $P \subset V$ and $Q \subset W$ be polytopes.

(a) An **isometry** from P to Q is a bijection $\alpha\colon P \to Q$ that preserves (euclidean) distances.

(b) A **linear isomorphism** between P and Q is a bijection $\alpha\colon P \to Q$ that can be extended to a linear map from V into W.

(c) An **affine isomorphism** between P and Q is a bijection $\alpha\colon P \to Q$ that can be extended to an affine map from V into W.

(d) A **combinatorial isomorphism** from P onto Q is a bijection

$$\alpha\colon \mathrm{Vert}(P) \to \mathrm{Vert}(Q)$$

that sends faces of P onto faces of Q.

The **isometry group** or **euclidean symmetry group** of P is the group of all isometries from P onto itself. Similarly, **linear, affine or combinatorial symmetries** of P are linear, affine or combinatorial isomorphisms of P onto itself. We write

$$\mathrm{Isom}(P), \quad \mathrm{GL}(P), \quad \mathrm{AGL}(P), \quad \mathrm{Comb}(P)$$

for the orthogonal, linear, affine and combinatorial symmetry group of P.

The first three definitions make sense for arbitrary subsets $S \subseteq V$ and $T \subseteq W$, and in particular, $\mathrm{Isom}(S)$, $\mathrm{GL}(S)$ and $\mathrm{AGL}(S)$ are defined for arbitrary subsets $S \subseteq V$. Each type of isomorphism of polytopes is determined by its action on the

vertices of P. In particular, we can identify $\mathrm{Isom}(P)$, $\mathrm{GL}(P)$ and $\mathrm{AGL}(P)$ with permutation groups on $\mathrm{Vert}(P)$, and then we have

$$\mathrm{Isom}(P) \subseteq \mathrm{AGL}(P) \subseteq \mathrm{Comb}(P) \quad \text{and} \quad \mathrm{GL}(P) \subseteq \mathrm{AGL}(P).$$

It is easy to see by examples that these containments can be strict. It is also easy to see that each polytope P is affinely isomorphic to a polytope Q such that $\mathrm{GL}(Q) = \mathrm{AGL}(Q)$ (simply translate P into a polytope with barycenter 0). Indeed, most questions about affine symmetries of polytopes reduce to questions about linear symmetries, which are usually easier to handle algebraically. On the other hand, $\mathrm{GL}(P)$ is not "intrinsically interesting" in the sense that $\mathrm{GL}(P)$ depends on the concrete embedding of the affine object P into a space, while $\mathrm{AGL}(P)$ is independent of the choice of a coordinate system of the surrounding affine space.

It is less obvious, but well known and not very difficult to see that each polytope P is affinely equivalent to a polytope Q such that $\mathrm{Isom}(Q) = \mathrm{AGL}(Q)$. Basically, this follows from the fact that for each finite group $G \leqslant \mathrm{GL}(d, \mathbb{R})$, there is a G-invariant scalar product on $\mathbb{R}^d$. This is a standard fact in the representation theory of finite groups.

It is not true, however, that every polytope is combinatorially equivalent to a polytope Q such that $\mathrm{AGL}(Q) = \mathrm{Comb}(Q)$. Indeed, in 1984, Bokowski, Ewald and Kleinschmidt [16] constructed a polytope P with a combinatorial symmetry $\varphi \in \mathrm{Comb}(P)$, such that for every combinatorial isomorphism $\alpha\colon P \to Q$ onto some polytope Q, we have $\alpha \circ \varphi \circ \alpha^{-1} \notin \mathrm{AGL}(Q)$. In other words, φ is not "affinely realizable". Since then, other examples of this kind have been constructed [33, 69].

2. Orbit polytopes

Suppose that $G \leqslant \mathrm{GL}(V)$ is a finite subgroup, where V is a finite dimensional vector space over $\mathbb{R}$. It seems to be a folklore result that in this situation, there are polytopes $P \subset V$ such that $G = \mathrm{GL}(P)$. How might one construct such a polytope? First we observe that it is easy to find polytopes such that $G \leqslant \mathrm{AGL}(P)$: just take a union of G-orbits of points and form the convex hull. The simplest case of this construction is that of an **orbit polytope**, the convex hull of the orbit Gv of some point $v \in \mathbb{R}^d$. We denote it by

$$\mathrm{P}(G, v) = \mathrm{conv}\{gv \mid g \in G\}.$$

Of course, such a polytope may have additional symmetries. For example, when $G \leqslant \mathbf{O}(\mathbb{R}^2)$ is the cyclic group generated by a rotation of order n, then every orbit of a point is a regular n-gone and has a linear symmetry group of order $2n > |G| = n$. The usual idea then is to take the G-orbit of a "sufficiently asymmetric" set, or to cut off pieces from a polytope constructed as above in a "sufficiently asymmetric"

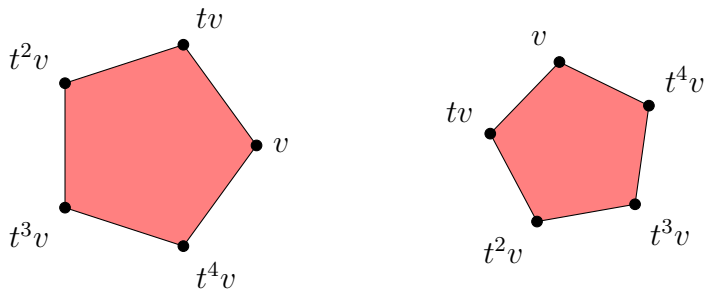

Figure 1. Two orbit polytopes of the group $G = \langle t \rangle$ of rotations preserving a pentagon. All nontrivial orbit polytopes have additional symmetries.

way. Different possibilities to do this are discussed in the answers to a MathOverflow question [59], for example.

However, there is also a short, elegant and elementary argument by I. M. Isaacs which shows that every finite group $G \leqslant \mathrm{GL}(V)$ is the full stabilizer of a finite, spanning set $X \subseteq V$, whenever V is a finite dimensional vector space over an infinite field [47]. A small modification of the argument shows that in the case of a real vector space, the set X can be chosen as the vertex set of a polytope. Isaacs' argument also shows that every abstract finite group is isomorphic to the linear symmetry group of a polytope, with at most two orbits on the vertices. (Let us mention here that only quite recently it has been shown that every finite group is isomorphic to the combinatorial symmetry group of a polytope [29, 74].)

Of course, we can still ask for which groups $G \leqslant \mathrm{AGL}(V)$ we can find an orbit polytope $\mathrm{P}(G, v)$ such that $G = \mathrm{AGL}(\mathrm{P}(G, v))$. This was one of the questions that motivated my two joint papers with Erik Friese [FL1, FL2]. Chapters II and IV contain parts of these papers in revised form.

For example, we have seen above that when $G \cong C_n$ is a cyclic group of order n generated by a rotation in 2-space, then every orbit polytope has additional symmetries. On the other hand, there are many finite groups $G \leqslant \mathrm{GL}(V)$ such that $G = \mathrm{GL}(\mathrm{P}(G, v))$ for some $v \in V$. This yields a number of related questions, for example:

2.1 Questions.

(a) For which subgroups $G \leqslant \mathrm{GL}(V)$ is $G = \mathrm{AGL}(\mathrm{P}(G, v))$ for some $v \in V$?
(b) Given $G \leqslant \mathrm{GL}(V)$, how are the symmetry groups $\mathrm{AGL}(\mathrm{P}(G, v))$ for different v related?
(c) Let G be an abstract finite group. For which representations $D\colon G \to \mathrm{GL}(V)$ do we have $D(G) = \mathrm{AGL}(\mathrm{P}(G, v))$ for some $v \in V$? (Here we extend the notation $\mathrm{P}(G, v)$ to mean $\mathrm{P}(G, v) = \mathrm{conv}\{D(g)v \mid g \in G\}$.)
(d) Which finite groups G are isomorphic to $\mathrm{AGL}(\mathrm{P}(G, v))$ for some $v \in V$ and some representation $D\colon G \to \mathrm{GL}(V)$?

Before we go on, let us mention that in all these question, it makes not really a difference whether we consider affine or linear symmetry groups (see Section 2 in Chapter II).

Another immediate observation is that we can replace the orbit polytope $\mathrm{P}(G, v)$ by its set of vertices, which is just the orbit Gv. Thereby, the problems become purely algebraical in nature. For example, the first question becomes whether we can find an orbit Gv such that $G = \mathrm{GL}(Gv)$. In the case that $V = \mathrm{Span}(Gv)$, this simply means that G is the setwise stabilizer of the subset $Gv \subset V$ in $\mathrm{GL}(V)$. It is clear that in this form of the problem, there is no reason to restrict oneself to the case of vector spaces over the real numbers. Instead one can work with vector spaces over an arbitrary field.

Recall that a group $G \leqslant \mathrm{GL}(V)$ (or a representation $D\colon G \to \mathrm{GL}(V)$) is said to be *absolutely irreducibly*, if only the scalar matrices centralize G (or $D(G)$, respectively). In the paper mentioned before, Isaacs [47] showed that when the finite group $G \leqslant \mathrm{GL}(V)$ is absolutely irreducible, where V is a vector space over an infinite field, then $G = \mathrm{GL}(Gv)$ for some orbit $Gv \subset V$. So this gives a sufficient condition for a positive answer to Question (a). As the example $C_n \leqslant \mathrm{GL}(2, \mathbb{R})$ shows, it is not sufficient to assume that V is irreducible over G.

Question (d) was in fact posed by Babai [2] in 1977. Notice that we could ask the same questions for isometries instead of affine or linear symmetries. With this modification, Question (d) was answered by Babai [2]. More precisely, Babai classified all finite groups which are not the euclidean symmetry group of an orbit polytope, namely:

2.2 Theorem (Babai [2]). *A finite group G is not isomorphic to the isometry group of an orbit polytope, if and only if one of the following holds:*

(i) *G is abelian, but not elementary 2-abelian.*

(ii) *G is generalized dicyclic.*

(We will recall the definition of generalized dicyclic groups in Chapter IV, Section 2.)

In the same paper, Babai asked for a characterization of finite groups which are isomorphic to the affine symmetry group of an orbit polytope, which is Question (d) above. (Babai asked also for the analogous characterizations with some other types of symmetries, namely sense-preserving (euclidean) and projective symmetries, but we will not consider these problems here.) In Chapter IV, we will answer Question (d). As we will explain later, a standard argument shows that a group which is isomorphic to the affine symmetry group of an orbit polytope, is also isomorphic to the euclidean symmetry group of an orbit polytope. The converse is not true, but the surprising outcome of the answer to Babai's question is that there are only three groups, which can be realized as euclidean symmetry groups

of orbit polytopes, but not as affine symmetry groups. These are the elementary abelian groups with the orders 4, 8 and 16.

Realizing a (finite) group as symmetry group of a polytope is a concrete example of a general kind of problem, namely realizing a given group as automorphism group of an object in a given class of mathematical objects. For example, the central problem of inverse Galois theory is whether every finite group is isomorphic to the Galois group of some finite extension field over $\mathbb{Q}$. Another example is a classical theorem of Frucht [32] that says that every finite group is the automorphism group of a (finite, simple, undirected) graph. The last problem can be made more interesting by asking which finite groups can be realized as the automorphism group of a vertex-transitive graph. This means that the automorphism group acts transitively on the vertices of the graph. Obviously, this is analogous to Question (d) above. Even more, it turns out that the problems are related, but the relation is not entirely understood.

The automorphism groups of finite vertex-transitive graphs have been completely classified by Hetzel (unpublished) and Godsil [34] building on work of others (a more complete list of references can be found in Babai's paper [2], in a subsequent paper of Babai and Godsil [4], or in the handbook chapter of Babai on this and related topics [3, Section 4.3]). The outcome of this classification is as follows:

2.3 Theorem. *The only finite groups which can not be realized as the automorphism group of a vertex-transitive graph, are the following:*

(i) *abelian groups of exponent* > 2,
(ii) *generalized dicyclic groups,*
(iii) 13 *other groups of order at most* 32, *including the elementary abelian groups of orders* 4, 8 *and* 16.

The graphs constructed by the various authors to represent other groups as transitive graph automorphism groups, are actually GRRs: A graph X is said to be a *GRR* (*graphical regular representation*) of the finite group G, when $\mathrm{Aut}(X) \cong G$ and $\mathrm{Aut}(X)$ acts *regularly* on the vertices of X.

It follows from Theorem 2.3 and our classification of affine symmetry groups of orbit polytopes, that every finite group admitting a GRR is also isomorphic to the affine symmetry group of an orbit polytope. We are not aware of any direct proof of this fact. On the other hand, Babai showed directly that every group admitting a GRR is isomorphic to the euclidean symmetry group of an orbit polytope. More precisely, Babai showed that a group G is the euclidean symmetry group of an orbit polytope if and only if G has an *SRR* (*symmetric regular representation*): An SRR of a group G can be defined as an edge-colored graph X such that $\mathrm{Aut}(X) \cong G$ and $\mathrm{Aut}(X)$ acts regularly on the vertices of X. Here $\mathrm{Aut}(X)$ is meant to preserve the edge colors. Obviously, any GRR is an SRR.

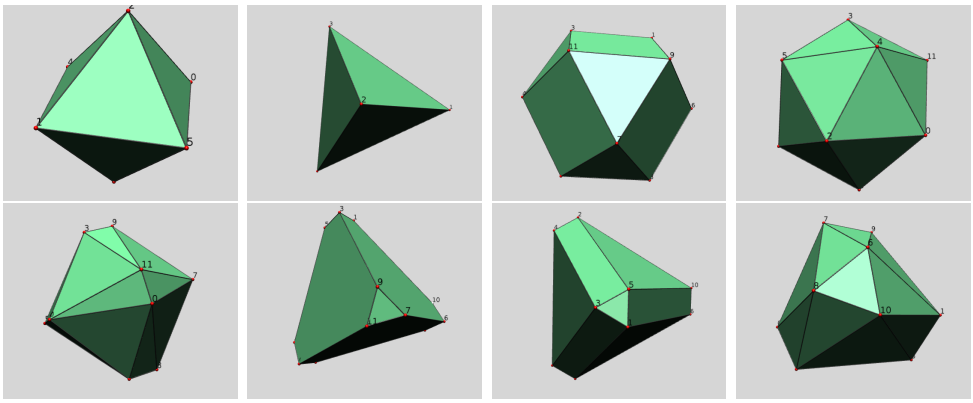

Figure 2. Examples of the different types of orbit polytopes of the tetrahedral rotation group $T \cong A_4$. First row (from left to right): Octahedron, tetrahedron, cuboctahedron, (regular) icosahedron, second row: skew icosahedron with symmetry group $\pm T$, truncated tetrahedron, skew cuboctahedron, and generic icosahedron with symmetry group T.

It also follows from the classifications that there are only 10 finite groups (up to isomorphism) which are isomorphic to the affine symmetry group of an orbit polytope, but admit no GRR.

3. Affine symmetries of orbit polytopes

Motivated by the questions in 2.1, we develop in Chapter II a general theory of orbit symmetries.

Let us begin with a concrete example. Let $G = T \subseteq \mathrm{GL}(3, \mathbb{R})$ be the rotation group of the tetrahedron, more concretely, let

$$G = T = \left\langle \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

This is the group of rotations of the tetrahedron with vertices $(\pm 1, \pm 1, \pm 1)$, where the number of -1-s is even. As an abstract group, $G \cong A_4$.

Now let us see what orbit polytopes we get for this group, depending on our starting point $v \in \mathbb{R}^3$. Of course, for $g \in G$ we have $\mathrm{P}(G, gv) = \mathrm{P}(G, v)$. For $\lambda \in \mathbb{R}$, we have $\mathrm{P}(G, \lambda v) = \lambda \, \mathrm{P}(G, v)$, and these two orbit polytopes are similar. A common generalization of these two observations is this: Suppose that

$$n \in \mathbf{N}_{\mathrm{GL}(3,\mathbb{R})}(G) := \{n \in \mathrm{GL}(3, \mathbb{R}) \mid n^{-1} G n = G\},$$

v	$\lvert Gv\rvert$	$\mathrm{P}(G,v)$	AGL	Comb
$(0,0,1)$	6	regular octahedron	$\pm O$	$\pm O$
$(1,1,1)$	4	regular tetrahedron	TO	TO
$(0,1,1)$	12	cuboctahedron	$\pm O$	$\pm O$
$(0,\varphi,1)$	12	regular icosahedron	$\pm I$	$\pm I$
$(0,c,1)$	12	skew icosahedron	$\pm T$	$\pm I$
$(c,c,1)$	12	truncated tetrahedron	TO	TO
$(c,1,1)$	12	skew cuboctahedron	TO	$\pm O$
$(c,d,1)$	12	skew icosahedron	T	$\pm I$

Table 1. The different orbit polytopes of the tetrahedral rotation group $T \cong A_4$. Here, $\varphi = (-1+\sqrt{5})/2$, the golden ratio, while c and d are arbitrary with $0 < c < 1$, and $0 < c < d < 1$, respectively. The last two columns give the affine and combinatorial symmetry group in notation following Conway and Smith [24].

the *normalizer* of G in $\mathrm{GL}(3,\mathbb{R})$. Then

$$\begin{aligned}\mathrm{P}(G,nv) = \mathrm{conv}(Gnv) = \mathrm{conv}(n\,n^{-1}Gnv) &= \mathrm{conv}(nGv)\\ &= n\,\mathrm{conv}(Gv)\\ &= n\,\mathrm{P}(G,v).\end{aligned}$$

This means that n induces a linear isomorphism from $\mathrm{P}(G,v)$ onto $\mathrm{P}(G,nv)$. These orbit polytopes are thus affinely equivalent.

In our concrete example, the group G is normalized by all scalar matrices, and also by the full symmetry group of the cube, consisting of all signed permutation matrices. Thus up to affine equivalence, and leaving aside the trivial case $v = 0$, we can choose our starting point $v = (x,y,z)$ such that $0 \leqslant x \leqslant y \leqslant z = 1$. Geometrically, this means that our point lies in a certain triangle on the surface of a cube.

It turns out that there are 8 different cases, counting the occurring combinations of combinatorial type and affine symmetry groups of the orbit polytope. These are listed in Table 1. Indeed, only 5 orbit polytopes up to combinatorial equivalence arise, but some of these occur with different affine symmetry groups. Namely, the icosahedron occurs with three different affine symmetry groups, and the cuboctahedron with two. The notation for the affine and combinatorial symmetry groups follows Conway and Smith [24], which is of course a slight abuse of notation in the case of combinatorial symmetry groups. Notice that in the few cases where the combinatorial symmetry group is strictly larger than the affine symmetry group, there is a starting point v yielding a combinatorial equivalent polytope and such that $\mathrm{AGL}(\mathrm{P}(G,v)) = \mathrm{Comb}(\mathrm{P}(G,v))$.

The truncated tetrahedron, which occurs in the table as orbit polytope of the point $(c,c,1)$, is in general not archimedean, as its hexagonal faces are not regular.

Only for a special value of c is this solid archimedean. However, this makes no difference for the affine symmetry group, and so we did not give separate mention to this case in the table.

The "generic" orbit polytope in this example is an icosahedron with no additional affine symmetries, and the generic starting point is a point $v = (x, y, z)$ with nonzero, pairwise different coordinates.

In Chapter II, we give a precise definition of generic points. Basically, a point $v \in \mathbb{K}^d$ is not generic for a group $G \leqslant \mathrm{GL}(d, \mathbb{K})$, if either its stabilizer $G_v = \{g \in G \mid gv = v\}$ is nontrivial, or if the linear span of the orbit Gv is a proper subspace of $\mathbb{K}^d$, or if the orbit has "more" affine symmetries than a generic orbit. We will prove that the non-generic points are the zero set of some nonzero polynomials.

In order to compare affine symmetry groups of different orbit polytopes, we will identify each affine symmetry group with a permutation group on G itself. The affine symmetry group of a generic orbit polytope is always minimal among all the permutation groups arising in this way from full-dimensional orbit polytopes.

Of course, in our example with the tetrahedral rotation group, every generic orbit polytope has just T as its affine symmetry group, which corresponds to the permutation group on T defined by the left regular action of T on itself. But in our earlier example with $G = \langle t \rangle \subseteq \mathrm{GL}(2, \mathbb{R})$ generated by a rotation (see Figure 1), each generic orbit polytope has additional affine symmetries. All affine symmetry groups of generic orbit polytopes correspond to *the same* permutation group on G. Moreover, the different affine symmetry groups of generic orbit polytopes are similar. These are special cases of general results we will prove in Chapter II.

In our examples, all generic orbit polytopes are combinatorially equivalent. This is not true in general. Onn [68] gave an example of a representation of S_4, where different "generic" points yield combinatorially nonisomorphic orbit polytopes. (The points termed "generic" by Onn are certainly generic in our sense, but not conversely.) In Onn's examples, S_4 acts on $\mathbb{R}^6$ by permuting coordinates, yielding 5-dimensional orbit polytopes. The corresponding representation of S_4 is the direct sum of three different representations, one of them trivial. In view of this example, Onn remarked that a representation being multiplicity free is not enough to have a trivial polytope stratification. But as we will see in Chapter II, there are cases where in fact all generic orbit polytopes are even affinely equivalent, namely when the multiplicities of the occurring irreducible constituents of a representation are as large as possible. (The multiplicities are bounded from above by the requirement that there are full-dimensional orbit polytopes. If some multiplicity of an irreducible constituent is too large, then every G-orbit will only span a proper G-invariant subspace.) This is somewhat contrary to the intuition suggested by Onn's remark.

A classical situation where all generic orbit polytopes are combinatorially equivalent is that of finite reflection groups. Indeed, here a point can be generic only if it does not belong to any of the "mirrors" of the reflection group (that is,

the hyperplanes fixed by the reflections), and all such points yield combinatorially equivalent orbit polytopes. Orbit polytopes of finite reflection groups are called *(generalized) permutahedra* [17, Chapter 14]. The geometrical structure is nicely related to the geometry of the Coxeter chamber complex. More generally, the combinatorial type of an orbit polytope $\mathrm{P}(G, v)$ depends only on the set of reflection hyperplanes that contain v [30, Proposition 3].

As already said, we will show that the affine symmetry group of a generic orbit polytope is minimal among the affine symmetry groups of full-dimensional orbit polytopes under the same group G (when viewed as permutation groups on G). As our example $G = T$ shows, no such thing is true for the combinatorial symmetry groups. Indeed, in our example, the combinatorial symmetry groups of the generic orbit polytopes have maximal size. Also notice that there is no containment between the groups TO (or $\pm O$) and $\pm I$. On the other hand, there are examples where the generic orbit polytopes have also minimal combinatorial symmetry group, for example the cube rotation group O. Here the generic orbit polytope is a snub cube (where some of the triangle faces are in general not regular). The combinatorial symmetry group of the snub cube is again only the cube rotation group.

In view of Babai's question mentioned above, it seems natural to ask which finite groups can appear as the combinatorial automorphism group of a polytope and act transitively on the vertices. In our example with $G = T$, all orbit polytopes have more combinatorial automorphisms than $T \cong A_4$, and thus one might wonder whether A_4 appears as combinatorial automorphism group of some orbit polytope at all. (It is known that A_4 is not isomorphic to the automorphism group of a vertex transitive graph.) But some of the orbit polytopes of A_4 in dimension 5 have indeed combinatorial symmetry group A_4.

Most of the deeper results in Chapters II and IV depend on the module theoretic view of representation theory. This viewpoint was introduced by Emmy Noether in 1929 [67], thereby creating a very effective conceptual framework for representation theory. Nowadays, this viewpoint is of course commonplace. Recall that the group algebra $\mathbb{K}G$ of a (finite) group G over the field $\mathbb{K}$ is by definition the set of formal sums

$$\sum_{g \in G} r_g g, \quad r_g \in \mathbb{K},$$

together with component-wise addition and multiplication extended distributively from multiplication in the group. Any representation $D\colon G \to \mathrm{GL}(V)$, where V is a vector space over $\mathbb{K}$, endows V with the structure of a left module over the group algebra $\mathbb{K}G$, by defining $\sum_g r_g g \cdot v = \sum_g r_g D(g)v$. Conversely, any left $\mathbb{K}G$ module V defines a representation $D\colon G \to \mathrm{GL}(V)$, where $D(g)\colon V \to V$ is the map $v \mapsto gv$. Similar representations correspond to isomorphic $\mathbb{K}G$-modules and conversely [49].

Let V be a left $\mathbb{K}G$-module and $v \in V$. The $\mathbb{K}$-subspace $\mathrm{Span}(Gv) = \mathrm{Span}\{gv \mid$

$g \in G\}$ generated by the G-orbit of v equals

$$\mathrm{Span}(Gv) = \{\sum_{g\in G} r_g gv \mid r_g \in \mathbb{K}\} = \{av \mid a \in \mathbb{K}G\} = \mathbb{K}Gv.$$

This is the *cyclic* $\mathbb{K}G$-module generated by v. So in order to study the linear symmetries of G-orbits, we need to consider only cyclic $\mathbb{K}G$-modules.

We can view a permutation $\pi \in \mathrm{Sym}(G)$ as a linear map on the group algebra. Then whether π represents a linear symmetry of one or all generic orbits $Gv \subseteq V$ is equivalent to π preserving certain left ideals of $\mathbb{K}G$.

In the case where $\mathbb{K}$ has characteristic zero, the group algebra $\mathbb{K}G$ is semisimple by Maschke's theorem, and left ideals have complements. Any cyclic $\mathbb{K}G$-module is then isomorphic to a left ideal. It turns out that a left ideal and its complement have the same generic symmetry group. This is related to Gale duality.

A special place is taken by cyclic modules which are isomorphic to two-sided ideals of $\mathbb{K}G$. These are exactly the $\mathbb{K}G$-modules, which are isomorphic to a module of the form $\mathrm{Span}(D(G))$, where $D\colon G \to \mathrm{GL}(V)$ is some representation. In particular, for $\mathbb{K} = \mathbb{R}$ the affine symmetries of generic orbit polytopes in such a module are in fact the affine symmetries of a representation polytope. We will show how to determine the permutations of G corresponding to the generic symmetries from the character of G on I, where I is the ideal of $\mathbb{K}G$ which is isomorphic to $\mathrm{Span}(D(G))$ as left $\mathbb{K}G$-module. (In general, the character on I is not the same as the character of the representation D.)

Computing the affine symmetry group of a representation polytope can be viewed as a *linear preserver problem*. A *linear preserver problem* is the problem of determining the set of linear transformations of $\mathbf{M}_n(\mathbb{K})$ that map a given subset $G \subseteq \mathbf{M}_n(\mathbb{K})$ to itself, where $\mathbf{M}_n(\mathbb{K})$ denotes the ring of $n \times n$-matrices with entries in $\mathbb{K}$. More generally, one may look for linear transformations which preserve certain invariants of matrices, like the determinant or the rank. Linear preserver problems have already been studied for various specific subsets G, usually infinite subsets like the set of all singular matrices. We refer the reader to the nice overview by Li and Pierce [53]. In a few cases, linear preservers of finite matrix groups G were studied, in particular when G is a finite irreducible reflection group [52, 54, 55].

Finally, in Section 10 of Chapter II, we show how to determine the generic orbit symmetries for a cyclic module in characteristic zero from the decomposition of the character of V into its irreducible constituents. In a sense, this result answers Question 2.1(c) above, but the answer is technical. However, the answer shows that for large classes of finite groups, it is true that for "most" representations $D\colon G \to \mathrm{GL}(V)$, we have $\mathrm{GL}(Gv) = D(G)$ for generic points $v \in V$.

4. Groups with a nontrivial ideal kernel

The main result of Chapter II, Section 10, and the desire to answer Babai's Question (d) yield a purely representation theoretical problem. Let $\mathbb{K}$ be a field of characteristic 0 and G a finite group. By Maschke's theorem, the group algebra $\mathbb{K}G$ is semisimple. There are only a finite number of non-isomorphic simple left $\mathbb{K}G$-modules, say $S_1, \ldots, S_r$ [50, Ch. XVII, §4]. By the general Wedderburn-Artin theory of semisimple rings and modules, we can write

$$\mathbb{K}G \cong d_1 S_1 \oplus \cdots \oplus d_r S_r \quad \text{with} \quad d_i \in \mathbb{N}.$$

A module V has the form $V = \mathbb{K}Gv$ for some $v \in V$, if and only if it is isomorphic to a submodule (that is, a left ideal) of the regular module $\mathbb{K}G$, and thus $V \cong m_1 S_1 \oplus \cdots \oplus m_r S_r$ with $m_i \leqslant d_i$ for all i.

Now let V be the module defined by

$$V := \bigoplus_{i\colon 1<d_i} S_i.$$

(If $d_i = 1$ for all i, then $V = \{0\}$.) If the action of G on V is faithful, then it follows from the main result of Chapter II, Section 10, that $\mathrm{GL}(Gv) = G$ for generic points $v \in V$. In the case $\mathbb{K} = \mathbb{R}$, this means that G is isomorphic to the affine symmetry group of an orbit polytope.

In general, we define $\mathrm{NKer}_{\mathbb{K}}(G)$ as the kernel of G on this particular module V. Thus when $\mathrm{NKer}_{\mathbb{K}}(G) = \{1\}$, then $G = \mathrm{GL}(Gv)$ for generic $v \in V$, and usually also for generic v's in certain other cyclic modules. In particular, when $\mathrm{NKer}_{\mathbb{R}}(G) = \{1\}$, then G is isomorphic to the affine symmetry group of an orbit polytope.

Thus we are led to the problem of classifying finite groups G with $\mathrm{NKer}_{\mathbb{K}}(G) \neq \{1\}$. (If $\mathrm{NKer}_{\mathbb{K}}(G) \neq \{1\}$, then it may still happen that $G = \mathrm{GL}(Gv)$ for some other $\mathbb{K}G$-module U and some $v \in U$.) The content of Chapter III is the classification of finite groups G with $\mathrm{NKer}_{\mathbb{R}}(G) \neq \{1\}$ or $\mathrm{NKer}_{\mathbb{Q}}(G) \neq \{1\}$.

Let us further elaborate on the meaning of the numbers d_i. By the Wedderburn-Artin structure theory of semisimple rings, we have that

$$\mathbb{K}G \cong \mathbf{M}_{d_1}(D_1) \times \cdots \times \mathbf{M}_{d_r}(D_r),$$

where $D_i := \mathrm{End}_{\mathbb{K}G}(S_i)$ is a division ring (by Schur's lemma). We also have $d_i = \dim_{D_i}(S_i)$.

When $\mathbb{K} = \mathbb{C}$, or more generally when $\mathbb{K}$ is algebraically closed, or just a *splitting field* for G, then

$$\mathbb{K}G \cong \mathbf{M}_{d_1}(\mathbb{K}) \times \cdots \times \mathbf{M}_{d_r}(\mathbb{K}).$$

(By an important theorem of Brauer [48, Theorem 10.3], a field $\mathbb{K}$ is already a splitting field for G when it contains a primitive $|G|$-th root of unity.) In this case, it follows that all d_i's are 1 if and only if G is abelian. It is also not difficult to see, using the orthogonality relations of character theory, that $\mathrm{NKer}_{\mathbb{C}}(G) \neq \{1\}$ if and only if G is (nontrivial) abelian (this is Corollary 3.3 in Chapter III). It follows that every nonabelian finite group is isomorphic to a subgroup of $\mathrm{GL}(d, \mathbb{C})$ that is the setwise stabilizer of some orbit in $\mathbb{C}^d$. (For abelian groups, the problem is open. We conjecture that only finitely many abelian groups can not be realized in this way.)

For general fields $\mathbb{K}$, all multiplicities $d_i = 1$ if and only if $\mathbb{K}G$ is a direct product of division rings. For other fields than $\mathbb{C}$, there exist non-abelian groups with that property. For example, when $G = Q_8$, the quaternion group of order 8, then

$$\mathbb{R}Q_8 \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H},$$

where $\mathbb{H}$ denotes Hamilton's skew field of the quaternions.

The finite groups G, such that $\mathbb{Q}G$ is a direct product of division rings, have been classified by Sehgal [76]: We have

4.1 Theorem (Sehgal 1975). *Let G be a finite group.*

(i) *$\mathbb{Q}G$ is a direct product of division rings if and only if G is abelian or $G \cong Q_8 \times (C_2)^r \times A$, where A is an abelian group of odd order and such that the multiplicative order of 2 modulo $|A|$ is odd.*

(ii) *$\mathbb{R}G$ is a direct product of division rings if and only if G is abelian or $G \cong Q_8 \times (C_2)^r$.*

(Statement (ii) does not appear in Sehgal's paper [76], but follows easily from Sehgal's methods or directly. See Corollary 9.3 in Chapter II.)

But it is also possible that some of the multiplicities d_i are greater than 1, but $\mathrm{NKer}_{\mathbb{K}}(G) \neq \{1\}$ nonetheless. For example, let G be the group of order 12 described by generators and relations as follows:

$$G := \langle a, b \mid a^4 = b^3 = 1, a^{-1}ba = b^{-1} \rangle.$$

Then one can show that

$$\mathbb{R}G \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C} \times \mathbb{H} \times \mathbf{M}_2(\mathbb{R}).$$

Thus there is only one simple module S which occurs with multiplicity $d = 2 > 1$ in the regular module $\mathbb{R}G$. On this module, a^2 acts trivially, and so S can in fact be seen as a module for $G/\langle a^2 \rangle \cong \mathrm{S}_3$. It turns out that G is not the affine symmetry group of any orbit polytope. (This follows also from Babai's classification, since G is dicyclic.)

Another example is the group $G = Q_8 \times C_4$. Again, $\mathrm{NKer}_{\mathbb{R}}(G) \neq \{1\}$. However, this group can be realized as symmetry group of an orbit polytope in dimension 10.

Fortunately, it turns out that the groups with $\mathrm{NKer}_{\mathbb{Q}}(G) \neq \{1\}$ and the groups with $\mathrm{NKer}_{\mathbb{R}}(G) \neq \{1\}$ can be classified, and this is what we do in Chapter III. It turns out that $\mathrm{NKer}_{\mathbb{K}}(G)$ is always contained in the intersection of all nonnormal subgroups of G. Finite groups where this intersection is nontrivial have been classified by Blackburn in 1966 [14], and we use this classification. It turns out that the proof for the real numbers is not very difficult or deep, and one could avoid Blackburn's classification (which itself is also not particularly difficult). On the other hand, the proof for the rational numbers is quite long and depends on some deep facts about Schur indices.

Let $\chi \in \operatorname{Irr} G$ be an irreducible character. There is a unique factor $\mathbf{M}_{d_i}(D_i)$ from the decomposition of $\mathbb{K}G$ as above, on which χ does not vanish. Then the center of D_i is isomorphic to the field $\mathbb{K}(\chi)$ generated by the values of χ, and the dimension of D_i over its center is a square of some number $m = m_{\mathbb{K}}(\chi)$, that is, $|D_i : \mathbf{Z}(D_i)| = m^2$. This number is called the *Schur index* of χ (over $\mathbb{K}$). It can also be characterized as the smallest integer m such that $m\chi$ is afforded by a representation with entries in $\mathbb{K}(\chi)$. We always have $\chi(1) = md_i$, and so $d_i = 1$ if and only if $\chi(1) = m$.

When G is a finite nonabelian group with $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$, then G has at least one irreducible character $\chi \in \operatorname{Irr} G$ with $\chi(1) = m_{\mathbb{Q}}(\chi) > 1$. This means that the corresponding block in the decomposition of $\mathbb{Q}G$ into simple algebras is a division ring. Thus $\mathbb{Q}G$ has a central idempotent e such that $\chi(e) = \chi(1)$ and $\mathbb{Q}Ge \cong D$ is a division ring. In particular, $G/\operatorname{Ker}(\chi)$ is isomorphic to a finite subgroup of the multiplicative group D^*. Finite groups which appear as subgroups of the multiplicative group of a division ring have been classified by Amitsur [1]. We do not use Amitsur's classification, but of course the groups G with $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$ are closely related to finite subgroups of division rings. For example, the smallest nonabelian group of *odd* order that appears as a subgroup of some division ring is the group G of order 63 which can be described by generators and relations as follows:

$$G = \langle a, b \mid a^9 = b^7 = 1,\ a^{-1}ba = b^2 \rangle.$$

(Previously, in 1953, Herstein [41] had conjectured that a finite multiplicative subgroup of a division ring which has odd order, is necessarily cyclic. The above G is the smallest counterexample to this conjecture.) It turns out that $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$ for this group G, and that G can not be realized as the affine symmetry group of an orbit polytope with *integral* (or *rational*) vertices. The group G *is* isomorphic to the affine symmetry group of an orbit polytope (in dimension 6), some of the vertices of such a polytope have necessarily irrational coordinates.

Brauer [18] showed that every positive integer occurs as the Schur index of

some irreducible character of some finite group. The groups used by Brauer to achieve this are metacyclic groups which have an irreducible character χ with $\chi(1) = m_{\mathbb{Q}}(\chi) = n$, for any given n. The group G of order 63 displayed above is an example of such a group. (In particular, Brauer almost surely knew already in 1930 that G is isomorphic to a subgroup of the multiplicative group of a division ring.)

For the classification of groups G with $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$, and in particular in order to see that $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$ for certain groups, we need several nontrivial facts about Schur indices and division algebras. For example, we use that Schur indices can be computed "locally", that is, by computing Schur indices over the fields of p-adic numbers and over the reals. To verify that certain characters have nontrivial Schur index, we use a result by Benard [12] which ultimately relies on modular representation theory. However, the reader can view these results as black boxes, if not familiar with the tools needed for their proofs.

The classification results of Chapter III then allows us to classify also the affine symmetry groups of orbit polytopes, and of orbit polytopes with rational (or integer) coordinates.

5. Core points

Recall that a **lattice polytope** is a polytope $P \subset \mathbb{R}^d$ whose vertices have coordinates in $\mathbb{Z}$. More generally, we could assume that some other lattice $\Lambda \subseteq \mathbb{R}^d$ is given, but we will not need this added generality here. A lattice polytope P is called **lattice-free**, if $P \cap \mathbb{Z}^d = \mathrm{Vert}(P)$. (Lattice-free polytopes are sometimes also called *empty lattice polytopes* [37, 75].) The theory of lattice polytopes, and of lattice points contained in polytopes, has connections to representation theory, number theory, commutative algebra, algebraic geometry, statistics, computer science and of course linear optimization. (For examples, see the papers in the Snowbird 2006 conference proceedings [11].)

Now let $G \leqslant \mathrm{GL}(d, \mathbb{Z})$ be a finite group. Often we will assume that G is a group of permutation matrices. Then for $v \in \mathbb{Z}^d$, the orbit polytope $\mathrm{P}(G, v)$ is of course a lattice polytope. We call v a **core point** (with respect to G) if the orbit polytope $\mathrm{P}(G, v)$ is lattice-free.

Core points are relevant to integer linear optimization: suppose we are given an integer linear program of the form

$$Ax \leqslant b, \quad c^t x \to \max \quad (x \in \mathbb{Z}^d), \tag{ILP}$$

and suppose that this problem is invariant under some finite group $G \leqslant \mathrm{GL}(d, \mathbb{Z})$. (This means that for all $g \in G$ we have $A(gx) \leqslant b$ if and only if $Ax \leqslant b$, and $gc = c$.) If we forget about the requirement $x \in \mathbb{Z}^d$, then (ILP) has optimal solutions in the

fixed space of G in $\mathbb{R}^d$,

$$\mathrm{Fix}_{\mathbb{R}^d}(G) := \{v \in \mathbb{R}^d \mid gv = v \text{ for all } g \in G\}.$$

(This is easy to see: If $x \in \mathbb{R}^d$ is optimal, then every element gx in the G-orbit is optimal. Thus the average $(1/|G|)\sum_g gx$ is optimal, too, and is in the fixed space.) There may be no optimal integral solutions in the fixed space, however. Instead, optimal integral solutions can be found among the core points [39, Theorem 4].

Core points were first introduced by R. Bödi, K. Herr and M. Joswig [15] with a different definition in the case where G is the alternating or symmetric group on d elements. Bödi, Herr and Joswig determined all core points of $G = A_d$ or S_d. The concept was generalized to arbitrary permutation groups by K. Herr, T. Rehn and A. Schürmann [39], who showed how core points can be used in integer optimization in certain cases. Both Herr and Rehn studied core points extensively in their doctoral theses [38, 72]. Some of their results are contained in another joint paper with A. Schürmann [40].

It is clear that when z is a core point for G and $t \in \mathbb{Z}^d$ is fixed by all of G, then $\mathrm{P}(G, z+t) = \mathrm{P}(G, z)+t$ and $z+t$ is also a core point. In this situation, let us call z and $z+t$ **translation equivalent**. Herr, Rehn and Schürmann [40] showed that when $G \leqslant \mathrm{S}_d$ is a permutation group acting transitively on the 2-subsets of $\{1, \ldots, d\}$, then there are only finitely many core points up to translation equivalence. They conjectured that there are infinitely many core points up to translation equivalence for all other transitive permutation groups, and showed this in two different special cases.

Here we study a natural generalization of translation equivalence. Namely, suppose that $n \in \mathbf{N}_{\mathrm{GL}(d,\mathbb{Z})}(G)$, the normalizer of G in $\mathrm{GL}(d, \mathbb{Z})$. Then one can easily show that $\mathrm{P}(G, nv) = n\,\mathrm{P}(G, v)$, and in particular, when $z \in \mathbb{Z}^d$ is a core point, then nz is also a core point. This leads to the notion of **normalizer equivalence**, which coarsens translation equivalence.

On the one hand, this sheds new light on the above mentioned problem: Namely, in many (but not all) cases, the new equivalence classes contain infinitely many points up to translation. In these cases, we see thus immediately that there are infinitely many core points up to translation.

On the other hand, we show that when $\mathbb{Q}^d/\,\mathrm{Fix}_{\mathbb{Q}^d}(G)$ is simple as a module over $\mathbb{Q}G$, then there are only finitely many core points up to normalizer equivalence. Our conjecture is that in all other cases, there are infinitely many core points up to normalizer equivalence. This generalizes the conjecture of Herr, Rehn and Schürmann, which remains open in general. (There are infinitely many lattice-free polytopes, not necessarily symmetric, up to a suitable equivalence relation. Indeed, Barany and Kantor [5] showed that the number of lattice-free simplices of dimension d and volume at most v, up to translations and $\mathrm{GL}(d, \mathbb{Z})$-transformations, is of magnitude v^{d-1}.)

Permutation groups G such that $\mathbb{Q}^d/\operatorname{Fix}_{\mathbb{Q}^d}(G)$ is irreducible were studied by Dixon [28], who called these groups **QI-groups**. Dixon's paper contains first steps towards a classification of QI-groups which are not 2-transitive. To complete this classification, one would very likely have to use the classification of the finite simple groups, as there are some nonsolvable examples of such groups (namely, $\mathrm{PSL}(2, 2^k)$ with $2^k - 1$ prime in a permutation representation of degree $d = 2^{k-1}(2^k - 1)$).

When $d = p$ is a prime, then any transitive group $G \leqslant \mathrm{S}_p$ is a QI-group. However, by a celebrated theorem of Burnside (which we mentioned already at the beginning of this introduction), either G is 2-transitive, or G is permutation similar to a proper subgroup of $\mathrm{AGL}(1, \mathbb{F}_p)$. In the first case, there are only finitely many core points up to translation equivalence, by the aforementioned result of Herr, Rehn and Schürmann. In the second case, the structure of G is already quite restricted, by Burnside's result. (Burnside proved his result by using characters [20, §251]. Perhaps the most direct proof is due to P. Müller [66], who also gives references to some other proofs.)

The easiest example of a QI-group is when $G = C_p$ is generated by a p-cycle (as permutation group), where p is a prime as before. Then the orbit polytopes of G are $(p-1)$-dimensional simplices, and thus in particular trivial from the viewpoint of Chapter II. But this is not true from the viewpoint of integer symmetries. The different orbit polytopes $\mathrm{P}(G, z)$ have all the same affine symmetry group, but not the same "lattice symmetries", that is, (affine) symmetries that also preserve the lattice $\mathbb{Z}^d$, and so are described by $\mathrm{GL}(p, \mathbb{Z})$-matrices. On the other hand, normalizer equivalent orbit polytopes have of course similar lattice preserving symmetry groups. It remains a challenging task to extend the theory of Chapter II to the case of lattice-preserving symmetries.

These simplices are also nontrivial from the viewpoint of integer programming, as it is in general difficult to decide whether such a simplex is lattice free or not. Some experiments conducted by A. Schürmann show that we can generate integer linear programs from orbit polytopes of small cyclic groups of prime orders, which seem to be difficult for commercial solvers like Gurobi. The trick is to transform orbit polytopes of "easy" core points with elements of infinite order from the normalizer of $G = C_p$ in $\mathrm{GL}(p, \mathbb{Z})$. Conversely, one can try to transform an arbitrary integer linear program with C_p-symmetry into a simpler one, by using $\mathrm{GL}(p, \mathbb{Z})$-matrices in the normalizer. The idea of using $\mathrm{GL}(d, \mathbb{Z})$-matrices to transform an integer linear program is not new. In fact, it is one of the ingredients of Lenstra's celebrated proof that integer linear programs in fixed dimension can be solved in polynomial time [51]. But in the case of problems with symmetry, it is natural to choose transformations preserving the symmetry. It may also be a more efficient way of finding transformations that simplify the problem. The torsion-free part of the normalizer of a p-cycle in $\mathrm{GL}(p, \mathbb{Z})$ is a free abelian group of rank $(p-3)/2$.

6. Two properties of the Birkhoff polytope

The Birkhoff polytope B_n, the convex hull of all permutation matrices of size $n \times n$, is probably the most celebrated example of a permutation polytope (or even an orbit polytope). It is also known as assignment polytope, perfect matching polytope of $K_{n,n}$, and the polytope of doubly stochastic matrices. The last name refers to the fact that B_n contains exactly the doubly stochastic matrices, which means that every doubly stochastic matrix can be written as a linear combination of permutation matrices. This was proved by G. Birkhoff [13] in 1946, but follows also easily from earlier results of D. Kőnig from 1916 (cf. the treatment by Lovasz and Plummer [56, Theorem 1.4.13]).

The result mentioned last also yields the dual description of B_n by equalities and inequalities, and thus the facet structure of B_n (for all $n \in \mathbb{N}$). This is a very unusual thing for permutation polytopes in general. For example, the face lattice of the permutation polytope of the alternating group is unknown, and there is little hope that it can be described in any easy way. Hood and Perkinson [45] describe exponentially many facets (in n) of this polytope. And even for a cyclic permutation group, the corresponding permutation polytope can have exponentially many facets [9]. There are a few other classes of permutation groups where a description of the face lattice can be given, namely Frobenius groups [23], dihedral groups [10] and cyclic groups with at most two orbits [9]. And of course when the permutation group $G \leqslant \mathrm{S}_n$ is regular, then the corresponding permutation polytope is a simplex of dimension $n-1$. In fact, the permutation polytope is then lattice isomorphic to the standard simplex spanned by the standard basis vectors of $\mathbb{R}^n$.

On the positive side, Guralnick and Perkinson give a concrete description of the smallest face of a (general) permutation polytope containing two given elements of the underlying permutation group [36].

Although the face lattice of the Birkhoff polytope is known, many other questions remain open [70]. For example, it is an outstanding problem to find the volume of the Birkhoff polytope. On the other hand, the volumes (even the Ehrhart polynomials) of some other classes of permutation polytopes are known [19].

The first main result of Chapter VI is the determination of the combinatorial symmetry group of the Birkhoff polytope, which is in fact straightforward from knowledge of the face lattice. It turns out that the Birkhoff polytope has only those symmetries that a representation polytope necessarily has: all combinatorial symmetries are induced by multiplications with permutation matrices from the left or the right, or by combining this with matrix transposition. (In the language of the linear preserver literature, these are *standard transformations* [53].) Thus all combinatorial symmetries of B_n are in fact isometries, and preserve the lattice. In terms of the standard basis of the space of matrices, all symmetries are described by permutation matrices. Thus for the Birkhoff polytope, all the symmetry groups

which we introduced so far coincide.

The linear symmetry group of the Birkhoff polytope has already been determined in the literature [54, 55], as an example of a linear preserver problem.

The other main result of Chapter VI confirms a conjecture of Baumeister, Haase, Nill and Paffenholz [8]. The result says that when P is some representation polytope of a faithful representation $D\colon G \to \mathrm{GL}(d,\mathbb{R})$ (that is, $P = \mathrm{conv}\{D(g) \mid g \in G\}$), and if P is combinatorially equivalent to the Birkhoff polytope B_n, then there is a group isomorphism $\alpha\colon S_n \to G$, such that $D \circ \alpha$ and the standard permutation representation of S_n have the same nontrivial irreducible constituents. (There is an exception for $n = 3$.) This is a uniqueness property of the Birkhoff polytope, and is surprising insofar as in general, one can not reconstruct a finite group from a permutation polytope. Of course, if P is affinely (or combinatorially) equivalent to the convex hull of some finite matrix group G, then the affine (or combinatorial) symmetry group of P contains a subgroup isomorphic with G. Since we may multiply with elements of G from the left or the right, we have in fact two subgroups (maybe the same) which are isomorphic with G, act regularly on the vertices of P, and centralize each other. In general, this is not enough to determine G up to isomorphism, as can be seen from the example of a simplex. Another key ingredient in our proof is the fact that $S_n \times S_n$ contains only one pair of regular, mutually centralizing subgroups, namely $\{S_n \times 1, 1 \times S_n\}$, when $n > 3$. To see this, we use a very elementary method found by Chermak and Delgado [22] in 1989.

7. Realizations of abstract regular polytopes

Peter McMullen has developed a theory of realizations of abstract regular polytopes [60, 61, 62, 63]. Actually, the theory generalizes to a theory of "realizations of transitive G-sets", as already pointed out by McMullen [62, Remark 2.1]. So let G be a finite group and Ω a transitive G-set.

A **realization** of (G,Ω) is a homomorphism of G-sets $A\colon \Omega \to V$, where V is an euclidean vector space equipped with an action of G by orthogonal maps. In other words, we are given a representation $D\colon G \to \mathbf{O}(V)$. Thus we have $A(g\omega) = D(g)A(\omega)$ for all $\omega \in \Omega$ and $g \in G$. (We should mention that in Chapter VII, we write all maps and G-actions *on the right*, other than in the rest of this thesis. So the last conditions becomes $(\omega g)A = \omega AD(g)$ for all $\omega \in \Omega$, $g \in G$. We are thereby following the convention used by McMullen in his papers on the topic. To keep this introduction consistent, we continue to write maps and group actions an the left for the rest of the introduction.)

The group G is usually assumed to be the automorphism group of an abstract regular polytope [64] with Ω as vertex set, and then realizations are called realizations of the abstract regular polytope.

The study of realizations of G-sets can be seen as the study of all orbit polytopes of a finite group G with a given subgroup H stabilizing one of the vertices. This is related to Chapter II, where we study all orbit polytopes of a given finite group, usually in a given $\mathbb{R}G$-module. Probably one can generalize the definitions of Chapter II to the situation, where one studies all orbit polytopes in a given $\mathbb{R}G$-module V, such that a given subgroup H stabilizes a vertex. Of course, this is only interesting when $\mathrm{Fix}_V(H) \neq \{0\}$.

A natural equivalence relation is defined for realizations of a fixed G-set Ω: Namely, $A_1 \colon \Omega \to V_1$ and $A_2 \colon \Omega \to V_2$ are called **congruent**, if there is a linear isometry σ from the linear span of $\{A\omega \mid \omega \in \Omega\}$ into V_2 such that $\sigma \circ A_1 = A_2$. The congruence classes of such realizations (and the corresponding orbit polytopes) form a pointed convex cone, the realization cone.

The relation of congruence corresponds to the relation of affine G-equivalence which we introduce in Chapter II (see Definition 6.1 there), where σ is only an affine isomorphism. This means that we further identify orbit polytopes in McMullen's realization cone. For example, the interior of the realization cone consists of non-congruent simplices, but these are all affinely equivalent. The isometry group of most of the simplices is usually just G (exceptions are when G is abelian of exponent greater than 2, or generalized dicyclic), while the affine symmetry group is the full symmetric group on Ω.

The paper, which is reproduced here as Chapter VII, arose initially from an attempt to understand McMullen's papers and theory from a more representation theoretical viewpoint. (McMullen's arguments are more in a geometrical spirit.) In particular, we prove a result on the structure of the realization cone. In part, this corrects a mistake in the proof of a corresponding result of McMullen and Monson [63], and in part this just reproves a structure theorem of McMullen. To be more specific, let $\mathbb{R}\Omega$ be the permutation module corresponding to the G-set Ω. Recall that $\mathbb{R}\Omega$ is the set of formal sums

$$\mathbb{R}\Omega := \{\sum_{\omega\in\Omega} r_\omega \omega \mid r_\omega \in \mathbb{R}\},$$

so that Ω can be viewed as a basis of $\mathbb{R}$. The group action of G on $\mathbb{R}\Omega$ is induced by the action of G on Ω, namely $g \cdot \sum_\omega r_\omega \omega := \sum_\omega r_\omega g\omega$. We can write $\mathbb{R}\Omega$ as a direct sum of simple $\mathbb{R}G$-modules:

$$\mathbb{R}\Omega \cong m_1 S_1 \oplus \cdots \oplus m_k S_k,$$

with natural numbers m_i, and where the different S_i's are non-isomorphic. To each isomorphism class of simple modules S corresponds a subcone $\mathcal{RC}_S(\Omega)$ of the realization cone $\mathcal{RC}(\Omega)$, and $\mathcal{RC}(\Omega)$ is the direct product of these subcones. Originally, this was proved by McMullen [60, Theorem 16], in the situation where

G is the automorphism group of an abstract regular polytope with vertex set Ω, and we reprove it in Chapter VII (for arbitrary G-sets Ω).

But the structure and the dimension of $\mathcal{RC}_S(\Omega)$ was described incorrectly by McMullen in the first of his series of papers [60], and also in the second (joint with Barry Manson) [63]. We correct the description in Chapter VII. It turns out that the subcone $\mathcal{RC}_{S_i}(\Omega)$ is isomorphic to $m_i \times m_i$-matrices of the form AA^* with entries either in $\mathbb{R}$, in $\mathbb{C}$ or in $\mathbb{H}$ (the quaternions). Here m_i is the multiplicity of S_i in $\mathbb{R}\Omega$, as introduced in the decomposition above. In other words, we have hermitian positive semidefinite matrices over $D = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. The division ring D is determined by $D := \mathrm{End}_{\mathbb{R}G}(S_i)$. This is a division ring by Schur's lemma, and thus either $D = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$ by a celebrated theorem of Frobenius.

In Section 4, we construct counterexamples to a result of Herman and Monson. This result was a consequence of the aforementioned errors. Since the result was stated for automorphism groups of abstract regular polytopes, our counterexamples must be objects of this kind, too.

Abstract regular polytopes are certain purely combinatorial objects, namely partially ordered sets which share certain properties with the face lattice of a regular polytope [64]. Abstract regular polytopes can also be defined in purely group theoretical terms by certain properties of their automorphism groups, which leads to the notion of *string C-groups*. These groups generalize Coxeter groups whose Coxeter diagram is a string. Our counterexamples realize projective special linear groups $\mathrm{PSL}(2, p)$ as automorphism groups of abstract regular polytopes, and we show that when $p \equiv -1 \mod 4$, then there is some simple module S with $\mathrm{End}_{\mathbb{R}G}(S) = \mathbb{C}$ and multiplicity m which is large when p is large. Our proof uses one of the irreducible constituents of the *Weil representation*[46, 71] of $\mathrm{SL}(2, p)$.

Other sections of Chapter VII consider relations between McMullen's theory and other aspects of representation theory, for example between McMullen's cosine vectors and spherical functions in the theory of Gelfand pairs [21]. In the context of finite groups, a *Gelfand pair* is just a group G with a subgroup $H \leqslant G$ such that the permutation module of G on the cosets of H in G is multiplicity free. The realization cone is then polyhedral, and McMullen's cosine vectors correspond to the spherical functions associated with the Gelfand pair (G, H).

8. Contributions to this thesis

To meet the requirements of the habilitation regulation, I have to specify my own contributions to the joint papers contained in this thesis. The references [FL1, FL2] appear in revised form in Chapters II and IV, while all other papers appear unchanged, except for occasional cross references.

- **Chapters II and IV** contain material from the references [FL1] and [FL2].

The material is slightly revised here, since the second of these papers repeated some results from the first paper under more general conditions. Specifically, Sections 1 to 3, 6, 8 and 9 from Chapter II and Section 1 in Chapter IV contain material from our first paper [FL1], while Sections 7 and 10 in Chapter II and Sections 2 and 3 in Chapter IV follow the second paper [FL2]. Sections 4 and 5 in Chapter II follows more the approach in our second paper [FL2], but the material is present in both papers, in less general form in the first one. Finally, Section 4 of Chapter IV is an updated and extended version of the last section of [FL1], and contains some open questions and conjectures. The material presented here in Chapter II, Sections 1 to 3, 6, 8 and 9, and in Chapter IV, Sections 2 and 3, is largely due to me. Most of the ideas in Sections 7 and 10 of Chapter II are due to my coauthor. The material in the present Sections 4 and 5 of Chapter II was mostly developed jointly. These two sections contain material that is in both papers [FL1, FL2], in less general form in the first one.
In particular, the definition of generic points in Section 4 was developed in various discussions with my coauthor. I first proved that generic points form a Zariski-open set in the case $\mathbb{K} = \mathbb{R}$ [FL1, Corollary 4.5]. This was later generalized by my coauthor Erik Friese, to arbitrary fields. I also proved that irreducible groups are generically closed (Theorem 5.8), and how to compute generic affine symmetry groups of representation polytopes from a character (Corollary 9.6). How to compute orbit symmetries from the character in general was developed in joint discussions, but the crucial ideas here are due to my coauthor. The construction of certain orbit polytopes for elementary abelian 2-groups is due to Erik Friese, we report only the results in Chapter IV, Section 1.

- **Chapter V [LS]:** Most of this paper is my own work. The only exception is the last section on applications (Section 6). The ideas there are due to Achill Schürmann, who also conducted the experiments described there.
- **Chapter VI [BL]:** I proved Theorem B on the combinatorial symmetry group of the Birkhoff polytope. The proof of Theorem A was developed jointly in discussions with Barbara Baumeister, who suggested the problem. I prepared the final presentation of the paper, and had the idea of using the Chermak-Delgado lattice for one of the crucial lemmas.

Papers contained in this thesis

FL1. Erik Friese and Frieder Ladisch. Affine symmetries of orbit polytopes. *Adv. Math.* **288** (2016), pp. 386–425. DOI: 10.1016/j.aim.2015.10.021, arXiv: 1411.0899v3 [math.MG]. MR3436389, Zbl. 1330.52017 (cited on pp. 5, 22, 23).

L1. Frieder Ladisch. Groups with a nontrivial nonideal kernel (July 2016). arXiv: 1608.00231v3 [math.GR].

FL2. Erik Friese and Frieder Ladisch. Classification of affine symmetry groups of orbit polytopes. *J. Algebraic Combin.* (Nov. 2017). DOI: 10.1007/s10801-017-0804-0, arXiv: 1608.06539v4 [math.GR] (cited on pp. 5, 22, 23).

LS. Frieder Ladisch and Achill Schürmann. Equivalence of lattice orbit polytopes (Mar. 2017). arXiv: 1703.01152v1 [math.MG] (cited on p. 23).

BL. Barbara Baumeister and Frieder Ladisch. A property of the Birkhoff polytope (Oct. 2016). (accepted by Algebraic Combinatorics). arXiv: 1610.02077v2 [math.CO] (cited on p. 23).

L2. Frieder Ladisch. Realizations of abstract regular polytopes from a representation theoretic view. *Aequationes Math.* **90**, no. 6 (2016), pp. 1169–1193. DOI: 10.1007/s00010-016-0434-y, arXiv: 1604.07066v2 [math.MG]. MR3575585, Zbl. 06667617.

References for Chapter I

1. S. A. Amitsur. Finite subgroups of division rings. *Trans. Amer. Math. Soc.* **80** (1955), pp. 361–386. DOI: 10.1090/S0002-9947-1955-0074393-9. MR0074393(17,577c), Zbl. 0065.25603 (cited on p. 15).
2. László Babai. Symmetry groups of vertex-transitive polytopes. *Geometriae Dedicata* **6**, no. 3 (1977), pp. 331–337. DOI: 10.1007/BF02429904. MR0486080(58#5868), Zbl. 0388.05025 (cited on pp. 6, 7).
3. László Babai. Automorphism groups, isomorphism, reconstruction. In: *Handbook of Combinatorics*. Ed. by Ronald Lewis Graham, Martin Grötschel, and László Lovasz. Elsevier, Amsterdam, 1995, pp. 1447–1540. MR1373683, Zbl. 0846.05042 (cited on p. 7).
4. László Babai and Chris D. Godsil. On the automorphism groups of almost all Cayley graphs. *European J. Combin.* **3**, no. 1 (1982), pp. 9–15. DOI: 10.1016/S0195-6698(82)80003-6. MR656006, Zbl. 0483.05033 (cited on p. 7).
5. Imre Bárány and Jean-Michel Kantor. On the number of lattice free polytopes. *European J. Combin.* **21**, no. 1 (2000), pp. 103–110. DOI: 10.1006/eujc.1999.0324. MR1737330, Zbl. 0954.52015 (cited on p. 17).
6. A[lexander] I. Barvinok and A[natoly] M. Vershik. Convex hulls of orbits of representations of finite groups, and combinatorial optimization. *Func. Anal. Appl.* **22**, no. 3 (1988), pp. 224–225. DOI: 10.1007/BF01077628. MR961762(90a:20024), Zbl. 0688.20006 (cited on p. 2).
7. Alexander Barvinok and Grigoriy Blekherman. Convex geometry of orbits. In: *Combinatorial and Computational Geometry*. Ed. by Jacob E. Goodman, János Pach, and Emo Welzl. MSRI Publ. 52. Cambridge University Press, 2005, pp. 51–77. arXiv: math/0312268 [Math.MG]. MR2178312(2007a:52006), Zbl. 1096.52002 (cited on p. 2).

8. Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. On permutation polytopes. *Adv. Math.* **222**, no. 2 (2009), pp. 431–452. DOI: 10.1016/j.aim.2009.05.003, arXiv: 0709.1615 [math.CO]. MR2538016(2010j:52042), Zbl. 1185.52006 (cited on pp. 2, 20).
9. Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. Permutation polytopes of cyclic groups (Sept. 2011). arXiv: 1109.0191 [math.CO] (cited on p. 19).
10. Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. Polytopes associated to dihedral groups. *Ars Math. Contemp.* **7**, no. 1 (2014), pp. 30–38. URL: http://amc-journal.eu/index.php/amc/article/view/289. MR3029450, Zbl. 1336.52016 (cited on p. 19).
11. Matthias Beck et al., eds. *Integer Points in Polyhedra — Geometry, Number Theory, Representation Theory, Algebra, Optimization, Statistics*. AMS-IMS-SIAM Joint Summer Research Conference. (Snowbird, UT, June 11/15, 2006). Contemporary Mathematics 452. American Mathematical Society, Providence, RI, 2008. DOI: 10.1090/conm/452. MR2416261, Zbl. 1135.52001 (cited on p. 16).
12. Mark Benard. Schur indices and cyclic defect groups. *Ann. Math. (2)* **103**, no. 2 (1976), pp. 283–304. DOI: 10.2307/1971007, JSTOR: 1971007. MR0412265, Zbl. 0308.20012 (cited on p. 16).
13. Garrett Birkhoff. Tres observaciones sobre el algebra lineal. (Spanish). *Univ. Nac. Tucumán Rev. Ser. A* **5** (1946), pp. 147–151. MR0020547, Zbl. 0060.07906 (cited on p. 19).
14. Norman Blackburn. Finite groups in which the nonnormal subgroups have nontrivial intersection. *J. Algebra* **3** (1966), pp. 30–37. DOI: 10.1016/0021-8693(66)90018-4. MR0190229, Zbl. 0141.02401 (cited on p. 15).
15. Richard Bödi, Katrin Herr, and Michael Joswig. Algorithms for highly symmetric linear and integer programs. *Math. Program. Ser. A* **137**, no. 1-2 (2013), pp. 65–90. DOI: 10.1007/s10107-011-0487-6. MR3010420, Zbl. 1262.90101 (cited on p. 17).
16. Jürgen Bokowski, Günter Ewald, and Peter Kleinschmidt. On combinatorial and affine automorphisms of polytopes. *Israel J. Math.* **47**, no. 2-3 (1984), pp. 123–130. DOI: 10.1007/BF02760511. MR738163(85i:52001), Zbl. 0546.52004 (cited on p. 4).
17. Alexandre V. Borovik and Anna Borovik. *Mirrors and Reflections. The Geometry of Finite Reflection Groups*. Universitext. Springer, New York, 2010. DOI: 10.1007/978-0-387-79066-4. MR2561378(2011b:20114), Zbl. 1193.20001 (cited on pp. 2, 11).
18. Richard Brauer. Untersuchungen über die arithmetischen Eigenschaften von Gruppen linearer Substitutionen. Zweite Mitteilung. (German). *Math. Z.* **31** (1930), pp. 733–747. DOI: 10.1007/BF01246444. JFM 56.0865.04 (cited on p. 15).
19. Katherine Burggraf, Jesús De Loera, and Mohamed Omar. On volumes of permutation polytopes. In: *Discrete Geometry and Optimization*. Fields Inst. Commun. 69. Springer, New York, 2013, pp. 55–77. DOI: 10.1007/978-3-319-00200-2_5, arXiv: 1103.0039 [math.CO]. MR3156777, Zbl. 1281.52010 (cited on p. 19).

20. William Burnside. *Theory of Groups of Finite Order*. Dover Publications, New York, 2nd ed. 1955. (Unabridged republication of 2nd 1911 edition, Cambridge University Press). Zbl. 0064.25105, JFM 42.0151.02 (cited on p. 18).
21. Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli. *Harmonic Analysis on Finite Groups*. Representation Theory, Gelfand Pairs and Markov Chains. Cambridge Studies in Advanced Mathematics 108. Cambridge University Press, 2008. DOI: 10.1017/CBO9780511619823. MR2389056(2009c:43001), Zbl. 1149.43001 (cited on p. 22).
22. Andrew Chermak and Alberto Delgado. A measuring argument for finite groups. *Proc. Amer. Math. Soc.* **107**, no. 4 (1989), pp. 907–914. DOI: 10.2307/2047648. MR994774(90c:20001), Zbl. 0687.20022 (cited on p. 20).
23. John Collins and David Perkinson. Frobenius polytopes (Feb. 2011). arXiv: 1102.0988 [math.CO] (cited on p. 19).
24. John H. Conway and Derek A. Smith. *On Quaternions and Octonions. Their Geometry, Arithmetic, and Symmetry*. A K Peters, Natick, MA, 2003. MR1957212, Zbl. 1098.17001 (cited on p. 9).
25. H. S. M. Coxeter. Wythoff's construction for uniform polytopes. *Proc. London Math. Soc. (2)* **38** (1934), pp. 327–339. DOI: 10.1112/plms/s2-38.1.327. JFM 60.0898.03 (cited on p. 2).
26. H. S. M. Coxeter. *Regular Polytopes*. Dover Publications, New York, 3rd ed. 1973. MR0370327 (cited on pp. 1, 2).
27. H. S. M. Coxeter. *Regular Complex Polytopes*. Cambridge University Press, 2nd ed. 1991. MR1119304(92h:51035), Zbl. 0732.51002 (cited on p. 2).
28. John D. Dixon. Permutation representations and rational irreducibility. *Bull. Austral. Math. Soc.* **71**, no. 3 (2005), pp. 493–503. DOI: 10.1017/S0004972700038508. MR2150939(2006c:20012), Zbl. 1114.20003 (cited on p. 18).
29. Jean-Paul Doignon. Any finite group is the group of some binary, convex polytope. *Discrete Comput. Geom.* (Oct. 2017). DOI: 10.1007/s00454-017-9945-0, arXiv: 1602.02987 [math.CO] (cited on p. 5).
30. Mathieu Dutour Sikirić and Graham Ellis. Wythoff polytopes and low-dimensional homology of Mathieu groups. *J. Algebra* **322**, no. 11 (2009), pp. 4143–4150. DOI: 10.1016/j.jalgebra.2009.09.031. MR2556144(2010j:20082), Zbl. 1186.20033 (cited on p. 11).
31. Graham Ellis, James Harris, and Emil Sköldberg. Polytopal resolutions for finite groups. *J. Reine Angew. Math.* **598** (2006), pp. 131–137. DOI: 10.1515/CRELLE.2006.071. MR2270569(2008g:20117), Zbl. 1115.20041 (cited on p. 2).
32. Robert Frucht. Herstellung von Graphen mit vorgegebener abstrakter Gruppe. (German). *Compos. Math.* **6** (1939), pp. 239–250. NUMDAM: CM_1939__6__239_0. Zbl. 0020.07804, JFM 64.0596.02 (cited on p. 7).
33. Gábor Gévay. A class of cellulated spheres with non-polytopal symmetries. *Canad. Math. Bull.* **52**, no. 3 (2009), pp. 366–379. DOI: 10.4153/CMB-2009-040-7. MR2547803, Zbl. 1181.52020 (cited on p. 4).

34. C[hristopher] D. Godsil. GRRs for nonsolvable groups. In: *Algebraic Methods in Graph Theory*. (Szeged, 1978). Colloq. Math. Soc. János Bolyai 25. North-Holland, Amsterdam and New York, 1981, pp. 221–239. MR642043(83b:05069), Zbl. 0476.05041 (cited on p. 7).
35. Branko Grünbaum. An enduring error. *Elem. Math.* **64**, no. 3 (2009), pp. 89–101. DOI: 10.4171/EM/120. MR2520469, Zbl. 1176.52002 (cited on p. 2).
36. Robert M. Guralnick and David Perkinson. Permutation polytopes and indecomposable elements in permutation groups. *J. Combin. Theory Ser. A* **113**, no. 7 (2006), pp. 1243–1256. DOI: 10.1016/j.jcta.2005.11.004, arXiv: math/0503015 [math.CO]. MR2259059(2007h:05076), Zbl. 1108.52014 (cited on pp. 2, 19).
37. Christian Haase and Günter M. Ziegler. On the maximal width of empty lattice simplices. *European J. Combin.* **21**, no. 1 (2000), pp. 111–119. DOI: 10.1006/eujc.1999.0325. MR1737331, Zbl. 0966.52013 (cited on p. 16).
38. Katrin Herr. *Core Sets and Symmetric Convex Optimization*. Dissertation. Technische Universität Darmstadt, 2013. Zbl. 1291.90002 (cited on p. 17).
39. Katrin Herr, Thomas Rehn, and Achill Schürmann. Exploiting symmetry in integer convex optimization using core points. *Oper. Res. Lett.* **41**, no. 3 (2013), pp. 298–304. DOI: 10.1016/j.orl.2013.02.007. MR3048847, Zbl. 1286.90097 (cited on p. 17).
40. Katrin Herr, Thomas Rehn, and Achill Schürmann. On lattice-free orbit polytopes. *Discrete Comput. Geom.* **53**, no. 1 (2015), pp. 144–172. DOI: 10.1007/s00454-014-9638-x. MR3293492, Zbl. 1325.52010 (cited on p. 17).
41. I. N. Herstein. Finite multiplicative subgroups in division rings. *Pacific J. Math.* **3** (1953), pp. 121–126. DOI: 10.2140/pjm.1953.3.121. MR0055319, Zbl. 0050.03004 (cited on p. 15).
42. Georg Hofmann and Karl-Hermann Neeb. On convex hulls of orbits of Coxeter groups and Weyl groups. *Münster J. Math.* **7**, no. 2 (2014), pp. 463–487. DOI: 10.17879/58269762646. MR3426226, Zbl. 1347.20040 (cited on p. 2).
43. Christophe Hohlweg. Permutahedra and associahedra: generalized associahedra from the geometry of finite reflection groups. In: *Associahedra, Tamari Lattices and Related Structures*. Prog. Math. Phys. 299. Birkhäuser/Springer, Basel, 2012, pp. 129–159. DOI: 10.1007/978-3-0348-0405-9_8, arXiv: 1112.3255v1 [math.CO]. MR3221538, Zbl. 1271.52012 (cited on p. 2).
44. Christophe Hohlweg, Carsten E. M. C. Lange, and Hugh Thomas. Permutahedra and generalized associahedra. *Adv. Math.* **226**, no. 1 (2011), pp. 608–640. DOI: 10.1016/j.aim.2010.07.005. MR2735770(2012d:20085) (cited on p. 2).
45. Jeffrey Hood and David Perkinson. Some facets of the polytope of even permutation matrices. *Linear Algebra Appl.* **381** (2004), pp. 237–244. DOI: 10.1016/j.laa.2003.11.015. MR2039809, Zbl. 1103.52010 (cited on p. 19).
46. Roger E. Howe. On the character of Weil's representation. *Trans. Amer. Math. Soc.* **177** (1973), pp. 287–298. DOI: 10.1090/S0002-9947-1973-0316633-5, JSTOR: 1996597. MR0316633(47#5180), Zbl. 0263.22014 (cited on p. 22).

47. I. M[artin] Isaacs. Linear groups as stabilizers of sets. *Proc. Amer. Math. Soc.* **62**, no. 1 (1977), pp. 28–30. DOI: 10.2307/2041939. MR0427489(55#521), Zbl. 0355.20014 (cited on pp. 5, 6).
48. I. Martin Isaacs. *Character Theory of Finite Groups*. Dover, New York, 1994. (Corrected reprint of the 1976 edition by Academic Press, New York). MR1280461, Zbl. 0849.20004 (cited on p. 14).
49. Gordon James and Martin Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 2nd ed. 2001. MR1864147(2002h:20010), Zbl. 0981.20004 (cited on p. 11).
50. Serge Lang. *Algebra*. Addison-Wesley, Reading, MA, 1965. MR0197234(33#5416), Zbl. 0193.34701 (cited on p. 13).
51. H. W. Lenstra Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.* **8**, no. 4 (1983), pp. 538–548. DOI: 10.1287/moor.8.4.538. MR727410, Zbl. 0524.90067 (cited on p. 18).
52. Chi-Kwong Li and Thomas Milligan. Linear preservers of finite reflection groups. *Linear Multilinear Algebra* **51**, no. 1 (2003), pp. 49–81. DOI: 10.1080/0308108031000053648. MR1950413(2003j:20068), Zbl. 1026.15002 (cited on p. 12).
53. Chi-Kwong Li and Stephen Pierce. Linear preserver problems. *Amer. Math. Monthly* **108**, no. 7 (2001), pp. 591–605. DOI: 10.2307/2695268, JSTOR: 2695268. MR1862098, Zbl. 0991.15001 (cited on pp. 12, 19).
54. Chi-Kwong Li, Ilya Spitkovsky, and Nahum Zobin. Finite reflection groups and linear preserver problems. *Rocky Mountain J. Math.* **34**, no. 1 (2004), pp. 225–251. DOI: 10.1216/rmjm/1181069902. MR2061128(2005e:20056), Zbl. 1060.15007 (cited on pp. 12, 20).
55. Chi-Kwong Li, Bit-Shun Tam, and Nam-Kiu Tsing. Linear maps preserving permutation and stochastic matrices. *Linear Algebra Appl.* **341** (2002), pp. 5–22. DOI: 10.1016/S0024-3795(00)00242-1. MR1873605(2002i:15005), Zbl. 0998.15004 (cited on pp. 12, 20).
56. László Lovász and Michael D. Plummer. *Matching Theory*. North-Holland Mathematics Studies 121. North-Holland, Amsterdam, 1986. (Annals of Discrete Mathematics 29). MR859549(88b:90087), Zbl. 0618.05001 (cited on p. 19).
57. Nicholas McCarthy, David Ogilvie, Ilya Spitkovsky, and Nahum Zobin. Birkhoff's theorem and convex hulls of Coxeter groups. *Linear Algebra Appl.* **347** (2002), pp. 219–231. DOI: 10.1016/S0024-3795(01)00556-0. MR1899891(2003g:51012), Zbl. 1042.51011 (cited on p. 2).
58. Nicholas McCarthy, David Ogilvie, Nahum Zobin, and Veronica Zobin[a]. Convex geometry of Coxeter-invariant polyhedra. In: *Trends in Banach Spaces and Operator Theory*. (Memphis, TN, 2001). Ed. by Anna Kamińska. Contemp. Math. 321. American Mathematical Society, Providence, RI, 2003, pp. 153–179. DOI: 10.1090/conm/321/05642. MR1978815(2004e:52014), Zbl. 1042.52011 (cited on p. 2).
59. Andrew McIntyre. *Is every finite group a group of "symmetries"?* Version 2009-10-18. (Mathoverflow question). Oct. 2009. URL: http://mathoverflow.net/q/993 (visited on 2017-02-15) (cited on p. 5).

60. Peter McMullen. Realizations of regular polytopes. *Aequationes Math.* **37**, no. 1 (1989), pp. 38–56. DOI: 10.1007/BF01837943. MR986092(90c:52014), Zbl. 0676.51008 (cited on pp. 20–22).
61. Peter McMullen. Realizations of regular polytopes, III. *Aequationes Math.* **82**, no. 1-2 (2011), pp. 35–63. DOI: 10.1007/s00010-010-0063-9. MR2807032, Zbl. 1226.51005 (cited on p. 20).
62. Peter McMullen. Realizations of regular polytopes, IV. *Aequationes Math.* **87**, no. 1-2 (2014), pp. 1–30. DOI: 10.1007/s00010-013-0187-9. MR3175095, Zbl. 1327.51023 (cited on p. 20).
63. Peter McMullen and Barry Monson. Realizations of regular polytopes, II. *Aequationes Math.* **65**, no. 1-2 (2003), pp. 102–112. DOI: 10.1007/s000100300007. MR2012404(2004k:51021), Zbl. 1022.51019 (cited on pp. 20–22).
64. Peter McMullen and Egon Schulte. *Abstract Regular Polytopes*. Encyclopedia of Mathematics and its Applications 92. Cambridge University Press, 2002. DOI: 10.1017/CBO9780511546686. MR1965665(2004a:52020), Zbl. 1039.52011 (cited on pp. 20, 22).
65. R. V. Moody and J. Patera. Voronoi domains and dual cells in the generalized kaleidoscope with applications to root and weight lattices. *Canad. J. Math.* **47**, no. 3 (1995), pp. 573–605. DOI: 10.4153/CJM-1995-031-2. MR1346154(97c:17008), Zbl. 0838.52019 (cited on p. 2).
66. Peter Müller. Permutation groups of prime degree, a quick proof of Burnside's theorem. *Arch. Math. (Basel)* **85**, no. 1 (2005), pp. 15–17. DOI: 10.1007/s00013-005-1421-z. MR2155105, Zbl. 1074.20001 (cited on p. 18).
67. Emmy Noether. Hyperkomplexe Größen und Darstellungstheorie. *Math. Z.* **30** (1929), pp. 641–692. DOI: 10.1007/BF01187794. JFM 55.0677.01 (cited on p. 11).
68. Shmuel Onn. Geometry, complexity, and combinatorics of permutation polytopes. *J. Combin. Theory Ser. A* **64**, no. 1 (1993), pp. 31–49. DOI: 10.1016/0097-3165(93)90086-N. MR1239510(94j:52020), Zbl. 0789.05095 (cited on pp. 2, 10).
69. Andreas Paffenholz. New polytopes from products. *J. Combin. Theory Ser. A* **113**, no. 7 (2006), pp. 1396–1418. DOI: 10.1016/j.jcta.2005.12.008. MR2259068, Zbl. 1106.52003 (cited on p. 4).
70. Igor Pak. Four questions on Birkhoff polytope. *Ann. Comb.* **4**, no. 1 (2000), pp. 83–90. DOI: 10.1007/PL00001277. MR1763951, Zbl. 0974.52010 (cited on p. 19).
71. Amritanshu Prasad. On character values and decomposition of the Weil representation associated to a finite abelian group. *J. Analysis* **17** (2009), pp. 73–85. arXiv: 0903.1486 [math.RT]. MR2722604(2012a:11053), Zbl. 1291.11084 (cited on p. 22).
72. Thomas Rehn. *Exploring Core Points for Fun and Profit. A study of lattice-free orbit polytopes*. Dissertation. Universität Rostock, 2013. urn:nbn:de:gbv:28-diss2014-0082-2 (cited on p. 17).
73. Raman Sanyal, Frank Sottile, and Bernd Sturmfels. Orbitopes. *Mathematika* **57**, no. 2 (2011), pp. 275–314. DOI: 10.1112/S002557931100132X, arXiv: 0911.5436 [math.AG]. MR2825238(2012g:52001), Zbl. 1315.52001 (cited on p. 2).

74. Egon Schulte and Gordon Ian Williams. Polytopes with preassigned automorphism groups. *Discrete Comput. Geom.* **54**, no. 2 (2015), pp. 444–458. DOI: 10.1007/s00454-015-9710-1, arXiv: 1505.06253 [math.CO]. MR3372119, Zbl. 1357.52018 (cited on p. 5).
75. András Sebő. An introduction to empty lattice simplices. In: *Integer Programming and Combinatorial Optimization (Graz, 1999)*. 7th International IPCO Conference. (Graz, June 9/11, 1999). Ed. by Gérard Cornuéjols, Rainer E. Burkard, and Gerhard J. Woeginger. Lecture Notes in Comput. Sci. 1610. Springer, Berlin, 1999, pp. 400–414. DOI: 10.1007/3-540-48777-8_30. MR1709397, Zbl. 0949.90079 (cited on p. 16).
76. Sudarshan K. Sehgal. Nilpotent elements in group rings. *Manuscripta Math.* **15**, no. 1 (1975), pp. 65–80. DOI: 10.1007/bf01168879. MR0364417(51#671), Zbl. 0302.16010 (cited on p. 14).
77. Günter M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics 152. Springer-Verlag, New York, 1995. DOI: 10.1007/978-1-4613-8431-1. MR1311028(96a:52011), Zbl. 0823.52002 (cited on p. 3).
78. Nahum Zobin and Veronica Zobina. Coxeter groups and interpolation of operators. *Integral Equations Operator Theory* **18**, no. 3 (1994), pp. 335–367. DOI: 10.1007/BF01206296. MR1260565(94k:46157), Zbl. 0807.46085 (cited on p. 2).

Chapter II.

Linear Symmetries of Orbits and Orbit Polytopes[1]

Erik Friese and Frieder Ladisch

Abstract. Let G be a finite group acting linearly on a vector space V. For a subset $S \subseteq V$, the *linear symmetry group* $\mathrm{GL}(S)$ is defined as the set of all linear maps of the linear span of S which permute S. We develop a general theory of possible linear symmetry groups $\mathrm{GL}(Gv)$ of orbits $Gv \subseteq V$. This includes a general theory of affine symmetry groups of orbit polytopes. (An orbit polytope is the convex hull of an orbit under a finite group $G \leqslant \mathrm{GL}(d, \mathbb{R})$.)

In the case where V is the linear span of at least one orbit Gv, we define a set of *generic points* in V, which is Zariski-open in V, and show that the groups $\mathrm{GL}(Gv)$ for v generic are all isomorphic, and isomorphic to a subgroup of every symmetry group $\mathrm{GL}(Gw)$ such that V is the linear span of Gw. If the underlying characteristic is zero, "isomorphic" can be replaced by "conjugate in $\mathrm{GL}(V)$".

In the characteristic zero case, we also show how the character of G on V determines the generic symmetry group of a spanning orbit.

2010 Mathematics Subject Classification. Primary 52B15, Secondary 52B12, 05E15, 15A86, 20B25, 20C15

Keywords. Orbit polytope, group representation, affine symmetry, representation polytope, permutation polytope, linear group,

1. Introduction

Let $G \leqslant \mathrm{GL}(d, \mathbb{R})$ be a finite group. An **orbit polytope** of G is defined as the convex hull of the orbit Gv of some point $v \in \mathbb{R}^d$. We denote it by

$$\mathrm{P}(G, v) = \mathrm{conv}\{gv \mid g \in G\}.$$

The content of this chapter is motivated by studying affine symmetry groups of orbit polytopes. Recall that an **affine symmetry** of a polytope $P \subset \mathbb{R}^d$ is a bijection of P which is the restriction of an affine map $\mathbb{R}^d \to \mathbb{R}^d$. We write $\mathrm{AGL}(P)$ for the affine symmetry group of a polytope P.

Clearly, the affine symmetry group of an orbit polytope $\mathrm{P}(G, v)$ always contains the symmetries induced by G. Depending on the group and on the point v, there

[1]This chapter contains material from references [FL1] and [FL2] in slightly revised form.

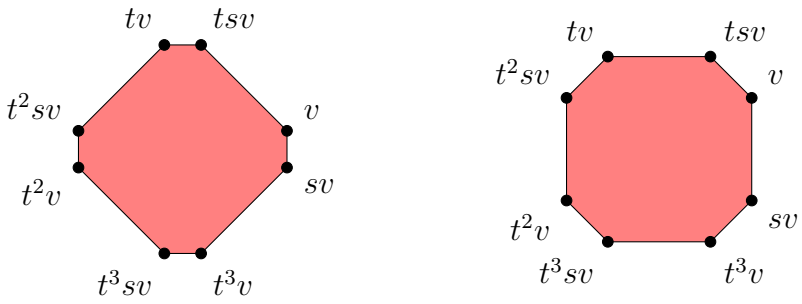

Figure 1. Two typical orbit polytopes of $D_4 = \langle t, s \rangle$, the group of the square. Both have no additional affine symmetries.

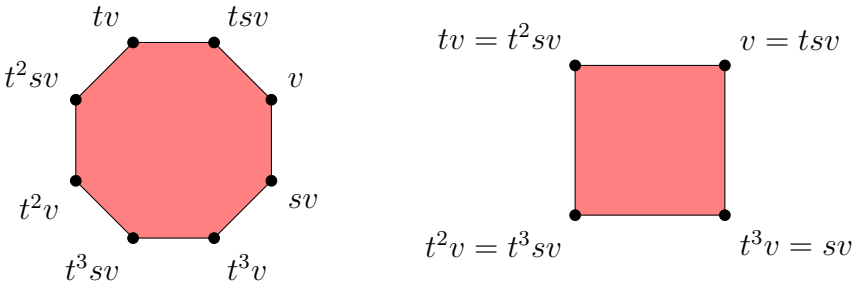

Figure 2. Two untypical orbit polytopes of $D_4 = \langle t, s \rangle$: The polytope on the left has additional affine symmetries, that on the right fewer vertices.

may be additional symmetries or not. In particular, certain symmetry groups imply additional symmetries for all orbit polytopes. In this chapter we develop a general theory to explain this phenomenon. We begin by looking at some very simple examples.

1.1 Illustrating examples

Let $G = \langle t, s \rangle \cong D_4$, the dihedral group[2] of order 8. Here t denotes a counterclockwise rotation by a right angle, and s a reflection (in the plane). Figure 1 shows two "generic" orbit polytopes. Their affine symmetry group is only the group G itself. In contrast, the orbit polytopes in Figure 2 are atypical: The first one has a larger affine symmetry group, namely the dihedral group D_8 of order 16. The other one has affine symmetry group D_4, but it has fewer vertices than the typical orbit polytope. Of course, this happens because the stabilizer of v is nontrivial. Finally, if we take for v the fixed point of the rotation, then we get a degenerate orbit polytope of dimension zero.

[2] We follow here the convention of geometers and write D_n for the group of the n-gone with $2n$ elements. Most group theorists write D_{2n} instead.

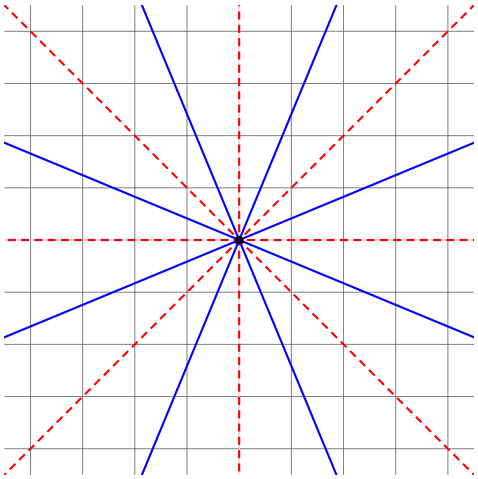

Figure 3. Exceptional points for D_4: Points with trivial stabilizer (dashed lines) or additional symmetries (solid lines).

In general, given a finite group $G \leqslant \mathrm{GL}(d, \mathbb{R})$, there may be three kinds of "exceptional" points: First, there may be points such that the orbit polytope $\mathrm{P}(G, v)$ is not full-dimensional. Let us call a point $v \in \mathbb{R}^d$ a *generating point* (for G) if $\mathbb{R}^d = \mathrm{Span}\{gv \mid g \in G\}$. If there exists a generating point, then the set of non-generating points is the zero set of some non-zero polynomials, as is not difficult to see (Lemma 4.10 below). In the example with $G = D_4$, only the origin does not generate a full-dimensional orbit polytope.

Second, there may be points v which are stabilized by some non-identity elements of G. The set of such points is a finite union of proper affine subspaces, since the fixed space of each $g \in G \setminus \{1\}$ is a proper subspace.

Finally, there may be points such that the corresponding orbit polytope has more symmetries than a "generic" orbit polytope. It is one purpose of this chapter is to make this statement more precise (see Lemma 4.14). In particular, it is not obvious in general that "almost all" orbit polytopes have the same symmetry group, and that the other ones usually have more symmetries. For example, it is known that in general orbit polytopes of the same group may have quite different face lattices, even for "generic" points [24].

In our example, the symmetry group of "almost every" orbit polytope is again G. This is not always the case. For a simple example, let $G = \langle t \rangle$, where t is a rotation by a right angle in 2-dimensional space. Then every orbit polytope is a square, and the affine symmetry group is always isomorphic to the dihedral group D_4 of order 8 (Figure 4). (Again, there is the trivial exception of the orbit of the fixed point of t.) From the first example, we know that if we take an orbit polytope of this new symmetry group, then its affine symmetry group does no longer grow for "almost all" points v. This will be seen to be a general phenomenon (Corollary 5.4).

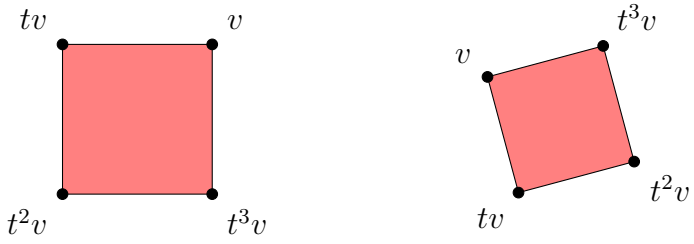

Figure 4. Two orbit polytopes of the group $G = \langle t \rangle$ of rotations preserving a square. All nontrivial orbit polytopes are affinely equivalent and have additional symmetries.

We also see that the different orbit polytopes of $G = \langle t \rangle$, as v varies, have not exactly *the same* symmetries (we have reflections at different axes), but the resulting groups are conjugate in the group of all affine isomorphisms. Actually, more is true: If we identify the vertices of an orbit polytope with the corresponding group elements, then the affine symmetry groups of all orbit polytopes induce the same permutations on G. This is true for general orbit polytopes, as will become clear in Sections 4 and 5.

1.2 Overview: generic points

Let $S \subseteq V$ be a subset of some vector space V. The **linear symmetry group** of S is the group of all linear automorphisms of the linear span of S, which map S onto itself. We denote it by $\mathrm{GL}(S)$. In other words, $\mathrm{GL}(S)$ is the setwise stabilizer of S in $\mathrm{GL}(\mathrm{Span}(S))$. Similarly, $\mathrm{AGL}(S)$ is the setwise stabilizer of S in $\mathrm{AGL}(\mathrm{Aff}(S))$. As we will see in Section 2, it is no loss of generality to replace affine symmetries by linear symmetries throughout when dealing with polytopes or finite subsets of real vector spaces. Moreover, we have $\mathrm{GL}(P) = \mathrm{GL}(\mathrm{Vert}(P))$ for any polytope P, and thus $\mathrm{GL}(\mathrm{P}(G, v)) = \mathrm{GL}(Gv)$. For this reasons, the study of affine symmetries of orbit polytopes reduces to the study of linear symmetries of orbits. This can of course be done for orbits of finite groups in vector spaces over arbitrary fields. Therefore, V will usually be a vector space over an arbitrary field $\mathbb{K}$.

In Section 4, we define a set of *generic points* for each finite subgroup $G \leqslant \mathrm{GL}(V)$, such that V is the linear span of at least one G-orbit. The set of generic points excludes the three kinds of exceptional points mentioned in the example subsection above. To identify orbits with "additional" symmetries, we proceed as follows: For each $v \in V$, we define the permutation group $\mathrm{Sym}(G, v)$ as the set of all permutations π of G such that there is a linear map $\alpha\colon V \to V$ with $\alpha(gv) = \pi(g)v$ for all $g \in G$. Thus $\mathrm{Sym}(G, v)$ contains the permutations of G corresponding to linear symmetries of the orbit Gv.

Then we define $\mathrm{Sym}(G, V)$ as the intersection of all the groups $\mathrm{Sym}(G, v)$ with v a generator of V. Finally, the set of generic points can be defined as the set of

generators v with trivial stabilizer in G and such that $\mathrm{Sym}(G, v) = \mathrm{Sym}(G, V)$. (In fact, as we will argue below, one should use a different definition of generic points when the field is finite. If V is a vector space over a finite field, then actually there may be no generic points in V.)

The orbit of a generic point is called a *generic orbit*. If $V \cong \mathbb{R}^d$ and $v \in V$ is generic, then we call $\mathrm{P}(G, v)$ a *generic orbit polytope*. We prove the following:

Theorem A. *The set of generic points is the complement of the zero set of certain non-zero polynomials. In other words, the generic points form a Zariski-open set, which is nonempty when the underlying field is infinite.*

In the examples above, the linear symmetry group of a generic orbit (polytope) has order 8 in both cases. In the case of $G = \langle t \rangle \cong C_4$, every point except the fixed point of t is generic. In the case of D_4, the non-generic points are the union of eight lines through the origin (Figure 3).

We should also mention that the exceptional points are not necessarily a finite union of proper subspaces, as is the case in our simple examples.

For every generator $v \in V$, we have a representation $D_v \colon \mathrm{Sym}(G, v) \to \mathrm{GL}(V)$, which we study in Section 5. In particular, we will show that the restrictions of D_v to $\mathrm{Sym}(G, V)$ are similar in characteristic zero. In the case of orbit polytopes, this means that the symmetry groups of generic orbit polytopes are all similar. This yields the following theorem:

Theorem B. *Let $\mathbb{K}$ be a field of characteristic 0. Suppose that $v \in V$ is generic and $w \in V$ is a generator (that is, the G-orbit of w spans V). Then $\mathrm{GL}(Gv)$ is conjugate in $\mathrm{GL}(V)$ to a subgroup of $\mathrm{GL}(Gw)$. In particular, the linear symmetry groups of generic orbits are conjugate in $\mathrm{GL}(V)$.*

It follows that every finite group $G \leqslant \mathrm{GL}(V)$ defines a unique conjugacy class of subgroups of $\mathrm{GL}(V)$ containing the groups $\widehat{G} = \mathrm{GL}(Gv)$ for $v \in V$ generic. Clearly, $Gv = \widehat{G}v$, but if $|G| < |\widehat{G}|$, then v has nontrivial stabilizer in $\widehat{G}$ and thus v is not generic for $\widehat{G}$. However, we have the following:

Theorem C. *Let $\widehat{G} = \mathrm{GL}(Gv)$ be the linear symmetry group of the orbit Gv, where $V = \mathrm{Span}(Gv)$ is a vector space over a field of characteristic 0. If w is generic for $\widehat{G}$, then $\mathrm{GL}(\widehat{G}w) = \widehat{G}$.*

Thus we have some sort of closure operator on the conjugacy classes of finite subgroups of $\mathrm{GL}(V)$ generating full-dimensional orbits. We call a group $G \leqslant \mathrm{GL}(V)$ *generically closed* if $\mathrm{GL}(Gv) = G$ for some (all) generic v. Thus the symmetry group of a spanning orbit is generically closed.

If a group is not generically closed, every full-dimensional orbit has additional linear symmetries, as in the example $G \cong C_4$ above.

Naturally, this leads to the problem of characterizing generically closed groups.

More generally, we may begin with an abstract finite group G, and consider various representations $D\colon G \to \mathrm{GL}(V)$ (for different V). We will see (Theorem 8.1) that there are only finitely many similarity classes of representations such that the space contains full-dimensional orbit polytopes of $D(G)$. We may ask: for which of these (faithful) representations of the given group is the image $D(G)$ generically closed? The following is an easy special case:

Theorem D. *If $D\colon G \to \mathrm{GL}(V)$ is absolutely irreducible, then a generic orbit in V has linear symmetry group $D(G)$.*

In essence, this result has been proved by I. M. Isaacs forty years ago [8].

For every group of order $\geqslant 3$, there are representations such that $D(G)$ is not generically closed (for example, the regular representation yields a simplex with $|G|$ vertices as orbit polytope). On the other hand, there may be no (faithful) representations such that $D(G)$ is generically closed. For example, abelian groups containing elements of order greater than 2 are never generically closed over the field of real numbers.

Studying the different possible orbit polytopes of a fixed group G is related to McMullen's theory of realizations of abstract regular polytopes [19, 20, 21, 22]. For a given finite group G and a subgroup $H \leqslant G$, McMullen studies congruence classes of orbit polytopes of G such that H fixes a vertex. The group G is usually assumed to be the automorphism group of an abstract regular polytope [23] and H a stabilizer of a vertex, and then the orbit polytopes are called realizations of the abstract regular polytope. However, most of the arguments are actually valid for an arbitrary group G and subgroup H. The congruence classes of such orbit polytopes form a pointed convex cone, the realization cone. Since we consider orbit polytopes up to a certain affine equivalence (see Definition 6.1), we further identify orbit polytopes in this cone. For example, the interior of the realization cone consists of non-congruent simplices, but these are all affinely equivalent.

1.3 Representation polytopes: results

An interesting class of orbit polytopes which have additional affine symmetries are the representation polytopes. A representation polytope is defined as the convex hull of $D(G)$, where $D\colon G \to \mathrm{GL}(d, \mathbb{R})$ is a representation of an abstract finite group G. If the image group consists of permutation matrices, the polytope is called a permutation polytope. A well-known example is the celebrated Birkhoff polytope of doubly stochastic matrices (also known as assignment polytope), which is the convex hull of *all* permutation matrices of a fixed dimension. Permutation polytopes and some other special classes of representation polytopes have also been studied by a number of people [2, 5, 6, 17].

In Section 6, we study representation polytopes as special cases of orbit polytopes. Representation polytopes usually have a big group of affine symmetries (with the notable exception of elementary abelian 2-groups, see below).

In Section 9, we show how the permutations of the vertices induced by the affine symmetry group of a representation polytope can be computed from a certain character. This result is in fact valid for arbitrary fields of characteristic 0. For simplicity, we assume that $\mathbb{K} \subseteq \mathbb{C}$, the field of complex numbers. We use the following notation: For a representation $D\colon G \to \mathrm{GL}(d, \mathbb{K})$, we write $\operatorname{Irr} D$ for the set of irreducible complex characters of G which occur in the character of D. Then we have:

Theorem E. *Let $D\colon G \to \mathrm{GL}(d, \mathbb{K})$ be a representation and set*

$$\gamma = \sum_{\chi \in \operatorname{Irr} D} \chi(1)\chi.$$

Let π be a permutation of G. Then $\pi \in \mathrm{Sym}(G, \mathrm{Span}(D(G))) = \mathrm{Sym}(G, I_n)$ if and only if

$$\gamma(\pi(g)^{-1}\pi(h)) = \gamma(g^{-1}h) \quad \text{for all} \quad g, h \in G.$$

Computing the affine symmetry group of a representation polytope or the group of linear maps preserving a finite matrix group, is a special case of a *linear preserver problem*. A *linear preserver problem* is the problem of determining the set of linear transformations of $\mathbf{M}_n(\mathbb{K})$ that map a given subset $S \subseteq \mathbf{M}_n(\mathbb{K})$ to itself, where $\mathbf{M}_n(\mathbb{K})$ denotes the ring of $n \times n$-matrices with entries in $\mathbb{K}$. This problem has already been studied for various specific subsets S, for example when S is a finite irreducible reflection group [14, 15, 16].

Finally, we have another amusing characterization of representation polytopes among orbit polytopes:

Theorem F. *The orbit polytope $\mathrm{P}(G, v)$ is affinely equivalent to a representation polytope of the same group G if and only if $\mathrm{P}(G, v)$ has an affine symmetry sending every vertex gv to $g^{-1}v$.*

1.4 Orbit symmetries and the group algebra

In Section 7, we begin to use, in as more systematic way, the module theoretic view of representation theory. Recall that any representation $D\colon G \to \mathrm{GL}(V)$, where V is a vector space over $\mathbb{K}$, endows V with the structure of a left module over the group algebra $\mathbb{K}G$, and conversely, any left $\mathbb{K}G$ module V defines a representation $D\colon G \to \mathrm{GL}(V)$, where $D(g)\colon V \to V$ is the map $v \mapsto gv$. Similar representations correspond to isomorphic $\mathbb{K}G$-modules and conversely [10, Theorem 7.6].

Let V be a left $\mathbb{K}G$-module and $v \in V$. The $\mathbb{K}$-subspace $\operatorname{Span}(Gv) = \operatorname{Span}\{gv \mid g \in G\}$ generated by the G-orbit of v equals

$$\operatorname{Span}(Gv) = \{\sum_{g\in G} r_g gv \mid r_g \in \mathbb{K}\} = \{av \mid a \in \mathbb{K}G\} = \mathbb{K}Gv.$$

This is the *cyclic* $\mathbb{K}G$-module generated by v. It follows that when we want to compute linear symmetries of orbits, then we need to consider only cyclic $\mathbb{K}G$-modules.

In Section 7, we view permutations $\pi \in \operatorname{Sym}(G)$ as linear maps on the group algebra and show that $\pi \in \operatorname{Sym}(G, v)$ or $\pi \in \operatorname{Sym}(G, V)$ is equivalent to π preserving certain left ideals of $\mathbb{K}G$.

In Section 8, we specialize again to the case where $\mathbb{K}$ has characteristic zero. Then $\mathbb{K}G$ is semisimple and left ideals have complements. Any cyclic $\mathbb{K}G$-module is isomorphic to a left ideal. It turns out that a left ideal and its complement have the same generic symmetry group.

A special place is taken by cyclic modules which are isomorphic to two-sided ideals of $\mathbb{K}G$. These are exactly the $\mathbb{K}G$-modules, which are isomorphic to a module of the form $\operatorname{Span}(D(G))$, where $D\colon G \to \operatorname{GL}(V)$ is some representation. Indeed, the character γ used in Theorem E is the character of G on I, where I is the (unique) ideal of $\mathbb{K}G$ which is isomorphic to $\operatorname{Span}(D(G))$ as left $\mathbb{K}G$-module. (In general, the character on I is not the same as the character of the representation D.) The proofs of Theorems E and F in Section 9 depend on these connections.

Finally, in Section 10 we show how to determine $\operatorname{Sym}(G, V)$ for a cyclic module in characteristic zero from the decomposition of the character of V into its irreducible constituents. If $\mathbb{K}$ is a field of characteristic zero, then the isomorphism type of V as $\mathbb{K}G$-module is determined by the character γ of G on V, and thus $\operatorname{Sym}(G, V)$ is also determined by γ. Suppose that $\mathbb{K} \subseteq \mathbb{C}$, the field of complex numbers (in fact, any algebraically closed field of characteristic zero would do), and let $\operatorname{Irr} G$ be the set of irreducible, complex valued characters (or with values in a fixed algebraically closed field containing $\mathbb{K}$). Then we can write γ in a unique way as sum of irreducible characters:

$$\gamma = \sum_{\chi\in\operatorname{Irr}(G)} m_\chi \chi.$$

When $V = \mathbb{K}Gv$ for some $v \in V$, then $m_\chi \leqslant \chi(1)$ for all $\chi \in \operatorname{Irr}(G)$. We call

$$\gamma_I := \sum_{\substack{\chi\in\operatorname{Irr}(G)\\ m_\chi=\chi(1)}} \chi(1)\chi$$

the *ideal part of* γ. With this notation, we have:

Theorem G. *Let γ be the character of the cyclic $\mathbb{K}G$-module V, where $\mathbb{K}$ has characteristic zero, and let $N = \operatorname{Ker}(\gamma - \gamma_I)$. Then a permutation $\pi \in \operatorname{Sym}(G)$ is in $\operatorname{Sym}(G, V)$ if and only if the following two conditions hold:*

(i) $\gamma_I\big(\pi(g)^{-1}\pi(h)\big) = \gamma_I(g^{-1}h)$ *for all g, $h \in G$, and*

(ii) $\pi(gN) = \pi(1)gN$ *(as sets) for all $g \in G$.*

For example, this means that when $N = \{1\}$, then $\operatorname{Sym}(G, V)$ contains only left multiplications with elements from G, and thus $\operatorname{GL}(Gv) \cong G$ for generic vectors $v \in V$.

When it happens that $\gamma = \gamma_I$, then the second condition in Theorem G is void, and Theorem G reduces to Theorem E.

In particular, it follows that for "most" groups G and representations $D\colon G \to \operatorname{GL}(V)$, we have $\operatorname{GL}(Gv) = D(G)$ for generic points $v \in V$. The classification of the groups for which this is not true (over $\mathbb{R}$ or $\mathbb{Q}$), is then the theme of the two subsequent Chapters III and IV.

2. Affine and linear symmetries

Let V be a finite-dimensional vector space over the field $\mathbb{K}$. We write $\operatorname{Aff} X$ for the affine hull of a set of points $X \subseteq V$. Recall that

$$\operatorname{Aff} X = \left\{ \sum_{x \in X} \lambda_x x \mid \lambda_x \in \mathbb{K}, \sum_{x \in X} \lambda_x = 1 \right\}.$$

As usual, $\operatorname{Span}(X)$ (or $\operatorname{Span}_{\mathbb{K}}(X)$) denotes the $\mathbb{K}$-linear span of a subset $X \subseteq V$.

We use the following general notation: For any set $S \subset V$, we write $\operatorname{AGL}(S)$ for the set of affine maps $\operatorname{Aff}(S) \to \operatorname{Aff}(S)$ that permute S, and $\operatorname{GL}(S)$ for the set of linear maps $\operatorname{Span}(S) \to \operatorname{Span}(S)$ that permute S.

We have the following very elementary observations:

2.1 Observation.

(i) *Let $S \subset V$ be a finite set such that $\operatorname{Char}(\mathbb{K})$, the characteristic of $\mathbb{K}$, does not divide $|S|$, the order of S. Then $\operatorname{AGL}(S)$ has a fixed point in $\operatorname{Aff}(S)$, namely $(1/|S|)\sum_{s \in S} s$.*

(ii) *Let G be a finite subgroup of $\operatorname{AGL}(V)$ such that $\operatorname{Char}(\mathbb{K})$ does not divide $|G|$. Then G fixes a point.*

Proof. The first statement is trivial, and the second follows by applying the first to any G-orbit. □

In particular, this means that in characteristic zero, the study of affine symmetries of finite point sets reduces to the study of linear symmetries of finite point

sets: Just choose a coordinate system with a fixed point as origin. Since affine symmetries of polytopes preserve the finite set of the vertices of the polytope, the same remark applies in this situation. We will confine ourself mostly to groups acting linearly from now on.

So let G be a finite group which acts *linearly* on V from the left. (In other words, V is a left $\mathbb{K}G$-module.) We need a straightforward generalization of an observation by Guralnick and Perkinson [5]. We use the notation

$$\operatorname{Fix} G = \operatorname{Fix}_V(G) = \{v \in V \mid gv = v \text{ for all } g \in G\}$$

for the fixed space of G in V.

2.2 Lemma. *Suppose that* $\operatorname{Char}(\mathbb{K})$ *does not divide* $|G|$. *Let* $v \in V$. *Then*

$$\left\{ \frac{1}{|G|} \sum_{g \in G} gv \right\} = \operatorname{Aff}(Gv) \cap \operatorname{Fix} G.$$

Thus the following are equivalent:

(i) $\sum_{g \in G} gv = 0$,
(ii) $0 \in \operatorname{Aff}(Gv) = \operatorname{Aff}\{gv \mid g \in G\}$.
(iii) $\operatorname{Span}\{gv \mid g \in G\} \cap \operatorname{Fix} G = \{0\}$.

Proof. Obviously, $(1/|G|) \sum_g gv \in \operatorname{Aff}(Gv) \cap \operatorname{Fix} G$. Let e_1 be the element

$$e_1 = \frac{1}{|G|} \sum_{g \in G} g \in \mathbb{K}G.$$

It is easy to see (and well known) that $w \in \operatorname{Fix} G$ if and only if $e_1 w = w$. Let $w \in \operatorname{Aff}(Gv) \cap \operatorname{Fix} G$ and write

$$w = \sum_{g \in G} \lambda_g gv, \quad \sum_{g \in G} \lambda_g = 1.$$

It follows

$$w = e_1 w = \sum_{g \in G} e_1 \lambda_g gv = \sum_{g \in G} \lambda_g e_1 v = e_1 v.$$

Thus $\operatorname{Aff}(Gv) \cap \operatorname{Fix} G = \{e_1 v\}$. The same argument shows that $\operatorname{Span}\{gv \mid g \in G\} \cap \operatorname{Fix} G = \operatorname{Span}(e_1 v)$.

The equivalence of the assertions follows. □

Note that $e_1 v$ can be seen as the barycenter of the orbit Gv (in particular when $\mathbb{K} = \mathbb{R}$), and that the translated orbit $Gv - e_1 v$ is the orbit of $v - e_1 v$. It is thus no loss of generality to assume that $e_1 v = 0$.

If we want to compute the affine symmetry group $\mathrm{AGL}(Gv)$ of an orbit Gv, we can restrict our attention to the affine space generated by the orbit Gv. We can thus assume that $V = \mathrm{Aff}(Gv)$. If $\mathrm{Char}(\mathbb{K})$ does not divide $|G|$, this already implies (by Lemma 2.2, (ii) $\Longrightarrow$ (i)) that $\sum_g gv = 0$. The affine symmetries of the orbit Gv are thus realized by linear maps.

When $\mathbb{K} = \mathbb{R}$, we denote by

$$\mathrm{P}(G, v) = \mathrm{conv}\{gv \mid g \in G\}$$

the orbit polytope of some $v \in V$. Notice that every gv is a vertex of $\mathrm{P}(G, v)$: A priori, the vertices are a subset of Gv. Every element of G induces a symmetry of $\mathrm{P}(G, v)$ onto itself and thus maps vertices to vertices. Thus every element of Gv is a vertex.

For any polytope P with vertex set S, we have $\mathrm{AGL}(P) = \mathrm{AGL}(S)$. Thus it follows from Lemma 2.2 that $0 \in \mathrm{P}(G, v)$ if and only if $\mathrm{P}(G, v)$ is centered at the origin. In this case, we have $\mathrm{AGL}(\mathrm{P}(G, v)) = \mathrm{GL}(\mathrm{P}(G, v)) = \mathrm{AGL}(Gv) = \mathrm{GL}(Gv)$.

3. Computing linear symmetries

In characteristic 0, we can compute the linear symmetries of a finite point set using a result by Bremner, Dutour Sikirić and Schürmann [3]. In this section, we give a simplified proof of a slightly more general version. In our first paper on affine symmetries of orbit polytopes [FL1], this result was crucial in some of the proofs, while in our second paper [FL2], its use was replaced by more general arguments which are also valid in positive characteristic. Thus the present section is kind of a digression in this thesis.

Actually, the result we are going to reprove is a criterion about isomorphisms of vector families. Let $\mathbb{K}$ be a field with some involution $*\colon \mathbb{K} \to \mathbb{K}$. The main cases to think of are $\mathbb{K} = \mathbb{R}$ with $* = \mathrm{id}$ and $\mathbb{K} = \mathbb{C}$ with $z^* = \overline{z}$ (complex conjugation). Let $(x_i \mid i \in I)$ and $(\tilde{x}_i \mid i \in I)$ be two families of vectors in $\mathbb{K}^d$ indexed by the same finite set I. Following Bremner, Dutour Sikirić and Schürmann [3], we form the $d \times d$-matrix

$$Q = \sum_{i \in I}^{n} x_i x_i^* = XX^*, \quad X = (v_i \mid i \in I).$$

Here X is a matrix with rows indexed by $1, \ldots, d$ and columns indexed by I. The matrix X^* has entries $y_{ij} = x_{ji}^*$, where $X = (x_{ji})$. Note that Q is invertible if $\mathbb{K} = \mathbb{C}$ and $\mathbb{K}^d = \mathrm{Span}(v_i \mid i \in I)$, since then Q is hermitian positive definite. Similarly, we write $\tilde{X} = (\tilde{x}_i \mid i \in I)$ and $\tilde{Q} = \tilde{X}\tilde{X}^*$. The next result generalizes [3, Proposition 3.1]:

3.1 Proposition. *Let Q and $\tilde{Q}$ be invertible. There is a $d \times d$-matrix A such that $Ax_i = \tilde{x}_i$ for all $i \in I$ if and only if $X^*Q^{-1}X = \tilde{X}^*\tilde{Q}^{-1}\tilde{X}$. In this case, we have $A = \tilde{X}X^*Q^{-1}$.*

Proof. Since Q and $\tilde{Q}$ have full rank, we must have $\mathbb{K}^d = \mathrm{Span}\{x_i \mid i \in I\} = \mathrm{Span}\{\tilde{x}_i \mid i \in I\}$. In particular, there is at most one A with $Ax_i = \tilde{x}_i$.

Assume that A exists. Note that A is necessarily invertible since it maps a spanning set to a spanning set. By assumption, $AX = \tilde{X}$. It follows

$$\begin{aligned}\tilde{X}^*\tilde{Q}^{-1}\tilde{X} = \tilde{X}^*\left(\tilde{X}\tilde{X}^*\right)^{-1}\tilde{X} &= \tilde{X}^*\left(AXX^*A^*\right)^{-1}\tilde{X} \\ &= \tilde{X}^*(A^*)^{-1}(XX^*)^{-1}A^{-1}\tilde{X} \\ &= X^*Q^{-1}X.\end{aligned}$$

Conversely, if $X^*Q^{-1}X = \tilde{X}^*\tilde{Q}^{-1}\tilde{X}$, then

$$\tilde{X} = \tilde{Q}\tilde{Q}^{-1}\tilde{X} = \tilde{X}\tilde{X}^*\tilde{Q}^{-1}\tilde{X} = \tilde{X}X^*Q^{-1}X,$$

so we can take $A = \tilde{X}X^*Q^{-1}$. □

Let $X = (x_i \mid i \in I)$ be a vector family in V and $\sigma \in \mathrm{Sym}(I)$ be a permutation of I. We say that σ is a **linear symmetry** of X if there is $A \in \mathrm{GL}(V)$ with $Ax_i = x_{\sigma(i)}$. We write

$$\mathrm{Sym}(I, X) = \{\sigma \in \mathrm{Sym}(I) \mid \exists A \in \mathrm{GL}(V)\colon Ax_i = x_{\sigma(i)}\}$$

and call this the **linear symmetry group** of $(x_i \mid i \in I)$. Proposition 3.1 gives, in particular, a criterion for when $\sigma \in \mathrm{Sym}(I, X)$.

3.2 Corollary. *Let $\sigma \in \mathrm{Sym}(I)$ and $X = (x_i \mid i \in I) \in \mathbb{K}^{d\times I}$ be such that $Q = XX^*$ is invertible, and set $W = X^*Q^{-1}X$. Then $\sigma \in \mathrm{Sym}(I, X)$ if and only if*

$$P(\sigma)^{-1}WP(\sigma) = W$$

where $P(\sigma) \in \mathbb{K}^{I\times I}$ is the permutation matrix corresponding to σ. In this case, for $A(\sigma) = XP(\sigma)X^*Q^{-1}$ we have $A(\sigma)x_i = x_{\sigma(i)}$ for all $i \in I$.

Proof. Write $\tilde{X} = XP(\sigma)$, so that $\tilde{X}$ has column $x_{\sigma(i)}$ at place i. Then $\tilde{X}\tilde{X}^* = XX^*$ since $P(\sigma)^* = P(\sigma)^{-1}$. The result follows from Proposition 3.1. □

If Q is invertible, write $W = X^*Q^{-1}X = (w_{ij})$, so $w_{ij} = x_i^*Q^{-1}v_j$. Let $G(X)$ be the complete graph with vertex set I, vertex colors w_{ii} and edge colors w_{ij}. The last corollary tells us that the linear symmetries of $(x_i \mid i \in I)$ yield isomorphisms of the edge colored graph $G(X)$ and vice versa. This means that in practice one can

compute the linear symmetries by computing graph automorphisms, using software like `nauty` [18].

The map $\sigma \mapsto A(\sigma)$ is a group homomorphism from $\mathrm{Sym}(I, X)$ onto $\mathrm{GL}(\{x_i \mid i \in I\})$. (Recall that we write $\mathrm{GL}(S)$ for the set of matrices $A \in \mathrm{GL}(d, \mathbb{K})$ mapping a set $S \subseteq \mathbb{K}^d$ onto itself. Under the assumptions of Corollary 3.2, $S = \{x_i \mid i \in X\}$ is finite and generates $\mathbb{R}^d$, so $\mathrm{GL}(S)$ is finite and isomorphic to a permutation group on S.) Notice that we do not exclude the possibility that $i \mapsto x_i$ is not injective. In that case, $\mathrm{Sym}(I, X) \to \mathrm{GL}(\{x_i \mid i \in I\})$ has a nontrivial kernel, namely the permutations preserving the fibers of $i \mapsto x_i$. If $i \mapsto x_i$ is injective, then $\mathrm{Sym}(I, X) \cong \mathrm{GL}(\{x_i \mid i \in I\})$.

Corollary 3.2 has the following amusing consequence. (One can also prove this using the representation theory of finite groups, in particular, the decomposition of a permutation representation into irreducible representations over $\mathbb{R}$.)

3.3 Corollary. *If the affine symmetry group of a polytope P acts transitively on the 2-subsets of its vertices, then P is a simplex.*

Proof. Without loss of generality, we may embed P in $\mathbb{R}^d$ such that P is full-dimensional and centered at the origin. We can thus assume that the affine symmetries of P are linear. Let $v_1, \ldots, v_n$ be the vertices of P and let $W = X^* Q^{-1} X = (w_{ij})$ be the corresponding vertex and edge color matrix. Let $i \neq j \in \{1, \ldots, n\}$. Then there is a linear symmetry of P mapping the vertices $\{x_1, x_2\}$ to $\{x_i, x_j\}$. It follows from Corollary 3.2 that $w_{ij} = w_{12}$ or $w_{ij} = w_{21}$. Since W is symmetric anyway, this means that $w_{ij} = w_{12}$ for all $i \neq j$. So all entries off the diagonal of W are equal.

A permutation group which acts transitively on the 2-subsets of a set with $n \neq 2$ elements is also transitive on the set itself. It follows $w_{11} = w_{22} = \cdots = w_{nn}$ for $n \neq 2$. (For $n = 2$, the corollary is trivially true anyway.)

Again by Corollary 3.2 it follows that every permutation of the vertices is induced by a linear map. It follows easily that P is a simplex: Let $\lambda = (\lambda_1, \ldots, \lambda_n)$ be a linear dependence of the vertices, that is, $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$. Every permutation of the coordinates of λ yields also a linear dependence. By applying the transposition (i, j) and subtracting dependencies, we see that $(\lambda_i - \lambda_j) x_i + (\lambda_j - \lambda_i) x_j = 0$. Since $x_i \neq x_j$, it follows that $\lambda_i = \lambda_j$ for all $i \neq j$. Therefore, there is, up to scalars, at most one linear dependence, and thus the affine hull of the vertices has dimension $n - 1$. It follows that P is a simplex. □

4. Generic points

In this section, $\mathbb{K}$ denotes an arbitrary field. As before, G is a finite group and V a left $\mathbb{K}G$-module (thus G acts $\mathbb{K}$-linearly on V).

We are interested in the various symmetry groups $\mathrm{GL}(Gv)$ of G-orbits Gv, where $v \in V$ is such that

$$V = \mathrm{Span}(Gv) = \Big\{ \sum_{g\in G} c_g gv \mid c_g \in \mathbb{K} \Big\} =: \mathbb{K}Gv.$$

It will be convenient to have a notation for the set of these $v \in V$ and thus we define

$$\mathrm{Gens}(V) := \{v \in V \mid V = \mathbb{K}Gv.\}$$

When there is $v \in V$ such that $V = \mathbb{K}Gv$, then V is called **cyclic** (as $\mathbb{K}G$-module), and v is called a **generator** of V.

In order to compare $\mathrm{GL}(Gv)$ and $\mathrm{GL}(Gw)$ for different v, $w \in \mathrm{Gens}(V)$, we introduce the following definition:

4.1 Definition. Let $v \in V$. A permutation $\pi \in \mathrm{Sym}(G)$ is called an **orbit symmetry with respect to** v, if there is a $\mathbb{K}$-linear map from V to V which maps gv to $\pi(g)v$ for all $g \in G$. We write $\mathrm{Sym}(G, v)$ for the set of all orbit symmetries of v:

$$\mathrm{Sym}(G, v) := \{\pi \in \mathrm{Sym}(G) \mid \exists A \in \mathrm{GL}(V) \colon \forall g \in G \colon Agv = \pi(g)v\}.$$

For $\pi \in \mathrm{Sym}(G, v)$, we write $D_v(\pi)$ for the unique $\mathbb{K}$-linear map $\mathbb{K}Gv \to \mathbb{K}Gv$ such that $D_v(\pi)gv = \pi(g)v$ for all $G \in G$. Thus $D_v(\pi)$ is the restriction of A to $\mathbb{K}Gv$.

In the notation of Section 3, $\mathrm{Sym}(G, v)$ is the group of linear symmetries of the vector family $(gv \mid g \in G)$, index by elements of G.

Clearly, the condition $Agv = \pi(g)v$ for all $g \in G$ shows that $A(\mathbb{K}Gv) = \mathbb{K}Gv$, and uniquely determines the restriction $D_v(\pi)$ of A to $\mathbb{K}Gv$. Conversely, when there is a linear map $D_v(\pi) \colon \mathbb{K}Gv \to \mathbb{K}Gv$ with $D_v(\pi)gv = \pi(g)v$ for all $g \in G$, then we can extend $D_v(\pi)$ (non-uniquely) to a linear map $A \colon V \to V$. When computing $\mathrm{Sym}(G, v)$, it is thus no loss of generality to assume $V = \mathbb{K}Gv$.

For later reference, we record the following easy observation:

4.2 Lemma. $\mathrm{Sym}(G, v)$ *is a subgroup of* $\mathrm{Sym}(G)$*, and the map*

$$D_v \colon \mathrm{Sym}(G, v) \to \mathrm{GL}(\mathbb{K}Gv)$$

is a group homomorphism, and thus a representation of $\mathrm{Sym}(G, v)$*. The image is* $D_v(\mathrm{Sym}(G, v)) = \mathrm{GL}(Gv)$*.*

Proof. For π, $\sigma \in \mathrm{Sym}(G, v)$ we have

$$D_v(\pi)D_v(\sigma)gv = D_v(\pi)\sigma(g)v = \pi(\sigma(g))v = D_v(\pi\sigma)gv.$$

That $D_v(\mathrm{Sym}(G, v)) = \mathrm{GL}(Gv)$ follows directly from the definitions. □

For the sake of completeness, and for later reference, we also compute the kernel of D_v:

4.3 Lemma. *Let $H = G_v := \{g \in G \mid gv = v\}$ be the stabilizer of v in G. Then*

$$\begin{aligned}\operatorname{Ker} D_v &= \{\pi \in \operatorname{Sym}(G) \mid \pi(gH) = gH \text{ for all cosets } gH\} \\ &\cong \operatorname{Sym}(H)^{|G:H|}.\end{aligned}$$

Proof. This follows immediately from the definitions. □

It is not difficult to show that $\operatorname{Sym}(G, v)$ is in fact isomorphic to a *wreath product* of $\mathrm{GL}(Gv)$ with $\operatorname{Sym}(H)$.

In particular, $\operatorname{Sym}(G, v)$ contains a subgroup isomorphic to $\operatorname{Sym}(H)^{|G:H|}$, containing "irrelevant" permutations. In view of this, the reader may wonder why we do not simply consider $\mathrm{GL}(Gv)$ instead of $\operatorname{Sym}(G, v)$. One reason is to make the next definition work:

4.4 Definition. Let V be a cyclic $\mathbb{K}G$-module. A permutation $\pi \in \operatorname{Sym}(G)$ is called an **orbit symmetry with respect to** V, if it is an orbit symmetry for any generator of V. We set

$$\operatorname{Sym}(G, V) := \bigcap_{v \in \operatorname{Gens}(V)} \operatorname{Sym}(G, v),$$

the group of all orbit symmetries for V.

For infinite fields $\mathbb{K}$, the group $\operatorname{Sym}(G, V)$ coincides with the *generic orbit symmetry group of* V which we will define later. For vector spaces over finite fields, $\operatorname{Sym}(G, V)$ is not generic enough, as we will explain later. However, our focus here is on infinite fields anyway.

Recall that G acts on itself by left multiplication (the **left regular action**). For any $h \in G$, let $\lambda_h \in \operatorname{Sym}(G)$ be the permutation induced by left multiplication with h, so $\lambda_h(g) = hg$ for all $g \in G$. As V is a $\mathbb{K}G$-module, G acts linearly on V, say by the representation $D\colon G \to \mathrm{GL}(V)$. Since $D(h)(gv) = hgv = \lambda_h(g)v$, we see that $\lambda_h \in \operatorname{Sym}(G, v)$ for any $v \in V$, and that $D_v(\lambda_h) = D(h)$. In particular, $\operatorname{Sym}(G, v)$ and $\operatorname{Sym}(G, V)$ always contain the regular subgroup $\lambda(G) \cong G$. This motivates the next definition:

4.5 Definition. The group $\operatorname{Sym}(G, V)$ is called the **generic closure** of G with respect to V. We say that V as $\mathbb{K}G$-module is **generically closed** if $\lambda(G) = \operatorname{Sym}(G, V)$, where $\lambda\colon G \to \operatorname{Sym}(G)$ is the left regular action as above.

Notice that V is generically closed, if and only if there exists $v \in \operatorname{Gens}(V)$ such that $\operatorname{Sym}(G, v) = \lambda(G)$, and then of course $\operatorname{Sym}(G, v) = \operatorname{Sym}(G, V)$.

Let us emphasize that we do *not* assume that G acts faithfully on V, that is,

$$\mathrm{Ker}(V) := \{g \in G \mid gv = v \text{ for all } v \in V\}$$

can be non-trivial. This means that $\mathrm{Sym}(G, V)$ contains by definition all permutations of G which map every left coset of $\mathrm{Ker}(V)$ onto itself. Of course, when $\pi \in \mathrm{Sym}(G)$ is a permutation that maps every left coset of $\mathrm{Ker}(V)$ onto itself, then we have $D_v(\pi) = \mathrm{id}_V$ for every generator v, and thus the set of these permutations is, in some sense, irrelevant. This could be avoided by replacing G by the factor group $G/\mathrm{Ker}(V)$. It turns out to be more convenient not to do this, for example in the following situation:

4.6 Lemma. *Suppose that $V = V_1 \oplus \cdots \oplus V_n$ is a direct sum of $\mathbb{K}G$-modules, where V is cyclic (that is, $\mathrm{Gens}(V) \neq \emptyset$). Then*

$$\bigcap_{i=1}^{n} \mathrm{Sym}(G, V_i) \subseteq \mathrm{Sym}(G, V).$$

Notice that it is perfectly possible that $\mathrm{Ker}(V) = 1$, while $\mathrm{Ker}(V_i) \neq 1$ for some V_i.

Proof of Lemma 4.6. Let $v \in \mathrm{Gens}(V)$ and write $v = v_1 + \cdots + v_n$ with $v_i \in V_i$. Then $v_i \in \mathrm{Gens}(V_i)$. Suppose that $\pi \in \mathrm{Sym}(G, V_i)$ for all i. Thus there is $A_i \in \mathrm{GL}(V_i)$ such that $\pi(g)v_i = A_i g v_i$ for all $g \in G$. Then for $A = A_1 \oplus \cdots \oplus A_n \colon V \to V$, we have $\pi(g)v = Agv$ for all $g \in G$, and thus $\pi \in \mathrm{Sym}(G, V)$ as claimed. □

We will show later that when $\mathbb{K}$ has characteristic zero, then there is a certain decomposition such that equality holds in Lemma 4.6. In general, the containment is of course strict.

4.7 Remark. When $1 < \mathrm{Ker}(V) < G$ or $|\mathrm{Ker}(V)| \geqslant 3$, then there is a permutation $\pi \neq \mathrm{id}_G$ of G which maps every coset of $\mathrm{Ker}(V)$ onto itself, and such that $\pi(1_G) = 1_G$. Then $\pi \in \mathrm{Sym}(G, V)$, but π is not of the form $\pi = \lambda_g$ for any $g \in G$. Hence, when G is generically closed with respect to V, then G must act faithfully on V (except in the trivial case $G = C_2$).

4.8 Lemma. *Let $\varphi \colon V \to W$ be an isomorphism of $\mathbb{K}G$-modules (that is, φ is $\mathbb{K}$-linear, bijective, and $\varphi(gv) = g\varphi(v)$ for $g \in G$, $v \in V$). Then:*

(i) $\mathrm{Sym}(G, v) = \mathrm{Sym}(G, \varphi(v))$ *for any $v \in V$.*
(ii) $D_{\varphi(v)}(\pi) = \varphi \circ D_v(\pi) \circ \varphi^{-1}$ *for $v \in V$ and $\pi \in \mathrm{Sym}(G, v)$.*
(iii) $\mathrm{Sym}(G, V) = \mathrm{Sym}(G, W)$.

Proof. Easy verifications. □

In view of this lemma, it is no loss of generality to assume that $V = \mathbb{K}^d$ as $\mathbb{K}$-space, so that the action of G on V is described by a matrix representation $D\colon G \to \mathrm{GL}(d, \mathbb{K})$. We do this in the rest of this section. In particular, this enables us to evaluate polynomials in d indeterminates at elements $v \in V$ in the usual, elementary way. We view $V = \mathbb{K}^d$ as equipped with the Zariski topology, that is, the closed subsets of V are by definition the zero sets of arbitrary families of polynomials in $\mathbb{K}[X_1, \ldots, X_d]$. Any finite dimensional $\mathbb{K}$-space can be equipped with the Zariski topology by choosing a basis, and the resulting topology does not depend on the choice of basis.

We now work to define *generic* points in V with respect to the action of G on V and linear symmetries of orbits in V. We will see that the non-generic points are the zero set of certain nonzero polynomials defined on $\mathbb{K}^d$. In particular, for infinite fields $\mathbb{K}$, generic points exist, and indeed "almost all" points are generic.

We begin by considering different sets of points which are not generic.

4.9 Lemma. *The set of points v such that*

$$G_v := \{g \in G \mid gv = v\} > \mathrm{Ker}(V) = \mathrm{Ker}(D)$$

is a finite union of proper subspaces of $V = \mathbb{K}^d$.

Proof. For every $g \in G \setminus \mathrm{Ker}(D)$, the fixed space $\{v \in V \mid gv = v\}$ is a proper subspace of V. We have $G_v > \mathrm{Ker}(D)$, if and only if v is in one of these fixed spaces. □

Points v with trivial stabilizer G_v are called "in general position" by Ellis, Harris and Sköldberg [4]. However, these points are not general enough for our purposes, so we do not adopt this terminology.

4.10 Lemma. *Let $m \in \mathbb{N}$. Then the sets*

$$\{v \in V \mid \dim(\mathrm{Span}(Gv)) < m\} \quad \textit{and} \quad \{v \in V \mid \dim(\mathrm{Aff}(Gv)) < m\}$$

are Zariski-closed.

Proof. Enumerate $G = \{g_1, \ldots, g_n\}$. For each $v \in \mathbb{K}^d$, we can form the $d \times n$-matrix M with columns $g_i v$. The rank $\mathrm{rk}(M)$ of M equals the dimension of $\mathbb{K}Gv$. We have $\mathrm{rk}(M) < m$ if and only if every $m \times m$ subdeterminant of M vanishes. These subdeterminants are polynomials in the entries of v.

For the statement about the affine hull, form the $(d+1) \times n$-matrix with columns $\binom{g_i v}{1} \in \mathbb{K}^{d+1}$. The rank of this matrix equals $\dim(\mathrm{Aff}(Gv))$. □

An immediate consequence of Lemma 4.10 is:

4.11 Corollary. $\mathrm{Gens}(V)$ *is Zariski-open in V.*

As before, let G act linearly on $\mathbb{K}^d$, by some matrix representation $D\colon G \to \mathrm{GL}(d,\mathbb{K})$. Let $X = (X_1, \ldots, X_d)^t$ be a vector of indeterminates. Then $X \in \mathbb{K}[X]^d \subset \mathbb{K}(X)^d$, where $\mathbb{K}(X) =: \mathbb{E}$ is the field of rational functions in d indeterminates X_1, $\ldots$, X_d. The representation D makes $\mathbb{E}^d$ into an $\mathbb{E}G$-module. (This is true for every field extension $\mathbb{E}$ of $\mathbb{K}$. For an arbitrary $\mathbb{K}G$-module V, this construction corresponds to forming the $\mathbb{E}G$-module $V \otimes_{\mathbb{K}} \mathbb{E}$.) In particular, $\mathrm{Sym}(G,X)$ is defined.

4.12 Definition. The group

$$\mathrm{Sym}(G,X) := \Big\{\pi \in \mathrm{Sym}(G) \mid \exists A \in \mathrm{GL}(d,\mathbb{K}(X))\colon \\ \forall g \in G\colon Agv = \pi(g)v\Big\}$$

is called the **generic symmetry group** of $V = \mathbb{K}^d$ with respect to G.

Next, we want to show that $\mathrm{Sym}(G,X) \leqslant \mathrm{Sym}(G,v)$ for all $v \in \mathrm{Gens}(V)$, and that for $\pi \in \mathrm{Sym}(G) \setminus \mathrm{Sym}(G,X)$, the set

$$N(\pi) := \{v \in \mathrm{Gens}(V) \mid \pi \in \mathrm{Sym}(G,v)\}$$

is the zero set of some nonzero polynomials *in* $\mathrm{Gens}(V)$. This means that $N(\pi)$ is relatively Zariski-closed in $\mathrm{Gens}(V)$. It is in general not true that the set $v \in V$ with $\pi \in \mathrm{Sym}(G,v)$ is closed in V itself:

4.13 Example. Let $G = D_4$ be the dihedral group of order 8, and represent G as the subgroup of $\mathrm{GL}(2,\mathbb{R})$ preserving a (fixed) square which is centered at the origin. Let V be the space of 2×2-matrices over $\mathbb{R}$, on which G acts by left multiplication. Let $\pi \in \mathrm{Sym}(G)$ be the permutation sending each element to its inverse. Then it is not difficult to verify that $\{v \in V \mid \pi \in \mathrm{Sym}(G,v)\} = \mathrm{Gens}(V) \cup \{0\}$. (This is also a consequence of Theorem F.)

In the proof of the next result, we use some elementary set-theoretic topology. Notice that $\mathrm{Gens}(V) = \bigcup_f O_f$, where $O_f := \{v \in V \mid f(v) \neq 0\}$ is the non-vanishing set of the polynomial f, and f runs through polynomials of the form

$$f(X) := \det(g_1X, \ldots, g_dX), \quad g_1, \ldots, g_d \in G.$$

The sets O_f are of course open in the Zariski topology, and form an open cover of $\mathrm{Gens}(V)$. (This is the proof of Corollary 4.11.) We will use that a subset $N \subseteq \mathrm{Gens}(V)$ is relatively closed in $\mathrm{Gens}(V)$ if and only if $N \cap O_f$ is relatively closed in O_f for all f.

4.14 Lemma.

(i) $\mathrm{Sym}(G,X) \leqslant \mathrm{Sym}(G,v)$ *for every* $v \in \mathrm{Gens}(V)$.

(ii) *For every* $\pi \in \mathrm{Sym}(G)$*, the set*

$$N(\pi) := \{v \in \mathrm{Gens}(V) \mid \pi \in \mathrm{Sym}(G, v)\}$$

is relatively (Zariski-) closed in $\mathrm{Gens}(V)$*. When* $\pi \notin \mathrm{Sym}(G, X)$*, then* $N(\pi)$ *is the zero set of some* nonzero *polynomials in* $\mathrm{Gens}(V)$*.*

Proof. Let $v \in \mathrm{Gens}(V)$ and fix $g_1, \ldots, g_d \in G$ such that $\{g_1 v, \ldots, g_d v\}$ is a basis of V. Thus $f(v) \neq 0$, where $f(X) = \det(g_1 X, \ldots, g_d X)$ as above. Let $\pi \in \mathrm{Sym}(G)$. Since $f(X) \neq 0$, the $(d \times d)$-matrix

$$A := A(X) := (\pi(g_1)X, \ldots, \pi(g_d)X) \cdot (g_1 X, \ldots, g_d X)^{-1}$$

is defined and has entries in the function field $\mathbb{K}(X)$. Obviously, $A(X)$ is the unique matrix mapping $g_i X$ to $\pi(g_i)X$. It follows that $\pi \in \mathrm{Sym}(G, X)$ if and only if $A(X)gX = \pi(g)X$ for *all* $g \in G$. Also, for any $v \in O_f$, we can evaluate $A(X)$ at v, and we have $\pi \in \mathrm{Sym}(G, v)$ if and only if $A(v)gv = \pi(g)v$ for all $g \in G$. This yields part (i). Since the entries of $f(X)\big(A(X)gX - \pi(g)X\big)$ are polynomials (for all $g \in G$), we see that $N(\pi) \cap O_f$ is relatively closed in O_f. When $\pi \notin \mathrm{Sym}(G, X)$, then some entries must be nonzero polynomials. Thus part (ii) follows, too. □

4.15 Remark. In the proof, we defined a $d \times d$-matrix $A(X)$ with entries in $\mathbb{K}(X)$, depending on the choice of d elements $g_1, \ldots, g_d \in G$ such that

$$f(X) = \det(g_1 X, \ldots, g_d X) \neq 0.$$

This matrix has the following property: For any $v \in N(\pi) \cap O_f$, we have $A(v) = D_v(\pi)$. In particular, $A(v)$ is invertible, and so when $N(\pi) \cap O_f \neq \emptyset$, then $A(X)$ must be invertible.

4.16 Remark. For $\mathbb{K} = \mathbb{R}$, there is an alternative proof of Lemma 4.14 using Corollary 3.2. For the moment, assume that $\mathbb{K} \subseteq \mathbb{C}$. For $v \in \mathbb{K}^d$, we consider the matrix

$$Q(v) = \sum_{g \in G} (gv)(gv)^* = \sum_{g \in G} g(vv^*)g^*.$$

As we have remarked before, when $v \in \mathrm{Gens}(\mathbb{K}^d)$, then $Q(v)$ is hermitian positive definite and in particular invertible. Conversely, when $Q(v)$ is invertible, then $v \in \mathrm{Gens}(V)$ (this is true for arbitrary fields). In other words, we have

$$v \in \mathrm{Gens}(V) \iff \det Q(v) \neq 0.$$

For $\mathbb{K} \subseteq \mathbb{R}$, this yields another proof of Corollary 4.11, since then $\det Q(v)$ is a polynomial in the entries of v. In general, we only have that $\det Q(v)$ is polynomial in v and $\overline{v}$.

Now assume $v \in \mathrm{Gens}(V)$. By Corollary 3.2, the group $\mathrm{Sym}(G, v)$ consists exactly of the graph isomorphisms of the vertex and edge colored graph with vertices $g \in G$ and colors $w_{g,h}(v) = (gv)^* Q(v)^{-1}(hv)$. Notice that the entries of $\det(Q(v)) \cdot Q(v)^{-1}$ are polynomials in v and $\overline{v}$. Thus $\det(Q(v)) w_{g,h}(v)$ is a polynomial in v and $\overline{v}$, too. In particular, for $\mathbb{K} \subseteq \mathbb{R}$ this yields another proof of Lemma 4.14.

4.17 Definition. Let V be a cyclic $\mathbb{K}G$-module. A point $v \in V$ is called a **generic point** of V, when v is a generator of V, when $G_v = \mathrm{Ker}(V)$ (the stabilizer has minimal possible size), and $\mathrm{Sym}(G, v) = \mathrm{Sym}(G, X)$, where $X = (X_1, \ldots, X_d)^t$ is a vector of indeterminates over $\mathbb{K}$.

The G-orbit of a generic point is called a **generic orbit**, and in the case $\mathbb{K} = \mathbb{R}$, the orbit polytope $\mathrm{P}(G, v)$ of a generic point v is called a **generic orbit polytope**. (This is well-defined since the orbit of a generic point contains only generic points.)

The next result contains Theorem A form the introduction.

4.18 Theorem. *Let V be a cyclic $\mathbb{K}G$-module. The set of generic points is open (in the Zariski topology). If $\mathbb{K}$ is infinite, then there exist generic points in $\mathbb{K}^d$.*

Proof. This is immediate from Lemmas 4.9 and 4.14 and Corollary 4.11. □

Recall that we defined

$$\mathrm{Sym}(G, V) := \bigcap_{v \in \mathrm{Gens}(V)} \mathrm{Sym}(G, v).$$

4.19 Corollary. *Let $\mathbb{K}$ be an infinite field and V a cyclic $\mathbb{K}G$-module. Then*

$$\mathrm{Sym}(G, X) = \mathrm{Sym}(G, V).$$

Proof. Immediate from Lemma 4.14. □

The next corollary will be an important tool in Section 10. It means that the generic symmetry group of a $\mathbb{K}G$-module does not change if we extend the field. In particular, we are always allowed to assume that $\mathbb{K}$ is algebraically closed.

4.20 Corollary. *Let $\mathbb{E}$ be an extension field of the infinite field $\mathbb{K}$, and let V be a cyclic $\mathbb{K}G$-module. Then* $\mathrm{Sym}(G, V) = \mathrm{Sym}(G, V \otimes_{\mathbb{K}} \mathbb{E})$.

Proof. Without loss of generality, we can assume that $V = \mathbb{K}^d$ and $V \otimes_{\mathbb{K}} \mathbb{E} = \mathbb{E}^d$. Let $X = (X_1, \ldots, X_d)^t$ be a vector of indeterminates over $\mathbb{E}$. By Corollary 4.19 applied first to $\mathbb{K}^d$, then to $\mathbb{E}^d$, we have, $\mathrm{Sym}(G, V) = \mathrm{Sym}(G, X) = \mathrm{Sym}(G, V \otimes_{\mathbb{K}} \mathbb{E})$. □

4.21 Remark. If $\mathbb{K}$ is a finite field and V a cyclic $\mathbb{K}G$-module, then we may have $\mathrm{Sym}(G, X) < \mathrm{Sym}(G, V)$. Thus $\mathrm{Sym}(G, V)$ should not be called the generic symmetry group in this case. On the other hand, we always have $\mathrm{Sym}(G, X) = \mathrm{Sym}(G, V \otimes_{\mathbb{K}} \mathbb{E})$ for $\mathbb{E}$ "sufficiently large". When $\mathbb{K}$ is finite, then V may not contain generic points, but $V \otimes_{\mathbb{K}} \overline{\mathbb{K}}$ does, where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$.

5. The generic symmetry group

As before, we assume that $D\colon G \to \mathrm{GL}(d,\mathbb{K})$ is a representation, and $\mathbb{K}^d$ is a cyclic $\mathbb{K}G$-module with respect to this representation. Recall the notations

$$\begin{aligned} \mathrm{GL}(Gv) &:= D_v(\mathrm{Sym}(G,v)) \subseteq \mathrm{GL}(d,\mathbb{K}) \\ \text{and} \quad \mathrm{GL}(GX) &:= D_X(\mathrm{Sym}(G,X)) \subseteq \mathrm{GL}(d,\mathbb{K}(X)). \end{aligned}$$

5.1 Lemma. *For $\pi \in \mathrm{Sym}(G,X)$, the matrix*

$$A(X) := D_X(\pi) \in \mathrm{GL}(d,\mathbb{K}(X))$$

can in fact be evaluated for all $v \in \mathrm{Gens}(V)$, and evaluates to $A(v) = D_v(\pi)$. Thus we have a commutative diagram:

$$\begin{array}{ccc} \mathrm{Sym}(G,X) & \xrightarrow{D_X} & \mathrm{GL}(GX) \\ \big\downarrow & & \big\downarrow{\scriptstyle \mathrm{eval}_v} \\ \mathrm{Sym}(G,v) & \xrightarrow[D_v]{} & \mathrm{GL}(Gv) \end{array}$$

Proof. Let v be a generating point, and let $g_1, \ldots, g_d \in G$ be elements such that $\{g_1 v, \ldots, g_d v\}$ is a basis of $\mathbb{K}^d$. Then $\{g_1 X, \ldots, g_d X\}$ is a basis of $\mathbb{K}(X)^d$, and we must have

$$A(X) = (\pi(g_1)X, \ldots, \pi(g_d)X) \cdot (g_1 X, \ldots, g_d X)^{-1}.$$

As $f(v) \neq 0$, where $f(X) = \det(g_1 X, \ldots, g_d X)$, it follows that $A(X)$ can be evaluated at v. Also, $A(v) = D_v(\pi)$ is clear then. Since $v \in \mathrm{Gens}(V)$ was arbitrary, the proof follows. □

5.2 Remark. For $\mathbb{K} = \mathbb{R}$ and $V = \mathbb{R}^d$, Corollary 3.2 gives the formula

$$A(X) = D_X(\pi) = B(X)P(\pi)B(X)^t Q(X)^{-1},$$

where $B(X)$ is the matrix with columns gX, $g \in G$, and $Q(X) = B(X)B(X)^t$. Obviously, this $A(X)$ can be evaluated for all $v \in \mathrm{Gens}(V)$. In fact, this matrix is defined even when $\pi \notin \mathrm{Sym}(G,X)$. When $\pi \in \mathrm{Sym}(G,v) \setminus \mathrm{Sym}(G,X)$, then evaluating $A(X)$ at v yields

$$A(v) = B(v)P(\pi)B(v)^t Q(v)^{-1} = D_v(\pi),$$

although $A(X)$ does not stabilize the orbit GX.

It is clear that the map $\mathrm{GL}(GX) \to \mathrm{GL}(Gv)$ is an isomorphism when v is generic. Somewhat more is true.

5.3 Lemma. *Let $v \in \mathrm{Gens}(V)$ be such that the characteristic of $\mathbb{K}$ does not divide the order of the stabilizer $H = G_v$ of v in G. Then evaluation at v yields an injective map $\mathrm{GL}(GX) \to \mathrm{GL}(Gv)$.*

Proof. Suppose that $A(X) \in \mathrm{GL}(GX)$ evaluates to the identity. Thus $A(v)gv = gv$ for all $g \in G$. This means that $A(X)$ maps the set gHX onto itself. Define

$$s_g(X) := \frac{1}{|H|} \sum_{h \in H} ghX \in \mathbb{K}[X]^d.$$

(Here we need that $|H|$ is invertible as an element of $\mathbb{K}$.) Then $A(X)s_g(X) = s_g(X)$ and $s_g(v) = gv$. As $V = \mathbb{K}^d$ is the $\mathbb{K}$-linear span of the elements $s_g(v) = gv$ $(g \in G)$, it follows that $\mathbb{K}(X)^d$ is the $\mathbb{K}(X)$-linear span of the elements $s_g(X)$ $(g \in G)$. Since $A(X)s_g(X) = s_g(X)$ for all g, it follows that $A(X) = I$ as claimed. □

Let $\widehat{G} = \mathrm{GL}(Gv)$, where Gv spans V. Then we can view V as a $\mathbb{K}\widehat{G}$-module, and we can speak of generic points for $\widehat{G}$. So suppose w is generic for $\widehat{G}$. Is it possible that $\widehat{G} < \mathrm{GL}(\widehat{G}w)$? The answer is "Yes" in general, but "No" when $\mathbb{K}$ has characteristic 0. This was first proved in the case $\mathbb{K} = \mathbb{R}$ [FL1, Corollary 5.4]. In fact, we have the following slightly more general result, which contains Theorem C from the introduction:

5.4 Corollary. *Let $\widehat{G} = \mathrm{GL}(Gv)$, where $v \in \mathrm{Gens}(V)$ (with respect to the action of G), and let $w \in V$ be generic for $\widehat{G}$. If the characteristic of $\mathbb{K}$ does not divide $|\widehat{G}_v|$, then $\widehat{G} = \mathrm{GL}(\widehat{G}w)$.*

Proof. By Lemma 5.1 applied to $\widehat{G}$ and w, it follows that $\mathrm{GL}(\widehat{G}X) \cong \mathrm{GL}(\widehat{G}w)$ by evaluation at w. (Since w is generic for $\widehat{G}$, we have that $\mathrm{Sym}(\widehat{G}, V) = \mathrm{Sym}(\widehat{G}, w)$.) By Lemma 5.3 applied to $\widehat{G}$ and v, it follows that $\mathrm{GL}(\widehat{G}X)$ maps injectively into $\mathrm{GL}(\widehat{G}v)$. But by definition of $\widehat{G}$, we have $\widehat{G}v = Gv$ and $\mathrm{GL}(Gv) = \widehat{G}$. Thus $\mathrm{GL}(\widehat{G}w) \cong \mathrm{GL}(\widehat{G}X)$ is isomorphic to a subgroup of $\widehat{G}$. On the other hand, $\widehat{G} \leqslant \mathrm{GL}(\widehat{G}w)$. The result follows. □

We now digress to give an example which shows that the conclusions of Lemma 5.3 and Corollary 5.4 may fail to hold if the characteristic of $\mathbb{K}$ divides the order of the stabilizer.

5.5 Example. Let $\mathbb{K}$ be a field of characteristic 2. Let $U \leqslant \mathbb{K}^2$ be a finite additive subgroup such that $(u, v) \in U$ implies $(0, u) \in U$. This condition ensures that

$$G := \left\{ \begin{pmatrix} 1 & u & v \\ & 1 & c \\ & & 1 \end{pmatrix} \mid (u, v) \in U, c \in \mathbb{F}_2 \right\}$$

is a finite subgroup of $\mathrm{GL}(3,\mathbb{K})$. Moreover, we assume that

$$\{\lambda \in \mathbb{K} \mid \lambda U \subseteq U\} = \{0,1\} = \mathbb{F}_2$$

and that $(\mathbb{F}_2)^2 \subseteq U$. (For example, we can choose $U = (\mathbb{F}_2)^2$.) A vector $(x,y,z)^t$ is a generator of $\mathbb{K}^3$ if and only if $z \neq 0$.

Let $W = (X,Y,Z)^t \in \mathbb{K}(X,Y,Z)^3$. It is easy to check that each element of

$$H = \left\{ \begin{pmatrix} 1 & (uY+vZ)/Z & (uY+vZ)Y/Z^2 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid (u,v) \in U \right\}$$

maps the orbit GW onto itself, and fixes W. For example, for $(u,v) = (1,1)$, we get the matrix

$$A(X,Y,Z) = \begin{pmatrix} 1 & Y/Z+1 & (Y/Z+1)Y/Z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \in \mathrm{GL}(GW).$$

On the other hand, we have $A(1,1,1) = I$, and so evaluation is not injective in this case. Lemma 5.3 does not apply here since 2 (the characteristic of $\mathbb{K}$) divides the order of the stabilizer of $(1,1,1)^t$ in G.

It is somewhat tedious, but elementary, to compute that H is in fact exactly the set of matrices that fix the generic vector W, and map its orbit GW onto itself. (Here we need that $\lambda U \subseteq U$ implies $\lambda \in \{0,1\}$.) Since G acts regularly on GW, it follows that $\mathrm{GL}(GW) = HG > G$.

Now suppose $w = (x,y,z)^t \in \mathbb{K}^3$ is a generic vector. (Recall that generic vectors exist when K is large enough, which we simply assume now.) It follows that $\widehat{G} := \mathrm{GL}(Gw)$ has also the form

$$\widehat{G} = \left\{ \begin{pmatrix} 1 & u & v \\ & 1 & c \\ & & 1 \end{pmatrix} \mid (u,v) \in \widehat{U}, c \in \mathbb{F}_2 \right\},$$

with a finite subgroup $\widehat{U} \leqslant \mathbb{K}^2$ such that $U < \widehat{U}$. If $\widehat{U}$ also fulfills the assumption that $\lambda\widehat{U} \subseteq \widehat{U}$ implies $\lambda \in \mathbb{F}_2$, then we can continue as before. For example, when $\mathbb{K} = \mathbb{F}_2(t)$ (the function field in one variable), this will be true automatically (as every $\lambda \in \mathbb{F}_2(t) \setminus \mathbb{F}_2$ has infinite order, but $\widehat{U}$ is finite). Thus we can start with $U = (\mathbb{F}_2)^2$, and we get an infinitely increasing chain of generic symmetry groups.

By Lemma 4.2, any generating point $v \in \mathrm{Gens}(V)$ defines a representation

$$D_v \colon \mathrm{Sym}(G,v) \to \mathrm{GL}(V).$$

We now consider the restrictions to the generic symmetry group, $\mathrm{Sym}(G,V)$.

5.6 Lemma. *The character of the restriction* $D_v\colon \mathrm{Sym}(G,V) \to \mathrm{GL}(V)$ *is independent of* $v \in \mathrm{Gens}(V)$.

Proof. Let $\pi \in \mathrm{Sym}(G,V)$ be a generic symmetry, and let $A(X) = D_X(\pi) \in \mathrm{GL}(GX)$ be the matrix realizing π as an orbit symmetry of the vector of indeterminates $X \in \mathbb{K}(X)^d$. By Lemma 5.1, $A(X)$ evaluates to $A(v) = D_v(\pi)$ for any $v \in \mathrm{Gens}(V)$. Thus the rational function $f(X) = \mathrm{Tr}(A(X)) \in \mathbb{K}(X)$ evaluates to $f(v) = \mathrm{Tr}(D_v(\pi))$. On the other hand, $A(X) = D_X(\pi)$ has finite order and thus $\mathrm{Tr}(A(X))$ is a sum of roots of unity. Thus $f(X)$ is algebraic over $\mathbb{K}$. Since $\mathbb{K}(X)/\mathbb{K}$ is purely transcendental, we conclude that $f(X) \in \mathbb{K}$, which means that $f(v) = \mathrm{Tr}(D_v(\pi))$ is independent of v. □

The next result does not hold in positive characteristic, as Example 5.5 shows. The result implies Theorem B from the introduction.

5.7 Corollary. *Let* $\mathbb{K}$ *be a field of characteristic* 0. *Let* v *and* $w \in \mathrm{Gens}(V)$. *Then the representations* D_X *and* D_v *are similar over* $\mathbb{K}(X)$, *and the representations* D_v *and* D_w *are similar over* $\mathbb{K}$, *that is, there exist* $S \in \mathrm{GL}(d, \mathbb{K}(X))$ *and* $T \in \mathrm{GL}(d, \mathbb{K})$ *such that*

$$D_v(\pi) = S^{-1} D_X(\pi) S = T^{-1} D_w(\pi) T$$

for all $\pi \in \mathrm{Sym}(G,V)$.

Proof. Representations over fields of characteristic zero are similar if and only if they have the same character [13, Ch. XVIII, Thm. 3]. Thus the result follows from Lemma 5.6. □

In our first paper, we proved the next result in the case $\mathbb{K} = \mathbb{R}$ [FL1, Theorem 5.5]. In fact, it holds for arbitrary fields. Moreover, this can be deduced from an old paper of Isaacs [8], in which he shows that $\mathrm{GL}(Gv) = D(G)$ for *some* point $v \in V$, if the field is infinite.

5.8 Theorem. *Let* $D\colon G \to \mathrm{GL}(V)$ *be an absolutely irreducible representation. Then* $\mathrm{GL}(Gv) = D(G)$ *for every generic point* $v \in V$.

Proof. Let $v, w \in \mathrm{Gens}(V)$ be arbitrary. By Lemma 5.6, the representations

$$D_v, D_w\colon \mathrm{Sym}(G,V) \to \mathrm{GL}(V)$$

have the same character. The representations D_v and D_w are absolutely irreducible, as D is absolutely irreducible. Since the character determines an irreducible representation up to equivalence [9, Corollary 9.22], D_v and D_w are equivalent. Thus there is a linear map S such that $D_v(\pi) = S^{-1} D_w(\pi) S$ for all $\pi \in \mathrm{Sym}(G,V)$. For $g \in G$, the group $\mathrm{Sym}(G,V)$ contains the permutation λ_g that maps $x \in G$

to gx, and we have $D_v(\lambda_g) = D(g) = D_w(\lambda_g)$. It follows that $S^{-1}D(g)S = D(g)$ for all $g \in G$. Since D is absolutely irreducible, this yields $S \in \mathbb{K}$ and thus $D_v(\pi) = D_w(\pi)$ for all π. It follows that $\hat{G} := D_v(\mathrm{Sym}(G, V))$ is independent of v, and thus $\hat{G} = \mathrm{GL}(Gv) = \mathrm{GL}(Gw)$ for all generic points v and w.

Now pick a point v that is generic for both G and $\hat{G}$. Then $\hat{G}v = Gv$ since $\hat{G} = \mathrm{GL}(Gv)$. Since v has trivial stabilizer in both groups, it follows that $\hat{G} = D(G)$. □

For later applications, we need the following technical corollary. It is essentially a reformulation of the last theorem.

5.9 Corollary. *If $D\colon G \to \mathrm{GL}(V)$ is absolutely irreducible, then*

$$D_v(\pi) = D(\pi(1)) \quad \textit{for all } v \in \mathrm{Gens}(V) \textit{ and } \pi \in \mathrm{Sym}(G, V).$$

Proof. Let w be generic for G. Let $\pi \in \mathrm{Sym}(G, V)$ and set $g = \pi(1)$. Then $D_w(\lambda_g^{-1}\pi)w = g^{-1}\pi(1)w = w$. By Theorem 5.8, we have $D_w(\lambda_g^{-1}\pi) = D(h)$ for some $h \in G$. Since w is generic for G and $D(h)w = w$, It follows that $\mathrm{id} = D(h) = D_w(\lambda_g^{-1}\pi)$. Thus $D_v(\pi) = D_w(\pi) = D_w(\lambda_g) = D(g)$ as claimed. □

6. Representation polytopes

Let G be a finite group and $D\colon G \to \mathrm{GL}(d, \mathbb{R})$ a real representation. The associated **representation polytope** $P(D)$ is the convex hull of the matrices $D(g)$ in the space $\mathbf{M}_d(\mathbb{R})$ of all $d \times d$-matrices [5]. Of course, a representation polytope is a very special orbit polytope, namely

$$P(D) = \mathrm{conv}\{D(g) \mid g \in G\} = \mathrm{P}(G, I),$$

where I is the identity matrix and $g \in G$ acts on the vector space of matrices by left multiplication with $D(g)$. However, in this section we show that representation polytopes are in fact generic orbit polytopes in a suitable space. We will see that their affine symmetry group is strictly bigger than G, except perhaps when G is an elementary 2-group.

More generally, we can apply the theory of the last sections to G acting on the $\mathbb{K}$-space generated by $D(G)$, where $D\colon G \to \mathrm{GL}(d, \mathbb{K})$ is a representation.

We need the following technical notion of equivalence between G-invariant subsets of vector spaces (or affine spaces).

6.1 Definition. Let G be an (abstract) finite group acting affinely (linearly) on two spaces V and W, and let $S \subseteq V$ and $T \subseteq W$ be G-invariant subsets. We say that S and T are **affinely G-equivalent** if there is an affine isomorphism $\alpha\colon \mathrm{Aff}(S) \to \mathrm{Aff}(T)$ such that $\alpha(S) = T$ and $\alpha(gs) = g\alpha(s)$ for all $s \in S$ and $g \in G$. We call S and T **linearly G-equivalent** when there is a linear isomorphism $\alpha\colon \mathrm{Span}(S) \to \mathrm{Span}(T)$ with these properties.

In characteristic 0, when S and T are affinely G-equivalent, then some translates of S and T are linearly G-equivalent.

This equivalence is stronger than mere affine equivalence. For example, if $G = D_4 = \langle t, s \mid s^2 = t^4 = 1, sts = t^{-1} \rangle$, the orbit polytope of a point v with $sv = v$ and the orbit polytope of a point w with $stw = w$ are affinely equivalent (both are squares), but not as G-sets. This follows from the fact that s fixes vertices of $\mathrm{P}(G, v)$, but not of $\mathrm{P}(G, w)$. Of course, in this case, there is an automorphism φ of the group mapping s to st, and so we can find an affine isomorphism $\alpha\colon \mathrm{P}(G, v) \to \mathrm{P}(G, w)$ with $\alpha(gx) = \varphi(g)\alpha(x)$. This leads to a weaker notion of equivalence [1], but we will not need this here.

For another example, let $G = C_4 \times V_4$ be the direct product of C_4, a cyclic group of order 4, and the Klein four group V_4. Both a square and a 3-simplex are orbit polytopes of C_4 and V_4, and thus we get the direct product of the square and the 3-simplex as an orbit polytope of G in two different ways. These are not affinely G-equivalent, not even in a weaker sense as in the last example.

6.2 Lemma. *Let $D\colon G \to \mathrm{GL}(d, \mathbb{K})$ be a representation and $A \in \mathrm{GL}(d, \mathbb{K})$. Then $G \cdot A$ and $G \cdot I$ are linearly G-equivalent. In particular, when $\mathbb{K} = \mathbb{R}$, then $\mathrm{P}(G, A)$ and $P(D) = \mathrm{P}(G, I)$ are linearly G-equivalent.*

Proof. Multiplication from the right with A yields an affine map from $G \cdot I$ (or $P(D) = \mathrm{P}(G, I)$) to $G \cdot A$ (or $\mathrm{P}(G, A)$) commuting with the left action of G, and multiplication with A^{-1} yields the inverse. □

The notions of the last sections apply to the subspace $V = \mathrm{Span}\{D(g) \mid g \in G\} \leqslant \mathbf{M}_d(\mathbb{K})$ generated by the image of a representation. Of course, this subspace is in general (much) smaller than the space of all matrices. (We have $V = \mathbf{M}_d(\mathbb{K})$ if and only if D is *absolutely irreducible* [9, Theorem 9.2].)

6.3 Proposition. *Let $D\colon G \to \mathrm{GL}(d, \mathbb{K})$ be a representation and let*

$$V = \mathrm{Span}(D(G)) \leqslant \mathbf{M}_d(\mathbb{K})$$

be the subspace generated by the image of G. If $A \in V$ is a generating point for G, then $G \cdot A$ and $G \cdot I$ are linearly G-equivalent. In particular, all generating points are generic, and all generic orbits are linearly equivalent.

Proof. From $I \in V = \mathrm{Span}\{D(g)A \mid g \in G\}$ it follows that $I = \sum_g r_g D(g)A$ for some $r_g \in \mathbb{K}$. But then A is invertible with inverse $\sum_g r_g D(g)$. The first claim follows from Lemma 6.2. Since all full-dimensional orbits in V are linearly G-isomorphic, their linear symmetry groups are conjugate, and its vertices have stabilizer $\mathrm{Ker}(D)$. Thus all generating points are generic. □

We mention in passing that $A \in V$ is a generating point in V for G if and only if it is invertible. This follows since V is a subalgebra of $\mathbb{K}^{d\times d}$.

In particular, the representation polytope $P(D)$ itself is generic in its space. The affine symmetry group of a representation polytope is always bigger than $D(G)$, except perhaps when G is an elementary abelian 2-group:

6.4 Proposition. *Let $D\colon G \to \mathrm{GL}(d,\mathbb{K})$ be a representation. Then the generic symmetry group $Sym(G, \mathrm{Span}(D(G)))$ contains the following maps:*

(i) *for every $h \in G$, the map sending g to hg,*

(ii) *for every $h \in G$, the map sending g to gh.*

In the case $\mathbb{K} = \mathbb{R}$, the generic symmetry group contains also

(iii) *the map sending $D(g)$ to $D(g^{-1})$.*

Thus $|\mathrm{Sym}(G,V)| \geqslant |G||G : \mathbf{Z}(G)|$, and for representation polytopes (that is, $\mathbb{K} = \mathbb{R}$) we have $|\mathrm{AGL}(P(D))| \geqslant 2|G||G : \mathbf{Z}(G)|$, except possibly when G is an elementary abelian 2-group.

Proof. By Proposition 6.3, $\mathrm{Sym}(G, \mathrm{Span}(D(G))) = \mathrm{Sym}(G, I)$. Left and right multiplication by $D(h)$ is a linear map on $\mathbb{K}^{d\times d}$ and permutes the generic orbit $D(G) = D(G) \cdot I$, thus (i) and (ii).

To see (iii), assume first that $D(g)$ is orthogonal for all $g \in G$. Then the linear map sending a matrix A to its transposed matrix A^t sends $D(g)$ to $D(g)^t = D(g^{-1})$ and thus maps $P(D)$ onto itself.

In general, the representation D is similar to an orthogonal one [7, Theorem 2.13], so there is a non-singular matrix S such that $S^{-1}D(g)S$ is orthogonal for all $g \in G$. Then the linear map $A \mapsto S(S^{-1}AS)^tS^{-1}$ sends $D(g)$ to $S(S^{-1}D(g)S)^tS^{-1} = S(S^{-1}D(g)S)^{-1}S^{-1} = D(g^{-1})$.

For every $g \in G$, let $\lambda(g) \in \mathrm{Sym}(G)$ be left multiplication with g, and $\varrho(g) \in \mathrm{Sym}(G)$ right multiplication with g. Every $\lambda(g)$ commutes with every $\varrho(h)$. We have $\lambda(g)\varrho(h) = \mathrm{id}_G$ if and only if $gxh = x$ for all $x \in G$, which is the case if and only if $g = h^{-1}$ and $g \in \mathbf{Z}(G)$. Thus $|\lambda(G)\varrho(G)| = |G||G : \mathbf{Z}(G)|$.

Finally, the map ε sending x to x^{-1} is in $\lambda(G)\varrho(G)$ if and only if there are g and $h \in G$ such that $x^{-1} = gxh$ for all $x \in G$. The case $x = 1$ yields then $g = h^{-1}$, and we have $(xy)^{-1} = (xy)^h = x^{-1}y^{-1}$ for all x, $y \in G$. Thus G is abelian and every element has order 2. Thus G is an elementary abelian 2-group. In every other case, we have $|\langle \varepsilon, \lambda(G), \varrho(G)\rangle| \geqslant 2|G||G : \mathbf{Z}(G)|$. □

6.5 Remark. The map ε above normalizes $\lambda(G)\varrho(G)$. Thus $\langle \varepsilon, \lambda(G), \varrho(G)\rangle$ has order $2|G||G : \mathbf{Z}(G)|$, except when G is an elementary abelian 2-group.

There exist representation polytopes of elementary abelian 2-groups that have no additional affine symmetries (Chapter IV, Section 1).

When $\mathbb{K} \neq \mathbb{R}$, then the map in (iii) is in general not an orbit symmetry. For example, for

$$C_4 \times C_2 \cong G = \langle \operatorname{diag}(1,-1,i), \operatorname{diag}(-1,1,1) \rangle \subseteq \mathrm{GL}(3,\mathbb{C}),$$

we have $\operatorname{Sym}(G,I) = \lambda(G)$. (This can be verified using Theorem E, which will be proved as Corollary 9.6 below.)

7. Generic symmetries and left ideals

In the following, we will characterize generic symmetries in terms of left ideals of the group algebra $\mathbb{K}G$. For a left $\mathbb{K}G$-module V and $v \in V$, we set

$$\operatorname{Ann}(v) := \operatorname{Ann}_{\mathbb{K}G}(v) := \{a \in \mathbb{K}G \colon av = 0\},$$

the annihilator of v in $\mathbb{K}G$. This is a left ideal of $\mathbb{K}G$.

Note that G is a basis of $\mathbb{K}G$, and so any permutation $\pi \in \operatorname{Sym}(G)$ uniquely extends to an automorphism of the $\mathbb{K}$-vector space $\mathbb{K}G$, which we will also denote by π.

7.1 Lemma. *Let $v \in \operatorname{Gens}(V)$ and $\pi \in \operatorname{Sym}(G)$. Then $\pi \in \operatorname{Sym}(G,v)$ if and only if $\pi(\operatorname{Ann}(v)) \subseteq \operatorname{Ann}(v)$.*

Proof. Let $\kappa_v \colon \mathbb{K}G \to V$ be the map defined by $\kappa_v(a) = av$. This is a homomorphism of left $\mathbb{K}G$-modules with kernel $\operatorname{Ann}(v)$. Since we assume that $v \in \operatorname{Gens}(V)$, we have $V = \mathbb{K}Gv$ and so κ_v is surjective and induces an isomorphism $V \cong \mathbb{K}G/\operatorname{Ann}(v)$.

By definition, π is an orbit symmetry for v, if and only if there is a linear map $\alpha \colon V \to V$, such that $\alpha(gv) = \pi(g)v$ for all $g \in G$. This means that α makes the following diagram commute:

$$\begin{array}{ccc} \mathbb{K}G & \xrightarrow{\pi} & \mathbb{K}G \\ \downarrow{\scriptstyle \kappa_v} & & \downarrow{\scriptstyle \kappa_v} \\ V & \xrightarrow{\alpha} & V \end{array}$$

Since κ_v is surjective, such an α exists if and only if $\operatorname{Ann}(v) = \operatorname{Ker}\kappa_v \subseteq \operatorname{Ker}(\kappa_v \circ \pi)$. The last equality is equivalent to $\pi(\operatorname{Ann}(v)) \subseteq \operatorname{Ann}(v)$, as π is invertible. □

7.2 Lemma. *Let $\pi \in \operatorname{Sym}(G)$ and $v \in \operatorname{Gens}(V)$, and set $L = \operatorname{Ann}(v)$. Then the following are equivalent:*

(i) $\pi \in \operatorname{Sym}(G,V)$,
(ii) $\pi(Ls) \subseteq Ls$ *for all units* $s \in (\mathbb{K}G)^\times$,
(iii) $\pi(\widetilde{L}) \subseteq \widetilde{L}$ *for every left ideal* $\widetilde{L}$ *that is isomorphic to* L *(as left* $\mathbb{K}G$*-module).*

Proof. We begin with "(i) $\Longrightarrow$ (iii)". Let $\pi \in \mathrm{Sym}(G, V)$ and assume that $L \cong \widetilde{L}$ as left $\mathbb{K}G$-modules. We claim that also $\mathbb{K}G/L \cong \mathbb{K}G/\widetilde{L}$ (as left $\mathbb{K}G$-modules). This is clear if $\mathbb{K}G$ is semisimple (which is the only case where we will apply this lemma), but is also true for Frobenius rings [11, Theorem 15.21], and $\mathbb{K}G$ is a Frobenius ring [11, Example 3.15E]. Thus $V = \mathbb{K}Gv \cong \mathbb{K}G/L \cong \mathbb{K}G/\widetilde{L}$, and $\mathrm{Sym}(G, V) = \mathrm{Sym}(G, \mathbb{K}G/\widetilde{L})$. As $\widetilde{L}$ is the annihilator of $1 + \widetilde{L}$ in $\mathbb{K}G$, Lemma 7.1 yields that $\pi(\widetilde{L}) \subseteq \widetilde{L}$.

That (iii) implies (ii) is clear since $Ls \cong L$.

Now assume (ii), and let $w \in \mathrm{Gens}(V)$ be another generator. By a theorem of Bass [12, 20.9] it follows that $v = sw$ for a *unit* $s \in (\mathbb{K}G)^\times$. Thus $\mathrm{Ann}(w) = \mathrm{Ann}(v)s = Ls$. Then Lemma 7.1 yields that $\pi \in \mathrm{Sym}(G, w)$, and thus $\pi \in \mathrm{Sym}(G, V)$. □

Let us mention in passing that in a Frobenius ring, every left ideal isomorphic to A is of the form As with some unit s [11, Proposition 15.20].

7.3 Corollary. *Suppose that* $\mathrm{Ann}(v)$ *is a (twosided) ideal of* $\mathbb{K}G$*, where* $v \in \mathrm{Gens}(V)$*. Then* $\mathrm{Sym}(G, w) = \mathrm{Sym}(G, v)$ *for all* $w \in \mathrm{Gens}(V)$*, and in fact all* $w \in \mathrm{Gens}(V)$ *are generic.*

Proof. The first assertion is immediate from Lemmas 7.1 and 7.2. The stabilizer in G of a point v is the set of $g \in G$ such that $g - 1 \in \mathrm{Ann}(v)$, and $\mathrm{Ann}(w) = \mathrm{Ann}(v)s = \mathrm{Ann}(v)$ for all $w \in \mathrm{Gens}(V)$. Thus all $w \in \mathrm{Gens}(V)$ are generic. □

7.4 Remark. The last corollary is in fact a restatement of Proposition 6.3. Let $D\colon G \to \mathrm{GL}(V)$ be the representation corresponding to the $\mathbb{K}G$-module V. When $\mathrm{Ann}(v)$ is an ideal for $v \in \mathrm{Gens}(V)$, then the map $V \to \mathrm{End}_{\mathbb{K}}(V)$ that sends $\sum_g c_g gv$ to $\sum_g c_g D(g)$ is well-defined and shows that $Gv \subseteq V$ and $D(G) \subseteq \mathrm{End}\, V$ are linearly G-equivalent.

Although very simple, Lemma 7.2 has quite remarkable consequences. For example, when π is a generic symmetry for the cyclic modules $\mathbb{K}G/L_1$ and $\mathbb{K}G/L_2$, where L_1 and L_2 are left ideals, then it is immediate from the characterization in Lemma 7.2 that π is also generic for the modules $\mathbb{K}G/(L_1 \cap L_2)$ and $\mathbb{K}G/(L_1 + L_2)$.

Also, when π is generic for $\mathbb{K}G/L$, and I is any left ideal which we get by repeatedly taking intersections and sums of left ideals isomorphic to L, then π is generic for $\mathbb{K}G/I$. For example, we can take for I the sum of all left ideals isomorphic to L. This will be used below in the case where $\mathbb{K}$ has characteristic zero.

8. Orbit polytopes as subsets of the group algebra

In this section, we assume that $\mathbb{K}$ is a field of characteristic 0. Then by Maschke's theorem, the group algebra $\mathbb{K}G$ is semisimple. (More generally, this remains true

when the characteristic of $\mathbb{K}$ does not divide the group order $|G|$. Some of the following holds in this greater generality, too.) Suppose that V is a cyclic $\mathbb{K}G$-module and $v \in \mathrm{Gens}(V)$. Since $\mathbb{K}G$ is semisimple, the annihilator $\mathrm{Ann}_{\mathbb{K}G}(v)$ has a complement L (say) in $\mathbb{K}G$, so that

$$\mathbb{K}G = L \oplus \mathrm{Ann}(v)$$

as left $\mathbb{K}G$-module. To this decomposition corresponds a decomposition $1 = e + f$ into idempotents e, f (that is, $e^2 = e$ and $f^2 = f$), with $L = \mathbb{K}Ge$ and $\mathrm{Ann}(v) = \mathbb{K}Gf$. The homomorphism $\mathbb{K}G \to V$ sending $a \in \mathbb{K}G$ to av induces an isomorphism $L \cong V$ which sends e to v. In particular, $\mathrm{Sym}(G, v) = \mathrm{Sym}(G, e)$. It is thus enough to be able to compute $\mathrm{Sym}(G, e)$ for idempotents e of the group algebra.

Conversely, each left ideal L of $\mathbb{K}G$ is generated by an idempotent e. Thus a $\mathbb{K}G$-module is cyclic if and only if it is isomorphic to a left ideal of $\mathbb{K}G$.

There are only a finite number of non-isomorphic simple left $\mathbb{K}G$-modules, say $S_1, \ldots, S_r$ [13, Ch. XVII, § 4]. Every $\mathbb{K}G$-module V of finite dimension over $\mathbb{K}$ is isomorphic to a direct sum $m_1S_1 \oplus \cdots \oplus m_rS_r$, where the multiplicities $m_i \in \mathbb{N}$ are uniquely determined by the isomorphism type of V. If $W \cong n_1S_1 \oplus \cdots \oplus n_rS_r$ is another left $\mathbb{K}G$-module, then V is isomorphic to a submodule of W if and only if $m_i \leqslant n_i$ for all i.

In particular, we can write $\mathbb{K}G \cong d_1S_1 \oplus \cdots \oplus d_rS_r$ with $d_i \in \mathbb{N}$. We have seen before that a module V has the form $V = \mathbb{K}Gv$, if and only if it is isomorphic to a submodule (that is, a left ideal) of the regular module $\mathbb{K}G$. Thus $V = m_1S_1 \oplus \cdots \oplus m_rS_r$ is cyclic as $\mathbb{K}G$-module if and only if $m_i \leqslant d_i$ for all i. In particular, there are only finitely many isomorphism classes of cyclic $\mathbb{K}G$-modules, and every possible orbit of G under *some* representation is contained in one of these cyclic modules, up to linear G-equivalence.

If we want to consider the situation only up to affine G-equivalence, then by Lemma 2.2 we may assume that $\sum_g gv = 0$. This means that the corresponding cyclic $\mathbb{K}G$-module does not contain the trivial module as constituent. Conversely, if $V = \mathrm{Aff}(Gv)$ for some orbit Gv, then $\sum_g gv = 0$ by Lemma 2.2, and the trivial module is not a constituent of V. Thus we have proved the following result (which holds as long as $\mathrm{Char}(\mathbb{K})$ does not divide $|G|$):

8.1 Theorem. *Let $S_1 = \mathbb{K}$ (the trivial module), $S_2, \ldots, S_r$ be a set of representatives of the different isomorphism classes of simple left $\mathbb{K}G$-modules, and let V be an arbitrary left $\mathbb{K}G$-module. Write*

$$V \cong m_1S_1 \oplus \cdots \oplus m_rS_r \quad \text{and} \quad \mathbb{K}G \cong d_1S_1 \oplus \cdots \oplus d_rS_r.$$

Then $V = \mathbb{K}Gv = \mathrm{Span}(Gv)$ for some $v \in V$ if and only if $m_i \leqslant d_i$ for all i, and $V = \mathrm{Aff}(Gv)$ for some $v \in V$ if and only if additionally $m_1 = 0$.

Now let V be a module not necessarily containing full-dimensional orbits. Suppose that $m = \dim(\mathbb{K}Gv_0)$ is the maximal possible dimension of a cyclic submodule of V. In Lemma 4.10 we showed that for "almost all" vectors $v \in V$, the subspace $\mathbb{K}Gv$ has the maximal possible dimension (namely, the set of such v is nonempty and Zariski-open). The general structure theory of semisimple rings yields also that all cyclic submodules of maximal dimension are isomorphic:

8.2 Proposition. *Let V be a finite dimensional $\mathbb{K}G$-module and set*

$$m := \max\{\dim_{\mathbb{K}}(\mathbb{K}Gv) \mid v \in V\}.$$

If $\dim_{\mathbb{K}}(\mathbb{K}Gv_1) = \dim_{\mathbb{K}}(\mathbb{K}Gv_2) = m$, then $\mathbb{K}Gv_1 \cong \mathbb{K}Gv_2$ as $\mathbb{K}G$-modules.

Proof. Let m_i and d_i be as before and set $e_i := \min\{m_i, d_i\}$. The multiplicity of S_i in any cyclic submodule $\mathbb{K}Gv \leqslant V$ is bounded from above by e_i. Thus the dimension of such a submodule over $\mathbb{K}$ is bounded from above by $e_1 \dim_{\mathbb{K}} S_1 + \cdots + e_r \dim_{\mathbb{K}} S_r$.

Since $e_i \leqslant m_i$, the module V has a submodule $W \cong e_1S_1 \oplus \cdots \oplus e_rS_r$, which is also isomorphic to a submodule of $\mathbb{K}G$. Then there is $v \in W \leqslant V$ such that $W = \mathbb{K}Gv = \operatorname{Span}\{gv \mid g \in G\}$. This shows that

$$e_1 \dim_{\mathbb{K}} S_1 + \cdots + e_r \dim_{\mathbb{K}} S_r = m,$$

and if $m = \dim_{\mathbb{K}}(\mathbb{K}Gv)$, then $\mathbb{K}Gv \cong e_1S_1 \oplus \cdots \oplus e_rS_r$. □

As a consequence, we can define generic points in arbitrary $\mathbb{K}G$-modules as points generating a submodule of the maximal possible dimension, and being generic in this submodule. Then all generic points v have the same orbit symmetry group $\operatorname{Sym}(G, v)$.

For the rest of this section, we assume that $\mathbb{K}$ is a subfield of $\mathbb{C}$, the field of complex numbers. However, the results remain valid for arbitrary fields of characteristic 0: Suppose that V is a cyclic $\mathbb{K}G$-module, where $\mathbb{K}$ is arbitrary of characteristic zero. By Corollary 4.20, we have $\operatorname{Sym}(G, V) = \operatorname{Sym}(G, V \otimes_{\mathbb{K}} \overline{\mathbb{K}})$, where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$. But over an algebraically closed field, any representation is similar to a representation with entries in $\overline{\mathbb{Q}}$, the algebraic closure of the rational numbers $\mathbb{Q}$ (which embeds into $\overline{\mathbb{K}}$). This means that there is a module V_0 over $\overline{\mathbb{Q}}G$ such that $V \otimes_{\mathbb{K}} \overline{\mathbb{K}} \cong V_0 \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{K}}$. By Lemma 4.8 and Corollary 4.20, we have

$$\operatorname{Sym}(G, V) = \operatorname{Sym}(G, V \otimes_{\mathbb{K}} \overline{\mathbb{K}}) = \operatorname{Sym}(G, V_0 \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{K}}) = \operatorname{Sym}(G, V_0).$$

Thus we can assume without loss of generality that $\mathbb{K} \subseteq \overline{\mathbb{Q}}$, or $\mathbb{K} \subseteq \mathbb{C}$.

The group algebra $\mathbb{C}G$ has a canonical inner product defined by $\langle g, h\rangle = \delta_{gh}$ for $g, h \in G$. For $a, b \in \mathbb{C}G$ we can write this scalar product as $\langle a, b\rangle = \lambda(ab^*)$, where

$\left(\sum_g b_g g\right)^* = \sum_g \overline{b_g} g^{-1}$ and $\lambda\left(\sum_g b_g g\right) = b_1$. Notice that $*$ defines an involution of $\mathbb{C}G$, that is, $a^{**} = a$ and $(ab)^* = b^* a^*$.

This inner product can be used to show that any left ideal of $\mathbb{C}G$ has a left ideal complement (Maschke's theorem for $\mathbb{C}G$): namely, the orthogonal complement of a (left) ideal is again a (left) ideal. We have the following characterization of idempotents corresponding to such orthogonal decompositions:

8.3 Lemma. *Let $e \in \mathbb{C}G$ be an idempotent. The decomposition*

$$\mathbb{C}G = \mathbb{C}Ge \oplus \mathbb{C}G(1-e)$$

is orthogonal if and only if $e^* = e$.

Proof. If $e^* = e$, then

$$\langle a(1-e), be\rangle = \lambda(a(1-e)e^*b^*) = \lambda(a(1-e)eb^*) = 0$$

for all a, $b \in \mathbb{C}G$, so the decomposition is orthogonal.

Conversely, when the decomposition is orthogonal, then $0 = \langle a(1-e), e\rangle = \langle a, e(1-e)^*\rangle$ for all $a \in \mathbb{C}G$, and thus $0 = e(1-e^*)$. Thus $e = ee^*$ and $e^* = (ee^*)^* = ee^* = e$ as claimed. □

8.4 Lemma. *Let $e \in \mathbb{C}G$ be an idempotent with $e^* = e$ and $\pi \in \mathrm{Sym}(G)$. Then the following are equivalent:*

(i) $\pi \in \mathrm{Sym}(G, e)$,
(ii) $\pi \in \mathrm{Sym}(G, 1-e)$,
(iii) $\pi(ge) = \pi(g)e$ *for all $g \in G$. (Here we view π as a linear map $\mathbb{C}G \to \mathbb{C}G$.)*

Proof. Notice that $\mathrm{Ann}(e) = \mathbb{C}G(1-e)$ and $\mathrm{Ann}(1-e) = \mathbb{C}Ge$. By Lemma 7.1, $\pi \in \mathrm{Sym}(G, 1-e)$ if and only if $\pi(\mathbb{C}Ge) \subseteq \mathbb{C}Ge$. But as $\mathbb{C}G(1-e) = (\mathbb{C}Ge)^\perp$ and $\pi\colon \mathbb{C}G \to \mathbb{C}G$ is unitary, this is equivalent to $\pi(\mathbb{C}G(1-e)) \subseteq \mathbb{C}G(1-e)$ and thus to $\pi \in \mathrm{Sym}(G, e)$. This shows the equivalence of (i) and (ii).

It is clear that (iii) implies $\pi(\mathbb{C}Ge) \subseteq \mathbb{C}Ge$ and thus (ii) (by Lemma 7.1 again).

Conversely, assume (i) and (ii). Then $\pi(ge) \in \mathbb{C}Ge$ and $\pi(g(1-e)) \in \mathbb{C}G(1-e)$. Thus

$$\pi(g)e = \pi(ge)e + \pi(g(1-e))e = \pi(ge),$$

as claimed. □

Note that the vector configuration $\{g(1-e) \mid g \in G\}$ is just the dual one to (the Gale diagram of) $\{ge \mid g \in G\}$ [26, Chapter 6]. (We think here especially of the case of orbit polytopes.). One should notice, however, that it is possible that e has a nontrivial stabilizer $H > 1$, while the stabilizer of $(1-e)$ is trivial. Indeed, if

$ge = e$ and $g(1-e) = 1-e$, then $g = g \cdot 1 = ge + g(1-e) = e + (1-e) = 1$. Thus the intersection of the two stabilizers is always trivial.

If H is the stabilizer of e, then every permutation of G which maps each left coset of H to itself is in $\mathrm{Sym}(G, e) = \mathrm{Sym}(G, (1-e))$. Such a permutation induces the identity on $\mathbb{C}Ge$ (or $\mathbb{R}Ge$), but in general induces a non-identity symmetry on $\mathbb{C}G(1-e)$. For example, we may view a tetrahedron as an orbit polytope of the symmetric group S_4, so that S_3 stabilizes a vertex. The dual of this polytope has dimension $24 - 1 - 3 = 20$, has 24 vertices and affine symmetry group of order $24 \cdot 6^4$.

It is maybe interesting that one can give a concrete formula for the idempotent e in the last lemma. In the next result, one can of course replace $\mathbb{C}$ by any subfield $\mathbb{K}$.

8.5 Theorem. *Let $D\colon G \to \mathrm{GL}(d, \mathbb{C})$ be a representation, let $V = \mathbb{C}^d$ be the corresponding $\mathbb{C}G$-module and $v \in \mathrm{Gens}(V)$. Set*

$$Q := \sum_{g \in G} (D(g)v)(D(g)v)^* \in \mathbb{C}^{d \times d}$$
$$\text{and} \quad e := \sum_{g \in G} \Big((D(g)v)^* Q^{-1} v \Big) \cdot g \in \mathbb{C}G.$$

Then e is an idempotent with $ev = v$, $\mathbb{C}Ge \cong V$ as $\mathbb{C}G$-modules and $e = e^*$.

The last equation means that $\mathbb{C}G = \mathbb{C}Ge \oplus \mathbb{C}G(1-e)$ is an *orthogonal* direct sum. Notice that Q is defined as in Remark 4.16.

Proof of Theorem 8.5. Define a map $\mu\colon V \to \mathbb{C}G$ by

$$\mu(w) = \sum_{g \in G} \Big((D(g)v)^* Q^{-1} w \Big) \cdot g, \quad w \in V.$$

Notice that $e = \mu(v)$. First we show that μ is a homomorphism of $\mathbb{C}G$-modules: We begin by observing that $D(h)^{-1} Q = Q D(h)^*$ for $h \in G$, which yields $Q^{-1} D(h) = D(h^{-1})^* Q^{-1}$. Thus for $h \in G$ and $w \in V$, we have

$$\begin{aligned}
\mu(D(h)w) &= \sum_{g \in G} \Big((D(g)v)^* Q^{-1} D(h) w \Big) g \\
&= \sum_{g \in G} \Big((D(g)v)^* D(h^{-1})^* Q^{-1} w \Big) g \\
&= \sum_{g \in G} \Big((D(h^{-1}g)v)^* Q^{-1} w \Big) g \\
&= \sum_{\tilde{g} \in G} \Big((D(\tilde{g})v)^* Q^{-1} w \Big) h\tilde{g} = h\mu(w).
\end{aligned}$$

Next we show that $\mu(w)v = w$ for all $w \in V$:

$$\begin{aligned}\mu(w)v &= \sum_{g\in G} \Big((D(g)v)^* Q^{-1} w\Big) D(g)v \\ &= \sum_{g\in G} (D(g)v) \cdot (D(g)v)^* Q^{-1} w = QQ^{-1}w = w.\end{aligned}$$

In particular, $ev = \mu(e)v = v$, and $e^2 = e\mu(v) = \mu(ev) = \mu(v) = e$.

Moreover, it follows that μ is injective, and is an isomorphism from V onto

$$\mu(V) = \mu(\mathbb{C}Gv) = \mathbb{C}G\mu(v) = \mathbb{C}Ge.$$

Finally, we have

$$\begin{aligned}e^* = \sum_g \overline{\Big((D(g)v)^* Q^{-1} v\Big)} g^{-1} &= \sum_g \Big((D(g)v)^* Q^{-1} v\Big)^* g^{-1} \\ &= \sum_g \Big(v^* Q^{-1} D(g) v\Big) g^{-1} \\ &= \sum_g \Big(v^* D(g^{-1})^* Q^{-1} v\Big) g^{-1} \\ &= \sum_g \Big((D(g^{-1})v)^* Q^{-1} v\Big) g^{-1} = e,\end{aligned}$$

where we have used again that $Q^{-1}D(g) = D(g^{-1})^* Q^{-1}$. □

The map μ of the last proof is a splitting of the left module homomorphism $\kappa\colon \mathbb{C}G \to V$ defined by $\kappa(a) = av$, since we have seen that $\mu(w)v = w$ for all $w \in V$. Moreover, $a \mapsto (\mu(\kappa(a)) = ae$ is the orthogonal projection from $\mathbb{C}G$ onto $\mathbb{C}Ge$.

9. Representation polytopes as subsets of the group algebra

In this section we characterize representation polytopes among orbit polytopes, and we show how to compute their affine symmetries from a certain character. More generally, we show how the *linear preservers* of a finite matrix group in characteristic zero are determined by a certain character of that group. We assume throughout that $\mathbb{K}$ is a field of characteristic 0. We begin with a lemma.

9.1 Lemma. *Let $e \in \mathbb{K}G$ be an idempotent and $L = \mathbb{K}Ge$. Then the following are equivalent:*

(i) *$e \in \mathbf{Z}(\mathbb{K}G)$,*

(ii) *L is an ideal of $\mathbb{K}G$,*

(iii) *The orbit Ge is linearly G-equivalent to $D(G)$ for some representation $D\colon G \to \mathrm{GL}(n, \mathbb{K})$.*

Proof. The equivalence of (i) and (ii) holds for arbitrary semisimple rings and is well known [12, Exercise 22.3B]. For completeness, we give a proof: Assume that Ae is an ideal of $A := \mathbb{K}G$ and set $f = 1 - e$. Then $eAf \subseteq Aef = \{0\}$. Thus we also have $(AfAeA)^2 = AfAeAfAeA = AfA0AeA = \{0\}$ and $AfAeA$ is a nilpotent ideal. Since A is semisimple, we have $fAe = \{0\}$. Thus $ea = ea(e + f) = eae = (e + f)ae = ae$ for $a \in A$, and $e \in \mathbf{Z}(A)$. Thus (ii) implies (i), and the converse is trivial.

If $e \in \mathbf{Z}(\mathbb{K}G)$, then $\mathbb{K}G(1 - e)$ is also an ideal and there is a representation D such that D as algebra homomorphism $\mathbb{K}G \to \mathbf{M}_n(\mathbb{K})$ has kernel $\mathbb{K}G(1 - e)$. (For example, we can take the representation corresponding to the action of G on $\mathbb{K}Ge$.) Then D yields a linear isomorphism of G-sets from Ge onto $D(G)$.

Conversely, assume that $D\colon G \to \mathrm{GL}(n, \mathbb{K})$ is a representation and $\alpha\colon \mathbb{K}Ge \to \mathbf{M}_n(\mathbb{K})$ is linear and injective such that $\alpha(ge) = D(g)$ for all $g \in G$. Then

$$\alpha\left(\sum_{g\in G} a_g ge\right) = \sum_{g\in G} a_g \alpha(ge) = \sum_{g\in G} a_g D(g) = D\left(\sum_{g\in G} a_g g\right).$$

Again, write $f = (1 - e)$ and $A = \mathbb{K}G$. We have $D(e) = \alpha(e \cdot e) = \alpha(e) = I$ and $D(f) = \alpha(fe) = \alpha(0) = 0$. Thus the kernel of D as a map $D\colon A \to \mathbf{M}_n(\mathbb{K})$ is exactly Af. Thus Af is a two-sided ideal of A and so $f \in \mathbf{Z}(A)$, and thus also $e = 1 - f \in \mathbf{Z}(A)$. □

9.2 Remark. Let $V = \mathbb{K}Ge$. In the notation of Theorem 8.1, $e \in \mathbf{Z}(\mathbb{R}G)$ if and only if each multiplicity m_i of the simple module S_i in V is either 0 or d_i (the multiplicity of S_i in $\mathbb{K}G$).

We notice here a consequence for orbit polytopes ($\mathbb{K} = \mathbb{R}$):

9.3 Corollary. *Let G be a finite group. The following are equivalent:*

(i) *Every orbit polytope for G is affinely G-equivalent to a representation polytope.*
(ii) *The group algebra $\mathbb{R}G$ is a direct product of division rings.*
(iii) *G is an abelian group or a direct product of the quaternion group of order 8 with an elementary abelian 2-group.*

Proof. A semisimple ring in general is (by Wedderburn-Artin) a direct product of matrix rings over division rings, and is thus a direct product of division rings if and only if all idempotents are central. By Section 8, every orbit polytope is linearly equivalent to an orbit polytope $\mathrm{P}(G, e)$ of an idempotent $e \in \mathbb{R}G$. Thus Lemma 9.1 yields the first equivalence.

That $\mathbb{R}G$ is a direct product of division rings if and only if G is abelian or $G \cong Q_8 \times (C_2)^r$ for some r will be proved below (Theorem 4.6 in Chapter III) as a consequence of more general results. □

9.4 Remark. Sehgal [25] has characterized groups G such that $\mathbb{Q}G$ is a direct product of division rings (Theorem 4.5 in Chapter III). Thus we have a similar result for orbit polytopes with rational vertices, or even lattice polytopes.

The central idempotents of the group algebra can be described using the irreducible characters. We first recall the description of the central idempotents in the complex group algebra $\mathbb{C}G$. As usual, we write $\operatorname{Irr} G$ for the set of complex irreducible characters of a group G. To every $\chi \in \operatorname{Irr} G$ corresponds the central idempotent [9, Theorem 2.12]

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g.$$

An arbitrary idempotent in $\mathbf{Z}(\mathbb{C}G)$ is the sum of some of these. Thus each idempotent e in $\mathbf{Z}(\mathbb{C}G)$ has the form

$$e = \frac{1}{|G|} \sum_{g \in G} \gamma(g^{-1})g \quad \text{with} \quad \gamma = \sum_{\chi \in S} \chi(1)\chi \quad \text{for some} \quad S \subseteq \operatorname{Irr} G.$$

This γ is actually the character of the ideal $\mathbb{C}Ge$ as left $\mathbb{C}G$-module.

For $e \in \mathbf{Z}(\mathbb{R}G)$, we get the same conclusion, with the additional requirement that χ and its complex conjugate $\overline{\chi}$ are either both in S or both not. For more general fields $\mathbb{K}$, the set S must be closed under Galois automorphisms over $\mathbb{K}$. Notice that it is not really a loss of generality to assume $\mathbb{K} \subseteq \mathbb{C}$ here.

9.5 Proposition. *Let I be an ideal of $\mathbb{K}G$, and suppose that γ is the character of I as left $\mathbb{K}G$-module, where $\mathbb{K}$ has characteristic zero. Then the permutation $\pi\colon G \to G$ is in $\operatorname{Sym}(G, I)$ if and only if*

$$\gamma(\pi(g)^{-1}\pi(h)) = \gamma(g^{-1}h) \quad \textit{for all} \quad g, h \in G.$$

(For example, this holds if π is a group automorphism of G fixing γ.)

Proof. Let e be the (unique) idempotent such that $I = \mathbb{K}Ge$. Then

$$e = \frac{1}{|G|} \sum_{g \in G} \gamma(g^{-1})g$$

by the remarks above. The annihilator of e in $\mathbb{K}G$ is $\mathbb{K}G(1-e)$, an ideal. Thus every generator of I is generic and we have $\operatorname{Sym}(G, I) = \operatorname{Sym}(G, e)$. Since $\mathbb{K}G(1-e)$ is

the only complement of I as left $\mathbb{K}G$-module, it is also the orthogonal complement of I. Thus Lemma 8.4 applies to e. It follows that $\pi \in \mathrm{Sym}(G, e)$ if and only if $\pi(ge) = \pi(g)e$ for all $g \in G$. Now the result follows by comparing the coefficients of $\pi(h)^{-1}$ in this equation. □

Given a representation $D\colon G \to \mathrm{GL}(n, \mathbb{K})$ (with $\mathbb{K} \subseteq \mathbb{C}$), we write $\mathrm{Irr}\, D$ for the set of (complex) irreducible constituents of the character of D. Then the kernel of D, viewed as algebra homomorphism $\mathbb{K}G \to \mathbf{M}_d(\mathbb{K})$, is $\mathbb{K}G(1-e)$, where e is the sum of those e_χ such that $\chi \in \mathrm{Irr}\, D$. As a corollary of Proposition 9.5, we get a characterization of the *linear preservers* of a finite matrix group.

9.6 Corollary. *Let $D\colon G \to \mathrm{GL}(n, \mathbb{K})$ be a representation and set*

$$\gamma = \sum_{\chi \in \mathrm{Irr}\, D} \chi(1)\chi.$$

For a permutation $\pi\colon G \to G$, there is a linear map sending each $D(g)$ to $D(\pi(g))$ if and only if

$$\gamma(\pi(g)^{-1}\pi(h)) = \gamma(g^{-1}h) \quad \text{for all} \quad g, h \in G.$$

(For example, this holds if π is a group automorphism of G fixing γ.)

Proof. For

$$e = \frac{1}{|G|} \sum_{g \in G} \gamma(g^{-1})g,$$

the representation D induces an isomorphism $\mathbb{K}Ge \cong \mathrm{Span}(D(G))$ of $\mathbb{K}G$-modules sending e to $D(1)$, by the proof of Lemma 9.1. Thus the result follows from Proposition 9.5. □

Notice that the character γ is in general *not* the character of the representation D. Two representations yield linearly G-equivalent matrix groups if and only if they have the same non-trivial constituents. For all these representations, we have to use the same character γ to compute the affine symmetries.

We close this section with a surprising characterization of representation polytopes among orbit polytopes. (So we work over $\mathbb{K} = \mathbb{R}$.)

9.7 Theorem. *Let $\mathrm{P}(G, v)$ be an orbit polytope of a finite group G. Then $\mathrm{P}(G, v)$ is affinely G-equivalent to a representation polytope of G if and only if $\varepsilon \in \mathrm{Sym}(G, v)$, where $\varepsilon(g) = g^{-1}$ for all $g \in G$.*

Proof. We have seen in Proposition 6.4(iii) that a representation polytope $P(D)$ has an affine symmetry mapping $D(g)$ to $D(g^{-1})$.

Conversely, assume that $\varepsilon \in \mathrm{Sym}(G, v)$. Let $e \in \mathbb{R}G$ be defined as in Theorem 8.5, so that $e^* = e$ and there is an isomorphism $\mu\colon \mathbb{R}Gv \to \mathbb{R}Ge$ sending v

to e. Notice that for $a \in \mathbb{R}G$, we have $\varepsilon(a) = a^*$, where $*$ is the involution of $\mathbb{C}G$ defined earlier, restricted to $\mathbb{R}G$. By Lemma 8.4, we have that

$$eg^{-1} = (ge)^* = \varepsilon(ge) = \varepsilon(g)e = g^{-1}e$$

for all $g \in G$. Thus $e \in \mathbf{Z}(\mathbb{R}G)$. Then Lemma 9.1 yields that $\mathrm{P}(G, e) \cong P(D)$ for some representation D. □

10. Character criteria

In this section, we work over the field $\mathbb{C}$ of complex numbers. The aim of this section is to describe the generic symmetries of some cyclic $\mathbb{C}G$-module V in terms of its character γ, and in particular, its decomposition into irreducible characters.

Any $\mathbb{C}G$-module V is determined up to isomorphism by its character $\gamma\colon G \to \mathbb{C}$, defined by $\gamma(g) = \mathrm{Tr}_V(g)$. This suggests the following definition:

10.1 Definition. Let γ be a character which is afforded by the cyclic $\mathbb{C}G$-module V. Then we set $\mathrm{Sym}(G, \gamma) = \mathrm{Sym}(G, V)$. We call $\mathrm{Sym}(G, \gamma)$ the **generic symmetry group** of γ.

By Lemma 4.8, $\mathrm{Sym}(G, \gamma)$ does not depend on the choice of the module V itself. More generally, if γ is afforded by some module $\widetilde{V}$ over $\mathbb{K}G$ for some other field $\mathbb{K}$, then $\mathrm{Sym}(G, \gamma)$ can also be defined with respect to $\widetilde{V}$, by Corollary 4.20.

As usual, the set of irreducible complex characters of G is denoted by $\mathrm{Irr}(G)$. We write ϱ_G for the *regular character* of G, that is, the character of $\mathbb{C}G$ as (left) module over itself.

As remarked in Section 8, an arbitrary $\mathbb{C}G$-module V is cyclic if and only if V is isomorphic to a left ideal of $\mathbb{C}G$, because any epimorphism $\mathbb{C}G \to V$ splits. Thus a character γ is afforded by a cyclic $\mathbb{C}G$-module if and only if γ is a constituent of ϱ_G (that is, $\varrho_G - \gamma$ is a character, too). As $\varrho_G = \sum_\chi \chi(1)\chi$, where χ runs over all irreducible characters of G, an arbitrary character $\gamma = \sum_\chi m_\chi \chi$ is afforded by a left ideal if and only if $m_\chi \leqslant \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$ (Theorem 8.1). Here we have $m_\chi = [\gamma, \chi] \leqslant \chi(1)$, where $[\ ,\ ]$ denotes the usual inner product for class functions, namely

$$[\alpha, \beta] = \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}.$$

We begin with the characterization of $\mathrm{Sym}(G, \chi)$ for $\chi \in \mathrm{Irr}(G)$, which is basically a reformulation of Theorem 5.8 (or Corollary 5.9).

10.2 Corollary. *Let $\chi \in \mathrm{Irr}(G)$ and set $K := \mathrm{Ker}(\chi)$. Then*

$$\mathrm{Sym}(G, \chi) = \{\pi \in \mathrm{Sym}(G) \mid \pi(gK) = \pi(1)gK \text{ for all } g \in G\}.$$

Proof. Let $D\colon G \to \mathrm{GL}(V)$ be a representation affording χ and suppose that $v \in V$ is generic, so that $K = \{g \in G \mid gv = v\}$. By Theorem 5.8, we have $D_v(\mathrm{Sym}(G,\chi)) = D(G)$. In view of Lemma 4.3, the description of $\mathrm{Sym}(G,\chi)$ follows. □

10.3 Proposition. *Let γ be the character of some left ideal and $\pi \in \mathrm{Sym}(G)$ be a permutation. The following are equivalent:*

(i) $\pi \in \mathrm{Sym}(G,\gamma)$.
(ii) $\pi \in \mathrm{Sym}(G, \varrho_G - \gamma)$.
(iii) $\pi(L) \subseteq L$ *for all left ideals L affording γ.*
(iv) $\pi(L) \subseteq L$ *for all left ideals L affording $\varrho_G - \gamma$ (where ϱ_G is the regular character of G, as before).*

Proof. The equivalence of (iii) and (iv) follows by taking orthogonal complements, and by the fact that a left ideal L is afforded by γ if and only if $L^\perp$ is afforded by $\varrho_G - \gamma$.

Let V be a $\mathbb{C}G$-module affording γ, and $v \in \mathrm{Gens}(V)$. By Lemma 7.2, $\pi \in \mathrm{Sym}(G,V) = \mathrm{Sym}(G,\gamma)$ if and only if π maps any isomorphic copy of $\mathrm{Ann}(v)$ in $\mathbb{C}G$ onto itself. As $\mathbb{C}G \cong V \oplus \mathrm{Ann}(v)$, these are precisely the left ideals affording the character $\varrho_G - \gamma$, which shows the equivalence of (i) and (iv). Now the result is clear. □

The last result is of course closely related to Lemma 8.4. Both results are only true in characteristic zero: If the characteristic of $\mathbb{K}$ divides the group order, then a left ideal of the group algebra $\mathbb{K}G$ may not even be cyclic as $\mathbb{K}G$-module. (As an example, take the Klein four group $G = C_2 \times C_2$ in characteristic 2. The augmentation ideal (the kernel of $\mathbb{K}G \to \mathbb{K}$) is not cyclic as $\mathbb{K}G$-module.) And even when the characteristic does not divide the group order, it is not true that a left ideal has the same generic symmetries as its complements. (An example exists with $G = C_7$ cyclic of order 7 and $\mathbb{K}$ of characteristic 2.)

Recall that now we know how to compute generic symmetries of characters of ideals (Proposition 9.5) and of irreducible characters (Corollary 10.2). We now work to show how to compute $\mathrm{Sym}(G,V)$ for an arbitrary left ideal V from the character of V.

10.4 Definition. Let γ be a character. The **ideal part** γ_I of γ is given by

$$\gamma_I = \sum_\psi \psi(1)\psi,$$

where ψ runs over all irreducible characters of G with $[\gamma,\psi] = \psi(1)$.

If L is any left ideal affording γ, then γ_I is the character of the largest twosided ideal contained in L.

10.5 Theorem. *A permutation $\pi \in \mathrm{Sym}(G)$ is generic for a character γ if and only if it is generic for γ_I and for any irreducible constituent of $\gamma - \gamma_I$.*

Proof. The "if" part is a direct consequence of Lemma 4.6.

For the "only if" part, assume $\pi \in \mathrm{Sym}(G, \gamma)$. By Proposition 10.3, we have $\pi(L) \subseteq L$ for all left ideals L affording γ. Thus $\pi(I) \subseteq I$, where I is the intersection of all these left ideals. I is the largest twosided ideal contained in a left ideal L affording γ, that is, I is the ideal affording γ_I. By Proposition 10.3 again, $\pi \in \mathrm{Sym}(G, \gamma_I)$.

Now let χ be any irreducible constituent of $\gamma - \gamma_I$, and let S be any left ideal affording χ. Then S is contained in a left ideal L affording γ. Since χ is not a constituent of γ_I, there is an isomorphic copy S' of S in $\mathbb{C}G$ with $S' \cap L = 0$. Let C be any complement of $L \oplus S'$ in $\mathbb{C}G$. Then $S \oplus C \cong S' \oplus C$ affords $\varrho - \gamma$, and so $\pi(S \oplus C) \subseteq S \oplus C$ by Proposition 10.3. Finally, as $S = L \cap (S \oplus C)$, we conclude $\pi(S) \subseteq S$. Since S was an arbitrary left ideal affording χ, Proposition 10.3 yields that $\pi \in \mathrm{Sym}(G, \chi)$. □

Putting the previous results together, we get a characterization of $\mathrm{Sym}(G, \gamma)$ in terms of γ (Theorem G from the introduction).

10.6 Theorem. *Let γ be the character of some left ideal of $\mathbb{C}G$ and $\pi \in \mathrm{Sym}(G)$. Then $\pi \in \mathrm{Sym}(G, \gamma)$ if and only if the following two conditions hold:*

(i) *For all $g, h \in G$ we have*

$$\gamma_I(\pi(h)^{-1}\pi(g)) = \gamma_I(h^{-1}g).$$

(ii) *For all $g \in G$ we have*

$$\pi\Big(g \operatorname{Ker}(\gamma - \gamma_I)\Big) = \pi(1)g \operatorname{Ker}(\gamma - \gamma_I).$$

Proof. By Theorem 10.5, a permutation $\pi \in \mathrm{Sym}(G)$ is in $\mathrm{Sym}(G, \gamma)$ if and only if $\pi \in \mathrm{Sym}(G, \gamma_I)$ and $\pi \in \mathrm{Sym}(G, \chi)$ for any irreducible constituent χ of $\gamma - \gamma_I$. By Proposition 9.5, $\pi \in \mathrm{Sym}(G, \gamma_I)$ is equivalent to (i). By Corollary 10.2, $\pi \in \mathrm{Sym}(G, \chi)$ for $\chi \in \mathrm{Irr}(G)$ is equivalent to $\pi(g \operatorname{Ker}(\chi)) = \pi(1)g \operatorname{Ker}(\chi)$ for all $g \in G$. Since $\operatorname{Ker}(\gamma - \gamma_I)$ is the intersection of the kernels of its irreducible constituents, the result follows. □

10.7 Corollary. *If $\gamma - \gamma_I$ is faithful, then G is generically closed with respect to γ. Thus in a module V affording γ, there are (infinitely many) $v \in V$ such that $\mathrm{Span}(Gv) = V$ and $G = \mathrm{GL}(Gv)$.*

Finally, recall the following: Let V be a left $\mathbb{C}G$-ideal affording the character γ. Then for any $v \in \mathrm{Gens}(V)$, a representation $D_v \colon \mathrm{Sym}(G, v) \to \mathrm{GL}(V)$ is defined. By Lemma 5.6, the character $\widehat{\gamma}$ of the restriction $D_v \colon \mathrm{Sym}(G, \gamma)$ is independent of v. Since the left regular action of G on itself yields an inclusion $\lambda \colon G \to \mathrm{Sym}(G, \gamma)$, we can view $\widehat{\gamma}$ as an extension of γ. Erik Friese found the following formula for $\widehat{\gamma}$:

10.8 Proposition. *Let γ be a character of G. Then for all $\pi \in \mathrm{Sym}(G, \gamma)$ we have*

$$\widehat{\gamma}(\pi) = \frac{1}{|G|} \sum_{g \in G} \gamma(g^{-1}\pi(g)).$$

Proof. By Theorem 10.5, it suffices to prove the claim for characters of ideals and for irreducible characters.

Let γ be irreducible. Then, by Corollary 10.2, $\pi(g) \in \pi(1)g \operatorname{Ker}(\gamma)$ for all $g \in G$, and thus $g^{-1}\pi(g) \in \pi(1) \operatorname{Ker}(\gamma)$. Therefore

$$\frac{1}{|G|} \sum_{g \in G} \gamma(g^{-1}\pi(g)) = \gamma(\pi(1)) = \widehat{\gamma}(\pi),$$

where the last equation follows from Corollary 5.9.

Now assume that γ is the character of the ideal $I = \mathbb{C}Ge$, where e is the corresponding central idempotent (Lemma 9.1). As usual, we view π as linear map on $\mathbb{C}G$. The equation $\pi(ge) = \pi(g)e$ of Lemma 8.4 for all $g \in G$ shows that $D_e(\pi) = \pi_{|I}$, that is, the restriction $\pi_{|I}$ is the linear map that shows that π is an orbit symmetry for e. The projection $e_r \colon \mathbb{C}G \to I$ is given by (left or right) multiplication with e. It follows

$$\begin{aligned} \widehat{\gamma}(\pi) = \mathrm{Tr}_I(\pi) = \mathrm{Tr}_{\mathbb{C}G}(\pi \circ e_r) &= \frac{1}{|G|} \sum_{g \in G} \varrho_G(g^{-1}\pi(ge)) \\ = \frac{1}{|G|} \sum_{g \in G} \varrho_G(g^{-1}\pi(g)e) &= \frac{1}{|G|} \sum_{g \in G} \gamma(g^{-1}\pi(g)). \end{aligned}$$

□

References for Chapter II

1. Barbara Baumeister and Matthias Grüninger. On permutation polytopes: notions of equivalence. *J. Algebraic Combin.* **41**, no. 4 (2015), pp. 1103–1114. DOI: 10.1007/s10801-014-0568-8, arXiv: 1301.2080 [math.CO]. MR3342715, Zbl. 1322.52010 (cited on p. 56).
2. Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. On permutation polytopes. *Adv. Math.* **222**, no. 2 (2009), pp. 431–452. DOI: 10.1016/j.aim.2009.05.003, arXiv: 0709.1615 [math.CO]. MR2538016(2010j:52042), Zbl. 1185.52006 (cited on p. 36).
3. David Bremner, Mathieu Dutour Sikirić, and Achill Schürmann. Polyhedral representation conversion up to symmetries. In: *Polyhedral Computation*. CRM Proc. Lecture Notes 48. American Mathematical Society, Providence, RI, 2009, pp. 45–71. arXiv: math/0702239v2 [math.MG]. MR2503772(2011d:68185), Zbl. 1170.68621 (cited on p. 41).

4. Graham Ellis, James Harris, and Emil Sköldberg. Polytopal resolutions for finite groups. *J. Reine Angew. Math.* **598** (2006), pp. 131–137. DOI: 10.1515/CRELLE.2006.071. MR2270569(2008g:20117), Zbl. 1115.20041 (cited on p. 47).
5. Robert M. Guralnick and David Perkinson. Permutation polytopes and indecomposable elements in permutation groups. *J. Combin. Theory Ser. A* **113**, no. 7 (2006), pp. 1243–1256. DOI: 10.1016/j.jcta.2005.11.004, arXiv: math/0503015 [math.CO]. MR2259059(2007h:05076), Zbl. 1108.52014 (cited on pp. 36, 40, 55).
6. Georg Hofmann and Karl-Hermann Neeb. On convex hulls of orbits of Coxeter groups and Weyl groups. *Münster J. Math.* **7**, no. 2 (2014), pp. 463–487. DOI: 10.17879/58269762646. MR3426226, Zbl. 1347.20040 (cited on p. 36).
7. Bertram Huppert. *Character Theory of Finite Groups*. De Gruyter Expositions in Mathematics 25. Walter de Gruyter, Berlin and New York, 1998. DOI: 10.1515/9783110809237. MR1645304(99j:20011), Zbl. 0932.20007 (cited on p. 57).
8. I. M[artin] Isaacs. Linear groups as stabilizers of sets. *Proc. Amer. Math. Soc.* **62**, no. 1 (1977), pp. 28–30. DOI: 10.2307/2041939. MR0427489(55#521), Zbl. 0355.20014 (cited on pp. 36, 54).
9. I. Martin Isaacs. *Character Theory of Finite Groups*. Dover, New York, 1994. (Corrected reprint of the 1976 edition by Academic Press, New York). MR1280461, Zbl. 0849.20004 (cited on pp. 54, 56, 66).
10. Gordon James and Martin Liebeck. *Representations and Characters of Groups*. Cambridge University Press, 2nd ed. 2001. MR1864147(2002h:20010), Zbl. 0981.20004 (cited on p. 37).
11. T[sit] Y[uen] Lam. *Lectures on Modules and Rings*. Graduate Texts in Mathematics 189. Springer, New York, Berlin, and Heidelberg, 1999. DOI: 10.1007/978-1-4612-0525-8. MR1653294(99i:16001), Zbl. 0911.16001 (cited on p. 59).
12. T[sit] Y[uen] Lam. *A First Course in Noncommutative Rings*. Graduate Texts in Mathematics 131. Springer, New York, Berlin, and Heidelberg, 2nd ed. 2001. DOI: 10.1007/978-1-4419-8616-0. MR1838439(2002c:16001), Zbl. 0980.16001 (cited on pp. 59, 65).
13. Serge Lang. *Algebra*. Addison-Wesley, Reading, MA, 1965. MR0197234(33#5416), Zbl. 0193.34701 (cited on pp. 54, 60).
14. Chi-Kwong Li and Thomas Milligan. Linear preservers of finite reflection groups. *Linear Multilinear Algebra* **51**, no. 1 (2003), pp. 49–81. DOI: 10.1080/0308108031000053648. MR1950413(2003j:20068), Zbl. 1026.15002 (cited on p. 37).
15. Chi-Kwong Li, Ilya Spitkovsky, and Nahum Zobin. Finite reflection groups and linear preserver problems. *Rocky Mountain J. Math.* **34**, no. 1 (2004), pp. 225–251. DOI: 10.1216/rmjm/1181069902. MR2061128(2005e:20056), Zbl. 1060.15007 (cited on p. 37).
16. Chi-Kwong Li, Bit-Shun Tam, and Nam-Kiu Tsing. Linear maps preserving permutation and stochastic matrices. *Linear Algebra Appl.* **341** (2002), pp. 5–22. DOI: 10.1016/S0024-3795(00)00242-1. MR1873605(2002i:15005), Zbl. 0998.15004 (cited on p. 37).

17. Nicholas McCarthy, David Ogilvie, Ilya Spitkovsky, and Nahum Zobin. Birkhoff's theorem and convex hulls of Coxeter groups. *Linear Algebra Appl.* **347** (2002), pp. 219–231. DOI: 10.1016/S0024-3795(01)00556-0. MR1899891(2003g:51012), Zbl. 1042.51011 (cited on p. 36).
18. Brendan D. McKay and Adolfo Piperno. Practical graph isomorphism, II. *J. Symbolic Comput.* **60** (2014), pp. 94–112. DOI: 10.1016/j.jsc.2013.09.003. MR3131381, Zbl. 06264238 (cited on p. 43).
19. Peter McMullen. Realizations of regular polytopes. *Aequationes Math.* **37**, no. 1 (1989), pp. 38–56. DOI: 10.1007/BF01837943. MR986092(90c:52014), Zbl. 0676.51008 (cited on p. 36).
20. Peter McMullen. Realizations of regular polytopes, III. *Aequationes Math.* **82**, no. 1-2 (2011), pp. 35–63. DOI: 10.1007/s00010-010-0063-9. MR2807032, Zbl. 1226.51005 (cited on p. 36).
21. Peter McMullen. Realizations of regular polytopes, IV. *Aequationes Math.* **87**, no. 1-2 (2014), pp. 1–30. DOI: 10.1007/s00010-013-0187-9. MR3175095, Zbl. 1327.51023 (cited on p. 36).
22. Peter McMullen and Barry Monson. Realizations of regular polytopes, II. *Aequationes Math.* **65**, no. 1-2 (2003), pp. 102–112. DOI: 10.1007/s000100300007. MR2012404(2004k:51021), Zbl. 1022.51019 (cited on p. 36).
23. Peter McMullen and Egon Schulte. *Abstract Regular Polytopes*. Encyclopedia of Mathematics and its Applications 92. Cambridge University Press, 2002. DOI: 10.1017/CBO9780511546686. MR1965665(2004a:52020), Zbl. 1039.52011 (cited on p. 36).
24. Shmuel Onn. Geometry, complexity, and combinatorics of permutation polytopes. *J. Combin. Theory Ser. A* **64**, no. 1 (1993), pp. 31–49. DOI: 10.1016/0097-3165(93)90086-N. MR1239510(94j:52020), Zbl. 0789.05095 (cited on p. 33).
25. Sudarshan K. Sehgal. Nilpotent elements in group rings. *Manuscripta Math.* **15**, no. 1 (1975), pp. 65–80. DOI: 10.1007/bf01168879. MR0364417(51#671), Zbl. 0302.16010 (cited on p. 66).
26. Günter M. Ziegler. *Lectures on Polytopes*. Graduate Texts in Mathematics 152. Springer-Verlag, New York, 1995. DOI: 10.1007/978-1-4613-8431-1. MR1311028(96a:52011), Zbl. 0823.52002 (cited on p. 62).

FL1. Erik Friese and Frieder Ladisch. Affine symmetries of orbit polytopes. *Adv. Math.* **288** (2016), pp. 386–425. DOI: 10.1016/j.aim.2015.10.021, arXiv: 1411.0899v3 [math.MG]. MR3436389, Zbl. 1330.52017 (cited on pp. 31, 41, 52, 54).
FL2. Erik Friese and Frieder Ladisch. Classification of affine symmetry groups of orbit polytopes. *J. Algebraic Combin.* (Nov. 2017). DOI: 10.1007/s10801-017-0804-0, arXiv: 1608.06539v4 [math.GR] (cited on pp. 31, 41).

Chapter III.

Groups with a Nontrivial Nonideal Kernel[1]

Frieder Ladisch

Abstract. We classify finite groups G, such that the group algebra, $\mathbb{Q}G$ (over the field of rational numbers $\mathbb{Q}$), is the direct product of the group algebra $\mathbb{Q}[G/N]$ of a proper factor group G/N, and some division rings.
2010 Mathematics Subject Classification. 20C15
Keywords. Characters, finite groups, representations, Schur indices, division rings

1. Introduction

Let G be a finite group and $\mathbb{K}$ a field of characteristic zero. By Maschke's theorem and Wedderburn-Artin theory, the group algebra $\mathbb{K}G$ of G over $\mathbb{K}$ is a direct product of matrix rings over division algebras:

$$\mathbb{K}G \cong \mathbf{M}_{d_1}(D_1) \times \cdots \times \mathbf{M}_{d_r}(D_r).$$

A natural question to ask is when each factor in this decomposition is actually a division ring (equivalently, the group algebra $\mathbb{K}G$ contains no nilpotent elements). In the classical case where $\mathbb{K}$ is algebraically closed, it is well known that $\mathbb{K}G$ is a direct product of division rings if and only if G is abelian. For $\mathbb{K} = \mathbb{Q}$, the question was solved by S. K. Seghal [11, Theorem 3.5] (see Theorem 4.5 below).

Here we consider a slightly more general question: Let $1 \neq N \trianglelefteq G$ be a normal subgroup. Then

$$\mathbb{K}G \cong \mathbb{K}[G/N] \times I,$$

where the (twosided) ideal I is the kernel of the canonical homomorphism $\mathbb{K}G \to \mathbb{K}[G/N]$. Now we ask: for which finite groups is there an $N \neq 1$ such that the ideal I above is a direct product of division rings? If there is such an N, then any nilpotent element of $\mathbb{K}G$ has constant coefficients on cosets of N. Also, only twosided ideals of $\mathbb{K}G$ can distinguish the elements of N.

The following is just a basic observation, which allows us to state our results more conveniently.

[1] arXiv: 1608.00231v3 [math.GR]. Submitted.

Lemma A. *For each field $\mathbb{K}$ (of characteristic zero) and each finite group G, there is a unique maximal normal subgroup N, denoted by $\mathrm{NKer}_{\mathbb{K}}(G)$, such that the kernel of the map $\mathbb{K}G \to \mathbb{K}[G/N]$ is a direct product of division rings.*

We will give a more direct definition of $\mathrm{NKer}_{\mathbb{K}}(G)$ in Section 3 below, before we prove Lemma A. We call $\mathrm{NKer}_{\mathbb{K}}(G)$ the **nonideal kernel** of G (over $\mathbb{K}$).

We view the zero ideal as an empty product of division rings, so possibly $\mathrm{NKer}_{\mathbb{K}}(G) = 1$. Indeed, this is the case for "most" groups, and we want to classify the groups G for which $\mathrm{NKer}_{\mathbb{K}}(G) \neq 1$. Our first result concerns the field $\mathbb{R}$ of real numbers.

We need to recall a definition: A nonabelian group G is called **generalized dicyclic**, if it has an abelian subgroup A of index 2 and an element $g \in G \setminus A$ such that $g^2 \neq 1$ and $a^g = a^{-1}$ for all $a \in A$. If A is cyclic, then G is called **dicyclic** (or generalized quaternion). Furthermore, Q_8 denotes the quaternion group of order 8 and C_n a cyclic group of order n.

Theorem B. *Let G be a finite group. Then $\mathrm{NKer}_{\mathbb{R}}(G) > 1$ if and only if one of the following holds:*

(i) *G is abelian and $G \neq \{1\}$.*
(ii) *G is generalized dicyclic.*
(iii) *$G \cong C_4 \times Q_8 \times (C_2)^r$, $r \in \mathbb{N}$.*
(iv) *$G \cong Q_8 \times Q_8 \times (C_2)^r$, $r \in \mathbb{N}$.*

The motivation for this work is the question of Babai [1] mentioned in the introduction to this thesis. Babai asked which finite groups are isomorphic to the affine symmetry group of an orbit polytope. (An orbit polytope is a polytope such that its (affine) symmetry groups acts transitively on the vertices of the polytope.) By the results of the last chapter, a group G is isomorphic to the affine symmetry group of an orbit polytope when $\mathrm{NKer}_{\mathbb{R}}(G) = 1$. When $\mathrm{NKer}_{\mathbb{R}}(G) > 1$, this may or may not be the case. Theorem B above is an essential ingredient in our answer to Babai's question in the next chapter. Similarly, when $\mathrm{NKer}_{\mathbb{Q}}(G) = 1$, then G can be realized as the affine symmetry group of an orbit polytope with vertices having rational coordinates.

The classification of groups with $\mathrm{NKer}_{\mathbb{Q}}(G) > 1$ is more complicated. To state it, we first describe a special type of such groups.

Lemma C. *Let p and q be primes, let $P = \langle g \rangle \times P_0$ be an abelian p-group and Q an abelian q-group. Suppose P acts on Q such that $x^g = x^k$ for all $x \in Q$ and some integer k independent of $x \in Q$, and such that $\mathbf{C}_P(Q) = \langle g^{p^c} \rangle \times P_0$. Suppose that $p^d = \mathbf{o}(g^{p^c})$ is the exponent of $\mathbf{C}_P(Q)$, and that $(q-1)_p$, the p-part of $q-1$, divides p^d. Then for the semidirect product $G = PQ$, we have $1 \neq \mathrm{NKer}_{\mathbb{Q}}(G) \cap \langle g \rangle$.*

Notice that the assumption on the action of g on Q and $|P/\mathbf{C}_P(Q)| = p^c$ imply that p^c divides $q-1$, and that the multiplicative order of k modulo the exponent of Q is just p^c. One can show that $\mathrm{NKer}_{\mathbb{Q}}(G) = \langle g^{p^s} \rangle$, where $p^s = p^{c-1}(q-1)_p$. Whenever we mention "groups as in Lemma C", we also use the notation established in the statement of Lemma C.

Theorem D. *Let G be a finite group. Then $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$ if and only if at least one of the following holds:*

(i) *G is abelian.*

(ii) *$G = S \times A$, where S is a 2-group of exponent 4 which appears on the list from Theorem B, the group A is abelian of odd order, and the multiplicative order of 2 modulo $|A|$ is odd.*

(iii) *G is generalized dicyclic.*

(iv) *$G = (PQ) \times B$, where the subgroups $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$ and B are abelian, PQ is as in Lemma C, and the p-part of the multiplicative order of q modulo $|B|$ divides the multiplicative order of q modulo p^d.*

(v) *$G = Q_8 \times (C_2)^r \times H$, where H is as in (iv) and has odd order, and the multiplicative order of 2 modulo $|H|$ is odd.*

Case (ii) contains the groups $G = Q_8 \times (C_2)^r \times A$, for which $\mathbb{Q}G$ is a direct product of division rings, as classified by Sehgal [11].

An important tool in the proofs of Theorems B and D is Blackburn's classification of finite groups in which all nonnormal subgroups have a nontrivial intersection [3]. As we will see below, $\mathrm{NKer}_{\mathbb{K}}(G)$ is always contained in the intersection of all nonnormal subgroups of G. While the proof of Theorem B is relatively elementary, the proof of Theorem D also depends on some deep facts about division algebras and Schur indices.

This chapter is organized as follows: In Section 2, we review some basic facts about representations and characters over fields not necessarily algebraically closed, and in particular Schur indices. We also introduce the auxiliary concept of *skew-linear characters*. In Section 3, we define $\mathrm{NKer}_{\mathbb{K}}(G)$ and prove some elementary properties. In Section 4, we consider Dedekind groups (groups such that all subgroups are normal). In such groups, we have either $\mathrm{NKer}_{\mathbb{K}}(G) = 1$, or $\mathrm{NKer}_{\mathbb{K}}(G) = G$, where the latter are exactly the groups such that $\mathbb{K}G$ is a direct product of division rings. Finally, Section 5 contains the proof of Theorem B, and Section 6 the (long) proof of Theorem D.

2. Skew-linear characters

Let G be a finite group. For simplicity, assume that $\mathbb{K} \subseteq \mathbb{C}$ and write $\mathrm{Irr}\, G$ for the set of irreducible complex characters of G. We begin by reviewing the relation between the representation theory of G over $\mathbb{K}$ and over $\mathbb{C}$ [6, § 38][7, Chapter 10].

By Maschke's theorem and general Wedderburn-Artin theory, the group algebra $\mathbb{K}G$ is the direct product of simple rings:

$$\mathbb{K}G = A_1 \times \cdots \times A_r.$$

Each A_i is a simple ideal, and the set of the A_i's is uniquely determined as the set of simple ideals of $\mathbb{K}G$. The A_i's are called the **block ideals of** $\mathbb{K}G$. Each A_i is generated by a central primitive idempotent $e \in \mathbf{Z}(\mathbb{K}G)$. By Wedderburn-Artin theory, each A_i is isomorphic to a matrix ring over a division ring.

We now relate the above decomposition to the complex irreducible characters of G. Recall that the **Schur index** of $\chi \in \operatorname{Irr} G$ over $\mathbb{K}$ is the smallest positive integer $m = m_{\mathbb{K}}(\chi)$ such that $m\chi$ is afforded by a representation with entries in $\mathbb{K}(\chi)$, the field generated by $\mathbb{K}$ and the values of χ.

2.1 Lemma. *Let $\chi \in \operatorname{Irr} G$.*

(i) *There is a unique block ideal A of $\mathbb{K}G$ such that $\chi(A) \neq 0$.*
(ii) *Let $\psi \in \operatorname{Irr} G$. Then $\psi(A) \neq 0$ if and only if ψ and χ are Galois conjugate over $\mathbb{K}$, that is, $\psi = \chi^\alpha$ for some $\alpha \in \operatorname{Gal}(\mathbb{K}(\chi)/\mathbb{K})$.*
(iii) *Write $A \cong \mathbf{M}_n(D)$ for some division ring D. Then $\mathbf{Z}(A) \cong \mathbf{Z}(D) \cong \mathbb{K}(\chi)$.*
(iv) *$|D : \mathbf{Z}(D)| = m_{\mathbb{K}}(\chi)^2$ and $\chi(1) = nm_{\mathbb{K}}(\chi)$.*

Proof. This is standard [6, Theorems 38.1 and 38.15]. □

It follows from Lemma 2.1 that A is itself a division ring if and only if $\chi(1) = m_{\mathbb{K}}(\chi)$. In this case, the projection $\mathbb{K}G \to A$ defines a homomorphism φ from G into the multiplicative group of D. Notice also that $\operatorname{Ker}(\varphi) = \operatorname{Ker}(\chi)$. For this reason, we call a character χ **skew-linear** (over $\mathbb{K}$), if $\chi(1) = m_{\mathbb{K}}(\chi)$. Thus skew-linear characters generalize linear characters. Since $m_{\mathbb{C}}(\chi) = 1$ for all χ, skew-linear over $\mathbb{C}$ is the same as linear.

If $\chi \in \operatorname{Irr}(G)$ is linear, then (trivially) the reduction to any subgroup is irreducible and linear. This fact generalizes to skew-linear characters as follows:

2.2 Lemma. *Let $\chi \in \operatorname{Irr}(G)$ be skew-linear over the field $\mathbb{K}$, and $H \leqslant G$. Then the irreducible constituents of χ_H are skew-linear over $\mathbb{K}$, and are Galois conjugate over the field $\mathbb{K}(\chi)$.*

Proof. Let $\vartheta \in \operatorname{Irr}(H)$ be a constituent of χ_H. Then [7, Lemma 10.4]

$$m_{\mathbb{K}}(\chi) \quad \text{divides} \quad [\chi_H, \vartheta]|\mathbb{K}(\chi, \vartheta) : \mathbb{K}(\chi)|m_{\mathbb{K}}(\vartheta).$$

Let $\sigma \in \operatorname{Gal}(\mathbb{K}(\chi, \vartheta)/\mathbb{K}(\chi))$. Then $[\chi_H, \vartheta^\sigma] = [\chi_H, \vartheta]$. Thus each of the $|\mathbb{K}(\chi, \vartheta) : \mathbb{K}(\chi)|$ characters ϑ^σ occurs in χ_H with multiplicity $[\chi_H, \vartheta]$. It follows that

$$\begin{aligned}[\chi_H, \vartheta]|\mathbb{K}(\chi, \vartheta) : \mathbb{K}(\chi)|\vartheta(1) &\leqslant \chi(1) = m_{\mathbb{K}}(\chi) \\ &\leqslant [\chi_H, \vartheta]|\mathbb{K}(\chi, \vartheta) : \mathbb{K}(\chi)|m_{\mathbb{K}}(\vartheta).\end{aligned}$$

This implies that equality holds throughout, in particular, $\vartheta(1) = m_{\mathbb{K}}(\vartheta)$ and $\chi_H = [\chi_H, \vartheta] \sum \vartheta^\sigma$, the sum running over $\sigma \in \mathrm{Gal}(\mathbb{K}(\chi, \vartheta)/\mathbb{K}(\chi))$. □

In the rest of this section, we record some (mostly well known) facts about Schur indices and blocks of group algebras for later reference.

Recall that

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1}) g$$

is the central primitive idempotent in $\mathbb{C}G$ corresponding to $\chi \in \mathrm{Irr}\, G$. The following simple observation will sometimes be useful. Notice that it provides an alternative proof of $\mathbf{Z}(A) \cong \mathbb{K}(\chi)$.

2.3 Lemma. *Let $\chi \in \mathrm{Irr}\, G$ and let A be the block ideal of $\mathbb{K}G$ such that $\chi(A) \neq 0$. Then*

$$A \cong \mathbb{K}(\chi) G e_\chi \quad \textit{by} \quad A \ni a \mapsto a e_\chi.$$

Proof. Set

$$e := \sum_{\alpha \in \mathrm{Gal}(\mathbb{K}(\chi)/\mathbb{K})} e_{\chi^\alpha}.$$

We claim that $A = \mathbb{K}Ge$. We can decompose 1 into a sum of primitive idempotents in $\mathbf{Z}(\mathbb{K}G)$, and then decompose further in $\mathbf{Z}(\mathbb{C}G)$. Thus there is a unique primitive idempotent f in $\mathbf{Z}(\mathbb{K}G)$ such that $f e_\chi = e_\chi$. But then also $f e_{\chi^\alpha} = e_{\chi^\alpha}$ for all $\alpha \in \mathrm{Gal}(\mathbb{K}(\chi)/\mathbb{K})$ and thus $fe = e$. On the other hand, $e_\chi \in \mathbb{K}(\chi)$ and $e \in \mathbb{K}G$, and thus $f = e$. This shows that $A = \mathbb{K}Ge$ as claimed.

For $\alpha \in \mathrm{Gal}(\mathbb{K}(\chi)/\mathbb{K})$,

$$b = \sum_g b_g g \in \mathbb{K}(\chi) G e_\chi \quad \text{implies} \quad b^\alpha := \sum_g b_g^\alpha g \in \mathbb{K}(\chi) G e_{\chi^\alpha}.$$

Using this, it is straightforward to check that

$$\mathbb{K}(\chi) G e_\chi \ni b \mapsto \sum_{\alpha \in \mathrm{Gal}(\mathbb{K}(\chi)/\mathbb{K})} b^\alpha \in \mathbb{K}Ge$$

yields the inverse of the map $a \mapsto a e_\chi$. □

Since we will often have to consider characters of direct products of groups, and the corresponding blocks of the group algebra, we record the following for later reference.

2.4 Lemma. *Let $G = U \times V$ be a direct product of groups, $\sigma \in \mathrm{Irr}\, U$ and $\tau \in \mathrm{Irr}\, V$. Then $\chi = \sigma \times \tau \in \mathrm{Irr}\, G$ and $\mathbb{K}(\chi) = \mathbb{K}(\sigma, \tau)$. Let $A_{\mathbb{K}}(\chi)$ be the block ideal of $\mathbb{K}G$ corresponding to χ, and $A_{\mathbb{K}}(\sigma)$ and $A_{\mathbb{K}}(\tau)$ the block ideals of $\mathbb{K}U$ and $\mathbb{K}V$ corresponding to σ and τ. Then*

$$A_{\mathbb{K}}(\chi) \cong \Big(A_{\mathbb{K}}(\sigma) \otimes_{\mathbb{K}(\sigma)} \mathbb{K}(\chi)\Big) \otimes_{\mathbb{K}(\chi)} \Big(A_{\mathbb{K}}(\tau) \otimes_{\mathbb{K}(\tau)} \mathbb{K}(\chi)\Big).$$

Proof. The irreducible characters of $U \times V$ are exactly the characters of the form $\chi = \sigma \times \tau$, with $\sigma \in \operatorname{Irr} U$ and $\tau \in \operatorname{Irr} V$ [7, Theorem 4.21]. Since $\chi((u,1)) = \sigma(u)\tau(1)$ for $u \in U$ and similarly $\chi((1,v)) = \sigma(1)\tau(v)$ for $v \in V$, we see that $\mathbb{K}(\chi) = \mathbb{K}(\sigma,\tau)$.

Set $\mathbb{L} = \mathbb{K}(\chi)$. The natural isomorphism

$$\mathbb{L}U \otimes_{\mathbb{L}} \mathbb{L}V \to \mathbb{L}G, \quad \sum_u a_u u \otimes \sum_v b_u v \mapsto \sum_{u,v} a_u b_v (u,v)$$

sends $e_\sigma \otimes e_\tau$ to e_χ and thus induces an isomorphism

$$\mathbb{L}Ue_\sigma \otimes_{\mathbb{L}} \mathbb{L}Ve_\tau \cong \mathbb{L}Ge_\chi$$

(by comparing dimensions). By Lemma 2.3, the right hand side is isomorphic to $A_{\mathbb{K}}(\chi)$, and on the left hand side we have

$$\mathbb{L}Ue_\sigma \cong \mathbb{K}(\sigma)Ue_\sigma \otimes_{\mathbb{K}(\sigma)} \mathbb{L} \cong A_{\mathbb{K}}(\sigma) \otimes_{\mathbb{K}(\sigma)} \mathbb{L},$$

and similarly for the other factor. The result follows. □

In Section 6, we need several deep facts about Schur indices, which we collect now. For a prime q, we write $m_q(\chi) := m_{\mathbb{Q}_q}(\chi)$, where $\mathbb{Q}_q$ denotes the field of q-adic numbers. Sometimes, it will be convenient to use this notation also for the "infinite prime", that is, $m_\infty(\chi) := m_{\mathbb{R}}(\chi)$.

2.5 Lemma. *Let $\chi \in \operatorname{Irr}(G)$.*

(i) *$m_{\mathbb{Q}}(\chi)$ is the least common multiple of the local indices $m_q(\chi)$, where q runs through all primes, including the infinite one. [10, (32.19)]*

(ii) *$m_{\mathbb{R}}(\chi)$ and $m_2(\chi)$ divide 2, and $m_q(\chi)$ divides $q-1$ for odd q. [13, Theorem 4.3, Corollary 5.5]*

(iii) *Let φ be an irreducible Brauer character for the prime q, and $d_{\chi\varphi}$ the decomposition number. Then $m_q(\chi)$ divides $d_{\chi\varphi}|\mathbb{Q}_q(\chi,\varphi) : \mathbb{Q}_q(\chi)|$. [4, Theorem IV.9.3]*

(iv) *If the finite prime q does not divide $|G|$, then $m_q(\chi) = 1$. [4, Corollary IV.9.5]*

2.6 Corollary. *Let $\chi \in \operatorname{Irr}(G)$ with $\chi(1) = m_q(\chi)$, where q is a prime number. If $H \leqslant G$ is not divisible by q, then any constituent of χ_H is linear.*

Proof. This is immediate from Lemma 2.2 and Lemma 2.5 (iv). □

3. The nonideal kernel

For every field $\mathbb{K}$ and any finite group G, we define

$$\operatorname{NKer}_{\mathbb{K}}(G) := \bigcap \{\operatorname{Ker}(\chi) \mid \chi(1) > m_{\mathbb{K}}(\chi)\}.$$

If $m_{\mathbb{K}}(\chi) = \chi(1)$ for every $\chi \in \operatorname{Irr}(G)$, we set $\operatorname{NKer}_{\mathbb{K}}(G) := G$. We call $\operatorname{NKer}_{\mathbb{K}}(G)$ the **nonideal kernel** of G over $\mathbb{K}$. Notice that $\operatorname{NKer}_{\mathbb{K}}(G)$, for any field $\mathbb{K}$, is characteristic in G.

3.1 Lemma. *Let $\mathbb{K} \subseteq \mathbb{L}$ be fields. Then* $\mathrm{NKer}_{\mathbb{L}}(G) \subseteq \mathrm{NKer}_{\mathbb{K}}(G)$.

Proof. Since $m_{\mathbb{L}}(\chi)$ divides $m_{\mathbb{K}}(\chi)$ for any $\chi \in \operatorname{Irr} G$, any character which is skew-linear over $\mathbb{L}$, is also skew-linear over $\mathbb{K}$. The result follows. □

3.2 Lemma. *Let G be a nonabelian group. Then*

$$\bigcap_{\substack{\chi \in \operatorname{Irr} G \\ \chi(1)>1}} \operatorname{Ker} \chi = \{1\}.$$

Proof. Suppose that $g \neq 1$ is contained in the kernel of all nonlinear characters. Then, by the second orthogonality relation [7, Theorem 2.18],

$$0 = \sum_{\chi \in \operatorname{Irr} G} \chi(1)\chi(g) = \sum_{\substack{\chi \in \operatorname{Irr} G \\ \chi(1)>1}} \chi(1)^2 + \sum_{\chi \in \operatorname{Lin} G} \chi(1)\chi(g).$$

The second sum runs over the irreducible characters of G/G' and has value $|G : G'|$ or 0, according to whether $g \in G'$ or not. It follows that the first sum must be empty. Thus G has no nonlinear characters, which means that G is abelian, as claimed. □

3.3 Corollary. *Let G be a nonabelian group. Then* $\mathrm{NKer}_{\mathbb{C}}(G) = 1$.

Let us say that a character α (not necessarily irreducible) is **strictly nonideal**, if $[\alpha, \chi] < \chi(1)$ for all $\chi \in \operatorname{Irr} G$. (Such a character is afforded by a left ideal of the group algebra, which does not contain any nonzero two-sided ideal.) If at the same time, α is the character of a representation with entries in $\mathbb{K}$, then $m_{\mathbb{K}}(\chi)$ divides $[\alpha, \chi]$ for all $\chi \in \operatorname{Irr} G$ [7, Corollary 10.2(c)]. Thus no constituent of α can be skew-linear over $\mathbb{K}$. Conversely, if S is a set of non-skew-linear characters over $\mathbb{K}$, then we may add the characters of the corresponding irreducible representations over $\mathbb{K}$ and get a strictly nonideal character α which is afforded by a $\mathbb{K}$-representation. Since $\operatorname{Ker} \alpha = \bigcap \operatorname{Ker} \chi$, where χ runs through the constituents of α, it follows that every group G has a strictly nonideal character α with $\operatorname{Ker} \alpha = \mathrm{NKer}_{\mathbb{K}}(G)$, and such that α is afforded by a representation over $\mathbb{K}$. (In the case where $G = \mathrm{NKer}_{\mathbb{K}}(G)$, the only such character is $\alpha = 0$, however.)

3.4 Lemma. *Let $H \leqslant G$ with $N := \mathrm{NKer}_{\mathbb{K}}(H) < H$. Then*

$$\mathrm{NKer}_{\mathbb{K}}(G) \leqslant \bigcap_{g \in G} N^g \leqslant \mathrm{NKer}_{\mathbb{K}}(H).$$

Proof. Let α be a strictly nonideal character of H with $N = \operatorname{Ker} \alpha$ and which is afforded by a representation over $\mathbb{K}$. Then $0 \neq \alpha^G$ is afforded by a representation over $\mathbb{K}$ and has kernel $\bigcap_{g \in G} N^g$ [7, Lemma 5.11].

Let ϱ_G be the regular character of G. Notice that a character β is strictly nonideal if and only if $\varrho_G - \beta$ is a character and $[\varrho_G - \beta, \chi] > 0$ for *all* $\chi \in \operatorname{Irr} G$. Since $\varrho_G = (\varrho_H)^G$, we have that $\varrho_G - \alpha^G = (\varrho_H - \alpha)^G$ is a character, and

$$[\varrho_G - \alpha^G, \chi] = [(\varrho_H - \alpha)^G, \chi] = [\varrho_H - \alpha, \chi_H]_H > 0$$

for all $\chi \in \operatorname{Irr} G$. Thus α^G is strictly nonideal. □

3.5 Lemma. *Let N be a normal subgroup of G, and set*

$$e_N = \frac{1}{|N|} \sum_{n \in N} n.$$

Then $\mathbb{K}Ge_N \cong \mathbb{K}[G/N]$. If $\chi \in \operatorname{Irr} G$, then $\chi(e_N) \neq 0$ if and only if $N \leqslant \operatorname{Ker}(\chi)$.

Proof. This is well known: The canonical epimorphism $\mathbb{K}G \to \mathbb{K}[G/N]$ is split by the map sending a coset Ng to $(1/|N|) \sum Ng = e_N g$. This proves the first statement.

If $N \leqslant \operatorname{Ker}(\chi)$, then any representation affording χ sends e_N to the identity map. If $N \not\leqslant \operatorname{Ker}(\chi)$, then any representation affording χ must send e_N to 0. □

3.6 Lemma. *Let $N := \operatorname{NKer}_{\mathbb{K}}(G)$, and e_N as in Lemma 3.5. Then $\mathbb{K}G(1 - e_N)$ is a direct product of division rings. In particular, every idempotent $f \in \mathbb{K}G$ with $fe_N = 0$ is central.*

Proof. By Lemma 3.5, it follows that $\mathbb{K}G(1 - e_N)$ is the direct product of the block ideals which correspond to $\chi \in \operatorname{Irr} G$ with $N \not\leqslant \operatorname{Ker}(\chi)$. By definition of N, any such χ is skew-linear over $\mathbb{K}$, and thus the corresponding block ideal is a division ring.

In a direct product of division rings, every idempotent is central. □

Proof of Lemma A. The first part of Lemma A is contained in Lemma 3.6. Conversely, if $\mathbb{K}G(1 - e_N)$ is a direct product of division rings, then the above considerations yield that when $m_{\mathbb{K}}(\chi) < \chi(1)$, we must have $N \subseteq \operatorname{Ker}(\chi)$, and thus $N \leqslant \operatorname{NKer}_{\mathbb{K}}(G)$. □

Following Blackburn [3], for any group G, we set

$$\mathbf{R}(G) := \bigcap \{U \leqslant G \mid U \text{ not normal in } G\}.$$

If every subgroup of G is normal, then we set $\mathbf{R}(G) = G$. Blackburn [3] classified finite groups in which $\mathbf{R}(G) \neq 1$. Therefore, a group G with $\mathbf{R}(G) \neq 1$ is called a **Blackburn group**. The following result shows why this is relevant for us:

3.7 Lemma. *For any finite group G and field $\mathbb{K}$ of characteristic zero, we have $\operatorname{NKer}_{\mathbb{K}}(G) \leqslant \mathbf{R}(G)$.*

Proof. Suppose $U \leqslant G$ is such that $N := \mathrm{NKer}_{\mathbb{K}}(G) \not\subseteq U \leqslant G$. We need to show that $U \trianglelefteq G$.

Set $f = (1 - e_N)e_U$, with e_N as before, and analogously

$$e_U := (1/|U|) \sum_{u \in U} u.$$

Then $f^2 = f \in \mathbb{K}G(1 - e_N)$, since e_N is central in $\mathbb{K}G$. Thus f is central in $\mathbb{K}G$ by Lemma 3.6. We compute

$$f = \frac{1}{|U|} \sum_{u \in U} u - \frac{1}{|NU|} \sum_{x \in NU} x.$$

As N is not contained in U, we have $U < NU$. As $g^{-1}fg = f$ for all $g \in G$, it follows that $U \trianglelefteq G$. □

4. Dedekind groups

In this section, we compute $\mathrm{NKer}_{\mathbb{K}}(G)$ for Dedekind groups, and determine when $\mathbb{K}G$ is a direct product of division rings. These results are mostly known.

Recall that a **Dedekind group** is a finite groups in which all subgroups are normal. First, we recall Dedekind's classification of these groups [5, Satz III.7.12 on p. 308].

4.1 Theorem (Dedekind 1897). *Let G be a finite group, such that every subgroup of G is normal. Then either G is abelian, or*

$$G \cong Q_8 \times (C_2)^r \times A \quad (r \geqslant 0),$$

where A is abelian of odd order.

Let $\tau \in \mathrm{Irr}(Q_8)$ be the irreducible, faithful character of degree 2. Then $\mathbb{H} := \mathbb{Q}Q_8 e_\tau$ is a division ring, the rational quaternions. $\mathbb{H}$ can also be described as the $\mathbb{Q}$-vector space with basis $\{1, i, j, k\}$ and multiplication defined by $i^2 = j^2 = -1$, $k = ij = -ji$.

4.2 Theorem. *Let $\mathbb{K}$ be a field and G be a group. Then $\mathbb{K}G$ is a direct product of division rings if and only if either G is abelian, or $G \cong Q_8 \times (C_2)^r \times A$, where A is abelian of odd order, and $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{K}(\lambda)$ is a division ring for all $\lambda \in \mathrm{Lin}(A)$.*

Proof. Suppose $\mathbb{K}G$ is a direct product of division rings. Then all subgroups of G are normal in G by Lemma 3.7 (as $\mathrm{NKer}_{\mathbb{K}}(G) = G$, or directly from the argument in the proof of Lemma 3.7). It follows that either G is abelian, or $G \cong Q_8 \times (C_2)^r \times A$ with A abelian of odd order.

In the second case, let $\tau \in \mathrm{Irr}(Q_8)$ be the irreducible, faithful character of degree 2. Then

$$\mathbb{K}Q_8 e_\tau \cong \mathbb{H} \otimes_{\mathbb{Q}} \mathbb{K},$$

the quaternions over $\mathbb{K}$. Any nonlinear, irreducible character of $G = Q_8 \times (C_2)^r \times A$ has the form $\chi = \tau \times \sigma \times \lambda$, where $\sigma \in \mathrm{Lin}(C_2)^r$ and $\lambda \in \mathrm{Lin}\, A$. The corresponding block ideal of the rational group algebra is, by Lemma 2.4, isomorphic to

$$\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{K}(\lambda).$$

The result follows. □

4.3 Remark. If $G \cong Q_8 \times (C_2)^r \times A$ with A abelian of odd order, then either $\mathbb{K}G$ is a direct product of division rings, or $\mathrm{NKer}_{\mathbb{K}}(G) = 1$.

Proof. Suppose that $\mathbb{K}G$ is not a direct product of division rings. Then there is some $\lambda \in \mathrm{Lin}(A)$ such that $\mathbb{K}(\lambda)$ is a splitting field for $\mathbb{H}$. As before, let $\tau \in \mathrm{Irr}(Q_8)$ be the faithful irreducible character of Q_8. Then $\mathrm{Ker}(\tau \times 1 \times \lambda) = 1 \times (C_2)^r \times \mathrm{Ker}(\lambda)$.

It follows that $\mathrm{NKer}_{\mathbb{K}}(G) \subseteq 1 \times \mathrm{Ker}(\mu)$ for every $\mu \in \mathrm{Lin}((C_2)^r \times A)$ such that $\mathbf{o}(\lambda)$ divides the order of μ. Since A contains elements of order $\mathbf{o}(\lambda)$, we see that $\mathrm{NKer}_{\mathbb{K}}(G) = 1$. □

Notice that for a linear character λ, we have $\mathbb{K}(\lambda) = \mathbb{K}(\varepsilon_n)$, where ε_n is a primitive n-th root of unity and $n = \mathbf{o}(\lambda)$. The following lemma collects some results. These will be needed also in the proof of Theorem D.

4.4 Lemma.

(i) $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{K}$ *is a division ring if and only if* -1 *is not a sum of two squares in* $\mathbb{K}$.

(ii) $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}_2$ *and* $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{R}$ *are division rings, and* $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ *for* p *odd is not a division ring. (Here* $\mathbb{Q}_p$ *is the field of* p*-adic numbers.)*

Let ε_n *be a primitive* n*-th root of unity, where* n *is odd. Then*

(iii) $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}(\varepsilon_n)$ *is a division ring if and only if the multiplicative order of* 2 *in* $(\mathbb{Z}/n)^*$ *is odd, if and only if* $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}_2(\varepsilon_n)$ *is a division ring.*

(iv) $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \varepsilon_n)$ *is a division ring only when* $n = 1$.

Proof. (i) and (ii) are well known [6, Example 38.13(a)] [12, Ch. III, Théorème 1]. Assertion (iii) is a result of Moser [9]. (This can be shown without using the Hasse-Minkowski principle: If the residue class of 2 in $(\mathbb{Z}/p)^*$ has even multiplicative order $2r$, then $2^r \equiv -1 \mod p$, and thus p divides $2^r + 1$. Then an elementary argument shows that -1 is a sum of two squares in $\mathbb{Q}(\varepsilon_p)$ [6, Example 38.13(d)]. If 2 has odd order in $(\mathbb{Z}/n\mathbb{Z})$, then $\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}_2(\varepsilon_n)$ is also a division ring.)

To see (iv), assume that $n > 1$. We have to show that -1 is a sum of two squares in $\mathbb{K} := \mathbb{Q}(\sqrt{2}, \varepsilon_n)$. By the Hasse-Minkowski principle, it suffices to show that -1 is a square in each possible completion of $\mathbb{K}$. Since $n > 1$, $\mathbb{K}$ can not

be embedded into $\mathbb{R}$. If p is odd, then -1 is a sum of two squares in $\mathbb{Q}_p$ already. Finally, $\mathbb{Q}_2(\sqrt{2})$ is a quadratic extension of $\mathbb{Q}_2$ and thus a splitting field of $\mathbb{H}$ [8, Lemma VI.2.14]. (We notice that in (iv), we can replace $\mathbb{Q}(\sqrt{2})$ by any field such that the completions at all prime ideals over 2 yield extensions of *even* degree over $\mathbb{Q}_2$.) □

As a consequence, we get the following results.

4.5 Theorem (Sehgal 1975 [11]). *The group algebra $\mathbb{Q}G$ is a direct product of division rings if and only if one of the following holds:*

(i) *G is abelian.*

(ii) *$G \cong Q_8 \times (C_2)^r \times A$, where $r \geqslant 0$, and A is abelian of odd order, and the multiplicative order of 2 in $(\mathbb{Z}/|A|)^*$ is odd.*

4.6 Theorem.

(i) *$\mathbb{Q}_2G$ is a direct product of division rings if and only if $\mathbb{Q}G$ is a direct product of division rings.*

(ii) *Let p be an odd prime. Then $\mathbb{Q}_pG$ is a direct product of division rings if and only if G is abelian.*

(iii) *$\mathbb{R}G$ is a direct product of division rings if and only if either G is abelian, or $G \cong Q_8 \times (C_2)^r$ for some $r \geqslant 0$.*

5. Classification over the reals

In this section, we prove Theorem B. We begin with the (maybe more interesting) "only if" part.

5.1 Lemma. *Suppose that $\mathrm{NKer}_{\mathbb{R}}(G) \neq 1$, and $\langle g\rangle \not\trianglelefteq G$. Then g has order 4, and $\mathrm{NKer}_{\mathbb{R}}(G) = \langle g^2\rangle$ has order 2.*

Proof. By Lemma 3.7 and the definition of $\mathbf{R}(G)$, we have

$$1 \neq N := \mathrm{NKer}_{\mathbb{R}}(G) \leqslant \mathbf{R}(G) < \langle g\rangle.$$

The last inequality is strict since $\mathbf{R}(G)$ is normal in G, but $\langle g\rangle$ is not. In particular, the first claim of the lemma implies the second one.

Let $\lambda \in \mathrm{Lin}\langle g\rangle$ be faithful. By Lemma 3.5 applied to $N \trianglelefteq \langle g\rangle$ and since $N \neq 1$, it follows $\lambda(e_N) = 0$. Thus

$$f = e_\lambda + e_{\overline{\lambda}} = \frac{1}{|\langle g\rangle|} \sum_{h\in\langle g\rangle} (\overline{\lambda}(h) + \lambda(h))h \in \mathbb{R}\langle g\rangle$$

is an idempotent with $fe_N = 0$. It follows from Lemma 3.6 that f is a central idempotent in $\mathbb{R}G$, and so $f^x = f$ for all $x \in G$. But by assumption, there is some $x \in G$ such that $g^x \notin \langle g\rangle$. It follows that $\overline{\lambda(g)} + \lambda(g) = 0$. As $\lambda(g)$ is an n-th root of unity, where $n = \mathbf{o}(g)$, this is only possible when $\mathbf{o}(g) = 4$. □

5.2 Lemma. *Suppose that* $1 < \mathrm{NKer}_{\mathbb{R}}(G) < G$ *and that* G *is not a 2-group. Then* G *is generalized dicyclic.*

Proof. By Lemma 5.1, we have that $\mathrm{NKer}_{\mathbb{R}}(G) = \mathbf{R}(G) = \langle z \rangle$, where z has order 2. Every odd-order subgroup of G is normal in G, and in particular the Sylow p-subgroups, for p odd, generate a normal 2-complement, U, of G. As U is Dedekind, it follows that U is abelian.

Now set $A = \mathbf{C}_G(U)$, which contains U. There is $g \in G$ such that $\langle g \rangle \not\trianglelefteq G$. By Lemma 5.1, we have $g^4 = 1$. If $gu = ug$ for some $u \in U$, then $\langle g \rangle$ is characteristic in $\langle gu \rangle = \langle g \rangle \times \langle u \rangle$, and thus $\langle gu \rangle \not\trianglelefteq G$. Again by Lemma 5.1, it follows that $(gu)^4 = 1$ and thus $u = 1$. Thus $\mathbf{C}_U(g) = 1$ and $g \notin A$. In particular, $A < G$.

Conversely, let $g \notin A$, and let $s = g_2$ be the 2-part of g. Then $gA = sA$ and thus $s \notin A$. Thus $u^s \neq u$ for some $u \in U$, and thus $s^u = s[s,u] \notin \langle s \rangle$. It follows that $\langle s \rangle$ is not normal in G, and thus $\langle g \rangle$ is not normal in G. By Lemma 5.1, it follows that $g^2 = z$ (and $s = g$).

In particular, for $g \in G \setminus A$ and $a \in A$, we have $g^2 = z = (ga)^2 = g^2 a^g a$, and thus $a^g = a^{-1}$. For $u \in U$ and $g,\ h \in G \setminus A$ we have $u^g = u^{-1} = u^h$ and thus $gh^{-1} \in \mathbf{C}_G(U) = A$, so $|G : A| = 2$. Thus G is generalized dicyclic. □

To finish the proof of the "only if" part of Theorem B, we use a part of Blackburn's classification [3, Theorem 1]:

5.3 Theorem (Blackburn 1966). *Let* G *be a* p*-group with* $\mathbf{R}(G) \neq 1$. *Then one of the following holds:*

(i) G *is abelian.*
(ii) $p = 2$ *and* G *is generalized dicyclic.*
(iii) $p = 2$ *and* $G \cong C_4 \times Q_8 \times (C_2)^r$, $r \in \mathbb{N}$.
(iv) $p = 2$ *and* $G \cong Q_8 \times Q_8 \times (C_2)^r$, $r \in \mathbb{N}$.

Using Theorem 5.3, it is rather straightforward to determine all finite groups G with $\mathbf{R}(G) \neq 1$, but a rather long list emerges [3, Theorem 2]. However, due to Lemma 5.2, we do not need to go through the longer list of finite groups with $\mathbf{R}(G) \neq 1$.

Proof of Theorem B, "only if". Suppose that $\mathrm{NKer}_{\mathbb{R}}(G) \neq 1$. If $\mathrm{NKer}_{\mathbb{R}}(G) = G$, then G is abelian or $G \cong Q_8 \times (C_2)^r$, by Theorem 4.6.

If $1 < \mathrm{NKer}_{\mathbb{R}}(G) < G$ and G is not a 2-group, then G is generalized dicyclic, by Lemma 5.2. If G is a 2-group, then it follows from Blackburn's classification of 2-groups with $\mathbf{R}(G) \neq 1$ (Theorem 5.3) that G appears on the list in Theorem B. □

We now show that conversely, the groups appearing in Theorem B all have $\mathrm{NKer}_{\mathbb{R}}(G) \neq 1$. To show that certain characters are skew-linear, we use the

Frobenius-Schur indicator. Recall that for $\chi \in \operatorname{Irr} G$, its **Frobenius-Schur indicator** is defined by

$$\nu_2(\chi) := \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

When $\nu_2(\chi) = 1$, then $\chi = \overline{\chi}$ and χ is afforded by a representation with entries in $\mathbb{R}$, so $m_{\mathbb{R}}(\chi) = 1$. When $\nu_2(\chi) = 0$, then $\chi \neq \overline{\chi}$, and again $m_{\mathbb{R}}(\chi) = 1$. Finally, when $\nu_2(\chi) = -1$, then $\chi = \overline{\chi}$, but $m_{\mathbb{R}}(\chi) = 2$. In the last case, there is a simple $\mathbb{R}G$-module affording 2χ, and $\operatorname{End}_{\mathbb{R}G}(S) \cong \mathbb{H}$, the division ring of Hamilton's quaternions [6, Theorem 13.12].

In particular, $\chi \in \operatorname{Irr} G$ is skew-linear over $\mathbb{R}$, if and only if either $\chi(1) = 1$ (χ is linear), or $\chi(1) = 2$ and $\nu_2(\chi) = -1$.

We begin by considering generalized dicyclic groups.

5.4 Lemma. *Let G be generalized dicyclic, and let $g \in G$ and $A \trianglelefteq G$ be as in the definition. Then $\mathbf{R}(G) = \operatorname{NKer}_{\mathbb{R}}(G) = G$ if $G/\langle g^2 \rangle$ is abelian, and $\mathbf{R}(G) = \operatorname{NKer}_{\mathbb{R}}(G) = \langle g^2 \rangle$ else.*

Proof. First, observe that $g^2 = (g^2)^g = g^{-2}$ and thus $g^4 = 1$. Moreover, for any $a \in A$, we have $(ga)^2 = g^2 a^g a = g^2$. By assumption, $g^2 \neq 1$.

In view of Lemma 5.1, it suffices to show that $\langle g^2 \rangle \subseteq \operatorname{NKer}_{\mathbb{R}}(G)$, that is, all characters $\chi \in \operatorname{Irr} G$ with $g^2 \notin \operatorname{Ker} \chi$ are skew-linear. (In the case when $G/\langle g^2 \rangle$ is abelian, all characters of $G/\langle g^2 \rangle$ are linear and thus it will follow that all characters of G are skew-linear and G is Dedekind. Conversely, if $\operatorname{NKer}_{\mathbb{R}}(G) > \langle g^2 \rangle$, then $\operatorname{NKer}_{\mathbb{R}}(G) = G$ by Lemma 5.1, and then $G \cong Q_8 \times (C_2)^r$ by Theorem 4.6 and $G/\langle g^2 \rangle$ is abelian.)

So suppose that $\chi \in \operatorname{Irr} G$ is not linear, and $g^2 \notin \operatorname{Ker} \chi$. Let $\lambda \in \operatorname{Lin} A$ be a constituent of the restriction χ_A. Then $\chi = \lambda^G$ by Clifford theory [7, Corollary 6.19]. As $a^g = a^{-1}$ for all $a \in A$, we have $\lambda^g = \overline{\lambda}$. Also, $\lambda(g^2) \neq 1$, and thus $\lambda(g^2) = -1$ and $\chi(g^2) = -2$. It follows that

$$\begin{aligned} \nu_2(\chi) = \frac{1}{|G|} \sum_{x \in G} \chi(x^2) &= \frac{1}{|G|} \sum_{a \in A} (\chi((ga)^2) + \chi(a^2)) \\ &= \frac{1}{|G|} \left(-2|A| + \sum_{a \in A} (\lambda(a^2) + \overline{\lambda(a^2)}) \right) \\ &= \frac{-2|A|}{|G|} = -1. \end{aligned}$$

Here we have used that $(ga)^2 = g^2$ for all $a \in A$, and that $\sum_{a \in A} \lambda(a^2) = \sum_{a \in A} \lambda^2(a) = 0$ since $\overline{\lambda} \neq \lambda$ and thus $\lambda^2 \neq 1$. Since $\nu_2(\chi) = -1$ and $\chi(1) = 2$, it follows that χ is indeed skew-linear, as claimed. □

5.5 Lemma. *When* $G = \langle u\rangle \times \langle x, y\rangle \times E$ *with* $\langle u\rangle \cong C_4$, $\langle x, y\rangle \cong Q_8$ *and* $E \cong (C_2)^r$, *then* $\mathrm{NKer}_{\mathbb{R}}(G) = \mathbf{R}(G) = \langle u^2x^2\rangle \neq 1$.

Proof. As $\langle ux\rangle \not\trianglelefteq G$, we have $\mathbf{R}(G) \leqslant \langle u^2x^2\rangle$. Let τ be the nonlinear irreducible character of $\langle x, y\rangle$ and λ a character of $\langle u\rangle$ with $\lambda \neq \overline{\lambda}$. If χ is a character with $\chi(u^2x^2) \neq \chi(1)$, then either χ is linear, or $\chi = \lambda^2 \times \tau \times \sigma$, $\sigma \in \operatorname{Lin} E$. The latter characters all have $\nu_2(\chi) = -1$. Thus $\langle u^2x^2\rangle \subseteq \mathrm{NKer}_{\mathbb{R}}(G)$. □

5.6 Lemma. *When* $G = \langle u, v\rangle \times \langle x, y\rangle \times E$ *with* $\langle u, v\rangle \cong \langle x, y\rangle \cong Q_8$ *and* $E \cong (C_2)^r$, *then* $\mathrm{NKer}_{\mathbb{R}}(G) = \mathbf{R}(G) = \langle u^2x^2\rangle \neq 1$.

Proof. As $\langle ux\rangle \not\trianglelefteq G$, we have $\mathbf{R}(G) \leqslant \langle u^2x^2\rangle$. Let τ_1 and τ_2 be the nonlinear characters of $\langle u, v\rangle$ and $\langle x, y\rangle$, respectively. If $\chi(u^2x^2) \neq \chi(1)$, then either $\chi = \tau_1 \times \lambda \times \sigma$ with $\lambda \in \mathrm{Lin}\langle x, y\rangle$ and $\sigma \in \mathrm{Lin}(E)$, or $\chi = \lambda \times \tau_2 \times \sigma$ with $\lambda \in \mathrm{Lin}\langle u, v\rangle$ and $\sigma \in \mathrm{Lin}(E)$. In both cases, $\nu_2(\chi) = -1$ and thus $\langle u^2x^2\rangle \leqslant \mathrm{NKer}_{\mathbb{R}}(G)$. □

This lemma finishes the proof of the "if" part of Theorem B.

6. Classification over the rational numbers

In this section ,we prove Theorem D. Throughout, we write

$$\mathrm{NKer}(G) := \mathrm{NKer}_{\mathbb{Q}}(G) \neq 1.$$

Recall that a *Blackburn group* is a finite group G such that $\mathbf{R}(G)$, the intersection of all nonnormal subgroups of G, is nontrivial. For later reference, we record the following observation (which is part of the argument used by Blackburn to classify these groups):

6.1 Lemma. *Let* G *be a Blackburn group and* p *a prime dividing* $|\mathbf{R}(G)|$. *Then* G *has a normal* p*-complement* A *such that every subgroup of* A *is normal in* G. *If* A *is nonabelian, then* $G = Q_8 \times (C_2)^r \times H$, *where* H *is a Blackburn group of odd order.*

Proof. By definition of $\mathbf{R}(G)$, all the Sylow q-subgroups for $q \neq p$ are normal in G, and thus generate a normal p-complement, A. By definition of $\mathbf{R}(G)$, it follows also that every subgroup of A is normal in G.

In particular, A is a Dedekind group. If A is nonabelian, then $S \in \mathrm{Syl}_2(G)$ is isomorphic to $Q_8 \times (C_2)^r$, by Theorem 4.1. As $S \trianglelefteq G$, there is a 2-complement H. Since every subgroup of S is normal in G, it is easy to see that H centralizes S and thus $G = S \times H$ (this is also shown in [3, Proof of Theorem 2(e)]). Any nonnormal subgroup of H is nonnormal in G and thus $\mathbf{R}(G) \leqslant \mathbf{R}(H)$. □

Thus A is a Dedekind group and $G = PA$ for any $P \in \mathrm{Syl}_p(G)$. The classification of Blackburn groups can now be obtained by considering the different possibilities for P and A (using the fact that P is also a Blackburn group and Theorem 5.3 for P, and Theorem 4.1 for A). However, in our proof of Theorem D, we do not have to consider all the cases of Blackburn's classification separately. First, we reduce to the case that A is abelian.

6.2 Theorem. *Let $G = Q_8 \times (C_2)^r \times H$ with H of odd order. Then $\mathrm{NKer}(G) \neq 1$ if and only if $\mathrm{NKer}(H) \neq 1$ and the multiplicative order of 2 in $(\mathbb{Z}/|H|)^*$ is odd.*

Proof. In view of Theorem 4.5, we may assume that H is nonabelian. Thus $\mathrm{NKer}(G) \leqslant \mathrm{NKer}(H) \leqslant \mathbf{R}(H) < H$ by Lemma 3.4 and Lemma 3.7. Assume $\mathrm{NKer}(G) \neq 1$ and let $z \in \mathrm{NKer}(G)$ have prime order p. Let A be the abelian p-complement of H and suppose $\lambda \in \mathrm{Lin}(\langle z, A\rangle)$ has maximal possible order. (This implies $\lambda(z) \neq 1$, in particular.) Then any $\chi \in \mathrm{Irr}(H \mid \lambda)$ is skew-linear. For $\tau \in \mathrm{Irr}(Q_8)$ with $\tau(1) = 2$, we must have that $\tau \times \chi$ is also skew-linear. Lemma 2.4 yields in particular, that $\mathbb{Q}(\chi)$ must not be a splitting field for $\mathbb{H}$ (the quaternions over $\mathbb{Q}$).

On the other hand, we have $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\varepsilon)$, where ε is a primitive $|H|$-th root of unity. Since every prime dividing $|H|$ also divides $\mathbf{o}(\lambda)$, we see that $|\mathbb{Q}(\lambda) : \mathbb{Q}(\chi_A)|$ is odd. Therefore, $|\mathbb{Q}(\varepsilon) : \mathbb{Q}(\chi)|$ is odd as well. Thus $\mathbb{Q}(\chi)$ is a splitting field for the quaternions, if and only if $\mathbb{Q}(\varepsilon)$ is a splitting field for the quaternions. Now Lemma 4.4(iii) yields that the condition on the order of 2 mod $|H|$ holds.

Conversely, assume that this condition holds, and let $\chi \in \mathrm{Irr}(H)$ be skew-linear over $\mathbb{Q}$, and $\sigma \in \mathrm{Irr}(S)$, where $S = Q_8 \times (C_2)^r$. Let D be the block ideal of $\mathbb{Q}H$ corresponding to χ. This is a division ring with center isomorphic to $\mathbb{Q}(\chi)$. If σ is linear, then the block ideal corresponding to $\sigma \times \chi$ is again isomorphic to D. If σ is nonlinear, then the block ideal corresponding to $\sigma \times \chi$ is isomorphic to

$$(\mathbb{H} \otimes_{\mathbb{Q}} \mathbb{Q}(\chi)) \otimes_{\mathbb{Q}(\chi)} D,$$

by Lemma 2.4. This is a division ring since both factors are division rings and one has dimension 4 over its center, and the other has odd dimension. Thus $\sigma \times \chi$ is skew-linear. This shows that $\mathrm{NKer}(G) = \mathrm{NKer}(H)$. The theorem follows. □

Next, we consider nilpotent groups.

6.3 Theorem. *Let G be nilpotent. Then $\mathrm{NKer}(G) \neq 1$ if and only if one of the following holds.*

(i) *G is abelian.*

(ii) *$G = S \times A$, where $S \in \mathrm{Syl}_2(G)$ is a nonabelian group from the list in Theorem 5.3 and has exponent 4, and A is abelian of odd order, and the multiplicative order of 2 in $(\mathbb{Z}/|A|)^*$ is odd.*

(iii) *G is a generalized dicyclic 2-group.*

Proof. If G is nonabelian, then the Sylow 2-subgroup S is nonabelian, and all other Sylow subgroups are abelian, by Theorem 5.3. Thus $G = S \times A$ with A abelian. If S has exponent 4, then the nonlinear, but skew-linear characters of S yield the quaternions over $\mathbb{Q}$ as block ideal of the rational group algebra $\mathbb{Q}S$, and the result follows from Lemma 4.4(iii), and Lemma 2.4.

If S contains elements of order 8 or greater, then S is generalized dicyclic, and there is a skew-linear $\sigma \in \operatorname{Irr} S$ such that $S/\operatorname{Ker}(\sigma)$ is a dicyclic (=generalized quaternion) group of order at least 16. Then $\mathbb{Q}(\sigma)$ contains $\sqrt{2}$. As $S/\operatorname{Ker}(\sigma)$ has a subgroup of order 8 isomorphic to the quaternion group, the block ideal of $\mathbb{Q}S$ corresponding to σ is isomorphic to the quaternions over a field containing $\sqrt{2}$. But since $\mathbb{H} \otimes \mathbb{Q}_2(\sqrt{2})$ splits (Lemma 4.4(iv)), the Schur index of such a character at the prime 2 is trivial. If $G = S \times A$, then any character $\sigma \times \lambda$ with $1_A \neq \lambda \in \operatorname{Lin} A$ has trivial Schur index over the reals, and over all other primes anyway. Thus we can have $\operatorname{NKer}(G) \neq 1$ only if $G = S$ in this case. □

To prove Theorem D, we can now assume that the p-complement A in Lemma 6.1 is abelian, and that $G = PA$ is not nilpotent. In other words, $\mathbf{C}_P(A) < P$, where $P \in \operatorname{Syl}_p(G)$. It is not difficult to see that P is then either abelian or generalized dicyclic: Namely, $\mathbf{R}(P) \neq 1$ and so P occurs on the list from Theorem 5.3. If $P \cong C_4 \times Q_8 \times (C_2)^r$ or $P \cong Q_8 \times Q_8 \times (C_2)^r$, however, then P is generated by elements u such that $\langle u \rangle \cap \mathbf{R}(P) = 1$ and thus P would centralize A, so this is impossible. (Alternatively, look at Blackburn's list [3, Theorem 2].)

It remains to show that in this situation, (iv) in Theorem D holds, or $p = 2$ and G is generalized dicyclic.

We begin with some elementary observations, which were also used in Blackburn's classification.

6.4 Lemma. *Let Q be a finite abelian q-group and suppose that P acts on Q by automorphisms such that every subgroup of Q is P-invariant, and $(|P|, |Q|) = 1$. Then $P/\mathbf{C}_P(Q)$ is cyclic of order dividing $q - 1$, and $\mathbf{C}_P(x) = \mathbf{C}_P(Q) = P_\lambda$ for every $1 \neq x \in Q$ and $1_Q \neq \lambda \in \operatorname{Lin} Q$.*

Proof. Take $x \in Q$ of maximal order and $u \in P$. Since $x^u \in \langle x \rangle$ by assumption, we have $x^u = x^k$ for some $k \in \mathbb{N}$. If $y \in Q$ with $\langle x \rangle \cap \langle y \rangle = 1$, then $y^u = y^k$, since u maps $\langle y \rangle$ and $\langle xy \rangle$ to itself. It follows that $y^u = y^k$ for all $y \in Q$.

Therefore, $P/\mathbf{C}_P(Q)$ is isomorphic to a q'-subgroup of $\operatorname{Aut}(\langle x \rangle)$, and thus is cyclic of order dividing $q - 1$.

Finally, suppose $1 \neq x \in Q$ and $x^u = x$ for some $u \in P$. As we have just seen, there is $k \in \mathbb{N}$ such that $y^u = y^k$ for all $y \in Q$. It follows that $k \equiv 1 \mod q$ (as $q \mid \mathbf{o}(x)$). Since $|P/\mathbf{C}_P(Q)|$ divides $q - 1$, it follows that $k^{q-1} \equiv 1 \mod q^n$, where

q^n is the exponent of Q. But this yields that $k \equiv 1 \mod q^n$ and thus $u \in \mathbf{C}_P(Q)$ as claimed. The proof for $\lambda \in \operatorname{Lin} Q$ is similar, using that there is ℓ such that $\mu^u = \mu^\ell$ for all $\mu \in \operatorname{Lin} Q$. □

6.5 Lemma. *Let $G = PA$ be a Blackburn group with normal abelian p-complement A and $\mathbf{R}(G) \leqslant P \in \operatorname{Syl}_p(G)$. Suppose that $\chi \in \operatorname{Irr}(G)$ is skew-linear over $\mathbb{Q}_q$, where q is a prime dividing $|A|$. Then P centralizes every Sylow r-subgroup R of A such that $r \neq q$ and $R \not\subseteq \operatorname{Ker}(\chi)$.*

Proof. Let $r \neq q$ and $R \in \operatorname{Syl}_r(A)$, and assume that $R \not\subseteq \operatorname{Ker}(\chi)$. Let $\lambda \in \operatorname{Lin}(R)$ be a linear constituent of χ_R, so that $\lambda \neq 1$.

By Lemma 6.4, $\mathbf{C}_P(R) = \mathbf{C}_P(x)$ for any $1 \neq x \in R$, and thus also

$$\mathbf{C}_P(R) = P_\lambda := \{u \in P \mid \lambda^u = \lambda\}.$$

Consider the subgroup $H = PR$, and choose a constituent $\vartheta \in \operatorname{Irr}(H)$ of χ_H that lies over λ. Then $\vartheta = \psi^H$ for some $\psi \in \operatorname{Irr}(H_\lambda)$, where $H_\lambda = \mathbf{C}_P(R)R$. Thus $\vartheta(1) \geqslant |P : \mathbf{C}_P(R)|$. On the other hand, by Corollary 2.6 we have that $\vartheta(1) = 1$, and thus $P = \mathbf{C}_P(R)$ as claimed. □

6.6 Lemma. *Let $G = PA$ be a group with a normal abelian p-complement A and $1 \neq \operatorname{NKer}(G) \leqslant P \in \operatorname{Syl}_p(G)$. Suppose that $|P : \mathbf{C}_P(A)| > 2$. Then P is abelian, and there is exactly one Sylow subgroup of A which is not centralized by P.*

Proof. Let $z \in \operatorname{NKer}(G) \subseteq P$ be an element of order p. Choose $\tau \in \operatorname{Irr}(P)$ with $z \notin \operatorname{Ker}(\tau)$.

For $\lambda \in \operatorname{Lin}(A)$ arbitrary, we have

$$[(\tau^G)_A, \lambda]_A = [(\tau_{P\cap A})^A, \lambda]_A = [\tau_{P\cap A}, \lambda_{P\cap A}]_{P\cap A} = \tau(1) > 0,$$

as $P \cap A = 1$. Thus for any $\lambda \in \operatorname{Lin}(A)$, there is $\chi \in \operatorname{Irr}(G)$ such that $[\chi, \tau^G] > 0$ and $[\chi_A, \lambda] > 0$. We apply this to a λ such that $\lambda_R \neq 1_R$ for each Sylow subgroup, R, of A. Thus there is a $\chi \in \operatorname{Irr}(G)$ lying over τ and such that $\operatorname{Ker}(\chi)$ contains no Sylow subgroup of A.

Notice that $\mathbf{C}_P(A) = P_\lambda$ for such a λ, by Lemma 6.4. As χ is induced from a character of G_λ, it follows that $\chi(1) \geqslant |G : G_\lambda| = |P : \mathbf{C}_P(A)| > 2$.

Because $z \notin \operatorname{Ker}(\chi)$ and $z \in \operatorname{NKer}(G)$, it follows that χ is skew-linear over $\mathbb{Q}$ and thus $m_{\mathbb{Q}}(\chi) = \chi(1)$. By Ito's theorem [7, Theorem 6.15], $\chi(1)$ divides $|G : A| = |P|$ and thus is a power of p. It follows from Lemma 2.5(i) that there is a prime q (possibly infinite) such that $m_q(\chi) = m_{\mathbb{Q}}(\chi) = \chi(1)$.

Since $\chi(1) \geqslant |P : \mathbf{C}_P(A)| > 2$, it follows from Lemma 2.5(ii) that the prime q, such that $m_q(\chi) = \chi(1)$, must be a finite, odd prime and $q \neq p$. It follows that q divides $|A|$. Now Corollary 2.6 yields that τ is linear. Since the only assumption on $\tau \in \operatorname{Irr} P$ was that $z \notin \operatorname{Ker}(\tau)$, Lemma 3.2 yields that P is abelian. Lemma 6.5 yields that P centralizes all Sylow subgroups of A except the Sylow q-subgroup. □

6.7 Lemma. *Let $G = SA$ be a group, where A is a normal (abelian) 2-complement and $1 \neq \mathrm{NKer}(G) \leqslant S \in \mathrm{Syl}_2(G)$, and suppose $|S : \mathbf{C}_S(A)| = 2$. Then either G is as in Lemma 6.6 (with $p = 2$), or G is generalized dicyclic.*

(Notice that A is automatically abelian here since A is a Dedekind group of odd order.)

Proof of Lemma 6.7. First we show that $C := \mathbf{C}_S(A)$ is abelian. Let $z \in \mathrm{NKer}(G)$ have order 2. Then $z \in \mathbf{Z}(G)$ and thus $z \in C$. If C is not abelian, there is $\tau \in \mathrm{Irr}(C)$ with $\tau(z) \neq \tau(1) > 1$ (Lemma 3.2). Let $t \in S \setminus C$, and let $\lambda \in \mathrm{Lin}(A)$ be such that $\lambda^t \neq \lambda$. Then $\chi := (\tau \times \lambda)^G \in \mathrm{Irr}(G)$, and $\chi(1) \geqslant 2\tau(1) > 2$. By Lemma 2.5 (ii), χ can not be skew-linear over $\mathbb{R}$ or $\mathbb{Q}_2$. Since χ_C has a non-linear constituent, χ can not be skew-linear over $\mathbb{Q}_q$ for odd primes q, by Corollary 2.6. As $\chi(1) = 2^r$, it follows from Lemma 2.5 (i) that $m_{\mathbb{Q}}(\chi) < \chi(1)$, and thus $z \notin \mathrm{NKer}(G)$, contradiction. Thus C is abelian as claimed, and $G = SA$ has the abelian subgroup CA of index 2.

Fix $t \in S \setminus C$. Notice that $A = [A, t] \times C_A(t)$. Since every subgroup of A is normal in G, the factors of this decomposition have coprime orders. Also, we have $[A, t] \neq 1$ by assumption, and t inverts the elements in $[A, t]$.

Consider first the case $\mathbf{C}_A(t) \neq 1$. Pick some $\lambda \in \mathrm{Lin}(A)$ such that $\mathrm{Ker}(\lambda)$ contains no Sylow subgroup of A. Then $\lambda^t \notin \{\lambda, \overline{\lambda}\}$. Consider extensions μ to CA with $\mu(z) = -1$, where $z \in \mathrm{NKer}(G)$ has order 2 as before. As $\mu^t \neq \mu$, we have $\chi = \mu^G \in \mathrm{Irr}(G)$. Then χ remains irreducible modulo 2, and thus $m_2(\chi) = 1$, by Lemma 2.5 (iii). As $\mu^t \neq \overline{\mu}$, we have also $m_{\mathbb{R}}(\chi) = 1$. But as $z \notin \mathrm{NKer}(G)$, it follows that $m_q(\chi) = 2$ for some odd prime q dividing $|A|$. Then Lemma 6.5 yields that S centralizes every Sylow subgroup of A except one. Also Corollary 2.6 yields that χ_S is a sum of linear characters. As μ was an arbitrary extension of λ to $CA = C \times A$ with $\mu(z) = -1$, this means that $\nu^t = \nu$ for all $\nu \in \mathrm{Lin}(C)$ with $\nu(z) = -1$. Thus S is abelian and G is as in Lemma 6.6 with $p = 2$ in this case.

Now assume that $\mathbf{C}_A(t) = 1$. If S is abelian and C is not just an elementary abelian 2-group, then again we find μ and χ as above, with $m_q(\chi) = 2$ for some odd prime q, and the result follows again.

If S is abelian and C is elementary 2-abelian, then $G = S[A, t]$ is generalized dicyclic.

Finally, assume that $\mathbf{C}_A(t) = 1$ and that S is nonabelian. Then S is generalized dicyclic, and S has an abelian subgroup D of index 2, such that $d^s = d^{-1}$ for all $d \in D$ and $s \in S \setminus D$. If $D = C$, then G is generalized dicyclic. Thus we may assume that $D \neq C$. If S is Dedekind, then $S \cong Q_8 \times (C_2)^r$, and we could choose $D = C$. So we can assume that S is not Dedekind, and thus $\mathbf{R}(S) = \langle z \rangle$ by Lemma 5.4. We may choose $t \in D \setminus C$ and $s \in C \setminus D$. Since both C and D are abelian, it follows that s centralizes $C \cap D$, and at the same time inverts the elements in $C \cap D$. Thus

$C \cap D$ has exponent 2. Since $|S : C| = |S : D| = 2$ and $z \in \langle s \rangle \cap \langle t \rangle$, it follows $s^2 = t^2 = z$. Since $st \notin D$, we also have $(st)^2 = z$. It follows that $\langle s, t \rangle \cong Q_8$ and $S = \langle s, t \rangle \times (C \cap D) \cong Q_8 \times (C_2)^r$. But then S is Dedekind and G generalized dicyclic, contradiction. □

The following is part of [3, Theorem 2(a)].

6.8 Lemma. *Let $G = PA$ be a Blackburn group such that $\mathbf{R}(G) \leqslant P \in \mathrm{Syl}_p(G)$ and such that P and the normal p-complement A are abelian. Then we can write $P = \langle g \rangle \times P_0$, such that $\mathbf{C}_P(A) = \langle g^{p^c} \rangle \times P_0$ ($c \geqslant 1$), and $p^d := \mathbf{o}(g^{p^c})$ is the exponent of $\mathbf{C}_P(A)$. There is a $k \in \mathbb{N}$ such that $a^g = a^k$ for all $a \in A$.*

6.9 Lemma. *Let $G = PA$ be a Blackburn group, with a normal abelian p-complement A and $P \in \mathrm{Syl}_p(G)$, where p divides $\mathbf{R}(G)$. Let q be a prime divisor of $|A|$, and H a q-complement in G. If $\chi \in \mathrm{Irr}(G)$, then $m_q(\chi) = |\mathbb{Q}_q(\chi, \vartheta) : \mathbb{Q}_q(\chi)|$ for any irreducible constituent $\vartheta \in \mathrm{Irr}(H)$ of χ_H.*

Proof. Let $Q \in \mathrm{Syl}_q(G)$. Notice that $Q \trianglelefteq G$ and thus Q has a complement H in G. Let $\lambda \in \mathrm{Lin}(Q)$ be a constituent of χ_Q. Then $K = \mathrm{Ker}(\lambda)$ is normal in G (by definition of $\mathbf{R}(G)$) and thus $K \subseteq \mathrm{Ker}(\chi)$. We may factor out K and assume without loss of generality that $K = 1$.

This means that Q is cyclic and thus χ is in a q-block with cyclic defect group. Thus we can apply Benard's theorem [2] to χ and conclude that $m_q(\chi) = |\mathbb{Q}_q(\chi, \varphi) : \mathbb{Q}_q(\chi)|$ for any irreducible Brauer constituent φ of χ. But an irreducible Brauer character of G contains the normal q-subgroup Q in its kernel, and thus can be identified with an ordinary character of the q'-group $H \cong G/Q$. Thus if φ is an irreducible Brauer constituent of χ, then $\varphi_H = \vartheta \in \mathrm{Irr}(H)$ is an irreducible constituent of χ, and the result follows from Benard's theorem. □

6.10 Lemma. *Let $G = PA$ be a Blackburn group, with a normal abelian p-complement A and $P \in \mathrm{Syl}_p(G)$, where p divides $\mathbf{R}(G)$. Assume that $A = Q \times B$, where $B = \mathbf{C}_A(P)$ and $Q \in \mathrm{Syl}_q(G)$, and set $C = \mathbf{C}_P(Q)$. Any nonlinear $\chi \in \mathrm{Irr}(G)$ has the form $\chi = (\mu \times \lambda)^G$ for some $\mu \in \mathrm{Lin}(CB)$ and $\lambda \in \mathrm{Lin}(Q)$. Let $\vartheta \in \mathrm{Lin}(PB \mid \mu)$. Then $m_q(\chi) = \ell/k$, where ℓ is the smallest positive integer such that $\mathbf{o}(\vartheta)$ divides $q^\ell - 1$, and k is the smallest positive integer such that $\mathbf{o}(\mu)$ divides $q^k - 1$.*

(In other words, ℓ and k are the multiplicative orders of q modulo $\mathbf{o}(\vartheta)$ and modulo $\mathbf{o}(\mu)$, respectively.)

Proof of Lemma 6.10. Notice that $CB = \mathbf{Z}(G)$, and that $H = PB$ is an abelian q-complement. Let $\chi \in \mathrm{Irr}(G)$. If $Q \leqslant \mathrm{Ker}(\chi)$, then χ is linear, since $G/Q = P \times B$ is abelian. (In fact, $Q = G'$.) Otherwise, let $\lambda \neq 1$ be a linear constituent of

χ_Q. Then $G_\lambda = CBQ = CA$, and χ is induced from some linear character of the abelian group CBQ, say $\chi = (\mu \times \lambda)^G$ with $\mu \in \mathrm{Lin}(CB)$. It follows that $\mathbb{Q}_q(\chi) = \mathbb{K}(\mu)$, where $\mathbb{K} \subseteq \mathbb{Q}_q(\lambda)$ is totally ramified over $\mathbb{Q}_q$, and the extension $\mathbb{K}(\mu)/\mathbb{K}$ is unramified. By the general form of unramified extensions, the residue field of $\mathbb{Q}_q(\chi) = \mathbb{K}(\mu)$ has order q^k, where k is the smallest positive integer such that $\mathbf{o}(\mu)$ divides $q^k - 1$.

The restriction χ_H to the q-complement $H = PB$ is the sum of all linear characters $\vartheta \in \mathrm{Lin}(H)$ lying over μ. Thus $\mathbb{Q}_q(\chi, \vartheta) = \mathbb{K}(\vartheta)$ is generated by $\mathbb{Q}_q(\chi)$ and a root of unity of order $\mathbf{o}(\vartheta)$. Since $\mathbf{o}(\vartheta)$ is not divisible by q, the extensions $\mathbb{Q}_q(\chi, \vartheta)/\mathbb{Q}_q(\chi)$ and $\mathbb{K}(\vartheta)/\mathbb{K}$ are unramified. We can thus compute $|\mathbb{Q}_q(\chi, \vartheta) : \mathbb{Q}_q(\chi)|$ by computing the degrees of the residue fields. As above, the residue field of $\mathbb{Q}_q(\chi, \vartheta) = \mathbb{K}(\vartheta)$ has order q^ℓ, where ℓ is the smallest positive integer such that $\mathbf{o}\,\vartheta$ divides $q^\ell - 1$. Now the result follows from Lemma 6.9. □

6.11 Lemma. *Let $G = (PQ) \times B$ be as in Theorem D (iv). Then* $\mathrm{NKer}_{\mathbb{Q}_q}(G) \neq 1$. *(More precisely,* $\mathrm{NKer}_{\mathbb{Q}_q}(G) \cap \langle g \rangle \neq 1$, *with $g \in P$ as in Lemma C.)*

Notice that this contains Lemma C from the introduction.

Proof. Recall that $P = \langle g \rangle \times P_0$, where g has order p^{c+d} and $C := \mathbf{C}_P(Q) = \langle g^{p^c} \rangle \times P_0$. Moreover, we assume that $(q-1)_p$ divides p^d. Let $z \in \langle g^{p^c} \rangle$ be an element of order p. We claim that $z \in \mathrm{NKer}_{\mathbb{Q}_q}(G)$.

Suppose that $\chi(z) \neq \chi(1)$ for $\chi \in \mathrm{Irr}\, G$. If $\chi(1) > 1$, then $\chi = (\mu \times \lambda)^G$ as in Lemma 6.10, with $\mu \in \mathrm{Lin}(CB)$ and $1 \neq \lambda \in \mathrm{Lin}\, Q$.

To compute the Schur index of such a χ, we apply Lemma 6.10. Since $\mu(z) \neq 1$, it follows that $\mathbf{o}(\mu) = p^d n$, where n divides the exponent of B. For $\vartheta \in \mathrm{Lin}(PB \mid \mu)$, we have $\mathbf{o}(\vartheta) = p^c\, \mathbf{o}(\mu) = p^{c+d} n$. Let f be the order of q modulo p^d, so that p^d divides $q^f - 1$. As $(q-1)_p$ divides p^d, it follows that $(q^f - 1)_p = p^d$. Thus the order of q modulo p^{c+d} is $p^c f$.

Let k and l be the multiplicative order of q modulo $p^d n$ and $p^{c+d} n$, respectively. The assumption in (iv) in Theorem D yields that k/f is not divisible by p. Thus we must have $l/k \geqslant p^c$ and thus $m_q(\chi) = p^c = \chi(1)$. This was to be shown. □

Proof of Theorem D. By Theorem 6.2, Theorem 6.3 and Lemma 6.11, each of the conditions in Theorem D ensures that $\mathrm{NKer}(G) \neq 1$.

Conversely, assume that $\mathrm{NKer}(G) \neq 1$. By Lemma 6.1, we have that $G = PA$, where $P \in \mathrm{Syl}_p(G)$ and A is a normal p-complement and a Dedekind group. By Theorem 6.2, we may assume that A is abelian. By Theorem 6.3, we can assume that G is not nilpotent, and thus $\mathbf{C}_P(A) < P$. By Lemmas 6.6 and 6.7, we can assume that $G = (PQ) \times B$, and that P is also abelian. Thus Lemma 6.8 applies. Write $P = \langle g \rangle \times P_0$ and $\mathbf{C}_P(A) = \langle g^{p^c} \rangle \times P_0$, as in that lemma.

Let $z \in \mathbf{R}(G) \subseteq \langle g^{p^c} \rangle$ have order p and notice that we must have $z \in \mathrm{NKer}(G)$, since $1 \neq \mathrm{NKer}(G) \leqslant \mathbf{R}(G)$. Thus we must have $m_{\mathbb{Q}}(\chi) = \chi(1)$ for any $\chi \in \mathrm{Irr}(G)$

with $\chi(z) \neq \chi(1)$. Suppose $\chi = (\mu \times \lambda)^G$ as in Lemma 6.10. By the local-global principle (Lemma 2.5 (i)), the Schur index of χ over some local field must equal $\chi(1) = |P : C| = p^c$. We claim that this local field must be $\mathbb{Q}_q$ at least for some nonlinear χ. If $p^c > 2$, then we must have $m_q(\chi) = \chi(1)$, by Lemma 6.5. In the case where $p^c = 2$, choose $\mu \in \mathrm{Lin}(CB)$ of order greater than 2. This is possible since when the exponent of $C \times B = \mathbf{Z}(G)$ divides 2, then G is generalized dicyclic, and the proof is finished. We have then $m_{\mathbb{R}}(\chi) = 1$. Also, χ is induced from a subgroup of index 2 (which is not a 2-group), and thus χ remains irreducible after reducing mod 2. Thus $m_2(\chi) = 1$ by Lemma 2.5 (iii). Thus in every case, we must have $m_q(\chi) = \chi(1)$.

We can now apply Lemma 6.10. Notice that since $\mu(z) \neq 1$ by assumption, we have $\mathbf{o}(\vartheta) = p^c\,\mathbf{o}(\mu)$, as can be seen from the structure of P (Lemma 6.8), and $\mathbf{o}(\mu) = p^d \cdot n$, where n divides the exponent of B, and thus is not divisible by p. We may choose μ such that n equals the exponent of B. Let f be the order of $q \mod p^d$ and let k' be the order of $q^f \mod n$. Then the order of $q \mod p^d n$ is $k = fk'$. If $p^d < (q-1)_p$, or if p divides k', then certainly $p^d < (q^k - 1)_p$. But this yields that $q^{kp^{c-1}} \equiv 1 \mod p^{c+d}n$, and thus Lemma 6.10 yields that $m_q(\chi) < p^c$, contradiction. This means that (iv) in Theorem D holds. □

Acknowledgment

I wish to thank Erik Friese for a thorough reading of the paper reproduced here, and for many useful remarks.

References for Chapter III

1. László Babai. Symmetry groups of vertex-transitive polytopes. *Geometriae Dedicata* **6**, no. 3 (1977), pp. 331–337. DOI: 10.1007/BF02429904. MR0486080(58#5868), Zbl. 0388.05025 (cited on p. 76).
2. Mark Benard. Schur indices and cyclic defect groups. *Ann. Math. (2)* **103**, no. 2 (1976), pp. 283–304. DOI: 10.2307/1971007, JSTOR: 1971007. MR0412265, Zbl. 0308.20012 (cited on p. 93).
3. Norman Blackburn. Finite groups in which the nonnormal subgroups have nontrivial intersection. *J. Algebra* **3** (1966), pp. 30–37. DOI: 10.1016/0021-8693(66)90018-4. MR0190229, Zbl. 0141.02401 (cited on pp. 77, 82, 86, 88, 90, 93).
4. Walter Feit. *The Representation Theory of Finite Groups*. North-Holland Mathematical Library 25. North-Holland, Amsterdam, New York, and Oxford, 1982. MR661045, Zbl. 0493.20007 (cited on p. 80).
5. Bertram Huppert. *Endliche Gruppen I*. Die Grundlehren der Mathematischen Wissenschaften 134. Springer, Berlin, Heidelberg, and New York, 1967. MR0224703 (37#302), Zbl. 0217.07201 (cited on p. 83).

6. Bertram Huppert. *Character Theory of Finite Groups*. De Gruyter Expositions in Mathematics 25. Walter de Gruyter, Berlin and New York, 1998. DOI: 10.1515/9783110809237. MR1645304(99j:20011), Zbl. 0932.20007 (cited on pp. 77, 78, 84, 87).
7. I. Martin Isaacs. *Character Theory of Finite Groups*. Dover, New York, 1994. (Corrected reprint of the 1976 edition by Academic Press, New York). MR1280461, Zbl. 0849.20004 (cited on pp. 77, 78, 80, 81, 87, 91).
8. T[sit] Y[uen] Lam. *Introduction to Quadratic Forms Over Fields*. Graduate Studies in Mathematics 67. American Mathematical Society, Providence, RI, 2005. MR2104929, Zbl. 1068.11023 (cited on p. 85).
9. Claude Moser. Représentation de -1 comme somme de carrés dans un corps cyclotomique quelconque. *J. Number Theory* **5** (1973), pp. 139–141. DOI: 10.1016/0022-314x(73)90067-x. MR0316423, Zbl. 0276.12010 (cited on p. 84).
10. Irving Reiner. *Maximal Orders*. L.M.S. Monographs 5. Academic Press, London and New York, 1975. MR0393100(52#13910), Zbl. 0305.16001 (cited on p. 80).
11. Sudarshan K. Sehgal. Nilpotent elements in group rings. *Manuscripta Math.* **15**, no. 1 (1975), pp. 65–80. DOI: 10.1007/bf01168879. MR0364417(51#671), Zbl. 0302.16010 (cited on pp. 75, 77, 85).
12. Jean-Pierre Serre. *Cours d'arithmétique*. Collection SUP: "Le Mathématicien" 2. Presses Universitaires de France, Paris, 1970. MR0255476, Zbl. 0225.12002 (cited on p. 84).
13. Toshihiko Yamada. *The Schur Subgroup of the Brauer Group*. Lecture Notes in Mathematics 397. Springer-Verlag, Berlin, 1974. DOI: 10.1007/BFb0061703. MR0347957(50#456), Zbl. 0321.20004 (cited on p. 80).

Chapter IV.

Classification of Orbit Symmetry Groups for some Fields[1]

Erik Friese and Frieder Ladisch

Abstract. We determine all finite groups that are isomorphic to the affine symmetry group of an orbit polytope, thereby answering a question of Babai. We also classify the finite groups that are isomorphic to the affine symmetry group of an orbit polytope with rational vertices.
2010 Mathematics Subject Classification. Primary 52B15, Secondary 52B12, 20B25
Keywords. Orbit polytope, affine symmetry, linear group,

1. Orbit polytopes of elementary abelian 2-groups

This chapter is a continuation of Chapter II. We determine all finite groups which are isomorphic to the affine symmetry group of a vertex-transitive polytope. As we will explain in Section 2 below, it follows from results of Babai that abelian groups of exponent > 2 can not be isomorphic to the affine symmetry of an orbit polytope. (Alternatively, it follows from Theorem 9.7, together with Corollary 9.3, that an orbit polytopes $\mathrm{P}(G, v)$ of an abelian group G always has an affine symmetry sending gv to $g^{-1}v$.)

In this section, we consider elementary abelian 2-groups. We show that the elementary abelian groups of orders 4, 8 and 16 are not generically closed with respect to any representation in characteristic 0.

It is also true that elementary abelian 2-groups of all other orders *are* generically closed with respect to some representation, and thus can be realized as linear symmetry groups of orbit polytopes. This yields counterexamples to a conjecture of Baumeister et al. [3, Conjecture 5.4]. Since the corresponding construction from our joint paper [FL1] is due to Erik Friese alone, it is not included in this thesis.

We begin with some general remarks. Recall that an elementary abelian 2-group G of order 2^n is isomorphic to the additive group $\mathbb{F}_2^n$ and can be viewed as a vector space over $\mathbb{F}_2$. Every representation $G \to \mathrm{GL}(d, \mathbb{C})$ is similar to a representation D

[1] This chapter contains material from references [FL1] and [FL2] in slightly revised form, and completes the results of Chapter II.

of the form

$$g \mapsto D(g) = \begin{pmatrix} \lambda_1(g) & & & \\ & \lambda_2(g) & & \\ & & \ddots & \\ & & & \lambda_d(g) \end{pmatrix},$$

where each $\lambda_i \colon G \to \{\pm 1\}$ is a linear character which is a constituent of D. For every field $\mathbb{K}$ of characteristic 0, every simple $\mathbb{K}G$-module is one-dimensional and corresponds to a unique linear character of G. We have $\mathbb{K}G \cong \mathbb{K}^{|G|}$ (as $\mathbb{K}$-algebras). By Theorem 8.1 from Chapter II, $\mathbb{K}^d$ is the affine hull of some G-orbit if and only if the λ_i's are different and also different from the trivial character.

It follows that every representation $D \colon \mathbb{F}_2^n \to \mathrm{GL}(d, \mathbb{K})$ is similar to one arising from the following construction: Let C be a $d \times n$-matrix over $\mathbb{F}_2$. For a vector $y = (y_1, \ldots, y_d)^t \in \mathbb{F}_2^d$, we write $(-1)^y = ((-1)^{y_1}, \ldots, (-1)^{y_d})^t \in \mathbb{K}^d$. Then define a representation D by $D(x) = \mathrm{diag}((-1)^{Cx})$ for $x \in \mathbb{F}_2^n$. The representation D is faithful if and only if C has rank n. Every G-orbit is affinely G-equivalent to an image of G under a representation. Since all representations of G in characteristic 0 are similar to a representation over $\mathbb{Q}$, all G-orbits can be identified with the vertices of a representation polytope over $\mathbb{Q}$.

Notice that the character of such a representation is given by $\gamma(x) = d - 2w(Cx)$, where $w(y)$ denotes the Hamming weight of $y \in \mathbb{F}_2^d$. The rows of C correspond to the irreducible constituents of D. The vector space $\mathbb{K}^d$ contains (linearly) full-dimensional orbits if all rows of C are different. Equivalently, we have $[\gamma, \lambda] \in \{0, 1\}$ for all $\lambda \in \mathrm{Irr}\, G$. For convenience, let us call such a character an **ideal character**. We have $\mathbb{K}^d = \mathrm{Aff}(Gv)$ for some orbit Gv if additionally C has no zero row (equivalently, $[\gamma, 1_G] = 0$). So it is no loss of generality to assume $[\gamma, 1_G] = 0$, but we will not need this.

If γ is an ideal character, then a permutation π of $G = \mathbb{F}_2^n$ describes a linear symmetry of $D(G)$ if and only if $\gamma(\pi(y) - \pi(x)) = \gamma(y - x)$ for all $x, y \in \mathbb{F}_2^n$. (This is Corollary 9.6 from Chapter II with additive notation for the group G.) In particular, every automorphism of $G = \mathbb{F}_2^n$ that fixes γ induces a linear symmetry of the orbit which maps 0 to 0. If there is such an automorphism, then $\mathrm{AGL}(P(D)) > D(G)$. This can be used to prove the following:

1.1 Lemma. *All orbit polytopes of the elementary abelian 2-groups of orders 4, 8 and 16 have additional affine symmetries.*

Proof. The group $\mathrm{Aut}(G) = \mathrm{GL}(n, 2)$ acts on the set of ideal characters of degree d by $(\gamma, A) \mapsto \gamma \circ A$ for a character γ and $A \in \mathrm{GL}(n, 2)$. There are $\binom{2^n - 1}{d}$ ideal characters of degree d. It follows that when $\binom{2^n - 1}{d} < |\mathrm{GL}(n, 2)|$, then every ideal character of degree d has non-trivial stabilizer in $\mathrm{GL}(n, 2)$. The elements in the stabilizer of an ideal character induce additional affine symmetries of the

corresponding orbit polytope. But for $n = 2$, 3 and 4, we have $\binom{2^n-1}{d} < |\mathrm{GL}(n,2)|$ for all d. (E. g., for $n = 4$, $d = 7$ we have $\binom{15}{7} = 6435 < |\mathrm{GL}(4,2)| = 20160$.) Thus orbit polytopes of the elementary abelian 2-groups of orders 4, 8 and 16 have additional affine symmetries. □

1.2 Remark. We now digress to describe the orbit polytopes for the elementary abelian groups of orders 4 and 8.

For $G = \mathbb{F}_2^2$, the only possible orbit polytopes of G with $|G| = 4$ vertices are the square in dimension 2 and the 3-simplex (tetrahedron) in dimension 3. The square has affine symmetry group D_4 of order 8, and the 3-simplex has affine symmetry group S_4 of order 24.

Before we describe the polytopes for $G = \mathbb{F}_2^3$, we make some general remarks. If two ideal characters of G are in the same orbit under $\mathrm{Aut}(G)$, then the corresponding orbit polytopes of G are affinely equivalent. (If the ideal characters belong to different orbits, then it can still happen that the corresponding orbit polytopes are affinely equivalent [2], but at least for the elementary abelian groups of orders 4, 8 and 16, this is not the case.) Thus the number of orbit polytopes up to affine equivalence is at most the number of $\mathrm{Aut}(G)$-orbits on the set of ideal characters.

From this count, we can exclude the ideal characters that have a nontrivial kernel, because then the corresponding orbit polytope can be viewed as an orbit polytope of a proper factor group. For example, for $G = \mathbb{F}_2^3$, we get six orbits of $\mathrm{Aut}(G) = \mathrm{GL}(3,2)$ on the faithful ideal characters, namely two on the faithful ideal characters of degree 4, and one in each of the dimensions 3, 5, 6 and 7. For $G = \mathbb{F}_2^4$, we get 36 orbits of faithful ideal characters, and it turns out that the polytopes associated with different orbits are not affinely equivalent.

We now briefly describe the six non-equivalent orbit polytopes of $G = \mathbb{F}_2^3$. In dimension 3, every orbit polytope is affinely equivalent to the cube, with symmetry group of order 48. (More generally, the only n-dimensional orbit polytope of $\mathbb{F}_2^n$ is the n-dimensional cube, up to affine equivalence.)

In dimension 4, there are two polytopes. The first one is a Gale dual of the 3-dimensional cube, as in the remarks following Lemma 8.4, and thus has an affine symmetry group of order 48 which is isomorphic to the group of the cube. The other polytope is a Gale dual of the 3-simplex, viewed as orbit polytope of G, where a subgroup of order 2 acts trivially. The affine symmetry group of this orbit polytope in dimension 4 is the wreath product $C_2 \wr S_4 = (C_2)^4 \rtimes S_4$ of order $2^4 \cdot 4! = 384$. (It is not difficult to see that in this particular case, the orbit polytope is just the 4-dimensional cross polytope.)

Similarly, the only orbit polytopes up to affine equivalence in dimensions 5 and 6 are Gale duals of a square and a line segment, and have affine symmetry groups of orders $2^4 \cdot 8 = 128$ and $(4!)^2 \cdot 2 = 1152$, respectively. And of course in dimension 7, there is only the simplex with affine symmetry group of order $8! = 40320$.

1.3 Example. Consider the following 12×5-matrix over $\mathbb{F}_2$:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}^t.$$

The representation

$$D\colon (\mathbb{F}_2)^5 \to \mathrm{GL}(12, \mathbb{Q}), \quad \text{defined by} \quad x \mapsto D(x) = \mathrm{diag}((-1)^{Cx}),$$

yields a subgroup of $\mathrm{GL}(12, \mathbb{Q})$ generated by diagonal matrices corresponding to the rows of the matrix above. We computed (using Corollary 9.6 and the computer algebra system GAP [10]) that the affine symmetry group of the corresponding representation polytope contains no additional elements. (This representation polytope is isomorphic to a permutation polytope of the same group, see Lemma 1.5 below.)

Computational experiments suggest that if $n < d < 2^n - 1 - n$ and d is "sufficiently far" from both n and $2^n - 1 - n$, then most possible choices of C yield a representation polytope $P(D)$ with no additional affine symmetries.

Erik Friese constructed, for all $n \geqslant 6$, an orbit polytope which has as linear symmetry group exactly the elementary abelian group of order 2^n. The construction involves cut polytopes of graphs. This yields the following result:

1.4 Theorem. *The elementary abelian 2-group of order 2^n is the affine symmetry group of one of its orbit polytopes if and only if $n \notin \{2, 3, 4\}$.*

Proof. Omitted. (See Theorem 9.9 in Ref. [FL1].) □

Finally, we consider permutation polytopes. Let $G \leqslant \mathrm{S}_d$ be a permutation group and let $D\colon G \to \mathrm{GL}(d, \mathbb{K})$ be the corresponding representation as a group of permutation matrices. Then $P(D)$ is called a **permutation polytope**, also written as $P(G)$. In their paper "On permutation polytopes" [3], Baumeister et al. point out that left and right multiplications with elements of $D(G)$ induce affine automorphisms of $P(G)$ and that thus the affine automorphism group of $P(G)$ is bigger than G for non-abelian groups. They conjecture this also to be true for abelian groups G of order $|G| > 2$. Now if G contains elements g with $g^2 \neq 1$, then transposition of matrices yields an additional affine symmetry of $P(G)$, thereby verifying the conjecture for these groups.[2]

[2] In fact, Thomas Rehn [15, Theorems A.2 and A.4] has shown that for abelian groups of exponent greater than 2, the affine symmetry group is usually much larger than $|G|$. But notice that the proof of Lemma A.7 and thus of Theorem A.2 for elementary abelian 2-groups is wrong.

However, for elementary abelian 2-groups of order $|G| \geqslant 2^5$, the conjecture is false. This follows from Theorem 1.4 and the following simple observation:

1.5 Lemma. *Let G be an elementary abelian 2-group. Then every orbit polytope of G is affinely G-equivalent to a permutation polytope.*

Proof. An orbit polytope of an abelian group is affinely G-equivalent to a representation polytope (Corollary 9.3 in Chapter II). Let D be a representation of G. The abelian group $D(G)$ is simultaneously diagonalizable. Let $\{b_1, \ldots, b_d\}$ be a basis of eigenvectors. Then $D(G)$ permutes the set $\{\pm b_1, \ldots, \pm b_d\}$, with d orbits of length 2. The corresponding permutation representation D_1 of G is similar to

$$\begin{pmatrix} I & 0 \\ 0 & D \end{pmatrix},$$

where I is the $d \times d$ identity matrix. It follows that the representation polytopes of D_1 and D are affinely equivalent as G-sets. □

2. Classification of affine symmetry groups of orbit polytopes

In this section, we classify the groups which are isomorphic to the affine symmetry group of an orbit polytope. Suppose the finite group G acts on $\mathbb{R}^d$ by affine transformations. Recall that an **orbit polytope** of G is the convex hull of an G-orbit of a point:

$$\mathrm{P}(G, v) := \mathrm{conv}\{gv \mid g \in G\}.$$

(As G fixes the barycenter of $\mathrm{P}(G, v)$, we can choose coordinates such that G acts linearly.) Let us say that $\mathrm{P}(G, v)$ is an **euclidean** orbit polytope, if G acts by (euclidean) isometries on $\mathbb{R}^d$. The euclidean symmetry group (or isometry group) of a d-dimensional polytope $P \subseteq \mathbb{R}^d$ is the group of isometries of $\mathbb{R}^d$ mapping P onto itself. (In the literature, the euclidean symmetry group is often called "the" symmetry group of P. For the sake of clarity, we do not follow this convention here.) The affine symmetry group of a d-dimensional polytope $P \subseteq \mathbb{R}^d$ is the group of all affine transformations of $\mathbb{R}^d$ mapping P onto itself. In both cases, a symmetry maps P onto itself if and only if it permutes the vertices of P.

Babai [1] classified the finite groups which are isomorphic to the isometry group of an euclidean orbit polytope, and asked which abstract finite groups occur as the affine symmetry group of an orbit polytope. In this section, we answer this question. We begin by recalling Babai's classification. Following Babai, we call a finite group G **generalized dicyclic**, if it has an abelian subgroup A of index 2 and an element $g \in G \setminus A$ of order 4 such that $g^{-1}ag = a^{-1}$ for all $a \in A$.

2.1 Theorem (Babai [1]). *Let G be a finite group. Then either G is isomorphic to the isometry group of an euclidean orbit polytope, or one of the following holds:*

(i) *G is abelian, but not elementary 2-abelian.*

(ii) *G is generalized dicyclic.*

Now if a finite group G (say) is the affine symmetry group of a polytope $P \subseteq \mathbb{R}^d$, then there is an affine automorphism σ of $\mathbb{R}^d$ such that $\sigma G \sigma^{-1}$ preserves lengths. Since $\sigma G \sigma^{-1}$ is the affine symmetry group of the polytope $\sigma(P)$, it is also the euclidean symmetry group of the polytope $\sigma(P)$. Thus as an immediate corollary of Babai's result, we get the following:

2.2 Corollary. *The following groups are not isomorphic to the affine symmetry group of an orbit polytope: abelian groups of exponent greater than 2, and generalized dicyclic groups.*

On the other hand, it may happen that G is isomorphic to the isometry group of an (euclidian) orbit polytope, but not to the affine symmetry group of an orbit polytope. For example, the Klein four group, V_4, is isomorphic to the isometry group of a rectangle with two different side lengths.

The affine symmetry group of a rectangle is isomorphic to the group of the square and has order 8, and indeed, the Klein four group can not be realized as the affine symmetry group of an orbit polytope, by Lemma 1.1.

In order to apply the results of Chapter II to our classification problem, we need the following observation.

2.3 Lemma. *A finite group G is isomorphic to the affine symmetry group of an orbit polytope if and only if G is generically closed with respect to some cyclic module over $\mathbb{R}G$.*

Proof. If G is generically closed with respect to some cyclic module V, then G is isomorphic to the linear symmetry group of the orbit polytope $\mathrm{P}(G, v)$ for every generic $v \in V$. If $\mathrm{Aff}(Gv) = \mathrm{Span}(Gv) = V$ for a generic v, then Lemma 2.2 in Chapter II yields that $\mathrm{GL}(Gv) = \mathrm{AGL}(Gv)$, and in the other case the affine and the linear symmetry group of $\mathrm{P}(G, v)$ are isomorphic (by restriction from the linear to the affine hull of Gv).

Conversely, suppose that G is the affine symmetry group of an orbit polytope $\mathrm{P}(H, v)$ of a group H. Then clearly $\mathrm{P}(H, v) = \mathrm{P}(G, v)$. Without loss of generality, we may assume that H and G are linear, by choosing the barycenter of $\mathrm{P}(G, v)$ as origin of our coordinate system. Set $V = \mathbb{R}Gv$, the $\mathbb{R}$-linear span of Gv, so that V is a cyclic $\mathbb{R}G$-module.

We have $Hv = Gv$ and $G = \mathrm{GL}(Hv)$. Corollary 5.4 yields that $G = \mathrm{GL}(Gw)$ for any $w \in V$ which is generic for G. Since G is by definition a subgroup of $\mathrm{GL}(V)$, this is equivalent to G being generically closed with respect to V. □

We need to recall some representation theory. We have already seen that a character

$$\gamma = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi$$

is afforded by a cyclic $\mathbb{C}G$-module, or a left ideal of $\mathbb{C}G$, if and only if $n_\chi \leqslant \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$. We now characterize which characters are afforded by a left ideal of $\mathbb{K}G$, where $\mathbb{K} \subseteq \mathbb{C}$.

Let $\chi \in \mathrm{Irr}\, G$. Recall that the *Schur index* $m_\mathbb{K}(\chi)$ of χ over $\mathbb{K}$ is by definition the smallest positive integer m such that $m\chi$ is afforded by a representation with entries in $\mathbb{K}(\chi)$, where $\mathbb{K}(\chi)$ is the field generated by the values of χ.

For $\mathbb{K} = \mathbb{R}$, only three different cases are possible, which can be recognized by the *Frobenius-Schur-indicator*

$$\nu_2(\chi) := \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

Namely, when $\nu_2(\chi) = 1$, then $\chi = \overline{\chi}$ and $m_\mathbb{R}(\chi) = 1$, so χ is afforded by a representation over $\mathbb{R}$. When $\nu_2(\chi) = 0$, then $\chi \neq \overline{\chi}$ and $m_\mathbb{R}(\chi) = 1$. Finally, when $\nu_2(\chi) = -1$, then $\chi = \overline{\chi}$, but χ is not afforded by a representation over $\mathbb{R}$, and $m_\mathbb{R}(\chi) = 2$ [12, Chapter 4].

2.4 Lemma. *Let $\mathbb{K} \subseteq \mathbb{C}$, and let*

$$\gamma = \sum_{\chi \in \mathrm{Irr}(G)} n_\chi \chi$$

be a character. Then γ is the character of a left ideal of $\mathbb{K}G$ if and only if the following conditions hold:

(i) *γ has values in $\mathbb{K}$,*
(ii) *$m_\mathbb{K}(\chi)$ divides n_χ for all $\chi \in \mathrm{Irr}\, G$,*
(iii) *$n_\chi \leqslant \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$.*

Proof. It follows from the general theory of the Schur index that γ is the character of a representation with entries in $\mathbb{K}$ if and only if the first two conditions hold [12, Corollary 10.2].

Let S be a simple $\mathbb{K}G$-module. The character of S has the form

$$m_\mathbb{K}(\chi) \sum_\alpha \chi^\alpha,$$

for some $\chi \in \mathrm{Irr}(G)$, where α runs over the Galois group of $\mathbb{K}(\chi)/\mathbb{K}$, so that χ^α runs over the Galois conjugacy class of χ over $\mathbb{K}$. Thus S occurs with multiplicity $\chi(1)/m_\mathbb{K}(\chi)$ as summand of the regular module $\mathbb{K}G$, and with multiplicity $n_\chi/m_\mathbb{K}(\chi)$ in a $\mathbb{K}G$-module affording γ. Thus a $\mathbb{K}G$-module affording γ is a direct summand of $\mathbb{K}G$ if and only if $n_\chi \leqslant \chi(1)$ for all χ. □

For a finite group G and a field $\mathbb{K} \subseteq \mathbb{C}$, we defined in the last chapter

$$\mathrm{NKer}_{\mathbb{K}}(G) := \bigcap \{\mathrm{Ker}(\chi) \colon \chi(1) > m_{\mathbb{K}}(\chi)\}.$$

If $\chi(1) = m_{\mathbb{K}}(\chi)$ for all $\chi \in \mathrm{Irr}\, G$, then we set $\mathrm{NKer}_{\mathbb{K}}(G) = G$.

Consider the character

$$\gamma := \sum_{\substack{\chi \in \mathrm{Irr}\, G \\ \chi(1) > m_{\mathbb{K}}(\chi)}} m_{\mathbb{K}}(\chi)\chi.$$

Then $\mathrm{Ker}\, \gamma = \mathrm{NKer}_{\mathbb{K}}(G)$, and γ is afforded by a left ideal of $\mathbb{K}G$, and the ideal part of γ is zero. So as a corollary of Corollary 10.7 in Chapter II and Lemma 2.3 above, we get the following.

2.5 Corollary. *Let $\mathbb{K} \subseteq \mathbb{R}$. If $\mathrm{NKer}_{\mathbb{K}}(G) = \{1\}$, then G is isomorphic to the affine symmetry group of an orbit polytope, such that its vertices have coordinates in $\mathbb{K}$.*

In particular, when $\mathrm{NKer}_{\mathbb{R}}(G) = \{1\}$, then G is isomorphic to the affine symmetry group of an orbit polytope. It remains to treat the groups G for which $\mathrm{NKer}_{\mathbb{R}}(G) \neq \{1\}$. These were classified in the last chapter (Theorem B).

2.6 Lemma. *Suppose that*

$$G \cong C_4 \times Q_8 \times C_2^r \quad \text{or} \quad G \cong Q_8 \times Q_8 \times C_2^r$$

for some integer $r \geqslant 0$. Then G is isomorphic to the affine symmetry group of an orbit polytope.

Proof. By Lemma 2.3, we need to find in each case a character γ of a left $\mathbb{R}G$-ideal such that $\mathrm{Sym}(G, \gamma) \cong G$.

Let $\tau \in \mathrm{Irr}\, Q_8$ be the faithful irreducible character of degree 2, and set $\varphi = \lambda + \overline{\lambda}$, where λ is a faithful linear character of C_4. Finally, let α be some faithful ideal character of C_2^r.

First, suppose that $G \cong C_4 \times Q_8 \times C_2^r$. Then we set

$$\gamma := \varphi \times \tau \times \alpha + 1 \times 2\tau \times 1 + \varphi \times 1 \times 1.$$

The irreducible constituents of the first summand have the form $\chi = \lambda \times \tau \times \sigma$, where $\lambda \in \mathrm{Lin}(C_4)$ is faithful and $\sigma \in \mathrm{Lin}(C_2^r)$. In particular, $\chi \neq \overline{\chi}$, and so $m_{\mathbb{R}}(\chi) = 1 < \chi(1) = 2$. It follows that the ideal part of γ (in the sense of Definition 10.4 in Chapter II) is given by

$$\gamma_I = 1 \times 2\tau \times 1 + \varphi \times 1 \times 1.$$

Now set $C_4 = \langle u \rangle$ and $Q_8 = \langle x, y \rangle$ as in Chapter III, Lemma 5.5. We see that $\mathrm{Ker}(\gamma - \gamma_I) = \langle z \rangle = \mathrm{NKer}_{\mathbb{R}}(G)$, where $z = u^2x^2$. We have $\gamma_I(z) = -6 = -\gamma_I(1)$ and thus $\gamma_I(gz) = \gamma_I(g)$ for all $g \in G$.

Suppose $\pi \in \mathrm{Sym}(G, \gamma)$ with $\pi(1) = 1$. By Theorem 10.6 from Chapter II, we have $\pi(g) \in \{g, gz\}$ for all $g \in G$ and $\gamma_I(\pi(g)^{-1}\pi(h)) = \gamma_I(g^{-1}h)$ for all $g, h \in G$. It is now easy to see that this implies $\pi = \mathrm{id}$. Since $\mathrm{Sym}(G, \gamma)$ contains the left regular action of G on itself, this implies $\mathrm{Sym}(G, \gamma) \cong G$.

In the case $G \cong Q_8 \times Q_8 \times C_2^r$, we set

$$\gamma := \tau \times \tau \times \gamma + 2\tau \times 1 \times 1 + 1 \times 2\tau \times 1.$$

Similar arguments as above show that $\mathrm{Sym}(G, \gamma) \cong G$. □

Now we can classify affine symmetry groups of orbit polytopes:

2.7 Theorem. *Let G be a finite group. Then G is isomorphic to the affine symmetry group of an orbit polytope, if and only if none of the following holds:*

(i) *G is abelian of exponent greater than 2.*
(ii) *G is generalized dicyclic.*
(iii) *G is elementary abelian of order $4, 8$ or 16.*

Proof. It follows from Corollary 2.2 that groups which are abelian, but not elementary 2-abelian, are not isomorphic to the affine symmetry group of an orbit polytope, and the same holds for generalized dicyclic groups. By Section 1, an elementary abelian 2-group G is isomorphic to the affine symmetry group of an orbit polytope if and only if its order, $|G|$, is not 4, 8 or 16. The groups $Q_8 \times C_4 \times C_2^r$ and $Q_8 \times Q_8 \times C_2^r$ are affine symmetry groups of orbit polytopes for any $r \geqslant 0$ by Lemma 2.6. All remaining groups have $\mathrm{NKer}_{\mathbb{R}}(G) = \{1\}$ and thus are affine symmetry groups of orbit polytopes by Corollary 2.5. □

We end this section with a related question. When G is a nonabelian group, then the intersection of the kernels of all *nonlinear* irreducible characters is the trivial subgroup (Lemma 3.2 in Chapter III). Thus when V is a $\mathbb{C}G$-module affording the character $\gamma = \sum_\chi \chi$, where the sum runs over the nonlinear irreducible characters of G, then G acts faithfully on V and is the setwise stabilizer of any generic G-orbit on V. In other words, $\mathrm{Sym}(G, V) \cong G$.

2.8 Question. Which finite abelian groups G are generically closed with respect to some representation $G \to \mathrm{GL}(d, \mathbb{C})$? Equivalently, which finite abelian groups are isomorphic to the linear symmetry group of some point set in $\mathbb{C}^d$ for some d, and act transitively on this set?

We conjecture that there are only finitely many abelian groups (up to isomorphism) that are not generically closed with respect to at least one representation. By Theorem D of Chapter II, every cyclic group is generically closed with respect to every faithful linear representation. The results of Section 1 together with Corollary 4.20, answer the above question for elementary abelian 2-groups. In particular, the elementary abelian 2-groups of orders 4, 8 and 16 are not generically closed with respect to some representation. One can check that the elementary abelian 3-group $C_3 \times C_3$ of order 9 is also not generically closed with respect to any representation. We conjecture that these four groups are the only exceptions. Thus any other abelian group should be the setwise stabilizer of an orbit in some $\mathbb{C}^d$.

3. Classification of affine symmetry groups of rational orbit polytopes

In this section, we classify affine symmetry groups of polytopes with rational coordinates. Since every polytope with rational coordinates can be scaled to a polytope with integer coordinates, this classifies also affine symmetry groups of lattice orbit polytopes.

By Corollary 2.5, it follows that when $\mathrm{NKer}_{\mathbb{Q}}(G) = \{1\}$, then G is isomorphic to the affine symmetry group of an orbit polytope with integer coordinates. The main result of this section depends on the classification of the finite groups G with $\mathrm{NKer}_{\mathbb{Q}}(G) \neq \{1\}$ (Theorem D in Chapter III).

The next lemma can often be used to show that a certain group is *not* the affine symmetry group of a rational orbit polytope. As a consequence of the classification of the finite groups G with $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$, it turns out that most of these groups satisfy the assumptions of the next lemma.

3.1 Lemma. *Suppose G has a normal subgroup N of prime index $|G : N| = p$ and an element z of order p, such that $z \in \langle g \rangle$ for every $g \in G \setminus N$. Fix an epimorphism $\kappa\colon G \to \langle z \rangle$ with kernel N and define $\alpha\colon G \to G$ by $\alpha(g) = g\kappa(g)$. Then $\alpha \in \mathrm{Sym}(G, I)$ for every ideal I of $\mathbb{Q}G$. If additionally $z \in \mathrm{NKer}_{\mathbb{Q}}(G)$, then G can not be isomorphic to the affine symmetry group of an orbit polytope with rational coordinates.*

Proof. First notice that $z \in \mathbf{Z}(G)$, since $G \setminus N$ centralizes z by assumption. This yields that α is a group automorphism of G, with inverse $g \mapsto g\kappa(g)^{-1}$.

By Lemma 4.6 in Chapter II, it suffices to assume that I is a simple ideal. Then the character of I has the form $\gamma = \chi(1) \sum_\sigma \chi^\sigma$ for some $\chi \in \mathrm{Irr}(G)$, where σ runs over the Galois group of $\mathbb{Q}(\chi)/\mathbb{Q}$. If $z \in \mathrm{Ker}(\chi)$, then $z \in \mathrm{Ker}(\gamma)$ and the result is clear (by the remarks before Chapter II, Lemma 4.6, or by Proposition 9.5 there.

So assume that $z \notin \mathrm{Ker}(\chi)$. Since $z \in \mathbf{Z}(G)$, we have that $\chi(z) = \chi(1)\zeta$ for some primitive p-th root of unity, ζ. Let $g \in G \setminus N$ be arbitrary. The restriction $\gamma_{|\langle g\rangle}$ decomposes into a sum of Galois orbits of linear characters. Since $\chi(z) = \chi(1)\zeta$, we have $\lambda(z) = \zeta \neq 1$ for each linear constituent λ of γ. Since $|G/N| = |\langle z\rangle| = p$ and $z \in \langle g\rangle$, we see that $\lambda(g)$ is a primitive k-th root of unity where p^2 divides k.

The Galois orbit of $\lambda(g)$ consists of all primitive k-th roots of unity. Since p^2 divides k, the Galois orbit of $\lambda(g)$ is a union of cosets of $\langle\zeta\rangle$, and so the sum over the Galois orbit is zero. It follows that $\gamma(g) = 0$. As $g \in G \setminus N$ was arbitrary, it follows that $\gamma_{G\setminus N} \equiv 0$. Since α is a group automorphism leaving each element of N fixed, we have that

$$\gamma(\alpha(g)^{-1}\alpha(h)) = \gamma(\alpha(g^{-1}h)) = \gamma(g^{-1}h)$$

for all $g, h \in G$. By Chapter II, Proposition 9.5, this shows that $\alpha \in \mathrm{Sym}(G, \gamma) = \mathrm{Sym}(G, I)$.

If $z \in \mathrm{NKer}_{\mathbb{Q}}(G)$, then $z \in \mathrm{Ker}(\gamma - \gamma_I)$ for every character γ of a cyclic $\mathbb{Q}G$-module, where γ_I denotes the ideal part of γ, as before. It follows from Theorem 10.6 of Chapter II that $\alpha \in \mathrm{Sym}(G, \gamma)$ for such γ. Since $\alpha(1_G) = 1_G$, but $\alpha \neq \mathrm{id}_G$, we have $|\mathrm{Sym}(G, \gamma)| > |G|$. □

3.2 Theorem. *The finite group G is not the affine symmetry of an orbit polytope with vertices with integer (rational) coordinates if and only if one of the following holds:*

(i) *G is abelian and either G has exponent greater than 2, or G is elementary abelian of order 4, 8 or 16.*

(ii) *$G = S \times A$, where S is a generalized dicyclic group of exponent 4, the group A is abelian of odd order, and the multiplicative order of 2 modulo $|A|$ is odd.*

(iii) *G is generalized dicyclic.*

(iv) *$G = (PQ) \times B$, where the subgroups $P \in \mathrm{Syl}_p(G)$, $Q \in \mathrm{Syl}_q(G)$ and B are abelian, $P = \langle g, \mathbf{C}_P(Q)\rangle$ and there is some integer k such that, $x^g = x^k$ for all $x \in Q$. If $p^c = |P/\mathbf{C}_P(Q)|$, then $p^d = \mathbf{o}(g^{p^c})$ is the exponent of $\mathbf{C}_P(Q)$, and $(q-1)_p$, the p-part of $q-1$, divides p^d. Finally, the p-part of the multiplicative order of q modulo $|B|$ divides the multiplicative order of q modulo p^d.*

(v) *$G = Q_8 \times (C_2)^r \times H$, where H is as in (iv) and has odd order, and the multiplicative order of 2 modulo $|H|$ is odd.*

Proof. When G is not the affine symmetry group of an orbit polytope with lattice points as vertices, then $\mathrm{NKer}_{\mathbb{Q}}(G) \neq 1$. The list of such groups consists of the groups in the above list, and the following groups:

(vi) $G = Q_8 \times C_4 \times (C_2)^r \times A$,

(vii) $G = Q_8 \times Q_8 \times (C_2)^r \times A$,

where in each case A is abelian of odd order, and the multiplicative order of 2 modulo $|A|$ is odd (Chapter III, Theorem D). However, these groups can be realized as symmetry groups of integer orbit polytopes. This can be shown as in Lemma 2.6 above. (Replace the character α in these proofs by a faithful ideal character of $(C_2)^r \times A$ with values in $\mathbb{Q}$.)

If G is abelian or generalized dicyclic, but not an elementary abelian 2-group, then G is not even the affine symmetry group of an orbit polytope. For elementary abelian 2-groups of order not 4, 8, or 16, we constructed in fact orbit polytopes with integer coordinates (Section 1). For all other groups on the above list, Lemma 3.1 applies. For example, when $G = (PQ) \times B$ as in (iv), then we choose for N the unique subgroup containing $\mathbf{C}_P(Q)QB$ of index p, and $z = g^{p^{c+d-1}}$. Notice that p^c divides $(q-1)_p$ and $(q-1)_p$ divides p^d, so $z \in \mathbf{Z}(G)$. For $u \in P \cap N$, we have $gu = ug$ and $\mathbf{o}(u) < p^{c+d}$ by assumption, so $(gu)^{p^{c+d-1}} = z$. For $x \in Q$, we have $(gx)^{p^c} = g^{p^c}$. Since g centralizes B, we have $z \in \langle gn \rangle$ for all $n \in N$, and also $z \in \langle h \rangle$ for all $h \in G \setminus N$. Moreover, $z \in \mathrm{NKer}_{\mathbb{Q}}(G)$ (by Lemma 6.11 in Chapter III) and thus Lemma 3.1 applies. The same argument applies to the groups in (v) (with N containing $Q_8 \times (C_2)^r$). If G is as in (ii), then we choose for N the direct product of A and the abelian subgroup of S from the definition of "generalized dicyclic". (In fact, Lemma 3.1 applies also to generalized dicyclic groups.) □

Thus there are quite a number of groups which can be realized as symmetry groups of orbit polytopes, but not as symmetry group of an orbit polytope with rational or integer coordinates. As an example, consider the group $G = Q_8 \times C_7$. Then it is known that $\mathbb{Q}G$ is a direct product of division rings [16] (see Theorem 4.5 in Chapter III). This is essentially due to the fact that $\mathbb{Q}(\varepsilon)$, where ε is a primitive 7-th root of unity, is not a splitting field of the quaternions over $\mathbb{Q}$. Equivalently, -1 is not a sum of two squares in $\mathbb{Q}(\varepsilon)$. More generally, for a field $\mathbb{K}$, we have that $\mathbb{K}G$ is a direct product of division rings if and only if -1 is not a sum of two squares in $\mathbb{K}(\varepsilon)$ (Theorem 4.2 in Chapter III). When $\mathbb{K}G$ is not a direct product of division rings, then $\mathbb{K}G$ contains a simple left ideal which is not a twosided ideal and on which G acts faithfully. Thus when $\mathbb{K} \subseteq \mathbb{R}$, then G is isomorphic to the affine symmetry group of an orbit polytope with vertex coordinates in $\mathbb{K}$ if and only if -1 is a sum of two squares in $\mathbb{K}(\varepsilon)$. There are many different such fields, for example, $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ or $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, and also the following fields: Choose $\alpha, \beta \in \mathbb{R}$ with $\alpha^2 + \beta^2 = 7$ (note that α can be transcendent). Then $\mathbb{Q}(\alpha, \beta, \varepsilon)$ is a splitting field for the quaternions, because -7 is a square in $\mathbb{Q}(\varepsilon)$. Thus G is isomorphic to the symmetry group of an orbit polytope with coordinates in $\mathbb{K} = \mathbb{Q}(\alpha, \beta)$. When α is transcendent, then one can show that $\mathbb{Q}(\alpha, \beta)$ contains no algebraic elements.

4. Open questions and conjectures

We make some remarks on open questions and conjectures which are related to the results of this chapter and of Chapter II.

4.1 Question. Let $\mathbb{K}$ be a field. For which finite groups G is there a cyclic $\mathbb{K}G$-module V such that $G = \mathrm{GL}(Gv)$ for some $v \in V$?

We have answered this question for the fields $\mathbb{K} = \mathbb{R}$ and $\mathbb{K} = \mathbb{Q}$. For $\mathbb{K} = \mathbb{C}$, only the case of abelian groups (noncyclic of exponent > 2) is open. For other fields of characteristic zero, one would have to complete a classification of groups G with $\mathrm{NKer}_{\mathbb{K}}(G) \neq 1$ as in Chapter III, and then consider these groups separately. If $\mathbb{K} \subseteq \mathbb{R}$, then abelian groups of exponent > 2 do not occur, but for other fields some abelian groups may occur. For example, when $\mathbb{K}$ contains a primitive n-th root of unity, then we conjecture that all but finitely many abelian groups of exponent n can be realized as $\mathbb{K}$-linear symmetry group of an orbit.

For fields of positive characteristic, or even finite fields, Question 4.1 is probably much more difficult.

The following questions are due to Babai [1]:

4.2 Questions. Which finite groups appear as

(a) the sense-preserving symmetry group of an orbit polytopes?

(b) the projective symmetry group of a polytope, such that the projective symmetry group acts transitively on the vertices of that polytope?

In fact, we can ask such questions in various other contexts. For example, let G be a finite group and $\mathbb{K}$ a field. Then we can ask whether G can be embedded into $\mathrm{SL}(d, \mathbb{K})$ for some d, such that G is the setwise stabilizer in $\mathrm{SL}(d, \mathbb{K})$ of some orbit. (For $\mathbb{K} = \mathbb{R}$, this is essentially Babai's question in 4.2(a) above.) Here, "SL" can be replaced by other algebraic groups like symplectic matrices, unitary matrices, and so on. Recently, Erik Friese [9] has shown that whenever G is a finite group of unitary matrices (over $\mathbb{C}$), such that some G-orbit spans the corresponding finite-dimensional Hilbert space, then G is the setwise stabilizer of some orbit in the unitary group. (As one would expect, this is then true for "almost all" orbits in the sense that the exceptional orbits come from points in a proper algebraic subset.)

We have said nothing in Chapters II and IV about the combinatorial symmetry group of orbit polytopes. A combinatorial symmetry of a polytope P is a permutation of its vertices which maps faces of P to faces of P. Of course, we can ask an analogous question to those in 4.2 above for the combinatorial automorphism group. Probably, an answer to this question would require some essentially new ideas.

Already the example of the dihedral group D_4 (or D_n) shows that the combinatorial symmetry group of an orbit polytope is usually bigger than the affine symmetry group. The generic orbit polytope of D_4 is combinatorially an octagon. There are, however, special points such that the orbit polytope is a regular octagon, and for these points, the combinatorial and the affine symmetry groups agree. We conjecture that this is a general phenomenon:

4.3 Conjecture. Let $G \leqslant \mathrm{GL}(d, \mathbb{R})$ be finite and $P(G, v)$ a full-dimensional orbit polytope. Then there is a point v_0 such that $P(G, v)$ and $P(G, v_0)$ are combinatorially equivalent and such that all combinatorial symmetries of $P(G, v_0)$ are affine symmetries of $P(G, v_0)$.

An interesting example in case is the rotation group T of the tetrahedron in dimension 3. This group is isomorphic to the alternating group A_4 and has order 12. The generic orbit polytope is an icosahedron, but of course a skew icosahedron having only T as affine symmetry group. However, for special points the orbit polytope is a regular icosahedron with symmetry group of order 120. This is also the combinatorial symmetry group of the icosahedron. We get such a special point by choosing the midpoint of a triangle from the tessellation of the 2-sphere associated to the reflection group of the regular tetrahedron. (As the referee[3] has pointed out, this construction of the icosahedron is analogous to the construction of the *snub cube* from the rotation group of the cube described by Coxeter [6, pp. 17–18]. This construction is a variant of Wythoff's construction.) If the tetrahedron we begin with has rational coordinates, then the points such that the orbit polytope is a regular icosahedron, all have irrational coordinates, because the 3-dimensional representation of the icosahedron group is not realizable over the rational numbers.

Bokowski, Ewald and Kleinschmidt [4] constructed the first example of a polytope such that its combinatorial symmetry group is bigger than the affine symmetry group of all possible realizations. Other examples have been constructed since then, but none of them, to the best of our knowledge, is an orbit polytope. On the positive side, McMullen [13] has shown that a combinatorially regular polytope is combinatorially equivalent to a regular polytope, and for such a polytope, all combinatorial symmetries come from orthogonal symmetries.

If $P(G)$ is a representation polytope belonging to the group $G \leqslant \mathrm{GL}(d, \mathbb{R})$, then $P(G)$ is affinely equivalent to every other orbit polytope $P(G, A)$ which generates the same subspace of the matrix space as G. Thus the following conjecture would follow from the last one:

4.4 Conjecture. The combinatorial and the affine symmetry group of representation polytopes agree.

[3] of our first paper [FL1] on affine symmetries of orbit polytopes

We have verified this for all rational representations of groups of order $\leqslant 31$ using GAP [10] and, in particular, M. Dutour Sikirić's collection of GAP-functions `polyhedral` [7]. (Both `polymake` [11] and `polyhedral` can compute only with polytopes with rational vertices or vertices in quadratic extension fields.) Another example is the Birkhoff polytope, the representation polytope of the natural representation of the symmetric group S_n. Using the known facet structure of the Birkhoff polytope, it is not too difficult to show that its combinatorial symmetry group only contains the symmetries described in Proposition 6.4, which are of course affine (see Theorem B in Chapter VI).

Finally, we mention the following question, which was already posed by Onn [14] (in a slightly different form):

4.5 Question. For which groups $G \leqslant \mathrm{GL}(d, \mathbb{R})$ is it true that all generic orbit polytopes are combinatorially equivalent?

For example, this is true when G is a finite reflection group [5, Theorem 14.1]. (See also [8, Proposition 3].) As mentioned before, Onn [14] showed by an example that in general, different generic orbit polytopes are not combinatorially equivalent. Onn's example is multiplicity free. On the other hand, we have seen in this paper that when each irreducible representation occurs in a representation with the same multiplicity as in the regular representation, or not at all, then all generic orbit polytopes are even affinely equivalent. (This follows from Proposition 6.3, since the orbit polytope of such a representation is affinely G-equivalent to a representation polytope.)

This is somewhat contrary to the intuition suggested in a remark by Onn[14]: In view of his example, Onn notes that a representation being multiplicity free is not enough to have a trivial polytope stratification (that is, all generic orbit polytopes are combinatorially equivalent). Onn proposed to study next the case of irreducible representations [14, p. 48]. But even when G acts irreducibly, it is possible to have combinatorially nonequivalent, generic orbit polytopes: for example, $G = \mathrm{PSL}(2, 5)$ is a permutation group on the projective line over the field with 5 elements, and thus is isomorphic to a subgroup of S_6. As such, it acts irreducibly on the orthogonal complement of the fixed space in $\mathbb{R}^6$. (As an abstract group, $G \cong A_5$.) By exactly analogous arguments and computations as in Onn's original example, one can confirm that the points $u = (1, 10, 11, 32, 71, 99)$ and $v = (1, 11, -40, 79, 37, 102)$ are "combinatorially generic" in the sense that all starting points in a small neighborhood yield combinatorially equivalent orbit polytopes, but $\mathrm{P}(G, u)$ and $\mathrm{P}(G, v)$ are not combinatorial equivalent. Even worse, the orbit polytopes $\mathrm{P}(G, u)$ and $\mathrm{P}(G, v)$ have different combinatorial symmetry groups: One has combinatorial symmetry group G, and the other combinatorial symmetry group isomorphic to S_5 of order $2|G|$.

Acknowledgments

We would like to thank Achill Schürmann and Mathieu Dutour Sikirić for many stimulating discussions. In particular, we acknowledge the efforts of Achill Schürmann who carefully read preliminary versions of the paper [FL1] and gave many useful hints to improve the exposition. We are grateful to Mathieu Dutour Sikirić also for useful pointers to the literature and for his help with using his GAP-functions in `polyhedral` [7]. Furthermore, we thank Christian Rosenke for his interest. The idea of using complements of trees in Section 1 came up in conversations of the first author with him. And we are grateful to Jan-Christoph Schlage-Puchta for communicating his proof of Corollary 5.4 (equivalently, Lemma 5.3) from Chapter IV in the case $\mathbb{K} = \mathbb{R}$ to us.

References for Chapter IV

1. László Babai. Symmetry groups of vertex-transitive polytopes. *Geometriae Dedicata* **6**, no. 3 (1977), pp. 331–337. DOI: 10.1007/BF02429904. MR0486080(58#5868), Zbl. 0388.05025 (cited on pp. 101, 102, 109).
2. Barbara Baumeister and Matthias Grüninger. On permutation polytopes: notions of equivalence. *J. Algebraic Combin.* **41**, no. 4 (2015), pp. 1103–1114. DOI: 10.1007/s10801-014-0568-8, arXiv: 1301.2080 [math.CO]. MR3342715, Zbl. 1322.52010 (cited on p. 99).
3. Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. On permutation polytopes. *Adv. Math.* **222**, no. 2 (2009), pp. 431–452. DOI: 10.1016/j.aim.2009.05.003, arXiv: 0709.1615 [math.CO]. MR2538016(2010j:52042), Zbl. 1185.52006 (cited on pp. 97, 100).
4. Jürgen Bokowski, Günter Ewald, and Peter Kleinschmidt. On combinatorial and affine automorphisms of polytopes. *Israel J. Math.* **47**, no. 2-3 (1984), pp. 123–130. DOI: 10.1007/BF02760511. MR738163(85i:52001), Zbl. 0546.52004 (cited on p. 110).
5. Alexandre V. Borovik and Anna Borovik. *Mirrors and Reflections. The Geometry of Finite Reflection Groups*. Universitext. Springer, New York, 2010. DOI: 10.1007/978-0-387-79066-4. MR2561378(2011b:20114), Zbl. 1193.20001 (cited on p. 111).
6. H. S. M. Coxeter. *Regular Complex Polytopes*. Cambridge University Press, 2nd ed. 1991. MR1119304(92h:51035), Zbl. 0732.51002 (cited on p. 110).
7. Mathieu Dutour Sikirić. *Polyhedral. GAP-package*. Version dated 2013-09-08. 2013. URL: http://mathieudutour.altervista.org/Polyhedral/ (visited on 2014-09-08) (cited on pp. 111, 112).
8. Mathieu Dutour Sikirić and Graham Ellis. Wythoff polytopes and low-dimensional homology of Mathieu groups. *J. Algebra* **322**, no. 11 (2009), pp. 4143–4150. DOI:

10.1016/j.jalgebra.2009.09.031. MR2556144(2010j:20082), Zbl. 1186.20033 (cited on p. 111).

9. Erik Friese. Unitary groups as stabilizers of orbits. *Arch. Math. (Basel)* **109**, no. 2 (2017), pp. 101–103. DOI: 10.1007/s00013-017-1065-9. MR3673628, Zbl. 1376.20002 (cited on p. 109).
10. *GAP – Groups, Algorithms, and Programming, Version 4.7.5*. The GAP Group. May 2014. URL: http://www.gap-system.org (cited on pp. 100, 111).
11. Ewgenij Gawrilow and Michael Joswig. Polymake: a framework for analyzing convex polytopes. In: *Polytopes—combinatorics and Computation*. (Oberwolfach, 1997). Ed. by Gil Kalai and Günter M. Ziegler. DMV Sem. 29. Birkhäuser, Basel, 2000, pp. 43–73. URL: http://www.polymake.org. MR1785292(2001f:52033), Zbl. 0960.68182 (cited on p. 111).
12. I. Martin Isaacs. *Character Theory of Finite Groups*. Dover, New York, 1994. (Corrected reprint of the 1976 edition by Academic Press, New York). MR1280461, Zbl. 0849.20004 (cited on p. 103).
13. Peter McMullen. Combinatorially regular polytopes. *Mathematika* **14** (1967), pp. 142–150. DOI: 10.1112/S0025579300003739. MR0221384(36#4436), Zbl. 0155.50002 (cited on p. 110).
14. Shmuel Onn. Geometry, complexity, and combinatorics of permutation polytopes. *J. Combin. Theory Ser. A* **64**, no. 1 (1993), pp. 31–49. DOI: 10.1016/0097-3165(93)90086-N. MR1239510(94j:52020), Zbl. 0789.05095 (cited on p. 111).
15. Thomas Rehn. *Polyhedral Description Conversion up to Symmetries*. Diploma thesis. Otto von Guericke Universität Magdeburg, 2010. URL: http://www.math.uni-rostock.de/~rehn/docs/diploma-thesis-ma-rehn.pdf (visited on 2017-03-22) (cited on p. 100).
16. Sudarshan K. Sehgal. Nilpotent elements in group rings. *Manuscripta Math.* **15**, no. 1 (1975), pp. 65–80. DOI: 10.1007/bf01168879. MR0364417(51#671), Zbl. 0302.16010 (cited on p. 108).

FL1. Erik Friese and Frieder Ladisch. Affine symmetries of orbit polytopes. *Adv. Math.* **288** (2016), pp. 386–425. DOI: 10.1016/j.aim.2015.10.021, arXiv: 1411.0899v3 [math.MG]. MR3436389, Zbl. 1330.52017 (cited on pp. 97, 100, 110, 112).

FL2. Erik Friese and Frieder Ladisch. Classification of affine symmetry groups of orbit polytopes. *J. Algebraic Combin.* (Nov. 2017). DOI: 10.1007/s10801-017-0804-0, arXiv: 1608.06539v4 [math.GR] (cited on p. 97).

Chapter V.

Equivalence of Lattice Orbit Polytopes[1]

Frieder Ladisch and Achill Schürmann

Dedicated to Jörg M. Wills on the occasion of his 80th birthday

Abstract. Let G be a finite permutation group acting on $\mathbb{R}^d$ by permuting coordinates. A *core point* (for G) is an integral vector $z \in \mathbb{Z}^d$ such that the convex hull of the orbit Gz contains no other integral vectors but those in the orbit Gz. Herr, Rehn and Schürmann considered the question for which groups there are infinitely many core points up to *translation equivalence*, that is, up to translation by vectors fixed by the group. In the present paper, we propose a coarser equivalence relation for core points called *normalizer equivalence*. These equivalence classes often contain infinitely many vectors up to translation, for example when the group admits an irrational invariant subspace or an invariant irreducible subspace occurring with multiplicity greater than 1. We also show that the number of core points up to normalizer equivalence is finite if G is a so-called *QI-group*. These groups include all transitive permutation groups of prime degree. We apply the concept of normalizer equivalence to simplify integer linear optimization problems.

2010 Mathematics Subject Classification. Primary 20C10; Secondary 16U60, 20B25, 20C15, 52B20, 90C10

Keywords. Orbit polytope, core points, group representation, lattice, integer linear programming

1. Introduction

Let $G \leqslant \mathrm{GL}(d, \mathbb{Z})$ be a finite group. We consider orbit polytopes $\mathrm{conv}(Gz)$ of integral vectors $z \in \mathbb{Z}^d$, that is, the convex hull of an orbit of a point z with integer coordinates. We call z a *core point* for G, when the vertices are the only integral vectors in the orbit polytope $\mathrm{conv}(Gz)$. Core points are relevant for symmetric convex integer optimization because any G-symmetric convex set contains an integer vector if and only if it contains a core point [9].

In the following, we write

$$\mathrm{Fix}(G) = \{v \in \mathbb{R}^d \mid gv = v \text{ for all } g \in G\}$$

for the fixed space of G in $\mathbb{R}^d$. Notice that when z is a core point and $t \in \mathrm{Fix}(G) \cap \mathbb{Z}^d$, then $z + t$ is another core point. We call the core points z and $z + t$ *translation*

[1] arXiv: 1703.01152v1 [math.MG]. Submitted.

equivalent. Herr, Rehn and Schürmann [10] consider the question whether there are finitely or infinitely many core points up to translation equivalence, in the case where G is a permutation group acting by permuting coordinates. Their methods can be used to show that there are only finitely many core points up to translation, when $\mathbb{R}^d/\operatorname{Fix}(G)$ has no G-invariant subspaces other than the trivial ones [20, Theorem 3.13]. It is conjectured that in all other cases, there are infinitely many core points up to translation. This has been proved in special cases, but is open in general.

In this paper, we consider a coarser equivalence relation, where we allow to multiply core points with invertible integer matrices $S \in \mathrm{GL}(d,\mathbb{Z})$ which centralize (or normalize) the subgroup G. Thus two points z and w are called *centralizer equivalent*, when $w = Sz + t$, where $S \in \mathrm{GL}(d,\mathbb{Z})$ is such that $Sg = gS$ for all $g \in G$, and $t \in \operatorname{Fix}(G) \cap \mathbb{Z}^d$. These coarser equivalence classes often contain infinitely many core points up to translation equivalence. For example, if $\mathbb{R}^d$ has an *irrational* invariant subspace $U \leqslant \mathbb{R}^d$ (that is, a subspace $\{0\} \neq U \leqslant \mathbb{R}^d$ such that $U \cap \mathbb{Z}^d = \{0\}$), then each integer point z with nonzero projection onto U is centralizer equivalent to infinitely many points, which are not translation equivalent. This yields another proof of the result of Herr, Rehn and Schürmann [10, Theorem 32] that there are infinitely many core points up to translation, when there is an irrational invariant subspace.

We also prove the following: Suppose that $G \leqslant \mathrm{S}_d$ is a transitive permutation group acting on $\mathbb{R}^d$ by permuting coordinates. Suppose that $\operatorname{Fix}(G)^\perp$ contains no rational G-invariant subspace other than $\{0\}$ and $\operatorname{Fix}(G)^\perp$ itself. (A subspace of $\mathbb{R}^d$ is rational, if it has a basis contained in $\mathbb{Q}^d$.) Such a group G is called a *QI-group*. Then there are only finitely many core points up to centralizer equivalence.

For example, this is the case, when $d = p$ is a prime number (and $G \leqslant \mathrm{S}_p$ is transitive). In the case that the group is not 2-homogeneous, there are infinitely many core points up to translation, but these can be obtained from finitely many by multiplying with invertible integer matrices from the centralizer.

The paper is organized as follows. In Section 2, we introduce different equivalence relations for core points and make some elementary observations. Section 3 collects some elementary properties of orders in semisimple algebras. In Section 4, we determine when the normalizer equivalence classes contain infinitely many points up to translation equivalence. In Section 5, we prove the aforementioned result on QI-groups. Sections 4 and 5 can mostly be read independently from another. In the final Section 6 we show how our theory can be applied to integer linear optimization problems with suitable symmetries.

2. Equivalence for core points

Let V be a finite-dimensional vector space over the real numbers $\mathbb{R}$ and G a finite group acting linearly on V.

2.1 Definition. An **orbit polytope** (for G) is the convex hull of the G-orbit of a point $v \in V$. It is denoted by

$$\mathrm{P}(G, v) = \mathrm{conv}\{gv \mid g \in G\}.$$

Let $\Lambda \subseteq V$ be a full $\mathbb{Z}$-lattice in V, that is, the $\mathbb{Z}$-span of an $\mathbb{R}$-basis of V. Assume that G maps Λ onto itself.

2.2 Definition. [9] An element $z \in \Lambda$ is called a **core point** (for G and Λ) if the only lattice points in $\mathrm{P}(G, z)$ are its vertices, that is, the elements in the orbit Gz. In other words, z is a core point if

$$\mathrm{P}(G, z) \cap \Lambda = Gz.$$

2.3 Remark. The barycenter

$$\frac{1}{|G|} \sum_{g \in G} gv \in \mathrm{P}(G, v)$$

is always fixed by G. If $\mathrm{Fix}_V(G)$, the set of vectors in V fixed by all $g \in G$, consists only of 0, then the barycenter of each orbit polytope is the zero vector. In this case, only the zero vector is a core point.

More generally, the map

$$e_1 = \frac{1}{|G|} \sum_{g \in G} g$$

gives the projection from V onto the fixed space $\mathrm{Fix}_V(G)$. The projection $e_1\Lambda$ is a full lattice in $\mathrm{Fix}_V(G)$ containing $\mathrm{Fix}_\Lambda(G) = \mathrm{Fix}_V(G) \cap \Lambda$. So when $\mathrm{Fix}_\Lambda(G) = e_1\Lambda$, then the only core points are the fixed points of G in Λ.

On the other hand, it is not difficult to see that for each $v \in e_1\Lambda$, there are core points z with $e_1 z = v$. Namely, among all $z \in \Lambda$ with $e_1 z = v$, there are elements with minimal squared norm $\|z\|^2$, and these are core points.

If z is a core point and $b \in \mathrm{Fix}_\Lambda(G)$, then $z + b$ is a core point, too, because $\mathrm{P}(G, z + b) = \mathrm{P}(G, z) + b$. Such core points should be considered as *equivalent*. This viewpoint was adopted by Herr, Rehn and Schürmann [9, 10]. In the present paper, we consider a coarser equivalence relation. We write $\mathrm{GL}(\Lambda)$ for the invertible $\mathbb{Z}$-linear maps $\Lambda \to \Lambda$. Since Λ contains a basis of V, we may view $\mathrm{GL}(\Lambda)$ as a subgroup of $\mathrm{GL}(V)$. (If $V = \mathbb{R}^d$ and $\Lambda = \mathbb{Z}^d$, then we can identify $\mathrm{GL}(\Lambda)$ with $\mathrm{GL}(d, \mathbb{Z})$, the set of matrices over $\mathbb{Z}$ with determinant ± 1.)

By assumption, G is a subgroup of $\mathrm{GL}(\Lambda)$. We use the following notation from group theory: The **normalizer** of G in $\mathrm{GL}(\Lambda)$ is the set

$$\mathbf{N}_{\mathrm{GL}(\Lambda)}(G) := \{S \in \mathrm{GL}(\Lambda) \mid \forall g \in G\colon S^{-1}gS \in G\}.$$

The **centralizer** of G in $\mathrm{GL}(\Lambda)$ is the set

$$\mathbf{C}_{\mathrm{GL}(\Lambda)}(G) := \{S \in \mathrm{GL}(\Lambda) \mid \forall g \in G\colon S^{-1}gS = g\}.$$

2.4 Definition. Two points z and w are called **normalizer equivalent**, if there is a point $b \in \mathrm{Fix}_\Lambda(G)$ and an element S in the normalizer $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ of G in $\mathrm{GL}(\Lambda)$ such that $w = Sz + b$. The points are called **centralizer equivalent** if $w = Sz + b$ with $S \in \mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ and $b \in \mathrm{Fix}_\Lambda(G)$. Finally, we call two points z and w **translation equivalent**, when $w - z \in \mathrm{Fix}_\Lambda(G)$.

This is justified by the following simple observation:

2.5 Lemma. *If*

$$w = Sz + b \quad \textit{with} \quad S \in \mathbf{N}_{\mathrm{GL}(\Lambda)}(G) \quad \textit{and} \quad b \in \mathrm{Fix}_\Lambda(G),$$

then $x \mapsto Sx + b$ defines a bijection between

$$\mathrm{P}(G, z) \cap \Lambda \quad \textit{and} \quad \mathrm{P}(G, w) \cap \Lambda.$$

In particular, z is a core point if and only if w is a core point.

Proof. The affine bijection $x \mapsto Sx + b$ maps the orbit polytope $\mathrm{P}(G, z)$ to another polytope. The vertex gz is mapped to the vertex

$$Sgz + b = (SgS^{-1})Sz + b = hSz + b = h(Sz + b) = hw,$$

where $h = SgS^{-1} \in G$ (since S normalizes G). The second last equality follows as b is fixed by G. As SgS^{-1} runs through G as g does, it follows that $x \mapsto Sx + b$ maps the orbit Gz to the orbit Gw and thus maps the orbit polytope $\mathrm{P}(G, z)$ to the orbit polytope $\mathrm{P}(G, w)$. Since $x \mapsto Sx + b$ also maps Λ onto itself, the result follows. □

Herr, Rehn and Schürmann [8, 10, 20] considered the question whether the set of core points up to translation is finite or infinite (in the case where G acts by permuting coordinates). We might ask the same question about core points up to normalizer equivalence as defined here. Also, it is of interest whether our bigger equivalence classes contain finitely or infinitely many points up to translation.

2.6 Remark. Notice that $\mathrm{Fix}_\Lambda(G)$ consists exactly of the points equivalent to 0, for all equivalences defined here. These are the **trivial core points**.

If z is any non-trivial core point, then we must have $e_1 z \notin \Lambda$, where $e_1 = (1/|G|)\sum g$ is the projection onto the fixed space. Suppose that $z \in V$ is such that the orbit Gz linearly spans V. Then $\mathrm{Fix}_V(G)$ has dimension at most 1. The elements of $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ map $\mathrm{Fix}_\Lambda(G)$ onto itself, and thus act on $\mathrm{Fix}_V(G)$ as ± 1. Thus

$$\Big(\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)z\Big) \cap \Big(z + \mathrm{Fix}_V(G)\Big) \subseteq \{z, z - 2z|_{\mathrm{Fix}_V(G)}\}.$$

This means that different elements in $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)z$ are almost never translation equivalent. In particular, if $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ is infinite, then the normalizer equivalence class of a nontrivial core point z contains infinitely many translation equivalence classes.

It is sometimes easier to work with the centralizer $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ instead of the normalizer $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$, which yields a slightly finer equivalence relation. By the following simple observation, the $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$-equivalence classes can not be much smaller than the $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$-equivalence classes:

2.7 Lemma. $|\mathbf{N}_{\mathrm{GL}(\Lambda)}(G) : \mathbf{C}_{\mathrm{GL}(\Lambda)}(G)|$ *is finite.*

Proof. The factor group $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)/\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$ [12, Corollary X.19], and $\mathrm{Aut}(G)$ is finite, since G itself is finite by assumption. □

3. Preliminaries on orders

In this section, we collect some simple properties of *orders* in semi-simple algebras over $\mathbb{Q}$. Orders are relevant for us since the centralizer $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ can be identified with the *unit group* of such an order, as we explain below.

Recall the following definition [21]: Let A be a finite-dimensional algebra over $\mathbb{Q}$ (associative, with one). An **order** (or $\mathbb{Z}$-**order**) in A is a subring $R \subset A$ which is finitely generated as $\mathbb{Z}$-module and such that $\mathbb{Q}R = A$. (Here, "subring" means in particular that R and A have the same multiplicative identity.) In other words, an order is a full $\mathbb{Z}$-lattice in A which is at the same time a subring of A.

As in the first section, let Λ be a lattice on which the finite group G acts. For the moment, let us change notation and write $V = \mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$. Let $A := \mathrm{End}_{\mathbb{Q}G}(V)$ be the ring of $\mathbb{Q}G$-module endomorphisms of V, that is, the set of linear maps $\alpha\colon V \to V$ such that $\alpha(gv) = g\alpha(v)$ for all $v \in V$ and $g \in G$. This is just the centralizer of G in the ring of all $\mathbb{Q}$-linear endomorphisms of V.

We claim that

$$R := \{\alpha \in A \mid \alpha(\Lambda) \subseteq \Lambda\}$$

is an order in A. Namely, choose a $\mathbb{Z}$-basis of Λ. This basis is also a $\mathbb{Q}$-basis of V. By identifying linear maps with matrices with respect to the chosen basis, A gets identified with the centralizer of G in the set of *all* $d \times d$ matrices over $\mathbb{Q}$, and R gets identified with the centralizer of G in the set of $d \times d$ matrices with entries in $\mathbb{Z}$. It follows that R is finitely generated as $\mathbb{Z}$-module, and for every $\alpha \in A$ there is an $m \in \mathbb{Z}$ such that $m\alpha \in R$. Thus R is an order of A. (Also, $R \cong \mathrm{End}_{\mathbb{Z}G}(\Lambda)$ naturally.)

Moreover, the centralizer $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ is exactly the set of invertible elements of R, that is, the unit group $\mathbf{U}(R)$ of R. For this reason, it is somewhat easier to work with $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ instead of the normalizer $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$. The unit group $\mathbf{U}(R)$ of an order R is a finitely generated (even finitely presented) group [13, § 3]. Finding explicit generators of $\mathbf{U}(R)$ (and relations between them) is in general a difficult task, but there do exist algorithms for this purpose [2]. The situation is somewhat better when R is abelian, for example when $R \cong \mathbb{Z}A$, where A is a finite abelian group [6]. Moreover, it is quite easy to give generators of a subgroup of $\mathbf{U}(\mathbb{Z}A)$ which has finite index in $\mathbf{U}(\mathbb{Z}A)$ [11, 16].

We now collect some general elementary facts about orders that we need. (For a comprehensive treatment of orders, not only over $\mathbb{Z}$, we refer the reader to Reiner's book on maximal orders [21]. For unit groups of orders, see the survey article by Kleinert [13].)

3.1 Lemma. *Let R_1 and R_2 be two orders in the $\mathbb{Q}$-algebra A. Then $R_1 \cap R_2$ is also an order in A.*

Proof. Clearly, $R_1 \cap R_2$ is a subring.

Since R_2 is finitely generated over $\mathbb{Z}$ and $\mathbb{Q}R_1 = A$, there is a non-zero integer $m \in \mathbb{Z}$ with $mR_2 \subseteq R_1$. Thus $mR_2 \subseteq R_1 \cap R_2$. Since mR_2 contains a $\mathbb{Q}$-basis of A, it follows that $R_1 \cap R_2$ contains such a basis. As a submodule of a finitely generated $\mathbb{Z}$-module, $R_1 \cap R_2$ is again finitely generated. Thus $R_1 \cap R_2$ is an order of A. □

3.2 Lemma. *Let R_1 and R_2 be orders in the $\mathbb{Q}$-algebra A with $R_1 \subseteq R_2$. Then $|\mathbf{U}(R_2) : \mathbf{U}(R_1)|$ is finite.*

Proof. There exists a non-zero integer m such that $mR_2 \subseteq R_1$. Suppose that u, $v \in \mathbf{U}(R_2)$ are such that $u - v \in mR_2$. Then $u \in v + mR_2$ and thus $uv^{-1} \in 1 + mR_2 \subseteq R_1$. Similarly, $vu^{-1} \in 1 + mR_2 \subseteq R_1$. Thus $uv^{-1} \in \mathbf{U}(R_1)$. This shows $|\mathbf{U}(R_2) : \mathbf{U}(R_1)| \leqslant |R_2 : mR_2| < \infty$, as claimed. □

3.3 Corollary. *Let R_1 and R_2 be two orders in the $\mathbb{Q}$-algebra A. Then $\mathbf{U}(R_1)$ is finite if and only if $\mathbf{U}(R_2)$ is finite.*

Proof. By Lemma 3.1, $R_1 \cap R_2$ is an order. By Lemma 3.2, the index $|\mathbf{U}(R_i) : \mathbf{U}(R_1 \cap R_2)|$ is finite for $i = 1, 2$. The result follows. □

4. Finiteness of equivalence classes

In this section we determine for which groups G the normalizer equivalence classes are finite or not, and in particular, when the normalizer $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ is finite or not.

We use the notation introduced in Section 2. So let V be a $\mathbb{R}G$-module and $\Lambda \subset V$ a full $\mathbb{Z}$-lattice which is stabilized by G. A subspace $U \leqslant V$ is called Λ-**rational** if $U \cap \Lambda$ contains a basis of U, and Λ-**irrational**, if $U \cap \Lambda = \{0\}$. If U is an irreducible $\mathbb{R}G$-submodule, then U is either Λ-rational or Λ-irrational.

4.1 Theorem. *Let*

$$V = U_1 \oplus \cdots \oplus U_r$$

be a decomposition of V into irreducible $\mathbb{R}G$-subspaces. Then $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ has finite order if and only if all the U_i's are Λ-rational and pairwise non-isomorphic.

Before proving this, let us mention the following:

4.2 Remark. Let $z \in V$ be an element such that the orbit Gz linearly spans V. Then the orbit $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)z$ has finite size if and only if $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ has finite size.

Proof. Clearly, when $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ has finite size, then every orbit of that group is finite.

Now assume that $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ has infinite order. By Lemma 2.7, the centralizer $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ has also infinite order. If $cz = z$ for $c \in \mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$, then $cgz = gcz = gz$ for all $g \in G$ and thus $c = 1$. Thus

$$\infty = |\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)| = |\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)z| \leqslant |\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)z|. \qquad \square$$

It follows from the theorem that when V has an irrational invariant subspace, then $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ is infinite. Thus if z is a core point, then there are infinitely many core points, even up to translation. This was first proved by Thomas Rehn [10, 20].

Another consequence of Theorem 4.1 is that $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ is infinite when V is not multiplicity-free (as $\mathbb{R}G$-module).

The proof of Theorem 4.1 involves some non-trivial representation and number theory. By Lemma 2.7, the normalizer $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$ is finite if and only if the centralizer $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ is finite. As remarked earlier, the centralizer can naturally be identified with the set of units of the ring $\mathrm{End}_{\mathbb{Z}G}(\Lambda)$, and $\mathrm{End}_{\mathbb{Z}G}(\Lambda)$ is an order in the $\mathbb{Q}$-algebra $\mathrm{End}_{\mathbb{Q}G}(\mathbb{Q}\Lambda)$, where $\mathbb{Q}\Lambda \cong \mathbb{Q} \otimes_{\mathbb{Z}} \Lambda$. For this reason, it is more convenient to work with the $\mathbb{Q}$-vector space $W := \mathbb{Q}\Lambda$.

Fix a decomposition of $W = \mathbb{Q}\Lambda$ into simple modules:

$$W \cong m_1 S_1 \oplus \cdots \oplus m_r S_r, \quad m_i \in \mathbb{N},$$

where we assume that $S_i \ncong S_j$ for $i \neq j$. Set $D_i := \mathrm{End}_{\mathbb{Q}G}(S_i)$, which is by Schur's lemma [14, (3.6)] a division ring, and finite dimensional over $\mathbb{Q}$.

4.3 Lemma. *With the above notation, we have*

$$\mathrm{End}_{\mathbb{Q}G}(V) \cong \mathbf{M}_{m_1}(D_1) \times \cdots \times \mathbf{M}_{m_r}(D_r),$$

where $\mathbf{M}_m(D)$ *denotes the ring of* $m \times m$ *matrices with entries in* D*. If* R_i *is an order in* D_i *for each* i*, then*

$$R := \mathbf{M}_{m_1}(R_1) \times \cdots \times \mathbf{M}_{m_r}(R_r)$$

is an order in $\mathrm{End}_{\mathbb{Q}G}(V)$*.*

Proof. The first assertion is a standard observation, used for example in one proof of the Wedderburn-Artin structure theorem for semisimple rings [14, Thm. 3.5 and proof]. The assertion on orders is then easy. □

In particular, the group of units of R is then isomorphic to the direct product of groups of the form $\mathrm{GL}(m_i, R_i)$. To prove Theorem 4.1, in view of Corollary 3.3, it suffices to determine when all these groups are finite. The following is a first step towards the proof of the theorem:

4.4 Corollary. *If some* $m_i > 1$*, then* $\mathbf{U}(R)$ *(and thus* $\mathbf{N}_{\mathrm{GL}(\Lambda)}(G)$*) is infinite.*

Proof. $\mathbf{U}(R)$ contains a subgroup isomorphic to $\mathrm{GL}(m_i, R_i)$, which contains the group $\mathrm{GL}(m_i, \mathbb{Z})$. This group is infinite if $m_i > 1$. □

To continue with the proof of Theorem 4.1, we have to look at the units of an order R_i in D_i. We use the following theorem of Käte Hey which can be seen as a generalization of Dirichlet's unit theorem:

4.5 Theorem. *[13, Theorem 1] Let* D *be a finite dimensional division algebra over* $\mathbb{Q}$*, and let* R *be an order of* D *with unit group* $\mathbf{U}(R)$*. Set*

$$S = \{d \in D \otimes_{\mathbb{Q}} \mathbb{R} \mid (\det d)^2 = 1\}.$$

Then $S/\mathbf{U}(R)$ *is compact. (Here* $\det d$ *refers to the action of* d *as linear operator on* $D \otimes_{\mathbb{Q}} \mathbb{R}$*. One can also use the reduced norm, of course.)*

From this, we can derive the following result (probably well known):

4.6 Lemma. *Let* D *be a finite dimensional division algebra over* $\mathbb{Q}$ *and* R *an order of* D*. Then* $|\mathbf{U}(R)| < \infty$ *if and only if* $D \otimes_{\mathbb{Q}} \mathbb{R}$ *is a division ring.*

Proof. Suppose $D_{\mathbb{R}} := D \otimes_{\mathbb{Q}} \mathbb{R}$ is a division ring. By Frobenius' theorem, we have $D_{\mathbb{R}} \cong \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. In each case, one checks that the set S defined in Theorem 4.5 is compact. Thus the discrete group $\mathbf{U}(R) \subseteq S$ must be finite. (Notice that we did not use Theorem 4.5 here, only that $\mathbf{U}(R) \subseteq S$.)

Conversely, suppose that $D_{\mathbb{R}}$ is not a division ring. Then there is some nontrivial idempotent $e \in D_{\mathbb{R}}$, that is, $e^2 = e$, but $e \neq 0, 1$. (This follows since $D_{\mathbb{R}}$ is semisimple.) Set $f = 1 - e$. Then for $\lambda, \mu \in \mathbb{R}$, we have $\det(\lambda e + \mu f) = \lambda^{k_1}\mu^{k_2}$ with $k_1 = \dim(D_{\mathbb{R}}e)$ and $k_2 = \dim(D_{\mathbb{R}}f)$. In particular, for every $\lambda \neq 0$ there is some μ such that $\lambda e + \mu f \in S$. This means that S is unbounded, and thus not compact. It follows from Theorem 4.5 that $\mathbf{U}(R)$ can not be finite. □

Proof of Theorem 4.1. First, assume that we are given a decomposition $V = U_1 \oplus \cdots \oplus U_r$ as in the theorem. Then $S_i := U_i \cap \mathbb{Q}\Lambda$ contains a basis of U_i and thus is non-zero, and necessarily simple as $\mathbb{Q}G$-module. Thus

$$W = V \cap \mathbb{Q}\Lambda = S_1 \oplus \cdots \oplus S_r$$

is a decomposition of W into simple $\mathbb{Q}G$-modules, which are pairwise nonisomorphic. It follows that

$$\mathrm{End}_{\mathbb{Q}}(W) \cong D_1 \times \cdots \times D_r,$$

where $D_i = \mathrm{End}_{\mathbb{Q}G}(S_i)$. Since $D_i \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{End}_{\mathbb{R}G}(U_i)$ is a division ring, too, it follows that the orders of each D_i have a finite unit group, by Lemma 4.6. Thus $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ is finite.

Conversely, assume that $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)$ is finite. It follows from Corollary 4.4 that W has a decomposition into simple summands which are pairwise non-isomorphic:

$$W = S_1 \oplus \cdots \oplus S_r.$$

Let $D_i = \mathrm{End}_{\mathbb{R}G}(S_i)$. Then Lemma 4.6 yields that $D_i \otimes_{\mathbb{Q}} \mathbb{R}$ is a division ring, too. Since $D_i \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{End}_{\mathbb{R}G}(S_i\mathbb{R})$, it follows that $U_i := S_i\mathbb{R}$ is simple. (Otherwise, the projection to a nontrivial invariant submodule would be a zero-divisor in $\mathrm{End}_{\mathbb{R}G}(U_i)$.) For $i \neq j$, we have $U_i \ncong U_j$ by the Noether-Deuring theorem [14, Theorem 19.25]. Thus V has a decomposition $V = U_1 \oplus \cdots \oplus U_r$ as required. □

4.7 Example. Consider the regular representation of a group G, that is, G acts on $\mathbb{Q}G$ by left multiplication, so it permutes the canonical basis G. As lattice, we choose the group ring $\mathbb{Z}G$, the vectors with integer coordinates. Then $\mathrm{End}_{\mathbb{Z}G}(\mathbb{Z}G) \cong \mathbb{Z}G$. Units of group rings are a much studied problem. A theorem of Higman says that $\mathbf{U}(\mathbb{Z}G)$ is finite if and only if G is abelian of exponent 1, 2, 3, 4 or 6, or $G \cong Q_8 \times E$ with $E^2 = \{1\}$. This is also easy to derive from Theorem 4.1.

For example, let the cyclic group C_4 of order 4 act on $\mathbb{R}^4$ by permuting coordinates. Then $\mathbf{U}(\mathbb{Z}C_4)$ is finite, and so the equivalence classes are finite (up to translation by fixed points). There are, however, infinitely many nonequivalent core points, as was shown by Herr, Rehn and Schürmann [10].

On the other hand, when p is a prime, then there are only finitely many core points up to equivalence in $\mathbb{Z}C_p$, by Theorem 5.1 below. If $p \geqslant 5$, then $\mathbf{U}(\mathbb{Z}C_p)$ is infinite.

5. Rationally irreducible

Suppose that $\Lambda = \mathbb{Z}^d$, and assume that G acts on $\mathbb{R}^d$ by matrices in $\mathrm{GL}(d,\mathbb{Z})$. A subspace $U \leqslant \mathbb{R}^d$ is called **irrational**, if $U \cap \mathbb{Q}^d = \{0\}$, and **rational**, if U has a basis contained in $\mathbb{Q}^d$. If U is an irreducible $\mathbb{R}G$-submodule, then U is either rational or irrational. In this section, we prove the following result:

5.1 Theorem. *Let $G \leqslant \mathrm{S}_d$ be a transitive permutation group acting on $\mathbb{R}^d$ by permuting coordinates, and such that $\mathrm{Fix}(G)^\perp$ does not contain any rational G-invariant subspace other than $\{0\}$ and $\mathrm{Fix}(G)^\perp$ itself. Then there are only finitely many core points up to equivalence. (That is, up to translation by fixed integer vectors and multiplication with elements of $\mathbf{N}_{\mathrm{GL}(d,\mathbb{Z})}(G)$).*

Notice that $\mathrm{Fix}(G)^\perp$ contains no non-trivial rational invariant subspaces if and only if $\mathrm{Fix}(G)^\perp \cap \mathbb{Q}^d$ contains no proper G-invariant subspace other than $\{0\}$. In algebraic language, this means that $\mathrm{Fix}(G)^\perp \cap \mathbb{Q}^d$ is a simple module over $\mathbb{Q}G$. Following Dixon [5], who studied such groups, we call a permutation group G a **QI-group**, when $\mathrm{Fix}(G)^\perp$ contains no non-trivial rational subspaces, equivalently, when $\mathrm{Fix}(G)^\perp \cap \mathbb{Q}^d$ is simple as $\mathbb{Q}G$-module.

We divide the proof of Theorem 5.1 into a number of lemmas. The idea is the following: We show that for any vector $z \in \mathbb{Z}^d$ there is some $c \in \mathbf{C}_{\mathrm{GL}(d,\mathbb{Z})}(G)$ such that the projections of cz to the different irreducible real subspaces of $\mathrm{Fix}(G)^\perp$ have approximately the same norm. (At the same time, this point cz is one with minimal norm in the orbit $\mathbf{C}_{\mathrm{GL}(\Lambda)}(G)z$.) When z is a core point, at least one of these norms must be "small", by a fundamental result of Herr, Rehn and Schürmann [10, Theorem 9] (Theorem 5.8 below).

The first lemma is taken from Dixon's paper [5, Lemma 6(b)]. Here $\mathrm{Irr}\, G$ is the set of irreducible characters of the group G (over the complex numbers), $\mathbb{Q}(\chi)$ is the field generated by the values of χ, which is a finite Galois extension of $\mathbb{Q}$, and $\mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ is the corresponding Galois group.

5.2 Lemma (Dixon [5]). *Let G be a QI-group and let π be the permutation character of G. Let $\chi \in \mathrm{Irr}\, G$ be an irreducible constituent of $\pi - 1$ (the character of G on $\mathrm{Fix}(G)^\perp$). Then*

$$\pi = 1 + \sum_{\alpha\in\Gamma} \chi^\alpha, \quad \textit{where} \quad \Gamma = \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q}).$$

For the moment, we work with the complex space $\mathbb{C}^d$, on which G acts by permuting coordinates. Recall that to each $\chi \in \mathrm{Irr}\, G$ corresponds a central primitive idempotent of the group algebra $\mathbb{C}G$, namely

$$e_\chi = \frac{\chi(1)}{|G|} \sum_{g\in G} \chi(g^{-1})g \in \mathbf{Z}(\mathbb{C}G).$$

If V is any $\mathbb{C}G$-module, then $e_\chi V$ is the χ-homogeneous component of V, and the character of $e_\chi V$ is an integer multiple of χ [22, Section 2.6]. In the present situation, it follows from Lemma 5.2 that

$$U := e_\chi \mathbb{C}^d = \{v \in \mathbb{C}^d \mid e_\chi v = v\}$$

is itself an irreducible module affording the character χ. In particular, U has a basis contained in K^d, where $K := \mathbb{Q}(\chi)$.

Another consequence of Lemma 5.2 is that we have the decomposition

$$\mathbb{C}^d = \mathrm{Fix}(G) \oplus \bigoplus_{\gamma\in\Gamma} U^\gamma.$$

Here U^γ means this: Since U has a basis in $\mathbb{Q}(\chi)^d$, we can apply γ to the coordinates of the vectors in such a basis. The linear span of the result is denoted by U^γ. This is independent of the chosen basis.

5.3 Lemma. *Set $A := \mathbf{C}_{\mathbf{M}_d(\mathbb{Q})}(G) \cong \mathrm{End}_{\mathbb{Q}G}(\mathbb{Q}^d)$. There is an algebra homomorphism $\lambda\colon A \to \mathbb{Q}(\chi)$ such that each $a \in A$ acts on U^γ by multiplication with $\lambda(a)^\gamma$, and such that $\lambda(a^t) = \overline{\lambda(a)}$. There is another homomorphism $m\colon A \to \mathbb{Q}$, such that*

$$A \cong \mathbb{Q} \times \mathbb{Q}(\chi) \quad \textit{via} \quad a \mapsto (m(a), \lambda(a)).$$

The isomorphism $A \cong \mathbb{Q} \times \mathbb{Q}(\chi)$ is contained in Dixon's paper [5, Lemma 6(d)], and follows from Lemma 5.2 together with general results in representation theory. But as we need the specific properties of the map λ from the lemma, we give a detailed proof:

Proof of Lemma 5.3. Suppose the matrix a centralizes G, and let $\lambda(a) \in \mathbb{C}$ be an eigenvalue of a on U. The corresponding eigenspace is G-invariant, since a centralizes G. Since U is irreducible, U is contained in the eigenspace of $\lambda(a)$.

When $a \in A \subseteq \mathbf{M}_d(\mathbb{Q})$, then a maps $U \cap \mathbb{Q}(\chi)^d \neq \{0\}$ to itself, and thus $\lambda(a) \in \mathbb{Q}(\chi)$. This defines the algebra homomorphism $\lambda\colon A \to \mathbb{Q}(\chi)$.

When $u \in U \cap \mathbb{Q}(\chi)^d$, $\gamma \in \Gamma$ and $a \in A$, then $au^\gamma = (au)^\gamma = \lambda(a)^\gamma u^\gamma$. Thus a acts as $\lambda(a)^\gamma$ on U^γ.

Each $a \in A$ acts also on the one-dimensional fixed space by multiplication with some $m(a) \in \mathbb{Q}$. As

$$\mathbb{C}^d = \mathrm{Fix}(G) \oplus \bigoplus_{\gamma\in\Gamma} U^\gamma,$$

we see that the space $\mathbb{C}^d$ has a basis of common eigenvectors for all $a \in A$. With respect to this basis, each a is a diagonal matrix, where $m(a)$ appears once and $\lambda(a)^\gamma$ appears $\chi(1)$-times for each $\gamma \in \Gamma$. In particular, the map $A \ni a \mapsto (m(a), \lambda(a))$ is injective.

Since G acts orthogonally with respect to the standard inner product on $\mathbb{C}^d$, the above decomposition into irreducible subspaces is orthogonal and we can find an orthonormal basis of common eigenvectors of all $a \in A$. From this, it is clear that $\lambda(a^t) = \lambda(a^*) = \overline{\lambda(a)}$.

To see that $a \mapsto (m(a), \lambda(a))$ is onto, let $(q, \mu) \in \mathbb{Q} \times \mathbb{Q}(\chi)$. Define

$$\begin{aligned}\varphi(q,\mu) &:= qe_1 + \sum_{\gamma\in\Gamma} (\mu e_\chi)^\gamma \\ &= q\frac{1}{|G|}\sum_{g\in G} g + \frac{\chi(1)}{|G|}\sum_{g\in G}\left(\sum_{\gamma\in\Gamma}\left(\mu\chi(g^{-1})\right)^\gamma\right) g \\ &\in \mathbf{Z}(\mathbb{Q}G).\end{aligned}$$

Then the corresponding map $v \mapsto \varphi(q,\mu)v$ is in A, and from $\varphi(q,\mu)e_1 = qe_1$ and $\varphi(q,\mu)e_\chi = \mu e_\chi$ we see that $m(\varphi(q,\mu)) = q$ and $\lambda(\varphi(q,\mu)) = \mu$. This finishes the proof that $A \cong \mathbb{Q} \times \mathbb{Q}(\chi)$. □

5.4 Lemma. *Set $W := (U + \overline{U}) \cap \mathbb{R}^d$. Then the decomposition of $\mathbb{R}^d$ into irreducible $\mathbb{R}G$-modules is given by*

$$\mathbb{R}^d = \mathrm{Fix}(G) \oplus \bigoplus_{\alpha\in\Gamma_0} W^\alpha, \quad \Gamma_0 = \mathrm{Gal}((\mathbb{Q}(\chi)\cap\mathbb{R})/\mathbb{Q}).$$

(In particular, W is irreducible as $\mathbb{R}G$-module.) For $w \in W^\alpha$ and $a \in A$, we have $\|aw\|^2 = \left(\overline{\lambda(a)}\lambda(a)\right)^\alpha \|w\|^2$.

Proof. When $\mathbb{Q}(\chi) \subseteq \mathbb{R}$, then $\overline{U} = U$ and $W = U \cap \mathbb{R}^d$. The result is clear in this case.

Otherwise, we have $U \cap \mathbb{R}^d = \{0\}$ and $U \cap \overline{U} = \{0\}$, and so $W = (U \oplus \overline{U}) \cap \mathbb{R}^d \neq \{0\}$, and thus again W is simple over $\mathbb{R}G$.

The extension $\mathbb{Q}(\chi)/\mathbb{Q}$ has abelian Galois group, and thus $\mathbb{Q}(\chi) \cap \mathbb{R}$ is also Galois over $\mathbb{Q}$. The Galois group Γ_0 is isomorphic to the factor group $\Gamma/\{\mathrm{id}, \kappa\}$, where κ denotes complex conjugation. Suppose $\alpha \in \Gamma_0$ is the restriction of $\gamma \in \Gamma$ to $\mathbb{Q}(\chi) \cap \mathbb{R}$. Then

$$W^\alpha = \left((U + \overline{U}) \cap \mathbb{R}^d\right)^\alpha = (U^\gamma + \overline{U}^\gamma) \cap \mathbb{R}^d = (U^\gamma + U^{\kappa\gamma}) \cap \mathbb{R}^d.$$

The statement about the decomposition follows.

The last statement is immediate from Lemma 5.3. □

5.5 Lemma. *Let $C := \mathbf{C}_{\mathrm{GL}(d,\mathbb{Z})}(G)$ and define*

$$L\colon C \to \mathbb{R}^{\Gamma_0}, \quad L(c) := \left(\log(\overline{\lambda(c)}\lambda(c))^\alpha\right)_{\alpha\in\Gamma_0}.$$

Then the image $L(C)$ of C under this map is a full lattice in the hyperplane

$$H = \{(x_\alpha)_{\alpha\in\Gamma_0} \mid \sum_{\alpha\in\Gamma_0} x_\alpha = 0\}.$$

We will derive this lemma from the following version of Dirichlet's unit theorem [18, Satz I.7.3]:

5.6 Lemma. *Let K be a finite field extension over $\mathbb{Q}$, let $\alpha_1, \dots, \alpha_r \colon K \to \mathbb{R}$ be the different real field embeddings of K, and let $\beta_1, \overline{\beta_1}, \dots, \beta_s, \overline{\beta_s} \colon K \to \mathbb{C}$ be the different complex embeddings of K, whose image is not contained in $\mathbb{R}$. Let O_K be the ring of algebraic integers in K and $l \colon K^* \to \mathbb{R}^{r+s}$ the map*

$$z \mapsto l(z) = (\log|z^{\alpha_1}|, \dots, \log|z^{\alpha_r}|, \log|z^{\beta_1}|, \dots, \log|z^{\beta_s}|) \in \mathbb{R}^{r+s}.$$

Then the image $l(\mathbf{U}(O_K))$ of the unit group of O_K under l is a full lattice in the hyperplane

$$H = \{x \in \mathbb{R}^{r+s} \mid \sum_{i=1}^{r+s} x_i = 0\}.$$

In the proof of Lemma 5.5, we will apply this result to $K = \mathbb{Q}(\chi)$. Set $F = K \cap \mathbb{R}$, $\Gamma_0 = \mathrm{Gal}(F/\mathbb{Q})$ and $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$. If $F = K \subseteq \mathbb{R}$, then $r = |K : \mathbb{Q}|$ and $s = 0$. In this case, $\{\alpha_1, \dots, \alpha_r\} = \Gamma = \Gamma_0$. If $K \not\subseteq \mathbb{R}$, then $|K : F| = 2$, $r = 0$ and $s = |F : \mathbb{Q}|$. In this case, we may identify the set $\{\beta_1, \dots, \beta_s\}$ with the Galois group Γ_0: for each $\alpha \in \Gamma_0$, there are two extensions of α to the field K, and these are complex conjugate. Thus we get a set $\{\beta_1, \dots, \beta_s\}$ as in Lemma 5.6 by choosing exactly one extension for each $\alpha \in \Gamma$. The map l is independent of this choice, anyway.

It follows that in both cases, we may rewrite the map l (somewhat imprecisely) as

$$l(z) = \left(\log|z^{\alpha}|\right)_{\alpha \in \Gamma_0}.$$

Proof of Lemma 5.5. First notice that the entries of $L(c)$ can be written as

$$\begin{aligned} \log\left(\overline{\lambda(c)}\lambda(c)\right)^{\alpha} = \log\left(\overline{\lambda(c)^{\alpha}}\lambda(c)^{\alpha}\right) &= \log|\lambda(c)^{\alpha}|^2 \\ &= 2\log|\lambda(c)^{\alpha}|, \end{aligned}$$

where we tacitly replaced α by an extension to $\mathbb{Q}(\chi)$, when $\mathbb{Q}(\chi) \not\subseteq \mathbb{R}$. Thus $L(c) = 2l(\lambda(c))$ for all $c \in C$, with l as in Lemma 5.6.

In view of Lemma 5.6, it remains to show that the group $\lambda(C)$ has finite index in $\mathbf{U}(O_K)$. We know that C is the group of units in $\mathbf{C}_{\mathbf{M}_d(\mathbb{Z})}(G) \cong \mathrm{End}_{\mathbb{Z}G}(\mathbb{Z}^d)$, which is an order in $A \cong \mathbb{Q} \times K$. Another order in $\mathbb{Q} \times K$ (in fact, the unique maximal order) is $\mathbb{Z} \times O_K$ with unit group $\{\pm 1\} \times \mathbf{U}(O_K)$. By Lemma 3.2, it follows that C has finite index in $\{\pm 1\} \times \mathbf{U}(O_K)$. Thus $\lambda(C)$ has finite index in $\mathbf{U}(O_K)$ and the result follows. □

For each $v \in \mathbb{R}^d$, let v_α be the orthogonal projection of v onto the simple subspace W^α.

5.7 Lemma. *There is a constant D, depending only on the group G, such that for every $v \in \mathbb{R}^d$ with $v_\alpha \neq 0$ for all $\alpha \in \Gamma_0$, there is an $c \in C$ with*

$$\frac{\|(cv)_\alpha\|^2}{\|(cv)_\beta\|^2} \leqslant D$$

for all α, $\beta \in \Gamma_0$.

As $\mathrm{Fix}(G)^\perp \cap \mathbb{Q}^d$ is a simple module, the assumption $v_\alpha \neq 0$ for all α holds in particular for all $v \in \mathbb{Q}^d \setminus \mathrm{Fix}(G)$.

Proof. By Lemma 5.5, there is a compact set T,

$$T \subset H = \{(x_\alpha) \in \mathbb{R}^{\Gamma_0} \mid \sum_\alpha x_\alpha = 0\},$$

such that $H = T + L(C)$. (For example, we can choose T as a fundamental parallelepiped of the full lattice $L(C)$ in H.)

For $v \in \mathbb{R}^d$ as in the statement of the lemma, define

$$N(v) = \left(\log\|v_\alpha\|^2\right)_\alpha \in \mathbb{R}^{\Gamma_0}.$$

Let $S \in \mathbb{R}^{\Gamma_0}$ be the vector having all entries equal to

$$s := \frac{1}{|\Gamma_0|} \sum_\alpha \log\|v_\alpha\|^2.$$

This s is chosen such that $N(v) - S \in H$. Thus there is $c \in C$ such that $L(c) + N(v) - S \in T$, say $L(c) + N(v) - S = t = (t_\alpha)$.

As

$$\|(cv)_\alpha\|^2 = \|cv_\alpha\|^2 = \left(\overline{\lambda(c)}\lambda(c)\right)^\alpha \|v_\alpha\|^2,$$

it follows that

$$N(cv) = L(c) + N(v)$$

in general. Thus

$$\begin{aligned}\log\|cv_\alpha\|^2 - \log\|cv_\beta\|^2 &= (\log\|cv_\alpha\|^2 - s) - (\log\|cv_\beta\|^2 - s)\\ &= (N(cv) - S)_\alpha - (N(cv) - S)_\beta\\ &= t_\alpha - t_\beta\\ &\leqslant \max_{\alpha,t} t_\alpha - \min_{\beta,t} t_\beta =: D_0.\end{aligned}$$

This maximum and minimum exist since T is compact. The number D_0 may depend on the choice of the set T, but not on v or c. Thus $\|cv_\alpha\|^2/\|cv_\beta\|^2$ is bounded by $D := e^{D_0}$. □

We see from the proof that we get a bound whenever we have a subgroup C_0 of $\mathbf{C}_{\mathrm{GL}(d,\mathbb{Z})}(G)$ such that $L(C_0)$ is a full lattice in the hyperplane H. Of course, we do not get the optimal bound then, but in practice it may be difficult to compute the full centralizer.

We will prove Theorem 5.1 by combining the last lemma with the following fundamental result [10, Theorem 9].

5.8 Theorem. *Let $G \leqslant \mathrm{S}_d$ be a transitive permutation group. Then there is a constant C (depending only on d) such that for each core point z, there is a non-zero invariant subspace $U \leqslant \mathrm{Fix}(G)^\perp$ over $\mathbb{R}$ such that $\|z|_U\|^2 \leqslant C$.*

In our situation, the W^α from Lemma 5.4 are the only irreducible subspaces, and thus for every core point z there is some $\alpha \in \Gamma_0$ with $\|z_\alpha\|^2 \leqslant C$.

We now prove the following more precise version of Theorem 5.1:

5.9 Theorem. *Let $G \leqslant \mathrm{S}_d$ be a QI-group. Then there is a constant M depending only on the group G such that for every core point z, there is a $c \in \mathbf{C}_{\mathrm{GL}(d,\mathbb{Z})}(G)$ and a vector $b \in \mathrm{Fix}(G) \cap \mathbb{Z}^d$, such that $\|cz + b\|^2 \leqslant M$.*

Proof. Let z be a core point with $z \notin \mathrm{Fix}(G)$. By Lemma 5.7, there is $c \in C$ such that $\|cz_\alpha\|^2 \leqslant D\|cz_\beta\|^2$ for all $\alpha, \beta \in \Gamma$, where D is some constant depending only on G, not on z.

Since $y = cz$ is also a core point (Lemma 2.5), Theorem 5.8 yields that there is a $\beta \in \Gamma$ with $\|y_\beta\|^2 \leqslant C$. It follows that the squared norms of the other projections y_α are bounded by CD. Thus

$$\|y|_{\mathrm{Fix}(G)^\perp}\|^2 \leqslant C + (|\Gamma| - 1)CD$$

is bounded.

Since the projection to the fixed space can be bounded by translating with some $b \in \mathrm{Fix}(G) \cap \mathbb{Z}^d$, the theorem follows. □

5.10 Example. Let p be a prime and let $G = C_p \leqslant \mathrm{S}_p$ be generated by a p-cycle. Then G is a QI-group. (Of course, every transitive group of prime degree is a QI-group.) For p odd, $\mathbb{R}^p$ decomposes into $\mathrm{Fix}(G)$ and $(p-1)/2$ irreducible subspaces of dimension 2. Here the lattice can be identified with the group ring $\mathbb{Z}G$, and thus $\mathbf{C}_{\mathrm{GL}(p,\mathbb{Z})}(G) \cong \mathbf{U}(\mathbb{Z}G)$. The torsion free part of this unit group is a free abelian group of rank $(p-3)/2$.

Let us see what constant we can derive for $p = 5$. For concreteness, let $g = (1,2,3,4,5)$ and $G = \langle g \rangle$. We have the decomposition

$$\mathbb{R}^5 = \mathrm{Fix}(G) \oplus W \oplus W'.$$

The projections from $\mathbb{R}^5$ onto W and W' are given by

$$e_W = \frac{1}{5}(2 + ag + bg^2 + bg^3 + ag^4), \qquad a = \frac{-1+\sqrt{5}}{2},$$
$$e_{W'} = \frac{1}{5}(2 + bg + ag^2 + ag^3 + bg^4), \qquad b = \frac{-1-\sqrt{5}}{2}.$$

The centralizer of G has the form

$$\mathbf{C}_{\mathrm{GL}(5,\mathbb{Z})}(G) = \{\pm I\} \times G \times \langle u \rangle,$$

where u is a unit of infinite order. Here we can choose $u = -1 + g + g^4$ with inverse $-1 + g^2 + g^3$. To u corresponds the matrix

$$\begin{pmatrix} -1 & 1 & 0 & 0 & 1 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 1 \\ 1 & 0 & 0 & 1 & -1 \end{pmatrix} \in \mathrm{GL}(5,\mathbb{Z}). \tag{1}$$

This unit acts on W as $-1 + a$ and on W' as $-1 + b$. For the constant D of Lemma 5.7, we get $D = (b-1)^2 = 2 - 3b = (7 + 3\sqrt{5})/2$. For the constant C in Theorem 5.8, we get a bound $C = 48/5$ (from the proof). We can conclude that every core point is equivalent to one with squared norm smaller than $M = (2/5) + (48/5)(1 + 2 - 3b) \approx 50.6$.

We can get somewhat better bounds by applying Theorem 5.8 "layer-wise". The k-layer is, by definition, the set of all $z \in \mathbb{Z}^d$ with $\sum z_i = k$. In our example, every lattice point is equivalent to one in layer 1 or layer 2.

For example, it can be shown that each core point in the 1-layer is equivalent to a point z with $\|z\|^2 \leqslant 31$. However, this bound is still far from optimal. Using the computer algebra system `GAP` [7], we found that the only core points of C_5 in the 1-layer up to normalizer equivalence are just

$$(1,0,0,0,0)^t, \quad (1,1,0,0,-1)^t, \quad (1,1,1,0,-2)^t,$$
$$(2,1,0,-1,-1)^t, \quad (2,1,-2,0,0)^t.$$

(The normalizer $\mathbf{N}_{\mathrm{GL}(5,\mathbb{Z})}(G)$ is generated by the centralizer and the permutation matrix corresponding to the permutation $(2,3,5,4)$.) For completeness, we also give a list of core points up to normalizer equivalence in the 2-layer:

$$(1,1,0,0,0)^t, \quad (1,1,1,0,-1)^t, \quad (2,1,0,0,-1)^t,$$
$$(2,1,1,-1,-1)^t, \quad (2,1,1,-2,0)^t.$$

Every core point for C_5 is normalizer equivalent to exactly one of these ten core points.

For this example, an infinite series of core points of the form

$$(f_{j+1}, 0, f_j, f_j, 0)^t,$$

where f_j is the j-th Fibonacci number, was found by Thomas Rehn [20, Section 5.2.2]. Each point in this series is equivalent to one of the two obvious core points $(1,0,0,0,0)^t$ and $(1,0,1,1,0)^t$. This follows from

$$(1 - g - g^4)(f_{j+1}, 0, f_j, f_j, 0)^t = (f_{j+1}, -f_{j+2}, 0, 0, -f_{j+2})^t$$

and thus

$$(1 - g - g^4)(f_{j+1}, 0, f_j, f_j, 0)^t + f_{j+2}(1,1,1,1,1)^t \\ = (f_{j+3}, 0, f_{j+2}, f_{j+2}, 0)^t.$$

5.11 Example. Now set

$$G = \langle (1,2,3,4,5),\ (1,4)(2,3) \rangle \cong D_5,$$

the dihedral group of order 10. Then

$$C_{\mathrm{GL}(5,\mathbb{Z})}(G) = \{\pm I\}\langle u \rangle,$$

where u is as in the previous example. The normalizer of G is the same as that of the cyclic group $C_5 = \langle (1,2,3,4,5) \rangle$. In particular, normalizer equivalence for D_5 and C_5 is the same equivalence relation. Of the core points from the last example, only $(1,0,0,0,0)^t$ and $(1,1,0,0,0)^t$ are also core points for D_5. (In fact, for most of the other points, we have some lattice point on an interval between two vertices, for example $(1,0,0,0,0)^t = (1/2)\big((1,1,0,0,-1)^t + (2,5)(3,4)(1,1,0,0,-1)^t\big)$. Thus there are only two core points up to normalizer equivalence in this example.

5.12 Remark. The number of core points up to normalizer equivalence seems to grow fast for cyclic groups of prime order. For $p = 7$, we get 515 core points up to normalizer equivalence.

Herr, Rehn and Schürmann [10] conjectured that a finite transitive permutation group G has infinitely many core points up to translation equivalence if the group is not 2-homogeneous. It is known that a permutation group $G \leqslant \mathrm{S}_d$ is 2-homogeneous if and only if $\mathrm{Fix}_{\mathbb{R}^d}(G)^\perp$ is irreducible [4, Lemma 2(iii)]. In this case, there are only finitely many core points up to translation equivalence [10, Corollary 10].

We propose the following conjecture, which is the converse of Theorem 5.1:

5.13 Conjecture. Let $G \leqslant \mathrm{S}_d$ be a transitive permutation group such that $\mathrm{Fix}(G)^\perp$ contains a rational G-invariant subspace other than $\{0\}$ and $\mathrm{Fix}(G)^\perp$ itself. Then there are infinitely many core points up to normalizer equivalence.

This can be seen as a generalization of the Herr-Rehn-Schürmann conjecture, since translation equivalence refines normalizer equivalence, and since whenever $\mathrm{Fix}(G)^\perp$ contains a nontrivial irrational G-invariant subspace, then there are infinitely many core points up to translation equivalence by Theorem 4.1 (or [10, Theorem 32]).

6. Application to integer linear optimization

In this last section we describe a possible application of our theory to symmetric integer linear optimization problems. For many years it has been known that symmetry leads often to difficult problem instances in integer optimization. Standard approaches like branching usually work particularly poorly when large symmetry groups are present. Although in the past decade a few methods to use symmetry for certain special classes of problems have been suggested, we are still far from a good general strategy to deal with problem symmetries (see the surveys by Margot [17] and Pfetsch and Rehn [19] for an overview). The core point concept is a geometric approach that allows in principle to reduce a given symmetric problem to a subset of integer vectors – the core points of the problem [9].

A general standard form of an integer linear optimization problem is

$$\max c^t x \quad \text{such that} \quad Ax \leqslant b,\ x \in \mathbb{Z}^d, \tag{2}$$

for some given matrix A and vectors b and c, all of them usually rational. If $c = 0$, then we have a so-called *feasibility problem*, asking simply whether or not there is an integral solution to a given system of linear inequalities. Geometrically, we are asking whether some polyhedral set (usually a polytope) contains an integral point.

A group $G \leqslant \mathrm{GL}(d, \mathbb{Z})$ is called a *group of symmetries* of problem (2) if the constraints $Ax \leqslant b$ and the linear utility function $c^t x$ are invariant under the action of G on $\mathbb{R}^d$, that is, if $c^t(gx) = c^t x$ and $A(gx) \leqslant b$ for all $g \in G$ whenever $Ax \leqslant b$. The first condition is for instance satisfied if c is in the fixed space $\mathrm{Fix}(G)$. Practically, computing a group of symmetries for a given problem is usually reduced to the problem of finding symmetries of a suitable colored graph [3, 19]. Quite often in optimization, the attention is restricted to groups $G \leqslant \mathrm{S}_d$ acting on $\mathbb{R}^d$ by permuting coordinates.

Knowing the core points of a symmetry group G allows to restrict the search for optima of any G-invariant problem (2) to this subset of $\mathbb{Z}^d$ [9]. There are many possible ways how core points could be used. For instance, one could use the

fact that core points are near invariant subspaces, by adding additional quadratic constraints (SDP-constraints). In the case of QI-groups, hence with finitely many core points up to normalizer equivalence, one could try to systematically run through core points x satisfying the constraint $Ax \leqslant b$. Here we want to describe a different approach that opens the possibility of obtaining an equivalent, but easier reformulation of a G-invariant problem (2).

Generally, a linear reformulation of a problem as in (2) can be obtained by an integral linear substitution $x \mapsto Sx$ for some matrix $S \in \mathrm{GL}(d, \mathbb{Z})$:

$$\max(c^t S)x \quad \text{such that} \quad (AS)x \leqslant b,\ x \in \mathbb{Z}^d. \tag{3}$$

We remark that reformulations as in (3) with a matrix $S \in \mathrm{GL}(d, \mathbb{Z})$ can of course be applied to any linear integer optimization problem. In fact, this is a key idea of Lenstra's famous polynomial time algorithm in fixed dimension d [15]. In Lenstra's algorithm, the transformation matrix S is chosen to correspond to a suitable LLL-reduction of the lattice, such that the transformed polyhedral set $\{x \in \mathbb{R}^d \mid (AS)x \leqslant b\}$ is sufficiently round. This idea has successfully been used for different problem classes of integer linear optimization problems (for an overview see [1]).

When we know that the optimization problem admits a group G as symmetry group, it seems natural to try to transform the problem with matrices S from the centralizer or normalizer of G. Note that when S is an element of the normalizer $\mathbf{N}_{\mathrm{GL}(d,\mathbb{Z})}(G)$, the problem (2) is G-invariant if and only if (3) is G-invariant. Note also that then $(c^t S)^t$ is in $\mathrm{Fix}(G)$.

We illustrate the idea with a small concrete problem instance of (2) which is invariant under the cyclic group C_5. In particular, we construct C_5-invariant integral optimization problems that are quite hard or even impossible to solve for state-of-the-art commercial solvers like `CPLEX` or `GUROBI`. For instance, this is often the case when the constraints $Ax \leqslant b$ can be satisfied by real vectors x, but not by integral ones.

6.1 Example. We use core points to construct infeasible integral optimization problems. The orbit polytope $P(C_5, z)$ of some integral point z has a description with linear inequalities of the form $x_1 + \ldots + x_5 = k$ and $Ax \leqslant b$, where A is a circulant 5×5-matrix

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_1 \\ a_3 & a_4 & a_5 & a_1 & a_2 \\ a_4 & a_5 & a_1 & a_2 & a_3 \\ a_5 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$$

with integral entries $a_1, \ldots, a_5$, and $b \in \mathbb{Z}^5$ satisfies $b_1 = \ldots = b_5$. If z is a core

point and if we replace b_i by $b'_i := b_i - 1$, then we get a system of inequalities having no integral solution.

Applying this construction to the core point

$$z = U^{10} \cdot (1, 1, 1, 0, -2)^t,$$

where U is the matrix from (1) in Example 5.10, we get parameters

$$\begin{aligned} a_1 &= 515161, & a_2 &= 18376, & a_3 &= -503804, \\ a_4 &= -329744, & a_5 &= 300011, & b'_1 &= 60. \end{aligned}$$

We can vary the values of $k \equiv 1 \mod 5$ (geometrically, this corresponds to translating the polytope by some integral multiple of the all-one-vector). This gives a series of problem instances on which the commercial solvers very often not finish within a time limit of 10000 seconds on a usual desktop computer. For $k = 1$, which seems computationally the easiest case, a solution always still takes more than 4000 seconds.

However, knowing that a given problem as the above is C_5-invariant, we can try to find an easier reformulation (3) by using matrices from the centralizer. As a rule of thumb, we assume that a transformed problem with smaller coefficients is "easier". Here, the torsion free part of the centralizer is generated by the matrix U from (1) in Example 5.10, and so the only possibilities for S are U or U^{-1}. (A matrix of finite order will probably not simplify a problem significantly.) Here, applying $S = U$ yields an easier problem, and one quickly finds that after applying S ten times, the problem is not simplified further by applying U (or U^{-1}). In other words, we transform the original problem instance with U^{10}. This yields an equivalent C_5-invariant feasibility problem, which is basically instantly solved by the commercial solvers (finding that there is no integral solution).

As far as we know, this approach is in particular by far better than any previously known one that uses the symmetries of a cyclic group. One standard approach is for example to add symmetry-breaking inequalities $x_1 \leqslant x_2, \ldots, x_1 \leqslant x_5$. This yields an improved performance in some cases, but is far from the order of computational gain that is possible with our proposed reformulations.

For a general QI-group $G \leqslant \mathrm{S}_d$, we can try a similar approach. The idea is that for QI-groups, it should be possible with matrices from the centralizer to make the feasible region sufficiently round. (By Lemma 5.7, for any vector $x \in \mathbb{R}^d$, there is an element $S \in \mathbf{C}_{\mathrm{GL}(d,\mathbb{Z})}(G)$ such that the projections of Sx to the different G-invariant subspaces have approximately the same norm. This means that the orbit polytope of Sx is "round".)

Our approach is particularly straightforward when the torsion free part of the centralizer $\mathbf{C}_{\mathrm{GL}(d,\mathbb{Z})}(G)$ has just rank 1, as in the example with $G = C_5$ above.

When the centralizer contains a free abelian group of some larger rank, then it is less clear how to reduce the problem efficiently. A possible heuristics is as follows: Recall that in Lemma 5.5, we described a map L which maps the centralizer, and thus its torsion-free part of rank r (say), onto a certain lattice in $\mathbb{R}^{r+1}$. The idea is to choose some set of matrices from the centralizer that corresponds to a reduced basis of that lattice, or "small" combinations of such a basis. Then we just transform the problem step by step with matrices from this finite set, until no further improvements are possible. For a thorough evaluation of this approach, further investigations are necessary.

References for Chapter V

1. Karen Aardal and Friedrich Eisenbrand. Integer programming, lattices, and results in fixed dimension. In: *Discrete Optimization*. Ed. by K. Aardal, G. L. Nemhauser, and R. Weismantel. Handbooks in Operations Research and Management Science 12. Elsevier, Amsterdam, 2005. Chap. 4, pp. 171–243. DOI: 10.1016/S0927-0507(05)12004-0. MR2265415, Zbl. 1172.90445 (cited on p. 133).
2. Oliver Braun, Renaud Coulangeon, Gabriele Nebe, and Sebastian Schönnenbeck. Computing in arithmetic groups with Voronoï's algorithm. *J. Algebra* **435** (2015), pp. 263–285. DOI: 10.1016/j.jalgebra.2015.01.022. MR3343219, Zbl. 1323.16014 (cited on p. 120).
3. David Bremner, Mathieu Dutour Sikirić, Dmitrii V. Pasechnik, Thomas Rehn, and Achill Schürmann. Computing symmetry groups of polyhedra. *LMS J. Comput. Math.* **17**, no. 1 (2014), pp. 565–581. DOI: 10.1112/S1461157014000400, arXiv: 1210.0206 [math.CO]. MR3356046, Zbl. 1351.52009 (cited on p. 132).
4. Peter J. Cameron. Bounding the rank of certain permutation groups. *Math. Z.* **124**, no. 4 (1972), pp. 343–352. DOI: 10.1007/BF01113925. MR0294471(45#3541), Zbl. 0238.20008 (cited on p. 131).
5. John D. Dixon. Permutation representations and rational irreducibility. *Bull. Austral. Math. Soc.* **71**, no. 3 (2005), pp. 493–503. DOI: 10.1017/S0004972700038508. MR2150939(2006c:20012), Zbl. 1114.20003 (cited on pp. 124, 125).
6. Paolo Faccin, Willem A. de Graaf, and Wilhelm Plesken. Computing generators of the unit group of an integral abelian group ring. *J. Algebra* **373** (2013), pp. 441–452. DOI: 10.1016/j.jalgebra.2012.09.031. MR2995037, Zbl. 1271.16038 (cited on p. 120).
7. *GAP – Groups, Algorithms, and Programming*. Version 4.8.6. The GAP Group. 2016. URL: http://www.gap-system.org (visited on 2017-03-02) (cited on p. 130).
8. Katrin Herr. *Core Sets and Symmetric Convex Optimization*. Dissertation. Technische Universität Darmstadt, 2013. Zbl. 1291.90002 (cited on p. 118).
9. Katrin Herr, Thomas Rehn, and Achill Schürmann. Exploiting symmetry in integer convex optimization using core points. *Oper. Res. Lett.* **41**, no. 3 (2013), pp. 298–

304. DOI: 10.1016/j.orl.2013.02.007. MR3048847, Zbl. 1286.90097 (cited on pp. 115, 117, 132).

10. Katrin Herr, Thomas Rehn, and Achill Schürmann. On lattice-free orbit polytopes. *Discrete Comput. Geom.* **53**, no. 1 (2015), pp. 144–172. DOI: 10.1007/s00454-014-9638-x. MR3293492, Zbl. 1325.52010 (cited on pp. 116–118, 121, 123, 124, 129, 131, 132).
11. Klaus Hoechsmann. Constructing units in commutative group rings. *Manuscripta Math.* **75**, no. 1 (1992), pp. 5–23. DOI: 10.1007/BF02567067. MR1156211, Zbl. 0773.16016 (cited on p. 120).
12. I. Martin Isaacs. *Finite Group Theory*. Graduate Studies in Mathematics 92. American Mathematical Society, Providence, RI, 2008. DOI: 10.1090/gsm/092. MR2426855(2009e:20029), Zbl. 1169.20001 (cited on p. 119).
13. Ernst Kleinert. Units of classical orders: a survey. *Enseign. Math. (2)* **40**, no. 3-4 (1994), pp. 205–248. DOI: 10.5169/seals-61112. MR1309127(95k:11151), Zbl. 0846.16027 (cited on pp. 120, 122).
14. T[sit] Y[uen] Lam. *A First Course in Noncommutative Rings*. Graduate Texts in Mathematics 131. Springer, New York, Berlin, and Heidelberg, 2nd ed. 2001. DOI: 10.1007/978-1-4419-8616-0. MR1838439(2002c:16001), Zbl. 0980.16001 (cited on pp. 121–123).
15. H. W. Lenstra Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.* **8**, no. 4 (1983), pp. 538–548. DOI: 10.1287/moor.8.4.538. MR727410, Zbl. 0524.90067 (cited on p. 133).
16. Zbigniew Marciniak and Sudarshan K. Sehgal. Generic units in abelian group rings. *J. Group Theory* **8**, no. 6 (2005), pp. 777–799. DOI: 10.1515/jgth.2005.8.6.777. MR2179670, Zbl. 1087.16018 (cited on p. 120).
17. François Margot. Symmetry in integer linear programming. In: *50 Years of Integer Programming 1958-2008. From the Early Years to the State-of-the-art*. Ed. by Michael Jünger et al. Springer, Berlin, 2010. Chap. 17, pp. 647–686. DOI: 10.1007/978-3-540-68279-0_17. MR2640549, Zbl. 1187.90200 (cited on p. 132).
18. Jürgen Neukirch. *Algebraische Zahlentheorie*. (German). Springer, Berlin and Heidelberg, Reprint of the 1992 original 2007. DOI: 10.1007/978-3-540-37663-7. Zbl. 1131.11002. English translation available (Springer 1999) (cited on p. 127).
19. Marc Pfetsch and Thomas Rehn. A computational comparison of symmetry handling methods for mixed integer programs. (Preprint). 2015. URL: http://www.optimization-online.org/DB_HTML/2015/11/5209.html (visited on 2017-02-24) (cited on p. 132).
20. Thomas Rehn. *Exploring Core Points for Fun and Profit. A study of lattice-free orbit polytopes*. Dissertation. Universität Rostock, 2013. urn:nbn:de:gbv:28-diss2014-0082-2 (cited on pp. 116, 118, 121, 131).
21. Irving Reiner. *Maximal Orders*. L.M.S. Monographs 5. Academic Press, London and New York, 1975. MR0393100(52#13910), Zbl. 0305.16001 (cited on pp. 119, 120).

22. Jean-Pierre Serre. *Linear Representations of Finite Groups*. Trans. from the French by Leonard Scott. Graduate Texts in Mathematics 42. Springer, New York, Heidelberg, and Berlin, 1977. DOI: 10.1007/978-1-4684-9458-7. MR0450380(56#8675), Zbl. 0355.20006 (cited on p. 125).

Chapter VI.

Uniqueness of the Birkhoff Polytope[1]

Barbara Baumeister and Frieder Ladisch

Abstract. The Birkhoff polytope B_n is the convex hull of all $n \times n$ permutation matrices in $\mathbb{R}^{n\times n}$. We compute the combinatorial symmetry group of the Birkhoff polytope.

A representation polytope is the convex hull of some finite matrix group $G \leqslant \mathrm{GL}(d, \mathbb{R})$. We show that the group of permutation matrices is essentially the only finite matrix group which yields a representation polytope with the same face lattice as the Birkhoff polytope.

2010 Mathematics Subject Classification. Primary 52B15, Secondary 05E18, 20B25, 20C15, 52B05, 52B12

Keywords. Birkhoff polytope, representation polytope, permutation polytope, combinatorial symmetry

1. Introduction

Let $P\colon G = S_n \to \mathrm{GL}(n, \mathbb{R})$ be the standard permutation representation of the symmetric group S_n on n letters. The *Birkhoff polytope* B_n is by definition the convex hull of all permutation matrices of size $n \times n$:

$$B_n := \mathrm{conv}\{P(\sigma) \mid \sigma \in S_n\}.$$

In this note, we prove a conjecture of Baumeister, Haase, Nill and Paffenholz [2, Conjecture 5.3] on the uniqueness of the Birkhoff polytope among permutation polytopes. In fact, we prove a slightly stronger result.

To state the result, we need the following notation. Let $D\colon G \to \mathrm{GL}(d, \mathbb{R})$ be a representation over the reals. The corresponding *representation polytope*, $P(D)$, is the convex hull of the image of D:

$$P(D) := \mathrm{conv}\{D(g) \mid g \in G\}.$$

If D is a permutation representation, then the representation polytope is called a *permutation polytope*.

[1] arXiv: 1610.02077v2 [math.CO]. To appear in *Algebraic Combinatorics*.

Two representations $D_i\colon G_i \to \mathrm{GL}(d_i, \mathbb{R})$ (where $i = 1, 2$) are called *effectively equivalent* if there is a group isomorphism $\varphi\colon G_1 \to G_2$ such that D_1 and $D_2 \circ \varphi$ are *stably equivalent*, which means that D_1 and $D_2 \circ \varphi$ have the same nontrivial irreducible constituents (not necessarily occuring with the same multiplicities). The representation polytopes of effectively representations are affinely isomorphic [1, Theorem 2.4] [2, § 2]. The converse is not true, for example, when D is the regular representation of a group, then $P(D)$ is a simplex of dimension $|G| - 1$. Thus groups that are not even isomorphic as abstract groups, may yield affinely equivalent representation polytopes.

From this viewpoint, the next result is somewhat surprising. Recall that two polytopes P and Q are *combinatorially equivalent* if there is a bijection between the vertices of P and the vertices of Q which maps faces of P onto faces of Q. Affinely equivalent polytopes are combinatorially equivalent, but not conversely.

Theorem A. *Let $D\colon G \to \mathrm{GL}(d, \mathbb{R})$ be a faithful representation such that the representation polytope $P(D)$ is combinatorially equivalent to the Birkhoff polytope B_n. Then either $n = 3$ and G is cyclic of order 6, or D and the standard permutation representation $P\colon S_n \to \mathrm{GL}(n, \mathbb{R})$ are effectively equivalent (in particular, $G \cong S_n$).*

In the exceptional case $n = 3$ and G cyclic, it is easy to see that D is not stably equivalent to a permutation representation. It follows also from the classification of permutation polytopes in small dimensions [2, Theorem 4.1] that B_3 is not combinatorially equivalent to any other permutation polytope. In particular, Theorem A answers [2, Conjecture 5.3] in the positive.

To prove Theorem A, we use the determination of the combinatorial symmetry group of the Birkhoff polytope, which may be of interest in its own right:

Theorem B. *For every combinatorial symmetry α of the Birkhoff polytope there are $\sigma, \tau \in S_n$ and $\varepsilon \in \{\pm 1\}$ such that $\alpha(\pi) = \sigma\pi^{\varepsilon}\tau$ for all $\pi \in S_n$. Every combinatorial symmetry comes from an isometry of the space of $n \times n$ matrices over $\mathbb{R}$.*

As we will explain below, this means that for $n \geqslant 3$, the combinatorial symmetry group of the Birkhoff polytope is isomorphic to the wreath product $S_n \wr C_2 = (S_n \times S_n) \rtimes C_2$.

Although not difficult, this result seems not to be in the literature yet. There are, however, two different published proofs that the above maps are all the linear maps preserving the Birkhoff polytope [7, 8]. Since every linear or affine symmetry of a polytope induces a combinatorial symmetry, Theorem B is actually stronger than the old result. As one would expect, our proof of Theorem B depends on the well known description of the facets and thus the combinatorial structure of the Birkhoff polytope. On the other hand, the combinatorial structure of representation and permutation polytopes in general can be quite complicated, even for cyclic groups, as examples show [3].

2. Preliminaries on permutation actions on a group

Let G be a finite group. For each $g \in G$, let $\lambda_g \in \operatorname{Sym} G$ be left multiplication with g (so $\lambda_g(x) = gx$), and ϱ_g be right multiplication with g^{-1}, that is, $\varrho_g(x) = xg^{-1}$. Thus $g \mapsto \lambda_g$ and $g \mapsto \varrho_g$ are the left and right regular permutation action. Also, let $\iota \in \operatorname{Sym} G$ be the map that inverts elements (so $\iota(x) = x^{-1}$ for all $x \in G$). Let $\Gamma(G) \leqslant \operatorname{Sym} G$ be the group generated by all these elements:

$$\Gamma(G) := \langle \lambda_g, \varrho_g, \iota \mid g \in G \rangle.$$

To describe $\Gamma(G)$, we need the *wreath product* $G \wr C_2$ of G with a cyclic group $C_2 = \langle s \rangle$ of order 2. Recall that this is the semidirect product of $G \times G$ with C_2, where s acts on $G \times G$ by exchanging coordinates: $(g, h)^s = (h, g)$ for g, $h \in G$. Then:

2.1 Lemma. *If G is not an elementary abelian 2-group, then $\Gamma(G) \cong (G \wr C_2)/Z$, where $Z = \{(z, z) \in G \times G \mid z \in \mathbf{Z}(G)\}$.*

Proof. We have that $\lambda(G)$ and $\varrho(G)$ centralize each other, and $(\lambda_g)^\iota = \varrho_g$. Thus sending $(g, h) \in G \times G$ to $\lambda_g \varrho_h$ and $s \in C_2 = \{1, s\}$ to ι defines a surjective group homomorphism $G \wr C_2 \to \Gamma(G)$ with Z in the kernel.

Suppose $\lambda_g \varrho_h = \mathrm{id}_G$. Then $gxh^{-1} = x$ for all $x \in G$. Taking $x = 1$ yields $g = h$, and it follows that $g \in \mathbf{Z}(G)$.

Now assume $\lambda_g \varrho_h \iota = \mathrm{id}$. Then $gx^{-1}h^{-1} = x$ for all $x \in G$, and $x = 1$ yields $g = h$. Moreover, we have $xy = g(xy)^{-1}g^{-1} = gy^{-1}g^{-1}\, gx^{-1}g^{-1} = yx$ for all x, $y \in G$. Thus G must be abelian in this case, and $x^{-1} = x$ for all $x \in G$.

So when G is not an elementary abelian 2-group, such an element can not be in the kernel of the action of $G \wr C_2$ on G. This shows the result. □

In the proof of Theorem A, we need the fact that $\Gamma(G)$ contains no pair of commuting, regular subgroups other than $\lambda(G)$ and $\varrho(G)$, when $G = S_n$ and $n \geqslant 4$. The exception in Theorem A for $n = 3$ comes from the fact that in $\Gamma(S_3)$, we have other pairs of commuting, regular subgroups, namely $U = V = C_2 \times C_3$ and $U = V = C_3 \times C_2$. Notice that we do not assume that the commuting, regular subgroups U, V of $\Gamma(G)$ have trivial intersection. If one assumes $U \cap V = 1$, one can give a somewhat shorter proof that $\{U, V\} = \{\lambda(G), \varrho(G)\}$ for almost simple groups G, but we need the stronger statement for the proof of Theorem A.

The most elegant and elementary way to prove that $\lambda(G)$ and $\varrho(G)$ form the only pair of commuting regular subgroups of $\Gamma(G)$ (when $G = S_n$, $n \geqslant 4$), seems to be to use a general argument due to Chermak and Delgado [4]. Let G be an arbitrary finite group. Following Isaacs [6, § 1G], we call $m_G(H) := |H||\mathbf{C}_G(H)|$ the *Chermak-Delgado measure* of the subgroup $H \leqslant G$.

2.2 Lemma. *[6, Theorem 1.44] Let G be a finite group and let $\mathcal{L} = \mathcal{L}(G)$ be the set of subgroups for which the Chermak-Delgado measure is as large as possible. Then for H, $K \in \mathcal{L}$, we have $H \cap K \in \mathcal{L}$, $\langle H, K\rangle = HK = KH \in \mathcal{L}$, and $\mathbf{C}_G(H) \in \mathcal{L}$.*

The *Chermak-Delgado lattice* of G is by definition the set of all subgroups of G for which the Chermak-Delgado measure is maximized. The last result tells us that this is indeed a sublattice of the lattice of all subgroups of G. We need the following, which is probably well known:

2.3 Corollary. *Any member of the Chermak-Delgado lattice of a finite group G is subnormal in G.*

Proof. If H is a member of the Chermak-Delgado lattice of G, then any conjugate H^g is also in the Chermak-Delgado lattice, and so $HH^g = H^gH$ by Lemma 2.2. But subgroups $H \leqslant G$ with $HH^g = H^gH$ for all $g \in G$ are subnormal [6, Theorem 2.8]. □

2.4 Lemma. *Suppose that G is almost simple (that is, G has a nonabelian simple socle). Then $|U||\mathbf{C}_G(U)| \leqslant |G|$ for any subgroup $U \leqslant G$, and equality holds if and only if $U = \{1\}$ or $U = G$. In particular, this holds for $G = S_n$, $n \geqslant 5$. The conclusion is also true for $G = S_4$.*

Proof. Suppose that $1 \neq H$ is a member of the Chermak-Delgado lattice. Then H is subnormal and thus contains the nonabelian simple socle of G. It follows that $\mathbf{Z}(H) = 1 = H \cap \mathbf{C}_G(H)$. Since $\mathbf{C}_G(H)$ is also a member of the Chermak-Delgado lattice, we must have $\mathbf{C}_G(H) = 1$. Since $|H||\mathbf{C}_G(H)| = |H| \leqslant |G|$ was supposed to be maximal possible, we see that $H = G$. Thus the Chermak-Delgado lattice contains exactly the groups 1 and G itself, and the first assertion follows. The case $G = S_4$ is a simple verification. □

We will need the following application (for $G = S_n$):

2.5 Lemma. *Let G be a group such that the Chermak-Delgado lattice of G contains exactly the groups 1 and G. Then $\lambda(G)$, $\varrho(G)$ is the only pair of commuting, regular subgroups of $\Gamma(G)$.*

Proof. Notice that $\mathbf{Z}(G) = \{1\}$, since otherwise $m_G(\mathbf{Z}(G)) = |\mathbf{Z}(G)||G| > |G| = m_G(1)$. Thus $\Gamma(G) \cong G \wr C_2$ and $\lambda(G)\varrho(G) \cong G \times G$.

We first show that a regular subgroup U of $\Gamma(G)$ is contained in the normal subgroup $\lambda(G)\varrho(G)$. Otherwise, U contains an element $u = \lambda_g\varrho_h\iota$ sending $x \in G$ to $gx^{-1}h^{-1}$. Then u^2 sends x to $ghxg^{-1}h^{-1}$, and in particular fixes g. By regularity, we must have $u^2 = \mathrm{id}_G$. This implies $gh = hg$ and $gh \in \mathbf{Z}(G) = \{1\}$. Thus u sends x to $gx^{-1}g$, and so fixes g, too, which contradicts the regularity. This shows that $U \leqslant \lambda(G)\varrho(G)$.

Since $\lambda(G)\varrho(G) \cong G \times G$, we may work in $G \times G$ from now on. Suppose that U and $V \leqslant G \times G$ both have size $|G|$, and commute with each other. Let U_L be the projection of U onto the first component, that is, the subgroup of elements $g \in G$ such that there is an $h \in G$ with $(g, h) \in U$. Let U_R be the projection of U on the second component. With this notation, $\mathbf{C}_{G\times G}(U) = \mathbf{C}_G(U_L) \times \mathbf{C}_G(U_R)$. Thus

$$|G|^2 = |U||V| \leqslant |U_L||U_R||\mathbf{C}_G(U_L)||\mathbf{C}_G(U_R)| \leqslant |G|^2,$$

where the last inequality follows from our assumption on the Chermak-Delgado lattice of G. Thus equality holds, and it follows also that U_L and U_R are trivial or the group G itself. Since both U and V have size $|G|$, it follows that $\{U, V\} = \{G \times 1, 1 \times G\}$. □

2.6 Corollary. *Let G be a group such that the Chermak-Delgado lattice of G contains exactly the groups 1 and G. Then $\mathbf{N}_{\mathrm{Sym}\, G}(\Gamma(G)) = (\mathrm{Aut}\, G)\Gamma(G)$.*

Proof. Let $\pi \in \mathbf{N}_{\mathrm{Sym}\, G}(\Gamma(G))$. Then $\lambda(G)^\pi$ and $\varrho(G)^\pi$ are commuting regular subgroups of $\Gamma(G)$, and thus $\{\lambda(G)^\pi, \varrho(G)^\pi\} = \{\lambda(G), \varrho(G)\}$. Since $\lambda(G)$ and $\varrho(G)$ are conjugate in $\Gamma(G)$, we may assume that $\lambda(G)^\pi = \lambda(G)$. Thus $\pi\lambda_g\pi^{-1} = \lambda_{\alpha g}$ for some bijection $\alpha\colon G \to G$. Clearly, α is a group automorphism.

As $\lambda(G)$ acts transitively on G, we may assume $\pi(1) = 1$. But then $\pi(g) = \pi\lambda_g\pi^{-1}(1) = \lambda_{\alpha g}(1) = \alpha(g)$, so $\pi \in \mathrm{Aut}\, G$. □

The conclusion of this corollary is also true for some other groups (for example, $G = S_3$), but not for all groups (for example, $G = S_3 \times S_3$).

3. The combinatorial symmetry group of the Birkhoff polytope

Let $D\colon G \to \mathrm{GL}(d, \mathbb{R})$ be a faithful representation and let $P(D) = \mathrm{conv}\{D(g) \mid g \in G\}$ be the corresponding representation polytope. Then the vertices of $P(D)$ correspond to the elements of G. We may thus view the affine and combinatorial symmetries as permutations of G itself.

3.1 Lemma. *Let $D\colon G \to \mathrm{GL}(d, \mathbb{R})$ be a faithful representation and $P(D)$ the representation polytope. Then the affine symmetry group $\mathrm{AGL}(P(D))$ as permutation group on G contains $\Gamma(G)$ as defined in the last section.*

Proof. The left multiplications λ_g are realized by left multiplication with $D(g)$, and the right multiplications ϱ_g by right multiplication with $D(g)^{-1}$. If D is an orthogonal representation, then the permutation $g \mapsto g^{-1}$ is realized by transposing matrices, sending $D(g)$ to $D(g)^t = D(g^{-1})$. The general case (which we will not need) can be reduced to the orthogonal case [FL1, Prop. 6.4][2]. □

[2] see Proposition 6.4 in Chapter II of this thesis

Now let $P\colon G = S_n \to \mathrm{GL}(n, \mathbb{R})$ be the standard permutation representation of the symmetric group S_n, and let

$$B_n := \mathrm{conv}\{P(\sigma) \mid \sigma \in S_n\}$$

be the Birkhoff polytope. Theorem B claims that $\Gamma(S_n)$ is the combinatorial symmetry group of B_n. (The second claim of Theorem B is that these symmetries come from isometries of the matrix space. This is then clear, since the symmetries in $\Gamma(S_n)$ even act by permuting coordinates of the matrices.)

Proof of Theorem B. Recall that the Birkhoff polytope consists of the doubly stochastic matrices [9, Corollary 1.4.14]. In particular, for each index pair (i, j), the equality $a_{ij} = 0$ describes a facet of the Birkhoff polytope. Thus its facets, as subsets of S_n, are given by the n^2 subsets

$$F_{ij} = \{\pi \in S_n \mid \pi(i) \neq j\}, \quad i, j = 1, \ldots, n.$$

It will be more convenient to work with the complements

$$A_{ij} = S_n \setminus F_{ij} = \{\pi \in S_n \mid \pi(i) = j\}$$

of the facets. For σ, $\tau \in S_n$, we have $\sigma A_{ij} \tau^{-1} = A_{\tau i, \sigma j}$. We also have $A_{ij}^{-1} := \{\pi^{-1} \mid \pi \in A_{ij}\} = A_{ji}$. Moreover, for i, j, k and l in $\{1, \ldots, n\}$ we have

$$|A_{ij} \cap A_{kl}| = \begin{cases} (n-1)!, & \text{if } i = k, j = l, \\ 0 & \text{if } i = k, j \neq l, \\ 0 & \text{if } i \neq k, j = l, \\ (n-2)! & \text{otherwise.} \end{cases}$$

Any combinatorial symmetry α permutes the facets and thus the sets A_{ij}, and preserves cardinalities of their intersections.

Let $\alpha\colon S_n \to S_n$ be an arbitrary combinatorial symmetry of the Birkhoff polytope. We have to show that $\alpha \in \Gamma(S_n)$, the group containing the maps $\pi \mapsto \sigma\pi^{\pm 1}\tau^{-1}$. After replacing α by $\gamma \circ \alpha$ for some $\gamma \in \Gamma(S_n)$ of the form $\gamma(\pi) = \sigma\pi\tau^{-1}$, we may assume that $\alpha(A_{11}) = A_{11}$. Then $|\alpha(A_{12}) \cap A_{11}| = |A_{12} \cap A_{11}| = 0$, and thus either $\alpha(A_{12}) = A_{1j}$ for some $j \neq 1$ or $\alpha(A_{12}) = A_{j1}$ for some $j \neq 1$. If the latter is the case, we compose α with the map $\pi \mapsto \pi^{-1}$, so we may assume that $\alpha(A_{12}) = A_{1j}$.

Multiplying A_{1j} from the left with the transposition $(2, j)$ yields the set A_{12}, and so we can assume that $\alpha(A_{12}) = A_{12}$.

Now for $j \geqslant 3$, the set $\alpha(A_{1j})$ has empty intersection with A_{11} and A_{12} and thus $\alpha(A_{1j}) \in \{A_{1k} \mid k \geqslant 3\}$. Thus α induces a permutation σ of $\{3, \ldots, n\}$ defined

by $\alpha(A_{1j}) = A_{1,\sigma j}$. Thus $\sigma^{-1}\alpha(A_{1j}) = A_{1j}$, and we may assume that $\alpha(A_{1j}) = A_{1j}$ for all j. Similarly, we can assume that $\alpha(A_{j1}) = A_{j1}$ for all j.

Thus, after composing α with suitable elements from $\Gamma(S_n)$, we may assume that α leaves each of the sets A_{1j} and A_{j1} invariant. For $k \geqslant 2$, $l \geqslant 2$ we have that A_{kl} is the unique set S among the sets A_{ij} (with $i \geqslant 2$, $j \geqslant 2$) such that $S \cap A_{k1} = \emptyset = S \cap A_{1l}$. It follows that $\alpha(A_{kl}) = A_{kl}$ for all k, l. Thus α is the identity. It follows that the original α was already in $\Gamma(S_n)$. □

4. Characterization of the Birkhoff polytope

In this section, we prove Theorem A. We first show the following weaker result.

4.1 Lemma. *Let $D\colon S_n \to \mathrm{GL}(d,\mathbb{R})$ be a representation such that the representation polytope $P(D)$ is combinatorially equivalent to the Birkhoff polytope. Then D is effectively equivalent to the standard representation of S_n.*

Proof. We have to show that D has the same nontrivial constituents as P, up to automorphisms of S_n. Since we can replace D by a stably equivalent representation, we may (and do) assume that the trivial character is not a constituent of the character of D.

A combinatorial isomorphism from the Birkhoff polytope B_n onto $P(D)$ sends a vertex $P(g)$ of B_n (where $g \in S_n$) to a vertex $D(\alpha(g))$ of $P(D)$, where $\alpha\colon S_n \to S_n$ is a permutation of S_n. Then the map sending $\gamma \in \operatorname{Sym} S_n$ to $\alpha \circ \gamma \circ \alpha^{-1}$ is an isomorphism from the combinatorial symmetry group of B_n onto the combinatorial symmetry group of $P(D)$. The combinatorial symmetry group of the Birkhoff polytope is $\Gamma(S_n)$, and the combinatorial symmetry group of $P(D)$ contains $\Gamma(S_n)$ (in its natural action on $P(D)$), by Lemma 3.1. Therefore, the combinatorial symmetry group of $P(D)$ is just $\Gamma(S_n)$. It follows that $\alpha \in \mathbf{N}_{\operatorname{Sym} S_n}(\Gamma(S_n))$. By Lemma 2.4, Corollary 2.6 applies to S_n and thus $\alpha \in (\operatorname{Aut} S_n)\Gamma(S_n)$. After multiplying α with an element of $\Gamma(S_n)$, we may thus assume $\alpha \in \operatorname{Aut} S_n$. Since then D and $D \circ \alpha$ are effectively equivalent, we may assume that $\alpha = \mathrm{id}_{S_n}$. This means that the combinatorial isomorphism from B_n onto $P(D)$ simply sends the vertex $P(g)$ to $D(g)$, for any $g \in S_n$. In particular, a subset of S_n corresponds to a face(t) of B_n (under P) if and only if it corresponds to a face(t) of the representation polytope $P(D)$ (under D).

Let $H \leqslant S_{n-1}$ be the stabilizer of a point, say n. (So $H \cong S_{n-1}$.) By the description of the facets of B_n, we know that $S_n \setminus H = \{g \in S_n \mid g(n) \neq n\}$ corresponds to a facet of B_n. Thus $D(S_n \setminus H)$ is a facet of $P(D)$.

Let φ be the character of D. The character of the standard permutation representation P has the form $(1_H)^{S_n} = 1_{S_n} + \chi$, where χ is an irreducible character of S_n. We are going to show that χ is the only nontrivial irreducible constituent of φ.

As we remarked in the first paragraph of the proof, we can assume that φ does not contain the trivial character. The matrix $\sum_{g\in S_n} D(g)$ is fixed under multiplication with elements from $D(S_n)$, and since the trivial representation is not a constituent of D, we have $\sum_{g\in S_n} D(g) = 0$. Geometrically, this means that the origin is the barycenter of the representation polytope $P(D)$. As $D(S_n \setminus H)$ is a facet of $P(D)$, we must have

$$\sum_{g\in S_n\setminus H} D(g) \neq 0, \quad \text{and} \quad \sum_{g\in H} D(h) \neq 0.$$

It follows that the restricted character φ_H contains the trivial character 1_H as a constituent. Using Frobenius reciprocity and the fact that $(1_H)^{S_n} = 1_{S_n} + \chi$, we get

$$0 \neq [\varphi_H, 1_H] = [\varphi, (1_H)^{S_n}] = [\varphi, 1_{S_n}] + [\varphi, \chi] = [\varphi, \chi].$$

Thus χ is a constituent of φ.

Since dimension is a combinatorial invariant, we must have $\dim P(D) = \dim B_n = \chi(1)^2$. On the other hand, we have $\dim P(D) = \sum_\psi \psi(1)^2$, where the sum runs over the nontrivial irreducible constituents ψ of φ, not counting multiplicities [5, Theorem 3.2]. It follows that χ is the only irreducible constituent of φ, and thus D and P are stably equivalent. □

4.2 Remark. In the preceding proof, we reduced to the case that the combinatorial isomorphism sends $P(g)$ to $D(g)$ (for any $g \in S_n$). If we could show that then $P(g) \mapsto D(g)$ can be extended to an affine isomorphism, Lemma 4.1 would follow from a characterization of effective equivalence by Baumeister and Grüninger [1, Corollary 4.5]. But we do not know how to do this, or whether this is even true more generally (for combinatorial isomorphisms of this form between representation polytopes of arbitrary groups).

Finally, we prove our main result:

Proof of Theorem A. Identify the vertices of $P(D)$ and B_n with G and S_n, respectively. Let $\gamma\colon G \to S_n$ be a combinatorial isomorphism. Then γ induces an isomorphism κ_γ from the combinatorial symmetry group A of $P(D)$ onto the combinatorial symmetry group $S_n \wr C_2$ of B_n sending $\alpha \in A$ to $\kappa_\gamma(\alpha) := \gamma \circ \alpha \circ \gamma^{-1}$. Obviously, we have $\gamma(\alpha g) = \kappa_\gamma(\alpha)(\gamma g)$. Thus the pair (κ_γ, γ) is an isomorphism from the A-set G onto the $(S_n \wr C_2)$-set S_n. In particular, κ_γ sends subgroups of A which act regularly on G, onto subgroups of $S_n \wr C_2$ which act regularly on S_n.

The left and right multiplications with elements of G induce regular subgroups of A. These are sent to regular subgroups L and R (say) of $S_n \wr C_2$. Since left and right multiplications centralize each other, the subgroups L and R centralize each other. If $n \geqslant 4$, then Lemma 2.5 yields that $L = S_n \times 1$ or $L = 1 \times S_n$. Since $L \cong G$, we have that $G \cong S_n$. In view of Lemma 4.1, this finishes the proof in case $n \geqslant 4$.

In the case $n = 3$, however, there is one additional possibility (up to conjugacy in $S_3 \wr C_2$), namely that $L = R = C_2 \times C_3 \cong C_6$. And indeed, the action of $C_2 \times C_3$ on $\mathbf{M}_3(\mathbb{R})$ yields the Birkhoff polytope B_3 as orbit polytope of C_6, and this orbit polytope is affinely equivalent to the representation polytope $P(D)$, where $D\colon C_6 \to \mathrm{GL}(4, \mathbb{R})$ sends a generator of C_6 to

$$\begin{pmatrix} 0 & 1 & & \\ -1 & -1 & & \\ & & 0 & -1 \\ & & 1 & 1 \end{pmatrix}. \qquad \square$$

Acknowledgments

Part of the work was done while the second author visited Bielefeld University. We wish to thank the CRC 701 "*Spectral Structures and Topological Methods in Mathematics*" for its support. The second author is also supported by the DFG through project SCHU 1503/6-1.

References for Chapter VI

1. Barbara Baumeister and Matthias Grüninger. On permutation polytopes: notions of equivalence. *J. Algebraic Combin.* **41**, no. 4 (2015), pp. 1103–1114. DOI: 10.1007/s10801-014-0568-8, arXiv: 1301.2080 [math.CO]. MR3342715, Zbl. 1322.52010 (cited on pp. 140, 146).
2. Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. On permutation polytopes. *Adv. Math.* **222**, no. 2 (2009), pp. 431–452. DOI: 10.1016/j.aim.2009.05.003, arXiv: 0709.1615 [math.CO]. MR2538016(2010j:52042), Zbl. 1185.52006 (cited on pp. 139, 140).
3. Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. Permutation polytopes of cyclic groups (Sept. 2011). arXiv: 1109.0191 [math.CO] (cited on p. 140).
4. Andrew Chermak and Alberto Delgado. A measuring argument for finite groups. *Proc. Amer. Math. Soc.* **107**, no. 4 (1989), pp. 907–914. DOI: 10.2307/2047648. MR994774(90c:20001), Zbl. 0687.20022 (cited on p. 141).

FL1. Erik Friese and Frieder Ladisch. Affine symmetries of orbit polytopes. *Adv. Math.* **288** (2016), pp. 386–425. DOI: 10.1016/j.aim.2015.10.021, arXiv: 1411.0899v3 [math.MG]. MR3436389, Zbl. 1330.52017 (cited on p. 143).

5. Robert M. Guralnick and David Perkinson. Permutation polytopes and indecomposable elements in permutation groups. *J. Combin. Theory Ser. A* **113**, no. 7 (2006), pp. 1243–1256. DOI: 10.1016/j.jcta.2005.11.004, arXiv: math/0503015 [math.CO]. MR2259059(2007h:05076), Zbl. 1108.52014 (cited on p. 146).

6. I. Martin Isaacs. *Finite Group Theory*. Graduate Studies in Mathematics 92. American Mathematical Society, Providence, RI, 2008. DOI: 10.1090/gsm/092. MR2426855(2009e:20029), Zbl. 1169.20001 (cited on pp. 141, 142).
7. Chi-Kwong Li, Ilya Spitkovsky, and Nahum Zobin. Finite reflection groups and linear preserver problems. *Rocky Mountain J. Math.* **34**, no. 1 (2004), pp. 225–251. DOI: 10.1216/rmjm/1181069902. MR2061128(2005e:20056), Zbl. 1060.15007 (cited on p. 140).
8. Chi-Kwong Li, Bit-Shun Tam, and Nam-Kiu Tsing. Linear maps preserving permutation and stochastic matrices. *Linear Algebra Appl.* **341** (2002), pp. 5–22. DOI: 10.1016/S0024-3795(00)00242-1. MR1873605(2002i:15005), Zbl. 0998.15004 (cited on p. 140).
9. László Lovász and Michael D. Plummer. *Matching Theory*. North-Holland Mathematics Studies 121. North-Holland, Amsterdam, 1986. (Annals of Discrete Mathematics 29). MR859549(88b:90087), Zbl. 0618.05001 (cited on p. 144).

Chapter VII.

Realizations of Abstract Regular Polytopes from a Representation Theoretic View[1]

Frieder Ladisch

Abstract. Peter McMullen has developed a theory of realizations of abstract regular polytopes, and has shown that the realizations up to congruence form a pointed convex cone which is the direct product of certain irreducible subcones. We show that each of these subcones is isomorphic to a set of positive semi-definite hermitian matrices of dimension m over either the real numbers, the complex numbers or the quaternions. In particular, we correct an erroneous computation of the dimension of these subcones by McMullen and Monson. We show that the automorphism group of an abstract regular polytope can have an irreducible character χ with $\chi \neq \overline{\chi}$ and with arbitrarily large essential Wythoff dimension. This gives counterexamples to a result of Herman and Monson, which was derived from the erroneous computation mentioned before.

We also discuss a relation between cosine vectors of certain pure realizations and the spherical functions appearing in the theory of Gelfand pairs.

2010 Mathematics Subject Classification. Primary 52B15, Secondary 20C15, 20B25

Keywords. Real representations of finite groups, abstract regular polytope, realization cone, C-string group

1. Introduction

These notes are the result of an attempt to understand realizations of abstract regular polytopes, as introduced by Peter McMullen [9, 11, 12, 13], from a representation theoretic viewpoint, thereby showing that the theory actually generalizes to a theory of "realizations of transitive G-sets". That the theory applies in this wider context was already pointed out by McMullen [12, Remark 2.1]. In particular, we will derive the exact structure of McMullen's *realization cone* using arguments from basic representation theory and linear algebra.

To explain this in more detail, and to state our main theorem, we have to introduce some notation. Let G be a finite group and Ω a transitive G-set. (In

[1]Aequationes Math. **90**, no. 6 (2016), pp. 1169–1193. arXiv: 1604.07066 [math.MG].

the original theory, Ω is the vertex set of an abstract regular polytope and G the automorphism group of the polytope. But this assumption is in fact unnecessary for a large part of the theory.) In this situation, one can define a closed pointed convex cone called the *realization cone* which describes *realizations* of the transitive G-set Ω up to congruence. (We will recall the exact definitions below.)

Let us write $\mathrm{Irr}_{\mathbb{R}} G$ for the set of characters of irreducible representations over the real numbers $\mathbb{R}$. McMullen [9] has shown that the realization cone is the direct product of subcones, each subcone corresponding to some $\sigma \in \mathrm{Irr}_{\mathbb{R}} G$ (or, what is the same, to a similarity class of irreducible representations of G). We write $\mathcal{RC}_\sigma(\Omega)$ for the subcone corresponding to $\sigma \in \mathrm{Irr}_{\mathbb{R}} G$. The main new result of this note concerns the structure of such a subcone.

To state this result, we need some more notation. Let $\pi = \pi_\Omega$ be the permutation character corresponding to the G-set Ω. We can write π as a sum of irreducible real characters:

$$\pi = \sum_{\sigma \in \mathrm{Irr}_{\mathbb{R}} G} m_\sigma \sigma.$$

The *multiplicities* m_σ are uniquely determined by this equation, and equal the *essential Wythoff dimension* defined by McMullen and Monson [13]. Moreover, to each $\sigma \in \mathrm{Irr}_{\mathbb{R}}(G)$ belongs a division ring $\mathbb{D}_\sigma$ (the centralizer ring of a representation affording σ), which is isomorphic to either the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$ or the Hamiltonian quaternions $\mathbb{H}$.

We write $\mathbf{M}_m(\mathbb{D})$ for the ring of $m \times m$-matrices over $\mathbb{D}$, and if $A \in \mathbf{M}_m(\mathbb{D})$, then A^* denotes the (complex/quaternion) conjugate transpose of A when $\mathbb{D} = \mathbb{C}$ or $\mathbb{H}$, and the transpose of A when $\mathbb{D} = \mathbb{R}$. With this notation, we have:

Theorem A. *The realization cone of Ω is the direct product of subcones $\mathcal{RC}_\sigma(\Omega)$ corresponding to $\sigma \in \mathrm{Irr}_{\mathbb{R}} G$, where each $\mathcal{RC}_\sigma(\Omega)$ is isomorphic to the set of matrices*

$$\{AA^* \mid A \in \mathbf{M}_{m_\sigma}(\mathbb{D}_\sigma)\}.$$

In other words, the subcone $\mathcal{RC}_\sigma(\Omega)$ is isomorphic to the set of hermitian positive semi-definite $m_\sigma \times m_\sigma$-matrices with entries in $\mathbb{D}_\sigma$, with appropriate meaning of "hermitian" (depending on whether $\mathbb{D}_\sigma = \mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$).

From the main theorem, one can immediately derive the dimension of $\mathcal{RC}_\sigma(\Omega)$ (see Corollary 3.7). This dimension has been computed by McMullen and Monson [13, Theorem 4.6] (using different notation). Unfortunately, the result of McMullen and Monson only matches with our description when $m_\sigma \leqslant 1$ or when $\mathbb{D}_\sigma = \mathbb{R}$. If the computation of McMullen and Monson [13, Theorem 4.6] were correct in the original situation, where G is the automorphism group of an abstract regular polytope with vertex set Ω, then it would follow that we always have $m_\sigma \leqslant 1$ or $\mathbb{D}_\sigma = \mathbb{R}$ for such G. And indeed, this is the main result of a paper by Herman and Monson [4]. They derive this from [13, Theorem 4.6] in a different way.

But unfortunately, the main result of Herman and Monson [4] is wrong: We show in Section 4 that we can have $\mathbb{D}_\sigma = \mathbb{C}$ and m_σ arbitrarily large even when G is the automorphism group of an abstract regular polytope with vertex set Ω. (See Example 4.1 for a concrete case where $m_\sigma = 2$. It seems to be unknown whether there are any abstract regular polytopes with $\mathbb{D}_\sigma \cong \mathbb{H}$ for some σ.) These examples show that the computation of McMullen and Monson must be wrong even in the original setting. At the end of Section 3, we briefly discuss where we see the flaw in McMullen's and Monson's proof.

A later result of McMullen [12, Theorem 5.2] can be interpreted as saying that the subcone $\mathcal{RC}_\sigma(\Omega)$ is isomorphic to the symmetric positive semi-definite matrices of size $m_\sigma \times m_\sigma$, with entries in the reals. This is in general not correct, the correct statement is the main theorem stated above.

Another consequence of the mistake in [13] is that the Λ-orthogonal basis described in [12] is in general too small. In Section 5, we briefly discuss the relation between McMullen's Λ-inner product and some other natural inner products, and indicate how to construct a complete orthogonal basis.

In Section 6, we discuss some relations between McMullen's cosine vectors and the spherical functions appearing in the theory of Gelfand pairs. It turns out that when (G, H) is a Gelfand pair (where H is the stabilizer of a vertex), then the cosine vectors are in principle the same as the spherical functions. (This applies to all classical regular polytopes in euclidean space, except the 120-cell.) We show that the values of cosine vectors are algebraic numbers, when the essential Wythoff dimension is 1. This was conjectured by McMullen [12, Remark 9.4]. Indeed, multiplied with the size of the corresponding layer, we get an algebraic *integer*.

Finally, in Section 7 we propose an explanation of an observation of McMullen [11, Remark 9.3] about the cosine vectors of the 600-cell.

2. Realizations as G-homomorphisms

Let G be a finite group. For convenience, we use the following terminology: An **euclidian G-space** is an euclidean vector space $(V, \langle \cdot, \cdot \rangle)$ on which the group G acts by orthogonal transformations. The action is denoted by $(v, g) \mapsto vg$. Equivalently, we are given an orthogonal representation $D\colon G \to \mathbf{O}(V)$, so that $D(g)$ is the map $v \mapsto vg = vD(g)$.

Let Ω be a transitive (right) G-set. A **realization** of (G, Ω) is a map $A\colon \Omega \to V$ into an euclidean G-space V such that $(\omega g)A = (\omega A)g$ for all $\omega \in \Omega$ and $g \in G$. This definition agrees with McMullen's definition [9, 11, 12] in the case where G is the automorphism group of an abstract regular polytope with vertex set Ω. We emphasize that in this paper, G is just some finite group and Ω a transitive G-set. For example, we could take $\Omega = G$, on which G acts by right multiplication.

Two realizations $A_1\colon \Omega \to V_1$ and $A_2\colon \Omega \to V_2$ are called **congruent**, if there is a linear isometry σ from the linear span of $\{\omega A_1 \mid \omega \in \Omega\}$ into V_2 such that $A_1\sigma = A_2$. (A peculiarity of this definition is that the realization $\Omega \to \mathbb{R}$ sending every $\omega \in \Omega$ to 0 is *not* congruent to the realization sending every $\omega \in \Omega$ to 1. It turns out to be useful to distinguish these.) The following is easy to see:

2.1 Lemma. *Two realizations $A_1\colon \Omega \to (V_1, \langle\cdot,\cdot\rangle_1)$ and $A_2\colon \Omega \to (V_2, \langle\cdot,\cdot\rangle_2)$ are congruent if and only if $\langle \xi A_1, \eta A_1\rangle_1 = \langle \xi A_2, yA_2\rangle_2$ for all ξ, $\eta \in \Omega$.*

Thus a realization $A\colon \Omega \to V$ is determined up to congruence by the $\Omega \times \Omega$ matrix $Q = Q(A)$ with entries $q_{\xi,\eta} = \langle \xi A, \eta A\rangle$. We call Q the **inner product matrix** of the realization A. It is a symmetric positive semi-definite matrix and G-invariant in the sense that $q_{\xi g,\eta g} = q_{\xi,\eta}$.

2.2 Remark. McMullen [11] uses *inner product vectors* instead of inner product matrices. The relation is as follows: A **diagonal class** is an orbit of G on the set of unordered pairs on Ω. Since the inner product matrix $Q = (q_{\xi,\eta})$ is symmetric and G-invariant, the map $\{\xi, \eta\} \mapsto q_{\xi,\eta}$ is well defined and constant along diagonal classes. Thus it is determined by its values on a set of representatives of the diagonal classes.

Now fix some "initial" vertex $\alpha \in \Omega$. A **layer** is the set of all elements $\omega \in \Omega$ such that $\{\alpha, \omega\}$ belongs to the same diagonal class. Choose a set of representatives $\xi_0 = \alpha$, ξ_1, …, ξ_r of the layers in Ω. Then the unordered pairs $\{\alpha, \xi_i\}$ represent all diagonal classes (as Ω is a transitive G-set). The vector of length $r + 1$ with values $q_{\alpha,\xi_i} = \langle \alpha A, \xi_i A\rangle$ as entries is the **inner product vector** of the realization [11]. It is clear that the inner product matrix is determined by the inner product vector. For the purposes of this paper, we find it more convenient to use the inner product matrix itself.

The set of all inner product matrices of realizations of Ω is called the **realization cone** of Ω, and denoted by $\mathcal{RC}(\Omega)$ or $\mathcal{RC}(G, \Omega)$ (in the first variant, the group G is understood to be implicit in Ω). It is in bijection to the set of all congruence classes of realizations.

The following operations on realizations show that the realization cone is indeed a cone: First, if $A_1\colon \Omega \to V_1$ and $A_2\colon \Omega \to V_2$ are two realizations, then their **blend** is the realization $A_1 \oplus A_2\colon \Omega \to V_1 \oplus V_2$ sending $\omega \in \Omega$ to $(\omega A_1, \omega A_2)$ in the (outer) orthogonal sum of the two euclidean spaces V_1 and V_2. (McMullen denotes the blend by $A_1 \# A_2$.) For the corresponding inner product matrices, we have $Q(A_1 \oplus A_2) = Q(A_1) + Q(A_2)$.

Second, we can scale realizations: for $A\colon \Omega \to V$ and $\lambda \in \mathbb{R}$, $\lambda A\colon \Omega \to V$ is defined by $\omega(\lambda A) = \lambda(\omega A)$. Obviously, $Q(\lambda A) = \lambda^2 Q(A)$.

For completeness, we mention a third operation, the *tensor product* $A_1 \otimes A_2\colon \Omega \to V_1 \otimes V_2$ of two realizations $A_i\colon \Omega \to V_i$, defined on Ω by $\omega(A_1 \otimes A_2) := (\omega A_1) \otimes (\omega A_2)$.

The inner product matrix $Q(A_1 \otimes A_2)$ is the entry-wise (Hadamard) product of $Q(A_1)$ and $Q(A_2)$.

It follows from blending and scaling that $\mathcal{RC}(\Omega)$ is a convex cone. It is also clear that $\mathcal{RC}(\Omega)$ has an apex at 0.

A realization $A\colon \Omega \to V$ is called **normalized**, if $\|\omega A\|^2 := \langle \omega A, \omega A\rangle = 1$ for some (and hence for all) $\omega \in \Omega$. If $\omega A \neq 0$, then we may scale the realization by $1/\|\omega A\|$, so that it becomes normalized. The inner product matrix of the normalized realization $(1/\|\omega A\|)A$ is called its **cosine matrix**, for obvious reasons. The set of cosine matrices of realizations forms a compact convex set.

2.3 Remark. As in Remark 2.2, a cosine matrix corresponds to a **cosine vector**, which contains the values $\langle \alpha A, \xi_i A\rangle / \langle \alpha A, \alpha A\rangle$, where ξ_i runs over a set of representatives of the layers. We have to caution the reader that McMullen [12] uses the term *cosine matrix* with a different meaning: In [12], this is a square matrix whose rows are cosine vectors of different realizations (and maybe certain *mixed cosine vectors*), and such that the rows are orthogonal with respect to a certain inner product (Λ-orthogonality, see Section 5 below). This matrix is similar to the character table of a finite group, and thus we find the name "cosine table" more appropriate for this object.

An especially important realization is the **simplex realization** which we now define. Recall that the permutation module $\mathbb{R}\Omega$ over $\mathbb{R}$ belonging to the G-set Ω is the set of formal sums

$$\mathbb{R}\Omega := \{\sum_{\omega\in\Omega} r_\omega \omega \mid r_\omega \in \mathbb{R}\},$$

on which G acts by $(\sum r_\omega \omega)g = \sum r_\omega(\omega g)$. Also we think of $\mathbb{R}\Omega$ as equipped with the standard scalar product

$$\left\langle \sum_\omega r_\omega \omega, \sum_\omega s_\omega \omega \right\rangle = \sum_\omega r_\omega s_\omega.$$

This makes $\mathbb{R}\Omega$ into an euclidean G-space. The natural map $\Omega \hookrightarrow \mathbb{R}\Omega$ is a realization, called the *simplex realization*. (We usually identify its image, the canonical basis of $\mathbb{R}\Omega$, with the set Ω.)

The next observation is obvious, but crucial for our proof of the structure theorems in the next section. Recall that a linear map $\widehat{A}\colon U \to V$ between two G-modules is a G-module homomorphism if $ug\widehat{A} = u\widehat{A}g$ for all $u \in U$ and $g \in G$. Since Ω is a basis of $\mathbb{R}\Omega$, we have the following:

2.4 Observation. *Realizations $A\colon \Omega \to V$ correspond to G-module homomorphisms $\widehat{A}\colon \mathbb{R}\Omega \to V$.*

From now on, we identify a realization $A\colon \Omega \to V$ with the corresponding linear map $\mathbb{R}\Omega \to V$, and use the same letter A for both. We also identify a linear map $A\colon \mathbb{R}\Omega \to V$ with its matrix A with respect to the canonical basis Ω and some fixed orthonormal basis of V. The inner product matrix of the realization A is then $Q = AA^t$, and does not depend on the choice of basis of V.

We also write $A^t\colon V \to \mathbb{R}\Omega$ for the *adjoint map* of $A\colon \mathbb{R}\Omega \to V$ with respect to the inner products on $\mathbb{R}\Omega$ and V; if A is a G-module homomorphism, then so is A^t. From this viewpoint, $Q = AA^t$ is a G-module endomorphism of $\mathbb{R}\Omega$.

2.5 Theorem. *Let Ω be a transitive G-set. Then*

$$\mathcal{RC}(\Omega) = \{AA^t \mid A \in \mathbf{M}_\Omega(\mathbb{R}) \text{ is } G\text{-invariant}\},$$

and this equals the set of G-invariant, symmetric positive semi-definite matrices.

This is the special case $U = \mathbb{R}\Omega$ of the following general observation:

2.6 Lemma. *Let U be an euclidean G-space and $Q \in \mathrm{End}_{\mathbb{R}}(U)$. The following are equivalent:*

(i) *There is an euclidean G-space V and a G-homomorphism $A\colon U \to V$ such that $Q = AA^t$.*
(ii) *Q is symmetric positive semi-definite and commutes with G.*
(iii) *There is $A \in \mathrm{End}_{\mathbb{R}G}(U)$ such that $Q = AA^t$.*

Proof. Obviously, (iii) is a special case of (i), and (i) implies (ii).

It remains to show that (ii) implies (iii), so assume Q is symmetric positive semi-definite and commutes with G. Then U is the orthogonal sum of the eigenspaces of Q, and the eigenvalues of Q are non-negative real numbers. For each eigenvalue λ of Q, let $p_\lambda\colon U \to U$ be the orthogonal projection onto the corresponding eigenspace of Q. Since Q commutes with G, it follows that the eigenspaces are G-invariant and thus the p_λ's commute with G.

Since U is the orthogonal sum of the eigenspaces, we have $\mathrm{id}_U = \sum_\lambda p_\lambda$. For $u \in U$, it follows

$$uQ = \sum_\lambda up_\lambda Q = \sum_\lambda \lambda(up_\lambda) = u\sum_\lambda \lambda p_\lambda.$$

Since $p_\lambda p_\mu = \delta_{\lambda,\mu} p_\lambda$ for eigenvalues λ, μ of Q, and since all $\lambda \geqslant 0$, we get

$$Q = \sum_\lambda \lambda p_\lambda = \left(\sum_\lambda \sqrt{\lambda} p_\lambda\right)^2.$$

Set $A = \sum_\lambda \sqrt{\lambda} p_\lambda$, an element commuting with G. Then $A = A^t$, since orthogonal projections are self-adjoint, and thus $Q = A^2 = AA^t$ as required. □

3. The structure of the realization cone

In this section, we determine the structure of the realization cone. The general idea is the following: We can write the module $\mathbb{R}\Omega$ as an orthogonal sum of simple modules, say

$$\mathbb{R}\Omega \cong m_1 S_1 \oplus \cdots \oplus m_k S_k,$$

with natural numbers m_i, and where the different S_i's are non-isomorphic. It is well known that then

$$\mathrm{End}_{\mathbb{R}G}(\mathbb{R}\Omega) \cong \mathbf{M}_{m_1}(\mathrm{End}_{\mathbb{R}G}(S_1)) \times \cdots \times \mathbf{M}_{m_k}(\mathrm{End}_{\mathbb{R}G}(S_k)),$$

where for each i the endomorphism ring $\mathbb{D}_i := \mathrm{End}_{\mathbb{R}G}(S_i)$ is a division ring by Schur's lemma, and thus either $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$. The aim of this section is to fill in the details and to show that the above isomorphism, when restricted to the realization cone $\mathcal{RC}(\Omega)$ as a subset of $\mathrm{End}_{\mathbb{R}G}(\mathbb{R}\Omega)$, yields a similar decomposition into subcones of the form $\{AA^* \mid A \in \mathbf{M}_{m_i}(\mathrm{End}_{\mathbb{R}G}(S_i))\}$.

We begin by recalling some general representation theory. As usual, we write $\mathrm{Irr}\, G$ for the set of irreducible complex characters of a group G. Furthermore, $\mathrm{Irr}_{\mathbb{R}}\, G$ denotes the set of characters of simple $\mathbb{R}G$-modules (equivalently, of irreducible representations $G \to \mathrm{GL}(d, \mathbb{R})$). For class functions α, $\beta\colon G \to \mathbb{C}$,

$$[\alpha, \beta] := \frac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}$$

denotes the usual inner product of class functions. It is well known that $\mathrm{Irr}\, G$ is an orthonormal basis of the space of class functions with respect to this inner product. For $\sigma \in \mathrm{Irr}_{\mathbb{R}}\, G$, we have the following possibilities [16, III.5A][7, Ch. 4]:

3.1 Lemma. *Let S be a simple $\mathbb{R}G$-module with character $\sigma \in \mathrm{Irr}_{\mathbb{R}}\, G$. Then one of the following three cases occurs:*

(i) $[\sigma, \sigma] = 1$, $\sigma \in \mathrm{Irr}\, G$ *and* $\mathrm{End}_{\mathbb{R}G}(S) \cong \mathbb{R}$,
(ii) $[\sigma, \sigma] = 2$, $\sigma = \chi + \overline{\chi}$ *with* $\chi \neq \overline{\chi} \in \mathrm{Irr}\, G$ *and* $\mathrm{End}_{\mathbb{R}G}(S) \cong \mathbb{C}$,
(iii) $[\sigma, \sigma] = 4$, $\sigma = 2\chi$ *with* $\chi = \overline{\chi} \in \mathrm{Irr}\, G$ *and* $\mathrm{End}_{\mathbb{R}G}(S) \cong \mathbb{H}$.

We call S and σ of real, complex or quaternion type, respectively.

Let S be a simple $\mathbb{R}G$-module with character σ. For any $\mathbb{R}G$-module V, let $V_\sigma = V_S$ be the sum of all submodules of V isomorphic to S. The submodule V_σ is called the σ-homogeneous component of V. Every module V is the direct sum of the V_σ, as σ runs over $\mathrm{Irr}_{\mathbb{R}}\, G$. This sum is orthogonal with respect to any G-invariant inner product defined on V. The orthogonal projection $V \to V_\sigma$ is given by the action of

$$e_\sigma = \frac{\sigma(1)}{[\sigma, \sigma]|G|} \sum_{g \in G} \sigma(g^{-1})g \in \mathbf{Z}(\mathbb{R}G)$$

on V. (The formula for the idempotent e_σ follows from the analogous one in the complex case [7, Theorem 2.12][16, III.7] together with Lemma 3.1.) We have

$$1 = \sum_{\sigma \in \mathrm{Irr}_{\mathbb{R}} G} e_\sigma, \quad \text{and} \quad e_\sigma e_\tau = \delta_{\sigma,\tau} e_\sigma \quad \text{for all } \sigma, \tau \in \mathrm{Irr}_{\mathbb{R}} G.$$

Notice that since $e_\sigma \in \mathbf{Z}(\mathbb{R}G)$, the action of e_σ on modules commutes with both the action of G and the action of G-module homomorphisms.

For each $\sigma \in \mathrm{Irr}_{\mathbb{R}} G$, define $\mathcal{RC}_\sigma(\Omega)$ to be the set of all inner product matrices which arise from a realization $A\colon \Omega \to V$ such that $V = V_\sigma$, so V has character $k\sigma$ for some $k \in \mathbb{N}$. Equivalently, if S is an irreducible module affording σ, then V is isomorphic to a direct sum of copies of S. (The subcone $\mathcal{RC}_\sigma(\Omega)$ is denoted by $\mathcal{P}_D$ in [9, 13], where D is an irreducible representation of G affording σ.)

In the next result, we view both the inner product matrix and the idempotent e_σ as operators on the permutation module $\mathbb{R}\Omega$.

3.2 Theorem. *(cf. [9, Theorem 16], [13, Theorem 4.1]) $\mathcal{RC}_\sigma(\Omega)$ is a closed subcone of $\mathcal{RC}(\Omega)$ and $\mathcal{RC}(\Omega)$ is the direct sum of the $\mathcal{RC}_\sigma(\Omega)$, where $\sigma \in \mathrm{Irr}_{\mathbb{R}} G$. More precisely, for $Q \in \mathcal{RC}(\Omega)$, we have*

$$Q = \sum_{\sigma \in \mathrm{Irr}_{\mathbb{R}} G} Q_\sigma, \quad \textit{where} \quad Q_\sigma = e_\sigma Q = Q e_\sigma \in \mathcal{RC}_\sigma(\Omega).$$

(In particular, $Q \in \mathcal{RC}_\sigma(\Omega)$ if and only if $e_\sigma Q = Q$, if and only if $Q = Q e_\sigma$.)

This means that if the inner product matrix Q of a realization has entries $q_{\xi,\eta}$, then the inner product matrix $Q_\sigma = e_\sigma Q$ of the σ-homogeneous component of the realization has entries

$$s_{\xi,\eta} := \frac{\sigma(1)}{[\sigma,\sigma]|G|} \sum_{g \in G} \sigma(g^{-1}) q_{\xi g,\eta} \quad \text{for all } \xi,\, \eta \in \Omega.$$

Proof of Theorem 3.2. Suppose $A\colon \mathbb{R}\Omega \to V$ is a realization with inner product matrix $Q = AA^t \in \mathcal{RC}(\Omega)$. Then $e_\sigma A = A e_\sigma$ is a realization $\mathbb{R}\Omega \to V e_\sigma$ with inner product matrix $(e_\sigma A)(e_\sigma A)^t = e_\sigma Q e_\sigma = e_\sigma Q$, since $e_\sigma^t = e_\sigma = e_\sigma^2$. Thus $e_\sigma Q$ is an inner product matrix in $\mathcal{RC}_\sigma(\Omega)$. Conversely, if $Q \in \mathcal{RC}_\sigma(\Omega)$, then $Q = AA^t$ for some realization A with $A = A e_\sigma$, and thus $Q = e_\sigma Q$.

Since $Q = \sum_\sigma e_\sigma Q$ for any inner product matrix, the result follows. □

(That $\mathcal{RC}_\sigma(\Omega)$ is a subcone and that $\mathcal{RC}(\Omega)$ is the sum of these subcones is also immediate from the equation $Q(A_1 \oplus A_2) = Q(A_1) + Q(A_2)$ and the fact that every $\mathbb{R}G$-module can be written as an orthogonal sum of simple modules.)

Next we determine the structure of $\mathcal{RC}_\sigma(\Omega)$, for $\sigma \in \mathrm{Irr}_{\mathbb{R}} G$. Let S be a simple $\mathbb{R}G$-module affording σ. We can write $(\mathbb{R}\Omega)_\sigma$ as the orthogonal sum of $m = m_\sigma =$

m_S copies of S, that is, $(\mathbb{R}\Omega)_\sigma \cong mS$. The non-negative integer m is called the *multiplicity* of S in $\mathbb{R}\Omega$ and of σ in the character $\pi = (1_H)^G$ of $\mathbb{R}\Omega$. In other words, we have

$$\pi = (1_H)^G = \sum_{\sigma \in \operatorname{Irr}_{\mathbb{R}} G} m_\sigma \sigma,$$

and this equation determines the m_σ's. (Here $H = G_\alpha$, the stabilizer of a vertex α.)

Recall that the *Wythoff space* W_S associated to S (and $\alpha \in \Omega$) is the fixed space of H on S. McMullen and Monson [13] defined the *essential Wythoff dimension* as the dimension of W_S over the centralizer ring $\mathbb{D} = \operatorname{End}_{\mathbb{R}G}(S)$.

3.3 Lemma. *The multiplicity $m_S = m_\sigma$ equals the essential Wythoff dimension.*

Proof. Let π be the character of $\mathbb{R}\Omega$. Then $[\pi, \sigma]_G = m_\sigma [\sigma, \sigma]_G = m_\sigma \dim_{\mathbb{R}}(\mathbb{D})$. On the other hand, $\pi = (1_H)^G$ and $[\pi, \sigma]_G = [1_H, \sigma_H]_H = \dim_{\mathbb{R}} W_S$ by Frobenius reciprocity. The result follows. □

Before we give our structure theorem for $\mathcal{RC}_\sigma(\Omega)$, we digress to reprove Theorems 4.4 and 4.5 of the McMullen-Monson paper [13], since, as we argue below, McMullen's and Monson's proofs of these theorems are not correct.

We recall that a realization $A\colon \mathbb{R}\Omega \to V$ and the corresponding polytope are called **pure**, when the image $A(\mathbb{R}\Omega)$ is simple as module over G. The following contains Theorems 4.4 and 4.5 from the paper of McMullen and Monson [13].

3.4 Theorem. *Every polytope in $\mathcal{RC}_\sigma(\Omega)$ is the blend of at most m_σ pure polytopes, and has dimension at most $m_\sigma \sigma(1)$, where $m_\sigma \sigma(1)$ is possible.*

Proof. Let $A\colon \Omega \to V$ be a realization, which we identify as usual with a G-homomorphism $\mathbb{R}\Omega \to V$. Without loss of generality, we can assume that $V = (\mathbb{R}\Omega)A$, that is, V is the linear span of $\{\omega A \mid \omega \in \Omega\}$. The orthogonal complement of $\operatorname{Ker} A$ in $\mathbb{R}\Omega$ is a G-invariant subspace isomorphic to V. In particular, if $V \cong kS$, where S affords σ, it follows from the uniqueness of the decomposition of $\mathbb{R}\Omega$ into irreducible summands that $k \leqslant m_\sigma$. Then A is the blend of k pure realizations, and the polytope spanned by $\{\omega A \mid \omega \in \Omega\}$ has dimension $k\sigma(1) \leqslant m_\sigma \sigma(1)$. Finally, e_σ viewed as realization $\mathbb{R}\Omega \to U = \mathbb{R}\Omega e_\sigma$ yields a polytope of dimension $\dim U = m_\sigma \sigma(1)$. □

In the description of $\mathcal{RC}_\sigma(\Omega)$, we use the following notation: for a matrix B over the complex numbers or the quaternions, B^* denotes the transposed conjugate. If B has real entries, then $B^* = B^t$, the transposed matrix.

3.5 Theorem. *Let S be a simple module affording $\sigma \in \operatorname{Irr}_{\mathbb{R}} G$, let $m = m_\sigma$ be its multiplicity in $\mathbb{R}\Omega$ and set $\mathbb{D} = \operatorname{End}_{\mathbb{R}G}(S)$. Then*

$$\mathcal{RC}_\sigma(\Omega) \cong \{BB^* \mid B \in \mathbf{M}_m(\mathbb{D})\}.$$

3.6 Example. Let Ω be the vertex set of the 120-cell (of size 600) and G its symmetry group. Using the computer algebra system GAP [3], one can compute the multiplicities of the irreducible characters in the permutation character. There are 15 characters occurring with multiplicity 1, three characters occurring with multiplicity 2 (of degrees 16, 16 and 48), and two characters occurring with multiplicity 3 (of degrees 25 and 36). All characters are of real type. The realization cone of the 120-cell is thus a direct product of 15 copies of $\mathbb{R}_{\geqslant 0}$, of three copies of the cone of symmetric positive semidefinite 2×2-matrices, and two copies of the cone of symmetric positive semidefinite 3×3-matrices. The 120-cell is the only classical regular polytope for which the realization cone is not polyhedral.

A corollary of the theorem is the correct version of [13, Theorem 4.6].

3.7 Corollary. *We have*

$$\begin{aligned}\dim \mathcal{RC}_\sigma(\Omega) &= m + \frac{m(m-1)}{2}[\sigma,\sigma] \\ &= \begin{cases} \frac{m(m+1)}{2} & \text{for} \quad \mathbb{D} \cong \mathbb{R}, \\ m^2 & \text{for} \quad \mathbb{D} \cong \mathbb{C}, \\ m(2m-1) & \text{for} \quad \mathbb{D} \cong \mathbb{H}. \end{cases}\end{aligned}$$

Proof. It follows from Theorem 3.5 that the linear span of $\mathcal{RC}_\sigma(\Omega)$ is isomorphic to the $m \times m$ self-adjoint matrices over $\mathbb{D}$. Since $[\sigma,\sigma] = \dim_{\mathbb{R}}(\mathbb{D})$, the result follows. □

In the proof of Theorem 3.5, and also later, we need the following simple observation:

3.8 Lemma. *Let S be an irreducible euclidean G-space and let $\mathbb{D} = \mathrm{End}_{\mathbb{R}G}(S)$. Then for $d \in \mathbb{D}$ we have $d^t = \overline{d}$ (that is, the adjoint map with respect to the scalar product on S equals the complex/quaternion conjugate).*

Proof. We have $d^t \in \mathbb{D}$ again and thus $dd^t \in \mathbb{D}$. The eigenspaces of dd^t on S are G-invariant, and thus $dd^t = \lambda \,\mathrm{id}_S$ with $\lambda \in \mathbb{R}_{\geqslant 0}$. This means that $\langle vd, vd\rangle = \lambda\langle v, v\rangle$ for all $v \in S$. For $d = i$ (or $d \in \{i, j, k\}$ when $D = \mathbb{H}$), it follows $\lambda = 1$ (because $\lambda^2\langle v, v\rangle = \langle vd^2, vd^2\rangle = \langle -v, -v\rangle$), and thus $d^t = \overline{d}$ in this case. The general case follows from this. □

Proof of Theorem 3.5. First, observe that it follows from Theorem 2.5 together with Theorem 3.2 that

$$\mathcal{RC}_\sigma(\Omega) = \{AA^t \mid A \in \mathrm{End}_{\mathbb{R}G}(\mathbb{R}\Omega), Ae_\sigma = A\}.$$

Fix a G-invariant inner product $\langle \cdot, \cdot \rangle_S$ on the simple module S affording σ. Suppose that $\mu\colon S \to \mathbb{R}\Omega$ is an isomorphism from S onto some simple submodule of $\mathbb{R}\Omega$ (necessarily, $S\mu \subseteq \mathbb{R}\Omega e_\sigma$). After eventually scaling μ, we may assume that $\langle v, w\rangle_S = \langle v\mu, w\mu\rangle_{\mathbb{R}\Omega}$. Then with $\pi = \mu^t\colon \mathbb{R}\Omega \to S$, we have $\mu\pi = \mathrm{id}_S$ and $\pi\mu$ is the orthogonal projection from $\mathbb{R}\Omega$ onto $S\mu$. We know that $\mathbb{R}\Omega e_\sigma$ is isomorphic to a sum of m copies of S. Thus we can find G-module homomorphisms $\mu_i\colon S \to \mathbb{R}\Omega$ and $\pi_i\colon \mathbb{R}\Omega \to S$, $i = 1, \ldots, m$, such that

$$\pi_i = \mu_i^t, \quad \mu_i\pi_j = \delta_{ij}\,\mathrm{id}_S, \quad \text{and} \quad e_\sigma = \sum_{i=1}^{m} \pi_i\mu_i.$$

Using these maps, we can describe the algebra isomorphism between

$$\{A \in \mathrm{End}_{\mathbb{R}G}(\mathbb{R}\Omega) \mid Ae_\sigma = A\} \quad \text{and} \quad \mathbf{M}_m(\mathbb{D}),$$

where $\mathbb{D} = \mathrm{End}_{\mathbb{R}G}(S)$: Send $A \in \mathrm{End}_{\mathbb{R}G}(\mathbb{R}\Omega)$ to the matrix $(\mu_i A \pi_j) \in \mathbf{M}_m(\mathbb{D})$. Conversely, map a matrix (b_{ij}) to $\sum_{i,j} \pi_i b_{ij} \mu_j$.

This isomorphism sends the adjoint map A^t to the matrix $(\mu_i A^t \pi_j) = (\pi_i^t A^t \mu_j^t) = ((\mu_j A \pi_i)^t) = (\overline{\mu_j A \pi_i})$, where the last equality follows from Lemma 3.8. Thus it sends a inner product matrix AA^t to a matrix BB^* as claimed. □

Finally, Theorem 4.7(b) of McMullen and Monson [13] has to be modified accordingly.

3.9 Corollary. *Let $r+1$ be the number of layers. Then*

$$r + 1 = \sum_{\sigma \in \mathrm{Irr}_{\mathbb{R}} G} m_\sigma + \sum_{\sigma \in \mathrm{Irr}_{\mathbb{R}} G} \frac{m_\sigma(m_\sigma - 1)}{2}[\sigma, \sigma].$$

We can rewrite the right hand side of the above formula in terms of the irreducible complex characters. Recall that $m_\sigma = [(1_H)^G, \sigma]/[\sigma, \sigma]$. Thus if $\sigma = \chi \in \mathrm{Irr}\, G$ or $\sigma = \chi + \overline{\chi}$ with $\chi \neq \overline{\chi}$, then $m_\sigma = m_\chi$ $(= [(1_H)^G, \chi])$, and if $\sigma = 2\chi$ with $\chi = \overline{\chi} \in \mathrm{Irr}\, G$, then $m_\sigma = m_\chi/2$. Also recall the Frobenius-Schur indicator $\nu_2(\chi) = (1/|G|)\sum_g \chi(g^2)$, which is 1, 0 and -1, respectively, in the three mentioned cases. Using all this, one can derive the following equation:

$$r + 1 = \frac{1}{2} \sum_{\chi \in \mathrm{Irr}\, G} m_\chi(m_\chi + \nu_2(\chi)).$$

Herman and Monson [4] derived this equation from Frame's formula for the number of symmetric cosets. Conversely, we can derive Frame's formula from the last equation.

We conclude this section with a discussion about what is actually wrong in McMullen's and Monson's proof [13]. The mistake is that the *essential Wythoff*

space defined before Theorem 4.4 has not all the properties the authors assume (implicitly). It is in general not true that a traverse of the action of the unit complex numbers (or the unit quaternions) can be chosen as a subspace. For example, if the Wythoff space W has dimension 4 over the reals and if the centralizer ring is the field $\mathbb{C}$ of complex numbers, then $W \cong \mathbb{C}^2$. Clearly, not every element of $\mathbb{C}^2$ can be written as $v \cdot z$ with $v \in \mathbb{R}^2$, $z \in \mathbb{C}$ and $|z| = 1$, for example, $(1, i)$ is not of this form. On the other hand, in the $\mathbb{R}$-linear hull of $\mathbb{R}^2 \cup \{(1, i)\}$ we have the vector $-(1, 0) + (1, i) = (0, i) = (0, 1)i$, so this is no longer a traverse for the unit complex numbers.

Of course, we can always choose a $\mathbb{D}$-basis of W and then let W^* be the $\mathbb{R}$-linear hull of this basis. This is what is essentially done in the proof of Theorem 4.4 in [13]. But then the sentence "The general pure polytope in $\mathcal{P}_G$ arises from a point $\alpha_1 p_1 + \cdots + \alpha_{w^*} p_{w^*} \in W^*$" is no longer true. We should allow coefficients $\alpha_i \in \mathbb{D}$, but then different points in the Wythoff space yield congruent realizations. So the proof must be modified somehow.

This flaw in the arguments also bears upon results in the later paper [12]. Namely, in Theorem 5.2 there and the remarks before, the definition of the matrix A has to be modified, allowing for entries in the centralizer ring. We may view Theorem 3.5 above as the correct version of [12, Theorem 5.2]. The Λ-orthogonal basis described in Sections 5 and 6 of [12] does not generate the full space of cosine vectors, if there is σ with $m_\sigma > 1$ and $\mathbb{D}_\sigma \ncong \mathbb{R}$, and has to be modified accordingly. (We will consider this below in Section 5.)

4. Counterexamples to a result of Herman and Monson

The main case of interest of the preceding theory is when Ω is the vertex set of an abstract regular polytope P and G is the automorphism group of P. Equivalently, $G = \langle s_0, s_1, \ldots, s_{n-1} \rangle$ is a *string C-group* and $H = \langle s_1, \ldots, s_{n-1} \rangle$ is the stabilizer of some element of Ω. By definition, this means that the generators s_0, s_1, ... are involutions, that the *intersection property*

$$\langle s_i \mid i \in I \rangle \cap \langle s_j \mid j \in J \rangle = \langle s_k \mid k \in I \cap J \rangle$$

holds for all subsets I, $J \subseteq \{0, 1, \ldots, n-1\}$, and that $s_i s_j = s_j s_i$ for $|i - j| \geqslant 2$. Since the polytope can be recovered from the group G and the distinguished generators s_0, s_1, ..., s_{n-1} [14, Section 2E], we do not need to recall here what an abstract regular polytope actually *is*. The concepts of abstract regular polytopes and string C-groups are, in a certain sense, equivalent, and we work solely with the latter.

We now give an example which shows that we can have $m_\sigma > 1$ for σ of complex type, even when Ω is the vertex set of an abstract regular polytope. This shows that Theorem 2 in [4] is wrong. The example is a special case of a more general construction which we will consider afterwards.

4.1 Example. Consider the matrices

$$S_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 0 & 2 \\ 9 & 0 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 8 & -7 \\ -7 & -8 \end{pmatrix} \in \mathrm{SL}(2, 19).$$

It is not difficult to see that their images s_0, s_1 and s_2 in $G := \mathrm{PSL}(2, 19)$ generate G and that G is a string C-group with respect to these involutions (see Lemma 4.2 below). The element $s_1 s_2$ has order 3 and thus $H = \langle s_1, s_2 \rangle \cong S_3$ has order 6. Now G has an irreducible character χ of degree 9 with $\chi \neq \overline{\chi}$. We have $[(1_H)^G, \chi]_G = [1_H, \chi_H] = 2 > 1$. Thus the corresponding irreducible module over the reals has a Wythoff space of dimension 4 and essential Wythoff dimension (=multiplicity) 2. (The corresponding abstract regular polytope has Schläfli type $\{9, 3\}$.)

We are now going to show that there are in fact string C-groups with irreducible representations of complex type and arbitrary large essential Wythoff dimension. The following is probably well known:

4.2 Lemma. *Let $\mathbb{F}$ be a field. Let*

$$S_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 0 & y \\ -y^{-1} & 0 \end{pmatrix}, \quad S_2 = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \in \mathrm{SL}(2, \mathbb{F}),$$

where $y \neq 0, \pm 1$, $a^2 + b^2 = -1$ and $a \neq 0$. Then

$$G = \langle S_0, S_1, S_2 \rangle / \{\pm 1\} \leqslant \mathrm{PSL}(2, \mathbb{F})$$

is a string C-group.

Proof. Let s_i be the image of S_i in $\mathrm{PSL}(2, \mathbb{F})$. It is easily checked that s_0, s_1 and s_2 are mutually distinct involutions and that $s_0 s_2 = s_2 s_0$.

It remains to check the intersection property. For this, it suffices to show that

$$\langle s_0, s_1 \rangle \cap \langle s_1, s_2 \rangle = \langle s_1 \rangle = \{1, s_1\},$$

the other equalities then follow [14, Proposition 2E16]. We have

$$\langle s_0, s_1 \rangle \cap \langle s_1, s_2 \rangle = \langle s_1 \rangle C \quad \text{where} \quad C = \langle s_0 s_1 \rangle \cap \langle s_1 s_2 \rangle,$$

and we want to show that $C = \{1\}$. As

$$S_0S_1 = \begin{pmatrix} -y^{-1} & 0 \\ 0 & -y \end{pmatrix}, \quad y \neq y^{-1},$$

the matrix S_0S_1 and its powers have eigenvectors $(1,0)$ and $(0,1)$. Since

$$S_1S_2 = \begin{pmatrix} yb & -ya \\ -y^{-1}a & -y^{-1}b \end{pmatrix}, \quad ya \neq 0,$$

the vectors $(1,0)$ and $(0,1)$ are not eigenvectors of S_1S_2, but S_1S_2 has an eigenvector, possibly over an algebraic extension $\mathbb{E}$ of $\mathbb{F}$. Thus the elements of C fix three different lines in $\mathbb{E}^2$, and thus come from scalar matrices as claimed. □

The matrices in the last lemma have been used by Cherkassoff and Sjerve [2] to generate $\mathrm{PSL}(2,q)$ for $q \equiv -1 \mod 4$, $q \geqslant 19$. In fact, their argument shows the following, which is sufficient for our purposes:

4.3 Lemma. *In Lemma 4.2, let $\mathbb{F}$ be a field with p elements, where p is a prime and $p \equiv -1 \mod 4$, and let s_i be the image of S_i in $\mathrm{PSL}(2,p)$. If the order of s_0s_1 or s_1s_2 is $\geqslant 6$, then $\langle s_0, s_1, s_2\rangle = \mathrm{PSL}(2,p)$.*

Proof. We use Dickson's classification of the subgroups of $\mathrm{PSL}(2,p)$ [17, Chapter 3, Theorem 6.25]. By this classification, each proper subgroup of $\mathrm{PSL}(2,p)$ is a subgroup of a dihedral group, a group of affine type, which means that it is isomorphic to a subgroup of

$$\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; a \in \mathbb{F}^*, b \in \mathbb{F} \right\} / \{\pm 1\},$$

or it is isomorphic to one of the groups A_4, S_4 or A_5.

Since $p \equiv -1 \mod 4$ and $y \neq \pm 1$, we see that s_1 does not commute with any of s_0, s_2 and s_0s_2. It follows (as in [2]) that $G = \langle s_0, s_1, s_2\rangle$ is not a subgroup of a dihedral group, since in such a group we would have $\langle s_0, s_2\rangle \cap \mathbf{Z}(G) \neq \{1\}$.

Since $C_2 \times C_2 \cong \langle s_0, s_2\rangle \leqslant G$, the group can not be of affine type, either. Since G contains an element of order $\geqslant 6$, the exceptional cases $G \cong A_4$, S_4 or A_5 are ruled out, too. Thus $G = \mathrm{PSL}(2,p)$, as claimed. □

4.4 Lemma. *If $p \equiv -1 \mod 4$, then there is $\chi \in \mathrm{Irr}(\mathrm{PSL}(2,p))$ such that*

$$\chi(1) = \frac{p-1}{2}, \quad \chi(g) \in \mathbb{C} \setminus \mathbb{R} \quad \textit{if} \quad \mathbf{o}(g) = p,$$
$$\textit{and} \quad \chi(g) \in \{-1, 0, 1\} \ \textit{else}.$$

In particular, $\overline{\chi} \neq \chi$.

Proof. We show this by using the Weil representation of $\mathrm{SL}(2,p)$, which equals the symplectic group in dimension 2. The character ψ of the Weil representation has the property $|\psi(g)|^2 = |\mathrm{Ker}(g-1)|$ for all $g \in \mathrm{SL}(2,p)$, and decomposes into two irreducible characters $\psi = \psi_+ + \psi_-$ [6, Theorem 4.8]. (See also [5] and [15] for an elementary approach to the Weil representation.) Here $\psi_+(-1) = \psi_+(1)$, so that the kernel of ψ_+ contains $\{\pm 1\} = \mathbf{Z}(\mathrm{SL}(2,p))$ and we can view $\chi = \psi_+$ as character of $\mathrm{PSL}(2,p)$. On the other hand, the constituent ψ_- is defined by $\psi_-(-1) = -\psi_-(1)$. Thus we have $\psi(g) = \psi_+(g) + \psi_-(g)$ and $\psi(-g) = \psi_+(g) - \psi_-(g)$. It follows that

$$\chi(g) = \psi_+(g) = \frac{1}{2}(\psi(g) + \psi(-g)).$$

In particular, $\chi(1) = (p \pm 1)/2$. For our application this is actually all we need to know, but for completeness, let us mention that for $p \equiv -1 \mod 4$ we have $\psi(-1) = -1$, so $\chi(1) = (p-1)/2$. (This follows from the known formulas for ψ [18], but is easiest seen from remarking that $\psi_-(1)$ must be even because -1 is in the kernel of the determinant of ψ.)

If $g \in \mathrm{SL}(2,p)$ has order p, then $\psi(g) = \pm\sqrt{-p}$ [6, Corollary 6.2][18], and $\psi(-g) = -1$. (Again, we only need to know that $|\psi(-g)| = 1$.) Therefore, $\chi(g) = (\pm\sqrt{-p} - 1)/2$, and thus $\chi(g) \neq \overline{\chi(g)}$.

If neither $g \in \mathrm{SL}(2,p)$ nor $-g$ has order p, then the order of g is not divisible by p. In this case, $\psi(g)$ is rational [5, Proposition 2]. Also, we have $\mathrm{Ker}(g-1) = \mathrm{Ker}(g+1) = \{0\}$, except when $g = \pm 1$. It follows that $\psi(g), \psi(-g) \in \{\pm 1\}$. Thus $\chi(g) = (1/2)(\pm 1 \pm 1) \in \{-1, 0, 1\}$. □

4.5 Theorem. *There are abstract regular polytopes which have a pure realization of complex type with arbitrary large essential Wythoff dimension.*

Proof. Let p be a prime such that $p \equiv -1 \mod 4$ and $p \equiv 1 \mod 7$. Choose $y \in \mathbb{F}_p$ in Lemma 4.2 of multiplicative order 7, and let S_i and s_i be as in Lemmas 4.2 and 4.3. Then $s_0 s_1$ has order 7. By these lemmas, $G = \mathrm{PSL}(2,p)$ is a string C-group with respect to s_0, s_1 and s_2. Thus there is an abstract regular polytope with vertex set the right cosets of $H = \langle s_0, s_1 \rangle$. (Compared with Example 4.1, the rôles of s_0 and s_2 are now interchanged.) Notice that H is a dihedral group of order $2 \cdot 7 = 14$.

Let χ be the character of Lemma 4.4 and S an irreducible module over $\mathbb{R}G$ with character $\chi + \overline{\chi}$. Then the essential Wythoff dimension of S is

$$[(1_H)^G, \chi]_G = [1_H, \chi]_H \geqslant \frac{1}{14}\left(\frac{p-1}{2} - 13\right) = \frac{p-1}{28} - \frac{13}{14}.$$

Since there are infinitely primes p with $p \equiv -1 \mod 4$ and $p \equiv 1 \mod 7$ by Dirichlet's theorem, we can make this lower bound as large as we wish. □

The condition $p \equiv 1 \mod 7$ in the proof was chosen only for convenience. It is clear from the preceding lemmas that for "big" primes p, we usually get a lot of possibilities of representing $\mathrm{PSL}(2,p)$ as a string C-group of type $\{k,l\}$, with one or both of k, l "small".

Checking small primes suggests that every $\mathrm{PSL}(2,p)$, $19 \leqslant p \equiv -1 \mod 4$, is even a string C-group with respect to some generating set $\{s_0, s_1, s_2\}$ such that $s_0 s_1$ has order 3.

In [12, Remark 5.4], McMullen says that he has "not as yet encountered any instances with [essential Wythoff dimension] $w^* > 2$". Of course, the examples of Theorem 4.5 are such instances. However, another example is the 120-cell. As we mentioned in Example 3.6, there are two pure realizations of the 120-cell having Wythoff space of essential dimension 3.

Even another example are the duals of the polytopes $\mathcal{L}_p^3$ with group $\mathrm{PGL}(2,p)$ [10, 11]. The stabilizer of a facet of $\mathcal{L}_p^3$ has order 6, this is the stabilizer of a vertex of the dual polytope. Since $\mathrm{PGL}(2,p)$ is 2-transitive on the $p+1$ lines of $\mathbb{F}_p$ (in fact, sharply 3-transitive), the corresponding permutation character contains an irreducible character of degree p, which has values in $\{-1,0,1\}$ on the non-identity elements of $\mathrm{PGL}(2,p)$. The corresponding Wythoff space has dimension at least $(p-5)/6$.

5. Orthogonality

On the set of matrices $\mathbf{M}_\Omega(\mathbb{R})$, the standard inner product is defined by

$$\langle A, B\rangle = \mathrm{tr}(AB^t).$$

Now assume that $A = (a_{\xi\eta})$ and $B = (b_{\xi\eta})$ are G-invariant matrices, and fix some $\alpha \in \Omega$. Then for $\xi = \alpha g$ (say) we have

$$\sum_{\eta\in\Omega} a_{\xi\eta} b_{\eta\xi} = \sum_{\eta\in\Omega} a_{\alpha g,\eta} b_{\eta,\alpha g} = \sum_{\eta\in\Omega} a_{\alpha g,\eta g} b_{\eta g,\alpha g} = \sum_{\eta\in\Omega} a_{\alpha\eta} b_{\eta\alpha}.$$

Thus

$$\mathrm{tr}(AB^t) = \sum_{\xi,\eta\in\Omega} a_{\xi\eta} b_{\eta\xi} = |\Omega| \sum_{\eta\in\Omega} a_{\alpha\eta} b_{\eta\alpha}.$$

If additionally A and B are symmetric (for example, A and B are inner product matrices of realizations of Ω), then $\eta \mapsto a_{\alpha\eta} b_{\eta\alpha}$ is constant on the layers of Ω. Let $\xi_0 = \alpha, \xi_1, \ldots, \xi_r$ be representatives of the layers and define vectors a, $b \in \mathbb{R}^{r+1}$ by $a_i = a_{\alpha,\xi_i}$, $b_i = b_{\alpha,\xi_i}$. Let ℓ_i be the size of the layer containing ξ_i. Then

$$\mathrm{tr}(AB^t) = |\Omega| \sum_{\eta\in\Omega} a_{\alpha\eta} b_{\eta\alpha} = |\Omega| \sum_{i=0}^{r} \ell_i a_i b_i = |\Omega|^2 \langle a, b\rangle_\Lambda,$$

where $\langle a, b\rangle_\Lambda$ is the Λ-inner product defined by McMullen [12] for inner product vectors. So the correspondence between inner product vectors and inner product matrices identifies the Λ-inner product of McMullen with the standard inner product on matrices, up to a scalar. To maintain consistency with McMullen's notation, we write

$$\langle A, B\rangle_\Lambda = \frac{1}{|\Omega|^2}\operatorname{tr}(AB^t)$$

for G-invariant, symmetric matrices A and B.

5.1 Theorem. *If the simplex realization is written as the blend of realizations $A_1 \oplus \cdots \oplus A_s$, $A_i\colon \mathbb{R}\Omega \to V_i$, with inner product matrices Q_i, then*

$$\langle Q_i, Q_j\rangle_\Lambda = \delta_{ij}\frac{\dim(V_i)}{|\Omega|^2}.$$

Proof. The simplex realization is simply the identity $\mathrm{id}\colon \mathbb{R}\Omega \to \mathbb{R}\Omega$. The A_i are then simply the orthogonal projections onto V_i, as are the $Q_i = A_iA_i^t = A_i^2 = A_i$. It follows $Q_iQ_j = 0$ for $i \neq j$, and $\operatorname{tr}(Q_i^2) = \operatorname{tr}(Q_i) = \dim V_i$. □

Notice that the A_i's are not normalized realizations. To normalize A_i, we have to scale A_i by a factor $\sqrt{|\Omega|/\dim(V_i)}$. So for the cosine matrices $C_i = |\Omega|/\dim(V_i)$ of the A_i, we get $\langle C_i, C_i\rangle_\Lambda = 1/\dim(V_i)$. This is in accordance with [12, Theorem 4.5].

The Λ-orthogonal basis of the realization cone which McMullen constructs in [12] is in general too small, due to the mistake in [13]. We now indicate how to repair this. We need to find orthogonal bases of the subcones $\mathcal{RC}_\sigma(\Omega)$, for each $\sigma \in \operatorname{Irr}_{\mathbb{R}} G$. For this, we have to see what the isomorphism of Theorem 3.5 does to the scalar product. Suppose that A and $B \in \operatorname{End}_{\mathbb{R}G}(\mathbb{R}\Omega)$ are such that $e_\sigma A = A$ and $e_\sigma B = B$. Choose μ_i and π_i as in the proof of Theorem 3.5, and let $U = \mathbb{R}\Omega e_\sigma$. Then

$$\begin{aligned}\operatorname{tr}_{\mathbb{R}\Omega}(AB^t) = \operatorname{tr}_U(AB^t) &= \operatorname{tr}_U\Big(\sum_i \pi_i\mu_i AB^t \sum_j \pi_j\mu_j\Big)\\ &= \sum_i \operatorname{tr}_S(\mu_i AB^t\pi_i) = \operatorname{tr}_S\Big(\sum_{i,j} a_{ij}\overline{b_{ij}}\Big),\end{aligned}$$

where $a_{ij} = \mu_iA\pi_j \in \mathbb{D}$ and $\overline{b_{ij}} = (b_{ij})^t = (\mu_iB\pi_j)^t = \mu_jB^t\pi_i$. Let $d = \sum_{i,j} a_{ij}\overline{(b_{ij})} = \operatorname{tr}((a_{ij})(b_{ij})^*)$. Then $\operatorname{tr}_S(d) = (\dim_{\mathbb{R}} S)(d + \overline{d})/2$.

Thus the isomorphism of Theorem 3.5 respects the canonical inner products on the involved spaces, up to a scaling. It is now clear how to choose an orthogonal basis in the linear span of $\mathcal{RC}_\sigma(\Omega)$. For example, if $m = 2$ and $\mathbb{D} = \mathbb{C}$, we choose matrices corresponding to

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix},\quad \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad \begin{pmatrix}0 & i\\ -i & 0\end{pmatrix}$$

under the isomorphism of Theorem 3.5. Notice that the last two matrices do not correspond to realizations (they are not positive semi-definite). Also, if $m > 1$, the isomorphism of Theorem 3.5 is by no means canonical, and thus we do not get a uniquely defined basis.

6. Cosine vectors and spherical functions

In this section, we explain the relation between cosine vectors and spherical functions, and use it to show that the entries of a cosine vector of a realization with essential Wythoff dimension 1 are algebraic numbers. We continue to assume that G is a finite group, Ω is a transitive G-set and $H = G_\alpha$ is the stabilizer of some fixed initial vertex α. In the following, we set

$$e_H := e_{1_H} = \frac{1}{|H|} \sum_{h \in H} h.$$

6.1 Theorem. *Let S be a simple euclidean G-space with character σ and with centralizer ring $\mathbb{D} = \mathrm{End}_{\mathbb{R}G}(S)$. Let $W = \mathrm{Fix}_S(H)$ be the Wythoff space in S and let $w_1, \ldots, w_m$ be a basis of W over $\mathbb{D}$ such that the following hold: We have $\langle w_i, w_i \rangle = 1$, and whenever $i \neq j$ and $d_1, d_2 \in \mathbb{D}$, then $\langle w_i d_1, w_j d_2 \rangle = 0$. Then for all $g \in G$ we have*

$$\sigma(e_H g) = [\sigma, \sigma] \sum_{i=1}^{m} \langle w_i g, w_i \rangle.$$

Before beginning with the proof, let us show how to construct a basis as in the theorem: Begin with some $w_1 \in W$ such that $\langle w_1, w_1 \rangle = 1$. The orthogonal complement U of $w_1\mathbb{D}$ is closed under multiplication with $\mathbb{D}$, since $\langle ud, w_1 \rangle = \langle u, w_1 \overline{d} \rangle = 0$ for $u \in U$ and $d \in \mathbb{D}$. By induction on the dimension, we find a basis in U with the required properties, and thus one in W.

The case $m = 1$ of the theorem is worth mentioning as a separate corollary:

6.2 Corollary. *Let S be a simple euclidean G-space with character σ and essential Wythoff dimension $m = 1$. Then for any $w \in W = \mathrm{Fix}_S(H)$ with $\langle w, w \rangle = 1$ we have*

$$\langle wg, w \rangle = \frac{\sigma(e_H g)}{[\sigma, \sigma]}.$$

Thus the cosine matrix of the corresponding pure realization can be expressed in terms of the character of the corresponding irreducible representation.

To put Corollary 6.2 in perspective, we recall the notions of *Gelfand pairs* and *spherical functions*. (See [8, VII.1] or [1] for more on Gelfand pairs and spherical functions.) Let π be the permutation character of G on Ω (we can think of Ω as the set of right cosets of H in G here). The pair (G, H) is called a *Gelfand pair*, if

π is multiplicity free (as G-module over $\mathbb{C}$), that is, if $[\pi, \chi] \leqslant 1$ for all $\chi \in \mathrm{Irr}(G)$. (In our terminology, this is equivalent to all essential Wythoff dimensions being 1, and the Wythoff dimensions itself are 1 or 2.) If $[\pi, \chi] = 1$, then the corresponding *spherical function* s_χ is defined by

$$s_\chi(g) = \chi(e_H g) = \frac{1}{|H|} \sum_{h \in H} \chi(hg).$$

Thus Corollary 6.2 says that if S is of real type, then the entries of the corresponding cosine vector are values of the spherical function s_χ, and if S is of complex type, then the values of the cosine vector are the real parts of the spherical function. It is well known that spherical functions can be expressed using a G-invariant inner product [8, VII (1.6)].

For example, it is a remarkable fact that the irreducible representations of all finite Coxeter groups are of real type, and it is another remarkable fact that the automorphism group of almost every classical regular polytope acts multiplicity freely on the vertices of the polytope; the only exception is the 120-cell. In the other cases, the cosine vectors of the pure realizations are thus the spherical functions. These cosine vectors have been computed by McMullen [9, 11, 12].

Notice that when $\pi = (1_H)^G$ has a constituent σ of quaternion type, then (G, H) can not be a Gelfand pair, since then $\sigma = 2\chi$ and $[(1_H)^G, \chi]$ is a multiple of 2. We may say that (G, H) is a Gelfand pair over $\mathbb{R}$, if $m_\sigma \in \{0, 1\}$ for $\sigma \in \mathrm{Irr}_{\mathbb{R}} G$, that is, all essential Wythoff dimensions are 0 or 1.

Proof of Theorem 6.1. Suppose $\overline{d} = -d$ for $d \in \mathbb{D}$. Then

$$\langle vd, v\rangle = \langle v, v\overline{d}\rangle = -\langle v, vd\rangle = -\langle vd, v\rangle$$

and thus $\langle vd, v\rangle = 0$. We now choose a basis B of $\mathbb{D}$ over $\mathbb{R}$. If $\mathbb{D} = \mathbb{R}$, we choose $B = \{1\}$, if $\mathbb{D} = \mathbb{C}$, we choose $B = \{1, i\}$, and if $\mathbb{D} = \mathbb{H}$, we choose $B = \{1, i, j, k\}$. In each case, it follows that $\langle vb, vc\rangle = 0$ for $b \neq c \in B$ and $\langle vb, wb\rangle = \langle v, w\rangle$. Thus $\{w_i b \mid i = 1, \ldots, m, b \in B\}$ is an orthonormal basis of W over $\mathbb{R}$. Extend this basis by some set X (say) to an orthonormal basis of the whole space S. For any $\mathbb{R}$-linear map $\alpha\colon S \to S$ we have

$$\mathrm{tr}(\alpha) = \sum_{i,b} \langle w_i b\alpha, w_i b\rangle + \sum_{x \in X} \langle x\alpha, x\rangle.$$

We apply this to the map induced by $e_H g$. Since $xe_H = 0$ for $x \notin W$ and $we_H = w$

for $w \in W$, we get

$$\begin{aligned}\sigma(e_H g) = \operatorname{tr}(e_H g) = \sum_{i=1}^{m} \sum_{b \in B} \langle w_i b e_H g, w_i b \rangle &= \sum_{i=1}^{m} \sum_{b \in B} \langle w_i g b, w_i b \rangle \\ &= \sum_{i=1}^{m} \sum_{b \in B} \langle w_i g, w_i \rangle \\ &= |B| \sum_{i=1}^{m} \langle w_i g, w_i \rangle \\ &= [\sigma, \sigma] \sum_{i=1}^{m} \langle w_i g, w_i \rangle,\end{aligned}$$

as claimed. □

It follows from Corollary 6.2 that the values of the cosine vector are algebraic numbers, if $m = 1$. This confirms a "guess" of McMullen [12, Remark 9.4]. We can say somewhat more: It is known [8, VII(1.10)] that $(|HgH|/|H|)s_\chi(g)$ is an algebraic integer for spherical functions s_χ. We can extend this to the case where the essential Wythoff dimension is 1.

6.3 Corollary. *Let S be an irreducible euclidean G-space with essential Wythoff dimension $m = 1$ and let $w \in W = \operatorname{Fix}_S(H)$ have norm 1. Then*

$$\frac{|HgH \cup Hg^{-1}H|}{|H|} \langle wg, w \rangle$$

is an algebraic integer.

Notice that $|HgH \cup Hg^{-1}H|/|H|$ is the size of the corresponding layer. Another formulation of the corollary is thus: the component-wise product of a cosine vector of a pure realization of essential Wythoff dimension 1 with the layer vector has algebraic integers as entries.

Proof. For each double coset $K = HgH$, let

$$e_K = \frac{1}{|H|} \sum_{x \in K} x \in \mathbb{R}G.$$

It is known [8, remarks before VII(1.10)] that the product of two such elements is a $\mathbb{Z}$-linear combination of these elements. Thus $\mathbb{Z}[e_K \mid K \in H \setminus G/H]$ is a ring which is finitely generated as $\mathbb{Z}$-module, so its elements are integral.

Let $W = Se_H \cong \mathbb{D} = \operatorname{End}_{\mathbb{R}G}(S)$ be the Wythoff space. Then $e_K = e_{HgH}$ acts as some $\mathbb{D}$-linear map on W, and can thus be identified with some $d \in \mathbb{D}$. Then

$e_K + e_{K^{-1}} = e_{HgH} + e_{Hg^{-1}H}$ acts as the scalar $\lambda = d + \overline{d}$ on W. Since e_K is integral over $\mathbb{Z}$, it follows that d and λ are integral over $\mathbb{Z}$. In the case where $d \in \mathbb{R}$ we have

$$d = \frac{\sigma(e_K)}{[\sigma,\sigma]} = \frac{\sigma(e_H e_K)}{[\sigma,\sigma]} = \frac{1}{|H|}\sum_{x\in K}\langle wx, w\rangle = \frac{|K|}{|H|}\langle wg, w\rangle,$$

and in any case we have

$$\lambda = \frac{\sigma(e_K + e_{K^{-1}})}{[\sigma,\sigma]} = 2\frac{\sigma(e_K)}{[\sigma,\sigma]} = 2\frac{|K|}{|H|}\langle wg, w\rangle.$$

Notice that if K is symmetric, then necessarily $d \in \mathbb{R}$. The result follows. □

7. On the realizations of the 600-cell

In this section we explain two observations of McMullen [11, Remark 9.3] about the pure realizations of the 600-cell. Namely, we have the following:

7.1 Theorem. *There is a "natural" bijection between the irreducible characters of the finite group* $\mathrm{SL}(2,5)$ *and the pure realizations of the* 600*-cell. If* $\varphi \in \mathrm{Irr}(\mathrm{SL}(2,5))$*, then the corresponding pure realization has dimension* $\varphi(1)^2$*, and the entries of its cosine vector are of the form* $\varphi(u)/\varphi(1)$*, where* u *runs through* $\mathrm{SL}(2,5)$*. (More precisely, we also have a natural bijection between the conjugacy classes of* $\mathrm{SL}(2,5)$ *and the layers of the* 600*-cell, and* $\varphi(u)/\varphi(1)$ *is the value at the layer corresponding to the conjugacy class of* u*.)*

This "explains" that the dimension of each pure realization is a square q^2, and that its cosine vector has entries of the form a/q, where a is an algebraic integer (in fact, $a \in \mathbb{Z}[\tau]$ with $\tau = (-1+\sqrt{5})/2$).

We have to warn the reader that the proof of Theorem 7.1, while not difficult, is rather long, in particular longer than working out the cosine vectors directly. On the other hand, we work out the realization cone of a class of G-sets, of which the 600-cell is an example.

We will use that the automorphism group of the 600-cell, the reflection group of type H_4, is the factor group of a certain wreath product: Let U be a group. The cyclic group $C_2 = \{1, t\}$ of order 2 acts on the direct product $U \times U$ be exchanging components, that is $(u,v)^t = (v,u)$. The corresponding semidirect product of C_2 and $U \times U$ is the wreath product, denoted by $U \wr C_2$. The following lemma is of course known, but for completeness, we work out a large part of the proof:

7.2 Lemma. *Set* $U = \mathrm{SL}(2,5)$ *and* $\widehat{G} = U \wr C_2$*, and let* $\widehat{H}$ *be the subgroup of* $\widehat{G}$ *generated by the pairs* $\{(u,u) \mid u \in U\}$ *and by* C_2*. (Notice that* $\widehat{H} \cong C_2 \times U$*.) The automorphism group of the 600-cell is isomorphic to the factor group* $\widehat{G}/\mathbf{Z}(\widehat{G})$ *in such a way that the stabilizer of a vertex is identified with* $\widehat{H}/\mathbf{Z}(\widehat{G})$*.*

Proof. We can express the automorphism group of the 600-cell as a group of transformations on the quaternions $\mathbb{H}$. For $u \in \mathbb{H}$, let $\lambda_u \colon \mathbb{H} \to \mathbb{H}$ and $\varrho_u \colon \mathbb{H} \to \mathbb{H}$ be the maps defined by

$$x\lambda_u = \overline{u}x \quad \text{and} \quad x\varrho_u = xu \quad (x \in \mathbb{H}).$$

Let $\sigma \colon \mathbb{H} \to \mathbb{H}$ be conjugation.

Let U be a (finite) subgroup of the multiplicative group $\mathbb{H}^*$. Mapping t to σ and $(u, v) \in U \times U$ to $\lambda_u\varrho_u$ defines a group homomorphism from $U \wr C_2$ into $\mathrm{GL}_{\mathbb{R}}(\mathbb{H}) \cong \mathrm{GL}(4, \mathbb{R})$. The kernel is $\langle(-1, -1)\rangle \subseteq U \times U$.

The reflection group of type H_4 can be realized as the image of such a homomorphism: Let

$$\alpha_1 = j, \quad \alpha_2 = \frac{1}{2}(ai + bj - k), \quad \alpha_3 = k, \quad \alpha_4 = \frac{1}{2}(a + bi - k),$$

where $a = 2\cos(2\pi/5) = (-1 + \sqrt{5})/2$ and $b = 2\cos(4\pi/5) = (-1 - \sqrt{5})/2$. Then $\alpha_1, \ldots, \alpha_4$ form a simple root system of type H_4.

Let $s_1, \ldots, s_4$ be the reflections corresponding to $\alpha_1, \ldots, \alpha_4$. These generate the automorphism group G of the 600-cell, and the stabilizer of a vertex is $H = \langle s_1, s_2, s_3\rangle$. (The vertices are all points in the orbit of $1 = 1_{\mathbb{H}}$.)

The reflection corresponding to an element $\alpha \in \mathbb{H}$ of norm 1 is the map

$$x \mapsto -\alpha\overline{x}\alpha = x\sigma\lambda_{-\overline{\alpha}}\varrho_\alpha,$$

as is easily checked (it sends α to $-\alpha$ and fixes $i\alpha$, $j\alpha$ and $k\alpha$). It follows that

$$\langle s_1, s_2, s_3, s_4\rangle \subseteq \{\mathrm{id}_{\mathbb{H}}, \sigma\}\{\lambda_u\varrho_v \mid u, v \in U\},$$

where U is the group generated by $\alpha_1, \ldots, \alpha_4$ and -1.

Since $\alpha_1^2 = -1$ and $\alpha_4 = (\alpha_1\alpha_2)^2$, we see that $U = \langle\alpha_1, \alpha_2, \alpha_3\rangle$. We see that the reflections s_1, s_2, s_3 generate the subgroup

$$H = \{\mathrm{id}_{\mathbb{H}}, \sigma\}\{\lambda_u\varrho_u \mid u \in U\}.$$

Then it is also not difficult to see that

$$\langle s_1, s_2, s_3, s_4\rangle = \{\mathrm{id}_{\mathbb{H}}, \sigma\}\{\lambda_u\varrho_v \mid u, v \in U\}.$$

We leave out the proof that $U \cong \mathrm{SL}(2, 5)$. Apart from this, the lemma is proved. □

We now slightly change notation. Let U be an arbitrary finite group, let G be the wreath product $U \wr C_2$ and let $H \leqslant G$ be the subgroup

$$H = \{1, t\}\{(u, u) \mid u \in U\} \cong C_2 \times U.$$

We will describe the realization cone of the G-set $[G : H]$ (the cosets of H in G) for such G and H.

Set $N = U \times U$, a normal subgroup of G of index 2. The irreducible characters of N are of the form $\varphi \times \vartheta$ with $\varphi, \vartheta \in \operatorname{Irr} U$ [16, Theorem III.9.1].

7.3 Lemma.

(i) *If $\varphi \neq \vartheta \in \operatorname{Irr} U$, then $(\varphi \times \vartheta)^G \in \operatorname{Irr} G$.*

(ii) *For $\varphi \in \operatorname{Irr} U$, the character $\varphi \times \varphi$ has exactly two extensions to a character of G, namely*

$$\chi(t(u,v)) = \varphi(uv) \quad \textit{and} \quad \chi(t(u,v)) = -\varphi(uv).$$

Proof. The first point is clear from Clifford theory ($(\varphi \times \vartheta)^G$ denotes the Frobenius induced character).

It is also known that $\varphi \times \varphi$ has two different extensions to G [16, III.11]. Here, we can describe these extensions explicitly. Let X be a $\mathbb{C}U$-module affording the character φ. We may define an action of t on $X \otimes X$ by $(x \otimes y)t = y \otimes x$ or $(x \otimes y)t = -y \otimes x$. These are the two extensions to a representation of G.

We treat the first case. Then

$$(x \times y)t(u,v) = yu \otimes xv.$$

Suppose that $\{e_i\}$ is a basis of X and $e_i u = \sum_j d_{ij}(u) e_j$. Then $\{e_i \otimes e_j\}$ is a basis of $X \otimes X$, and we get for the trace of $t(u,v)$ on $X \otimes X$:

$$\chi(t(u,v)) = \sum_{i,j} d_{ji}(u) d_{ij}(v) = \sum_j d_{jj}(uv) = \varphi(uv). \qquad \square$$

Let U, G, H and N be as defined before the last lemma.

7.4 Lemma. *If $\chi \in \operatorname{Irr} G$ with $[\chi_H, 1] \neq 0$, then either $\chi = (\varphi \times \overline{\varphi})^G$ with $\varphi \neq \overline{\varphi} \in \operatorname{Irr} U$, or $\chi_N = \varphi \times \varphi$ with $\varphi = \overline{\varphi} \in \operatorname{Irr} U$ and $\chi(\sigma(u,v)) = \nu_2(\varphi)\varphi(uv)$. In both cases, $[\chi_H, 1] = 1$.*

(Here $\nu_2(\varphi)$ denotes the Frobenius-Schur indicator of φ. Recall that for $\varphi \in \operatorname{Irr} U$,

$$\nu_2(\varphi) = \frac{1}{2|U|} \sum_{u \in U} \varphi(u^2) \in \{0, \pm 1\},$$

and $\nu_2(\varphi) \neq 0$ if and only if $\varphi = \overline{\varphi}$ [16, Theorem III.5.1].)

Lemma 7.4 explains the first part of Theorem 7.1. Since $U = \mathrm{SL}(2,5)$ has only real-valued characters, every pure realization corresponds to a $\varphi \in \operatorname{Irr} U$ and has dimension $\varphi(1)^2$.

In the general case, notice that the realizations correspond to $\operatorname{Irr}_{\mathbb{R}} U$. The Wythoff dimension is 1 for all pure realizations. (In particular, the corresponding irreducible representations are of real type.) Thus the realization cone is polyhedral, in fact a direct product of copies of $\mathbb{R}_{\geqslant 0}$ by Theorem 3.5.

Proof of Lemma 7.4. First, suppose that $\chi = (\varphi \times \vartheta)^G$ with $\varphi \neq \vartheta \in \operatorname{Irr} U$. Then

$$\begin{aligned}[\chi_H, 1_H] = \Big[\big((\varphi \times \vartheta)^G\big)_H, 1_H\Big] &= \Big[\big((\varphi \times \vartheta)_{H\cap N}\big)^H, 1_H\Big] \\ &= [(\varphi \times \vartheta)_{H\cap N}, 1_{H\cap N}] \\ &= \frac{1}{|U|}\sum_{u\in U} \varphi(u)\vartheta(u) \\ &= [\varphi, \overline{\vartheta}]_U = \delta_{\varphi,\overline{\vartheta}}.\end{aligned}$$

Here the second equality follows from $G = HN$ and Mackey's formula, and the third equality follows from Frobenius reciprocity. Thus $\vartheta = \overline{\varphi} \neq \varphi$ when $[\chi_H, 1_H] \neq 0$.

Second, suppose that χ extends $\varphi \times \varphi$, and that $\chi(t(u, v)) = \varepsilon\varphi(uv)$. Then

$$\begin{aligned}[\chi_H, 1_H] &= \frac{1}{2|U|}\sum_{u\in U}\big(\chi((u, u)) + \chi(t(u, u))\big) \\ &= \frac{1}{2|U|}\left(\sum_{u\in U}\varphi(u)^2 + \sum_{u\in U}\varepsilon\varphi(u^2)\right) = \frac{1}{2}([\varphi, \overline{\varphi}] + \varepsilon\nu_2(\varphi)).\end{aligned}$$

The last expression is non-zero only when $\varphi = \overline{\varphi}$ and $\varepsilon = \nu_2(\varphi)$, and in this case $[\chi_H, 1] = 1$. □

The next result finishes the proof of Theorem 7.1. As in the last results, we only assume that $G = U \wr C_2$ for some finite group U, and that $H = C_2\{(u, u) \mid u \in U\}$. We notice in passing that in this situation,

$$Ht(x, y)H = H(x, y)H \leftrightarrow (x^{-1}y)^U \cup (y^{-1}x)^U$$

defines a bijection between double cosets of H and "symmetrized" conjugacy classes of U. The double cosets of H in turn correspond to the layers. (If $U = \mathrm{SL}(2, 5)$, then all conjugacy classes of U are real, that is, u and u^{-1} are always conjugate.) The following lemma describes an arbitrary entry of a cosine vector of a pure realization.

7.5 Lemma. *Let V be an irreducible euclidean G-space and suppose the non-zero element $w \in V$ is fixed by H. Then the character χ of V is irreducible. Let $\varphi \in \operatorname{Irr} U$ be the character defined in Lemma 7.4. Let $n = (x, y) \in N = U \times U$. Then*

$$\frac{\langle wn, w\rangle}{\langle w, w\rangle} = \frac{\varphi(x^{-1}y)}{\varphi(1)}.$$

Proof. Since $w \neq 0$ is fixed by H, we have $[\chi_H, 1_H] \neq 0$. It follows from Lemma 7.4 that $[\chi_H, 1_H] = 1$, and χ is as in that lemma. We may assume that $\langle w, w\rangle = 1$

and apply Corollary 6.2. We only treat the case that $\chi_N = \varphi \times \varphi$. (The case $\chi = (\varphi \times \overline{\varphi})^G$ is similar, but in fact simpler.) We get

$$\begin{aligned}\langle wn, w\rangle = \chi(e_H n) &= \frac{1}{2|U|}\left(\sum_{u\in U}\chi((ux,uy)) + \sum_{u\in U}\chi(t(ux,uy))\right)\\ &= \frac{1}{2|U|}\left(\sum_{u\in U}\varphi(ux)\varphi(uy) + \sum_{u\in U}\nu_2(\varphi)\varphi(uxuv)\right).\end{aligned}$$

The first sum equals $|U|\varphi(x^{-1}y)/\varphi(1)$ by the generalized orthogonality relation [7, Theorem 2.13] and the fact that $\varphi(uy) = \overline{\varphi(uy)} = \varphi(y^{-1}u^{-1})$. For the second sum, we get

$$\frac{1}{|U|}\sum_{u\in U}\varphi(uxuy) = \frac{1}{|U|}\varphi\left(\sum_{v\in U} v^2 x^{-1} y\right) = \varphi(zx^{-1}y),$$

where $z = (1/|U|)\sum_{v\in U} v^2$ is a central element in the group algebra and is mapped to a scalar matrix by any irreducible representation. Thus $\varphi(zx^{-1}y) = (\varphi(z)/\varphi(1))\varphi(x^{-1}y)$. But clearly, $\varphi(z) = \nu_2(\varphi)$. Plugging in above, we get that $\chi(e_H g) = \varphi(x^{-1}y)/\varphi(1)$ as claimed. □

References for Chapter VII

1. Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli. *Harmonic Analysis on Finite Groups*. Representation Theory, Gelfand Pairs and Markov Chains. Cambridge Studies in Advanced Mathematics 108. Cambridge University Press, 2008. DOI: 10.1017/CBO9780511619823. MR2389056(2009c:43001), Zbl. 1149.43001 (cited on p. 166).
2. Michael Cherkassoff and Denis Sjerve. On groups generated by three involutions, two of which commute. In: *The Hilton Symposium 1993*. (Montreal, Quebec). Ed. by Guido Mislin. CRM Proc. Lecture Notes 6. Amer. Math. Soc., Providence, RI, 1994, pp. 169–185. URL: http://www.math.ubc.ca/~sjer/3inv.pdf. MR1290589(95h:20039), Zbl. 0818.20035 (cited on p. 162).
3. *GAP – Groups, Algorithms, and Programming, Version 4.7.6*. The GAP Group. 2014. URL: http://www.gap-system.org (cited on p. 158).
4. Allen Herman and Barry Monson. On the real Schur indices associated with infinite Coxeter groups. In: *Finite Groups 2003*. Proceedings of the Gainesville Conference on Finite Groups. Ed. by Chat Yin Ho, Peter Sin, Pham Huu Tiep, and Alexandre Turull. Walter de Gruyter, Berlin and New York, 2004, pp. 185–194. MR2125072(2005k:20093), Zbl. 1135.20305 (cited on pp. 150, 151, 159, 161).
5. Roger E. Howe. On the character of Weil's representation. *Trans. Amer. Math. Soc.* **177** (1973), pp. 287–298. DOI: 10.1090/S0002-9947-1973-0316633-5, JSTOR: 1996597. MR0316633(47#5180), Zbl. 0263.22014 (cited on p. 163).

6. I. Martin Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math.* **95**, no. 3 (1973), pp. 594–635. DOI: 10.2307/2373731, JSTOR: 2373731. MR0332945(48#11270), Zbl. 0277.20008 (cited on p. 163).
7. I. Martin Isaacs. *Character Theory of Finite Groups*. Dover, New York, 1994. (Corrected reprint of the 1976 edition by Academic Press, New York). MR1280461, Zbl. 0849.20004 (cited on pp. 155, 156, 173).
8. Ian Grant Macdonald. *Symmetric Functions and Hall Polynomials*. Oxford Mathematical Monographs. Oxford University Press, 2nd ed. 1995. (With contributions by A. Zelevinsky). MR1354144(96h:05207), Zbl. 0824.05059 (cited on pp. 166–168).
9. Peter McMullen. Realizations of regular polytopes. *Aequationes Math.* **37**, no. 1 (1989), pp. 38–56. DOI: 10.1007/BF01837943. MR986092(90c:52014), Zbl. 0676.51008 (cited on pp. 149–151, 156, 167).
10. Peter McMullen. Regular polyhedra related to projective linear groups. *Discrete Math.* **91**, no. 2 (1991), pp. 161–170. DOI: 10.1016/0012-365X(91)90107-D. MR1124763(92f:52023), Zbl. 0746.52016 (cited on p. 164).
11. Peter McMullen. Realizations of regular polytopes, III. *Aequationes Math.* **82**, no. 1-2 (2011), pp. 35–63. DOI: 10.1007/s00010-010-0063-9. MR2807032, Zbl. 1226.51005 (cited on pp. 149, 151, 152, 164, 167, 169).
12. Peter McMullen. Realizations of regular polytopes, IV. *Aequationes Math.* **87**, no. 1-2 (2014), pp. 1–30. DOI: 10.1007/s00010-013-0187-9. MR3175095, Zbl. 1327.51023 (cited on pp. 149, 151, 153, 160, 164, 165, 167, 168).
13. Peter McMullen and Barry Monson. Realizations of regular polytopes, II. *Aequationes Math.* **65**, no. 1-2 (2003), pp. 102–112. DOI: 10.1007/s000100300007. MR2012404(2004k:51021), Zbl. 1022.51019 (cited on pp. 149–151, 156–160, 165).
14. Peter McMullen and Egon Schulte. *Abstract Regular Polytopes*. Encyclopedia of Mathematics and its Applications 92. Cambridge University Press, 2002. DOI: 10.1017/CBO9780511546686. MR1965665(2004a:52020), Zbl. 1039.52011 (cited on pp. 160, 161).
15. Amritanshu Prasad. On character values and decomposition of the Weil representation associated to a finite abelian group. *J. Analysis* **17** (2009), pp. 73–85. arXiv: 0903.1486 [math.RT]. MR2722604(2012a:11053), Zbl. 1291.11084 (cited on p. 163).
16. Barry Simon. *Representations of Finite and Compact Groups*. Graduate Studies in Mathematics 10. American Mathematical Society, Providence, RI, 1996. MR1363490(97c:22001), Zbl. 0840.22001 (cited on pp. 155, 156, 171).
17. Michio Suzuki. *Group Theory I*. Grundlehren der Mathematischen Wissenschaften 247. Springer-Verlag, Berlin, Heidelberg, and New York, 1982. (Translated from the Japanese by the author). MR648772(82k:20001c), Zbl. 0472.20001 (cited on p. 162).
18. Teruji Thomas. The character of the Weil representation. *J. London Math. Soc. (2)* **77**, no. 1 (2008), pp. 221–239. DOI: 10.1112/jlms/jdm098. MR2389926(2008k:11049), Zbl. 1195.11058 (cited on p. 163).

Selbständigkeitserklärung

Ich versichere hiermit an Eides statt, dass ich die vorliegende Arbeit selbständig angefertigt und ohne fremde Hilfe verfasst habe, keine außer den angegebenen Hilfsmitteln und Quellen dazu verwendet habe und die den benutzten Werken inhaltlich oder wörtlich entnommenen Stellen als solche kenntlich gemacht habe.

Rostock, den 30. Mai 2017.

Declaration (English translation of the above)

I hereby declare under oath that I have completed the work submitted here independently and have composed it without outside assistance. Furthermore, I have not used anything other than the resources and sources stated and where I have taken sections from these works in terms of content or text, I have identified this appropriately.