UPPSALA
UNIVERSITET

An Introduction to the McKay Correspondence
Master Thesis in Physics

Author: Max Lindh
Supervisor: Martin Herschend
Examiner: Rikard Enberg

Abstract

In this project we provide an introduction to the classical McKay correspondence. After first laying out the framework for how the finite subgroups of SU(2) are obtained from the Platonic solids, we provide summaries of the basics in the relevant mathematical fields needed to state the correspondence. In Chapter 2, we present the foundational results of character theory, and outline the Dixon restricted character algorithm for finding the irreducible representation matrices of finite groups. In Chapter 3, we give an introduction to classical algebraic geometry, introducing the notions of affine and projective algebraic sets, provide a justification for the notion of a morphism thereof, and employ these tools to construct the blow-up of a singularity. In Chapter 4, we provide a brief overview of the elements of classical invariant theory, including Hilbert's theorem for the finite generation of invariants under the action of finite groups, and then use this information to express orbifolds formed under the action of the finite subgroups of SU(2) as algebraic sets. Finally, we present the McKay correspondence in the ultimate chapter, and provide brief comments on how the McKay correspondence has been explained and generalized in recent decades.

Populärvetenskaplig Sammanfattning

Denna avhandlingen söker ge en heuristisk introduktion till McKays överensstämmelse som visar på en stark koppling mellan den algebraiska geometrin och representationsteorin för undergrupperna till den speciella unitära gruppen av dimension två. Mer specifikt upptäckte John McKay vid slutet av sjuttiotalet att de diagram som man får fram av upplösningen av singulariteterna hos varieteterna som beskriver orbifalderna av det två-dimensionella komplexa rummet under verkan av dessa undergrupper stämmer överens med de diagram som man får fram av att betrakta samma undergruppers irreducibla representationers morfismegenskaper.

För att kunna uttala sig om detta i mer precision går vi i denna avhandling igenom grunderna till karaktärsteori, algebraisk geometri, och invariantteori. I synnerhet så ger vi en kort överblick över en algoritm för att finna de irreducibla representationerna till ändliga grupper. Samtliga av dessa grenar har visat sig ha stora användningsområden inom teoretisk fysik, i synnerhet inom strängteori och spegelsymmetri. En bättre förståelse av denna överensstämmelse, och de närliggande matematiska redskapen, hjälper oss att utforma, och tolka, nya fysikaliska teorier.

The number of people who have helped me on this thesis is far from insignificant. I would like to start by thanking my supervisor Martin Herschend for his extensive patience, generosity, attention to detail, and never-failing commitment in guiding me through this long process.

Additionally, I would like to thank Jian Qiu and Alexandra Gasanova for the many enlightening discussions we have had and the help and guidance they have provided me, in light on neither of them being, in any official capacity, my supervisor. Also, I should mention Igor Dolgachev, one of the authors in my bibliography, who is not just a scholar, but also a gentleman who answered several letters I wrote him regarding his text, offering detailed clarifications.

Of my friends, I would be amiss if I did not acknowledge the support shown to me by Nikos Iakovidis, Lisa Lokteva, Angelo Barthélemy, and Marisa Wood.

In particular Xiao Kaijian stands out, who more than any friend I have ever had has never ceased to be there for me in the worst of times.

Finally, but most importantly, I would like to thank my parents. I could not have done this without you.

"Digressions, incontestably, are the sun-shine;—they are the life, the soul of reading;—take them out of this book for instance,—you might as well take the book along with them;—one cold eternal winter would reign in every page of it; restore them to the writer;—he steps forth like a bridegroom,—bids All hail; brings in variety, and forbids the appetite to fail."

Rev. Laurence Sterne,
The Life and Opinions of Tristram Shandy, Gentleman.

"A proof is a proof. What kind of a proof? It's a proof. A proof is a proof. And when you have a good proof, it's because it's proven."

The Rt Hon. Jean Chrétien,
Prime Minister of Canada,
1993 – 2003.

Contents

CHAPTER 1

Introduction

As a field of study in theoretical physics, mirror symmetry has its origin in an observation made in the late 1980s that different couples of Calabi-Yau manifolds and Kähler classes living on these manifolds may give rise to string theories that are physically equivalent in that all their predictions are the same. Further investigation would soon enough establish that such couples always appeared in pairs, soon to be termed *mirror pairs.* At this early stage, as is often the case in theoretical physics, the theory was mathematically ill-defined, vague, and ambiguous, but soon enough mathematicians were introduced to the phenomenon, and in the early 1990s, a fully rigorous field was established in *homological mirror symmetry* [1].

It is in connection with mirror symmetry that the McKay correspondence (in fact discovered long before mirror symmetry even emerged on the scene) proves itself to be of relevance for the physicist. In fact, mirror symmetry is but one area in which algebraic geometry as a tool and the McKay correspondence in particular demonstrate their usefulness for the same. The specifics of this connection—Fourier-Mukai, quiver representations and quiver gauge theory, derived category theory, the dynamics of Dirichlet branes—is of course far beond the scope of this master thesis, however interesting they nonetheless may be. Suffice it to say that more than ample justification exists for a physicist to want to study this seemingly entirely abstract mathematical phenomenon. Here we will concern ourselves with the McKay correspondence in its simplest incarnation, the one in which John McKay originally discovered it [2].

Before we may do so, however, a little background is needed to provide some solid ground on which to stand. Above all, we need to specify in the relation to the study of what particular constructs the McKay correspondence appears. To do so, we commence by going back to the ancient Greeks.

1. The Platonic Solids

It is lost to history which mortal mind first conceived of the Platonic solids. Certainly it was not Plato, for in the Platonic dialogue in which they appear, *Timaeus* [3], he does not lay claim to their discovery but attributes it to others. The Platonic dialogues, when arranged in order, form a grand narrative of the life of Plato's master Socrates, and in this context, *Timaeus* takes place just the day after Socrates has delivered his fanciful discourse on how a city-state most ideally should be governed, which is recorded in *The Republic.* The philosopher has invited over three of his guests who heard him speak last night, these being Critias, Hermocrates, and the titular character Timaeus. As yesterday Socrates gave a grand oration on politics for the benefit of the three gentlemen, by prior agreement they are now to give similar presentations on their areas of expertise as repayment for the entertainment.

First out is Timaeus. A man from Locri, a Greek colony in Southern Italy, in fact just down the coast from Croton, where Pythagoras and his disciples had lived and worked a hundred years earlier [4], Timaeus is presented to us as "an expert in astronomy [who] has made it his main business to know the nature of the universe". Fittingly, he delivers as his discourse an account of how the Demiurge created the cosmos, which takes up the rest of the dialogue.

It may well be said that *Timaeus* is one of the strangest works in the Platonic corpus, reading like a hybrid of Euclid's *Elements* and Ovid's *Metamorphoses*, though lacking the former's clarity and the latter's poetry. The passages that concern us appear about a thirdway through Timaeus' monologue, when, noting that the classical elements of earth, water, air, and fire occupy volume, the eponymous hero ventures to assign them their ideal shapes. Arguing that the right angled isosceles triangles and the right angled triangle whose hypotenuse is twice its opposite are the "most excellent" two-dimensional shapes there are, Timaeus constructs from them the equilateral triangle, the square, and the regular pentagon, and from these in turn he constructs the five Platonic solids.

Being the least mobile of the elements, earth is assigned the cube, and being the most mobile, fire is assigned the tetrahedron. Awkwardly in-between these two extremes, air is assigned the octahedron and water is assigned the icosahedron. We are left with the dodecahedron, which Timaeus informs us is the shape in which the Demiurge has created the universe. (See Fig. 1.1.) On the basis of these axioms, Timaeus is able to derive an entire theory of geometrical alchemy, whilst the venerable Socrates, in other dialogues ever so eager to question the seemingly most self-evident of propositions, sits back and takes in the lecture without protest.

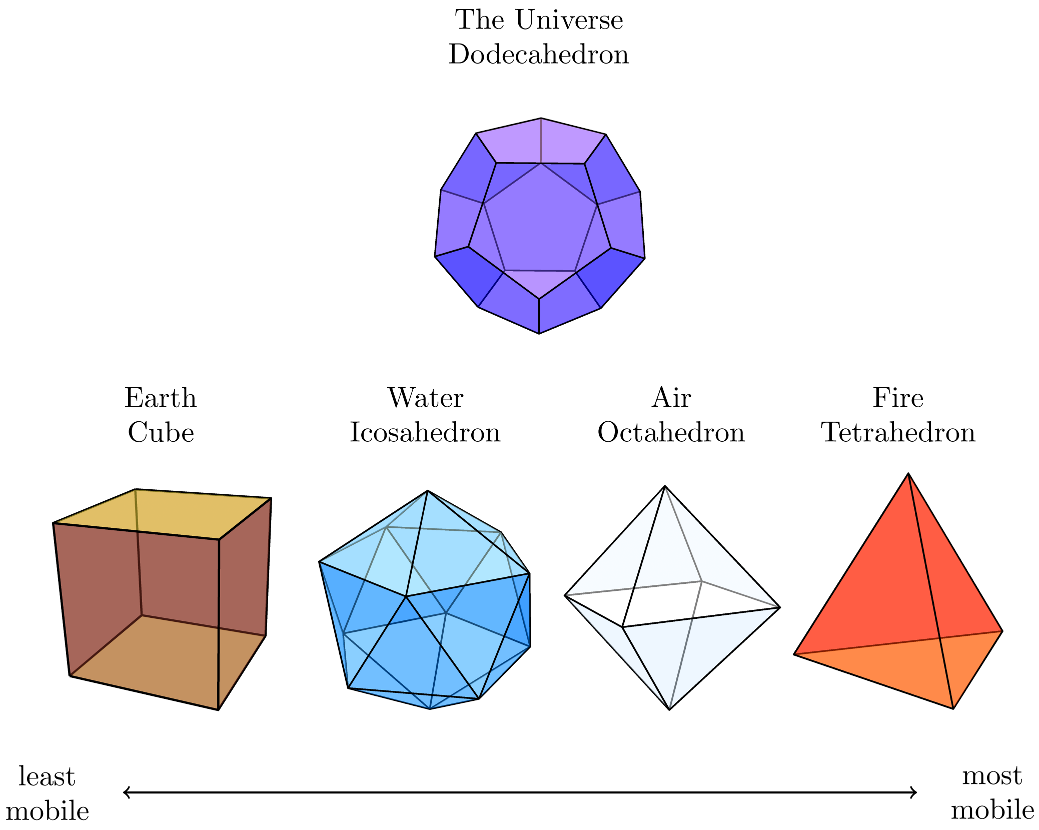


FIGURE 1.1. The Platonic solids and Timaeus' system of geometrical alchemy.

For the most part, the overwhelming majority, *Timaeus* is of course as textbook an example of sophistry as you are ever likely to find. Nonetheless, as Alfred Tarski duly noted [5], Plato may be an enemy, but falsehood is an even greater enemy, and by pure serendipity, Plato does appear to have stumbled upon a grain of truth when he writes that there is something transcendent about the solids which have come to bear his name.

2. The Finite Subgroups of SO(3)

Another "perfect shape" that figures in *Timaeus*—not counted among the Platonic solids as it is a surface and not a volume—is of course the sphere. Aesthetically pleasing as it was to the ancient philosopher, so it is too to us latter-day sophists on account of its symmetry, "its centre equidistance from its extremities in all directions, this of all shapes the most complete and most like itself, [...] incalculably more excellent than unlikeness" [3]. The study of symmetry being the domain of the group theorist, it is only appropriate to express this in group theoretical language.

Taking the sphere and rotating it by any angle around any axis, the result is a shape indistinguishable from what one started out with. Thus we say that the *rotational symmetry group* of the sphere is SO(3), the group of all rotations in three-dimensional space. All polyhedra possess such rotational symmetry groups—though of course in many cases, that group consists solely of the identity transformation—and these will all be finite subgroups of SO(3), congruent with the observation that under any rotation for which a polygon exhibits symmetry, a sphere too exhibits the same. When one then seeks to classify these finite subgroups, the Platonic solids, already noted for their three-dimensional symmetries, resurface.

At first glance, the task of such classification appears futile. Disregarding the trivial subgroup, there exists a limitless number of symmetrical polyhedra, and so one would expect there to exist a limitless number of finite subgroups of SO(3) as well, even up to isomorphism. We approach the problem systematically however, in the fashion laid out in [6], taking an arbitrary symmetrical polyhedron and its associated finite subgroup of SO(3) and noting that the action of any element of the group is to rotate the solid by some angle through an axis running through the center of the polyhedron. Since there is an finite number of elements in the group, there is a finite number of such associated axes. It follows from the symmetry of the polyhedron under the action of the group that the effect of the rotations on the axes will be to keep one fixed while permuting the others. Letting these axes then traverse the sphere rather than the polyhedron, the axes intersect the sphere exactly twice—upon entering and upon exiting—and labelling these points, it is then clear that the effect of the group action will be to permute them (see Fig. 1.2). The permutations thus incurred determine the finite subgroup completely.

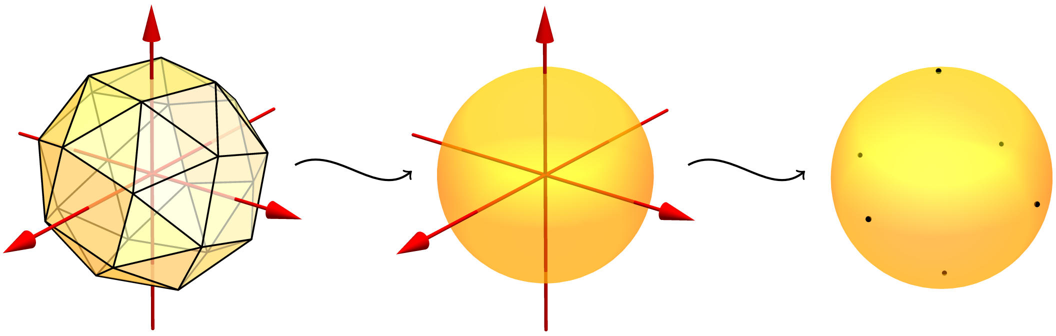


Figure 1.2. The axes of rotation of a general polyhedron (in this case the the snub cube) define points on the sphere that are permuted under rotation.

Our problem is thus rendered concrete and accessible: which such configurations of points on a sphere constrained by the nature of the group action (rotation) are permissible? To answer this question, we recall two results of elementary group theory.

Theorem 1.3. (Orbit-Stabilizer.) Let G be a finite group acting on a finite set X, of which x is an arbitrary element. If $G(x)$ and G_x is the orbit and stabilizer of x respectively, then

$$|G(x)||G_x| = |G|.$$

LEMMA 1.4. (BURNSIDE.) Let G be a finite group acting on a finite set X, and let X^g for $g \in G$ be the set of elements in X stabilized or "fixed" by g, and let N be the number of orbits in X. Then,

$$N = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

With this formula, the number of orbits N is then readily available. Every element $g \in G \backslash \{e\}$ fixes precisely two elements (the entry and exit of the pole) and e fixes every point on the sphere. Therefore,

$$N = \frac{1}{|G|}\big(2(|G|-1) + |X|\big). \tag{1.5}$$

If we pick N different points $x_1, \ldots, x_N$ from X, one from each orbit, then $|X| = \sum_{i=1}^N |G(x_i)|$. Plugging this into (1.5) and re-arranging, we obtain

$$2\left(1 - \frac{1}{|G|}\right) = N - \frac{1}{|G|}\sum_{i=1}^{N} |G(x_i)|.$$

Further taking into account the Orbit-Stabilizer Theorem then and rearranging, we have

$$2\left(1 - \frac{1}{|G|}\right) = \sum_{i=1}^{N}\left(1 - \frac{1}{|G_{x_i}|}\right). \tag{1.6}$$

Additional constraints may be placed on the values of the left and the right hand sides. Evidently, the left hand side cannot be greater than 2, since $1/|G| > 0$, and since G is not the trivial subgroup of SO(3), $|G| > 1$, meaning $(1 - \frac{1}{|G|}) \geq (1 - \frac{1}{2}) = \frac{1}{2}$, giving us

$$1 \leq 2\left(1 - \frac{1}{|G|}\right) < 2.$$

Pertaining to the right hand side, each point in the orbit is fixed by the action of at least two elements, a rotation around the axis going through the point, and the identity element. This gives us a lower boundary. As for the higher, each orbit may at most contain the same number of elements as the group itself, and since this number is finite, $(1 - \frac{1}{|G_{x_i}|}) < 1$. Therefore,

$$\frac{1}{2} \leq 1 - \frac{1}{|G_{x_i}|} < 1, \quad 1 \leq i \leq N.$$

If $N > 3$, then the right hand side of (1.6) must be equal to or larger than 2, making the equality unbalanced. Similarly, if $N = 1$, then the right hand side must be less than 1, once again making the equation unbalanced. Thus we may conclude that the subgroups of SO(2) must at least have two orbits and may at most have three.

Assume then that $N = 2$. Then,

$$2 - \frac{2}{|G|} = 2 - \left(\frac{1}{|G_{x_1}|} + \frac{1}{|G_{x_2}|}\right) \quad \Leftrightarrow \quad \frac{2}{|G|} = \frac{|G(x_1)|}{|G|} + \frac{|G(x_2)|}{|G|} \quad \Leftrightarrow \quad 2 = |G(x_1)| + |G(x_2)| = X,$$

thus obtaining that the set X consists of solely 2 points, which then define a single axis of rotation. The possible finite subgroups of SO(3) then obtained are those generated by rotations in the plane. From elementary considerations, it is easy to show that these are all cyclic groups.

If $N = 3$, then similarly to the case above, we obtain the formula

$$\frac{2}{|G|} + 1 = \frac{1}{|G_x|} + \frac{1}{|G_y|} + \frac{1}{|G_z|}. \tag{1.7}$$

Since $1/|G_i| < 1$, and the left hand side is strictly larger than one, (1.7) is considerably constrained in the number of solutions that it accepts. Specifically, only the possibilities listed in Tab. 1.8 are valid solutions.

	Stabilizers			*Orbits*			
Solution	$\lvert G_x\rvert$	$\lvert G_y\rvert$	$\lvert G_z\rvert$	$\lvert G(x)\rvert$	$\lvert G(y)\rvert$	$\lvert G(z)\rvert$	$\lvert G\rvert$
Regular n-gon	2	2	n	n	n	2	$2n$
Tetrahedron	2	3	3	6	4	4	12
Octahedron	2	3	4	12	8	6	24
Icosahedron	2	3	5	30	20	12	60

Table 1.8. Admissible solutions to equation (1.7), listed along with the cardinalities of the corresponding orbits, the symmetry groups, and the name of the polyhedra to which the symmetry groups correspond.

From symmetry considerations, it follows that the points in an orbit must be spread isometrically over the sphere, and through a series of similar and not too convoluted geometric and algebraic arguments, outlined in detail in [6] it is possible to ascertain what precisely these relative configurations of points are.

Identifying the points of the different orbits as corresponding to axes going through the vertices, edges, and faces of polyhedra respectively, we obtain that these are the symmetry groups of the regular n-gon; the tetrahedron; the octahedron (and/or the cube); and the icosahedron (and/or the dodecahedron) respectively (see Fig. 1.9). Thus we have once again obtained our Platonic solids.

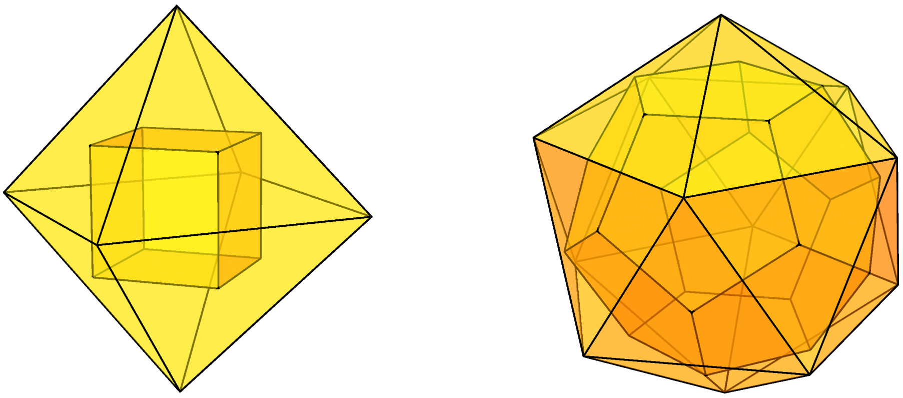


Figure 1.9. The cube and octahedron, and the icosahedron and dodecahedron respectively define the same subgroups of SO(3) as the orbits defined by their axes of rotation coincide.

3. The Finite Subgroups of SU(2)

To bring ourselves from SO(3) to SU(2), we begin by reminding ourselves of that both those groups are not only groups, but are also *topological spaces*. For this section, we draw on [7] and [8].

Definition 1.10. (Covering space.) Let X and Y be connected topological spaces. If there exists a continuous map $\varphi : Y \to X$ such that φ is surjective and for each $x \in X$ there exists an open subset $U \subset X$ containing x such that $\varphi^{-1}(U)$ is a disjoint union of open connected subsets in Y, each of which are mapped homeomorphically unto U by φ (see Fig. 1.11), Y is said to be a *covering space* of X.

The connectedness criteria ensures that the number of points in the preimage of any point in X is the same regardless of from where in X the point was chosen. We call this number the

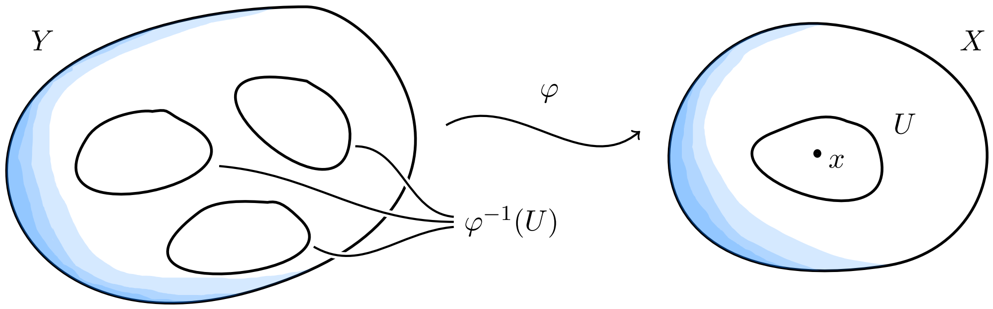


FIGURE 1.11. Schematic illustration of the concept of a covering space. The style of the illustration is inspired by the figures that may be found in [9].

index of the covering space. If X and Y both are topological groups (as indeed all Lie groups are), we may talk of Y as being a *covering group* of X if φ is additionally a continuous group morphism. In particular, if the index of this covering is two, then Y is said to be a *double cover of* X.

SU(2) does indeed provide such a double cover for SO(3) through a map of kernel $\{\pm\mathbb{1}\}$, the details of which can be found in [10]. Though the derivation of the form of this morphism $\varphi : \mathrm{SU}(2) \to \mathrm{SO}(3)$, the so-called *canonical mapping*, certainly is an interesting procedure on its own, as for now, for our purposes, we need only know *that* it exists and not precisely what it looks like.

LEMMA 1.12. Every finite subgroup of SU(2) is either the preimage of a finite subgroup of SO(3) under the canonical mapping, or is a cyclic group of odd order.

PROOF. It follows from the properties of a group morphism that every subgroup of SU(2) must map to a subgroup of SO(3) under φ. Self-evidently, every finite subgroup of SU(2) must be either of even or odd order. If a subgroup $\Gamma < \mathrm{SU}(2)$ then is of even order, 2 divides it, and so by Cauchy's theorem [11], it contains an element of order 2. The only such element of SU(2) is $-\mathbb{1}$, and so we may conclude that Γ is precisely the preimage of a finite subgroup of SO(3).

If, on the other hand, Γ is of odd order, φ then must map its elements one-to-one to an odd order subgroup of SO(3). The only such subgroups of SO(3) are the cyclic groups of odd order. This finishes the proof. □

As an additional note we may add that the preimage of a cyclic group of order n of SO(3) is a cyclic subgroup of order $2n$ of SU(2).

Our task is then clear: find a way to construct the preimages of the subgroups of SO(3)—which we had found earlier—and the finite subgroups of SU(2) will appear. Though in general the derivation of the form of the preimage of any given element of SO(3) in SU(2) under φ is just as tedious a procedure as deriving the form of φ itself, in our case we are lucky, since the cyclic groups are each one of them generated by just a single rotation, and all other finite subgroups of SO(3) are generated by just two. If we can find the preimages of just these at most two elements, the entirety of the preimage of the full subgroup will be available to us. To accomplish this, we take a look at the associated Lie algebras of SO(3) and SU(2).

Leaving aside the issue of providing a holistic definition of the Lie algebra (good examples of such descriptions can be found in [9] and [7]), we restrict ourselves to a definition sufficient for our particular needs. Both SO(3) and SU(2) are *matrix Lie groups*, and so we adopt the following definition from [8]:

Definition 1.13. (Exponential of a matrix.) Let X be a square matrix of finite dimension. The *matrix exponential of* X, denoted e^X or $\exp(X)$ is defined as

$$e^X := \sum_{m=0}^{\infty} \frac{X^m}{m!}.$$

Definition 1.14. (Lie algebra of a matrix Lie group.) Let $\mathcal{G}$ be a matrix Lie group. The *Lie algebra* of $\mathcal{G}$, denoted $\mathfrak{g}$, is the set of all matrices X such that $e^{tX} \in \mathcal{G}$ for all $t \in \mathbb{R}$.

We need of course point out that as a function the exponential map from a Lie algebra $\mathfrak{g}$ to its associated Lie group $\mathcal{G}$ needs not be surjective. Fortunately, this is not a problem for the two Lie groups currently under consideration. It is known that for every compact, connected Lie group, the exponential map from the Lie algebra to the Lie group is surjective [12]. As both SO(3) and SU(2) are compact and connected, we may conclude that every element in either group may be expressed as exponentials of elements in the algebras $\mathfrak{so}(3)$ and $\mathfrak{su}(2)$ respectively.

We state without proof (though proof can be found in [13]) that bases for the Lie algebras $\mathfrak{so}(3)$ and $\mathfrak{su}(2)$ may be given by the matrices

$$J_x = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad J_y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \qquad J_z = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and

$$\sigma_x = -\frac{1}{2}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad \sigma_y = -\frac{1}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \sigma_z = -\frac{1}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$

respectively (the latter are commonly referred to as the *Pauli matrices*). It is a matter of straight-forward computation to verify that the two bases obey the same commutation relations, specifically

$$[J_a, J_b] = \varepsilon_{abc} J_c, \qquad \text{and} \qquad [\sigma_a, \sigma_b] = \varepsilon_{abc}\sigma_c.$$

The two algebras then are isomorphic, with the isomorphism explicitly being given by $\overline{\varphi} : \mathfrak{su}(2) \to \mathfrak{so}(3)$, $x\sigma_x + y\sigma_y + z\sigma_z \mapsto xJ_x + yJ_y + zJ_z$. To properly then be able to make use of these tools, we add two final ingredients to the mixture.

Theorem 1.15. Let $\mathcal{G}$ and $\mathcal{H}$ be two Lie groups, with Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ respectively, and let $\Phi : \mathcal{G} \to \mathcal{H}$ be a Lie group homomorphism. Then there exists a unique linear map $\phi : \mathfrak{g} \to \mathfrak{h}$ such that

$$\Phi(e^X) = e^{\phi(X)}$$

for all $X \in \mathfrak{g}$. This map has the additional property that $\phi(AXA^{-1}) = \Phi(A)\phi(X)\Phi(A)^{-1}$ for all $X \in \mathfrak{g}$, $A \in \mathcal{G}$.

Proof. See [8]. □

Theorem 1.16. Let $\mathcal{G}$ and $\mathcal{H}$ be two Lie groups, with Lie algebras $\mathfrak{g}$ and $\mathfrak{h}$ respectively, suppose $\mathcal{G}$ to be simply connected, and let $\phi : \mathfrak{g} \to \mathfrak{h}$ be a Lie algebra homomorphism. Then there exists a unique Lie group homomorphism $\Phi : \mathcal{G} \to \mathcal{H}$ such that

$$\Phi(e^X) = e^{\phi(X)}$$

for all $X \in \mathfrak{g}$.

Proof. See [8]. □

Theorems 1.15 and 1.16 then allow us to draw up the following commutative diagram,

$$\begin{tikzcd}
\mathrm{SU}(2) \arrow[r, "\varphi"] & \mathrm{SO}(3) \\
\mathfrak{su}(2) \arrow[u, two heads, "\exp"] \arrow[r, "\sim", "\overline{\varphi}"'] \arrow[ur, phantom, "\circlearrowright"] & \mathfrak{so}(3) \arrow[u, two heads, "\exp"']
\end{tikzcd}$$

and we may finally obtain the elements of the subgroups of SU(2) in that Lie group's defining representation.

Example 1.17. (Binary Octahedral Group.) The octahedral group can be generated from two elementary operations: a rotation by $\frac{\pi}{2}$ in the $x-y$ plane, and a rotation by $\frac{\pi}{2}$ in the $x-z$ plane (see Fig. 1.18). A rotation by θ in the $x-y$ plane is given by the matrix

$$\begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

which have eigenvectors

$$\begin{pmatrix} 1 \\ i \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 \\ -i \\ 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

with eigenvalues of $e^{+i\theta}$, $e^{-i\theta}$, and 1 respectively. Thus we may diagonalize to obtain

$$\begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ i & -i & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} e^{i\theta} & 0 & 0 \\ 0 & e^{-i\theta} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{i}{2} & 0 \\ \frac{1}{2} & \frac{i}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The central matrix on the right hand-side equals to the exponention of the diagonal matrix with diagonal entires $i\theta$, $-i\theta$, and 0, and so by Thm. 1.15, we find

$$\log \begin{pmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ i & -i & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} i\theta & 0 & 0 \\ 0 & -i\theta & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{2} & -\frac{i}{2} & 0 \\ \frac{1}{2} & \frac{i}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \theta & 0 \\ -\theta & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = -\theta J_z.$$

Similarly, a rotation by ϕ in the $x-z$ plane is given by the matrix

$$\begin{pmatrix} \cos\phi & 0 & -\sin\phi \\ 0 & 1 & 0 \\ \sin\phi & 0 & \cos\phi \end{pmatrix},$$

and by the same method as above, we obtain

$$\log \begin{pmatrix} \cos\phi & 0 & -\sin\phi \\ 0 & 1 & 0 \\ \sin\phi & 0 & \cos\phi \end{pmatrix} = \begin{pmatrix} 0 & 0 & -\phi \\ 0 & 0 & 0 \\ \phi & 0 & 0 \end{pmatrix} = -\phi J_y.$$

Passing these under the inverse of the isomorphism $\overline{\varphi}$, we then obtain

$$-\theta\sigma_z = \frac{\theta}{2}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \text{and} \qquad -\phi\sigma_y = \frac{\phi}{2}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

respectively. Exponentiating these and plugging in $\theta = \phi = \frac{\pi}{2}$, we then have the preimages of the generator elements being given by

$$a = \begin{pmatrix} e^{i\frac{\pi}{4}} & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix}, \qquad \text{and} \qquad b = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

As $a^4 = b^4 = -\mathbb{1}$, these elements then generate the entire preimage of the octahedral subgroup in SU(2), a subgroup that is known as the *binary octahedral group* and is commonly denoted $\mathbb{BO}$.

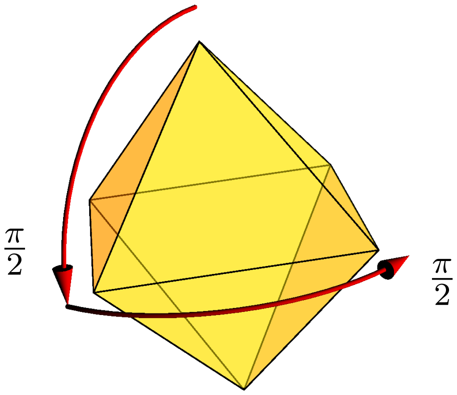


FIGURE 1.18. Generating elements of the octahedral rotational symmetry group.

Through this method of "reverse engineering", we obtain a complete list of all possible finite subgroups of SU(2). These are then the cyclical groups and the so-called *binary dihedral groups*, $\mathbb{B}D_{2n}$, and the *binary polyhedral groups* $\mathbb{BT}$, $\mathbb{BO}$, and $\mathbb{BD}$. The representation in which we obtain them is the *defining*, or *natural representation* of SU(2), restricted to the subgroups in question. For the rest of this work, whenever we shall say that a subgroup of SU(2) is in the natural representation, this is what we will be referring to.

4. The Classical McKay Correspondence

We are now finally at a position to introduce the classical McKay correspondence. Having found the finite subgroups of SU(2), we can delve into representation theory further and find their irreducible representations. For a given subgroup, we may take its irreducible representations and take the tensor products of each one with the natural representation. Morphisms may be constructed from these product representations back to the irreducible representations, and given a product representation and an irreducible representation, the set of morphisms from the former to the latter defines a vector space. Concerning ourselves with the dimensionalities of these morphism spaces, for each subgroup we may encode all this information in the form of a diagram.

On the other hand, we may consider the finite subgroups from the point of view of their action on $\mathbb{C}^2$ in the natural representation. $\mathbb{C}^2$ being a manifold, these actions define *orbifolds*, and using the tools of invariant theory, we may give these algebraic descriptions, embedding them as surfaces in $\mathbb{C}^3$, thereby taking on the form of *varieties*—a basic construct of algebraic geometry. The varieties thus obtained exhibit *singularities*, and when we resolve these through the process known as *blowing-up*, we end up with webs of subspaces known as *exceptional divisors*. The information of their intersections may similarly be encoded in diagrams.

When we compare the two sets of diagrams constructed, we discover that there is a close similarity, a similarity indicative of a deep relationship between these structures seemingly so alien to one another. This phenomenon is known as the *classical McKay correspondence*, and illuminating the process so hastily summarized in yet undefined jargon in the above two paragraphs will be the subject matter of the rest of this work.

In the next three chapters will respectively focus on the representation theoretical; the algebro-geometrical; and the invariant theoretical aspects of the McKay correspondence.

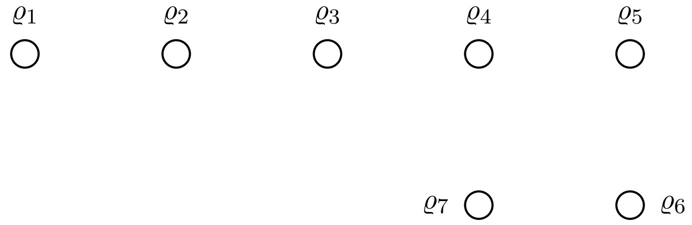
CHAPTER 2

Representation Theory

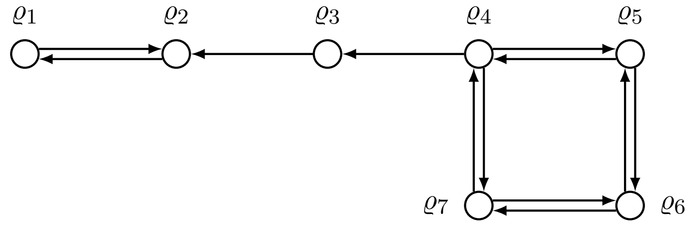
The subject matter of the following chapter is the construction of the irreducible representations of the different finite subgroups of SU(2) and how morphisms may be constructed between them and their tensor products with the natural representation. From the information contained therein, the so-called McKay quivers are then drawn up. We will show how these morphisms may be deduced using character theory, for which we restate the basic results. The irreducible representations of the cyclic and binary dihedral groups will be constructed from fundamental algebraic arguments. To find the irreducible representations of the binary polyhedral groups however, we shall make use of a schema known as Dixon's restricted character algorithm, which we furthermore shall provide exposition of. Throughout, we will liberally make use of results listed in Appendix A. Before we may start in earnest however, we need to establish what the McKay quiver of a group actually is.

Definition 2.1. (McKay Quiver.) Given a finite group G with natural representation ϱ_{Nat} and irreducible representations ϱ_i, the McKay quiver is constructed as follows:

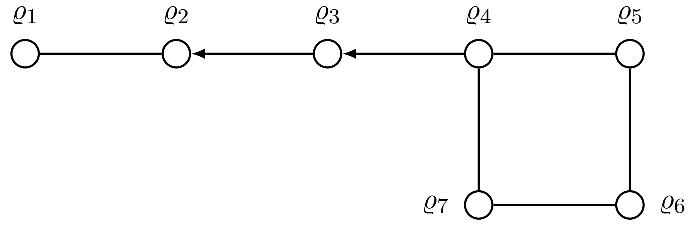
1. For every irreducible representation of G, draw a node.



2. If the dimensionality of the homomorphism space from the representation $\varrho_{\mathrm{Nat}} \otimes \varrho_i$ to the representation ϱ_j is n, draw n arrows from i to j.



3. In the diagram, for every time that two arrows occur going between two nodes in the opposite direction, replace said two arrows with a single undirected line.



The resultant figure is then the McKay quiver of the group G.

1. Character Theory

We assume the reader to be familiar with the basic results of character theory within the field of representation theory of finite groups. For the purpose of clarity, we restate the basic definitions and some associated results, drawing on [14], [15], and [16].

As detailed in Appendix A, every representation ϱ of a group G can be extended into a representation $\tilde{\varrho}$ of its group algebra over a field $\mathbb{F}$, $\mathbb{F}[G]$, by having it act on a generic element $a = \sum_{i=1}^{|G|} a_i g_i \in \mathbb{F}[G]$ as

$$\tilde{\varrho}\Big(\sum_{i=1}^{|G|} a_i g_i\Big) = \sum_{i=1}^{|G|} a_i \varrho(g_i), \qquad a_i \in \mathbb{F}.$$

We shall henceforth use ϱ when referring to a representation of a group and $\tilde{\varrho}$ when referring to the representation of an algebra. Furthermore, as detailed in the aforementioned appendix, every irreducible representation of a group is an irreducible representation of the group algebra and vice versa, and so we can transfer our entire discussion back and forth without any loss of generality.

Definition 2.2. (Character of a representation.) Let G be a finite group, and ϱ be a representation thereof over the field $\mathbb{C}$. The character χ of the representation ϱ is then defined to be a function $\chi : G \to \mathbb{C}$ given by

$$\chi(g) := \mathrm{tr}(\varrho(g))$$

Lemma 2.3. Let χ_V, χ_W be the characters of two representations of the group G corresponding to modules V and W over the field $\mathbb{C}$. Then the following statements hold true:

(i) $\chi_V(e) = \dim V$;
(ii) $\chi_V(g) = \chi_V(h)$ if $g, h \in G$ belong to the same conjugacy class;
(iii) $\chi_{V \oplus W}(g) = \chi_V(g) + \chi_W(g)$, $\forall g \in G$;
(iv) $\chi_{V \otimes W}(g) = \chi_V(g)\chi_W(g)$, $\forall g \in G$;
(v) $\chi_{V^*}(g) = \overline{\chi_V(g)}$, $\forall g \in G$, (V^* being the dual vector space of V);
(vi) $V \cong W \Rightarrow \chi_V(g) = \chi_W(g)$, $\forall g \in G$.

Definition 2.4. (Class functions.) The set of all functions $G \to \mathbb{C}$, call it $\mathcal{F}[G]$, form an associative algebra under addition given by $(f_1 + f_2)(g) := f_1(g) + f_2(g)$ and multiplication by scalars given by $(\lambda f)(g) := \lambda f(g)$. A subset of these is the set of functions that are invariant on the conjugacy classes of G. We call these the *class functions on* G, denoted $\mathcal{CF}[G]$, and note that this subset actually forms a subalgebra of $\mathcal{F}[G]$.

Lemma 2.5. The dimensionality of $\mathcal{CF}[G]$ equals to the number of conjugacy classes of G.

Proof. If the group G in question consists of n conjugacy classes $\{K_i\}$, then a natural basis for the algebra $\mathcal{CF}[G]$ is given by the class functions f_i defined by

$$f_i(g) := \begin{cases} 1, & g \in K_i, \\ 0, & g \notin K_i. \end{cases}$$

Thus we may conclude that $\mathcal{CF}[G]$ is of dimension n. □

Definition 2.6. (Inner product of class functions.) Let G be a group and let $\mu, \nu : G \to \mathbb{C}$ be two class functions. The inner product of μ and ν is then given as

$$\langle \mu, \nu \rangle := \frac{1}{|G|} \sum_{g \in G} \mu(g)\overline{\nu(g)}.$$

Lemma 2.7. Let V and W be two modules of a finite group G. Then the set of all vector space morphisms from V to W, denoted $\mathrm{Hom}(V, W)$, is itself a module of G.

Proof. In Cor. A.24 we note that the set of all group module morphisms from V to W has the structure of a vector space, and we may readily extend this structure to render all of $\mathrm{Hom}(V, W)$ a vector space, defining $(k\varphi) := k(\varphi(v))$ and $(\varphi + \theta)(v) := \varphi(v) + \theta(v)$ for all $\varphi, \theta \in \mathrm{Hom}(V, W)$. To see that this vector space is a group module, simply define a group action upon it from the predefined group actions $\circ$ and $\bullet$ on V and W by $\star : G \times \mathrm{Hom}(V, W) \to \mathrm{Hom}(V, W)$, $g \star \varphi(v) := g \bullet \varphi(g^{-1} \circ v)$, a group action which without difficulty can be verified to endow $\mathrm{Hom}(V, W)$ with the structure of a G-module. □

Lemma 2.8. For the group action defined above, every element of $\mathrm{Hom}_G(V, W)$ is invariant under the action of any element of G.

Proof. We have $\mathrm{Hom}_G(V, W) = \{\varphi \in \mathrm{Hom}(V, W) | \varphi(g \circ v) = g \bullet \varphi(v),\ \forall g \in G, v \in V\}$. Therefore, $g \star \varphi(v) = g \bullet \varphi(g^{-1} \circ v) = g \bullet g^{-1} \bullet \varphi(v) = \varphi(v)$, for all $\varphi \in \mathrm{Hom}_G(V, W)$. □

Being a G-invariant subspace of $\mathrm{Hom}(V, W)$, $\mathrm{Hom}_G(V, W)$ is as such of course a submodule of $\mathrm{Hom}(V, W)$.

Lemma 2.9. As G-modules, $\mathrm{Hom}(V, W)$ and $V^* \otimes W$ are isomorphic (V^* being the dual vector space of V).

Proof. $\dim(\mathrm{Hom}(V, W)) = \dim V \dim W = \dim V^* \dim W = \dim(V^* \otimes W)$, so the dimensionalities agree. We then define the map $\Phi : V^* \otimes W \to \mathrm{Hom}(V, W)$ by $f \otimes w \mapsto \alpha_{f \otimes w}$ such that $\alpha_{f\otimes w}(v) := f(v)w$. To demonstrate isomorphism, first we need to show that this map is well-defined as a bilinear map. We find

$$\begin{aligned}
\Phi((f + f') \otimes w)(v) &= (f + f')(v)w = f(v)w + f'(v)w = \Phi(f \otimes w)(v) + \Phi(f' \otimes w)(v),\\
\Phi(f \otimes (w + w'))(v) &= f(v)(w + w') = f(v)w + f(v)w' = \Phi(f \otimes w')(v) + \Phi(f \otimes w')(v),\\
\Phi((\lambda f) \otimes w)(v) &= (\lambda f)(v)w = \lambda(f(v)w) = \Phi(\lambda(f \otimes w))(v),\\
\Phi(f \otimes (\lambda w))(v) &= f(v)(\lambda)w = \lambda(f(v)w) = \Phi(\lambda(f \otimes w))(v).
\end{aligned}$$

Next, we verify that Φ is surjective. With a basis $\{v_1, \ldots, v_n\}$ of V and $\{w_1, \ldots, w_m\}$ of W, the morphisms β_{ij} defined by

$$\beta_{ij}(v_k) := \begin{cases} 0, & k \neq j, \\ w_i, & k = j, \end{cases}$$

provide a basis for $\mathrm{Hom}(V, W)$. Let $\{f_1, \ldots, f_n\}$ be a dual basis for V^* such that $f_i(v_j) = \delta_{ij}$. Then $\Phi(f_i \otimes w_j) = \beta_{ij}$, making Φ a surjective map. Finally, we show that Φ is a module homomorphism. Let $\diamond$ be the group action induced on $V^* \otimes W$ by $\circ$ and $\bullet$. Then,

$$\Phi(g \diamond (f \otimes w))(v) = \Phi(f(g^{-1} \circ v) \otimes (g \bullet w)) = g \bullet (f(g^{-1} \circ v)w) = g \star \Phi(f \otimes w)(v),$$

and the proof is done. □

Corollary 2.10. The subspace $(V^* \otimes W)_G := \{x \in V^* \otimes W | g \diamond x = x,\ \forall g \in G\}$ is isomorphic as a G-module to $\mathrm{Hom}_G(V, W)$.

Theorem 2.11. (The Grand Orthogonality Theorem.) The characters of the irreducible representations of a group are orthonormal with respect to the inner product up to equivalence.

Proof. (Mathematician's version.[1]) Let χ_V and χ_W be the characters of two irreducible representations corresponding to simple modules V and W. Then,

$$\begin{aligned}\langle\chi_W,\chi_V\rangle &= \frac{1}{|G|}\sum_{g\in G}\chi_W(g)\overline{\chi_V(g)} \\ &= \frac{1}{|G|}\sum_{g\in G}\chi_{V^*}(g)\chi_W(g) && \text{(by 2.3.v)} \\ &= \frac{1}{|G|}\sum_{g\in G}\chi_{V^*\otimes W}(g). && \text{(by 2.3.iv)}\end{aligned}$$

To evaluate this sum, we start by considering the element in the algebra $\mathbb{C}[G]$ defined by

$$\phi = \frac{1}{|G|}\sum_{g\in G} g,$$

and consider its action on elements of $V^*\otimes W$. For $x \in (V^*\otimes W)_G$, we find

$$\phi\diamond x = \frac{1}{|G|}\sum_{g\in G} g\diamond x = \frac{1}{|G|}\sum_{g\in G} x = x,$$

and for generic $x \in V^*\otimes W$, $h\in G$, we find

$$h\diamond(\phi\diamond x) = h\diamond\frac{1}{|G|}\sum_{g\in G} g\diamond x = \frac{1}{|G|}\sum_{g\in G}(h\diamond g)\diamond x = \frac{1}{|G|}\sum_{g\in G} g\diamond x = (\phi\diamond x),$$

meaning $\phi\diamond x\in(V^*\otimes W)_G$ for all $x\in V^*\otimes W$. Consequently, ϕ acts as a projection operator $V^*\otimes W\to(V^*\otimes W)_G$. If ϱ then is the representation corresponding to the module $V^*\otimes W$, then in it, ϕ is represented by

$$\varrho(\phi) = \frac{1}{|G|}\sum_{g\in G}\varrho(g),$$

which then has trace

$$\operatorname{tr}(\varrho(\phi)) = \frac{1}{|G|}\sum_{g\in G}\chi_{V^*\otimes W}(g) = \langle\chi_W,\chi_V\rangle,$$

and so, this construction has allowed us to get closer to determining the inner product $\langle\chi_W,\chi_V\rangle$. Now given a vector space X with subspace Y, and a projection operator $\varphi : X\to Y$, we can always change to a basis in which the matrix representation for φ is of the form

$$\begin{pmatrix} \overbrace{\begin{matrix}1 & \dots & 0\end{matrix}}^{n} & \overbrace{\begin{matrix}0 & \dots & 0\end{matrix}}^{m} \\ \begin{matrix}\vdots & \ddots & \vdots\end{matrix} & \begin{matrix}\vdots & \dots & \vdots\end{matrix} \\ \begin{matrix}0 & \dots & 1\end{matrix} & \begin{matrix}0 & \dots & 0\end{matrix} \\ \begin{matrix}0 & \dots & 0\end{matrix} & \begin{matrix}0 & \dots & 0\end{matrix} \\ \begin{matrix}\vdots & \ddots & \vdots\end{matrix} & \begin{matrix}\vdots & \ddots & \vdots\end{matrix} \\ \begin{matrix}0 & \dots & 0\end{matrix} & \begin{matrix}0 & \dots & 0\end{matrix} \end{pmatrix},$$

in which the first n columns correspond to the basis vectors of the subspace Y, and the latter m columns correspond to the orthogonal complement of Y in X, thus signifying that the part of a vector being operated upon that are in Y is left intact, while the component outside of Y is annihilated. Since the trace of a matrix is invariant under a change of basis, $\operatorname{tr}(\operatorname{Mat}(\varphi)) = \dim(Y)$, and consequently, $\operatorname{tr}(\varrho(\phi)) = \dim((V^*\otimes W)_G)$.

[1] The physicist's version, which may be found in [17], makes use of unitarity and is more matrix-oriented in nature.

As noted in Cor. 2.10, $(V^* \otimes W)_G$ and $\mathrm{Hom}_G(V,W)$ are isomorphic, and since V and W are both simple modules, by Schur's lemma (Lems. A.38, A.39),

$$\dim(\mathrm{Hom}_G(V,W)) = \begin{cases} 1, & \text{if } V \cong W, \\ 0, & \text{if } V \ncong W, \end{cases}$$

Thus

$$\langle \chi_W, \chi_V \rangle = \langle \chi_V, \chi_W \rangle = \begin{cases} 1, & \text{if } V \cong W, \\ 0, & \text{if } V \ncong W, \end{cases}$$

and the proof is finished. □

Lemma 2.12. The characters of the irreducible representations of a group G (up to isomorphism) provide a basis for $\mathcal{CF}[G]$.

Proof. Thm. 2.11 establishes orthonormality between the characters of irreducible representations up to isomorphism, and so all that remains is to show that these truly span all of $\mathcal{CF}[G]$. We do this by showing that any class function $\alpha \in \mathcal{CF}[G]$ orthogonal to all characters of irreducible representations ($\langle \alpha, \chi_V \rangle = 0$ for all simple modules V and by extension $\langle \alpha, \chi_W \rangle = 0$ for all semisimple modules W) must be the zero map.

For any $\beta \in \mathcal{CF}[G]$, we may define the element $\sigma_\beta \in \mathbb{C}[G]$ by

$$\sigma_\beta := \frac{1}{|G|} \sum_{g \in G} \beta(g) g.$$

As β is a class function, $\beta(g) = \beta(h^{-1}gh)$ for any $g, h \in G$, and so

$$h^{-1}\sigma_\beta h = \frac{1}{|G|} \sum_{g \in G} \beta(g) h^{-1}gh = \frac{1}{|G|} \sum_{g \in G} \beta(h^{-1}gh) h^{-1}gh = \sigma_\beta,$$

meaning that the action of σ_β commutes with the action of any $h \in G$. Consider then a module W. Since $g \cdot w \in W$ for each $g \in G$, $w \in W$, it follows that $\sigma_\beta \cdot w \in W$. But σ_β is not just a *self-mapping* $W \to W$. By the commutativity shown above,

$$\sigma_\beta \cdot (g \cdot w) = (\sigma_\beta g) \cdot w = (g \sigma_\beta) \cdot w = g \cdot (\sigma_\beta \cdot w),$$

meaning that the action of σ_β defines a full *module endomorphism* $W \to W$.

Take then σ for α mentioned before, and let it act upon a simple module V corresponding to an irreducible representation ϱ. As σ_α defines a module endomorphism, by Schur's lemma, $\varrho(\sigma_\alpha) = \lambda \cdot \mathbb{1}$ for some $\lambda \in \mathbb{C}$ for all $g \in G$. Therefore, $\mathrm{tr}(\varrho(\sigma_\alpha)) = \lambda \dim V$, and so,

$$\lambda = \frac{1}{\dim V} \mathrm{tr}(\varrho(\sigma_\alpha)) = \frac{1}{\dim V} \frac{1}{|G|} \sum_{g \in G} \alpha(g) \chi_V(g) = \frac{1}{\dim V} \frac{1}{|G|} \sum_{g \in G} \alpha(g) \overline{\chi_{V^*}(g)} = \frac{1}{\dim V} \langle \alpha, \chi_{V^*} \rangle = 0,$$

as we set $\langle \alpha, \chi_W \rangle = 0$ for all semisimple modules W. Thus the action of σ_α on any simple module is the zero map, and so it follows that it must also be on all semisimple modules. In particular, this holds true for $(\mathbb{C}[G])^\circ$ itself, giving us

$$0 = \sigma_\alpha \cdot 1 = \frac{1}{|G|} \alpha(g) g \cdot 1 = \frac{1}{|G|} \alpha(g) g,$$

and so $\alpha(g) = 0$ for all $g \in G$ by the linear independence of the group elements in the group algebra, meaning $\alpha = 0$. This finishes the proof. □

Corollary 2.13. The number of inequivalent irreducible representations of a finite group equals its number of conjugacy classes.

Lemma 2.14. Let $V \cong \bigoplus_i V_i^{m_i}$ be a module of a finite group G, which by Maschke's theorem (Thm. A.42) is isomorphic to a direct sum of simple modules V_i, each appearing with multiplicity m_i. Then,

$$\langle \chi_V, \chi_{V_i} \rangle = m_i.$$

Proof.

$$\langle \chi_V, \chi_{V_i} \rangle = \langle \chi_{\bigoplus_j V_j^{m_j}}, \chi_{V_i} \rangle = \sum_j m_j \langle \chi_{V_j}, \chi_{V_i} \rangle = \sum_j m_j \delta_{ij} = m_i,$$

the first three equalities following from Lems. 2.3.vi, 2.3.iii, and 2.11 respectively. □

Lemma 2.15. The dimensionality of the homomorphism space $\mathrm{Hom}_G(V, V_i)$ is $\langle \chi_V, \chi_{V_i} \rangle$.

Proof.

$$\begin{aligned} \mathrm{Hom}_G(V, V_i) &\cong \mathrm{Hom}_G(\bigoplus_j V_j^{m_j}, V_i) && (\text{as } V \cong \textstyle\bigoplus_i V_i^{m_i}) \\ &\cong \bigoplus_j \mathrm{Hom}_G(V_j, V_i)^{m_j} && (\text{by Lem. A.25}) \end{aligned}$$

By Schur's lemma then, $\dim(\bigoplus_j \mathrm{Hom}_G(V_j, V_i)^{m_j}) = m_i$, and by Lem. 2.14, $m_i = \langle \chi_V, \chi_{V_i} \rangle$. □

As is outlined in Appendix A, given an semisimple algebra A and a simple A-module M, the regular module A° admits at least one submodule isomorphic to M. When we are looking at a group algebra $\mathbb{F}[G]$, then the representation theory of groups allows us to say more.

When we write up the representation matrix of a particular group element, what we are doing is encoding the group action of the element upon the basis vectors of the module that the representation corresponds to. The first column encodes the action on the first basis vector, the second column on the second basis vector, and so on, the ith column encoding the action on the the ith basis vector. Now when we are working with the regular representation, we are looking at $|G| \times |G|$-matrices, and there exists an intuitive set of basis vectors to work with—the group elements themselves.

The reader will recall that two group elements multiplied with one another deliver a third that is that same as one of the first two ones if and only if the other is the identity. In the languages of modules, calling the group element whose action we are interested in g and the set of basis vectors $\{g_i\}$, this is the same as saying

$$g \cdot g_i = g_j, \quad \text{where} \quad \begin{cases} i \neq j, \text{ if } g \neq 1, \\ i = j, \text{ if } g = 1. \end{cases}$$

Encoding this in the representation matrices, this means that if $g \neq 1$, the matrix will have nothing but zeros in the diagonal, since no part of any basis vector is ever mapped back onto itself, and if $g = 1$, the matrix will have nothing but ones in its diagonals, since every basis vector is mapped back unaltered unto itself. Since the character of a representation is merely the trace of the representation matrices, if we call the character of $(\mathbb{C}[G])^\circ$ by χ we may thus write

$$\chi(g) = \begin{cases} |G|, & \text{if } g = 1, \\ 0, & \text{if } g \neq 1. \end{cases} \tag{2.16}$$

Lemma 2.17. Let G be a finite group, and let $\{V_1, \dots, V_k\}$ be a representative set of the isomorphism classes of simple G-modules. Then

$$(\mathbb{C}[G])^\circ \cong \bigoplus_{i=1}^{k} V_i^{\oplus \dim V_i}.$$

Proof. By Maschke's theorem (Thm. A.42), the regular module is semisimple, and so $(\mathbb{C}[G])^\circ \cong \bigoplus_{i=1}^{k} V_i^{\oplus m_i}$ for some $m_i \in \mathbb{N}$. By (2.16) then, if V_i is a simple module,

$$\langle \chi_{V_i}, \chi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{V_i}(g)\overline{\chi(g)} = \frac{1}{|G|} \chi_{V_i}(e)\overline{\chi(e)} = \frac{1}{|G|} \dim V_i \cdot |G| = \dim V_i.$$

By Lem. 2.14 then it follows that $(\mathbb{C}[G])^\circ \cong \bigoplus_{i=1}^{k} V_i^{\oplus \dim V_i}$. □

With these results at our disposal then, finding the dimensionalities in question becomes a matter of simple computation.

Lemma 2.18. Let G be an abelian group of order n. Then the number of conjugacy classes of G is also n.

Proof. Two elements $a, b \in G$ are conjugate if and only if there exists an element $g \in G$ such that $gag^{-1} = b$. Since G is abelian, however, for all $g \in G$, we have $gag^{-1} = gg^{-1}a = a$, and so the only element to which a can be conjugate is itself. From this it follows that all conjugacy classes in G consist of single elements, and since G is of order n, so there must exist n conjugacy classes of G. □

Example 2.19. (The cyclical group, C_n.) A cyclical group can be generated by every non-identity element therein, so taking an arbitary $a \in C_n \backslash \{e\}$, we can express any two elements $b, c \in C_n$ as $b = a^m$, $c = a^n$ for some $m, n \in \mathbb{N}$. Thus, $bc = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = cb$, demonstrating the cyclical group to be abelian. By Lem. 2.18, it therefore consists of n conjugacy classes. By Cor. 2.13, it therefore has n irreducible representations.

C_n	e	a	a^2	a^3	$\dots$	a^{n-1}
Triv.	1	1	1	1	$\dots$	1
ϱ_1	1	ζ	ζ^2	ζ^3	$\dots$	ζ^{n-1}
ϱ_2	1	ζ^2	ζ^4	ζ^6	$\dots$	$\zeta^{2(n-1)}$
ϱ_3	1	ζ^3	ζ^6	ζ^9	$\dots$	$\zeta^{3(n-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
ϱ_k	1	ζ^k	ζ^{2k}	ζ^{3k}	$\dots$	$\zeta^{k(n-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
ϱ_{n-1}	1	ζ^{n-1}	$\zeta^{2(n-1)}$	$\zeta^{3(n-1)}$	$\dots$	$\zeta^{(n-1)^2}$

Table 2.20. The reduced character table for the cyclic group of order n, where $\zeta = e^{i\frac{2\pi}{n}}$.

Since every mapping $e \mapsto 1$, $a \mapsto \zeta^m$, $\zeta = e^{i\frac{2\pi}{n}}$ constitutes a distinct irreducible representation for $m \in \{1, \dots, n\}$, it follows that these are all the irreducible representations of C_n. These all being one-dimensional, it is very easy to construct the reduced character table (see Tab. 2.20). We denote a^k by $\overline{k}$, and the representation that maps $\overline{1} \mapsto \zeta^p$ by ϱ_p. The natural representation ϱ_{Nat} in this case is given by

$$\varrho_{\text{Nat}}(\overline{k}) = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}, \qquad k \in \{0, 1, \dots, n-1\}.$$

Then, using Lem. 2.15, we find that the number of arrows from the node p to the node q is

$$n_{pq} = \frac{1}{n}\sum_{k=0}^{n-1} \chi(\varrho_{\mathrm{Nat}}(\overline{k}))\chi(\varrho_p(\overline{k}))\overline{\chi(\varrho_q(\overline{k}))}.$$

For arbitrary $\overline{k}$, we find

$$\begin{aligned}\chi(\varrho(\overline{k}))\chi(\varrho_p(\overline{k}))\overline{\chi(\varrho_q(\overline{k}))} &= (\zeta^k + \zeta^{-k})\zeta^{pk}\zeta^{-qk}\\ &= (\zeta^k + \zeta^{-k})\zeta^{k(p-q)}\\ &= \zeta^{k(p-q+1)} + \zeta^{k(p-q-1)}.\end{aligned}$$

This leaves us with

$$n_{pq} = \frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q+1)} + \frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q-1)},$$

that is, the sum of two geometric series. Now,

$$\sum_{k=0}^{n-1} ar^k = a + ar + ar^2 + ar^3 + \cdots + ar^{n-2} + ar^{n-1} = a\frac{1-r^n}{1-r},$$

for $r \neq 1$, of course, as one would not want to divide by zero. In the case in which $r = 1$, then clearly $\sum_{k=0}^{n-1} ar^k = a + a + \cdots + a = na$. Thus,

$$\frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q+1)} = \frac{1}{n}\frac{1-\zeta^{n(p-q+1)}}{1-\zeta^{p-q+1}}, \qquad \text{and} \qquad \frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q-1)} = \frac{1}{n}\frac{1-\zeta^{n(p-q-1)}}{1-\zeta^{p-q-1}}.$$

Now, $\zeta^n = 0$, and so, $\zeta^{n(p-q+1)} = (\zeta^n)^{(p-q+1)} = 1^{(p-q+1)} = 1$, and analogously for the $(p-q-1)$ case. Thus,

$$\frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q+1)} = \frac{1}{n}\frac{1-1}{1-\zeta^{p-q+1}} = 0, \qquad \text{and} \qquad \frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q-1)} = \frac{1}{n}\frac{1-1}{1-\zeta^{p-q-1}} = 0,$$

in all cases, except when $p-q+1 = 0 \pmod n$ and $p-q-1 = 0 \pmod n$ respectively, in which case the $\sum_{k=0}^{n-1} ar^k = a + a + \cdots + a = na$ condition kicks in, and we end up with

$$\frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q+1)} = \frac{1}{n}\cdot n \cdot 1 = 1, \qquad \text{and} \qquad \frac{1}{n}\sum_{k=0}^{n-1}\zeta^{k(p-q-1)} = \frac{1}{n}\cdot n\cdot 1 = 1,$$

respectively. This occurs when

$$p = q-1 \pmod n, \quad \text{and} \quad p = q+1 \pmod n,$$

respectively. So, for each node p, draw arrows to nodes $p-1$ and $p+1$. Going through with the procedure for all nodes, we obtain the diagram shown in Fig. 2.21.

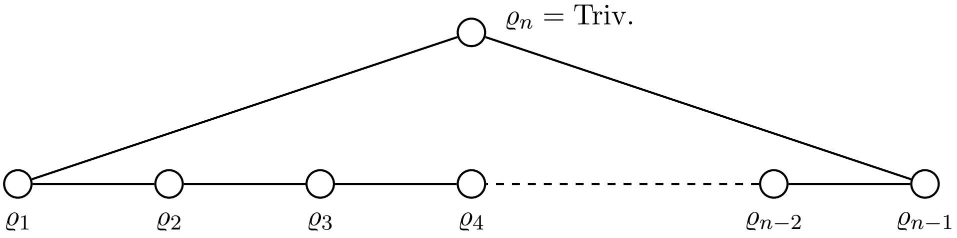


FIGURE 2.21. The McKay quiver of the cyclic group of order n.

Example 2.22. (The binary dihedral group, $\mathbb{B}\mathrm{D}_{2n}$.) The binary dihedral group $\mathbb{B}\mathrm{D}_{2n}$ is given by the presentation

$$\mathbb{B}\mathrm{D}_{2n} := \langle r, s | r^{2n} = e, s^2 = r^n, s^{-1}rs = r^{-1} \rangle,$$

and it is known from group theory that it is of order $4n$ and consists of $n+3$ conjugacy classes, these being $\{e\}$ and $\{s^2\}$ with one element each, $\{r, r^{2n-1}\}, \{r^2, r^{2n-2}\}, \dots, \{r^{n-1}, r^{n+1}\}$ with two elements each, and $\{s, sr^2, \dots, sr^{2n-2}\}$ and $\{sr, sr^3, \dots, sr^{2n-1}\}$ with n elements each.

For a one-dimensional representation, the characters are the 1×1-matrices, and since we concern ourselves with a finite group, every element taken to some power must be the identity element. Thus every character must be a root of unity. Looking at the generators r, s then, it is immediately clear that if we set $\zeta = e^{i\pi/2n}$, then $\varrho(r) = \zeta^{2k}$ and $\varrho(s) = \zeta^{kn+2an}$, $a \in \mathbb{Z}$, satisfy the first two defining relations for all $0 \leq k \leq n-1$. The final relation however can only be satisfied if $\zeta^{2k} = \zeta^{-2k}$, which can only be the case if $\zeta^k \in \{1, -1, i, -i\}$. Consequently, as $\varrho(s) = (-1)\zeta^{kn}$, the specifics of the different one-dimensional irreducible representations are going to depend on whether n is even or odd. If n is even,

$$(\varrho(r), \varrho(s)) \in \{(1,1), (1,-1), (-1,1), (-1,-1)\}.$$

If n is odd,

$$(\varrho(r), \varrho(s)) \in \{(1,1), (1,-1), (-1,i), (-1,-i)\}.$$

In either event, we obtain four one-dimensional irreducible representations, the trivial, call it Triv. and three additional ones which we call 1A, 1B, and 1C.

In the natural representation, the generators are given by the matrices

$$\varrho_{\mathrm{Nat}} \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \qquad \varrho_{\mathrm{Nat}}(s) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Taking the inner product of its character with itself, we obtain unity and so may conclude that it too is an irreducible representation of the binary dihedral group: let H be a set of elements of $\mathbb{B}\mathrm{D}_{2n}$, containing exactly one element from each of the different conjugacy classes. Then,

$$\begin{aligned} \langle \chi_{\mathrm{Nat}}, \chi_{\mathrm{Nat}} \rangle &= \frac{1}{|\mathbb{B}\mathrm{D}_{2n}|} \sum_{h \in H} |\mathrm{Cl}(h)| \chi_{\mathrm{Nat}}(h) \overline{\chi_{\mathrm{Nat}}(h)} \\ &= \frac{1}{4n} \left[2 \cdot 2 + (-2) \cdot (-2) + 2 \sum_{j=1}^{n-1} (\zeta^j + \zeta^{-j})(\zeta^{-1} + \zeta^j) + 0 + 0 \right] \\ &= \frac{1}{4n} \left[8 + 2 \sum_{j=1}^{n-1} (2 + \zeta^{2j} + \zeta{-2j}) \right] \\ &= \frac{1}{4n} \left[8 + 4(n-1) - 4 \right] = 1, \end{aligned}$$

where we have used the property that the nth roots of unity always add up to zero.

Further, we note from the defining relations that since $r^n = s^2$, $r^{2n} = e$, and $s^{-1}rs = r^{-1}$, if k is an odd number, then $(r^k)^n = s^2$, $(r^k)^{2n} = e$, and $s^{-1}(r^k)s = (r^k)^{-1}$ also. This means that for odd k, further representations of the group may be given by $\varrho_k(r) := (\varrho_{\mathrm{Nat}}(r))^k$, $\varrho_k(s) := \varrho_{\mathrm{Nat}}(s)$. For even k, this schema fails as $(r^k)^n = e$, and in particular, $(\varrho_{\mathrm{Nat}}(r)^k)^n = \mathbb{1} \neq -\mathbb{1} = \varrho_{\mathrm{Nat}}(s)^2$. The situation can be remedied however by letting $\varrho_k := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, as then $\varrho_k(s)^2 = \mathbb{1}$ while the relation $\varrho_k(s^{-1})\varrho_k(r)\varrho_k(s) = \varrho_k(r^{-1})$ remains intact. Thus we have an additional $n-2$ two-dimensional representations being given by

$$\varrho_k(r) = \begin{pmatrix} \zeta^k & 0 \\ 0 & \zeta^{-k} \end{pmatrix}, \qquad \varrho_k(s) = \begin{pmatrix} 0 & 1 \\ (-1)^k & 0 \end{pmatrix}, \qquad 2 \leq k \leq n-1.$$

These, too, turn out to be irreducible representations: again, let H be a set of elements of $\mathbb{BD}_{2n}$, containing exactly one element from each of the different conjugacy classes.

$$\begin{aligned}\langle \chi_k, \chi_k \rangle &= \frac{1}{|\mathbb{BD}_{2n}|} \sum_{h \in H} |\mathrm{Cl}(h)| \chi_k(h) \overline{\chi_k(h)} \\ &= \frac{1}{4n} \left[2 \cdot 2 + (-1)^{2k} 2 \cdot 2 + 2 \sum_{j=1}^{n-1} (\zeta^{jk} + \zeta^{-jk})(\zeta^{-jk} + \zeta^{jk}) + 0 + 0 \right] \\ &= \frac{1}{4n} \left[8 + 2 \sum_{j=1}^{n-1} (2 + \zeta^{2jk} + \zeta - 2jk) \right] \\ &= \frac{1}{4n} \left[8 + 4(n-1) - 4 \right] = 1, \end{aligned}$$

where we have used the fact that any integer power of an nth root of unity is itself always an nth root of unity, and so as a geometric sum, we obtain

$$\sum_{j=1}^{n-1} (\zeta^{2k})^j = \frac{\zeta^{2k}(1 - \zeta^{2k(n-1)})}{1 - \zeta^{2k}} = \frac{1 - \zeta^{-2k}}{\zeta^{-2k} - 1} = -1.$$

Having thus found $n+3$ irreducible representations, the same as the number of conjugacy classes, we conclude that we have found them all, and so draw up the reduced character table (see Tab. 2.23).

$\mathbb{BD}_{2n}$	e	s^2	r	r^2	$\ldots$	r^{n-1}	s	sr
Triv.	1	1	1	1	$\ldots$	1	1	1
1A	1	1	1	1	$\ldots$	1	-1	-1
1B	1	$(-1)^n$	-1	1	$\ldots$	$(-1)^{n-1}$	i^n	$-i^n$
1C	1	$(-1)^n$	-1	1	$\ldots$	$(-1)^{n-1}$	$-i^n$	i^n
Nat.	2	-2	$\zeta + \zeta^{-1}$	$\zeta^2 + \zeta^{-2}$	$\ldots$	$\zeta^{n-1} + \zeta^{1-n}$	0	0
ϱ_k	2	$(-1)^k 2$	$\zeta^k + \zeta^{-k}$	$\zeta^{2k} + \zeta^{-2k}$	$\ldots$	$\zeta^{k(n-1)} + \zeta^{k(1-n)}$	0	0

TABLE 2.23. The reduced character table for the binary dihedral group $\mathbb{BD}_{2n}$.

The McKay quiver is now found through character theory. It is immediately clear that the inner products of the characters of both the trivial representation and 1A with the natural one yields back the natural, while those of 1B and 1C with the same yields ϱ_{n-1}. The outstanding question then is what the tensor product is of the natural and a generic two-dimensional irreducible representation ϱ_k? The character table is readily available as a matter of computation:

	e	s^2	r	$\ldots$	r^{n-1}	s	sr
Nat. $\otimes\, \varrho_k$	4	$(-1)^{k+1} 4$	$(\zeta^{k+1} + \zeta^{-k-1})$ $+(\zeta^{k-1} + \zeta^{1-k})$	$\ldots$	$(\zeta^{(k+1)(n-1)} + \zeta^{(k+1)(1-n)})$ $+(\zeta^{(k-1)(n-1)} + \zeta^{(k-1)(1-n)})$	0	0

Inspection reveals that provided $1 < k < n-1$, then Nat. $\otimes\, \varrho_k \cong \varrho_{k-1} \oplus \varrho_{k+1}$. The two exceptions are of course the natural representation itself and ϱ_{n-1}, in which cases we have:

	e	s^2	r	$\ldots$	r^{n-1}	s	sr
Nat. $\otimes$ Nat.	4	4	$(\zeta^2 + \zeta^{-2}) + 1 + 1$	$\ldots$	$(\zeta^{n-1} + \zeta^{1-n}) + 1 + 1$	0	0
Nat. $\otimes\, \varrho_{n-1}$	4	$(-1)^n 4$	$-1 - 1 + (\zeta^{n-2} + \zeta^{2-n})$	$\ldots$	$(-1)^{n-1} + (-1)^{n-1})$ $+(\zeta^{(n-2)(n-1)} + \zeta^{(n-2)(1-n)})$	0	0

Once again, it is immediately clear that Nat. $\otimes$ Nat. $\cong \varrho_2 \oplus$ Triv. $\oplus$ 1A and Nat. $\otimes\, \varrho_{n-1} \cong \varrho_{n-2} \oplus$ 1B $\oplus$ 1C. All that remains is drawing up the McKay quiver (see Fig. 2.24).

The cyclic and binary dihedral groups having been dispensed with, we now move on to the binary polyhedral groups. Though the process is somewhat tedious, it is entirely possible from

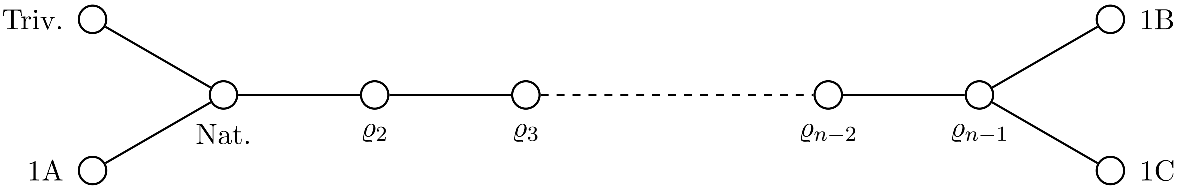


FIGURE 2.24. The McKay quiver of the binary dihedral group $\mathbb{BD}_{2n}$.

as little as only knowing the characters of the trivial and natural representations (which are always a given) to deduce the entire reduced character table. From this in turn, using the inner product and old-fashioned arithmetic, the full McKay quivers may be constructed.

Though we do not therefore need the actual representation matrices for any of our overarching purposes, they could well prove to be fruitful for future endeavours, and their inclusion certainly would satisfy our desire for completeness. Above all, the literature available on the subject is avaricious in listing them, and the method for finding them remains, unfortunately, obscure. As such, the author judges it prudent to present it here.

The method, which has applications ranging far beyond our particular line of inquiry, was originally developed in the 1990s by the Canadian computational mathematician John D. Dixon [18]. A very powerful algorithm, it allows one to construct the irreducible representation matrices of a wide variety of finite groups provided one knows their multiplication tables and their restricted character tables. In particular, it allows for the computation of all irreducible representations of dimension less than 32 of simple groups. Beyond drawing on Dixon's original article, we shall also draw on the dissertation of his doctoral student Vahid Dabbaghian-Abdoly [19].

2. Dixon's Restricted Character Algorithm

We denote the regular representation by ϱ and its character by χ. As noted earlier in Lem. 2.17,

$$(\mathbb{C}[G])^\circ \cong \bigoplus_{i=1}^{k} V_i^{\dim V_i}, \tag{2.25}$$

where the $\{V_i\}$ form a representative set of the isomorphism classes of the simple group modules, each corresponding to an irreducible representation ϱ_i, and each with the associated character χ_i. From this, it further follows that

$$\chi(g) = \sum_{i=1}^{k} \chi_i(g)\chi_i(1), \tag{2.26}$$

for each and every element $g \in G$, denoting the identity of the group by 1. Extending this formula to cover the algebra representations, we get that for generic element $a \in \mathbb{C}G$, we have

$$\tilde{\chi}(a) = \sum_{i=1}^{k} \tilde{\chi}_i(a)\chi_i(1), \tag{2.27}$$

where we have extended the definition of the character of a group representation to also cover the group algebra representation, hence the tilde. Consider the central idempotent e_i associated with the V_i-homogeneous submodule $V_i(\mathbb{C}[G])$. It stands to reason that it may be written as

$$e_i = \sum_{k=1}^{|G|} a_{i,k} g_k, \tag{2.28}$$

with coefficients $a_{i,k} \in \mathbb{C}$. The inevitable question that arises is, what are those $a_{i,k}$'s? To answer this question, we look at $\mathbb{C}[G]$ as an algebra and consider what the regular character of the element $e_i g_k^{-1}$ is,

$$\tilde{\chi}(e_i g_k^{-1}) = \tilde{\chi}\Big(\sum_{\ell=1}^{|G|} a_{i,\ell} g_\ell g_k^{-1}\Big) = \sum_{\ell=1}^{|G|} a_{i,\ell}\chi(g_\ell g_k^{-1}).$$

The only summand above that does not vanish is the case of $\ell = k$, in which case $\chi(g_\ell g_k^{-1}) = \chi(g_k g_k^{-1}) = \chi(1) = |G|$. This leaves us with

$$a_{i,k} = \frac{1}{|G|}\tilde{\chi}(e_i g_k^{-1}).$$

Next, we express the $a_{i,k}$'s in terms of the characters of the irreducible representations. Since $\tilde{\varrho}_i(e_j) = \delta_{ij}\mathbb{1}$ and since the $\{\tilde{\varrho}_i\}$ are morphisms, it follows that $\tilde{\varrho}_j(e_i g_k^{-1}) = \delta_{ij}\varrho(g_k^{-1})$, from whence it in turn follows that $\tilde{\chi}_j(e_i g_k^{-1}) = \delta_{ij}\chi_j(g_k^{-1})$. Then, with reference to (2.27), we obtain

$$a_{i,k} = \frac{1}{|G|}\sum_{j=1} \delta_{ij}\chi_j(g_k^{-1})\chi_j(1) = \frac{1}{|G|}\chi_i(g_k^{-1})\chi_i(1).$$

Plugging this expression into (2.28), we finally obtain

$$e_i = \frac{\chi_i(1)}{|G|}\sum_{k=1}^{|G|} \chi_i(g_k^{-1})g_k. \tag{2.29}$$

To recapitulate, if e_i is the central idempotent associated with the irreducible representation ϱ_i with character χ_i, then it may be decomposed in the basis $\{g_k | g_k \in G\}$ of the algebra $\mathbb{C}[G]$ as above. For the remainder of this section, we shall use $d_i = \dim(V_i)$ in place of $\chi_i(1)$.

The following lemma forms the very heart of the algorithm:

Lemma 2.30. (Dixon and Dabbaghian-Abdoly.) If $a \in \mathbb{C}[G]$ such that $\tilde{\varrho}_i(a)$ has rank 1, then $\mathbb{C}Ge_i a$ is a submodule of $\mathbb{C}Ge_i$ of dimension d_i which affords the character χ_i.

Proof. Letting e_i act on the entirety of $\mathbb{C}[G]$ from the right delivers the V_i-homomorphic submodule of $(\mathbb{C}[G])^\circ$, which by Cor. A.49 is isomorphic to $V_i^{\oplus d_i}$. For any $w = (vae_i) \in \mathbb{C}[G]ae_i = \mathbb{C}[G]e_i a$ and any $x \in \mathbb{C}[G]$, $xw = x(vae_i) = (xv)ae_i \in \mathbb{C}[G]ae_i$, making $\mathbb{C}[G]e_i a$ a submodule of $\mathbb{C}[G]e_i$.

Since $\ker(\tilde{\varrho}) = (1-e_i)\mathbb{C}[G]$, by Thm. A.37, there exists an isomorphism $\mathbb{C}[G]/(1-e_i)\mathbb{C}[G] \cong \mathrm{Mat}_{d_i\times d_i}(\mathbb{C})$, where, specifically, the isomorphism may be given in terms of $\tilde{\varrho}_i$ as $\overline{\tilde{\varrho}_i}(\bar{c}) = \tilde{\varrho}_i(c)$ for $c \in \mathbb{C}[G]$ and $\bar{c} \in \mathbb{C}[G]/(1-e_i)\mathbb{C}[G]$,

$$\begin{tikzcd}
\mathbb{C}[G] \arrow[r, "\tilde{\varrho}_i"] \arrow[d, two heads] \arrow[dr, phantom, "\circlearrowright"] & \mathrm{Mat}_{|G|\times|G|}(\mathbb{C}) \\
\mathbb{C}[G]/(1-e_i)\mathbb{C}[G] \arrow[r, "\sim", "\overline{\tilde{\varrho}}_i"'] & \mathrm{Mat}_{d_i\times d_i}(\mathbb{C}) \arrow[u, hook]
\end{tikzcd}$$

By the quotient $\mathbb{C}[G]/(1-e_i)\mathbb{C}[G]$ we mean that all elements in the algebra $\mathbb{C}[G]$ that differ by a term in $(1-e_i)\mathbb{C}[G]$ are counted as the same element. For any element $b \in \mathbb{C}[G]$ we can always write

$$b = 1b = (1-e_i+e_i)b = e_i b + (1-e_i)b = be_i + (1-e_i)b,$$

and so it becomes readily apparent that $\mathbb{C}[G]/(1-e_i)\mathbb{C}[G] \cong \mathbb{C}[G]e_i$, and $\mathbb{C}[G]e_i \cong \tilde{\varrho}_i(\mathbb{C}[G]e_i) = \mathrm{Mat}_{d_i\times d_i}(\mathbb{C})$, the last equality following from Cor. A.55.

It thus being established that there exists an isomorphism between $\mathbb{C}[G]e_i$ and $\tilde{\varrho}_i(\mathbb{C}[G]e_i)$, it follows by necessity that there must exist an isomorphism between every subalgebra of $\mathbb{C}[G]e_i$ and the image of the subalgebra under $\tilde{\varrho}_i$. Additionally, we recall that $\tilde{\varrho}_i$ is a morphism, and thus, for $c, d \in \mathbb{C}[G]$ we have $\tilde{\varrho}_i(cd) = \tilde{\varrho}_i(c)\tilde{\varrho}_i(d)$. If $a \in \mathbb{C}[G]$, we may then write,

$$\mathbb{C}[G]e_ia \cong \tilde{\varrho}_i(\mathbb{C}[G]e_ia) = \tilde{\varrho}_i(\mathbb{C}[G]e_i)\tilde{\varrho}_i(a) = \mathrm{Mat}_{d\times d}(\mathbb{C})\tilde{\varrho}_i(a).$$

Further, if a is of rank 1, that means that there must exist invertible matrices C, D such that

$$\varrho_i(a) = CE_{11}D,$$

where E_{ij} is the matrix with entry 1 at position (i, j) and 0 everywhere else. This then means that

$$\mathbb{C}[G]e_ia \cong \mathrm{Mat}_{d\times d}(\mathbb{C})\tilde{\varrho}_i(a) = \mathrm{Mat}_{d\times d}(\mathbb{C})CE_{11}D = \mathrm{Mat}_{d\times d}(\mathbb{C})E_{11}D.$$

The action of E_{11} on the matrices $\mathrm{Mat}_{d\times d}(\mathbb{C})$ from the left becomes the next focal point for our attention in proving this lemma. $E_{i1}E_{11} = E_{i1}$ and $E_{ij}E_{11} = 0$ for $j \geq 2$. Since $\{E_{ij} | 1 \leq i, j \leq d\}$ is a basis for $\mathrm{Mat}_{d\times d}(\mathbb{C})$, $\{E_{i1} | 1 \leq i \leq d\}$ is a basis for $\mathrm{Mat}_{d\times d}(\mathbb{C})E_{11}$. Now consider the morphism $\phi : \mathrm{Mat}_{d\times d}(\mathbb{C})E_{11} \to \mathrm{Mat}_{d\times d}(\mathbb{C})E_{11}D$, $A \mapsto AD$. The morphism is self-evidently surjective, and since D is invertible, the kernel is trivial. Thus it is an isomorphism, and $\mathrm{Mat}_{d\times d}(\mathbb{C})E_{11} \cong \mathrm{Mat}_{d\times d}(\mathbb{C})E_{11}D$, and $\mathrm{Mat}_{d\times d}(\mathbb{C})E_{11}D$ has dimension d_i. Ergo, $\mathbb{C}[G]e_ia$ has dimension d_i.

Finally, we need to show that $\mathbb{C}[G]e_ia$ truly yields character χ_i. From character theory, we know that two representations yield the same character if and only if they are isomorphic. Since $\mathbb{C}[G]e_ia$ is isomorphic to a submodule of $M_i^{\oplus d_i}$, we look at submodules of $M_i^{\oplus d_i}$. $\mathbb{C}[G]e_ia$ is of dimension d_i, and the only submodules of $M_i^{\oplus d_i}$ of dimension d_i are isomorphic to M_i itself. M_i has character χ_i, and so $\mathbb{C}[G]e_ia$ has character χ_i as well. □

In order for us to make use of this lemma for finding irreducible representations with the characters we want, we need to find a good general way for finding such suitable *rank-1 elements* a. Though Dixon leaves open the question of how to construct rank-1 elements for general groups and irreducible representations (although such elements must by necessity exist for every group and irreducible representation), he makes the observation that if one can find a subgroup H of G such that the restriction of χ_i to H, $\chi_{i,H}$ contains a constituent irreducible character θ of H of degree 1 and multiplicity 1, then a rank-1 element is given by

$$a := \sum_{h\in H} \theta(h^{-1})h.$$

Dabbaghian-Abdoly refers to such subgroups H as χ_i-subgroups. Let us show that a in the formula above truly is a rank-1 element. First, take the product of a by itself. Since θ is of degree one, $\theta(h_1h_2) = \theta(h_1)\theta(h_2)$ for every $h_1, h_2 \in H$, and thus

$$a^2 = \sum_{h_1\in H}\sum_{h_2\in H} \theta(h_1^{-1})h_1\theta(h_2^{-1})h_2 = \sum_{h_1\in H}\sum_{h_2\in H} \theta(h_2^{-1}h_1^{-1})h_1h_2 = |H|\sum_{h\in H}\theta(h^{-1})h = |H|a.$$

Consequently, $a/|H|$ is idempotent. Further,

$$\mathrm{tr}(\varrho_i(a)) = \mathrm{tr}\left(\varrho_i\left(\sum_{h\in H}\theta(h^{-1})h\right)\right) = \sum_{h\in H}\theta(h^{-1})\mathrm{tr}\left(\varrho_i\left(h\right)\right) = \sum_{h\in H}\theta(h^{-1})\chi_i(h) = |H|\langle\theta, \chi_{i,H}\rangle = |H|,$$

since for any character γ and group element g, we have $\gamma(g^{-1}) = \overline{\gamma(g)}$. This means that $\varrho_i(a/|H|)$ has trace 1. Since the trace of an idempotent matrix equals to the rank of the matrix, it follows that $\varrho_i(a/|H|)$ has rank 1, and so by extension does $\varrho_i(a)$ have.

Multiplication by scalars does not affect the rank of a matrix, so we may multiply it by a prefactor of $(|G|/d)$, then $f := e_i a$ where e_i is defined as in (2.29) becomes

$$f = \sum_{h\in H}\sum_{g\in G}\theta(h^{-1})h\chi_i(g^{-1})g = \sum_{g\in G}\sum_{h\in H}\theta(h^{-1})\chi_i(g^{-1})hg = \sum_{g\in G}\sum_{h\in H}\theta(h^{-1})\chi_i(hg^{-1})g,$$

or, $f = \sum_{g\in G}\alpha(g)g$, where

$$\alpha(g) := \sum_{h\in H}\theta(h^{-1})\chi_i(hg^{-1})$$

By Lem. 2.30, we then have a desired module of $\mathbb{C}[G]$ in $\mathbb{C}[G]f$. Now we just need to make a set of matrices out of it.

To do that we first of all seek to establish a basis for $\mathbb{C}[G]f$. That is easy, the $\{g_i\}$ is a complete basis of $\mathbb{C}[G]$, so among the $\{g_i f\}$ we must necessarily be able to find d_i linearly independent elements which then form a basis for $\mathbb{C}[G]f$. Find d_i elements $g_i, \ldots, g_d$ then such that the $\{g_i f\}$ are linearly independent. Then, for every $x \in G$, we can find a representation matrix by calculating the components ξ_{ij} when we consider the left action of x on every $(g_i f)$,

$$x(g_i f) = \sum_{j=1}^{d}\xi_{ij}(g_j f).$$

That is

$$\begin{aligned}
\sum_{t\in G}\alpha(g_i^{-1}t)xt &= \sum_{j=1}^{d}\xi_{ij}\sum_{t\in G}\alpha(g_j^{-1}t)t\\
\sum_{t\in G}\alpha(g_i^{-1}x^{-1}t)t &= \sum_{t\in G}\sum_{j=1}^{d}\xi_{ij}\alpha(g_j^{-1}t)t\\
\Rightarrow \quad \alpha(g_i^{-1}x^{-1}g_k)g_k &= \sum_{j=1}^{d}\xi_{ij}\alpha(g_j^{-1}g_k)g_k, \quad \text{for } 1\le k\le d
\end{aligned}$$

writing $A(x)_{ab} = \alpha(x_a^{-1}x^{-1}x_b)$, we have

$$A(x)_{ik} = \sum_{j=1}^{d}\xi_{ij}A(1)_{jk}, \quad \text{for } 1\le k\le d$$

Rewriting this as a matrix equation,

$$A(x) = [\xi_{ij}]A(1),$$

meaning that the mapping $x \mapsto A(x)A(1)^{-1}$ gives us the desired representation it being easy to check that $A(x)$ is non-singular for every $x \in G$.

Thus armed with the formidable tool of the restricted character algorithm, we may finally find the full sets of irreducible representations for each of the remaining subgroups $\mathbb{BT}$, $\mathbb{BO}$, and $\mathbb{BD}$. This was accomplished through the authoring of a Python script that implemented the algorithm outlined above.

Example 2.31. (Binary tetrahedral group, $\mathbb{BT}$.) In the natural representation, two generator elements (call them a and b) are given by

$$\varrho_{\text{Nat}}(a) = \frac{1}{2}\begin{pmatrix}1+i\sqrt{3} & 0\\ 0 & 1-i\sqrt{3}\end{pmatrix}, \qquad \varrho_{\text{Nat}}(b) = \frac{1}{2\sqrt{3}}\begin{pmatrix}\sqrt{3}-i & -i2\sqrt{2}\\ -i2\sqrt{2} & \sqrt{3}+i\end{pmatrix}.$$

The group consists of 24 elements, which come in 7 conjugacy classes, which in terms of a and b are given as

$$\begin{aligned}
\mathrm{Cl}(e) &= \{e = a^6\},\\
\mathrm{Cl}(a) &= \{a, b, a^2b^2, b^2a^2\},\\
\mathrm{Cl}(a^2) &= \{a^2, b^2, a^4b, a^3ba\},\\
\mathrm{Cl}(ab) &= \{ab, ba, a^5, a^3b^2\},\\
\mathrm{Cl}(a^3) &= \{a^3\},\\
\mathrm{Cl}(a^2b) &= \{a^2b, aba, ab^2, ba^2, b^2a, a^4ba\},\\
\mathrm{Cl}(a^4) &= \{a^4, a^3b, a^2ba, aba^2\}.
\end{aligned}$$

Character theory allows us to conclude that the natural representation is an irreducible representation of $\mathbb{BT}$. The trivial representation is always a given, and two more one-dimensional irreducible representations may be found by algebraic means. As a, b are in the same conjugacy class, for any representation they have the same character, and in particular, in any one-dimensional representation, they must be represented by the same single-entry matrix. As $a^6 = e$, and the identity is represented by unity in any one-dimensional representation, we conclude that $\varrho_{\text{one-dim.}} : a, b \mapsto \zeta^m$ for $\zeta = e^{i\frac{\pi}{3}}$ and some $m \in \{1, 2, 3, 4, 5\}$ must define the representation(s). If $\varrho_{\text{one-dim.}} \neq \varrho_{\text{Triv.}}$, character theory then informs us that we must have $\langle \chi_{\text{one-dim.}}, \chi_{\text{Triv.}} \rangle = 0$. This in conjunction with our knowledge of the form of the conjugacy classes then allows us to set up the equation,

$$\frac{1}{24}(1 + 4\zeta^m + 4\zeta^{2m} + 4\zeta^{2m} + \zeta^{3m} + 6\zeta^{3m} + 4\zeta^{4m}) = 0,$$

which we find has two solutions in $m = 2, 4$, which we call 1A and 1B, and which are defined by $\varrho_{1\mathrm{A}} : a \mapsto \frac{1}{2}(-1 + i\sqrt{3})$ and $\varrho_{1\mathrm{B}} : a \mapsto \frac{1}{2}(-1 - i\sqrt{3})$ respectively. Having thus found four of the seven irreducible representations of the group, we have sufficient information to find the characters of the remaining three, to draw up the reduced character table (see Tab. 2.32), and finally to draw the associated McKay quiver (see Fig. 2.33).

As we may deduce from thence, $\varrho_{1\mathrm{A}} \otimes \varrho_{\mathrm{Nat.}} \cong \varrho_{2\mathrm{A}}$ and $\varrho_{1\mathrm{B}} \otimes \varrho_{\mathrm{Nat.}} \cong \varrho_{2\mathrm{B}}$, and so the generator elements are given by

$$\varrho_{2\mathrm{A}}(a) = \frac{1}{2}\begin{pmatrix} -2 & 0 \\ 0 & 1 + i\sqrt{3} \end{pmatrix}, \qquad \varrho_{2\mathrm{A}}(b) = \frac{1}{2\sqrt{3}}\begin{pmatrix} 2i & \sqrt{6} + i\sqrt{2} \\ \sqrt{6} + i\sqrt{2} & i - \sqrt{3} \end{pmatrix},$$

and

$$\varrho_{2\mathrm{B}}(a) = \frac{1}{2}\begin{pmatrix} 1 - i\sqrt{3} & 0 \\ 0 & -2 \end{pmatrix}, \qquad \varrho_{2\mathrm{B}}(b) = \frac{1}{2\sqrt{3}}\begin{pmatrix} -\sqrt{3} - i & -\sqrt{6} + i\sqrt{2} \\ -\sqrt{6} + i\sqrt{2} & -2i \end{pmatrix},$$

in representations 2A and 2B respectively.

Finally, we have the irreducible representation 3A. The element a generates a subgroup of $\mathbb{BT}$ that is isomorphic to the cyclic group of order 6, $\mathbb{Z}_6 \cong \langle a \rangle < \mathbb{BT}$, and when we consider the restriction of $\varrho_{3\mathrm{A}}$ to $\langle a \rangle$, we find that the trivial representation of $\langle a \rangle$, $\theta_{\mathrm{Triv.}}$, occurs with multiplicity 1 in the decomposition of $\varrho_{3\mathrm{A}}|_{\langle a \rangle}$,

	e	a	a^2	a^3	a^4	a^5
$\varrho_{3\mathrm{A}}\|_{\langle a \rangle}$	3	0	0	3	0	0
$\theta_{\mathrm{Triv.}}$	1	1	1	1	1	1

$$\langle \varrho_{3\mathrm{A}}|_{\langle a \rangle}, \theta_{\mathrm{Triv.}} \rangle = \frac{1}{6}(3 + 0 + 0 + 3 + 0 + 0) = 1.$$

We may thus use the subgroup $\langle a \rangle$ to find a rank-1 element, and, using Dixon's restricted character algorithm, find the matrices making up the representation 3A. With

$$\alpha(g) = \sum_{a \in \langle a \rangle} \theta_{\mathrm{Triv.}}(a^{-1})\chi_{3\mathrm{A}}(ag^{-1}) = \sum_{k=0}^{5} \chi_{3\mathrm{A}}(a^k g^{-1}),$$

and choosing a basis of $\{a, b, ab\}$, we obtain

$$A(1) = \begin{pmatrix} 6 & -2 & -2 \\ -2 & 6 & -2 \\ -2 & -2 & 6 \end{pmatrix}, \qquad A(a) = \begin{pmatrix} 6 & -2 & -2 \\ -2 & -2 & 6 \\ -2 & -2 & -2 \end{pmatrix}, \qquad A(b) = \begin{pmatrix} -2 & 6 & -2 \\ -2 & -2 & -2 \\ -2 & -2 & 6 \end{pmatrix},$$

and consequently,

$$\varrho_{3\mathrm{A}}(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix}, \qquad \varrho_{3\mathrm{A}}(b) = \begin{pmatrix} 0 & 1 & 0 \\ -1 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

	e	a	a^2	ab	a^3	a^2b	a^4
Triv.	1	1	1	1	1	1	1
1A	1	$\frac{1}{2}(-1+i\sqrt{3})$	$\frac{1}{2}(-1-i\sqrt{3})$	$\frac{1}{2}(-1-i\sqrt{3})$	1	1	$\frac{1}{2}(-1+i\sqrt{3})$
1B	1	$\frac{1}{2}(-1-i\sqrt{3})$	$\frac{1}{2}(-1+i\sqrt{3})$	$\frac{1}{2}(-1+i\sqrt{3})$	1	1	$\frac{1}{2}(-1-i\sqrt{3})$
Nat.	2	1	-1	1	-2	0	-1
2A	2	$\frac{1}{2}(-1+i\sqrt{3})$	$\frac{1}{2}(1+i\sqrt{3})$	$\frac{1}{2}(-1-i\sqrt{3})$	-2	0	$\frac{1}{2}(1-i\sqrt{3})$
2B	2	$\frac{1}{2}(-1-i\sqrt{3})$	$\frac{1}{2}(1-i\sqrt{3})$	$\frac{1}{2}(-1+i\sqrt{3})$	-2	0	$\frac{1}{2}(1+i\sqrt{3})$
3D	3	0	0	0	3	-1	0

TABLE 2.32. The reduced character table of the binary tetrahedral group.

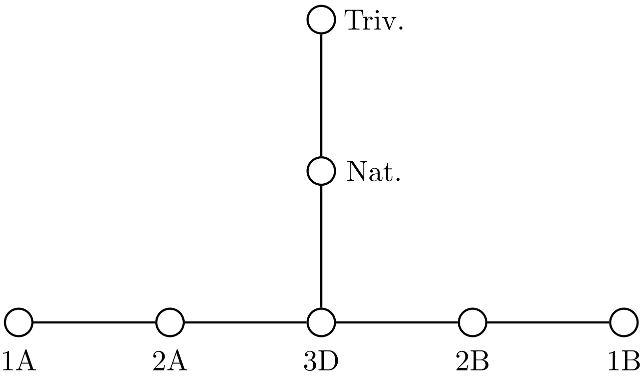


FIGURE 2.33. The McKay quiver of the binary tetrahedral group.

EXAMPLE 2.34. (BINARY OCTAHEDRAL GROUP, $\mathbb{BO}$.) In the natural representation, we have generator elements being represented by

$$\varrho_{\mathrm{Nat}}(a) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix}, \qquad \text{and} \qquad \varrho_{\mathrm{Nat}}(b) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}.$$

The group consists of 48 elements in 8 conjugacy classes,

$$\begin{aligned} \mathrm{Cl}(e) &= \{e = a^8\}, \\ \mathrm{Cl}(a) &= \{a, b, a^7, a^4b^3, a^3b^3a, ab^3a^3\}, \\ \mathrm{Cl}(a^2) &= \{a^2, b^2, a^2b^2, b^2a^2, a^6, a^4b^2\}, \\ \mathrm{Cl}(ab) &= \{ab, ba, a^3b^3, a^2b^3a, ab^3a^2, ba^3b^2, b^2a^3b, b^3a^3\}, \\ \mathrm{Cl}(a^3) &= \{a^3, b^3, a^5, a^4b, a^3ba, aba^3\}, \\ \mathrm{Cl}(a^2b) &= \{a^2b, aba, ab^2, ba^2, b^2a, a^3b^2, a^2b^3, ab^3a, ba^3b, b^2a^3, b^3a^2, a^5ba\}, \\ \mathrm{Cl}(a^4) &= \{a^4\}, \\ \mathrm{Cl}(a^3b) &= \{a^3b, a^2ba, aba^2, ab^3, ba^3, b^3a, a^5b, a^4ba\}. \end{aligned}$$

The trivial representation, $\varrho_{\text{Triv.}}$, which maps $a, b \mapsto 1$ is a given, and similarly to the case above, since a and b belong to the same conjugacy class, another one-dimensional irreducible representation may be found by solving the equation

$$\frac{1}{48}(1 + 6\zeta^m + 6\zeta^{2m} + 8\zeta^{2m} + 6\zeta^{3m} + 12\zeta^{3m} + \zeta^{4m} + 8\zeta^{4m}) = 0,$$

where $\zeta = e^{i\frac{\pi}{4}}$ for $m \in \{1, 2, 3, 4, 5, 6, 7\}$. The solution occurs when $m = 4$, and so we have our second one-dimensional irreducible representation 1B being given by $a, b \mapsto \zeta^4 = (-1)$. This information is all we need in order to deduce the complete reduced character table of $\mathbb{BO}$, displayed in Tab. 2.35, and the McKay quiver which may be found therefrom, displayed in Fig. 2.36.

Character theory immediately gives us that $\varrho_{1\text{B}} \otimes \varrho_{\text{Nat}} \cong \varrho_{2\text{B}}$, and so our second two-dimensional irreducible representation is given by

$$\varrho_{2\text{B}}(a) = \frac{1}{\sqrt{2}}\begin{pmatrix} -1-i & 0 \\ 0 & -1+i \end{pmatrix}, \qquad \text{and} \qquad \varrho_{2\text{B}}(b) = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & i \\ i & -1 \end{pmatrix}.$$

Next is the irreducible representation 3A. This time the element a generates a subgroup isomorphic to the cyclic group of order 8, $\mathbb{Z}_8 \cong \langle a \rangle < \mathbb{BO}$, and when we consider the restriction of $\varrho_{3\text{A}}$ to $\langle a \rangle$, we find that the trivial representation $\theta_{\text{Triv.}}$ of $\langle a \rangle$ occurs with multiplicity 1 in the decomposition of $\varrho_{3\text{A}}|_{\langle a \rangle}$, nicely in line with the case of $\mathbb{BT}$,

	e	a	a^2	a^3	a^4	a^5	a^6	a^7
$\varrho_{3\text{A}}\|_{\langle a \rangle}$	3	1	−1	1	3	1	−1	1
$\theta_{\text{Triv.}}$	1	1	1	1	1	1	1	1

$$\langle \varrho_{3\text{A}}|_{\langle a \rangle}, \theta_{\text{Triv.}} \rangle = \frac{1}{8}(3+1-1+1+3+1-1+1) = 1.$$

Again, we use the subgroup $\langle a \rangle$ to find a rank-1 element, and, using Dixon's restricted character algorithm, find the matrices making up the representation 3A. With

$$\alpha(g) = \sum_{a \in \langle a \rangle} \theta_{\text{Triv.}}(a^{-1})\chi_{3\text{A}}(ag^{-1}) = \sum_{k=0}^{7} \chi_{3\text{A}}(a^k g^{-1}),$$

and choosing a basis of $\{a, b, ab\}$, we obtain

$$A(1) = \begin{pmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{pmatrix}, \qquad A(a) = \begin{pmatrix} 8 & 0 & 0 \\ 0 & 0 & 8 \\ 0 & -8 & 0 \end{pmatrix}, \qquad A(b) = \begin{pmatrix} 0 & 8 & 0 \\ -8 & 0 & 0 \\ 0 & 0 & 8 \end{pmatrix},$$

and consequently,

$$\varrho_{3\text{A}}(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \qquad \varrho_{3\text{A}}(b) = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Character theory further informs us that $\varrho_{1\text{B}} \otimes \varrho_{3\text{A}} \cong \varrho_{3\text{B}}$, and so we may right away give the representation 3B by the matrices

$$\varrho_{3\text{B}}(a) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad \varrho_{3\text{B}}(b) = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

For the representation 2C, we are once more in luck, as the trivial representation $\theta_{\text{Triv.}}$ of $\langle a \rangle$ occurs with multiplicity 1 in the decomposition of $\varrho_{2\text{C}}|_{\langle a \rangle}$,

	e	a	a^2	a^3	a^4	a^5	a^6	a^7
$\varrho_{3\text{A}}\|_{\langle a \rangle}$	2	0	2	0	2	0	2	0
$\theta_{\text{Triv.}}$	1	1	1	1	1	1	1	1

$$\langle \varrho_{2\text{C}}|_{\langle a \rangle}, \theta_{\text{Triv.}} \rangle = \frac{1}{8}(2+0+2+0+2+0+2+0) = 1.$$

With a basis of $\{a, b\}$, we find

$$A(1) = \begin{pmatrix} 8 & -4 \\ -4 & 8 \end{pmatrix}, \qquad A(a) = \begin{pmatrix} 8 & -4 \\ -4 & -4 \end{pmatrix}, \qquad A(b) = \begin{pmatrix} -4 & 8 \\ 8 & -4 \end{pmatrix},$$

and consequently,

$$\varrho_{2\mathrm{C}}(a) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \qquad \varrho_{2\mathrm{C}}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

As $\varrho_{\mathrm{Nat}} \otimes \varrho_{2\mathrm{C}} \cong \varrho_{4\mathrm{A}}$, we get the final irreducible representation by

$$\varrho_{4\mathrm{A}}(a) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1+i & 0 & 0 & 0 \\ 0 & 1-i & 0 & 0 \\ -1-i & 0 & -1-i & 0 \\ 0 & -1+i & 0 & -1+i \end{pmatrix}, \qquad \varrho_{4\mathrm{A}}(b) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & -i \\ 0 & 0 & -i & 1 \\ 1 & -i & 0 & 0 \\ -i & 1 & 0 & 0 \end{pmatrix}.$$

	e	a	a^2	ab	a^3	a^2b	a^4	a^3b
Triv.	1	1	1	1	1	1	1	1
1B	1	-1	1	1	-1	-1	1	1
Nat.	2	$\sqrt{2}$	0	1	$-\sqrt{2}$	0	-2	-1
2B	2	$-\sqrt{2}$	0	1	$\sqrt{2}$	0	-2	-1
2C	2	0	2	-1	0	0	2	-1
3A	3	1	-1	0	1	-1	3	0
3B	3	-1	-1	0	-1	1	3	0
4A	4	0	0	-1	0	0	-4	1

TABLE 2.35. The reduced character table of the binary octahedral group.

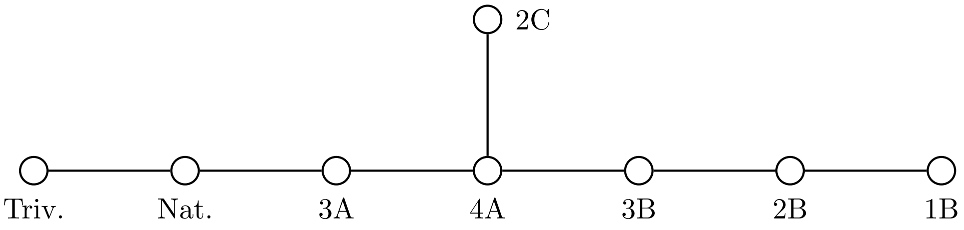


FIGURE 2.36. The McKay quiver of the binary octahedral group.

EXAMPLE 2.37. (BINARY DODECAHEDRAL GROUP, $\mathbb{BD}$.) Finally then is the binary dodecahedral group. In the natural representation, we have generator elements being represented by

$$\varrho_{\mathrm{Nat}}(a) = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^9 \end{pmatrix}, \qquad \varrho_{\mathrm{Nat}}(b) = \frac{1}{10} \begin{pmatrix} 5(\zeta - \zeta^4) - \sqrt{5}(\zeta + \zeta^4) & -2\sqrt{5}(\zeta + \zeta^4) \\ -2\sqrt{5}(\zeta + \zeta^4) & 5(\zeta - \zeta^4) + \sqrt{5}(\zeta + \zeta^4) \end{pmatrix}, \tag{2.38}$$

where $\zeta = e^{i\frac{\pi}{5}}$. The group consists of 120 elements, which come in 9 conjugacy classes. This is all the information we need to deduce their reduced character table (see Tab. 2.39), and the associated McKay quiver (see Fig. 2.40).

Restricting the natural representation to the subgroup $\mathbb{Z}_4 \cong \langle a^3b \rangle < \mathbb{BD}$, we find that $\varrho_{\mathrm{Nat}}|_{\langle a^3b \rangle} \cong \theta_1 \oplus \theta_3$, where θ_1, θ_3 are the first and third irreducible representations of $\mathbb{Z}_4$ (listed as ϱ_1 and ϱ_3 in Tab. 2.20). Then, using a basis of $\{a, b\}$, we can apply Dixon's restricted character algorithm on the natural representation itself, to obtain it in a much cleaner form, the end result being equivalent to an appropriate change of basis:

$$\varrho_{\mathrm{Nat}}(a) = \begin{pmatrix} 0 & i \\ i & \frac{1}{2}(1+\sqrt{5}) \end{pmatrix}, \qquad \varrho_{\mathrm{Nat}}(b) = \begin{pmatrix} -i & i \\ -\frac{1}{2}(1+\sqrt{5}) & \frac{1}{2}(1+\sqrt{5}) + i \end{pmatrix}.$$

This actually turns out to be of great use to us, as the Python script written by the author treats the group from the point of view of the faithful representation that the natural representation is. Writing the generator elements in this new form is a far less computationally expensive approach than that of (2.38). To illustrate, whereas in the latter case, it takes the author's laptop 9 minutes and 33 seconds to generate the entire group, in this new form, the same is accomplished in merely 2 minutes and 32 seconds. Changing from one to the other, then, we have greatly reduced the time it will take us to complete the example.

We are further fortunate in that restricting the representation 2B to $\langle a^3b\rangle$, we again obtain a representation isomorphic to $\theta_1 \oplus \theta_3$. Thus, again choosing $\{a, b\}$ for our basis, we find

$$\varrho_{2\mathrm{B}}(a) = \begin{pmatrix} 0 & i \\ i & \frac{1}{2}(1-\sqrt{5}) \end{pmatrix}, \qquad \varrho_{2\mathrm{B}}(b) = \begin{pmatrix} -i & i \\ -\frac{1}{2}(1-\sqrt{5}) & \frac{1}{2}(1-\sqrt{5})+i \end{pmatrix}.$$

The next subgroup of interest is $\mathbb{BD}_{2\cdot 3} \cong \langle ab^2, a^3b\rangle < \mathbb{BD}$. The isomorphism being given by the mapping $ab^2 \mapsto r$, $a^3b \mapsto s$, we find that the representation $\theta_{1\mathrm{B}}$ of $\mathbb{BD}_{2\cdot 3}$ (listed as $\varrho_{1\mathrm{B}}$ in Tab. 2.20) occurs once as a summand in the representation 6A restricted to $\langle ab^2, a^3b\rangle$. Choosing a basis of $\{a, b, ab, ba, ab^2a, ababa\}$, we obtain

$$\varrho_{6\mathrm{A}}(a) = \frac{1}{5}\begin{pmatrix} 0 & -5i & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 & 0 \\ 2-i & -5i & -4-3i & 3-4i & -1-2i & -2+6i \\ -4+2i & 5i & -2+i & -1+3i & -3-i & -1-2i \\ 0 & 0 & 0 & -5 & 0 & 0 \\ 0 & 0 & 0 & 0 & -5 & 0 \end{pmatrix},$$

$$\varrho_{6\mathrm{A}}(b) = \frac{1}{5}\begin{pmatrix} 0 & 0 & 0 & 5 & 0 & 0 \\ -1-2i & -5 & -3+4i & -4+3i & -2+i & 6+2i \\ 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & -5 \\ -5i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5i & 0 & 0 & 0 \end{pmatrix}.$$

Restriction of the representation 4A to $\langle ab^2, a^3b\rangle$ also features the irreducible representation $\theta_{1\mathrm{B}}$ occurring only once as a summand in its decomposition. Picking a basis of $\{a, b, ab, ba\}$, we find

$$\varrho_{4\mathrm{A}}(a) = \begin{pmatrix} 0 & -i & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 2 & 1+2i & -i & -2-i \\ -1 & -1-2i & 1+i & 1+i \end{pmatrix}, \qquad \varrho_{4\mathrm{A}}(b) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -2i & 2-i & -1 & -1+2i \\ -1-2i & 1-2i & i & 2i \\ 1-i & 2+i & -1-i & -1 \end{pmatrix}.$$

Restricting the representation 4B to $\langle ab^2, a^3b\rangle$ on the other hand features the trivial representation of $\mathbb{BD}_{2\cdot 3}$ as a lone constituent component. Picking a basis of $\{a, b, ab, ba\}$, we find

$$\varrho_{4\mathrm{B}}(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & 1 \\ -1 & 1 & -2 & -2 \end{pmatrix}, \qquad \varrho_{4\mathrm{B}}(b) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & -1 & 1 & 1 \\ 1 & -1 & 1 & 0 \\ -2 & 1 & -2 & -1 \end{pmatrix}.$$

Finally, we turn to the subgroup $\mathbb{Z}_{10} \cong \langle a\rangle < \mathbb{BD}$. We find that its trivial representation occurs precisely once in the restrictions of the representations 3A, 3B, and 5A to $\langle a\rangle$. With a basis of $\{a, b, ab\}$, then, we find

$$\varrho_{3\mathrm{A}}(a) = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ -1+\sqrt{5} & -2 & -1+\sqrt{5} \end{pmatrix}, \qquad \varrho_{3\mathrm{A}}(b) = \frac{1}{2}\begin{pmatrix} 0 & 2 & 0 \\ 1-\sqrt{5} & 2 & 1-\sqrt{5} \\ -2 & -1+\sqrt{5} & -1+\sqrt{5} \end{pmatrix},$$

and

$$\varrho_{3\mathrm{B}}(a) = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 2 \\ -1-\sqrt{5} & -2 & -1-\sqrt{5} \end{pmatrix}, \qquad \varrho_{3\mathrm{B}}(b) = \frac{1}{2}\begin{pmatrix} 0 & 2 & 0 \\ 1+\sqrt{5} & 2 & 1+\sqrt{5} \\ -2 & -1-\sqrt{5} & -1-\sqrt{5} \end{pmatrix},$$

and using a basis of $\{a, b, ab, a^2b, a^3b\}$, we find

$$\varrho_{5\mathrm{A}}(a) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 & -1 \end{pmatrix}, \qquad \varrho_{5\mathrm{A}}(b) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Finally, there is of course the trivial representation, which is (trivially) given by the mapping $\varrho_{\mathrm{Triv.}} : a, b \mapsto 1$.

	e	a	a^2	a^3	a^2b	a^4	a^3b	a^5	a^4b
Triv.	1	1	1	1	1	1	1	1	1
Nat.	2	$\frac{1}{2}(1+\sqrt{5})$	$-\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$	1	$-\frac{1}{2}(1+\sqrt{5})$	0	-2	-1
3A	3	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$	0	$\frac{1}{2}(1+\sqrt{5})$	-1	3	0
4A	4	1	-1	1	-1	-1	0	-4	1
5A	5	0	0	0	-1	0	1	5	-1
6A	6	-1	1	-1	0	1	0	-6	0
2B	2	$\frac{1}{2}(1-\sqrt{5})$	$-\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$	1	$-\frac{1}{2}(1-\sqrt{5})$	0	-2	-1
4B	4	-1	-1	-1	1	-1	0	4	1
3C	3	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$	0	$\frac{1}{2}(1-\sqrt{5})$	-1	3	0

TABLE 2.39. The reduced character table of the binary octahedral group.

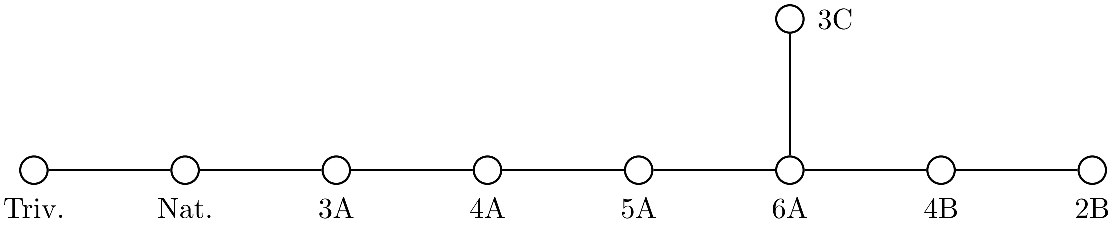


FIGURE 2.40. The McKay quiver of the binary dodecahedral group.

CHAPTER 3

A Crash Course in Algebraic Geometry

For being a highly abstract area of mathematics, the basic idea underlying all of algebraic geometry is actually simple enough. Namely, it is possible to describe geometric shapes and structures by algebraic equations. As a friendly example, a circle of radius unity can be described by the set of points which are the solutions of the equation $x^2 + y^2 = 1$. In this vein, we may describe a wide range of shapes, curves, surfaces, volumes, and set of points as being the simultaneous equations for a system of algebraic equations.

An appealing property of algebraic equations is that for every one of them, we may find a polynomial function whose roots cover all the solutions of that algebraic equation. For example, the solutions to $y = \sqrt{\frac{1-x^2}{1+x^2}}$ can all be found among the roots of the polynomial $f(x, y) = y^2x^2 + y^2 + x^2 - 1$. Therefore, rather than discussing points as being the simultaneous solutions to systems of algebraic equations, we may just as well discuss them as being zero loci of a set of polynomials. In fact, it is more than just as well. The set of polynomials over a base field forms a ring, and in particular, the set of polynomials that are zero at a specific set of points form an ideal, and so we may begin to use tools from ring theory to explore geometric constructs.

This insight then gently opens the gates to classical algebraic geometry, which in its generalized and abstracted form of modern algebraic geometry allows for the study of far more sophisticated structures than the ones mentioned heretofore. Lofty ambitions of understanding *that*, however, is of course far beyond the scope of this thesis[1], and in this introductory chapter on the subject we shall be satisfied with tracing the outlines of the basic building blocs of classical algebraic geometry which we will make use of, and endeavour to provide exposition for what purposes these building blocs serve. The important point that the author wishes for the reader to take away from these opening remarks is that *algebraic geometry is the study of geometric structures through the lens of polynomials.*

In the following, we will rely mainly on [20] and [21]. We will also draw on [22], [23], and [24].

1. The Mathematics of Zero Loci

We begin by codifying the points outlined in the opening remarks in clear terminology, and start our journey by working in the simplest type of space which we can conceive of for a given field $\mathbb{F}$, which we will take to be algebraically closed[2].

Definition 3.1. (Affine space.) We define the *affine space* of dimension n over a field $\mathbb{F}$ to simply be the vector space $\mathbb{F}^n$. This is denoted $\mathbb{A}\mathbb{F}^n$, or more commonly just $\mathbb{A}^n$,

$$\mathbb{A}^n := \{(a_1, \dots, a_n) | a_1, \dots, a_n \in \mathbb{F}\}.$$

[1] Not to mention the author's own knowledge!

[2] Meaning that though the results all apply to $\mathbb{C}$, they may not necessarily apply to $\mathbb{R}$.

Definition 3.2. (Polynomial ring.) Given a field $\mathbb{F}$, the polynomial ring of n variables, $\mathbb{F}[z_1, \dots, z_n]$, is the set of all functions $\mathbb{F}^n \to \mathbb{F}$ that are of polynomial form,

$$\mathbb{F}[z_1, \dots, z_n] := \{\sum_I a_I z^I | a_I \in \mathbb{F}\},$$

where I is a multi-index, $I = (i_1, \dots, i_n)$ and $z^I = z_1^{i_1} \dots z_n^{i_n}$.

Definition 3.3. (Zero locus on an affine space.) Let T be a subset of $\mathbb{F}[z_1, \dots, z_n]$. Then the *zero locus* of T, denoted $Z(T)$ is defined as

$$Z(T) := \{(a_1, \dots, a_n) \in \mathbb{A}^n | f(a_1, \dots, a_n) = 0,\ \forall f \in T\}.$$

Definition 3.4. (Affine algebraic set.) Let X be a subset of $\mathbb{A}^n$. If there exist a subset $T \subset \mathbb{F}[z_1, \dots, z_n]$ so that $X = Z(T)$, then X is called an *affine algebraic set.*

The intersection of two algebraic sets is itself an algebraic set. Further the union of two algebraic sets is itself also an algebraic set. This means that we can define a topology on $\mathbb{A}^n$ in terms of the algebraic sets.

Definition 3.5. (Zariski topology.) Let $\mathbb{A}^n$ be an affine space. The *Zariski topology* of $\mathbb{A}^n$ is the topology whose closed sets are the algebraic sets of $\mathbb{A}^n$.

Definition 3.6. (Affine variety.) Let V be an algebraic subset of $\mathbb{A}^n$. If V cannot be expressed as the union of two distinct proper algebraic subsets, then V is called an *affine (algebraic) variety.* An open subset of an affine variety is called a *quasi-affine variety.*

Some writers (c.f. Harris), refer to all algebraic sets as varieties, and refer to the construct in the definition above specifically as an *irreducible variety*, seeing it is an irreducible subset of the Zariski topology.

Being a collection of points at which a set of polynomials vanish, it is apparent that one can often define the same algebraic set in a large number of ways. For example, letting our base field be $\mathbb{C}$, the algebraic set $A = Z(x)$ is the same as $Z(x^2)$ and again the same as $Z(x^3)$. In fact, given two polynomials f and g which are zero at a point p, $f + g$ must also be zero at p, and if f is zero at p and h is any other polynomials, fh must also be zero at p. In other words, not just can there exist a plurality of polynomials which vanish at a given point, or a given set of points, these points form an ideal:

Definition 3.7. (Ideal of an affine algebraic set.) Let $X \subset \mathbb{A}^n$ be an algebraic set. Then the set of all polynomials in $\mathbb{F}[z_1, \dots, z_n]$ which vanish at every point in X form an ideal of $\mathbb{F}[z_1, \dots, z_n]$, called the *ideal of* X, which we will denote by $I(X)$.

Lemma 3.8. X is a variety if and only if $I(X)$ is prime.

Proof. If $X = X_1 \cup X_2$, then $I(X) = I(X_1) \cap I(X_2)$. If $I(X)$ is prime, from ring theory we know that it cannot be the intersection of two ideals both properly containing $I(X)$, and so we must have either $I(X) = I(X_1)$ or $I(X) = I(X_2)$. This in turn means that either $X = X_1$ or $X = X_2$. That is, X is a variety.

Suppose then that $I(X)$ is not prime. Then, there exists two polynomials $f_1, f_2 \notin I(X)$ such that $f_1 f_2 \in I(X)$. Since we are working over a field, if $f_1(p)f_2(p) = 0$ at any p, then either $f_1(p) = 0$ or $f_2(p) = 0$. Consequently, we may write $X = (X \cap Z(f_1)) \cup (X \cap Z(f_2))$. Since $Z(f_1) \not\supset X$ and $Z(f_2) \not\supset X$ either, $(X \cap Z(f_1))$ and $(X \cap Z(f_2))$ are both proper closed subsets of X, meaning that X is not a variety. □

From the definition of the ideal of an algebraic set, it follows that given an algebraic set $X \subset \mathbb{A}^n$, we could well describe it as $Z(T)$, where T is any generating subset of $I(X)$. Returning to the particular example of the algebraic set A, we could well have written it $Z(T)$, where $T = \{x^n | n \in \mathbb{Z}_+\}$, which is an infinitely large set of polynomials. While such a cumbersome definition is clearly unnecessary to give a complete description of A, the question does arise: Are there any algebraic sets which can *only* be written as $Z(T)$ for infinitely large T? The answer is no, and we shall now prove it.

Definition 3.9. Let R be a ring. If every infinitely ascending chain of ideals in R is stationary, that is, if $I_1 \subset I_2 \subset I_3 \subset \dots$ is a chain of ideals in R, we always eventually reach a point where $I_m = I_{m+1} = I_{m+2} = \dots$, R is said to be *Noetherian.*

Lemma 3.10. A ring is Noetherian if and only if every ideal in it can be generated by finitely many elements.

Proof. Let R be a ring in which every ideal can be generated by finitely many elements. Take an infinite ascending chain of ideals in R, $I_1 \subset I_2 \subset I_3 \subset \dots$, and consider the union of all these ideals, $I := \cup_i I_i$. Being a union of a chain of ideals, I itself must be an ideal as well, and so it can be generated by finitely many elements. This means that there must exist I_m such that every generating element is contained within it. This then means that $I = I_m$, and in turn, $I_m = I_{m+1} = I_{m+2} = \dots$. Consequently R must be Noetherian.

Now instead let R be a Noetherian ring, and assume it contains an ideal that cannot be finitely generated. Then, there must exist an infinite set of distinct elements $\{r_i\}$ such that the ascending chain of ideals

$$(r_1) \subset (r_1, r_2) \subset (r_1, r_2, r_3) \subset \dots$$

is non-stationary. But this would then mean that R is not Noetherian! By contradiction, a Noetherian ring must then by necessity allow for every ideal in it to be finitely generated. □

Theorem 3.11. (Hilbert's Basis Theorem.) Let R be a Noetherian ring. Then the ring of polynomials in one variable over R, $R[z]$, is also a Noetherian ring.

Proof. The proof consists of making use of the knowledge that every ideal in R is finitely generated to demonstrate that every ideal in $R[z]$ must also be finitely generated. The standard way of doing this is through proof by contradiction, and we will replicate it here.

Pick an arbitrary ideal I in $R[z]$, and assume it not to be finitely generated. The elements of this ideal are then polynomials of the form $f(z) = a_n z^n + \cdots + a_1 z + a_0$. Given a generic polynomials $f_i \in I$, denote its leading term by a_i. For the set of polynomials $\{f_i\}$ in $R[z]$ we have a corresponding set of elements $\{a_i\}$ in R. Since the $\{f_i\}$ form an ideal in $R[z]$, the $\{a_i\}$ must form an ideal in R, call it J.

In I, we may then pick a set of distinct polynomials f_i after the following scheme. For f_1, we pick a polynomials of minimal degree. For f_2, pick a polynomial of minimal degree in $I \backslash (f_1)$, for f_3 pick a polynomial of minimal degree in $I \backslash (f_1, f_2)$, and so on, for f_i picking any polynomial of minimal degree in $I \backslash (f_1, \dots, f_{i-1})$.

We then turn our attention back to J. Since R is Noetherian, J is finitely generated, and so in our course of picking f_i's, we will eventually each an f_m such that $(a_1, \dots, a_m) = J$. We claim then that $\{f_1, \dots, f_m\}$ similarly generates I, and to demonstrate this, we arrive at the proof by contradiction.

Pick f_{m+1} according to the scheme above, and assume that $f_{m+1} \notin (f_1, \ldots, f_m)$. Since $(a_1, \ldots, a_m) = J$, it follows that for the leading coefficient of f_{m+1} we have

$$a_{m+1} = \sum_{i=1}^{m} r_i a_i, \quad \text{for some } r_i \in R.$$

Consider then the polynomial

$$g = f_{m+1} - \sum_{i=1}^{m} r_i f_i z^{\deg(f_{m+1}) - \deg(f_i)}.$$

Since the second term clearly is in $(f_1, \ldots, f_m)$, g cannot be in $(f_1, \ldots, f_m)$, as otherwise f_{m+1} would have to be in $(f_1, \ldots, f_m)$ as well. However, since both terms in g have the same leading coefficient, the degree of g is strictly smaller than that of f_{m+1}, meaning that f_{m+1} is not minimal with the property of not being in $(f_1, \ldots, f_m)$. We have arrived at a contradiction, and may thus conclude that $I = (f_1, \ldots, f_m)$. □

Corollary 3.12. If $\mathbb{F}$ is a field, then its only ideals are $\{0\}$ and $\mathbb{F}$ itself, which are generated by 0 and 1 respectively. Consequently, $\mathbb{F}$ is Noetherian, and so is $\mathbb{F}[z_1]$, $\mathbb{F}[z_1, z_2]$, $\mathbb{F}[z_1, z_2, z_3]$, and by extension $\mathbb{F}[z_1, \ldots, z_n]$ for any $n \in \mathbb{Z}_+$.

Closely related to the Noetherian ring is the Noetherian topological space.

Definition 3.13. (Noetherian topological space.) Let T be a topological space. If every infinitely descending chain of closed subsets of T is stationary, that is, if $S_1 \supset S_2 \supset S_3 \supset \ldots$ is a chain of closed subsets of T, we always eventually reach a point where $S_m = S_{m+1} = S_{m+2} = \ldots$, T is said to be a *Noetherian topological space.*

Lemma 3.14. $\mathbb{A}^n$ is a Noetherian topological space in the Zariski topology.

Proof. By Cor. 3.12, $\mathbb{F}[z_1, \ldots, z_n]$ is a Noetherian ring. Given an infinitely descending chain $S_1 \supset S_2 \supset S_3 \supset \ldots$ of $\mathbb{A}^n$ then, $I(S_1) \subset I(S_2) \subset I(S_3) \subset \ldots$ is an infinitely ascending chain of $\mathbb{F}[z_1, \ldots, z_n]$ and so there exists m such that $I(S_m) = I(S_{m+1}) = I(S_{m+2}) = \ldots$. Since $X = Z(I(X))$ for any algebraic set X, $S_m = S_{m+1} = S_{m+2} = \ldots$, and so $\mathbb{A}^n$ is Noetherian. □

Theorem 3.15. Every algebraic set in $\mathbb{A}^n$ may be expressed uniquely as a finite union of affine varieties, no one containing another.

Proof. Assume that there exists algebraic sets in $\mathbb{A}^n$ which cannot be expressed as a finite union of affine varieties. Collect all such then in a set $\mathcal{A}$. Since $\mathbb{A}^n$ is a Noetherian topological space, there must in $\mathcal{A}$ exist minimal elements, algebraic sets which do not contain proper algebraic subsets. Let X be such a minimal element. X cannot be an affine variety, as then it would be trivial to write it as a finite union of affine varieties, disqualifying it from membership in $\mathcal{A}$. This means that there exists proper algebraic subsets X_1, X_2 of X such that $X = X_1 \cup X_2$. But this then means that X is not minimal. The only way to avoid a contradiction is to conclude that all algebraic sets in $\mathbb{A}^n$ may be expressed as finite unions of affine varieties. For an algebraic set X then, given a set of varieties $\{X_i\}$ whose union is X, we may always discard all elements in $\{X_i\}$ that are proper subsets of other elements in $\{X_i\}$, obtaining a finite union of affine varieties whose union is X, no one containing another.

Finally we prove uniqueness. Let $\{Y_1, \ldots, Y_n\}$ and $\{Z_1, \ldots, Z_m\}$ be two such sets whose unions make up the algebraic set X, none of the Y_i containing another and none of the Z_j containing another. Then $Y_1 \subset Z_1 \cup \cdots \cup Z_m$. Since the intersection of a set of algebraic sets is itself always an algebraic set, Y_1 must be found in precisely one of the Z_j, otherwise it would be possible to express it as a union of proper algebraic subsets, meaning it wouldn't be a variety. Thus there exists Z_k such that $Y_1 \subset Z_k$. Relabel the Z_j then so that Z_k becomes Z_1. Since

$Z_1 \subset Y_1 \cup \cdots \cup Y_n$, by the same reasoning, there exists Y_ℓ such that $Y_1 \subset Z_1 \subset Y_\ell$. But since none of the Y_i contain one another, we must have $\ell = 1$, and then $Y_1 = Z_1$. Then simply remove Y_1 from X and consider $X \backslash Y_1$. By repeating this procedure for all $Y_i \in \{Y_1, \ldots, Y_n\}$, uniqueness then follows. □

Given an algebraic set X then, seeing that $X = Z(I(X))$, and $I(X)$ is finitely generated, we can always write $X = Z(f_1, \ldots, f_m)$, where $\{f_1, \ldots, f_m\}$ is the generating set of $I(X)$. This does certainly seem a neater and more complete way of expressing things. After all, why write $Z(x^6, x^9, x^{42})$ when you can write $Z(x)$? And this leads us to our next point of inquiry, what is the most complete way of expressing algebraic sets?

As we've noted thus far, given an algebraic set $X = Z(T)$, then $X = Z((T))$ also, where (T) is the ideal generated by T, self-evidently a subset of $I(X)$. Further, if $f \in (T)$, then $f^k \in (T)$ for $k \in \mathbb{Z}_+$, for example, since $x^6 \in (x^6, x^9, x^{42})$, so $x^{12} = (x^6)^2 \in (x^6, x^9, x^{42})$ as well. The reverse, however, is plainly not true, for example, $x^3 \notin (x^6, x^9, x^{42})$, even though $x^6 = (x^3)^2 \in (x^6, x^9, x^{42})$. However, $x^3 \in (x)$, and we are led to make the following definition.

Definition 3.16. (Radical of an Ideal.) Given an ideal I of a ring R, the set of all elements $r \in R$ such that $r^k \in I$ for some $k \in \mathbb{Z}_+$ themselves form an ideal, known as the *radical of* I, denoted $\sqrt{I}$.

With this definition, we may write $(x) = \sqrt{(x^6, x^9, x^{42})}$. Returning to our specific discussion of zero loci of polynomials, as we noted that any algebraic set X may be expressed as $X = Z(T)$ where T is any subset of polynomials in $I(X)$ which vanish at X and nowhere else, we make the following statement:

Theorem 3.17. (Hilbert's Nullstellensatz.) Given any algebraic set $X = Z(T)$, $X \subset \mathbb{A}^n$, $T \subset \mathbb{F}[z_1, \ldots, z_n]$, the ideal of functions vanishing on X is the radical of the ideal generated by the set of polynomials T,

$$I(Z(T)) = \sqrt{(T)}.$$

Consequently, there exists a bijective correspondence between radical ideals in $\mathbb{F}[z_1, \ldots, z_n]$ and algebraic subsets of $\mathbb{A}^n$.

On the face of it, this statement may seem perfectly obvious, but actually proving it is not a trivial feat. Nevertheless, not just for completeness, but also because the *Nullstellensatz* will provide light for us as we explore the foundations of algebraic geometry further down this chapter, we will furnish a proof of it.

First we prove the *Nullstellensatz* in a very special case, namely when (T) is the entirety of $\mathbb{F}[z_1, \ldots, z_n]$. Since this contains the constant polynomials, which are zero nowhere, $Z(T) = \emptyset$. Further, the radical of $\mathbb{F}[z_1, \ldots, z_n]$ is $\mathbb{F}[z_1, \ldots, z_n]$ itself. We are thus looking at proving the following:

Theorem 3.18. (Weak Nullstellensatz.) The only ideal $I \subset \mathbb{F}[z_1, \ldots, z_n]$ for which $Z(I) = \emptyset$ is $I = \mathbb{F}[z_1, \ldots, z_n]$.

Proof. It is known that in a commutative ring with unity, every proper ideal is contained within a maximal ideal. Seeing that $\mathbb{F}[z_1, \ldots, z_n]$ is a commutative ring with unity, if we can show that every maximal ideal in $\mathbb{F}[z_1, \ldots, z_n]$ has a non-empty zero locus, the weak *Nullstellensatz* follows. □

This, in turn, will be guaranteed if the following lemma is proven to hold:

LEMMA 3.19. Every maximal ideal $\mathfrak{m}$ in the ring $\mathbb{F}[z_1, \ldots, z_n]$ is a *point ideal*, that is, it is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_i \in \mathbb{F}$.

The reason why $(x_1 - a_1, \ldots, x_n - a_n)$ is called a point ideal is because the effect of taking the quotient $\mathbb{F}[z_1, \ldots, z_n]/(x_1 - a_1, \ldots, x_n - a_n)$ is equivalent to evaluating the polynomial at $(a_1, \ldots, a_n) \in \mathbb{A}^n$. Specifically, if φ is the quotient map $\mathbb{F}[z_1, \ldots, z_n] \to \mathbb{F}[z_1, \ldots, z_n]/(x_1 - a_1, \ldots, x_n - a_n)$ and $f(z_1, \ldots, z_n) \in \mathbb{F}[z_1, \ldots, z_n]$, then $\varphi(f(z_1, \ldots, z_n)) = f(a_1, \ldots, a_n) + (x_1 - a_1, \ldots, x_n - a_n)$, and we may write $\mathbb{F}[z_1, \ldots, z_n]/\mathfrak{m} \cong \mathbb{F}[a_1, \ldots, a_n]$.

From ring theory, it is known that an ideal $\mathfrak{a}$ of a ring R is maximal if and only if $R/\mathfrak{a}$ is a field, and so since $\mathfrak{m}$ is maximal, it follows that $\mathbb{F} \subset \mathbb{F}[z_1, \ldots, z_n]/\mathfrak{m}$ is a field extension. Since we had at the beginning established that $\mathbb{F}$ was algebraically closed, its only algebraic field extension is $\mathbb{F} \subset \mathbb{F}$. This means that Lem. 3.19 in turn will follow from the following:

LEMMA 3.20. (ZARISKI'S LEMMA.) If an integral domain over a field $\mathbb{F}$ of the form $\mathbb{F}[\xi_1, \ldots, \xi_n]$, is itself also a field, then $\mathbb{F} \subset \mathbb{F}[\xi_1, \ldots, \xi_n]$ is an algebraic field extension.

There are different ways in which to prove Zariski's lemma. Harris [20] begins by proving the Noether normalization lemma, and then shows how Zariski's lemma follows as a consequence. One may also prove it within the context of Jacobson rings (see [25]). Zariski himself in his original paper [26] relied on nothing other than mathematical induction, and in the interest of elegance, that is the version of the proof we shall replicate here.

PROOF. First we prove the base case. If $\mathbb{F}[\xi_1]$ is a field, then there exist an inverse to every nonzero element in it. In particular, there exists $f(\xi_1) \in \mathbb{F}[\xi_1]$ such that $\xi_1 f(\xi_1) = 1$. Then evidently ξ_1 is a root of the polynomial $xf(x) - 1$, and $\mathbb{F} \subset \mathbb{F}[\xi_1]$ is an algebraic field extension.

Next, assume it has been proven that if $\mathbb{F}[\xi_1, \ldots, \xi_{n-1}]$ is a field, then it is an algebraic extension of $\mathbb{F}$. Then consider $\mathbb{F}[\xi_1, \ldots, \xi_{n-1}, \xi_n]$. If it is a field, then every nonzero element in it has an inverse, and in particular there exists an element $(\xi_1)^{-1}$ therein. Thus, $\mathbb{F}(\xi_1)$ is a subfield of $\mathbb{F}[\xi_1, \ldots, \xi_n]$. Since $\mathbb{F}(\xi_1)[\xi_2, \ldots, \xi_n] \subset \mathbb{F}[\xi_1, \ldots, \xi_n]$ and $\mathbb{F}(\xi_1)[\xi_2, \ldots, \xi_n] \supset \mathbb{F}[\xi_1, \ldots, , \xi_n]$, it follows that $\mathbb{F}(\xi_1)[\xi_2, \ldots, , \xi_n] = \mathbb{F}[\xi_1, \ldots, \xi_n]$. Since we had already proven that the lemma held true for $n-1$ ξ_i's over *any* field, it follows that $\mathbb{F}[\xi_1, \ldots, \xi_n]$ must be an algebraic field extension of $\mathbb{F}(\xi_1)$. All that remains to show is that the element ξ_1 in particular is algebraic over $\mathbb{F}$ and we are done.

First, $\mathbb{F}[\xi_1, \ldots, \xi_n] = \mathbb{F}[\xi_1][\xi_2, \ldots, \xi_n]$, and it is further easy to see that given any $\omega \in \mathbb{F}[\xi_1][\xi_2, \ldots, \xi_n]$ and $\beta \in \mathbb{F}[\xi_1]$, for sufficiently large ρ, we have $\omega\beta^\rho \in \mathbb{F}[\xi_1][\beta\xi_2, \ldots, \beta\xi_n]$.

Since $\mathbb{F}(\xi_1) \subset \mathbb{F}(\xi_1)[\xi_2, \ldots, \xi_n]$ is an algebraic extension, each ξ_i, $2 \leq i \leq n$ is the root of some polynomial $g_i(z) \in \mathbb{F}(\xi_1)[z]$. Let v_i be the product of the denominators of all the coefficients in $g_i(z)$, and set $f_i(z) = v_i g_i(z)$. Then f_i has all its coefficients in $\mathbb{F}[\xi_1]$, and furthermore, ξ_i is a root of f_i. Setting $m_i = \deg(f_i)$ then have

$$f_i(\xi_i) = a_{m_i}\xi_i^{m_i} + a_{m_i-1}\xi_i^{m_i-1} + \cdots + a_1\xi_i + a_0 = 0,$$

where all $a_i \in \mathbb{F}[\xi_1]$. Denoting a_{m_i}, the leading coefficient of f_i by b_i and rearranging, we have

$$b_i\xi_i^{m_i} = -a_{m_i-1}\xi_i^{m_i-1} - \cdots - a_1\xi_i - a_0. \tag{3.21}$$

As before mentioned, given any ω and β, there exists a ρ such that $\omega\beta^\rho \in \mathbb{F}[\xi_1][\beta\xi_2, \dots, \beta\xi_n]$. Let then $\beta = b_2 \dots b_n$. This then means that we can express $\omega\beta^\rho$ as

$$\begin{aligned}\omega\beta^\rho &= \sum_{j_2,\dots,j_n} \omega_{j_2,\dots,j_n}(\beta\xi_2)^{j_2}\dots(\beta\xi_n)^{j_n} \\ &= \sum_{j_2,\dots,j_n} \omega_{j_2,\dots,j_n}\beta^{j_2+\dots+j_n}\xi_2^{j_2}\dots\xi_n^{j_n},\end{aligned}$$

all $\omega_{j_2,\dots,j_n} \in \mathbb{F}[\xi_1]$. Viewing this strictly as a sum of power products $\xi_2^{j_2}\dots\xi_n^{j_n}$, we may simplify it further: Any time a factor of $\xi_i^{m_i}$ appears in a term, we may break out a b_i from $\beta^{j_2+\dots+m_i+\dots+j_n}$, couple it with $\xi_i^{m_i}$ and substitute for (3.21). To recapitulate, what this all means is that given any element $\omega \in \mathbb{F}[\xi_1, \dots, \xi_2]$, there exists an integer ρ such that $\omega(b_2 \dots b_n)^\rho$ can be expressed as a linear combination of the power products $\xi_2^{j_2}\dots\xi_n^{j_n}$, $0 \le j_i \le m_i - 1$, all coefficients being in $\mathbb{F}[\xi_1]$.

Next, let ν be the relative degree of the field extension $\mathbb{F}(\xi_1) \subset \mathbb{F}(\xi_1)[\xi_2, \dots, \xi_n]$, and let $\omega_1 = 1, \omega_2, \dots, \omega_\nu$ be an $\mathbb{F}(\xi_1)$-basis of $\mathbb{F}(\xi_1)[\xi_2, \dots, \xi_n]$. Then every element $g \in \mathbb{F}(\xi_1)[\xi_2, \dots, \xi_n]$ can be expressed uniquely as a linear combination of the form

$$g = a_1 + a_2\omega_2 + \dots + a_\nu\omega_\nu, \quad a_i \in \mathbb{F}(\xi_1).$$

Further, we may always find $h \in \mathbb{F}[\xi_1]$ such that the first coefficient in the expansion of gh is in $\mathbb{F}[\xi_1]$, and by extension, given any collection of elements $\{g_1, \dots, g_k\}$, we may always find an element h such that the first coefficients of all linear expansions $\{g_1h, \dots, g_kh\}$ are in $\mathbb{F}[\xi_1]$. This applies to the power products $\xi_2^{j_2}\dots\xi_n^{j_n}$ we just recently discussed as well, of course. Let us denote the element we choose to accomplish this particular task for the power products by b_1.

Now then, we may consider the expression ωb^ρ where $b = b_1b_2\dots b_n$. It follows from the definition of b_1 that in the expansion $\omega b^\rho = a_1 + a_2\omega_2 + \dots + a_\nu\omega_\nu$, $a_1 \in \mathbb{F}[\xi_1]$. This now applies for any element $\omega \in \mathbb{F}[\xi_1][\xi_2, \dots, \xi_n]$, so let us pick $\omega = (\zeta)^{-1}$ where ζ is an arbitrary element of $\mathbb{F}[\xi_1]$. This then means that $\omega b^\rho \in \mathbb{F}(\xi_1)$, and so in the expansion

$$\omega b^\rho = a_1 + a_2\omega_2 + \dots + a_\nu\omega_\nu$$

since the ω_i's are all linearly independent, $a_i = 0$ for all $i \ge 2$. In other words, $(\zeta)^{-1}b^\rho = a_1$, or $\zeta a_1 = b^\rho$, all of $\zeta, a_1, b^\rho \in \mathbb{F}[\xi_1]$. Now we may finally prove that ξ_1 is algebraic over $\mathbb{F}$.

If ξ_1 *weren't* algebraic, then it would have to be transcendental, and $\mathbb{F}[\xi_1] \cong \mathbb{F}[z]$. $\mathbb{F}[z]$ is a unique factorization domain, being a principal ideal domain, and so b may be factorized into a finite product of irreducible elements $\{\phi_i\}$, $b = \prod_i \phi_i$. We have just shown that for every $\zeta \in \mathbb{F}[\xi_1]$, there necessarily exists $\rho \in \mathbb{N}$ such that $\zeta | b^\rho$. This must then hold true if ζ is irreducible as well. However, since the set $\{\phi_i\}$ is finite and there exists an infinite number of inequivalent irreducible elements in $\mathbb{F}[z]$, clearly if $\mathbb{F}[\xi_1] \cong \mathbb{F}[z]$ we arrive at a contradiction, and we conclude that ξ_1 is algebraic over $\mathbb{F}$. From that, Zariski's lemma in its entirety follows. □

With Zariski's lemma proven, as outlined above, the weak *Nullstellensatz* follows. We now prove the full *Nullstellensatz* by showing how it follows from the weak version of it.

Proof. (Rabinowitsch' Trick.) First, it is clear that $\sqrt{(T)} \subset I(Z(T))$. After all, given any $f^k \in (T)$ and $p \in Z(T)$, $f^k(p) = 0$, and so $f(p) = 0$ as well since we are working over a field $\mathbb{F}$, and fields do not allow for the existence of zero-divisors. To prove that $I(Z(T)) \subset \sqrt{(T)}$, what we need to prove is that for every $f \in I(Z(T))$, there exists an integer k such that $f^k \in (T)$. Let us write out the generating polynomials of $I(Z(T))$ as $\{f_1, \dots, f_m\}$.

Let us then take an arbitrary $f \in I(Z(T))$. By definition, $f(z_1, \ldots, z_n) = 0$ for all $(z_1, \ldots, z_n) \in Z(T) \subset \mathbb{A}^n$. Rabinowitsch' famous trick then consists of "moving up a dimension", and look at our system from the point of view of $\mathbb{A}^{n+1}$ and $\mathbb{F}[z_1, \ldots, z_{n+1}]$. We may then consider the ideal generated by the polynomials $\{f_1, \ldots, f_m, 1 - z_{n+1}f(z_1, \ldots, z_n)\}$. At all points at which $\{f_1, \ldots, f_m\}$ all vanish, $f = 0$, and so evidently, the final polynomial must yield the value of 1. In other words, this algebraic set does not have any common zero points, and so the weak *Nullstellensatz* applies—the ideal they generate is $\mathbb{F}[z_1, \ldots, z_{n+1}]$ in its entirety. This means that 1 is contained within $(f_1, \ldots, f_m, 1 - z_{n+1}f(z_1, \ldots, z_n))$, and we may thus find polynomials $g_0, g_1, \ldots, g_m \in \mathbb{F}[z_1, \ldots, z_{n+1}]$ such that

$$1 = g_0(z_1, \ldots, z_{n+1})(1 - z_{n+1}f(z_1, \ldots, z_n)) + \sum_{i=1}^{m} g_i(z_1, \ldots, z_{n+1})f_i(z_1, \ldots, z_n).$$

This equality must hold true for all values of $\{z_1, \ldots, z_n, z_{n+1}\}$, so we are at liberty to set $z_{n+1} = 1/f(z_1, \ldots, z_n)$. Then we obtain the equation,

$$1 = \sum_{i=1}^{m} g_i(z_1, \ldots, z_n, 1/f(z_1, \ldots, z_n))f_i(z_1, \ldots, z_n).$$

g_i will then be of the form

$$g_i(z_1, \ldots, z_n, 1/f(z_1, \ldots, z_n)) = \sum_{j_1, \ldots, j_{n+1}} \frac{\gamma_{j_1, \ldots, j_{n+1}} z_1^{j_1} \ldots z_n^{j_n}}{f(z_1, \ldots, z_n)^{j_{n+1}}},$$

all $\gamma_{j_1, \ldots, j_{n+1}} \in \mathbb{F}$. This means that for sufficiently large k, we may write

$$g_i(z_1, \ldots, z_n, 1/f(z_1, \ldots, z_n)) = \frac{h_i(z_1, \ldots, z_n)}{f(z_1, \ldots, z_n)^k}, \quad h_i \in \mathbb{F}[z_1, \ldots, z_n],$$

for all g_i. This means that we end up with the equation

$$1 = \sum_{i=1}^{m} \frac{h_i(z_1, \ldots, z_n)f_i(z_1, \ldots, z_n)}{f(z_1, \ldots, z_n)^k},$$

which, after re-arranging, is

$$f(z_1, \ldots, z_n)^k = \sum_{i=1}^{m} h_i(z_1, \ldots, z_n)f_i(z_1, \ldots, z_n).$$

In other words, $f^k \in I(Z(T))$. The proof is finished. □

Corollary 3.22. If f is an irreducible polynomial, then $Z(f)$ is a variety.

Proof. Since f is irreducible, (f) is prime, and further, $(f) = \sqrt{(f)}$. By the *Nullstellensatz*, we then have $(f) = I(Z(f))$. Since $I(Z(f))$ then is prime, Lem. 3.8, $Z(f)$ is a variety. □

Definition 3.23. (Products of affine varieties.) We may endow $\mathbb{A}^n \times \mathbb{A}^m$ with the structure of the affine space $\mathbb{A}^{n+m}$ by the map $\tau : (x_1, \ldots, x_n) \times (y_1, \ldots, y_m) \mapsto (x_1, \ldots, x_n, y_1, \ldots, y_m)$. If X, Y are algebraic sets, then $\tau(X \times Y)$ is an algebraic set in $\mathbb{A}^{n+m}$, given by $\tau(X \times Y) = Z(\{f_i(x_1, \ldots x_n)\} \cup \{g_j(y_1, \ldots, y_m)\})$, as $\mathbb{F}[x_1, \ldots, x_n] \subset \mathbb{F}[x_1, \ldots, x_n, y_1, \ldots, y_m] \supset \mathbb{F}[y_1, \ldots, y_m]$.

Having studied affine algebraic sets in some detail, we now turn our eyes on a different type of algebraic set—projective ones. To do that however, we first need to define the concept of a projective space.

Definition 3.24. (Projective space.) Given a field $\mathbb{F}$, we create the affine space $\mathbb{A}^{n+1}$. The set of equivalence classes of vectors in $\mathbb{A}^{n+1} \backslash \{0\}$ which are related by $(z_1, \ldots, z_{n+1}) \sim (\lambda z_1, \ldots, \lambda z_{n+1})$, $\lambda \in \mathbb{F} \backslash \{0\}$ forms *projective space* of dimension n over the field $\mathbb{F}$, which is denoted $\mathbb{FP}^n$, or more commonly just $\mathbb{P}^n$.

While it would be possible to work in $n+1$ affine coordinates in $\mathbb{A}^{n+1}$ to describe $\mathbb{P}^n$, it is more commonly swifter to work in $n+1$ *homogeneous coordinates.* By $[Z_0, \ldots, Z_n] \in \mathbb{P}^n$ we would then refer to the equivalence class which contains all non-zero scalar multiples of the vector $(Z_0, \ldots, Z_n)$ in $\mathbb{A}^{n+1}$.

In general, the values that a polynomial $F \in \mathbb{F}[Z_0, \ldots, Z_n]$ assume on $\mathbb{P}^n$ are not well-defined. Since $[Z_0, \ldots, Z_n] \equiv [\lambda Z_0, \ldots, \lambda Z_n]$, we would have to require $F(Z_0, \ldots, Z_n) = F(\lambda Z_0, \ldots, \lambda Z_n)$ for all $\lambda \in \mathbb{F}$. Unless F happens to be a constant polynomial, this is not the case.

However, if F happens to be homogeneous of some degree d, that is

$$F(\lambda Z_0, \ldots, \lambda Z_n) = \lambda^d F(Z_0, \ldots, Z_n),$$

we can still in a meaningful sense talk about its zero locus, as if $F(a_0, \ldots, a_n) = 0$ at some point $(a_0, \ldots, a_n)$, then $F(\lambda a_0, \ldots, \lambda a_n) = 0$ for all values of λ still. Thereby, we may make the following definition.

Definition 3.25. (Projective algebraic set.) Let X be a subset of $\mathbb{P}^n$. If there exist a subset of homogeneous polynomials $T \subset \mathbb{F}[Z_0, \ldots, Z_n]$ so that $X = Z(T)$, then X is called an *projective algebraic set.*

The reader may be inclined to protest, and argue that this is too narrow a definition. Homogeneous polynomials vanishing at a point $(a_0, \ldots, a_n)$ are not the only polynomials F such that if $F(a_0, \ldots, a_n) = 0$, then $F(\lambda a_0, \ldots, \lambda a_n) = 0$ for all $\lambda \in \mathbb{F}$. Any and all sums of homogeneous polynomials of arbitrary degrees that vanish at $(a_0, \ldots, a_n)$ also vanish at $(a_0, \ldots, a_n)$, and they need not be homogeneous. For example, $f(x, y) = x - \frac{1}{2}y + x^2 - \frac{1}{4}y^2$ vanishes not just at $(1, 2)$, but vanish at $(\lambda, 2\lambda)$ for any $\lambda \in \mathbb{C}$, and yet f is not homogeneous. The reader need not worry however, since if F is the sum of a set of homogeneous polynomials F_i of degrees d_i, then the zero locus of $F[Z_0, \ldots, Z_n] = \sum_i F_i[Z_0, \ldots, Z_n]$ is equivalent to the common zero locus of all the homogeneous polynomials F_i, and so it is seen that this definition of a projective set does indeed encapsulate all polynomials vanishing on $(\lambda a_0, \ldots, \lambda a_n)$ for every $\lambda \in \mathbb{F}$ if they vanish at $(a_0, \ldots, a_n)$.

In line with our discussion earlier regarding affine algebraic sets, we may define the Zariski topology on $\mathbb{P}^n$, and introduce the notions of *projective varieties* and *quasi-projective varieties.* We may also define the notion of the homogeneous ideal associated with a projective variety.

Definition 3.26. (Homogeneous ideal of a projective algebraic set.) Let $X \subset \mathbb{P}^n$ be an algebraic set. Then the homogeneous ideal generated by all homogeneous polynomials in $\mathbb{F}[Z_0, \ldots, Z_n]$ which vanish at every point in X form an ideal of $\mathbb{F}[Z_0, \ldots, Z_n]$, called the *homogeneous ideal of* X, which we will denote by $I(X)$.

Do note that despite its name, not all elements in a homogeneous ideal are homogeneous. For example, the ideal generated by x^2 contains the polynomial $x^2(y-1)$ which clearly isn't homogeneous. It is possible to derive the analogue of the *Nullstellensatz* for projective algebraic sets, though for lack of space, we will not do so here. The reader is encouraged to look up Andreas Gathmann's online lecture notes on algebraic geometry on the matter, as he does so in a very elegant way involving cones.

On the subsets $U_i \subset \mathbb{P}^n$ defined by all points $[Z_0, \ldots, Z_n]$ at which $Z_i \neq 0$, the ratios Z_j/Z_i are well defined for all $0 \leq j \leq n$. We may therefore construct bijective maps on these subsets $\varphi_i : U_i \to \mathbb{A}^n$ by $[Z_0, \ldots, Z_n] \mapsto (Z_0/Z_i, \ldots, Z_{i-1}/Z_i, Z_{i+1}/Z_i, \ldots, Z_n)$. Not just are these maps bijective, as now follows, they also preserve the Zariski topology, making them homeomorphisms.

Example 3.27. Let $X \subset \mathbb{P}^n$ be a projective algebraic set defined by the homogeneous polynomials $\{F_\alpha\}$. Then $\varphi_i(X \cap U_i)$ will be exactly the zero locus of the polynomials defined by

$$\begin{aligned} f_\alpha(z_1, \ldots, z_n) &= F_\alpha(Z_0, \ldots Z_n)/Z_i^d \\ &= F_\alpha(Z_0/Z_i, \ldots, 1, \ldots, Z_n/Z_i), \end{aligned}$$

where d is the degree of F_α. Conversely, if $Y \subset \mathbb{A}^n$ is an affine algebraic set defined by the polynomials $\{f_\alpha\}$, then we find that the points on $\varphi^{-1}(Y)$ are exactly described by the homogeneous polynomials defined by

$$\begin{aligned} F_\alpha(Z_0, \ldots, Z_n) &= Z_i^d f(Z_0/Z_i, \ldots, Z_n/Z_i) \\ &= Z_i^d \sum a_{j_1,\ldots,j_n} \left(\frac{Z_0}{Z_i}\right)^{j_1} \cdots \left(\frac{Z_n}{Z_i}\right)^{j_n} \\ &= \sum a_{j_1,\ldots,j_n} Z_i^{d-\sum j_\ell} Z_0^{j_1} \ldots Z_n^{j_n}. \end{aligned}$$

Consequently, φ_i maps projective algebraic sets to affine algebraic sets and vice versa for φ_i^{-1}. To be as specific as possible, since the U_i provides a covering for $\mathbb{P}^n$, a projective space may be regarded as a union of affine spaces, and a subset $X \subset \mathbb{P}^n$ is a projective algebraic set if and only if $\varphi_i(X \cap U_i)$ are affine algebraic sets for all i.

Still, one key ingredient is missing before we may access all our above results for affine algebraic sets when dealing with projective varieties, by regarding simply them through the lens of the maps φ_i. We need to establish that the bijection φ truly gives an isomorphism of algebraic sets, and defining what that is will be the topic of our next section.

Definition 3.28. (Segre embedding.) As we noted earlier in Def. 3.23, it is easy to endow $\mathbb{A}^n \times \mathbb{A}^m$ with the structure of an affine variety through a mapping $\mathbb{A}^n \times \mathbb{A}^m \to \mathbb{A}^{n+m}$. We cannot do the same thing for projective space and projective varieties though, as $\mathbb{P}^n \times \mathbb{P}^m$ and $\mathbb{P}^{n+m}$ are not homeomorphic as spaces. Nonetheless, it is still possible to give the space $\mathbb{P}^n \times \mathbb{P}^m$ the structure of a projective variety through the so-called Segre embedding, $\sigma : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$, given by

$$[X_0, \ldots, X_n] \times [Y_0, \ldots, Y_m] \mapsto [X_0Y_0, \ldots, X_iY_j, \ldots, X_nY_m].$$

Do note that the image of σ is not the entirety of $\mathbb{P}^{(n+1)(m+1)-1}$, but merely a subset of it. Nonetheless, this image is indeed a projective variety. If we denote the values assumed along the vectors X_i by a_i and denote the values assumed along the vectors Y_i by b_i, then since we must have $a_ib_ja_kb_\ell = a_ib_\ell a_kb_j$, it follows that the image of $\mathbb{P}^n \times \mathbb{P}^m$ may be given as the zero locus of the polynomials $Z_{i,j}Z_{k,\ell} = Z_{i,\ell}Z_{j,k}$. With this, along with the fact that $\mathbb{A}^n$ may always be embedded in $\mathbb{P}^n$, we may always discuss $\mathbb{A}^n \times \mathbb{P}^m$ and $\mathbb{P}^n \times \mathbb{P}^m$ as varieties.

Ex. 3.27 taken together with Thm. 3.15 determines that *all* algebraic sets may be expressed as finite unions of varieties. With this in mind, we can henceforth focus our attention entirely on varieties without having to consider the more general notion of algebraic sets, secure in the knowledge that all definitions we make regarding the former can always be extended to cover the latter.

2. Morphisms of Varieties

So far we have discussed in much detail the algebra of varieties, but we have yet to actually have touched on their geometry. We need to develop a notion for when two varieties "look like one another" in a rigorous sense, that is, we need to establish what it means for two varieties to be isomorphic. To do that, we need to establish what a morphism from one variety to another in the first place is, and that is what this section is intended to cover.

It is often the case in mathematics that when we study a class of objects that we wish to develop a notion of a structure-preserving map, or a *morphism*, between objects in that class. If we know how to construct such a map, then, upon having studied the properties of one object, we may apply our map and deduce properties of the other object. Hence, for example, we have our notions of group morphisms in group theory (which ensures that the structure of group multiplication is preserved) and smooth manifold morphisms in differential geometry (which ensures that smooth curves on one manifold are mapped to smooth curves on another manifold). Algebraic geometry is no different.

The reader might initially be a bit confused by the prompt that we have to develop a definition for morphisms between varieties. A variety is just a collection of points, they might say, they have no structure, any mapping from a collection of points to another another collection of points should be equally valid as an example of a morphism.

Not quite so. We recall our original definition. A variety is not just a collection of points, but a collection of points *which may be expressed as the zero locus of a set of polynomials.* The properties of a variety will be described in terms of polynomials that live on this variety, and so a morphism between two varieties must be defined in such a way as to reflect this polynomial structure. Let us restrict ourselves to the affine case for now, and begin by making the following definition.

Definition 3.29. (Coordinate ring of a variety.) Let $X \subset \mathbb{A}^n$ be an affine variety. We define the *coordinate ring of* X, denoted $\mathbb{F}[X]$, to be the polynomial ring $\mathbb{F}[z_1, \dots, z_n]$ restricted to the coordinates of X,

$$\mathbb{F}[X] = \mathbb{F}[z_1, \dots, z_n]\big|_X.$$

If two polynomials $f, g \in \mathbb{F}[z_1, \dots, z_n]$ are the same everywhere in X, then they may be regarded as being the same element in $\mathbb{F}[X]$.

It makes sense then, that we begin our line of inquiry in attempting to define a morphism between varieties by looking at morphisms between their coordinate rings. If we briefly return to the entirety of $\mathbb{F}[x_1, \dots, x_n]$ and $\mathbb{F}[y_1, \dots, y_m]$, we have that a morphism between them maps every element of one to the other, and particular, this applies to the generating elements $\{x_i\}$, so the morphism is completely determined by the maps $x_i \mapsto f_i(y_1, \dots, y_m)$, where $f_i \in \mathbb{F}[y_1, \dots, y_m]$. This then, in turn, induces a unique map $\mathbb{A}^m \to \mathbb{A}^n$ by $(x_1, \dots, x_m) \mapsto (f_1(y_1, \dots, y_m), \dots, f_n(y_1, \dots, y_m))$, which in turn of course uniquely induces back to the original morphism $\mathbb{F}[x_1, \dots, x_n] \to \mathbb{F}[y_1, \dots, y_m]$. In line with established nomenclature, let us denote the map $\mathbb{A}^m \to \mathbb{A}^n$ by ϕ and the map $\mathbb{F}[x_1, \dots, x_n] \to \mathbb{F}[y_1, \dots, y_m]$ by $\phi^{\#}$.

If we then restrict ϕ so that the domain is only $Y \subset \mathbb{A}^m$, and the codomain is only $X \subset \mathbb{A}^n$ by letting the $\{f_i\}$ only be elements of $\mathbb{F}[X]$, we obtain a corresponding morphism $\mathbb{F}[X] \to \mathbb{F}[Y]$. We denote the former by φ and the latter by $\varphi^{\#}$. We find that the morphism $Y \to X$ is in fact a continuous map in the Zariski topology—in other words, a topological morphism—from Y to X. If $V \subset X$ is an algebraic set, then it is the zero locus of a set of polynomials $\{g_i(x_1, \dots, x_n)\}$ in $\mathbb{F}[X]$, and so $\varphi^{-1}(V)$ is the intersection of the zero locus of polynomials $\{\varphi^{\#}(g_i(x_1, \dots, x_n)) = g_i \circ \varphi(y_1, \dots, y_m) = g_i(f_1(y_1, \dots, y_m), \dots, f_n(y_1, \dots, y_m))\} \in \mathbb{F}[y_1, \dots, y_m]$ with Y itself, making it a closed subset of Y, i.e. the zero locus of some polynomials $\{h_i(y_1, \dots, y_m)\} \in \mathbb{F}[Y]$.

While it does not escape us that such a definition may be seen as "backwards" as $Y \to X$ corresponds to $\mathbb{F}[X] \to \mathbb{F}[Y]$, polynomial maps $\mathbb{A}^m \to \mathbb{A}^n$ restricted to Y and X clearly encapsulate the structure preservation that we would like to see in a morphism between algebraic varieties $Y \to X$. In particular, we would have that $X \cong Y$ if and only if $\mathbb{F}[X] \cong \mathbb{F}[Y]$.

One key ingredient is still missing, however, as it is after all the *points* in the variety that we ultimately are interested in, and polynomial maps are defined *globally, for all points* in the source variety. We need to devise a *local* version of this definition, and so, we bring forth the heavy machinery.

Lemma 3.30. (Coordinate ring of an affine variety, Redux.) Let $X \subset \mathbb{A}^n$ be an affine variety. Then the quotient ring $A(X)$ defined by

$$A(X) := \mathbb{F}[z_1, \dots, z_n]/I(X),$$

is isomorphic to the coordinate find $\mathbb{F}[X]$.

Proof. We construct the morphism $\psi : A(X) \to \mathbb{F}[X]$ by $f + I(X) \mapsto f|_X$. If $f + I(X) \equiv g + I(X)$ in $A(X)$, then they may only differ by an element of $I(X)$, and as such, are the same everywhere on X, meaning they may be regarded as the same element in $I(X)$. Furthermore, if $f|_X \equiv g|_X$, then they may only differ by a polynomial that vanishes everywhere on X, that is, an element in $I(X)$, and as such correspond to the same element in $A(X)$. This makes the mapping well-defined. Further, since $\varphi(f+g) = \varphi(f) + \varphi(g)$ and $\varphi(fg) = \varphi(f)\varphi(g)$ it is indeed a morphism. It is clearly both surjective and injective, that is, it is an isomorphism. □

This isomorphism is so useful, that many authors tend to define $A(X)$ itself to be the coordinate ring. This is regrettable, since then the etymology of the term *coordinate ring* is lost. Nonetheless, in keeping with changing winds of mathematical terminology, henceforth, when referring to the *coordinate ring of* X, we will be referring to $A(X)$ rather than $\mathbb{F}[X]$, and as such, we will be looking at morphisms $A(Y) \to A(X)$ rather than $\mathbb{F}[Y] \to \mathbb{F}[X]$, as they are, indeed, equivalent.

Before we move on, as a final note, since we are only concerned with X being a variety, the ideal $I(X)$ is prime, and then, by Lem. 3.8, $A(X)$ is an integral domain.

Definition 3.31. (Localization.) Let R be a commutative ring with unity and $S \subset R$ a *multiplicatively closed* subset of R, and define an equivalence relation $\sim$ on $R \times S$ by letting $(r, s) \sim (r', s')$ if there exists $u \in S$ such that $u(rs' - r's) = 0$. Denoting the equivalence class of the pair (r, s) be $\frac{r}{s}$, we define the *localization of* R *to the subset* S, $S^{-1}R$, to be the ring of equivalence classes

$$S^{-1}R := \left\{ \frac{r}{s} \middle| r \in R, s \in S \right\},$$

where addition and multiplication is defined as for fractions. Note that if R contains no zero divisors, it can easily always be embedded into its localization $S^{-1}R$ by the map $r \mapsto \frac{r}{1}$, and we may just as well say that R is a subring of its localization.

An immediate question might be why this is called the *localization* of R at S and not the "*fractionalization*" of R at S. We now answer that question.

Example 3.32. (Total ring of fractions.) Let R be a commutative ring with unity and let S be the set of all elements of R which are not zero divisors. Then the *total ring of fractions of* R is defined to be the localization of R at S. This may be viewed as the generalization of the field of fractions which are defined for integral domains.

Example 3.33. (Localization at a prime ideal.) Let R be a commutative ring with unity, and let $\mathfrak{p}$ be a prime ideal thereof. Then $R\backslash\mathfrak{p}$ is multiplicatively closed, and $\mathfrak{p}^{-1}R$ is a localization denoted $R_\mathfrak{p}$.

Example 3.34. (Localization at a maximal ideal.) Let R be a domain. Then, all maximal ideals of R are prime. We have the relation

$$R = \bigcap_{\mathfrak{m}} R_\mathfrak{m},$$

where $\mathfrak{m}$ runs over all maximal ideals in R. To see that this is the case, note that since $R \subset R_{\mathfrak{m}}$ for all $\mathfrak{m}$, $R \subseteq \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$ trivially. Next, conceive of an element $z \in R_{\mathfrak{m}}$ for all $\mathfrak{m}$ such that $z \notin R$. Then we may construct the ideal $\mathfrak{n} := \{a \in R | az \in R\}$. It is easy to verify that this is in fact an ideal, and furthermore, since $z \notin R$, $1 \notin \mathfrak{n}$, meaning that it must be a proper ideal of R. This proper ideal must be contained within some maximal ideal $\mathfrak{q}$ in R. Since we have established that $z \in R_{\mathfrak{m}}$ for all $\mathfrak{m}$, it follows that $z \in R_{\mathfrak{q}}$, and so is a fraction $z = \frac{x}{y}$ for some $x \in R$, $y \in R \backslash \mathfrak{q}$. Then $yz \in R$. But if $yz \in R$, then $y \in \mathfrak{n}$, and since $\mathfrak{n} \subseteq \mathfrak{q}$, $y \in \mathfrak{q}$. We thus have a contradiction and (3.34).

Next, let $X \subset \mathbb{A}^n$ be an affine or quasi-affine variety. We now have four further definitions that at first glance appear to be totally unrelated to anything we have done so far.

Definition 3.35. (Regularity on a (quasi-)affine variety.) A function $f : X \to \mathbb{F}$ is said to be *regular at the point* p is there exists an open neighbourhood U, $p \in U \subseteq X$ and polynomials $g, h \in \mathbb{F}[z_1, \dots, z_n]$, h being nowhere zero on U, such that $f = g/h$ on U.

Definition 3.36. (Ring of regular functions.) The *ring of regular functions on* X is the set of all functions that are regular at every point in X. We denote it by $\mathcal{O}(X)$.

Definition 3.37. (Local ring of a point.) Let p be a point on X. We define the *local ring of p on X* to be the ring of equivalence classes $\langle U, f\rangle$, where U is an open subset of X containing p, and f is a regular function on U, and two pairs $\langle U, f\rangle, \langle V, g\rangle$ are defined to be equivalent if $f = g$ on $U \cap V$. We denote it by $\mathcal{O}_p$.

Definition 3.38. (Rational functions.) A *rational function* on X is an equivalence class of pairs $\langle U, f\rangle$ where U is a nonempty open subset of X and f is a regular function on U, and two pairs $\langle U, f\rangle$ and $\langle V, g\rangle$ are equivalent if $f = g$ on $U \cap V$.

From simple topological considerations, on an irreducible set, two open subsets cannot have an empty intersection. It they did, then the union of their complements would be the original set, which would contradict its irreducibility. As such, given any representative pairs $\langle U, f\rangle$ and $\langle V, g\rangle$ of rational functions on X, there is always an intersection $U \cap V \neq \emptyset$, and on this intersection we may define addition and multiplication as usual, giving the set of all rational functions on X, $K(X)$, the structure of a ring. Furthermore, any nonzero pair $\langle U, f\rangle$ has an inverse in $\langle U \backslash Z(f), 1/f\rangle$, meaning $K(X)$ has the structure of a field, called the *function field of* X.

Remark 3.39. $\mathcal{O}(X) \subseteq \mathcal{O}_p \subseteq K(X)$ for every $p \in X$, and in particular, $\mathcal{O}(X) = \bigcap_{p \in X} \mathcal{O}_p$.

Remark 3.40. If two globally regular functions f_1, f_2 are equal on a non-empty open subset $U \subset X$, then by definition, they correspond to the same element of $K(X)$, and so must correspond to the same element in $\mathcal{O}(X)$. That is, they are equal everywhere in X.

We define the injective map $\alpha : A(X) \to \mathcal{O}(X)$ by $f + I(X) \mapsto \frac{f}{1}$, and finally we tie everything together in a few short, but extremely powerful, theorems.

Theorem 3.41. There exists a one-to-one correspondence between points of X and maximal ideals of $A(X)$.

Proof. By Lem. 3.19, it follows that there must be a one-to-one-correspondence between points in X and maximal ideals in $\mathbb{F}[z_1, \dots, z_n]$ containing $I(X)$. Then by the correspondence theorem for rings, there exists a one-to-one correspondence between maximal ideals in $\mathbb{F}[z_1, \dots, z_n]$ containing $I(X)$ and maximal ideals in $A(X) = \mathbb{F}[z_1, \dots, z_n]/I(X)$. The reader need not be concerned about if $I(X)$ itself is one of those maximal ideals of $\mathbb{F}[z_1, \dots, z_n]$. True, then it corresponds to the zero ideal in $A(X)$, but since $I(X)$ is maximal, we also have that

$A(X)$ is a field, and in a field, the zero ideal is maximal. Putting one-to-one to one-to-one together, the theorem follows. Specifically, we have $\mathfrak{m}_p = \{f \in A(X) | f(p) = 0\}$. □

THEOREM 3.42. For each $p \in X$, $\mathcal{O}_p \cong A(X)_{\mathfrak{m}_p}$.

PROOF. The aforementioned injective ring morphism α induces a ring morphism $\alpha' : A(X)_{\mathfrak{m}_p} \to \mathcal{O}_p$, by $\frac{f+I(X)}{g+I(X)} \mapsto \frac{f}{g}$. It is seen that since $g + I(X) \notin \mathfrak{m}_p$, $\frac{f}{g}$ is always regular at p. This map inherits its injectivity from α, and as can plainly be seen, is surjective. □

THEOREM 3.43. $\mathcal{O}(X) \cong A(X)$.

PROOF. Using α', embed $A(X)$ and $A(X)_{\mathfrak{m}_p}$ for every p in $K(X)$. Then we have the tower,

$$A(X) \subseteq \mathcal{O}(X) \subseteq \bigcap_{p \in X} \mathcal{O}_p = \bigcap_{\mathfrak{m}_p} A(X)_{\mathfrak{m}_p} = A(X),$$

where the final equality follows from Example 3.34. We conclude $\mathcal{O}(X) \cong A(X)$. □

COROLLARY 3.44. If $\frac{f}{g} \in \mathcal{O}(X)$, then there exists $h + I(X) \in A(X)$ such that $h = \frac{f}{g}$.

This isomorphism between the ring of regular functions $\mathcal{O}(X)$ and the coordinate ring $A(X)$ is truly remarkable. For one thing, the name *localization* is justified. Just as $A(X)$ gives a description of the global regular functions on X, so $A(X)_{\mathfrak{m}_p}$ gives a description of the local regular functions at p. But more importantly, it allows us to finally give a definition for what a morphism between varieties should look like, and allows us to do so locally.

DEFINITION 3.45. We define a continuous map (in the Zariski topology) $\psi : X \to Y$ between varieties to be a *morphism*, if for every open set $U \subset Y$, and every regular function $f : U \to \mathbb{F}$, $f \circ \psi : \psi^{-1}(U) \to \mathbb{F}$ is a regular function.

DEFINITION 3.46. Let $\varphi : X \to Y$ be a morphism of varieties. If φ admits an inverse morphism $\varphi^{-1} : Y \to X$ such that $\varphi \circ \varphi^{-1} = 1_X$ and $\varphi^{-1} \circ \varphi = 1_Y$, then φ is said to be an *isomorphism* and X and Y are said to be *isomorphic*.

LEMMA 3.47. Let X be any variety, and let Y be an affine variety. Then $\psi : X \to Y$ is a morphism if and only if $y_i \circ \psi$ is a regular function for each and every i.

PROOF. Since the y_i are trivially regular functions on Y, it follows by definition that the $y_i \circ \psi$ are regular functions on X. Proving the converse, since all regular functions on Y are quotients of polynomial functions of the y_i, it follows that if a function f is regular on Y, then $f \circ \psi$ is regular on X. In particular, if f is a polynomial on Y, then $f \circ \psi$ is a regular function on X which we may denote g/h. Since any closed subset V of Y is the zero locus of a set of polynomials f_i, it follows that on X, $\psi^{-1}(V)$ the zero locus of the regular functions g_i/h_i. But since h_i are nowhere zero on X, it follows that it is the zero locus of the polynomials g_i, meaning that $\psi^{-1}(V)$ is itself a closed subset of X. Thus ψ is continuous. Thus ψ is a morphism. □

We now show that the definition given in 3.45 really does encapsulate what we want it to encapsulate, namely that for affine varieties, there is a bijection between variety morphisms $X \to Y$ and ring morphisms $A(Y) \to A(X)$.

PROPOSITION 3.48. Let X and Y be affine varieties. Then there is a natural bijection

$$\mathrm{Hom}(X, Y) \tilde{\to} \mathrm{Hom}(A(Y), A(X)).$$

PROOF. For affine varieties X, Y we have $A(X) \cong \mathcal{O}(X)$ and $A(Y) \cong \mathcal{O}(Y)$. In proving the bijection left-to-right, it therefore suffices to show that every morphism $X \to Y$ induces a unique morphism $\mathcal{O}(Y) \to \mathcal{O}(X)$. This follows from that a morphism $\varphi : X \to Y$ carries locally regular functions on each open subset $V \subset Y$ to locally regular functions on each open subset $\varphi^{-1}(V)$, and so induces a morphism $\varphi^{\#} : \mathcal{O}(Y) \to \mathcal{O}(X)$ of the globally regular functions.

A concern might be that there is no apparent guarantee that a global regular function f on Y is carried back to the same global regular function for every open subset $U \subset Y$. However, a closer look reveals that the mathematics has already provided that guarantee for us. Let f be a regular function on Y and let U and V be open subsets on Y. Let g_1 be the pullback of f to X on U and let g_2 be the pullback of f to X on V. Since Y is a variety, U and V have a non-empty intersection, and so on the open subset $\varphi^{-1}(U \cap V)$, we should at least have $g_1 = g_2$. Since $\varphi^{-1}(U)$ and $\varphi^{-1}(V)$ are open subsets of X, they have nonempty intersection, and since $\varphi^{-1}(U) \cap \varphi^{-1}(V) = \varphi^{-1}(U \cap V)$, it follows that $\varphi^{-1}(U \cap V)$ is non-empty. By Remark 3.40, we then have that $g_1 = g_2$ everywhere on X, ensuring that $\varphi^{\#}$ is well-defined.

This mapping is furthermore injective, since if $\psi^{\#} = \phi^{\#}$, then $y_i \circ \psi = y_i \circ \phi$ for all i, and so since the morphisms ψ and ϕ are defined by the regular functions $y_i \circ \psi$ and $y_i \circ \phi$, it follows that $\psi = \phi$.

For right-to-left, again make use of $A(X) \cong \mathcal{O}(X)$, and consider a generic morphism $h : A(Y) \to \mathcal{O}(X)$. Let $\overline{y}_i$ be the image of y_i under the quotient morphism $\mathbb{F}[y_1, \dots, y_n] \to A(Y)$, and let us denote $\xi_i = h(\overline{y}_i)$. These ξ are then globally regular functions on X, and so, by Lem. 3.47, the map $\psi : X \to \mathbb{A}^m$ given by $p \mapsto (\xi_1(p), \dots, \xi_m(p))$ constitutes a morphism. All that remains is proving that the image truly is contained in Y. This is done by noting that $Y = Z(I(Y))$, and so if we can prove that if f is any polynomial in $I(Y)$ and p is any point in X, that $f(\psi(p)) = 0$, then we are done.

Here then comes the sneaky part. If β is a polynomial function, for any ring morphism θ we have $\beta(\theta(r_1), \dots, \theta(r_\ell)) = \theta(\beta(r_1, \dots, r_\ell))$. Therefore,

$$\begin{aligned} f(\psi(p)) &= f(\xi_1(p), \dots, \xi_m(p)) \\ &= f(h(\overline{y}_1)(p), \dots, h(\overline{y}_m)(p)) = (f(h(\overline{y}_1), \dots, h(\overline{y}_m))(p) \\ &= (h(f(\overline{y}_1, \dots, \overline{y}_m)))(p), \end{aligned}$$

but, as established, $f \in I(Y)$, meaning that $h(f(\overline{y}_1, \dots, \overline{y}_m)) = h(0) = 0$, so trivially, $f(\psi(p)) = 0$. The proof is finished. □

EXAMPLE 3.49. Consider the affine varieties $X = Z(z - x^2 - y^2)$ and $Z(z - 2(x^2 + y^2 - \frac{1}{2})^2 - \frac{1}{2})$ (see Fig. 3.50). One can then construct a morphism $\varphi : X \to Y$ by the tuple of regular functions $(x, y, z) \mapsto (x, y, 2(x^2 + y^2 - \frac{1}{2})^2 - \frac{1}{2})$. This is an isomorphism, and an inverse function φ^{-1} can be given by $(x, y, z) \mapsto (x, y, x^2 + y^2)$.

The reader will have noted that in Def. 3.45, we did not specify that the variety X had to be affine. This is because the definition had already been extended to cover all sorts of varieties, be they quasi-affine, projective, or quasi-projective. We did however not give a definition of the regularity of a function in projective space, something which we will now remedy.

DEFINITION 3.51. (REGULARITY ON A QUASI-PROJECTIVE VARIETY.) Let $X \subset \mathbb{P}^n$ be a quasi-projective variety. A function $f : X \to \mathbb{F}$ is said to be *regular at the point* p is there exists an open neighbourhood U, $p \in U \subseteq X$ and homogeneous polynomials of the same degree $g, h \in \mathbb{F}[Z_0, \dots, Z_n]$, h being nowhere zero on U, such that $f = g/h$ on U. The requirement that g, h are of the same degree is necessary for f to be well-defined on X.

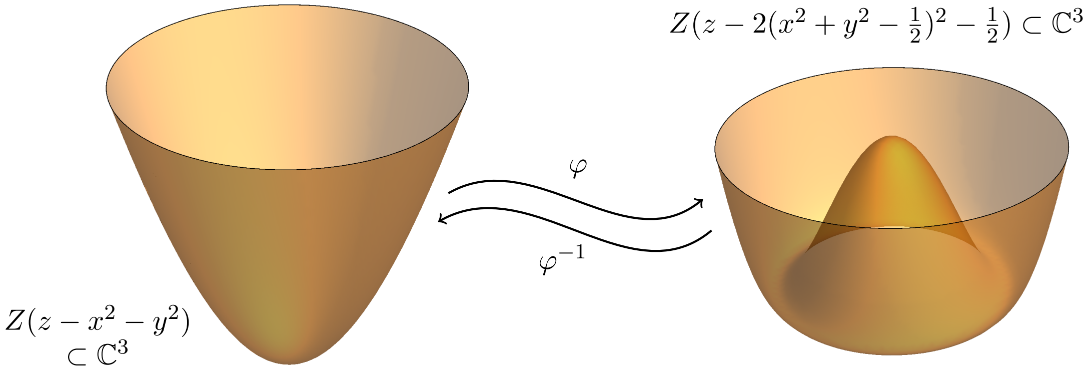

$Z(z-2(x^2+y^2-\frac{1}{2})^2-\frac{1}{2}) \subset \mathbb{C}^3$
φ
φ^{-1}
$Z(z-x^2-y^2)$
$\subset \mathbb{C}^3$

FIGURE 3.50. The real parts of the isomorphic varieties $Z(z-x^2-y^2)$ and $Z(z-2(x^2+y^2-\frac{1}{2})^2-\frac{1}{2})$.

Regular rings of a projective variety and local rings are defined in a similar fashion. By this definition, the bijection in Example 3.27 is easily verified to indeed be an isomorphism. Continuing on, we may also define the homogeneous coordinate ring of a projective variety.

DEFINITION 3.52. Let $X \subset \mathbb{P}^n$ be a projective variety, and let $I(X)$ be its corresponding homogeneous ideal. We define

$$S(X) := \mathbb{F}[Z_0, \dots, Z_n]/I(X)$$

to be the *homogeneous coordinate ring of* X. The homogeneous elements of it correspond to the set of homogeneous polynomials in $\mathbb{F}[Z_0, \dots, Z_n]$ restricted to X.

The reader may be wondering if in lieu of Prop. 3.48, the exists a similar correspondence between morphisms between projective varieties $X \to Y$ and homogeneous coordinate rings $S(Y) \to S(X)$. It turns out there isn't. Even more worryingly, it turns out that two isomorphic projective varieties need not necessarily have isomorphic homogeneous coordinate rings. Still, all is not lost. The correspondence still exists locally after a fashion in that an analogue of Thm. 3.42 can still be constructed for the local ring. If we by $S(X)_{(\mathfrak{m}_p)}$ denote the ring formed by elements of $S(X)_{\mathfrak{m}_p}$ that are of degree 0 (that is, the denominator and numerator are of the same degree), then we do in fact find that $\mathcal{O}_p \cong S(X)_{(\mathfrak{m}_p)}$. I will not include a proof of it here, but for reference, one such may be found in [21] (Theorem I.3.4 (b)).

3. Blowing Stuff Up: A Map of the Problematique

As the reader no doubt will have deduced by now from simply looking at the pictures, it is entirely possible for a variety to also be a manifold. Again, just consider the complex circle which may be given as the zero locus of the polynomial $x^2 + y^2 = 1$. As the reader no doubt also will have realized, this is not always necessarily the case, as the curves, or surfaces, or hypersurfaces that a variety may define need not be smooth, that is, they need not have well-defined tangent spaces. Just consider the variety defined by the polynomial $x^2 + y^2 + \frac{1}{5}z^3$ (see Fig. 3.53), where the tangent space is ill-defined at $(0, 0, 0)$. We encapsulate this distinction in the following definition.

DEFINITION 3.54. (NONSINGULARITY.) Let $Y = Z(f_1, \dots, f_\ell) \subseteq \mathbb{A}^n$ be an affine variety. We say that Y is *nonsingular at a point* $p \in Y$ if the Jacobian matrix $[(\partial f_i/\partial x_j)(p)]_{\substack{1\leq i\leq \ell \\ 1\leq j\leq n}}$ is of rank $n - r$, where r is the dimension of Y. We say that Y is *singular* at a point if at that point Y is nonnonsingular. If Y is nonsingular at every point $p \in Y$, we say that Y is a *nonsingular affine variety.*

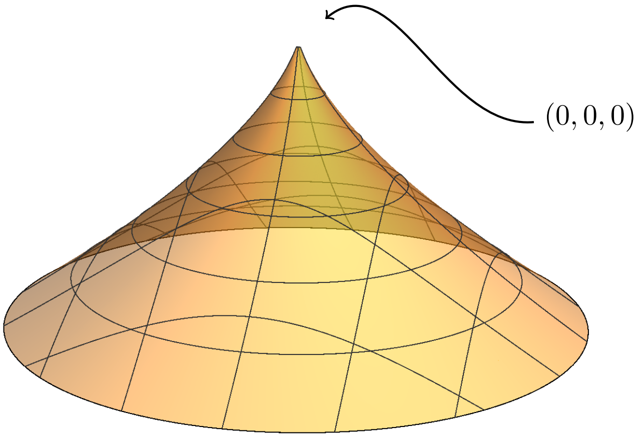


FIGURE 3.53. The zero locus of the polynomial $x^2+y^2+\frac{1}{5}z^3=0$ defines a cusp, which has an ill-defined tangent space at the point $(x,y,z)=(0,0,0)$.

To borrow Hartshorne's expression [21], "over the complex numbers, [...] nonsingular varieties are [then] those which in the 'usual' topology are complex manifolds". Without going into specifics, suffice to say that working with varieties with singularities can be very problematic indeed, and so we do not want to do it. Of course, this does not mean that the laws of mathematics will acquiesce to our requests and make every variety nonsingular, so if we want the singularities to go away, we have to find a way around the laws of mathematics.

Fair enough, but how does one actually do it? Well, these varieties, they will be embedded in some affine or projective space, so if we could find some other variety in some other space, and a morphism such that the image of the morphism is the entirety of the first space, then, since a morphism is a continuous map, we could simply do our work in the preimage of the first variety which will also be an algebraic set.

Fair enough again, but how then would one always be able to systematically construct such a space, such a variety, and such a morphism?

Let us restrict ourselves once again to affine varieties, and consider an illustrative example, the Maclaurin trisectrix, $x^2(a-y)-y^2(y+3a)=0$, which has a singularity at the origin (see Fig. 3.55). The most fundamental clue we can take from it is that as the curve intersects itself, it does so *from different directions*. It would therefore make sense to look at a space which is formed by the points in $\mathbb{A}^2$ but with the origin replaced by the directions running through the origin. Since the lines through the origin are the elements of $\mathbb{P}^1$, this would then have to be the space $\mathbb{A}^2\times\mathbb{P}^1$. However, the specific variety we are interested in constructing will not be the entirety of $\mathbb{A}^2\times\mathbb{P}^1$, as after all, it only is the origin that is problematic. In line with this, we make the following definition.

DEFINITION 3.56. (BLOW-UP OF THE AFFINE SPACE AT THE ORIGIN.) We define the *blowing up of* $\mathbb{A}^n$ *at the origin* to be the closed subset X of $\mathbb{A}^n\times\mathbb{P}^{n-1}$ defined by the equations $\{x_iy_j = x_jy_i | 1\leq i,j\leq n\}$, where the x_i are the affine coordinates of $\mathbb{A}^n$ and the y_i are the homogeneous coordinates of $\mathbb{P}^{n+1}$.

Being a closed subset, X is an algebraic set, and what is more, it can in fact be shown to be a full-fledged variety. Furthermore, it invites a natural morphism to $\mathbb{A}^n$, call it φ, by

$$(a_1,\dots,a_n)\times[b_1,\dots,b_n]\mapsto(a_1,\dots,a_n).$$

We now claim that the blow-up is exactly the variety that we have been looking for.

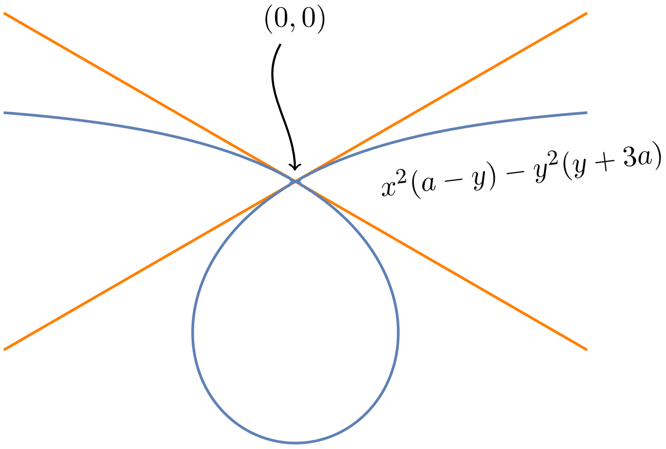


FIGURE 3.55. The Maclaurin trisectrix in blue which has a singularity at the origin. The lines in orange gives the tangent of the curve as it enters and leaves the origin both times.

PROPOSITION 3.57. There exists a one-to-one correspondence between points in $\mathbb{A}^n \backslash \{0\}$ and points in $\varphi^{-1}(\mathbb{A}^n \backslash \{0\})$.

PROOF. At first glance, this injectivity seems unlikely, seeing the morphism φ is defined entirely in terms of the a_i, and that the b_i may assume whatever values they like and still lead to the same point in $\mathbb{A}^n$. This would be true if we were working in the entirety of $\mathbb{A}^n \times \mathbb{P}^{n-1}$, but remember, we are restricted to X, and so $a_i b_j = a_j b_i$. As such, since we are not looking at the preimage of the origin, there exist at least one $a_i \neq 0$, and so we are looking at a morphism

$$(a_1, \ldots, a_n) \times \left[\frac{b_i}{a_i} a_1, \frac{b_i}{a_i} a_2, \ldots, \frac{b_i}{a_i} a_n\right] \mapsto (a_1, \ldots, a_n).$$

and since $[a_1, \ldots, a_n] \sim [\lambda a_1, \ldots, \lambda a_n]$ for homogeneous coordinates, we see that φ when restricted to $\varphi^{-1}(\mathbb{A}^n \backslash \{0\})$ truly is injective. □

DEFINITION 3.58. (EXCEPTIONAL DIVISOR.) Given a blow-up of the affine space $X \subset \mathbb{A}^n \times \mathbb{P}^{n-1}$ with associated morphism φ, we call the preimage of the origin in $\mathbb{A}^n$ the *exceptional divisor.*

PROPOSITION 3.59. There is a one-to-one correspondence between points in the exceptional divisor and lines running through the origin.

PROOF. To see this, we need to consider what elements in X that are mapped to the origin. That is plainly all elements $(0, \ldots, 0) \times [b_1, \ldots, b_n]$ for which $0 \cdot b_i = 0 \cdot b_j$ for all b_i, b_j. This is true for all values of b_i, b_j, and so we have that the points of the exceptional divisor are $\{0\} \times \mathbb{P}^{n-1} \cong \mathbb{P}^{n-1}$. But as we will recall from the definition, $\mathbb{P}^{n-1}$ *is* the set of lines running through the origin in $\mathbb{A}^n$, and so the proposition holds. □

If we let L be any line in $\mathbb{A}^n$ running through the origin, we may then create the punctated line $L' = L \backslash \{0\}$, and consider its preimage in X. The closure of $\varphi^{-1}(L')$ will then be found to be precisely the point in the exceptional divisor corresponding to the line L through the origin, and so since every point in $\mathbb{A}^n$ lies along a line running through the origin, we may write $X = \overline{\varphi^{-1}(\mathbb{A}^n \backslash \{0\})}$ where the overline denotes topological closure. We therefore may further make the following definition.

Definition 3.60. (Blow-up of an affine variety in a point.) Let $Y \subseteq \mathbb{A}^n$ be a variety, and let φ be the morphism associated with the blowing-up of $\mathbb{A}^n$ at the origin. We define the *blowing-up of Y are the origin* to be $\tilde{Y} = \overline{\varphi^{-1}(Y\backslash\{0\})}$. Its associated morphism is φ restricted to $\tilde{Y}$, often also denoted φ.

This is of course not a definition so much as it is a corollary. The use of a tilde to denote that it is a blow-up is conventional. To consolidate our understanding, let us consider three illustrative (and illustrated) examples.

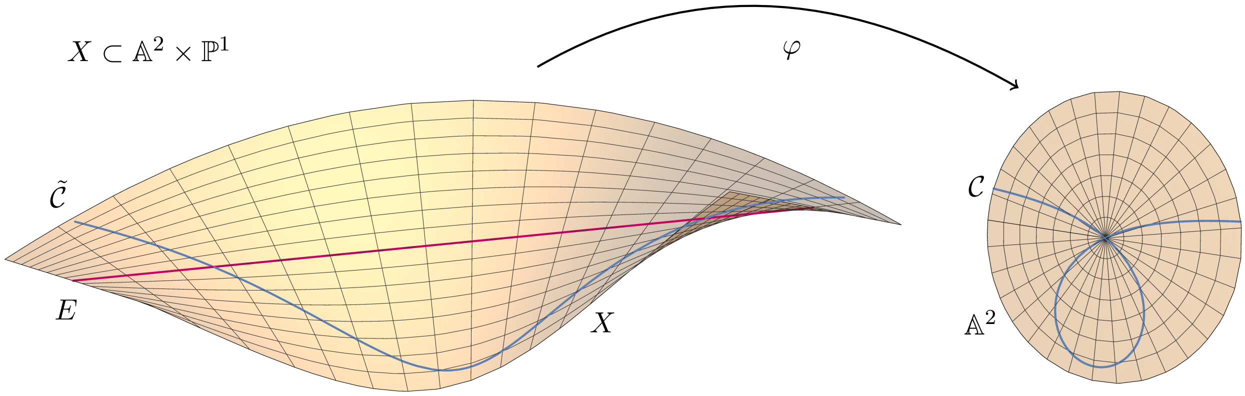


Figure 3.61. The blow-up of the affine plane $\mathbb{A}^2$ and the variety $\mathcal{C}$ defined by the Maclaurin trisectrix, at the origin. The blow-ups are denoted X and $\tilde{\mathcal{C}}$ respectively. The exceptional divisor of the former is the red line running through X, which we denote E. The exceptional divisor of the latter consists of the two points where $\tilde{\mathcal{C}}$ intersects E.

Example 3.62. (The Maclaurin Trisectrix.) We return to the aforementioned Maclaurin trisectrix, which is given by the equation $x^2(a-y)-y^2(y+3a)=0$, which we denote by $\mathcal{C}$. As we move up to X to study $\tilde{\mathcal{C}}$ that basic equation remains intact, but we have also now added two new homogeneous coordinates u, t which relate to the affine x, y by $xu = yt$. Picking a chart where $t \neq 0$, we may use the fact that u and t are homogeneous to set $u = 1$, and treat t as an affine coordinate. We are then looking at the system of equations describing $\tilde{\mathcal{C}}$,

$$\begin{aligned} x^2(a-y)-y^2(y+3a)&=0,\\ xt&=y, \end{aligned}$$

The second equation in particular is telling of what we are doing here—we are making the slope through the origin itself into a variable. Plugging the second equation into the first, we obtain $t^2y^2(a-y)-y^2(y+3a)=0$ which may be simplified into $y^2(y(t^2+1)-a(t^2-3))=0$, which has two irreducible factors, which give us two possible sets of solutions. Either $x, y = 0$ and t may assume any values—this corresponds to all of the exceptional divisor E—or $y(t^2+1)=a(t^2+3)$, $y = xt$—which corresponds to what we are looking for, $\tilde{\mathcal{C}}$. The two curves intersect at two points, at $t=\sqrt{3}$ and $t=-\sqrt{3}$ respectively. these two points, $(0,0)\times[\sqrt{3},1]$ and $(0,0)\times[-\sqrt{3},1]$ then form the exceptional divisor of the blow-up of $\mathcal{C}$.

In Fig. 3.61 we illustrate this blow-up of the Maclaurin trisectrix and the affine plane. Owing to the problem of graphing projective space, the figure is more conceptual than it is exact.

Example 3.64. (The Double Cone.) The double cone is given by the equation $Y = Z(x^2 + y^2 - z^2) \subset \mathbb{A}^3$. Calling the homogeneous coordinates a, b, c, we then look at the system of

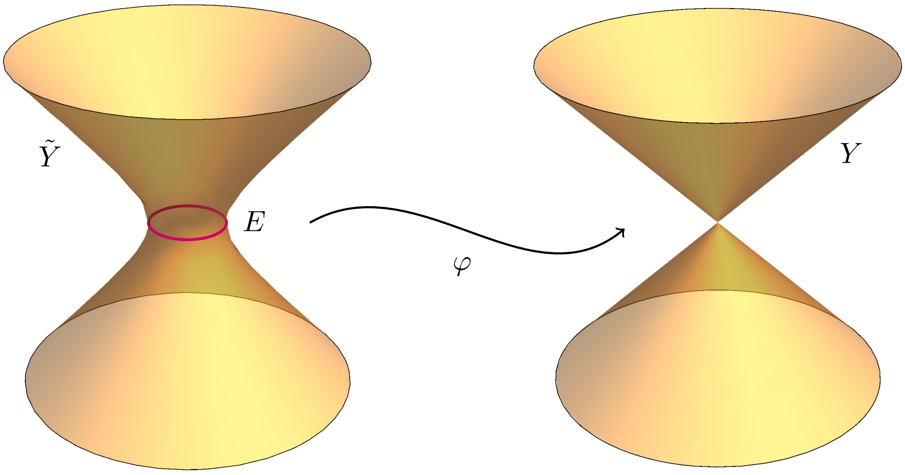


FIGURE 3.63. The blow-up $\tilde{Y}$ of the double cone Y defined by $x^2+y^2-z^2=0$. The exceptional divisor E is shown in red.

equations

$$\begin{aligned} x^2+y^2-z^2 &= 0, \\ xb &= ya, \\ yc &= zb, \\ za &= xc. \end{aligned}$$

Picking $c=1$ for our chart, we may treat a, b as affine coordinates. We then obtain $z^2(a^2+b^2-1)=0$, which has two irreducible components, corresponding to x, y, z all being zero and a, b assuming whatever values they wish—this corresponds to the exceptional divisor of the blow-up of the entirety of $\mathbb{A}^3$—and $a^2+b^2=1$ and $za=x, y=zb$—which gives us $\tilde{Y}$. The exceptional divisor of the blow-up of Y, denote it E, is where these two intersect, at $x, y, z=0$, $a^2+b^2=1$. This means that E is in fact homeomorphic to the unit circle in $\mathbb{A}^2$, and so we may draw this blow-up as a "blown-up double-cone" (see Fig. 3.63).

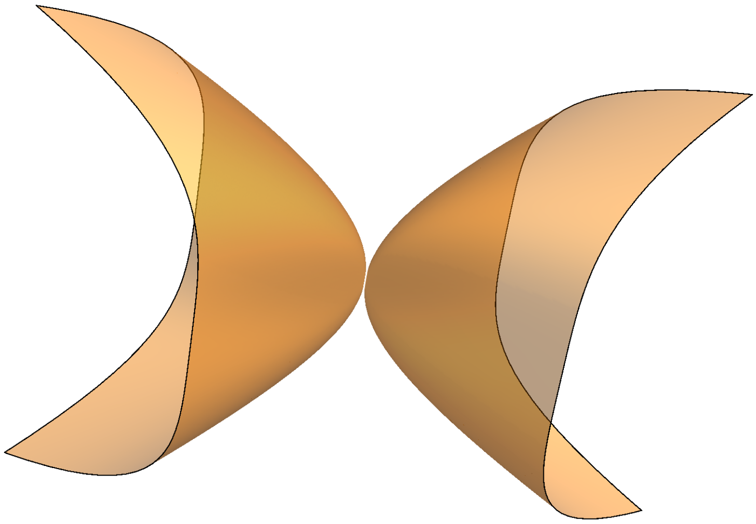


FIGURE 3.65. The variety defined by the polynomial $xy+z^4$, here plotted with the origin at the centre.

EXAMPLE 3.66. To finally give a more interesting example, one which will be of value to our later investigations, we will turn now to the surface $Z(xy+z^4) \subset \mathbb{A}^3$ (see Fig. 3.65), which we will treat in a little more detail than we did the earlier two examples. Of particular interest is going to be the irreducible components of the exceptional divisor. Further, as this example will illustrate, sometimes one blow-up is not enough for the resolution of a singularity.

As before, we start by picking three homogeneous coordinates s_1, s_2, s_3, related to the affine coordinates x, y, z by

$$xs_2 = ys_1, \quad ys_3 = zs_2, \quad zs_1 = xs_3.$$

Let us view the blowup B in each of the three different charts B_1, B_2, B_3, determined by $s_1 = 1, s_2 = 1, s_3 = 1$ respectively, where in each case we may regard the other two homogeneous coordinates as affine. In B_1, we then obtain, by substitution, that $x^2(s_2 + s_3^2x^2)$, with an irreducible component E_1 of the exceptional divisor of the variety being given by $s_2 = 0$, s_3 being free, and $x = 0, y = 0, z = 0$, that is $(x, s_2, s_3) = (0, a, 0)$, where $a \in \mathbb{C}$, or, to express it in fullness, it is given by $(0, 0, 0) \times [1, 0, a]$.

By symmetry of the x, y coordinates, in B_2, we obtain by substitution the condition $y^2(s_1+s_3^2y^2)$, with an irreducible component of the exceptional divisor being given by $(s_1, y, s_3) = (0, 0, a)$, $a \in \mathbb{C}$, or, to express it in all fullness $(0, 0, 0) \times [0, 1, a]$. This is clearly different than E_1, so we call this second irreducible component by E_2.

We now consider the chart B_3, in which $s_3 = 1$. We then obtain $z^2(s_1s_2 + z^2)$, where we find the part of exceptional divisor of the variety to be given by $s_1s_2 = 0$, $(x, y, z) = (0, 0, 0)$. This part then has two irreducible components in turn, being given by $(s_1, s_2, z) = (a, 0, 0)$ and $(s_1, s_2, z) = (0, a, 0)$ respectively. In fullness, we are then looking at $(0, 0, 0) \times [a, 0, 1]$ and $(0, 0, 0) \times [0, a, 1]$, $a \in \mathbb{C}$, which we recognize as E_1 and E_2 respectively, and these two components intersect in at $(0, 0, 0) \times [0, 0, 1]$.

But all is not well in paradise, for by evaluating the Jacobian of B_3, we unravel a new singularity at the origin. This means that we have to perform yet another blowup to get a complete resolution of the singularity, and this we do in the affine coordinates s_1, s_2, z. Picking homogeneous coordinates t_1, t_2, t_3 obeying relations

$$s_1t_2 = s_2t_1, \quad s_2t_3 = zt_2, \quad zt_1 = s_1t_3,$$

we obtain in the chart C_3, in which $t_3 = 1$, the expression $z^4(t_1t_2 + 1)$, from which we obtain a third irreducible component of the irreducible divisor $(t_1, t_2, z) = (a, -1/a, 0)$, or, $(s_1, s_2, z) \times [t_1, t_2, t_3] = (0, 0, 0) \times [a, -1/a, 1]$. Given any curve $(s_1(\lambda), s_2(\lambda), z(\lambda))$ in B_3, it corresponds to a curve $(t_1(\lambda), t_2(\lambda), \xi(\lambda)) = (s_1(\lambda)/z(\lambda), s_2(\lambda)/z(\lambda), z(\lambda))$ in C_3 for which $t_1t_2 + 1 = 0$. It can thus be seen that in the chart C_3, neither E_1 nor E_2 can be seen. Therefore, we consider the charts C_1 and C_2 instead, for which $t_1 = 1$ and $t_2 = 1$ respectively.

In C_1, we obtain $s_1^4t_3^2(t_2 + t_3^2) = 0$, with the irreducible component of the exceptional divisor being given by $(0, -a^2, a)$, or in fullness as $(0, 0, 0) \times [1, -a^2, a]$, $a \in \mathbb{C}$. We find

$$(0, 0, 0) \times [1, -a^2, a] \sim (0, 0, 0) \times [1/a, -a, 1] \sim (0, 0, 0) \times [b, -1/b, 1], \quad b \in \mathbb{C},$$

and so recognize this as being the same as E_3. In this chart, we can in fact see E_1, here being given by $(0, a, 0)$, and we find that it intersects with E_1 at the origin. By symmetry, in the chart B_2, we once again recover E_3, and can now see E_2 and that it too intersects with E_3, again in the origin. All of this is graphed out in the affine charts in Fig. 3.67.

We may schematically draw the irreducible components of the exceptional divisors. Drawing from [27], eeeing each irreducible component is isomorphic to $\mathbb{CP}^1$, we depict them as circles. When two circles touch, that is to indicate an intersection. The result is displayed in Fig. 3.68. As can already be seen, the result is eerily reminiscent of the McKay diagrams from before, something we will revisit in the final chapter.

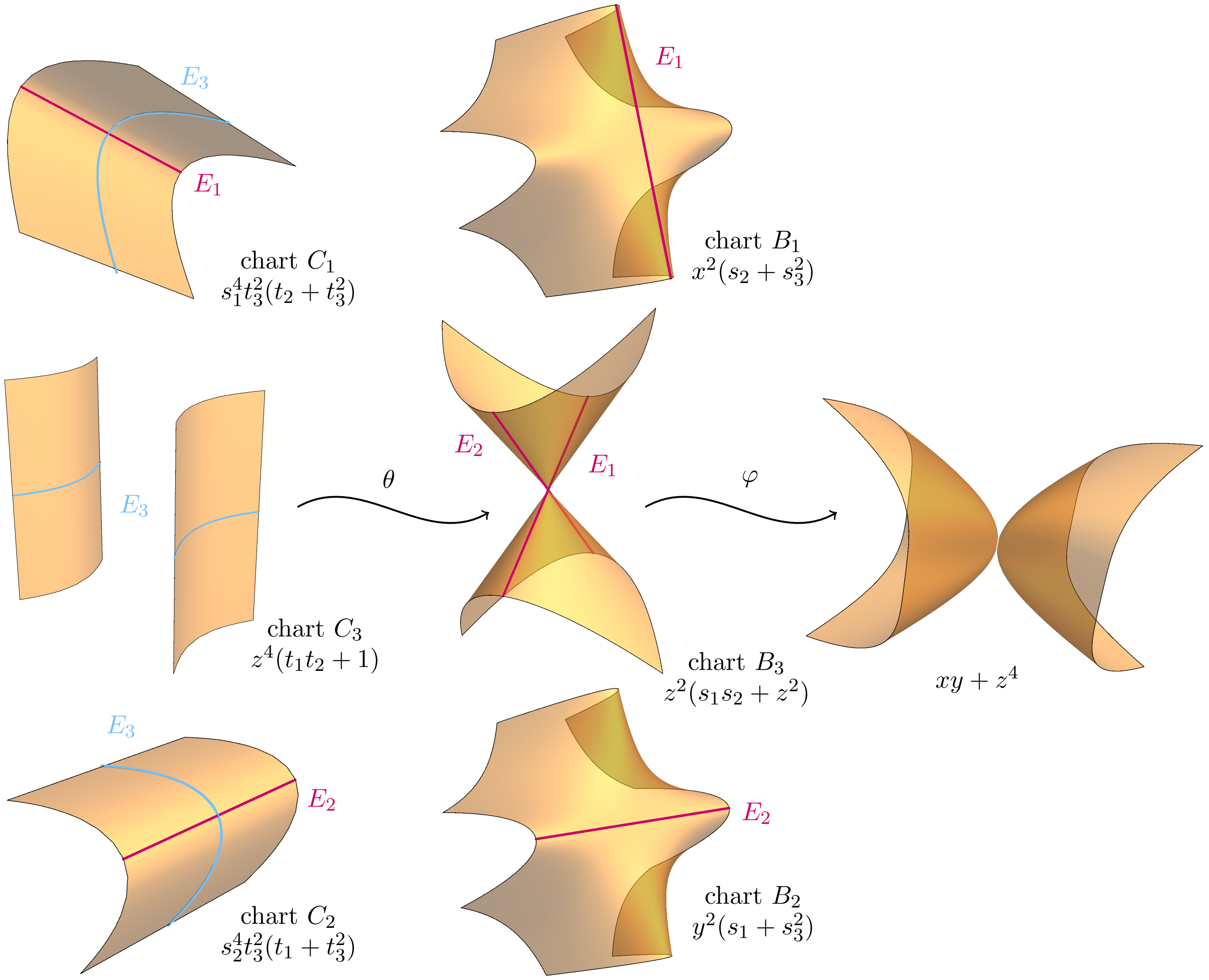


FIGURE 3.67. The blow-up of the affine variety $Z(xy+z^4) \subset \mathbb{A}^3$. Each step of the way, we have drawn graphs in suitable affine charts of the blown-up space to illustrate the intersections of the irreducible components of the exceptional divisor.

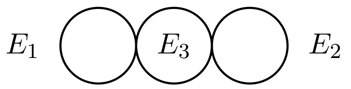


FIGURE 3.68. Schematic of the irreducible components of the exceptional divisor of the blown-up variety $Z(xy+z^4) \subset \mathbb{A}^3$.

CHAPTER 4

Invariant Theory

Given a group G, an n-dimensional vector space V, n being finite, and a group action $G \times V \to V$ on that space, a new action is induced on the set of functions on V, $\mathcal{F}[V]$, as $G \times \mathcal{F}[V] \to \mathcal{F}[V]$, $g \cdot f(\vec{v}) = f(g^{-1} \cdot \vec{v})$. In particular, if V is a G-module, and if we restrict outselves to considering polynomials on V, the group action induces automorphisms on the polynomial ring $\mathbb{F}[z_1, \ldots, z_n]$ by

$$\sigma_g : \mathbb{F}[z_1, \ldots, z_n] \to \mathbb{F}[z_1, \ldots, z_n]; \quad f(z_1, \ldots, z_n) \mapsto f(g^{-1} \cdot z_1, \ldots, g^{-1} \cdot z_n).$$

With automorphisms induced for each and every element in the group, the fundamental problem of classical invariant theory is to find the subring of polynomials that are invariant under the action of the entire group, denoted $\mathbb{F}[z_1, \ldots, z_n]^G$.

While this task is of course an interesting and worthwhile endeavour in its own right, for our purposes it becomes relevant in that we want to give an algebraic description of the orbit spaces $\mathbb{C}^2/G$, where G are the finite subgroups of $\mathrm{SU}(2)$ acting on $\mathbb{C}^2$ as per the natural representations. Before we can show how the ring of invariant polynomials allows us to do this, however, we need to establish a few foundational results of invariant theory, which is the topic of the following chapter.

1. The Problem of Finite Generation

The task of cataloging the set of invariant polynomials on a given space under the action of a group is made significantly easier if the ring which these polynomials form is finitely generated. Let us illustrate this with a classical example [28].

Example 4.1. (Symmetric polynomials.) A friendly group action on a vector space is given by how the symmetric group S_n acts on $\mathbb{C}^n$ in the natural representation. Given a basis of $\mathbb{C}^n$, the action of elements of S_n is to permute the basis vectors, and so in the induced action on $\mathbb{C}[z_1, \ldots, z_n]$, the action translates into the permutation of the variables $\{z_i\}$. For example,

$$(1\ 2\ 4) \cdot (z_1 + z_2 z_3 + z_4^2 z_1) = z_2 + z_4 z_3 + z_1^2 z_2.$$

It does not take the reader long to realize that the only polynomials in $\mathbb{C}[z_1, \ldots, z_n]$ that are invariant under this action of S_n are those that are symmetric in all its variables $\{z_i\}$. Basic examples are those provided by the k^{th} *elementary symmetric polynomials*, which are those of the form $s_k := \sum_{i_1 < \cdots < i_k} z_{i_1} \ldots z_{i_k}$, those are

$$\begin{aligned} s_1 &= z_1 + z_2 + \cdots + z_n, \\ s_2 &= z_1 z_2 + z_1 z_3 + \cdots + z_1 z_n + z_2 z_3 + \cdots + z_{n-1} z_n, \\ &\vdots \\ s_n &= z_1 \ldots z_n. \end{aligned}$$

We claim that all symmetric polynomials $\mathbb{C}[z_1, \ldots, z_n]^{S_n}$ are generated by the k^{th} elementary symmetric polynomials. To prove it, we first define the *leading monomial* of any polynomial p to be term $c z_1^{\alpha} \ldots z_n^{\alpha_n}$, $c \in \mathbb{C}$ of it such that the tuple $(\alpha_1, \ldots, \alpha_n)$ is lexicographically larger than all other analogous tuples associated with all other terms of p.

Given any $f \in \mathbb{C}[z_1, \ldots, z_n]^{S_n}$, we have that its leading monomial $cz_1^{\alpha} \ldots z_n^{\alpha_n}$ is such that $\alpha_1 \geq \cdots \geq \alpha_n$, as otherwise a permutation of the variables $\{z_i\}$ would result in a monomial with strictly larger lexicographical order, meaning that either $cz_1^{\alpha} \ldots z_n^{\alpha_n}$ is in fact not the leading monomial of f, or $f \notin \mathbb{C}[z_1, \ldots, z_n]^{S_n}$. In either eventuality, we would have a contradiction.

Let us then look at the polynomial $g := cs_n^{\alpha_n} s_{n-1}^{\alpha_{n-1}-\alpha_n} \ldots s_2^{\alpha_2-\alpha_3} s_1^{\alpha_1-\alpha_2}$. Its leading monomial is equal to that of f. Since the difference of two symmetric polynomials is a symmetric polynomial, $f' := f - g$ is a symmetric polynomial of leading coefficient that is lexicographically strictly smaller than that of f. We may continue algorithmically to repeat this procedure, but seeing that it is impossible to construct an infinite lexicographically strictly decreasing chain of monomials, we will eventually reach a step where the difference is a constant term. Thus it follows that f is a polynomial in the $\{s_i\}$, and seeing that the choice of $f \in \mathbb{C}[z_1, \ldots, z_n]^{S_n}$ was arbitrary, the symmetric polynomials are indeed generated by the k^{th} elementary symmetric polynomials.

As the reader may have noted above, the k^{th} elementary symmetric polynomials are all homogeneous polynomials. This does in fact set up a regular pattern, as polynomial ring morphisms are all induced by the group action on the underlying vector space in its capacity as a group module, they will always be such that they transform the variables $\{z_i\}$ *linearly*,

$$z_i \mapsto \sum_{j=1}^{n} a_j z_j, \quad a_j \in \mathbb{F}.$$

Consequently a monomial of order m entering into a polynomial will always, under the group action, be rendered into a sum of monomials of order m. From this it follows that every invariant polynomial will always be expressible as a sum of invariant homogeneous polynomials, and so we may focus on them exclusively, thereby simplifying the task before us.

When first charting the waters of invariant theory at the turn of the twentieth century, mathematicians found that finite groups did not satisfy their appetites, but gave themselves the far more Sisyphean task of looking at polynomials invariant under the much broader class of *algebraic groups*. What Hilbert and his contemporaries conjectured was that all such rings of invariant polynomials were indeed finitely generated, and Hilbert considered the need to formulate a formal proof of this proposition to be of such paramount importance that he included it as number fourteen on his famous list of twenty-four problems [29]. Unfortunately for him, the question was settled conclusively and rather anticlimactically in 1958 when Japanese algebraist Nagata Masayoshi devised a counter-example, demonstrating that the conjecture was in fact wrong [30].

As disheartening as this result might well be, all is not lost, for in his own day, Hilbert had a lot more success with a special case of his fourteenth problem. Specifically, when he restricted himself to the polynomials in two variables being acted upon by elements of the special linear group of dimension two, Hilbert was able to prove that the ring of invariant polynomials was indeed finitely generated. This more than well covers all the rings we have to concern ourselves with, and seeing that his proof if not just supremely witty, but also provides a good opening of an introduction to classical invariant theory, we shall furnish a recount of it here.

Prior to Hilbert, invariant theory had been ruled supremely by Paul Gordan, as evangelical a believer in constructive mathematics as they came, and his approach, and the approach of all his disciples, had been to try to devise algorithms for constructing the generators in the case of each and every group [29]. It goes without saying that constructing a generalized algorithm was quite a task.

Hilbert took an entirely different approach [31]. His first ingredient was the basis theorem, which we have already treated in detail in our chapter on algebraic geometry (see Thm. 3.11). His second ingredient was the so-called Reynolds operator, which maps elements of $\mathbb{F}[x_1, \dots, x_n]$ to elements of $\mathbb{F}[x_1, \dots, x_n]^G$. For continuous groups, the Reynolds operator can be a bit of a problem, nonetheless, for finite groups, it has a very neat definition.

Definition 4.2. (Reynolds operator for finite groups.) Let $\mathbb{F}$ be a field of characteristic zero, and let G be a finite group. Then the *Reynolds operator* $\phi : \mathbb{F}[x_1, \dots, x_n] \to \mathbb{F}[x_1, \dots, x_n]^G$ is defined as

$$\phi(f) := \frac{1}{|G|} \sum_{g \in G} g \cdot f.$$

It is easy to see that if $f \in \mathbb{F}[x_1, \dots, x_n]^G$, then $\phi(f) = f$, and that if f, g are any polynomials in $\mathbb{F}[x_1, \dots, x_n]$, then $\phi(f + g) = \phi(f) + \phi(g)$. Finally, and this is important, the Reynolds operator preserves degree.

Now then comes Hilbert's famous finiteness theorem, which, being an existence theorem, caused quite some furore in its day. Tradition has it that Paul Gordan at first exclaimed, "This is not mathematics, it is theology!" but at heart a man who valued mathematical truth more than he valued his own pride, a little later, he graciously admitted that "I have convinced myself that even theology has its advantage" [32]. Without further ado, here is the proof.

Theorem 4.3. (Hilbert's finiteness theorem.) Let G be a finite group acting on a ring of polynomials $\mathbb{F}[x_1, \dots, x_n]$. Then the ring of invariant polynomials $\mathbb{F}[x_1, \dots, x_n]^G$ is finitely generated.

Proof. Let I be the ideal of $\mathbb{F}[x_1, \dots, x_n]$ generated by all homogeneous elements of $\mathbb{F}[x_1, \dots, x_n]^G$ of degree greater than zero. Since $\mathbb{F}$ is Noetherian, $\mathbb{F}[x_1, \dots, x_n]$ is also Noetherian (by Thm. 3.11), and so all ideals contained therein are finitely generated, and in particular I. Since each homogeneous part of a polynomial in I must also belong to I, we note that the generators must themselves be homogeneous and that they must also be invariants. Thus we have a finite set $\{f_1, \dots, f_k\}$ of invariant homogeneous generators of I. We now prove that $\mathbb{F}[x_1, \dots, x_n]^G = \mathbb{F}[f_1, \dots, f_k]$. Since each generator is invariant, it is clear that $\mathbb{F}[f_1, \dots, f_k] \subseteq \mathbb{F}[x_1, \dots, x_n]^G$. We prove that $\mathbb{F}[x_1, \dots, x_n]^G \subseteq \mathbb{F}[f_1, \dots, f_k]$ by induction. Let f be a homogeneous invariant polynomial of degree d. If $d = 0$, then $f \in \mathbb{F}[f_1, \dots, f_k]$ trivially. Now assume that all invariant homogeneous polynomials of degree $d < \ell$ are in $\mathbb{F}[f_1, \dots, f_k]$. Assume then that f is an invariant homogeneous polynomial of degree $d = \ell$. Then, it is expressible as

$$f = \sum_{i=1}^{k} g_i f_i$$

for some $g_i \in \mathbb{F}[x_1, \dots, x_n]$. Since $f \in \mathbb{F}[x_1, \dots, x_n]^G$, applying the Reynolds operator yields

$$f = \phi(f) = \sum_{i=1}^{k} \phi(g_i f_i) = \sum_{i=1}^{k} \phi(g_i) f_i.$$

Since every $\phi(g_i) \in \mathbb{F}[x_1, \dots, x_n]^G$ and since $\deg(g_i) < \deg(f)$, by the induction hypothesis, $\phi(g_i) \in \mathbb{F}[f_1, \dots, f_k]$ for every i. Thus $f \in \mathbb{F}[f_1, \dots, f_k]$. Since every polynomial in $\mathbb{F}[x_1, \dots, x_n]^G$ is expressible in terms of homogeneous invariants, the theorem is proven. □

Having established the finite generation of the ring of invariants, we now explain how this is of interest to us in studying orbifolds from an algebro-geometric point of view.

Definition 4.4. (The quotient map [28].) Let G be a finite group and let W be a finite-dimensional G-module. By Hilbert's finiteness theorem, the ring $\mathbb{C}[W]^G$ is then finitely generated by some set of polynomials $\{f_1, \dots, f_k\}$. The *quotient map* is then defined as the map of spaces

$$\pi : \ W \to \mathbb{C}^k, \quad w \mapsto (f_1(w), \dots, f_k(w)).$$

The image of this map will then be the set of points in $\mathbb{C}^k$ which satisfy the relations of the generators $\{f_1, \dots, f_k\}$. Specifically, if they satisfy the relations $\{h_i(f_1, \dots, f_k) = 0\}$, then $\operatorname{im} \pi = \{(x_1, \dots, x_k) | h_i(x_1, \dots, x_k) = 0\}$. Furthermore, we observe that the pre-image of any point in $\operatorname{im} \pi$ is an orbit of G in W, making the induced map

$$\tilde{\pi} : \ W/G \to \operatorname{im}(\pi), \quad \overline{w} \mapsto (f_1(w), \dots, f_k(w))$$

a homeomorphism. Consequently, *we may realize orbifolds as algebraic sets.* This then justifies our search for the generators of the rings of invariants, and the algebraic relations between them.

2. Down to the Basics: *Grundformen*

The following section draws heavily on Felix Klein's classic work *Lectures on the Icosahedron* [33], which in recent times has been elaborated upon by Igor Dolgachev in his book on the McKay correspondence [34].

Lemma 4.5. Any finite subgroup of $\mathrm{SL}_2(\mathbb{C})$ is isomorphic to a finite subgroup of $\mathrm{SU}(2)$.

Proof. $\mathrm{SL}_2(\mathbb{C})$ consists of all special linear matrices over the complex numbers of dimension two, and $\mathrm{SU}(2)$ is a subgroup of this, with the additional restraint that the matrices must also be unitary. The proof consists of showing that given a finite subgroup $G < \mathrm{SL}_2(\mathbb{C})$, we can always perform a change of basis to render all matrices making up G unitary.

G consists of 2×2-matrices $\mathbf{A}_i$. A hermitian matrix is a matrix $\mathbf{M}$ such that $\mathbf{M}^\dagger = \mathbf{M}$. Self-evidently then, $\mathbf{A}_i\mathbf{A}_i^\dagger$ is hermitian for all $1 \leq i \leq |G|$, and by extension

$$\mathbf{H} := \sum_{i=1}^{|G|} \mathbf{A}_i\mathbf{A}_i^\dagger$$

is a hermitian matrix. We recall from linear algebra that any hermitian matrix may be diagonalized by a change of basis by unitary matrices with the eigenvalues of the matrix being the diagonal entires. Thus,

$$\mathbf{d} = \mathbf{U}^{-1}\mathbf{H}\mathbf{U} = \sum_{i=1}^{|G|} \mathbf{U}^{-1}\mathbf{A}_i\mathbf{A}_i^\dagger\mathbf{U} = \sum_{i=1}^{|G|} \mathbf{U}^{-1}\mathbf{A}_i\mathbf{U}\mathbf{U}^{-1}\mathbf{A}_i^\dagger\mathbf{U} = \sum_{i=1}^{|G|} \mathbf{A'}_i\mathbf{A'}_i^\dagger,$$

for some unitary matrix $\mathbf{U}$ and $\mathbf{A'}_i := \mathbf{U}^{-1}\mathbf{A}_i\mathbf{U}$. While it is known from linear algebra that the eigenvalues of a hermitian matrix are by necessity real, here we can say more. Consider a generic diagonal entry $[\mathbf{d}]_{jj}$,

$$[\mathbf{d}]_{jj} = \sum_{k=1}^{2}\sum_{i=1}^{|G|}[\mathbf{A'}_i]_{jk}[\mathbf{A'}_i^\dagger]_{kj} = \sum_{i=1}^{|G|}\sum_{k=1}^{2}[\mathbf{A'}_i]_{jk}[\mathbf{A'}_i]_{jk}^* = \sum_{i=1}^{|G|}\sum_{k=1}^{2}|[\mathbf{A'}_i]_{jk}|^2 \geq 0,$$

where we may in fact dismiss the equality as an impossibility, as it would imply that the matrices $\mathbf{A'}_i$ have determinant zero, meaning $\mathbf{A}_i$ could not be special linear. Since $\mathbf{d}$ then only has positive real diagonal entires, $\mathbf{d}^{\frac{1}{2}}$ and $\mathbf{d}^{-\frac{1}{2}}$ are well-defined and diagonal too, giving us

$$\mathbf{d} = \mathbf{d}^{\frac{1}{2}}\mathbf{d}^{\frac{1}{2}} = \sum_{i=1}^{|G|} \mathbf{A}'_i \mathbf{A}'^{\dagger}_i \qquad \Leftrightarrow \qquad \mathbb{1} = \mathbf{d}^{-\frac{1}{2}} \sum_{i=1}^{|G|} \mathbf{A}'_i \mathbf{A}'^{\dagger}_i \mathbf{d}^{-\frac{1}{2}}.$$

Then defining a new set of matrices by the change of basis $\mathbf{A}''_i := \mathbf{d}^{-\frac{1}{2}}\mathbf{A}'_i\mathbf{d}^{\frac{1}{2}}$, we find the $\{\mathbf{A}''_i\}$ all to be unitary.

$$\begin{aligned}\mathbf{A}''_j\mathbf{A}''^{\dagger}_j &= \mathbf{d}^{-\frac{1}{2}}\mathbf{A}'_j\mathbf{d}^{\frac{1}{2}}\left[\mathbf{d}^{-\frac{1}{2}}\sum_{i=1}^{|G|}\mathbf{A}'_i\mathbf{A}'^{\dagger}_i\mathbf{d}^{-\frac{1}{2}}\right]\mathbf{d}^{\frac{1}{2}}\mathbf{A}'^{\dagger}_j\mathbf{d}^{-\frac{1}{2}} \\ &= \mathbf{d}^{-\frac{1}{2}}\sum_{i=1}^{|G|}\mathbf{A}'_j\mathbf{A}'_i\mathbf{A}'^{\dagger}_i\mathbf{A}'^{\dagger}_j\mathbf{d}^{-\frac{1}{2}} \\ &= \mathbf{d}^{-\frac{1}{2}}\sum_{i=1}^{|G|}\mathbf{A}'_j\mathbf{A}'_i(\mathbf{A}'_j\mathbf{A}'_i)^{\dagger}\mathbf{d}^{-\frac{1}{2}} \\ &= \mathbf{d}^{-\frac{1}{2}}\sum_{i=1}^{|G|}\mathbf{A}'_k\mathbf{A}'^{\dagger}_k\mathbf{d}^{-\frac{1}{2}} = \mathbb{1}.\end{aligned}$$

Thus the change of basis incurred by $\mathbf{A}_i \mapsto \mathbf{d}^{-\frac{1}{2}}\mathbf{U}^{-1}\mathbf{A}_i\mathbf{U}\mathbf{d}^{\frac{1}{2}}$ does indeed isomorphically map any subgroup of $\mathrm{SL}_2(\mathbb{C})$ to one of $\mathrm{SU}(2)$. □

The lemma and proof above are taken from [17], supplemented by [35], where it is presented in a slightly more general form, and where it forms a key step in the physicist's proof of the grand orthogonality theorem mentioned in Chap. 2. An immediate consequence of this lemma is that it is equivalent to talk about irreducible representations of finite subgroups of SU(2) and finite subgroups of $\mathrm{SL}_2(\mathbb{C})$, and as we shall now see, for the rest of this chapter it is more profitable to regard our problem from the latter point of view.

Let $\mathbb{C}^2$ be a natural G-module for some finite subgroup $G < \mathrm{SL}_2(\mathbb{C})$, and let F be a homogeneous polynomial in two variables. F then defines a projective variety, which is a set of points in $\mathbb{CP}^1$. Writing $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$, the elements of $\mathbb{CP}^1$ are equivalence classes of the form

$$[z] = \{\lambda z \in \mathbb{C}^2\backslash\{0\} | \lambda \in \mathbb{C}^*\},$$

and the action of the special linear group on $\mathbb{C}^2$ induces an action of $\mathbb{CP}^1$ by $g \cdot [z] = [g \cdot z]$. Since $g \cdot \lambda z = \lambda(g \cdot z)$ for all $\lambda \in \mathbb{C}^*$, $g \in G$, the action is not dependent on choice of representative and is as such well-defined. If we let K be the kernel of the special linear group's action on $\mathbb{CP}^1$ (a set which contains only the elements $\mathbb{1}$ and $-\mathbb{1}$), we may equivalently regard the action as one of the group $\mathrm{PSL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})/K$ on $\mathbb{CP}^1$, where denoting $\overline{g}$ as the equivalency class in $\mathrm{PSL}_2(\mathbb{C})$ to which g belongs, $\overline{g} \cdot [z] = g \cdot [z]$. $\mathrm{PSL}_2(\mathbb{C})$ is called the *projective special linear group* over the complex numbers of degree 2, and it is natural to look at the action on $\mathbb{CP}^1$ through this lense. As such, we shall study the action of the finite subgroups of $\mathrm{PSL}_2(\mathbb{C})$ to which the finite subgroups of $\mathrm{SL}_2(\mathbb{C})$ correspond.

In Chap. 1, however, we noted that the kernel of the canonical morphism $\varphi : \mathrm{SU}(2) \to \mathrm{SO}(3)$ was just $\{\pm\mathbb{1}\}$, and so this fact, taken in conjunction with that every finite subgroup of $\mathrm{SL}_2(\mathbb{C})$ is isomorphic to a finite subgroup of SU(2), that the kernel of the projection morphism $\mathrm{SL}_2(\mathbb{C}) \to \mathrm{PSL}_2(\mathbb{C})$ is also $\{\pm\mathbb{1}\}$, and Noether's first isomorphism theorem, allows us to deduce that the finite subgroups of $\mathrm{PSL}_2(\mathbb{C})$ are isomorphic to the finite subgroups of SO(3). This then means that the finite subgroups of $\mathrm{PSL}_2(\mathbb{C})$ are our old friends, the rotational symmetry groups of the Platonic solids! It goes without saying that this comes in quite handy. Denoting the finite subgroups of $\mathrm{PSL}_2(\mathbb{C})$ by $\overline{G}$ and their elements by $\overline{g}$, we continue.

Since

$$\begin{aligned} z \in \overline{g} \cdot Z(F) \quad &\Leftrightarrow \quad \overline{g}^{-1} \cdot z \in Z(F) \quad \Leftrightarrow \quad F[\overline{g}^{-1} \cdot z] = 0 \\ &\Leftrightarrow \quad (\overline{g} \cdot F)[z] = 0 \quad \Leftrightarrow \quad z \in Z(\overline{g} \cdot F), \end{aligned}$$

we have that

$$\overline{g} \cdot Z(F) = Z(\overline{g} \cdot F). \tag{4.6}$$

Definition 4.7. (Relative invariant.) A homogeneous polynomial F is called a *relative invariant* of $\overline{G}$ if for every $\overline{g} \in \overline{G}$,

$$\overline{g} \cdot Z(F) = Z(F).$$

Two homogeneous polynomials $F, H \in \mathbb{C}[t_0, t_1]$ only define the same variety in $\mathbb{CP}^1$ if they differ by a multiplicative factor, and so from (4.6), it follows that F is a relative invariant if and only if for every $g \in G$, $g \cdot F = a_g F$ for some $a_g \in \mathbb{C}^*$. The set $R = \{f \in \mathbb{C}[t_0, t_1] | g \cdot f = a_g f, \ \forall g \in G\}$ (containing not just homogeneous polynomials) form a one-dimensional module of G under the group action $G \times R \to R$, $(g, f) \mapsto a_g f$. As a representation, we have the group element g corresponding to the matrix $[a_g]$. This justifies the following naming convention:

Definition 4.8. (Character of a relative invariant.) Let the homogeneous polynomial F be a relative invariant of the group G. The group morphism $\chi : G \to \mathbb{C}^*$, $g \mapsto a_g$ is then called the *character of F*.

In our case, since $\overline{G}$ is a finite group, for every $\overline{g}$ there exists $n \in \mathbb{N}$ such that $\overline{g}^n = e$, and so we may conclude that the characters may only ever yield roots of unity.

Seeing that the absolute invariants form a subset of the relative invariants, if we can find the general form of the relative invariants, then we may narrow it down to find the general form of the absolute invariants, and from that, we may find the finite generators.

Given any relative invariant F, if $[z] \in Z(F)$, then $\overline{g}^{-1} \cdot [z] \in Z(F)$ too for every $\overline{g} \in \overline{G}$. From this it follows that the entire $\overline{G}$-orbit to which $[z]$ belongs must lie in $Z(F)$, and so we deduce that $Z(F)$ must be a union of $\overline{G}$-orbits in $\mathbb{CP}^1$. Specifically, given two relative invariants F, H, we have $Z(FH) = Z(F) \cup Z(H)$.

Lemma 4.9. Every homogeneous polynomial f of degree n in two variables x, y may be uniquely factorized as

$$f(x, y) = (a_1 x - b_1 y)(a_2 x - b_2 y) \dots (a_n x - b_n y),$$

where the $\{[b_i, a_i]\}$ are the set of zeroes of f in $\mathbb{CP}^1$.

Proof. Since f is homogeneous, we may write $f(x, y) = y^n f(\frac{x}{y}, 1)$. $f(s, 1)$ is a polynomial in one variable of degree n, and so by the fundamental theorem of algebra, we can factorize it uniquely as

$$f(s, 1) = (a_1 s - b_1)(a_2 s - b_2) \dots (a_n s - b_n).$$

Set $s = \frac{x}{y}$ and multiply by y^n. We then obtain

$$f(x, y) = (a_1 x - b_1 y)(a_2 x - b_2 y) \dots (a_n x - b_n y).$$

Clearly every $[b_i, a_i]$ is a solution to $f(x, y) = 0$. Further, since $\mathbb{C}$ lacks zero divisors, if $f(b_i, a_i) = 0$, then there must exist a factor that is a multiple of $(a_i x - b_i y)$ for the polynomial to evaluate as zero. The lemma follows. □

Consequently, we may surmise that all relative invariants may be factorized uniquely into homogeneous polynomials of minimal degree corresponding to the specific orbits. This prompts the following definition.

Definition 4.10. (Grundformen, General and Special.) A *Grundform* (plural *Grundformen*) is a relative invariant of minimal degree whose set of zeroes correspond to a single orbit. If the orbit is non-exceptional (its stabilizer is trivial), we say that it is a *general Grundform.* If the orbit is exceptional (its stabilizer is non-trivial), we say that it is a *special Grundform.*[1]

It is clear then from Lem. 4.9 that a general Grundform must be of degree $|\overline{G}|$ and a special Grundform must be of degree $|\overline{G}|/e_i$, where e_i is the cardinality of the stabilizer of the orbit in question. At first glance, this does not seem to help us much in finding the general form of the relative invariants, since it would take forever to list the general Grundformen. Simply pick any point you like in $\mathbb{CP}^1$ that is not in an exceptional orbit, operate on it with all the elements of $\overline{G}$, and construct the corresponding homogeneous polynomial using Lem. 4.9. However, Klein [33] noticed something truly important that Dolgachev [34] distilled in form of the following lemma.

Lemma 4.11. (Klein, Dolgachev.) If there exist distinct special Grundformen F_1 and F_2 corresponding to exceptional orbits of cardinalities $|\overline{G}|/e_1$ and $|\overline{G}|/e_2$ respectively and their characters χ_1 and χ_2 obey the relationship

$$\chi_1^{e_1} = \chi_2^{e_2},$$

then every general Grundform may be expressed as a linear combination of $F_1^{e_1}$ and $F_2^{e_2}$.

Proof. Let F be an arbitrary general Grundform corresponding to an exceptional orbit $\mathcal{O}$, and let $\Phi = aF_1^{e_1} + bF_2^{e_2}$. Since $\chi_1^{e_1} = \chi_2^{e_2}$, $g \cdot \Phi = a(g \cdot F_1)^{e_1} + b(g \cdot F_2)^{e_2} = a\chi_1^{e_1}F_1^{e_1} + b\chi_2^{e_2}F_2^{e_2} = \chi_1^{e_1}(aF_1^{e_1} + bF_2^{e_2}) = \chi_1^{e_1}\Phi$, confirming Φ to be a relative invariant. It is furthermore of order $|\overline{G}|$, making it a Grundform. Let now (x, y) be a point in the orbit $\mathcal{O}$. Any relative invariant of order $|\overline{G}|$ which is zero at (x, y) must then be a scalar multiple of F, since all its other zeroes too must lie in $\mathcal{O}$. Though neither F_1 nor F_2 may be zero at (x, y) since $\mathcal{O}$ is non-exceptional, we can always choose a, b such that the linear combination Φ is zero at (x, y), specifically, let simply $b = -aF_1(x, y)/F_2(x, y)$. Then Φ is simply a scalar multiple of F, and the lemma follows. □

If we can prove that special Grundformen of that property exist for every finite subgroup of $\mathrm{PSL}_2(\mathbb{C})$, then all we need to do is to find the special Grundformen, and from them we may write down the form of a general relative invariant. This must be done for each and every case, and can be quite tedious. Dolgachev does present all the computations in [34], but we will satisfy ourselves with a single example.

Example 4.12. Let $G = \mathbb{BO}$, so that $\overline{G} = \mathbb{O}$. As stated earlier in Chap. 2, in the natural representation, the binary octahedral group may be expressed as being generated by

$$\varrho(a) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix}, \qquad \text{and} \qquad \varrho(b) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}.$$

To find the exceptional orbits, we start by searching for the fixed points of each $\overline{g} \in \mathbb{G}$, that is, the points of $\mathbb{CP}^1$ that are invariant under the action of $\overline{g}$. These points then belong to orbits whose stabilizer includes $\overline{g}$ and thus are exceptional. By then operating on those points with all other elements of $\overline{G}$, we obtain the full orbits. Seeing that $\overline{g} \cdot p = [g \cdot p]$, and two non-zero points $p, q \in \mathbb{C}^2$ correspond to the same point in $\mathbb{CP}^1$ if $p = \lambda q$ for some non-zero $\lambda \in \mathbb{C}^*$, the task of finding the fixed points of $\overline{g}$ amounts to finding the eigenvectors of the matrix $\varrho(g)$.

With this in mind, we may start by considering the fixed points of $\overline{a}$, which turn out to be $[1, 0]$ and $[0, 1]$. Operating on these points by the other elements of $\overline{G}$, we find that they belong to

[1] These definitions of *Grundformen* are taken from Felix Klein's *Lectures on the Icosahedron.* It is worth to point out that they are at odds with the traditional definition of a *Grundform*, which is an element of a minimal set of generators of the rings of invariants [29]. This motivates the German name *Grundformen*, which in English may be rendered as *base-forms* or *ground-forms.*

the same orbit, which also includes the points $[1,1]$, $[-1,1]$, $[i,1]$, and $[-i,1]$. Thus we have an orbit of cardinality 6 and stabilizer of cardinality 4, and the special Grundform corresponding to this orbit is

$$\begin{aligned}\Psi_1 &= t_0t_1(t_0+t_1)(t_0-t_1)(t_0+it_1)(t_0-it_1)\\ &= t_0t_1(t_0^4-t_1^4).\end{aligned}$$

Next, we may consider the element $\overline{ab}$, whose fixed points are $[1+\sqrt{3},1-i]$ and $[1+\sqrt{3},-1+i]$. Operating on these with the other elements of $\overline{G}$, we obtain $[1+\sqrt{3},1+i]$, $[1+\sqrt{3},-1-i]$, $[1+i,1+\sqrt{3}]$, $[1-i,1+\sqrt{3}]$, $[-1+i,1+\sqrt{3}]$, and $[-1-i,1+\sqrt{3}]$. Thus we have an orbit of cardinality 8 and stabilizer of cardinality 3, and the corresponding special Grundform is

$$\Psi_2 = (t_0^4+2\sqrt{3}i\ t_0^2t_1^2+t_1^4)(t_0^4-2\sqrt{3}i\ t_0^2t_1^2+t_1^4).$$

Finally, we consider the element $\overline{abb}$, whose fixed points are $[1+i,\sqrt{2}]$ and $[-1-i,\sqrt{2}]$. The other points in the orbit are $[1-i,\sqrt{2}]$, $[-1+i,\sqrt{2}]$, $[1+\sqrt{2},1]$, $[1-\sqrt{2},1]$, $[-1+\sqrt{2},1]$, $[-1-\sqrt{2},1]$, $[1+\sqrt{2},i]$, $[1-\sqrt{2},i]$, $[-1+\sqrt{2},i]$, and $[-1-\sqrt{2},i]$. Thus we have an orbit of cardinality 12, stabilizer of cardinality 2, and a corresponding Grundform of

$$\begin{aligned}\Psi_3 &= (t_0^4+t_1^4)(t_0^4-6t_0^2t_1^2+t_1^4)(t_0^4+6t_0^2t_1^2+t_1^4)\\ &= (t_0^4+t_1^4)((t_0^4+t_1^4)^2-36t_0^4t_1^4).\end{aligned}$$

All fixed points of all elements then being accounted for, we have by exhaustion found all exceptional orbits of $\overline{G}$ and their corresponding special Grundformen. We find

$$\begin{aligned}\chi_1(a)&=-1, &\chi_2(a)&=1, &\chi_3(a)&=-1,\\ \chi_1(b)&=-1, &\chi_2(b)&=1, &\chi_3(b)&=-1,\end{aligned}$$

from which it follows that $\chi_1^4=\chi_2^3=\chi_3^2$, and so every general Grundform may be expressed in terms of the special Grundformen.

Subgroup of $\mathrm{PSL}_2(\mathbb{C})$	Special *Grundformen*	Order of stabilizer
C_n/K	$\Psi_1=t_0$ $\Psi_2=t_1$	n if n is odd, $n/2$ if n is even
D_n	$\Psi_1=t_0^2+t_1^2$ $\Psi_2=t_0^2-t_1^2$ $\Psi_3=t_0t_1$	2 2 n
$\mathbb{T}$	$\Psi_1=t_0t_1(t_0^4-t_1^4)$ $\Psi_2=t_0^4+2\sqrt{3}i\ t_0^2t_1^2+t_1^4$ $\Psi_3=t_0^4-2\sqrt{3}i\ t_0^2t_1^2+t_1^4$	2 3 3
$\mathbb{O}$	$\Psi_1=t_0t_1(t_0^4-t_1^4)$ $\Psi_2=t_0^8+14t_0^4t_1^4+t_1^8$ $\Psi_3=(t_0^4+t_1^4)((t_0^4+t_1^4)^2-36t_0^4t_1^4)$	4 3 2
$\mathbb{D}$	$\Psi_1=t_0^{30}+t_1^{30}+522(t_0^{25}t_1^5-t_0^5t_1^{25})-10005(t_0^{20}t_1^{10}+t_0^{10}t_1^{20})$ $\Psi_2=-(t_0^{20}+t_1^{20})+228(t_0^{15}t_1^5-t_0^5t_1^{15})-494t_0^{10}t_1^{10}$ $\Psi_3=t_0t_1(t_0^{10}+11t_0^5t_1^5-t_1^{10})$	2 3 5

TABLE 4.13. The sets of *Grundformen* for the relative invariants of each $\overline{G}\subset\mathrm{PSL}_2(\mathbb{C})$.

The full set of special Grundformen for each $\overline{G}$ is given in Tab. 4.13, and by exhaustion, it is obtained that for each of them $\chi_1^{e1} = \chi_2^{e2} = \chi_3^{e3}$. Therefore, any relative invariant must be of the form

$$\Psi_1^\alpha \Psi_2^\beta \Psi_3^\gamma \prod_i (a_i \Psi_1^{e1} + b_i \Psi_2^{e2}), \tag{4.14}$$

for some $\alpha, \beta, \gamma \in \mathbb{N}$ and $a_i, b_i \in \mathbb{C}$. (With the minor exception of the cyclical group, which only admits two special Grundformen, but still exhibits $\chi_1^{e1} = \chi_2^{e2}$, and so the analogue of (4.14) is obtained by simply discarding the factor of Ψ_3^γ.) Since absolute invariants are always relative invariants, it follows that they too can always be written in the form 4.14, that is, as a polynomial in Grundformen. The question then becomes, what restrictions need we impose for a polynomial in Grundformen to be an absolute invariant?

Lemma 4.15. Relative invariants of different characters are linearly independent.

Proof. The proof is by induction over the number of relative invariants of different character, and contradiction. For our base case, we choose a set consisting of a single relative invariant, which is clearly linearly independent. We now take it to be proven that $k-1$ relative invariants of different characters must be linearly independent, and assume the k^{th} case to be different. Then there exists a linear combination $A = \sum_{i=1}^k c_i \Phi_i = 0$, not all c_i being zero. We may always reorder the terms such that $c_2 \neq 0$, and take a generic element $g \in G$ such that $\chi_1(g) \neq \chi_2(g)$, and element that must exist since $\chi_1 \neq \chi_2$. Then,

$$0 = g \cdot A - \chi_1(g) = c_2(\chi_2(g) - \chi_1(g))\Phi_2 + \cdots + c_k(\chi_k(g) - \chi_1(g))\Phi_k = 0.$$

This then implies that the $k-1$ relative invariants $\{\Phi_2, \ldots, \Phi_k\}$ must be linearly independent, giving us our contradiction. The lemma follows. □

Lemma 4.16. Any linear combination of a set of relative invariants, all having the same character, is itself a relative invariant of that very character.

Proof.

$$g \cdot \sum_{i=1}^k c_i \Phi_i = \sum_{i=1}^k c_i (g \cdot \Phi_i) = \sum_{i=1}^k c_i \chi(g) \Phi_i = \chi(g) \sum_{i=1}^k c_i \Phi_i.$$

□

Lemma 4.17. No linear combination of a set of two or more relative invariants, all having different characters, may be an absolute invariant.

Proof. Assume the converse. Then there exist relative invariants of different characters Φ_i and $c_i \in \mathbb{C}$ such that

$$0 = \sum_{i=1}^k c_i \Phi_i - g \cdot \sum_{i=1}^k c_i \Phi_i = \sum_{i=1}^k c_i \Phi_i - \sum_{i=1}^k c_i \chi_i(g) \Phi_i = \sum_{i=1}^k c_i (1 - \chi_i(g)) \Phi_i.$$

But this would then imply that the Φ_i are linearly dependent, which by Lemma 4.15 they may not be. The lemma follows. □

Lemma 4.18. A polynomial in special Grundformen is an absolute invariant if and only if every monomial term in it is an absolute invariant.

Proof. All monomials in a polynomial $F(\Psi_1, \ldots, \Psi_n)$ of the same character may by Lem. 4.16 be lumped together into a new relative invariant of that character. Thus F can be expressed as a linear combination of a set of invariants, all of different characters. If this set is greater than one, by Lem. 4.17, F may not be an absolute invariant, so if we want that to be the case, all monomials must have the same character. If this character is anything other than one for every element in the group, F may not be an absolute invariant. Thus we conclude that F is an absolute invariant if and only if every monomial is of trivial character, that is, every monomial is an absolute invariant. □

With that established, to find the minimal generating set of the rings of invariant polynomials, we simply need to find the absolute invariant monomials in the special Grundformen that may not be expressed as products of other absolute invariant monomials.

Example 4.19. Let $G = \mathbb{BO}$, so that $\overline{G} = \mathbb{O}$. Inspecting the characters we found earlier, we note that Ψ_1^2, Ψ_2, $\Psi_1\Psi_3$, and Ψ_3^2 are all absolute invariants under the action of the octahedral group. We do however find that

$$\begin{aligned}\Psi_2^3 - 108\Psi_1^4 &= (t_0^8 + 14t_0^4t_1^4 + t_1^8)^3 - 108(t_0t_1(t_0^4 - t_1^4))^4 \\ &= t_0^{24} - 66t_0^{20}t_1^4 + 1023t_0^{16}t_1^8 + 2180t_0^{12}t_1^{12} + 1023t_0^8t_1^{16} - 66t_0^4t_1^{20} + t_1^{24} \\ &= ((t_0^4 + t_1^4)((t_0^4 + t_1^4)^2 - 36t_0^4t_1^4))^2 = \Psi_3^2,\end{aligned}$$

so multiples of Ψ_3^2 may always be expressed in terms of multiples of Ψ_2 and Ψ_1^2. Let then $\Psi_1^a\Psi_2^b\Psi_3^c$ be a monomial entering an invariant polynomial under $\mathbb{O}$. We may factor out Ψ_2^b entirely since Ψ_2 is invariant to find that $\Psi_1\Psi_3^c$ must be invariant. If a is even, then we may factor our Ψ_1^a entirely, and find Ψ_3^c to be invariant, which may only be the case if c too is even, meaning that Ψ_3^c is expressible as a power of Ψ_3^2, making it expressible in turn in terms of Ψ_1^4 and Ψ_2^3. If a is odd, then we may factor out Ψ_1^{a-1}, leaving us with $\Psi_1\Psi_3^c$, from which we may factor out $\Psi_1\Psi_3$. Ψ_3^{c-1} is only invariant if c is odd, and so we are left with some power of $(\Psi_2^3 - 108\Psi_1^4)$. We then conclude that the monomials Ψ_1^2, Ψ_2, and $\Psi_1\Psi_3$ generate the entire ring of invariant polynomials under $\mathbb{O}$. Setting $x = \sqrt[3]{108}\Psi_1^2$, $y = -\frac{1}{\sqrt[9]{108}}\Psi_2$, $z = \Psi_1\Psi_3$, we see that $\{x, y, z\}$ is a minimal generating set of the ring of invariant polynomials, and that they further obey the relation

$$\begin{aligned}z^2 = \Psi_1^2\Psi_3^2 &= \Psi_1^2(\Psi_2^3 - 108\Psi_1^4) \\ &= \frac{x}{\sqrt[3]{108}}(-\sqrt[3]{108}y^3 - \sqrt[3]{108}x^2) \\ &= -x(y^3 + x^2),\end{aligned}$$

and so we obtain

$$\mathbb{C}[t_0, t_1]^{\mathbb{BO}} \cong \mathbb{C}[x, y, z]/(z^2 + x(y^3 + x^2)).$$

In this fashion, we find generating sets for the rings of invariants for all finite subgroups of $\mathrm{SL}_2(\mathbb{C})$. Again the details may be found in [34]. They are listed in Tab. 4.20.

Subgroup of $\mathrm{SL}_2(\mathbb{C})$	Generating set	Relation between generators
C_n	$x = \Psi_1^n$ $y = \Psi_2^n$ $z = \Psi_1\Psi_2$	$xy + z^n = 0$
$\mathbb{BD}_n$	$x = \sqrt[n]{4}\Psi_3^2$ $y = \frac{1}{\sqrt[2n]{4}}\Psi_1\Psi_2$ $z = \Psi_3\Psi_2^2$	$z^2 + x(y^2 + x^n) = 0$
$\mathbb{BT}$	$x = \Psi_1$ $y = \sqrt[3]{4}\Psi_2\Psi_3$ $z = i(\Psi_2^3 + \Psi_3^3)$	$z^2 + x^4 + y^3 = 0$
$\mathbb{BO}$	$x = \sqrt[3]{108}\Psi_1^2$ $y = -\frac{1}{\sqrt[9]{108}}\Psi_2$ $z = \Psi_1\Psi_3$	$z^2 + x(y^3 + x^2) = 0$
$\mathbb{BD}$	$x = \Psi_1$ $y = \Psi_2$ $z = \sqrt[5]{-1728}\Psi_3$	$x^2 + y^3 + z^5 = 0$

TABLE 4.20. The sets of generators for the ring of invariants of each $G \subseteq \mathrm{SL}_2(\mathbb{C})$.

CHAPTER 5

Conclusion and Prospects

The time has come to gather up our results. In Chap. 4, we found a way to express the orbifolds that are defined by the action of the finite subgroups of SU(2) on $\mathbb{C}^2$ in the natural representation as algebraic varieties, surfaces embedded in $\mathbb{C}^3$. These varieties (listed in Tab. 4.20) are far from trivial, and in fact, all of them are singular, something that we may observe the moment we plot out their real parts (see Fig. 5.1).

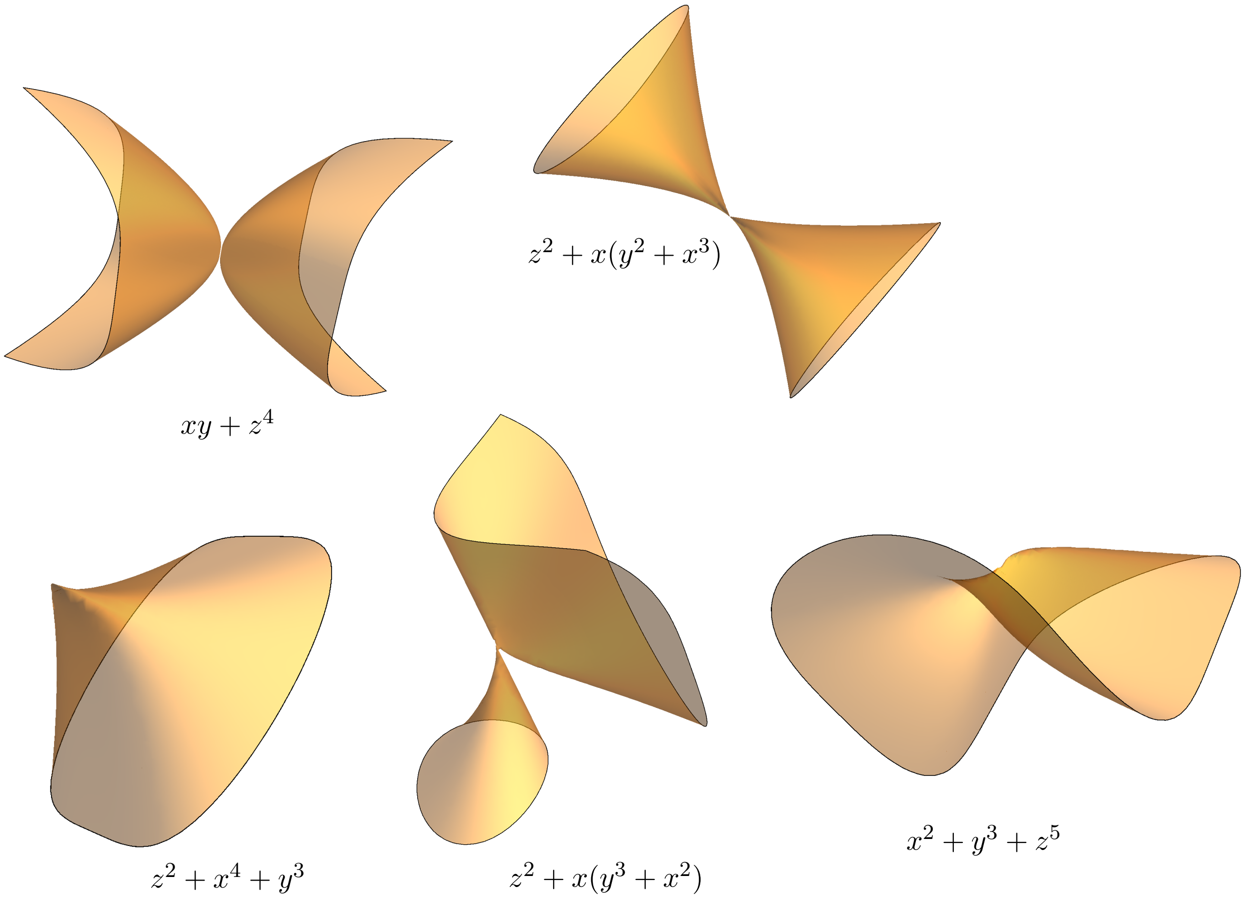


Figure 5.1. The real parts of the varities defined by the different orbifolds.

Using the tools then that we have so carefully constructed in Chap. 3, we resolve these singularities with blow-ups. While doing so, we do of course keep track of the irreducible components of the exceptional divisors and note how these intersect one another. Schematically, the result is displayed in Fig. 5.2, and the result is quite telling: they look very familiar to a result we observed earlier in our quest. To make this more clear, we change our schematic way of illustrating the intersection of the irreducible components of the exceptional divisor—we draw each irreducible component as a node, and when two nodes intersect, we draw a line between their nodes. The result is displayed in Tab. 5.3.

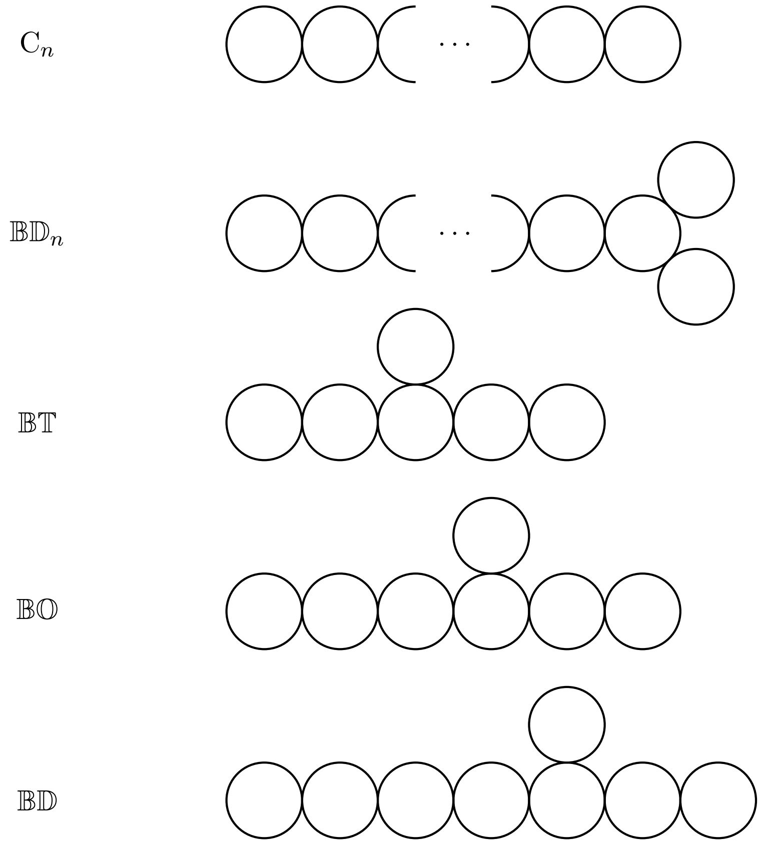


FIGURE 5.2. Schematic of the irreducible components of the exceptional divisors of the blown-up varieties of the different orbifolds. Seeing each irreducible component is isomorphic to $\mathbb{CP}^1$, they are depicted as circles. When two circles touch, that is to indicate an intersection.

What we have uncovered appears to be the same diagrams we obtained for the morphism spaces between the different groups' irreducible representations when the tensor product is taken with the natural representation in Chap. 2, but with one crucial difference—one node is missing. There very clearly appears to be a deep connection between the two, a connection that is further illuminated when we turn to Lie theory, which we for brevity's sake hitherto have sought to treat to a minimum. The diagrams we obtain when blowing up the singularities of the orbifolds are the so-called *Dynkin diagrams* of finite-dimensional semisimple Lie algebras [13], whereas the diagrams obtained from the representation theoretical treatments are their counterparts obtained in the infinite-dimensional case, the *affine Dynkin diagrams* [36]. With this branching into Lie theory establishing its third leg, we have thus, finally, outlined the classical McKay correspondence.

There is much more to be said of the McKay correspondence, of course. All we've done in this treatment is to explain what part of it is, as we have not even touched upon the Lie theory needed to properly establish its third leg. We certainly have not explained *why* it comes about, which would require much more algebraic geometry as well as much more module theory and homological algebra. Nonetheless, the author would be amiss if he did not at the very least give reference to where such explanations may be found.

González-Sprinberg and Verdier were able, shortly after McKay had published his original paper, to establish the connection between the algebro-geometrical and representation theoretical aspects, which they published (in French) in [37] and [38]. In [39], Slodowy gives a qualitative summary of their argument. A more informal treatment of the same in the context of skew group algebras may be found in [40].

For the connection between the algebro-geometrical and the Lie theoretical aspects, the works of Steinberg [41], Kostant [42], and in particular, Brieskorn [43] are instructive. Brieskorn (whose discovery actually predates McKay's observation by a decade), has been able to show that from the simply connected simple complex Lie groups to which the aforementioned Dynkin diagrams correspond, one may construct the Kleinian singularities, which when blown up give the original diagrams, thus "closing the circle" in the words of my supervisor [44]. For a review of Brieskorn's method, see [45], and for a more extensive treatment of the same, see [46].

And still this only establishes the McKay correspondence in *two* dimensions. Generalizations to dimensions three and higher have been made in the decades since McKay's original discovery, see for example the work of Ito Yukari and Miles Reid in [47]. Of particular interest is the work of Tamar Friedmann in [48], where in treating the three-dimensional case, she is able to develop a connection to the "n-ary Lie algebras" or "Lie algebras of the n-th kind" originally developed by Filippov in the 1980s [49]. Friedmann further elaborates on how this phenomenon can be useful in the study of Yang-Mills theory.

The aforementioned Miles Reid's work on the topic goes even further, and in collaboration with Tom Bridgeland and Alastair King [50], treatment of the phenomenon has been made within the context of derived category theory, and further points of contact have been found with Hodge theory and string theory [51].

At present, there is little more the author can add on the topic. In fine, suffice to say that John McKay was right on the money when he said [2] "If this approach is to be successful, its merit will lie in its unifying power and its elegance. Would not the Greeks appreciate the result that the simple Lie algebras may be derived from the Platonic solids?"

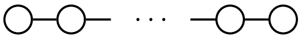
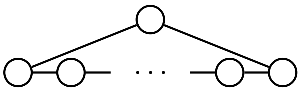
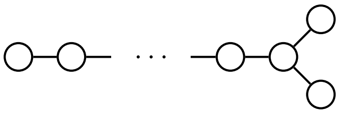
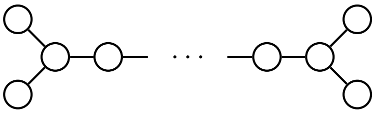
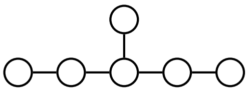
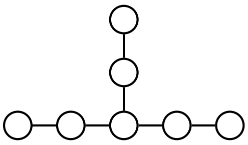
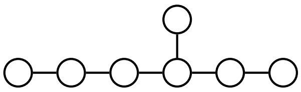
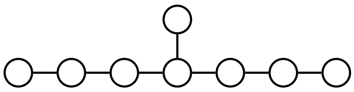
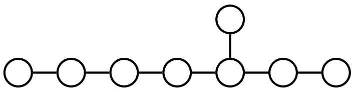
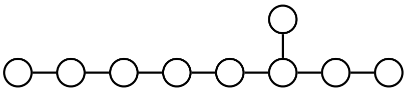
Subgroup of SU(2)	Algebraic Geometry	Representation Theory
C_n		
$\mathbb{B}D_n$		
$\mathbb{BT}$		
$\mathbb{BO}$		
$\mathbb{BD}$		

Table 5.3. The intersection diagrams for the irreducible representations of the exceptional divisor, listed next to the homomorphism dimensionality diagrams of the irreducible representations.

APPENDIX A

Algebra

The following appendix is intended to provide the reader with an introduction to a number of algebraic structures and results that are referenced and applied in the text of Chap. 2. The author draws heavily on the basic structure of [52], and the appendix as a whole may well be regarded as the author's reworking of that text's first and second chapters. The reader is of course welcome (if not outright encouraged) to check out the book for themselves and so to say, "drink from the source".

I will assume that the reader has a basic understanding of group and representation theory, including an understanding of the concept of the module of a group and how this correspond to a representation. If so happens not to be the case however, I would refer them to sections 1.1−1.5 of [14], which cover all of these topics (and more) in a brief yet thoroughly comprehensive manner.

Other structures I will assume knowledge of are those of rings and fields. All the concepts which we will draw on are more than well contained within sections III.1 – III.4 of [11].

1. Algebras, Modules, and Homomorphisms: The Basic Definitions

Definition A.1. (Vector space.) Let V be a set and $\mathbb{F}$ be a field. If V is endowed with an additive operation $V \times V \to V$ obeying

$$\begin{aligned} v + w &= w + v, \\ (v + w) + u &= v + (w + u), \end{aligned}$$

for all $u, v, w \in V$; a scalar multiplicative operation $\mathbb{F} \times V \to V$ obeying

$$\begin{aligned} \lambda(v + w) &= \lambda v + \lambda w, \\ (\lambda + \mu)v &= \lambda v + \mu v, \\ \lambda(\mu v) &= (\lambda\mu)v, \end{aligned}$$

for all $v, w \in V$, and all $\lambda, \mu \in \mathbb{F}$; a null vector $0 \in V$ such that

$$v + 0 = 0$$

for all $v \in V$; the unity element $1 \in \mathbb{F}$ operates as

$$1v = v$$

for all $v \in V$; and for every $v \in V$ there exists a vector $-v$ such that

$$v + (-v) = 0,$$

then V is said to be a *vector space over the field* $\mathbb{F}$.

The most natural example of a vector space is of course the standard three-dimensional space we all live in, which is a vector space over $\mathbb{R}$ where the real numbers scale vectors in space in the intuitive way. However, the point that is important to bring across is that a vector space is generalized to cover so much more than that. We may choose many other fields beyond $\mathbb{R}$, and the space need not be of the nature we intuitively conceive of when we hear the word "space". All it really needs to be is *a set conforming to the aforementioned conditions.* For the rest of this appendix, we will only concern ourselves with $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and vector spaces that are of finite dimension.

Definition A.2. (Linear dependence and linear independence.) Let V be a vector space over a field $\mathbb{F}$. A set of vector $\{v_1, v_2, \ldots, v_k\} \in V$ are said to be *linearly dependent* if there exists a set $\{a_1, a_2, \ldots, a_k\} \in \mathbb{F}$, not all of them 0, such that

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0.$$

If no such not-all-zeroes set of elements of $\mathbb{F}$ can be found, the vectors $\{v_1, v_2, \ldots, v_k\}$ are said to be *linearly independent.*

Definition A.3. (Basis.) Let V be a vector space over a field $\mathbb{F}$. A basis of V is a set of vectors $\{v_1, v_2, \ldots, v_n\} \in V$ that are linearly independent and such that every vector in V may be expressed as a linear combination of $\{v_1, v_2, \ldots, v_n\}$.

Definition A.4. (Hermitian inner product.) A *Hermitian inner product* (or just *inner product* or *Hermitian form*) is an operation $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}$ ($\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$) defined such that for every $u, v, w \in V$, $\alpha \in \mathbb{F}$:

(i) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$,
(ii) $\langle \alpha v, w \rangle = \alpha \langle v, w \rangle$,
(iii) $\langle v, w \rangle = \overline{\langle w, v \rangle}$,
(iv) $\langle v, v \rangle \geq 0$, where the equality applies if and only if $v = 0$.

If $\mathbb{F} = \mathbb{R}$, then $\overline{x} = x$, and if $\mathbb{F} = \mathbb{C}$, then $\overline{x}$ is the complex conjugate of x. If for two vectors $v, w \in V$ we have $\langle v, w \rangle = 0$, we say that the two vectors are *orthogonal.*

Dot product, such as we know it when working in conventional three-dimensional space, is merely one example of such an inner product. Do note, and this is very important, that two vectors that are orthogonal with respect to one inner product defined over the vector space, may very well be non-orthogonal under another inner product. And just as there are innumerable ways to pick a basis, there are innumerable ways to pick an inner product.

Another concept that follows from the concept of a vector space is that of a direct sum.

Definition A.5. (Sum of vector spaces.) Let U and W be subspaces of a vector space V. The *sum* of U and W (denoted $U + W$) is then defined as the set of all vectors that may be written as linear combinations of vectors in U and W,

$$U + W = \{u + w | u \in U, w \in W\}.$$

Definition A.6. (Direct sum of vector spaces.) Let U and W be two vector spaces. The *direct sum* of U and W (denoted $U \oplus W$) is then defined as the set of ordered pairs of vectors in U and W, and is itself a vector space,

$$U \oplus W = \{(u, w) | u \in U, w \in W\}.$$

It is easy to verify that the direct sum vector space $U \oplus W$ posses subspaces isomorphic to U and W respectively. In literature, it is often written that if $V = U \oplus W$, then $U \subseteq V$ and $W \subseteq V$.

These two definitions, though at first glance similar, are not the same, and the reader is advised to take special note of this. Specifically, in the case where U and W are subspaces of the same vector space V, while it is a given that $U + W \subseteq V$, it is not a given that $U \oplus V$ is isomorphic to any subspace of V.

Example A.7. Consider the vector space $V \cong \mathbb{R}^4$ endowed with a basis $\{\vec{x}, \vec{y}, \vec{z}, \vec{w}\}$. The spaces $U = \{a\vec{x} + b\vec{y} | a, b \in \mathbb{R}\}$ and $W = \{b\vec{y} + c\vec{z} + d\vec{w} | b, c, d \in \mathbb{R}\}$ are both subspaces of V. We then have

$$U + W = \{a\vec{x} + b\vec{y} + c\vec{z} + d\vec{w} | a, b, c, d \in \mathbb{R}\} = V,$$

which as expected is in line with $U + W \subseteq V$. However, $U \oplus W \cong \mathbb{R}^5$, which evidently cannot be isomorphic to any subspace of V.

Definition A.8. (Complementary subspaces.) Let V be a vector space with subspaces W and U. If $U + W = V$, and $U \cap W = \{0\}$, then $U \oplus W \cong V$, and U and W are said to be *complementary subspaces*, or just *complements*, of one another.

Example A.9. Let V be a vector space with basis $\{v_1, v_2, v_3, v_4\}$. Then V is the direct sum of the vector space spanned by $\{v_1, v_2\}$, call it V_1, and the vector space spanned by $\{v_3, v_4\}$, call it V_2. It is of course to be noted that in deciding on a basis for V in this example, even after pinning down $\{v_1, v_2\}$ as our first two basis vectors, we still have considerable liberty with which to choose our third and fourth basis vectors. Indeed, the third and fourth basis vectors need not even be linear combinations solely of v_3 and v_4 above. $v_{\text{III}} := 2v_1 + v_3$ and $v_{\text{IV}} := 5v_2 + 4v_4$ would do the trick just as well. In other words, given a subspace $W \in V$, there are innumerable ways in which to choose a complementary subspace U such that $W \oplus U \cong V$. This leads us to our next definition.

Definition A.10. (Orthogonal complement.) Let V be a vector space, W be a subspace of V, and let $\langle \cdot, \cdot \rangle$ be an inner product on V. Then

$$W^{\perp} := \{v \in V | \langle v, w \rangle = 0, \ \forall w \in W\}$$

is a complement of W in V called the *orthogonal complement of* W.

Do note that an orthogonal complement is only defined with respect to an inner product, and as such the former is no less arbitrary than the latter. Nonetheless, as will be seen when we revisit it soon, it is nonetheless a very useful construct.

Definition A.11. (Quotient space.) Let V be a vector space and let W be a subspace thereof. Let $\sim$ be an equivalence relation on V defined by $v_1 \sim v_2$ if and only if $v_1 - v_2 \in W$. Then the *quotient space* V/W is the set of all equivalence classes under this relation. It is easily verified that if V is a vector space, then so is V/W. Elements of V/W are commonly denoted $v + W$, where $v \in V$.

Definition A.12. (Algebra over a field.) Let $\mathbb{F}$ be a field, and A be a vector space over $\mathbb{F}$ that is furthermore a unitary ring. Then A is called an *algebra over* $\mathbb{F}$ if

$$c(xy) = (cx)y = x(cy)$$

For all $x, y \in A$, and all $c \in \mathbb{F}$.

Example A.13. Let V be a vector space over a field $\mathbb{F}$. The set of vector space homomorphisms from V to itself, $\text{Hom}(V, V)$, or, $\text{End}(V)$, then can be endowed with the structure of an algebra by letting addition be defined by standard addition of functions, $(\varphi + \theta)(v) = \varphi(v) + \theta(v)$, and letting multiplication be defined by composition of functions $(\varphi\theta)(v) = \varphi(\theta(v))$.

Another basic example of an algebra, and one we will look closer into both in this appendix and in the main text, is that of the algebra of a group.

Definition A.14. (The group algebra over a field.) Let G be a group. We may then construct its *group algebra over a field* $\mathbb{F}$, whose elements are formal linear combinations of the group elements. These are of the form

$$\sum_{i}^{|G|} a_i g_i, \quad a_i \in \mathbb{F}, g_i \in G.$$

It is easy to verify that this fits the definition of an algebra: As a vector space, its basis vectors are the group elements $\{g_i\}$, and as a ring, the additive operation is formal summation in conjunction with the additive operation of the field,

$$\sum_i^{|G|} a_i g_i + \sum_i^{|G|} b_i g_i = \sum_i^{|G|} (a_i + b_i) g_i$$

multiplication is inherited from as it is defined for the group in conjunction with how it is defined for the field,

$$\left(\sum_i^{|G|} a_i g_i \right) \left(\sum_j^{|G|} b_j g_j \right) = \sum_i^{|G|} \sum_j^{|G|} (a_i b_j)(g_i g_j),$$

and the unital element is the unital element of $\mathbb{F}$ multiplied by the identity of the group. For given group G and field $\mathbb{F}$, this structure is denoted $\mathbb{F}[G]$.

Definition A.15. (Subalgebra.) Let B be a subset of A that is a vector space over $\mathbb{F}$ in its own right, and is furthermore closed under ring addition and multiplication. Then B is called a *sub algebra of* A.

Definition A.16. (Algebra homomorphism.) Let A and B be two $\mathbb{F}$-algebras. If the map $\varphi : A \to B$ satisfies

(i) $\varphi(cx) = c\varphi(x)$
(ii) $\varphi(x + y) = \varphi(x) + \varphi(y)$
(iii) $\varphi(xy) = \varphi(x)\varphi(y)$
(iv) $\varphi(1_A) = 1_B$

for all $x, y \in A$, $c \in \mathbb{F}$, then φ is called an *algebra homomorphism over the field* $\mathbb{F}$.

Note that since A, B, in their capacities as being algebras, are rings, φ is also a ring homomorphism, and so the result that $\ker \varphi$ is an ideal in A and $\operatorname{im} \varphi$ is an ideal in B follows.

The reader will recall from group theory the notion of the group action. In a very similar vein, one develops the notion of an action of an algebra. Specifically, given a set S and an algebra A, an action is a map $\cdot : A \times S \to S$, $(a, s) \mapsto a \cdot s$. With this tool at our disposal, we may now construct another concept very similar to one found in group and representation theory.

Definition A.17. (Module of an algebra.) Let A be an $\mathbb{F}$-algebra, V be a vector space over $\mathbb{F}$, and $\cdot$ be an action of A on V. V is then called a *module of* A, or an A*-module* if the following structural properties are obeyed for all $x, y \in A$, $v, w \in V$, and $c \in \mathbb{F}$:

(i) $x \cdot (v + w) = x \cdot v + x \cdot w$
(ii) $(x + y) \cdot v = x \cdot v + y \cdot v$
(iii) $(xy) \cdot v = x \cdot (y \cdot v)$
(iv) $c(x \cdot v) = (cx) \cdot v = x \cdot (cv)$
(v) $1 \cdot v = v$.

It is easy to verify that an algebra A itself is an A-module, where the elements of the algebra are viewed as vectors in a vector space, and the action of the algebra upon the vectors are those of the algebra's standard left-multiplication. When discussing A in this context, it is conventional (and convenient) to denote it by A° instead to remind readers that it is now treated from the point of view of modules. A° is formally called the *regular module* of the algebra A. Less immediately clear is that all ideals of A are also A-modules, but it too can be swiftly and easily verified as following from the definition that if $x \in I$, I being an ideal of A, then $a \cdot x \in I$.

Example A.18. Let V be an A-module. Then for each $x \in A$, we may construct a homomorphism $x_V : V \to V$, $v \mapsto x \cdot v$. We noted earlier in A.13 that the set $\mathrm{End}(V)$ was an $\mathbb{F}$-algebra, and so we may construct an algebra homomorphism $\alpha_V : A \to \mathrm{End}(V)$ by $x \mapsto x_V$. We call the image of α_V in $\mathrm{End}(V)$ A_V, something which we will revisit later.

Comparing the structure of an algebra module with the structure of a group module, a relationship readily becomes apparent: every module of a group is a module of its group algebra as defined above, and every module of a group algebra can be seen to be a module of the original group by just considering the actions of the elements in the algebra that are elements of the group. We may therefore without any loss of generality jump between G-modules and $\mathbb{F}[G]$-modules.

Definition A.19. (Representation of an Algebra.) Let V be a vector space of dimension d over a base field $\mathbb{F}$, and A be an algebra. A *representation of A on V* is an algebra homomorphism $\varphi : A \to \mathrm{Mat}_{d\times d}(\mathbb{F}) \cong \mathrm{End}(V)$. Two representations φ, θ are said to be *equivalent* if there exists a nonsingular matrix D such that $\theta(a) = D\varphi(a)D^{-1}$, $\forall a \in A$.

It is immediately observed that as in the case of group modules and group representations, every algebra module corresponds to an algebra representation and vice versa. Further, in line with Def. A.14, every group module and representation extends to a module and a representation of the group algebra, and all of the latter restrict to the former.

Definition A.20. (Submodule.) Let V be a module of an algebra A. A subspace of V, $W \subseteq V$, is called a *submodule* if it is invariant under the action of the algebra in that for every $a \in A$, $w \in W$, $a \cdot w$ lies in W. Inheriting the structural properties A.17 (i)-(v) from V, W itself is an A-module.

Lemma A.21. (Quotient module.) Let V be an A-module and W be a submodule of V. Then V/W is a A-module called a *quotient module* under the algebra action $\star$ defined by

$$a \star (v + W) = (a \cdot v) + W.$$

Just as we may construct homomorphisms between algebras, so one can construct homomorphisms between modules of the same algebra.

Definition A.22. (Module homomorphism.) Let V and W be A-modules. A *module homomorphism* is a linear transformation $\varphi : V \to W$ obeying

$$\varphi(x \cdot v) = x \cdot \varphi(v),$$

for every $v \in V$ and every $x \in A$.

It can readily be checked that both the kernel and image of a module homomorphism are closed under the action of the algebra. From this, we may conclude that if $\varphi : V \to W$ is a module homomorphism, then $\ker\varphi$ is a submodule of V and $\mathrm{im}\,\varphi$ is a submodule of W.

Do note that a module homomorphism is more than just a homomorphism between vector spaces, but is in fact a vector space homomorphism that *preserves the module structure*. The set of module homomorphisms from V to W is denoted by $\mathrm{Hom}_A(V, W)$, and the set of vector space homomorphisms from V to W is denoted by just $\mathrm{Hom}(V, W)$. It goes without saying that $\mathrm{Hom}_A(V, W) \subseteq \mathrm{Hom}(V, W)$.

Example A.23. ($\mathrm{Hom}_A(V, W)$ as a vector space.) We may endow the set $\mathrm{Hom}_A(V, W)$ with the structure of an $\mathbb{F}$-space by defining multiplication by scalars $k \in \mathbb{F}$ by $(k\varphi)(v) = k(\varphi(v))$, and addition by $(\varphi + \theta)(v) = \varphi(v) + \theta(v)$.

Corollary A.24. In line with earlier discussion on the relationship between a group G and its group algebra $\mathbb{F}[G]$, the set $\mathrm{Hom}_G(V, W)$ may also be endowed with the structure of a vector space over $\mathbb{F}$.

Lemma A.25. Let U, V, W be modules of the algebra A. Viewing the set of module morphisms from U, V, and $U \oplus V$ to W as vector spaces,

$$\mathrm{Hom}_A(U \oplus V, W) \cong \mathrm{Hom}_A(U, W) \oplus \mathrm{Hom}_A(V, W).$$

Proof. Let $\varphi : U \oplus V \to W$, $(u, v) \mapsto \varphi(u, v)$ be an arbitrary element of $\mathrm{Hom}_A(U \oplus V, W)$. φ then induces homomorphisms $\varphi_1 \in \mathrm{Hom}_A(U, W)$, $\varphi_2 \in \mathrm{Hom}_A(V, W)$ by $\varphi_1(u) := \varphi(u, 0)$, $\varphi_2(v) := \varphi(0, v)$. The mapping $\mathrm{Hom}_A(U \oplus V, W) \to \mathrm{Hom}_A(U, W) \oplus \mathrm{Hom}_A(V, W)$, $\varphi \mapsto (\varphi_1, \varphi_2)$ is then both linear and bijective. □

Earlier, in A.13, we noted that $\mathrm{End}(V)$ was an $\mathbb{F}$-algebra, and it turns out that so is $\mathrm{Hom}_A(V, V)$, the latter being a subalgebra of the former. In fact, looking at $\mathrm{Hom}_A(V, V)$ as a subset of $\mathrm{End}(V)$,

$$\mathrm{Hom}_A(V, V) = \{\varphi \in \mathrm{End}(V) | \varphi(x \cdot v) = x \cdot \varphi(v),\ \forall x \in A, v \in V\},$$

we see that it is identical to the centralizer of A_V from A.18 in $\mathrm{End}(V)$,

$$\mathrm{C}_{\mathrm{End}(V)}(A_V) = \{\varphi \in \mathrm{End}(V) | \varphi(x_V(v)) = x_V(\varphi(v)),\ \forall x_V \in A_V, v \in V\}.$$

If one, like the author, happens to have a fondness for the movie *Inception*, one would be inclined to ask the question, what is the centralizer of this centralizer, $\mathrm{C}_{\mathrm{End}(V)}(\mathrm{C}_{\mathrm{End}(V)}(A_V))$? It follows from fundamental algebra that if the subalgebra R is the centralizer of the subalgebra S, then S must form at least part of the centralizer of R. After all, since R is the set of all elements commuting with every element of S, clearly every element of S commutes with every element of R. Of course, we may not rule out that there exists elements outside of S that also commutes with every element of R. Applied to our particular case, this establishes that

$$A_V \subseteq \mathrm{C}_{\mathrm{End}(V)}(\mathrm{C}_{\mathrm{End}(V)}(A_V)).$$

As we shall eventually see in a powerful result known as the Double Centralizer Theorem, if certain conditions on A and V are met, this $\subseteq$ does in fact become an $=$.

Earlier we introduced the concepts of sums and direct sums of subspaces. These notions apply to modules and submodules as well. If U and W are submodules of an A-modules V, we can establish two things immediately.

Lemma A.26. Let W and U be two submodules of V. Then their sum and their intersection are both submodules of V.

Proof. First we prove that $U + W$ is a submodule of V, that is that it is closed under the action of the algebra. Let v be a vector in $U + W$. Then it may be written as $v = u + w$, $u \in U$ and $w \in W$. Since U, W are submodules, $a \cdot u \in U$ and $a \cdot w \in W$, and so $a \cdot (u + w) \in U + W$. Thus, $U \oplus W$ is a submodule of V.

Next we prove that $W \cap U$ also is closed under the action of the algebra. Let v be a vector in $W \cap U$. Since W and U are submodules, $a \cdot v$ lies in W as well as in U. This holds true for all $v \in W \cap U$. Thus, $W \cap U$ is a submodule of V. □

This simple lemma turns out to be surprisingly useful as we go on.

Further, if U and W are both A-modules (denote their algebra actions by $\bullet$ and $\circ$ respectively), then $U \oplus W$ is an A-module under the algebra action $\star$ defined by

$$a \star (u, w) := (a \bullet u, a \circ w).$$

From this construction, it follows that the module $U \oplus W$ must have subspaces $U' \cong U$ and $W' \cong W$ such that $U' + W' = U \oplus W$. Conversely, if an A-module V can be written as $U + W$ for two submodules U and W such that $U \cap W = \{0\}$, then $V \cong U \oplus W$.

Lemma A.27. Let V be an A-module that is the direct sum of two A-modules U and W. Then $U \cong V/W'$, where W' is a submodule of V such that $W' \cong W$.

Proof. Since $V = U \oplus W$, there exists $W' \subseteq V$ such that $W \cong W'$. Since $V = U \oplus W$, for every v in V there exists unique $u \in U$ and $w \in W$ such that $v = (u, w)$. Without loss of generality we may denote the elements of V/W by their parts in U' plus W'. Then it is self-evident that the map $\varphi : V/W' \to U$, $(u, 0) + W' \mapsto u$ is an isomorphism. □

To say something about the relationship between sums of submodules and direct sums of submodules, we introduce a new construct.

Definition A.28. (Simple module.) Let V be an A-module. If the only submodules of V are V itself and the zero module $\{0\}$, V is said to be a *simple module.*

Example A.29. Let V be a one-dimensional A-module. Since V only permits two subspaces, itself and $\{0\}$, it follows that it may only permit those as submodules as well. That is, every one-dimensional A-module is simple.

Lemma A.30. Let V be an A-module that can be expressed as a finite sum of its simple submodules. Then V must be isomorphic to a direct sum of some of those simple submodules.

Proof. We write $V = \sum_\alpha V_\alpha$, $V_\alpha \subseteq V$ all being simple modules. Then, since the number of submodules in this sum is finite, we may pick a maximal submodule $W \subseteq V$ such that W is isomorphic to a direct sum of some of the V_α. If for every V_α we have $V_\alpha \subseteq W$, then, since $V = \sum_\alpha V_\alpha$, it follows that $W = V$, and we are done. Consequently, if $W \subsetneq V$, then there must exist an V_α such that $V_\alpha \nsubseteq W$. However, since V_α is simple, by Lem. A.26, its intersection with W must be zero. By A.27, $W' = W + V_\alpha$ is then isomorphic to $W \oplus V_\alpha$. Then W is evidently not maximal and we have obtained a contradiction. The lemma follows. □

Definition A.31. (Semisimple module.) Let V be an A-module. If for every submodule $W \subseteq V$ there exists a submodule $U \subseteq V$ such that $W \oplus U \cong V$, then V is said to be a *semisimple module.*

Lemma A.32. Every submodule of a semisimple module is itself semisimple.

Proof. Let V be a semisimple A-module, and W be a submodule of V. If W is simple, then evidently, W is semisimple. If W is non-simple, then let X be a submodule of W. X must also be a submodule of V, and so there exists a submodule $Y \subseteq V$ such that $X \oplus Y \cong V$. The intersection $W \cap Y$ must also be a submodule of W. Furthermore, since $X \oplus Y \cong V$, $\dim(X) + \dim(Y) = \dim(V)$, we have $\dim(X \cap Y) = 0$ by necessity, meaning that $X \cap U = \{0\}$, from which it follows that $X \oplus (W \cap Y) \cong W$. Thus W is semisimple. □

Simple and semisimple modules are related in an interesting way.

Lemma A.33. Let V be a A-module. Then V is semisemiple if and only if it is isomorphic a direct sum of simple modules.

Proof. It is clear that if V is isomorphic to a direct sum of simple modules V_i, then it may be written as a sum of simple submodules V_i', where for each i, $V_i \cong V_i'$. By A.30, if V is a sum of its set of simple modules, then it follows that it must be isomorphic a direct sum of some of those simple modules. Consequently, we only need to prove that V is semisimple if and only if it is a sum of simple modules.

Let V be a sum of simple modules, which we write $V = \sum_i V_i$. Pick an arbitrary submodule $W \subseteq V$. Since V is of finite dimension, we may then pick a submodule $U \subseteq V$ which is maximal in the property that $U \cap W = 0$. Then $U \oplus W = V$. After all, if not, then there must exist $V_i \subseteq V$ such that $V_i \nsubseteq (U + W)$. Since V_i is simple, it may not have a non-zero overlap with either U or W because such an overlap would be a submodule of V_i. Then, we can construct the module $V_i + U \subseteq V$ which is strictly larger than U and which is such that $(V_i + U) \cap W = 0$. But we had established that U was maximal with that very property, and so we have a contradiction. Thus, $U + W = V$, and V is semisimple.

Conversely, let V be semisimple. Then, let W be the sum of all simple submodules of V. Assume that $W \subsetneq V$. Since V is semisimple, there must then exist a submodule $U \subseteq V$ such that $U \oplus W \cong V$, meaning that $U \cap W = \{0\}$. Since V is semisimple, so too must U be. We may take submodules of U, and further submodules of submodules of U, but since V is of finite dimensionality, so too is U, and eventually, we must reach simple submodules, if not before we reach one-dimensional submodules, then when we reach them. These simple submodules must then also, by definition, be in W. But $U \cap W = \{0\}$, and so we have arrived at a contradiction. Thus $V = W$. □

Corollary A.34. If V is a semisimple A-module, then it is isomorphic to a direct sum of a set of distinct simple submodules of V.

Definition A.35. (Semisimple algebra.) An algebra A is said to be semisimple if its regular module A° is a semisimple module.

With that, we have now assembled enough building blocks to start building things with them.

2. The Foundational Results: Noether, Schur, and Maschke

The first important theorem we visit is Emmy Noether's celebrated First Isomorphism Theorem. The isomorphism theorem exists for a wide variety of structures—groups, semigroups, rings, etc.—but here we will concern ourselves with the two structures that are immediately of interest to us.

Theorem A.36. (The First Isomorphism Theorem for Algebras.) Let $\varphi : A \to B$ be an algebra homomorphism. Then $A/\ker\varphi \cong \operatorname{im}\varphi$.

Proof. As established, $\ker\varphi$ is an ideal in A, and $\operatorname{im}\varphi$ is a subalgebra of B. Furthermore, $A/\ker\varphi$ is an algebra. Obviously, the restricted map $\varphi|_A : A \to \operatorname{im}\varphi$, $a \mapsto \varphi(a)$ is surjective, and we may create maps $\mu : A \to A/\ker\varphi$ and $\nu : A/\ker\varphi \to \operatorname{im}\varphi$ such that $\varphi|_A = \nu \circ \mu$, by $\mu(a) = a + \ker\varphi$ ad $\nu(a + \ker\varphi) = \varphi(a)$. To show that this functional composition is indeed legitimate, let us look closer.

It is readily apparent that both maps are surjective: For every $a + \ker\varphi \in A/\ker\varphi$ there exists a pre-image under μ in a, and for every $\varphi(a) \in \operatorname{im}\varphi$, there exists a pre-image under ν in $a + \ker\varphi$. It is easy to further see that μ is well-defined, though it might not be immediately obvious that ν is well-defined as well. However, if $\varphi(a) = \varphi(b)$, then $0 = \varphi(b - a)$, and so $b - a \in \ker\varphi$. Then, $a + \ker\varphi = a + b - a + \ker\varphi = b + \ker\varphi$, and so well-definedness follows.

All that is left is showing that ν is an isomorphism. It is already established that it is an epimorphism, so let us establish that it is a monomorphism by determining its kernel to be trivial. This is immediately obvious since $\ker \nu = 0 + \ker \varphi$ which indeed is trivial. Thus, $A/\ker\varphi \cong \operatorname{im}\varphi$. □

Theorem A.37. (The First Isomorphism Theorem for Modules.) Let $\psi : V \to W$ be a module homomorphism. Then $V/\ker\psi \cong \operatorname{im}\psi$.

Proof. Similar to the proof of A.36. □

Next, there is the topic of Schur's Lemma, and the author should begin by pointing out that in the literature, there is some ambiguity as to what Schur's Lemma actually is. Depending on where you look, Schur's Lemma is one of the following two which are always presented in conjunction with one another, with the other either being a lemma you need for proving Schur's, or a corollary which one immediately concludes from Schur's.

Lemma A.38. (Schur's Lemma I.) Let V and W be simple modules of some algebra A, and let φ be a homomorphism from V to W. Then, either φ is the zero-map, or φ is an isomorphism.

Proof. That the zero-map is a homomorphism from V to W is immediately obvious. All that remains to prove is that if $\varphi : V \to W$ is not the zero-map, then φ must be an isomorphism.

Every homomorphism has a kernel, and since φ is not the zero-map, its kernel cannot be all of V. Since the kernel of a module homomorphism is itself a module and V as established is a simple module, the only other available option is that the kernel is trivial. The image of a module homomorphism too must be a module, and since W is simple and φ is not the zero-map, the only available option is that the image is all of W. Then, by A.37,

$$V/\{0\} \cong V \cong W,$$

and φ is an isomorphism. □

Lemma A.39. (Schur's Lemma II.) Let V be a simple module of an algebra A over $\mathbb{C}$. Then $\operatorname{Hom}_A(V,V)$ $(= \mathrm{C}_{\operatorname{End}(V)}(A_V))$ consists solely of scalar multiplications.

Proof. It goes without saying that multiplication by scalars are homomorphisms from V to V itself. Given $\varphi \in \operatorname{Hom}_A(V,V)$, it follows from the fact that φ by definition must be a linear transformation of a vector space unto itself that φ has an eigenvalue λ with a non-zero eigenvector v such that

$$\varphi(v) = \lambda v.$$

This then means that $\psi := \varphi - \lambda$ is a homomorphism from V to itself that is not invertible, because $\psi(v) = 0$. Since it's not invertible, by Lem. A.38, it must be the zero-map. Then $0 = \varphi(w) - \lambda w$ and $\varphi(w) = \lambda w$. This finishes the proof. □

Next, we wish to look more specifically at group algebras. As promised, we now finally revisit the notion of the orthogonal complement.

Lemma A.40. Let G be a finite group and let V be an $\mathbb{F}[G]$-module. If V admits an inner product $\langle\cdot,\cdot\rangle$ which is invariant under the action of every $g \in G$ (G-invariant), then V is semisimple.

Proof. We show that for every submodule $W \subseteq V$, its orthogonal complement with respect to $\langle\cdot,\cdot\rangle$, $W^\perp$, is a $\mathbb{F}[G]$-submodule. This is done by showing that if $u \in W^\perp$, then $a \cdot u \in W^\perp$ as well for every $a \in \mathbb{F}[G]$.

If $a = 0$, then $av = 0$, which evidently is in $W^{\perp}$. If $a \neq 0$, then we are looking at an element of the form

$$a = \sum_{i=1}^{|G|} a_i g_i.$$

We now need to show that $\langle au, w \rangle = 0$ for every $u \in W^{\perp}$ and every $w \in W$. From the definitions of inner product and the module of an algebra, we have

$$\langle a \cdot u, w \rangle = \langle \sum_{i=1}^{|G|} a_i g_i \cdot u, w \rangle = \sum_{i=1}^{|G|} a_i \langle g_i \cdot u, w \rangle.$$

Thus, if we can show that for every $g \in G$, $\langle g \cdot u, w \rangle = 0$, the proof is complete. From G-invariance of the inner product, it follows that

$$\langle g \cdot u, w \rangle = \langle g^{-1} g \cdot u, g^{-1} \cdot w \rangle = \langle u, g^{-1} \cdot w \rangle = 0,$$

where the final equality follows from $u \in W^{\perp}$, and W being an $\mathbb{F}[G]$-module, so $g^{-1} \cdot w \in W$. We are done. □

Unfortunately, not every group G is such that it admits a G-invariant inner product for all $\mathbb{F}[G]$-modules. However, if G is a finite group, things are different.

Lemma A.41. If G is a finite group, then every $\mathbb{F}[G]$-module admits a G-invariant inner product.

Proof. Let V be $\mathbb{F}[G]$-module, and let $\langle \cdot, \cdot \rangle$ be an inner product on V that is not necessarily G-invariant. Then the inner product $\langle \cdot, \cdot \rangle'$ defined by

$$\langle v, w \rangle' = \sum_{g \in G} \langle g \cdot v, g \cdot w \rangle$$

is G-invariant. It is easily verified that $\langle \cdot, \cdot \rangle'$ obeys each of the conditions A.4 (i)-(iv). Furthermore, given $g, h, k \in G$, $hg = kg$ if and only if $h = k$, it follows that

$$\langle g \cdot v, g \cdot w \rangle' = \sum_{h \in G} \langle hg \cdot v, hg \cdot w \cdot \rangle = \sum_{\ell \in G} \langle \ell \cdot v, \ell \cdot w \rangle = \langle v, w \rangle', \quad \forall g \in G.$$

□

The results of Lems. A.40 and A.41 taken together forms Maschke's theorem, which lies at the foundation of (as we shall see) the representation theory of finite groups.

Theorem A.42. (Maschke's Theorem.) Let G be a finite group. Then every $\mathbb{F}[G]$-module is semisimple.

Corollary A.43. The group algebra of every finite group is semisimple.

3. M-homogeneous submodules, Central Idempotents, and Wedderburn

We now construct yet another structure.

Definition A.44. (M-homogeneous submodule.) Let V be a semisimple A-module and let M be a simple A-module. Then the sum of all simple submodules of V isomorphic to M is called the *M-homogeneous submodule of* V, denoted $M(V)$.

In line with [52], when we are looking at the specific case of $V = A^{\circ}$, we shall denote the M-homogeneous submodule of A° by $M(A)$ rather than $M(A^{\circ})$ for notational economism.

Lemma A.45. Let V be an A-module, and let M be an arbitrary simple A-module. Then $M(V)$ is a $\mathrm{C}_{\mathrm{End}(V)}(A_V)$-submodule of V.

Proof. Given V, it has the structure of a $\mathrm{C}_{\mathrm{End}(V)}(A_V)$-module under the action that for every $\varphi \in \mathrm{C}_{\mathrm{End}(V)}(A_V) = \mathrm{Hom}_A(V, V)$, $\varphi \cdot v = \varphi(v)$. What we need to show is that given $\theta \in \mathrm{C}_{\mathrm{End}(V)}(A_V)$, $\theta(M(V)) \subseteq M(V)$. Since $M(V)$ is the sum of all simple submodules of V isomorphic to M, if we can show that given an M-isomorphic submodule W or V, $\theta(W) \subseteq M(V)$ we are done. While θ acts on all of V, since we're only interested in its action of W, we may, without fearing running into problems later, restrict its domain to W and instead focus on $\theta_W \in \mathrm{Hom}_A(W, V)$. Being a module homomorphism, its kernel and image must be submodules of its domain and co-domain. Since W is simple, $\ker\theta \in \{\{0\}, W\}$. If it is the latter, then θ maps every element of W to 0, which lies in $M(V)$ and we are done. If it is the former, then by the first isomorphism theorem, W (the domain) is isomorphic to the image, that is, $\theta(W)$. By transitivity of isomorphisms, $\theta(W)$ is then isomorphic to M, and so is contained in $M(V)$. Thus, $M(V)$ is closed under the action of $\mathrm{C}_{\mathrm{End}(V)}(A_V)$, and so a $\mathrm{C}_{\mathrm{End}(V)}(A_V)$-module. □

Lemma A.46. Let V be a semisimple A-module. As such, by Cor. A.34, it may be written as $V \cong \bigoplus_i W_i$, where W_i are distinct simple submodules of V. Let M be any simple A-module. $M(V)$ consists solely of the sum of those W_i that are isomorphic to M.

Proof. By definition, $\sum_{W_i \cong M} W_i \subseteq M(V)$. Since the W_i are distinct, $\sum_i W_i = V$. Take a generic module $W \subseteq V$ such that $W \cong M$. Then, since $W = W \cap V = W \cap (\sum_i W_i) = \sum_i (W \cap W_i)$, $W \cap W_i$ cannot be zero for all i. If $W \cap W_j \neq 0$, then, since both W and W_j are simple modules, their intersection must contain both all of W and all of W_j. In other words, $W = W_j$, and so $W_j \cong M$. By extension, $W \subseteq \{\sum_i W_i | W_i \cong M\}$. Since $M(V)$ is the sum of all such W, it follows that $M(V) \subseteq \sum_{W_i \cong M} W_i$. Thus, the lemma holds. □

Corollary A.47. Let V be a semisimple A-module, and let M and N be two non-isomorphic A-modules. Then $M(V) \cap N(V) = \{0\}$.

Definition A.48. Let $\mathscr{M}(A)$ be a set of simple A-modules such that every conceivable simple A-module is isomorphic to exactly one element in the set. $\mathscr{M}(A)$ is then called a *representative set of modules* for the algebra A.

With this definition, we may extend A.47 into a more all-encompassing form.

Corollary A.49. Let V be a semisimple A-module. Then it is isomorphic to a direct sum of its M-homogeneous parts, varying M over $\mathscr{M}(A)$,

$$V \cong \bigoplus_{M \in \mathscr{M}(A)} M(V).$$

Lemma A.50. Let A be a semisimple algebra. Then every simple A-module is isomorphic to a submodule of A°.

Proof. Let V be a simple A-module and let v be a nonzero element of V. Then, we may construct the module homomorphism $\theta : A^\circ \to V$ by $a \mapsto a \cdot v$. The image of θ must be all of V since V is a simple module and the image cannot be zero, since evidently $1_{A^\circ} \in A^\circ$ maps to $v \in V$ which as established is nonzero. Thus, by A.37,

$$A^\circ / \ker\theta \cong V.$$

$\ker\theta$ is a submodule of A°, and since A° is a semisimple module, there exists $U \subseteq A^\circ$ such that $\ker\theta \oplus U \cong V$. By A.27, $A^\circ / \ker\theta \cong U$. Thus $U \cong V$, and the lemma is proven. □

Corollary A.51. Given any semisimple algebra A, $\mathscr{M}(A)$ is a finite set.

PROOF. Every simple A-module M is isomorphic to a submodule of A°, and so $M(A) \neq 0$ for all M. Since $A^\circ \cong \bigoplus_{M \in \mathscr{M}(A)} M(A)$ is finite dimensional, it follows that $\mathscr{M}(A)$ must be a finite set. □

We now have enough background to prove Wedderburn's theorem, which we state and prove in the form it is presented in [52].

THEOREM A.52. (WEDDERBURN.) Let A be a semisimple algebra, and let M be a simple A-module. Then,

(a) $M(A)$ is an ideal of A;
(b) If W is a simple A-module, then it is annihilated by $M(A)$ unless $W \cong M$, that is, for every $w \in W$ and every $m \in M(A)$, $m \cdot w = 0$;
(c) The map $\phi : M(A) \to A_M$, $x \mapsto x_M$ is injective;
(d) $M(A)$ is a minimal ideal.

PROOF. (a) To accomplish this part of the proof, we need to demonstrate that for every $a \in A$, $a \cdot M(A) \subseteq M(A)$ *and* $M(A) \cdot a \subseteq M(A)$. Since $M(A)$ is an A-module, for every $m \in M(A)$, $a \cdot m \in M(A)$, and so multiplication from the left is thus handled. Pertaining to multiplication from the right, let us for each $a \in A^\circ$ create a map $\theta_a : A^\circ \to A^\circ$, $b \mapsto b \cdot a$. Evidently, this map belongs to $\mathrm{Hom}_A(A^\circ, A^\circ) = \mathrm{C}_{\mathrm{End}(A^\circ)}(A_{A^\circ})$. Now, we have already established that $M(A)$ is a $\mathrm{C}_{\mathrm{End}(A^\circ)}(A_{A^\circ})$-module in A.45, so it follows that $M(A) \cdot a = \theta_a(M(A)) \subseteq M(A)$. Thus, $M(A)$ is indeed an ideal in A.

(b) It has already been established in A.47 that if $W \ncong M$, then $W(A) \cap M(A) = \{0\}$. Since $M(A)$ and $W(A)$ are both ideals of A by the previous point, their multiplication by every element of one with every element of the other must lie in both of them. The only way this is possible is if $m \cdot w = w \cdot m = 0$ for every $m \in M(A)$, $w \in W(A)$. Thus $M(A)$ and $W(A)$ annihilate one another. By A.50, if W is a simple A-module, then there exists a submodule $W_\circ \subseteq A^\circ$ such that $W_\circ \cong W$. This means there is an isomorphism map $\varphi : W_\circ \to W$. Given $m \in M(A)$, $w \in W$, we then have

$$0 = \varphi(0) = \varphi(m \cdot w) = m \cdot \varphi(w),$$

that is, $M(A)$ annihilates all of W.

(c) From the above, it follows that x_W maps every element $x \in M(A)$ to 0 if $W \ncong M$. Consequently, from the sum decomposition $A \cong \bigoplus_{M \in \mathscr{M}(A)} M(A)$, it follows that the only part of y_M that actually maps to anything nonzero (for $y \in A$) is the component of y that lies in $M(A)$. We call this x_M. Thus we may write $y_M = x_M$. Thus, ϕ maps $M(A)$ unto A_M. To prove injectivity, we show that the kernel of ϕ is trivial. If $x \in M(A)$ and $x_M = 0$, then by (b), x annihilates not just every element in every module isomorphic to M, but every module non-isomorphic to M as well, and thus all of A°. Consequently, $x \cdot A^\circ$. This is only possible if $x = 0$, and so the kernel is indeed trivial.

(d) We prove this by proving that every subideal of $M(A)$ that is not $M(A)$ itself must be the zero ideal. Take an ideal $I \subset M(A)$. This ideal is, as noted at the beginning of the appendix, an A-module. Since $M(A)$ is a sum of A-modules isomorphic to M, then there must exist at least one nonzero A-module $M_0 \subset M(A)$, $M_0 \cong M$ such that $M_0 \not\subseteq I$. Since M_0 is a simple module, $M_0 \not\subseteq I$ implies that $M_0 \cap I = \{0\}$. Since I is an ideal, then for every $i \in I$, $m \in M_0$, we must have $i \cdot m = m \cdot i = 0$. That is, I annihilates M_0. By (b) it must then annihilate every module isomorphic to M_0 as well, that is, the entirety of $M(A)$. By (c), this means that $I = \{0\}$, and we are done.

□

The annihilation bit is of interest, as it implies that the unity element in a semisimple algebra A can be partitioned up into a set of "subunities" so to speak, each one being the unity element in their particular submodule $M_i(A)$,

$$1_A = \sum_{i=1}^{|\mathscr{M}(A)|} e_i.$$

These "subunities" are *central idempotents* in A. *Central*, in that they commute with every element in the algebra and so are in the centre, and *idempotent* in that each and every e_i obeys $e_i = e_i^2 = e_i^3 = \dots$. They turn out to be of significant interest to us in the main text.

Finally, we have enough understanding of the basic structures of algebras to tackle the question we raised earlier in this appendix, given an algebra A and an A-module V, what is the centralizer of this centralizer, $\mathrm{C}_{\mathrm{End}(V)}(\mathrm{C}_{\mathrm{End}(V)}(A_V))$?

4. The Double Centralizer Theorem

THEOREM A.53. (DOUBLE CENTRALIZER THEOREM.) Let A be a semisimple algebra and M a simple A-module. Then $\mathrm{C}_{\mathrm{End}(M)}(\mathrm{C}_{\mathrm{End}(M)}(A_M)) = A_M$.

PROOF. By A.50, every simple A-module is isomorphic to a submodule of A°, and so we might just assume that M in this case is a submodule of A°, since due to isomorphism, the results we derive for such a submodule would apply to any other module isomorphic to it.

As noted way back, $A_M \subseteq \mathrm{C}_{\mathrm{End}(M)}(\mathrm{C}_{\mathrm{End}(M)}(A_M))$ due to the definition of what a centralizer is, so that is already taken care of. All that remains it to prove that $\mathrm{C}_{\mathrm{End}(M)}(\mathrm{C}_{\mathrm{End}(M)}(A_M)) \subseteq A_M$. That is, that for every $\varphi \in \mathrm{C}_{\mathrm{End}(M)}(\mathrm{C}_{\mathrm{End}(M)}(A_M))$, there exists an element $u \in A$ such that $\varphi(m) = u \cdot m$.

Let θ be an arbitrary element in $\mathrm{C}_{\mathrm{End}(M)}(\mathrm{C}_{\mathrm{End}(M)}(A_M))$, meaning that

$$\theta(\alpha(m)) = \alpha(\theta(m)), \quad \forall \alpha \in \mathrm{C}_{\mathrm{End}(M)}(A_M),\ m \in M.$$

Given $m \in M$, we define the vector space endomorphism $\alpha_m : M \to M$ by $n \mapsto n \cdot m$. This vector space endomorphism actually turns out to be a full-fledged module homomorphism, as for every $a \in A$,

$$\alpha_m(a \cdot x) = (a \cdot x) \cdot m = a \cdot (x \cdot m) = a \cdot \alpha_m(x),$$

so we can safely assert that $\alpha_m \in \mathrm{Hom}_A(M, M) = \mathrm{C}_{\mathrm{End}(M)}(A_M)$. Therefore, since $\theta \in \mathrm{C}_{\mathrm{End}(M)}(\mathrm{C}_{\mathrm{End}(M)}(A_M))$, given $m, n \in M$, it follows that

$$\theta(n \cdot m) = \theta(\alpha_m(n)) = \alpha_m(\theta(n)) = \theta(n) \cdot m. \tag{A.54}$$

Now, taking an arbitrary nonzero element $n \in M$, we can form a principal ideal AnA. Since $n \in M$ and $M \subseteq M(A)$, $M(A)$ being an ideal in its own right by A.52 (a), $AnA \subseteq M(A)$. However, by A.52 (d), $M(A)$ is minimal, and so $AnA = M(A)$. This leads to a remarkable insight: Given any non-zero vector $n \in M$, every element $x \in M(A)$ may be expressed as $x = \sum_i a_i \cdot n \cdot b_i$ for some set of a_i's and b_i's. In particular, this holds true for the central idempotent associated with $M(A)$, which acts as the identity within $M(A)$. Call this e_M. Then, $e_M = \sum_i a_i \cdot n \cdot b_i$ for some $\{a_i, b_i\}$. This in turns means that given arbitrary $m \in M$, we have

$$m = e_M \cdot m = \left(\sum_i a_i \cdot n \cdot b_i\right) \cdot m = \sum_i (a_i \cdot n) \cdot (b_i \cdot m).$$

Noting that M is an A-module, $(a_i \cdot n), (b_i \cdot m) \in M$ for all $a_i, b_i \in A$. We can then make use of (A.54) to get

$$\begin{aligned}
\theta(m) &= \theta\left(\sum_i (a_i \cdot n) \cdot (b_i \cdot m)\right) \\
&= \sum_i \theta\left((a_i \cdot n) \cdot (b_i \cdot m)\right) \\
&= \sum_i \theta\left((a_i \cdot n)\right) \cdot (b_i \cdot m) \\
&= \left(\sum_i \theta\left((a_i \cdot n)\right) \cdot b_i\right) \cdot m,
\end{aligned}$$

that is $\theta(m) = u \cdot m$ where $u = \sum_i \theta\left((a_i \cdot n)\right) \cdot b_i$. The inclusion is proven and the Double Centralizer Theorem follows. □

Corollary A.55. Let $\mathbb{C}[G]$ be a group algebra of some finite group, and let M be a simple module of this group algebra. Then $(\mathbb{F}[G])_M$, the set of all maps $\phi_x : M \to M$, $\phi_x(m) = x \cdot m$, $x \in \mathbb{F}[G]$, is isomorphic to the set of $\dim(M) \times \dim(M)$-matrices over $\mathbb{F}$, $\mathrm{Mat}_{\dim(M)\times\dim(M)}(\mathbb{F})$.

Proof. By Maschke's theorem (see Thm. A.42), $\mathbb{F}[G]$ is a semisimple algebra. By the Double Centralizer theorem (see Thm. A.53), $(\mathbb{F}[G])_M = \mathrm{C}_{\mathrm{End}(M)}(\mathrm{C}_{\mathrm{End}(M)}((\mathbb{F}[G])_M))$. By Schur's lemma (see Lem. A.39), $\mathrm{C}_{\mathrm{End}(M)}((\mathbb{F}[G])_M) = \mathrm{Hom}_{\mathbb{F}[G]}(M, M) = \mathbb{F} \cdot 1$. By definition, multiplication by scalars commutes with every other element of $\mathrm{End}(M)$, and so $\mathrm{C}_{\mathrm{End}(M)}(\mathbb{F} \cdot 1) = \mathrm{End}(M)$. By elementary linear algebra, $\mathrm{End}(M) \cong \mathrm{Mat}_{\dim(M)\times\dim(M)}(\mathbb{F})$. The corollary is proven. □

Specifically, this means that an n-dimensional irreducible representation of a group algebra $\mathbb{F}[G]$ consists of the entire set of $n \times n$-matrices over the field $\mathbb{F}$. This is actually a fairly well-known result, and is often used without any justification given for it. As the reader can see, however, it's actually far from trivial to prove it. Indeed, this entire appendix was just added to prove that very specific thing.

Bibliography

[1] Paul S. Aspinwall et al. *Dirichlet Branes and Mirror Symmetry*. Vol. 4. American Mathematical Society, 2009.

[2] John McKay. "Graphs, Singularities, and Finite Groups". In: *Proceedings of Symposia in Pure Mathematics*. Ed. by Bruce Cooperstein and Geoffrey Mason. Vol. 37. American Mathematical Society, 1980, pp. 183–186.

[3] Plato and pseudopigraphers. *Plato: Complete Works*. Ed. by John M. Cooper. Ed. by D. S. Hutchinson. Trans. by Donald J. Zeyl et al. Indianapolis, Indiana, United States: Hackett Publishing Company, Inc., 1997.

[4] Walter Burkert. *Lore and Science in Ancient Pythagoreanism*. Harvard University Press, 1972.

[5] Peter Thomas Geach. *Logic Matters*. Vol. 222. University of California Press, 1980.

[6] Hannah Mark. *Classifying Finite Subgroups of $SO(3)$*. 2011. URL: http://www.math.uchicago.edu/~may/VIGRE/VIGRE2011/REUPapers/MarkH.pdf.

[7] Nakahara Mikio. *Geometry, Topology and Physics*. 2nd ed. Milton Park, Abingdon, United Kingdom: Taylor & Francis Group, 2003.

[8] Brian Hall. *Lie groups, Lie Algebras, and Representations: An Elementary Introduction*. Vol. 222. Springer, 2015.

[9] Chris J. Isham. *Modern Differential Geometry for Physicists*. 2nd ed. Vol. 61. World Scientific Publishing Co. Pte. Ltd., 1999.

[10] J. R. Cornwell. *Group Theory in Physics*. Vol. 1. 1984.

[11] Pierre Antoine Grillet. *Abstract algebra*. 2nd ed. Vol. 242. Springer Science & Business Media, 2007.

[12] Terence Tao. *Two small facts about Lie groups*. 2011. URL: https://terrytao.wordpress.com/2011/06/25/two-small-facts-about-lie-groups/.

[13] Howard Georgi. *Lie algebras in particle physics: from isospin to unified theories*. Vol. 54. Westview press, 1999.

[14] Bruce E. Sagan. *The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions*. Vol. 203. Springer Science & Business Media, 2013.

[15] Isaac Ottoni Wilhelm. *Some Elementary Results in Representation Theory*. 2010. URL: http://www.math.uchicago.edu/~may/VIGRE/VIGRE2010/REUPapers/Wilhelm.pdf.

[16] Volodymyr "Walter" Mazorchuk. "Representation Theory of Finite Groups". Unpublished lecture notes. 2016.

[17] Michael Tinkham. *Group Theory and Quantum Mechanics*. Courier Corporation, 2003.

[18] John D. Dixon. "Constructing Representations of Finite Groups". In: *Groups and Computation* 11 (1993), pp. 105–112.

[19] Vahid Dabbaghian-Abdoly. *An Algorithm to Construct Representations of Finite Groups*. Carleton University, 2003.

[20] Joe Harris. *Algebraic Geometry: A First Course*. Vol. 133. Springer Science & Business Media, 2013.

[21] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Springer Science & Business Media, 2013.

[22] David Eisenbud. *Commutative Algebra: with a view toward algebraic geometry*. Vol. 150. Springer Science & Business Media, 2013.

[23] Andreas Gathmann. *Algebraic Geometry*. 2002. URL: https://pdfs.semanticscholar.org/e921/4a30c8754b3285a0e2046549c2d218c38a63.pdf.

[24] Judy Holdener. *Algebraic Geometry: Class Handouts*. 2013. URL: https://www.math.cornell.edu/~dmehrle/notes/old/alggeo/.

[25] Tsit Yuen Lam. *A First Course in Noncommutative Rings*. Vol. 131. Springer Science & Business Media, 2013.

[26] Oscar Zariski. "A New Proof of Hilbert's Nullstellensatz". In: *Bulletin of the American Mathematical Society* 53.4 (1947), pp. 362–368.

[27] Raf Bocklandt. *Kleinian Singularities*. 2006. URL: https://staff.fnwi.uva.nl/r.r.j.bocklandt/notes/kleinian.pdf.

[28] Jan Draisma and Dion Gijswijt. *Invariant Theory with Applications*. 2009. URL: http://www.win.tue.nl/~jdraisma/teaching/invtheory0910/lecturenotes12.pdf.

[29] Thomas Hawkins. *Emergence of the theory of Lie groups: An essay in the history of mathematics 1869–1926*. Springer Science & Business Media, 2012.

[30] Nagata Masayoshi. "On the 14-th problem of Hilbert". In: *American Journal of Mathematics* 81.3 (1959), pp. 766–772.

[31] Edward F. Hughes. *Invariant Theory and David Hilbert*. 2012. URL: https://edwardfhughes.wordpress.com/2012/08/05/invariant-theory-and-david-hilbert/.

[32] Colin McLarty. "Theology and its discontents: David Hilbert's foundation myth for modern mathematics". In: *Mathematics and narrative* (2011).

[33] Felix Klein. *Lectures on the Icosahedron*. Trans. by George Gavin Morrice. London, United Kingdom: Trübner & Co., Ludgate Hill, 1888.

[34] Igor Dolgachev. *McKay correspondence. Winter 2006/07*. 2009. URL: http://www.math.lsa.umich.edu/~idolga/McKaybook.pdf.

[35] Ferdi Aryasetiawan. *Group Theory*. 1997. URL: http://www.matfys.lth.se/education/FYS256/aryasetiawan.pdf.

[36] Victor G Kac. *Infinite-dimensional Lie algebras*. Vol. 44. Cambridge university press, 1994.

[37] Gerardo González-Sprinberg and Jean-Louis Verdier. "Points doubles rationnels et représentations de groupes". In: *CR Acad. Sci. Paris Sér. I Math* 293.2 (1981), pp. 111–113.

[38] Gerard Gonzalez-Sprinberg and J-L Verdier. "Construction géométrique de la correspondance de McKay". In: *Annales Scientifiques de l'École Normale Supérieure*. Vol. 16. 3. Elsevier. 1983, pp. 409–449.

[39] Peter Slodowy. "Platonic solids, Kleinian singularities, and Lie groups". In: *Algebraic geometry*. Springer, 1983, pp. 102–138.

[40] Graham Leuschke. *The McKay Correspondence*. 2006. URL: http://www.leuschke.org/uploads/McKay-total.pdf.

[41] Robert Steinberg. "Kleinian singularities and unipotent elements". In: *Proceedings of Symposia in Pure Mathematics*. Ed. by Bruce Cooperstein and Geoffrey Mason. Vol. 37. American Mathematical Society, 1980, pp. 265–270.

[42] Bertram Kostant. "The McKay correspondence, the Coxeter element and representation theory". In: *Elie Cartan et le mathématiques d'ajourd'hui* (1985), pp. 209–255.

[43] Egbert Brieskorn. "Singular elements of semi-simple algebraic groups". In: *Actes du Congres International des Mathématiciens (Nice, 1970)*. Vol. 2. 1970, pp. 279–284.

[44] Martin Herschend. "To: Max Lindh; From: Martin Herschend". Private correspondence. 2018.

[45] Joris van Hoboken. "Platonic solids, binary polyhedral groups, Kleinian singularities and Lie algebras of type A, D, E". MA thesis. University of Amsterdam, 2002. URL: http://math.ucr.edu/home/baez/joris_van_hoboken_platonic.pdf.

[46] Peter Slodowy. *Simple Singularities and Simple Algebraic Groups*. Vol. 815. Springer, 2006.

[47] Ito Yukari and Miles Reid. "The McKay correspondence for finite subgroups of $\mathrm{SL}(3, \mathbb{C})$". In: *Higher Dimensional Complex Varieties: Proceedings of the International Conference held in Trento, Italy, June 15-24, 1994*. Walter de Gruyter. 1996, p. 221.

[48] Tamar Friedmann. "Orbifold singularities, Lie algebras of the third kind (LATKes), and pure Yang–Mills with matter". In: *Journal of Mathematical Physics* 52.2 (2011), p. 022304.

[49] Valerii Terent'evich Filippov. "n-Lie algebras". In: *Siberian Mathematical Journal* 26.6 (1985), pp. 879–891.

[50] Tom Bridgeland, Alastair King, and Miles Reid. “The McKay correspondence as an equivalence of derived categories”. In: *Journal of the American Mathematical Society* 14.3 (2001), pp. 535–554.

[51] Miles Reid. “McKay correspondence”. In: *arXiv preprint alg-geom/9702016* (1997).

[52] I. Martin Isaacs. *Character theory of finite groups*. Vol. 69. Courier Corporation, 1994.