Syracuse University

MAT 830:
The McKay Correspondence

Professor: Dr. Graham Leuschke
Notes By: Caleb McWhorter

Fall 2018

Last Updated: November 13, 2018

Contents

0 Introduction

The M^{c}Kay Correspondence (pronounced mc-eye) is an umbrella for a family of correspondences linking finite groups, resolutions of singularities of algebraic varieties, Lie Algebras, Character Theory, Invariant Theory, Representations of Quivers, and Cohen-Macaulay modules. It will not be our goal to see any particular connection in depth, but rather a surface level introduction to these correspondences generally, with a strong emphasis on examples.

> *"The problem is to find a common origin of the ADE Classification Theorems, and to substitute a priori proofs to a posteriori verifications of the parallels of the classification.*
>
> – V.I. Arnold ,1976

The organizational scheme for the M^{c}Kay Correspondence is the Coxeter-Dynkin diagrams. The Coxeter-Dynkin ADE diagrams classify objects in each of the areas above, plus subadditive functions, root systems, Weyl groups, String Theory, Cluster Algebras, etc.. An example theorem demonstrating the M^{c}Kay Correspondence is the following, due to M^{c}Kay , Auslander, Reiten, Artin, Verdier, Gonzalzez-Springber, Herzog, et al.,

Theorem 0.1. *Let G be a small finite subgroup of $\mathrm{SL}_2(\mathbb{C})$, acting linearly on $S = \mathbb{C}[x, y]$. Denote by $R = S^G$ the ring of invariants. Then there is a one-to-one correspondence between the following:*

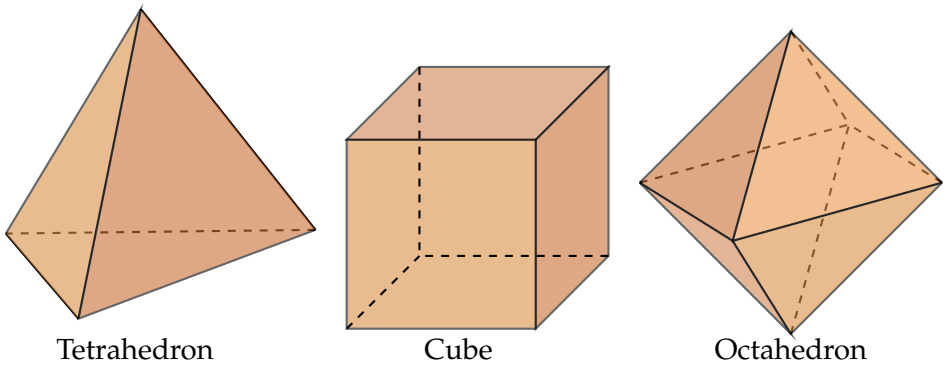
- *Irreducible representations of G*
- *Indecomposable reflexive R-modules*
- *Irreducible Components of the exceptional fiber of minimal resolution of singularities of* Spec R.

These correspondences extend to isomorphisms between

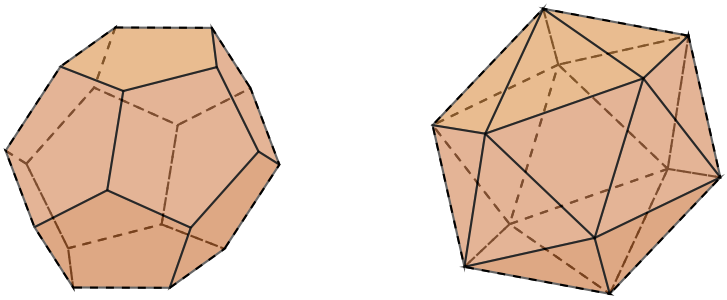
- *the M^{c}Kay Correspondence of G*
- *the Auslander-Reiten quiver of R*
- *the dual desingularization graph of* Spec R.

1 Platonic Solids and Finite Groups of Matrices

A Platonic solid is a regular, convex polyhedron, constructed by congruent regular polygonal faces with the same number of faces meeting at each vertex; that is, the platonic solids are defined by the property that the faces are each convex and pairwise congruent. The solids shown below are the only five solids satisfying these properties.



Tetrahedron Cube Octahedron



Dodecahedron Icosahedron

Proposition 1.1. *The solids above are the only possible Platonic solids.*

Proof. Suppose a solid has faces with p sides and q faces meeting at each vertex. We write this as a pair $\{p, q\}$, called the Schläfli symbol. The external angles of each face add to 2π radians, as is the case with any convex polygon. Each exterior angle is then $\frac{2\pi}{p}$ radians. The internal angles are then $\pi - \frac{2\pi}{p}$. So around each vertex, the sum of the angles is $q(\pi - \frac{2\pi}{p})$. This angle cannot be larger than 2π as the faces are concave if and only if $\dfrac{2}{p} + \dfrac{2}{q} > 1$, and we require convex faces. Furthermore, this sum cannot be 2π for then the solid would be flat, i.e. a tiling of the plane. Therefore, we have the relation

$$q\left(\pi - \frac{2\pi}{p}\right) < 2\pi.$$

$\{p,q\}$	Name	F	E	V
$\{p,2\}$	dihedron	2	q	q
$\{2,q\}$	hosohedron	p	p	2
$\{3,3\}$	tetrahedron	4	6	4
$\{3,4\}$	octahedron	8	12	6
$\{4,3\}$	cube	6	12	8
$\{3,5\}$	icosahedron	20	30	12
$\{5,3\}$	dodecahedron	12	30	20

The integer solutions are $\{p,2\}$, $\{2,q\}$ or $\{3,3\}$, $\{3,4\}$, or $\{3,5\}$. Then Euler's Formula $V-E+F=1$ allows one to compute V, E, F, as found in the table. □

Notice that the above proof is merely a uniqueness proof and does *not* show the existence of these solids. We shall prove existence by classifying the rotational symmetry groups of these solids. We shall find

- the dihedral group, D_{2k}, of the symmetries of the dihedron/hosohedron.
- the tetrahedral group, $\mathbb{T}$, of the 12 rotational symmetries of a tetrahedron.
- the octahedral group, $\mathbb{O}$, of the 24 rotational symmetries of the octahedron.
- the icoahedral/dodecahedral group, $\mathbb{I}$, of 60 the rotational symmetries of the icosahedron/dodecahedron

Note that dual pairs[1] of polyhedra have the same rotational symmetry groups. Furthermore, these will all be familiar groups. For example, we shall find $\mathbb{T} \cong A_4$ and $\mathbb{O} \cong S_4$. This follows from the fact that symmetries of the faces of one polyhedron correspond to symmetries of the centers of their faces, and vice versa. For instance, the cube and the octahedron both have the same symmetry group, $\mathbb{O} \cong S_4$, because they are dual. From the table in Proposition 1.1, we can see that the dihedron and hosohedron are dual, the octahedron and cube are dual, the icosahedron and dodecahedron are dual, and the tetrahedron is self-dual. Finally, the groups D_{2k}, $\mathbb{T}$, $\mathbb{O}$, and $\mathbb{I}$, along with the cyclic groups C_n for $n \in \mathbb{N}$, are the *only* finite groups of rotations of $\mathbb{R}^3$.

Theorem 1.1. *Along with the degenerate case of the cyclic group C_k for any $k \geq 1$ corresponding to rotation of $\mathbb{R}^3$ by $\frac{2\pi}{k}$, the groups D_{2k}, $\mathbb{T}$, $\mathbb{O}$, and $\mathbb{I}$ are all of the finite groups of rotations of $\mathbb{R}^3$.*

[1] The dual of a polyhedron P has a vertex at the center of each face of P, and two vertices joined by an edge if the faces abut each other.

1.1 Matrix Groups

To classify the finite groups of rotational symmetries, we begin by recalling a few definitions.

Definition (Orthogonal Group)**.** The orthogonal group, $O(n)$, is the set of all invertible orthogonal matrices, i.e. $O(n) := \{A \in \mathrm{GL}_n(\mathbb{R})\colon AA^T = I_n\}$.

Example 1.1. The following are all orthogonal matrices:

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad B = \frac{1}{3}\begin{pmatrix} 2 & -2 & 1 \\ 1 & 2 & 2 \\ 2 & 1 & -2 \end{pmatrix}$$

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

◁

A routine exercise verifies that the orthogonal group is also equivalent to any of the following:

$$\begin{aligned} O(n) &:= \{A \in \mathrm{GL}_n(\mathbb{R})\colon AA^T = I_n\} \\ &= \{A\colon |Ax| = |x| \text{ for all } x \in \mathbb{R}^n\} \\ &= \{A\colon Ax \cdot Ay = x \cdot y, \text{ for all } x, y \in \mathbb{R}^n\} \\ &= \{A\colon \text{ rows of } A \text{ form orthonormal basis for } \mathbb{R}^n\} \\ &= \{A\colon \text{ columns of } A \text{ form orthonormal basis for } \mathbb{R}^n\} \\ &= \{\text{set of linear isometries of } \mathbb{R}^n\}. \end{aligned}$$

Note that we have defined $O(n)$ in terms of the symmetric bilinear form $\langle A, B\rangle = AB^T$. Generally, if $\langle\cdot,\cdot\rangle$ is a symmetric bilinear form then you can define the orthogonal group of the form $\langle\cdot,\cdot\rangle$ to be $\{A \in \mathrm{GL}(\mathbb{R})\colon \langle Ax, Ay\rangle = \langle x, y\rangle \text{ for all } x, y \in \mathbb{R}\}$. Observe also that from the relation $AA^T = I_n$, we obtain $\det(AA^T) = 1$. Recall that $\det(AB) = \det(A)\det(B)$, and $\det(A) = \det(A^T)$. It then follows that $\det(A)^2 = 1$, and then $\det A = \pm 1$. A special subset of these matrices are our next group of interest.

Definition (Special Orthogonal Group)**.** The special orthogonal group, $\mathrm{SO}(n)$, is the subgroup of $O(n)$ of matrices having determinant 1, i.e. $\mathrm{SO}(n) := \{A \in \mathrm{GL}_n(\mathbb{R})\colon AA^T = I_n, \det A = 1\}$.

Example 1.2. The case of $n = 1$ is dull, consisting only of the identity matrix. The case of $n = 2$ is a bit more interesting. Suppose that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SO}(2) \subseteq O(2)$. Since $A \in O(2)$, we know that the columns of A are orthogonal, giving

$$\begin{pmatrix} a \\ c \end{pmatrix} \begin{pmatrix} b \\ d \end{pmatrix}^T = 0.$$

A simple calculation shows that $\begin{pmatrix} a \\ c \end{pmatrix} \begin{pmatrix} c \\ -a \end{pmatrix}^T = 0$. But then by linear independence, $\begin{pmatrix} b \\ d \end{pmatrix}$ must be a multiple of $\begin{pmatrix} c \\ -a \end{pmatrix}$. But these are also unit vectors, so the multiplier is ± 1. This gives two possible cases for A:

$$A = \begin{pmatrix} a & -c \\ c & a \end{pmatrix} \text{ or } \begin{pmatrix} a & c \\ c & -a \end{pmatrix}.$$

Since $A \in \mathrm{SO}(2)$, we know that $\det A = 1$. This gives $a^2 + c^2 = 1$. Then we can find an angle $\theta \in [0, 2\pi)$ so that $a = \cos\theta$ and $c = \sin\theta$. Using this in our possibilities above, we have

$$A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \text{ or } \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

While the left matrix is an element of $\mathrm{SO}(2)$, the other has determinant -1. Therefore, we must have $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, a rotation by θ counterclockwise about the origin. The second matrix on the right above corresponds to the reflection across the line at angle $\theta/2$ through the origin. Therefore, the group $\mathrm{SO}(2)$ is precisely the group of rotations in the plane. Similarly, $\mathrm{SO}(3)$ is the group of rotations for three-dimensional space, see Theorem 1.3. ◁

Definition (Rotation of $\mathbb{R}^n$)**.** Let $n > 2$. A rotation of $\mathbb{R}^n$ is a linear map $\phi : \mathbb{R}^n \to \mathbb{R}^n$ satisfying

- ϕ fixes a line ℓ through the origin
- $\phi|_{\ell^\perp}$ is a rotation of the subspace orthogonal to ℓ

Sometimes the definition of rotations of $\mathbb{R}^n$ is instead given as follows: a rotation of $\mathbb{R}^n$ is a linear operator if T fixes a unit vector p, called a pole, and the restriction of T to $(\mathrm{span}(p))^\perp \cong \mathbb{R}^2$ is a rotation of $\mathbb{R}^2$. We will make use of this alternate definition later. For now, we shall prove that the finite subgroups of linear isometries of the plane are a cyclic group or a dihedral group.

Theorem 1.2. *The finite subgroups of linear isometries of the plane are a cyclic group or a dihedral group.*

Proof (Sketch). If $G \subseteq \mathrm{SO}(2)$ is a finite group, then G consists only of rotations by Example 1.2. One can check that G is generated by the rotation with smallest positive angle. Now if $G \subseteq O(2) \setminus \mathrm{SO}(2)$, then G must contain a reflection B, and $G \cap \mathrm{SO}(2) = \langle A \rangle$ will be cyclic. One then verifies that $G = \{I, A, \ldots, A^{n-1}, B, BA, \ldots, BA^{n-1}\}$. □

Corollary 1.1. $\mathrm{SO}(2)$ *consists of the rotations of* $\mathbb{R}^2$.

Proof. By Example 1.2, we know that $\mathrm{SO}(2)$ is contained in the group of rotations of $\mathbb{R}^2$. Since every rotation of $\mathbb{R}^2$ can be represented by a matrix in the form of $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$, the containment holds in the other direction. □

Note that $\mathrm{SO}(3) = \{\text{rotations of } \mathbb{R}^3\}$ but $\mathrm{SO}(n)$ strictly contains the rotations of $\mathbb{R}^n$ for $n \geq 4$. We now come to yet another theorem of Euler.

Theorem 1.3 (Euler's Theorem)**.**

$$\mathrm{SO}(3) = \{\textit{rotation of } \mathbb{R}^3\}$$

In particular, the composition of two rotations of $\mathbb{R}^3$ *is another rotation.*

Proof. Suppose T is a rotation. We can find a basis for $\mathbb{R}^3$ of the form $\mathcal{B} := \{p, x_1, x_2\}$, where p a pole for T and $\{x_1, x_2\}$ is a basis for $\mathbb{R}^2 = (\mathrm{span}(p))^{\perp}$. With respect to the basis $\mathcal{B}$,

$$[T]_{\mathcal{B}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}(3).$$

Now let $A \in \mathrm{SO}(3)$. We need find a pole for A, i.e. a nonzero vector fixed by A. If this were the case, then A must have 1 as an eigenvector. Using the fact that $\det A = 1$, we have

$$\begin{aligned} \det(A - I) &= \det(A)\det(A - I) \\ &= \det(A^T)\det(A - I) \\ &= \det(A^T A - A^T) \\ &= \det(I - A^T) \\ &= \det(I - A) \\ &= \det(-(A - I)) \\ &= (-1)^3 \det(A - I) \\ &= -\det(A - I). \end{aligned}$$

Therefore, $\det(A - I) = 0$. But then A has a unit eigenvector, say p. The restriction of A to $(\text{span}(p))^\perp$ still preserves the dot product, and so A is a rotation of $\mathbb{R}^3$ by the SO(2) case. □

Theorem 1.4. *The finite subgroups of* SO(3) *are cyclic, dihedral, or the group of rotational symmetries of a tetrahedron, an octahedron, or an icosahedron (the symmetry groups of the Platonic solids).*

Proof. Let $G \subseteq \text{SO}(3)$ be finite with $|G| = N > 1$, and define $P = \{\vec{p} \in \mathbb{R}^3 \colon \vec{p} \text{ pole of some } 1 \neq g \in G\} = \{\vec{p} \in \mathbb{R}^3 \colon |\vec{p}| = 1, g\vec{p} = g \text{ for some } g \neq 1\}$. We claim that G acts on P, i.e. if $\vec{p} \in P$, $g \in G$, then $g\vec{p} \in P$. If $\vec{p}$ is a pole of $h \in G$, then $(ghg^{-1})(g\vec{p}) = g\vec{p}$ since h fixes $\vec{p}$. But then $g\vec{p}$ is a pole of ghg^{-1}. Observe each $1 \neq g \in G$ has two poles, so $|P| < \infty$. For $\vec{p} \in P$, let $G_{\vec{p}} := \text{stab}_{\vec{p}} = \{g \in G \colon \vec{p} \text{ pole of } g\} \cup \{1_G\}$.

Now $G_{\vec{p}}$ is the set of all rotations with pole $\vec{p}$, and $G_{\vec{p}}$ is cyclic by the $n = 2$ case. Furthermore, $G_{\vec{p}}$ is generated by the smallest nonzero rotation. Let $r_{\vec{p}} := |G_{\vec{p}}|$, and $n_{\vec{p}} := |O_{\vec{p}}|$, where $O_{\vec{p}}$ is the orbit of $\vec{p}$. So $r_{\vec{p}} n_{\vec{p}} = |G|$ by the Orbit-Stabilizer Theorem. We count pairs $(\vec{p}, g)$, where $\vec{p}$ is a pole of $g \neq 1$. Now each g has two poles so

$$|\{(\vec{p}, g) \colon \vec{p} \in P, g\vec{p} = \vec{p}, g \neq 1\}| = 2(N-1) = \sum_{\vec{p} \in P} r_{\vec{p}} - 1$$

where the last equality follows since $G_{\vec{p}}$ is the set of g's with pole $\vec{p}$. Replacing $r_{\vec{p}}$ with $N/n_{\vec{p}}$, we obtain

$$2N - 2 = \sum_{\vec{p} \in P} \frac{N}{n_{\vec{p}}} - 1 = \sum_{\text{orbits } O_{\vec{p}}} n_{\vec{p}} \left(\frac{N}{n_{\vec{p}}} - 1 \right) = \sum_{\text{orbits } O_{\vec{p}}} N - \frac{N}{r_{\vec{p}}}.$$

But then we have

$$2 - \frac{2}{N} = \sum_{i=1}^{k} \left(1 - \frac{1}{r_i} \right),$$

where we have labeled the orbits $O_1, \ldots, O_k$ and $r_i = |G_{\vec{p}_i}|$. This equation is known as Lüroth's Equation.

Lüroth's equation implies that $k \leq 3$, as each term on the right hand side is at least $1/2$ and the left hand side is less than 2. If $k = 1$, then there is a unique orbit or poles and thus $2 - \frac{2}{N} = 1 - \frac{1}{r}$. But the left hand side is at least 1, while the right hand side is less than 1, a contradiction. Now if $k = 2$, then there are two orbits of poles so that

$$\left(1 - \frac{1}{r_1} \right) + \left(1 - \frac{1}{r_2} \right) = 2 - \frac{2}{N} \iff \frac{1}{r_1} + \frac{1}{r_2} = \frac{2}{N} \iff n_1 + n_2 = 2,$$

where the last equivalence follows since $r_i n_i = N$, where $n_i = |O_i|$. But then each orbit is a singleton set, implying there are two poles. Furthermore, $r_i = N$ for $i = 1, 2$ so that every

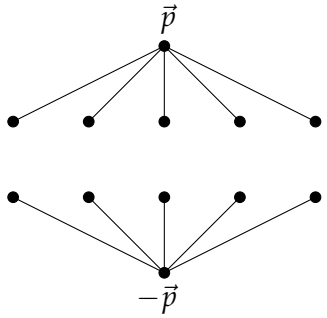
group element fixes both poles. Then $G \cong C_N$ by the $n = 2$ case. In the case of $k = 3$, we have

$$\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} = 1 + \frac{2}{N} > 1.$$

The number of algebraic possibilities are limited. We can assume $r_1 \leq r_2 \leq r_3$ and so $r_1 < 3$. The solutions are $(2, 2, k)$ for any $k \geq 2$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$. We can construct the polyhedron in each case.

- $(2, 2, k)$: We have $\frac{1}{2} + \frac{1}{2} + \frac{1}{k} = 1 + \frac{2}{N}$, so $N = 2k$. But then there are two orbits of size k and one of size 2, say $O_3 = \{\vec{p}, \vec{p}'\}$. Half the elements of G, i.e. k elements, fix $\vec{p}$ and $\vec{p}'$, while the remaining elements swap the elements. But then $G \cong D_k$.

- $(2, 3, 5)$: We have $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1 + \frac{2}{N}$ so that $N = 60$. The orbits have sizes 30, 20, and 12. Let $V = O_3$ be the orbit of size 12. Choose $p \in V$ to be the north pole, and let $H = G_{\vec{p}}$ be the stabilizer of p. We have $|H| = \frac{60}{12} = 5$. In particular, H is cyclic with order 5. Now H (with order 5) acts on V (of order 12), fixing $\vec{p}$ and $-\vec{p}$. But then the orbits have size 1, 1, 5, and 5. Now V is the set of vertices of the icosahedron.



- The cases of $(2, 3, 3)$ and $(2, 3, 4)$ are handled the same as the case above.

□

Corollary 1.2. *The finite subgroups of* $\mathrm{SO}(3)$ *have presentations*

$$\begin{aligned}
\mathbb{C}_n &= \langle x \mid x^n = 1 \rangle \\
\mathbb{D}_n &= \langle x, y \mid x^2 = y^n = (xy)^2 = 1 \rangle \\
\mathbb{T} &= \langle x, y \mid x^2 = y^3 = (xy)^3 = 1 \rangle \\
\mathbb{O} &= \langle x, y \mid x^2 = y^3 = (xy)^4 = 1 \rangle \\
\mathbb{I} &= \langle x, y \mid x^2 = y^3 = (xy)^5 = 1 \rangle
\end{aligned}$$

Proof (Sketch). Suppose we have the Schäfli symbol $\{p, q\}$, i.e. each face has p sides, and q meet at each vertex. Fix a vertex, and let τ be rotation by $2\pi/q$ around this vertex. But then $|\tau| = q$. Also, fix an edge incident to our vertex, and let σ be the rotation swapping the ends of this edge. Then $|\sigma| = 2$.

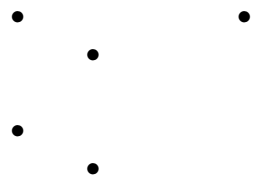
Focus on the face fo the right of our edge, and consider $\sigma\tau$. This rotates the face by $2\pi//p$. So we must have $|\sigma\tau| = p$, and we have elements σ, τ satisfying $\sigma^2 = \tau^q = (\sigma\tau)^p = 1$. One needs to check that σ, τ generate G, and that

$$|\langle x, y \mid x^2 = y^q = (xy)^p = 1\rangle| = |G|.$$

□

Corollary 1.3. *We have isomorphisms* $\mathbb{T} \cong A_4$, $\mathbb{O} \cong S_4$, $\mathbb{I} \cong A_5$.

Note that the group $\langle x, y \mid x^r = y^s = (xy)^t = 1\rangle$ is *only* finite in the cases above. Associate to this the graph $T_{r,s,t}$, shown below.



with total $+s + t - 2$ vertices.

C_n: $(n, 1, n)$ give horizontal line with dots, the dynkin A_{2n-1} D_n: $(2, n, 2)$ D_{n+1} T: $(2, 3, 3)$ E_6 $O(2, 3, 4)$ E_7 $I(2, 3, 5)$ E_8

These are the ADE Coxeter-Dynkin diagrams.

Our next goal is to classify the finite subgroups of $\mathrm{SL}_2(\mathbb{C})$. We travel from $\mathrm{SO}(3)$, to $\mathrm{SU}(2)$, onto $\mathrm{SL}_2(\mathbb{C})$.

Definition (Unitary Group)**.** $U(n) := \{A \in \mathrm{GL}_n(\mathbb{C})\colon A^*A = I_n\}$, where $A^* = \overline{A^T}$. But this is also $\{A\colon |Ax| = |x|\}$ Euclidean norm $= \{A\colon (Ax)^*(Ay) = x^*y\}$ i.e. A preserves the Hermitian inner product $\langle x, y\rangle = x^*y$. That is the $\{A\colon$ rows/col of A are orthogonal basis for $\mathbb{C}^n\}$.

As before $U(n)$ can be described as the set of matrices preserving an arbitrary Hermitian inner product.

Definition (Special Unitary Group)**.** $\mathrm{SU}(n) := \{A \in U(n)\colon \det A = 1\}$.

Lemma 1.1. *Every finite subgroup of* $\mathrm{GL}_n(\mathbb{C})$ *is conjugate to a finite subgroup of* $U(n)$*. In particular, every subgroup of* $\mathrm{SL}_n(\mathbb{C})$ *is conjugate to a finite subgroup of* $\mathrm{SL}_n(\mathbb{C})$ *and* $\mathrm{SU}(n)$*.*

Proof. Let $G \subseteq \mathrm{GL}_n(\mathbb{C})$ be a finite subgroup. We construct a new Hermitian inner product on $\mathbb{C}^n$ so that a given finite group G preserves the product. Define $\langle u, v\rangle := \frac{1}{|G|}\sum_{g\in G}(gu)^*(gv)$. Then for any $h \in G$, $u, v \in \mathbb{C}^n$,

$$\langle hu, hv\rangle = \frac{1}{|G|}\sum_{g\in G}(ghu)^*(ghv) = \frac{1}{|G|}\sum_{k\in G}(ku)^*(kv) = \langle u, v\rangle.$$

Let $\mathcal{B} = \{b_1, \ldots, b_n\}$ be an orthonormal basis with respect to the form $\langle\ ,\ \rangle$ for $\mathbb{C}^n$, and let $\rho : \mathbb{C}^n \to \mathbb{C}^n$ be the change of basis taking the standard basis to B. Then

$$\langle \rho e_i, \rho e_j\rangle = \langle b_i, b_j\rangle = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

It follows from linearity that $\langle \rho e_i, \rho e_j\rangle = u^*v$. Then for any $g \in G$, we claim that $\rho^{-1}g\rho \in U(n)$. It is sufficient to show that $\rho^{-1}g\rho$ preserves the usual Hermitian inner product. We have

$$u^*v = \langle \rho u, \rho v\rangle = \langle g\rho u, g\rho v\rangle = (\rho^{-1}g\rho u)^*(\rho^{-1}h\rho v),$$

since ρ^{-1} is the opposite change of basis. Therefore, $\rho^{-1}G\rho \subseteq U(n)$. As conjugation preserves the dot product, if $G \subseteq \mathrm{SL}_n(\mathbb{C})$, then $\rho^{-1}G\rho \subseteq \mathrm{SU}(n)$. □

In order to classify the finite subgroups of $\mathrm{SL}_2(\mathbb{C})$, we need to understand $\mathrm{SU}(2)$. We know

$$\mathrm{SU}(2) = \left\{ A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \;\middle|\; A^* = A^{-1}, \det A = 1 \right\} = \left\{ \begin{pmatrix} \alpha & -\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}.$$

To relate $\mathrm{SO}(3)$ and $\mathrm{SU}(2)$, we define a map $\pi : \mathrm{SU}(2) \to \mathrm{SO}(3)$. The group $\mathrm{SO}(3)$ is the group of symmetries of the unit sphere S^2. We define an action of $\mathrm{SU}(2)$ on S^2 by rotations. Since $\mathrm{SU}(2)$ acts naturally on $\mathbb{C}^2$, i.e. 2×2 matrices, hence on $\mathbb{P}^1_{\mathbb{C}} = \mathbb{C}^2/\sim$ (since the determinant is 1).

Topologically, $\P^1_{\mathbb{C}}$ is a real 2-sphere. But this gives a natural map $\pi : \mathrm{SU}(2) \to \mathrm{SO}(3)$, which one routinely verifies is a group homomorphism, and $-I_2$ acts trivially. In fact, one can verify that $\ker \pi = \{\pm I_2\}$. Therefore, π is a two-to-one cover of $\mathrm{SO}(3)$.

Lemma 1.2. *The only element of order 2 in* $\mathrm{SU}(2)$ *is* $-I_2$.

Proof (Sketch). Use the explicit form of the elements of $\mathrm{SU}(2)$. □

Theorem 1.5. *A finite subgroup of* $\mathrm{SU}(2)$ *is either cyclic of odd order or a double cover of a finite subgroup of* $\mathrm{SO}(3)$.

Proof. Let $\Gamma \subseteq \mathrm{SU}(2)$ be a finite subgroup. If Γ has odd order, then by Lagrange's Theorem Γ has no elements of order 2. Then $\Gamma \cap \ker \pi = \{I_2\}$ so that $\pi|_\Gamma : \Gamma \to \mathrm{SO}(3)$ maps Γ bijectively to a finite subgroup of $\mathrm{SO}(3)$. The only such of odd order are the cyclic groups. If Γ has even order, then by Cauchy's Theorem Γ contains an element of order 2. Then $\ker \pi \subseteq \Gamma$ so that $\pi|_\Gamma$ is a two-to-one homomorphism onto a finite subgroup of $\mathrm{SO}(3)$. □

Theorem 1.6. *The finite subgroups of* $\mathrm{SL}_2(\mathbb{C})$*, up to conjugacy, are*

$$\mathbb{C}_n = \left\langle \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \right\rangle, B\mathcal{D}_n := \left\langle \mathbb{C}_{2n}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\rangle$$

$$B\mathcal{T} := \left\langle B\mathcal{D}_2, \frac{1}{\sqrt{2}} \begin{pmatrix} \omega_8 & \omega_8^3 \\ \omega_8 & \omega_8^7 \end{pmatrix} \right\rangle$$

$$B\mathcal{O} = \left\langle B\mathcal{T}, \begin{pmatrix} \omega_8^3 & 0 \\ 0 & \omega_8^5 \end{pmatrix} \right\rangle$$

$$B\mathbb{I} = \langle ???? \rangle$$

where ω is a primitive n^{th} root of unity. The group $B\mathcal{D}_n$ is the binary dihedral group of order $4n$, $B\mathcal{T}$ is the binary tetrahedral group of order 24, $B\mathcal{O}$ the binary octahedral group of order 48, and $B\mathbb{I}$ the binary icosahedral group of order 120.

The explicit generators come from the quaternionic description of π. There is also a classification of finite subgroups of $\mathrm{GL}_2(\mathbb{C})$, coming from the extension of groups

$$1 \longrightarrow \mathrm{SL}_2(\mathbb{C}) \longrightarrow \mathrm{GL}_2(\mathbb{C}) \xrightarrow{\det} \mathbb{C}^\times \longrightarrow 1.$$

So any $G \subseteq \mathrm{GL}_2(\mathbb{C})$ is an extension of $G \cap \mathrm{SL}_2(\mathbb{C})$ by a finite subgroup of $\mathbb{C}^\times$—which are cyclic. Though it takes a certain amount of work, one can classify the finite subgroups of $\mathrm{SL}_3(\mathbb{C})$ using $A \in \mathrm{SL}_3(\mathbb{C})$

$$A \in \mathrm{SL}_3(\mathbb{C}) \rightsquigarrow \left(\begin{array}{c|c} \det B^{-1} & \\ \hline & B \\ & \end{array}\right), B \in \mathrm{GL}_2(\mathbb{C}).$$

2 Group Representations & Characters

2.1 Group Representations

Our final goal for this section will be M^{c}Kay original observation that the character tables of the binary polyhedral groups 'are' the extended A-D-E diagrams. We begin with an introduction to group representations.

Definition (Representation)**.** Let G be a finite group. A (complex) representation of G is a group homomorphism

$$\rho : G \to \mathrm{GL}_n(\mathbb{C}),$$

for some $n \geq 1$. We call n the dimension of ρ.

Remark. We call the representation $G \to \mathbb{C}^* = \mathrm{GL}_1(\mathbb{C})$ given by $g \mapsto 1$ for all $g \in G$ the trivial representation. Every finite group admits at least a trivial representation.

We will identify $\mathrm{GL}_n(\mathbb{C})$ as the automorphism group of $\mathbb{C}^n$, i.e. invertible linear maps. In this way, a representation is equivalent to an action of G on $\mathbb{C}^n$. Write ρ_g for the linear operator $\rho(g) : \mathbb{C}^n \to \mathbb{C}^n$. Avoiding a choice of basis, we write $\rho : G \to \mathrm{GL}(V)$ for a vector space V. Often, we will not distinguish between ρ and V, unless doing so would cause confusion.

Recall the group algebra $\mathbb{C}[G]$ is the $\mathbb{C}$-vector space spanned by the elements of G,

$$\mathbb{C}[G] = \left\{ \sum_{g \in G} \alpha_g g \;\middle|\; \alpha_g \in \mathbb{C} \right\},$$

with addition given componentwise and multiplication given by $(\alpha g)(\beta h) := (\alpha\beta)(gh)$, extended by linearity. Suppose M is a finitely generated $\mathbb{C}[G]$-module. Then M is also a finitely generated $\mathbb{C}$-module, i.e. a $\mathbb{C}$-vector space.

Therefore, $M \cong \mathbb{C}^n$ as vector spaces for some n. Multiplication by group elements define invertible linear operators $(M \xrightarrow{\cdot g} M) \in \mathrm{GL}(M) \cong \mathrm{GL}_n(\mathbb{C})$. Therefore, we obtain a map $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ given by $g \mapsto (M \xrightarrow{g} M)$, i.e. a representation of G. Conversely, a representation V is equivalent to a $\mathbb{C}[G]$-module. Therefore, the following are equivalent

- a representation of a group G
- a $\mathbb{C}[G]$-module
- an action of G on $\mathbb{C}^n$

This shows that representations of G are the same as $\mathbb{C}[G]$-modules.

We can take direct sum of representations: given two representations $\rho : G \to \mathrm{GL}_n(\mathbb{C})$, $\rho' : G \to \mathrm{GL}_m(\mathbb{C})$, their direct sum is $\rho \oplus \rho' : G \to \mathrm{GL}_{n+m}(\mathbb{C})$ given by

$$g \mapsto \left(\begin{array}{c|c} \rho(g) & 0 \\ \hline 0 & \rho'(g) \end{array}\right);$$

that is, $\rho \oplus \rho' : G \to \mathrm{GL}_n(\mathbb{C}) \oplus \mathrm{GL}_m(\mathbb{C}) \subseteq \mathrm{GL}_{n+m}(\mathbb{C})$ is given by $(\rho \oplus \rho')(g) := (\rho(g), \rho'(g))$.

Definition (Indecomposable)**.** If ρ cannot be written as a direct sum of two representations, then we call the representation indecomposable. Otherwise, we call the representation decomposable.

If ρ is decomposable, there are invariant, i.e. stabilized, subspaces of the vector space $V \oplus V'$. There is a stronger condition on representations than indecomposability, namely irreducibility.

Definition (Irreducible)**.** We say that a representation $\rho : G \to \mathrm{GL}(V)$ is irreducible if ρ has no invariant subspaces, i.e. no submodules other than $\{0\}$ and V. Otherwise, we say that ρ is reducible.

Clearly, a decomposable representation must be reducible, which immediately gives the following by contrapositive.

Theorem 2.1. *Any irreducible representation is indecomposable.*

Proof. If $\mathrm{im}(\rho \oplus \rho') \cong V \oplus V'$, then the action of G stabilizes V, V'. □

Example 2.1. Let $G = S_3$. What are the representations of S_3? There is always the *trivial representation* $1 : S_3 \to \mathbb{C}^*$ given by $\sigma \mapsto 1$ for all $\sigma \in S_3$. This representation is clearly 1-dimensional.

We also have the *alternating representation* (or *sign representation*) $a : S_3 \to \mathbb{C}^\times$ given by $\sigma \mapsto \mathrm{sign}\ \sigma$, where sign σ is $+1$ for even permutations and -1 for odd permutations. This representation is also 1-dimensional.

Now every permutation can be represented by a matrix given by mapping a permutation σ to the result of the permutation σ acting on the rows of I_3, i.e. a permutation of a basis of $\mathbb{C}^3$. Explicitly, $\pi : S_3 \to \mathrm{GL}_3(\mathbb{C})$ is given by $(\pi\sigma)(z_1, z_2, z_3) = (z_{\pi^{-1}(1)}, z_{\pi^{-1}(2)}, z_{\pi^{-1}(3)})$. For example,

$$(2\ 3) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This gives a homomorphism $\pi : S_3 \to \mathrm{GL}_3(\mathbb{C})$, called the *permutation representation*.

Now which of these permutations are indecomposable or irreducible, if any? Since the trivial and sign representations are both 1-dimensional, they are clearly both indecomposable and irreducible. The permutation representation has stable subspaces, namely the one spanned by $(1,1,1)$, so that it cannot be indecomposable, i.e. the permutation representation is decomposable. But then the permutation representation is also reducible.

We can also create submodule/subrepresentations by 'modding out.' For example, define

$$V = \{(z_1, z_2, z_3) \in \mathbb{C}^3 \colon z_1 + z_2 + z_3 = 0\},$$

the natural representation modulo the trivial representation, with the permutation action. This is called the standard representation. This space is 2-dimensional, and one can check the permutation representation is isomorphic to $1 \oplus V$, i.e. the direct sum of the trivial representation and the standard representation. ◁

Indecomposability and irreducibility are generally not equivalent. As noted before, irreducibility is a stronger condition than indecomposability. However over $\mathbb{C}$, indecomposability and irreducibility are equivalent.

Theorem 2.2 (Maschke's Theorem)**.** *Every indecomposable representation over $\mathbb{C}$ of a finite group is irreducible. Therefore, a representation over $\mathbb{C}$ of a finite group is indecomposable if and only if it is irreducible.*

Proof. Suppose that V is a representation of G and $W \subseteq V$ is a subrepresentation, i.e. a G-stable subspace. Fix a linear projection $\pi : V \twoheadrightarrow W$, and G-linearize it:

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

Now notice we have

$$\begin{aligned} h\widetilde{\pi}(v) &= h \frac{1}{|G|} \sum_{g} (g\pi g^{-1})(v) \\ &= \frac{1}{|G|} \sum_{g} hg\pi g^{-1}h^{-1}hv \\ &= \frac{1}{|G|} \sum_{hg} (hg)\pi(hg^{-1})(hv) \\ &= \widetilde{\pi}(hv). \end{aligned}$$

Therefore, $h\widetilde{\pi}(v) = \widetilde{\pi}(hv)$ so $\widetilde{\pi}$ is G-linear. It is routine to verify that $\widetilde{\pi}$ fixes W, and we know $\widetilde{\pi}$ projects V onto W. Then $\widetilde{\pi}$ is a split-surjective morphism of representations, and hence $V \cong W \oplus \ker \widetilde{\pi}$. But then V is reducible. □

Remark. This works over any field of characteristic zero or any field for which $|G|$ is invertible. Another way to say this is that the group algebra $\mathbb{C}[G]$ is semisimple, i.e. short exact sequences of $\mathbb{C}[G]$-modules split.

Note that the proof of Maschke's Theorem uses a sort of 'averaging': $\frac{1}{|G|}\sum_{g\in G}(g\pi g^{-1})(v)$. This is a common trick that will appear many times.

2.2 Characters

Given a finite group G, we want to be able to classify all the irreducible representations of G, and for any given representation ρ of G, decompose ρ into a direct sum of irreducible representations; that is, write $\rho = \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t}$, where $\rho \ncong \rho_j$ for $i \neq j$ are irreducible representations and the a_i are some multiplicities. We did this in Example 2.1. However, we did not prove that these were all the representations. To do this generally, we will need Character Theory.

Definition (Character)**.** Let $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ be a representation of G. The character of ρ is defined by $\chi_\rho := \mathrm{tr}(\rho_g)$, i.e. the trace of the matrix given by the composition

$$G \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{C}) \xrightarrow{\mathrm{tr}} \mathbb{C}, \qquad G \xrightarrow{\chi_\rho} \mathbb{C}$$

When the representation is apparent, we denote this simply as χ.

Observe that χ_ρ is *not* generally a homomorphism as the trace is not generally multiplicative, i.e. $\mathrm{tr}(AB) \neq \mathrm{tr}(A)\,\mathrm{tr}(B)$. In the case of $n = 1$, clearly χ_ρ is a homomorphism. Now while the trace map is not generally multiplicative, we do have that $\mathrm{tr}(AB) = \mathrm{tr}(BA)$. More generally, $\mathrm{tr}(\cdot)$ is invariant under cyclic permutation of products. Therefore, χ_ρ is a *class function*, i.e. χ_ρ is constant on conjugacy classes:

$$\begin{aligned}
\chi_\rho(g^{-1}hg) &= \mathrm{tr}(\rho(g^{-1}hg)) \\
&= \mathrm{tr}(\rho(g)^{-1}\rho(h)\rho(g)), && \rho \text{ homo.} \\
&= \mathrm{tr}(\rho(h)\rho(g)^{-1}\rho(g)), && \mathrm{tr}(AB) = \mathrm{tr}(BA) \\
&= \mathrm{tr}(\rho(h)), && \rho \text{ homo.} \\
&= \chi_\rho(h).
\end{aligned}$$

Example 2.2. Consider again the example of $G = S_3 = \{(1), (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, c.f. Exercise 2.1. The conjugacy classes of S_n are classified by cycle type—corresponding to integer partitions of n. The conjugacy classes are then represented by

$$\{(1)\},\ \ \{(1\ 2), (2\ 3), (1\ 3)\},\ \ \{(1\ 2\ 3), (1\ 3\ 2)\}.$$

We shall create a table for the characters of S_n. We will need a row per distinct representation but (since the representation acts the same on each conjugacy class) we need only one colum per conjugacy class.

The trivial representation takes every σ to the identity, so $\chi_{\text{triv}}(\sigma) = 1$ for all $\sigma \in S_3$. For the alternating representation, we know that

$$a(\sigma) = \begin{cases} 1, & \sigma \text{ even} \\ -1, & \sigma \text{ odd} \end{cases}$$

So a takes the 3-cycles to 1 and the 2-cycles to -1. For the permutation representation $\pi : S_3 \to \mathrm{GL}_3(\mathbb{C})$, we have

$$1 \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (1\,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (1\,2\,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Therefore, $\chi_\pi(1) = 3$, $\chi_\pi((123)) = 0$, and $\chi_\pi((12)) = 1$. Our table is then thus far,

	(1)	$(1\,2\,3)$	$(1\,2)$
χ_{triv}	1	1	1
χ_{a}	1	1	-1
χ_{perm}	3	0	-1

We only need consider the standard representation, V. We knew that the permutation representation was isomorphic to the direct sum of the trivial representation with the standard representation. Since the trace of a block matrix is the sum of the traces, we know that $\chi_{\text{perm}} = \chi_{\text{std}} + \chi_{\text{triv}}$. We can then easily calculate the row for χ_{std}, and add this to our table. Since $\chi_{\text{perm}} = \chi_{\text{std}} + \chi_{\text{triv}}$, we can add the first and last row to find χ_{perm}, making

	(1)	$(1\,2\,3)$	$(1\,2)$
χ_{triv}	1	1	1
χ_{a}	1	1	-1
χ_{perm}	3	0	-1
χ_{std}	2	-1	0

the row redundant. If we remove the redundant χ_{perm} row, we obtain the following table:

	(1)	$(1\,2\,3)$	$(1\,2)$
χ_{triv}	1	1	1
χ_{a}	1	1	-1
χ_{std}	2	-1	0

We make the following seemingly coincidental observations:

1. The table is square, and the number of characters is the number of conjugacy classes.

2. The columns are orthogonal.

3. The rows are orthogonal if one weights each column by the number of elements in that class, e.g.
$$\langle \chi_{\text{triv}}, \chi_{\text{std}} \rangle = 1(1 \cdot 2) + 3(1 \cdot 0) + 2(1 \cdot -1) = 0.$$

4. The first column yields the dimension of ρ. In general, $\chi_p(1) = \text{tr}(\rho(1)) = \text{tr}(I_n) = n$.

5. The sum of the squares of the first column is $6 = |S_3|$. ◁

Proposition 2.1. *Let G be a finite group, ρ a finite dimensional representation of G, and χ its corresponding character. Then*

(i) *χ is a class function.*

(ii) *$\chi(1) = n$.*

(iii) *The characters of a direct sum of representations is the sum of the characters.*

(iv) *The character of a tensor product of representations is the product of the characters.*

(v) *$\chi(g^{-1}) = \overline{\chi(g)}$*

(vi) *If $|g| = k$, then the eigenvalues of the matrix ρ_g are powers of the k^{th} roots of unity, and $\chi(g)$ is a sum of such things.*

Recall that if V and W are vector spaces with basis $\{e_1, \ldots, e_n\}$ and $\{f_1, \ldots, f_m\}$, respectively, then $V \otimes W$ is the vector space with basis $\{e_i \otimes f_j\}_{i=1,\ldots,n;j=1,\ldots,m}$ and scalar multiplication $\alpha(e_i \otimes f_j) = \alpha e_i \otimes f_j = e_i \otimes f_j$. If V and W carry actions of G, then so does $V \otimes W$ by $g(v \otimes w) = g(v) \otimes g(w)$. If $g^k = 1$, then $(\rho_g)^k = I_n$ so the minimal polynomial of ρ_g divides $x^k - 1$. Therefore, its roots are roots of unity. The trace of a matrix is the sum of its eigenvalues.

2.3 Orthogonality Relations

Let $\mathcal{H}$ denote the set of all class functions $G \to \mathbb{C}$. This contains the characters of G. Define a Hermitian inner product on $\mathcal{H}$

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

Theorem 2.3. *The irreducible characters, i..e the characters of irreducible representations, are an orthonormal basis for $\mathcal{H}$ with respect to this inner product. In particular,*

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \begin{cases} 1, & \rho \cong \rho' \\ 0, & \rho \neq \rho' \end{cases}$$

Proof. The proof will proceed in eight steps.

(i) For any representation V, the fixed subspace $V^G := \{v \in V : gv = v \text{ for all } g \in G\}$ is a subrepresentation of V. There is a natural projection

$$\pi : V \longrightarrow V^G \subseteq V$$

$$v \longmapsto \frac{1}{|G|} \sum_{g \in G} gv.$$

(ii) Compute the trace of π. First, extend a basis for V^G to a basis for V. Then and so $\mathrm{tr}(\pi) = \dim V^G$. Now the trace of a sum is the sum of the traces, so

$$\mathrm{tr}(\pi) = \mathrm{tr}\left(\frac{1}{|G|} \sum_{g \in G} g(\cdot) \right) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}(\rho_g) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g).$$

In other words, $\dim V^G$ is the average value of χ_ρ.

(iii) For representations V and W, we have

$$\mathrm{Hom}_{\mathbb{C}}(V, W) = \{\text{linear maps } V \to W\}$$

$$\mathrm{Hom}_G(V, W) = \{G\text{-linear maps, i.e. } gf(v) = f(gv)\}$$

Now $\dim \mathrm{Hom}_{\mathbb{C}}(V, W) = \dim V \cdot \dim W$. However, what is $\dim \mathrm{Hom}_G(V, W)$?

(iv) We know that $\mathrm{Hom}_{\mathbb{C}}(V, W)$ is again a representation of G: for $g \in G$, $f : V \to W$ a linear map, define $(gf)(v) := g(f(g^{-1}v))$.

(v) Now $\mathrm{Hom}_{\mathbb{C}}(V, W)^G = \{f \in \mathrm{Hom}_{\mathbb{C}}(V, W) : gf = f \text{ for all } g \in G\}$. That is, $\{f : (gf)(v) = f(v) \text{ for all } g \in G, v \in V\}$. which is $\{f : g(f(g^{-1}(v))) = f(v) \text{ for all } g, v\}$, rearranging is $f(g^{-1}(v)) = g^{-1}(f(v))$ for all g, which is $\mathrm{Hom}_G(V, W)$.

So if V and W are irreducible,

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

and on the other hand, $\dim \mathrm{Hom}_G(V,W) = \dim(\mathrm{Hom}_{\mathbf{C}}(V,W)^G)$ by 5, which is $= \dim((V^* \otimes_{\mathbf{C}} W)^G)$, which is the average value of $\chi_{V^* \otimes W}$ which is the average value of $\overline{\chi_V}\chi_W$ which is $\langle \chi_V, \chi_W \rangle$.

Consequently, the characters determine the representations; that is, $\rho \cong \rho'$ if and only if $\chi_\rho = \chi_{\rho'}$.

The number of irreducible representations of G is equal to the number of conjugacy classes. [Because $\mathcal{H}$ has a basis given by the characteristic functions of the conjugacy classes.]

A representation ρ is irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$. [For any ρ, Maschke's Theorem allows one to write $\rho \cong \rho_1^{a_1} \oplus \cdots \oplus \rho_r^{a_r}$, where the ρ_i are distinct, irreducible, and a_i is its multiplicity. But then $\chi_\rho = a_1\chi_{\rho_1} + \cdots + a_r\chi_{\rho_r}$. But then

$$\langle \chi_\rho, \chi_\rho \rangle = \sum_{i,j} a_i a_j \langle \chi_{\rho_i}, \chi_{\rho_j} \rangle = \sum_{i=1}^{r} a_i^2.$$

Therefore, $\rho = \rho_i$ must be irreducible. The other direction follows straight from the theorem.

The multiplicity of an irreducible representation ρ_i in a given representation is $\langle \chi_{\rho_i}, \chi_\rho \rangle$.

Definition (Regular Representation)**.** The regular representation of G is a $\mathbb{C}$-vector space $\mathbb{C}[G]$. Equivalently, $\mathbb{C}[G]$, as a module over itself, or $G \to \mathrm{GL}(\mathbb{C}[G])$.

Recall $\mathbb{C}[G]$ has a basis $\{g \in G\}$. The action of $h \in G$ is given by $g \mapsto hg$, i.e. h permutes basis elements.

Proposition 2.2. *Every irreducible representation V appears as a direct summand in the regular representation, with multiplicity equal to its dimension, i.e.*

$$\mathbb{C}[G] \cong \bigoplus_{i=1}^{r} V_i^{\dim V_i},$$

where $V_1, \ldots, V_r$ are the irreducible representations. In particular,

$$|G| = \sum_{i=1}^{r} (\dim V_i)^2 = \sum_{i=1}^{r} (\chi_i(1))^2.$$

Proof. L.T.R. □

Corollary 2.1. *G is abelian if and only if every representation is 1-dimensional.*

Proof. G is abelian if and only if every conjugacy class is a singleton if and only if there are $|G|$ classes if and only if there are $|G|$ irreducibles if and only if all the representations have dimension 1. □

Example 2.3. (i) $G = S_3$. We found three irreducible representations: $\chi_{\mathrm{triv}}, \chi_{\mathrm{akt}}, \chi_{\mathrm{std}}$. Since $1^2 + 1^2 + 2^2 = 6 = |S_3|$, this must be all the irreducible representations for S_3.

(ii) Let $G = C_n = \langle x \colon x^n = 1 \rangle$. Every irreducible is a map $G \to \mathbb{C}^\times$ completely determined by the image of x. Since the map is a morphism, $1 \mapsto 1$, which implies that the image of x must be an n^{th} root of unity. But then we obtain

$$\begin{aligned} \rho_k : \ x &\mapsto \omega_n^j \\ x^r &\mapsto \omega_n^{j_r} \end{aligned}$$

for $j = 0, \ldots, n-1$, where ρ_0 is the trivial representation. Then we have character table

	$\{1\}$	$\{x\}$	$\{x^2\}$	$\cdots$	$\{x^{n-1}\}$
ρ_0	1	1	$\cdots$	1	
ρ_1	ω	ω^2	$\cdots$	ω^{n-1}	
ρ_2	1	ω^2	ω^4	$\cdots$	$\omega^{2(n-1)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
ρ_{n-1}	1	ω^{n-1}	$\omega^{2(n-1)}$	$\cdots$	$\omega^{(n-1)^2}$

(iii) Let $G = S_4$. We have cycle types $1, (1\ 2), (1\ 2\ 3), (1\ 2\ 3\ 4), (1\ 2)(3\ 4)$, with multiplicity, $1, 6, 2\binom{4}{3} = 8, 3! = 6, 3$, respectively.

χ_{triv}	1	1	1	1	1
χ_{alt}	1	-1	1	-1	1
χ_{std}	3	1	0	-1	-1
χ_{perm}	4	2	1	0	0
$\chi_{\text{std}} \otimes \chi_{\text{alt}}$	3	-1	0	1	-1
R	2	0	-1	0	2

Is the standard representation irreducible> We have $\langle \chi_{\text{std}}, \chi_{\text{std}} \rangle = \dfrac{1}{|G|}(1 \cdot 3^2 + 6 \cdot 1^2 + 6 \cdot 0^2 + 6(-1)^2 + 3(-1)^3) = \dfrac{1}{24} \cdot 24 = 1$, so yes. Are we done? Well, we have $1^2 + 1^2 + 3^2 = 11 < 24$, so no. A sneaky trick is to tensor with the known representations. Tensoring with the trivial one does nothing so we proceed with the others. The tensor of the standard with the alternating representation is 3-dimensional and irreducible by the same calculation. So now $1^2 + 1^2 + 3^2 + 3^2 = 20$, missing 4. So missing one two dimensional or 4 1-dimensional. In either case, there is (at least one) 2-dimensional representation, say R. So the first row of the entry for R must be 2. Call the other entries a, b, c, and d respectively. Using the orthogonality relations, one finds a system of four equations and four unknowns only to find $a = c = 0$, $b = -1$, $d = 2$. Finally, $\langle \chi_R, \chi_R \rangle = \cdots = 1$, so R is irreducible, as expected. This is then the complete character table.

(iv) $G = A_4 \subseteq S_4$. The Class Equation tells that the number of things in each conjugacy class must divide the order of the group. So unlike the situation in S_4, $(1\ 2\ 3)$ is not a conjugacy class (size 8, $|A_4| = 12$). ?????????

So $(1\ 2\ 3) \not\sim (1\ 3\ 2)$.

So it must split into at least to conjugacy classes. These are 1, $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2)(3\ 4)$, of sizes 1, 4, 4, and 3, respectively.

	1	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 2)(3\ 4)$
χ_{triv}	1	1	1	1
χ_{std}	3	0	0	-1
R	2	-1	-1	2

We always have the trivial representation. We can always restrict any representation of S_4 to A_4. Doing so with the alternating representation gives the trivial representation. The standard tensor alternating restricted to A_4 is the standard representation on A_4. Note one can restrict an irreducible representation and no longer be irreducible. We have $\langle \chi_{\text{std}}, \chi_{\text{std}} \rangle = 1$, $\langle R, R \rangle = \frac{1}{12}(1 \cdot 2^2 + 4(-1)^2 + 4(-1)^2 + 3 \cdot 2^2) = 2$, not irreducible. So the restriction of R to A_4 splits into two 1-dimensional representations. So we must split the R row into two, say U and U'.

	1	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 2)(3\ 4)$
χ_{triv}	1	1	1	1
χ_{std}	3	0	0	-1
U	1	a	b	c
U'	1	$-1-a$	$-1-b$	$2-c$

Once we have a, b, c, we know that the rows of U, U' add to the rows of R, hence the last row must be what is given above. Linear Algebra gives $a = \omega_3$, $b = \omega_3^2$, and $c = 1$. Could we have seen that without Linear Algebra? If we have a quotient of A_4, where characters we know, we can restrict along the quotient map. Normal subgroup in A_4: $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$. The quotient is, having order 3, C_3, which has two nontrivial irreducible representations. Let's say $C_3 = \langle (1\ 2\ 3) \rangle$. Then these representations are $(1\ 2\ 3) \mapsto \omega_3$, $(1\ 3\ 2) \mapsto \omega_3^2$ and $(1\ 2\ 3) \mapsto \omega_3^2$, $(1\ 3\ 2) \mapsto \omega_3$.

	1	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 2)(3\ 4)$
χ_{triv}	1	1	1	1
χ_{std}	3	0	0	-1
U	1	ω	ω^2	1
U'	1	ω^2	ω	1

(v) Take $G = B\mathcal{T} \subseteq \mathrm{SL}_2(\mathbb{C})$, which has a 2-to-1 map $B\mathcal{T} \to \mathcal{T}$, where $\mathcal{T}$ is the tetrahedral group of order 12. We know that $\mathcal{T} \cong A_4$. Then we know that we can restrict the

4 irreducibles of A_4 to $B\mathcal{T}$. Then the preimage of a conjugacy class in $\mathcal{T}$ is either a single conjugacy class in $B\mathcal{T}$ of twice the size, or 2 classes, each of the same size as the original. So to start, just lump the classes together. The classes are 1, $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2)(3\ 4)$, of sizes 2, 8, 8, 6.

$$\begin{array}{cccccc} \chi_{\text{triv}} & 1 & 1 & 1 & 1 \\ \chi_{\text{std}} & 3 & 0 & 0 & -1 \\ U & 1 & \omega & \omega^2 & 1 \\ U' & 1 & \omega^2 & \omega & 1 \\ \rho \otimes U & \rho \otimes U' & & & \end{array}$$

There is also the "given rep" $B\mathcal{T} \hookrightarrow \mathrm{GL}_2(\mathbb{C})$, which is two-dimensional. Also, $\rho \otimes U$, $\rho \otimes U'$, there are two more 2-dimensional. So we'll have different values in the $(1\ 2\ 3)$ column, a, ωa, $\omega^2 a$ for some a. So they are pairwise nonisomorphic. Fact, ρ is irreducible (we had explicit matrix generators for $B\mathcal{T}$). So $\rho \otimes U$, $\rho \otimes U'$ are too. Then $1^2 + 3^2 + 1^2 + 1^2 + 2^2 + 2^2 + 2^2 = 24$, and that is all. There are then seven conjugacy classes in $B\mathcal{T}$. The preimage of $\{1\}$ is $\{\pm 1\}$, the identity matrix. So that class splits in two. Fact: the class $\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ in $\mathcal{T}$ lifts to a single class of size 6. Then the other two split into two.

$$\begin{array}{ccccccccc} & 1 & 1 & 4 & 4 & 4 & 4 & 6 \\ \chi_{\text{triv}} & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \chi_{\text{std}} & 3 & 3 & 0 & 0 & 0 & 0 & -1 \\ U & 1 & 1 & \omega & \omega & \omega^2 & \omega^2 & 1 \\ U' & 1 & 1 & \omega^2 & \omega^2 & \omega & \omega & 1 \\ \rho & 2 & -2 & 1 & -1 & 1 & -1 & 0 \\ \rho \otimes U & 2 & -2 & \omega & -\omega & \omega^2 & -\omega^2 & 0 \\ \rho \otimes U' & 2 & -2 & \omega^2 & -\omega^2 & \omega & -\omega & 0 \end{array}$$

Note that the character table does not determine the group. For example D_4 and Q_8 have the same character table. [Lose a lot passing to conugacy classes.] However, the character table carries a lot of information about the group. For example, if $\rho_1, \ldots, \rho_r$ are the irreducible representations, then for every i, j,

$$\rho_i \otimes \rho_j \cong \bigoplus_{k=1}^{r} \rho_k^{c_{i,j}^k}$$

for some *structure constants* of the group, $c_{i,j}^k$. When G is given to us as a subgroup of GL, it's already interesting to look at

$$\rho \otimes \rho_j = \bigoplus_{i=1}^{r} \rho_i^{c_{i,j}},$$

where ρ is the given representation. Then

$$\chi\chi = \sum c_{i,j}\chi_i$$

and we can read the $c_{i,j}$'s from the character table. Back to $B\mathcal{T}$. We are given ρ, the 5th row of the table. Let's decompose $\rho \otimes \text{std}$. We have $\rho \otimes \text{std} : 6, -6, 0, 0, 0, 0, 0$. Checking carefully and using the properties of ω, this is the sum of ρ, $|\rho \otimes U$, and $\rho \otimes U'$.

Definition (McKay Quiver)**.** Let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{C})$. The McKay quiver of G has vertices $\rho_1, \ldots, \rho_r$, the irreducible representations of G, arrows m_{ij} for $\rho_i \to \rho_j$ if ρ_i appears with multiplicity m_{ij} in $\rho \otimes \rho_j$.

Recall $m_{ij} = \dim \mathrm{Hom}_G(V_i, V \otimes V_j) = \langle \chi_i, \chi\chi_j \rangle$ (abstract stuff on boses). We have $G = C_2$ embedded in $\mathrm{GL}_3(\mathbb{C})$ as $\left\langle \begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix} \right\rangle$. We know the irreducible representations of $C_2 = \langle \sigma \colon \sigma^2 = 1 \rangle$. The two representations must be $\sigma \mapsto 1$, $\sigma \mapsto -1$, call the first ρ_1 and the second ρ_{-1}. Notice $\rho(\text{given}) \cong \rho_{-1}^{(3)}$ and

	ρ_1	ρ_{-1}
ρ_1	ρ_1	ρ_{-1}
ρ_{-1}	ρ_{-1}	ρ_1

So $\rho \otimes \rho_1 = \rho = \rho_{-1}^{(3)}$, $\rho \otimes \rho_{-1} = \rho_{-1}^{(3)} \otimes \rho_{-1} = \rho_1^{(3)}$. Then we have

Now consider $C_n = \left\langle \begin{pmatrix} \omega_n & \\ & \omega_n^{-1} \end{pmatrix} \right\rangle \subseteq \mathrm{SL}_2(\mathbb{C})$. We know the irreducible representations of C_n : $\rho_0, \rho_1, \ldots, \rho_{n-1}$, where ρ_j takes the generator of C_n to ω_n^j. Our given representation is $\rho \cong \rho_1 \otimes \rho_{n-1}$. What is $\rho_j \otimes \rho_k$? It's ρ_{j+k}, with jk taken mod n. So $\rho \otimes \rho_j = (\rho_1 \oplus \rho_{n-1}) \otimes \rho_j = \rho_{j+1} \oplus \rho_{j-1}$, where again indices are taken mod n.

We get the above diagram for every j.

Example

D_4	$\{1\}$	$\{x^2\}$	$\{x, x^3\}$	$\{y, x^2y\}$	$\{y, x^3y\}$
β_{++}	1	1	1	1	1
β_{+-}	1	1	1	-1	-1
β_{-+}	1	1	-1	-1	-1
β_{--}	1	1	-1	-1	1
ρ	2	-2	0	0	0

where $\rho_{\pm\pm}(x) = \pm 1$, $\beta_{\pm\pm}(y) = \pm 1$, and ρ is the "geometric" representation as symmetries of an n-gon in $\mathbb{C}^2$.

Now let's compute the McKay quiver of D_4 with respect to $\rho : D_4 \hookrightarrow \mathrm{GL}_2(\mathbb{C})$.

$$\rho \otimes \beta_{++} \cong \rho$$
$$\rho \otimes \beta_{+-} \cong \rho$$
$$\rho \otimes \beta_{-+} \cong \rho$$
$$\rho \otimes \beta_{--} \cong \rho$$
$$\rho \otimes \rho \cong \beta_{++} \oplus \beta_{+-} \oplus \beta_{-+} \oplus \beta_{--}$$

Then picture

McKay observed that the arrows in the McKay quiver of the binary tetrahedral groups come in opposing pairs, no more than one between any two vertices, and if you remove the trivial representation, one obtains an ADE Dynkin diagram.

The first two parts are relatively simple to prove without knowing the classification. For example, $m_{ji} = \langle \chi_j, \chi\chi_i \rangle$. Now χ is the character of $G \hookrightarrow \mathrm{SL}_2(\mathbb{C})$ is self-adjoint since it is in SL_2. But then $m_{ji} = \langle \chi_j, \chi\chi_i \rangle = \langle \chi_j\chi, \chi_i \rangle = \langle \chi_i, \chi, \chi_j \rangle = m_{ij}$.

Our next goal is to give a uniform proof (meaning without classification) of McKay 's observation about ADE diagrams.

2.4 ADE and Extended ADE Diagrams

A list:

The extended ADE diagrams have one extra vertex, circled. Then have $n+1$ vertices. They have the weird property that ...

Lemma 2.1. *Let T be a connected finite graph (possibly with multiple edges). Then either T is an ADE diagram or T contains an extended ADE, and not both.*

Proof. If T does not contain an extended ADE, $\tilde{A}_n$ then no cycles, so a tree. not contain $\tilde{D}_n$ so then at most one branch point of valence $= 3$. So its a T_{pqr},

Assume that $p \leq q \leq r$. Not contain $\tilde{E}_6$ so that $p \leq 2$. Not contain $\tilde{E}_7$, so then $q \leq 3$. Not contain $\tilde{E}_8$ so that $r \leq 5$. But then $T_{1,1,n}$, $T_{2,2,n}$, or $T_{2,3,3}$, $T_{2,3,4}$, $T_{2,3,5}$, and these are A_n, D_{n+2}, E_6, E_7, or E_8, respectively. □

There are two 'birthplaces' for extended ADE diagrams. The first is additive functions on graphs, the second is Tits quadratic forms of graphs.

Definition. Let T be a finite connected graph on a vertex set $\{1, \ldots, n\}$. Then an additive function on T is a function $a : \{1, \ldots, n\} \to \mathbb{N}_{>0}$ such that for every i

$$\sum_{\text{there is edge i - j}} a_j = 2a_i$$

whee $a_i = a(i)$. It is subadditive if less than or equal to. Strictly subadditive if strict inequalty.

Example is a subadditive function since $2 \geq 1$. Could there be an additive function? We would need $2a_1 = a_2$ and $2a_2 = a_1$, impossible.

Example Now $a_1 = 1 = a_2$ is an additive function because we count each edge separately. $2a_1 = 2a_2$.

Ecample We would need $2a_1 \leq 3a_2$, $2a_2 \leq 3a_1$, impossible.

Example $\tilde{D}_5$

So carries additive function.

The crucial observation is that if T is the M^{c}Kay graph of a subgroup of $\mathrm{SL}_2(\mathbb{C})$ (replace each left/right arrow with dash), then labeling each vertex with the dimension of the corresponding representation is an additive function! This is because we tensor with the given 2-dimensional representation ρ, and connect ρ_i to all the ρ_j appearing in $\rho \otimes \rho_i$. So

$$2 \dim \rho_i = \dim(\rho \otimes \rho_i) = \sum_{\rho_i - \rho_j} \dim \rho_j.$$

Theorem 2.4. *A graph T carries an additive function if and only if it is extended ADE. It carries a strictly subadditive function if and only if it is ADE.*

Lemma 2.2. *The extended ADE graphs carry additive functions, and the ADE graphs carry strictly subadditive functions.*

Proof. Write them down. □

We need to reinterpret additive functions. Write a function $a : \{1, \ldots, n\} \to \mathbb{N}_{>0}$ as a column vector $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. Then a is subadditive if and only if $2 \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \geq \begin{pmatrix} \sum a_j \\ \vdots \\ \sum a_j \end{pmatrix}$

$= \text{indicdence matrix} \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$, i.e. $2I - A$ has nonnegative entries, where I is the identity matrix and A is the indicence matrix and $[A]_{ij}$ is the number of edges between i and j.

Lemma 2.3. *If T admits an additive function, then every subadditive function on T is additive.*

Proof. Set $C = 2I_n - A$, where A is the incidence matrix of T.. Assume a is an additive function and b is a subadditive function. We need show that b is additive. Consider $b^T C a$. Since a is additive, $Ca = 0$. But we also know $b^T C a = b^T C^T a$ since C is symmetric, which is $(Cb) \cdot a$, which is a positive linear combination of entries of Cb (since entries of a are positive). But then $Cb = 0$, which implies that b is additive. □

Corollary 2.2. *Every subadditive function on an extended ADE diagram is additive.*

Lemma 2.4. *Suppose that $T \subsetneq T'$ are finite connected graphs. If T' carries a subadditive function a, the restriction of a to T is strictly subadditive.*

Proof. We know

$$2a_i \geq \sum_{i-j \in T'} a_j \geq \sum_{i-j \in T}$$

where second inequality follows since every edge in T is an edge in T'. Since $T' \neq T$, there is at least one edge in T' not in T, so the inequality must be strict. □

We can now prove a previously stated theorem.

Theorem 2.5. *A graph T carries an additive function if and only if it is extended ADE. It carries a strictly subadditive function if and only if it is ADE.*

Proof. First, Lemma 2.2 does $\leftarrow$ for both. For $\rightarrow$, assume carries an additive function a and is not an extended ADE. Then by Lemma 2.1, either T is ADE or T *strictly* contains an extended ADE.

If T is ADE, then T carries a strictly subadditive function, contradicting Lemma 2.3. If T strictly contains an extended ADE, then this ADE carries a strictly subadditive function by Lemma 2.4, contradicting Lemma 2.3.

Finally if T carries a strictly subadditive function and its not ADE, then T contains an extended ADE, which must carry a strictly subadditive function by Lemma 2.4, contradicting Corollary 2.2. □

Corollary 2.3. *The M^{c}Kay graph of a binary polyhedral group is extended ADE, with additive function given by the dimensions of the irreducible representations. In particular, the 'extra vertex' has value 1.*

2.5 Another Aside: The Quadratic Form of a Graph

Definition. Let T be a finite connected graph, possibly with multiple edges. A quadratic form of T, also known as a Tits form, is the polynomial $q_T(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2 - \sum_{i-j} x_i x_j$, where as usual we count edges with multiplicity.

Example 2.4. $q_T(x_1, x_2) = x_1^2 + x_2^2 - x_1 x_2$.
$q_T(x_1, x_2) = x_1^2 + x_2^2 - 3x_1 x_2$

Observe that $q(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T C \mathbf{x}$, where C is the Coxeter matrix of T. So we wonder if q_T is related to (sub)additive functions.

Theorem 2.6. *The quadratic form q_T is positive definite, i.e. $q(x) \geq 0$ for all x and only zero for $x = 0$, if and only if T is an ADE diagram, and positive semidefinite, i.e. $q(x) \geq 0$, if and only if T is extended ADE.*

The theorem can be proved directly. Show that if q_T is positive definite, then T does not contain any cycles, or more than one branch point, or a vertex of degree > 3. So T is a T_{pqr} tree. Show that q_T is positive definite if and only if $1/p + 1/q + 1/r > 1$., so then ADE. □

One can also prove the theorem by translating q_T into the additive function notation:

Proposition 2.3. *If a is an additive function on T, then q_T is positive semidefinite. (also strictly subadditive then positive definite).*

Proof. Assume a is an additive function. For each edge $e : i - j$, define $q_e(x_1, \ldots, x_n) = \frac{1}{2a_ia_j}(a_ix_j - a_jx_i)^2$. The coefficient of x_i^2 is $\frac{1}{2a_ia_j}a_j^2 = \frac{a_j}{2a_i}$. The coefficient of x_ix_j is $\frac{1}{a_ia_j}(-2a_ia_j) = -1$. Consider the sum $\sum_e q_e(x_1, \ldots, x_n)$. Coefficient of x_ix_j is number of edges $i - j$. The coefficient of x_i^2 is $\sum_{\text{Edges e containing i}} \frac{a_j}{2a_i} = \frac{1}{2a_i}\sum a_j = 1$. So $q_T = \sum q_e$'s is a sum of squares, so positive semidefinite.

3 Invariant Theory & Resolution of Singularities

3.1 A Motivating Example

We now make a transition from groups and graphs to Commutative Algebra and Algebraic Geometry. We begin with a motivating example.

Example 3.1. Consider $C_2 \subseteq \mathrm{SL}_2(\mathbb{C})$, with generator $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Then C_2 acts on $\mathbb{C}^2$ by $\sigma(p) = -p$, i.e. σ is a rotation of Arg p by π. The quotient space of this group action has for points the orbit of the action: for every nonzero point $\{p, -p\}$, along with $\{0\}$. A fundamental domain for this action, i.e. a subset of $\mathbb{C}^2$ containing exactly one point from each orbit.

More precisely, let $\mathcal{C}$ denote a cone. We can define a continuous surjective map $\pi : \mathbb{C}^2 \to \mathcal{C}$ such that the fibers of π are precisely the orbits of the action. Choose coordinates so that the cone is defined by $y^2 = xz$, then $\pi(u, v) = (u^2, uv, v^2)$ is such a map. To be more systematic, instead consider the ring of polynomials $\mathbb{C}[u, v]$, thought of as the set of polynomials on $\mathbb{C}^2$. [The function u picks out the first coordinate of a point $p \in \mathbb{C}^2$ and so forth.]

The polynomial functions on the quotient space $\mathbb{C}^2/C_2$ are exactly the polynomials on $\mathbb{C}^2$ that are constant on orbits; that is, the polynomial functions are the set $\{f \in \mathbb{C}[u, v] \colon f(p) = f(-p) \text{ for all } p \in \mathbb{C}^2\} = \mathbb{C}[u^2.uv, v^2] \subseteq \mathbb{C}[u, v]$, note $\mathbb{C}[u^2, uv, v^2] \cong \mathbb{C}[x, y, z]/(y^2 - xz)$. Note that the ring $R := \mathbb{C}[u^2, uv, v^2]$ is an integral domain of dimension two, graded, integrally closed, Cohen-Maccaulay (in fact gorenstein), reflexive, and the polynomial ring $\mathbb{C}[u, v]$ is a finitely generated module over it. In fact, $\mathbb{C}[u, v] \cong R \oplus (Ru + Rv)$. Finally, every indecomposable reflexive R-module appears as a direct summand of the polynomial ring $\mathbb{C}[u, v]$. ◁

The question we shall explore is how many properties of the ring R in Example 3.1 are specific to this example, and how many are properties hold more generally.

3.2 Classical Invariant Theory of Finite Groups

Invariant Theory has connections to many fields, including tori and Lie groups. However, we shall only consider finite groups, so these shall not make an appearance. For this material, we follow Kraft-Procesi. In particular, we take a coordinate free approach whenever possible. Now let k be an infinite field and W a finite dimensional vector space. We say that a function $f : W \to k$ is regular if it is a polynomial in the elements of some basis of W—this is independent of basis. Let $k[W]$ be the ring of regular functions on W. If $\{x_1, \ldots, x_n\}$ were a basis for $W^* = \mathrm{Hom}(W, k)$, then $k[W] \cong k[x_1, \ldots, x_n]$ is a polynomial ring. This holds because the field is infinite, and this is not true for finite fields (the obstruction is nonzero vanishing functions).

Definition (Homogenous Function)**.** A regular function $f \in k[W]$ is homogeneous of degree d if $f(\lambda w) = \lambda^d w$ for all $\lambda \in k$ and $w \in W$.

Concretely in terms of a basis for W^*, this means that f is a linear combination of monomials of degree d, i.e. $x_1^{d_1} \cdots x_n^{d_n}$ with $d_1 + \cdots + d_n = d$. Since every polynomial is a sum of such monomials, every polynomial is a sum of homogeneous polynomials; that is, $f \in k[W]$ is uniquely a sum of homogeneous polynomials, so $k[W] \cong \bigoplus_{d \geq 0} k[W]_d$, where $k[W]_d =$ homogeneous regular functions of degree d. In particular, $k[W]$ is a graded ring, i.e. $A = \bigoplus A_i$ as abelian groups such that $A_i A_j \subseteq A_{i+j}$. As a final remark, we know that $k[W] \cong k[x_1, \ldots, x_n]$. Fixing a basis $\{e_1, \ldots, e_n\}$ for W, then $x_1, \ldots, x_n$ is a dual basis for W^*, i.e. $x_i(e_j) = \delta_{ij}$.

Now suppose we have a subgroup $G \subseteq \mathrm{GL}(W)$, or more generally a representation $\rho : G \to \mathrm{GL}(W)$. This gives an action of G on W: $gw := \rho(g)w$. In turn, this gives an action of G on $k[W]$, $(gf)(w) := f(g^{-1}w)$ (the (-1)-power is needed to get a left action). Moreover, this action is compatible (in fact the same as) the action of G on the dual space W^*. Keep in mind that $k[W]_1$ is the set of linear maps from $W \to k$, i.e. W^*. In fact, $k[W]_d = \mathrm{Sym}_d(W^*)$, the d^{th} symmetric power of W^*, as such it inherits the action of G on W^*.

Definition (Invariant Function)**.** A function $f \in k[W]$ is invariant (G-invariant) if $gf = f$ for all $g \in G$. Equivalently, $f(w) = f(gw)$ for all $g^{-1} \in G$, i.e. $g \in G$. We write $k[W]^G$ for the set $\{f \in k[W] : f \text{ invariant}\}$.

One can check that $k[W]^G$ is a ring: each $g \in G$ acts as an automorphism of $k[W]$.

Example 3.2. Let S_n be the symmetric group on n letters. Now S_n has an action on $W = k^n$ via $\sigma(e_i) = e_{\sigma(i)}$. Equivalently, $\sigma(a_1, \ldots, a_n) = (a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)})$. Then S_n also acts on $k[W] \cong k[x_1, \ldots, x_n]$, where $\{x_i\}_{i=1}^n$ is the dual basis. What is $\sigma(x_i)$? We know $x_i(e_j) = \delta_{ij}$, so

$$(\sigma x_i)(e_j) = x_i(\sigma^{-1}(e_j)) = x_i e_{\sigma^{-1}(j)} = \delta_{i\sigma^{-1}(j)}.$$

But this means $(\sigma x_i)(e_j) = \delta_{i\sigma^{-1}(j)} = 1$ if and only if $\sigma^{-1}(j) = i$ if and only if $\sigma(i) = j$. Therefore, $\sigma x_i = x_{\sigma(i)}$. Generally for any $f \in k[x_1, \ldots, x_n]$, $(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Now the question is which functions are invariant; that is, which functions of $k[x_1, \ldots, x_n]$ are independent of the order of the x_i? These are the symmetric polynomials, e.g. $x_1 + \cdots + x_n$, $x_1 \cdots x_n$, $x_1^7 + \cdots + x_n^7$. ◁

The symmetric polynomials in n variables are all composed of the elementary symmet-

ric polynomials, given as follows:

$$\begin{aligned}
s_0(x_1,\dots,x_n) &:= 1\\
s_1(x_1,\dots,x_n) &:= \sum_{1\le i\le n} x_i = x_1+\cdots+x_n\\
s_2(x_1,\dots,x_n) &:= \sum_{1\le i<j\le n} x_ix_j\\
s_3(x_1,\dots,x_n) &:= \sum_{1\le i<j<k\le n} x_ix_jx_k\\
&\vdots\\
s_n(x_1,\dots,x_n) &:= x_1\cdots x_n
\end{aligned}$$

Theorem 3.1 (Fundamental Theorem of Symmetric Functions/Newton's Theorem)**.** *Any symmetric polynomial in $x_1,\dots,x_n$ is uniquely expressible as a linear combination of elementary symmetric polynomials.*

In particular, the s_i's are algebraically independent of each other, i.e. there are no nontrivial polynomial relations among them. Therefore, it must be that $k[x_1,\dots,x_n]^{S_n} = k[s_1,\dots,s_n]$. This is indeed a polynomial ring since the s_i have no relations between them. There are algorithms to write any symmetric polynomial in the elementary symmetric polynomials.

Example 3.3.

(i) $x^2+y^2 = (x+y)^2-2xy = s_1^2-2s_2$

(ii) $x_1^3+x_2^3+x_3^3 = s_1^3-3s_1s_2+3s_3$

(iii) $x_1^2x_2+x_1^2x_3+x_2^2x_1+x_2^2x_3+x_3^2x_1+x_3^2x_2 = s_1s_2-3s_3$

◁

Remark. The power sums, $p_1(x_1,\dots,x_n) = x_1+\cdots+x_n$, $p_2(x_1,\dots,x_n) = x_1^2+\cdots+x_n^2$, …, $p_n(x_1,\dots,x_n) = x_1^n+\cdots+x_n^n$, also generate the ring of symmetric polynomials. The complete symmetric polynomials, the Schur polynomials, etc. all also generate the ring of symmetric polynomials. Hence, there are procedures from going from one set of these polynomials to another. The transition functions between them are crucial in the representation of S_n and GL_n (Schur-Weyl Theory).

As another aside, the discriminant of S_n acting on $x_1,\dots,x_n$ is[2]

$$\Delta = \prod_{i<j}(x_i-x_j)^2$$

The discriminant is symmetric, so it must be a polynomial in $s_1,\dots,s_n$.

[2]To some, this is the square of what they would define as the discriminant.

Example 3.4. If $n = 2$, then $\Delta = (x-y)^2 = x^2 - 2xy + y^2 = s_1^2 - 4s_2$. If $n = 3$, $\Delta = (x-y)^2(x-z)^2(y-z)^2 = s_1^2 s_2^2 - 4s_2^3 - 4s_1^3 s_3 - 27s_3^2 + 18s_1 s_2 s_3$.

Given a polynomial $g(t) \in \mathbb{C}[t]$ with roots $a_1, \ldots, a_n$ (with multiplicity), the discriminant of g is

$$\Delta(g) = \Delta(a_1, \ldots, a_n) = \prod_{i<j} (a_i - a_j)^2$$

Observe $\Delta(g) = 0$ if and only if g has a repeated root. For example, $g(t) = t^2 + bt + c$, then $\Delta(g) = b^2 - 4c$. An exercise for the reader is to show $\Delta(g) = (\det V)^2$, where V is the Vandermonde matrix:

$$V = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}$$

3.3 Restricting the Action of S_n

We want to restrict the action of S_n on $k[x_1, \ldots, x_n]$ to the subgroup $A_n \subseteq S_n$. All the symmetric functions are still invariant. Is anything else invariant? Notice that $(i\ j)\sqrt{\Delta} = -\sqrt{\Delta}$. So if σ is an even permutation, $\sigma(\sqrt{\Delta}) = \sqrt{\Delta}$.

FACT: $k[x_1, \ldots, x_n]^{A_n} = k[s_1, \ldots, s_n, \sqrt{\Delta}]$.

Indeed, we can think of $k[x_1, \ldots, x_n]^{A_n}$ as consisting of the symmetric polynomials and the sign-symmetric polynomials: $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = (-1)^{\mathrm{sgn}(\sigma)} f(x_1, \ldots, x_n)$.

Moreover, $\Delta = (\sqrt{\Delta})^2$ is a polynomial in the 'variables' $s_1, \ldots, s_n$. But then $k[x_1, \ldots, x_n]^{A_n}$ is isomorphic to a hypersurface ring: $k[y_1, \ldots, y_n, z]/(z^2 - f(y_1, \ldots, y_n))$.

First, a few basic questions about $k[W]^G$:

1. (Generators and Relations): Given a finite group $G \subseteq \mathrm{GL}(W)$, is the ring of invariants $k[W]^G$ a finitely generated k-algebra?

2. If so, describe them explicitly and also is the ideal of relations among the generators finitely generated?If so, describe them explicitly.

Following theorem due to Hilbert and Noether:

Theorem 3.2 (First Fundamental Theorem of Invariant Theory for Finite Groups)**.** *Let $k = \mathbb{C}$. The invariant ring $\mathbb{C}[W]^G$ is generated as a $\mathbb{C}$-algebra by at most $\binom{|G| + \dim W}{\dim W}$ homogeneous polynomials of degree at most $|G|$.*

Note $\binom{n+d}{d}$ is the vector space dimension of homogenous polynomials of degree d in n variables. Hilbert proved finiteness as an application of the Hilbert-Basis Theorem [1890]. The proof given was nonconstructive. There is a story that Gordan (rep. theory of binary forms, was constructive), is said to have a said thats not math thats theology. Mostly

believed to be a story. Hilbert later gave a constructive proof. [1890s]. Noether gave the bound in the theorem which is tight, by showing $k[W]^G$ is generated by

$$\left\{ \frac{1}{|G|} \sum_{g \in G} gm \colon m \text{ runs over monomials of degree } \leq |G| \right\}$$

Sketch of Hilbert's (nonconstructive proof)

Theorem 3.3 (Hilbert Basis Theorem)**.** *The polynomial ring $k[x_1, \ldots, x_n]$ is noetherian, i.e. every ideal of $k[x_1, \ldots, x_n]$ is finitely generated, where k is a field.*

Let $S = k[x_1, \ldots, x_n]$, $R = k[x_1, \ldots, x_n]^G \subseteq S$. Let I be the ideal of R generated by all invariants of positive degree.

Exercise: If I is a finitely generated ideal of $R = k[f_1, \ldots, f_t]$, say $I = Rf_1 + \cdots + Rf_t$, then $\{f_i\}$ generate the ring of invariants as a k-algebra. The proof follows by induction on the degree.

We know that IS is a finitely generated ideal of S by the Hilbert Basis Theorem. Define the Reynold's operator

$$\rho : S \to R$$
$$f \mapsto \frac{1}{|G|} \sum_{g \in G} gf.$$

Observe that

1. $\rho(S) \subseteq R$. We have seen this before in a different form. 2. ρ fixes R elementwise. 3. ρ is a ring homomorphism, and is R-linear: if $h \in S^G$, $f \in S$, then $\rho(hf) = h\rho(f)$ 4. For any ideal J of R, $JS = \{\sum as \colon a \in J, s \in S\}$. So $\rho(JS) = \{\rho(\sum as) \colon a \in J, s \in S\} = \{\sum \rho(as) \colon a \in J, s \in S\} = \{\sum \rho(s)a \colon a \in J, s \in S\} = \{\sum ra \colon r \in R, a \in J\} = J$. But then $\rho(JS) = J$. (3rd $=$ sign follows from 3) and last from ρ maps S onto R.

Then the ideal I generated by the invariants of positive degree is the same as $\rho(IS)$, and IS is finitely generated so I is as well.

Theorem 3.4 (The Second Fundamental Theorem of Invariant Theory for Finite Groups)**.** *The invariant ring is finitely generated. [Hilbert's Syzygy Theorem]*

There are versions of the 1st and 2nd Fundamental Theorem of Invariant Theory for many classes of groups.

Hilbert's 14$^{\text{th}}$ Problem (1900): $k[W]^G$ is *always* a finitely generated k-algebra, for any group G. Nagata gave the first counterexample in 1958.

A second problem is when is $k[W]^G$ a polynomial ring? More generally, does $k[W]$ always contain a polynomial ring over which it is a finitely generated module? Examples $k[W]^{S_n}$, $k[W]^{A_n}$, respectively. Completely solved by Chevalley and Shephard-Todd. Answer yes, as long as char $k \nmid |G|$. The key ideas are Noether normalization, which we shall address later.

Definition (Reflection)**.** An element $1 \neq g \in \mathrm{GL}(W)$ is a (true) reflection if fixes a hyperplane, i.e. a codimension one hyperspace, and satisfies $g^2 = 1$. Equivalently, g is conjugate to a diagonal matrix $(1, 1, \ldots, 1, -1)$. A pseudo-reflection if it fixes a hyperplane and has finite order. Equivalently if k is algebraically closed, then g is conjugate to a diagonal matrix $1, 1, \ldots, 1, \omega$, where ω is some n^{th} root of unity.

Definition. Let $G \subseteq \mathrm{GL}(W)$ be finite. Let G'' be the subgroup generated by reflections. G' be the subgroup generated by pseudo-reflections. Then $G'' \subseteq G' \subseteq G$.

Note: Both are normal in G, since a conjugate of a (psuedo-) reflection

Definition (Reflection Group)**.** We say G reflection group if $G'' = G$, i.e. G is generated by reflections. G pseudo-reflection group (or sometimes complex reflection group) if $G' = G$, i.e. G is generated by pseudo-reflections.

Example 3.5.

(i) S_n acting on $k[x_1, \ldots, x_n]$ is generated by reflections: $(i\ j)$ fixes the subspace $\langle x_3, --, x_n, x_1 + x_2 \rangle$, etc..

(ii) S_n acting on the subspace $W \subseteq k^n$ defined by $x_1 + \cdots + x_n = 0$ (standard representation). This is also a reflection group (ltr).

Theorem 3.5 (Chevalley, Shepherd-Todd)**.** *Let $G \subseteq \mathrm{GL}(W)$ be a finite group. Then $k[W]^G$ is a polynomial ring, i.e. is generated over k by algebraically independent elements if and only if G is a pseudo-reflection group.*

At the other end of the spectrum, say G is small if it contains no pseudo-reflections.

First, if $G \subseteq \mathrm{SL}(W)$, then any $g \in G$ has $\det g = 1$, so G must be small.

Second, can always reduce to the small case in studying $k[W]^G$. Let $G' \subseteq G$ be the subspace generated by pseudo-reflections. Then $k[W]^G \subseteq k[W]^{G'}$. The right side is a polynomial ring by Theorem 3.5. In fact, $k[W]^G \cong (k[W]^{G'})^{G/G'}$, on right G acts as identity on $k[W]^{G'}$ and the quotient kills it so should be the same.

Back to examples. Aiming to understand binary polyhedral groups. Recall in the example of A_n, we looked at the 'sign-symmetric' polynomials, i.e. $\{f \in k[W] \colon \sigma f = (-1)^{\mathrm{sgn}(\sigma)} f\}$. This is a special case of relative invariants.

Definition. Suppose there is a function $\chi : G \to k^\times$ so that $gf = \chi(g)f$ for all $g \in G$. Say that f is a relative invariant for χ. We say that f is a relative invariant for χ.

Notice that χ is a homomorphism of groups. In other words, χ is a 1-dimensional representation of G, also known in this context as a linear character. Let $k[W]^G_\chi$ be the set of all such things, i.e. $\{f \in k[W] \colon f \text{ relative invariant for } \chi\}$. In particular, $k[W]^G_{\mathrm{triv}} = \{f \in k[W] \colon gf = \mathrm{triv}(g)f \text{ for all g}\} = k[W]^G$.

Observe that $k[W]^G_\chi$ is a module over $k[W]^G$. So if f is an invariant, h relative invariant, then for any $g \in G$

$$g(fh) = g(f)g(h) = f\chi(g)h = \chi(g)fh.$$

Example 3.6.

(i) $C_n \subseteq \mathrm{GL}_2(k)$, generated by $\sigma = \begin{pmatrix} \omega_n & \\ & \omega_n \end{pmatrix}$. Then C_n acts on $k[x,y]$ by $\sigma(x) = \omega x$, $\sigma(y) = \omega y$, $\omega = \omega_n$, $\sigma(x^a y^b) = \omega^{a+b} x^a y^b$. So $x^a y^b \in k[x,y]^{C_n}$ if and only if $a + b \equiv 0 \mod n$. Every invariant polynomial is a sum of invariant monomials since each monomial is taken to a scalar multiple of itself. So $k[x,y]^{C_n} = k[\{x^a y^b : a + b \equiv 0 \mod n, a, b \geq 0\}]$. In fact, $k[x^n, x^{n-1}y, x^{n-2}y^2, \ldots, xy^{n-1}, y^n]$, the n^{th} Veronese subring of $k[x,y]^n$.

Take a character χ_j of C_n, which takes σ to ω^j, $0 \leq j < n$. $k[x,y]^{C_n}_{\chi_j} = \{f \in k[x,y] : gf = \chi_j(g)f\} = \{f : \sigma f = \chi_j(\sigma) f\} = \{f : \sigma f = \omega^j f\}$. A monomial $x^a y^b$ is χ_j relatively invariant if and only if $a + b \equiv j \mod n$.

If $j = 1$: Get x, y. Then obtain $k[x,y]$. Oops, not a ring! As a module over $R := k[x^n, x^{n-1}y, x^{n-2}y^2, \ldots, xy^{n-1}, y^n]$ is generated by x and y. Contains monomials such as $x, y, x^{n+1}, x^n y, x^{n-1}y^2, \ldots$.

If j arbitrary, then $k[x,y]^{C_n}_{\chi_j} = R(x^j, x^{j-1}y, \ldots, xy^{j-1}, y^j)$, the R span of the monomials given. "the k-span of all monomials of degree $j \mod n$." In this case, we get $k[x,y] = \bigoplus_{j=0}^{n-1} k$-span of monomials deg $j \mod n$, which is $R \oplus I_1 \oplus I_2 \oplus \cdots \oplus I_{n-1}$, where $I_j := R(x^j, x^{j-1}y, \ldots, xy^{j-1}, y^j)$, a direct sum decomposition of $k[x,y]$ as an R-module.

Remark that R is the same as $k[a_1, \ldots, a_{n+1}]/J$, where J is generated by the two-by-two minors

(ii) $C_n \subseteq \mathrm{SL}_2(k)$, generated by $\sigma = \begin{pmatrix} \omega_n & \\ & \omega_n^{-1} \end{pmatrix}$. This acts on $k[u,v]$. by $\sigma(u) = \omega u$, $\sigma(v) = \omega^{-1} v$. Suffices to consider only monomials. $\sigma(u^a v^b) = \omega^{a-b} u^a v^b$. Then $k[u,v]^{C_n} = k[\{u^a v^b : a - b \equiv 0 \mod n\} = k[u^n, uv, v^n] \cong k[x,y,z]/(xz - y^n)$.

Do not have to work only with monomials. Another generating set of invariants: $u^n + v^n, uv, u^n - v^n$ (as long as we can divide by 2 in k). These three are related by $(u^n + v^n)^2 = (u^n - v^n)^2 + 4(uv)^n$. Letting $X^2 = Z^2 + 4Y^n$. Could also replace Y by $\sqrt[n]{\frac{1}{4}Y}$, turning into pure power so that $Z^2 = X^2 - Y^n$.

For a character χ_j are before, $k[u,v]^{C_n}_{\chi_j}$ is k-span of monomials $u^a v^b$, such that $a - b \equiv j \mod n$.

(iii)

Example 3.7. The binary dihedral group $B\mathbf{D}_4$ of order 16 generated by $C_4 = \langle \begin{pmatrix} \omega_4 & \\ & \omega_4^{-1} \end{pmatrix} \rangle = \langle \begin{pmatrix} i & \\ & -i \end{pmatrix} \rangle = \sigma$ and $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. The matrix A sends u to iv, v to iu. The invariants of C_4

are generated by u^4, uv, v^4. The matrix A sends u^4 to $(iv)^4 = v^4$. uv to $(iv)(iu) = -uv$, v^4 to u^4. So in this case monomials not always sent to scalar multiples of themselves. So it is not necessarily the case that a polynomial is invariant iff all its monomials are. But we can see that $u^4 + v^4$ is invariant under C_4 and A, hence is invariant of $B\mathbf{D}_4$. Ditto for u^2v^2 and $uv(u^4 - v^4)$. Not too hard to see thats all. So $k[u,v]^{B\mathbf{D}_4} = k[u^4 + v^4, u^2v^2, uv(u^4 - v^4)]$, label these X, Y, Z. $Z^2 = Y(X^2 - 4Y^2x^2Y - 4Y^3$. Possible to adjust Y so that relation is $Z^2 = X^2Y - Y^3$. Therefore, $k[u,v]^{B\mathbf{D}_4} \cong k[x,y,z]/(z^2 - x^2y + y^3)$.

More generally, $k[u,v]^{B\mathbf{D}_n} \cong k[x,y,z]/(z^2 - x^2y + y^{n-1})$.

Theorem 3.6 (Klein, 1884)**.** *For each of the binary polyhedral groups G in $\mathrm{SL}_2(\mathbb{C})$, the ring of invariants $\mathbb{C}[u,v]^G$ is generated by three fundamental invariants which satisfy a single relation. Therefore, $\mathbb{C}[u,v]^G \cong \mathbb{C}[x,y,z]/(f(x,y,z))$, where The polynomials are called the Kleinian*

Name	Group	$f(x,y,z)$
(A_{n-1})	C_n	$xz - y^n$ or $z^2 - x^2 - y^n$
(D_{n+1})	$B\mathbf{D}_n$	$z^2 - x^2y + y^{N-1}$
(E_6)	$B\mathbf{T}$	$z^2 - x^3 - y^4$
(E_7)	$B\mathbf{O}$	$z^2 - x^3 - xy^3$
(E_8)	$B\mathbf{I}$	$z^2 - x^3 - y^5$

hypersurface singularities.

Proof (Sketch). We sketch the proof in the Platonic solids case E_6, E_7, E_8. Let $G = B\mathbf{T}, B\mathcal{O}, B\mathbf{I} \subseteq \mathrm{SL}_2(\mathbb{C})$. Then G acts on $\mathbb{C}^2$ so that it acts on the projective line $\mathbb{P}^1$, identified with the 2-sphere by stereographic projection

Given a point $[a\colon b] \in \mathbb{P}^1$ $(= [\lambda a\colon \lambda b], \lambda \neq 0)$. It has an orbit under G, say $\mathcal{O} = \{[a_1\colon b_1] = [a\colon b], [a_2\colon b_2], \ldots, [a_t\colon b_t]\}$. The polynomial

$$f(u,v) = \prod_{i=1}^{t}(b_iu - a_iv) \in \mathbb{C}[u,v]$$

is invariant under the action of G since G simply permutes its factors. Geometrically, $\mathcal{O}$ is the zero set of $f(u,v)$ in $\mathbb{P}^1$. Call $\mathcal{O}$ the divisor of f. On the other hand, given a homogeneous polynomial $f(u,v) \in \mathbb{C}[u,v]$, there is a factorization (FTOA)

$$f(u,v) = \prod_{i=1}^{t}(b_iu - a_iv)$$

only unique up to scalar multiples of the factors. So the set of points $\{[a_i\colon b_i]\}$ is well-defined on the projective line. We know (Klein knew) 3 particular orbits

so we get

$$V(u,v) = \prod_{vertices [a_i,b_i]} (b_i u - a_i v)$$

$$E(u,v) = \prod_{edgescenters}$$

$$F(u,v) = \prod_{facecenters}$$

Klein knew these *explicitly*. Next, use the group theory and degrees of polynomials to show that V, E, F generate all invariants. Then, use the explicit forms to find the relation. □

Details for $B\mathbf{I}$, see Nash "On Klein's Icosahedral Solution of the Quintic." on BB.

3.4 Deformation Theory

Another place where the Kleinian singularities appear, this time as the "simple singularities." Roughly speaking, these are the ones that deform into finitely many others.

This section we work with germs of hypersurface singularities up to right equivalence: these are pairs (f, O), where f is convergent power series in n variables O is the origin in $\mathcal{A}^n$ and $(f, O) \sim (g, O)$ if there is an automorphism ϕ of $\mathcal{A}^n$ and an open (in Euclidean topology) neighborhood U of O so that $f = g\phi$ on U. So we focus on local properties of f.

EG $f(x,y) = xy(x-y)(x-\lambda y)$. for $\lambda \neq 0, 1$. Then f defines a (germ of a) plane curve. We can associate to f the 4 points on $\mathbb{P}^1$: $0, 1, \infty, \lambda$. The cross-ratios of 4 points on $\mathbb{P}^1$, $z_1, \ldots, z_4$ is

$$(z_1, z_2; z_3, z_4) = \frac{(z_3 - z_1)(z_4 - z_2)}{(z_3 - z_2)(z_4 - z_1)}$$

An exercise is to show that any automorphism of $\mathbb{C}[x,y]$ takes $f(x,y)$ another product of 4 linear factors, leaving the cross-ratio invariant. So there are infinitely many right equivalence classes of quartic germs.

Definition (Singularity)**.** $f(x_1, \ldots, f_n)$ has a singular point at 0 if f vanishes at 0 and so do all partial derivatives $\dfrac{\partial f}{\partial x_i}$ for $i = 1, \ldots, n$.

Example 3.8. $f(x,y) = x^2 + y^n$ has partials $2x$ and ny^{n-1}. These both vanish at $(0,0)$ and $f(0,0) = 0$ so the origin is a singular points.

$n = 2$, $x^2 + y^2 = (x - iy)(x + iy)$ so the singular points looks like the intersection of two lines.

$n = 3$: $x^2 + y^3$

This is a cusp.

$n \geq 4$ "higher-order cusp".

Example 3.9. $f(x,y,z) = xy^2 + z^2$, $\nabla f = \langle y^2, 2xy, 2z\rangle$. These all vanish if and only if $y = 0 = z$ and x arbitrary. So x-axis. We say that these are non-isolated singular points.

Definition (Deformation)**.** A deformation of a germ (f, O) (or of its vanishing set $(V(f), 0)$) is a flat morphism $\pi : \mathfrak{X} \to B$, where B has a distinguished point $b \in B$ and $\pi^{-1}(b)$ is isomorphic to $V(f)$.

For us, B will always be $\mathcal{A}^n$. Possible for $\pi^{-1}(b)$ to have singularities. Think of the $\mathfrak{X}$ as a family parametrized by B. The flatness assumption has two critical consequences: it forces all the fibers $\pi^{-1}(c)$ to have the same dimension as c runs over B (weird for curve to deform to surface) and "multiplicity is upper semi-continuous" in flat families, so the singularities of other fibers are no worse than those with which we started with.

Example 3.10. Take $f(x,y) = x^2 + y^3$. Let B be the affine plane $\mathcal{A}^2$, with coordinates u, v. Let $\mathfrak{X}$ be the subset of $\mathcal{A}^4$ $\{(x,y,u,v)\colon x^2 + y^3 + uv + v = 0\}$ and define $\pi : \mathfrak{X} \to B$ given by $(x,y,u,v) \mapsto (u,v)$. The fiber over $0 \in B$ is $\{(x,y,u,v)\colon x^2 + y^3 + uy + v = 0, u = v = 0\}$. $= \{(x,y,0,0)\colon x^2 + y^3 = 0\}$, clearly isomorphic to $V(f)$.

The fiber over $(-3,2)$ is the vanishing set of $x^2 + y^3 - 3y + 2 = 0$. if and only if $x^2 + (y-1)^2(y+2) = 0$. is isomorphic to the vanishing set of $x^2 + y^2$.

So this is just the vanishing set consisting of two lines crossing

We discussed deformations 'geometrically' and also algebraically as introducing new parameters, e.g. $x^2 + y^3 + uy + v$ is a deformation of $x^2 + y^3$ over the base $\mathcal{A}^2$ with coordinates u, v.

Fact: There is a certain deformation of an isolated (see below) hypersurface singularity from which all others can be obtained, up to right equivalence of germs—called a versal deformation. [Note that versal means there exists, universal means there exists a unique.]

The hypersurface $f(x_1, \ldots, x_n) = 0$ has an isolated singularity at 0 if 0 is a singular point (all partials vanish) but there is a neighborhood of 0 not containing any other singular points. Equivalently, the ideal of $\mathbb{C}\{x_1, \ldots, x_n\}$ generated by $f, \frac{\partial f}{\partial x}, \ldots, \frac{\partial f}{\partial x_n}$, contains a power of the ideal generated by $(x_1, \ldots, x_n)$, i.e. its m-primary ideal.

Theorem 3.7. *Let $f(x_1, \ldots, x_n) \in \mathbb{C}\{x_1, \ldots, x_n\}$ have an isolated singularity at 0. Let $T^1 := \mathbb{C}\{x_1, \ldots, x_n\}/(f, \frac{\partial f}{\partial x}, \ldots, \frac{\partial f}{\partial x_n})$, the Tjurina algebra of f, and let $g_1, \ldots, g_m$ be a $\mathbb{C}$-basis for $\mathbb{C}$. Then*

$$f + \sum_{i=1}^{m} u_i g_i$$

defines a versal deformation of f over the base $\mathcal{A}^m$ with coordinates $u_1, \ldots, u_m$.

Example 3.11. $f(x,y) = x^2 + y^3$ $T^1 = \mathbb{C}\{x,y\}/(x^2 + y^3, 2x, 3y^2)$. Observe 2,3 do nothing as invertible, so $T^1 = \mathbb{C}\{x,y\}/(x^2 + y^3, x, y^2)$. Killed x so may as well not include $\mathbb{C}\{y\}/(y^3, y^2)$. Killed y^2 so no need to kill y^3, that's just mean $\mathbb{C}\{y\}/(y^2)$. A basis is $\{1, y\}$. So $f + u_1 1 + u_2 y$ is a versal deformation of f. It's isomorphic to $x^2 + y^3 + uy + v$, which is an example we saw presviously.

Example 3.12. $f(x,y) = xy^2$, y axis and two x-axes. $T^1 = \mathbb{C}\{x,y\}/(xy^2, y^2, 2xy) = \mathbb{C}\{x,y\}/(xy^2, y^2, xy) = \mathbb{C}\{x,y\}/(y^2, xy)$. A basis as a $\mathbb{C}$ vector space is $\{1, y, x, x^2, \ldots\}$. But this is not finite as f does not define an isolated singularity.

Example 3.13. $f(x,y) = x^4 + y^4$. $T^1 = \mathbb{C}\{x,y\}/(x^4 + y^4, x^3, y^3\} = \mathbb{C}\{x,y\}/(x^3, y^3)$.

A versal defomration is $x^4 + y^4 + u_1 1 + u_2 x + u_3 y + \cdots + u_9 x^2 y^2$ In particular, there is a deformation of $x^4 + y^4$ given by $x^4 + y^4 + \lambda x^2 y^2$. This is right equivalent to $xy(x-y)(x-\mu y)$ which are non-equivalent for distinct values of μ. So $x^4 + y^4$ deforms to infinitely many equivalence classes of singularities.

Example 3.14. $f(x,y,z) = x^2 + y^2 + z^2$, the cone.

$T^1 = \mathbb{C}\{x,y,z\}/(x^2 + y^2 + z^2, x, y, z) = \mathbb{C}$. So the versal deformation is $x^2 + y^2 + z^2 + u$.

One may then ask which singularities deform to only finitely many others? More generally, which ones deform to a k-parameter family? (modality k). The answer to the first is Kleinian singularities.

Theorem 3.8 (V.I. Arnold)**.** *Let $f(x,y) = 0$ be a germ of a plane n-dimensional hypersurface curve singularity with an isolated singularity at 0. Then f is simple, i.e. deforms to only finitely many right equivalence classes of singularities if and only if f is one of the following: $x^2 + y^{n+1} + z_1^2 + \cdots + z_{n-1}^2$ $n \geq 1$, $x^2 y + y^{n-1} + z_1^2 + \cdots + z_{n-1}^2$ $n \geq 4$, $x^3 + y^4 + z_1^2 + \cdots + z_{n-1}^2$, $x^3 + xy^3 + z_1^2 + \cdots + z_{n-1}^2$, $x^3 + y^3 + z_1^2 + \cdots + z_{n-1}^2$, named A_n, D_n, E_6, E_7, E_8, respectively. In particular, $n = 2$ gives the Kleinian singularities.*

3.5 Resolving Singularities

Won't say the word scheme–that gives it power.

Resolving singularities of Kleinian singularities via blowups of points. Our goal will be to compute the dual graphs of the resolutions of the ADE surface singularities.

Definition (Singular Locus)**.** The singular locus of a hypersurface defined by $f(x_1, \ldots, x_n) = 0$ is the vanishing set of the ideal $(f, \frac{\partial f}{\partial x}, \ldots, \dfrac{\partial f}{\partial x_n})$. It is a subset of $V = V(f)$.

The goal of a resolution of singularities is to replace $V(f)$ by another algebraic set which is isomorphic to $V(f)$ 'almost everywhere' and is nonsingular (has empty singular locus), almost everywhere here meaning everywhere except the singular locus. Let V_{sing} be the singular locus of V and V_{smooth} be $V \setminus V_{\text{sing}}$.

Definition. A resolution of singularities of an algebraic set V is a map $\pi : X \to V$ such that

- X is nonsingular
- π is a bijection over $\pi|_{\pi^{-1}(V_{\text{smooth}})} : \pi^{-1}(V_{\text{smooth}}) \to V_{\text{smooth}}$ is $\cong$

- π is proper, e.g. X is a subset of some projective space over V.

Theorem 3.9 (Hironaka, 1964)**.** *These exist for any algebraic set V defined over a field of characteristic zero.*

This is still open in characteristic p, dimension 4 or higher. The main tool was the blowup of a nonsingular subset of V (for us a point). We replace the origin by a projective space $\mathbb{P}^n$, the points of which correspond to the "directions of approach" to the origin.

First, blowing up the origin in affine space. Take $\mathcal{A}^n$ with coordinates $x_1, \ldots, x_n$, $\mathbb{P}_{n-1}$ with coordinates $[u_1, \ldots, u_n]$. Consider the subset $X \subseteq \mathcal{A}^n \times \mathbb{P}^{n-1}$ defined by $X = \{\{(x_1, \ldots, x_n); [u_1, \ldots, u_n]\} : x_i u_j = x_j u_i, i < j\}$

In the case $n = 2$, $\mathcal{A}^2_{x,y}$, $\mathbb{P}^1_{u:v}$. $X = \{((x, y), [u : v]) \colon xv = yu\}$. There is a map $X \to \mathcal{A}^2$ sending $((x, y), [u : v]) \mapsto (x, y)$ if $(x, y) \neq (0, 0)$. What is $\pi^{-1}(x, y)$? $((2, -3), [2\colon -3]) \mapsto (2, -3)$, exactly one such point. At the origin, $\pi^{-1}(0, 0) = \{((0, 0), [u : v])\} \cong \mathbb{P}^1$.

Remark. $X = \mathrm{Proj}(S[x_1 t, \ldots, x_n t])$, where $S = \mathbb{C}[x_1, \ldots, x_n]$ is degree 0 with $\deg t = 1$. Note that $S[x_1 t, \ldots, x_n t] \subseteq S[t]$. Defining $u_k := x_i t$, the relations $x_i u_j = x_j u_i$ imply $x_i(x_j t) = x_j(x_i t)$.

Observations about X.

- We have a map $\pi : X \to \mathcal{A}^n$ given by $(p, q) \mapsto p$.
- The fiber of π over the origin $(0, \ldots, 0)$ is $\{(x_1, \ldots, x_n); [u_1, \ldots, u_n] \colon x_1 = x_2 = \cdots = x_n = 0\} \cong \mathbb{P}^{n-1}$.
- The fiber over a point $(x_1, \ldots, x_n) \neq (0, 0, \ldots, 0)$ is the single point $((x_1, \ldots, x_n), [x_1 : x_2 : \cdots : x_n])$. Therefore, π is a bijection away from the origin.

Then X looks like a copy of $\mathcal{A}^n$ with the origin replaced by $\mathbb{P}^{n-1}$.

- X is not just the union of $(\mathcal{A}^n \setminus \{0\}) \cup \mathbb{P}^{n-1}$, in fact, it is irreducible (as a variety, or a topological space in the Zariski topology), which we shall show soon (see the notes)
- In the case $n = 2$,
$$X = \{((x, y), [u : v]) \colon xv = yu\}.$$
Consider a line through the origin in $\mathcal{A}^2$ and its preimage in X.

  $L = \{(ta, tb) \colon t \in \mathbb{C}\}$. For $t \neq 0$, there is a unique point in X lying over that point on the line. So if we let $L' = L \setminus \{(0, 0)\}$, then $\pi^{-1}(L')$ is a punctured line in X. Its closure in X, $\overline{\pi^{-1}(L')}$ is $\overline{\{((ta, tb), [ta : tb]) \colon t \neq 0\}} = \{((ta, tb), [ta : tb])\} = \{((ta, tb), [a : b])\}$. The 'new point' must be on the 'exceptional fiber' $\mathbb{P}^1$, the point $[a : b]$ on $\mathbb{P}^1$. The correspondence sending the line $L = \{(ta, tb)\}$ to the point $[a : b]$ is a bijection between points of the exceptional fibre and lines through the origin. The same is true for all n.

Blowing up the origin in a subset of $\mathcal{A}^n$.

Suppose $Y \subseteq \mathcal{A}^n$ containing $(0,0,\ldots,0)$. Then the blowup of Y at $(0,0,\ldots,0)$ is

$$\overline{Y} := \overline{\pi^{-1}(Y \setminus \{(0,0,\ldots,0)\})},$$

where $\pi : X \to \mathcal{A}^n$ is the blowup from before.

The blow up of a line through the origin is just a line in X, which meets the exceptional fiber at one point.

FACT: $\tilde{Y}$ is defined as a subset of $\mathcal{A}^n \times \mathbb{P}^{n-1}$ by the equations defining Y, plus $x_i u_i = x_j u_i$ for $i \neq j$.

We have $\pi^{-1}(Y) = \pi^{-1}(Y \setminus \{(0,0,\ldots,0)\}) \cup \pi^{-1}((0,0,\ldots,0)) = \tilde{Y} \cup E$, where $E \cong \mathbb{P}^{n-1}$ is the exceptional fiber. We call $\tilde{Y}$ the strict transform of Y and $\pi^{-1}(Y)$ the total transform.

Example 3.15. Take Y to be the union of the x and y axes in $\mathcal{A}^2$ defined by $xy = 0$. In fact, the total transform $\pi^{-1}(Y)$ is defined by the equations of Y and $x_i u_j = x_j u_i$

We know the preimage of the x-axis is a line in x meeting E, the exceptional fiber, at the point $[1:0]$. Similarly, the preimage of the y-axis os a line meeting E, the exceptional fiber, at the point $[0:1]$. So $\tilde{Y}$ is the union of two skew lines.

Recall $\mathbb{P}^{n-1} = \{[u_1,\ldots,u_n] \colon u_i \text{ not all } 0/\sim$ is covered by affine chartsL $U_1 = \{[u_1,\ldots,u_n] \colon u_i \neq 0\} \cong \mathcal{A}^{n-1}$, since we can scale so that $u_i = 1$, so $= \{[u_1,\ldots,1,u_i,\ldots,u_n]\}$

Continuing the example. Consider the chart where $u \neq 0$. On this chart, $\tilde{Y}$ is defined by $xy = 0$ and $y = xv$. So it is defined by $x^2 v = 0$ ($y = vx$). This is the union of $\{x^2 = 0\}$ with $\{v = 0\}$. If $x^2 = 0$, then $x = 0$, so $y = xv = 0$. So we have the point $\{(0,0),[1:v]\}$.

Alternatively, consider subset of X where $v = 0$. Then in particular $u \neq 0$.

So in this char $u = 1$, we have $x = 0 : E$, $v = 0 : ((x,0),[1:0])$, $\pi^{-1}(x - axis)$.

In the chart $v = 1$, we get $y = 0$: the $v = 1$ chart of E, $u = 0 : \pi^{-1}(y - axis)$.

Example 3.16. $Y : \{x^2 + y^3 = 0\}$ cusp, (A_2) singularity from previous table. The total transform $\pi^{-1}(Y)$ is defined by $x^2 + y^3 = 0$, $xv = yu$ in $\mathcal{A}^2 \times \mathbb{P}^1$. Charts again: $u = 1$: Here $y = xv$ and $x^2 + (xv)^3 = 0$. Then $x^2(1 + xv^3) = 0$. This defines a union of two algebraic sets: $x^2 = 0$ and $1 + xv^3 = 0$.

There are then two cases: $x^2 = 0$. Then $y = 0$ as well so then $\{((0,0),[1:v])\}$, an affine chart of $E \cong \mathbb{P}^1$.

In the case of $1 + xv^3 = 0$.....who knows but there are no singular points (partials vanish only at $x = v = 0$, which is not on vanishing set of $1 + xv^3$. For any $x \neq 0$, there are three distinct points, the three cube roots.

In the other chart, $v = 1$, $x^2 + y^3 = 0$, $x = yu$. We substitute in: $y^2u^2 + y^3 = 0$. Gives $y^2(u^2 + y) = 0$.

y^2 is part of E and $u^2 + y$ is a parabola.

Following image from Hauser:

We have resolved the singularity of the curve at the origin. But could do more, or ask for more. The total transform $(E \cup \tilde{Y})$ still has a singularity (see the intersection of line and parabola, meet at point of tangency). We could blow up again, and again,... until the total transform has 'simple normal crossing' singularities, i.e. no tangency. So we would blow up the vanishing set of $y^2(u^2+y)$ in the uy-plane at the origin in the (u,y)-plane.

Exercise: One more blowup is enough: we get x crossing for total transform.

The composition takes $\tilde{\tilde{Y}}$ to Y and collapses both E's to the origin. The exceptional fiber of the whole operation is

The number of times we have to blow up is measure of how singular the original was, i.e. its 'multiplicity.'

There are examples where blowing up increases the multiplicity. However, there are other numbers one can attach to these that go down when blowing up. Hironaka's proof is 17 nested inductions to show that blow-ups and normalization eventually resolve the singularities.

Notice: $\pi^{-1}(Y) = \tilde{Y} \cup \pi^{-1}((0,0,\ldots,0))$ is cut out by $f_1 = \cdots = f_n = 0$ and the equations defining X. The exceptional fiber of the blowup of Y is $\tilde{Y} \cap \pi^{-1}(0) = E$. Equivalently, it is $(\pi|_{\tilde{Y}})^{-1}((0,0,\ldots,0))$.

E.g. $f = x^2 + y^3$.

Chart: $u = 1$: $y = xv$ then $x^2 + c^3v^3 = 0$, then $x^2(1+xv^3) = 0$. $x^2 = 0$ defines the exceptional fiber of the blowup of $\mathcal{A}^n$ $1 + xv^3 = 0$ defines the strict transform in this chart (which is smooth curve in xv-plane) $x^2 = 0 = 1 + xv^3$ defines the exceptional fiber of the blowup of Y. It's empty.

Chart $v = 1$: $x = yu$ then $y^2u^2 + y^3 = 0$, then $y^2(u^2+y) = 0$. Now $y = 0$ gives exceptional fiber $\mathbb{P}^1$. $u^2 + y = 0$ gives strict transform of Y (the blowup of Y), which in this case is smooth (a parabola). The exceptional fiber is $y^2 = u^2 + y = 0$ is the u-axis intersected the curve $-u^2$ so it is a single point—$(0,0)$.

Example 3.17. $f = x^2 + y^2 + z^2$, the cone. This is an A_1 singularity: $A_n : x^2 + y^{n+1} + z^2$. First, we blowup $\mathcal{A}^3$ at $(0,0,\ldots,0)$.

$$X = \{((x,y,z),[u:v:w]) \colon xv = yu, xw = zu, yw = zv\} \subseteq \mathcal{A}^3 \times \mathbb{P}^2.$$

Consider the chart $u = 1$. Then $y = xv$, $z = xw$. We also have $yw = zv$. Then f becomes $x^2 + x^2v^2 + x^2w^2 = 0$. $x^2(1 + v^2 + w^2) = 0$. Now $x^2 = 0$ so $x = 0$ but then $y = z = 0$, this defines $\pi^{-1}(0)$. Now $1 + v^2 + w^2 = 0$ defines a cylinder in xvw-space. So the blowup of Y is a cylinder. The exceptional fiber of this blowup is defined by $x^2 = 1 + v^2 + w^2 = s0$. The intersection of the cylinder with the vw-plane

By symmetry, $\tilde{Y}$ is smooth in all three charts, and the exceptional fiber of $\tilde{Y} \to Y$ is a projective line $\mathbb{P}^1$ (by theorems it's a projective rational curve). The dual graph of the resolution

Example 3.18. All A_n singularities at once: $x^2 + y^{n+1} + z^2 = 0$, where $n \geq 2$. Start with the chart where $v = 1$.

$v = 1$: $x = yu$, $z = yw$. Then $y^2u^2 + y^{n+1}y^2w^2 = 0$. Then $y^2(u^2 + y^{n-1} + w^2) = 0$. The y^2 is the exceptional fiber. The strict fiber is given by $u^2 + y^{n-1} + w^2 = 0$, which is sort of A_{n-2}. If $n = 1$, (the previous example), then it's the cylinder, so smooth, and the exceptional fiber is a single $\P^1$.

If $n = 2$, $u^2 + y + w^2 = 0$ is smooth (by Jacobian criterion). The exceptional fiber is $y^2 = 0 = u^2 + y + w^2$. The first says $y^2 = 0$ so $y = 0$ then $u^2 + w^2 = 0$ in uw-plane. Then $(u - iw)(u + iw) = 0$ is a pair of crossing lines.

If $n \geq 3$, then the blowup is an A_{n-2} singularity in yuw-space. The exceptional fiber is again two lines. So now we just iterate blowing up the origin in yuw-space and continue. Each time the subscript of A_{n-2} decreases down until we hit either of the cases above. So it depends only on the parity, i.e. last blowup is either of type A_2 or A_1.

For all n, the dual graph is the A_n Coxeter-Dynkin diagram.

Example 3.19. D_4: $x^3 + x^3y + z^2 = 0$. The $v = 1$ and $w = 1$ charts are smooth (check!) So these are boring. Consider now

$u = 1$: $y = xv$, $z = xw$. We then get $x^2(xv + xv^3 + w^2) = 0$. x^2 is the exceptional fiber. Now $xv + xv^3 + w^2$ has gradient $\nabla = \langle v + v^3, x + 3xv^2, 2w \rangle$ so that $w = 0$. There are, as it turns out, three singular points: $(0, 0, 0)$, $(0, i, 0)$, $(0, -i, 0)$. Observe $xv + xv^3 + w^2 = xv(v_i)(v - i) + w^2$ has A_1 singularities at the points $(xv + w^2 \sim x^2 + v^2 + w^2)$. Blow up each of those and the result is smooth.

The exceptional set of the first blowup is defined by $x^2 = xv + xv^3 + w^2 = 0$ in xvw=-space. $x = w = 0$, the v-axis, i.e. a line E_0. Notice that the three A_1 singularities lie on the exceptional fiber. So when we blow them up and replace them by a $\mathbb{P}^1$, which intsects E_0.

The geometric picture is

Example 3.20. D_n: $x^2y + y^{n-1} + z^2$ for $n \geq 5$. Blowing up the origin gives a D_{n-2} with an exceptional fiber of two $\mathbb{P}^1$'s.

Example 3.21. E_6 $x^2 + y^3 + z^4 = 0$. This takes 4 blowups.

Blowup 1, chart $w = 1$: $x = zu$, $y = zv$. We then get $z^2u^2 + z^3v^3 + z^4 = z^2(u^2 + zv^3 + z^2)$. We have exceptional fiber z^2. Notice that $u^2 + zv^3 + z^2 = u^2 + (z + v^3/2)^2 - v^6/4$. A change of variables leads to $u^2 + z'^2 - v'^6$, an A_5 singularity. The exceptional fiber defined by $z^2 = u^2 + zv^3 + z^2 = 0$ first gives $z = 0$ but then $u^2 = 0$ so that v arbitrary is the line $z = u = 0$ in zuv-space.

You run out of letters fast. We reset notation. Consider $x^2 + zy^3 + z^2 = 0$. and line $z = x = 0$. Call this E_0.

Blowup 2, chart $v = 1$: We get $y^2u^2 + y^4w + y^2w^2 = y^2(u^2 + y^2w + w^2)$. Again, exceptional fiber is y^2 and again, complete square: $u^2 + (w + y^2/2)^20y^4/4$. an A_3 singularity. The exceptional fiber of the blowup is again a pair of lines. $u \pm iw = 0$. call the lines $E_1^{\pm}$.

Reset notation again. Consider $x^2 + y^2z + z^2 = 0$. We get an A_1 singularity. Again, with two lines in the exceptional fiber.

We have picture

Dual graph to this is

Which is of course E_6.

The cases of E_7 and E_8 work similarly.

Example 3.22. $T_{3,3,3}$ singularity: $x^3 + y^3 + z^3 + xyz$. Blowup the origin and look at the $u = 1$ chart: we have $y = xv, z = xw$. Then $x^3 + xv^3 + x^3w^3 + x^3vw = 0$. Factoring out x^3, we have $x^3(1 + v^3 + w^3 + vw) = 0$. The strict transform is defined by $1 + v^3 + w^3 + vw = 0$ in xvw-space. Taking partials yields that this is singular at three lines: $(x, -1, 1)$, (x, θ, θ^2), (x, θ^2, θ), where x is arbitrary and θ is a cube root of unity. This is a surface with three lines of singularities, i.e. highly non-isolated singularities. Blowing up wont help you, at least blowing up at a point. One can however can blowup arbitrary subvarities. The thing to do is 'normalize', i.e. take integral closure, to replace the non-embedded singularities by isolated ones.

Theorem 3.10. *The Kleinian surface singularities are the only surface singularities that can be resolved using only blow-ups at a point.*

One can prove this using direct calculations. However, there is a uniform proof of this due to Artin-Verdier going via the reflective modules over the invariant ring $k[u, v]^G$ and using more Algebraic Geometry.

Our next project is to understand the module theory of invariant rings $k[x_1, \ldots, x_n]^G$.

4 Commutative Algebra of Invariant Rings

4.1 Noether's Theorem

There are two standard approaches to this topic: a graded ring approach and a local ring approach. We shall take the former. Let k be a field and W a d-dimensional k-vector space. Furthermore, let $G \subseteq \mathrm{GL}_n(W) \cong \mathrm{GL}_n(k)$ be a finite group with $|G| \in k^\times$. Define $S = k[W] \cong k[x_1, \ldots, x_d]$ and let $R = S^G$ be its invariant ring. In particular, $R \subseteq S$ is a subalgebra. Now invariant rings are 'nicer' than a typical randomly chosen subring of a polynomial ring, by which we mean that there is a 'nice' operator on the invariant subring, namely the Reynold's operator $\rho : S \to R$ given by

$$\rho(s) = \frac{1}{|G|} \sum_{g \in S} g_S.$$

The Reynold's operator is an R-linear split surjection, so $S \cong R \oplus \ker \rho$ as R-modules. Furthermore, when working with the ring of invariants, one works with symmetric polynomials, which are inherently 'nicer' than typical functions. The goal of this section will be to prove the following theorem of Noether:

Theorem 4.1 (Noether, 1928)**.** *The ring R is a noetherian integrally closed domain of Krull dimension $d = \dim_k W$.*

Remark. None of these properties of Noether's Theorem hold for arbitrary subrings of polynomial rings.

Recall that the Krull dimension of a k-algebra A is the maximal number of algebraically independent elements over k. This definition is equivalent to the transcendence degree of the quotient field $Q(A)$ over k. If A is the $\mathbb{C}$-algebra given by the coordinate ring of a collection of polynomials, xthen the Krull dimension is the topological dimension of the vanishing set corresponding to A; that is, if $A = k[y_1, \ldots, y_m]/(f_1, \ldots, f_r)$, then $\dim A = \dim V(f_1, \ldots, f_r) \subseteq \mathbb{C}^m$. We first show that a polynomial ring is an integral extension of its invariants ring.

Lemma 4.1. *Let $S = [k_1, \ldots, x_d]$ and $R = S^G$ its ring of invariants. The extension $R \hookrightarrow S$ is integral, i.e. every element of S is a root of a monic polynomial with coefficients in R.*

Proof. For $s \in S$, define $f_s(t) := \prod_{g \in G}(t - gs)$. Then $f_s(t)$ is monic in t and has s as a root since $t - s$ is a factor of $f_s(t)$. The action of G permutes the factors of $f_s(t)$, so it fixes the coefficients of $f_s(t)$. Therefore, $f_s(t) \in R[x]$. □

This already shows that $\dim R = \dim S = d$ since integral extensions satisfy Going-Up and Going-Down, and thus preserve dimension. We know also that if $A \hookrightarrow B$ is an integral extension of rings and B is finitely generated as an A-algebra, then B is finitely generated as an A-module (see Atiyah-MacDonald [AM69, Ch. 5]). It then follows that

Corollary 4.1. *Let $S = [k_1, \ldots, x_d]$ and $R = S^G$ its ring of invariants. Then S is a finitely generated R-module of rank $|G|$.*

Proof. It is enough to show that S is a finitely generated R-algebra. Now S is generated over k by $x_1, \ldots, x_d$, so that it is generated over R by $x_1, \ldots, x_d$ as well so that S is a finitely generated R-module. It remains to show that S has rank $|G|$. Recall that the rank of a module M over a domain A is $\dim_{Q(A)} M \otimes_A Q(A)$. So we need to compute $\dim_{Q(R)}(S \otimes_R Q(R))$. But $S \otimes_R Q(R)$ is just $Q(S)$ by integrality. Then any $s \in S$ satisfies an equation $s^p + r_1 s^{p-1} + \cdots + r_{p-1}s + r_p = 0$, where $r_i \in R$ and $r_p \neq 0$. Then $s(s^{p-1} + r_1 s^{p-2} + \cdots + r_{p-1}) = -r_p$. Then

$$\frac{1}{s} = -\frac{1}{r_p}\left(r_1 s^{p-2} + \cdots + r_{p-1}\right).$$

If you invert everything in R, then you have effectively inverted everything in s by the above. So we need $\dim_{Q(R)} Q(S)$. This a Galois field extension, $Q(S)^G = Q(R)$ so it has degree $|G|$. □

We now prove that R is noetherian:

We know that S is integral over R, so that each x_i is integral over R. Let $f_1(t), \ldots, f_d(t)$ be monic polynomials with $f_i(x_i) = 0$. Let $B \subseteq R$ be the k-subalgebra generated by all the coefficients of $f_1, \ldots, f_d$. Then B is finitely generated as a k-algebra so that it is noetherian by the Hilbert Basis Theorem. S is integral over B, and finitely generated as a B-algebra, so finitely generated as a B-module. Now B is noetherian and S is a finitely generated B-module, every B-submodule of S is a finitely generated module. In particular, R must be a finitely generated B-module and hence is a noetherian module. Ideals in R are B-submodules of R and hence satisfy the ascending chain condition. Hence, R is noetherian. □

We now prove that R is integrally closed in its quotient field (normal):

We know that $Q(S)^{=}Q(R)$.

If $x = a/b \in Q(R)$ is integral over R, then in particular $x \in Q(S)$ and is integral over S. Polynomial rings are integrally closed in their quotient field. So $x \in S$. Hence, $x \in S \cap Q(R) = S \cap Q(S)^G = S^G = R$. When is R a UFD? Always? Never? In between? We know that $S \cong k[x_1, \ldots, x_d]$ is a UFD but $k[u, v]^{C_2} = k[u^2, uv, v^2] \cong k[a, b, c]/(ac - b^2)$ is not a UFD since $u^2 \cdot v^2 = (uv)^2$. If we assume that G has no nontrivial linear characters, i.e. no group homomorphisms $G \to k^\times$, then the invariant ring is a UFD.

Proof. Let $r \in R$, then $r \in S$, so we can factor $r = q_1^{a_1} \cdots q_m^{a_n}$, where each q_i is irreducible in S are pairwise non-associate. The q_i's are not necessarily permuted by G, but the ideals

$(q_1), \ldots, (q_m) \subseteq S$ are. Let $O_1, \ldots, O_e$ be the orbits of the ideals $(q_1), \ldots, (q_m)$ under this action and set

$$Q_j = \prod_{(q_i) \in O_j} q_i^{a_i}$$

for $j = 1, \ldots, e$. The ideal (Q_j) is stable under the action of G, so in particular for any $g \in G$, $gQ_j \in (Q_j)$ so gQ_j is a multiple of Q_j. For degree reasons, $gQ_j = \lambda_g Q_j$ for some $\lambda_g \in k^\times$. The function $\lambda : G \to k^\times$ given by $g \mapsto \lambda_g$ (we get one such function for each orbit) and it is a group homomorphism. By assumption, λ must be trivial, i.e. $gQ_j = Q_j$ for every $g \in G$ and $j = 1, \ldots, e$. Then $Q_j \in R$ for every j and $r = Q_1 Q_2 \cdots Q_e$ is a factorization in R. Each Q_j is irreducible because it is a product over a single orbit. It is routine, although tedious, to check uniqueness. □

Example 4.1. $R = S^G$ is a UFD in the following cases (this is not a complete list, just examples): if G is a nonabelian simple group, e.g. A_n for $n \geq 5$ note that A_5 is the $\mathcal{I} \cong A_5$ group, then we see that the E_8 singularity defined by $x^2 + y^3 + z^5 = 0$ is a UFD. Or $G = [G, G]$, i.e. every element is a commutator or a product of commutators (in $k^\times$ they are forced to be abelian so go to 1), such groups are called perfect. OR $k = \mathbb{Q}$ and G has odd order (so then does every element) and every image of every element must then be of odd order, which there are none. One can generalize this to $|k| = p^e$ and $\gcd(|G|, |k^\times| = q - 1)$.

Having proved Noether's Theorem, our next goal is the Hochster-Eagon Theorem that $R = S^G$, i.e. invariant rings are Cohen-Macaulay. We work with graded rings (recall that $k[x_1, \ldots, x_n] = \bigoplus_p k[x_1, \ldots, x_n]_p$), the pth graded piece consisting of homogeneous polynomials of degree p and our group actions preserve degree so $k[x_1, \ldots, x_n]^= \bigoplus_p k[x_1, \ldots, x_n]_p^G$. Let $A = \bigoplus_{i=1}^\infty A_i = A_0 \oplus A_1 \oplus \cdots$ be a graded ring with $A_0 = k$ a field. Sometimes [Bruns-Herzog] such rings are called *local since they have a unique homogeneous maximal ideal $\mathfrak{m} = A_1 \oplus A_2 \oplus \cdots$.

Definition (Homogenous System of Parameters)**.** A homogeneous system of parameters for A is a sequence of elements $a_1, \ldots, a_t$ such that A is a finitely generated module over the (graded subring) $k[a_1, \ldots, a_t]$.

4.2 Cohen-Macaulay Rings & Modules

Definition (Homogeneous)**.** Let $A = \bigoplus_{i=0}^\infty A_i$ be an $\mathbb{N}$-graded ring with $A_0 = k$ a field. An element $a \in A$ is homogeneous if it lies in a unique A_i.

Definition (Homogeneous System of Parameters)**.** Let $A = \bigoplus_{i=0}^\infty A_i$ be an $\mathbb{N}$-graded ring with $A_0 = k$ a field. A sequence $a_1, \ldots, a_m$ of homogeneous elements is called a homogeneous system of parameters (hsop) if $m = \dim A$ and A is a finitely generated module over the graded subring $k[a_1, \ldots, a_n]$. Equivalently, $A/(a_1, \ldots, a_m)$, where $k = \dim A$, is a finite dimensional k-vector space.

Example 4.2.

(i) Consider the polynomial ring $A = k[x^2, xy, y^2]$. We claim $\{x^2, y^2\}$ is a hsop. Consider $B = k[x^2, y^2] \subseteq A$. As a B-module, A is generated by 1 and xy. Equivalently, $A \cong k[a, b, c]/(ac - b^2)$, $\{a, c\}$ is a hsop as $A/(a, c) \cong k[a, b, c]/(ac - b^2, a, c) \cong k[b]/(b^2)$.

(ii) Consider the ring $A = k[x^2, x^3, y, xy]$. Note that $k[x, y]$ is an integral extension of A since x is a root of $t^2 - x^2$. Therefore, dim $A = 2$. Now $\{x^2, y\}$ is a hsop: if $B = k[x^2, y]$, then $A = B1 + Bx^3 + Bxy$.

Theorem 4.2 (Noether)**.** *Let k be a field and A be a finitely generated k-algebra. Then there exist homogeneous elements $a_1, \ldots, a_d$ which are algebraically independent over k and such that A is a finitely generated module over $k[a_1, \ldots, a_d]$ (which is isomorphic to a polynomial ring).*

It is worth noting that if k is infinite, then there is a probabilistic algorithm for getting the a_i's. In this case, we could take for the a_i's a 'sufficiently general' k-linear combination of the generators of A. This is Noether's Normalization Lemma. Furthermore, the integer d is uniquely determined; it is the Krull dimension of A. In the case that A is an integral domain, d is also the transcendence degree of the field of fractions of A over k.

Definition (Cohen-Macaulay (CM))**.** If $A = \bigoplus_{i=0}^{\infty} A_i$ is an $\mathbb{N}$-graded ring with $A_0 = k$ a field, then if for some (equivalently, any) hsop $a_1, \ldots, a_d$, A is a free module over the Noether normalization $k[x_1, \ldots, x_d]$, we say that A is Cohen-Macaulay (CM).

Example 4.3.

(i) Let $A := k[x^2, xy, y^2] \supseteq B := k[x^2, y^2]$. Observe $A = B1 + Bxy$ and $\{1, xy\}$ are B-linearly independent. Noting also that $1, xy$ are free generators, i.e. A is free over B, we see that A is CM.

(ii) Let $A := k[x^2, x^3, y, xy] \supseteq B := k[x^2, y]$. Observing that $A = B1 + Bx^3 + Bxy$ but $y(x^3) - x^2(xy) = 0$, we see that A is not CM.

(iii) Define $A_1 = k[x^4, x^3y, x^2y^2, xy^3, y^4]$ and $A_2 = k[x^4, x^3y, xy^3, y^4]$. Only one of these is CM, the other is not. (Which?!)

Definition (Maximal Cohen-Macaulay (MCM))**.** Let A be as above and M be a finitely generated A-module. We say that M is maximal Cohen-Macaulay (MCM) if for some (equivalently, any) hsop, M is a free module over the Noether normalization.

So A is a CM ring if and only if it is a maximal MCM module over itself.

Remark. These are not the typical definitions of CM or MCM. They are equivalent, of course. However, one usually begins by considering the local ring case rather than the graded case. However, we choose this approach for clarity and consistency of approach with the rest of the notes.

Example 4.4.

(i) Let $A = k[x_1, \ldots, x_d]$ be a polynomial ring and M a finitely generated A-module. When is M a maximal Cohen-Macaulay module? We know that $\{x_1, \ldots, x_d\}$ form a hsop. But then M is MCM if and only if it is free over $k[x_1, \ldots, x_d] = A$. Therefore for polynomial rings, the MCM rings are the free modules.

(ii) Let $A = k[x^2, xy, y^2]$, and let $I = (x^2, xy)A$ be an ideal of A. We claim that I is MCM as an A-module. Notice that I is isomorphic to the A-submodule of $k[x, y]$ generated by x and y. Furthermore, $k[x, y] \cong A \oplus (x, y)A$ as A-modules. Notice that $\{x^2, y^2\}$ is a hsop for $k[x, y]$. Since polynomial rings are CM, $k[x, y]$ is a free module $k[x^2, y^2]$-module. Then so too must its summands be free. This shows $(x, y)A$ is a free $k[x^2, y^2]$-module as well.

As noted, we have taken a non-standard approach to CM and MCM rings. We shall still need alternative definitions for these concepts in places, so we approach them here.

Definition (M-Regular)**.** Let $(A, \mathfrak{m})$ be a local ring, where $\mathfrak{m}$ is the maximal ideal, and M is a finitely generated A-module. A sequence $a_1, \ldots, a_t \in \mathfrak{m}$ is an M-regular sequence if

- a_1 is a nonzerodivisor on M
- a_{i+1} is not a zero divisor on $M/(a_1, \ldots, a_i)$ for $i = 1, \ldots, t-1$

Definition (Depth)**.** Let $(A, \mathfrak{m})$ be a local ring. The depth of a finitely generated A-module M is the length of the longest possible M-regular sequence.

It is known that the depth depth M is bounded above by dim A, and M is MCM if and only if equality occurs.

Theorem 4.3 (Hochster-Eagon)**.** *Let G be a finite subgroup of $\mathrm{GL}(W)$, and assume $|G| \neq 0$ in k. Then the invariant ring $k[W]^G$ is a CM ring.*

Proof. Recall Reynold's operator $\rho : k[W] \twoheadrightarrow k[W]^G$. Let $f_1, \ldots, f_d$ be a hsop in $k[W]^G$. Let $B = k[f_1, \ldots, f_d]$, $R := k[W]^G$, and $S := k[W]$. Then $B \subseteq R \subseteq S$, and S is a finitely generated R-module. But then S is a finitely generated B-module. Therefore, $f_1, \ldots, f_d$ form a hsop in S. Since polynomial rings are CM, S is a free B-module. The Reynold's operator makes R into a direct summand of S, as R-modules. Hence, the Reynold's operator turns R into a B-direct summand of a free B-module. Therefore, R is free over B, as desired. □

Note that the assumption on $|G|$ is necessary: if we take C_4 act by index permutation on $\mathbb{F}_2[x_1, x_2, x_3, x_4]$, then $\mathbb{F}_2[x_1, \ldots, x_4]^{C_4}$ is not CM. This was shown by Bertin in 1967, see Neusel-Smith. Finally, notice that the proof of Theorem 4.3 holds for any R-direct summand of S. In other words, writing $S = R \oplus M_1 \oplus \cdots \oplus M_r$ as a direct sum of R-modules, then

each M_i is a MCM R-module. What are the R-direct summands of S? This is a central question of these notes, which we shall spend most of the remaining text trying to answer.

Recall that if $\chi : G \to k^\times$ is a linear character, then we have the semi-invariants $k[W]^G_\chi := \{f \in k[W] : gf = \chi(g)f \text{ for all } g \in G\}$. We claim that $k[W]^G_\chi$ is an R-direct summand of $k[W]$. Define a 'fancy' Reynold's operator $\rho_\chi : k[W] \to k[W]^G_\chi$ by

$$\rho_\chi(f) := \frac{1}{|G|} \sum_{g \in G} \chi(g)^{-1} gf.$$

Though it is not immediately obvious, we can show that $\operatorname{im} \rho_\chi \subseteq k[W]^G_\chi$ as follows:

$$\begin{aligned} h\rho_\chi(f) &= \vdots \\ &= \vdots \\ &= \text{sum over } h^{-1}g \text{see Reynold's proof} \\ &= \chi(h)\rho_\chi(f). \end{aligned}$$

Furthermore, the map ρ_χ is R-linear and splits the inclusion $k[W]^G_\chi \subseteq k[W]$. In other words, ρ_χ fixes $k[W]^G_\chi$. This shows that each semi-invariant is an R-direct summand of $k[W]$. But that is not all!

4.3 Isotypic Components

Isotypic components are the 'jazzy' versions of semi-invariants for higher dimensional representations. Let $\chi : G \to k^\times$ be a linear character and $k[W]^G_\chi$ be its ring of semi-invariants. We know that G acts on the polynomial ring $k[W]$ in a way that preserves degrees. But then G acts on each graded piece $k[W]_t$. By Maschke's Theorem, each $k[W]_t$ decomposes into irreducible representations. Fix an irreducible representation ρ, and let $k[W]^G_\rho$ be the direct sum of all appearances of ρ in the decomposition above, each in its appropriate degree. This is the isotypic component of $k[W]$ corresponding to ρ. 'Obviously',

$$k[W] \cong \bigoplus_{\rho \text{ irred rep}} k[W]^G_\rho.$$

SO each $k[W]^G_\chi$ is an R-module, and by the proof of Theorem 4.3, this is a MCM R-module. Though this technically answers our question, it does not held up gain any deeper understanding. Moreover, are these even all the MCM R-modules? If not, how do the other MCM R-modules relate to the ones arising in the way above?

Let $\operatorname{MCM}(R)$ denote the set of all MCM R-modules. For any ring R and A-module M, let $\operatorname{add}_A(M)$ be the set of all direct summands and direct sums of copies of M, called the "additive closure" of M. So far we know that $\operatorname{add}_R(S) \subseteq \operatorname{MCM}(R)$. This begs the question,

$$\operatorname{add}_R(S) = \operatorname{MCM}(R)?$$

If not, can we measure the difference between them? Note that it is a conjecture (the Small CM Conjecture, Hochster) that every complete local ring has a MCM module and has been open since the 1960s. Finally, note that $R \in \mathrm{add}_R(S)$ by use of the Reynold's operator.

Now let $d = \dim_k W$. In the case that $d = 1$, then $\mathrm{GL}(W) = \mathrm{GL}_1(k) = k^\times$, so that $G \subseteq k^\times$, a finite group. But any such group must be cyclic, say then that $G \cong C_n$ is generated by a primitive nth root of unity, ω. The action of ω on $k[W] \cong k[x]$ sends x to ωx. What are the invariants? We know $k[x]^{C_n} = k[x^n]$, which is isomorphic to a polynomial ring. We know that every MCM module over a polynomial ring is free. As a $k[x^n]$-module, $k[x] = \bigoplus_{i=0}^{n-1} k[x^n]x^i$, a free module of rank n with basis $\{1, x, \ldots, x^{n-1}\}$.

Now let $d = 2$. This case includes all finite subgroups of $\mathrm{SL}_2(\mathbb{C})$. First, we shall need some background on reflexive modules, which are slightly weaker than MCM modules, i.e. there are more reflexive modules than MCM modules.

Definition (Reflexive Module)**.** Let A be a commutative ring and M be an A-module. Define an A-module $M^* := \mathrm{Hom}_A(M, A)$ via $(af)(x) = f(ax)$, where $a \in A$, $x \in M$, and $f : M \to A$ is an A-map.

We can then define $M^{**} := (M^*)^* = \mathrm{Hom}_A(M^*, A) = \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A)$. However, there is a natural map $\theta_M : M \to M^{**}$ given by $x \mapsto e_x$, where $e_x : \mathrm{Hom}_A(M, A) \to A$ is evaluation at x, i.e. $f \mapsto f(x)$. In other words, $\theta_M(x)(f) = f(x)$. We say that M is torsionless if θ_M is injective. We say that M is reflexive if θ_M is an isomorphism. In particular, $M^{**} \cong M$.

Remark. Torsionless means $\theta_M(x) = 0$ is the zero map $M^* \to A$ implies that $x = 0$. Equivalently, $f(x) = 0$ for all $f : M \to A$ implies that $x = 0$. This implies that torsionfreeness. Recall that M is torsionfree if $x \neq 0$, $a \in A$, a nonzerodivisor implies $ax \neq 0$. If $ax = 0$ for some $x \in M$, nonzerodivisor a, then $0 = f(ax) = af(x)$, for all $f \in M^*$. Since a is a nonzerodivisor, this implies $f(x) = 0$ for all f. By torsionlessness, we get $x = 0$. In fact, the two are equivalent over domains.

To discuss reflexivity, we need a bit more about depth. However, we shall only sketch proofs of any of the results here.

Lemma 4.2. *Let $(A, \mathfrak{m})$ be a local ring or a graded ring. Let*

$$0 \longrightarrow L \longrightarrow M \longrightarrow P \longrightarrow 0$$

be a short exact sequence of A-modules. Then

- $\mathrm{depth}\, L \geq \min\{\mathrm{depth}\, M, \mathrm{depth}\, N + 1\}$
- $\mathrm{depth}\, M \geq \min\{\mathrm{depth}\, L, \mathrm{depth}\, N\}$
- $\mathrm{depth}\, N = \min\{\mathrm{depth}\, M, \mathrm{depth}\, L - 1\}$.

Corollary 4.2. *If* depth $A \geq 2$, *then every A-module has depth at least 2.*

Proof. Let M be reflexive, and begin a free resolution of the dual M^*:

$$A^m \longrightarrow A^n \longrightarrow M^* \longrightarrow 0.$$

Now applying $\mathrm{Hom}_A(-, A)$, we obtain the exact sequence

$$0 \longrightarrow M^{**} \longrightarrow (A^n)^* \xrightarrow{f^*} (A^m)^*.$$

Let $C := \operatorname{coker} f^*$, the Auslander transpose of M^*. Then

$$0 \longrightarrow M \longrightarrow A^n \xrightarrow{f^*} A^m \longrightarrow C \longrightarrow 0$$

is an exact sequence. By Lemma 4.2, we must have depth $M = \operatorname{depth} C + 2$ or depth $M =$ depth A, which are both at least two. □

This argument can be modified to show that $\operatorname{depth} \mathrm{Hom}_A(M, N) \geq 2$ as long as depth $N \geq 2$.

Remark. This is a special property of '2' since the same does not hold replacing 2s by 3s, 4s, etc.. The proof also shows that any reflexive module over any ring is a kernel of a map homomorphism between free modules, i.e. a second syzygy.

Example 4.5. In the case of CM rings of dimension at least 2, e.g. $A = k[x_1, \ldots, x_n]^G$ with $n \geq 2$, depth $A \geq 2$.

Our next goal will be to show that over normal domains that reflexive modules are precisely second syzygies.

Serre's Conditions

Theorem 4.4 (Serre)**.** *Let A be a noetherian domain. The following are equivalent:*

(i) A is integrally closed in its quotient field, i.e. "normal"

(ii) A satisfies (R_1): A_p is a local domain for all primes of height one. (S_2): depth $A_p \geq \min\{2, \operatorname{height} p\}$ *for all primes p.*

One can define Serre's condition (S_k) for modules $\operatorname{depth} M_p \geq \min\{k, \dim M_p\}$. An interesting fact is that MCM implies that (S_k) for all k.

Lemma 4.3. *Let $f : M \to A$ be a homomorphism of A-modules. Assume that N satisfies (S_1) and M satisfies (S_2). Then f is an isomorphism if and only if $f_p : M_p \to N_p$ is an isomorphism for every prime of height at most one.*

Proof. See the notes.

Proposition 4.1. *Let A be a normal domain and M an A-module. Then the following are equivalent:*

(i) M is reflexive

(ii) M is a second syzygy

(iii) M satisfies (S_2)

Proof. We have already seen that (i) implies (ii). Lemma 4.2 shows (ii) implies (iii). It remains to show that (iii) implies (i). To show that M is reflexive, consider $\theta_M : M \to M^{**}$. Since M satisfies (S_2) and M^{**} is a second syzygy, it also satisfies (S_2). Then θ_M is an isomorphism if and only if the localization $(\theta_M)_p$ is an isomorphism for all primes p of height at most one. So we localize at a prime p of height one. By Serre's Theorem, A satisfies (R_1) so that A_p is a regular local ring of dimension one. The A_p-module M_p has depth one by the (S_2) condition. But then M_p is a MCM module over the regular local ring A_p, hence free. Free modules are reflexive so $(\theta_M)_p$ is an isomorphism. □

The point is that over a (graded) normal domain, MCM modules are reflexive. The converse holds if the ring has dimension at most two. The converse fails in dimension three or more.

Example 4.6. Let $A = k[x, y, z]$ and M be the ideal (x, y). We have a short exact srquence

$$0 \longrightarrow (x, y) \longrightarrow k[x, y, z] \longrightarrow \frac{k[x, y, z]}{(x, y)} \longrightarrow 0$$

Note that $k[x, y, z]/(x, y) \cong k[z]$, which has depth 1. We know that $k[x, y, z]$ has depth 3. By Lemma 4.2, we know that $\operatorname{depth}(x, y) \geq \min\{3, 1 + 1\} = 2$. We know $1 = \operatorname{depth} k[x] \geq \min\{3, \operatorname{depth}(x, y) - 1\}$. But then $\operatorname{depth}(x, y) = 2$. In particular, (x, y) is a reflexive A-module by the Proposition. It is not MCM because it is not free.

Example 4.7. Let $A = k[x, y, z]$ and $M = (x, y)$. We have the short exact sequence

$$0 \longrightarrow (x, y) \longrightarrow A \longrightarrow \frac{A}{(x, y)} \longrightarrow 0.$$

We know $A/(x, y) \cong k$, a field, so this has depth 0. We know that $\operatorname{depth} A = 2$. Then it must be that $\operatorname{depth}(x, y) = 1$. So (x, y) is neither reflexive nor MCM. What is M^{**}? Consider the free resolution

$$A \longrightarrow A \oplus A \longrightarrow (x, y) \longrightarrow 0$$

with maps $a \mapsto (y, -x)$ and $(a, b) \mapsto ax + by$. Taking duals yields,

$$0 \longrightarrow (x, y)^* \longrightarrow (A \oplus A)^* \xrightarrow{i^*} A^*$$

Now $i^*(e_1)$ (the first coordinate function) is $i^*(e_1) = e_1 i = y$ and $i^*(e_2) = e_2 i = -x$. Then i^* is the map $(a, b) \mapsto ay - bx$ and further $(x, y)^* \cong \ker i^* \cong A(x, y) \cong A$. But $(x, y)^{**} \cong A^* \cong A$.

Theorem 4.5 (Herzog, 1978)**.** *Let $S = k[u, v]$, $G \subseteq \mathrm{GL}_2(k)$ a finite group with $|G| \in k^*$. Set $R = \widehat{S^G}$, the completion of the invariant ring. Then every indecomposable MCM R-module is a direct summand of $\hat{S} = k[\![u, v]\!]$.*

Proof. We shall assume the Krull-Schmidt property for R and S, and leave the details passing between the ring and its completion for the reader. Let M be an indecomposable MCM (reflexive) R-module. We want M to be a direct summand of S as an R-module. Since $|G| \in k^\times$, we have the Reynold's operator, so R is a direct summand of S as R-modules. So we have the split monic $R \hookrightarrow S$. Apply $\mathrm{Hom}_R(M^*, -)$. Then we have $\mathrm{Hom}_R(M^*, R) \to \mathrm{Hom}_R(M^*, S)$ still splits. However, $\mathrm{Hom}_R(M^*, R) = M^{**} \cong M$ as M is reflexive. The R-module $\mathrm{Hom}_R(M^*, S)$ is naturally an S-module: $(sf)(\lambda) := s(f(\lambda))$ for $s \in S$, $f : M^* \to S$, $\lambda \in M^*$. Furthermore, we have proved that Hom modules have depth ≥ 2. So $\mathrm{Hom}_R(M^*, S)$ is an S-module of depth 2, hence an MCM S-module, hence free. So M is a direct summand over R of a free S-module. $M \mid S^n$ for some n. But M is indecomposable, and we have Krull-Schmidt, so M must be a direct summand of S, i.e. $M \mid S$, which is what we wanted to show. □

Remark. We need the 'hats' in order to use the Krull-Schmidt uniqueness theorem for direct-sum decompositions. This fails even for $k[u, v]$. Could get away with much less, the Hensalization for example.

Corollary 4.3. *For 2-dimensional rings of invariants $R = S^G$. $\mathrm{add}_R(S) = MCM(R)$.*

Example 4.8. Let $C_n = \langle \sigma \colon \sigma^n = 1 \rangle$ act on $S = k[u, v]$ via $\sigma(x) = \omega_n x$, $\sigma(y) = \omega_n^{-1} y$, i.e.

$$\sigma = \begin{pmatrix} \omega_n & \\ & \omega_n^{-1} \end{pmatrix} \in \mathrm{SL}_2(k).$$

Then $R = S^G = k[u^n, u^{n-1}v, \ldots, v^n]$ (we worked this out before). Furthermore, we worked out $S \cong_{R-mod} R \oplus I_1 \oplus I_2 \oplus \cdots \oplus I_{n-1}$, where I_j is generated as an R-module by monomials of degree $j \mod n$. Explicitly, $I_j = (u^j, u^{j-1}v, \ldots, v^j)R \cong (u^j v^{n-j}, u^{j-1}v^{n-j+1}, \ldots, v^n)$. By Herzog's Theorem, every maximal MCM (or reflexive) can be written $R^{a_0} \oplus I_1^{a_1} \oplus I_2 \oplus \cdots \oplus I_{n-1}^{a_{n-1}}$.

Definition. We say that a (local or graded) ring A has finite CM representation type (fCMt) if it has finitely many indecomposable MCM modules up to isomorphism.

Corollary 4.4. *$k[u,v]^G$ have fCMt.*

Note that Herzog's Theorem does not hold in dimension greater than two.

Example 4.9. Let $C_2 = \{\pm 1\}$ act on $k[x,y,z]$. Then $R = k[x^2, y^2, z^2, xy, xz, yz]$. As R-modules, S has rank 2 (by previous work) $S \cong R \oplus I$, where I is all monomials of odd degree, i.e. $(x,y,z)R \cong (x^2, xy, xz)R$. Take a syzygy of I:

$$0 \longrightarrow N := \ker \pi \longrightarrow R^3 \xrightarrow{\pi} I \longrightarrow 0$$

FACT: Another theorem of Herzog coming soon. N is indecomposable. [Theorem says it is a syzygy of an indecomposable MCM module. So N is an indecomposable MCM module of rank 2, hence it is not isomorphic to either R or I, so does not appear as a summand of S (technically, this requires Krull-Schmidt).

4.4 The Gorenstein and Isolated Singularity Properties

Goal is to determine when invariant rings have these properties, then use them in Auslander version of the M$^{\text{c}}$Kay Correspondence.

Definition (Gorenstein)**.** Let $A = A_0 \oplus A_1 \oplus \cdots \oplus A_s$ be a graded algebra over $A_0 = k$, a field. Assume that $A_s = 0$ but $A_{>s} = 0$. Say that A is Gorenstein (or a Poincaré duality algebra) if $A_s \cong k$ is a 1-dimensional vector space and for every i, the mapping $A_i \times A_{s-i} \to A_s \cong k$ given by $(a, a') \mapsto aa'$ is a perfect pairing. [Recall a bilinear map $\langle , \rangle : V \times W \to k$ is a perfect pairing if the induced map $V \to W^\vee := \text{Hom}_k(W,k)$ is an isomorphism of vector spaces, where the induced map is given by $v \mapsto \langle v, - \rangle : W \to k$.]

In particular, if A is Gorenstein, then $A_i^\vee \cong A_{s-i}$. By the way, this is equivalent to the usual definition that $\text{soc}\, A = \{a \colon aA_{\geq 1} = 0\}$ is 1-dimensional. Notice A_s is always in $\text{soc}\, A$, and if soc were to contain any elements of degree $i \neq s$, say a, then the map $A_i \to A_{s-i}^\vee$ given by $v \mapsto \mu_v$, multiplication by v, would have a in the kernel so that it would not be an $\cong$.

Bookkeeping devices: For a graded ring $A = \bigoplus_{i=0}^\infty A_i$ where $A_0 = k$, the Hilbert function counts vector space dimensions, $H_A(n) \stackrel{def}{=} \dim_k A_n$. One can do this for modules also, $H_M(n) \stackrel{def}{=} \dim_k M_n$. If now $A = A_0 \oplus \cdots \oplus A_s$ is a finite dimensional Gorenstein ring, then $A_i \cong A_{s-i}^\vee$ so they have the same k-dimension, so $H_A(i) = H_A(s-i)$, where $i = 0, \ldots, s$. That is, the Hilbert function is symmetric. Caution: symmetric hilbert function does not imply gorenstein. Note also $\sum_i H_A(i) = \dim_k(\oplus A_i) = \dim_k A$. The Hilbert series of A is the generating function for its Hilbert function $h_A(t) = \sum_{n \geq 0} H_A(n) t^n$. Notice that $h_A(t)$ is a polynomial if and only if $A_i = 0$ for $i \gg 0$ if and only if $\dim_k A < \infty$.

Theorem 4.6 (Hilbert). *For $n \gg 0$, $H_A(n)$ agrees with a polynomial $P_A(n)$ of degree* $\dim A + 1$, *called the Hilbert polynomial. In particular, $h_A(t)$ is a rational function of t.*

Again let A be a finite dimensional Gorenstein graded ring. Since the Hilbert function is symmetric, $h_A(t) = h_0 + h_1 t + h_2 t^2 + \cdots + h_s t^s$ with $h_i = H_A(i)$ and $h_i = h_{s-i}$. Then

$$h_A(1/t) = t^{-s} h_A(t).$$

Example 4.10. $A = k[x,y]/(x^2, y^2) = k \oplus \langle x, y\rangle \oplus \langle xy\rangle$. So $s = 2$. The bilinear map $A_1 \times A_2 \to A_2$ is a perfect pairing, so A is Gorenstein. $h_A(t) = 1 + 2t + t^2$, so $h_A(1/t) = 1 + 2/t + 1/t^2 = 1/t^2(1 + 2t + t^2)$.

Example 4.11. $A = k[x,y]/(x^2, xy, y^3)$. $H_A : (1,2,1)$ same Hilbert function as previous example but A is not Gorenstein since x kills all terms in degree 1, $xA_{\geq 1} = 1$ but x does not have degree 2=s.

4.5 Module-Theoretic Properties of Gorenstein Rings

Observe that for any finite dimensional graded algebra A, the k-dual $A^\vee = \mathrm{Hom}_k(A,k)$ is an injective A-module. This follows directly from Hom $-\otimes$ adjointness, we want ot show $\mathrm{Hom}_A(-, A^\vee)$ is exact. But $\mathrm{Hom}_A(-, A^\vee) = \mathrm{Hom}_A(-, \mathrm{Hom}_k(A,k)) = \mathrm{Hom}_k(- \otimes_A A, k) = \mathrm{Hom}_k(-,k)$, which is exact.

$$A^\vee = \mathrm{Hom}_k(A,k) = \mathrm{Hom}_k(\oplus_{i=0}^s A_i, k) = \oplus_{i=0}^s \mathrm{Hom}_k(A_i, k) \cong \oplus_{i=0}^s A_{s-i}$$

So $A^\vee \cong A$ as vector spaces. One can check that $A^\vee \cong A$ as A-modules. The upside is that a Gorenstein finite dimensional algebra is self injective, i.e. injective as a module over itself. The converse is also true: sketch: show $A^\vee = \mathrm{Hom}_k(A,k)$ is the injective hull of k, since A is self-injective and contains k, conclude $A \cong A^\vee$.

It follows that if A is Gorenstein, then every finitely generated A-module is torsionless and in fact is reflexive. Sketch: Start with $k = A/A_{\geq 1}$. We have $k^* = \mathrm{Hom}_A(k, A) = \mathrm{ann}_A A_{\geq 1} = \mathrm{soc}\, A \cong k$, where the last isomorphism follows since A is Gorenstein. So $k^{**} \cong k$ also, and we just have to show $k \to k^{**}$ is not zero. Then finish by induction on $\dim_k M$.

Definition. A graded algebra $A = \oplus_{i=0}^\infty A_i$ with $A_0 = k$ a field is called Gorenstein if there is a regular sequence $x_1, \ldots, x_d$, of elements of positive degree so that $\overline{A} := A/(x_1, \ldots, x_d)$ is a finite dimensional Gorenstein ring. Note d is necessarily $\dim A$.

Equivalently, though we we will not prove this, the quotient $A/(x_1, \ldots, x_d)$ is a finite-dimensional Gorenstein ring for every regular sequence $x_1, \ldots, x_d$. How do Hilbert series behave when we kill a regular sequence?

Proposition 4.2. *Let A be a graded ring and $x \in A$ a homogeneous element of degree $e > 0$. Then*

$$h_A(t) = \frac{h_{A/(x)}(t) - t^e h_{\operatorname{ann} x}(t)}{1 - t^e}$$

In particular, x is a nonzero divisor if and only if $h_{A/(x)}(t) = (1 - t^e)h_A(t)$.

The "in particular" is clear by subsitution, get zero, but that's the sum of dimensions of graded pieces so must be zero ring?

For the rest, consider a more general situation. Let

$$0 \longrightarrow L \longrightarrow M \longrightarrow N \longrightarrow 0$$

be an exact sequence of graded A-modules and homogeneous maps of degree zero so $L_i \hookrightarrow M_i$, $M_i \twoheadrightarrow N_i$. Then for each degree n, we get

$$0 \longrightarrow L_n \xrightarrow{f_n} M_n \xrightarrow{g_n} N_n \longrightarrow 0$$

is an exact sequence of vector spaces. But then we can easily calculate dimensions. Then $\dim_k M_N = \dim_k L_n + \dim_k N_n$. Or in terms of Hilbert functions, $H_M(n) = H_L(n) + H_N(n)$ so that $h_M(t) = h_L(t) + h_N(t)$.

Now assume that f and g are homogeneous of degrees a and b, respectively, i.e. $f(L_n) \subseteq M_{n+a}$, $g(M_N) \subseteq N_{n+b}$. Then for each n, we get a short exact sequence

$$0 \longrightarrow L_n \xrightarrow{f_n} M_{n+a} \xrightarrow{g_{n+a}} N_{n+a+b} \longrightarrow 0$$

Then

$$H_L(n) - H_M(n+a) + H_N(n+a+b) = 0$$

Now

$$\sum_n H_M(n+a)t^n = t^{-a} \sum_n H_M(n+a)t^{n+a} = t^{-a} h_M(t)$$

So that

$$h_L(t) - t^{-a} h_M(t) + t^{-a-b} h_N(t) = 0$$

Long exact sequences give similar alternating sums.

Proof of Prop: We have the exact sequence

$$0 \longrightarrow \operatorname{ann}(x) \xrightarrow{i} A \xrightarrow{x} A \xrightarrow{\pi} A/(x) \longrightarrow 0$$

where $\deg i = 0$, $\deg x = e$, $\deg \pi = 0$. Then we get exact sequences

$$0 \longrightarrow \operatorname{ann}(x)_n \longrightarrow A_n \longrightarrow A_{n+e} \longrightarrow (A/(x))_{n+e} \longrightarrow 0$$

of vector spaces. By above, we get

$$h_{\operatorname{ann} x}(t) - h_A(t) + t^{-e}h_A(t) - t^{-e}h_{A/(x)}(t) = 0$$

Multiplying by t^e and juggling,

$$(1-t^e)h_A(t) = h_{A/(x)}(t) - t^e h_{\operatorname{ann} x}(t)$$

□

Corollary 4.5. *Le tA be as above and $x_1, \ldots, x_c$ be homogeneous elements of positive degrees $e_1, \ldots, e_c$. Then we have a coefficient-wise inequality of power series*

$$h_A(t) \preccurlyeq \frac{h_{A/(x_1,\ldots,x_e)}(t)}{\prod_{i=1}^{c}(1-t^{e_i})}$$

with equality if and only if $x_1, \ldots, x_c$ is a regular sequence.

Example 4.12. We can compute the Hilbert series for any complete intersection: $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_c)$, where $\deg x_i = d_i$, $\deg f_i = e_i$, and $f_1, \ldots, f_c$ is a regular sequence. First, let $S = k[x_1, \ldots, x_n]$ with $\deg x_i = e_i$. Then $x_1, \ldots, x_n$ is an S-regular sequence with $S/(x_1, \ldots, x_n) = k$. So

$$h_S(t) = \frac{h_k(t)}{\prod_{i=1}^{n}(1-t^{d_i})}$$

Then $h_A(t) = h_{S/(f_1,\ldots,f_c)} = h_S(t)\prod_{j=1}^{c}(1-t^{e_j}) = \dfrac{\prod_{j=1}^{c}(1-t^{e_j})}{\prod_{i=1}^{n}(1-t^{d_i})}$.

Proposition 4.3. *Let A be a Gorenstein graded ring of Krull dimension d. Then $h_A(1/t) = (-1)^d t^a h_A(t)$ for some integer a.*

Proof. Let $x_1, \ldots, x_d$ be a regular sequence so that $\overline{A} = A/(x_1, \ldots, x_d) = \overline{A}_0 \oplus \cdots \oplus \overline{A}_s$ is a finite dimensional Gorenstein algebra. Let $e_i = \deg x_i$. Then we know

(i) $h_A(t) = \dfrac{h_{\overline{A}}(t)}{\prod_{i=1}^{d}(1-t^{e_i})}$

(ii) $h_{\overline{A}}(1/t) = t^{-s}h_{\overline{A}}(t)$

$$\text{So } h_A(1/t) = \frac{h_{\overline{A}}(1/t)}{\prod_{i=1}^{d}(1-(1/t)^{e_i})} = \frac{t^{-s}h_{\overline{A}}(t)}{t^{-e_1-e_2-\cdots-e_d}\prod_{i=1}^{d}(t^{e_i}-1)} = (-1)^d t^{s+e_1+\cdots+e_d}h_A(t)$$

□

Remark. We know that the formula $h_A(1/t) = (-1)^d t^a h_A(t)$ follows from the Gorenstein property, but is not equivalent (even when $d = 0$). Stanley proved that the two are equivalent when A is a CM domain. We will not prove this.

Back to invariant theory. So $S = k[x_1, \ldots, x_n]$, $G \subseteq \mathrm{GL}_n(k)$ finite with $|G| \in k^\times$ and $R = S^G$. We will assume k is algebraically closed.

Definition. The Hilbert series of R is called the Molien series of G.

$$M_G(t) = h_R(t)$$

We will compute $M_G(t)$ in terms of G. More generally, the Molien series of a linear character $\chi : G \to k^\times$ is the Hilbert series of the semi-invariants

$$R_\chi = S^G_\chi = \{f \in S \colon gf = \chi(g)f\}$$

These are graded subsets of S.

$$M_\chi(t) = \sum_{i \in \mathbb{Z}} \dim_k (R_\chi)_i t^i$$

If χ is trivial, then $M_{\text{triv}}(t) = N_G(t)$.

Remark. One can also do this for isotypic components but we will not.

So we want to compute $\dim_k(R_\chi)_i$. Recall that we have the fancy Reynold's operators $\rho_\chi : S \to S$ given by $f \mapsto \frac{1}{|G|} \sum_{g \in G} \chi(g)^{-1} gf$ with image R_χ, and $(\rho_\chi)^2 = \rho_\chi$. These properties preserve degrees, so we get linear maps $(\rho_\chi)_i : S_i \to S_i$ with image $(R_\chi)_i$. We can choose bases for S_i so that $(\rho_\chi)_i$ is in rank normal form: $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$. Then $\dim_k(R_\chi)_i = \dim_k(\mathrm{im}(\rho_\chi)_i) = \mathrm{trace}((\rho_\chi)_i)$. PLug in the formula for ρ_χ: $\dim(R_\chi)_i = \frac{1}{|G|} \sum_{g \in G} \chi(g)^{-1} \mathrm{trace}(g|_{S_i})$.

Theorem 4.7 (Molien)**.**

$$M_\chi(t) = \frac{1}{|G|} \sum_{g \in G} \frac{\chi(g)^{-1}}{\det(I - tg)}$$

In particular,

$$M_G(t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - tg)}$$

Example 4.13. $R = k[u,v]^{C_2} = k[u^2, uv, v^2] \cong k[x,y,z]/(xz - y^2), C_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$.

Then $M_G(t) = \frac{1}{2}\left(\frac{1}{\det(I - tI)} + \frac{1}{\det(I + tI)} \right)$ which is $\frac{1}{2}\left(\frac{1}{(1-t)^2} + \frac{1}{(1+t)^2} \right)$. which is

$$\frac{1 + t^2}{(1 - t^2)^2}$$

which is also the Hilbert series of $k[x,y,z]/(f)$ with $\deg x = \deg y = \deg z = 2$, $\deg f = 4$

$$\frac{1 - t^4}{(1 - t^2)^3} = \frac{1 + t^2}{(1 - t^2)^2}$$

We had to use those degrees to get a graded isomorphism.

We will now focus on the case where $\chi = \text{triv}$, so we want

$$h_R(t) = M_G(t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - tg)}$$

We computed $\dim_k R_i = \frac{1}{|G|} \sum \operatorname{tr}(g|_{S_i})$. So we know that $M_G(t) = \sum_k \dim_k(R_i) t^i = \frac{1}{|G|} \sum_i \sum_{g \in G} \operatorname{tr}(g|_{S_i}) t^i$. Then it suffices to show that

$$\frac{1}{\det(I - tg)} = \sum_{i=0}^{\infty} \operatorname{tr}(g|_{S_i}) t^i$$

for each $g \in G$. So fix $g \in G$. Since G is finite, g has finite order. The formula is true for all $g \in \mathrm{GL}_n(k)$, but finite order makes the proof simpler. In particular, if $g^r = I$, then the minimal polynomial of g divides $x^r - 1$. The roots of $x^r - 1$ are distinct since $\operatorname{char} k \nmid |G|$ (note that if $\operatorname{char} k \mid r$, then $\operatorname{char} k \mid G$ since $r \mid G$). Therefore, the eigenvalues of g are distinct. But then g is diagonalizable. We may assume $g = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, where λ_i are the eigenvalues. In particular, $gx_i = \lambda_i x_i$ for each $x_i \in S = k[x_1, \ldots, x_n]$. The ith graded piece S_i has basis

$$\left\{ x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} : a_1 + \cdots + a_n \right\}.$$

The action of g on S_i sends that basis vector to $\lambda_1^{a_1} \cdots \lambda_n^{a_n} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$. So the action of g on S_i is also diagonal and

$$\operatorname{tr}(g|_{S_i}) = \sum_{a_1 + \cdots + a_n = i} \lambda_1^{a_1} \cdots \lambda_n^{a_n}.$$

So now we use the geometric series:

$$\begin{aligned}\sum_{i=0}^{\infty}\operatorname{tr}(g|_{S_i})t^i &= \sum_{i=0}^{\infty}\sum_{a_1+\cdots+a_n=i}\lambda_1^{a_1}\cdots\lambda_n^{a_n}t^i\\ &= \sum_{i=0}^{\infty}\sum_{a_1+\cdots+a_n=i}(\lambda_1^{a_1}t^{a_1})(\lambda_2^{a_2}t^{a_2})\cdots(\lambda_n^{a_n}t^{a_n})\\ &= \sum_{i=0}^{\infty}\sum_{a_1+\cdots+a_n=i}(\lambda_1 t)^{a_1}(\lambda_2 t)^{a_2}\cdots(\lambda_n t)^{a_n}\\ &= \frac{1}{1-\lambda_1 t}\,\frac{1}{1-\lambda_2 t}\cdots\frac{1}{1-\lambda_n t}\\ &= \frac{1}{\prod_{j=1}^{n}(1-\lambda_j t)}\end{aligned}$$

Now

$$\prod_{j=1}^{n}(1-\lambda_j t) = \frac{\prod_{j=1}^{n}\lambda_j^{-1}}{\prod_{j=1}^{n}(\lambda_j^{-1}-t)} = \frac{\det(g^{-1})}{\deg(g^{-1}-tI)}\cdot\frac{\det g}{\det g} = \frac{1}{\det(I-tg)}$$

□

Example 4.14. Using Molien's formula to compute invariants Let

$$G = \left\{\begin{pmatrix}\pm 1 & \\ & \pm 1\end{pmatrix}\begin{pmatrix}\pm i & 0\\ 0 & \mp i\end{pmatrix}\begin{pmatrix}0 & \pm i\\ \pm i & 0\end{pmatrix}, \begin{pmatrix}\pm 1 & \\ & \pm 1\end{pmatrix}\right\} = Q_8$$

What is $k[u,v]^G$? Molien's fomula says

$$h_R(t) = \frac{1}{8}\left(\frac{1}{(1-t)^2}+\frac{1}{(1+t)^2}+\frac{6}{1+t^3}\right) = \frac{1+t^6}{(1-t^4)^2} = 1+2t^4+t^6+\cdots$$

So R contains 2 linearly independent polynomials of degree 4 and 6. After a brief such, u^2v^2 and u^4+v^4 are invariant. Since they're invariant, so is their Jacobian so that $u^5v-uv^5 \in R_6$. Set $X = u^4+v^4$, $Y = u^2v^2$, and $Z = u^5-uv^5$. These must then live inside: so $k[X,Y,Z] \subseteq R = k[u,v]^G$. Any 3 polynomials in $k[u,v]$ have some defining relation so can cretae that $Z^2 = X^2Y - 4Y^3$. So $A = k[X,Y,Z] \cong k[y,z,]/(z^2-x^2y+4y^3)$. Then $h_A(t) = \dfrac{1-t^{1/2}}{(1-t^4)^2(1-t^6)} = \dfrac{1}{t^6}(1-t^4)^2 = h_R(t)$. But then $A = R$. Finally when S^G is gorenstein, recall a pseudo-reflection is an $n\times n$ matrix of finite order having 1 as an eigenvalue of multiplicity $n-1$.

$$g = \begin{pmatrix}1 & 1 & \cdots\\ & 1 & \\ & \ddots & \\ & & \lambda\end{pmatrix}, \quad \lambda^r = 1.$$

Theorem 4.8 (Stanley, Watanabe). *Let $G \subseteq \mathrm{GL}_n(k)$ be a finite subgroup with $|G| \in k^\times$. Then $R = k[x_1, \ldots, x_n]^G$ is gorenstein if and only if*

$$\sum_{g \in G} \frac{1}{\det(I - tg)} = t^{-m} \sum_{g \in G} \frac{\det g}{\det(I - tg)}$$

where m is the number of pseudo-relections in G. In particular, when G is small (i.e. $m = 0$), then R is Gorenstein if and only if $G \subseteq \mathrm{SL}_n(k)$.

Proof. We will use fact that since R is a domain, R is gorenstein if and only if

$$h_A(1/t) = (-1)^d t^a h_A(t)$$

for some $a \in \mathbb{Z}$. Plug in our formula for $h_R(t) = M_G(t)$

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - tg)} = h_R(t) = (-1)^d t^{-a} h_R(1/t) = \frac{1}{|G|}(-1)^d t^{-a} \sum_{g \in G} \frac{1}{\det(I - t^{-1}g)} \cdot \frac{t \deg(g)^{-1}}{t(\det g)^{-1}} = \frac{1}{|G|}(-1$$

Now

$$\sum_{g \in G} \frac{1}{\det(I - t^{-1}g)} = (-1)^n \sum_{g \in G} \frac{1}{\det(t^{-1}g - I)} = (-1) \sum_{g \in G} \frac{\deg(g)^{-1}}{\det(t^{-1}I - g^{-1})} = (-1) \sum_{g \in G} \frac{\det g}{\det(t^{-1}I - g)} = (-$$

So

$$\sum_{g \in G} \frac{1}{\det(I - tg)} = t^{-a+n} \sum_{g \in G} \frac{\det g}{\det(I - tg)}$$

up to sign. So we need to just identify $m = a - n$ as the number of pseudo-reflections. Expanding both sides of the above as Laurent series in $1 - t$. Recall that a Laurent series $\frac{c_r}{(1-t)^r} + \frac{c_{r-1}}{(1-t)^{r-1}} + \cdots$ with $c_r \neq 0$ has a pole of order r at $t = 1$. We know each term $\frac{1}{\det(I - tg)}$ is equal to

$$\frac{1}{\prod_{j=1}^n (\lambda_j - t)}$$

since g is diagonalizable and $k = \bar{k}$. We need to know the multiplicity of 1 as an eigenvalue—that will be the order of the pole at $t = 1$. The biggest the multiplicity can be is n, when $g = I$, if and only if $g = I$. The next biggest is $n - 1$ if and only if g is a pseudo-reflection. So

$$\sum_{g \in G} \frac{1}{\det(I - tg)} = \frac{1}{(1-t)^n} + \sum_{g \text{ ps ref}} \frac{1}{(1-t)^{n-1}(\det g - t)} + \text{h.o.t.} = \frac{1}{(1-t)^n} + \frac{1}{(1-t)^{n-1}} \sum_{g \text{ps}} \frac{1}{\det g - t} + \text{h.o}$$

To get this in terms of only $(1-t)$, we need

$$\frac{1}{(1-t)^{n-1}} \sum_{g\text{ps}} \frac{1}{\det g - t} = \frac{c_{n-1}}{(1-t)^{n-1}} + \frac{c_{n-2}}{(1-t)^{n-2}} + \cdots$$

To solve for c_{n-1}, multiply by $(1-t)^{n-1}$ and plug in $t = 1$.

$$\sum_{g\text{psd}} \frac{1}{\det g - 1} = c_{n-1}$$

and that is equal to $\sum_{g\text{psd}} \frac{1}{1-\det g}$. On the left hand side, we have

$$\frac{1}{(1-t)^n} + \frac{1}{(1-t)^{n-1}} + \sum_{g\text{psd}} \frac{1}{1-\det g} + \text{h.o.t.}$$

The right hand side is, using $t^{-m} = \left(\frac{1}{t}\right)^m = \left(\frac{1}{1-(1-t)}\right)^m = \left(\sum_{i=0}^{\infty}(1-t)^i\right)^m = (1+(1-t)+(1-t)^2+\cdots)^m = 1 + m(1-t) + \cdots$

$$t^{-m} \sum_{g\in G} \frac{\det g}{\det(I-tg)} = (1 + m(t-1) + \cdots) \cdot \left(\frac{1}{(1-t)^n} + \frac{1}{(1-t)^{n-1}} \sum_{g\text{psd}} \frac{\det g}{1-\det g} + \cdots\right)$$

The coefficient of $\frac{1}{(1-t)^{n-1}}$ in this product is $m + \sum_{g\text{psd}} \frac{\det g}{1-\det g}$. Now we are done by comparing coefficients we obtain that

$$\sum_{g\text{psd}} \frac{1}{1-\det g} = m + \sum_{g\text{psd}} \frac{\det g}{1-\det g}$$

Moving over left sum, obtain

$$\sum_{g\text{psd}} 1 = m$$

so that m is the number of pseudo-reflections. □

For the last sentence, we just need to show that $\sum_{g\in G} 1 = \sum_{g\in G} \det g$ if and only if $\det g = 1$ for all g. If $\det g = 1$, then simple. For the other direction, recall $\det g$ is a root of unity. So then must be all 1 since add to 1.

Corollary 4.6 (Watanabe). *If $G \subseteq \mathrm{SL}_n$, then R is Gorenstein. Furthermore, if G is small, then the converse holds.*

Proof. If $G \subseteq \mathrm{SL}_n$, then $\det g = 1$ for all $g \in G$. There are no pseudo-reflections in SL. In particular, there are no pseudo-reflections in G. The last part was done above (all parts of G are roots of unity). □

When is $R = k[W]^G$ an isolated singularity? Postpone this until ramification theory. (Answer: when no $g \in G \setminus \{1\}$ has 1 for an eigenvalue, which is stronger than no pseudo-reflections.)

Recall our goal is to understand the direct summands of $S = k[W]$ as an R-module (they are all MCM modules) and the structure of

1) the maps between them 2) the relationship with the rest of the R-modules.

Main tool: the skew group algebra (twisted group ring, smash product, ...)

Let S be a commutative ring (lose nothing by pretending $S = k[W]$) and G be a group acting on S by automorphisms. The skew group algebra $S\#G$ is an S-module, free on the elements of G, so the elements of $S\#G$ are formal sums $\sum_{g\in G} s_g \cdot g$, where $s_g \in S$ for all $g \in G$. The action is $(s \cdot g)(t \cdot h) = sg(t)gh$ for $s, t \in S$ and $g, h \in G$. So moving g past t twisted the ring element. Why? Patience. What are the $S\#G$ modules?

Notice S sits inside $S\#G$ as $\{s \cdot 1_G\}$ as a subring. So $S\#G$ is an S-algebra. In particular, any $S\#G$-module M is an S-module by restriction of scalar. On the other hand, G also sits inside $S\#G$ as $\{1_s \cdot g\}$. So M comes with a G-action $g(x) = (1_s \cdot g)x$, $x \in M$, $g \in G$. So $S\#G$-module is an S-module with an action of G. That action is compatible with the S-module structure:

$$\begin{aligned} g(sx) &= g((s1)x) \\ &= (1g)(s1)x \\ &= (g(s)g)x \\ &= (g(s)1)(1g)x \\ &= g(s)g(x) \end{aligned}$$

Conversely, an S-module M with an action of G that satisfies $g(sx) = g(s)g(x)$ is an $S\#G$-module.

Remark. This allows us to talk about the invariants of an $S\#G$-module, namely $M^G := \{x \in M : gx = x\}$. Also notice that S itself is an S-module with a compatible G-action. So we can consider S^G.

Similarly, an $S\#G$-homomorphism between $S\#G$-modules M, N is an S-module homomorphism that respects the group action. So $f : M \to N$ is $S\#G$-linear if and only if it is S-linear and $f(g(x)) = g(f(x))$ for all $x \in M$, $g \in G$.

We can define an $S\#G$-module structure on $\mathrm{Hom}_S(M, N)$: given $f : M \to N$ and $g \in G$, $(gf)(x) = g(f(g^{-1}(x)))$. It is routine to check that the action is compatible with the S-module structure.

What is $\mathrm{Hom}_S(M,N)^G$? Well, f is invariant if and only if $gf = f$ for all g if and only if $(gf)(x) = f(x)$ for all g if and only if $g(f(g^{-1}(x))) = f(x)$ for all g if and only if $f(g^{-1}(x)) = g^{-1}(f(x))$ for all g. So an S-linear map is invariant if and only if it is $S\#G$-linear. Another way of saying this is $\mathrm{Hom}_S(M,N)^G = \mathrm{Hom}_{S\#G}(M,N)$ (an actual equality).

Fact: If $|G|$ is invertible in S, then taking G-invariants is an exact functor, i.e. if $0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$ is an exact sequence of $S\#G$-modules, then

$$0 \longrightarrow L^G \xrightarrow{\text{res } \alpha} M^G \xrightarrow{\text{res } \beta} N^G \longrightarrow 0$$

is an exact sequence.

Check: The restriction of an injective is clearly injective. Clearly the composition of the restrictions is also 0. We will only check surjectivity. Take $y \in N^G \subseteq N$. Then there is $x \in M$ with $\beta(x) = y$. Notice for any $g \in G$, $\beta(gx) = g(\beta x) = g(y) = y$. So

$$\beta\left(\frac{1}{|G|}\sum_{g\in G} g(x)\right) = y$$

and the sum is in M^G. The same trick works for exactness in the middle.

Consequently, $\mathrm{Ext}^i_{S\#G}(M,N) = \mathrm{Ext}^i_S(M,N)^G$.

Corollary 4.7. *An $S\#G$-module is projective if and only if it is projective over S.*

Proof. We know P is projective over a ring T if and only if $\mathrm{Ext}^i_T(P,-) = 0$ for $i > 0$. Then ${}_{S\#G}M$ is projective if and only if $\mathrm{Ext}^i_{S\#G}(M,-) = 0$ for $i > 0$ if and only if $\mathrm{Ext}^i_S(M,-)^G = 0$. We know $\mathrm{Ext}^i_S(M,-) = 0$ if and only if ${}_SM$ is projective. It remains to show that $\mathrm{Ext}^i_S(M,-)^G = 0$ if and only if $\mathrm{Ext}^i_S(M,-) = 0$.

It is clear that if $\mathrm{Ext}^i_S(M,-) = 0$ then $\mathrm{Ext}^i_S(M,-)^G = 0$. Now if M is projective, i.e. $\mathrm{Ext}^i_S(M,-) = 0$, it is a direct summand of $(S\#G)^n$ for some n. But $S\#G$ is free as an S-module, so M is also projective over S. □

Corollary 4.8. *If $S = k[x_1,\dots,x_n]$, then $S\#G$ has global dimension n, i.e. $n = \max\{\text{proj dim}_{S\#G}M\colon M \text{ f.g. over } S\#G\}$.*

Proof. Recall $\mathrm{proj\,dim}_{S\#G}M = \max\{i\colon \mathrm{Ext}^i_{S\#G}(M,-) \neq 0\}$. But this is $\max\{i\colon \mathrm{Ext}^i_S(M,-)^G \neq 0\}$. But this is at most $\max\{i\colon \mathrm{Ext}^i_S(M,-) \neq 0\}$, which is at most n by Auslander-Buchsbaum-Serre, which says that the global dimension of a polynomial ring (or any regular ring) is n. So g, $\dim S\#G \leq n$. To show equality, we must construct an $S\#G$-module of projective dimension n. The short version is that the Kozul Complex on $x_1,\dots,x_n$ is an $S\#G$-linear free resolution of $S/(x_1,\dots,x_n) \cong k$.

The longer version: Let $V = (x_1,\dots,x_n)/(x_1,\dots,x_n)^2$. This is a k-vector space of rank n with basis $x_1,\dots,x_n$ (really bars). And $K_p := S \otimes_k \bigwedge^p V$, where $p \geq 0$ and $\bigwedge^p V$ is the pth

exterior power of V. This means it has basis $\{x_{i_1} \wedge x_{i_2} \wedge \cdots \wedge x_{i_p} : i_1 < i_2 < \cdots < i_p\}$. Then $S \otimes_k \bigwedge^p V$ is the free S-module on the same basis. Since G acts on S linearly, it acts on V. It therefore acts on $\bigwedge^p V$ for all p. The main thing about $\bigwedge^p V$ is $v \wedge w = -(w \wedge v)$ for all $v, w \in V$. With that, not only is each $\bigwedge^p$ a representation of G, the maps $\bigwedge^p V \to \bigwedge^{p+1} V$ given by $\omega \mapsto \omega \wedge (\sum x_i) = \sum(\omega \wedge x_i)$ and the maps are G-linear. The exact sequence

$$0 \longrightarrow S \otimes \overset{0}{\bigwedge} V \longrightarrow S \otimes \overset{1}{\bigwedge} V \longrightarrow S \otimes \overset{2}{\bigwedge} V \longrightarrow \cdots \longrightarrow S \otimes \overset{n}{\bigwedge} V \longrightarrow 0$$

is an S-linear free resolution of $S/(x_1, \ldots, x_n)$. Note the last two above are congruent to $S^n \to S$ with map $e_i \mapsto \sum x_j$, $j \neq i$. Furthermore, each free module and each map (differential) is G-linear. So this is a free resolution of k over $S\#G$. This can not be a shorter one since we know that proj $\dim_S k = n$. So gl $\dim S\#G = n$. □

So in the case where $S = k[W]$, the ring $S\#G$ encodes all S-modules with G-action, and has global dimension $n = \dim W$ (like S).

The "twist" in the algebra structure is cooked up exactly to make a certain map a ring homomorphism. Let $S = k[W]$, G a finite group with $|G| \in k^\times$, and $R = S^G$. Consider the endomorphism ring $\mathrm{End}_R(S)$ of S as an R-module. Define

$$\gamma : S\#G \longrightarrow \mathrm{End}_R(S)$$

by considering an S-linear combination of endomorphisms of S as an endomorphism of S.

$$\sum s_g \cdot g \mapsto \sum s_g g.$$

Note: each $g \in G$, considered as an endomorphism of S, is R-linear

$$g(rs) = g(r)g(s) = rg(s)$$

for $r \in R$, $s \in S$. Finally, γ is a ring homomorphism. Moreover, γ is not generally injective or surjective.

Theorem 4.9 (Auslander, 62)**.** *If G is small, then γ is an isomorphism.*

To prove this, we will need Ramification Theory, i.e. unramified and étale maps.

4.6 Ramification Theory

Recall a ring homomorphism $A \to B$, where A, B are commutative noetherian rings, is of *finite type* if B is a finitely generated A-algebra, i.e. $B \cong A[x_1, \ldots, x_r]/I$ for some ideal I. The morphism is *essentially of finite type* if B is a localization of an A-algebra of finite type, i.e. $B \cong (A[x_1, \ldots, x_r]/I)_S$.

Definition (Ramified)**.** Let $\phi : (A, \mathfrak{m}, k) \to (B, \mathfrak{n}, l)$ is a local homomorphism ($\phi(\mathfrak{m}) \subseteq \mathfrak{n}$, i.e. no non-unites of A become units in B) of local noetherian rings. We say ϕ is unramified if

(i) it is essentially of finite type

(ii) $\mathfrak{m}B = \mathfrak{n}$

(iii) $k \to l$ is a finite separable field extension

If in addition $A \to B$ is flat, ϕ is called étale.

Remark. Some people call this "essentially unramified" and reserve unramified for maps of finite type. Intuition if p is a prime element in $\mathbb{Z}$ and $\mathcal{O}$ is some finite $\mathbb{Z}$-algebra, the prime p might split, $qr = p$, or ramify, $q^e = p$.

Example 4.15. 1) A finite separable field extension is unramified and even étale.

2) Any quotient $A \to A/I$, $I \neq 0$, is unramified (with no residue field growth) but never flat, so not étale.

3) Let $(A, \mathfrak{m}, k)$ be a local ring, $f(x) \in A[x]$ a monic irreducible polynomial, and $q \subseteq A[x]$ a prime ideal containing $\mathfrak{m}$ not containing $f'(x)$. Set $B = (A[x]/(f(x)))_q$. What is $B/\mathfrak{m}B$? Well

$$B \otimes_A A/\mathfrak{m} \cong (k[x]/(f(x)))_{\overline{q}} = k[x]/(f(x))$$

and in particular $f'(x) \neq 0$ in this ring (really its image). But then this is a finite separable extension of k. In particular, $\mathfrak{m}B$ must be a maximal ideal (following the congruences, get a field), so $\mathfrak{m}B = qB = \mathfrak{n}$ is the unique maximal ideal of B. So B is unramified over A. This is also étale, though we will not show this. This construction is called a pointed étale neighborhood of A.

Facts: a) Every unramified local map $A \to B$ is 'basically' of this form: every unramified local map $A \to B$ factors as a sequence of pointed étale neighborhood followed by a surjection. ("Local Structure Theorem for Étale Maps").

b) Taking $\varinjlim\{$ pointed étale neighborhoods of $A\}$ is "the" Henselization of A, the smallest A-algebra satisfying Hensel's Lemma $A \hookrightarrow A^n \hookrightarrow \widehat{A}$.

Extended definition: A ring homomorphism $A \to B$ is unramified at a prime ideal q in Spec B if the induced map $A_{q \cap A} \to B_q$ is unramified. It is unramified if it is unramified at every prime ideal.

Example 4.16. If $l_1, \ldots, l_t$ are finite separable field extensions of a field k, then $k \to l_1 \times \cdots \times l_t$ is unramified (and in fact étale).

BIG FACT: Every unramified field extension of a field is of this form, products of finite separable extensions. (Serre, 50s?).

Why is this truly a more general definition? Problem: For this to be consistent with the old definition, we need unramified-ness to localize. To do this, we need to give a different definition which is equivalent and obviously localizes.

Definition (Enveloping Algebra)**.** Let $A \to B$ be a ring homomorphism. The enveloping algebra is $B \otimes_A B$.

BTW if A and B were noncommutative, what we would use is $B \otimes_A B^{\mathrm{op}}$. There is a natural map $\mu : B \otimes_A B \to B$ given by $b \otimes b' \mapsto bb'$, extending by linearity. This is a surjective ring homomorphism.

Set $J = \ker \mu$, an ideal of $B \otimes_A B$. Then $B \cong B \otimes_A B/J$. Equivalently, we have a short exact sequence

$$0 \longrightarrow J \longrightarrow B \otimes_A B \longrightarrow B \longrightarrow 0.$$

Remarks: J is generated (as an ideal of $B \otimes_A B$) by elements of the form $b \otimes 1 - 1 \otimes b$. Certainly, J contains those. On the other hand if

$$\mu\left(\sum_i b_i \otimes b_i'\right) = 0,$$

then $\sum_i b_i b_i' = 0$. But $\sum_i b_i b_i' = \sum_o (1 \otimes b_i')(b_i \otimes 1 - 1 \otimes b_i)$ is generated by elements of the appropriate 'shape.'

2) Caution: $B \otimes_A B$ has two B-module structures on the left and on the right: $b \cdot (b' \otimes b'') = bb' \otimes b''$, $(b' \otimes b'')b = b' \otimes b''b$ and *they do not have to agree*. In particular, J has two distinct B-module structures. Luckily, they coincide modulo J^2: Claim for any $b, b' \in B$

$$b(b' \otimes 1 - 1 \otimes b') - (b' \otimes 1 - 1 \otimes b')b \in J^2.$$

This is

$$bb' \otimes 1 - b \otimes b' - b' \otimes b + 1 \otimes b'b = (b \otimes 1 - 1 \otimes b)(b' \otimes 1 - 1 \otimes b') \in J^2$$

So J/J^2 has an unambiguous B-module structure. By the way, this is sometimes called the *module of Kähler differentials* of B/A, written $\Omega^1_{B/A}$.

3) If $A \to B$ is essentially of finite type, then J/J^2 is a finitely generated B-module. Specifically, if $B = (A[x_1, \ldots, x_r]/I)_W$, then J/J^2 is generated over B by $\overline{x_i \otimes 1 - 1 \otimes x_i}$, $i = 1, \ldots, r>$ So J/J^2 localizes well: it vanishes if and only if it vanishes locally at every maximal or prime ideal.

Lemma 4.4. *Let $A \to B$ be a ring homomorphism, essentially of finite type. TFTA:*

i) B is projective as a $B \otimes_A B$-module. ii) the exact sequence

$$0 \longrightarrow J \longrightarrow B \otimes_A B \xrightarrow{\mu} B \longrightarrow 0$$

splits as $B \otimes_A B$-modules.

(iii) $\mu(\mathrm{ann}_{B \otimes_A B} J) = B$.

iv) J is generated by an idempotent of $B \otimes_A B$: a single element e satisfying $e^2 = e$

v) $J/J^2 = 0$.

Proof. (i) $\iff$ (ii) is obvious. via the exact sequence.

(ii) $\iff$ (iii): The map μ splits if and only if the induced homomorphism

$$\mathrm{Hom}_{B\otimes_A B}(B,\mu) : \mathrm{Hom}_{B\otimes_A B}(B, B\otimes B) \xrightarrow{\mu\otimes -} \mathrm{Hom}_{B\otimes_A B}(B,B)$$

the identity is in the image, i.e. the map is surjective. We know $B \cong B\otimes_A B/J$ as $B\otimes_A B$-modules, so $\mathrm{Hom}_{B\otimes_A B}(B,X) = \mathrm{Hom}_{B\otimes_A B}(B\otimes_A B/J, X) \cong \{x\in X\colon Jx=0\} = \mathrm{ann}_X J$. So in those terms, we want

$$\mathrm{ann}_{B\otimes_A B} J \xrightarrow{\mu} \mathrm{ann}_B J$$

to be surjective. So μ splits if and only if $\mu(\mathrm{ann}_{B\otimes_A B} J) = B$.

Finally, (iv) $\iff$ (v) are true for any finitely generated ideals.

(ii) $\iff$ (iv): If $\mu : B\otimes_A B \to B$ splits, there is some $B\otimes_A B$-linear map $j : B \to B\otimes_A B$ with $\mu j = 1_B$. Set $e = j(1)$ (a separability idempotent). Then $e^2 = e$ and e generates (Check) J as $B\otimes_A B$-ideal. □

Proposition 4.4. *Let $A \to B$ be essentially of finite type. TFAE:*

i) the exact sequence

$$0 \longrightarrow J \longrightarrow B\otimes_A B \xrightarrow{\mu} B \longrightarrow 0$$

splits as $B\otimes_A B$-modules.

ii) $A \to B$ is unramified

iii) $A_{\mathfrak{m}} \to B_{\mathfrak{n}}$ is unramified for every maximal ideal $\mathfrak{n} \subseteq B$ with $\mathfrak{m} = \mathfrak{n}\cap A$.

Proof. In the notes. □

We shall try to explain what $\Omega_{B/A} = J/J^2$ has to do with (un)ramified-ness. The connection is derivations.

Definition (Derivation)**.** Let A be a ring and M an A-module. A function $D : A \to M$ is called a derivation if

- $D(a+b) = D(a) + D(b)$
- $D(ab) = aD(b) + D(a)b$ (Leibniz/Product Rule)

for all $a, b \in A$

Technically, this is a $\mathbb{Z}$-derivation. If $k \subseteq A$ is a subring so that D is k-linear, i.e. $D(\alpha a) = \alpha D(a)$ for $\alpha \in k$, $a \in A$, then D is called a k-derivation.

Remark. These behave like derivatives: 1) $D(1) = 0$ 2) D is k-linear iff $D(k) = 0$, i.e. $D(\alpha) = 0$ for all $\alpha \in k$. (Use product rule) 3) $D^{-1}(\{0\})$ is a subring of A, so there is a unique largest k such that D is k-linear. 4) $D(a^n) = na^{n-1}D(a)$ for any $a \in A$, $n \geq 0$. Simple

to prove by induction. In particular, if char $A = n$, then $D(a^n) = 0$ so D is necessarily A^n-linear. Extending this, if $a \in A$ and $f(x) \in A[x]$, $D(f(a)) = f'(a)D(a)$! 5) If $\phi : M \to N$ is an A-module homomorphism and $D : A \to M$ is any derivation, then $\phi \circ D : A \to N$ is also a derivation. So if we write $\mathrm{Der}_k(A, M) = \{\text{k-linear derivations } A \to M\}$, then $\mathrm{Der}_k(A, M)$ is an A-module. [Take ϕ to be $M \xrightarrow{a} M$.] And in fact, $\mathrm{Der}_k(A, M)$ is a functor: any $\phi : M \to N$ induces a map $\mathrm{Der}_k(A, M) \to \mathrm{Der}_k(A, N)$ given by $\phi \mapsto \phi\circ$ and is an A-module homomorphism.

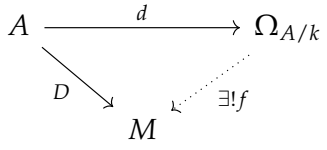
Is this functor representable, i.e. can it be written as a Hom? Specifically, is there a "special" A-module Ω such that $\mathrm{Der}_k(A, M) \cong \mathrm{Hom}_A(\Omega, M)$ for every M? As it turns out, this is the case and we will construct this Ω.

Example 4.17. Take $A = k[x]$. What is in $\mathrm{Der}_k(A, A)$? We know that $D(k) = 0$ for all $k \in k$. If we know $D(x)$, then we are done as $D(f(x)) = f'(x)D(x)$ for all f, so D is determined by $D(x)$. In fact, $D(x)$ can be arbitrary. [Check the rules. Keeping in mind you have defined this on a generator.] If say $D(x) = q(x)$, then for any $f(x)$, $D(f(x)) = f'(x)q(x)$. In other words, $D = q(x)\dfrac{d}{dx}$. Equivalently, $\mathrm{Der}_k(A, A) \cong A\dfrac{d}{dx}$ is a free A-module of rank 1, generated by $\dfrac{d}{dx}$.

Example 4.18. $A = k[x_1, \ldots, x_n]$. Any function of the form $\sum_{i=1}^n q_i(x)\dfrac{\partial}{\partial x_i}$ is a derivation and these are in fact all the derivations. So $\mathrm{Der}_k(A, A) = \bigoplus_{i=1}^n A\dfrac{\partial}{\partial x_i}$ is a free module of rank n.

Example 4.19. Take $A = k[x]$. What is in $\mathrm{Der}_k(A, M)$? We know that $D(k) = 0$ for all $k \in k$. If we know $D(x)$, then we are done as $D(f(x)) = f'(x)D(x)$ for all f, so D is determined by $D(x)$. In fact, $D(x)$ can be arbitrary. [Check the rules. Keeping in mind you have defined this on a generator.] If say $D(x) = m$, then for any $f(x)$, $D(f(x)) = f'(x)m$. In other words, $D = m\dfrac{d}{dx}$. Equivalently, $\mathrm{Der}_k(A, M) \cong M\dfrac{d}{dx}$ is a free A-module of rank 1, generated by $\dfrac{d}{dx}$.

Using these examples, we can see that for $A = k[x_1, \ldots, x_n]$, it should be the case that $\Omega A/k = A^n$. Now we actually construct $\Omega_{A/k}$. Now $\Omega_{A/k}$ should come with a universal derivation $d : A \to \Omega_{A/k}$ such that for any derivation $D : A \to M$, there is a unique A-module homomorphism $f : \Omega \to M$ making the following diagram commute



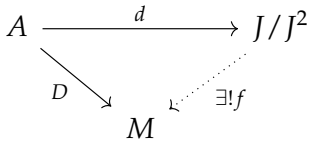
If such an object exists, it is unique by traditional abstract nonsense. It will turn out that $\Omega_{A/k} \cong J/J^2$, where $J = \ker(A \otimes_k A \xrightarrow{\mu} A)$. You can construct $\Omega_{A/k}$ abstractly. Let F be the free A-module on symbols $\{d_a\}_{a\in A}$. Let H be the submodule generated by $\{d_{a+b} - d_A - d_b, d_{ab} - ad_b - bd_a, d_\alpha\}_{a,b\in A,\alpha\in k}$. Then $A \to F/H$ given by $a \mapsto d_a$ is the correct object. However, this definition is not useful. Is this even nonzero?! We focus on the fact that we shall have $\Omega_{A/k} \cong J/J^2$, and follow an alternative construction.

Let $J = \ker(A \otimes_k A \to A)$. Then we know that J/J^2 is an A-module. Define $d : A \to J/J^2$ by $a \mapsto a \otimes_1 -1 \otimes a$. Is this a derivation? The only real question here is does this satisfy the Leibniz rule?

$$\begin{aligned} d(ab) &= ab \otimes 1 - 1 \otimes ab \\ &= a(b \otimes 1 - 1 \otimes b) + (a \otimes 1 - 1 \otimes a)b \\ &= ad(b) + bd(a) \mod J^2 \end{aligned}$$

Proposition 4.5. *$(J/J^2, d)$ has the desired universal property.*

Proof. Let $D : A \to M$ be a derivation.



We use the "idealization" or "trivial extension" of M. The trivial extension is a ring $B = A \ltimes M = \left\{ \begin{pmatrix} a & m \\ 0 & a \end{pmatrix} : a \in A, m \in M \right\}$ under matrix multiplication. This is the same as $\{(a, m) \colon A \oplus M\}$ with multiplication $(a, m)(a', m') = (aa', am' + a'm)$. Then B is a ring, commutative if A is commutative. We have $A \hookrightarrow B$ as $\{(a, 0)\}_{a\in A}$ as a subring, and $M \hookrightarrow B$ as $\{(0, m)\}_{m\in M}$. Notice that $(a, 0)(0, m) = (0, am')$ so M is an ideal of B. Furthermore, $M^2 = 0$ by considering $(0, m)(0, m')$. There is a ring homomorphism $A \otimes_k A \to B = A \ltimes M$ given by $a \otimes a' \mapsto (aa', a'(Da))$. In particular, $h(a \otimes 1) = (a, D(a)), h(1 \otimes a) = (a, 0)$. What happens to J^2? $h(a \otimes 1 - 1 \otimes a) = (a, D(a)) - (a, 0) = (0, D(a)) \in M$. In particular, J^2 maps into $M^2 = 0$. So h induces a homomorphism $J/J^2 \to M$ given by $a \otimes 1 - 1 \otimes a \mapsto D(a)$. This is exactly what is needed (along with $J^2 \to 0$) to make the diagram commute. □

Proposition 4.6 (Basic Properties of $\Omega_{A/k}$)**.**

(i) if A is generated as a k-algebra by elements $\{a_\lambda\}_{\lambda\in\Lambda}$, then $\Omega_{A/k}$ is generated by $\{a_\lambda \otimes 1 - 1 \otimes a_\lambda\}_{\lambda\in\Lambda} = \{d(a_\lambda)\}_{\lambda\in\Lambda}$.

(ii) if $A \cong k[\{x_\lambda\}_{\lambda\in\Lambda}]$ is a polynomial ring over k, then $\Omega_{A/k}$ is a free A-module on $\{d(x_\lambda)\}_{\lambda\in\Lambda}$.

(iii) *if $\{A_\lambda\}_{\lambda\in\Lambda}$ is a directed system of k-algebras, and $A = \varinjlim A_\lambda$, then $\Omega_{A/k} = \varinjlim \Omega_{A_\lambda/k}$.*

(iv) *if $\phi : A \to A'$ is a ring homomorphism and $D : A' \to N$ is a derivation, then $D \circ \phi : A \to N$, so we obtain a map $\mathrm{Der}_k(A', N) \to \mathrm{Der}_k(A, N)$.*

(v) *if $\phi : A \to A'$ is a ring homomorphism, there is an induced A-linear map $\Omega_{A/k} \to \Omega_{A'/k}$ given by $d(a) \mapsto d(\phi(a))$ and so an A'-linear map $A' \otimes_A \Omega_{A/k} \to \Omega_{A'/k}$.*

Proof.

1) we have seen

3) do not care

4) is routine

2) We construct a k-derivation from $A \to \bigoplus A\, d(x_\lambda)$ and show that it has the universal property. We should send x_λ to $d(x_\lambda)$. Extend this to monomials in the variables x_λ using the Leibniz rule, and extend by additivity to all of A. In the end, this defines $\delta : A \to \bigoplus_{\lambda\in\Lambda} A\, d(x_\lambda)$ given by $f(\underline{x}) \mapsto \sum_\lambda \dfrac{\partial f}{\partial x_\lambda}\, d(x_\lambda)$. each polynomial involves only finitely many λ's, so the sum is indeed finite. To show universality, let $D : A \to M$ be the derivation,

$$\begin{array}{ccc} A & \xrightarrow{\quad d \quad} & \bigoplus A\, d(x_\lambda) \\ & \searrow^{D} & \vdots\, f \\ & & M \end{array}$$

We have to define $f(d(x_\lambda)) = D(x_\lambda)$. This forms a well defined map since the $\{d(x_\lambda)\}$ form a basis. Commutativity and uniqueness are now also both obvious.

5) Given $\phi : A \to A'$, we have

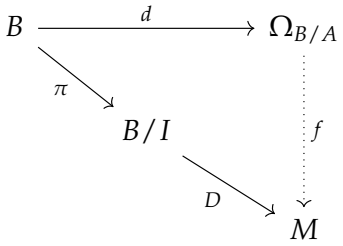
$$\begin{array}{ccc} A & \xrightarrow{d_A} & \Omega_{A/k} \\ \downarrow{\scriptstyle \phi} & & \vdots \\ A' & \xrightarrow{d_{A'}} & \Omega_{A'/k} \end{array}$$

By (4), the diagonal $d_{A'} \circ \phi : A \to \Omega_{A'/k}$ is a derivation. By the universal property of $\Omega_{A/k}$, there is a unique A-module homomorphism $\Omega_{A/k} \to \Omega_{A'/k}$ making the diagram commute. The last assertion that this induces an $A' \otimes_A \Omega_{A/k} \to \Omega_{A'/k}$ is just a general fact about tensor products. □

Let $A \to B$ be a map.

Proposition 4.7. *Let B be an A-algebra and $I \subseteq B$ an ideal. Then $\Omega_{(B/I)/A} \cong \Omega_{B/A}/K$, where K is the B-span of $\{d(i)\}_{i\in I}$.*

Proof. First, for any $b \in B$ and $i \in I$, $id(b) = d(bi) - bd(i)$, which are both in K. Therefore, $I\Omega_{B/A} \subseteq K$ since B is generated by $\{d(b)\}_{b\in B}$. But then $\Omega_{B/A}/K$ is a B/I-module. To check the universal property, observe we have an induced derivation $\overline{d} : B/I \to \Omega_{B/A}/I$ given by $\overline{b} \mapsto \overline{d(b)}$, which is well defined by the work above. Suppose then that $D : B/I \to M$ is any A-linear derivation.



We know $D \circ \pi$ is still a derivation, so there exists a unique $f : \Omega_{B/A} \to M$ such that $f \circ d = D \circ \pi$. Then $f(d(i)) = D(\pi(i)) = 0$so f maps K to zero. Therefore, we have an induced map $\Omega_{B/A}/K \xrightarrow{\overline{f}} M$ which is clearly unique. □

Proposition 4.8. *Let k be a field and $p(x) \in k[x]$ be an irreducible polynomial, i.e. $A = k[x]/(p(x))$ is a field. Then $\Omega_{A/k} \cong A/(p'(x)) = k[x]/(p(x), p'(x))$. In particular, $\Omega_{A/k} = 0$ if and only if $k \to A$ is separable, i.e. unramified.*

Proof. The last sentence follows from the first as the extension is separable if and only if $\gcd(p, p') = 1$ if and only if $(p, p') = k[x]$. Set $S = k[x]$. We know that $\Omega_{S/k} \cong S\,\frac{d}{dx}$. Using Proposition 4.7, we have

$$\Omega_{A/k} \cong \Omega_{S/k}/S\text{-span of } \{d(i)\}_{i\in(p)}.$$

However, elements in (p) are of the form gp for some $g \in k[x]$. Then $d(gp) = gd(p) + pd(g) = gp'd(x) + pg'd(x) \in S$-span of $p'd(x)$ and $pd(x)$. On the other hand, $p'd(x) = d(p) \in \{d(i)\}$, and $pd(x) = d(px) - xd(p) \in S$-span of $\{d(i)\}$. Therefore, the S-span of $\{d(i)\}$ is the submodule of $S\,dx$ generated by $p'dx$ and pdx. Hence,

$$\Omega_{A/k} \cong S\,dx/S(p'\,dx, p\,dx) \cong S/(p, p').$$

□

Remark. The proof that $A \to B$ is unramified if and only if $\Omega_{B/A} = 0$ proceeds by reducing to the case where A is a field, then using direct limits to reduce to the case of finite type, then (more work in this step) reducing to the case where B is a simple field extension of A, which is the case we just completed.

Remark. If $A = k[x_1, \ldots, x_n]/(p_1, \ldots, p_r)$, then $\Omega_{A/k} \cong A^n / \operatorname{im} J$, where J is the Jacobian matrix

$$J_{n\times r} := \left(\frac{\partial P_j}{\partial x_i}\right)_{i,j}$$

Recall that we were trying to prove

Theorem 4.10 (Auslander, 1962)**.** *Let $S = k[x_1, \ldots, x_n]$, $G \subseteq \mathrm{GL}_n(k)$ such that $|G| \in k^\times$, and $R = S^G$. If $R \to S$ is unramified in codimension 1, then $\gamma : S\#G \to \mathrm{End}_R(S)$ is an isomorphism (here unramified in codimension 1 means unramified when localized at any height 1 prime of S):*

$$R_{q\cap R} \to S_q$$

is unramified at every height 1 $q \in \operatorname{Spec} S$. Equivalently, $(\Omega_{S/R})_q = 0$.

Proof. As a first step, we reduce to the case of dimension 1. Recall from an old Lemma that if A is a noetherian commutative ring and $M \xrightarrow{f} N$ is a A-homomorphism with M satisfying (S_2) and N satisfying (S_1), then f is an isomorphism if and only if f_p is an isomorphism for every height 1 $p \in \operatorname{Spec} A$. In our situation, $M = S\#G$ is free over S, hence (S_2). Then $N = \mathrm{End}_R(S)$ must also have depth 2 by an old lemma. So to show γ is an isomorphism to show γ_q is an isomorphism for every height 1 $q \in \operatorname{Spec} S$. So from now on we assume $R \to S$ is unramified.

As a second step, it is enough to show that γ is a split surjection. Both source and target are torsion-free S-modules and have ranks

$$\operatorname{rank}(S\#G) = \operatorname{rank}_R(\bigoplus_{g\in G} S) = \operatorname{rank}_R(S)|G| = |G|^2.$$

On other hand, $\operatorname{rank}_R(\mathrm{End}_R(S)) = \operatorname{rank}_R(\mathrm{Hom}_R(S,S)) = (\operatorname{rank}_R(S))^2 = |G|^2$. Any split surjection between them is an isomorphism. The remainder of the proof constructs a splitting as in this diagram

$$\begin{array}{ccc} S\#G & \xrightarrow{\quad\gamma\quad} & \mathrm{End}_R(S) \\ {\scriptstyle\tilde{\mu}}\uparrow & & \downarrow{\scriptstyle f\mapsto f\otimes\hat{\rho}} \\ S\otimes_R (S\#G) & \xleftarrow[\mathrm{ev}_\epsilon]{} & \mathrm{Hom}_S(S\otimes_R S, S\otimes_R (S\#G)) \end{array}$$

where going around the square yields the identity.

Step 3: Right map: We already know that $S \hookrightarrow S\#G$ by sending $s \in S$ to $s \cdot 1_G$. It also sits inside via a "Reynold's type" map $\hat{\rho} : S \to S\#G$ via $s \mapsto \frac{1}{|G|}\sum_{g\in G} g(s)\cdot g$. It is routine to check that $\hat{\rho}$ is an injective ring homomorphism, and $\hat{\rho}(1) = \frac{1}{|G|}\sum_{g\in G} g$ is an idempotent of

$S\#G$. The image of $\hat{\rho}$ is the set of fixed points $(S\#G)^G$ and $(\gamma \circ \hat{\rho})(1)$ is the Reynolds operator $\rho : S \to S$. Tensoring with $\hat{\rho}$ over R sends $f : S \to S$ to $f \otimes \hat{\rho} : S \otimes_R S \to S \otimes_R (S\#G)$.

Step 4: $\tilde{\mu}$. We use the assumption that $R \to S$ is unramified. Equivalently, the short exact sequence of $S \otimes_R S$-modules

$$0 \longrightarrow J \longrightarrow S \otimes_R S \xrightarrow{\mu} S \longrightarrow 0$$

splits. As S-modules, this is trivial. As R-modules, tensoring with S on the right by $S\#G$

$$0 \longrightarrow J \otimes_S (S\#G) \longrightarrow S \otimes_R S \otimes_S (S\#G) \xrightarrow{\tilde{\mu}} S \otimes_S (S\#G) \longrightarrow 0.$$

This is

$$0 \longrightarrow J \otimes_S (S\#G) \longrightarrow S \otimes_R (S\#G) \xrightarrow{\tilde{\mu}} S\#G \longrightarrow 0.$$

This stays exact since the other one was split. By the way, it is important to use the *left* S-module structure in this sequence (the left was 'used up'). The map $\tilde{\mu}$ is $t \otimes (s \cdot g) \mapsto ts \cdot g$.

Step 5: ϵ. We will construct a certain element $\epsilon \in S \otimes_R S$ and evaluate homomorphisms at ϵ.

Back to

$$0 \longrightarrow J \longrightarrow S \otimes_R S \xrightarrow{\mu} S \longrightarrow 0$$

Let $j : S \to S \otimes_R S$ be a splitting for μ, so j is $S \otimes_R S$-linear and $\mu \circ j = 1\, ids$. Set $\epsilon = j(1)$. Then of course, $\mu(\epsilon) = 1$. Furthermore, ϵ kills J, i.e. $\epsilon(s \otimes 1 - 1 \otimes s) = 0$ for every $s \in S$.

Step 6: A short computation: Write $\epsilon = \sum x_i \otimes y_i$ for $x_i, y_i \in S$. We claim that for any $g \in G$,

$$\sum x_i g(y_i) = \begin{cases} 1, & g = 1_G \\ 0, & \text{otherwise} \end{cases}$$

To see this, if $g = 1_G$, then the left hand side is $\sum x_i y_i = \mu(\epsilon) = 1$. Also for any $s \in S$,

$$(s \otimes 1)(\sum x_i \otimes y_i) = (\sum x_i \otimes y_i)(1 \otimes s)$$

Otherwise, if and only if $\sum sx_i \otimes y_i = \sum x_i \otimes sy_i$. Apply $1 \otimes g$ to both sides

$$\sum sx_i \otimes g(y_i) = \sum x_i \otimes g(s)g(y_i)$$

Collapse the $\otimes$ with μ

$$s \sum x_i g(y_i) = g(s) \sum x_i g(y_i)$$

If $g \neq 1$, then there is some s with $g(s) \neq s$. So $\sum x_i g(y_i) = 0$.

Step 7: A bigger computation: Start with $f \in \mathrm{End}_R(S)$.

$$\begin{aligned}
\gamma(\tilde{\mu}(\mathrm{ev}_\epsilon(f \otimes \hat{\rho})))(s) &= \gamma(\tilde{\mu}((f \otimes \hat{\rho})(\epsilon)))(s) \\
&= \gamma(\tilde{\mu}((f \otimes \hat{\rho})(\sum_i x_i \otimes y_i)))(s) \\
&= \gamma(\tilde{\mu}(\sum_i f(x_i) \otimes \hat{\rho}(y_i)))(s) \\
&= \gamma(\sum_i f(x_i)\hat{\rho}(y_i))(s) \\
&= \gamma(\sum_i f(x_i)(\frac{1}{|G|}\sum_{g\in G} g(y_i)g))(s) \\
&= \frac{1}{|G|}\sum f(x_i) \qquad \underbrace{\sum_{g\in G} g(y_i)g(s)}_{\text{fixed by every grp elmnt in } R \text{ is } R\text{-lin}} \\
&= \frac{1}{|G|} f\left(\sum_i \sum_g x_i g(y_i) g(s)\right) \\
&= \frac{1}{|G|} f\left(\sum_g \left(\sum_i x_i g(y_i)\right) g(s)\right) \\
&\overset{*}{=} \frac{1}{|G|} f\left(\left(\underbrace{\sum x_i y_i}_{=1}\right) s\right) \\
&= \frac{1}{|G|} f(s)
\end{aligned}$$

since only term which survives is where $g = 1$. Then the whole composition is multiplication by $1/|G|$. Rescale to get the identity so γ is a split surjection. □