What is a Representation?

Let G be a finite group of order n, and k an algebraically closed field. A *representation* of G consists of a pair $\langle \rho, V\rangle$, where V is a vector space over k, and $\rho : G \to \mathrm{GL}(V)$ is a group homomorphism.

Example 1. One can realize the dihedral group of order 8 as folows:

$$\begin{aligned} D_* &:= \langle r, s \mid r^4 = s^2 = 1, rsr = s\rangle \\ &\cong \mathbb{Z}/4 \rtimes \mathbb{Z}/2 \end{aligned}$$

and more importantly for our situation:

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

This defines a representation

$$\rho(r) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(s) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

where $V = \mathbb{C}^2$.

Linear Actions

A representation $\langle \rho, V\rangle$ for a finite group G induces a linear action of $G \curvearrowright V$ by defining:

$$g \cdot v = \rho(g)v$$

Remark 1. The action is linear because ρ is

$$\begin{aligned} g \cdot (v + \alpha w) &= \rho(v + \alpha w) \\ &= \rho(v) + \alpha\rho(w) \\ &= g \cdot v + \alpha(g \cdot w) \end{aligned}$$

for every $\alpha \in k$ and $v, w \in V$.

Group Rings

One can look at the group ring $k[G]$, where each element in $k[G]$ is a formal sum

$$x = \sum_{g \in G} \alpha_g \cdot g, \quad \alpha_g \in k.$$

Proposition 1. *Linear representations of V are $k[G]$-modules.*

Let G be a group acting on a vector space V by $g \cdot v$, for every $g \in G$. Define a group homomorphism:

$$\begin{aligned} G &\xrightarrow{\rho} \mathrm{GL}(V) \\ g &\longmapsto \varphi \end{aligned}$$

where

$$\begin{aligned} \varphi : V &\longrightarrow V \\ v &\longmapsto g \cdot v \end{aligned}$$

Hence, every group action on a vector space gives rise to a representation. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. We can define $g \cdot v = \rho(g)v$. Notice that:

(1) $1_G \cdot v = \mathrm{Id}_V \cdot v = v$
(2) $(gh) \cdot v = \rho(gh)v = \rho(g)\rho(h)v = g \cdot (\rho(h)v) = g \cdot (h \cdot v)$

and therefore every representation gives rise to an action of G on V. We form the group ring $\mathbb{C}[G]$ whose elements are formal sums:

$$\sum_{g \in G} \alpha_g \cdot g \quad \text{where } \alpha_g \in \mathbb{C}.$$

Proposition 2. *Linear representations of G are $\mathbb{C}[G]$-modules.*

Proof. Let $\langle V, \rho \rangle$ be a linear representation of G. Let $x \in \mathbb{C}[G]$ written as $x = \sum_{g \in G} \alpha_g \cdot g$. We have that

$$x \cdot v = \left(\sum_{g \in G} \alpha_g \cdot g \right) v = \sum_{g \in G} \alpha_g \, (g \cdot v)$$

and therefore V is a $\mathbb{C}[G]$-module.

Conversely, suppose that V is a $\mathbb{C}[G]$-module. Then there is an action of G on V that gives rise to a representation of G. $\square$

Invariants

Since we have an action of G on V, we also have an action of G on $\mathrm{Hom}_k(V, k)$. This action is given by

$$g \cdot f(v) = f(g^{-1} \cdot v).$$

In this way, we can get an action of G on $k[x_1, \ldots, x_n]$, for an n-dimensional representation V. One goal of invariant theory is to understand the subring

$$k[x_1, \ldots, x_n]^G = \{ f \in k[x_1, \ldots, x_n] \mid f(g \cdot v) = f(v) \quad \forall\, g \in G \}.$$

This subring is referred to as the *ring of invariants*.

Q: Is the ring of invariants $k[x_1, \ldots, x_n]^G$ finitely generated?

1. What is Invariant Theory?

The most encountered example of a ring of invariants is the symmetric polynomials $k[x_1, \ldots, x_n]^{S_n}$, where the action of S_n on $k[x_1, \ldots, x_n]$ is

$$\sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

The symmetric polynomials are

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n \\ &\vdots \\ s_n &= x_1 \cdots x_n. \end{aligned}$$

We notice that the permutation $(1\,2\,3)$ holds the following polynomial invariant

$$\begin{aligned} s_2 &= x_1 x_2 + x_1 x_3 + x_2 x_3 \\ (1\,2\,3) \cdot s_2 &= x_3 x_1 + x_3 x_2 + x_1 x_2. \end{aligned}$$

Example 2. Suppose the characteristic of k is not 2. Let $G = \mathbb{Z}/2$ and consider the representation of $\mathbb{Z}/2$ given by $\{I_2, -I_2\}$. Notice that a monomial $x^i y^j$ is invariant only when $i + j$ is even because the action of $-I_2$ on x and y yiled $-x$ and $-y$. We get the idea that

$$k[x, y]^{\mathbb{Z}/2} = k[x^2, xy, y^2].$$

Notice that this ring is not factorial because

$$(x^2)(y^2) = x^2 y^2 = (xy)^2.$$

Proposition 3. *If $\rho : G \to G$ is a faithful representation and there is no nontrivial linear character $\lambda : G \to k^*$, then $k[V]^G$ is a unique factorization domain.*

Remark 2. This proposition is applicable in a number of situations. Note that λ sends the commutator subgroup $[G, G]$ on 1 and $\mathrm{Ker}\, \lambda$ is a normal subgroup of G

(1) G is a simple nonabelian group such as A_5.
(2) G is a perfect group; $G = [G, G]$ such as $\mathrm{SL}_2(\mathbb{F}_5)$.

Example 3. Let $G = \mathbb{Z}/4$ and consider the representation

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

These are the rotational symmetries of the square. The ring of invariants is:

$$\mathbb{C}[x, y]^{\mathbb{Z}/4} = \{ f \in \mathbb{C}[x, y] \mid f(x, y) = f(-y, x) \}.$$

We would like to find a set of generators for the ring of invariants.

Theorem 1 (Molien's Theorem)**.** *The Hilbert series of the invariant ring* $\mathbb{C}[x_1, \ldots, x_n]^G$ *is*

$$\phi_G = \frac{1}{\#G} \sum_{g \in G} \frac{1}{\det(I - z\rho(g))}.$$

This is the average of the inverted characteristic polynomials of all the group elements.

g	$\det(I - g \cdot z)$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$(1-t)^2$
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	$t^2 + 1$
$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	$(1+t)^2$
$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$	$t^2 + 1$

Using the theorem we see that:

$$\begin{aligned} \phi_G(t) &= \frac{1}{(1-t)^2} + \frac{2}{t^2+1} + \frac{1}{(1+t)^2} \\ &= \frac{1+t^4}{(1-t^2)(1-t^4)} \end{aligned}$$

Proposition 4. *Every* $G \leq \mathrm{GL}(\mathbb{C})$ *of finite order has* n *algebraically independent invariants.*

In our example above, the ring of invariants $\mathbb{C}[x, y]^{\mathbb{Z}/4}$ has two algebraically independent invariants. The above series tells us we should be looking for invariants of degree 2 and degree 4

- $f_1 = x^2 + y^2$
- $f_2 = x^2 y^2$

These can be shown to be algebraically independent. Modulo some information in the next section and Chern classes:

$$\mathbb{C}[x, y]^{\mathbb{Z}/4} \cong \mathbb{C}[f_1, f_2] \oplus \mathbb{C}[f_1, f_2] f_3$$

and one can compute $f_3 = x^3 y - x y^3$.

Example 4. We recall that $D_8 = \mathbb{Z}/4 \rtimes \mathbb{Z}/2$. Let $\langle \rho, \mathbb{C}^2 \rangle$ be the representation defined by

$$\rho(r) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(s) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

The polynomials $x^2 + y^2$ and $x^2 y^2$ are invariant under this action. So we know that

$$\mathbb{C}[x^2 + y^2, x^2 y^2] \subseteq \mathbb{C}[x, y]^{D_8}.$$

Let

$$f(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_1 x y^{n-1} + a_0 y^n$$

be an invariant homogeneous polynomial of degree n. Since f is invariant under D_8 it is in particular invariant under s

$$s \cdot f(x,y) = f(x,y) = (-1)^n a_n x^n + (-1)^{n-1} x^{n-1} y + \cdots + (-1) a_1 x y^{n-1} + a_0 y^n.$$

We quickly see that f containss only even powers of x. Hence $f \in k[x^2, y]$. Further, r acts on y by $y \mapsto -x$. Hence, f cannot be soley dependent on x or y. Further, if the monomial $x^l y^k$ appears in f, then $x^k y^l$ appears in f also. Then

$$f(x,y) = a_n x^{2n} + a_{n-1} x^{2(n-1)} y^2 + \cdots + a_1 x^2 y^{2(n-1)} = a_0 y^{2n}.$$

One then does an analysis of the action of r on f to conclude that $P_{n,m} = x^{2n} y^{2m} + x^{2m} y^{2n} \in \mathbb{C}[x^2+y^2, x^2y^2]$ and finishes the proof by doing induction on $n - m$.

2. Gröbner Bases

We want to generalize three familiar algorithms:

(1) Euclidean Algorithm (single variable)
(2) Gaussian Elimination (linear polynomials)
(3) Elimination of Variables

Consider the polynomial ring $\mathbb{C}[x,y]$. We chose an ordering for the variables $x > y$. We get the *lexicographic* order

$$1 < y < y^2 < \cdots < x < xy < xy^2 < \cdots < x^2 < \cdots$$

of monomials.

Example 5 (Ideal Membership)**.** Let $I = \langle x^2 + y^2 + 1, x \rangle$. Does $x^2 y \in I$? Observation will tell you yes. However, if you attempt polynomial division it is possible to obtain a nonzero remainder.

A: Yes $x^2 y \in I$ because we were able to write it as a multiple of x. However, we see that the remainders need not be unique.

Fact: A zero remainder is sufficient but not necessary for $f \in I$.

Generating the Ring of Invariants

We want to find invariant polynomials $f_1, \ldots, f_m$ such that $k[x_1, \ldots, x_n]^G = k[f_1, \ldots, f_m]$.

Suppose that $R = \bigoplus_{d=0}^{\infty} R_d$ is a graded algebra over a field $k = R_0$. A set $f_1, \ldots, f_m$ of homogeneous elements is called a homogeneous system of parameters if

(1) The f_i are algebraically independent.
(2) $k[f_1, \ldots f_m] \hookrightarrow R$ is module-finite.

If $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]^G$ are a homogeneous system of parameters, then we say that the f_i are *primary invariants.* Since, $k[x_1, \ldots x_n]^G$ is finitely generated over $k[f_1, \ldots f_m]$ every $f \in k[x_1, \ldots, x_n]^G$ can be written

$$f = F_1 g_1 + \cdots + F_m g_s$$

where the g_i are all homogeneous in $k[x_1, \ldots, x_n]^G$. The g_i are said to be *secondary invariants.*

Example 6. Returning to our example for $\mathbb{Z}/4$:

$$\mathbb{C}[x,y]^{\mathbb{Z}/4} = \mathbb{C}[x^2+y^2, x^2y^2] \oplus f_3 \mathbb{C}[x^2+y^2, x^2y^2],$$

where $f_3 = x^3 y - x y^3$. The f_1 and f_2 are primary invariants and f_3 is a secondary invariant.

We would like to understand the algebraic relations between the primary and secondary invariants. For $f_1, f_2,$ and f_3 we have the algebraic relation $f_3^2 - f_2 f_1^2 - 4 f_2^2$. This relation can be found using Gröbner bases. It generates the syzygy ideal, and one has that

$$\mathbb{C}[x,y]^{\mathbb{Z}/4} \cong \frac{k[u,v,w]}{I_F}.$$