Universität Rostock

Traditio et Innovatio

Generic Symmetries of Group Representations

Dissertation

zur

Erlangung des akademischen Grades

doctor rerum naturalium (Dr. rer. nat.)

der Mathematisch-Naturwissenschaftlichen Fakultät

der Universität Rostock

vorgelegt von
Erik Friese, geb. am 22.03.1989 in Pasewalk
aus Rostock
Rostock, 20.08.2018

https://doi.org/10.18453/rosdok_id00002383

Gutachter:

Prof. Dr. Achill Schürmann, Universität Rostock

PD Dr. Barbara Baumeister, Universität Bielefeld

PD Dr. Frieder Ladisch, Universität Rostock

Tag der öffentlichen Verteidigung:

28.11.2018

Abstract

In the seventies, László Babai has classified all finite groups isomorphic to Euclidean symmetry groups of vertex transitive polytopes. In the same paper, Babai asked for a related classification of the affine symmetry groups of orbit polytopes. The present dissertation introduces an algebraic theory of "generic symmetries" of group representations which is capable not only to reprove Babai's classical result, but also to answer Babai's question.

To any representation $D\colon G \to \mathrm{GL}(V)$ of a finite group, we associate a permutation group $\mathrm{Sym}(G,V)$ on G which is connected to the linear symmetry groups of G-orbits in V. Under some mild hypotheses, we show that $\mathrm{Sym}(G,V) \cong \mathrm{GL}(Gv)$ holds for "almost all" $v \in V$. Over fields of characteristic zero, we derive an explicit formula characterizing $\mathrm{Sym}(G,V)$ only in terms of the character of D. In this way, any character of a real representation explicitly gives rise to the affine symmetry group of an orbit polytope (up to isomorphism).

Babai's question is answered by constructing specific characters. We show that the only finite groups not isomorphic to affine symmetry groups of orbit polytopes are the abelian groups of exponent greater than two, the generalized dicyclic groups, and the elementary abelian groups of order 4, 8, and 16.

Contents

1 Introduction

This dissertation is inspired by geometrical questions on the symmetries of orbit polytopes. We develop an algebraic theory on “generic symmetries” of modules over group algebras which is capable to answer not only these geometrical questions, but also more general algebraic questions which arise naturally in this context. We primarily use methods from (finite) group theory, representation theory, and algebraic geometry.

1.1 Motivation

For the moment, an *orbit polytope* P is defined as the convex hull of an orbit of a finite matrix group $G \leq \mathrm{GL}(n, \mathbb{R})$. That is, we have

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

for some $v \in \mathbb{R}^n$ (a more general definition will be given later). The vertex set of P is precisely the orbit Gv. Evidently, the multiplication by any element of G is a permutation on P. Let us call a matrix $A \in \mathrm{GL}(n, \mathbb{R})$ a *linear symmetry* of P if it satisfies $AP = P$. The set of all linear symmetries of P is a subgroup of $\mathrm{GL}(n, \mathbb{R})$ which we (for now) simply call the *linear symmetry group* of P. This group permutes the vertices of P, so it is finite provided that Gv is a generating set of $\mathbb{R}^n$. Now we see that, independently of v, G is always contained in the linear symmetry group of $\mathrm{Orb}(G, v)$. However, it depends both on G and on v to which extent an orbit polytope $\mathrm{Orb}(G, v)$ can have symmetries not contained in G.

Let us consider a very simple example. Let $G \leq \mathrm{GL}(2, \mathbb{R})$ be the cyclic rotation group of order four which is generated by the matrix

$$r = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Among the orbit polytopes of G, there is the trivial polytope $\mathrm{Orb}(G, 0)$ for which of course any matrix is a linear symmetry. For all nonzero points $v \in \mathbb{R}^2$, the polytope $P = \mathrm{Orb}(G, v)$ is a square centered at the origin. In any case, P has further linear symmetries not contained in G. As in Figure 1.1, we consider the points $v = (2, 2)^t$ and $w = (2, 1)^t$. It is easy to check that $\mathrm{Orb}(G, v)$ has an additional linear symmetry A, and $\mathrm{Orb}(G, w)$ has an additional linear symmetry B, where

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ and } B = \frac{1}{5}\begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix}.$$

Note that neither is A a linear symmetry of $\mathrm{Orb}(G, w)$, nor is B a linear symmetry of

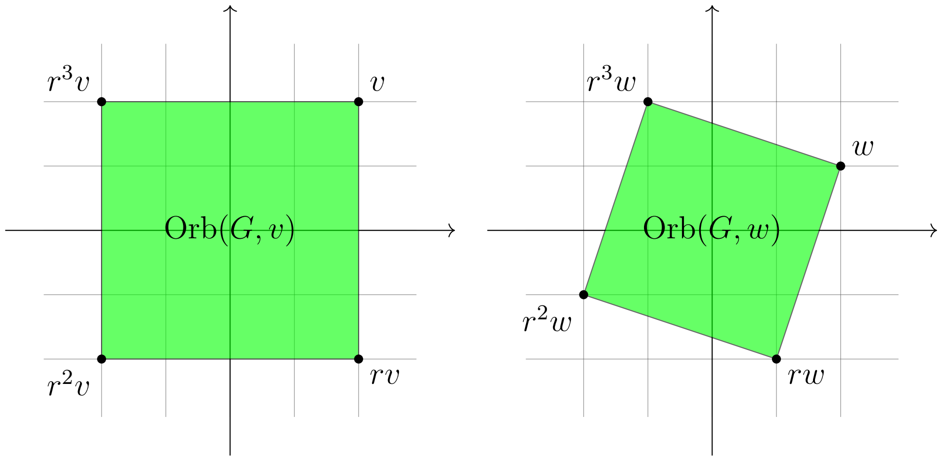


Figure 1.1: Nontrivial orbit polytopes of the cyclic rotation group of order four.

$\mathrm{Orb}(G, v)$. So different orbit polytopes of G can have different linear symmetry groups (which is actually the usual case). However, by regarding symmetries of a polytope as permutations of its vertices, we can see that A acts on $\mathrm{Orb}(G, v)$ in the same manner as B acts on $\mathrm{Orb}(G, w)$. As can be observed in Figure 1.1, the vertices of any nontrivial orbit polytope P of G can be labeled by the elements of G. Therefore, the linear symmetry group of P can (as it permutes the vertices of P) always be regarded as a permutation group on the group G itself. With that point of view, both A and B are naturally identified with the permutation (r, r^3) on G which interchanges the elements of order four, while leaving the other two elements fixed. In fact, the linear symmetry group of an arbitrary nontrivial orbit polytope of G is isomorphic to the permutation group $\langle (1, r, r^2, r^3), (r, r^3) \rangle \leq \mathrm{Sym}(G)$ which is a dihedral group of order eight. In conclusion, the linear symmetry groups of “almost all” orbit polytopes of G are isomorphic to the dihedral group of order eight. (For now, we use the term “almost all” just as a vivid phrase. Later on, we will give a precise mathematical meaning to it.)

In the last example we have observed only one orbit polytope which was exceptional in some sense (namely the trivial orbit polytope at the origin). To see other phenomena which may occur in this setting, we need to consider a slightly more complicated example (which is actually a linear symmetry group occurring in the last example). We consider the dihedral group $G \leq \mathrm{GL}(2, \mathbb{R})$ of order eight generated by the matrices

$$r = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } s = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

As before, we will determine the linear symmetry groups of the orbit polytopes of G. For a “generic point” $v \in \mathbb{R}^2$, the orbit polytope $\mathrm{Orb}(G, v)$ is a non-regular octagon with two different alternating lengths of edges, as shown in Figure 1.2. It can be shown that for these polytopes, G is the full linear symmetry group, and the permutations on G induced by linear symmetries are precisely the left multiplications by elements of G.

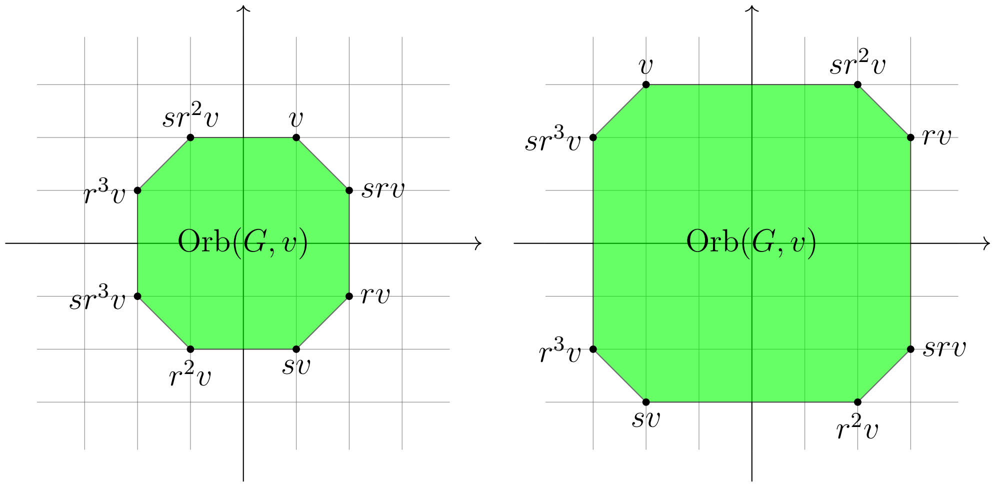


Figure 1.2: Orbit polytopes of G at "generic" points.

In contrast to the previous example, we can now distinguish three classes of exceptional orbit polytopes. To begin with, there is of course the trivial orbit polytope $\mathrm{Orb}(G,0)$ which does not contain a generating set of $\mathbb{R}^2$, which means that its linear symmetry group has infinite order. It is the only orbit polytope of G which is not full dimensional. Since G has order eight, all orbit polytopes of G have at most eight vertices. Among the two dimensional orbit polytopes, there is an exceptional class of polytopes $\mathrm{Orb}(G,v)$ with less than $|G|$ vertices. This happens precisely if the stabilizer G_v of v (and then also the stabilizer at any other vertex of $\mathrm{Orb}(G,v)$) in G is nontrivial. Figure 1.3 shows the orbit polytopes of G at $v=(2,2)^t$ and at $w=(2,0)^t$ which both are squares. As we have seen before, the linear symmetry groups of squares

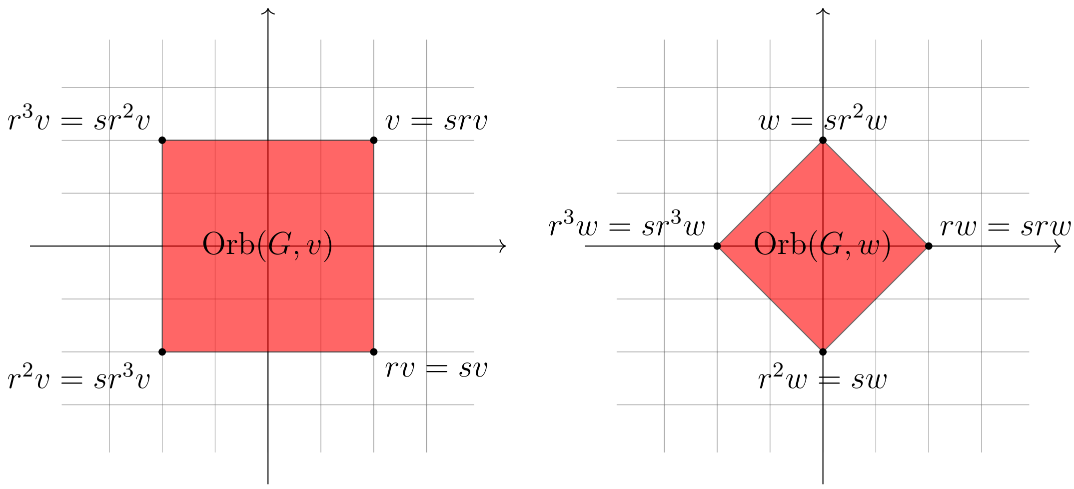


Figure 1.3: Exceptional class of orbit polytopes with nontrivial stabilizers at the vertices.

are always dihedral groups of order eight, so G is in fact the full linear symmetry group of both $\mathrm{Orb}(G, v)$ and $\mathrm{Orb}(G, w)$. However, as we can see in the picture, the vertices of $\mathrm{Orb}(G, v)$ and $\mathrm{Orb}(G, w)$ are not in one to one correspondence with the elements of G anymore. Instead, each vertex is labeled by a left coset of G_v, or of G_w, respectively. For this reason, linear symmetries can still be described by permutations on G, but not in a unique manner. For example, the identity permutation and the permutation $\pi = (r, s) \in \mathrm{Sym}(G)$ both describe the trivial symmetry of $\mathrm{Orb}(G, v)$. Also note that there is no linear symmetry of $\mathrm{Orb}(G, w)$ which is described by π. In fact, the permutations on G describing linear symmetries for all exceptional orbit polytopes of this class, are the left multiplications by elements of G.

By looking at the pictures, one might guess that by choosing a point $v \in \mathbb{R}^2$ carefully, we might get an orbit polytope $\mathrm{Orb}(G, v)$ which is a regular octagon, and so has further linear symmetries. This is indeed the case. These polytopes form the last exceptional class consisting of all those orbit polytopes $\mathrm{Orb}(G, v)$ which have full dimension, and trivial stabilizers at the vertices, but strictly more linear symmetries than the "generic" orbit polytopes. One such example, $P = \mathrm{Orb}(G, v) = \mathrm{Orb}(G, w)$ for $v = (1 + \sqrt{2}, 1)$, and $w = sr^2v = (-1 - \sqrt{2}, 1)$, is shown in Figure 1.4. Up to dilation, P is the only orbit

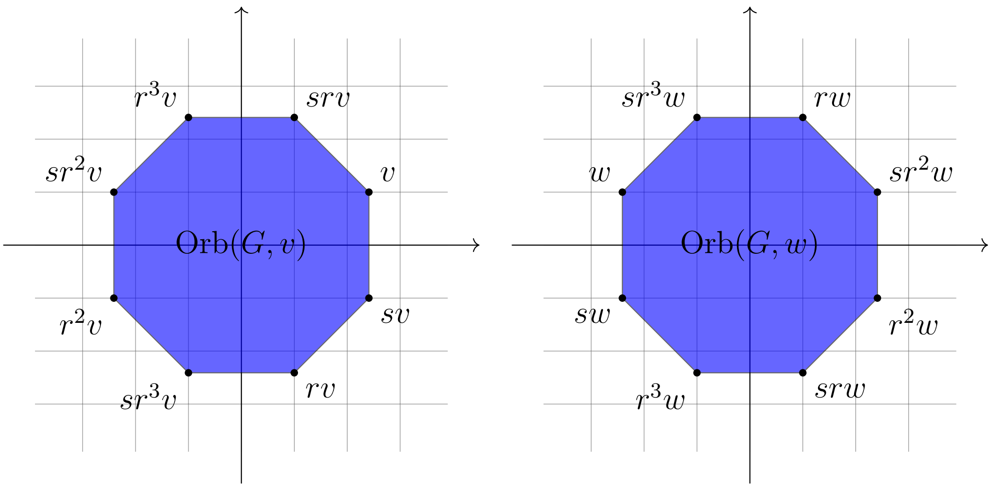


Figure 1.4: Two different labelings of an orbit polytope with extra symmetries.

polytope of G with additional linear symmetries. All exceptional orbit polytopes of this type have the same linear symmetry group, a dihedral group of order 16 (generated by s and by a rotation matrix of order 8). However, different labelings of the vertices of P lead to different permutation groups on G. For example, the labeling given by v (on the left side in Figure 1.4) has a linear symmetry described by the permutation $\pi = (1, s, r, sr^3, r^2, sr^2, r^3, sr)$, and in fact the full linear symmetry group of P is generated as a permutation group on G by the left multiplications and by π. But π does obviously not describe a linear symmetry of P with respect to the labeling given by w (see the right side in Figure 1.4). So we see again that the linear symmetry groups of exceptional orbit polytopes may induce different permutation groups on G. We shall see later that this obstruction does not occur for "generic" orbit polytopes.

Figure 1.5 gives an overview about the distribution of generic and exceptional points of G in the plane. The red colored points have a nontrivial stabilizer in G, and so their

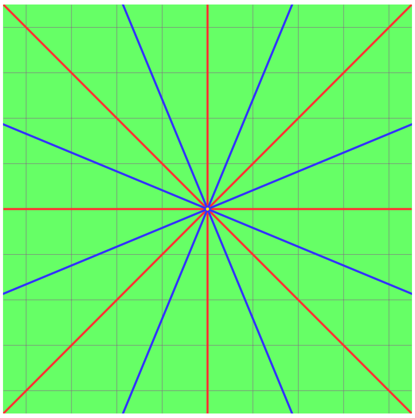


Figure 1.5: Generic and exceptional regions for the dihedral group of order eight.

orbit polytopes have fewer vertices than G has elements. The blue colored points are those whose orbit polytopes have extra symmetries (in comparison to the other full dimensional orbit polytopes). Finally, the green colored points are those which we will call "generic" points. As a permutation group on the vertices, the linear symmetry group of any generic orbit polytope is isomorphic to a specific permutation group on the group G itself. In the picture, we see that the generic points cover almost the entire plane. So, as in the previous example, we see that almost all orbit polytopes of G have isomorphic (in this case even identical) linear symmetry groups.

1.2 Some main results

The previously introduced geometrical observations were communicated to me by Achill Schürmann, who conjectured that similar phenomena occur for arbitrary matrix groups in any dimension. I have worked on these questions in cooperation with Frieder Ladisch. To a large extent, the results presented here are already published in [8, 9, 10, 19]. My objective is to present the essential part of our theory in a straight-lined, and self contained way. Many definitions and results are generalized, some results are even improved. Most of the matrix-theoretic arguments are replaced by coordinate-free arguments, and some proofs are simplified.

In the following chapters, we will show that the previous observations actually generalize to arbitrary finite matrix groups $G \leq \mathrm{GL}(n, \mathbb{R})$ in any dimension. (We will also consider other fields than the real numbers, but for simplicity, we keep considering this example in the present section.) It is always true that almost all points of the space are generic in the sense that their orbit polytopes have linear symmetry groups which are isomorphic to a specific permutation group on G (Theorem 3.5.2). We call this permutation group the *generic symmetry group* of G. Moreover, the linear symmetry groups of generic orbit polytopes are conjugated (not merely isomorphic) in $\mathrm{GL}(n, \mathbb{R})$

(Proposition 3.8.2). Recall that the dihedral group we considered in the second example (which was constructed as the linear symmetry group of an orbit polytope in the first example) has the property that its generic orbit polytopes admit no further linear symmetries. We call a matrix group with that property *generically closed*. It is a general fact that linear symmetry groups of orbit polytopes are generically closed (Theorem 3.8.6).

Another interesting fact is that the generic symmetry group of G is uniquely determined by the character χ of G (that is, by the traces of the matrices in G). This is where representation theory comes into play. Later on, we drop the geometric viewpoint, and we define the generic symmetry group of any character of an abstract finite group G to be the generic symmetry group of a corresponding representation. Among many other structural results, we give a characterization of the generic symmetry group of a character χ of G in terms of a formula only depending on χ (Theorem 5.1.10). This characterization allows us to compute the linear symmetry groups (as permutation groups) of the generic orbit polytopes of some matrix group G just by looking at the traces of the matrices in G. On the other hand, Theorem 5.1.10 also has stunning theoretical consequences. We use it to classify all finite groups which are isomorphic to the *affine symmetry group* of an orbit polytope (Theorem 6.4.4). Thereby, we answer a question of Babai from 1977 who classified the finite groups isomorphic to Euclidean symmetry groups of vertex transitive polytopes (so Theorem 6.4.4 is the affine analog to Babai's classification) [1]. To demonstrate the power of the theory developed here, we give a new proof of Babai's classification (Theorem 7.2.2). Finally, in Theorem 7.3.1, we answer an analogous question on unitary matrix groups, which is not about polytopes anymore, but which comes up naturally in our setting.

It is worth noting that, in contrast to the previous examples, different generic orbit polytopes of a matrix group do not necessarily have the same combinatorial type. In [29, Theorem 5.5], Onn gave an example of two orbit polytopes of the symmetric group S_4 acting on a 5-dimensional Euclidean space, which are generic in our sense but which have different numbers of facets. But anyway, we drop the notion of polytopes later on, as we merely study the linear symmetries of the orbits of a group. This perspective allows a generalization to arbitrary fields. Since there is no notion of convexity over arbitrary fields, we shall not address questions on the combinatorial type of orbit polytopes.

1.3 Related work

It is probably folklore that any finite group is isomorphic to the (affine or Euclidean) symmetry group of some polytope. A result of Isaacs [16] implies that any finite group can be realized as the symmetry group of a polytope having at most two orbits of vertices. Moreover, Schulte and Willems have shown that any finite group can be realized as the combinatorial symmetry group of some polytope [32]. A shorter proof of a slightly stronger statement has been given by Doignon [6].

Orbit polytopes can be seen as the building blocks for polytopes with symmetries in general. They turn up for example in (integer) convex optimization problems, where the exploitation of their symmetries can be effectively used to reduce computation time [13, 14, 20]. Orbit polytopes have been studied by a number of authors [2, 28, 29, 31, 34]. An important subclass of orbit polytopes is the class of *representation polytopes*. A representation polytope is the convex hull of a finite matrix group over the real numbers. If the group consists of permutation matrices, the polytope is called a *permutation polytope*. Representation polytopes and permutation polytopes have received considerable attention [3, 12, 15, 27]. The determination of their linear symmetries is called a *linear preserver problem*, which has been studied especially in the case of finite reflection groups [24, 25, 26].

As already mentioned before, Babai has classified the finite groups isomorphic to Euclidean symmetry groups of vertex transitive polytopes [1]. It is easy to see (by choosing an appropriate inner product) that the affine symmetry group of any orbit polytope is isomorphic to the Euclidean symmetry group of a vertex transitive polytope (the converse does not hold). Babai's classification is closely related to the *GRR-problem*. It asks whether a finite group G admits a *graphical regular representation*, that is, a simple graph Γ with vertex set G such that G is the full automorphism group of Γ acting regularly on itself. Babai has shown directly that any finite group admitting a GRR is isomorphic to the Euclidean symmetry group of a vertex transitive polytope (in fact, a certain simplex). The finite groups not admitting a GRR have been classified in [11]. It follows from this classification, and our Theorem 6.4.4 that there are exactly ten finite groups (up to isomorphism) which are isomorphic to the affine symmetry group of an orbit polytope, but admit no GRR. Only three of them are not isomorphic to the Euclidean symmetry group of a vertex transitive polytope.

By dropping the notion of convexity, one might consider more generally the linear symmetry groups (that is, the setwise stabilizers) of the orbits of finite matrix groups $G \leq \mathrm{GL}(n, \Bbbk)$ over arbitrary fields $\Bbbk$. A classical result of Isaacs states that G is the full linear symmetry group of one of its orbits (that is, $G = \mathrm{GL}(Gx)$ for some $x \in \Bbbk^n$) provided that $\Bbbk$ has infinite order, and G is absolutely irreducible on $\Bbbk^n$ [16]. We generalize that statement in Theorem 4.5.4. As an immediate application, we conclude that any non-abelian finite group G embeds as a subgroup into $\mathrm{GL}(n, \mathbb{C})$ for some n such that $G = \mathrm{GL}(Gx)$ for some $x \in \mathbb{C}^n$ (see Theorem 6.1.1).

1.4 Outline

The dissertation is organized as follows. The following Chapter 2 introduces some standard techniques from algebraic geometry which will be used continuously.

In Chapter 3, we introduce all concepts mentioned in the motivational examples in a very general context. Initially, we consider an arbitrary finite group G, and an arbitrary field $\Bbbk$ of infinite order (later on, finite fields are considered as well). We give a precise mathematical meaning to the phrase "almost all", which we used in an informal way so far. Using this terminology, we associate to any finitely generated $\Bbbk G$-module V a finite permutation group $\mathrm{Sym}(G, V)$ on G, which only depends on the isomorphism type of V. We call $\mathrm{Sym}(G,V)$ the *generic symmetry group* of V. We show that the linear symmetry groups (when appropriately defined) of almost all G-orbits in V are isomorphic to (a certain quotient of) $\mathrm{Sym}(G,V)$, which leads to the notion of *generic points*. The finite groups isomorphic to the affine symmetry groups of orbit polytopes are characterized as those groups G admitting a *generically closed* $\mathbb{R}G$-module, that is, an $\mathbb{R}G$-module V on which G acts faithfully satisfying $|\,\mathrm{Sym}(G,V)| = |G|$.

In Chapter 4, we take a completely different view on generic symmetries. The key observation is that the generic symmetries of a $\Bbbk G$-module are precisely those permutations on G fixing a corresponding isomorphism class of left ideals in $\Bbbk G$. By studying these *ic-symmetries* separately, we finally obtain structural results on generic symmetry groups. Most importantly, we obtain (with some restrictions) an abstract characterization of the generic symmetries of a module just in terms of its isomorphism type. It implies a strong sufficient criterion for being generically closed, generalizing the result of Isaacs mentioned before.

In Chapter 5, we restrict the attention to fields $\Bbbk$ of characteristic zero, where all $\Bbbk G$-modules are determined up to isomorphism by their characters. We translate the main definitions and the main results to the character-theoretic language. Most importantly, we associate to any character χ of G the *generic symmetry group* $\mathrm{Sym}(G,\chi)$, which is characterized by a formula in terms of two certain constituents of χ. We develop a foundation, allowing the application of that characterization to induced characters in several situations.

In Chapter 6, we study which finite groups admit generically closed modules over the fields of real and complex numbers. In the complex case, this question is positively answered for all non-abelian groups, but it remains open for most abelian groups. In the real case, we give a complete classification. Thereby, we also classify all finite groups isomorphic to affine symmetry groups of orbit polytopes. This answers a question of Babai (1977) who classified the Euclidean symmetry groups of vertex transitive polytopes.

Finally, in Chapter 7, we show that the theory on generic symmetries can be easily extended to achieve results about *orthogonal symmetries* of orbits (and about Euclidean symmetry groups of vertex transitive polytopes). In complete analogy to the considerations of Chapter 3, we associate to any finitely generated $\mathbb{R}G$-module V (or equivalently, to its character χ) a permutation group $\mathrm{OSym}(G,V)$ ($\mathrm{OSym}(G,\chi)$, respectively) on G which we call an *orthogonal generic symmetry group*. If G acts on V by orthogonal transformations then the orthogonal symmetry groups of almost all G-orbits in V are isomorphic to (a certain quotient of) $\mathrm{OSym}(G,V)$. That is, we have an analog of *generic points* also in the orthogonal setting. As an immediate application, we give a new proof of Babai's classification. We also consider the case of *unitary symmetries* of orbits, which turns out to be particularly simple.

2 Prerequisites

In this chapter, we recall some basic facts from algebraic geometry which are needed in the following chapters. The literature is usually divided into classical algebraic geometry which studies zero sets of polynomials over algebraically closed fields, and into modern algebraic geometry which is the geometry of schemes. We need some topological aspects of algebraic geometry which are closely related to the classical theory, but we need to consider arbitrary fields (of infinite order) instead of algebraically closed fields only. There are textbooks covering this setting to a certain extent (such as [7]), but there are still some basic facts which seem to be folklore but which are hard to find in literature. We present such standard facts here with proofs included.

2.1 Zariski topology

We introduce the *Zariski topology* which can be defined on any finite dimensional vector space. Let $\Bbbk$ be a field, and let V be a finite dimensional $\Bbbk$-vector space with basis $B = \{b_1, \dots, b_n\}$, say. A map $f\colon V \to \Bbbk$ is said to be *polynomial* if there is a polynomial $p \in \Bbbk[X_1, \dots, X_n]$ such that

$$f(\lambda_1 b_1 + \cdots + \lambda_n b_n) = p(\lambda_1, \dots, \lambda_n) \text{ for all } \lambda_i \in \Bbbk.$$

This definition does not depend on the actual choice of the basis B, so polynomial maps are defined intrinsically on V. The set of all polynomial maps $V \to \Bbbk$ is denoted by $\Bbbk[V]$. With respect to the usual addition and multiplication of functions, $\Bbbk[V]$ is a finitely generated commutative $\Bbbk$-algebra (generated by any dual basis of V). By Hilbert's basis theorem [7, 15.1 Corollary 5], $\Bbbk[V]$ is a Noetherian ring, that is, all ideals of $\Bbbk[V]$ are finitely generated.

For any set of polynomial maps $I \subseteq \Bbbk[V]$ on V, we consider the corresponding zero set in V, that is, the set

$$\operatorname{zeros}(I) = \{v \in V : f(v) = 0 \text{ for all } f \in I\}.$$

It is easy to see that the ideal of $\Bbbk[V]$ generated by I has the same zero set as I, so we may restrict to the zero sets of ideals. Of course, we have $\operatorname{zeros}(\{0\}) = V$, and $\operatorname{zeros}(\Bbbk[V]) = \emptyset$. Moreover, we have

$$\operatorname{zeros}(I) \cup \operatorname{zeros}(J) = \operatorname{zeros}(IJ), \text{ and } \bigcap_k \operatorname{zeros}(I_k) = \operatorname{zeros}\left(\sum_k I_k\right)$$

for all ideals $I, J \subseteq \Bbbk[V]$, and for all (possible infinite) families of ideals $(I_k)_k$. So the zero sets of ideals of $\Bbbk[V]$ form the closed subsets of a topology on V, which is called the *Zariski topology* on V. For any polynomial map $f \in \Bbbk[V]$ there is a corresponding *principal open set* $V_f = \{v \in V : f(v) \neq 0\}$. As the name suggests, all principal open sets are open in the Zariski topology. Conversely, any open set of V is a union of principal open sets (in fact a finite union, as we will see soon). So the principal open sets form a basis of the Zariski topology.

Many properties of the Zariski topology ultimately rely on the following well known fact.

Lemma 2.1.1. *Let $\mathbb{E}$ be a field, let $\Bbbk \subseteq \mathbb{E}$ be a subfield of infinite order, and let n be any positive integer. Then the only polynomial $p \in \mathbb{E}[X_1, \dots, X_n]$ vanishing on all elements of $\Bbbk^n$ is the zero polynomial $p = 0$.*

Proof. This is proven by induction on n. For $n = 1$ we are done by the well known fact that any nonzero polynomial in one indeterminate has only finitely many zeros. For $n > 1$, we consider p as

$$p = \sum_{i=0}^{m} p_i(X_1, \dots, X_{n-1}) X^i \text{ for certain } p_i \in \mathbb{E}[X_1, \dots, X_{n-1}],$$

where $p_m \neq 0$. By the inductive hypothesis, there are elements $\lambda_1, \dots, \lambda_{n-1} \in \Bbbk$ such that $p_m(\lambda_1, \dots, \lambda_{n-1}) \neq 0$. Now $p(\lambda_1, \dots, \lambda_{n-1}, X_n)$ is a nonzero polynomial in one indeterminate, which does not vanish on some $\lambda_n \in \Bbbk$. □

Let V be an n-dimensional vector space over an infinite field $\Bbbk$. As an immediate consequence of Lemma 2.1.1, we get that any morphism $\Bbbk[X_1, \dots, X_n] \to \Bbbk[V]$ of $\Bbbk$-algebras sending the indeterminates to a dual basis of V is an isomorphism. In particular, $\Bbbk[V]$ is a factorial integral domain.

Lemma 2.1.2. *Let V be a finite dimensional vector space over a field $\Bbbk$ carrying the Zariski topology. Then the following holds.*

(1) All finite subsets of V are closed (that is, V satisfies the T_1-axiom).

(2) Any subset of V is compact.

(3) If $\Bbbk$ has infinite order then V is an irreducible topological space, that is, the intersection of any two nonempty open subsets is nonempty again.

Here we call a topological space X *compact* if any open cover of X has a finite subcover. We do not impose a compact space to satisfy the Hausdorff property.

Proof. Concerning (1), it suffices to show that all singletons are closed. This comes down to show that for any two distinct points $v, w \in V$, there is a polynomial map $f \in \Bbbk[V]$ such that $f(v) = 0$ and $f(w) \neq 0$. There is certainly a linear form $\lambda\colon V \to \Bbbk$ such that $\lambda(v) \neq \lambda(w)$. Then f can be chosen as the map $x \mapsto \lambda(x) - \lambda(v)$.

Concerning (2), let $X \subseteq V$ be any subset, and let $X \subseteq \bigcup_{f \in I} V_f$ be a covering of X by principal open sets, where $I \subseteq \Bbbk[V]$. We have to show that X is already covered by a finite subcollection of these sets. By Hilbert's basis theorem, there is a finite set $I_0 \subseteq I$ such that I and I_0 generate the same ideal of $\Bbbk[V]$. Therefore, we have $\operatorname{zeros}(I) = \operatorname{zeros}(I_0)$, and hence $\bigcup_{f\in I} V_f = \bigcup_{f\in I_0} V_f$. In particular, X is already covered by the finitely many sets V_f for $f \in I_0$.

Concerning (3), we may also restrict to principal open sets. Since we have $V_f \cap V_g = V_{fg}$ for all $f, g \in \Bbbk[V]$, the claim follows immediately by Lemma 2.1.1 (and by the subsequent observation that $\Bbbk[V]$ is an integral domain). □

As before, let V be any finite dimensional $\Bbbk$-vector space carrying the Zariski topology. If $\mathbb{E}$ is any extension field of $\Bbbk$, we may consider the $\mathbb{E}$-vector space $V^{\mathbb{E}} = \mathbb{E} \otimes_{\Bbbk} V$ which is called the *scalar extension* of V to $\mathbb{E}$. Since $\dim_{\mathbb{E}}(V^{\mathbb{E}}) = \dim_{\Bbbk}(V)$, the extended space $V^{\mathbb{E}}$ is finite dimensional again, and so carries a Zariski topology (over $\mathbb{E}$). By considering the canonical injective $\Bbbk$-linear map $V \to V^{\mathbb{E}}$, $v \mapsto 1 \otimes v$, we may regard V as a subset of $V^{\mathbb{E}}$. The following lemma shows that V is actually a topological subspace of $V^{\mathbb{E}}$ in that way.

Lemma 2.1.3. *Let $\mathbb{E}/\Bbbk$ be any field extension, let V be a $\Bbbk$-vector space carrying the Zariski topology over $\Bbbk$, and let $V^{\mathbb{E}}$ be the scalar extension of V carrying the Zariski topology over $\mathbb{E}$. Then the natural map $\kappa\colon V \to V^{\mathbb{E}}$, $v \mapsto 1 \otimes v$ is an embedding of topological spaces (that is, the induced map $V \to \kappa(V)$ is a homeomorphism). If, moreover, $\Bbbk$ has infinite order then $\kappa(V)$ is dense in $V^{\mathbb{E}}$.*

Proof. By fixing a $\Bbbk$-basis $\{b_1, \dots, b_n\}$ of V, any polynomial $p \in \Bbbk[X_1, \dots, X_n]$ can be regarded as a polynomial map $V \to \Bbbk$. The corresponding principal open set is denoted by V_p. We use the $\mathbb{E}$-basis $\{1 \otimes b_1, \dots, 1 \otimes b_n\}$ of $V^{\mathbb{E}}$ to relate polynomials $p \in \mathbb{E}[X_1, \dots, X_n]$ to principal open sets $V_p^{\mathbb{E}}$ in the same way. Now we have $V_p = \kappa^{-1}(V_p^{\mathbb{E}})$ for all $p \in \Bbbk[X_1, \dots, X_n]$, which already shows that any (principal) open subset of V is also open in the subspace topology inherited by $V^{\mathbb{E}}$.

To prove the first claim, it remains to show that any (principal) open set of $V^{\mathbb{E}}$ has an open pre-image in V. Let $p \in \mathbb{E}[X_1, \dots, X_n]$ be any polynomial. It can be written as

$$p = \sum_{i=1}^{m} \lambda_i p_i \text{ with } \lambda_i \in \mathbb{E}, \text{ and } p_i \in \Bbbk[X_1, \dots, X_n],$$

where $\lambda_1, \dots, \lambda_m$ are linearly independent over $\Bbbk$. So p vanishes on an n-tuple $x \in \Bbbk^n$ if and only if each p_i vanishes on x. Consequently, we have $\kappa^{-1}(V_p^{\mathbb{E}}) = V_{p_1} \cup \dots \cup V_{p_m}$, proving that the Zariski topology on V coincides with the subspace topology inherited by $V^{\mathbb{E}}$.

Now suppose that $\Bbbk$ is a field of infinite order. Proving that κ has a dense image in $V^{\mathbb{E}}$ means to show that any nonempty (principal) open set of $V^{\mathbb{E}}$ has a nonempty pre-image in V. This follows by Lemma 2.1.1. □

It is well known that, when it comes to the Zariski topology, the product topology is not the "right topology" on a Cartesian product of vector spaces (and other algebraic varieties). For example, over the field $\mathbb{C}$ of complex numbers the product topology on the Cartesian product $\mathbb{C} \times \mathbb{C}$ of one dimensional spaces is different from the Zariski topology on the two dimensional space $\mathbb{C}^2$. To keep things simple, we shall agree that a direct sum $V_1 \oplus V_2$ of vector spaces V_1, V_2 does always carry the Zariski topology. Any open subset $O \subseteq V$ of a vector space V will be regarded as a topological subspace of V. In particular, if $O_1 \subseteq V_1$ and $O_2 \subset V_2$ are open subsets, $O_1 \times O_2$ carries the subspace topology inherited by the Zariski topology on $V_1 \oplus V_2$. For linear subspaces $W \leq V$ there is no ambiguity since the Zariski topology on W coincides with the subspace topology inherited by V.

2.2 Rational maps

As usual in topology, we will frequently use continuous maps to construct open sets as pre-images of other open sets. However, when it comes to the Zariski topology, continuous maps are not as well behaved as one would expect from elementary calculus for example. A prominent example is the complex conjugation $\mathbb{C} \to \mathbb{C}$. This map is continuous in the Zariski topology of $\mathbb{C}$, but the map $\mathbb{C} \to \mathbb{C}$, $x \mapsto \overline{x} + x$ is not. So we see that the sum of two continuous maps does not need to be continuous anymore. To fix that problem, we restrict to a subclass of continuous maps which is closed under taking sums, products, etc.

Definition 2.2.1. Let $O \subseteq V$ be an open subset of a finite dimensional vector space V. A map $f\colon O \to \Bbbk$ is called *rational* if there are polynomial maps $g, h \in \Bbbk[V]$ such that h vanishes nowhere on O, and

$$f(x) = \frac{g(x)}{h(x)} \text{ holds for all } x \in O.$$

If, more generally, W is another finite dimensional vector space, a map $f\colon O \to W$ is called *rational* if the compositions $p \circ f\colon O \to \Bbbk$ are rational for all $p \in \Bbbk[W]$.

Note that if $f\colon O \to W$ is a map between an open subset $O \subseteq V$ of a vector space V and another vector space W then f is rational provided that the (finitely many) maps $p_1 \circ f, \ldots, p_m \circ f$ are rational, where $p_1, \ldots, p_m \in \Bbbk[W]$ is any dual basis of W. In particular, there is no ambiguity in the definition of rational maps $O \to \Bbbk$ for open subsets $O \subseteq V$.

Lemma 2.2.2. *Let V, W be finite dimensional vector spaces, and let $O \subseteq V$ be open. Then all rational maps $O \to W$ are continuous.*

Proof. Let $f\colon O \to W$ be a rational map. We show that any (principal) open subset of W has an open pre-image in O. Let $p \in \Bbbk[W]$ be a polynomial function. Then $p \circ f$ is a rational function $O \to \Bbbk$ by definition. So there are polynomial maps $g, h \in \Bbbk[V]$ such that h vanishes nowhere on O, and $p(f(x)) = g(x)/h(x)$ holds for all $x \in O$. Therefore, we get that $f^{-1}(W_p) = V_g \cap O$ is open in O. □

By choosing a basis, we may always identify a finite dimensional $\Bbbk$-vector space with a standard space $\Bbbk^n$ of appropriate dimension n. If $O \subseteq \Bbbk^n$ is any open subset, the rational maps $O \to \Bbbk^m$ are precisely those maps of the form

$$x \mapsto \left(\frac{g_1(x)}{h_1(x)}, \dots, \frac{g_m(x)}{h_m(x)} \right),$$

where $g_i, h_i \in \Bbbk[X_1, \dots, X_n]$ are polynomials such that the h_i vanish nowhere on O. With that argument in mind, it is utterly routine to prove the following properties of rational maps.

Lemma 2.2.3. *Let V, W and $V_1, \dots, V_n$ be finite dimensional vector spaces, and let $O \subseteq V$ and $O_i \subseteq V_i$ be open subsets for all i.*

(1) All constant maps $O \to W$ are rational.

(2) All multilinear maps $V_1 \times \cdots \times V_n \to W$ are rational.

(3) Compositions, sums, differences, and dilations of rational maps are rational.

(4) Let $f\colon O \to W$ and $g\colon O \to \Bbbk$ be rational. Then $g \cdot f\colon O \to W$ is rational. Moreover, if g vanishes nowhere on O then $\frac{1}{g} \cdot f\colon O \to W$ is rational.

(5) If $f\colon O_1 \times \cdots \times O_n \to W$ and $g_i\colon O \to O_i$ are rational maps for all i then the composed map $O \to W$, $x \mapsto f(g_1(x), \dots, g_n(x))$ is rational.

We finish this chapter with a gluing property of rational maps. Recall that if X is a topological space covered by open sets $X = \bigcup_i O_i$, and if $f_i\colon O_i \to Y$ are continuous maps into a space Y such that any two of them agree on the intersection of their domains, there is a unique continuous map $f\colon X \to Y$ extending all f_i. This elementary fact, which appears in similar fashions in many geometric theories (including algebraic geometry and differential geometry), is called *gluing* of maps. In the case of rational maps between vector spaces over infinite fields, we have an even stronger property. It is ultimately due to the fact that the polynomial functions on a finite dimensional vector space form a factorial domain.

Lemma 2.2.4. *Let V, W be finite dimensional vector spaces over an infinite field $\Bbbk$, and let $O_1, \dots, O_n \subseteq V$ be nonempty open subsets. If $f_i\colon O_i \to W$ are rational maps which agree on a nonempty open subset of $\bigcap_{i=1}^n O_i$ then there is a unique rational map $f\colon \bigcup_{i=1}^n O_i \to W$ extending all f_i.*

Proof. By choosing a basis of W, and by considering each coordinate separately, we can restrict to the one dimensional case $W = \Bbbk$. For all i, let $g_i, h_i \in \Bbbk[V]$ be polynomial maps such that h_i vanishes nowhere on O_i, and $f_i(x) = g_i(x)/h_i(x)$ holds for all $x \in O_i$. Since $\Bbbk[V]$ is a Noetherian domain, we can assume without loss of generality that g_i and h_i are coprime for all i. For any $1 \le i, j \le n$, we consider the set

$$A_{i,j} = \{x \in V\colon h_i(x) g_j(x) = h_j(x) g_i(x)\}.$$

This set is closed in V by definition, and by the assumption, it has a nonempty interior in V. Since V is an irreducible topological space by Lemma 2.1.2, we conclude $A_{i,j} = V$, whence we get an equation $h_i g_j = h_j g_i$ in $\Bbbk[V]$. Since $\Bbbk[V]$ is a factorial domain, and since the elements g_i, h_i have been chosen to be coprime for all i, we get that each pair (g_i, h_i) equals (g_j, h_j) up to a nonzero scalar factor. Since i, j were arbitrarily chosen, we see that the polynomial map h_1 vanishes nowhere on $O = \bigcup_{i=1}^{n} O_i$, and that $O \to W$, $x \mapsto g_1(x)/h_1(x)$ is a (necessarily unique) rational extension of all f_i. $\square$

3 The geometric view on generic symmetries

In this chapter, we develop a mathematical framework capable of handling the questions raised in the introduction. In the motivational examples, we have considered finite matrix groups $G \leq \mathrm{GL}(n, \mathbb{R})$ acting on the Euclidean space $\mathbb{R}^n$. From now on, we aim for a greater generality. We consider finite dimensional vector spaces V over arbitrary fields $\Bbbk$. Instead of matrix groups, we consider abstract finite groups G acting linearly on V in terms of *representations*, that is, by homomorphisms $G \to \mathrm{GL}(V)$. It is convenient to use the module theoretic language here. Recall that if $\Bbbk$ is an arbitrary field, and if G is any finite group then there is a finite dimensional (unital, associative) $\Bbbk$-algebra $\Bbbk G$ which is called a *group algebra.* The elements of $\Bbbk G$ are the formal linear combinations

$$\sum_{g \in G} \lambda_g g, \quad \lambda_g \in \Bbbk,$$

of the elements of G. So G is a basis of $\Bbbk G$ as a $\Bbbk$-vector space, and we have $\dim_{\Bbbk} \Bbbk G = |G|$. The multiplication on $\Bbbk G$ is uniquely given as the bilinear extension of the multiplication of the group G. Although group algebras can be defined more generally for coefficient rings which are not fields and for infinite groups, the term $\Bbbk G$ will throughout be reserved for the group algebra corresponding to a field $\Bbbk$ and to a finite group G.

If V is a $\Bbbk$-vector space then any representation $G \to \mathrm{GL}(V)$ of groups extends uniquely to a homomorphism $\Bbbk G \to \mathrm{End}(V)$ of $\Bbbk$-algebras, whence V can be regarded as a left module over $\Bbbk G$. In that way, the representations of G on $\Bbbk$-vector spaces are in one-to-one correspondence with the left modules of $\Bbbk G$. As usual, a representation $D\colon G \to \mathrm{GL}(V)$ is called *faithful*, and we say that G acts *faithfully* on the $\Bbbk G$-module V, if D is an injective map (or equivalently, if the only element $g \in G$ satisfying $gv = v$ for all $v \in V$ is the identity).

Since G is finite, a left $\Bbbk G$-module V is finitely generated if and only if V is finite dimensional over $\Bbbk$. The module V is called *cyclic* if V is generated by one element over $\Bbbk G$ (that is, if $V = \Bbbk G v$ for some $v \in V$). (There is also a correspondence between the G-representations over $\Bbbk$ and the right modules of $\Bbbk G$, but we have no reason to consider modules of different type.) From now on, a module over $\Bbbk G$ will be always understood to be a left module. For a comprehensive view on the representation theory of finite groups, we refer to [17] and to [4].

For any set X the *symmetric group* (that is, the group of all permutations) on X will be denoted by $\mathrm{Sym}(X)$. If $X \subseteq V$ is a subset of some $\Bbbk$-vector space V, we define the *linear symmetry group* $\mathrm{GL}(X) \subseteq \mathrm{Sym}(X)$ of X as the group of all permutations on X arising as restrictions of linear maps $V \to V$. This definition agrees with the usual notion of the general linear groups of vector spaces. In particular, if $X \leq V$ is a linear subspace then $\mathrm{GL}(X)$ is just the group of all invertible linear maps $X \to X$.

As already illustrated in the introduction, we are mainly interested in the linear symmetry groups $\mathrm{GL}(Gv)$ of the orbits of a finite group G with respect to the elements $v \in V$ of a finitely generated $\Bbbk G$-module V. The main object of our investigations is the *generic symmetry group* which we associate to any finitely generated $\Bbbk G$-module V. This group, which we denote by $\mathrm{Sym}(G, V)$, is a certain subgroup of $\mathrm{Sym}(G)$ only depending on the isomorphism type of V. As $\mathrm{Sym}(G, V)$ will always contain the left multiplications by all elements of G, we will regard G as a subgroup of $\mathrm{Sym}(G, V)$. The name "generic symmetry group" comes from the fact that (assuming $\Bbbk$ is infinite and G acts faithfully on V for simplicity) $\mathrm{Sym}(G, V)$ is isomorphic to the linear symmetry groups $\mathrm{GL}(Gv)$ for "almost all" $v \in V$ (Theorem 3.5.2). This result leads to the notion of *generic points*.

We also introduce the notion of *generically closed* $\Bbbk G$-modules which is a central aspect of our theory. A finitely generated $\Bbbk G$-module is called generically closed if G acts faithfully on V and if $\mathrm{Sym}(G, V) = G$ (that is, if the generic symmetry group of V is as small as possible). In Theorem 3.8.5 and in Proposition 3.8.8, we give two sufficient criteria for recognizing generically closed modules (Proposition 3.8.8 is essentially a reformulation of a classical result of Isaacs).

Finally, we show how orbit polytopes and their affine symmetry groups fit into our theory. In Theorem 3.9.6, we characterize the affine symmetry groups of orbit polytopes as those finite groups G for which generically closed $\mathbb{R}G$-modules exist. This is the starting point of our classification of all affine symmetry groups of orbit polytopes.

Most results of the present chapter have already appeared in [9] and [10] in a similar fashion. However, the focus was originally on cyclic $\mathbb{R}G$-modules (as those are most closely related to the geometric questions raised in the introduction), and later on cyclic $\Bbbk G$-modules over infinite fields $\Bbbk$. In the following, we aim for a maximal degree of generality. We impose restrictions on $\Bbbk$ and V only when necessary, and we give new examples illustrating the advantages of such restrictions in some cases. Moreover, many proofs have been replaced by coordinate free arguments using the algebraic geometric concepts of Chapter 2.

3.1 Orbit symmetries

In the following, we consider an arbitrary field $\Bbbk$, a finite group G, and a $\Bbbk G$-module V. Our objective is the study of the linear symmetry groups of the orbits of G in V. As already illustrated in the motivational examples, these groups $\mathrm{GL}(Gv)$ can be quite different for distinct points $v \in V$ when regarded as groups of linear operators. In order to make linear symmetry groups comparable, we regard them as permutation groups on the group G itself.

Definition 3.1.1. Let V be a $\Bbbk G$-module. A permutation $\pi \in \mathrm{Sym}(G)$ is called an *orbit symmetry* of $v \in V$ if there is a linear symmetry $\alpha \in \mathrm{GL}(Gv)$ such that

$$\alpha(gv) = \pi(g)v \text{ for all } g \in G.$$

This unique map α is called the *realization* of π as an orbit symmetry of v. The set of all orbit symmetries of v is denoted by $\mathrm{Sym}(G, v)$.

It is routine to check that $\mathrm{Sym}(G, v)$ is a subgroup of the symmetric group $\mathrm{Sym}(G)$ for all $v \in V$, and that the map $D_v\colon \mathrm{Sym}(G, v) \to \mathrm{GL}(Gv)$ sending an orbit symmetry to its realization is a homomorphism. In Proposition 3.1.4, we show that D_v is always surjective but, as already observed in the second motivational example, it needs not to be injective. We will see that the kernel of D_v depends on the *stabilizer* $G_v = \{g \in G : gv = v\}$ of v in G.

Definition 3.1.2. A permutation $\pi \in \mathrm{Sym}(G)$ is called an *irrelevant orbit symmetry* of some point $v \in V$ if π fixes all left cosets of G_v in G as sets. The set of all irrelevant orbit symmetries of v is denoted by $\mathrm{Iv}(G, v)$.

In Proposition 3.1.4, we show that $\mathrm{Iv}(G, v) = \mathrm{Ker}(D_v)$, so $\mathrm{Iv}(G, v)$ is a normal subgroup of the orbit symmetry group $\mathrm{Sym}(G, v)$. It is evident from the definition that $\mathrm{Iv}(G, v)$ is isomorphic to a power of a full symmetric group (it is straightforward to show that $\mathrm{Iv}(G, v) \cong \mathrm{Sym}(G_v)^{|G:G_v|}$).

Before proving the precise relations between the groups $\mathrm{Iv}(G, v)$, $\mathrm{Sym}(G, v)$, and $\mathrm{GL}(Gv)$, we need a technical lemma on permutation groups. Recall that a homomorphism $\varphi\colon G \to H$ of groups is called a *split epimorphism* if φ has a right inverse, that is, if there is a homomorphism $\psi\colon H \to G$ such that $\varphi \circ \psi = \mathrm{id}_H$. Recognizing split epimorphisms is important as they give rise to semidirect product decompositions. More precisely, if $\varphi\colon G \to H$ is a split epimorphism of groups, and if $K = \mathrm{Ker}(\varphi)$ is the kernel of φ then the image of any right inverse of φ is a complement of K in G. Hence, G "splits" into a semidirect product $G \cong K \rtimes H$. For the details, we refer to [30, Ch. 7]. For a comprehensive view on permutation groups, we refer to [5].

Lemma 3.1.3. *Let G be a group acting transitively on a set X, let $x \in X$ be some fixed element, and let $P \leq \mathrm{Sym}(G)$ be the group of all permutations on G which map all left cosets of G_x to left cosets of G_x again. Then P acts on X by*

$$P \times X \to X, \quad (\pi, gx) \mapsto \pi(g)x,$$

and the corresponding homomorphism $P \to \mathrm{Sym}(X)$ is a split epimorphism.

Proof. The given action of P on X is well defined since $gx = hx$ holds if and only if g and h lie in the same left coset of G_x, and since all elements of P preserve these left cosets. Since G acts transitively on X, there is a map $f\colon X \to G$ such that $f(y)x = y$ for all $y \in X$. It is routine to check that $\mathrm{Sym}(X)$ acts on G by

$$\mathrm{Sym}(X) \times G \to G, \quad (\pi, g) \mapsto f(\pi(gx))f(gx)^{-1}g,$$

and that this action permutes the left cosets of G_x in G. So the action induces a morphism $\mathrm{Sym}(X) \to P$, which is easily seen to be a right inverse of the given morphism $P \to \mathrm{Sym}(X)$. □

Proposition 3.1.4. *Let V be a $\Bbbk G$-module, and let $v \in V$ be arbitrary. Then the homomorphism $D_v\colon \operatorname{Sym}(G, v) \to \operatorname{GL}(Gv)$ sending an orbit symmetry to its realization is a split epimorphism with $\operatorname{Ker}(D_v) = \operatorname{Iv}(G, v)$.*

Proof. Let $P \le \operatorname{Sym}(G)$ be the group of all permutations on G permuting the left cosets of G_v in G. Then by Lemma 3.1.3, there is a split epimorphism $\varphi\colon P \to \operatorname{Sym}(Gv)$ with $\varphi(\pi)(gv) = \pi(g)v$ for all $\pi \in P$ and all $g \in G$. By definition, we have $\operatorname{Ker}(\varphi) = \operatorname{Iv}(G, v)$. We claim that $\operatorname{Sym}(G, v) = \varphi^{-1}(\operatorname{GL}(Gv))$.

Let $\pi \in \operatorname{Sym}(G, v)$ be arbitrary, and let $g, h \in G$ lie in the same left coset of G_v. Then we have $gv = hv$ and hence $\pi(g)v = D_v(gv) = D_v(hv) = \pi(h)v$. So $\pi(g)$ and $\pi(h)$ again lie in the same left coset of G_v, which shows $\operatorname{Sym}(G, v) \subseteq P$. Since $D_v(\pi) = \varphi(\pi)$ for all $\pi \in \operatorname{Sym}(G, v)$, we get $\operatorname{Sym}(G, v) \subseteq \varphi^{-1}(\operatorname{GL}(Gv))$. Conversely, if $\pi \in P$ satisfies $\varphi(\pi) \in \operatorname{GL}(Gv)$ then, by definition, π is an orbit symmetry of v realized by $\varphi(\pi)$. So $\varphi^{-1}(\operatorname{GL}(Gv)) \subseteq \operatorname{Sym}(G, v)$.

Now since $\operatorname{Sym}(G, v) = \varphi^{-1}(\operatorname{GL}(Gv))$, and since D_v agrees with φ on $\operatorname{Sym}(G, v)$, it follows immediately that $\operatorname{Ker}(D_v) = \operatorname{Ker}(\varphi) = \operatorname{Iv}(G, v)$. Moreover, any right inverse of φ restricts to a right inverse of D_v, proving that D_v is a split epimorphism. □

Proposition 3.1.4 shows that an orbit symmetry group $\operatorname{Sym}(G, v)$ is a semidirect product $\operatorname{Sym}(G, v) \cong \operatorname{Iv}(G, v) \rtimes \operatorname{GL}(Gv)$. So roughly speaking, we see that the linear symmetry group $\operatorname{GL}(Gv)$ of a G-orbit can always be restored from the corresponding orbit symmetry group by passing over to the quotient $\operatorname{Sym}(G, v)/\operatorname{Iv}(G, v)$.

Besides the irrelevant orbit symmetries, there is another class of permutations on G which are always orbit symmetries. For any element $g \in G$, the left multiplication $\iota_g\colon h \mapsto gh$ is a permutation on G, and the map $G \to \operatorname{Sym}(G)$ sending g to ι_g is an injective homomorphism usually called the (left) *Cayley embedding*. By means of that embedding, we will always regard G as a subgroup of $\operatorname{Sym}(G)$.

Lemma 3.1.5. *Let V be a $\Bbbk G$-module and let $v \in V$ be arbitrary. Then $\operatorname{Sym}(G, v)$ contains the left multiplications by all element of G. That is, $G \le \operatorname{Sym}(G, v)$.*

Proof. For any element $g \in G$, the left multiplication by g can be regarded both as a permutation ι_g on G, and as a linear map $\alpha \in \operatorname{GL}(V)$. Evidently, α fixes any orbit Gv, and the restriction $\alpha_{|Gv}$ is a realization of ι_g as an orbit symmetry of v. □

Example 3.1.6. We reconsider the first motivational example from the introduction. Let $V = \mathbb{R}^2$ be the Euclidean plane, and let $G = \langle g \rangle$ be a cyclic group of any order n acting on V by the rotation representation $D\colon G \to \operatorname{GL}(2, \mathbb{R})$ given by

$$D\left(g^k\right) = \begin{pmatrix} \cos\frac{2k\pi}{n} & -\sin\frac{2k\pi}{n} \\ \sin\frac{2k\pi}{n} & \cos\frac{2k\pi}{n} \end{pmatrix} \text{ for all } k \in \mathbb{Z}.$$

Let $\sigma \in \operatorname{Sym}(G)$ be the permutation sending each element of G to its inverse. We claim that σ is an orbit symmetry of any nonzero point $v \in V$.

Let $S \in \operatorname{GL}(V)$ be the unique reflection fixing v, and let $h \in G$ be arbitrary. Since $D(h)$ is a rotation, $D(h)S$ must be a reflection. So $D(h)SD(h)S = (D(h)S)^2$ is the identity, and hence $SD(h)S = D(h)^{-1} = D(\sigma(h))$. Finally, we get

$$\sigma(h)v = SD(h)Sv = S(hv),$$

which proves $\sigma \in \mathrm{Sym}(G, v)$.

It can be easily shown by geometric arguments (as done in the introduction) that $\mathrm{GL}(Gv)$ is the dihedral group D_n of order $2n$. Since v has a trivial stabilizer in G, the orbit symmetry group $\mathrm{Sym}(G, v)$ is isomorphic to $\mathrm{GL}(Gv)$, and $\mathrm{Sym}(G, v)$ must actually be generated by ι_g and σ. Later, in Example 5.1.9, we come to the same conclusion by a very simple application of our theory.

We next show that orbit symmetries are compatible with isomorphisms of modules. Recall that for any point $v \in V$, there is a unique smallest (cyclic) $\Bbbk G$-submodule $\Bbbk Gv$ of V containing v. As a $\Bbbk$-vector space, $\Bbbk Gv$ is generated by the orbit Gv. In the following, we identify any linear symmetry $\alpha \in \mathrm{GL}(Gv)$ with its unique linear extension to $\Bbbk Gv$.

Definition 3.1.7. Let V be a $\Bbbk G$-module, and let $\pi \in \mathrm{Sym}(G)$ be a permutation. Then $V(\pi)$ denotes the subset of points of V having π as an orbit symmetry. That is,

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

Lemma 3.1.8. *Let $\varphi\colon V \to W$ be an isomorphism of $\Bbbk G$-modules, and let $v \in V$, $\pi \in \mathrm{Sym}(G)$ be arbitrary. Then we have*

(1) $\mathrm{Sym}(G, \varphi(v)) = \mathrm{Sym}(G, v)$, *and*

(2) $\varphi(V(\pi)) = W(\pi)$.

Proof. The isomorphism φ restricts to an isomorphism $\psi\colon \Bbbk Gv \to \Bbbk G\varphi(v)$. It is easily verified that a permutation $\pi \in \mathrm{Sym}(G)$ is an orbit symmetry of v realized by $\alpha \in \mathrm{GL}(Gv)$ if and only if π is an orbit symmetry of $\varphi(v)$ realized by $\psi\alpha\psi^{-1} \in \mathrm{GL}(G\varphi(v))$. Both statements now follow immediately from the definitions. □

3.2 Generic symmetries

We come to the definition of *generic symmetries* of a finitely generated $\Bbbk G$-module V over an infinite field $\Bbbk$. Recall that we observed in the motivational examples that “almost all” points of a module have the same orbit symmetries, but there may be exceptional points where the situation is different. Of course we always have $\mathrm{Sym}(G, 0) = \mathrm{Sym}(G)$, so in most cases the zero point of V will have more orbit symmetries than the other points of V. But moreover, there may even be points $v \in V$ such that $\mathrm{Sym}(G, v)$ is strictly larger than the orbit symmetry groups of the majority of points, although the orbit Gv is a generating set of V of the same size as G. In order to turn these intuitive observations into precise statements, we need a mathematical notion of the term "almost all". For that purpose, we restrict to fields of infinite order (for now), and we equip any finitely generated $\Bbbk G$-module V with the *Zariski topology* (see Section 2.1). In that topology, the nonempty open sets are very large in the sense that the intersection of finitely many nonempty open sets is nonempty again (Lemma 2.1.2).

Definition 3.2.1. Let P be any property of elements of some finite dimensional vector space V over an infinite field $\Bbbk$. We say that *almost all* elements of V satisfy P if the set of elements of V satisfying P has a nonempty interior in V (with respect to the Zariski topology).

The most important properties of the "almost all" quantifier to keep in mind are listed in the following lemma. We will frequently use them without further reference.

Lemma 3.2.2. *Let V be a finite dimensional vector space over an infinite field, and let P and Q be properties of points of V.*

(1) If all but finitely many points of V satisfy P then almost all points of V satisfy P.

(2) If almost all points of V satisfy P then there is a generating set of V, each point of which satisfies P.

(3) If almost all points of V satisfy P, and almost all points of V satisfy Q then almost all points of V satisfy both P and Q at the same time.

Proof. All these statements are consequences of Lemma 2.1.2. The first statement follows from the fact that finite sets are always closed in the Zariski topology. Concerning the second statement, let $O \subseteq V$ be a nonempty open set of points satisfying P. As any linear subspace of V, the linear span $W = \langle O \rangle$ is closed in V. Now the open sets O and $V \setminus W$ intersect trivially, which forces $V \setminus W = \emptyset$, and hence $V = W$. The third statement also follows easily from the fact that the intersection of any two nonempty open sets is nonempty again. □

We see that, roughly speaking, "almost all" can be regarded as a quantifier sitting in-between the universal quantifier and the existential quantifier. With that terminology, the *generic symmetries* of a module can be defined in a very natural way.

Definition 3.2.3. Let V be a finitely generated $\Bbbk G$-module, where $\Bbbk$ is an infinite field. A permutation $\pi \in \mathrm{Sym}(G)$ is a *generic symmetry* of V if π is an orbit symmetry of almost all elements of V. The set of all generic symmetries of V is denoted by $\mathrm{Sym}(G, V)$.

Note that, although this definition seems natural, its justification will only be given later (in Theorem 3.5.2) when we show that $\mathrm{Sym}(G, V)$ is the orbit symmetry group of almost all points of a module V. Later on, we extend the definition of generic symmetries to cover modules over finite fields as well (see Definition 3.4.1). At that point it will be obvious that all of the following results (unless they are stated explicitly for infinite fields) actually hold for arbitrary fields.

Lemma 3.2.4. *Let V be a finitely generated $\Bbbk G$-module. Then $\mathrm{Sym}(G, V)$ is a subgroup of $\mathrm{Sym}(G)$ containing all left multiplications by elements of G. That is, we have $G \leq \mathrm{Sym}(G, V)$.*

Proof. Of course $\mathrm{Sym}(G, V)$ is nonempty, as it contains the identity permutation. Let $\pi, \sigma \in \mathrm{Sym}(G, V)$. We have $\pi \in \mathrm{Sym}(G, v)$ for almost all $v \in V$ and $\sigma \in \mathrm{Sym}(G, v)$ for almost all $v \in V$. It follows $\pi, \sigma \in \mathrm{Sym}(G, v)$, and hence $\pi^{-1}\sigma \in \mathrm{Sym}(G, v)$ for almost all $v \in V$. This proves $\pi^{-1}\sigma \in \mathrm{Sym}(G, V)$, so $\mathrm{Sym}(G, V)$ is a subgroup of $\mathrm{Sym}(G)$. Since by Lemma 3.1.5, any left multiplication ι_g is an orbit symmetry of all points of V, ι_g is a generic symmetry of V in particular. □

The next lemma shows that $\mathrm{Sym}(G, V)$ only depends on the isomorphism type of the $\Bbbk G$-module V. This fact is central for our theory, as it opens the door for applications of representation theory.

Lemma 3.2.5. *Let V and W be finitely generated $\Bbbk G$-modules. If $V \cong W$ then $\mathrm{Sym}(G, V) = \mathrm{Sym}(G, W)$.*

Proof. Let $\varphi \colon V \to W$ be an isomorphism of $\Bbbk G$-modules, and let $\pi \in \mathrm{Sym}(G)$. By Lemma 3.1.8, we have $\varphi(V(\pi)) = W(\pi)$. As any isomorphism of vector spaces, φ is also a homeomorphism with respect to the Zariski topologies on V and W. So $V(\pi)$ has nonempty interior in V if and only $W(\pi)$ has nonempty interior in W. Hence, we have $\pi \in \mathrm{Sym}(G, V)$ if and only if $\pi \in \mathrm{Sym}(G, W)$. □

We go on by studying a second class of permutations which are generic symmetries for trivial reasons. Let V be a $\Bbbk G$-module, where G acts on V by the representation $D \colon G \to \mathrm{GL}(V)$. The *kernel* $\mathrm{Ker}(V) \subseteq G$ of V is defined as the kernel of D. That is, we have

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

We see that $\mathrm{Ker}(V)$ is a normal subgroup of G which can also be described as the intersection of the stabilizers G_v for all $v \in V$. We have seen in (the proof of) Proposition 3.1.4 that all permutations fixing the left cosets of a stabilizer G_v are (irrelevant) orbit symmetries of the point $v \in V$. Consequently, a permutation fixing the cosets of $\mathrm{Ker}(V)$ in G must actually be a generic symmetry of V.

Definition 3.2.6. A permutation $\pi \in \mathrm{Sym}(G)$ is an *irrelevant generic symmetry* of a finitely generated $\Bbbk G$-module V if π fixes all cosets of $\mathrm{Ker}(V)$ in G. The set of all irrelevant generic symmetries of V is denoted by $\mathrm{Iv}(G, V)$.

By the previous discussion, it is evident that $\mathrm{Iv}(G, V)$ is a subgroup of $\mathrm{Sym}(G, V)$ (in fact a normal subgroup, as we will show soon), consisting of those permutations which are irrelevant orbit symmetries for all $v \in V$. In analogy to the groups of irrelevant orbit symmetries, we see that a group of irrelevant generic symmetries is also isomorphic to the power of a full symmetric group. In fact, we have an isomorphism

$$\mathrm{Iv}(G, V) \cong \mathrm{Sym}(\mathrm{Ker}(V))^{|G:\mathrm{Ker}(V)|}.$$

Note that if a $\Bbbk G$-module V has the kernel K in G then V can also be regarded as a $\Bbbk[G/K]$-module in a natural way. In particular, we may consider the generic symmetry group $\operatorname{Sym}(G/K, V)$. The next lemma shows that $\operatorname{Sym}(G/K, V)$ embeds into $\operatorname{Sym}(G, V)$ as a complement of $\operatorname{Iv}(G, V)$, whence we get a semidirect product decomposition

$$\operatorname{Sym}(G, V) = \operatorname{Iv}(G, V) \rtimes \operatorname{Sym}(G/K, V).$$

So, roughly speaking, we may regard $\operatorname{Sym}(G/K, V)$ as the group of "relevant" generic symmetries on V.

Proposition 3.2.7. *Let V be a finitely generated $\Bbbk G$-module with kernel K. Then there is a split epimorphism $p\colon \operatorname{Sym}(G, V) \to \operatorname{Sym}(G/K, V)$ with $\operatorname{Ker}(p) = \operatorname{Iv}(G, V)$ satisfying $p(\pi)(gK) = \pi(g)K$ for all $\pi \in \operatorname{Sym}(G, V)$ and $g \in G$.*

Proof. Let $P \leq \operatorname{Sym}(G)$ be the subgroup of all elements permuting the cosets of K in G. By Lemma 3.1.3, there is a split epimorphism $\varphi\colon P \to \operatorname{Sym}(G/K)$ such that $\varphi(\pi)(gK) = \pi(g)K$ for all $\pi \in \operatorname{Sym}(G, V)$ and $g \in G$. By definition, we have $\operatorname{Ker}(\varphi) = \operatorname{Iv}(G, V)$. Analogously to the proof of Proposition 3.1.4, we claim that $\operatorname{Sym}(G, V) = \varphi^{-1}(\operatorname{Sym}(G/K, V))$. Afterwards, it follows immediately that the restriction of φ to $\operatorname{Sym}(G, V)$ has the desired properties.

We begin by showing that $\operatorname{Sym}(G, V)$ is a subgroup of P. If $\pi \in \operatorname{Sym}(G, V)$ then there is a generating set $E \subseteq V$ over $\Bbbk$ such that π is an orbit symmetry of all $v \in E$. By (the proof of) Proposition 3.1.4, π fixes the left cosets of the stabilizers G_v for all $v \in E$. Therefore, π fixes the left cosets of $K = \bigcap_{v \in E} G_v$ in particular. So $\operatorname{Sym}(G, V) \leq P$.

Let $v \in V$ and let $\pi \in P$ be arbitrary. To finish the proof, we show that π is an orbit symmetry of v if and only if $\varphi(\pi)$ is an orbit symmetry of v. By definition, $\varphi(\pi) \in \operatorname{Sym}(G/K, v)$ holds if and only if there is a map $\alpha \in \operatorname{GL}(Gv)$ such that $\alpha((gK)v) = \varphi(\pi)(gK)v$ for all $g \in G$. Since $(gK)v = gv$ and since $\varphi(\pi)(gK)v = (\pi(g)K)v = \pi(g)v$, we see that $\varphi(\pi) \in \operatorname{Sym}(G/K, v)$ is equivalent to $\pi \in \operatorname{Sym}(G, v)$. Since $\pi \in P$ and $v \in V$ were arbitrary, we conclude $\operatorname{Sym}(G, V) = \varphi^{-1}(\operatorname{Sym}(G/K, V))$. □

It is natural to ask why we care about irrelevant symmetries at all. Of course by Proposition 3.2.7, we may always pass over to the quotient $\operatorname{Sym}(G, V)/\operatorname{Iv}(G, V) \cong \operatorname{Sym}(G/K, V)$, which may seem to be a better candidate for a symmetry group associated to V in comparison to $\operatorname{Sym}(G, V)$. The answer is that the actual definition of the generic symmetry group is compatible with direct sums of modules.

Lemma 3.2.8. *Let $V = V_1 \oplus \cdots \oplus V_n$ be a direct sum of $\Bbbk G$-modules. Then we have*

$$\begin{aligned} \operatorname{Sym}(G, V_1) \cap \cdots \cap \operatorname{Sym}(G, V_n) &\subseteq \operatorname{Sym}(G, V), \text{ and} \\ \operatorname{Iv}(G, V_1) \cap \cdots \cap \operatorname{Iv}(G, V_n) &= \operatorname{Iv}(G, V). \end{aligned}$$

Proof. Let $\pi \in \operatorname{Sym}(G, V_i)$ for all i. Then there are nonempty open sets $O_i \subseteq V_i(\pi)$ by definition. We consider the set $O = O_1 \times \cdots \times O_n$ which is nonempty and open in V. For any $v = (v_i)_i \in O$ it is easy to see that the restriction of the map

$$D_{v_1}(\pi) \oplus \cdots \oplus D_{v_n}(\pi) \in \operatorname{GL}(\Bbbk G v_1 \oplus \cdots \oplus \Bbbk G v_n)$$

to $\Bbbk Gv$ is a realization of π as an orbit symmetry of v. Hence, we have $O \subseteq V(\pi)$, which shows that π is a generic symmetry of V. This proves the first assertion.

Concerning the second assertion, note that $\mathrm{Ker}(V) = \mathrm{Ker}(V_1) \cap \cdots \cap \mathrm{Ker}(V_n)$. By that equation, it is evident that any permutation $\pi \in \mathrm{Sym}(G)$ fixing the cosets of all $\mathrm{Ker}(V_i)$ also fixes the cosets of $\mathrm{Ker}(V)$. Conversely, for each i, we have that any coset of $\mathrm{Ker}(V_i)$ is a disjoint union of cosets of $\mathrm{Ker}(V)$. So any permutation on G fixing the cosets of $\mathrm{Ker}(V)$ also fixes the cosets of $\mathrm{Ker}(V_i)$. □

Note that, in the situation of Lemma 3.2.8, even if G acts faithfully on V it is perfectly possible that a generic symmetry $\pi \in \bigcap_i \mathrm{Sym}(G, V_i)$ is irrelevant with respect to some summands V_i. In that way, irrelevant symmetries may actually give rise to relevant symmetries. Although it can be very fruitful to consider such direct sum decompositions to get generic symmetries of V as common generic symmetries of the summands V_i, there is no equality $\mathrm{Sym}(G, V) = \bigcap_i \mathrm{Sym}(G, V_i)$ in general. In fact, it is a main objective of Chapter 4 to find direct sum decompositions of V, where this equality holds.

At this point, we have identified two subgroups of an arbitrary generic symmetry group $\mathrm{Sym}(G, V)$, namely the left regular subgroup G, and the group of irrelevant generic symmetries $\mathrm{Iv}(G, V)$. Since the latter subgroup is even normal, the product $G \cdot \mathrm{Iv}(G, V)$ is a subgroup of $\mathrm{Sym}(G, V)$ as well (the intersection $G \cap \mathrm{Iv}(G, V)$ consists of all left multiplications by elements of $\mathrm{Ker}(V)$). For reasons explained later, we are particularly interested in the case where $\mathrm{Sym}(G, V) = G \cdot \mathrm{Iv}(G, V)$ holds.

Definition 3.2.9. Let V be a finitely generated $\Bbbk G$-module. We call V *weakly generically closed* if $\mathrm{Sym}(G, V) = G \cdot \mathrm{Iv}(G, V)$ holds. If moreover, $\mathrm{Iv}(G, V) = 1$ (that is, if G acts faithfully on V) then V is called *generically closed.*

Remark 3.2.10. In [10], we have defined V to be generically closed if $\mathrm{Sym}(G, V) = G$, which is a little bit weaker in comparison to the present definition. More precisely, a finitely generated $\Bbbk G$-module V satisfies $\mathrm{Sym}(G, V) = G$ and $\mathrm{Iv}(G, V) > 1$ at the same time if and only if G is cyclic of order two, acting trivially on V. The present definition is chosen to exclude this pathological example.

Lemma 3.2.11. *Let V be a finitely generated $\Bbbk G$-module with $K = \mathrm{Ker}(V)$. Then the following statements are equivalent.*

(1) V is a weakly generically closed $\Bbbk G$-module.

(2) V is a generically closed $\Bbbk[G/K]$-module.

(3) For all $\pi \in \mathrm{Sym}(G, V)$ and all $g \in G$, we have $\pi(gK) = \pi(1)gK$.

Proof. We first prove (1) $\iff$ (2). There is a natural homomorphism $G/K \to \mathrm{Sym}(G, V)/\mathrm{Iv}(G, V)$ which is surjective if and only if V is weakly generically closed. There is also a natural morphism $G/K \to \mathrm{Sym}(G/K, V)$ which is surjective if and only if V is generically closed as a $\Bbbk[G/K]$-module (note that $\mathrm{Iv}(G/K, V) = 1$ since G/K

acts faithfully on V). The equivalence follows by applying the natural isomorphism $p\colon \operatorname{Sym}(G,V)/\operatorname{Iv}(G,V) \to \operatorname{Sym}(G/K,V)$ given by Proposition 3.2.7.

Next, we prove (1) $\iff$ (3). If V is weakly generically closed then any generic symmetry $\pi \in \operatorname{Sym}(G,V)$ is a product $\pi = \iota_g \circ \sigma$ of a left multiplication ι_g, and an irrelevant generic symmetry $\sigma \in \operatorname{Iv}(G,V)$. Since $\sigma(1) \in K$, and since left multiplications by elements of K are irrelevant, we may assume $\sigma(1) = 1$, whence $\pi(1) = g$. Now if $C \subseteq G$ is any coset of K then $\pi(C) = g\sigma(C) = \pi(1)C$. Conversely, if $\pi \in \operatorname{Sym}(G)$ is any permutation satisfying $\pi(C) = \pi(1)C$ for all cosets C of K then $\sigma = \iota_{\pi(1)^{-1}} \circ \pi$ is an irrelevant generic symmetry of V, whence $\pi = \iota_{\pi(1)} \circ \sigma \in G \cdot \operatorname{Iv}(G,V)$. □

There is another decomposition of $\operatorname{Sym}(G,V)$ into a product of subgroups which we shall use frequently. It is a direct consequence of the following well known lemma which is one of many variations of the *Frattini argument*. As before, if a group G acts on a set X then the stabilizer of G at some point $x \in X$ will be denoted by G_x. In particular, if V is a finitely generated $\Bbbk G$-module then $\operatorname{Sym}(G,V)_1$ denotes the subgroup of $\operatorname{Sym}(G,V)$ fixing the identity of G.

Lemma 3.2.12 (Frattini argument)**.** *Let G be a group acting on a set X, and let $H \leq G$ be a transitive subgroup. Then for any element $x \in X$, we have $G = H \cdot G_x$.*

Proof. Let $g \in G$ be arbitrary. Since H acts transitively on X, there is some $h \in H$ such that $gx = hx$. Then $h^{-1}g \in G_x$, and $g = h(h^{-1}g) \in H \cdot G_x$. □

Corollary 3.2.13. *Let V be a finitely generated $\Bbbk G$-module. The generic symmetry group* $\operatorname{Sym}(G,V)$ *decomposes as*

$$\operatorname{Sym}(G,V) = G \cdot \operatorname{Sym}(G,V)_1, \quad \text{where } G \cap \operatorname{Sym}(G,V)_1 = 1.$$

Because of Corollary 3.2.13, many questions on a generic symmetry group $\operatorname{Sym}(G,V)$ can be reduced to questions on the stabilizer $\operatorname{Sym}(G,V)_1$. For example, if G acts faithfully on a finitely generated $\Bbbk G$-module V then V is generically closed if and only if $\operatorname{Sym}(G,V)_1$ is trivial. We will use Corollary 3.2.13 without further reference.

3.3 Ample points

The next goal is to show that the generic symmetry group $\operatorname{Sym}(G,V)$ of any finitely generated $\Bbbk G$-module V is the orbit symmetry group of almost all points of V (which we called “generic points” in the introductory examples). However, it is not trivial to show that such points even exist. To begin with, we study the orbit symmetries of certain elements of V which are well accessible. Thereby, we get important characterizations of generic symmetries (Theorem 3.3.4).

Definition 3.3.1. Let V be a finitely generated $\Bbbk G$-module over an infinite field $\Bbbk$, and let n be the maximal dimension (over $\Bbbk$) of a cyclic submodule of V. We call $v \in V$ an *ample point* of V, if $\dim(\Bbbk G v) = n$. The set of all ample points of V is denoted by $\operatorname{Amp}(V)$.

Note that, although the definition of ample points seems valid for finite fields as well, there are good reasons for choosing a different definition in that setting. This is explained in Section 3.4.

To prove the existence of generic points, we pursue the following strategy. We begin by showing that almost all points of V are ample, and that $\mathrm{Sym}(G, V)$ is contained in the orbit symmetry group of any ample point. Afterwards, it turns out that the ample points of V having non-generic orbit symmetries form a proper closed subset of V. This shows that all remaining ample points only have generic orbit symmetries.

In the following we will frequently use the well known fact from linear algebra that elements $v_1, \ldots, v_n \in V$ are linearly independent if and only if there is an alternating form $\alpha\colon V^n \to \Bbbk$ such that $\alpha(v_1, \ldots, v_n) \neq 0$. Since alternating forms are rational functions, they can be used for the construction of open subsets of V.

Lemma 3.3.2. *Let V be a finitely generated $\Bbbk G$-module over an infinite field $\Bbbk$. Then $\mathrm{Amp}(V)$ is a nonempty open subset of V. In particular, almost all points of V are ample.*

Proof. Let n be the maximal dimension of a cyclic $\Bbbk G$-submodule of V. An element $v \in V$ is ample if and only if

$$\alpha(g_1 v, g_2 v, \ldots g_n v) \neq 0$$

for some alternating form $\alpha\colon V^n \to \Bbbk$ and some choice of $g_1, \ldots, g_n \in G$. So $\mathrm{Amp}(V)$ is the union of nonzero sets of rational functions, hence open in V. Of course $\mathrm{Amp}(V)$ is nonempty by definition. □

Let V be a finitely generated $\Bbbk G$-module, and let $\pi \in \mathrm{Sym}(G)$ be any permutation. Recall that $V(\pi)$ denotes the subset of points of V for which π is an orbit symmetry. To each point $v \in V(\pi)$ we can assign the unique realization $D_v(\pi) \in \mathrm{GL}(\Bbbk Gv)$ of π as an orbit symmetry of v. By extending these realizations (non-uniquely) to endomorphisms of V, we get a map $\varphi\colon V(\pi) \to \mathrm{End}(V)$. In general, it is too much to ask for φ being (the restriction of) a rational map. However, at least we may construct φ in such a way that it agrees with a rational map in a neighborhood of an arbitrarily chosen point. This is the objective of the following lemma.

To construct a rational map into $\mathrm{End}(V)$, we will use the well known canonical isomorphism $V^* \otimes_{\Bbbk} V \to \mathrm{End}(V)$, where $V^* = \mathrm{Hom}(V, \Bbbk)$ denotes the *dual space* of V. This isomorphism is given on the pure tensors by

$$\lambda \otimes v \mapsto (w \mapsto \lambda(w)v).$$

Since any isomorphism of vector spaces is a rational map, we may construct φ as a map with codomain $V^* \otimes_{\Bbbk} V$ instead of $\mathrm{End}(V)$.

Lemma 3.3.3. *Let V be a finitely generated $\Bbbk G$-module, and let $\pi \in \mathrm{Sym}(G)$ be any permutation. There is an open cover $\mathrm{Amp}(V) = O_1 \cup \cdots \cup O_n$ and rational maps*

$\varphi_i\colon O_i \to \mathrm{End}(V)$ *such that*

$$O_i \cap V(\pi) = \{v \in O_i : \varphi_i(v)gv = \pi(g)v \text{ for all } g \in G\}.$$

In particular, $O_i \cap V(\pi)$ *is closed in* O_i*, and* $\mathrm{Amp}(V) \cap V(\pi)$ *is closed in* $\mathrm{Amp}(V)$.

Proof. For any $v \in \mathrm{Amp}(V)$ we construct an open neighborhood $O \subseteq \mathrm{Amp}(V)$ and a rational map $\varphi\colon O \to \mathrm{End}(V)$ such that

$$O \cap V(\pi) = \{x \in O : \varphi(x)gx = \pi(g)x \text{ for all } g \in G\}.$$

This will show in particular that $O \cap V(\pi)$ is closed in O. The claim then follows since $\mathrm{Amp}(V)$ is a compact topological space (see Lemma 2.1.2), and since being closed can be verified locally.

Let $v \in \mathrm{Amp}(V)$ be arbitrary, and let $n = \dim(\Bbbk Gv)$. We pick $g_1, \ldots, g_n \in G$ and an alternating form $\alpha\colon V^n \to \Bbbk$ such that $\alpha(g_1 v, \ldots, g_n v) \neq 0$. This form defines an open neighborhood $O \subseteq \mathrm{Amp}(V)$ of v by

$$O = \{x \in V : \alpha(g_1 x, \ldots, g_n x) \neq 0\}.$$

For any $1 \leq i \leq n$, we define maps $\lambda_i\colon O \to V^*$ by

$$\lambda_i(x)\colon y \mapsto \frac{\alpha(g_1 x, \ldots, g_{i-1}x, y, g_{i+1}x, \ldots, g_n x)}{\alpha(g_1 x, \ldots, g_n x)}.$$

These maps are constructed from multilinear maps in compliance with Lemma 2.2.3, so all λ_i are rational maps. By definition, they satisfy

$$\lambda_i(x)(g_j x) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}.$$

Finally, we define the rational map

$$\varphi\colon O \to V^* \otimes_\Bbbk V, \quad x \mapsto \sum_{i=1}^{n} \lambda_i(x) \otimes \pi(g_i)x.$$

With respect to the canonical identification of $V^* \otimes_\Bbbk V$ and $\mathrm{End}(V)$, one easily checks that $\varphi(x)g_i x = \pi(g_i)x$ for all $1 \leq i \leq n$. Since $g_1 x, \ldots, g_n x$ is a $\Bbbk$-basis of $\Bbbk Gx$ for all $x \in O$, we have $\varphi(x)gx = \pi(g)x$ for all $g \in G$ if and only if $x \in V(\pi)$. □

Lemma 3.3.3 has some important consequences. To begin with, we get new characterizations of generic symmetries.

Theorem 3.3.4. *Let* V *be a finitely generated* $\Bbbk G$*-module over an infinite field* $\Bbbk$*, and let* $\pi \in \mathrm{Sym}(G)$ *be any permutation. The following statements are equivalent characterizations of* π *being a generic symmetry of* V.

(1) $\mathrm{Amp}(V) \subseteq V(\pi)$,

(2) $V(\pi)$ has nonempty interior in V, and

(3) $V(\pi)$ is dense in V.

Proof. Since (2) is the definition of a generic symmetry, we only have to show the equivalence of these statements. The implication (1) $\implies$ (2) is clear by Lemma 3.3.2, and (2) $\implies$ (3) holds since V is an irreducible topological space (Lemma 2.1.2). It remains to show (3) $\implies$ (1). Since $V(\pi)$ is dense in V, and since $\mathrm{Amp}(V)$ is open in V, we get that $V(\pi) \cap \mathrm{Amp}(V)$ is dense in $\mathrm{Amp}(V)$. By Lemma 3.3.3, $V(\pi) \cap \mathrm{Amp}(V)$ is also closed in $\mathrm{Amp}(V)$, whence $V(\pi) \cap \mathrm{Amp}(V) = \mathrm{Amp}(V)$. □

We will see in the next section that the maps φ_i from Lemma 3.3.3 can be glued to a single map $\varphi\colon \mathrm{Amp}(V) \to \mathrm{End}(V)$ if V is a cyclic module. This cannot be done in general. We give an example over $\mathbb{R}$, where a single rational map φ satisfying Lemma 3.3.3 exists, but after a scalar extension to $\mathbb{C}$ multiple maps are needed to cover $\mathrm{Amp}(V)$.

Example 3.3.5. Let $G = \langle s, t \mid s^2 = t^2 = (st)^2 = 1\rangle$ be the Klein four-group acting on $V = \Bbbk^3$ by

$$s\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}-x\\y\\-z\end{pmatrix} \text{ and } t\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x\\-y\\z\end{pmatrix},$$

where $\Bbbk$ is an infinite field of any characteristic different from two. Let $v = (x, y, z)^\intercal \in V$ be arbitrary. It is easy to see that the dimension of $\Bbbk G v$ is always less than three, and the dimension equals two if and only if $xy \neq 0$ or $yz \neq 0$. So the dimension of a maximal cyclic submodule of V is two, and we have

$$V \setminus \mathrm{Amp}(V) = \mathrm{zeros}(X, Z) \cup \mathrm{zeros}(Y)$$

(X, Y, Z being the usual coordinate functions). Geometrically, the complement of $\mathrm{Amp}(V)$ in V is the union of a line and a plane.

We demonstrate Lemma 3.3.3 with respect to the permutation $\pi = (s, t) \in \mathrm{Sym}(G)$, which turns out to be a generic symmetry of V. We consider the open cover $\mathrm{Amp}(V) = O_1 \cup O_2$, where

$$O_1 = \{(x, y, z)^\intercal \in V : xy \neq 0\} \text{ and } O_2 = \{(x, y, z)^\intercal \in V : yz \neq 0\}.$$

Moreover, we define rational maps $\varphi_i\colon O_i \to \mathrm{End}(V)$ by

$$\varphi_1\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}0 & \frac{x}{y} & 0\\ \frac{y}{x} & 0 & 0\\ 0 & \frac{z}{y} & 0\end{pmatrix}, \text{ and } \varphi_2\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}0 & \frac{x}{y} & 0\\ 0 & 0 & \frac{y}{z}\\ 0 & \frac{z}{y} & 0\end{pmatrix}.$$

It can be easily verified that $\varphi_i(v)gv = \pi(g)v$ for all $g \in G$ and all $v \in O_i$. In particular, this proves $\pi \in \mathrm{Sym}(G, V)$.

Of course, the above maps φ_i cannot be glued to a single rational map since they do not agree on $O_1 \cap O_2$. But for the field $\Bbbk = \mathbb{R}$ of real numbers, there is another choice for a rational map $\varphi\colon \operatorname{Amp}(V) \to \operatorname{End}(V)$ with actually satisfies $\varphi(v)gv = \pi(g)v$ for all $v \in \operatorname{Amp}(V)$ and all $g \in G$. It can be given by

$$\varphi \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 & \frac{x}{y} & 0 \\ \frac{xy}{x^2+z^2} & 0 & \frac{yz}{x^2+z^2} \\ 0 & \frac{z}{y} & 0 \end{pmatrix}.$$

This map is well defined on $\operatorname{Amp}(V)$ since $x^2 + z^2 = 0$ implies $x = 0$ and $z = 0$ over the real numbers. Over the complex numbers this implication does of course not hold, and actually in that case we cannot choose a single rational map to satisfy Lemma 3.3.3.

Claim. For $\Bbbk = \mathbb{C}$ there is no rational map $\varphi\colon \operatorname{Amp}(V) \to \operatorname{End}(V)$ with $\varphi(v)gv = \pi(g)v$ for all $v \in \operatorname{Amp}(V)$ and all $g \in G$.

Proof. Let $\mathbb{E} = \mathbb{C}(X, Y, Z)$ be the field of rational functions over $\mathbb{C}$ in three indeterminates. Suppose the claim is wrong, so that such a rational map $\varphi\colon \operatorname{Amp}(V) \to \operatorname{End}(V)$ exists. This means there is a matrix $A \in \mathbb{E}^{3\times 3}$ with entries defined on $\operatorname{Amp}(V)$ such that $A(v)gv = \pi(g)v$ for all $v \in \operatorname{Amp}(V)$ and all $g \in G$. We pick some common denominator of A, that is, a polynomial $f \in \mathbb{C}[X, Y, Z]$ such that f is nonzero on $\operatorname{Amp}(V)$, and the entries of fA are polynomials. Then

$$\operatorname{zeros}(f) \subseteq V \setminus \operatorname{Amp}(V) = \operatorname{zeros}(X, Z) \cup \operatorname{zeros}(Y),$$

and by the *principal ideal theorem* (see e.g. [18, Theorem 2.6.1]) we even have $\operatorname{zeros}(f) \subseteq \operatorname{zeros}(Y)$. By Hilbert's Nullstellensatz (see e.g. [18, Theorem 1.4.5]), it follows $f = cY^n$ for some $0 \neq c \in \mathbb{C}$ and $n \in \mathbb{N}$. In particular, all entries of $Y^n \cdot A$ are polynomials.

Since the equations $A(v)v = v$ and $A(v)tv = sv$ hold for almost all points $v \in V$, we get equations of rational functions

$$A \cdot (X, Y, Z)^\intercal = (X, Y, Z)^\intercal \text{ and } A \cdot (X, -Y, Z)^\intercal = (-X, Y, -Z)^\intercal.$$

Summing up both equations and multiplying by Y^n, we get polynomial equations

$$Y^n A \cdot (X, 0, Z)^\intercal = (0, Y^{n+1}, 0)^\intercal.$$

But now reduction modulo the ideal $(X, Z) \trianglelefteq \mathbb{C}[X, Y, Z]$ yields $(0, 0, 0)^\intercal \equiv (0, Y^{n+1}, 0)^\intercal$ which is a contradiction. □

Example 3.3.5 also shows that the set $V(\pi)$ of points having a certain orbit symmetry does not need to be open or closed in V.

3.4 Scalar extensions

Many results in representation theory of finite groups require the ground field to be sufficiently large. In order to use these results, we will sometimes need to pass over to field extensions of $\Bbbk$. More precisely, if V is a finitely generated $\Bbbk G$-module, and if $\mathbb{E}/\Bbbk$ is any field extension then we can form the *scalar extension* $V^{\mathbb{E}} = \mathbb{E} \otimes_{\Bbbk} V$ which is a finitely generated $\mathbb{E}G$-module by means of the natural action (on the pure tensors)

$$G \times V^{\mathbb{E}} \to V^{\mathbb{E}}, \quad (g, e \otimes v) \mapsto e \otimes gv.$$

Scalar extensions are transitive in the sense that for any tower of field extensions $\mathbb{L}/\mathbb{E}/\Bbbk$, we have a natural isomorphism $(V^{\mathbb{E}})^{\mathbb{L}} \cong V^{\mathbb{L}}$ of $\mathbb{L}G$-modules (given by the mutually inverse homomorphisms $l \otimes (e \otimes v) \mapsto le \otimes v$ and $l \otimes v \mapsto l \otimes (1 \otimes v)$ for $l \in \mathbb{L}, e \in \mathbb{E}, v \in V$ on the pure tensors). So all scalar extensions of $V^{\mathbb{E}}$ are already scalar extensions of V. We also have a natural $\Bbbk G$-linear map $\kappa\colon V \to V^{\mathbb{E}}$ given by $v \mapsto 1 \otimes v$ which is an embedding of topological spaces (even a dense embedding if $\Bbbk$ has infinite order) by Lemma 2.1.3. It is easily seen by elementary linear algebra that scalar extensions do not affect the orbit symmetry groups of V in the sense that

$$\mathrm{Sym}(G, v) = \mathrm{Sym}(G, \kappa(v)) \text{ holds for all } v \in V.$$

In other words, we have $V(\pi) = \kappa^{-1}(V^{\mathbb{E}}(\pi))$ for all $\pi \in \mathrm{Sym}(G)$. It is rather surprising however, that scalar extensions do also not affect the generic symmetry group of V. This result (Proposition 3.4.2) is essentially an application of Theorem 3.3.4.

Recall that generic symmetries where only defined for infinite fields by now. We now extend this definition to modules over finite fields in the only possible way ensuring that Proposition 3.4.2 holds for arbitrary fields.

Definition 3.4.1. Let V be a finitely generated $\Bbbk G$-module, where $\Bbbk$ is a finite field. A permutation $\pi \in \mathrm{Sym}(G)$ is a *generic symmetry* of V if π is a generic symmetry of $V^{\mathbb{E}}$ for all field extensions $\mathbb{E}/\Bbbk$ of infinite order. As before, the set of all generic symmetries of V is denoted by $\mathrm{Sym}(G, V)$.

Proposition 3.4.2. *Let V be a finitely generated $\Bbbk G$-module, and let $\mathbb{E}/\Bbbk$ be a field extension. Then we have $\mathrm{Sym}(G, V) = \mathrm{Sym}\left(G, V^{\mathbb{E}}\right)$ as well as $\mathrm{Iv}(G, V) = \mathrm{Iv}(G, V^{\mathbb{E}})$, where $V^{\mathbb{E}}$ denotes the scalar extension of V to an $\mathbb{E}G$-module.*

Proof. The assertion on the groups of irrelevant generic symmetries follows easily by definition since we always have $\mathrm{Ker}(V^{\mathbb{E}}) = \mathrm{Ker}(V)$. So it remains to show that $\mathrm{Sym}(G, V^{\mathbb{E}}) = \mathrm{Sym}(G, V)$.

We first consider the case where $\Bbbk$ is a field of infinite order. Let $\kappa\colon V \to V^{\mathbb{E}}$ denote the dense embedding of topological spaces given by Lemma 2.1.3. For any $\pi \in \mathrm{Sym}(G, V^{\mathbb{E}})$ the set $V^{\mathbb{E}}(\pi)$ has nonempty interior in $V^{\mathbb{E}}$ by definition, so $V(\pi) = \kappa^{-1}(V^{\mathbb{E}}(\pi))$ has a nonempty interior in V. Hence, $\pi \in \mathrm{Sym}(G, V)$. Conversely, let $\pi \in \mathrm{Sym}(G, V)$ be arbitrary. Then $V(\pi)$ has nonempty interior in V, so $V^{\mathbb{E}}(\pi)$ contains the dense subset $\kappa(V(\pi))$ of $V^{\mathbb{E}}$. Consequently, $V^{\mathbb{E}}(\pi)$ is a dense subset of $V^{\mathbb{E}}$, and Theorem 3.3.4 implies that $\pi \in \mathrm{Sym}(G, V^{\mathbb{E}})$. This proves the assertion for infinite fields.

Now suppose that $\Bbbk$ is of finite order, and that $\mathbb{E}$ is of infinite order. Then by definition, we clearly have the inclusion $\mathrm{Sym}(G, V) \subseteq \mathrm{Sym}(G, V^{\mathbb{E}})$. For proving the converse direction, we have to show that $\mathrm{Sym}(G, V^{\mathbb{E}})$ is contained in $\mathrm{Sym}(G, V^{\mathbb{K}})$ for any extension field $\mathbb{K}/\Bbbk$ of infinite order. For doing so, we consider an arbitrary field $\mathbb{L}$ which is an extension of both $\mathbb{E}$ and $\mathbb{K}$ (for example, $\mathbb{L}$ can be chosen as any quotient of the $\Bbbk$-algebra $\mathbb{E} \otimes_{\Bbbk} \mathbb{K}$ by a maximal ideal). Then, by what we have proven so far, we get

$$\mathrm{Sym}(G, V^{\mathbb{E}}) = \mathrm{Sym}(G, V^{\mathbb{L}}) = \mathrm{Sym}(G, V^{\mathbb{K}}),$$

proving the assertion.

It remains to consider the case, where both $\Bbbk$ and $\mathbb{E}$ are finite fields. This case also follows immediately by what we have proven so far. Let $\mathbb{L}$ be any extension field of $\mathbb{E}$ of infinite order (for example $\mathbb{L} = \mathbb{E}(T)$, the function field over $\mathbb{E}$ in one indeterminate). Then we get

$$\mathrm{Sym}(G, V) = \mathrm{Sym}(G, V^{\mathbb{L}}) = \mathrm{Sym}(G, V^{\mathbb{E}}),$$

which finishes the proof. □

Recall that ample points have only be defined for fields of infinite order so far. The following definition of ample points over finite fields is chosen in the only possible way ensuring that ample points remain ample after extending the ground field. With that definition, it becomes a general fact that the generic symmetry group $\mathrm{Sym}(G, V)$ is contained in the orbit symmetry groups $\mathrm{Sym}(G, v)$ of all ample points $v \in \mathrm{Amp}(V)$ (which was already clear for infinite fields by Theorem 3.3.4).

Definition 3.4.3. Let V be a finitely generated $\Bbbk G$-module, where $\Bbbk$ is a finite field. An element $v \in V$ is called *ample* if for all field extensions $\mathbb{E}/\Bbbk$ of infinite order, $1 \otimes v$ is an ample point of the $\mathbb{E}G$-module $V^{\mathbb{E}}$. As before, the set of all ample points of V is denoted by $\mathrm{Amp}(V)$.

Lemma 3.4.4. *Let V be a finitely generated $\Bbbk G$-module, and let $\mathbb{E}/\Bbbk$ be a field extension. Then we have $\mathrm{Amp}(V) = \kappa^{-1}(\mathrm{Amp}(V^{\mathbb{E}}))$, where $\kappa\colon V \to V^{\mathbb{E}}$ denotes the canonical embedding.*

Proof. As before, we begin by proving the assertion in the case where $\Bbbk$ is a field of infinite order. Since $\mathbb{E}G\kappa(v)$ is the $\mathbb{E}$-linear span of $\{1 \otimes gv : g \in G\}$ for all $v \in V$, we always have $\dim_{\Bbbk}(\Bbbk Gv) = \dim_{\mathbb{E}}(\mathbb{E}G\kappa(v))$. Let d denote the maximal dimension of cyclic $\Bbbk G$-submodules of V. We have to prove that d is also the maximum dimension of cyclic $\mathbb{E}G$-submodules of $V^{\mathbb{E}}$. Since $\mathrm{Amp}(V)$ is nonempty and open in V (Lemma 3.3.2), since κ has a dense image in $V^{\mathbb{E}}$ (Lemma 2.1.3), and since nonempty open subsets are dense (Lemma 2.1.2), we see that $\kappa(\mathrm{Amp}(V))$ is a dense subset of $V^{\mathbb{E}}$ consisting of points each of which generates a d-dimensional cyclic $\mathbb{E}G$-submodule of $V^{\mathbb{E}}$. Since $\mathrm{Amp}(V^{\mathbb{E}})$ is open in $V^{\mathbb{E}}$, there is a nonempty intersection of $\mathrm{Amp}(V^{\mathbb{E}})$ and $\kappa(\mathrm{Amp}(V))$. This proves the assertion.

Now suppose that $\Bbbk$ is a finite field, and let $v \in V$ be arbitrary. We have to show that v is ample if and only if $\kappa(v)$ is an ample point of $V^{\mathbb{E}}$. If v is ample then, by definition, $1 \otimes v$ is an ample point of $V^{\mathbb{L}}$ for all infinite field extensions $\mathbb{L}/\Bbbk$. So if $\mathbb{E}$ is an infinite field then $\kappa(v)$ is ample for trivial reasons. If, on the other hand, $\mathbb{E}$ is a finite field then $1 \otimes \kappa(v)$ is an ample point of $(V^{\mathbb{E}})^{\mathbb{L}} \cong V^{\mathbb{L}}$ for all infinite field extensions $\mathbb{L}/\mathbb{E}$ by transitivity of scalar extensions. So $\kappa(v)$ is ample in that case as well.

To prove the converse implication, suppose that $\kappa(v) \in V^{\mathbb{E}}$ is ample. By definition of ample points over finite fields, we have to show that $1 \otimes v$ is an ample point of $V^{\mathbb{K}}$ for any infinite field extension $\mathbb{K}/\Bbbk$. As in the proof of Proposition 3.4.2, we consider any field $\mathbb{L}$ which is a common extension of both $\mathbb{K}$ and $\mathbb{E}$. By what we have proven so far, and by transitivity of scalar extensions, we see that $1 \otimes \kappa(v)$ is ample in $(V^{\mathbb{E}})^{\mathbb{L}}$, whence $1 \otimes v$ is ample in $V^{\mathbb{L}}$. Since $V^{\mathbb{L}} \cong (V^{\mathbb{K}})^{\mathbb{L}}$, and since both $\mathbb{K}$ and $\mathbb{L}$ are infinite fields, the same argument shows that $1 \otimes v$ is an ample point of $V^{\mathbb{K}}$. □

Corollary 3.4.5. *Let V be a finitely generated $\Bbbk G$-module, and let $v \in \operatorname{Amp}(V)$ be an ample point. Then we have $\operatorname{Sym}(G, V) \subseteq \operatorname{Sym}(G, v)$.*

Proof. By Lemma 3.4.4 and Proposition 3.4.2, we may assume without loss of generality that $\Bbbk$ is a field of infinite order. In that case, the assertion is already implied by Theorem 3.3.4. □

It is natural to ask whether the present definition of ample points over finite fields differs from the naive definition of ample points as those points generating a cyclic submodule of maximum dimension. The actual difference is illustrated in the following example.

Example 3.4.6. Let $G = (C_2)^3 = \langle x, y, z\rangle$ be the elementary abelian group with eight elements, and let $\Bbbk$ be a field of characteristic two. We consider the $\Bbbk$-linear action of G on $V = \Bbbk^5$ given by

$$x \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ a+d \\ e \end{pmatrix}, \quad y \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \\ b+e \end{pmatrix}, \quad z \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ e \end{pmatrix} = \begin{pmatrix} a \\ b \\ a+b+c \\ d \\ e \end{pmatrix}.$$

Then V is a $\Bbbk G$-module. It can be shown by examining all cases that $\dim(\Bbbk G v) \leq 3$ for all points $v \in \mathbb{F}_2^5$ having coefficients in the prime field. If $\Bbbk$ contains more than two elements however, there are points $v \in V$ such that $\dim(\Bbbk G v) = 4$ (for example, $v = (1, b, 0, 0, 0)^\intercal$ for an arbitrary element $b \in \Bbbk \setminus \mathbb{F}_2$). So in the case $\Bbbk = \mathbb{F}_2$, the $\Bbbk G$-module V does not contain ample points.

Although there are $\Bbbk G$-modules without ample points, we will usually deal with modules for which the existence of ample points is guaranteed. For example, if V is a cyclic $\Bbbk G$-module then the ample points of V are precisely the generators of V (in particular, $\operatorname{Amp}(V) \neq \emptyset$). In Section 3.6, we introduce another class of modules which always have ample points.

3.5 Generic points

We are finally able to prove that the generic symmetry group $\operatorname{Sym}(G,V)$ of any finitely generated $\Bbbk G$-module V is the orbit symmetry group of almost all $v \in V$ (thereby justifying our definition of generic symmetries), provided that $\Bbbk$ is an infinite field.

Definition 3.5.1. Let V be a finitely generated $\Bbbk G$-module. An ample point $v \in \operatorname{Amp}(V)$ is called a *generic point* of V if $\operatorname{Sym}(G,v) = \operatorname{Sym}(G,V)$. The set of all generic points of V is denoted by $\operatorname{Gen}(V)$.

Theorem 3.5.2. *Let V be a finitely generated $\Bbbk G$-module. If $\Bbbk$ is an infinite field then $\operatorname{Gen}(V)$ is nonempty and open in V. In particular, we have $\operatorname{Sym}(G,V) = \operatorname{Sym}(G,v)$ for almost all $v \in V$ in that case.*

Proof. We express the set of generic points as

$$\operatorname{Gen}(V) = \bigcap_{\pi \notin \operatorname{Sym}(G,V)} \operatorname{Amp}(V) \setminus V(\pi).$$

By Theorem 3.3.4, $\operatorname{Amp}(V) \setminus V(\pi)$ is nonempty provided that $\pi \notin \operatorname{Sym}(G,V)$, and by Lemma 3.3.3, $\operatorname{Amp}(V) \setminus V(\pi)$ is always open in V. As a finite intersection of nonempty open sets, $\operatorname{Gen}(V)$ is nonempty and open as well (by Lemma 2.1.2). $\square$

If V is a $\Bbbk G$-module over a finite field $\Bbbk$ then $\operatorname{Gen}(V)$ may be empty (even if $\operatorname{Amp}(V)$ is nonempty), as we will see in Example 3.6.4. In [10], we additionally imposed generic points to have a minimum possible stabilizer in G. However, this property is already implied by the present definition, as the following lemma shows. Note that the results of the latter section imply that generic points remain generic after extending the ground field. Thus, many questions on generic points over arbitrary fields can be reduced to the case of infinite fields.

Lemma 3.5.3. *Let V be a finitely generated $\Bbbk G$-module. For any generic point $v \in \operatorname{Gen}(V)$, we have $G_v = \operatorname{Ker}(V)$. In particular, we have $\operatorname{Iv}(G,v) = \operatorname{Iv}(G,V)$.*

Proof. By passing over to an extension field if necessary, we may assume without loss of generality that $\Bbbk$ is a field of infinite order. Let $H = G_v$ be the stabilizer of v in G. Of course we have $\operatorname{Ker}(V) \subseteq H$. Suppose there is an element $h \in H \setminus \operatorname{Ker}(V)$. As a linear operator on V, h has an eigenvalue 1 since $hv = v$. On the other hand, V is not an eigenspace of h, so the union of all eigenspaces of h is a proper closed subset of V by Lemma 2.1.2. Hence, there is a point $w \in \operatorname{Amp}(V)$ lying in no eigenspace of h. We choose $g_3, \ldots, g_n \in G$ such that $w, hw, g_3 w \ldots, g_n w$ is a basis of $\Bbbk Gw$. As $|G : H| = |Gv| \geq n$, there is a left coset gH different from $H, g_3 H, \ldots, g_n H$. We consider the permutation $\pi = (g, gh)$ which is an (irrelevant) orbit symmetry of v. Since v is a generic point, π is a generic symmetry of V. By Theorem 3.3.4, π must be an orbit symmetry of w as well, realized by $\alpha \in \operatorname{GL}(Gw)$, say. By construction, α fixes a basis of $\Bbbk Gw$, so α is the identity. We conclude $ghw = \pi(g)w = \alpha(gw) = gw$, and hence $hw = w$. This contradicts the fact that w lies in no eigenspace of h. $\square$

We pause to give a short summary of what we have proven so far. Let V be a finitely generated $\Bbbk G$-module over an infinite field $\Bbbk$, and let $K = \operatorname{Ker}(V)$ be the kernel of V in G. We have assigned to V the generic symmetry group $\operatorname{Sym}(G, V)$ which solely depends on the isomorphism type of V. Almost all points $v \in V$ are generic, that is, the orbit Gv has the maximum possible size, Gv spans a subspace of maximum possible dimension in V, and any orbit symmetry of v is an orbit symmetry of almost all points of V. If $v \in \operatorname{Gen}(V)$ is any generic point, we have a chain of canonical isomorphisms

$$\operatorname{Sym}(G/K, V) \cong \operatorname{Sym}(G, V)/\operatorname{Iv}(G, V) = \operatorname{Sym}(G, v)/\operatorname{Iv}(G, v) \cong \operatorname{GL}(Gv).$$

So the orbits of all generic points in V have isomorphic linear symmetry groups.

As we will see in Example 3.6.4, it can be tedious to determine generic points of some given module. By passing over to a certain field extension however, we can easily name a concrete generic point. The following proposition serves as a simple computational tool for determining generic symmetry groups.

Proposition 3.5.4. *Let $D\colon G \to \operatorname{GL}(n, \Bbbk)$ be a matrix representation, and let $\mathbb{E} = \Bbbk(T)$, where $T = (T_1, \ldots, T_n)$ is a vector of indeterminates over $\Bbbk$. Then T is a generic point of $\mathbb{E}^n$ regarded as an $\mathbb{E}G$-module given by D.*

Proof. Let $U = \Bbbk^n$ be the $\Bbbk G$-module given by the representation D, and let $V = \mathbb{E}^n$ be the $\mathbb{E}G$-module given by D. Note that V is canonically isomorphic to the scalar extension $U^{\mathbb{E}}$ (the isomorphism is given by $e \otimes x \mapsto ex$). We have to show that T is an ample point of V with $\operatorname{Sym}(G, T) = \operatorname{Sym}(G, V)$. By Proposition 3.4.2 and Lemma 3.4.4, we may assume without loss of generality that the field $\Bbbk$ has infinite order (otherwise, we replace $\Bbbk$ by some infinite extension $\mathbb{K}$ and $\mathbb{E} = \Bbbk(T)$ by $\mathbb{K}(T)$ such that T is still a vector of indeterminates over $\mathbb{K}$).

Let $v \in U$ be any ample point. Then v is still an ample point of V by Lemma 3.4.4, so T is ample if and only if $\dim_{\Bbbk}(\Bbbk Gv) \leq \dim_{\mathbb{E}}(\mathbb{E}GT)$. Let $M_1 \in \Bbbk^{n \times |G|}$ be the matrix with columns $D(g)v$ for $g \in G$, and let $M_2 \in \mathbb{E}^{n \times |G|}$ be the matrix with columns $D(g)T$, respectively. Then M_1 is the result of the substitution (that is, of the unique $\Bbbk$-algebra homomorphism $\Bbbk[T] \to \Bbbk$) $T_i \mapsto v_i$ applied to the entries of M_2. By considering the minors of M_1 and M_2, we see that the rank of M_2 is at least the rank of M_1, proving that $T \in V$ is ample.

By Corollary 3.4.5 and Proposition 3.4.2, we have $\operatorname{Sym}(G, U) = \operatorname{Sym}(G, V) \subseteq \operatorname{Sym}(G, T)$. We finish the proof by showing that any orbit symmetry $\pi \in \operatorname{Sym}(G, T)$ is a generic symmetry of U. Let $A \in \mathbb{E}^{n \times n}$ be any matrix (A may be non-unique unless $V = \mathbb{E}GT$) satisfying

$$AD(g)T = D(\pi(g))T \text{ for all } g \in G.$$

There is a nonempty open subset $O \subseteq U$ such that the entries of A can be evaluated at any point of O (for example $O = \{x \in U : f(x) \neq 0\}$, where $f \in \Bbbk[T]$ is any nonzero polynomial such that all entries of $f \cdot A$ are polynomials). If $A_x \in \Bbbk^{n \times n}$ denotes the matrix obtained by the substitution $T_i \mapsto x_i$ applied to A, we get equations

$$A_x D(g)x = D(\pi(g))x \text{ for all } g \in G, x \in O.$$

So π is an orbit symmetry of any element of the nonempty open subset $O \subseteq V$. By definition, we conclude $\pi \in \mathrm{Sym}(G, U)$. □

Remark 3.5.5. Proposition 3.5.4 shows that any generic symmetry group can be computed as the orbit symmetry group of a certain point. This approach can be refined if the ground field is contained in the field $\mathbb{C}$ of complex numbers. In that case, the computation of a generic symmetry group can actually be reduced to a (colored) graph automorphism problem. This was shown in [9, Theorem 4.3] for the field of real numbers, but the argument generalizes to any subfield of $\mathbb{C}$. In [9] we actually defined a generic symmetry group (which we called *generic orbit permutation group* then) as the orbit symmetry group of a vector of indeterminates.

3.6 Generic symmetries of submodules

In the following, we study the connection between generic symmetry groups $\mathrm{Sym}(G, V)$ of $\Bbbk G$-modules V and generic symmetry groups $\mathrm{Sym}(G, W)$ of submodules $W \leq V$. In general, there is no set inclusion between $\mathrm{Sym}(G, V)$ and $\mathrm{Sym}(G, W)$ in any direction. There are positive results however, provided that W contains ample points, or even generic points of V. Before stating these results, we need to recall some standard facts on semisimple modules and rings.

A module M over any ring is called *simple* if M is a nonzero module having no nonzero proper submodules. A module M is called *semisimple* if M is the sum of its simple submodules. In that case, M is even a direct sum of certain simple submodules, and any submodule of M has a complement in M [22, Theorem 2.4]. Moreover, all submodules and all quotients of semisimple modules are semisimple again [23, Ch. XVII Proposition 2.2]. Let N, M be finitely generated semisimple modules with direct sum decompositions

$$M \cong S_1^{(e_1)} \oplus \cdots \oplus S_n^{(e_n)}, \quad N \cong S_1^{(f_1)} \oplus \cdots \oplus S_n^{(f_n)}$$

into non-isomorphic simple modules S_i with (possibly zero) integral multiplicities e_i, f_i. By the Jordan-Hölder theorem for modules [4, Theorem 3.11], these multiplicities are unique. Moreover, N is isomorphic to a submodule of M (or equivalently, to a quotient of M) if and only if $f_i \leq e_i$ for all i. A ring R is called semisimple if R is semisimple regarded as a left module over itself. In that case, all left and all right R-modules are automatically semisimple, projective, and injective [22, Theorem 2.5]. If G is a finite group and if $\Bbbk$ is any field such that $\mathrm{char}(\Bbbk) \nmid |G|$ then Maschke's theorem states that $\Bbbk G$ is a semisimple ring. In particular, if $\Bbbk$ is a field of characteristic zero, then all finite dimensional group algebras over $\Bbbk$ (and all their modules) are semisimple. If, on the other hand, the characteristic of $\Bbbk$ divides the order of G (or if G is an infinite group) then $\Bbbk G$ is not semisimple, as the trivial $\Bbbk G$-module $\Bbbk$ is not projective [22, Theorem 6.1].

If R is a finite dimensional algebra over a field (or more generally, a semilocal ring) then there is a unique minimal two sided ideal $J \subset R$ (namely, the Jacobson radical) of R such that R/J is a semisimple ring. Moreover, all semisimple R-modules are annihilated by J, and so are R/J-modules in a natural way [22, Proposition 4.8, Theorem 4.14].

Among all $\Bbbk$-algebras, group algebras have the special property that scalar extensions of their semisimple modules always stay semisimple. Equivalently, if $\Bbbk G$ is a group algebra with Jacobson radical $J \subset \Bbbk G$, and if $\mathbb{E}/\Bbbk$ is any field extension, then the Jacobson radical of $\mathbb{E}G$ is given by the $\mathbb{E}$-linear span $\mathbb{E}J$ of J. There is a canonical isomorphism $(\Bbbk G/J)^{\mathbb{E}} \cong \mathbb{E}G/\mathbb{E}J$ of $\mathbb{E}$-algebras [4, Theorem 7.10]. Furthermore, if S, T are simple $\Bbbk G$-modules then the semisimple $\mathbb{E}G$-modules $S^{\mathbb{E}}$ and $T^{\mathbb{E}}$ have no common simple constituents (up to isomorphism) [4, Theorem 7.9].

For further details, we refer to [22, Ch. 1,2], [23, Ch. XVII], and to [4, §7A].

Lemma 3.6.1. *Let V be a finitely generated semisimple $\Bbbk G$-module. Then $\operatorname{Amp}(V)$ is nonempty. Moreover, we have $\Bbbk Gx \cong \Bbbk Gy$ for all $x, y \in \operatorname{Amp}(V)$.*

Proof. Let J be the Jacobson radical of $\Bbbk G$ as in the preceding discussion. The semisimple cyclic $\Bbbk G$-modules are precisely the quotients of the semisimple left $\Bbbk G$-module $\Bbbk G/J$. So a submodule $M \leq V$ is cyclic if and only if M is isomorphic to a quotient of $\Bbbk G/J$. We consider direct sum decompositions

$$V \cong S_1^{(e_1)} \oplus \cdots \oplus S_n^{(e_n)}, \quad \Bbbk G/J \cong S_1^{(f_1)} \oplus \cdots \oplus S_n^{(f_n)}$$

into non-isomorphic simple $\Bbbk G$-modules S_i. By the previous discussion, M is a cyclic submodule of maximum dimension if and only if

$$M \cong S_1^{(\min(e_1,f_1))} \oplus \cdots \oplus S_n^{(\min(e_n,f_n))}.$$

In particular, all those maximal cyclic submodules of V are isomorphic. It remains to show that the dimensions of cyclic submodules of scalar extensions of V do not exceed the value

$$d = \dim_{\Bbbk}(M) = \min(e_1, f_1) \cdot \dim_{\Bbbk}(S_1) + \cdots + \min(e_n, f_n) \cdot \dim_{\Bbbk}(S_n).$$

Let $\mathbb{E}/\Bbbk$ be any field extension. Then, by the previous discussion, the scalar extension $S_i^{\mathbb{E}}$ of each simple $\Bbbk G$-module S_i decomposes into a direct sum $S_i^{\mathbb{E}} \cong \bigoplus_{j=1}^{l_i} T_{i,j}^{(k_{i,j})}$ into non-isomorphic simple $\mathbb{E}G$-modules $T_{i,j}$. The decompositions of V and $\mathbb{E}G/\mathbb{E}J$ into their simple constituents are uniquely given by

$$V^{\mathbb{E}} \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} T_{i,j}^{(e_i \cdot k_{i,j})} \text{ and } \mathbb{E}G/\mathbb{E}J \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{l_i} T_{i,j}^{(f_i \cdot k_{i,j})}.$$

So, by the same reasoning as before, the cyclic submodules $M' \leq V^{\mathbb{E}}$ of maximum dimension are isomorphic to $\bigoplus_{i,j} T_{i,j}^{(\min(e_i k_{i,j}, f_i k_{i,j}))}$. Their dimension is given by

$$\dim_{\mathbb{E}} M' = \sum_{i=1}^{n} \min(e_i, f_i) \sum_{j=1}^{l_i} k_{i,j} \dim_{\mathbb{E}}(T_{i,j}) = \sum_{i=1}^{n} \min(e_i, f_i) \dim_{\mathbb{E}}(S_i^{\mathbb{E}}) = d.$$

□

Proposition 3.6.2. *Let V be a finitely generated $\Bbbk G$-module over an infinite field $\Bbbk$, and let $W \leq V$ be a submodule containing an ample point of V. Then we have* $\operatorname{Sym}(G, V) \subseteq \operatorname{Sym}(G, W)$. *Equality holds if and only if W contains a generic point of V.*

Proof. Since W contains an ample point of V, we have $\operatorname{Amp}(W) \subseteq \operatorname{Amp}(V)$. By Theorem 3.3.4, we have $\operatorname{Amp}(V) \subseteq V(\pi)$, and hence $\operatorname{Amp}(W) \subseteq W(\pi)$ for all π in $\operatorname{Sym}(G, V)$. So $W(\pi)$ contains a nonempty open subset of W for all $\pi \in \operatorname{Sym}(G, V)$, which proves $\operatorname{Sym}(G, V) \subseteq \operatorname{Sym}(G, W)$.

If $\operatorname{Sym}(G, V) = \operatorname{Sym}(G, W)$ holds then any generic point of W (which exists by Theorem 3.5.2) is also a generic point of V. Conversely, if W contains a generic point of V then $\operatorname{Gen}(V) \cap W$ is a nonempty open subset of W. By Theorem 3.5.2 and since W is an irreducible topological space (Lemma 2.1.2), there is an element $v \in \operatorname{Gen}(V) \cap \operatorname{Gen}(W)$. We conclude $\operatorname{Sym}(G, V) = \operatorname{Sym}(G, v) = \operatorname{Sym}(G, W)$. □

Corollary 3.6.3. *Let V be a semisimple $\Bbbk G$-module, and let $W \leq V$ be a submodule containing an ample point of V. Then we have* $\operatorname{Sym}(G, V) = \operatorname{Sym}(G, W)$.

Proof. By Proposition 3.4.2 and Lemma 3.4.4, we may assume without loss of generality that $\Bbbk$ has infinite order. Let $w \in W \cap \operatorname{Amp}(V)$ and $v \in \operatorname{Gen}(V)$ be arbitrary. By Proposition 3.6.2 and Lemma 3.6.1, we conclude

$$\operatorname{Sym}(G, W) \subseteq \operatorname{Sym}(G, \Bbbk G w) = \operatorname{Sym}(G, \Bbbk G v) = \operatorname{Sym}(G, V) \subseteq \operatorname{Sym}(G, W).$$

□

Proposition 3.6.2 shows that the generic symmetry group of any finitely generated $\Bbbk G$-module V is already attained at some cyclic submodule of V (generated by a generic point), provided that $\Bbbk$ is an infinite field (the analog statement for finite fields does not necessarily hold, as the following example shows). If V is semisimple, such a cyclic submodule is easy to find as we can take any module generated by an ample point of V. In general however, finding a suitable cyclic submodule seems to be equally hard as finding a generic point.

Example 3.6.4. Let $\Bbbk$ be a field of characteristic two, and let

$$G = \langle s, t : s^2 = t^2 = (st)^2 = 1 \rangle$$

be the Klein four-group acting on $V = \Bbbk^3$ by

$$s\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x+y\\y\\z\end{pmatrix} \text{ and } t\begin{pmatrix}x\\y\\z\end{pmatrix} = \begin{pmatrix}x+z\\y\\z\end{pmatrix}.$$

To find the generic points of V, we shall compute the orbit symmetry groups of all elements $v = (x, y, z)^\intercal \in V$. It is easy to see that the orbit Gv always spans a linear subspace of V of dimension less or equal than two, where equality holds if and only if $y \neq 0$ or $z \neq 0$. Thus, we have

$$\mathrm{Amp}(V) = \{(x, y, z)^\intercal \in V : y \neq 0 \text{ or } z \neq 0\}.$$

Case 1: Let $y = z = 0$ (that is, v is not ample), then G acts trivially on $\Bbbk Gv$, so that $\mathrm{Sym}(G, v) = \mathrm{Iv}(G, v) = \mathrm{Sym}(G) \cong S_4$.

Case 2: Let exactly one of $y = 0, z = 0$, or $y = z$ hold (that is, v is ample, but has a nontrivial stabilizer in G). Then there are precisely two linear maps in $\mathrm{GL}(Gv)$ permuting the two elements of the orbit Gv, both of which are realized by left multiplications by elements of G. We get $\mathrm{Sym}(G, v) = G \cdot \mathrm{Iv}(G, v) \cong D_4$.

Case 3: Let $yz \neq 0$, $y \neq z$ (so that v has a trivial stabilizer in G), and suppose $y^3 = z^3$. We claim that $\mathrm{Sym}(G, v)$ consists of all even permutations on G. In particular, $\mathrm{Sym}(G, v) \cong A_4$.

Proof. It suffices to show that $H = \mathrm{Sym}(G, v)_1$, the stabilizer of $\mathrm{Sym}(G, v)$ at $1 \in G$, is cyclic of order three. Since $y^3 = z^3$, the element $\lambda = yz^{-1}$ is a primitive third root of unity, satisfying $\lambda^2 + \lambda + 1 = 0$. It follows $y^2 z^{-1} = y + z$. With that equation in mind, one easily checks that left multiplication by the matrix

$$A = \begin{pmatrix} yz^{-1} & x(y^{-1} + z^{-1}) & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

permutes the orbit Gv. More precisely, A restricts to a realization of the permutation $\pi = (s, st, t) \in \mathrm{Sym}(G)$ as an orbit symmetry of v. To finish the proof, it remains to show that H does not contain transpositions. But this is clear, since any linear map in $\mathrm{GL}(Gv)$ fixing two (necessarily linearly independent) points of Gv must be the identity map. □

Case 4: Let $yz \neq 0$, and $y^3 \neq z^3$. We claim that $\mathrm{Sym}(G, v) = G$.

Proof. Let $\alpha \in \mathrm{GL}(Gv)$ be a linear map permuting the elements of Gv such that

$\alpha(v) = v$. This map also permutes the three element set

$$\Omega = \{sv - v, tv - v, stv - v\} = \{(y, 0, 0)^\intercal, (z, 0, 0)^\intercal, (y + z, 0, 0)^\intercal\}$$

which has a one dimensional linear span U in V. The restriction of α to U is the left multiplication by an element $\lambda \in \Bbbk$ with multiplicative order less or equal than three. If λ has order three then $y = \lambda z$ or $y = \lambda^2 z$, and hence $y^3 = z^3$ which contradicts our assumption. Since $\Bbbk$ has characteristic two, λ cannot have order two. It follows $\lambda = 1$, and α acts trivially on Ω. Hence, α is the identity map, which shows that $\mathrm{Sym}(G, v) = G$. □

This case-by-case analysis shows that the generic points of V are given by

$$\mathrm{Gen}(V) = \{(x, y, z)^\intercal \in V : yz \neq 0 \text{ and } y^3 \neq z^3\}.$$

Moreover, we find $\mathrm{Sym}(G, V) = G$, and V is generically closed. However, although V always contains ample points, $\mathrm{Gen}(V)$ is nonempty only if $\Bbbk$ has more than four elements (and V has points belonging to Case 3 only if $\Bbbk$ contains a primitive third root of unity). If $v \in V$ is an element considered in the i-th case, then all ample points of $\Bbbk Gv$ also belong to the same case. Thus, we actually have $\mathrm{Sym}(G, v) = \mathrm{Sym}(G, \Bbbk Gv)$ for all $v \in V$ in this example (this can be easily seen directly, but it also follows from Theorem 4.1.7 which we prove later). In particular, the generic symmetry groups of the maximal cyclic submodules of V are isomorphic to either D_4, A_4, or $C_2 \times C_2$. In fact, if $\Bbbk$ is a subfield of $\mathbb{F}_4$ then no proper submodule of V has the same generic symmetry group as V. This does not contradict Corollary 3.6.3, but it merely shows that V is not a semisimple $\Bbbk G$-module.

3.7 Relevant eigenvalues

A very common strategy for determining a group G which acts on some set Ω is to determine a stabilizer G_ω for some $\omega \in \Omega$ first and then to determine the left cosets of G_ω in G. By the Orbit-Stabilizer theorem, the left cosets of G_ω correspond to the elements of the orbit $G\omega$. For that reason, any information constraining the orbits of G can be very useful. In the following, we introduce such a constraint on the orbits of $\mathrm{Sym}(G, V)_1$.

Definition 3.7.1. Let V be a finitely generated $\Bbbk G$-module, and let $\lambda \in \Bbbk$ be an eigenvalue of an element $g \in G$ with respect to its action on V. We call λ *relevant* if the corresponding eigenspace $\mathrm{Eig}(g, \lambda)$ contains an ample point of V (that is, if $\mathrm{Eig}(g, \lambda) \cap \mathrm{Amp}(V) \neq \emptyset$).

Proposition 3.7.2. *Let V be a finitely generated $\Bbbk G$-module. If $g, h \in G$ are elements lying in the same orbit of $\mathrm{Sym}(G, V)_1$, then g and h have the same relevant eigenvalues in $\Bbbk$. Moreover, for each common relevant eigenvalue $\lambda \in \Bbbk$ of g and h, we have $\mathrm{Eig}(g, \lambda) = \mathrm{Eig}(h, \lambda)$.*

Proof. By Proposition 3.4.2 and Lemma 3.4.4, we may assume without loss of generality that $\Bbbk$ is of infinite order. Let $\pi \in \mathrm{Sym}(G,V)_1$ a generic symmetry with $\pi(g) = h$, let λ be a relevant eigenvalue of g, and let $v \in \mathrm{Eig}(g,\lambda) \cap \mathrm{Amp}(V)$ be a corresponding ample eigenvector. Let $\alpha \in \mathrm{GL}(Gv)$ be a realization of π as an orbit symmetry of v. Then we have

$$hv = \pi(g)v = \alpha(gv) = \lambda\alpha(v) = \lambda\pi(1)v = \lambda v,$$

whence $v \in \mathrm{Eig}(h,\lambda)$. This shows that λ is a relevant eigenvalue of h as well, and that $\mathrm{Eig}(g,\lambda)\cap\mathrm{Amp}(V) \subseteq \mathrm{Eig}(h,\lambda)$. By Lemma 2.1.2 and Lemma 3.3.2, $\mathrm{Eig}(g,\lambda)\cap\mathrm{Amp}(V)$ is a dense subset of $\mathrm{Eig}(g,\lambda)$. Since linear subspaces of vector spaces are closed in the Zariski topology, we conclude $\mathrm{Eig}(g,\lambda) \subseteq \mathrm{Eig}(h,\lambda)$. The reverse inclusion follows by symmetry. □

Proposition 3.7.2 provides a powerful tool for eliminating possibilities when computing generic symmetry groups, as we will see in Example 3.8.7. But there are also theoretical applications. In Proposition 3.8.8, we reprove a result of Isaacs stating (in our terminology) that all absolutely simple $\Bbbk G$-modules are weakly generically closed. For that purpose, we use a nontrivial result from the representation theory of finite dimensional $\Bbbk$-algebras. In the special case where $|G|$ is not divisible by $\mathrm{char}(\Bbbk)$ however, Isaacs' theorem is already an immediate consequence of Proposition 3.4.2, Proposition 3.7.2, and the elementary fact that all matrices in $\mathrm{GL}(n,\Bbbk)$ of finite order coprime to $\mathrm{char}(\Bbbk)$ can be diagonalized.

3.8 Generic symmetries of cyclic modules

Lemma 3.5.3 and Proposition 3.6.2 show that any finitely generated $\Bbbk G$-module over an infinite (or at least over a sufficiently large) field contains a cyclic submodule (generated by a generic point) with the same kernel in G and the same generic symmetries. For these reasons, many questions on generic symmetries of arbitrary modules can be reduced to questions on cyclic modules. In this section we study the specifics of cyclic modules in the context of generic symmetries.

In the following, let V be any cyclic $\Bbbk G$-module with corresponding representation $D\colon G \to \mathrm{GL}(V)$. Note that in the case of cyclic modules, ample points are the same as generators (in particular, cyclic modules always have ample points). If $w \in V$ is any generator of V, we get a representation $D_w\colon \mathrm{Sym}(G,w) \to \mathrm{GL}(V)$ extending D such that

$$D_w(\pi)gw = \pi(g)w \text{ for all } g \in G, \pi \in \mathrm{Sym}(G,w).$$

In that way, V can be given the structure of a $\Bbbk\,\mathrm{Sym}(G,w)$-module, extending the action of G on V, by setting

$$\pi x = D_w(\pi)x \text{ for all } x \in V, \pi \in \mathrm{Sym}(G,w).$$

We will denote this $\Bbbk\,\mathrm{Sym}(G,w)$-module by $\widehat{V}_w$. By Corollary 3.4.5, we always have $\mathrm{Sym}(G,V) \subseteq \mathrm{Sym}(G,w)$, so by restriction of scalars, each of these modules $\widehat{V}_w$ is also a

$\Bbbk\,\mathrm{Sym}(G,V)$-module. Recall that $\mathrm{Sym}(G,V) = \mathrm{Sym}(G,V^{\mathbb{E}})$ for all field extensions $\mathbb{E}/\Bbbk$. It is easy to see by definition that we have $D_{1\otimes w}(\pi) = 1 \otimes D_w(\pi)$ for all $\pi \in \mathrm{Sym}(G,V)$ and $w \in \mathrm{Amp}(V)$. So there are equations (not merely isomorphisms) $(\widehat{V}_w)^{\mathbb{E}} = \widehat{(V^{\mathbb{E}})}_{1\otimes w}$ of $\mathbb{E}\,\mathrm{Sym}(G,V)$-modules for all $w \in \mathrm{Amp}(V)$.

In general, different choices of $w \in \mathrm{Amp}(V)$ (even of generic points) may lead to non-isomorphic modules over $\Bbbk\,\mathrm{Sym}(G,V)$, as we will see in Example 3.8.7. In the following, we develop some conditions under which these modules are isomorphic.

Recall that the *character* of a finitely generated $\Bbbk G$-module V is the map $\Bbbk G \to \Bbbk$ sending each element $x \in \Bbbk G$ to the trace of x as a linear operator on V. Since the trace function is $\Bbbk$-linear, and since G is a $\Bbbk$-basis of $\Bbbk G$, characters are usually regarded as functions $G \to \Bbbk$. Note that if V is a $\Bbbk G$-module with character $\chi\colon G \to \Bbbk$, and if $\mathbb{E}/\Bbbk$ is any field extension then $V^{\mathbb{E}}$ has the same character χ.

Lemma 3.8.1. *Let V be a cyclic $\Bbbk G$-module. Then the $\Bbbk\,\mathrm{Sym}(G,V)$-modules $\widehat{V}_w$ have the same character for all $w \in \mathrm{Amp}(V)$.*

Proof. By Proposition 3.4.2 and by the preceding discussion, we may assume without loss of generality that $\Bbbk$ is of infinite order. Let $\pi \in \mathrm{Sym}(G,V)$ be any generic symmetry, and let $\varphi\colon \mathrm{Amp}(V) \to \mathrm{GL}(V)$ be the map sending a generator $w \in \mathrm{Amp}(V)$ to the unique realization $D_w(\pi)$ of π as an orbit symmetry of w. We have to show that all images of φ have the same trace.

By Lemma 3.3.3, φ agrees locally with certain rational maps. By Lemma 2.2.4, φ must be already a rational map. For each $w \in \mathrm{Amp}(V)$, the endomorphism $\varphi(w)$ permutes a generating set Gw of V over $\Bbbk$ according to π. In particular, each operator $\varphi(w)$ has a finite order dividing $k = o(\pi)$. Now the trace $\mathrm{Tr}(\varphi(w))$ is a sum of $\dim(V)$ many k-th roots of unity. In particular, the image of the composition $\mathrm{Tr}\circ\varphi$ in $\Bbbk$ is a finite subset. On the other hand, $\mathrm{Tr}\circ\varphi$ is a rational map with an irreducible domain (as a topological space), so its image is irreducible as well (here, we use the elementary fact that the image of an irreducible topological space under a continuous map is irreducible again). Now the only finite irreducible subsets of $\Bbbk$ are the singletons, so we conclude that $\mathrm{Tr}\circ\varphi$ is a constant map. □

A standard result from the representation theory of finite groups states that the characters of non-isomorphic simple $\Bbbk G$-modules are always linearly independent as functions $G \to \Bbbk$ [17, Corollary 9.22]. For that reason, there are many situations where the character of a module V characterizes V up to isomorphism.

Proposition 3.8.2. *Let V be a cyclic $\Bbbk G$-module, and suppose that any of the following statements hold.*

(1) $\mathrm{char}(\Bbbk) = 0$

(2) $\mathrm{char}(\Bbbk) > |G|$

(3) V is simple

Then the $\Bbbk\,\mathrm{Sym}(G,V)$-modules $\widehat{V}_w$ are isomorphic for all $w \in \mathrm{Amp}(V)$.

Proof. By Lemma 3.8.1, the $\Bbbk\,\mathrm{Sym}(G,V)$-modules $\widehat{V}_w$ have the same character for all $w \in \mathrm{Amp}(V)$. So it suffices to show that the isomorphism type of $\widehat{V}_w$ is uniquely determined by its character. We argue that in each case, this is a consequence of the fact that the characters of non-isomorphic simple modules over group algebras are linearly independent.

If (3) holds then $\widehat{V}_w$ is simple for all $w \in \mathrm{Amp}(V)$, so there is nothing to show. If (1) or (2) holds then $\mathrm{char}(\Bbbk)$ does not divide the order of $\mathrm{Sym}(G)$, so the group algebra $\Bbbk\,\mathrm{Sym}(G,V)$ is semisimple. Then $\widehat{V}_w$ decomposes into a direct sum of simple $\Bbbk\,\mathrm{Sym}(G,V)$-modules, each occurring with a multiplicity less or equal to $|G|$ (by a comparison of dimensions). So the character of $\widehat{V}_w$ is a linear combination of the (linearly independent) characters of simple $\Bbbk\,\mathrm{Sym}(G,V)$-modules with nonnegative integral coefficients less or equal to $|G|$. By the hypothesis, the multiplicities of the simple constituents of $\widehat{V}_w$ (and thereby the isomorphism type of $\widehat{V}_w$) are uniquely determined by the character of $\widehat{V}_w$. □

The statement of Proposition 3.8.2 will be further refined in Theorem 4.6.4.

Corollary 3.8.3. *Let V be a cyclic $\Bbbk G$-module satisfying the hypothesis of Proposition 3.8.2. Then the linear symmetry groups* $\mathrm{GL}(Gv)$ *of the orbits of the generic points* $v \in \mathrm{Gen}(V)$ *are conjugated in* $\mathrm{GL}(V)$.

Proof. If $v \in \mathrm{Gen}(V)$ is a generic point then $\mathrm{GL}(Gv)$ is the image of the representation $D_v\colon \mathrm{Sym}(G,V) \to \mathrm{GL}(V)$. The claim follows by Proposition 3.8.2. □

We have seen so far that if G acts on a cyclic module V, then also $\mathrm{Sym}(G,V)$ acts on V (in various ways) extending the action of G. In principle, we can continue this process by considering the generic symmetry group of V with respect to the action of $\mathrm{Sym}(G,V)$ on V we have chosen. Continuing in that way, we get a sequence of groups $G_1 \leq G_2 \leq G_3 \leq \dots$, where $G_{i+1} = \mathrm{Sym}(G_i,V)$ acts on V with respect to an arbitrarily chosen generator of V for all i. It is a natural question, whether this process terminates at some point, that is, whether G_i is (weakly) generically closed for some i. To answer that question, we develop two sufficient conditions ensuring that a given module is (weakly) generically closed.

To begin with, we need to determine the kernel of $\widehat{V}_w$ in $\mathrm{Sym}(G,V)$, where $w \in \mathrm{Amp}(V)$ is any generator. If a generic symmetry $\pi \in \mathrm{Sym}(G,V)$ acts trivially on $\widehat{V}_w$ then $\pi \in \mathrm{Iv}(G,w)$ is an irrelevant orbit symmetry of w. So Lemma 3.5.3 shows $\mathrm{Ker}(\widehat{V}_w) = \mathrm{Iv}(G,V)$, provided that w is a generic point of V. Suppose that we are in the situation of Proposition 3.8.2. Then the modules $\widehat{V}_w$ are isomorphic for all $w \in \mathrm{Amp}(V)$ (regardless of w being generic or not), so the kernel of $\widehat{V}_w$ consists of the irrelevant generic symmetries of V in any case (if V does not contain generic points, we come to the same conclusion by a field extension argument). This remarkable observation will be the key ingredient for the proof of Theorem 3.8.5. To be as general as possible, we prove that statement under an even weaker hypothesis than that of Proposition 3.8.2.

Lemma 3.8.4. *Let V be a cyclic $\Bbbk G$-module, and let $w \in \mathrm{Amp}(V)$ be an ample point such that* $\mathrm{char}(\Bbbk) \nmid |G_w : \mathrm{Ker}(V)|$. *Then we have* $\mathrm{Ker}(\widehat{V}_w) = \mathrm{Iv}(G,V)$.

Proof. By Proposition 3.4.2 and Lemma 3.4.4, we may assume without loss of generality that $\Bbbk$ is of infinite order. By Proposition 3.2.7, we may further assume without loss of generality that G acts faithfully on V. We have to show that $\operatorname{Sym}(G, V)$ acts faithfully on $\widehat{V}_w$. Let $\pi \in \operatorname{Ker}(\widehat{V}_w)$ be arbitrary. That is, π is any permutation fixing all left cosets of $H = G_w$. Let $g_1, \ldots, g_d \in G$ be such that $g_1 w, \ldots, g_d w$ is a $\Bbbk$-basis of V. We consider the rational maps

$$\begin{aligned} s\colon \operatorname{Amp}(V) &\to V, \quad v \mapsto \frac{1}{|H|}\sum_{h\in H} hv, \text{ and} \\ d\colon \operatorname{Amp}(V) &\to \Bbbk, \quad v \mapsto \det(g_1 s(v), \ldots, g_d s(v)), \end{aligned}$$

where $\det\colon V^d \to \Bbbk$ is any nonzero alternating form. Note that s is well defined since $|H|$ is nonzero in $\Bbbk$ by assumption. By definition, we have $s(w) = w$, whence $d(w) \neq 0$. Since d is rational, and since $\operatorname{Gen}(V)$ is dense in V, there is a generic point $v \in \operatorname{Gen}(V)$ such that $d(v) \neq 0$. Therefore, the orbit $Gs(v)$ is a generating set of V over $\Bbbk$. Since π fixes the left cosets of H, it follows $D_v(\pi)gs(v) = gs(v)$ for all $g \in G$. So $D_v(\pi)$ fixes a generating set of V, which shows that π acts trivially on $\widehat{V}_v$. The claim now follows by Lemma 3.5.3. □

As an immediate consequence, we get the first sufficient criterion for a module being (weakly) generically closed.

Theorem 3.8.5. *Let V be a finitely generated $\Bbbk G$-module with corresponding representation $D\colon G \to \operatorname{GL}(V)$. If there is an ample point $v \in \operatorname{Amp}(V)$ such that $\operatorname{char}(\Bbbk) \nmid |G_v : \operatorname{Ker}(V)|$ and $D(G) = \operatorname{GL}(Gv)$, then V is weakly generically closed.*

Proof. By assumption, both maps $D\colon G \to \operatorname{GL}(Gv)$ and $D_v\colon \operatorname{Sym}(G, V) \to \operatorname{GL}(Gv)$ are surjective, and Lemma 3.8.4 states that $\operatorname{Ker}(D_v) = \operatorname{Iv}(G, V)$. By Proposition 3.2.7, we get a chain of canonical group isomorphisms

$$G/K \cong \operatorname{GL}(Gv) \cong \operatorname{Sym}(G, V)/\operatorname{Iv}(G, V) \cong \operatorname{Sym}(G/K, V),$$

where $K = \operatorname{Ker}(D)$. So V is generically closed as a $\Bbbk[G/K]$-module. By Lemma 3.2.11, V is weakly generically closed as a $\Bbbk G$-module. □

As a first application of Theorem 3.8.5, we give an answer to the question whether the process of taking generic symmetry groups of generic symmetry groups terminates at some point. In fact, under a mild hypothesis, any cyclic $\Bbbk G$-module is weakly generically closed as a $\Bbbk \operatorname{Sym}(G, V)$-module. This result explains in particular why the second motivational example in the introduction was generically closed.

Theorem 3.8.6. *Let V be a cyclic $\Bbbk G$-module with kernel $K = \operatorname{Ker}(V)$. Suppose that $\operatorname{char}(\Bbbk) \nmid |\operatorname{Sym}(G/K, V)_1|$ holds. Then $\widehat{V}_w$ is a weakly generically closed $\Bbbk \operatorname{Sym}(G, V)$-module for all $w \in \operatorname{Gen}(V)$.*

If either $\operatorname{char}(\Bbbk) = 0$ or $\operatorname{char}(\Bbbk) > |\operatorname{Sym}(G/K, V)|$ holds then $\widehat{V}_w$ is weakly generically closed for all (not necessarily generic) ample points $w \in \operatorname{Amp}(V)$.

Proof. Let $w \in \mathrm{Gen}(V)$ be any generic point. Then $\mathrm{Sym}(G,V)$ acts on $\widehat{V}_w$ with Kernel $\mathrm{Ker}(\widehat{V}_w) = \mathrm{Iv}(G,V)$ by Lemma 3.5.3. So by Proposition 3.2.7, the quotient group $\mathrm{Sym}(G/K,V) \cong \mathrm{Sym}(G,V)/\,\mathrm{Iv}(G,V)$ acts faithfully on $\widehat{V}_w$. By Lemma 3.2.11, we may assume without loss of generality that G acts faithfully on V and that $\mathrm{Sym}(G,V)$ acts faithfully on $\widehat{V}_w$. Then the stabilizer $\mathrm{Sym}(G,V)_w$ at $w \in V$ equals the stabilizer $\mathrm{Sym}(G,V)_1$ with respect to the action of $\mathrm{Sym}(G,V)$ on G. If $D_w\colon \mathrm{Sym}(G,V) \to V$ denotes the defining representation of $\widehat{V}_w$ then we have

$$D_w(\mathrm{Sym}(G,V)) = \mathrm{GL}(Gw) = \mathrm{GL}(\mathrm{Sym}(G,V)w),$$

so the first claim follows by Theorem 3.8.5 applied to $\mathrm{Sym}(G,V)$ acting on $\widehat{V}_w$. The second claim follows by the first part and by Proposition 3.8.2, after possibly extending the ground field to ensure that generic points exist in V (Proposition 3.4.2, Lemma 3.4.4). □

The following example shows that we cannot drop the hypotheses in the previous results.

Example 3.8.7. Let $\Bbbk$ be an infinite field of characteristic two without nontrivial roots of unity (for example, the rational function field over $\mathbb{F}_2$ in one indeterminate). We consider the infinite groups

$$\mathcal{G} = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} : a,b \in \Bbbk, c \in \{0,1\} \right\} \text{ and } \mathcal{H} = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & 0 \\ & & 1 \end{pmatrix} : a,b \in \Bbbk \right\},$$

where $\mathcal{H}$ is a subgroup of index two in $\mathcal{G}$. Let $G \le \mathcal{G}$ be any finite subgroup containing the matrices

$$s = \begin{pmatrix} 1 & 1 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \text{ and } t = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 1 \\ & & 1 \end{pmatrix}$$

(the smallest example is $G = \langle s,t \rangle$, the dihedral group of order eight). We also consider the subgroup $H = G \cap \mathcal{H}$ which has index two in G. Since any element of $\mathcal{G}$ has an order dividing four, the order of G is a power of two. Let G act on $V = \Bbbk^3$ by left multiplication, so that V becomes a $\Bbbk G$-module. This module is cyclic. In fact, for $v = (x,y,z)^\intercal \in V$ we have that $\{v, sv, tv\}$ is a basis of V if $yz \neq 0$, and $\{v, tv, (st)^2 v\}$ is a basis of V if $z \neq 0$, as can be easily seen by taking determinants. As G consists of upper triangular matrices, the latter statement implies

$$\mathrm{Amp}(V) = \{(x,y,z)^\intercal \in V : z \neq 0\}.$$

In the following, we determine the generic symmetry group of V and its corresponding representations on V with respect to ample points.

Claim. We have

$$\mathrm{Sym}(G,V)_1 = \{\pi \in \mathrm{Sym}(G) : \pi(h) = h \text{ and } \pi(th) = \pi(t)h \text{ for all } h \in H\},$$

so G is a proper subgroup of $\mathrm{Sym}(G,V)$. For any ample point $v \in \mathrm{Amp}(V)$, the image of the representation $D_v\colon \mathrm{Sym}(G,V) \to \mathrm{GL}(V)$ is contained in $\mathcal{G}$. Furthermore, there are infinitely many generic points $v \in \mathrm{Gen}(V)$ such that the corresponding representations D_v are pairwise non-isomorphic.

Proof. Let $v = (x,y,z)^\intercal \in \mathrm{Amp}(V)$ be any ample point. If $\pi \in \mathrm{Sym}(G)$ is any permutation satisfying $\pi(h) = h$ and $\pi(th) = \pi(t)h$ for all $h \in H$, one can easily verify that $\pi(g)v = A_\pi gv$ holds for all $g \in G$, where $A_\pi \in \Bbbk^{3\times 3}$ is the matrix defined in the following way:

$$\text{if } \pi(t) = \begin{pmatrix} 1 & u & v \\ & 1 & 1 \\ & & 1 \end{pmatrix} \text{ then } A_\pi = \begin{pmatrix} 1 & \frac{uy+vz}{z} & \frac{(uy+vz)y}{z^2} \\ & 1 & 0 \\ & & 1 \end{pmatrix}.$$

So $\pi \in \mathrm{Sym}(G,V)_1$ is a generic symmetry, and $D_v(\pi) = A_\pi$.

Conversely, let $\pi \in \mathrm{Sym}(G,V)_1$ be any generic symmetry fixing $1 \in G$, and let $v = (x,y,z)^\intercal \in \mathrm{Gen}(V)$ be any generic point. By Lemma 3.5.3, we have $G_v = 1$, and hence $y \neq 0$ and $z \neq 0$. It is easy to see that the elements of H are precisely those elements of G with a relevant eigenvalue 1. By Proposition 3.7.2, it follows $\pi(t) \in tH$. On the other hand, since $s \in H$ fixes the ample point $(0,0,1)^\intercal$, Proposition 3.7.2 shows that s is mapped to another element of G fixing $(0,0,1)^\intercal$. It follows

$$\pi(s) = \begin{pmatrix} 1 & \lambda & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \text{ for some } \lambda \in \Bbbk.$$

The equation

$$D_v(\pi)(sv - v) = \pi(s)v - v = \lambda(sv - v)$$

shows that λ is an eigenvalue of $D_v(\pi)$. Since $D_v(\pi)$ has finite multiplicative order, and since $\Bbbk$ contains only the trivial root of unity, the only possibility is $\lambda = 1$, and hence $\pi(s) = s$. Now we have seen that $D_v(\pi)$ agrees with A_π on the basis $\{v, sv, tv\}$ of V, so we conclude $D_v(\pi) = A_\pi$. As we have verified before, the equations

$$\pi(h)v = A_\pi hv = hv \text{ and } \pi(th)v = A_\pi thv = \pi(t)hv$$

hold for all $h \in H$, and, since $G_v = 1$, we conclude

$$\pi(h) = h \text{ and } \pi(th) = \pi(t)h \text{ for all } h \in H.$$

This proves our first claim. The second claim follows immediately, as we have

$$D_v(\mathrm{Sym}(G,V)) = G \cdot D_v(\mathrm{Sym}(G,V)_1) \subseteq \mathcal{G} \cdot \mathcal{G} \subseteq \mathcal{G}$$

for all $v \in \mathrm{Amp}(V)$.

Concerning the last claim, let $v, w \in \mathrm{Amp}(V)$ be such that D_v and D_w are isomorphic. That is, there is a matrix $Q \in \mathrm{GL}(V)$ with $Q^{-1}D_v(\pi)Q = D_w(\pi)$ for all $\pi \in \mathrm{Sym}(G,V)$.

In particular, $Q^{-1}sQ = Q^{-1}D_v(\iota_s)Q = D_w(\iota_s) = s$, and analogously $Q^{-1}tQ = t$. These equations already imply

$$Q = \begin{pmatrix} a & 0 & b \\ & a & 0 \\ & & a \end{pmatrix}$$

for certain $a, b \in \Bbbk$. It is easy to check that Q commutes with any element of $\mathcal{G}$, and hence $D_v = D_w$. Therefore, the representations of $\mathrm{Sym}(G, V)$ given by ample points are isomorphic if and only if they coincide. So it suffices to show that there are infinitely many distinct representations given by generic points. Let $v = (x, y, z)^\intercal \in \mathrm{Gen}(V)$ be a generic point, and let $\pi \in \mathrm{Sym}(G, V)_1$ be the generic symmetry with $\pi(t) = ts$. The corresponding matrix

$$D_v(\pi) = A_\pi = \begin{pmatrix} 1 & \frac{y}{z} & \frac{y^2}{z^2} \\ & 1 & 0 \\ & & 1 \end{pmatrix}$$

is uniquely determined by the fraction yz^{-1}. We consider the rational map

$$f\colon \mathrm{Amp}(V) \to \Bbbk \quad (x, y, z)^\intercal \mapsto yz^{-1},$$

which is clearly surjective. Since $\mathrm{Gen}(V)$ is dense in $\mathrm{Amp}(V)$, it follows that $f(\mathrm{Gen}(V))$ is dense in $\Bbbk$. In particular, there are infinitely many values of $f(v) = yz^{-1}$ attained by generic points v, which shows that $\{D_v(\pi) : v \in \mathrm{Gen}(V)\}$ is an infinite set. □

We have seen in the last example that any finite subgroup $G \leq \mathcal{G}$ acts faithfully $V = \Bbbk^3$ such that V is not generically closed as a $\Bbbk G$-module. There are infinitely many natural choices (even up to isomorphism) for letting $\mathrm{Sym}(G, V)$ act on V. If $w \in \mathrm{Gen}(V)$ is any generic point then $D_w(\mathrm{Sym}(G, V))$ is again a finite subgroup of $\mathcal{G}$. So regardless of the choice of w, the $\Bbbk\,\mathrm{Sym}(G, V)$-module $\widehat{V}_w$ is not generically closed either. Proceeding in that way, we get an infinite sequence of groups of strictly increasing order $G_1 \lneq G_2 \lneq G_3 \lneq \dots$ such that $G_{i+1} = \mathrm{Sym}(G_i, V)$ acts faithfully on V with respect to a generic point of G_i for all i.

This example also shows that $\mathrm{Sym}(G, V)$ does not need to act faithfully on V (with respect to non-generic ample points), even if G does. Indeed, if we consider the generic symmetry $\pi \in \mathrm{Sym}(G, V)_1$ with $\pi(t) = ts$, and the ample point $v = (0, 0, 1)^\intercal \in \mathrm{Amp}(V)$, then $D_v(\pi)$ is the identity matrix.

We close this section with a second sufficient criterion on a module for being (weakly) generically closed. The following result is originally due to Isaacs [16]. We reprove it in a completely different way, using the previously developed techniques. Later on, we give a vast generalization of that result (see Theorem 4.5.4). Recall that a $\Bbbk G$-module V is called *absolutely simple* if the scalar extension $V^{\mathbb{E}}$ is a simple $\mathbb{E}G$-module for all field extensions $\mathbb{E}/\Bbbk$. A well know result from representation theory states that a simple $\Bbbk G$-module V is absolutely simple if and only if $\mathrm{End}_{\Bbbk G}(V) = \Bbbk$ [22, Theorem 7.5].

Proposition 3.8.8 (Isaacs)**.** *Let* $\Bbbk$ *be an arbitrary field, and let* G *be any finite group. Then all absolutely simple* $\Bbbk G$*-modules are weakly generically closed.*

Proof. Let V be an absolutely simple $\Bbbk G$-module with corresponding representation $D\colon G \to \mathrm{GL}(V)$. By passing over to a field extension if necessary, we may assume without loss of generality that V contains generic points. Let $v, w \in \mathrm{Amp}(V)$ be arbitrary ample points. We claim that $D_v = D_w$. By Proposition 3.8.2, there is an isomorphism $\alpha\colon \widehat{V}_v \to \widehat{V}_w$ of $\Bbbk\,\mathrm{Sym}(G, V)$-modules. By restriction of scalars, α is also an automorphism of V as a $\Bbbk G$-module. Since V is absolutely simple, it follows that α is the left multiplication by some nonzero element of $\Bbbk$. This implies $D_v = D_w$.

Now let $v \in \mathrm{Gen}(V)$ be a fixed generic point, and let $\pi \in \mathrm{Sym}(G, V)_1$ be arbitrary. By the previous considerations, we have

$$D_v(\pi)w = D_w(\pi)w = \pi(1)w = w \text{ for all } w \in \mathrm{Amp}(V),$$

which shows that $D_v(\pi)$ is the identity on V. By Lemma 3.5.3, it follows $\pi \in \mathrm{Ker}(D_v) = \mathrm{Iv}(G, V)$. We conclude $\mathrm{Sym}(G, V) = G \cdot \mathrm{Iv}(G, V)$. □

3.9 Affine symmetries of orbit polytopes

As mentioned in the introduction, the theory on generic symmetries is originally motivated by geometric questions about orbit polytopes. In this section, we develop the connection between the abstract notions of generic symmetry groups of modules and of affine symmetry groups of orbit polytopes. Most importantly, we establish a necessary and sufficient condition on an abstract group to be isomorphic to the affine symmetry group of an orbit polytope (Theorem 3.9.6). This criterion can be seen as the starting point of our classification of the affine symmetry groups of orbit polytopes (which will ultimately be completed in Theorem 6.4.4).

In the following, we recall a minimal amount of basic facts on polytopes which are necessary for our purposes. For a comprehensive view on polytopes, we refer to [33]. A *polytope* $P \subseteq V$ is the convex hull of finitely many points of a real vector space V. A point $p \in P$ is called a *vertex* of V if there is some linear form $\lambda\colon V \to \mathbb{R}$ and a constant $c \in \mathbb{R}$ with $\lambda(x) \leq c$ for all $x \in P$ such that equality holds only for $x = p$. The set $\mathrm{Vert}(P)$ of all vertices of P is a finite set, which is characterized as the unique smallest subset $X \subseteq P$ such that $P = \mathrm{conv}\,X$ [33, Proposition 2.2]. There are different notions of symmetries of a polytope, but in any case, it is desirable that translations of a single polytope have isomorphic symmetry groups. For that reason, we cannot impose symmetries of polytopes to be linear maps. A reasonable notion of symmetry is given by affine maps.

Definition 3.9.1. Let V be a real vector space, and let $X \subseteq V$ be an arbitrary subset. An *affine symmetry* of X is a permutation on X which is the restriction of some affine map $V \to V$. The group of all affine symmetries of X is denoted by $\mathrm{AGL}(X)$.

If the vector space under consideration is an inner product space, one usually restricts to *isometric symmetries*, that is, to those affine symmetries preserving distances and angles. The following considerations are equally valid in that setting, but for simplicity, we only treat the general case of affine symmetries.

If $f \in \mathrm{AGL}(P)$ is an affine symmetry of some polytope P, it is evident from the definition that f permutes the vertices of P, and that f is uniquely determined by its restriction to $\mathrm{Vert}(P)$. In other words, $\mathrm{AGL}(P)$ acts faithfully on $\mathrm{Vert}(P)$, and the corresponding group homomorphism $\mathrm{AGL}(P) \to \mathrm{AGL}(\mathrm{Vert}(P))$ is an isomorphism. In particular, the affine symmetry group of any polytope is finite.

Definition 3.9.2. A polytope P is called an *orbit polytope* if $\mathrm{AGL}(P)$ acts transitively on $\mathrm{Vert}(P)$.

By definition, if P is an orbit polytope then P is the convex hull of one particular orbit of $\mathrm{AGL}(P)$. This observation leads to a general construction of orbit polytopes. Let $G \leq \mathrm{AGL}(V)$ be any finite subgroup, and let $v \in V$ be an arbitrary element. We define

$$\mathrm{Orb}(G, v) = \mathrm{conv}\, Gv = \mathrm{conv}\{gv : g \in G\}.$$

Lemma 3.9.3. *Keeping the previous notations, $P = \mathrm{Orb}(G, v)$ is an orbit polytope with vertex set $\mathrm{Vert}(P) = Gv$.*

Proof. Since $\mathrm{Vert}(P)$ is the unique smallest set X such that $P = \mathrm{conv}\, X$, we have $\mathrm{Vert}(P) \subseteq Gv$. By restriction of maps to P, we get a homomorphism $G \to \mathrm{AGL}(P)$ of groups. Since $\mathrm{AGL}(P)$ acts on $\mathrm{Vert}(P)$, and since a subgroup of $\mathrm{AGL}(P)$ acts transitively on the superset Gv of $\mathrm{Vert}(P)$, we conclude $\mathrm{Vert}(P) = Gv$. □

We call $\mathrm{Orb}(G, v)$ the orbit polytope of G at v. In the following, we establish the connection between the current setting and the theory of generic symmetries.

Let G be any finite group, and let V be an $\mathbb{R}G$-module such that G acts faithfully on V. Then G can be regarded as a subgroup of $\mathrm{GL}(V)$, and we may consider the orbit polytopes $P = \mathrm{Orb}(G, v)$ of G at elements $v \in V$. By the previous discussion, we may identify the affine symmetry group $\mathrm{AGL}(P)$ with the group $\mathrm{AGL}(Gv)$. The crucial point is that (since G is a linear group) we actually have $\mathrm{AGL}(Gv) = \mathrm{GL}(Gv)$. For that reason, orbit symmetry groups come into play naturally.

Lemma 3.9.4. *Let V be an $\mathbb{R}G$-module, and let $v \in V$ be arbitrary. Then we have $\mathrm{GL}(Gv) = \mathrm{AGL}(Gv)$.*

Proof. We only have to prove the inclusion $\mathrm{AGL}(Gv) \subseteq \mathrm{GL}(Gv)$. Let $f\colon V \to V$ be any affine map permuting the elements of the orbit Gv. We have to show that f agrees with a linear map on Gv. We consider the element $e = \frac{1}{|G|} \sum_{g \in G} g \in \mathbb{R}G$, and the affine map $h\colon V \to V$, $x \mapsto f(x - ex + ev) + ex - ev$. Since ev is an affine combination of the elements of Gv, and since f is an affine permutation on Gv, we have $f(ev) = ev$, and hence $h(0) = 0$. So h is a linear map. For all $g \in G$, we have $eg = e$, and consequently $h(gv) = f(gv)$. □

Now if V is a finitely generated $\mathbb{R}G$-module on which G acts faithfully, then (by the preceding discussion and by Proposition 3.1.4) we have natural isomorphisms $\mathrm{Sym}(G, v) \cong \mathrm{AGL}(\mathrm{Orb}(G, v))$ for all points $v \in V$ with a trivial stabilizer in G. In particular (by Theorem 3.5.2 and Lemma 3.5.3), we have $\mathrm{Sym}(G, V) \cong \mathrm{AGL}(\mathrm{Orb}(G, v))$ for all generic points $v \in \mathrm{Gen}(V)$.

We have seen that the generic symmetry group of any $\mathbb{R}G$-module V on which G acts faithfully is isomorphic to the affine symmetry group of orbit polytopes of G in V. In particular, G is isomorphic to the affine symmetry group of an orbit polytope, provided there is a generically closed $\mathbb{R}G$-module. It is rather surprising that the converse holds as well. More precisely, if G is a finite group isomorphic to the affine symmetry group of an orbit polytope then there exists a generically closed $\mathbb{R}G$-module. To begin with, we show that G is also the linear symmetry group of an orbit polytope in that case.

Lemma 3.9.5. *Let V be a real vector space, and let $P \subset V$ be an orbit polytope. Then there is an orbit polytope $Q \subset V$ such that* $\mathrm{AGL}(P) \cong \mathrm{AGL}(Q)$ *and* $\mathrm{AGL}(Q) = \mathrm{GL}(Q)$.

Proof. We use a similar argument to Lemma 3.9.4. Let $X = \mathrm{Vert}(P)$ be the vertex set, and let $b = \frac{1}{|X|}\sum_{x \in X} x \in P$ be the *barycenter* of P. We consider the translated polytope $Q = P - b = \mathrm{conv}\{x - b : x \in X\}$. Note that we have $f(b) = b$ for all symmetries $f \in \mathrm{AGL}(P)$, and we have $0 \in Q$. It is routine to check that the map $\mathrm{AGL}(P) \to \mathrm{AGL}(Q)$ sending a symmetry $f \in \mathrm{AGL}(P)$ to the map $x \mapsto f(x + b) - b$ is an isomorphism. As $\mathrm{AGL}(P)$ acts transitively on $\mathrm{Vert}(P)$, it follows that $\mathrm{AGL}(Q)$ acts transitively on $\mathrm{Vert}(Q) = \{x - b : x \in X\}$, proving that Q is an orbit polytope as well. Moreover, the isomorphism also shows that all affine symmetries of Q fix the origin of V. This proves $\mathrm{AGL}(Q) = \mathrm{GL}(Q)$. □

As before, let G be any finite group isomorphic to the affine symmetry group of an orbit polytope. Then by Lemma 3.9.5, there is an orbit polytope Q with $\mathrm{GL}(Q) = \mathrm{AGL}(Q)$ and an isomorphism $D\colon G \to \mathrm{GL}(Q)$. We regard D as a representation $G \to \mathrm{GL}(V)$, where V denotes the linear span of Q in its ambient space. In that way, V becomes an $\mathbb{R}G$-module on which G acts faithfully. If $v \in \mathrm{Vert}(Q)$ is any vertex of Q then we have $\mathrm{Vert}(Q) = Gv$, as Q is an orbit polytope. In particular, V is a cyclic $\Bbbk G$-module generated by v, and we have $D(G) = \mathrm{GL}(Gv)$. By Theorem 3.8.5, it follows that V is generically closed. We have proven the main result of the present section.

Theorem 3.9.6. *Let G be a finite group. Then G is isomorphic to the affine symmetry group of an orbit polytope if and only if there is a generically closed $\mathbb{R}G$-module.*

During the following chapters, we study the generic symmetries of $\Bbbk G$-modules from different viewpoints, and we develop certain methods for recognizing modules as generically closed. In combination with Theorem 3.9.6, we are able to identify an abstract finite group as the affine symmetry group of an orbit polytope. In Theorem 6.4.4, we ultimately give a complete classification of these groups.

4 The algebraic view on generic symmetries

In the last chapter, we studied the generic symmetries of a $\Bbbk G$-module V from a geometric perspective. In this chapter, we derive further insights by taking a completely different point of view. Our considerations are based on the observation that a permutation $\pi \in \mathrm{Sym}(G)$ is an orbit symmetry of some point of $v \in V$ if and only if π fixes the annihilator $\mathrm{Ann}(v)$ of v in $\Bbbk G$ as a set (Lemma 4.1.1). As a consequence, we obtain an algebraic characterization of the generic symmetries of V as those permutations fixing all left ideals of $\Bbbk G$ of a certain isomorphism type (Theorem 4.1.6).

This leads to the notion of *isomorphism class symmetries* (or *ic-symmetries* for short). We call a permutation $\pi \in \mathrm{Sym}(G)$ an ic-symmetry of a left ideal $L \leq \Bbbk G$ if π fixes all left ideals of $\Bbbk G$ isomorphic to L. Using the basic observation that any permutation fixing two left ideals $L_1, L_2 \leq \Bbbk G$ also fixes their sum $L_1 + L_2$ and their intersection $L_1 \cap L_2$, we show that an ic-symmetry π of one left ideal is usually an ic-symmetry of many other (non-isomorphic) left ideals. After restricting to semisimple group algebras (and later to the subclass of *admissible* ic-symmetries), we get a good understanding of the set of left ideals of $\Bbbk G$ for which π is an (admissible) ic-symmetry (Theorem 4.2.9 and Theorem 4.3.6).

These results on ic-symmetries of left ideals have many implications on the generic symmetries of modules. For any cyclic module V over a semisimple group algebra, we introduce a canonical decomposition $V = V_{\mathcal{I}} \oplus V_{\mathcal{N}}$ into its *ideal constituent* $V_{\mathcal{I}}$ and its *non-ideal constituent* $V_{\mathcal{N}}$. We show that non-ideal constituents are always weakly generically closed (Theorem 4.5.4), thereby generalizing a classical result of Isaacs [16] (which is Proposition 3.8.8 here). This result will be essential for the construction of generically closed $\mathbb{R}G$-modules in Chapter 6.

For the general treatment of $\Bbbk G$-modules V over arbitrary fields, we will restrict our attention to the subgroup $\mathrm{Sym}^{\mathrm{ad}}(G,V) \leq \mathrm{Sym}(G,V)$ of *admissible* generic symmetries of V. (This is actually not a restriction if $\Bbbk$ has characteristic zero or if the characteristic of $\Bbbk$ exceeds the order of G, in which case we always have $\mathrm{Sym}^{\mathrm{ad}}(G,V) = \mathrm{Sym}(G,V)$.) We show that admissible generic symmetries of a cyclic module V are also admissible generic symmetries of the constituents $V_{\mathcal{I}}$ and $V_{\mathcal{N}}$ (Proposition 4.6.1), thereby obtaining a formula for $\mathrm{Sym}^{\mathrm{ad}}(G,V)$ which only depends on the character of $V_{\mathcal{I}}$ and on the kernel of $V_{\mathcal{N}}$ (Theorem 4.6.2). We also obtain new structural insights into the $\Bbbk\mathrm{Sym}^{\mathrm{ad}}(G,V)$-modules $\widehat{V}_w$ (Theorem 4.6.4). These results are the starting point for our study of generic symmetries from the character theoretic perspective in Chapter 5.

Most results of the present chapter have already appeared in [10], but only in the characteristic zero case. While the approach taken here is similar, the considerations of ic-symmetries are substantially harder in the general setting compared to the characteristic zero case (see the discussion at the beginning of Section 4.3). In fact, the existence of non-admissible ic-symmetries (Example 4.3.9 and 4.3.10) already shows that some techniques used in [10] cannot be applied to group algebras over fields of positive characteristics. We develop a unifying theory here which applies to arbitrary fields. This theory is capable not only of reproving the known results in characteristic zero, but also of proving analogous results for admissible generic symmetries in positive characteristics.

For a comprehensive view on the algebraic background of the techniques used here, we refer to the standard textbooks [21], [22], and [4].

4.1 An algebraic characterization of generic symmetries

As before, we consider an arbitrary field $\Bbbk$, and any finite group G. Justified by Proposition 3.6.2, our focus will be mainly on cyclic modules. Recall that if V is a cyclic $\Bbbk G$-module then the ample points of V are precisely the generators of V (in particular, cyclic modules always have ample points). Moreover, for any such $v \in \operatorname{Amp}(V)$ there is a unique epimorphism $\alpha_v \colon \Bbbk G \to V$ of $\Bbbk G$-modules sending $1 \in G$ to v. Consequently, α_v induces an isomorphism

$$V \cong \Bbbk G / \operatorname{Ker}(\alpha_v) = \Bbbk G / \operatorname{Ann}(v),$$

where $\operatorname{Ann}(v) = \{x \in \Bbbk G : xv = 0\}$ is the *annihilator* of v. In particular, V is a quotient of the group algebra by a left ideal (and conversely, any quotient of $\Bbbk G$ is a cyclic module).

In the following, we need to consider a different module structure on $\Bbbk G$. Since G is a $\Bbbk$-basis of $\Bbbk G$, any permutation $\pi \in \operatorname{Sym}(G)$ uniquely extends to a $\Bbbk$-linear map $\Bbbk G \to \Bbbk G$

$$\sum_{g \in G} \lambda_g g \mapsto \sum_{g \in G} \lambda_g \pi(g),$$

which we denote by the same symbol π. In that way, $\Bbbk G$ can be regarded as a $\Bbbk \operatorname{Sym}(G)$-module. More generally, for any subgroup $P \leq \operatorname{Sym}(G)$ containing all left multiplications by elements of G (most importantly, orbit symmetry groups and generic symmetry groups), we will regard $\Bbbk G$ as a $\Bbbk P$-module. This constraint on P ensures that all $\Bbbk P$-submodules of $\Bbbk G$ are left ideals of $\Bbbk G$ in the usual sense.

Lemma 4.1.1. *Let V be a $\Bbbk G$-module with some point $w \in V$, and let $L = \operatorname{Ann}(w)$ be the annihilator of w. Then*

$$\operatorname{Sym}(G, w) = \{\pi \in \operatorname{Sym}(G) : \pi(L) \subseteq L\}.$$

If $V = \Bbbk G w$ is cyclic then there is a unique epimorphism $\Bbbk G \to \widehat{V}_w$ of $\Bbbk \operatorname{Sym}(G, w)$-modules sending $1 \in G$ to w. In particular, we have an isomorphism $\Bbbk G/L \cong \widehat{V}_w$ of $\Bbbk \operatorname{Sym}(G, w)$-modules.

Proof. By passing over to the cyclic submodule $\Bbbk G w \leq V$ if necessary, we may assume without loss of generality that w is a generator of V. Let $\pi \in \operatorname{Sym}(G, w)$ be some orbit symmetry, and let $\alpha_w \colon \Bbbk G \to V$ denote the epimorphism of $\Bbbk G$-modules sending $1 \in G$

to w. As before, the representation $\mathrm{Sym}(G, w) \to \mathrm{GL}(V)$ sending an orbit symmetry to its realization is denoted by D_w. Then for all $g \in G$ we have

$$\alpha_w(\pi(g)) = \pi(g)w = D_w(\pi)gw = \pi \cdot \alpha_w(g).$$

Since G generates $\Bbbk G$ as a vector space, and since α_w is a linear map, we see that α_w is actually a morphism of $\Bbbk\,\mathrm{Sym}(G, w)$-modules. In particular, $L = \mathrm{Ker}(\alpha_w)$ is a $\Bbbk\,\mathrm{Sym}(G, v)$-submodule. That is, we have $\pi(L) \subseteq L$ for all $\pi \in \mathrm{Sym}(G, w)$.

Conversely, let $\pi \in \mathrm{Sym}(G)$ be any permutation such that $\pi(L) \subseteq L$. Then π induces a linear map $\Bbbk G/L \to \Bbbk G/L$. Let $\psi \colon V \to V$ be the unique linear map such that the following diagram commutes.

$$\begin{array}{ccc} \Bbbk G/L & \xrightarrow{\ \pi\ } & \Bbbk G/L \\ \downarrow{\scriptstyle \alpha_w} & & \downarrow{\scriptstyle \alpha_w} \\ V & \xrightarrow{\ \psi\ } & V \end{array}$$

Then for all $g \in G$ we have

$$\psi(gw) = \psi(\alpha_w(g)) = \alpha_w(\pi(g)) = \pi(g)w,$$

whence $\pi \in \mathrm{Sym}(G, w)$ is an orbit symmetry of w realized by ψ. □

Since a permutation $\pi \in \mathrm{Sym}(G)$ is a generic symmetry of a cyclic module V if and only π is an orbit symmetry of all generators of V (Theorem 3.3.4), Lemma 4.1.1 gives rise to an algebraic characterization of generic symmetries. Before stating that characterization, we need to recall some special ring theoretical facts about group algebras.

Lemma 4.1.2. *Let $V = \Bbbk Gx$ be a cyclic $\Bbbk G$-module. The following statements hold.*

(1) $\mathrm{Amp}(V) = \{ux : u \in (\Bbbk G)^\times\}$.

(2) Two left ideals $L_1, L_2 \leq \Bbbk G$ are isomorphic if and only if $L_2 = L_1 u$ for some unit $u \in (\Bbbk G)^\times$.

(3) If a left ideal $L \leq \Bbbk G$ is isomorphic to a two-sided ideal $I \leq \Bbbk G$ then $L = I$.

(4) A left ideal $L \leq \Bbbk G$ is the annihilator of some generator of V if and only if L is isomorphic to $\mathrm{Ann}(x)$.

Proof. These results rely on the well known facts that group algebras over fields are Frobenius algebras [21, Example 16.56, Theorem 16.21], and (in particular) semilocal rings. Then (1) is a consequence of a theorem of Bass [22, Theorem 20.9], and (2) follows by [21, Proposition 15.20]. Both (3) and (4) are immediate consequences of (1), (2), and of the equation

$$\mathrm{Ann}(uw) = \mathrm{Ann}(w)u^{-1} \text{ for all } w \in V \text{ and } u \in (\Bbbk G)^\times,$$

which is easily verified. □

The last assertion in Lemma 4.1.2 can be generalized to non-cyclic modules in the semisimple setting. For non-semisimple modules however, annihilators of ample points may be non-isomorphic (this can be observed in Example 3.6.4).

Lemma 4.1.3. *Let V be a finitely generated semisimple $\Bbbk G$-module, and let $v, w \in \operatorname{Amp}(V)$ be ample points. Then we have an isomorphism $\operatorname{Ann}(v) \cong \operatorname{Ann}(w)$ of $\Bbbk G$-modules.*

Proof. By Lemma 3.6.1, we have $\Bbbk Gv \cong \Bbbk Gw$, so $\operatorname{Ann}(w)$ is also the annihilator of some generator of $\Bbbk Gv$. The claim follows by Lemma 4.1.2, as all annihilators of generators of $\Bbbk Gv$ are isomorphic. □

For any $\Bbbk G$-module V we can form its *automorphism group* $\mathrm{GL}_{\Bbbk G}(V)$ consisting of all bijective $\Bbbk G$-linear maps $V \to V$. It is routine to check that the automorphisms of a cyclic $\Bbbk G$-module V map generators of V to generators again. In other words, $\mathrm{GL}_{\Bbbk G}(V)$ acts on $\operatorname{Amp}(V)$ as a permutation group. We will see that there are nice consequences on the generic symmetries of V if this action is transitive. The following lemma characterizes that situation.

Lemma 4.1.4. *Let $V = \Bbbk Gw$ be a cyclic $\Bbbk G$-module. The following statements are equivalent.*

(1) $\operatorname{Ann}(w)$ *is a two-sided ideal of* $\Bbbk G$.

(2) $\operatorname{Ann}(v) = \operatorname{Ann}(w)$ *for all* $v \in \operatorname{Amp}(V)$.

(3) $\mathrm{GL}_{\Bbbk G}(V)$ *acts transitively on* $\operatorname{Amp}(V)$.

Proof. We prove (1) $\implies$ (2) $\implies$ (3) $\implies$ (1). If (1) holds then by Lemma 4.1.2, the annihilators of all generators of V are isomorphic to the same two-sided ideal $\operatorname{Ann}(w)$. Hence, they all coincide, and (2) holds.

Suppose (2) holds, and let $v \in \operatorname{Amp}(V)$ be any generator of V. Then we have an isomorphism $\alpha\colon \Bbbk G/\operatorname{Ann}(w) \to V$ sending $\overline{1}$ to w, as well as an isomorphism $\beta\colon \Bbbk G/\operatorname{Ann}(v) \to V$ sending $\overline{1}$ to v. Since $\operatorname{Ann}(v) = \operatorname{Ann}(w)$, we can form the composition $\alpha\beta^{-1}$ which is an automorphism of V sending v to w. So (3) holds.

Finally, suppose that (3) holds, and let $g \in G$ be arbitrary. By the hypothesis, there is an automorphism $\gamma \in \mathrm{GL}_{\Bbbk G}(V)$ such that $\gamma(w) = gw$. We compute

$$\operatorname{Ann}(w)g^{-1} = \operatorname{Ann}(gw) = \operatorname{Ann}(\gamma(w)) = \operatorname{Ann}(w).$$

Since $g \in G$ was arbitrary, this shows that $\operatorname{Ann}(w)$ is a two-sided ideal of $\Bbbk G$, whence (1) holds. □

As before, we will sometimes need to extend the ground field to ensure for example that generic points exist, or that simple modules are absolutely simple. In view of the previous results, it is clear that we need to keep track of how annihilators are affected by scalar extensions. In the following, we consider any field extension $\mathbb{E}/\Bbbk$ and any finite group G. As we have seen before, if V is any $\Bbbk G$-module then the scalar extension $V^{\mathbb{E}} = \mathbb{E} \otimes_{\Bbbk} V$ is an $\mathbb{E}G$-module in a natural way. Recall that if $f\colon V \to W$ is a homomorphism of $\Bbbk G$-modules then

$$f^{\mathbb{E}}\colon V^{\mathbb{E}} \to W^{\mathbb{E}}, \quad e \otimes x \mapsto e \otimes f(x)$$

defines a unique homomorphism of $\mathbb{E}G$-modules. Since we consider tensor products over fields (and since vector spaces over fields are free modules), $f^{\mathbb{E}}$ is an injective (surjective) homomorphism provided that f is injective (surjective). Moreover, if $k\colon K \to V$ is a *kernel* of f (that is, if k is a monomorphism of $\Bbbk G$-modules whose image in V is the kernel of f in the usual sense) then $k^{\mathbb{E}}$ is a kernel of $f^{\mathbb{E}}$. These exactness properties of tensor products are best understood in terms of *flat modules*. For the details, we refer to [21, Ch. 2].

Lemma 4.1.5. *Let V be a $\Bbbk G$-module, let $\mathbb{E}/\Bbbk$ be a field extension, and let $v \in V$ be arbitrary. Then the annihilator of $1 \otimes v \in V^{\mathbb{E}}$ is the image of the monomorphism*

$$\operatorname{Ann}(v)^{\mathbb{E}} \to \mathbb{E}G, \quad e \otimes x \mapsto ex.$$

In other words, $\operatorname{Ann}(1 \otimes v)$ *is given by the $\mathbb{E}$-linear span of* $\operatorname{Ann}(v)$ *in* $\mathbb{E}G$.

Proof. We first note that there is a natural isomorphism $\varphi\colon (\Bbbk G)^{\mathbb{E}} \to \mathbb{E}G$ of $\mathbb{E}G$-modules given by $e \otimes x \mapsto ex$ on the pure tensors (the inverse homomorphism is uniquely given by $1 \mapsto 1 \otimes 1$). Let $k\colon \operatorname{Ann}(v) \to \Bbbk G$ be the set inclusion, and let $f\colon \Bbbk G \to V$ be the unique homomorphism sending $1 \in G$ to v. Then k is a kernel of f, whence $k^{\mathbb{E}}$ is a kernel of $f^{\mathbb{E}}$. It is easy to check that we get a commutative diagram

$$\begin{array}{ccccc} \operatorname{Ann}(v)^{\mathbb{E}} & \xrightarrow{k^{\mathbb{E}}} & (\Bbbk G)^{\mathbb{E}} & \xrightarrow{f^{\mathbb{E}}} & V^{\mathbb{E}} \\ & \searrow^{k'} & \downarrow \varphi & \nearrow_{f'} & \\ & & \mathbb{E}G & & \end{array}$$

where k' is given by $e \otimes x \mapsto ex$, and where f' is given by $1 \mapsto 1 \otimes v$. By a simple diagram chasing argument, we see that k' is a kernel of f'. The claim follows since $\operatorname{Ker}(f') = \operatorname{Ann}(1 \otimes v)$. □

We are now ready to prove the main results of this section. The following theorem is the promised algebraic characterization of generic symmetries.

Theorem 4.1.6. *Let $\Bbbk$ be a field of infinite order, and let V be a finitely generated $\Bbbk G$-module with an ample point $w \in \operatorname{Amp}(V)$. Suppose that V is either semisimple or cyclic. Then we have*

$$\operatorname{Sym}(G, V) = \{\pi \in \operatorname{Sym}(G) : \pi(L) \subseteq L \textit{ for all } L \leq \Bbbk G \textit{ with } L \cong \operatorname{Ann}(w)\}.$$

If V is cyclic then there is an epimorphism $\Bbbk G \to \widehat{V}_w$ of $\Bbbk\operatorname{Sym}(G,V)$-modules sending $1 \in G$ to w. In particular, we have $\Bbbk G/\operatorname{Ann}(w) \cong \widehat{V}_w$ as $\Bbbk\operatorname{Sym}(G,V)$-modules.

Proof. By Theorem 3.3.4, and by Lemma 4.1.1, a permutation $\pi \in \operatorname{Sym}(G)$ is a generic symmetry of V if and only if π fixes the annihilators of all ample points of V. By Lemma 4.1.2 and Lemma 4.1.3, these annihilators form a single isomorphism class of left ideals in $\Bbbk G$. The final assertion follows by Lemma 4.1.1 by restriction of scalars. □

In view of Theorem 4.1.6, the situation is of course particularly nice if the hypotheses of Lemma 4.1.4 hold, since then we only have to consider a single annihilator. This situation is given for example if G is an abelian group since then the group algebra $\Bbbk G$ is commutative, and any left ideal of $\Bbbk G$ is a two-sided ideal.

Theorem 4.1.7. *Let V be a cyclic $\Bbbk G$-module such that $\operatorname{Ann}(w)$ is a two-sided ideal for some $w \in \operatorname{Amp}(V)$. Then all generators of V are generic points. Furthermore, the $\Bbbk\operatorname{Sym}(G,V)$-modules $\widehat{V}_w$ are isomorphic for all $w \in \operatorname{Amp}(V)$.*

Proof. For proving the first assertion, we may assume without loss of generality that V contains generic points (otherwise, by Lemma 4.1.5, we may pass over to a suitable scalar extension $V^{\mathbb{E}}$, and the lemma guarantees that $\operatorname{Ann}(1 \otimes w) \subseteq \mathbb{E}G$ is still a two-sided ideal). By Lemma 4.1.4, $\operatorname{GL}_{\Bbbk G}(V)$ acts transitively on $\operatorname{Amp}(V)$, so by Lemma 3.1.8, all generators of V have the same orbit symmetry groups. Since V contains generic points, it follows that all generators of V are generic.

Concerning the second assertion, we apply Lemma 4.1.4 again to get the existence of a two-sided ideal $I \leq \Bbbk G$ satisfying $\operatorname{Ann}(w) = I$ for all $w \in \operatorname{Amp}(V)$. By Lemma 4.1.1, we get isomorphisms $\widehat{V}_w \cong \Bbbk G/I$ of $\Bbbk\operatorname{Sym}(G,V)$-modules for all $w \in \operatorname{Amp}(V)$. □

Remark 4.1.8. Let V be a cyclic $\Bbbk G$-module over an infinite field, and let $L \leq \Bbbk G$ be the annihilator of some generator of V. We know by Theorem 3.3.4 that in order to test whether a permutation $\pi \in \operatorname{Sym}(G)$ is a generic symmetry of V we do not have to consider all generators of V, but only a dense subset of them. From the algebraic perspective, Theorem 4.1.6 tells us that π is a generic symmetry of V provided that π fixes all left ideals of the set $\mathcal{L} = \{L' \leq \Bbbk G : L' \cong L\}$. In view of Theorem 3.3.4, one might guess that we do not have to check all members of $\mathcal{L}$ either, but only a "dense" subset of them. This intuition can actually be made precise. We can introduce a suitable quotient topology on $\mathcal{L}$ coming from $\operatorname{Amp}(V)$. Then $\mathcal{L}$ becomes a compact and irreducible topological T_1-space. With respect to that topology, it can be shown that π is a generic symmetry of V provided that π fixes a dense subset of $\mathcal{L}$. Interesting examples of dense subsets of $\mathcal{L}$ are the left ideals of $\mathcal{L}$ which have one specific complement in $\Bbbk G$, or the left ideals of $\mathcal{L}$ generated by elements with coefficients in a smaller (while still infinite) subfield of $\Bbbk$.

4.2 Isomorphism class symmetries of left ideals

We have seen in Theorem 4.1.6 that the generic symmetries of $\Bbbk G$-modules are characterized as those permutations fixing a certain isomorphism class of left ideals of $\Bbbk G$.

The objective of this section is to study the set theoretic consequences in that situation. Note that if a permutation $\pi \in \mathrm{Sym}(G)$ fixes two left ideals $A, B \leq \Bbbk G$ then π also fixes their intersection $A \cap B$ and their sum $A + B$. Following that observation, we will identify many other isomorphism classes of left ideals fixed by π.

Definition 4.2.1. Let $L \leq \Bbbk G$ be a left ideal. We say that a permutation $\pi \in \mathrm{Sym}(G)$ *fixes* L if $\pi(L) \subseteq L$. We call π an *ic-symmetry* (short for *isomorphism class symmetry*) of L if π fixes all left ideals of $\Bbbk G$ isomorphic to L.

Note that if $\Bbbk$ is an infinite field then a permutation $\pi \in \mathrm{Sym}(G)$ is an ic-symmetry of a left ideal $L \leq \Bbbk G$ if and only if π is a generic symmetry of the cyclic $\Bbbk G$-module $\Bbbk G/L$ (Theorem 4.1.6). However, our considerations on ic-symmetries are independent of the cardinality of $\Bbbk$.

In the following, we study the set of left ideals of $\Bbbk G$ for which a fixed permutation $\pi \in \mathrm{Sym}(G)$ is an ic-symmetry.

Definition 4.2.2. Let $\Bbbk G$ be a group algebra. Then $\mathcal{L}_{\Bbbk G}$ denotes the lattice of all left ideals of $\Bbbk G$. For any permutation $\pi \in \mathrm{Sym}(G)$, we denote the set of all left ideals of $\Bbbk G$ for which π is an ic-symmetry by $\mathcal{L}_{\Bbbk G}(\pi)$.

It is clear by definition that each set $\mathcal{L}_{\Bbbk G}(\pi)$ is closed under taking isomorphic copies. It is less obvious however, that $\mathcal{L}_{\Bbbk G}(\pi)$ is actually a sublattice of $\mathcal{L}_{\Bbbk G}$, that is, that $\mathcal{L}_{\Bbbk G}(\pi)$ is closed under taking sums and intersections.

Lemma 4.2.3. *$\mathcal{L}_{\Bbbk G}(\pi)$ is a sublattice of $\mathcal{L}_{\Bbbk G}$ for all permutations $\pi \in \mathrm{Sym}(G)$.*

Proof. Let $A, B \in \mathcal{L}_{\Bbbk G}(\pi)$ be left ideals for which π is an ic-symmetry. We have to show that π fixes all isomorphic copies of $A \cap B$ and of $A + B$ in $\Bbbk G$. By Lemma 4.1.2, the isomorphic copies of $A \cap B$ are given by $(A \cap B)u = Au \cap Bu$ for unit elements $u \in (\Bbbk G)^\times$. Accordingly, the isomorphic copies of $A + B$ are given by $(A + B)u = Au + Bu$ for $u \in (\Bbbk G)^\times$. The claim follows since Au is an isomorphic copy of A, and since Bu is an isorphic copy of B, which are both fixed by π. □

As a consequence of Lemma 4.2.3, we see that if π is an ic-symmetry of some left ideal L then π is also an ic-symmetry of any left ideal which is obtained by taking sums and intersections of isomorphic copies of L. In the semisimple case, we will obtain a whole interval of left ideals for which π is an ic-symmetry in that way (Theorem 4.2.9). The bounds of that interval are given by certain two-sided ideals.

Definition 4.2.4. Let $L \leq \Bbbk G$ be a left ideal. The *ideal constituent* $L_{\mathcal{I}}$ of L is the greatest two-sided ideal of $\Bbbk G$ contained in L. Accordingly, the *ideal closure* $L_{\mathcal{J}}$ of L is defined as the smallest two-sided ideal of $\Bbbk G$ containing L.

We collect some simple properties of ideal constituents and ideal closures.

Lemma 4.2.5. *Let $A, B, L \leq \Bbbk G$ be left ideals.*

(1) We have $L_{\mathcal{I}} = \bigcap_{g \in G} Lg$ and $L_{\mathcal{J}} = \sum_{g \in G} Lg$.

(2) If $A \cong B$ *then* $A_{\mathcal{I}} = B_{\mathcal{I}}$ *and* $A_{\mathcal{J}} = B_{\mathcal{J}}$.

(3) We always have $(A \cap B)_{\mathcal{I}} = A_{\mathcal{I}} \cap B_{\mathcal{I}}$ *and* $(A + B)_{\mathcal{J}} = A_{\mathcal{J}} + B_{\mathcal{J}}$.

(4) If $L \in \mathcal{L}_{\Bbbk G}(\pi)$ *for some* $\pi \in \mathrm{Sym}(G)$ *then* $L_{\mathcal{I}} \in \mathcal{L}_{\Bbbk G}(\pi)$ *and* $L_{\mathcal{J}} \in \mathcal{L}_{\Bbbk G}(\pi)$.

Proof. Let $I = \bigcap_{g \in G} Lg$ and $J = \sum_{g \in G} Lg$. By definition, I and J are left ideals satisfying $Ig = I$ and $Jg = J$ for all $g \in G$. So I and J are two-sided ideals, and of course we have $I \subseteq L \subseteq J$. Let I' and J' be arbitrary two-sided ideals such that $I' \subseteq L \subseteq J'$. Then for all $g \in G$, we have

$$I' = I'g \subseteq Lg \subseteq J'g = J',$$

whence $I' \subseteq I$ and $J \subseteq J'$. This proves (1).

Both (3) and (4) are immediate consequences of (1) and Lemma 4.2.3. It remains to prove (2). If A and B are isomorphic left ideals then, by Lemma 4.1.2, we have $B = Au$ for some unit $u \in (\Bbbk G)^{\times}$. It follows

$$A_{\mathcal{I}} = (A_{\mathcal{I}})u \subseteq Au = B, \text{ and } B = Au \subseteq (A_{\mathcal{J}})u = A_{\mathcal{J}},$$

and consequently $A_{\mathcal{I}} \subseteq B_{\mathcal{I}}$ and $B_{\mathcal{J}} \subseteq A_{\mathcal{J}}$. The converse inclusions follow by symmetry. □

It can be easily shown that all left ideals of $\Bbbk G$ which can be written in terms of sums and intersections of isomorphic copies of a single left ideal L lie between $L_{\mathcal{I}}$ and $L_{\mathcal{J}}$. We will see that for semisimple group algebras the converse statement holds as well. Thereby, we show that an ic-symmetry of L is also an ic-symmetry of any left ideal between $L_{\mathcal{I}}$ and $L_{\mathcal{J}}$ (Theorem 4.2.9).

From now on, we impose the group algebra $\Bbbk G$ under consideration to be semisimple (see the discussion at the beginning of section 3.6), that is, we impose that the characteristic of the field $\Bbbk$ does not divide the order of the group G. In that case, all $\Bbbk G$-modules (and in particular, all left ideals of $\Bbbk G$) are semisimple. Any left ideal of $\Bbbk G$ can be decomposed into a direct sum of simple left ideals, and any left ideal has a complement in $\Bbbk G$. If

$$\Bbbk G = L_1 \oplus \cdots \oplus L_n$$

is any direct sum decomposition of $\Bbbk G$ into left ideals then there is a unique corresponding decomposition $1 = e_1 + \cdots + e_n$ of the unit element into elements $e_i \in L_i$. It is easy to see that all e_i are *orthogonal idempotents* (that is, we have $(e_i)^2 = e_i$ and $e_i e_j = 0$ for all $i \neq j$) and that each e_i is a generator of L_i. Conversely, if $e_1, \ldots, e_n \in \Bbbk G$ are orthogonal idempotents summing up to 1 then we get an associated direct sum decomposition

$$\Bbbk G = \Bbbk G e_1 \oplus \cdots \oplus \Bbbk G e_n$$

of left ideals. Since all left ideals have complements in $\Bbbk G$, we see that any left ideal of $\Bbbk G$ is a cyclic $\Bbbk G$-module generated by an idempotent element (which is non-unique in general). If $L \leq \Bbbk G$ is a left ideal then any idempotent generator $e \in L$ gives rise to a complement $\Bbbk G(1-e)$ of L generated by the idempotent $1-e$. In that way, the complements of a fixed left ideal L are in one-to-one correspondence with the idempotent generators of L. For the general theory of idempotents, we refer to [22, Ch. 7].

We will frequently use the following standard arguments.

Lemma 4.2.6. *Let $A, B \leq \Bbbk G$ be left ideals of a semisimple group algebra $\Bbbk G$, and let S be a simple submodule of $A+B$. Then S is isomorphic to a submodule of either A or B.*

Proof. Let $\iota\colon S \to A+B$ be the set inclusion, and let $\kappa\colon A+B \to (A+B)/B$ be the canonical projection. If $\kappa \circ \iota$ is the zero map then S is actually a submodule of B. If $\kappa \circ \iota$ is nonzero then it must be a monomorphism as S is simple. We conclude that S is isomorphic to a submodule of $(A+B)/B \cong A/(A \cap B)$. The claim follows since $A/(A\cap B)$ is isomorphic to a submodule of A (in fact to any complement of $A \cap B$ in A). □

The idempotent generators of two-sided ideals $I \leq \Bbbk G$ are special, as they are uniquely given by a formula in terms of the character of I. Recall that the character of a finitely generated $\Bbbk G$-module V is the map $\Bbbk G \to \Bbbk$ sending an element $x \in \Bbbk G$ to its trace as a linear operator on V. Since the trace map is $\Bbbk$-linear, and since G is a $\Bbbk$-basis of $\Bbbk G$, characters are usually regarded as functions $G \to \Bbbk$.

Lemma 4.2.7. *Let $\Bbbk G$ be a semisimple group algebra, and let $L \leq \Bbbk G$ be a left ideal generated by some idempotent $e \in \Bbbk G$. Then the following statements are equivalent.*

(1) L is a two-sided ideal.

(2) e is central*, that is, we have $ex = xe$ for all $x \in \Bbbk G$.*

If any of these statements is true then e is uniquely given by the formula

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

where χ is the character of L. Moreover, L has a unique complement in $\Bbbk G$, and this complement is a two-sided ideal again.

Proof. If e is central then $L = \Bbbk Ge$ is obviously a two-sided ideal, so the implication (2) $\implies$ (1) is trivial. Suppose that (1) holds. We first show that L has a unique complement in $\Bbbk G$. Let $C_1, C_2 \leq \Bbbk G$ be complements of L, and let $C = C_1 + C_2$. Then we certainly have $L + C = \Bbbk G$. Suppose that $L \cap C \neq 0$, and let $S \leq L \cap C$ be any simple submodule. By Lemma 4.2.6, we may assume without loss of generality that S is isomorphic to a submodule $S' \leq C_1$. By Lemma 4.1.2, we have $S' = Su$ for some unit $u \in (\Bbbk G)^\times$, and hence $S' = Su \leq Lu = L$. This contradicts $L \cap C_1 = 0$. So C must actually be a complement of L in $\Bbbk G$, and we conclude $C_1 = C = C_2$, proving uniqueness.

By the previous discussion, the idempotent generators of L are in one-to-one correspondence with the complements of L in $\Bbbk G$. Since L has only one complement, there is a unique idempotent generator $e \in L$. Since $L = Lg$ holds for all $g \in G$, it is easy to see that $g^{-1}eg$ is also an idempotent generator of L for all $g \in G$. Consequently, we have $g^{-1}eg = e$ for all $g \in G$, and hence (since G is a $\Bbbk$-basis of $\Bbbk G$), $ex = xe$ for all $x \in \Bbbk G$. This proves (2). Now the unique complement C of L is generated by by the central idempotent $1 - e$, and we already have proved that C is a two-sided ideal in that case.

It remains to determine the coefficients λ_g of $e = \sum_{g \in G} \lambda_g g$. For that purpose, we need to consider the character ρ of $\Bbbk G$ regarded as a module over itself. It is straightforward to check (by considering the standard basis G of $\Bbbk G$) that

$$\rho(1) = |G| \text{ and } \rho(g) = 0 \text{ for all } g \in G \setminus \{1\}.$$

The character of the unique complement $C = \Bbbk G(1-e)$ of I is given by $\psi = \rho - \chi$. Since $I = \Bbbk Ge$, and since e is a central idempotent, the left multiplication by e is the identity on I, and the zero map on C. Consequently, we get

$$|G| \cdot \lambda_g = \rho(eg^{-1}) = \chi(eg^{-1}) + \psi(eg^{-1}) = \chi(g^{-1})$$

for all $g \in G$. The claim follows since $\Bbbk G$ is semisimple, which means that $|G|$ is nonzero in $\Bbbk$. □

In the following, we frequently need two calculation rules for manipulating left ideals. The first rule is usually known as the *modular law*, which essentially states that the two obvious ways of mapping an arbitrary left ideal X to a left ideal between two given left ideals $A \subseteq B$ yield the same result. Formally, if $A, B, X \leq \Bbbk G$ are left ideals with $A \subseteq B$, then we have

$$(A + X) \cap B = A + (X \cap B).$$

The proof of the modular law is elementary and utterly routine. In fact, it applies more generally to submodules of any module over an arbitrary ring.

The second law we need is a distributive law. Note that lattices of submodules are usually not distributive, that is, we usually have

$$(A + B) \cap C \neq (A \cap C) + (B \cap C)$$

for submodules A, B, C of a fixed module (even for subspaces of vector spaces). However, if A, B, C are left ideals of a semisimple ring, and if we require C to be a two-sided ideal, we actually get an equality.

Lemma 4.2.8. *Let $\Bbbk G$ be a semisimple group algebra, let $A, B \leq \Bbbk G$ be left ideals, and let $I \leq \Bbbk G$ be a two-sided ideal. Then we have $(A + B) \cap I = (A \cap I) + (B \cap I)$.*

Proof. The right-to-left inclusion trivially holds without any assumption on I. So it remains to prove $(A + B) \cap I \subseteq (A \cap I) + (B \cap I)$. By Lemma 4.2.7, there is a central idempotent element $e \in \Bbbk G$ such that $I = \Bbbk Ge$. Then $f = 1 - e$ is a central idempotent such that $I = \{x \in \Bbbk G : fx = 0\}$. Let $a \in A$ and $b \in B$ be arbitrary such that $a + b \in I$. Then we have $0 = f(a+b) = fa + fb$. Since A and B are left ideals, we have $a' = a - fa \in A$ and $b' = b - fb \in B$. Furthermore, since f is idempotent, we have $fa' = fb' = 0$. So $a', b' \in I$. Finally, we see that $a + b = a' + b' \in (A \cap I) + (B \cap I)$. □

With all these arguments in mind, we are ready to prove the following important result which is (among others) a key ingredient for our generalization of Isaacs' theorem (Theorem 4.5.4).

Theorem 4.2.9. *Let $\Bbbk G$ be semisimple, and let $\pi \in \mathrm{Sym}(G)$ be an ic-symmetry of some left ideal $L \leq \Bbbk G$. Then π is an ic-symmetry of all left ideals between $L_{\mathcal{I}}$ and $L_{\mathcal{J}}$. That is, we have an implication*

$$L \in \mathcal{L}_{\Bbbk G}(\pi) \implies \{X \leq \Bbbk G : L_{\mathcal{I}} \subseteq X \subseteq L_{\mathcal{J}}\} \subseteq \mathcal{L}_{\Bbbk G}(\pi).$$

Proof. For keeping notations short, we set $\mathcal{L} = \mathcal{L}_{\Bbbk G}(\pi)$, $I = L_{\mathcal{I}}$ and $J = L_{\mathcal{J}}$. We have to show that any left ideal $X \leq \Bbbk G$ with $I \subseteq X \subseteq J$ is contained in $\mathcal{L}$. We consider some complement of I in X, which we decompose into a direct sum of simple left ideals. That is, we may write

$$X = I \oplus S_1 \oplus \cdots \oplus S_n$$

for certain simple left ideals $S_i \subseteq J$. Since $\mathcal{L}$ is a lattice by Lemma 4.2.3, it suffices to show that $\mathcal{L}$ contains all left ideals of the form $I \oplus S$, where $S \leq J$ is a simple left ideal with $S \cap I = 0$. Since J is a finite sum of isomorphic copies of L (Lemma 4.2.5), we see by Lemma 4.2.6 that S is isomorphic to a submodule of L. Since $\mathcal{L}$ contains all isomorphic copies of its members, and since no isomorphic copy of S is contained in I, we may further assume without loss of generality that S is contained in L.

We define the left ideal D to be the intersection of all isomorphic copies of L containing S. Since $\Bbbk G$ is a finite dimensional vector space, and since all left ideals are linear subspaces of $\Bbbk G$, D can also be written as the intersection of a finite subcollection of those copies of L. So we have $D \in \mathcal{L}$ by Lemma 4.2.3, and by definition, we have $I + S \subseteq D \subseteq L$. We will show that $I + S = D$, in which case we are done.

Suppose that $I + S$ is a proper submodule of D. Then there is another simple submodule $T \leq D$ with $(I + S) \cap T = 0$. By choosing complements, we may consider direct sum decompositions

$$J = L \oplus C \text{ and } L = L' \oplus T$$

with respect to certain left ideals $C, L' \leq \Bbbk G$, where $I + S \leq L'$. By the distributive law (Lemma 4.2.8), we have

$$T_{\mathcal{J}} = J \cap T_{\mathcal{J}} = (L \cap T_{\mathcal{J}}) \oplus (C \cap T_{\mathcal{J}}).$$

Since T is not contained in I (or equivalently, $T_{\mathcal{J}} \not\subseteq L$), we have $L \cap T_{\mathcal{J}} \subsetneq T_{\mathcal{J}}$, and hence $C \cap T_{\mathcal{J}} \neq 0$. By Lemma 4.2.6, and since $T_{\mathcal{J}}$ is a sum of isomorphic copies of T, there must be a simple submodule $T' \leq C$ isomorphic to T. We define $L'' = L' \oplus T'$. By definition, L'' is isomorphic to L, and $I + S \subseteq L''$, whence $D \subseteq L \cap L''$. By the modular law, we get

$$T \subseteq D \subseteq L \cap L'' = (L' + T') \cap L = L' + (T' \cap L) = L'.$$

This contradicts the fact that T has a trivial intersection with L'. □

4.3 Admissible ic-symmetries

The consideration of ic-symmetries is a lot easier in the case where the ground field has characteristic zero. In [10] we have shown that it suffices to consider the field $\mathbb{C}$ of complex numbers in that case, where we have canonical choices for complements of left ideals in $\mathbb{C}G$. In summary, if we consider the inner product on $\mathbb{C}G$ for which G is an orthonormal basis, then all permutations $\pi \in \mathrm{Sym}(G)$ act as orthogonal operators on $\mathbb{C}G$. Consequently, if π fixes some left ideal $L \leq \mathbb{C}G$ then it has to fix the orthogonal complement $L^\perp$, which is a left ideal again. With that observation, it is easy to see that if π is an ic-symmetry of L then π is also an ic-symmetry of any complement of L. Unfortunately, the idea of this approach does not apply to fields of positive characteristics, and in fact, an ic-symmetry of some left ideal $L \leq \Bbbk G$ does not have to be an ic-symmetry of a complement of L in general (see Example 4.3.9 and 4.3.10). To overcome that problem, we will exclude such “problematic” ic-symmetries from our considerations by restring to the subclass of *admissible* ic-symmetries. This subclass is designed to fulfill the same criteria as the full class of ic-symmetries in the characteristic zero case.

Although there are no canonical choices for taking complements of left ideals in general, we know that two-sided ideals have unique complements in semisimple group algebras (Lemma 4.2.7). We introduce the following terminology. For any two-sided ideal $I \leq \Bbbk G$ of a semisimple group algebra $\Bbbk G$, we denote the unique complement of I by $I^\perp$. It is easy to see that the map sending a two-sided ideal I to $I^\perp$ is a self-inverse inclusion reversing bijection (that is, an anti-automorphism) on the lattice of all two-sided ideals in $\Bbbk G$. In particular, this map interchanges intersections and sums, that is, for all two-sided ideals $I, J \leq \Bbbk G$, we have

$$(I \cap J)^\perp = I^\perp + J^\perp \text{ as well as } (I + J)^\perp = I^\perp \cap J^\perp.$$

We now restrict our attention to those ic-symmetries fixing certain complements of two-sided ideals.

Definition 4.3.1. Let $\pi \in \mathrm{Sym}(G)$ be an ic-symmetry of a left ideal $L \leq \Bbbk G$. Then π is called *admissible* (with respect to L) if π fixes both $(L_{\mathcal{I}})^\perp$ and $(L_{\mathcal{J}})^\perp$. The set of all left ideals of $\Bbbk G$ for which π is an admissible ic-symmetry is denoted by $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$.

It can be easily verified that the set of all admissible ic-symmetries of some left ideal L is a subgroup of $\mathrm{Sym}(G)$, but we will not use this observation in the present section.

By Lemma 4.2.5, we see that $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ contains all isomorphic copies of its members, and by definition, $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ is a subset of $\mathcal{L}_{\Bbbk G}(\pi)$. However, we have to put some efforts into showing that $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ is actually a sublattice. Before doing so, we identify some situations, where ic-symmetries are automatically admissible.

Lemma 4.3.2. *Let* $\Bbbk G$ *be a semisimple group algebra, and let* $\pi \in \mathrm{Sym}(G)$ *be a permutation satisfying any of the following properties.*

(1) π *is a left multiplication by some element of* G*.*

(2) The characteristic of $\Bbbk$ *does not divide the order of* P*, where* P *is the subgroup of* $\mathrm{Sym}(G)$ *generated by* G *and* π*.*

(3) π *is an automorphism or an* anti-automorphism *of* G*.*

If π *fixes any two-sided ideal* $I \leq \Bbbk G$ *then* π *also fixes the unique complement* $I^{\perp}$*. Moreover, we have* $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi) = \mathcal{L}_{\Bbbk G}(\pi)$ *in that situation.*

Here we call π an anti-automorphism if $\pi(gh) = \pi(h)\pi(g)$ holds for all $g, h \in G$. For example, the inversion map is always an anti-automorphism.

Proof. The second assertion is an immediate consequence of the first assertion and of Lemma 4.2.5. So it remains to show that π fixes $I^{\perp}$ provided that π fixes I.

Of course, there is nothing to show if (1) holds. Suppose that (2) holds. Then by Maschke's Theorem [22, Theorem 6.1], $\Bbbk P$ is a semisimple group algebra, whence $\Bbbk G$ can be regarded as a semisimple module over $\Bbbk P$. Since I is fixed by π, I is a $\Bbbk P$-submodule of $\Bbbk G$ which has a complement I' over $\Bbbk P$. Since G is a subgroup of P, I' is also a left ideal of $\Bbbk G$, and we conclude $I' = I^{\perp}$ by Lemma 4.2.7. In particular, $I^{\perp}$ is fixed by π.

Finally, suppose that (3) holds, and let $e \in I$ be the unique central idempotent generator of I given by Lemma 4.2.7. Since π is an (anti-) automorphism of G, its unique linear continuation to $\Bbbk G$ is an (anti-) automorphism as well, that is, we have $\pi(xy) = \pi(x)\pi(y)$ (or $\pi(xy) = \pi(y)\pi(x)$) for all $x, y \in \Bbbk G$. Since e is central, $\pi(e)$ is central again, and we get $\pi(xe) = \pi(x)\pi(e)$ for all $x \in \Bbbk G$ in any case. In particular, $\pi(e)$ is idempotent, and since $I = \pi(I) = \pi(\Bbbk G e) = \Bbbk G \pi(e)$, we see that $\pi(e)$ is actually an idempotent generator of I. By uniqueness, we conclude $\pi(e) = e$, and hence $\pi(1-e) = 1-e$. Finally, we get $\pi(I^{\perp}) = \pi(\Bbbk G(1-e)) = \Bbbk G \pi(1-e) = I^{\perp}$. □

Most importantly, Lemma 4.3.2 shows that if $\Bbbk$ has characteristic zero, or if the characteristic of $\Bbbk$ exceeds the order of G then all ic-symmetries are automatically admissible. In that case, all of the following considerations are valid for arbitrary ic-symmetries.

The main result of this section will be Theorem 4.3.6, which shows that admissible ic-symmetry is actually a reasonable notion of symmetry (for example, that $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ is a lattice in the first place). As a first step towards that goal, we will prove a variation of Theorem 4.2.9 in the admissible setting.

In the following, we will frequently (and implicitly) use the argument that for any left ideal $X \leq \Bbbk G$ and for any two-sided ideal $I \leq \Bbbk G$ the statements $X \cap I = 0$ and $X \subseteq I^\perp$ are equivalent. While the implication $X \subseteq I^\perp \implies X \cap I = 0$ is trivial, the other direction is an application of the distributive law. Since $(X + I^\perp) \cap I = X \cap I = 0$, $X + I^\perp$ is a complement of I in $\Bbbk G$, whence $X + I^\perp = I^\perp$.

Lemma 4.3.3. *Let $\Bbbk G$ be a semisimple group algebra, and let $\pi \in \mathrm{Sym}(G)$ be any permutation. If $L \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ then $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ contains all left ideals $X \leq \Bbbk G$ satisfying*

$$X \cap L_{\mathcal{I}} \in \{0, L_{\mathcal{I}}\} \text{ and } X \cap (L_{\mathcal{J}})^\perp \in \{0, (L_{\mathcal{J}})^\perp\}.$$

Proof. By definition of $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$, it suffices to show that $X \in \mathcal{L}_{\Bbbk G}(\pi)$, $(X_{\mathcal{I}})^\perp \in \mathcal{L}_{\Bbbk G}(\pi)$, and $(X_{\mathcal{J}})^\perp \in \mathcal{L}_{\Bbbk G}(\pi)$. In fact, we claim that it suffices to prove only the first of these three assertions as $(X_{\mathcal{I}})^\perp$ and $(X_{\mathcal{J}})^\perp$ also satisfy the hypotheses of Lemma 4.3.3. It is easy to see that if $I \leq \Bbbk G$ is any two-sided ideal then $X \cap I \in \{0, I\}$ implies $(X_{\mathcal{I}})^\perp \cap I = (X_{\mathcal{I}} + I^\perp)^\perp \in \{0, I\}$, and accordingly, $(X_{\mathcal{J}})^\perp \cap I = (X_{\mathcal{J}} + I^\perp)^\perp \in \{0, I\}$.

It remains to show that $X \in \mathcal{L}_{\Bbbk G}(\pi)$. We set $I = L_{\mathcal{I}}$ and $J = L_{\mathcal{J}}$. Then we have $I^\perp, J^\perp \in \mathcal{L}_{\Bbbk G}(\pi)$ since π is admissible with respect to L, and since two-sided ideals have no additional isomorphic copies (Lemma 4.1.2). Furthermore, the left ideal $X' = (I + X) \cap J$ obviously satisfies the hypotheses of Theorem 4.2.9, whence $X' \in \mathcal{L}_{\Bbbk G}(\pi)$. Now it is easy to see (using the modular law) that for any two-sided ideal $K \leq \Bbbk G$ we have the implications

$$\begin{aligned} X \cap K = 0 &\implies X = (X + K) \cap K^\perp, \text{ and} \\ X \cap K^\perp = K^\perp &\implies X = K^\perp + (K \cap X). \end{aligned}$$

Consequently, X can be written in terms of sums and intersections of X', $I^\perp$ and $J^\perp$. More precisely, we have $X \in \{X', X' \cap I^\perp, X' + J^\perp, (X' \cap I^\perp) + J^\perp\}$. Since $\mathcal{L}_{\Bbbk G}(\pi)$ is a lattice by Lemma 4.2.3, we conclude $X \in \mathcal{L}_{\Bbbk G}(\pi)$. □

We next show that for semisimple group algebras, the ideal constituent $L_{\mathcal{I}}$ of any left ideal L has a unique complement in L which we will call the *non-ideal constituent* of L. Later, it turns out to be a crucial fact that all admissible ic-symmetries of L respect the decomposition of L into its ideal constituent and its non-ideal constituent.

Definition 4.3.4. Let $L \leq \Bbbk G$ be a left ideal of a semisimple group algebra. Then we call $L_{\mathcal{N}} = L \cap (L_{\mathcal{I}})^\perp$ the *non-ideal constituent* of L.

Lemma 4.3.5. *Let $\Bbbk G$ be a semisimple group algebra, and let $L \leq \Bbbk G$ be some left ideal. Then the non-ideal constituent $L_{\mathcal{N}}$ of L is the unique complement of the ideal constituent $L_{\mathcal{I}}$ in L.*

Proof. We clearly have $L_{\mathcal{I}} \cap L_{\mathcal{N}} = 0$, and by the modular law, we get

$$L_{\mathcal{I}} + L_{\mathcal{N}} = L_{\mathcal{I}} + ((L_{\mathcal{I}})^\perp \cap L) = (L_{\mathcal{I}} + (L_{\mathcal{I}})^\perp) \cap L = L.$$

So $L_{\mathcal{N}}$ is a complement of $L_{\mathcal{I}}$ in L. Now if $C \leq L$ is any complement of $L_{\mathcal{I}}$ then $C \cap L_{\mathcal{I}} = 0$ implies $C \subseteq (L_{\mathcal{I}})^{\perp}$, whence $C = L_{\mathcal{N}}$. □

We now are ready to prove the essential properties of admissible ic-symmetries.

Theorem 4.3.6. *Let $\Bbbk G$ be a semisimple group algebra, let $\pi \in \mathrm{Sym}(G)$ be any permutation, and let $L \leq \Bbbk G$ be any left ideal. Then the following statements hold.*

(1) $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ is a sublattice of $\mathcal{L}_{\Bbbk G}(\pi)$ containing all isomorphic copies of its members.

(2) If $L \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ then all complements of L are contained in $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$.

(3) We have $L \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ if and only if both $L_{\mathcal{I}} \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ and $L_{\mathcal{N}} \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$.

Proof. We begin by proving (2), which is a simple application of Lemma 4.3.3. Let C be any complement of L in $\Bbbk G$. Then we clearly have $L_{\mathcal{I}} \cap C = 0$, and the distributive law shows

$$(L_{\mathcal{J}})^{\perp} = (L \oplus C) \cap (L_{\mathcal{J}})^{\perp} = C \cap (L_{\mathcal{J}})^{\perp},$$

whence $C \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$.

We next prove (1). We have already noticed that $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ is contained in $\mathcal{L}_{\Bbbk G}(\pi)$ by definition, and that Lemma 4.2.5 implies that $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ contains all isomorphic copies of its members. Let $A, B \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ be arbitrary. We claim that both $A \cap B$ and $A + B$ are contained in $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$.

We first consider the intersection $A \cap B$, which is certainly contained in $\mathcal{L}_{\Bbbk G}(\pi)$ by Lemma 4.2.3. By Lemma 4.2.5, we also see that $((A \cap B)_{\mathcal{I}})^{\perp} = (A_{\mathcal{I}})^{\perp} + (B_{\mathcal{I}})^{\perp}$ is fixed by π. So proving $A \cap B \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ comes down to showing that π fixes $((A \cap B)_{\mathcal{J}})^{\perp}$. For that purpose, we consider any direct sum decomposition

$$A \cap B = (A \cap B)_{\mathcal{I}} \oplus S_1 \oplus \cdots \oplus S_k, \tag{4.1}$$

where $S_i \leq \Bbbk G$ are simple left ideals for all i. We will apply Lemma 4.3.3 to each S_i separately. Since each S_i is contained in both A and B, we have $S_i \cap (A_{\mathcal{J}})^{\perp} = S_i \cap (B_{\mathcal{J}})^{\perp} = 0$. Furthermore, since each S_i intersects $(A \cap B)_{\mathcal{I}} = A_{\mathcal{I}} \cap B_{\mathcal{I}}$ trivially, we either have $S_i \cap A_{\mathcal{I}} = 0$ or $S_i \cap B_{\mathcal{I}} = 0$. In either case, we conclude $S_i \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$. In particular, π fixes the ideals $((S_i)_{\mathcal{J}})^{\perp}$ for all i. By taking ideal closures and complements on both sides in (4.1), we obtain

$$((A \cap B)_{\mathcal{J}})^{\perp} = ((A \cap B)_{\mathcal{I}})^{\perp} \cap ((S_1)_{\mathcal{J}})^{\perp} \cap \cdots \cap ((S_k)_{\mathcal{J}})^{\perp}.$$

Since we have already shown that π fixes $((A \cap B)_{\mathcal{I}})^{\perp}$, we condlude that π also fixes $((A \cap B)_{\mathcal{J}})^{\perp}$. This finally shows that $A \cap B \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$.

To prove that $A + B \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$, we use a duality argument. We will construct a complement C_A of A and a complement C_B of B in $\Bbbk G$ such that $C_A \cap C_B$ is a complement of $A + B$. Then, by what we have proven so far, we get $C_A, C_B \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$, and hence $A + B = C_A \cap C_B \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$. To construct these complements, we consider direct sum decompositions

$$A = A' \oplus (A \cap B), \quad B = B' \oplus (A \cap B), \quad \Bbbk G = (A + B) \oplus C,$$

where $A', B', C \leq \Bbbk G$ are arbitrary complements. Since $B' \cap A = B' \cap (A \cap B) = 0$, we see that $A + B = A' \oplus (A \cap B) \oplus B'$ and hence $\Bbbk G = A' \oplus (A \cap B) \oplus B' \oplus C$ are direct sum decompositions. Consequently, $C_A = B' \oplus C$ is a complement of A, while $C_B = A' \oplus C$ is a complement of B in $\Bbbk G$. We use the modular law to compute

$$C_A \cap C_B = (C + B') \cap C_B = C + (B' \cap C_B) = C + 0 = C.$$

This finishes the proof of (1).

It reimains to prove (3), which is a simple application of (1) and (2). Suppose that $L \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$. Since $L_{\mathcal{I}}$ is a finite intersection of isomorphic copies of L (Lemma 4.2.5), it is contained in $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ by (1). By (1) and (2), we conclude $L_{\mathcal{N}} = L \cap (L_{\mathcal{I}})^{\perp} \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$.

Conversely, suppose that both $L_{\mathcal{I}}$ and $L_{\mathcal{N}}$ are contained in $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$. Then, by Lemma 4.3.5 and by (1), we get $L = L_{\mathcal{I}} + L_{\mathcal{N}} \in \mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$. □

We close this section with a characterization of admissible ic-symmetries of two-sided ideals I. It turns out that these symmetries can be characterized in terms of the character of I as a $\Bbbk G$-module (Proposition 4.3.8).

Lemma 4.3.7. *Let $\Bbbk G$ be a group algebra decomposing into a direct sum of left ideals $\Bbbk G = A \oplus B$, and let $1 = e + f$ be the corresponding decomposition of the unit element into idempotent generators $e \in A$, and $f \in B$. Let $\pi \in \mathrm{Sym}(G)$ be any permutation. Then the following statements are equivalent.*

(1) π fixes both A and B.

(2) For all $g \in G$ we have $\pi(ge) = \pi(g)e$.

Proof. If (2) holds, then π maps a generating set of A (as a $\Bbbk$-vector space) into A, whence $\pi(A) \subseteq A$. Since $f = 1 - e$, we easily see that (2) is symmetric in the sense that also $\pi(gf) = \pi(g)f$ holds for all $g \in G$. So by the same argument, we have $\pi(B) \subseteq B$.

Suppose (1) holds. Then for all $g \in G$ we have $\pi(g(1-e)) = \pi(gf) \in B$ and hence $\pi(g(1-e))e = 0$. Expanding the left hand term, and using $\pi(ge)e = \pi(ge)$, we conclude $\pi(g)e = \pi(ge)$. □

Proposition 4.3.8. *Let $\Bbbk G$ be a semisimple group algebra, and let $I \leq \Bbbk G$ be a two-sided ideal with corresponding character χ. Then a permutation $\pi \in \mathrm{Sym}(G)$ is an admissible ic-symmetry of I (or equivalently, of $I^{\perp}$) if and only if*

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

Proof. By Lemma 4.1.2, I is the only left ideal of $\Bbbk G$ isomorphic to I. Therefore, π is an admissible ic-symmetry of I if and only if π fixes I and $I^{\perp}$. By Lemma 4.3.7, this is equivalent to $\pi(ge) = \pi(g)e$ for all $g \in G$, where $e \in I$ is the unique central idempotent generator of I given by Lemma 4.2.7. Now the assertion follows by the formula given in Lemma 4.2.7 after a comparison of coefficients. □

Recall that by Lemma 4.3.2, ic-symmetries are automatically admissible if the ground field $\Bbbk$ has characteristic zero, or if $\Bbbk$ has a sufficiently large characteristic. Nevertheless, in any positive characteristics there are infinitely many group algebras with two-sided ideals admitting non-admissible ic-symmetries.

Example 4.3.9. Let p be a prime number and let n be some integer such that $n \geq 2$ and $p^n \neq 4$. Then the semisimple group algebra $\mathbb{F}_p C_{p^n-1}$ has a two-sided ideal affording non-admissible ic-symmetries.

Proof. We consider the group $G = (\mathbb{F}_{p^n})^\times$ (which is cyclic of order $p^n - 1$) acting linearly on the $\mathbb{F}_p$-space $V = \mathbb{F}_{p^n}$. Then for $v = 1 \in V$, the orbit Gv consists of all nonzero elements of V. Thus, we have $\mathrm{GL}(Gv) = \mathrm{GL}(V)$, and hence $\mathrm{Sym}(G, v) = \mathrm{GL}(G) = \mathrm{GL}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$. Since the group algebra $\mathbb{F}_p G$ is commutative, the left ideal $I = \mathrm{Ann}(v) \subset \mathbb{F}_p G$ is two-sided. By Lemma 4.1.1 and Lemma 4.1.2, the ic-symmetries of I are given precisely by the $\mathbb{F}_p$-linear permutations on G.

Since V is isomorphic to a complement of I in $\mathbb{F}_p G$, and by Proposition 4.3.8, the admissible ic-symmetries of I are given by those (necessarily $\mathbb{F}_p$-linear) permutations π on G such that

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

where χ is the character afforded by V. In the present example, χ coincides with the relative trace map of the field extension $\mathbb{F}_{p^n}/\mathbb{F}_p$. That is, we have

$$\chi(g) = \mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(g) = g + g^p + g^{p^2} + \cdots + g^{p^{n-1}}$$

for all $g \in G$ (the sum being taken in the field $\mathbb{F}_{p^n}$). It is well known that the trace map $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p} \colon \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a surjective $\mathbb{F}_p$-linear map, having a kernel of size p^{n-1}. Since $n \geq 2$ and since $p^n \neq 4$, there are elements $x, y \in G$ with $\chi(x) \neq \chi(y)$ such that both x and y are linearly independent of 1 (there are $p^n - p$ elements in G which are linearly independent of 1, but only p^{n-1} of them can have the same trace). Now any $\mathbb{F}_p$-linear permutation π of G with $\pi(1) = 1$ and $\pi(x) = y$ is a non-admissible ic-symmetry of I since

$$\chi(\pi(1)^{-1}\pi(x)) = \chi(y) \neq \chi(x) = \chi(1^{-1}x).$$

□

The smallest example of the latter kind is the group algebra $\mathbb{F}_2 C_7$. If g denotes some generator of C_7 then (after identifying g with a suitable generator of $(\mathbb{F}_8)^\times$) the two-sided ideal I mentioned in the proof is generated by the central idempotent $e = g + g^2 + g^4 \in \mathbb{F}_2 C_7$. There are 168 ic-symmetries of I, only 21 of which are admissible. The group of admissible ic-symmetries of I is a semidirect product of the type $C_7 \rtimes C_3$ generated by the left multiplication ι_g and by the automorphism $h \mapsto h^2$ of C_7. One particular example of a non-admissible ic-symmetry of I is the permutation

$\pi = (g, g^2, g^5)(g^3, g^6, g^4)$. In fact, it can be easily checked that $\pi(ge)(1-e) = 0$ holds for all $g \in G$, so π certainly fixes I. By Lemma 4.3.7 however, $\pi(e) \neq \pi(1)e$ implies that π does not fix $I^\perp$.

The latter examples are particularly simple in the sense that they only involve two-sided ideals, for which ic-symmetries can be determined easily. With some more efforts however, these examples can also be used to construct one-sided left ideals (of non-commutative group algebras) admitting non-admissible ic-symmetries. In the following, we use some results which have not been presented so far. The reader might want to revisit this point after finishing Chapter 4.

Example 4.3.10. Let (p, n) be as in Example 4.3.9, and let H be any non-abelian group of order not divisible by p. Let $G = C_{p^n-1} \times H$, and let $\Bbbk$ be any (finite) field of characteristic p which is a splitting field for H (that is, all simple $\Bbbk H$-modules are absolutely simple). Then the semisimple group algebra $\Bbbk G$ has a one-sided left ideal affording non-admissible ic-symmetries.

Proof. Let $C = C_{p^n-1}$ be the cyclic group of order $p^n - 1$. By Example 4.3.9, the semisimple group algebra $\Bbbk C$ contains a two-sided ideal $I \leq \Bbbk C$ admitting non-admissible ic-symmetries. That is, if $I = \Bbbk Ce$ is generated by the central idempotent $e \in \Bbbk C$, there is a permutation $\pi \in \mathrm{Sym}(C)$ such that $\pi(ce)(1-e) = 0$ for all $c \in C$ but $\pi(c'e) \neq \pi(c')e$ for some $c' \in C$. Let $e_1 = \frac{1}{|C|}\sum_{c\in C} c$ be the trivial central idempotent of $\Bbbk C$. We either have $ee_1 = 0$ or $ee_1 = e_1$. By replacing e by $e - e_1$ in the latter case, we may assume without loss of generality that $ee_1 = 0$.

Since C is contained in the center of $G = C \times H$, we may also regard e as a central idempotent element of $\Bbbk G$, generating a two-sided ideal $J = \Bbbk Ge$. We define a permutation $\pi' \in \mathrm{Sym}(G)$ by setting

$$\pi'(hc) = h\pi(c) \text{ for all } h \in H, c \in C.$$

By definition, π' fixes all cosets of C in G, and it is easy to check that this permutation satisfies $\pi'(ge)(1-e) = 0$ for all $g \in G$ but $\pi'(c'e) \neq \pi'(c')e$. Thus, π' is a non-admissible ic-symmetry of J.

Since H is non-abelian, and since $\Bbbk$ is a splitting field for H, there is an absolutely simple $\Bbbk[G/C]$-module of dimension at least two. Accordingly, there is a one-sided simple left ideal $S \leq \Bbbk G$ with $C \subseteq \mathrm{Ker}(S)$. Then π' fixes all cosets of $\mathrm{Ker}(S)$ in G, so π' is an (admissible) ic-symmetry of S by Proposition 4.4.6 and Corollary 4.4.3. By Lemma 4.2.3, π' is an ic-symmetry of $L = J + S$. Since C acts trivially on S, we have $eS = ee_1S = 0$. So S is not contained in J, which shows that the left ideal L is not two-sided. Moreover, we obtain $L_{\mathcal{I}} = J$. Since π' does not fix $J^\perp$, we see that π' is a non-admissible ic-symmetry of L. □

We have seen that in any positive characteristic there are infinitely many examples of group algebras having (both one-sided and two-sided) left ideals which admit non-admissible ic-symmetries. One particular example of a non-commutative group algebra having such a one-sided left ideal is $\mathbb{F}_3[C_8 \times D_4]$.

4.4 Admissible generic symmetries

From now on, our objective is to use the results on ic-symmetries to get corresponding results on generic symmetries. In the present preparatory section, we establish the connections between these two notions of symmetry. Since many results of the last section depend on semisimplicity assumptions, we will throughout assume that the given group algebra $\Bbbk G$ is semisimple. Moreover, as we got best results only for the subclass of admissible ic-symmetries, we will introduce the corresponding notion of *admissible generic symmetries.*

Definition 4.4.1. Let $\Bbbk G$ be a semisimple group algebra, and let V be a finitely generated $\Bbbk G$-module. We call a generic symmetry $\pi \in \mathrm{Sym}(G, V)$ *admissible* if π fixes the ideals $(\mathrm{Ann}(v)_{\mathcal{I}})^{\perp}$ and $(\mathrm{Ann}(v)_{\mathcal{J}})^{\perp}$ for all ample points $v \in \mathrm{Amp}(V)$. The set of all admissible generic symmetries of V is denoted by $\mathrm{Sym}^{\mathrm{ad}}(G, V)$.

Note that all finitely generated modules over semisimple group algebras are semisimple, and so have ample points by Lemma 3.6.1. Moreover, the annihilators of all ample points of a semisimple module are isomorphic by Lemma 4.1.3. Thus, by Lemma 4.2.5, the question whether a generic symmetry is admissible can be answered by considering only one annihilator of an arbitrary ample point.

It is clear by definition that $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ is a subgroup of $\mathrm{Sym}(G, V)$ which only depends on the isomorphism type of V. We will show that the group $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ satisfies many properties which are similar to properties of $\mathrm{Sym}(G, V)$.

Lemma 4.4.2. *Let* $\Bbbk G$ *be a semisimple group algebra, and let* V *be a finitely generated* $\Bbbk G$*-module. If* $v \in \mathrm{Amp}(V)$ *is any ample point then* $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ *consists of admissible ic-symmetries of* $\mathrm{Ann}(v)$*. If* $\Bbbk$ *is of infinite order then the converse holds as well, that is, any admissible ic-symmetry of* $\mathrm{Ann}(v)$ *is contained in* $\mathrm{Sym}^{\mathrm{ad}}(G, V)$.

Proof. Let $\pi \in \mathrm{Sym}^{\mathrm{ad}}(G, V)$ be any admissible generic symmetry of V. Then π is an orbit symmetry of any ample point of V by Corollary 3.4.5, so by Lemma 4.1.1, π fixes all annihilators of all ample points of V. By Lemma 4.1.3 and Lemma 4.1.2, these annihilators range over all left ideals of $\Bbbk G$ isomorphic to $\mathrm{Ann}(v)$. So π is an ic-symmetry of $\mathrm{Ann}(v)$. By definition of admissible generic symmetries, π must in fact be an admissible ic-symmetry of $\mathrm{Ann}(v)$, proving the first claim.

Now let $\Bbbk$ be a field of infinite order. Then by Theorem 4.1.6, $\mathrm{Sym}(G, V)$ consists precisely of the ic-symmetries of $\mathrm{Ann}(v)$. Again by definition, we conclude that $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ consists precisely of the admissible ic-symmetries of $\mathrm{Ann}(v)$. □

The situation is special for left ideals $L \leq \Bbbk G$ since in that case, we have notions of admissible generic symmetries of L, as well as of admissible ic-symmetries of L. The following corollary shows how these notions are connected.

Corollary 4.4.3. *Let* $\Bbbk G$ *be a semisimple group algebra, and let* $L \leq \Bbbk G$ *be a left ideal. Then* $\mathrm{Sym}^{\mathrm{ad}}(G, L)$ *consists of admissible ic-symmetries of* L*. If* $\Bbbk$ *is of infinite order then the converse holds as well, that is, all admissible ic-symmetries of* L *are contained in* $\mathrm{Sym}^{\mathrm{ad}}(G, L)$.

Proof. Let $C \leq \Bbbk G$ be any complement of L in $\Bbbk G$, and let $1 = e + f$ be the unique decomposition of $1 \in G$ into idempotent generators $e \in L$ and $f \in C$. By Theorem 4.3.6, L and C have the same admissible ic-symmetries. Since we have $\mathrm{Ann}(e) = \Bbbk G(1-e) = C$, the claim follows by Lemma 4.4.2. □

We continue the discussion on tensor products before Lemma 4.1.5. Let $\mathbb{E}/\Bbbk$ be a field extension. We have already noticed that tensoring by a field $\mathbb{E}$ sends injective (surjective) morphisms $f\colon V \to W$ of $\Bbbk G$-modules to injective (surjective) morphisms $f^{\mathbb{E}}\colon V^{\mathbb{E}} \to W^{\mathbb{E}}$ of $\mathbb{E}G$-modules, where kernels are mapped to kernels. Moreover, we have a canonical isomorphism on external direct sums $(V \oplus W)^{\mathbb{E}} \to V^{\mathbb{E}} \oplus W^{\mathbb{E}}$ given by $e \otimes (v, w) \mapsto (e \otimes v, e \otimes w)$. As we already noticed, if $U \leq V$ is a submodule then the set inclusion $U \to V$ gives rise to a canonical embedding $U^{\mathbb{E}} \to V^{\mathbb{E}}$ (given by $e \otimes u \mapsto e \otimes u$ on the pure tensors). Therefore, $U^{\mathbb{E}}$ can safely be regarded as a submodule of $V^{\mathbb{E}}$. As in the proof of Lemma 4.1.4, we identify $(\Bbbk G)^{\mathbb{E}}$ with $\mathbb{E}G$ by means of the canonical isomorphism $e \otimes x \mapsto ex$. In particular, if $L \leq \Bbbk G$ is any left ideal then $L^{\mathbb{E}}$ will be regarded as a left ideal of $\mathbb{E}G$.

The following facts seem to be folklore but they are hard to find in literature. We sketch their proofs for convenience.

Lemma 4.4.4. *Let V be a $\Bbbk G$-module and let $\mathbb{E}/\Bbbk$ be a field extension. Then for all submodules $U, W \leq V$ we have $(U + W)^{\mathbb{E}} = U^{\mathbb{E}} + W^{\mathbb{E}}$ and $(U \cap W)^{\mathbb{E}} = U^{\mathbb{E}} \cap W^{\mathbb{E}}$ as submodules of $V^{\mathbb{E}}$. In particular, for any left ideal $L \leq \Bbbk G$ we have $(L_{\mathcal{I}})^{\mathbb{E}} = (L^{\mathbb{E}})_{\mathcal{I}}$ and $(L_{\mathcal{J}})^{\mathbb{E}} = (L^{\mathbb{E}})_{\mathcal{J}}$ as ideals of $\mathbb{E}G$.*

Proof. The first assertion is straightforward to show as both $(U + W)^{\mathbb{E}}$ and $U^{\mathbb{E}} + W^{\mathbb{E}}$ are generated as $\Bbbk$-vector spaces by the pure tensors of the form $e \otimes u$ and $e \otimes w$ for $e \in E$, $u \in U$, $w \in W$.

Concerning the second assertion, is is easy to see that we have at least an inclusion $(U \cap W)^{\mathbb{E}} \subseteq U^{\mathbb{E}} \cap W^{\mathbb{E}}$ as submodules of $V^{\mathbb{E}}$. Let $U \oplus W$ be the external direct sum of U and W. We consider the morphisms $\delta\colon U \cap W \to U \oplus W$, $x \mapsto (x, x)$ and $\mu\colon U \oplus W \to V$, $(u, w) \mapsto u - w$. Then δ is a kernel of μ, whence $\delta^{\mathbb{E}}$ is a kernel of $\mu^{\mathbb{E}}$. We get a commutative diagram

$$\begin{array}{ccccc}
(U \cap W)^{\mathbb{E}} & \xrightarrow{\delta^{\mathbb{E}}} & (U \oplus W)^{\mathbb{E}} & \xrightarrow{\mu^{\mathbb{E}}} & V^{\mathbb{E}} \\
\downarrow{\scriptstyle i} & & \downarrow{\scriptstyle c} & \nearrow{\scriptstyle \mu'} & \\
U^{\mathbb{E}} \cap W^{\mathbb{E}} & \xrightarrow{\delta'} & U^{\mathbb{E}} \oplus W^{\mathbb{E}} & &
\end{array}$$

where i is the set inclusion, c is the canonical isomorphism, and δ' and μ' are defined analogously to δ and μ (in particular, δ' is a kernel of μ'). Now a simple diagram chasing argument shows that i must be an isomorphism.

The remaining assertion on the ideal constituent and the ideal closure of some left ideal $L \leq \Bbbk G$ now follows by Lemma 4.2.5 and by the simple fact that $(Lg)^{\mathbb{E}} = (L^{\mathbb{E}})g$ holds for all $g \in G$. □

Proposition 4.4.5. *Let* $\Bbbk G$ *be a semisimple group algebra, let* $\mathbb{E}/\Bbbk$ *be a field extension, and let* V *be a finitely generated* $\Bbbk G$*-module. Then* $\operatorname{Sym}^{\mathrm{ad}}(G,V) = \operatorname{Sym}^{\mathrm{ad}}(G,V^{\mathbb{E}})$.

Proof. By Proposition 3.4.2, we have $\operatorname{Sym}(G,V) = \operatorname{Sym}(G,V^{\mathbb{E}})$. So it remains to show that a generic symmetry π is admissible for V if and only if π is admissible for $V^{\mathbb{E}}$.

By Lemma 3.6.1, there is an ample point $v \in \operatorname{Amp}(V)$, and by Lemma 4.1.3, the annihilators of all ample points of V are isomorphic to $L = \operatorname{Ann}(v)$. So by Lemma 4.2.5, they all have the same ideal constituent $L_{\mathcal{I}}$ and the same ideal closure $L_{\mathcal{J}}$. By Lemma 3.4.4, $1 \otimes v$ is an ample point of $V^{\mathbb{E}}$, and by the same reasoning as before, the annihilators of all ample points of $V^{\mathbb{E}}$ are isomorphic to $L' = \operatorname{Ann}(1 \otimes v)$. Furthermore, they all have the same ideal constituent $L'_{\mathcal{I}}$ and the same ideal closure $L'_{\mathcal{J}}$. So it remains to show that π fixes both $(L_{\mathcal{I}})^{\perp}$ and $(L_{\mathcal{J}})^{\perp}$ if and only if π fixes both $(L'_{\mathcal{I}})^{\perp}$ and $(L'_{\mathcal{J}})^{\perp}$.

By Lemma 4.1.5, we have a canonical isomorphism $L^{\mathbb{E}} \to L'$ of $\mathbb{E}G$-modules. By Lemma 4.4.4, we get a canonical isomorphism $(L_{\mathcal{I}})^{\mathbb{E}} \to L'_{\mathcal{I}}$. Therefore, if $e \in \Bbbk G$ is the central idempotent generator of $L_{\mathcal{I}}$ given by Lemma 4.2.7 then e (regarded as an element of $\mathbb{E}G$) also generates the two-sided ideal $L'_{\mathcal{I}}$ of $\mathbb{E}G$. Now Lemma 4.3.7 shows that π fixes $(L_{\mathcal{I}})^{\perp}$ if and only if π fixes $(L'_{\mathcal{I}})^{\perp}$ (since both statements are equivalent to $\pi(ge) = \pi(g)e$ for all $g \in G$). Exactly the same reasoning holds verbatim for the ideal closures of L and L'. □

By Proposition 4.4.5, many questions on admissible generic symmetries over arbitrary fields can be reduced to the case of infinite fields. The proof of the following statement relies on a simple application of that reduction.

Proposition 4.4.6. *Let* $\Bbbk G$ *be a semisimple group algebra, and let* V *be a finitely generated* $\Bbbk G$*-module. Then we have*

$$G \cdot \operatorname{Iv}(G,V) \leq \operatorname{Sym}^{\mathrm{ad}}(G,V).$$

Moreover, a generic symmetry $\pi \in \operatorname{Sym}(G,V)$ *is admissible if it suffices one of the hypotheses of Lemma 4.3.2.*

Proof. By Proposition 3.4.2 and Proposition 4.4.5, we may assume without loss of generality that $\Bbbk$ is of infinite order. Let $v \in \operatorname{Amp}(V)$ be arbitrary, and let $L = \operatorname{Ann}(v)$. Then by Theorem 4.1.6, $\operatorname{Sym}(G,V)$ consists precisely of the ic-symmetries of L, while by Lemma 4.4.2, $\operatorname{Sym}^{\mathrm{ad}}(G,V)$ consists precisely of the admissible ic-symmetries of L. Now almost all assertions follow by Lemma 4.3.2. It only remains to show that any irrelevant generic symmetry $\pi \in \operatorname{Iv}(G,V)$ fixes both $(L_{\mathcal{I}})^{\perp}$ and $(L_{\mathcal{J}})^{\perp}$.

By definition, π fixes all cosets of $K = \operatorname{Ker}(V)$ in G. We consider the left ideal $I \leq \Bbbk G$ generated by all elements of the form $1 - g$ for $g \in K$. Then we have $I \subseteq L$ by definition, and since K is a normal subgroup of G, it is easy to see that I is actually a two-sided ideal, whence $I \subseteq L_{\mathcal{I}}$. So if $f \in (L_{\mathcal{I}})^{\perp}$ is the central idempotent generator given by Lemma 4.2.7 then we have $I \cdot f = 0$, and hence $gf = f$ for all $g \in K$. So we see that the normal subgroup $K \leq G$ acts trivially on the ideal $(L_{\mathcal{I}})^{\perp}$. This shows that the coefficients of all elements of $(L_{\mathcal{I}})^{\perp}$ (with respect to the standard basis G of $\Bbbk G$)

are constant on the cosets of K. By the assumption on π, it follows that $\pi(x) = x$ for all $x \in (L_{\mathcal{I}})^{\perp}$. Since $(L_{\mathcal{J}})^{\perp} \subseteq (L_{\mathcal{I}})^{\perp}$, we see that π fixes both $(L_{\mathcal{I}})^{\perp}$ and $(L_{\mathcal{J}})^{\perp}$. ☐

Most importantly, Proposition 4.4.6 shows that we have an equation

$$\mathrm{Sym}^{\mathrm{ad}}(G, V) = \mathrm{Sym}(G, V)$$

provided that the ground field $\Bbbk$ has characteristic zero or that $\Bbbk$ has a characteristic exceeding the order of G. The following lemma is the analog to Lemma 3.2.8 for admissible generic symmetries.

Lemma 4.4.7. *Let $\Bbbk G$ be a semisimple group algebra, and let V be a finitely generated $\Bbbk G$-module decomposing into a direct sum $V = V_1 \oplus \cdots \oplus V_n$ of submodules. Then we have*

$$\mathrm{Sym}^{\mathrm{ad}}(G, V_1) \cap \cdots \cap \mathrm{Sym}^{\mathrm{ad}}(G, V_n) \subseteq \mathrm{Sym}^{\mathrm{ad}}(G, V).$$

Proof. By Proposition 4.4.5, we may assume without loss of generality that $\Bbbk$ is of infinite order. Since the set $\mathrm{Amp}(V_1) + \cdots + \mathrm{Amp}(V_n)$ is open in V by Lemma 3.3.2, it has a nonzero intersection with $\mathrm{Amp}(V)$ by Lemma 2.1.2. Therefore, we find an ample point $v = v_1 + \cdots + v_n \in \mathrm{Amp}(V)$ such that $v_i \in \mathrm{Amp}(V_i)$ for all i. One easily checks that $\mathrm{Ann}(v) = \mathrm{Ann}(v_1) \cap \cdots \cap \mathrm{Ann}(v_n)$. Since (by Lemma 4.4.2) $\mathrm{Sym}^{\mathrm{ad}}(G, V_i)$ consists precisely of the admissible ic-symmetries of $\mathrm{Ann}(v_i)$ for all i, and since $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ consists of the admissible ic-symmetries of $\mathrm{Ann}(v)$, the claim follows by Theorem 4.3.6 which shows that $\mathcal{L}^{\mathrm{ad}}_{\Bbbk G}(\pi)$ is closed under taking intersections for all $\pi \in \mathrm{Sym}(G)$. ☐

4.5 Ideal constituents and a generalized Isaacs' theorem

From now on, we restrict our attention to cyclic modules. We have already observed in the context of left ideals that the investigation of ic-symmetries naturally leads to certain two-sided ideals which have to be treated separately. In the present section, we introduce the analogous notion of the *ideal constituent* $V_{\mathcal{I}} \leq V$ of a cyclic module V which turns out to be an important invariant for the recognition of (admissible) generic symmetries. We show that in the extremal cases $V_{\mathcal{I}} = 0$ and $V_{\mathcal{I}} = V$, the group of admissible generic symmetries of V is easy to compute.

Lemma 4.5.1. *Let $\Bbbk G$ be a semisimple group algebra, and let V be a cyclic $\Bbbk G$-module. Then there is a unique submodule $I \leq V$ maximal subject to the following equivalent conditions:*

(1) I is isomorphic to a two-sided ideal of $\Bbbk G$,

(2) $\mathrm{GL}_{\Bbbk G}(I)$ acts transitively on $\mathrm{Amp}(I)$.

This uniquely determined submodule I also has a unique complement in V.

Proof. Since V is cyclic, and since $\Bbbk G$ is semisimple, V is isomorphic to a left ideal $L \leq \Bbbk G$. By Lemma 4.1.2, a submodule of L is isomorphic to a two-sided ideal only if it is already a two-sided ideal. Consequently, the unique submodule of L satisfying (1) is just the ideal constituent $L_{\mathcal{I}}$, and by Lemma 4.3.5, there is a unique complement $L_{\mathcal{N}}$ of $L_{\mathcal{I}}$ in L. Since $L \cong V$, the same holds for V.

It remains to show the equivalence of (1) and (2). By Lemma 4.2.7, any two-sided ideal $J \leq \Bbbk G$ is generated by a central idempotent $e \in \Bbbk G$, and then $\operatorname{Ann}(e) = \Bbbk G(1-e)$ is also a two-sided ideal. So by Lemma 4.1.4, any $\Bbbk G$-module satisfying (1) also satisfies (2). Conversely, if I is a module satisfying (2) then by the same arguments, $\operatorname{Ann}(w)$ is a two-sided ideal for some $w \in \operatorname{Amp}(I)$ and $I \cong \Bbbk G/\operatorname{Ann}(w)$ is isomorphic to the unique complement of a two-sided ideal, which must be two-sided again. □

Definition 4.5.2. Let $\Bbbk G$ be a semisimple group algebra, and let V be a cyclic $\Bbbk G$-module. The unique maximal submodule of V satisfying the conditions of Lemma 4.5.1 is denoted by $V_{\mathcal{I}}$. We call it the *ideal constituent* of V. The unique complement $V_{\mathcal{N}}$ of $V_{\mathcal{I}}$ in V is called the *non-ideal constituent* of V.

Note that the notion of ideal and non-ideal constituents of modules is a generalization of the previously introduced notion in the case of left ideals. That is, if the module V under consideration is actually a left ideal then in any case $V_{\mathcal{I}}$ is simply the largest two-sided ideal contained in V.

Proposition 4.5.3. *Let $\Bbbk G$ be a semisimple group algebra, and let V be a cyclic $\Bbbk G$-module with $V_{\mathcal{I}} = V$. Then we have*

$$\operatorname{Sym}^{\mathrm{ad}}(G,V) = \{\pi \in \operatorname{Sym}(G) : \chi(\pi(g)^{-1}\pi(h)) = \chi(g^{-1}h) \text{ for all } g,h \in G\},$$

where χ is the character of V.

Proof. Without loss of generality, we may assume that $V = I$ is a two-sided ideal in $\Bbbk G$. As in the proof of Lemma 4.5.1, we see that I is generated by a central idempotent $e \in \Bbbk G$, and $\operatorname{Ann}(e) = \Bbbk G(1-e)$ is a two-sided ideal. By Theorem 4.1.7, e is a generic point of I, and Lemma 4.1.1 implies that the admissible generic symmetries of I are precisely those permutations of $\operatorname{Sym}(G)$ fixing both $\operatorname{Ann}(e)$ and its unique complement I. The claim now follows by Proposition 4.3.8. □

The next result is particularly important, as it suggests a general procedure for constructing (weakly) generically closed modules. Recall that Isaacs' theorem (Proposition 3.8.8) states that any absolutely simple $\Bbbk G$-module V is weakly generically closed. (As before, a $\Bbbk G$-module V is called absolutely simple if the scalar extensions $V^{\mathbb{E}}$ are simple $\mathbb{E}G$-modules for all field extensions $\mathbb{E}/\Bbbk$, or equivalently, if $\operatorname{End}_{\Bbbk G}(V) = \Bbbk$.) Since absolutely simple modules are simple, we have either $V_{\mathcal{I}} = 0$ or $V_{\mathcal{I}} = V$, and it is easy to show that the latter case is only possible if V is one dimensional over $\Bbbk$. Indeed, if $I \leq \Bbbk G$ is an absolutely simple two-sided ideal then the right multiplication by any element $g \in G$ is (as a $\Bbbk G$-linear operator on I) equal to the multiplication by some element $\lambda_g \in \Bbbk$. So if $e \in I$ is the central idempotent generator of I given by

Lemma 4.2.7 then we have $ge = eg = \lambda_g e$ for all $g \in G$. In particular, $I = \Bbbk Ge = \Bbbk e$ is one dimensional. For that reason, the following theorem can be seen as a generalization of Isaacs' result.

Theorem 4.5.4. *Let* $\Bbbk G$ *be a semisimple group algebra, and let* V *be a cyclic* $\Bbbk G$*-module with* $V_{\mathcal{I}} = 0$*. Then we have*

$$\mathrm{Sym}(G, V) = \mathrm{Sym}^{\mathrm{ad}}(G, V) = G \cdot \mathrm{Iv}(G, V).$$

In particular, V *is weakly generically closed.*

Proof. By Proposition 4.4.6, the inclusions $G \cdot \mathrm{Iv}(G, V) \subseteq \mathrm{Sym}^{\mathrm{ad}}(G, V) \subseteq \mathrm{Sym}(G, V)$ do always hold. So it remains to show that any generic symmetry $\pi \in \mathrm{Sym}(G, V)$ with $\pi(1) = 1$ is contained in $\mathrm{Iv}(G, V)$.

By Proposition 3.4.2 and Lemma 4.4.4, we may assume without loss of generality that $\Bbbk$ is a field of infinite order and that V decomposes into a direct sum

$$V = S_1 \oplus \cdots \oplus S_n$$

of absolutely simple $\Bbbk G$-modules S_i. Let $L \leq \Bbbk G$ be the annihilator of some generator $v \in \mathrm{Amp}(V)$. Then by Theorem 4.1.6, π is an ic-symmetry of L.

We claim that $L_{\mathcal{J}} = \Bbbk G$. By considering the isomorphisms $V \cong \Bbbk G/L$ and $\Bbbk G/L_{\mathcal{J}} \cong (L_{\mathcal{J}})^{\perp}$ as well as the canonical epimorphism $\Bbbk G/L \to \Bbbk G/L_{\mathcal{J}}$, we see that $(L_{\mathcal{J}})^{\perp}$ is isomorphic to a quotient of V. Since V is semisimple, the two-sided ideal $(L_{\mathcal{J}})^{\perp}$ is also isomorphic to a submodule of V. Since $V_{\mathcal{I}} = 0$, we conclude $(L_{\mathcal{J}})^{\perp} = 0$, whence $L_{\mathcal{J}} = \Bbbk G$. So by Theorem 4.2.9, it follows that π is an ic-symmetry of all left ideals of $\Bbbk G$ above L.

We consider the decomposition $v = s_1 + \cdots + s_n$ of the generator into unique elements $s_i \in S_i$. Then each s_i is a generator of S_i, and we have $L \leq \mathrm{Ann}(s_i)$ for all i. So π is an ic-symmetry of all these annihilators, and by applying Theorem 4.1.6 again, we get $\pi \in \mathrm{Sym}(G, S_i)$ for all i. By Isaacs' theorem (Proposition 3.8.8), we get $\pi \in \mathrm{Iv}(G, S_i)$ for all i, and by Lemma 3.2.8, we conclude $\pi \in \mathrm{Iv}(G, V)$. □

Theorem 4.5.4 suggests a natural approach for constructing a (weakly) generically closed $\Bbbk G$-module for any finite group G. We may always define a $\Bbbk G$-module V as the direct sum of all simple $\Bbbk G$-modules S (one of each isomorphism type) with $S_{\mathcal{I}} = 0$. Then V has also a zero ideal constituent (so V is weakly generically closed), and actually V has the smallest kernel in G among all cyclic $\Bbbk G$-modules with zero ideal constituent. So V can be expected to be a good candidate for a generically closed module. We will take that approach to construct generically closed $\mathbb{R}G$-modules for a great variety of groups in Chapter 6, thereby proving that these groups are isomorphic to affine symmetry groups of orbit polytopes. In fact, we will classify the exceptional finite groups for which that approach fails (Theorem 6.2.3).

4.6 Structure theorems

At this point, we know how to compute the group of admissible generic symmetries of cyclic $\Bbbk G$-modules in the extremal cases where V has zero ideal constituent, and where V is its own ideal constituent. This is actually all we need to know. In this section, we show that the admissible generic symmetries of any cyclic module V are precisely the common admissible generic symmetries of the modules $V_{\mathcal{I}}$ and $V_{\mathcal{N}}$ (Proposition 4.6.1) which in turn leads to a formula for $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ only depending on the character of $V_{\mathcal{I}}$ and on the kernel of $V_{\mathcal{N}}$ in G (Theorem 4.6.2). Moreover, we obtain new insights into the action of $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ on the modules $\widehat{V}_w$ for $w \in \mathrm{Amp}(V)$. Recall that we already know by Proposition 3.8.2 that all modules $\widehat{V}_w$ are isomorphic over $\Bbbk\,\mathrm{Sym}(G, V)$ provided that $\Bbbk$ has characteristic zero, or that the characteristic of $\Bbbk$ exceeds the order of G. This result is sharpened in Theorem 4.6.4 which shows that these modules are always isomorphic (to a submodule of $\Bbbk G$) when regarded as $\Bbbk\mathrm{Sym}^{\mathrm{ad}}(G, V)$-modules.

Proposition 4.6.1. *Let $\Bbbk G$ be a semisimple group algebra, let V be a cyclic $\Bbbk G$-module, and let W be any $\Bbbk G$-module such that $V \oplus W \cong \Bbbk G$. Then we have*

$$\mathrm{Sym}^{\mathrm{ad}}(G, W) = \mathrm{Sym}^{\mathrm{ad}}(G, V) = \mathrm{Sym}^{\mathrm{ad}}(G, V_{\mathcal{I}}) \cap \mathrm{Sym}^{\mathrm{ad}}(G, V_{\mathcal{N}}).$$

Proof. Since V and W are cyclic modules over a semisimple group algebra $\Bbbk G$, and since the assertions do only depend on the isomorphism type of V and W, we may assume without loss of generality that both V and W are left ideals of $\Bbbk G$. Since we know by Lemma 4.4.4 that $(V_{\mathcal{I}})^{\mathbb{E}} = (V^{\mathbb{E}})_{\mathcal{I}}$ holds for all field extensions $\mathbb{E}/\Bbbk$, and since ideal constituents have unique complements by Lemma 4.3.5, we also have $(V_{\mathcal{N}})^{\mathbb{E}} = (V^{\mathbb{E}})_{\mathcal{N}}$. So by Proposition 4.4.5, we may further assume without loss of generality that $\Bbbk$ is a field of infinite order. Now Corollary 4.4.3 applies, that is, admissible generic symmetries are characterized as admissible ic-symmetries in the current setting. All assertions follow at once by Theorem 4.3.6. □

Putting everything together, we are finally able to derive a formula for $\mathrm{Sym}^{\mathrm{ad}}(G, V)$ which only depends on the character of $V_{\mathcal{I}}$ and on the kernel of $V_{\mathcal{N}}$. This result leads to the important observation that in characteristic zero, the generic symmetries of modules are completely understood in terms of characters. The study of generic symmetries of characters will be our objective in the next chapter.

Theorem 4.6.2. *Let $\Bbbk G$ be a semisimple group algebra, and let V be a cyclic $\Bbbk G$-module. Then we have*

$$\mathrm{Sym}^{\mathrm{ad}}(G, V) = \left\{ \pi \in \mathrm{Sym}(G) : \begin{array}{rcll} \chi(\pi(g)^{-1}\pi(h)) & = & \chi(g^{-1}h) & \text{for all } g, h \in G \\ \pi(gK) & = & \pi(1)gK & \text{for all } g \in G \end{array} \right\},$$

where χ is the character of $V_{\mathcal{I}}$, and where K is the kernel of $V_{\mathcal{N}}$ in G.

Proof. This is an immediate consequence of Proposition 4.6.1, Proposition 4.5.3, and Theorem 4.5.4. □

We close this chapter with a structural result on the $\Bbbk\mathrm{Sym}^{\mathrm{ad}}(G, V)$-modules $\widehat{V}_w$ given by the generators $w \in \mathrm{Amp}(V)$. More precisely, we show that independently of the choice of the generator w, these modules have a unique isomorphism type, and we determine a family of submodules of $\widehat{V}_w$ which come up naturally. For that purpose, we need a strengthening of Maschke's Theorem, which is probably well known. However, since it is a nice application of the geometric methods developed in Chapter 3, we give a proof here.

Lemma 4.6.3. *Let $\Bbbk$ be a field of infinite order, let $\Bbbk G$ be a semisimple group algebra, and let $L_1, \dots, L_k \leq \Bbbk G$ be isomorphic left ideals. Then there is a left ideal $C \leq \Bbbk G$ which is a complement in $\Bbbk G$ for every L_i.*

Proof. We claim that there is a cyclic $\Bbbk G$-module V such that the annihilators of all generators of V are isomorphic to $\Bbbk G/L_i$ for all i. Note that by Lemma 4.1.2, the annihilators of all generators of a cyclic module are isomorphic. Moreover, since the left ideals L_i are isomorphic by assumption, the quotients $\Bbbk G/L_i$ are isomorphic as well (by semisimplicity). For these reasons, $V = L_1$ has the desired properties.

For any i, we consider the set

$$X_i = \{x \in \mathrm{Amp}(V) : \mathrm{Ann}(x) \cap L_i = 0\}.$$

We claim that each X_i is nonempty and open in V. Assuming this assertion to be true for a moment, these sets X_i have a nonempty intersection by Lemma 2.1.2, so there is some element $x \in \mathrm{Amp}(V)$ such that $\mathrm{Ann}(x) \cap L_i = 0$ for all i. By definition of V, we also have $\mathrm{Ann}(x) \cong \Bbbk G/L_i$, and hence

$$\dim(\Bbbk G) = \dim(L_i) + \dim(\mathrm{Ann}(x))$$

for all i. Consequently, $\mathrm{Ann}(x)$ is a common complement in $\Bbbk G$ for every L_i.

It remains to show that each X_i is nonempty and open in V. Let $1 \leq i \leq k$ be arbitrary. Since $\Bbbk G$ is semisimple, there exists a complement $C \leq \Bbbk G$ of L_i. By definition of V and by Lemma 4.1.2, C is the annihilator of some generator of V. So X_i is nonempty. Let $x \in V$ be arbitrary. Since $\dim(L_i) = \dim(V)$, x is an element of X_i if and only if the right multiplication by x is an isomorphism $L_i \to V$ of vector spaces. So if $l_1, \dots, l_d \in L_i$ is any $\Bbbk$-basis of L_i, and if $\det\colon V^d \to \Bbbk$ is any nonzero alternating form, we see that $X_i = \{x \in V : \det(l_1 x, \dots, l_d x) \neq 0\}$ is open in V. □

Although the following result is valid for arbitrary fields, it relies on results which are valid only for infinite fields. To set up a reduction argument to infinite fields as before, we need the Noether-Deuring theorem [22, Theorem 19.25]. Let V, W be finitely generated $\Bbbk G$-modules, and let $\mathbb{E}/\Bbbk$ be any field extension. If V and W are isomorphic, it is clear that any isomorphism $f\colon V \to W$ extends to an isomorphism $f^{\mathbb{E}}\colon V^{\mathbb{E}} \to W^{\mathbb{E}}$ of $\mathbb{E}G$-modules, whence $V^{\mathbb{E}}$ is isomorphic to $W^{\mathbb{E}}$. The Noether-Deuring theorem states that the converse holds as well. That is, if $V^{\mathbb{E}}$ and $W^{\mathbb{E}}$ are isomorphic $\mathbb{E}G$-modules then V and W must be already isomorphic as $\Bbbk G$-modules (although there is no natural choice for an isomorphism is that situation). We also note that a permutation

$\pi \in \mathrm{Sym}(G)$ fixes a left ideal $L \leq \Bbbk G$ if and only if π fixes $L^{\mathbb{E}}$ regarded as a left ideal of $\mathbb{E}G$. Furthermore, if V is a cyclic $\Bbbk G$-module with generator $w \in \mathrm{Amp}(V)$ then we have an equality (not merely an isomorphism) $(\widehat{V}_w)^{\mathbb{E}} = \widehat{(V^{\mathbb{E}})}_{1\otimes w}$ of $\mathbb{E}\,\mathrm{Sym}(G,w)$-modules by definition (cf. Section 3.8).

Theorem 4.6.4. *Let $\Bbbk G$ be a semisimple group algebra, and let V be a cyclic $\Bbbk G$-module with corresponding group $\widehat{G} = \mathrm{Sym}^{\mathrm{ad}}(G,V)$ of admissible generic symmetries. The following statements hold independently of the choice of a generator $w \in \mathrm{Amp}(V)$ and of the choice of a left ideal $L \leq \Bbbk G$ isomorphic to V.*

(1) $V_{\mathcal{I}}$ is a $\Bbbk\widehat{G}$-submodule of $\widehat{V}_w$.

(2) Any $\Bbbk G$-submodule of $V_{\mathcal{N}}$ is a $\Bbbk\widehat{G}$-submodule of $\widehat{V}_w$.

(3) L is a $\Bbbk\widehat{G}$-submodule of $\Bbbk G$, and we have $\widehat{V}_w \cong L$ as $\Bbbk\widehat{G}$-modules.

Proof. We consider the direct sum decomposition $V = V_{\mathcal{I}} \oplus V_{\mathcal{N}}$ as $\Bbbk G$-modules. Let $w = x + y$ be the unique decomposition of the generator w into generators $x \in V_{\mathcal{I}}$ and $y \in V_{\mathcal{I}}$. Since we have $\widehat{G} \subseteq \mathrm{Sym}^{\mathrm{ad}}(G,V_{\mathcal{I}}) \cap \mathrm{Sym}^{\mathrm{ad}}(G,V_{\mathcal{N}})$ by Proposition 4.6.1, there are representations $D_x\colon \widehat{G} \to \mathrm{GL}(V_{\mathcal{I}})$ and $D_y\colon \widehat{G} \to \mathrm{GL}(V_{\mathcal{N}})$ such that

$$D_x(\pi)gx = \pi(g)x \quad \text{and} \quad D_y(\pi)gy = \pi(g)y \quad \text{for all } g \in G, \pi \in \widehat{G}.$$

It is easy to check that $D_x \oplus D_y$ is exactly the representation $D_w\colon \widehat{G} \to \mathrm{GL}(V)$, which shows that $V_{\mathcal{I}}$ and $V_{\mathcal{N}}$ are $\Bbbk\widehat{G}$-submodules of $\widehat{V}_w$. Now since $\mathrm{Sym}^{\mathrm{ad}}(G,V_{\mathcal{N}}) = G \cdot \mathrm{Iv}(G,V_{\mathcal{N}})$ by Theorem 4.5.4, we have

$$D_w(\pi)z = D_y(\pi)z = \pi(1)z \quad \text{for all } \pi \in \widehat{G}, z \in V_{\mathcal{N}}.$$

This shows that all $\Bbbk G$-submodules of $V_{\mathcal{N}}$ are $\Bbbk\widehat{G}$-submodules. So we have proven (1) and (2).

To prove (3), we may assume (by the preceding discussion) without loss of generality that the field $\Bbbk$ has infinite order. Let $L' \leq \Bbbk G$ be any complement of $\mathrm{Ann}(w)$ in $\Bbbk G$ as $\Bbbk G$-modules. By Lemma 4.4.2 and Corollary 4.4.3, all elements of $\widehat{G}$ are admissible ic-symmetries of L, L' and $\mathrm{Ann}(w)$. In particular, all these left ideals are $\Bbbk\widehat{G}$-submodules of $\Bbbk G$. By Theorem 4.1.6, we get $\widehat{V}_w \cong \Bbbk G/\mathrm{Ann}(w) \cong L'$ as $\Bbbk\widehat{G}$-modules. It remains to show that the isomorphic left ideals L and L' are also isomorphic as $\Bbbk\widehat{G}$-modules. This is a consequence of Lemma 4.6.3. By that lemma, there is a left ideal $C \leq \Bbbk G$ which is a complement of both L and L' in $\Bbbk G$. Since C is $\Bbbk G$-isomorphic to $\mathrm{Ann}(w)$, C is a $\Bbbk\widehat{G}$-submodule of $\Bbbk G$. It follows $L \cong \Bbbk G/C \cong L'$ as $\Bbbk\widehat{G}$-modules. □

Theorem 4.6.4 shows in particular that for any semisimple group algebra $\Bbbk G$ and for any cyclic $\Bbbk G$-module V, the modules $\widehat{V}_w$ given by ample points $w \in \mathrm{Amp}(V)$ belong to a single isomorphism class with respect to the group algebra $\Bbbk\mathrm{Sym}^{\mathrm{ad}}(G,V)$. This result is a refinement of Proposition 3.8.2.

5 The character theoretic view on generic symmetries

From now on, we restrict to fields $\Bbbk$ of characteristic zero. In that case, all group algebras $\Bbbk G$ are semisimple, and all $\Bbbk G$-modules are uniquely determined by their characters. Moreover, generic symmetries are automatically admissible in that case (Proposition 4.4.6), so the formula in Theorem 4.6.2 characterizes all generic symmetries of a given module. The objective of this chapter is to introduce a theory of generic symmetries which only uses the character theoretic language, without referring to modules or representations.

To begin with, note that since $\Bbbk G$-modules are uniquely determined by their characters up to isomorphism, we can safely define the *generic symmetry group* $\mathrm{Sym}(G, \chi)$ of a character $\chi\colon G \to \Bbbk$ as the generic symmetry group of V for an arbitrary $\Bbbk G$-module V affording χ. For cyclic modules V, we have seen that the generic symmetry group acts on V in various ways (any generator gives rise to a corresponding action of $\mathrm{Sym}(G, V)$ on V), all of which leading to the same character of $\mathrm{Sym}(G, V)$ (Lemma 3.8.1). Accordingly, if χ is the character of a cyclic $\Bbbk G$-module V, we can unambiguously define $\widehat{\chi}$ to be the character of $\mathrm{Sym}(G, \chi)$ afforded by $\widehat{V}_w$ for some generator $w \in \mathrm{Amp}(V)$. Since G can be regarded as a subgroup of $\mathrm{Sym}(G, \chi)$, the character $\widehat{\chi}$ can be regarded as an extension of χ.

Analogously to the case of modules, we introduce the *ideal constituent* $\chi_{\mathcal{I}}$ and the *non-ideal constituent* $\chi_{\mathcal{N}}$ of a character χ, which are specific characters of G uniquely determined by χ. The generic symmetry group $\mathrm{Sym}(G, \chi)$ is characterized by a formula only depending on $\chi_{\mathcal{I}}$ and on (the kernel of) $\chi_{\mathcal{N}}$ (Theorem 5.1.10). Motivated by that result, we point out some possibilities for determining these constituents of a given character. In general, there are formulas for $\chi_{\mathcal{I}}$ and $\chi_{\mathcal{N}}$ depending on χ and on the character table of G. In Section 5.3, we develop more involved methods for finding $\chi_{\mathcal{I}}$ and $\chi_{\mathcal{N}}$ (without knowledge of the full character table of G) in the case where χ is an induced character.

In any case, the extended character $\widehat{\chi}$ is easily computed by a formula only depending on χ (Theorem 5.1.15). We obtain structural information on the constituents of $\widehat{\chi}$ in terms of certain constituents of χ (Theorem 5.1.12). We will illustrate how the knowledge of the extended character can help to get results on the corresponding generic symmetry group. For example, we show that $\mathrm{Sym}(G, \chi)$ is doubly transitive on G only if $\mathrm{Sym}(G, \chi) = \mathrm{Sym}(G)$ is the full symmetric group (Corollary 5.1.13).

In Section 5.2, we give suggestions on how the considerations of generic symmetries could be used in character theory of groups. We give a sufficient criterion ensuring that a character of a subgroup $H \leq G$ can be extended (by an explicit formula) to a character of G provided that H has a complement in G (Proposition 5.2.1).

The results of Section 5.1 have already appeared in [10], while the results of Section 5.3 are extracted from [19]. The considerations of Section 5.2 have not been published so far. In this chapter, we use many standard techniques from representation theory of finite groups. For a comprehensive view on representation theory, we refer to the textbooks [17] and [4].

5.1 Generic symmetries of characters

In the following, we essentially reformulate the results of Chapter 4 into the character theoretic language. To begin with, we recall some basic facts of the character theory of finite groups which can be found in most textbooks. For a comprehensive view, we refer to [17].

The character of a finitely generated $\Bbbk G$-module V is defined as the function $\Bbbk G \to \Bbbk$ sending each element $x \in \Bbbk G$ to its trace as a linear operator on V. Since the trace map is $\Bbbk$-linear and since G is a $\Bbbk$-basis of $\Bbbk G$, characters are usually regarded as functions $G \to \Bbbk$. If $\Bbbk$ has characteristic zero then $\Bbbk G$ is semisimple by Maschke's theorem. So all $\Bbbk G$-modules decompose into a direct sum of simple modules. Since the characters of simple modules are always linearly independent as functions $G \to \Bbbk$ (see [17, Corollary 9.22]), all finitely generated $\Bbbk G$-modules are uniquely determined by their character up to isomorphism. Moreover, characters are not affected by scalar extensions. That is, if V is any finitely generated $\Bbbk G$-module with character χ and if $\mathbb{E}/\Bbbk$ is any field extension then the character of $V^{\mathbb{E}}$ coincides with χ on the elements of G.

As already mentioned, we want to restrict to fields of characteristic zero, but for the greatest convenience, we will actually consider only the field $\mathbb{C}$ of complex numbers. There is no loss of generality in doing so, since all $\Bbbk G$-modules in characteristic zero arise as $\mathbb{C}G$-modules in a certain sense. Indeed, if V is any $\Bbbk G$-module over a field $\Bbbk$ of characteristic zero then we may choose a common field extension $\mathbb{E}$ of $\Bbbk$ and $\mathbb{C}$ (any quotient of the $\mathbb{Q}$-algebra $\Bbbk \otimes_{\mathbb{Q}} \mathbb{C}$ by a maximal ideal serves as an example). Since $\mathbb{E}G \cong (\mathbb{C}G)^{\mathbb{E}}$ and since all simple $\mathbb{C}G$-modules modules are absolutely simple, all $\mathbb{E}G$-modules are scalar extensions of $\mathbb{C}G$-modules (up to isomorphism). In particular, there must be a $\mathbb{C}G$-module W such that $V^{\mathbb{E}} \cong W^{\mathbb{E}}$. By Proposition 3.4.2, we conclude (in the case of finitely generated modules)

$$\operatorname{Sym}(G, V) = \operatorname{Sym}(G, V^{\mathbb{E}}) = \operatorname{Sym}(G, W^{\mathbb{E}}) = \operatorname{Sym}(G, W).$$

So all generic symmetry groups of $\Bbbk G$-modules in characteristic zero are actually generic symmetry groups of $\mathbb{C}G$-modules.

From now on, a character χ of a finite group G will always be understood as the character of some finitely generated $\mathbb{C}G$-module V (in particular, as a function $\chi\colon G \to \mathbb{C}$). The *degree* of χ is defined as the dimension of V over $\mathbb{C}$, or equivalently, as the value $\chi(1)$. We always have $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$, and the kernel of χ (which is the kernel of V by definition) is given by

$$\operatorname{Ker}(\chi) = \{g \in G : \chi(g) = \chi(1)\}.$$

A character ψ of G is called a *constituent* of χ if ψ is afforded by a submodule of V (or equivalently, if $\chi - \psi$ is also a character of G). An *irreducible* character is by definition the character of an (absolutely) simple $\mathbb{C}G$-module. The set of all irreducible characters of G is denoted by $\mathrm{Irr}(G)$. Characters of G are *class functions*, that is, they are constant on the conjugacy classes of G. The set of all class functions $G \to \mathbb{C}$ is a complex inner product space with respect to the (Hermitian) inner product

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

The first part of Schur's *orthogonality relations* states that $\mathrm{Irr}(G)$ is an orthonormal basis of the space of all class functions $G \to \mathbb{C}$. In particular, a class function $\alpha\colon G \to \mathbb{C}$ is a character if and only if $\langle \alpha, \chi \rangle$ is a nonnegative integer for all $\chi \in \mathrm{Irr}(G)$. We will see that the characters of left ideals and of two sided ideals of $\mathbb{C}G$ are characterized in a similar manner.

As an important example, we consider the character ρ of $\mathbb{C}G$ regarded as a module over itself which is usually called the *regular character* of G. As we have already seen in the proof of Lemma 4.2.7, the regular character is easily computed as

$$\rho(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases} \quad \text{for all } g \in G.$$

For each irreducible character $\psi \in \mathrm{Irr}(G)$ we have $\langle \rho, \psi \rangle = \psi(1)$, so the regular character decomposes (uniquely) as

$$\rho = \sum_{\psi \in \mathrm{Irr}(G)} \psi(1)\psi$$

into a linear combination of irreducible characters. Since left ideals are precisely the submodules of $\mathbb{C}G$, we see that a character χ of G is the character of a left ideal (or equivalently, of a cyclic module) if and only if χ is a constituent of ρ. This in turn is equivalent to $\langle \chi, \psi \rangle \leq \psi(1)$ for all $\psi \in \mathrm{Irr}(G)$. Moreover, since a left ideal is a two sided ideal if and only if it contains all isomorphic copies of its simple constituents, we see that χ is the character of a two sided ideal if and only if $\langle \chi, \psi \rangle \in \{0, \psi(1)\}$ for all $\psi \in \mathrm{Irr}(G)$.

While the latter notations and facts are completely standard, we also introduce the following non-standard terminology.

Definition 5.1.1. Let χ be a character of a finite group G. Then χ is called

(1) a *left ideal character* if χ is afforded by a left ideal (or equivalently, by a cyclic module) of $\mathbb{C}G$,

(2) an *ideal character* if χ is afforded by a two sided ideal of $\mathbb{C}G$,

(3) a *non-ideal character* if χ is afforded by a left ideal of $\mathbb{C}G$ with trivial ideal constituent.

Moreover, we define the characters

$$\chi_{\mathcal{L}} = \sum_{\psi \in \mathrm{Irr}(G)} \min(\langle \chi, \psi \rangle, \psi(1))\psi, \quad \chi_{\mathcal{I}} = \sum_{\substack{\psi \in \mathrm{Irr}(G) \\ \langle \chi, \psi \rangle = \psi(1)}} \psi(1)\psi, \quad \chi_{\mathcal{N}} = \chi_{\mathcal{L}} - \chi_{\mathcal{I}},$$

where $\chi_{\mathcal{L}}$ is called the *left ideal constituent* of χ, $\chi_{\mathcal{I}}$ is called the *ideal constituent* of χ, and $\chi_{\mathcal{N}}$ is called the *non-ideal constituent* of χ.

By the previous discussion, we see that $\chi_{\mathcal{L}}$ is the unique left ideal character of maximum degree which is a constituent of χ, while $\chi_{\mathcal{I}}$ is the unique ideal character of maximum degree which is a constituent of χ. Consequently, $\chi_{\mathcal{N}}$ is the unique non-ideal character satisfying $\chi_{\mathcal{L}} = \chi_{\mathcal{I}} + \chi_{\mathcal{N}}$. Note that these constituents of χ are easily computed if all irreducible characters of G are known. In general, finding those constituents of χ can be quite involved (see Section 5.3 for positive results), but at least there is a simple intrinsic characterization of ideal characters.

Lemma 5.1.2. *A class function $\chi\colon G \to \mathbb{C}$ is an ideal character of G if and only if*

$$\chi(g) = \frac{1}{|G|} \sum_{h \in G} \chi(gh^{-1})\chi(h) \text{ for all } g \in G.$$

In that case, χ is afforded by a $\Bbbk G$-module, where $\Bbbk = \mathbb{Q}(\chi)$ is the field generated by the values $\{\chi(g) : g \in G\}$ over $\mathbb{Q}$.

Proof. We consider the element

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

which is central in the group algebra since χ is a class function. If χ is the character of a two sided ideal I then e_χ is the unique idempotent of $\mathbb{C}G$ with $I = \Bbbk Ge$ by Lemma 4.2.7. Conversely, if e_χ is idempotent then the left ideal $\mathbb{C}Ge_\chi$ is a two sided ideal (since e_χ is central) affording the character χ (by Lemma 4.2.7 again). In conclusion, testing whether a class function χ is an ideal character comes down to check whether the element e_χ is idempotent. The claim follows by comparing the coefficients of e_χ and $(e_\chi)^2$.

The second assertion follows immediately, since the $\Bbbk G$-module $\Bbbk Ge_\chi$ affords the character χ. □

We now define the main objects of investigations of the present chapter. The following notations are well defined since isomorphic $\mathbb{C}G$-modules have the same generic symmetry group (Lemma 3.2.5).

Definition 5.1.3. Let χ be a character of G. We define the *generic symmetry group* $\mathrm{Sym}(G, \chi)$ of χ as $\mathrm{Sym}(G, V)$, where V is any $\mathbb{C}G$-module affording χ. Accordingly, the group of *irrelevant* generic symmetries $\mathrm{Iv}(G, \chi)$ of χ is defined as $\mathrm{Iv}(G, V)$. We call χ (weakly) generically closed if V is (weakly) generically closed.

Note that $\mathrm{Iv}(G, \chi)$ is just the subgroup of all elements of $\mathrm{Sym}(G)$ fixing all cosets of $\mathrm{Ker}(\chi)$ in G. Since the kernel of χ is given by a simple formula in terms of χ, the irrelevant generic symmetries of a character are easily determined.

Recall that if V is a cyclic $\mathbb{C}G$-module then $\mathrm{Sym}(G, V)$ has natural actions on V (given by the generators of V) which all lead to the same character of the generic symmetry group (Lemma 3.8.1). This character of $\mathrm{Sym}(G, V)$ is uniquely determined by the character of V.

Definition 5.1.4. Let χ be a left ideal character of G. Then $\widehat{\chi}$ denotes the character of $\mathrm{Sym}(G, \chi)$ afforded by $\widehat{V}_w$, where V is any $\mathbb{C}G$-module affording χ, and where $w \in \mathrm{Amp}(V)$ is any generator of V.

We will see that to a great extent, considerations on generic symmetries of $\mathbb{C}G$-modules can be done at the level of characters. We begin with simple estimates on sums and differences of characters.

Proposition 5.1.5. *Let χ and ψ be characters of G.*

(1) We always have $\mathrm{Sym}(G, \chi) \cap \mathrm{Sym}(G, \psi) \leq \mathrm{Sym}(G, \chi + \psi)$.

(2) If χ is a left ideal character then we have $\mathrm{Sym}(G, \rho - \chi) = \mathrm{Sym}(G, \chi)$*, where ρ is the regular character of G.*

(3) If χ is a left ideal character, and if ψ is a constituent of χ then we have $\mathrm{Sym}(G, \chi) \cap \mathrm{Sym}(G, \psi) \leq \mathrm{Sym}(G, \chi - \psi)$.

Proof. Let χ be afforded by the $\mathbb{C}G$-module V, and let ψ be afforded by the $\mathbb{C}G$-module W. By Lemma 3.2.8, we have $\mathrm{Sym}(G, V) \cap \mathrm{Sym}(G, W) \leq \mathrm{Sym}(G, V \oplus W)$, proving the first assertion

If χ is a left ideal character then V is isomorphic to a left ideal of $\mathbb{C}G$. By semisimplicity, there is a $\mathbb{C}G$-module W such that $V \oplus W \cong \mathbb{C}G$. The second assertion follows by Proposition 4.6.1, since the character of W is given by $\rho - \chi$.

Finally, suppose that χ is a left ideal character and that ψ is a constituent of χ. Then, using the previous statements, we compute

$$\begin{aligned} \mathrm{Sym}(G, \chi - \psi) &= \mathrm{Sym}(G, \rho - \chi + \psi) \geq \mathrm{Sym}(G, \rho - \chi) \cap \mathrm{Sym}(G, \psi) \\ &= \mathrm{Sym}(G, \chi) \cap \mathrm{Sym}(G, \psi). \end{aligned}$$

□

In general, the set inclusions in Proposition 5.1.5 are strict, but there is an important special case, where we always have equality. The following result is the reason why (left) ideal characters and non-ideal characters are essential notions in the character theoretic approach to generic symmetries. In particular, it shows that many questions on generic symmetries of arbitrary characters can be reduced to the case of left ideal characters.

Proposition 5.1.6. *Let χ be any character of G. Then we have*

$$\mathrm{Sym}(G,\chi) = \mathrm{Sym}(G,\chi_{\mathcal{L}}) = \mathrm{Sym}(G,\chi_{\mathcal{I}}) \cap \mathrm{Sym}(G,\chi_{\mathcal{N}}).$$

Proof. Let V be a $\mathbb{C}G$-module affording χ, and let $U \leq V$ be a cyclic submodule generated by an ample point of V. Then by definition, U is a cyclic submodule of V of maximum dimension, so the character of U must be $\chi_{\mathcal{L}}$. By Corollary 3.6.3, we have $\mathrm{Sym}(G,V) = \mathrm{Sym}(G,U)$, proving the first equality. The second equality is a consequence of Proposition 4.6.1 since $\chi_{\mathcal{I}}$ and $\chi_{\mathcal{N}}$ are the characters of $U_{\mathcal{I}}$ and $U_{\mathcal{N}}$ by definition. □

By Proposition 5.1.6, the task of determining generic symmetries of characters clearly reduces to the special cases of ideal characters and non-ideal characters. The following result is the character theoretic version of the generalized Isaacs' theorem (Theorem 4.5.4).

Theorem 5.1.7. *Let χ be a non-ideal character of G, that is, a character of G satisfying $\langle\chi,\psi\rangle < \psi(1)$ for all $\psi \in \mathrm{Irr}(G)$. Then χ is weakly generically closed, that is, we have*

$$\mathrm{Sym}(G,\chi) = G \cdot \mathrm{Iv}(G,\chi).$$

Moreover, we have $\widehat{\chi}(\pi) = \chi(\pi(1))$ for all $\pi \in \mathrm{Sym}(G,\chi)$.

Proof. Let V be a $\mathbb{C}G$-module affording χ. Then V is a cyclic module with trivial ideal constituent by the hypothesis on χ. So V is weakly generically closed by Theorem 4.5.4. Let $\pi \in \mathrm{Sym}(G,V)$ be any generic symmetry. Then there is a decomposition $\pi = \iota_g \circ \sigma$, where ι_g is the left multiplication by some $g \in G$, and where $\sigma \in \mathrm{Iv}(G,V)$ is irrelevant with $\sigma(1) = 1$. If $w \in \mathrm{Amp}(V)$ is any generator then σ acts trivially on $\widehat{V}_w$. So π acts on $\widehat{V}_w$ in the same way as ι_g does. Hence, $\widehat{\chi}(\pi) = \widehat{\chi}(\iota_g) = \chi(g) = \chi(\pi(1))$. □

For an ideal character χ of G, we already know by Proposition 4.5.3 a characterization of $\mathrm{Sym}(G,\chi)$ in terms of a certain formula depending on χ. It actually turns out that the same formula gives a necessary condition in the more general setting of left ideal characters.

Theorem 5.1.8. *Let χ be a left ideal character of G, and let $\pi \in \mathrm{Sym}(G)$ be a permutation. If π is a generic symmetry of χ then we have*

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

If χ is even an ideal character, the converse holds as well.

Proof. The assertion on ideal characters immediately follows by Proposition 4.5.3. So let χ be a left ideal character, and let $\pi \in \mathrm{Sym}(G,\chi)$ be any generic symmetry. By Proposition 5.1.6 π is a generic symmetry of both $\chi_{\mathcal{I}}$ and $\chi_{\mathcal{N}}$. Since the assertion holds for ideal characters, we clearly have $\chi_{\mathcal{I}}(\pi(g)^{-1}\pi(h)) = \chi_{\mathcal{I}}(g^{-1}h)$ for all $g,h \in G$. Since

χ is a left ideal character, we have $\chi = \chi_{\mathcal{I}} + \chi_{\mathcal{N}}$, and it remains to show that also $\chi_{\mathcal{N}}(\pi(g)^{-1}\pi(h)) = \chi_{\mathcal{N}}(g^{-1}h)$ holds for all $g, h \in G$.

We set $\psi = \chi_{\mathcal{N}}$. By Theorem 5.1.7, ψ is weakly generically closed, so π is an irrelevant generic symmetry of ψ. Let $K = \mathrm{Ker}(\psi)$ be the kernel of ψ, and let $g, h \in G$ be arbitrary elements. Then there are elements $k_1, k_2 \in K$ such that $\pi(g) = gk_1$ and $\pi(h) = hk_2$. We conclude $\psi(\pi(g)^{-1}\pi(h)) = \psi(k_1^{-1}(g^{-1}h)k_2) = \psi(g^{-1}h)$. □

Example 5.1.9. We finish the considerations of Example 3.1.6. In that example, we have considered the cyclic group $G = \langle x \rangle$ of order n acting on the Euclidean plane by rotations. The corresponding left ideal character (which is actually an ideal character) is given by

$$\chi(x^k) = 2\cos\left(\frac{2k\pi}{n}\right) \text{ for all } k \in \mathbb{Z}.$$

We have already noticed that the permutation $\sigma \in \mathrm{Sym}(G)$ sending each group element to its inverse is an orbit symmetry of any element of the plane, and hence a generic symmetry of χ. So $\mathrm{Sym}(G, \chi)$ contains the subgroup U of order $2n$ generated by the left multiplications ι_g and by σ. We will use Theorem 5.1.8 to show that actually $U = \mathrm{Sym}(G, \chi)$, or equivalently, $\mathrm{Sym}(G, \chi)_1 = \langle \sigma \rangle$ holds.

Let $\pi \in \mathrm{Sym}(G, \chi)_1$ be any generic symmetry stabilizing $1 \in G$. Note that for arbitrary elements $g, h \in G$, we have $\chi(g) = \chi(h)$ if and only if $g = h$ or $g = h^{-1}$. Applying Theorem 5.1.8 to $g = 1$, we see that $\chi(\pi(h)) = \chi(h)$, and hence $\pi(h) \in \{h, h^{-1}\}$ holds for all $h \in G$. We have to show that π is either the identity or the inversion map. Otherwise, we would have $\pi(g) = g^{-1}$ and $\pi(h) = h$ for some elements $g, h \in G$ with $g^2, h^2 \neq 1$. Then $\pi(g)^{-1}\pi(h) = gh$ is certainly different from both $g^{-1}h$ and $h^{-1}g$, which implies $\chi(\pi(g)^{-1}\pi(h)) \neq \chi(g^{-1}h)$. This contradicts Theorem 5.1.8.

Combining the previous results on the generic symmetries of (left) ideal characters and non-ideal characters, we get a formula for $\mathrm{Sym}(G, \chi)$ for arbitrary characters χ of G. Thus, we see that (if there are sufficiently many information on the constituents of χ available) the generic symmetries of a character can be determined without referring to a module at all.

Theorem 5.1.10. *Let χ be a character of G. Then we have*

$$\mathrm{Sym}(G,\chi) = \left\{ \pi \in \mathrm{Sym}(G) : \begin{array}{rcll} \chi_{\mathcal{I}}(\pi(g)^{-1}\pi(h)) & = & \chi_{\mathcal{I}}(g^{-1}h) & \text{for all } g,h \in G \\ \pi(gK) & = & \pi(1)gK & \text{for all } g \in G \end{array} \right\},$$

where K is the kernel of $\chi_{\mathcal{N}}$ in G.

Proof. This is an immediate consequence of Proposition 5.1.6, Theorem 5.1.7, and Theorem 5.1.8. □

As a first application of Theorem 5.1.10, we determine those characters for which the inversion map is a generic symmetry. The following observation is an important detail in the considerations of the next chapter.

Corollary 5.1.11. *Let χ be a left ideal character of G. The inversion of group elements $\sigma\colon g \mapsto g^{-1}$ is a generic symmetry of χ if and only if χ is a real valued ideal character. In particular, χ is afforded by an $\mathbb{R}G$-module in that case.*

Proof. If χ is a real valued ideal character then σ must be a generic symmetry of χ by Theorem 5.1.8 and by the fact that $\chi(g^{-1}) = \overline{\chi(g)}$ for all $g \in G$. By Lemma 5.1.2, χ is afforded by an $\mathbb{R}G$-module in that case.

Conversely, suppose that σ is a generic symmetry of χ, and let $K = \mathrm{Ker}(\chi_{\mathcal{N}})$ be the kernel of the non-ideal constituent of χ. By Theorem 5.1.10, σ fixes all cosets of K in G which is equivalent to G/K being an elementary abelian 2-group. Since all left ideal characters of abelian groups are ideal characters, it follows that $\chi_{\mathcal{N}}$ is an ideal character, whence $\chi_{\mathcal{N}} = 0$. So χ must be an ideal character, and by the same argument as before, we conclude $\chi = \overline{\chi}$. ☐

Before stating the next theorem, we need to recall some standard facts about permutation characters. Let P be any finite group acting on a finite set Ω by permutations. Then P acts linearly on the complex vector space $\mathbb{C}^{\Omega}$ by permuting coordinates. As a $\mathbb{C}P$-module, $\mathbb{C}^{\Omega}$ is called the *permutation module* corresponding to the action of P on Ω. The corresponding character χ is called a *permutation character*. For any $g \in P$ the value of $\chi(g)$ equals the number of fixed points of g on Ω. Since P acts trivially on the one dimensional subspace of $\mathbb{C}^{\Omega}$ generated by the all-one-vector, the trivial character 1_P is always a constituent of χ. It is well known that the inner product $\langle \chi, 1_P \rangle$ is equal to the number of orbits of P on Ω, and that the inner product $\langle \chi, \chi \rangle = \langle \chi^2, 1_P \rangle$ is exactly the number of orbits of P on Ω^2. Consequently, by calculating the inner product $\langle \chi - 1_P, \chi - 1_P \rangle$, we see that the character $\chi - 1_P$ is irreducible if and only if P is doubly transitive on Ω.

We go on by examining the canonical extension $\widehat{\chi}$ of any left ideal character χ of G. The following structure theorem shows how $\widehat{\chi}$ decomposes into smaller constituents in accordance with a certain decomposition of χ. In that situation, it is useful to regard $\widehat{\chi}$ not only as a character of the generic symmetry group $\mathrm{Sym}(G, \chi)$ but also as a character of any subgroup between G and $\mathrm{Sym}(G, \chi)$ (formally, we consider restrictions of $\widehat{\chi}$). The following result is essentially an application of Theorem 4.6.4. If χ is the character of any left ideal $L \leq \mathbb{C}G$ then Theorem 4.6.4 shows that L is also a $\mathbb{C}\,\mathrm{Sym}(G, \chi)$-submodule of $\mathbb{C}G$ affording the character $\widehat{\chi}$.

Theorem 5.1.12. *Let $\widehat{G} \leq \mathrm{Sym}(G)$ be any permutation group on G containing all left multiplications by elements of G. Let χ, ψ be left ideal characters of G such that $\widehat{G} \subseteq \mathrm{Sym}(G, \chi)$ and $\widehat{G} \subseteq \mathrm{Sym}(G, \psi)$. Then the following statements hold.*

(1) If ρ is the regular character of G then $\widehat{G} \subseteq \mathrm{Sym}(G, \rho)$, and $\widehat{\rho}$ is exactly the permutation character of $\widehat{G}$ acting on G.

(2) If χ is a constituent of ψ then $\widehat{\chi}$ is a constituent of $\widehat{\psi}$ as characters of $\widehat{G}$.

(3) If $\chi + \psi$ is a left ideal character of G then $\widehat{G} \subseteq \mathrm{Sym}(G, \chi + \psi)$ and $\widehat{\chi + \psi} = \widehat{\chi} + \widehat{\psi}$ as characters of $\widehat{G}$.

(4) We have $\widehat{G} \subseteq \mathrm{Sym}(G, \chi_{\mathcal{I}})$*, and* $\widehat{\chi_{\mathcal{I}}}$ *is a constituent of* $\widehat{\chi}$ *as characters of* $\widehat{G}$*.*

(5) Let α *be any constituent of* $\chi_{\mathcal{N}}$*. Then* $\widehat{G} \subseteq \mathrm{Sym}(G, \alpha)$*, and* $\widehat{\alpha}$ *is a constituent of* $\widehat{\chi}$ *as characters of* $\widehat{G}$*.*

Proof. The regular character ρ of G is afforded by the group algebra $\mathbb{C}G$ as a left module over itself. Of course, we have $\mathrm{Sym}(G, \rho) = \mathrm{Sym}(G)$ (for example, by Theorem 5.1.10), so $\widehat{G} \subseteq \mathrm{Sym}(G, \rho)$ in particular. By Theorem 4.6.4, the extended character $\widehat{\rho}$ is afforded by $\mathbb{C}G$ regarded as a $\mathbb{C}\widehat{G}$-module, which is exactly the permutation module of $\widehat{G}$ acting on G. Thus, $\widehat{\rho}$ is the permutation character of $\widehat{G}$ acting on G. This proves (1).

We go on by proving (2). Since χ is a constituent of ψ, there are left ideals $A \leq B \leq \mathbb{C}G$ such that χ is afforded by A, and ψ is afforded by B. By Theorem 4.6.4, A and B are $\mathbb{C}\widehat{G}$-submodules of $\mathbb{C}G$ affording the characters $\widehat{\chi}$ and $\widehat{\psi}$, respectively. This shows that $\widehat{\chi}$ is a constituent of $\widehat{\psi}$.

Suppose that the hypothesis of (3) holds. We have $\widehat{G} \subseteq \mathrm{Sym}(G, \chi + \psi)$ by Proposition 5.1.5. Let $L = A \oplus B$ be an internal direct sum of left ideals of $\mathbb{C}G$ such that χ is afforded by A, and ψ is afforded by B (of course, then L is afforded by $\chi + \psi$). By Theorem 4.6.4, A, B, and L are $\mathbb{C}\widehat{G}$-submodules of $\mathbb{C}G$ affording the extended characters $\widehat{\chi}$, $\widehat{\psi}$, and $\widehat{\chi + \psi}$. Thus, we have $\widehat{\chi} + \widehat{\psi} = \widehat{\chi + \psi}$.

Finally, we have $\widehat{G} \subseteq \mathrm{Sym}(G, \chi) = \mathrm{Sym}(G, \chi_{\mathcal{I}}) \cap \mathrm{Sym}(G, \chi_{\mathcal{N}})$ by Proposition 5.1.6. By Theorem 5.1.7, any constituent α of $\chi_{\mathcal{N}}$ (including $\chi_{\mathcal{N}}$ itself) is weakly generically closed. Since $\mathrm{Ker}(\chi_{\mathcal{N}}) \subseteq \mathrm{Ker}(\alpha)$, we see that $\widehat{G} \subseteq \mathrm{Sym}(G, \chi_{\mathcal{N}}) \subseteq \mathrm{Sym}(G, \alpha)$. By what we have already shown, we conclude that both $\widehat{\chi_{\mathcal{I}}}$ and $\widehat{\alpha}$ are constituents of $\widehat{\chi}$, proving (4) and (5). □

Recall that a generic symmetry group $\mathrm{Sym}(G, \chi)$ is always transitive on G as it contains a regular subgroup (isomorphic to G). However, we will see that this action is rarely 2-transitive.

Corollary 5.1.13. *Let* χ *be a character of* G *such that* $\mathrm{Sym}(G, \chi)$ *is doubly transitive on* G*. Then* $\mathrm{Sym}(G, \chi) = \mathrm{Sym}(G)$*, and either* χ *is a scalar multiple of the trivial character, or* $\rho - 1_G$ *is a constituent of* χ*, where* ρ *denotes the regular character of* G*.*

Proof. Let $\widehat{G} = \mathrm{Sym}(G, \chi)$. By Theorem 5.1.12 and Proposition 5.1.5, the $\widehat{G}$-character $\widehat{\chi_{\mathcal{L}}}$ is a constituent of $\widehat{\rho} = \widehat{\rho - 1_G} + \widehat{1_G}$. Since $\widehat{\rho}$ is the permutation character of a doubly transitive action, both $\widehat{\rho - 1_G}$ and $\widehat{1_G} = 1_{\widehat{G}}$ are irreducible. So we have $\widehat{\chi_{\mathcal{L}}} \in \{\widehat{1_G}, \widehat{\rho - 1_G}, \widehat{\rho}\}$, and by restriction to G, we get $\chi_{\mathcal{L}} \in \{1_G, \rho - 1_G, \rho\}$. In any case, we have $\mathrm{Sym}(G, \chi) = \mathrm{Sym}(G, \chi_{\mathcal{L}}) = \mathrm{Sym}(G)$ by Propositions 5.1.6 and 5.1.5. □

Remark 5.1.14. The proof of Corollary 5.1.13 essentially relies on the fact that the permutation module of a doubly transitive group action decomposes into the trivial module and exactly one other simple module in characteristic zero. This does not necessarily hold in positive characteristics. In fact, we have already observed in Example 4.3.9 that a generic symmetry group may be doubly transitive without being a full symmetric group.

The last main result of this section is a formula for the extended character $\widehat{\chi}$ which only relies on χ. It is a remarkable coincidence that, although the generic symmetries of ideal characters and of non-ideal characters are characterized in completely different ways, their character values are given by the same formula.

In the following proof, it is convenient to use the canonical isomorphism

$$V^* \otimes_{\mathbb{C}} V \to \mathrm{End}_{\mathbb{C}}(V), \quad \lambda \otimes v \mapsto (x \mapsto \lambda(x)v)$$

to identify the endomorphisms of a finite dimensional $\mathbb{C}$-space V with the elements of $V^* \otimes_{\mathbb{C}} V$, where $V^* = \mathrm{Hom}_{\mathbb{C}}(V, \mathbb{C})$ is the dual space of V. Recall that the trace of an endomorphism $\sum_{i=1}^n \lambda_i \otimes v_i$ given in that way is simply the sum $\sum_{i=1}^n \lambda_i(v_i)$.

Theorem 5.1.15. *Let χ be a left ideal character of G, and let $\widehat{\chi}$ be the character associated to* $\mathrm{Sym}(G, \chi)$. *Then for all $\pi \in \mathrm{Sym}(G, \chi)$ we have*

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

Moreover, $\widehat{\chi}$ is a weakly generically closed character of $\mathrm{Sym}(G, \chi)$*.*

Proof. By Theorem 3.8.6, $\widehat{\chi}$ is always weakly generically closed. Let $\widehat{G} = \mathrm{Sym}(G, \chi)$. Since we have $\widehat{\chi} = \widehat{\chi_{\mathcal{I}}} + \widehat{\chi_{\mathcal{N}}}$ as characters of $\widehat{G}$ by Theorem 5.1.12, we may assume for the rest of the proof that χ is either an ideal character or a non-ideal character.

Suppose that χ is a non-ideal character, and let $K = \mathrm{Ker}(\chi)$. By Theorem 5.1.7, we have $\pi(gK) = \pi(1)gK$ as well as $\widehat{\chi}(\pi) = \chi(\pi(1))$ for all $g \in G, \pi \in \widehat{G}$. For any $g \in G$, and any $\pi \in \widehat{G}$, there is an element $k \in K$ such that $\pi(g) = \pi(1)gk$. Consequently, we have

$$\chi(g^{-1}\pi(g)) = \chi(g^{-1}\pi(1)gk) = \chi(g^{-1}\pi(1)g) = \chi(\pi(1)).$$

So in the present case, the assertion follows immediately.

Now suppose that χ is an ideal character afforded by a two sided ideal $I \leq \mathbb{C}G$, say. By Theorem 4.6.4, I is also a $\mathbb{C}\widehat{G}$-submodule of $\mathbb{C}G$ affording the extended character $\widehat{\chi}$. We consider central idempotent generator $e = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g \in \mathbb{C}G$ of I given by Lemma 4.2.7. Let $\pi \in \mathrm{Sym}(G, \chi)$ be any generic symmetry of χ. We claim that π is given as a $\mathbb{C}$-linear operator on I by the endomorphism $\alpha = \frac{1}{|G|} \sum_{g \in G} \lambda_g \otimes \pi(ge) \in I^* \otimes_{\mathbb{C}} I$, where λ_g is the linear form $x \mapsto \chi(g^{-1}x)$. In fact, for all $h \in G$ we have

$$\alpha(he) = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}h)\pi(ge) = \pi\left(\frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})hge\right) = \pi(hee) = \pi(he),$$

proving that assertion. Since we have $\pi(he) = \pi(h)e$ for all $h \in G$ (for example, by Theorem 5.1.8, or by Lemma 4.3.7 and 4.3.2), we conclude

$$\widehat{\chi}(\pi) = \mathrm{Tr}_I(\alpha) = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}\pi(ge)) = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}\pi(g)).$$

□

We have already seen in the proof of Corollary 5.1.13 that the consideration of the extended character $\widehat{\chi}$ of a left ideal character χ can be very useful in order to achieve results on the generic symmetry group $\mathrm{Sym}(G, \chi)$. Theorem 5.1.15 is remarkable as it shows that $\widehat{\chi}$ can be computed without any knowledge about the ideal constituent of χ. We give a very simple example which illustrates how the formula for $\widehat{\chi}$ can be used to show that a permutation is *not* a generic symmetry without referring to Theorem 5.1.10 (which requires knowledge about $\chi_{\mathcal{I}}$).

Example 5.1.16. Let $G = \langle r, s : r^4 = s^2 = 1, srs = r^{-1} \rangle$ be the dihedral group of order eight, and let χ be the character of the usual action of G on the Euclidean plane by rotations and reflections (we have $\chi(1) = 2, \chi(r^2) = -2$, and $\chi(g) = 0$ for all $g \in G \setminus \langle r^2 \rangle$). Suppose that we have no information about the constituents of χ (which is actually an irreducible character). In view of Theorem 5.1.8, we may identify the group inversion $\sigma \colon g \mapsto g^{-1}$ as a potential candidate for a generic symmetry of χ. Assuming $\sigma \in \mathrm{Sym}(G, \chi)$, we use Theorem 5.1.15 to compute

$$\widehat{\chi}(\sigma) = \frac{1}{8} \sum_{g \in G} \chi(g^2) = \frac{1}{8}(6 \cdot 2 + 2 \cdot (-2)) = 1.$$

This is impossible however, since any matrix $A \in \mathrm{GL}(n, \mathbb{C})$ of order two has an integral trace satisfying $\mathrm{Tr}(A) \equiv n \mod 2$ (as follows easily by diagonalization). So σ cannot be a generic symmetry of χ.

5.2 Continuation of characters

In the last section, we introduced a framework allowing us to handle generic symmetry groups only in terms of characters, without referring to modules or representations. The aim of the present section is to give suggestions on how this framework may actually be useful to study characters of finite groups. In general, if G is a finite group, and if U is a subgroup with some character χ, one might ask whether χ is the restriction of some character of G. In that case, we say that χ admits a continuation to G. We give a sufficient condition for χ admitting a continuation in the special case, where U has a complement in G. The following considerations have not been published so far.

In the following, we consider a finite group G with subgroups $H, A \leq G$ such that $G = HA$ and $H \cap A = 1$ (G is called a Zappa-Szép product of H and A). In that case, the left cosets of A in G can be naturally identified with the elements of H. Since G acts on the left cosets of A by left multiplication, any element of G can be regarded as a permutation on H. More precisely, for all $g \in G$ there is a unique permutation $\pi_g \in \mathrm{Sym}(H)$ such that

$$ghA = \pi_g(h)A \text{ for all } h \in H.$$

From that equation it follows immediately that the map $\Psi \colon G \to \mathrm{Sym}(H)$, $g \mapsto \pi_g$ is a homomorphism. Under that morphism, any element $h \in H$ is sent to the left multiplication ι_h. Furthermore, we have $\pi_g(1) = 1$ if and only if $g \in A$, so A is the preimage under Ψ of the stabilizer $\mathrm{Sym}(H)_1$. In particular, we have

$$\mathrm{Ker}(\Psi) = \bigcap_{g \in G} A^g = \bigcap_{h \in H} A^h,$$

which is usually called the *core* of A in G. Now suppose that we have a left ideal character χ of H such that $\Psi(G) \subseteq \mathrm{Sym}(H, \chi)$ (or equivalently, $\Psi(A) \subseteq \mathrm{Sym}(H, \chi)$). Then by Theorem 5.1.15, χ can be extended to a character $\widehat{\chi}$ of $\Psi(G)$ in a very specific way. Consequently, we get a canonical continuation $\widehat{\chi} \circ \Psi$ of χ to G. This idea is refined in the following Proposition.

Proposition 5.2.1. *Let $G = HA$, where $H, A \leq G$ are subgroups such that $H \cap A = 1$. Let χ be a left ideal character of H such that $\Psi(A) \subseteq \mathrm{Sym}(H, \chi)$. Then χ can be extended to a character $\widehat{\chi}$ of G with*

$$\widehat{\chi}(g) = \frac{1}{|H|} \sum_{h \in H} \chi(h^{-1} \pi_g(h))$$

for all $g \in G$. Furthermore, the following holds.

(1) If χ is an ideal character then

$$\langle \widehat{\chi}, \widehat{\chi} \rangle = \frac{1}{|A|} \frac{1}{|H|^2} \sum_{a \in A} \sum_{h_1, h_2 \in H} \chi(h_2^{-1} h_1 \pi_a(h_1)^{-1} \pi_a(h_2)).$$

(2) Suppose that $\Psi(A)$ contains all inner automorphisms of H. Let χ be an ideal character of H which, among all nonzero ideal characters of H, is minimal subject to $\Psi(A) \subseteq \mathrm{Sym}(H, \chi)$. Then $\widehat{\chi}$ is an irreducible character of G.

Proof. We have already seen in the previous discussion that χ can be extended to a character $\widehat{\chi}$ by that formula. If χ is an ideal character, we compute

$$\begin{aligned} \langle \widehat{\chi}, \widehat{\chi} \rangle = \frac{1}{|G|} \sum_{x \in H, a \in A} \overline{\widehat{\chi}(xa)} \widehat{\chi}(xa) &= \frac{1}{|G|} \frac{1}{|H|^2} \sum_{a \in A} \sum_{x, h_1, h_2 \in H} \overline{\chi(h_1^{-1} x \pi_a(h_1))} \chi(h_2^{-1} x \pi_a(h_2)) \\ &= \frac{1}{|G|} \frac{1}{|H|} \sum_{a \in A} \sum_{h_1, h_2 \in H} \chi(h_2^{-1} h_1 \pi_a(h_1)^{-1} \pi_a(h_2)), \end{aligned}$$

where the last equality is due to Lemma 5.1.2.

Concerning the last assertion, note that $\widehat{\chi}$ is the character of the permutation group $\Psi(G)$ acting on a two sided ideal I of the group algebra $\mathbb{C}H$ (Theorem 4.6.4). If $\Psi(A)$ contains all inner automorphisms of H then all $\mathbb{C}\Psi(G)$-submodules of I are two sided ideals of $\mathbb{C}H$, whence all constituents of $\widehat{\chi}$ restrict to ideal characters of H. If χ is minimal among all nonzero ideal characters subject to $\Psi(A) \subseteq \mathrm{Sym}(H, \chi)$ then I must be a simple $\mathbb{C}\Psi(G)$-module, and $\widehat{\chi}$ must be an irreducible character. □

The situation simplifies a lot when H is normal in G. Then the core of A in G equals the centralizer $C_A(H)$, and π_a is simply the (left) conjugation by a (that is, $\pi_a(x) = axa^{-1}$) for all $a \in A$.

Corollary 5.2.2. *Let $G = H \rtimes A$ be a semidirect product, and let χ be an ideal character of H which is invariant under conjugation by A. Then χ can be extended to a character $\widehat{\chi}$ of G such that*

$$\widehat{\chi}(ha) = \frac{1}{|H|}\sum_{x\in H}\chi(haxa^{-1}x^{-1}) \text{ for all } h \in H, a \in A.$$

(1) We have

$$\langle\widehat{\chi},\widehat{\chi}\rangle = \frac{1}{|A|}\sum_{a\in A}\widehat{\chi}(a) = \langle\widehat{\chi}_{|A}, 1_A\rangle.$$

(2) If $H \leq C_G(H)A$, and if χ has no nontrivial proper ideal constituents invariant under A then $\widehat{\chi}$ is irreducible.

Proof. Since χ is an A-invariant (and hence G-invariant) ideal character, we have $\Psi(G) \subseteq \mathrm{Sym}(H,\chi)$ by Theorem 5.1.10 (in the notation of Proposition 5.2.1). The formula for $\widehat{\chi}$ is an immediate consequence of Proposition 5.2.1 since we have

$$\chi(x^{-1}\pi_{ha}(x)) = \chi(x^{-1}haxa^{-1}) = \chi(haxa^{-1}x^{-1})$$

for all $x, h \in H$ and $a \in A$. The inner product formula of Proposition 5.2.1 simplifies as

$$\begin{aligned}\langle\widehat{\chi},\widehat{\chi}\rangle &= \frac{1}{|A|}\frac{1}{|H|^2}\sum_{a\in A}\sum_{h_1,h_2\in H}\chi((h_2^{-1}h_1)a(h_2^{-1}h_1)^{-1}a^{-1})\\ &= \frac{1}{|A|}\frac{1}{|H|}\sum_{a\in A}\sum_{x\in H}\chi(x^{-1}axa^{-1}) = \frac{1}{|A|}\sum_{a\in A}\widehat{\chi}(a) = \langle\widehat{\chi}_{|A}, 1_A\rangle.\end{aligned}$$

Finally, suppose we have $H \leq C_G(H)A$. Then for any $h \in H$ there are elements $c \in C_G(H)$ and $a \in A$ such that $h = ca$. For all $x \in H$ we have $x^h = x^{ca} = x^a$, so $\pi_a \in \mathrm{Sym}(H)$ is just the conjugation by h. Since h was arbitrary, $\Psi(A)$ contains all inner automorphisms of H. By Theorem 5.1.8, all ideal characters ψ of H with $\Psi(A) \subseteq \mathrm{Sym}(G,\psi)$ are A-invariant. Since χ has no nonzero proper A-invariant constituents, $\widehat{\chi}$ is irreducible by Proposition 5.2.1. □

Example 5.2.3. Let $G = \mathrm{GL}(2,3)$ be the group of all invertible (2×2)-matrices over the field with three elements. This group of order 48 acts transitively on the set of nonzero vectors $\Omega = \mathbb{F}_3^2 \setminus \{0\}$. We also consider the subgroup $\mathrm{SL}(2,3) \leq \mathrm{GL}(2,3)$ of all matrices with determinant 1. This group of order 24 still acts transitively on Ω. By the Cayley-Hamilton theorem one easily checks that $\mathrm{SL}(2,3)$ has exactly one involution (the negative identity matrix -1), six elements of order four, namely

$$\begin{pmatrix} x & -x^2/y \\ y & -x \end{pmatrix} \text{ for } x \in \mathbb{F}_3 \text{ and } y \in \mathbb{F}_3^\times,$$

and no element of order eight. So these six elements of order four together with 1 and -1 form the unique Sylow 2-subgroup of $\mathrm{SL}(2, 3)$ which we call H. Being a unique Sylow subgroup of a characteristic subgroup, H is normal in G. From the element orders of H we already see that H is isomorphic to the quaternion group Q_8. Since all point stabilizers of $\mathrm{SL}(2, 3)$ have order three, and since $|H| = 8$, we see that H acts regularly on Ω. Let $A = G_v$ denote the stabilizer (of order six) in G of some vector $v \in \Omega$. By the Frattini argument, we see that G is an internal semidirect product $G = H \rtimes A$. Since H is regular on Ω, the natural action of A on Ω is equivalent to the action of A on H by conjugation. In particular, A centralizes precisely the elements $\pm 1 \in H$, whereas A acts regularly on the six elements of order four of H. Moreover, A faithfully permutes the three conjugacy classes of length two in H, which shows that A is isomorphic to S_3.

We now consider the character $\chi = 2\psi$ of H, where $\psi \in \mathrm{Irr}(H)$ is the unique irreducible character of degree two (ψ is zero on the six elements of order four, and minus two on the unique involution). Then χ is a G-invariant ideal character of H, and by Corollary 5.2.2, χ extends to a character $\widehat{\chi}$ of G. We claim that $\widehat{\chi}$ is irreducible. Since we do not have $H \leq C_G(H)A$ in this example (so the sufficient criterion of Corollary 5.2.2 does not apply), we will compute the values of $\widehat{\chi}_{|A}$ and the inner product $\langle \widehat{\chi}, \widehat{\chi} \rangle$.

Of course we have $\widehat{\chi}(1) = \chi(1) = 4$. Since conjugation by any nonidentity element $1 \neq a \in A$ fixes exactly two elements of H, the equation $axa^{-1}x^{-1} = 1$ has exactly two solutions $x \in H$. If $a \in A$ is an element of order three, and if $x \in H \setminus \{\pm 1\}$ then x and axa^{-1} lie in different conjugacy classes of H. Therefore, we have $axa^{-1}x^{-1} \neq -1$ for all $x \in H$. We conclude

$$\widehat{\chi}(a) = \frac{1}{8}(4 + 4 + 0 + 0 + 0 + 0 + 0 + 0) = 1$$

for all elements $a \in A$ of order three. If $b \in A$ is an element of order two, conjugation by b fixes precisely one of the three conjugacy classes of length two in H, and b acts as a transposition on that class. So the equation $bxb^{-1}x^{-1} = -1$ holds for precisely two elements $x \in H$. We conclude

$$\widehat{\chi}(b) = \frac{1}{8}(4 + 4 - 4 - 4 + 0 + 0 + 0 + 0) = 0$$

for all $b \in A$ of order two. Now $A \cong S_3$ has two elements of order three and three elements of order two. By Corollary 5.2.2, we get

$$\langle \widehat{\chi}, \widehat{\chi} \rangle = \frac{1}{6}(4 + 1 + 1 + 0 + 0 + 0) = 1.$$

So the extension $\widehat{\chi}$ of χ is indeed an irreducible character of G.

5.3 Induced characters

Although we have determined the generic symmetry group of an arbitrary character χ in terms of a formula only depending on χ (Theorem 5.1.10), we still need to know the ideal constituent and the non-ideal constituent of χ for applying that formula. Since we cannot always assume to know the character table of a given group in practice, we need other techniques to find these constituents. In this section, we develop techniques for extracting the ideal and non-ideal constituents of *induced characters*. The results of the present section are due to Ladisch. They are extracted from [19], where they (partly) appear implicitly in different proofs.

We recall some standard facts about induction of modules and characters. Let G be a finite group, and let $U \leq G$ be a subgroup. If V is any $\mathbb{C}U$-module, the tensor product $\mathbb{C}G \otimes_{\mathbb{C}U} V$ is a $\mathbb{C}G$-module in a natural way (where $\mathbb{C}G$ is considered as a $\mathbb{C}G$-$\mathbb{C}U$-bimodule in the canonical way). It is called an *induced module*. If V affords the character χ of U, the *induced character* χ^G afforded by $\mathbb{C}G \otimes_{\mathbb{C}U} V$ is given by the formula

$$\chi^G(g) = \frac{1}{|U|} \sum_{\substack{t \in G \\ g^t \in U}} \chi(g^t) \text{ for all } g \in G.$$

This formula already shows that character induction is additive (that is, $(\chi + \psi)^G = \chi^G + \psi^G$ holds for arbitrary characters χ, ψ of U), and that the kernel of any nonzero induced character is given by

$$\operatorname{Ker}\left(\chi^G\right) = \bigcap_{g \in G} \operatorname{Ker}(\chi)^g.$$

It is well known that tensor products are associative. That is, if $H \leq U \leq G$ is a chain of subgroups, and if V is any $\mathbb{C}H$-module, we have natural isomorphisms

$$\mathbb{C}G \otimes_{\mathbb{C}U} (\mathbb{C}U \otimes_{\mathbb{C}H} V) \cong (\mathbb{C}G \otimes_{\mathbb{C}U} \mathbb{C}U) \otimes_{\mathbb{C}H} V \cong \mathbb{C}G \otimes_{\mathbb{C}H} V.$$

Consequently, for any character χ of H we have $(\chi^U)^G = \chi^G$. The isomorphism $\mathbb{C}G \otimes_{\mathbb{C}U} \mathbb{C}U \cong \mathbb{C}G$, which we have just used implicitly, also shows that inducing the regular character of U yields the regular character of G.

Another important property is that character induction does not affect the field of definition. That is, if $\Bbbk$ is any field between $\mathbb{Q}$ and $\mathbb{C}$, and if χ is a character afforded by a $\Bbbk U$-module then the induced character χ^G is afforded by a $\Bbbk G$-module. This is due to the canonical isomorphism

$$\mathbb{C} \otimes_{\Bbbk} (\Bbbk G \otimes_{\Bbbk U} V) \cong \mathbb{C}G \otimes_{\mathbb{C}U} (\mathbb{C} \otimes_{\Bbbk} V)$$

of $\mathbb{C}G$-modules which holds for any $\Bbbk U$-module V. (This can be seen directly by constructing two (canonical) inverse morphisms, but it follows more abstractly from the fact that both induction and scalar extension are left adjoints of certain forgetful functors.)

The inner product of an induced character with another character is most easily computed by the *Frobenius reciprocity.* That is, if χ is any character of U and if ψ is any character of G then we have

$$\langle \chi^G, \psi \rangle = \langle \chi, \psi_{|U} \rangle.$$

Since group algebras over fields of characteristic zero are semisimple, all their modules are flat (even projective). So tensoring with any fixed module is an exact functor, which (in particular) preserves injective morphisms. Let $L \leq \mathbb{C}U$ be any left ideal. Then the inclusion morphism $L \hookrightarrow \mathbb{C}U$ gives rise to a monomorphism

$$\mathbb{C}G \otimes_{\mathbb{C}U} L \hookrightarrow \mathbb{C}G \otimes_{\mathbb{C}U} \mathbb{C}U = \mathbb{C}G.$$

For that reason, $\mathbb{C}G \otimes_{\mathbb{C}U} L$ may be regarded as a left ideal of $\mathbb{C}G$. More precisely, if $e \in \mathbb{C}U$ is any idempotent generator of L then e (regarded as an element of $\mathbb{C}G$) also generates a left ideal of $\mathbb{C}G$ canonically isomorphic to $\mathbb{C}G \otimes_{\mathbb{C}U} L$. In particular, we see that if χ is any left ideal character of U then χ^G is a left ideal character of G.

The following definition is not standard, but it generalizes the standard terminology of invariant characters in the case where U is a normal subgroup of G.

Definition 5.3.1. Let χ be a character of a subgroup $U \leq G$. We define a function $\dot{\chi}\colon G \to \mathbb{C}$ by

$$\dot{\chi}(g) = \begin{cases} \chi(g) & \text{if } g \in U \\ 0 & \text{if } g \notin U \end{cases}.$$

The character χ is called *invariant* under G if $\dot{\chi}$ is a class function of G.

Lemma 5.3.2. *Let χ be a left ideal character of $U \leq G$. Then the induced character χ^G is a left ideal character of G. Moreover, χ^G is an ideal character of G if and only if χ is an G-invariant ideal character of U.*

Proof. Let L be a left ideal of $\mathbb{C}U$ affording χ, and let $e \in L$ be an idempotent generator of L. By the preceding discussion, $L' = \mathbb{C}Ge$ is a left ideal of $\mathbb{C}G$ affording the induced character χ^G (in particular, χ^G is a left ideal character). By Lemma 4.2.7, L' is a two sided ideal if and only if e is central in $\mathbb{C}G$ which holds if and only if L is a two sided ideal of $\mathbb{C}U$ and $g^{-1}eg = e$ holds for all $g \in G$. If any of these equivalent statements holds then e is uniquely given by the formula

$$e = \frac{1}{|U|} \sum_{u \in U} \chi(u^{-1})u.$$

So the condition $g^{-1}eg = e$ for all $g \in G$ is equivalent to χ being G-invariant. □

In view of Theorem 5.1.7, it is particularly important to recognize non-ideal characters. The following simple observation already has strong consequences.

Lemma 5.3.3. *Let χ be a non-ideal character of a subgroup $U \leq G$. Then χ^G is a non-ideal character as well.*

Proof. Let ρ be the regular character of G, and let ρ' be the regular character of U. By definition, χ is a left ideal character, and any irreducible character of U occurs as a constituent of $\rho' - \chi$. By Frobenius reciprocity, we have

$$\langle \rho - \chi^G, \psi \rangle = \langle (\rho' - \chi)^G, \psi \rangle = \langle \rho' - \chi, \psi_{|U} \rangle > 0,$$

for all $\psi \in \mathrm{Irr}(G)$. So any irreducible character of G is a constituent of $\rho - \chi^G$. It follows that χ^G is a non-ideal character. □

In combination with Theorem 5.1.7, Lemma 5.3.3 is a powerful tool to construct (weakly) generically closed characters. In the next chapter, we classify all finite groups isomorphic to affine symmetry groups of orbit polytopes (that is, those groups having generically closed $\mathbb{R}G$-modules). At this point, we can already identify a very large class of such groups.

Example 5.3.4. Let G be a finite group containing two non-commuting involutions. Then G is isomorphic to the affine symmetry group of an orbit polytope.

Proof. The subgroup $U = \langle x, y \rangle$ generated by non-commuting involutions $x, y \in G$ is a non-commutative dihedral group, which has a faithful irreducible character χ afforded by an $\mathbb{R}U$-module (given by rotations and reflections on the Euclidean plane). By Lemma 5.3.3, χ^G is a faithful non-ideal character afforded by an $\mathbb{R}G$-module. By Theorem 5.1.7, χ^G is generically closed. So by Theorem 3.9.6, G is isomorphic to the affine symmetry group of an orbit polytope. □

We next consider the induction $(1_U)^G$ of the trivial character 1_U of a subgroup $U \le G$ which is actually the permutation character of G acting on the left cosets of U. It turns out that its ideal constituent is also a very specific permutation character.

Lemma 5.3.5. *Let $U \le G$ be any subgroup, and let $\chi = (1_U)^G$. Then the ideal constituent of χ is $\chi_{\mathcal{I}} = (1_N)^G$, where $N = \langle U^g : g \in G \rangle$ is the normal subgroup of G generated by U. Moreover, if $U \lneq N$ then we have* $\mathrm{Ker}(\chi_{\mathcal{N}}) = \bigcap_{g\in G} U^g$.

Proof. Let $\psi \in \mathrm{Irr}(G)$ be any irreducible character. Then, by Frobenius reciprocity, ψ is a constituent of $\chi_{\mathcal{I}}$ if and only if $\psi(1) = \langle \chi, \psi \rangle = \langle 1_U, \psi_{|U} \rangle$. This in turn is equivalent to $\psi_{|U} = \psi(1)1_U$. So $\chi_{\mathcal{I}}$ has exactly those irreducible constituents $\psi \in \mathrm{Irr}(G)$ for which $U \subseteq \mathrm{Ker}(\psi)$, or equivalently, $N \subseteq \mathrm{Ker}(\psi)$ holds (each constituent occurring with multiplicity $\psi(1)$). Hence, $\chi_{\mathcal{I}}$ is exactly the regular character of G/N, regarded as character of G. That is, we have $\chi_{\mathcal{I}}(g) = |G : N|$ for all $g \in N$, and $\chi_{\mathcal{I}}(h) = 0$ for all $h \in G \setminus N$. These values coincide with those of the induced character $(1_N)^G$, so we have $\chi_{\mathcal{I}} = (1_N)^G$. We finally compute

$$\begin{aligned}\mathrm{Ker}(\chi_{\mathcal{N}}) &= \mathrm{Ker}(\chi - \chi_{\mathcal{I}}) = \mathrm{Ker}(((1_U)^N - 1_N)^G) = \bigcap_{g\in G} \mathrm{Ker}((1_U)^N - 1_N)^g \\ &= \bigcap_{g\in G} \mathrm{Ker}((1_U)^N)^g = \bigcap_{g\in G} \left(\bigcap_{h\in N} \mathrm{Ker}(1_U)^h \right)^g = \bigcap_{g\in G} U^g.\end{aligned}$$

□

Most importantly, Lemma 5.3.5 shows that for any subgroup $U \leq G$ not normal in G there is a non-ideal character χ of G afforded by a $\mathbb{Q}G$-module such that $\mathrm{Ker}(\chi)$ is the core of U in G.

The last result of this section considers character inductions from a normal subgroup N of G. We will see that the ideal constituent of an induced left ideal character can always be identified in that case. Before proving the following lemma, we recall some standard facts from Clifford theory.

Let χ be a character of a normal subgroup $N \trianglelefteq G$, and let $g \in G$ be any element. Then there is a *conjugated character* χ^g of N which is given by

$$\chi^g(x) = \chi(gxg^{-1}) \text{ for all } x \in N.$$

In that way, G acts on the (irreducible) characters of N. A character χ of N is said to be G-invariant if $\chi^g = \chi$ holds for all $g \in G$. In that case, G permutes the (irreducible) constituents of χ. So the irreducible constituents of N are partitioned into orbits, where all constituents of any orbit occur with the same multiplicity in χ. The stabilizer of some character χ of N in G (that is, the largest subgroup $N \leq I \leq G$ such that χ is I-invariant) is called the *inertia subgroup* of χ. It is usually denoted by

$$I_G(\chi) = \{g \in G : \chi^g = \chi\}.$$

One of the main theorems of Clifford theory states that if $\psi \in \mathrm{Irr}(G)$ is an irreducible character of G then the irreducible constituents of the restriction $\psi_{|N}$ (being a G-invariant character) fall into one single G-orbit. That is, for any irreducible character $\psi \in \mathrm{Irr}(G)$ there is an irreducible character $\chi \in \mathrm{Irr}(N)$ and a nonnegative integer $e \in \mathbb{Z}$ such that

$$\psi_{|N} = e(\chi^{g_1} + \cdots + \chi^{g_t}),$$

where $\{g_1, \ldots, g_t\}$ is any set of right coset representatives of $I_G(\chi)$ in G. A second main theorem of Clifford theory implies that ψ is induced by a certain irreducible character η of $I_G(\chi)$ such that χ is a constituent of $\eta_{|N}$.

We finally note that any character χ of a normal subgroup $N \trianglelefteq G$ has a unique maximal G-invariant constituent. It is given by the formula

$$\sum_{\psi \in \mathrm{Irr}(N)} k_\psi \psi,$$

with multiplicities $k_\psi = \min\{\langle \chi, \psi^g \rangle : g \in G\}$ (which could possibly be zero).

Lemma 5.3.6. *Let $N \trianglelefteq G$ be a normal subgroup, and let χ be a left ideal character of N. If ψ denotes the maximal G-invariant constituent of $\chi_{\mathcal{I}}$ then ψ^G is the ideal constituent of χ^G.*

Proof. First of all, we easily see that ψ is an ideal character of N since the multiplicity of any irreducible character $\tau \in \mathrm{Irr}(N)$ in ψ satisfies

$$\langle \psi, \tau \rangle = \min\{\langle \chi_I, \tau^g \rangle : g \in G\} \in \{0, \tau(1)\}.$$

Since ψ is G-invariant by definition, it follows by Lemma 5.3.2 that ψ^G is an ideal character of G.

It remains to show that the character $\chi^G - \psi^G$ of G is a non-ideal character. Let $\tau \in \mathrm{Irr}(G)$ be any irreducible constituent of $\chi^G - \psi^G$. Its restriction to N decomposes as

$$\tau_{|N} = k_1\eta_1 + \cdots + k_t\eta_t,$$

into distince irreducible characters $\eta_i \in \mathrm{Irr}(N)$ with nonnegative multiplicities $k_i \in \mathbb{Z}$. Since $\tau_{|N}$ is G-invariant, G permutes the characters η_i by conjugation. Since (by construction) the character $\chi - \psi$ has no G-invariant ideal constituent, at least one of the η_i occurs with a multiplicity less than $\eta_i(1)$ as a constituent of $\chi - \psi$. So by Frobenius reciprocity, we have

$$0 < \langle \chi^G - \psi^G, \tau \rangle = \langle \chi - \psi, \tau_{|N} \rangle = \sum_{i=1}^{t} k_i \langle \chi - \psi, \eta_i \rangle < \sum_{i=1}^{t} k_i \eta_i(1) = \tau(1).$$

Since τ was an arbitrary irreducible constituent of $\chi^G - \psi^G$, we see that $\chi^G - \psi^G$ is a non-ideal character. □

6 Generically closed modules over the real and complex numbers

In this chapter, we classify all finite groups which are isomorphic to the affine symmetry group of an orbit polytope (Theorem 6.4.4). Thereby, we answer an old question of Babai who answered the analogous question on the Euclidean symmetry groups of vertex transitive polytopes (we reprove Babai's result later in Theorem 7.2.2). The proof of our classification proceeds in several steps. Note that by Theorem 3.9.6, we already know that a finite group G is isomorphic to the affine symmetry group of an orbit polytope if and only if there is a generically closed $\mathbb{R}G$-module. We begin by classifying all finite groups G admitting a faithful non-ideal $\mathbb{R}G$-module (Theorem 6.2.3) which is automatically generically closed by the generalized Isaacs' Theorem. The remaining finite groups fall into four families. These are the abelian groups, the generalized dicyclic groups, and the groups of the form $Q_8 \times C_4 \times C_2^r$ and $Q_8 \times Q_8 \times C_2^r$ for any nonnegative integer r. The generalized dicyclic groups are easily excluded either by using Babai's classification or by a simple application of our methods (Lemma 6.4.1). While it is easy to see that abelian groups of exponent greater than two never have generically closed $\mathbb{R}G$-modules, it is a challenging combinatorial task to construct generically closed modules for abelian groups of exponent two. We use a graph theoretic approach to show that the group $G = C_2^r$ has a generically closed $\mathbb{R}G$-module if and only if $r \notin \{2, 3, 4\}$ (Theorem 6.3.8). The classification is finished by the Lemmas 6.4.2 and 6.4.3 which construct characters of generically closed $\mathbb{R}G$-modules for all groups of the form $G = Q_8 \times C_4 \times C_2^r$ or $G = Q_8 \times Q_8 \times C_2^r$.

The results of the present chapter have been published, distributed among the papers [9], [10], and [19]. The classification of all finite groups G admitting a faithful non-ideal $\mathbb{R}G$-module (Theorem 6.2.3) is originally due to Ladisch. The result presented here is slightly improved by a new, purely group theoretical, characterization of those groups. We also give a new simplified proof. Ladisch also classified the finite groups G admitting a faithful non-ideal $\mathbb{Q}G$-module, which leads to a classification of all finite groups isomorphic to the affine symmetry group of an orbit polytope with integral vertices [19]. This result however, is not presented here.

6.1 Groups G with generically closed $\mathbb{C}G$-modules

Before we restrict our attention to characters afforded by $\mathbb{R}G$-modules, we briefly discuss the general question of which finite groups have generically closed characters (of $\mathbb{C}G$-modules). Surprisingly, the answer is particularly simple in the case of non-abelian groups. The following result essentially relies on the well known facts that a finite group G is abelian if and only if all irreducible characters of G are linear, and that the multiplication with any linear character of G permutes the irreducible characters of G. The next result is equivalent to Lemma 3.2 in [19].

Theorem 6.1.1. *Let G be a non-abelian finite group. Then G has a faithful non-ideal character. In particular, G has generically closed characters.*

Proof. Let χ be the sum of all irreducible characters of G which are not linear. Since G is non-abelian, χ is nonzero. The ideal constituent of χ is trivial by definition. We claim that χ is faithful (then we are done by Theorem 5.1.7).

Suppose there is a non-identity element $1 \neq g \in \mathrm{Ker}(\chi)$. Since the regular character of G is faithful, there must be an irreducible character $\lambda \in \mathrm{Irr}(G)$ such that $g \notin \mathrm{Ker}(\lambda)$. By definition of χ, the character λ must in fact be linear. But then we have $\lambda\chi = \chi$, and hence $g \notin \mathrm{Ker}(\lambda\chi) = \mathrm{Ker}(\chi)$. This is a contradiction. □

The question of which finite abelian groups have generically closed characters is much more challenging (as they have no non-ideal characters at all). Of course, any cyclic group has a faithful linear character which is generically closed by Proposition 3.8.8. For abelian groups of exponent two, the question will be fully answered later in this chapter through the application of graph theory. For non-cyclic abelian groups of exponent greater than two it seems to be generally open whether there exist generically closed characters. At least, we know that such characters cannot be real valued by Corollary 5.1.11. So these cases become irrelevant when restricting the attention to characters of $\mathbb{R}G$-modules.

6.2 Groups G with faithful non-ideal $\mathbb{R}G$-modules

In this section, we classify all finite groups G admitting a faithful non-ideal $\mathbb{R}G$-module. The idea is very similar to the proof of Theorem 6.1.1. If G is any finite group, we can easily construct a non-ideal character of G afforded by an $\mathbb{R}G$-module whose kernel is as small as possible. More precisely, we may define a character χ to be the sum of the characters of all simple non-ideal $\mathbb{R}G$-modules. However, in contrast to the situation in Theorem 6.1.1, χ may have a nontrivial kernel even if G is non-abelian. (For example, all left ideals of $\mathbb{R}Q_8$ are two sided ideals, where Q_8 is the quaternion group of order 8. In that case, χ is just the zero character.) The kernel of χ can also be defined in the following way.

Definition 6.2.1. Let G be a finite group. The *non-ideal kernel* of G is defined by

$$\mathrm{NKer}(G) = \bigcap_{\chi} \mathrm{Ker}(\chi),$$

where χ runs over all non-ideal characters of G afforded by (simple) $\mathbb{R}G$-modules. If G has no such characters, we set $\mathrm{NKer}(G) = G$.

By definition of the non-ideal kernel, a finite group G satisfies $\mathrm{NKer}(G) = 1$ if and only if G admits a faithful non-ideal $\mathbb{R}G$-module (which is generically closed by

Theorem 4.5.4). In the following, we classify the exceptional finite groups G for which $\mathrm{NKer}(G)$ is nontrivial.

In the proof of the following Theorem 6.2.3, we frequently need to know whether an irreducible character of G is afforded by an $\mathbb{R}G$-module. A very useful tool for recognizing such characters is the *Frobenius-Schur indicator* (see [17, Ch. 4] for further reference). For any character χ of G the Frobenius-Schur indicator $\iota\chi \in \mathbb{C}$ is defined by

$$\iota\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

If χ is irreducible then we have $\iota\chi \in \{-1, 0, 1\}$, and these values can be interpreted in the following way. If $\iota\chi = 1$ then χ is afforded by an absolutely simple $\mathbb{R}G$-module. If $\iota\chi = 0$ then χ is not real valued, and consequently not afforded by an $\mathbb{R}G$-module. In that case, the character $\chi + \overline{\chi}$ is afforded by a simple $\mathbb{R}G$-module. Finally, if $\iota\chi = -1$ then χ is real valued, but not afforded by an $\mathbb{R}G$-module either. In that case, 2χ is afforded by a simple $\mathbb{R}G$-module.

If $G = A \times B$ is a direct product of two (necessarily normal) subgroups A, B then we have a canonical bijection $\mathrm{Irr}(G) = \mathrm{Irr}(A) \times \mathrm{Irr}(B)$. More precisely, if $\alpha \in \mathrm{Irr}(A)$ and $\beta \in \mathrm{Irr}(B)$ are irreducible characters, then there is an irreducible character $\alpha \times \beta \in \mathrm{Irr}(G)$ sending a product $a \cdot b$ to $\alpha(a)\beta(b)$ for all $a \in A$, $b \in B$. Any irreducible character of G arises uniquely in that way. It is easily seen that the Frobenius-Schur indicator of such characters evaluates to $\iota(\alpha \times \beta) = \iota\alpha \cdot \iota\beta$.

According to Babai, we call a finite group G *generalized dicyclic* if there is a normal abelian subgroup $A \leq G$ of index two in G such that some (and hence every) element $g \in G \setminus A$ has order four, and acts on A by inverting elements. We need the following facts about the irreducible characters of generalized dicyclic groups, which are easily proven by Clifford theory (see the discussion before Lemma 5.3.6).

Lemma 6.2.2. *Let $G = A\langle g \rangle$ be a generalized dicyclic group, where A is of index two in G, and where g is an element of order four acting as the inversion on A. Let $\chi \in \mathrm{Irr}(G)$ be any irreducible character with $g^2 \notin \mathrm{Ker}(\chi)$.*

(1) If χ is linear then χ is not real valued, and the character $\chi + \overline{\chi}$ is zero on $G \setminus A$.

(2) If χ is non-linear then χ is a real valued character of degree two. Furthermore, χ is zero on $G \setminus A$, and we have $\chi(h^2) = \chi(h)^2 - 2$ for all $h \in G$. Its Frobenius-Schur indicator is $\iota\chi = -1$.

Proof. Suppose that χ is linear, and let $h \in G \setminus A$ be arbitrary. Then we have $h = ga$ for some $a \in A$, and hence $h^2 = (ga)^2 = g^2 a^g a = g^2$. Since $\chi(h^2) = \chi(g)^2 \neq 1$, we have $\chi(h) = \pm i$ (in particular, χ is not real valued), and hence $\chi(h) + \overline{\chi(h)} = 0$.

Now suppose that χ is non-linear, and let $\lambda \in \mathrm{Irr}(A)$ be an irreducible constituent of $\chi_{|A}$. By Clifford theory, we have $\chi_{|A} = \lambda + \lambda^g = \lambda + \overline{\lambda}$. In particular, we have $\chi(1) = 2$, $\chi(g^2) = -2$, and $\chi(a^2) = \chi(a)^2 - 2$ for all $a \in A$. Furthermore, we easily see that $I_G(\lambda) = A$, so $\chi = \lambda^G$ is an induced character which clearly vanishes outside A. As before, any element $h \in G \setminus A$ squares to g^2. So we have $\chi(h^2) = \chi(g^2) = -2 = \chi(h)^2 - 2$ for all $h \in G \setminus A$. Since any element of A is conjugated to its inverse in G, and since χ vanishes outside A, we get $\chi = \overline{\chi}$. Finally, we compute

$$\iota\chi = \frac{1}{|G|} \sum_{h \in G} \chi(h^2) = \frac{1}{|G|} \sum_{h \in G} \chi(h)^2 - 2 = \langle \chi, \overline{\chi} \rangle - 2 = -1.$$

□

We are ready to classify all finite groups G admitting faithful non-ideal $\mathbb{R}G$-modules (or equivalently, all finite groups G with $\mathrm{NKer}(G) = 1$). Note that the equivalence (1) $\iff$ (4) was originally proven by Ladisch using the classification of the so called *Blackburn groups* (which in turn relies on the well known classification of all *Dedekind groups*) [19]. By a careful analysis of that proof, it was possible to extract a new intermediate characterization (3) of the groups G admitting a faithful non-ideal $\mathbb{R}G$-module, which is of purely group theoretical nature. We prove (1) $\implies$ (3) and (4) $\implies$ (1) by using the methods we developed so far. The implication (3) $\implies$ (4) is proven just by elementary group theory. In particular, the proof of Theorem 6.2.3 does neither rely on Blackburn's classification, nor on Dedekind's classification.

In the following, it turns out to be important to recognize which cyclic subgroups of the given group G are normal. For simplicity, we call an element $g \in G$ *normal* if the cyclic subgroup $\langle g \rangle$ generated by g is a normal subgroup of G. The other elements of G are called *non-normal*.

Theorem 6.2.3. *Let G a nontrivial finite group. The following statements are equivalent:*

(1) $\mathrm{NKer}(G) > 1$.

(2) $\bigcap_{\psi} \mathrm{Ker}((\psi^G)_{\mathcal{N}}) > 1$, *where ψ runs over all characters afforded by simple $\mathbb{R}U$-modules for cyclic subgroups $U \leq G$.*

(3) All normal elements $g \in G$ satisfy $g^G \subseteq \{g, g^{-1}\}$. All non-normal elements of G have order four, and all these elements have the same square.

(4) G belongs to any of the following four families:

- *G is abelian,*
- *G is generalized dicyclic,*
- *$G \cong Q_8 \times C_4 \times C_2^r$ for some $r \geq 0$, or*
- *$G \cong Q_8 \times Q_8 \times C_2^r$ for some $r \geq 0$.*

Proof. We begin by proving the implications (1) $\implies$ (2) $\implies$ (3) and (4) $\implies$ (1). The proof of the remaining part, (3) $\implies$ (4), is split into several lemmas afterwards.

Of course the direction (1) $\implies$ (2) is trivial by definition. For proving the implication (2) $\implies$ (3), we set $K = \bigcap_{\psi} \mathrm{Ker}((\psi^G)_{\mathcal{N}})$, where ψ runs over the characters of all simple

$\mathbb{R}U$-modules for cyclic subgroups $U \leq G$. Let $h \in G$ be any non-normal element. We consider the permutation character $\chi = (1_{\langle h \rangle})^G$. By Lemma 5.3.5, the kernel of $\chi_{\mathcal{N}}$ is strictly contained in $\langle h \rangle$, so we have $K \subsetneq \langle h \rangle$. In particular, we have $o(h) > 2$. We now consider the character $\psi = \lambda + \overline{\lambda}$, where $\lambda \in \mathrm{Irr}(\langle h \rangle)$ is a faithful linear character. By the previous discussion, ψ is afforded by a simple $\mathbb{R}\langle h \rangle$-module (it is actually the character of the usual representation of the cyclic group $\langle h \rangle$ acting on the Euclidean plane, where h acts as a rotation of order $o(h)$). Let τ be any irreducible constituent of ψ^G. By Frobenius reciprocity, we have

$$0 < \langle \psi^G, \tau \rangle = \langle \psi, \tau_{|\langle h \rangle} \rangle = \langle \lambda, \tau_{|\langle h \rangle} \rangle + \langle \overline{\lambda}, \tau_{|\langle h \rangle} \rangle,$$

so $\tau_{|\langle h \rangle}$ has a faithful linear constituent. In particular, we have $\mathrm{Ker}(\tau) \cap \langle h \rangle = 1$, and hence $K \not\subseteq \mathrm{Ker}(\tau)$. By definition of K, it follows that τ is actually a constituent of $(\psi^G)_{\mathcal{I}}$. Since τ was chosen arbitrarily, ψ^G must be an ideal character. By Lemma 5.3.2, it follows that ψ is G-invariant. Since h is non-normal, this implies $\psi(h) = 0$, and hence $o(h) = 4$. Since K is a nontrivial proper subgroup of $\langle h \rangle$, we conclude $K = \langle h^2 \rangle$. Since h was arbitrary, we see that all non-normal elements of G have the same square.

Now let $g \in G$ be a normal element. If $g^2 = 1$ then g is central, and there is nothing to prove. Suppose that $o(g) > 2$. As before, we consider the character $\psi = \lambda + \overline{\lambda}$, where $\lambda \in \mathrm{Irr}(\langle g \rangle)$ is faithful. Then ψ is an ideal character of the normal subgroup $\langle g \rangle \trianglelefteq G$. Since λ is G-invariant if and only if $\overline{\lambda}$ is G-invariant, the maximal G-invariant constituent of ψ is either 0 or ψ. So by Lemma 5.3.6, ψ^G is either an ideal character or a non-ideal character, depending on whether ψ is G-invariant or not. Since $\mathrm{Ker}(\psi^G) = 1$ does not contain K, we conclude that ψ^G is an ideal character, and that ψ is G-invariant. By definition of ψ, we have $\psi(x) = \psi(y)$ for some $x, y \in \langle g \rangle$ if and only if $y \in \{x, x^{-1}\}$. From $\psi(g) = \psi(g^h)$ for all $h \in G$, we conclude $g^G \subseteq \{g, g^{-1}\}$.

Next, we prove (4) $\implies$ (1). If G is abelian then every left ideal character of G is an ideal character, so $\mathrm{NKer}(G) = G > 1$.

Let G be generalized dicyclic. Let $A \leq G$ be an abelian normal subgroup of index two, and let $g \in G \setminus A$ be an element of order four, acting on A by inverting elements. We claim that $g^2 \in \mathrm{NKer}(G)$. Indeed, if $\chi \in \mathrm{Irr}(G)$ is any non-linear irreducible character with $g^2 \notin \mathrm{Ker}(\chi)$ then, by Lemma 6.2.2, χ has degree two, and 2χ is the unique character afforded by a simple $\mathbb{R}G$-module having χ as a constituent. But 2χ is an ideal character. By contraposition, g^2 lies in the kernel of all non-ideal characters afforded by (simple) $\mathbb{R}G$-modules. That is, $g^2 \in \mathrm{NKer}(G)$.

Let $G = \langle i, j \rangle \times \langle g \rangle \times H$, where $\langle i, j \rangle \cong Q_8$, $\langle g \rangle \cong C_4$, and $H \cong C_2^r$. We claim that $(ig)^2 \in \mathrm{NKer}(G)$. Let $\chi \in \mathrm{Irr}(G)$ be non-linear with $(ig)^2 \notin \mathrm{Ker}(\chi)$, say $\chi = \alpha \times \beta \times \gamma$, where $\alpha \in \mathrm{Irr}(\langle i, j \rangle)$, $\beta \in \mathrm{Irr}(\langle g \rangle)$, and $\gamma \in \mathrm{Irr}(H)$. Since χ is non-linear, α has to be the quaternionic character of degree two, and hence $\chi(1) = 2$. Since $\chi((ig)^2) \neq 2$ and $\alpha(i^2) = -2$, it follows $\beta(g^2) = 1$, and hence $\iota\beta = 1$. We compute $\iota\chi = \iota\alpha \cdot \iota\beta \cdot \iota\gamma = -1$. So the unique character of a simple $\mathbb{R}G$-module having χ as a constituent is 2χ, which is clearly an ideal character. Hence, $(ig)^2 \in \mathrm{NKer}(G)$.

Finally, let $G = \langle i, j \rangle \times \langle i', j' \rangle \times H$, where $\langle i, j \rangle, \langle i', j' \rangle \cong Q_8$, and $H \cong C_2^r$. We claim that $(ii')^2 \in \mathrm{NKer}(G)$. Let $\chi \in \mathrm{Irr}(G)$ be non-linear with $(ii')^2 \notin \mathrm{Ker}(\chi)$, say $\chi = \alpha \times \beta \times \gamma$, where $\alpha \in \mathrm{Irr}(\langle i, j\rangle)$, $\beta \in \mathrm{Irr}(\langle i', j'\rangle)$, and $\gamma \in \mathrm{Irr}(H)$. Since χ is non-linear, one of α or β must be the quaternionic character of degree two. Since $(ii')^2 \notin \mathrm{Ker}(\chi)$, one of α or β must be linear. Hence, $\chi(1) = 2$, and $\iota\chi = \iota\alpha \cdot \iota\beta \cdot \iota\gamma = -1$. As before, it follows that the unique character of a simple $\mathbb{R}G$-module having χ as a constituent is an ideal character. Consequently, $(ii')^2 \in \mathrm{NKer}(G)$.

The direction (3) $\Longrightarrow$ (4) will be handled in the rest of this section. □

From now on let G be any finite group satisfying (3) of Theorem 6.2.3. That is, any normal element $g \in G$ satisfies $g^G \subseteq \{g, g^{-1}\}$, and all non-normal elements of G (if there are any) have the same square, which is a (necessarily central) involution. We have to show that G is isomorphic to a group listed in (4).

As usual in group theory, we denote the *commutator* of two elements $g, h \in G$ by $[g, h] = g^{-1}h^{-1}gh$. By definition, g and h commute if and only if $[g, h] = 1$, and there are the obvious calculation rules $hg[g, h] = gh$ and $[g, h][h, g] = 1$. If the commutator $[g, h]$ commutes with both g and h, we obtain from these elementary observations the very useful equation $(gh)^n = g^n h^n [h, g]^{\binom{n}{2}}$ for all non-negative integers n. Moreover, there are well known (and straightforward to verify) equations

$$[gh, x] = [g, x]^h \cdot [h, x] \text{ for all } g, h, x \in G.$$

In particular (setting $g = h$), if $g, x \in G$ are elements such that g commutes with $[g, x]$ then we have $[g, x]^n = [g^n, x]$ for all nonnegative integers n.

Lemma 6.2.4. *If all normal elements of G are central then G is abelian.*

Proof. Let $Z = Z(G)$ be the center of G which contains all normal elements of G by the hypothesis. Then all elements outside Z (being non-normal) have the same square which is a central involution. For a proof by contradiction, we assume that G is non-abelian. Then G/Z is an abelian group of exponent two. Let $h \in G \setminus Z$ be arbitrary. For all elements $g \in G$ with $g \in Z$ or $g \in hZ$ we have $h^g = h$. If $g \in G \setminus Z$ is such that $gZ \neq hZ$ then the three elements g, h, and gh are all outside of Z, so they all have order four, and they all have the same square $z \in Z$. Furthermore, since G/Z is abelian, we have $[h, g] \in Z$. We conclude

$$h^2 = z = (gh)^2 = g^2h^2[h, g] = z^2[h, g] = [h, g],$$

which implies $h^g = h^{-1}$. So we see that h is normal in G but not central, which contradicts the hypothesis. □

From now on, we suppose that G is non-ablian. We fix some element $x \in G$ such that $o(x) > 2$ and $x^G = \{x, x^{-1}\}$ (which exists by Lemma 6.2.4). Then $N = C_G(x)$ is a normal subgroup of index two in G.

Lemma 6.2.5. *For all $g \in G \setminus N$ we have $o(g) = 4$. If an element $g \in G \setminus N$ is normal in G then $\langle g, x\rangle$ is isomorphic to the quaternion group Q_8.*

Proof. Of course we have $o(g) = 4$ for all non-normal elements $g \in G$. If $g \in G \setminus N$ is normal then we have both $x^g = x^{-1}$ and $g^x = g^{-1}$. Thereby, we get equations $g^2 = [x, g] = x^{-2}$, which show in particular that g^2 commutes with x, x^2 commutes with g, and both g and x commute with $[x, g]$. So $g^4 = [x, g]^2 = [x^2, g] = 1$, and analogously, $x^4 = [g, x]^2 = [g^2, x] = 1$. As a product of two cyclic normal subgroups of order four with nontrivial intersection, we see that $\langle g, x\rangle$ is the quaternion group of order eight. □

Lemma 6.2.6. *If all elements in $G \setminus N$ are non-normal then G is generalized dicyclic.*

Proof. Let $g \in G \setminus N$ be fixed. For all $y \in N$, we have $gy \notin N$, so gy is non-normal, and we have $g^2 = (gy)^2 = g^2 y^g y$. It follows $y^g = y^{-1}$. In particular, N must be abelian. □

For any group H, we use H^2 to denote $\langle h^2 : h \in H\rangle$, the subgroup generated by all squares of H. This soubgroup is normal (even characteristic) in H, and the quotient H/H^2 is an abelian group of exponent less or equal than two.

Lemma 6.2.7. *If some element $g \in G \setminus N$ is normal in G then there is a subgroup $H \leq N$ such that $G = \langle g, x\rangle \times H$, all elements of H are normal in G, and $|H^2| \leq 2$.*

Proof. Let $Q = \langle g, x\rangle$ which is the quaternion group by Lemma 6.2.5. Being generated by normal elements, Q is a normal subgroup of G. We consider the centralizer $C = C_G(Q) = C_N(g)$ which is (being the centralizer of a normal subgroup) also normal in G. It is easy to see that $Q \cap C = \langle g^2\rangle$. Since G acts on Q by inner automorphisms of Q, we also have $G = QC$. We claim that all elements of C are normal in G, that $|C^2| \leq 2$, and that g^2 is not a square in C.

Let $h \in C$ be arbitrary. Then $gh \notin N$, so $o(gh) = 4$ by Lemma 6.2.5, and hence $h^4 = 1$. So the exponent of C divides four. If gh is normal in G for some $h \in C$ then $g^3h^3 = (gh)^x = g^{-1}h$, and hence $h^2 = 1$. By contraposition, we see that for all elements $h \in C$ of order four the product gh is non-normal. So $o(gh) = 4$, and hence $g^2 \neq h^2$. This shows that g^2 is not a square in C. If $h_1, h_2 \in C$ are both of order four, then $(gh_1)^2 = (gh_2)^2$, and hence $h_1^2 = h_2^2$, proving $|C^2| \leq 2$. Finally, if some element $h \in C$ would be non-normal in G then we would have $o(h) = 4$, so (since gh also is non-normal in that case, as shown before) $h^2 = (gh)^2 = g^2h^2$, and hence $g^2 = 1$. This contradiction shows that all elements of C are normal in G.

To finish the proof, we show that $\langle g^2\rangle \leq C$ has a complement H in C. As we have just seen, we have $g^2 \notin C^2$. So, as C/C^2 is elementary abelian, there is a complement H/C^2 of the nontrivial subgroup $\langle g^2\rangle C^2/C^2$ in C/C^2. Then H is a complement of $\langle g^2\rangle$ in C, and hence a complement of Q in G. Being a subgroup of C, H also commutes with Q, so we get $G = Q \times H$. It is clear that all elements of H are normal in G and that $|H^2| \leq 2$ holds, since the same even holds for C. □

Continuation of the proof of Theorem 6.2.3. We finally prove the direction (3) $\Longrightarrow$ (4). If G is not abelian, and not generalized dicyclic, then by Lemma 6.2.5 and

Lemma 6.2.7 we have $G = Q \times H$, where Q is the quaternion group of order eight, and H consists of normal elements of orders dividing four, where any two elements of order four have the same square. If H is abelian, then we either have $H \cong C_2^r$, or $H \cong C_4 \times C_2^r$ for some $r \geq 0$. In the first case G is generalized dicyclic, in the second case we have $G \cong Q_8 \times C_4 \times C_2^r$.

If H is not abelian, then we apply Lemma 6.2.5 and Lemma 6.2.7 to H instead of G to obtain $H = W \times U$, where W is the quaternion group of order eight, and U is a certain complement of W. Since all elements of H have an order dividing four, and all elements of order four have the same square, U must be an elementary abelian 2-group. It follows $G \cong Q_8 \times Q_8 \times C_2^r$ for some $r \geq 0$. □

6.3 Generically closed $\mathbb{R}G$-modules of abelian groups

As already mentioned before, the $\mathbb{R}G$-modules of abelian groups of exponent greater than two are never generically closed since the inversion of group elements is always a generic symmetry by Corollary 5.1.11. The objective of this section is to classify which abelian groups of exponent two have generically closed characters. (Note that all characters of elementary abelian 2-groups are afforded by $\mathbb{R}G$-modules since their linear characters obviously are.)

Recall that the generic symmetry group of a character χ always coincides with the generic symmetry group of its left ideal constituent (Proposition 5.1.6), and that any left ideal character of an abelian group is an ideal character (the group algebra being commutative). So we may restrict our attention to ideal characters which we characterize in the following. It is convenient to regard any finite elementary abelian 2-group G as a vector space over $\mathbb{F}_2$, the field with two elements. As such, G is isomorphic to $\mathbb{F}_2^n$ for some $n \geq 0$. So it suffices to consider the concrete examples $\mathbb{F}_2^n$ (consisting of row vectors) which we regard both as additive groups, and as $\mathbb{F}_2$-spaces. The linear characters of $G = \mathbb{F}_2^n$ are uniquely described by their values (± 1) on the unit vectors. So the linear characters $\lambda_v \in \mathrm{Irr}(G)$ are in bijective correspondence to the vectors $v \in \mathbb{F}_2^n$, by

$$\lambda_v(x) = (-1)^{xv^t} \text{ for all } x \in G.$$

An arbitrary ideal character of degree m is the sum of m distinct linear characters. So the ideal characters χ_C of G of degree m are in bijective correspondence to the subsets $C \subseteq \mathbb{F}_2^n$ of size m. It is often convenient to regard such an m-subset $C \subseteq \mathbb{F}_2^n$ as a matrix $C \in \mathbb{F}_2^{n \times m}$ by regarding the elements of C as column vectors which appear in any order. By doing so, we see that any ideal character χ_C of G is given by the formula

$$\chi_C(x) = \sum_i (-1)^{xv_i} = m - 2\,\mathrm{wt}(xC) \text{ for all } x \in G,$$

where $\mathrm{wt}(y)$ denotes the *weight* of a vector y (that is, the number of its nonzero coordinates). In particular, we see that the kernel of χ_C is exactly the (left) kernel of the matrix C. So the faithful characters of G correspond to those matrices with linearly independent rows. By Theorem 5.1.8, a permutation $\pi \in \mathrm{Sym}(G)$ is a generic symmetry of the ideal character χ_C if and only if we have

$$\mathrm{wt}(\pi(x)C + \pi(y)C) = \mathrm{wt}(xC + yC) \text{ for all } x, y \in G.$$

Let $K = \mathrm{Ker}(\chi_C)$ be the (left) kernel of the matrix C. Then the right multiplication by C induces an isomorphism of the quotient group G/K and the row space V of C. So χ_C can be regarded as a faithful ideal character of V. Identifying G/K and V, we get that a permutation $\sigma \in \mathrm{Sym}(V)$ is a generic symmetry of χ_C if and only if

$$\mathrm{wt}(\sigma(x) + \sigma(y)) = \mathrm{wt}(x + y) \text{ for all } x, y \in V.$$

Recall that the generic symmetry group $\mathrm{Sym}(G, \chi_C)$ is a semidirect product

$$\mathrm{Sym}(G, \chi_C) \cong \mathrm{Iv}(G, \chi_C) \rtimes \mathrm{Sym}(V, \chi_C)$$

by Proposition 3.2.7, so we see that the row space of C actually contains the most relevant information on the generic symmetries of the character χ_C.

Using these observations, we will answer the question of which of the elementary abelian 2-groups of order up to 32 have generically closed characters. Concerning $\mathbb{F}_2$, the smallest groups among them, we see that $\mathbb{F}_2 = \mathrm{Sym}(\mathbb{F}_2)$. So in fact, all faithful characters of $\mathbb{F}_2$ are generically closed for trivial reasons. By a counting argument, it can be easily shown that the next three candidates do not have generically closed (ideal) characters.

Lemma 6.3.1. *Let G be an elementary abelian group of order $4, 8$, or 16. Then no character of G is generically closed.*

Proof. Without loss of generality, we may assume $G = \mathbb{F}_2^n$, where $n \in \{2, 3, 4\}$. Any ideal character χ_C of G of degree $1 \leq m \leq 2^n$ corresponds to an m-subset $C \subseteq \mathbb{F}_2^n$. There are $\binom{2^n}{m}$ such subsets. The group $\mathrm{GL}(n, 2)$ acts on those m-sets by left multiplications. Since $|\,\mathrm{GL}(n, 2)| = \prod_{i=0}^{n-1}(2^n - 2^i)$ is strictly larger than $\binom{2^n}{m}$ for the given values of n and m, there must be a non-identity matrix $A \in \mathrm{GL}(n, 2)$ such that $AC = C$. By the previous considerations, we see that the permutation $x \mapsto xA$ is a generic symmetry of χ_C (which is not a translation). So χ_C is not generically closed. $\square$

The elementary abelian group of order 32 actually has a generically closed character.

Example 6.3.2. We consider the following matrix $C \in \mathbb{F}_2^{5\times 12}$:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

The corresponding character χ_C of $\mathbb{F}_2^5$ is generically closed.

The following proof is elementary but relies on enumerating all vectors of a space with 32 elements and many calculations. It is recommended to use a computer algebra system for verification.

Proof. Let V be the column space of C. The rows of C obviously are linearly independent, so the character χ_C is faithful, and it suffices to show that any permutation $\pi \in \mathrm{Sym}(V)$ with $\pi(0) = 0$ and $\mathrm{wt}(\pi(x) + \pi(y)) = \mathrm{wt}(x + y)$ for all $x, y \in V$ must be the identity. We will frequently use the argument that if $p \in V$ is any fixed point of π and if $x, y \in V$ are in the same orbit under π then $x + p$ and $y + p$ must have the same weight. In particular (setting $p = 0$), all orbits of π must have some constant weight.

The nonzero vectors of V distribute into 1 vector of weight 3, 2 vectors of weight 4, 7 vectors of weight 5, 8 vectors of weight 6, 7 vectors of weight 7, 5 vectors of weight 5, and 1 vector of weight 9. Let v_3 be the unique vector of weight 3, and let v_9 be the unique vector of weight 9. By uniqueness, both v_3 and v_9 are fixed by π. Let $v_{4,1}, v_{4,2} \in V$ be the two vectors of weight 4. Then we calculate $\mathrm{wt}(v_{4,1} + v_3) \neq \mathrm{wt}(v_{4,2} + v_3)$ which shows that both $v_{4,1}$ and $v_{4,2}$ must be fixed by π. Now if $x, y \in V$ are arbitrary distinct vectors of the same weight $\mathrm{wt}(x) = \mathrm{wt}(y) \in \{5, 6, 7, 8\}$, we see that at least one of the inequalities

$$\begin{aligned}&\mathrm{wt}(x + v_3) \neq \mathrm{wt}(y + v_3), \mathrm{wt}(x + v_9) \neq \mathrm{wt}(y + v_9),\\ &\mathrm{wt}(x + v_{4,1}) \neq \mathrm{wt}(y + v_{4,1}), \text{ or } \mathrm{wt}(x + v_{4,2}) \neq \mathrm{wt}(y + v_{4,2})\end{aligned}$$

holds. So any two vectors of V lie in different orbits of π which shows that π is the identity. □

In the remainder of this section, we will show that all elementary abelian groups of order 2^n for $n \geq 6$ have generically closed characters. For simplification, we will restrict our attention to those ideal characters χ_C coming from matrices C, where each column has exactly two nonzero entries. These are precisely the incidence matrices of finite simple graphs, and in fact it turns out to be very convenient to use the graph theoretic language.

In the following, a graph is always understood as a finite undirected graph $\Gamma = (V, E)$ with vertex set V and edge set E without loops or multiple edges. That is, the edges $e \in E$ of Γ are 2-subsets $e = \{x, y\}$ of vertices $x, y \in V$. For keeping the notation simple, an edge $e = \{x, y\}$ is denoted by $e = xy$. We consider the power sets $\mathcal{P}(V)$ and $\mathcal{P}(E)$ as vector spaces over $\mathbb{F}_2$, where the vector addition is given by symmetric difference, that is, $A + B = (A \setminus B) \cup (B \setminus A)$. These spaces are of course canonically isomorphic to $\mathbb{F}_2^{(V)}$ and $\mathbb{F}_2^{(E)}$, respectively (any subset being identified with its characteristic vector). Let $C \in \mathbb{F}_2^{V \times E}$ be the incidence matrix of Γ, that is, $C = (c_{v,e})_{v \in V, e \in E}$ with entry $c_{v,e} = 1$ if $v \in e$ and $c_{v,e} = 0$ otherwise. The right multiplication by C corresponds to the linear map

$$\mathcal{P}(V) \to \mathcal{P}(E), \quad A \mapsto \{e \in E : |e \cap A| = 1\},$$

which sends a vertex set $A \subseteq V$ to the set of all edges connecting a vertex of A with a vertex of $V \setminus A$. We denote that linear map by the same symbol C, and we call the image of C in $\mathcal{P}(E)$ (which corresponds to the row space of the incidence matrix) the *cut space* of Γ. The cut space of Γ is denoted by $C\Gamma$, and its elements are called *cut sets*. Note that $C(A) = C(V \setminus A)$ for all subsets $A \subseteq V$, so the map C is never injective. We collect its rank and another simple fact we need in the following lemma.

Lemma 6.3.3. *Let $\Gamma = (V, E)$ be a graph.*

(1) The kernel of $C\colon \mathcal{P}(V) \to \mathcal{P}(E)$ is generated by the vertex sets of the connected components of Γ. Therefore, $C\Gamma$ is a $(|V| - t)$-dimensional subspace of $\mathcal{P}(E)$, where t is the number of those components.

(2) If Γ is connected then $C\Gamma$ has dimension $|V| - 1$.

(3) As a subgraph of Γ, any cut set is bipartite. In particular, all circles in a cut set are of even length.

Proof. A subset $A \subseteq V$ is in the kernel of C if and only if no edge of Γ leaves A. This is equivalent to A being a disjoint union of the connected components of Γ, which proves (1). Of course (2) is an immediate consequence of (1). Finally, if $C(A) \in C\Gamma$ is an arbitrary cut set then the disjoint union $A \sqcup (V \setminus A)$ is a bipartition of $C(A)$ as a subgraph of Γ, proving (3). □

We now proceed as follows. We consider some connected graph $\Gamma = (V, E)$ with n vertices and m edges, which has an associated $(n-1)$-dimensional $\mathbb{F}_2$-space $C\Gamma$. By the previous discussion, there is a faithful ideal character χ of $C\Gamma$ (corresponding to the incidence matrix of Γ) of degree m. Since the weight of a vector of $\mathbb{F}_2^{(E)}$ is just the cardinality of the corresponding subset of E, the values of χ are given by

$$\chi(S) = m - 2|S| \text{ for all } S \in C\Gamma.$$

We wish to find a graph theoretical condition on Γ ensuring that χ is generically closed. By Theorem 5.1.10, a generic symmetry of χ is a permutation $\pi \in \mathrm{Sym}(C\Gamma)$ such that $|S^\pi + T^\pi| = |S + T|$ (we use the exponential notation S^π instead of $\pi(S)$ here) for all cut sets $S, T \in C\Gamma$. Since we only want to know whether $\mathrm{Sym}(C\Gamma, \chi)$ is strictly larger than $C\Gamma$, we may restrict our attention to those generic symmetries fixing the identity $\emptyset \in C\Gamma$. For convenience, we introduce the following terminology.

Definition 6.3.4. Let Γ be a graph. A permutation $\pi \in \mathrm{Sym}(C\Gamma)$ is called a *cut symmetry* of Γ if $\emptyset^\pi = \emptyset$, and $|S^\pi + T^\pi| = |S + T|$ for all $S, T \in C\Gamma$.

By the previous discussion, the character χ associated to (the incidence matrix of) a graph Γ is a generically closed character of the cut space $C\Gamma$ if and only if Γ has only the trivial cut symmetry. The following simple characterization of cut symmetries will be frequently used.

Lemma 6.3.5. *Let Γ be a graph. A permutation $\pi \in \mathrm{Sym}(C\Gamma)$ is a cut symmetry of Γ if and only if*

(1) $|S^\sigma| = |S|$, *and*

(2) $|S^\sigma \cap T^\sigma| = |S \cap T|$

holds for all cut sets $S, T \in C\Gamma$.

Proof. This is an immediate consequence of the equation $|S+T| = |S| + |T| - |S \cap T|$ which actually holds for arbitrary finite sets S, T. □

Let π be a graph automorphism of a graph Γ (that is, a permutation of the vertices which also permutes the edges of Γ). Then π induces a cut symmetry σ of Γ by setting $C(A)^\sigma = C(A^\pi)$. The cut symmetries obtained in that way are special as they permute the cut sets of the form $C(\{v\})$ for vertices v of Γ. We will call the cut sets given by single vertices *principal cut sets*, and we will denote them by $C(v)$ for short. In general, not every cut symmetry of a graph permutes its principal cut sets. For example if $\Gamma = (V, E)$ is a tree then $C\Gamma$ is the entire power set $\mathcal{P}(E)$. Thus each permutation of the edges leads to a cut symmetry, whereas of course not every permutation of edges have to permute the principal cut sets.

It is also worth noting that not every cut symmetry permuting the principal cut sets in $C\Gamma$ must be induced by a graph automorphism. Consider the graph Γ shown in Figure 6.1. The nonzero, non-principal cut sets of Γ are $\{a, c\}$, $\{b, d\}$, and $\{a, b, c, d\}$.

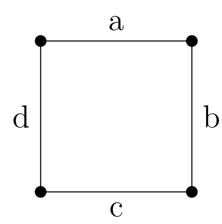


Figure 6.1: Cycle of length four.

It can be easily seen that the permutation $\sigma \in \mathrm{Sym}(C\Gamma)$ which transposes $\{a, c\}$ and $\{b, d\}$, and which leaves all other cut sets fixed is actually a cut symmetry of Γ. However, σ is the identity permutation on the principal cut sets of Γ (although it is of course not induced by the identity automorphism). We will show that this example is in fact prototypical.

Lemma 6.3.6. *Let* Γ *be a graph such that no cut set is a cycle of length* 4. *Then any cut symmetry of* Γ *permuting the principal cut sets is induced by a graph automorphism.*

Proof. Let $\Gamma = (V, E)$, and let $\sigma \in \mathrm{Sym}(C\Gamma)$ be a cut symmetry permuting the principal cut sets. Then there is a corresponding permutation $\pi \in \mathrm{Sym}(V)$ which satisfies $C(u)^\sigma = C(u^\pi)$ for all $u \in V$. We claim that π is a graph automorphism. Indeed, two vertices $v, w \in V$ are adjacent if and only if $|C(v) \cap C(w)| = 1$, which is equivalent to $|C(v)^\sigma \cap C(w)^\sigma| = 1$. This in turn is equivalent to v^π and w^π being adjacent, proving the claim. Since any graph automorphism induces a cut symmetry permuting the principal cut sets, we may assume without loss of generality that π is the identity. It remains to show that any cut symmetry σ of Γ fixing all principal cut sets must be the identity.

For that purpose, we will first show that the cut set $S = C(u) + C(v)$ is fixed by σ for any pair of adjacent vertices $u, v \in V$. Let $e = uv \in E$. We have $C(u) \cap S = C(u) \setminus \{e\}$ and $|C(u) \cap S^\sigma| = |C(u) \cap S| = |C(u)| - 1$. Suppose we have $e \notin S^\sigma$. Then $C(u) \cap S^\sigma = C(u) \cap S = C(u) \setminus \{e\}$, and similarly $C(v) \cap S^\sigma = C(v) \cap S = C(v) \setminus \{e\}$. Since $|S^\sigma| = |S| = |C(u)| + |C(v)| - 2$, it follows $S = S^\sigma$.

By contraposition, if $S^\sigma \neq S$ then $e \in S^\sigma$. In that case, there must be an edge $f \in C(u) \setminus S^\sigma$, and an edge $g \in C(v) \setminus S^\sigma$, with $f = ux$ and $g = vy$ for some vertices $x \neq v$ and $y \neq u$. Thus S^σ contains all edges of S but f and g, and it contains the edge e which is not in S. Since $|S^\sigma| = |S|$, there is exactly one further edge h in $S^\sigma \setminus S$. Since $|C(x) \cap S^\sigma| = |C(x) \cap S|$, and $f \in C(x) \cap S$ but $f \notin C(x) \cap S^\sigma$, and $e \notin C(x)$, we conclude that $h \in C(x) \cap S^\sigma$. The same argument with y and g instead of x and f shows that $h \in C(y) \cap S^\sigma$. Thus we have $h \in C(x) \cap C(y)$. So either $x = y$ or $h = xy$.

If $x = y$, then the cut set $S^\sigma + C(x)$ contains the cycle uvx of odd length 3 contradicting Lemma 6.3.3. If $h = xy$, then $S^\sigma + S = \{f, g, e, h\}$ is a cut set of Γ which clearly forms a cycle of length 4 in contradiction to the hypothesis. Hence, we have shown that $S^\sigma = S$.

To finish the proof, we note that for any edge $e = uv$ and any cut set S, we have $e \in S$ if and only if $|S \cap (C(u) + C(v))| < |S \cap C(u)| + |S \cap C(v)|$. By the previous step and by Lemma 6.3.5, the latter condition is clearly invariant under σ. That is, we have $e \in S$ if and only if $e \in S^\sigma$. This finally shows that $S^\sigma = S$ holds for all cut sets $S \in C\Gamma$. □

We now introduce a family of asymmetric graphs which satisfy the hypotheses of Lemma 6.3.6 for all cut symmetries. Therefore, all of them only have the trivial cut symmetry, and their cut spaces have generically closed characters. This family consists of the complements of the trees with $n \geq 7$ vertices shown in Figure 6.2. (Recall that the complement $\overline{\Gamma}$ of a graph Γ has the same vertex set as Γ but the complementary set of edges.) Note that the analogous graph with $n = 6$ vertices has a nontrivial automorphism, and so has a nontrivial cut symmetry. In fact, all graphs with 6 vertices have nontrivial cut symmetries (although there are asymmetric graphs of that size). So the graph theoretic approach does not produce a generically closed character for the elementary abelian group of order 32.

Lemma 6.3.7. *The complementary graph of any tree shown in Figure 6.2 has no nontrivial cut symmetries.*

Proof. Let $\Gamma = (V, E)$ be one of the trees shown in Figure 6.2 with $n \geq 7$ vertices, and let $\overline{\Gamma} = (V, \overline{E})$ be its complement. It is evident that Γ (and hence also $\overline{\Gamma}$) has no nontrivial automorphism. So by Lemma 6.3.6, it suffices to show that no cut set of $\overline{\Gamma}$ is a cycle of length four, and that any cut symmetry of $\overline{\Gamma}$ permutes the principal cut sets. We begin by estimating the sizes of these cut sets.

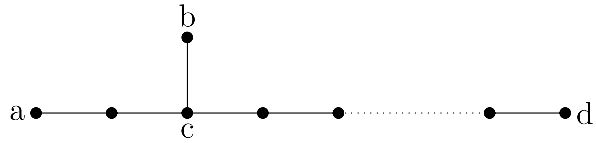


Figure 6.2: A family of asymmetric trees with n vertices for any $n \geq 7$.

Let $a, b, c, d \in V$ be the vertices labeled in Figure 6.2. The corresponding principal cut sets have cardinalities

$$|C(a)| = |C(b)| = |C(d)| = n - 2, \text{ and } |C(c)| = n - 4.$$

All remaining principal cut sets of have cardinality $n-3$. In particular, we see that any principal cut set of $\overline{\Gamma}$ has at most $n-2$ elements.

Now let $C(A)$ be an arbitrary non-principal cut set of $\overline{\Gamma}$. Since $C(A) = C(V \setminus A)$, we may assume without loss of generality $2 \leq |A| \leq n/2$. For the moment, we also assume $|A| > 2$. Since Γ is a tree, there are at most $n-1$ edges between A and $V \setminus A$ in Γ. So in $\overline{\Gamma}$, there must be at least $|A| \cdot (n - |A|) - (n-1)$ edges between A and $V \setminus A$. By elementary calculus, the real valued function $f\colon [3, n/2] \to \mathbb{R}$, $x \mapsto x \cdot (n-x) - (n-1)$ is increasing, so it attains its global minimum at $x = 3$. We conclude

$$|C(A)| \geq f(|A|) \geq f(3) = 2n - 8 \geq n - 1$$

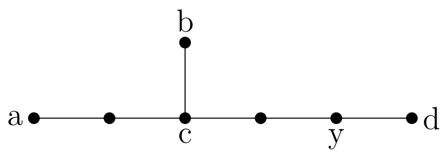
for all subsets $A \subseteq V$ with $3 \leq |A| \leq n/2$.

Finally, let $A = \{x, y\}$ be any 2-subset of V with $|C(x)| \leq |C(y)|$, say. Then, since there is a unique principal cut set of minimum size, we have

$$|C(A)| = |C(x)| + |C(y)| - 2|C(x) \cap C(y)| \geq (n-4) + (n-3) - 2 = 2n - 9,$$

where equality holds if and only if $x = c$, and $y \in V \setminus \{a, b, c, d\}$ is any vertex not adjacent to c in the tree Γ. At this point, we see that all non-principal cut sets of $\overline{\Gamma}$ contain more than four elements. In particular, no cut set is a cycle of length four. Furthermore, if $n \geq 8$ then $|C(A)| \geq n-1$, and we see that all non-principal cut sets are strictly larger than any principal cut set. In particular, any cut symmetry must permute the principal cut sets, and we are done in that case.

It remains to consider $n = 7$, in which case $\overline{\Gamma}$ has a unique non-principal cut set $S = C(c) + C(y)$ of size less than $n-1$ (namely, $n-2$). The only other cut sets of



the same size are the principals $C(a), C(b)$, and $C(d)$. Let $\sigma \in \mathrm{Sym}(C\overline{\Gamma})$ be any cut symmetry. We have to show that σ fixes S. Since $C(c)$ is the unique cut set of size 3, σ certainly fixes $C(c)$. Hence, we have

$$|S^\sigma + C(c)| = |S + C(c)| = |C(y)| = 4.$$

For $x \in \{a, b, d\}$, however, we have

$$|C(x) + C(c)| = |C(x)| + |C(c)| - 2|C(x) \cap C(c)| \in \{6, 8\}.$$

So $S^\sigma \neq C(x)$ for all these x, and the only possibility left is $S^\sigma = S$. This completes the proof. □

At this point, we completed the iteration through all elementary abelian 2-groups.

Theorem 6.3.8. *The elementary abelian group of order 2^n has a generically closed character if and only if $n \notin \{2, 3, 4\}$.*

Proof. The case $n = 1$ is trivial, and Lemma 6.3.1 shows that there are no generically closed characters for $n \in \{2, 3, 4\}$. The case $n = 5$ was handled in Example 6.3.2. For $n > 5$, consider the tree Γ with $n + 1$ vertices shown in Figure 6.2. Its complement $\overline{\Gamma}$ is clearly connected, so the cut space $C\overline{\Gamma}$ is an elementary abelian group of order 2^n. By Lemma 6.3.7, $\overline{\Gamma}$ has no nontrivial cut symmetries, so the corresponding character of $C\overline{\Gamma}$ is generically closed. □

6.4 Generically closed $\mathbb{R}G$-modules of arbitrary groups

To answer the question of which finite groups G have generically closed $\mathbb{R}G$-modules, we have shown that all groups with trivial non-ideal kernel have such modules, and we classified the exceptional groups having a nontrivial non-ideal kernel. Among these exceptional groups, we have already handled all abelian groups. It remains to consider the generalized dicyclic groups, and the two families $Q_8 \times C_4 \times C_2^r$, and $Q_8 \times Q_8 \times C_2^r$ for $r \geq 0$.

A generalized dicyclic group G does not have generically closed $\mathbb{R}G$-modules. This can already be deduced from Babai's classification of the Euclidean symmetry groups of vertex transitive polytopes (Theorem 7.2.2) but at this point it seems more reasonable to give a direct proof.

Lemma 6.4.1. *Let $G = A\langle g \rangle$ be a generalized dicyclic group, where A is of index two in G, and where g is an element of order four acting as the inversion on A. Let $\pi \in \mathrm{Sym}(G)$ be the permutation which is the identity on A, and which is the multiplication by g^2 on $G \setminus A$. Then π is a generic symmetry of every $\mathbb{R}G$-module.*

Proof. By Proposition 5.1.5, it suffices to show that $\pi \in \mathrm{Sym}(G, \chi)$ for any character χ afforded by a simple $\mathbb{R}G$-module. If $g^2 \in \mathrm{Ker}(\chi)$ then π fixes all cosets of $\mathrm{Ker}(\chi)$ in G, and π is even an irrelevant symmetry of χ. So we may assume $g^2 \notin \mathrm{Ker}(\chi)$ in the rest of the proof. By Lemma 6.2.2, χ then must be an ideal character which is zero on the coset gA. Let $x, y \in G$ be arbitrary. If x and y both lie in the same coset of A then we have $\pi(x)^{-1}\pi(y) = x^{-1}y$. If they lie in different cosets then both $x^{-1}y$ and $\pi(x)^{-1}\pi(y) = g^2x^{-1}y$ are elements of the coset gA on which χ vanishes. So in any case, we have $\chi(\pi(x)^{-1}\pi(y)) = \chi(x^{-1}y)$. By Theorem 5.1.8, we get $\pi \in \mathrm{Sym}(G, \chi)$. □

The remaining two families of exceptional groups both have generically closed $\mathbb{R}G$-modules whose characters can be constructed explicitly. Recall that the irreducible characters of a direct product of groups are given by products of irreducible characters of the factors, and that the Frobenius-Schur indicator is multiplicative with respect to such products (see the discussion at 6.2).

Lemma 6.4.2. *Let $G = Q_8 \times C_4 \times C_2^r$ for some $r \geq 0$. Then G is generically closed with respect to some $\mathbb{R}G$-module.*

Proof. Let $\alpha \in \mathrm{Irr}(Q_8)$ be the faithful irreducible character of degree 2. Let $\beta = \lambda + \overline{\lambda}$, where λ is a faithful linear character of $C_4 = \langle c \rangle$. Finally, let γ be a faithful ideal character of C_2^r. Then we claim that the character

$$\chi = (\alpha \times \beta \times \gamma) + (2\alpha \times 1 \times 1) + (1 \times \beta \times 1)$$

is afforded by a generically closed $\mathbb{R}G$-module.

The irreducible constituents of the first summand have the form $\tau = \alpha \times \mu \times \sigma$, where $\mu \in \{\lambda, \overline{\lambda}\}$, and $\sigma \in \mathrm{Irr}(C_2^r)$. We have $\tau \neq \overline{\tau}$, $\tau(1) = 2$, and $\iota\tau = 0$. Moreover, both τ and $\overline{\tau}$ occur in χ with multiplicity 1.

The other irreducible constituents η of χ, that is,

$$\eta \in \{\alpha \times 1 \times 1, 1 \times \lambda \times 1, 1 \times \overline{\lambda} \times 1\},$$

each occur with multiplicity $\eta(1)$. Thus χ is a left ideal character afforded by a $\mathbb{R}G$-module, and the ideal constituent of χ is

$$\chi_{\mathcal{I}} = (2\alpha \times 1 \times 1) + (1 \times \beta \times 1).$$

An easy calculation shows $\mathrm{Ker}(\chi_{\mathcal{N}}) = \mathrm{Ker}(\alpha \times \beta \times \gamma) = \langle u \rangle$, where $u = (-1, c^2, 1)$. We have $\chi_{\mathcal{I}}(u) = -6 = -\chi_{\mathcal{I}}(1)$, so u is in the center of $\chi_{\mathcal{I}}$. In particular, we have $\chi_{\mathcal{I}}(gu) = -\chi_{\mathcal{I}}(g)$ for all $g \in G$.

Let $\pi \in \mathrm{Sym}(G, \chi)$ be any generic symmetry with $\pi(1) = 1$. By Theorem 5.1.10, π leaves the cosets of $\mathrm{Ker}(\chi_{\mathcal{N}})$ setwise fixed. Suppose that π is not the identity, then there is an element $g \in G$ with $\pi(g) = gu$. Then, again by Theorem 5.1.10, we have $\chi_{\mathcal{I}}(g) = \chi_{\mathcal{I}}(\pi(g)) = -\chi_{\mathcal{I}}(g)$, so $\chi_{\mathcal{I}}(g) = 0$ which means $g = (x, y, z)$ with $x \in Q_8 \setminus \{\pm 1\}$ and $y^2 \neq 1$. Let $h = (x, 1, 1)$. Then $0 \neq \chi_{\mathcal{I}}(h) = 2$, so $\pi(h) = h$, and $0 \neq \chi_{\mathcal{I}}(h^{-1}g) = 2$. But then $\chi_{\mathcal{I}}(\pi(h)^{-1}\pi(g)) = \chi_{\mathcal{I}}(h^{-1}ug) = -\chi_{\mathcal{I}}(h^{-1}g)$ is a contradiction to Theorem 5.1.10, which shows that π must be the identity. Hence, χ is generically closed. □

Lemma 6.4.3. *Let $G = Q_8 \times Q_8 \times C_2^r$ for some $r \geq 0$. Then G is generically closed with respect to some $\mathbb{R}G$-module.*

Proof. As in the proof of Lemma 6.4.2, $\alpha \in \mathrm{Irr}(Q_8)$ denotes the faithful character of degree two, and γ denotes a faithful character of C_2^r. We claim that the character

$$\chi = (\alpha \times \alpha \times \gamma) + (2\alpha \times 1 \times 1) + (1 \times 2\alpha \times 1)$$

is afforded by a generically closed $\mathbb{R}G$-module.

The proof follows the same lines as in Lemma 6.4.2. For the same reasons as above, χ is a left ideal character afforded by an $\mathbb{R}G$-module, and its ideal constituent is given by

$$\chi_{\mathcal{I}} = (2\alpha \times 1 \times 1) + (1 \times 2\alpha \times 1).$$

We also have $\mathrm{Ker}(\chi_{\mathcal{N}}) = \mathrm{Ker}(\alpha \times \alpha \times \gamma) = \langle u \rangle$, where $u = (-1, -1, 1)$. We have $\chi_{\mathcal{I}}(u) = -8 = -\chi_{\mathcal{I}}(1)$, so u is in the center of $\chi_{\mathcal{I}}$, and we have $\chi(gu) = -\chi(g)$ for all $g \in G$. Let $\pi \in \mathrm{Sym}(G, \chi)$ with $\pi(1) = 1$. Suppose that π is not the identity. Then there is an element $g \in G$ with $\pi(g) = gu$. By Theorem 5.1.10, we have $\chi_{\mathcal{I}}(g) = \chi_{\mathcal{I}}(\pi(g)) = -\chi_{\mathcal{I}}(g)$, and hence $\chi_{\mathcal{I}}(g) = 0$. Therefore, we have $g = (x, y, z)$ with either $(x, y) \in \{(1, -1), (-1, 1)\}$ or $x, y \in Q_8 \setminus \{\pm 1\}$. In the first case, set $h = (a, 1, 1)$, where a is any element in $Q_8 \setminus \{\pm 1\}$; in the second case, set $h = (x, 1, 1)$. In both cases, we have $\chi_{\mathcal{I}}(h) \neq 0$, so $\pi(h) = h$, and $\chi_{\mathcal{I}}(h^{-1}g) \neq 0$. Again, as in the proof above, we obtain a contradiction to Theorem 5.1.10 by $\chi_{\mathcal{I}}(\pi(h)^{-1}\pi(g)) = \chi_{\mathcal{I}}(h^{-1}ug) = -\chi_{\mathcal{I}}(h^{-1}g)$. So π must be the identity, and χ is generically closed. □

At this point, we finished the iteration through all finite groups. The following theorem summarizes all results of this chapter, and it completes the classification of the affine symmetry groups of orbit polytopes. Moreover, it answers a question of Babai (1977) who classified the Euclidean symmetry groups of vertex transitive polytopes.

Theorem 6.4.4. *Let G be a finite group. The following statements are equivalent.*

(1) There is a generically closed $\mathbb{R}G$-module.

(2) G is isomorphic to the affine symmetry group of an orbit polytope.

(3) G is neither generalized dicyclic, nor abelian of exponent greater than two, nor elementary abelian of order $4, 8,$ or 16.

Proof. The equivalence of (1) and (2) was already proven in Theorem 3.9.6. The equivalence of (1) and (3) was the objective of the present section: Of course every $\mathbb{R}G$-module is generically closed if $G = 1$ is the trivial group. If G is an abelian group of exponent two then, by Theorem 6.3.8, there is a generically closed $\mathbb{R}G$-module if and only if $|G| \notin \{4, 8, 16\}$. An abelian group of exponent greater than two has no generically closed module over $\mathbb{R}$ by Corollary 5.1.11. By Lemma 6.4.1, generalized dicyclic groups have no generically closed modules over $\mathbb{R}$. If G is isomorphic to either $Q_8 \times C_4 \times C_2^r$ or $Q_8 \times Q_8 \times C_2^r$ for some $r \geq 0$ then there are generically closed

$\mathbb{R}G$-modules by Lemma 6.4.2 and 6.4.3. By Theorem 6.2.3, all other groups G not mentioned so far have a faithful non-ideal character afforded by an $\mathbb{R}G$-module, which is generically closed by Theorem 5.1.7. □

Babai's classification (which we reprove in Theorem 7.2.2) asserts that any finite group is isomorphic to the Euclidean symmetry group of some vertex transitive polytope unless it is abelian of exponent greater than two, or generalized dicyclic. In combination with Theorem 6.4.4, we get the surprising result that there are up to isomorphism only three groups which arise as the Euclidean symmetry group of some vertex transitive polytope but not as the affine symmetry group of an orbit polytope, namely C_2^2, C_2^3, and C_2^4.

7 Orthogonal and unitary generic symmetries

So far we have considered the most general class of reasonable symmetries on vector spaces, namely (affine) linear symmetries. However, in some situations (especially when studying polytopes) one is often interested in more restricted classes of symmetries which, for example, also preserve distances and angles. The most prominent examples of such symmetries are of course (affine) orthogonal and unitary maps. In this chapter we show that the previously developed theory of generic symmetries can be extended without many efforts to achieve results about orthogonal or unitary symmetries of orbits.

In the following, we introduce the notion of orthogonal generic symmetries of $\mathbb{R}G$-modules in complete analogy to ordinary generic symmetries (replacing linear permutations by orthogonal permutations). Surprisingly, the group $\mathrm{OSym}(G, V)$ of all orthogonal generic symmetries of a $\mathbb{R}G$-module V does not rely on a specific inner product on V, but is completely determined by the character of V. In Theorem 7.1.8, we give a characterization of $\mathrm{OSym}(G, V)$ by a formula only depending on χ. We also have an orthogonal analog of generic points (Theorem 7.1.10). That is, if G acts faithfully on V by orthogonal transformations then $\mathrm{OSym}(G, V)$ is isomorphic to the orthogonal symmetry groups of almost all orbits of G in V. As an application of these results, we give an new proof of Babai's classification of the Euclidean symmetry groups of vertex transitive polytopes (Theorem 7.2.2).

In the unitary setting, the situation is much simpler. In Theorem 7.3.1, we show that if V is a complex inner product space on which G acts faithfully by unitary transformations then G is already the unitary symmetry group of almost all of its orbits in V.

The following theory on orthogonal generic symmetries has not been published so far. The main result on unitary generic symmetries has appeared in [8].

7.1 Orthogonal generic symmetries

In this section, we only consider finite dimensional inner product spaces over the field $\mathbb{R}$ of real numbers (although some results have generalizations to other fields and other geometries). As before, we consider a fixed finite group G together with some finitely generated $\mathbb{R}G$-module V. A standard averaging argument shows that there exists a G-invariant inner product on V (that is, we have $\langle gx, gy\rangle = \langle x, y\rangle$ for all $g \in G$, $x, y \in V$). More precisely, if $\alpha\colon V \times V \to \mathbb{R}$ is an arbitrary inner product, a G-invariant inner product is obtained by setting

$$\langle x, y\rangle = \frac{1}{|G|}\sum_{g\in G}\alpha(gx, gy) \text{ for all } x, y \in V.$$

For the rest of the section, we consider V as an inner product space on which G acts by orthogonal transformations. For any subset $X \subseteq V$, we define the *orthogonal symmetry group* $O(X) \leq \mathrm{Sym}(X)$ as the group of all permutations on X arising as restrictions of orthogonal maps $V \to V$. Of course, this definition agrees with the usual definition of orthogonal groups of inner product spaces. That is, if $X \leq V$ is a linear subspace then $O(X)$ consists precisely of the orthogonal maps $X \to X$.

With that terminology, orthogonal orbit symmetries and orthogonal generic symmetries can be defined in complete analogy to ordinary orbit symmetries and generic symmetries by replacing each occurrence of $\mathrm{GL}(X)$ by $O(X)$.

Definition 7.1.1. A permutation $\pi \in \mathrm{Sym}(G)$ is an *orthogonal orbit symmetry* of a point $v \in V$ if there is an orthogonal map $\alpha \in O(Gv)$ such that

$$\alpha(gv) = \pi(g)v \text{ for all } g \in G.$$

A permutation π is a *orthogonal generic symmetry* of V if π is an orthogonal orbit symmetry of almost all points of V. The set of all orthogonal orbit symmetries of $v \in V$ is denoted by $\mathrm{OSym}(G, v)$. The set of orthogonal generic symmetries of V is denoted by $\mathrm{OSym}(G, V)$.

In the following, we show that many of the basic results on generic symmetries are easily adaptable to orthogonal generic symmetries. To begin with, it is utterly routine to check that both $\mathrm{OSym}(G, v)$ and $\mathrm{OSym}(G, V)$ are subgroups of $\mathrm{Sym}(G)$ containing all left multiplications by elements of G (cf. Proposition 3.1.4, 3.2.4, 3.1.5). Moreover, the usual epimorphism $D_v\colon \mathrm{Sym}(G, v) \to \mathrm{GL}(Gv)$ restricts to an epimorphism $\mathrm{OSym}(G, v) \to \mathrm{O}(Gv)$, whose kernel consists of all irrelevant orbit symmetries of v by Proposition 3.1.4. So if v has a trivial stabilizer in G then we have a natural isomorphism $\mathrm{OSym}(G, v) \cong O(Gv)$. For adapting some more advanced results on generic symmetries, we need the following restatements of orthogonal orbit symmetries and orthogonal generic symmetries.

Lemma 7.1.2. *Let V be a real inner product space on which G acts by orthogonal transformations. A permutation $\pi \in \mathrm{Sym}(G)$ is an orthogonal orbit symmetry of some point $x \in V$ if and only if π is an (ordinary) orbit symmetry of x, and we have*

$$\langle \pi(g)x, \pi(h)x \rangle = \langle gx, hx \rangle \textit{ for all } g, h \in G.$$

Proof. It is clear by definition that $\mathrm{OSym}(G, x) \subseteq \mathrm{Sym}(G, x)$. Let $\pi \in \mathrm{Sym}(G, x)$ be an orbit symmetry of x realized by a linear map $\alpha \in \mathrm{GL}(Gx)$. We have $\pi \in \mathrm{OSym}(G, x)$ if and only if $\alpha \in O(Gx)$, which is equivalent to

$$\langle \alpha(gx), \alpha(hx) \rangle = \langle gx, hx \rangle \text{ for all } g, h \in G.$$

By definition of α, this in turn is equivalent to

$$\langle \pi(g)x, \pi(h)x \rangle = \langle gx, hx \rangle \text{ for all } g, h \in G.$$

□

Lemma 7.1.2 suggests that the group of orthogonal orbit symmetries $\mathrm{OSym}(G, x)$ of some point $x \in V$ does essentially depend on the inner product on V. In fact, this observation can be easily confirmed by looking at simple examples. It is rather surprising however, that the orthogonal generic symmetry group $\mathrm{OSym}(G, V)$ is independent of the choice of an inner product on V. This follows immediately from the next lemma.

For any $\mathbb{R}G$-module V, we set $\mathrm{Ann}(V) = \{x \in \mathbb{R}G : xv = 0 \text{ for all } v \in V\}$. This *annihilator* of V is a two sided ideal of $\mathbb{R}G$ which can also be expressed as the intersection of the annihilators of all elements of V.

Lemma 7.1.3. *Let V be a finite dimensional real inner product space on which G acts by orthogonal transformations. A permutation $\pi \in \mathrm{Sym}(G)$ is an orthogonal generic symmetry of V if and only if π is an (ordinary) generic symmetry of V, and one of the following equivalent statements holds.*

(1) We have $\langle \pi(g)v, \pi(h)v\rangle = \langle gv, hv\rangle$ for all $g, h \in G$ and all $v \in V$.

(2) We have $\pi(h)^{-1}\pi(g) + \pi(g)^{-1}\pi(h) - h^{-1}g - g^{-1}h \in \mathrm{Ann}(V)$ for all $g, h \in G$.

In that case, π is an orthogonal orbit symmetry of all ample points of V.

Proof. It is clear from the definition that any orthogonal generic symmetry of V is also an (ordinary) generic symmetry of V. Let $\pi \in \mathrm{Sym}(G, V)$ be arbitrary. If π is orthogonally generic, then by Lemma 7.1.2, we have

$$\langle \pi(g)v, \pi(h)v\rangle = \langle gv, hv\rangle \tag{7.1}$$

for all $g, h \in G$ and for almost all $v \in V$. As the set of all $v \in V$ satisfying (7.1) is closed in V, this equation must actually hold for all $v \in V$. Conversely, if $\pi \in \mathrm{Sym}(G, V)$ is such that (7.1) holds for all $v \in V$ then π is an orthogonal orbit symmetry of any $v \in V$ for which it is an orbit symmetry. In summary, a permutation $\pi \in \mathrm{Sym}(G)$ is in $\mathrm{OSym}(G, V)$ if and only if π is in $\mathrm{Sym}(G, V)$ and (1) holds. By Theorem 3.3.4, in that case π is an orthogonal orbit symmetry of any ample point of V.

It remains to prove the equivalence of (1) and (2). By substituting $v = x + y$, we see that (1) holds if and only if

$$\langle \pi(g)(x + y), \pi(h)(x + y)\rangle = \langle g(x + y), h(x + y)\rangle$$

holds for all $x, y \in V$ and all $g, h \in G$. By expanding both sides, and applying (7.1) repeatedly, we see that (1) is equivalent to

$$\langle \pi(g)x, \pi(h)y\rangle + \langle \pi(g)y, \pi(h)x\rangle = \langle gx, hy\rangle + \langle gy, hx\rangle$$

for all $x, y \in V$ and all $g, h \in G$. By G-invariance and by symmetry of the inner product, this in turn is equivalent to

$$\langle (\pi(h)^{-1}\pi(g) + \pi(g)^{-1}\pi(h) - h^{-1}g - g^{-1}h)x, y\rangle = 0$$

for all $x, y \in V$ and all $g, h \in G$. Since the inner product is non-degenerate, this is equivalent to

$$(\pi(h)^{-1}\pi(g) + \pi(g)^{-1}\pi(h) - h^{-1}g - g^{-1}h)x = 0$$

for all $g, h \in G$ and all $x \in V$. This is precisely the statement of (2). □

Among others, Lemma 7.1.3 shows that for any finitely generated $\mathbb{R}G$-module V, the group $\mathrm{OSym}(G, V)$ is unambiguously defined. More precisely, $\mathrm{OSym}(G, V)$ does only depend on the isomorphism type of V, that is, on the character of V.

Definition 7.1.4. Let χ be a character of G afforded by an $\mathbb{R}G$-module V. Then we set $\mathrm{OSym}(G, \chi) = \mathrm{OSym}(G, V)$ with respect to an arbitrary G-invariant inner product on V.

Remark 7.1.5. In principle, $\mathrm{OSym}(G, V)$ can be defined for a $\Bbbk G$-module V over an arbitrary field $\Bbbk$ with respect to a symmetric G-invariant form $\beta\colon V \times V \to \Bbbk$. If β is non-degenerate, the statement of Lemma 7.1.3 holds as well by the same proof. However, there is no guarantee for such a non-degenerate form existing. In fact, if V is a simple $\mathbb{C}G$-module which is not a scalar extension of an $\mathbb{R}G$-module, the only symmetric G-invariant form $V \times V \to \mathbb{C}$ is the zero map. So $\mathrm{OSym}(G, \chi)$ cannot be defined for all characters of G in a reasonable way.

Lemma 7.1.3 shows that we may freely choose a G-invariant inner product on V for the determination of $\mathrm{OSym}(G, V)$. As a consequence, we can easily adapt the proof of Lemma 3.2.8 to get an analog result in the orthogonal setting.

Lemma 7.1.6. *Let χ and ψ be characters of G afforded by $\mathbb{R}G$-modules. Then*

$$\mathrm{OSym}(G, \chi) \cap \mathrm{OSym}(G, \psi) \subseteq \mathrm{OSym}(G, \chi + \psi).$$

Proof. Let U_1, U_2 be $\mathbb{R}G$-modules affording the characters χ and ψ, respectively. Let further β_i be arbitrary G-invariant inner products on U_i. Then $V = U_1 \oplus U_2$ becomes an inner product space on which G acts by orthogonal transformations with respect to the form

$$((x_1, x_2), (y_1, y_2)) \mapsto \beta_1(x_1, y_1) + \beta_2(x_2, y_2).$$

The rest of the proof follows the lines of the proof of Lemma 3.2.8 verbatim: Let $\pi \in \mathrm{OSym}(G, U_1) \cap \mathrm{OSym}(G, U_2)$ be an orthogonal generic symmetry, and let $O_i \subseteq U_i$ be nonempty open sets of points for which π is an orthogonal orbit symmetry. Then $O = O_1 \times O_2$ is open in V, and it is easy to see that π is an orthogonal orbit symmetry of all points of O. □

Since the group $\mathrm{OSym}(G, \chi)$ is uniquely determined by χ, we may hope to find a formula characterizing the orthogonal generic symmetries only in terms of the character χ. In fact, by Theorem 5.1.10 and by Lemma 7.1.3, we only need to find a formula characterizing the annihilator of a module in terms of its character. Such a formula is doubtlessly well known. Nevertheless, we give a proof of the following statement for convenience.

Lemma 7.1.7. *Let χ be a character of G afforded by an $\mathbb{R}G$-module V. Then we have*

$$\mathrm{Ann}(V) = \{x \in \mathbb{R}G : \chi(gx) = 0 \textit{ for all } g \in G\}.$$

Proof. The left-to-right inclusion is easy to see, for if $x \in \mathrm{Ann}(V)$ then each element $gx \in \mathbb{R}G$ acts as the zero endomorphism on V, which of course has a zero trace. Hence $\chi(gx) = 0$ for all $g \in G$.

Conversely, let $x \in \mathbb{R}G$ be any element such that $\chi(gx) = 0$ for all $g \in G$. Since $\mathrm{Ann}(V)$ is a two sided ideal of $\mathbb{R}G$, it is generated by a central idempotent $f \in \mathbb{R}G$ by Lemma 4.2.7. Let $L = \mathbb{R}G(1-f)x$ be the left ideal generated by $(1-f)x$. By construction, we have $fy = 0$ and $\chi(y) = 0$ for all $y \in L$. Let $e \in L$ be an idempotent generator of L. Since e acts as a projection on V, $\chi(e)$ is precisely the rank of e as a linear operator of V by linear algebra. Since $\chi(e) = 0$, e must be the zero endomorphism on V, so we have $e \in \mathrm{Ann}(V)$. Consequently, we have $e = fe = 0$, and hence $L = 0$. In particular, we have $(1-f)x = 0$ which shows that $x \in \mathrm{Ann}(V)$. □

Combining Theorem 5.1.10, Lemma 7.1.3, and Lemma 7.1.7 we get a purely character theoretic characterization of orthogonal generic symmetries. Recall that for any character χ of G we have introduced its ideal constituent $\chi_{\mathcal{I}}$, and its non-ideal constituent $\chi_{\mathcal{N}}$ (cf. Chapter 5).

Theorem 7.1.8. *Let χ be a character of G afforded by an $\mathbb{R}G$-module. Then a permutation $\pi \in \mathrm{Sym}(G)$ is in $\mathrm{OSym}(G,\chi)$ if and only if the following statements hold.*

(1) $\chi_{\mathcal{I}}(\pi(g)^{-1}\pi(h)) = \chi_{\mathcal{I}}(g^{-1}h)$ *for all* $g, h \in G$,

(2) $\pi(gK) = \pi(1)gK$ *for all* $g \in G$, *where* $K = \mathrm{Ker}(\chi_{\mathcal{N}})$,

(3) $\chi(g\pi(x)^{-1}\pi(y)) + \chi(g\pi(y)^{-1}\pi(x)) = \chi(gx^{-1}y) + \chi(gy^{-1}x)$ *for all* $g, x, y \in G$.

Proof. Let V be an $\mathbb{R}G$-module affording the character χ. By Lemma 7.1.3, a permutation $\pi \in \mathrm{Sym}(G)$ is in $\mathrm{OSym}(G,\chi)$ if and only if $\pi \in \mathrm{Sym}(G,\chi)$ and $w_{x,y} \in \mathrm{Ann}(V)$ for all $x, y \in G$, where

$$w_{x,y} = \pi(x)^{-1}\pi(y) + \pi(y)^{-1}\pi(x) - x^{-1}y - y^{-1}x.$$

By Theorem 5.1.10, $\pi \in \mathrm{Sym}(G,\chi)$ is equivalent to (1) and (2). By Lemma 7.1.7, $w_{x,y} \in \mathrm{Ann}(V)$ is equivalent to $\chi(gw_{x,y}) = 0$ for all $g \in G$. This in turn is equivalent to (3). □

As a very simple application, we determine the orthogonal generic symmetries of the group algebra $\mathbb{R}G$ for any elementary abelian 2-group G. Recall that the (regular) character ρ of $\mathbb{R}G$ sends $1 \in G$ to the order $|G|$, and any other element of G to 0.

Example 7.1.9. Let $G \cong C_2^r$ be an elementary abelian 2-group, and let ρ be its regular character. Then $G = \mathrm{OSym}(G,\rho)$.

Proof. Since G is always a subgroup of $\mathrm{Sym}(G,\rho)$, it suffices to show that any permutation $\pi \in \mathrm{OSym}(G,\rho)$ with $\pi(1) = 1$ is the identity. This is almost immediate from Theorem 7.1.8. By setting $g = x$ and $y = 1$, we get from (3) that $2\rho(x\pi(x)) = 2\rho(1)$ holds for all $x \in G$. This implies $\pi(x) = x$ for all $x \in G$. □

Recall that the relevance of generic symmetry groups lies in the fact that (assuming G acts faithfully on V) a generic symmetry group $\mathrm{Sym}(G,V)$ is isomorphic to the linear symmetry groups of almost all orbits of G in V (Theorem 3.5.2). This observation essentially enables us to use character theory in order to prove statements about linear symmetry groups of orbits. The next result is the orthogonal analog of Theorem 3.5.2. Roughly speaking, it states that generic points also exist in the orthogonal setting.

Theorem 7.1.10. *Let V be a finite dimensional real inner product space on which G acts by orthogonal transformations. Then we have* $\mathrm{OSym}(G,x) = \mathrm{OSym}(G,V)$ *for almost all $x \in V$.*

Proof. For any permutation $\pi \in \mathrm{Sym}(G)$, we consider the set

$$O_\pi = \{x \in V : \langle \pi(g)x, \pi(h)x\rangle \neq \langle gx, hx\rangle \text{ for some } g,h \in G\}.$$

This set is open by construction, although it may be empty for some π (such as for the identity). We define $O \subseteq V$ to be the intersection of $\mathrm{Gen}(V)$ and of all these sets O_π, $\pi \in \mathrm{Sym}(G)$, which are nonempty. Then O is by construction (and by Theorem 3.5.2) a nonempty open set. We claim that $\mathrm{OSym}(G,x) = \mathrm{OSym}(G,V)$ for all $x \in O$.

The right-to-left inclusion holds by Lemma 7.1.3 since O consists of ample points. Concerning the other inclusion, let $\pi \in \mathrm{OSym}(G,x)$ be arbitrary. Since x is a generic point, we clearly have $\pi \in \mathrm{Sym}(G,V)$. On the other hand, we have $x \notin O_\pi$, and consequently $O_\pi = \emptyset$. By definition of O_π, it follows that for all $y \in V$ and all $g,h \in G$ we have

$$\langle \pi(g)y, \pi(h)y\rangle = \langle gy, hy\rangle.$$

So π must be an orthogonal generic symmetry of V by Lemma 7.1.3. This proves the left-to-right inclusion. □

The next result is the orthogonal analog of Theorem 3.8.6, which is proven exactly in the same way. To keep things simple, we exclude irrelevant generic symmetries by assuming that G acts faithfully on V.

Proposition 7.1.11. *Let $D\colon G \to O(V)$ be a faithful orthogonal representation for some finite dimensional real inner product space V. Suppose there is an element $v \in V$ such that $V = \mathbb{R}Gv$ and $D(G) = O(Gv)$. Then we have $G = \mathrm{OSym}(G,V)$.*

Proof. Let $D_v\colon \mathrm{OSym}(G,V) \to O(V)$ be the canonical orthogonal representation (which is the restriction of the canonical map $D_v\colon \mathrm{Sym}(G,V) \to \mathrm{GL}(V)$) associated to $\mathrm{OSym}(G,V)$. Since D is faithful, D_v must be faithful as well by Lemma 3.8.4. Since the representations D and D_v have the same images, they give rise to isomorphisms

$$G \cong O(Gv) \cong \mathrm{OSym}(G,V).$$

Since G and $\mathrm{OSym}(G, V)$ are finite groups with $G \leq \mathrm{OSym}(G, V)$, equality follows. □

7.2 Babai's classification

As an illustrating application of the theory of orthogonal generic symmetries developed so far, we reprove a classical result of Babai (Theorem 7.2.2). Let V be finite dimensional real inner product space, and let $P \subset V$ be a polytope. An *isometry* of P is understood as a permutation $P \to P$ which is the restriction of an isometry (that is, of a distance preserving affine map) $V \to V$. The *Euclidean symmetry group of* P is the group consisting of all isometries of P. The polytope P is called *vertex transitive* if its Euclidean symmetry group acts transitively on the vertices of P. Babai has classified all finite groups which are isomorphic to an Euclidean symmetry group of a vertex transitive polytope.

The idea of the following proof of Theorem 7.2.2 is essentially the same as of the proof of Theorem 6.4.4. As a first step, we translate the property of being isomorphic to an Euclidean symmetry group of a vertex transitive polytope into a purely character theoretic statement (Proposition 7.2.1). To a great extent, this part is analog to the considerations done in Section 3.9. For the sake of clarity, we will skip some details which can be adapted verbatim, and focus on the new obstacles arising. In a second step, we need to determine whether a finite group G has a faithful character χ afforded by an $\mathbb{R}G$-module such that $G = \mathrm{OSym}(G, \chi)$ holds. This question is answered by using the techniques developed in the last three chapters.

Proposition 7.2.1. *Let G be a finite group. Then the following statements are equivalent.*

(1) There is a faithful character χ of G afforded by an $\mathbb{R}G$-module such that $G = \mathrm{OSym}(G, \chi)$ holds.

(2) There is a finite subset $X \subset V$ of some real inner product space V such that $G \cong O(X)$, and $O(X)$ acts transitively on X.

(3) G is isomorphic to the Euclidean symmetry group of some vertex-transitive polytope.

Sketch of a proof. We show the implications (3) $\implies$ (2) $\implies$ (1) $\implies$ (3). To a great extent, the argumentation follows the lines of Section 3.9 proving Theorem 3.9.6.

Suppose that (3) holds. Then there is a real inner product space V and a vertex transitive polytope $P \subset V$ whose Euclidean symmetry group is isomorphic to G. By translating P if necessary, we may assume without loss of generality that the barycenter of P is the origin of V. Then all isometries of P are restrictions of orthogonal maps on V. If X denotes the vertex set of P then $O(X)$ acts transitively on X and is isomorphic to the Euclidean symmetry group of P. So (2) holds.

Suppose that (2) holds. We may assume without loss of generality that V is the $\mathbb{R}$-linear span of X. Then any isomorphism $D\colon G \to O(X)$ can be regarded as a faithful orthogonal representation $G \to O(V)$. Since $O(X)$ is transitive on X, we have $X = Gv$ for any $v \in X$. In particular, we have $D(G) = O(X) = O(Gx)$. Now Proposition 7.1.11 implies $G = \mathrm{OSym}(G, V) = \mathrm{OSym}(G, \chi)$, where χ is the character of D. So (1) holds.

Finally, suppose that (1) holds. Then G acts faithfully on some finite dimensional real inner product space V by orthogonal transformations such that $G = \mathrm{OSym}(G, V)$. By Theorem 7.1.10, there is some point $x \in V$ such that $G_x = 1$ and $\mathrm{OSym}(G, x) = \mathrm{OSym}(G, V)$. It follows that G is isomorphic to the orthogonal symmetry group $O(Gx)$. Let $P \subset V$ be the convex hull of Gx. Then the orbit Gx is also the vertex set of the polytope P, and $O(P)$ consists precisely of the left multiplications by the elements of G. In particular, P is vertex transitive, and $G \cong O(P)$. To prove (3), it remains to show that $O(P)$ is the full Euclidean symmetry group of P. Let $\varphi\colon V \to V$ be any isometry of V permuting the elements (or equivalently, the vertices) of P. By Lemma 3.9.4, there is a linear map $\psi\colon V \to V$ agreeing with φ on (the vertices of) P. We claim that φ restricts to an orthogonal map on the $\mathbb{R}$-linear span W of P. Afterwards, after altering the action of ψ on the orthogonal complement $W^\perp$ in V if necessary to ensure that ψ is an orthogonal map on V, we have proven that φ agrees with an orthogonal map on P. To finish the proof, we have to show that $\langle \psi(gx), \psi(hx) \rangle = \langle gx, hx \rangle$, or equivalently, that $\langle \varphi(gx), \varphi(hx) \rangle = \langle gx, hx \rangle$ holds for all $g, h \in G$. Since φ is an isometry of V, it preserves the distances between elements of V. Furthermore, since G acts on V by orthogonal transformations, and since φ permutes the elements of Gx, we have $\|\varphi(gx)\| = \|gx\|$ for all $g \in G$. The assertion now follows by the well known equation

$$\langle y, z \rangle = \frac{1}{2}\left(\|y\|^2 + \|z\|^2 - \|y - z\|^2\right)$$

which holds for all $y, z \in V$. □

Theorem 7.2.2 (Babai)**.** *A finite group G is not isomorphic to the Euclidean symmetry group of a vertex transitive polytope if and only if G is abelian of exponent greater than two, or generalized dicyclic.*

Proof. Let G be a group which is not isomorphic to the Euclidean symmetry group of a vertex transitive polytope. By Proposition 7.2.1, this is equivalent to $G \subsetneq \mathrm{OSym}(G, \chi)$ for all characters χ afforded by $\mathbb{R}G$-modules. In particular, we have $G \subsetneq \mathrm{Sym}(G, \chi)$ for all those χ which by Theorem 6.4.4 implies that G must be either abelian of exponent greater than two, or generalized dicyclic, or G must be isomorphic to one of C_2^2, C_2^3, or C_2^4. The last three cases are excluded by Example 7.1.9.

Conversely, let G be any finite abelian group of exponent greater than two, and let χ be a left ideal character afforded by an $\mathbb{R}G$-module. Since the exponent of G is not two, the permutation $\pi\colon g \mapsto g^{-1}$ is not a left multiplication by some element of G. We apply Theorem 7.1.8 to show that π is an orthogonal generic symmetry of χ. By Corollary 5.1.11, π is a generic symmetry of χ, so the first two items are satisfied. In fact, the third requirement of Theorem 7.1.8 is satisfied for trivial reasons, so π is indeed an orthogonal generic symmetry of χ. Hence, $G \subsetneq \mathrm{OSym}(G, \chi)$.

Finally, let $G = A\langle g \rangle$ be a generalized dicyclic group with an abelian subgroup A of index two, where $g \in G \setminus A$ is an element of order four acting on A as the inversion.

Let $\pi \in \mathrm{Sym}(G)$ be the permutation which is the identity on A, and which is the multiplication by (the central element) g^2 on $G \setminus A$. We claim that π is an orthogonal generic symmetry of any simple $\mathbb{R}G$-module. By Lemma 7.1.6, it then follows that π is orthogonally generic for any $\mathbb{R}G$-module, that is, $G \subsetneq \mathrm{OSym}(G, \chi)$ for all characters χ afforded by $\mathbb{R}G$-modules.

Let χ be the character of any simple $\mathbb{R}G$-module. We again apply Theorem 7.1.8 to χ and π. By Lemma 6.4.1, π is an ordinary generic symmetry of χ, so the first two requirements of the theorem are satisfied. We show that the third requirement is satisfied as well. Of course there is nothing to show if $g^2 \in \operatorname{Ker}\chi$. If $g^2 \notin \operatorname{Ker}\chi$ then, by Lemma 6.2.2, we see that χ is zero on $G \setminus A$. Let $x, y \in G$ be arbitrary elements. If x and y lie in the same coset of A then we have $\pi(x)^{-1}\pi(y) = x^{-1}y$, and hence $\chi(h\pi(x)^{-1}\pi(y)) = \chi(hx^{-1}y)$ for all $h \in G$. If x and y lie in different cosets of A then we have $\pi(x)^{-1}\pi(y) = g^2x^{-1}y$, and both $\pi(x)^{-1}\pi(y)$ and $x^{-1}y$ are not in A. Let $h \in G$ be arbitrary. If $h \in A$ then neither $h\pi(x)^{-1}\pi(y)$ nor $hx^{-1}y$ are in A, and hence we get $\chi(h\pi(x)^{-1}\pi(y)) = \chi(hx^{-1}y) = 0$. If on the other hand $h \in gA$, say $h = ga = a^{-1}g$, then we compute

$$\chi(h\pi(x)^{-1}\pi(y)) = \chi(g^3ax^{-1}y) = \chi(y^{-1}xa^{-1}g) = \chi(hy^{-1}x).$$

In any case, we see that the third requirement of Theorem 7.1.8 is satisfied, whence π is an orthogonal generic symmetry of χ. □

It is worth noting that, although Babai's theorem is an easy consequence of the results developed before, our proof of Theorem 7.2.2 does not give many information about the polytopes P constructed implicitly. Babai's original proof gives more insight. In fact, Babai always constructs P as a simplex whose vertices are arbitrarily chosen within certain open regions (in the Euclidean topology). So in our notation, Babai has shown that if G is not of one of the exceptional types, we have $G = \mathrm{OSym}(G, \rho)$, where ρ is the regular character of G.

7.3 Unitary generic symmetries

We have seen that the theory of generic symmetries can be easily extended to achieve results about orthogonal symmetries of orbits. As one might expect, the original theory can be modified in a similar way to handle questions on unitary symmetries of orbits. In principle, many definitions from the theory of orthogonal generic symmetries can be adapted easily to complex inner product spaces. However, the situation becomes much more transparent in the unitary setting. We will see that if a finite group G acts faithfully on a finite dimensional complex inner product space V by unitary transformations then most of its orbits admit no additional unitary symmetries (Theorem 7.3.1). In other words, if we define an "unitary generic symmetry group" $\mathrm{USym}(G, V)$ in a reasonable way, we would always have $G = \mathrm{USym}(G, V)$. For that reason, we will state Theorem 7.3.1 without introducing any terminology on unitary orbit symmetries or unitary generic symmetries.

In the following, we consider a finite dimensional complex inner product space V. The Hermitian inner product on V is assumed to be linear in the first argument and semi-linear in the second argument. For any subset $X \subseteq V$, we consider the *unitary symmetry group* $U(X)$ consisting of all permutations $X \to X$ which are restrictions of unitary maps $V \to V$. Of course, this definition coincides with the usual notion of unitary groups of inner product spaces if X is a linear subspace of V.

In contrast to our former approach, we will not equip V with its usual Zariski topology over the complex numbers. Instead, we equip V with the "real Zariski topology", that is, with the Zariski topology of V regarded as a vector space over $\mathbb{R}$. This is essentially due to the fact that the complex conjugation $\mathbb{C} \to \mathbb{C}$ is a rational map only if $\mathbb{C}$ is considered as a vector space over $\mathbb{R}$. In fact, a Hermitian inner product $V \times V \to \mathbb{C}$ is a rational map if V and $\mathbb{C}$ are regarded as vector spaces over $\mathbb{R}$, but it is not even continuous in the ordinary Zariski topology of complex vector spaces. The consequences of that obstacle are well illustrated in Example 7.3.2. Note that the real Zariski topology of V is strictly finer than the ordinary Zariski topology, that is, any subset of V which is open (or closed) in the ordinary Zariski topology is also open (or closed) in the real Zariski topology of V.

As we have already observed in the orthogonal setting, if G is any finite group acting linearly on a complex vector space V then B can be equipped with a G-invariant inner product so that G acts on V by unitary transformations. This is proven by the same averaging argument. More precisely, we can choose an arbitrary inner product $\beta\colon V \times V \to C$ to obtain a G-invariant inner product by setting

$$\langle x, y\rangle = \frac{1}{|G|}\sum_{g\in G}\beta(gx, gy).$$

So any linear action of G on some $\mathbb{C}$-vector space can be regarded as a unitary action.

We are ready to prove the main result of this section.

Theorem 7.3.1. *Let G be a finite group acting faithfully on a finite dimensional complex inner product space V by unitary transformations. Then there is a nonempty subset $O \subseteq V$ which is open in the real Zariski topology of V such that $G = U(Gx)$ holds for all $x \in O$.*

Proof. We consider V to be equipped with the real Zariski topology. We begin by constructing O as the intersection of finitely many nonempty open subsets of V. Since V is an irreducible topological space (Lemma 2.1.2), O must be a nonempty open set as well.

We first consider the set

$$X = \{x \in V : gx \neq x \text{ for all } g \in G \setminus \{1\}\} = \bigcap_{g\neq 1}\{x \in V : gx \neq x\}.$$

Since G acts faithfully on V, we see that X is a finite intersection of nonempty open subsets of V. So X is nonempty and open in V. For any permutation $\pi \in \mathrm{Sym}(G)$, we consider the set

$$O_\pi = \{x \in V : \langle \pi(g)x, \pi(1)x\rangle \neq \langle gx, x\rangle \text{ for some } g \in G\}.$$

This set is open by construction, although it may be empty for some π (such as for the identity). We define $O \subseteq V$ to be the intersection of X and of all those sets O_π, $\pi \in \mathrm{Sym}(G)$, which are nonempty. Then O is by construction a nonempty open set. We claim that the canonical morphism $G \to U(Gx)$ is an isomorphism for all $x \in O$.

Let $w \in O$ be arbitrary. Since $w \in X$, it is clear that $G \to U(Gw)$ is injective. To prove surjectivity, let $\alpha \in U(V)$ be an arbitrary unitary transformation permuting the elements of the orbit Gw, say $\alpha(gw) = \pi(g)w$ for all $g \in G$, where $\pi \in \mathrm{Sym}(G)$ is a certain permutation. We get

$$\langle \pi(g)w, \pi(1)w\rangle = \langle \alpha(gw), \alpha(w)\rangle = \langle gw, w\rangle \text{ for all } g \in G.$$

This means $w \notin O_\pi$, which by definition of O, implies $O_\pi = \emptyset$. Consequently, the equations

$$\langle \pi(g)v, \pi(1)v\rangle = \langle gv, v\rangle \tag{7.2}$$

hold for all $v \in V$ and all $g \in G$. By plugging $v = x+y$ into (7.2) for $x, y \in V$ arbitrary, and expanding both sides, we get

$$\begin{aligned}\langle \pi(g)x, \pi(1)x\rangle + \langle \pi(g)x, \pi(1)y\rangle + \langle \pi(g)y, \pi(1)x\rangle + \langle \pi(g)y, \pi(1)y\rangle \\ = \langle gx, x\rangle + \langle gx, y\rangle + \langle gy, x\rangle + \langle gy, y\rangle\end{aligned}$$

for all $x, y \in V$ and all $g \in G$. By applying (7.2) again and canceling common terms, we get

$$\langle \pi(g)x, \pi(1)y\rangle + \langle \pi(g)y, \pi(1)x\rangle = \langle gx, y\rangle + \langle gy, x\rangle \tag{7.3}$$

for all $x, y \in V$ and all $g \in G$. In (7.3) we replace y by iy, and we multiply both sides by i to obtain the equations

$$\langle \pi(g)x, \pi(1)y\rangle - \langle \pi(g)y, \pi(1)x\rangle = \langle gx, y\rangle - \langle gy, x\rangle \tag{7.4}$$

for all $x, y \in V$ and all $g \in G$. Finally, by taking sums of (7.3) and (7.4) and dividing both sides by two, we get $\langle \pi(g)x, \pi(1)y\rangle = \langle gx, y\rangle$ and hence $\langle \pi(1)^{-1}\pi(g)x, y\rangle = \langle gx, y\rangle$ for all $x, y \in V$ and all $g \in G$. Since G acts faithfully on V, we conclude $\pi(g) = \pi(1)g$ for all $g \in G$. By definition of π, we get $\alpha(gw) = \pi(g)w = \pi(1)gw$ for all $g \in G$. This finally shows that the restriction of α to the orbit Gw is just the left multiplication by some element of G (proving the surjectivity of $G \to U(Gw)$). □

The proof of Theorem 7.3.1 is constructive, as it gives a concrete prescription how to find points $x \in V$ satisfying $G = U(Gx)$. We illustrate how such points can be found by looking at a small (but nontrivial) example.

Example 7.3.2. We consider $V = \mathbb{C}^2$ with the standard inner product ($\langle x, y\rangle = xy^*$). Let $G \leq U(V)$ be the cyclic group of order four generated by the matrix

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

In the following, we determine those points $x \in V$ for which $G = U(Gx)$ holds.

To exclude the trivial case, we observe that for $x = 0$ the canonical map $G \to U(Gx)$ is not injective. For all other points $0 \neq x \in V$, the map $G \to U(Gx)$ is injective since no non-identity element of G has the eigenvalue 1. In the terminology of the proof of Theorem 7.3.1, we have $X = V \setminus \{0\}$.

Next, we consider any nonzero point $x = (a, b)^\intercal \in V$ such that $\overline{a} \cdot b = a \cdot \overline{b}$. This property ensures that x and gx are orthogonal (and, in particular, linearly independent). Now the linear map $\alpha \in \mathrm{GL}(V)$ with $\alpha(x) = x$ and $\alpha(gx) = -gx$ is clearly unitary (since it maps an orthonormal basis to another orthonormal basis), and it permutes the orbit Gx (since $g^2x = -x$ and $g^3x = -gx$). As a non-identity map fixing x, α cannot be a left multiplication by some element of G, so we see that $G \to U(Gx)$ is not surjective.

Finally, let $x = (a, b)^\intercal \in V$ be an arbitrary point such that $\overline{a} \cdot b \neq a \cdot \overline{b}$. Then we see that the four complex numbers $\langle hx, x\rangle$, $h \in G$, are all distinct. In the notation of the proof of Theorem 7.3.1, we see that $x \in O_\pi$ holds for any permutation $\pi \in \mathrm{Sym}(G)$ which is not the left multiplication by $\pi(1)$. Since $O_\pi = \emptyset$ if π is a left multiplication, we see that $x \in O$, and the proof of Theorem 7.3.1 guarantees that $G \to U(Gx)$ is actually an isomorphism.

In conclusion, a point $x \in V$ satisfies $G = U(Gx)$ if and only if x is an element of the set

$$O = \left\{(a, b)^\intercal \in V : \overline{a} \cdot b \neq a \cdot \overline{b}\right\}.$$

This set is clearly open in the real Zariski topology of V (Theorem 7.3.1 only guarantees that it has a nonempty interior). In the ordinary Zariski topology of V however, O has an empty interior since its complement $V \setminus O$ contains the dense subset $\mathbb{R}^2 \subset V$. So in fact both O and $V \setminus O$ are dense in the ordinary Zariski topology of V.

Bibliography

[1] László Babai. “Symmetry Groups of Vertex-transitive Polytopes”. In: *Geometriae Dedicata* 6.3 (1977). DOI: 10.1007/BF02429904 (cit. on pp. 6, 7).

[2] Alexander I. Barvinok and Anatoly M. Vershik. “Convex Hulls of Orbits of Representations of Finite Groups, and Combinatorial Optimization”. In: *Func. Anal. Appl.* 22.3 (1988), pp. 224–225. DOI: 10.1007/BF01077628 (cit. on p. 7).

[3] Barbara Baumeister, Christian Haase, Benjamin Nill, and Andreas Paffenholz. “On Permutation Polytopes”. In: *Adv. Math.* 222.2 (2009), pp. 431–452. DOI: 10.1016/j.aim.2009.05.003 (cit. on p. 7).

[4] Charles W Curtis and Irving Reiner. *Methods of Representation Theory: With Applications to Finite Groups and Orders. Vol. I.* New York: Wiley, 1990 (cit. on pp. 15, 34, 35, 50, 78).

[5] John D Dixon and Brian Mortimer. *Permutation groups*. Vol. 163. Graduate Texts in Mathematics. New York: Springer, 1996 (cit. on p. 17).

[6] Jean-Paul Doignon. “Any Finite Group is the Group of Some Binary, Convex Polytope”. In: *Discrete Comput. Geom.* 59.2 (2018), pp. 451–460. DOI: 10.1007/s00454-017-9945-0 (cit. on p. 6).

[7] David Steven Dummit and Richard M Foote. *Abstract algebra*. Vol. 3. Hoboken: Wiley, 2004 (cit. on p. 9).

[8] Erik Friese. “Unitary groups as stabilizers of orbits”. In: *Arch. Math. (Basel)* 109.2 (2017), pp. 101–103. DOI: 10.1007/s00013-017-1065-9 (cit. on pp. 5, 115).

[9] Erik Friese and Frieder Ladisch. “Affine Symmetries of Orbit Polytopes”. In: *Adv. Math.* 288 (2016), pp. 386–425. DOI: 10.1016/j.aim.2015.10.021 (cit. on pp. 5, 16, 34, 97).

[10] Erik Friese and Frieder Ladisch. “Classification of affine symmetry groups of orbit polytopes”. In: *J. Algebr. Comb* (2017). DOI: 10.1007/s10801-017-0804-0 (cit. on pp. 5, 16, 23, 32, 49, 50, 60, 77, 97).

[11] Christopher D. Godsil. “GRRs for Nonsolvable Groups”. In: *Algebraic Methods in Graph Theory.* (Szeged, 1978). Colloq. Math. Soc. János Bolyai 25. Amsterdam: North-Holland, 1981, pp. 221–239 (cit. on p. 7).

[12] Robert M. Guralnick and David Perkinson. “Permutation Polytopes and Indecomposable Elements in Permutation Groups”. In: *J. Combin. Theory Ser. A* 113.7 (2006), pp. 1243–1256. DOI: 10.1016/j.jcta.2005.11.004 (cit. on p. 7).

[13] Katrin Herr, Thomas Rehn, and Achill Schürmann. "Exploiting symmetry in integer convex optimization using core points". In: *Operations Research Letters* 41.3 (2013), pp. 298–304. DOI: `https://doi.org/10.1016/j.orl.2013.02.007` (cit. on p. 7).

[14] Katrin Herr, Thomas Rehn, and Achill Schürmann. "On Lattice-Free Orbit Polytopes". In: *Discrete Comput. Geom.* 53.1 (2015), pp. 144–172. DOI: `10.1007/s00454-014-9638-x` (cit. on p. 7).

[15] Georg Hofmann and Karl-Hermann Neeb. "On Convex Hulls of Orbits of Coxeter Groups and Weyl Groups". In: *Münster J. Math.* 7.2 (2014), pp. 463–487. DOI: `10.17879/58269762646` (cit. on p. 7).

[16] I. Martin Isaacs. "Linear Groups as Stabilizers of Sets". In: *Proc. Amer. Math. Soc.* 62.1 (1977), pp. 28–30. DOI: `10.2307/2041939` (cit. on pp. 6, 7, 45, 49).

[17] I. Martin Isaacs. *Character Theory of Finite Groups*. corrected reprint. New York: Dover Publications, 1994 (cit. on pp. 15, 40, 78, 99).

[18] George Kempf. *Algebraic varieties*. Vol. 172. LMS Lecture Note Series. Cambridge University Press, 1993 (cit. on p. 28).

[19] Frieder Ladisch. "Groups with a Nontrivial Nonideal Kernel". In: *Arxiv Preprint* (2016) (cit. on pp. 5, 77, 91, 97, 98, 100).

[20] Frieder Ladisch and Achill Schürmann. "Equivalence of Lattice Orbit Polytopes". In: *Arxiv Preprint* (2017) (cit. on p. 7).

[21] Tsit Yuen Lam. *Lectures on Modules and Rings*. Graduate Texts in Mathematics 189. New York: Springer, 1999. DOI: `10.1007/978-1-4612-0525-8` (cit. on pp. 50, 51, 53).

[22] Tsit Yuen Lam. *A First Course in Noncommutative Rings*. 2nd ed. Graduate Texts in Mathematics 131. New York: Springer, 2001. DOI: `10.1007/978-1-4419-8616-0` (cit. on pp. 34, 35, 45, 50, 51, 57, 61, 74).

[23] Serge Lang. *Algebra*. Vol. 211. Graduate Texts in Mathematics. New York: Springer, 2002 (cit. on pp. 34, 35).

[24] Chi-Kwong Li and Thomas Milligan. "Linear Preservers of Finite Reflection Groups". In: *Linear Multilinear Algebra* 51.1 (2003), pp. 49–81. DOI: `10.1080/0308108031000053648` (cit. on p. 7).

[25] Chi-Kwong Li, Ilya Spitkovsky, and Nahum Zobin. "Finite Reflection Groups and Linear Preserver Problems". In: *Rocky Mountain J. Math.* 34.1 (2004), pp. 225–251. DOI: `10.1216/rmjm/1181069902` (cit. on p. 7).

[26] Chi-Kwong Li, Bit-Shun Tam, and Nam-Kiu Tsing. "Linear Maps Preserving Permutation and Stochastic Matrices". In: *Linear Algebra Appl.* 341 (2002), pp. 5–22. DOI: `10.1016/S0024-3795(00)00242-1` (cit. on p. 7).

[27] Nicholas McCarthy, David Ogilvie, Ilya Spitkovsky, and Nahum Zobin. "Birkhoff's Theorem and Convex Hulls of Coxeter Groups". In: *Linear Algebra Appl.* 347 (2002), pp. 219–231. DOI: `10.1016/S0024-3795(01)00556-0` (cit. on p. 7).

[28] Nicholas McCarthy, David Ogilvie, Nahum Zobin, and Veronica Zobina. "Convex Geometry of Coxeter-Invariant Polyhedra". In: *Trends in Banach Spaces and Operator Theory.* (Memphis, TN, 2001). Ed. by Anna Kamińska. Contemp. Math. 321. Providence, RI: Amer. Math. Soc., 2003, pp. 153–179. DOI: 10.1090/conm/321/05642 (cit. on p. 7).

[29] Shmuel Onn. "Geometry, Complexity, and Combinatorics of Permutation Polytopes". In: *J. Combin. Theory Ser. A* 64.1 (1993), pp. 31–49. DOI: 10.1016/0097-3165(93)90086-N (cit. on pp. 6, 7).

[30] Joseph J Rotman. *An introduction to the theory of groups.* Vol. 148. Graduate Texts in Mathematics. New York: Springer, 1995 (cit. on p. 17).

[31] Raman Sanyal, Frank Sottile, and Bernd Sturmfels. "Orbitopes". In: *Mathematika* 57.2 (2011), pp. 275–314. DOI: 10.1112/S002557931100132X (cit. on p. 7).

[32] Egon Schulte and Gordon Ian Williams. "Polytopes with Preassigned Automorphism Groups". In: *Discrete Comput. Geom.* 54.2 (2015), pp. 444–458. DOI: 10.1007/s00454-015-9710-1 (cit. on p. 6).

[33] Günter M Ziegler. *Lectures on polytopes.* Vol. 152. Graduate Texts in Mathematics. New York: Springer, 1995 (cit. on p. 46).

[34] Nahum Zobin and Veronica Zobina. "Coxeter Groups and Interpolation of Operators". In: *Integral Equations Operator Theory* 18.3 (1994), pp. 335–367. DOI: 10.1007/BF01206296 (cit. on p. 7).

List of abbreviations

$(\Bbbk G)^\times$ group of multiplicative units of the algebra $\Bbbk G$, page 51

$[g,h]$ commutator of group elements g,h, page 102

$\mathrm{AGL}(P)$ affine symmetry group of a polytope P, page 46

$\mathrm{Amp}(V)$ set of ample points of a module V, page 25

$\mathrm{Ann}(V)$ annihilator of a module V, page 117

$\mathrm{Ann}(v)$ annihilator of v, page 50

$\mathrm{Sym}^{\mathrm{ad}}(G,V)$ group of admissible generic symmetries of V, page 67

$\chi \times \psi$ Character of a group which is a direct product $G = A \times B$, given by characters χ of A and ψ of B, page 99

χ^G induced character, page 91

$\mathrm{Eig}(g,\lambda)$ Eigenspace of a group element $g \in G$ (in some given $\Bbbk G$-module) with corresponding eigenvalue λ, page 38

$\mathbb{F}_q$ finite field of order q, page 31

$\mathrm{Gen}(V)$ set of all generic points of V, page 32

$\mathrm{GL}(X)$ linear symmetries of a set X, page 15

$\mathrm{GL}_{\Bbbk G}(V)$ automorphism group of a $\Bbbk G$-module V, page 52

$L_{\mathcal{J}}$ ideal closure of a left ideal L, page 55

$\chi_{\mathcal{I}}$ ideal constituent of a character χ, page 80

$L_{\mathcal{I}}$ ideal constituent of a left ideal L, page 55

$V_{\mathcal{I}}$ ideal constituent of a cyclic module V, page 71

$\iota\chi$ Frobenius-Schur indicator of a character χ, page 99

ι_g left multiplication by a group element g, page 18

$\mathrm{Iv}(G,V)$ irrelevant generic symmetries of a module V, page 21

$\mathrm{Iv}(G,v)$ irrelevant orbit symmetries of v, page 17

$\Bbbk G$ Group algebra associated to a field $\Bbbk$ and a finite group G, page 15

$\Bbbk[V]$ $\Bbbk$-algebra of polynomial functions $V \to \Bbbk$, page 9

$\mathrm{Ker}(\chi)$ kernel of a character χ, page 79

$\mathrm{Ker}(V)$ kernel of V, page 21

$\chi_{\mathcal{L}}$ left ideal constituent of a character χ, page 80

$\mathcal{L}_{\Bbbk G}$ lattice of left ideals of $\Bbbk G$, page 55

$\mathcal{L}_{\Bbbk G}(\pi)$ lattice of left ideals of $\Bbbk G$ for which π is an ic-symmetry, page 55

$\mathcal{L}_{\Bbbk G}^{\mathrm{ad}}(\pi)$ lattice of left ideals of $\Bbbk G$ for which π is an admissible ic-symmetry, page 60

$\chi_{\mathcal{N}}$ non-ideal constituent of a character χ, page 80

$L_{\mathcal{N}}$ non-ideal constituent of a left ideal L, page 62

$V_{\mathcal{N}}$ non-ideal constituent of a cyclic module V, page 71

$\mathrm{Orb}(G, v)$ orbit polytope of a group G at some vector v, page 47

$\mathrm{OSym}(G, \chi)$ orthogonal generic symmetry group of a character χ of G, page 118

$\mathrm{OSym}(G, V)$ group of orthogonal generic symmetries of V, page 116

$\mathrm{OSym}(G, v)$ group of orthogonal orbit symmetries of v, page 116

$\mathcal{P}(X)$ power set of a set X, page 107

$\mathrm{Sym}(G, V)$ generic symmetry group of V, page 20

$\mathrm{Sym}(G, v)$ orbit symmetries of v, page 17

$\mathrm{Sym}(X)$ symmetric group on a set X, page 15

$\widehat{V}_w$ the natural $\Bbbk\,\mathrm{Sym}(G, w)$-module given by a generator w of a cyclic $\Bbbk G$-module V, page 39

$\mathrm{wt}(x)$ weight of a vector x, page 104

$\mathrm{zeros}(I)$ common zero set of a set I of polynomial functions, page 9

$C\Gamma$ cut space of a graph Γ, page 107

C_n cyclic group of order n, page 19

D_n dihedral group of order $2n$, page 19

$f^{\mathbb{E}}$ natural extension of a homomorphism to scalar extensions, page 53

G^2 subgroup of G generated by all squares, page 103

G_v stabilizer of v in G, page 17

Q_8 quaternion group of order 8, page 90

$V(\pi)$ set of all points of V with orbit symmetry π, page 19

V^* dual space of a vector space V, page 25

$V^{\mathbb{E}}$ scalar extension of a vector space V to an extension field $\mathbb{E}$, page 11

Index