Classical Invariant Theory

Pre-REU Day 11

May 19, 2025

Introduction

So far, we have seen groups as "acting" on the plane $\mathbb{R}^2$, i.e., our groups were transformation subgroups of $\mathrm{Sym}(\mathbb{R}^2)$. Moreover, we focused our attention to groups preserving structure, e.g., by considering only the isometries. In this lecture, we will consider the action of matrix groups on *rings*. We will focus our attention on the so-called *classical groups* with their "classical representations" and look at the *invariant* rings.

§1. The classical matrix groups

By a classical group, we shall mean one of the following:

- (General linear group) The group $\mathrm{GL}_n(\mathbb{R})$ of invertible $n \times n$ matrices.
- (Special linear group) The group $\mathrm{SL}_n(\mathbb{R})$ of $n \times n$ matrices with determinant one.
- (Orthogonal group) The group $\mathrm{O}_n(\mathbb{R})$ of $n \times n$ matrices satisfying $MM^\mathsf{T} = I$.
- (Symplectic group) The group $\mathrm{Sp}_{2n}(\mathbb{R})$ of $2n \times 2n$ invertible matrices satisfying $M\Omega M^\mathsf{T} = \Omega$, where Ω is the $2n \times 2n$ block matrix given as $\Omega = \left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$.

The general linear group is the most general group of invertible matrices; each of the other can be thought of as preserving something:

- The special lienar group preserves the (n-dimensional) volume.
- As we saw in class, the orthogonal group is the group of matrices that preserves the usual dot product (and this was equivalent to preserving the lengths, thanks to the parallelogram law).
- The symplectic group arises as the group of matrices that preserves a certain other kind of product. Why is this product relevant? As per Wikipedia[1]: "[The symplectic group] comes up in classical physics as the symmetries of canonical coordinates preserving the Poisson [product]."

[1] https://en.wikipedia.org/wiki/Symplectic_group

§2. Action on rings

Now, let us consider the set $R = \mathbb{R}[x_1, \ldots, x_n]$—this is the set of all polynomials in the variables $x_1, \ldots, x_n$. Furthermore, the set R is equipped with the two natural binary operations of addition and multiplication that satisfy certain axioms such as commutativity, associativity, distributivity, and having the necessary identities and inverses—this makes R a *ring*.

Given an $n \times n$ matrix M, it defines a function on R. Let us consider this by means of an example: say $n = 2$, and we write $R = \mathbb{R}[x, y]$ and consider $M = \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right)$. First, we define the function on the variables x and y using matrix multiplication as following: we have

$$M \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 3y \\ y \end{bmatrix}.$$

So, $M(x) = x + 3y$ and $M(y) = y$. We now extend this to all polynomials by extending it "polynomially". For example, if we have the polynomial $f = 10 + 2x + 3xy - y^2$, then we define

$$\begin{aligned} M(f) &= M(10 + 2x + 3xy - y^2) \\ &= 10 + 2M(x) + 3M(x)M(y) - M(y)^2. \end{aligned}$$

We can now use the values of $M(x)$ and $M(y)$ from before to compute the above.

By defining the action in this way, we get that M acts on R via *ring homomorphisms*—the action of M preserves the addition and multiplication operations.

We could generalise the above further: say M in as $n \times n$ matrix, and R is a polynomial ring in nm variables for some $n, m \geqslant 1$. Then, we can again define an action of M on R by arranging the variables in an $n \times m$ matrix and proceeding as before.

Let us look at an example of this, say $R = \mathbb{R}[w, x, y, z]$ is a polynomial ring in four variables, and $M = \left(\begin{smallmatrix} 1 & 3 \\ 0 & 1 \end{smallmatrix}\right)$ as before. We then have

$$M \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} w + 3y & x + 3z \\ y & z \end{bmatrix}.$$

In particular, $M(y) = y$ and $M(z) = z$, giving us two *fixed points*. Are there any others?

A first source of fixed points is "any polynomial in y and z", e.g., y^2z because we have $M(y^2z) = M(y)^2M(z) = y^2z$.

Let us try to come up with fixed points not of this form. We have

$$\begin{aligned} M(wz) = M(w)M(z) = (w + 3y)z = wz + 3yz, \\ M(xy) = M(x)M(y) = (x + 3z)y = xy + 3zy. \end{aligned}$$

Can we get an invariant from the above two equations? Yes! We have

$$M(wz - xy) = M(wz) - M(xy) = (wz + 3yz) - (xy + 3zy) = wz - xy.$$

Thus, the determinant is a fixed point or an *invariant*. This is not surprising: the matrix M that we started out with, had determinant 1. Invariant theory is concerned with the study of the ring of invariants. Instead of studying the fixed points of one given function, we will instead consider a group of functions.

Definition 2.1. Let G be a group acting on a ring R. The ring of invariants is defined as

$$R^G \coloneqq \{r \in R : g(r) = r \text{ for all } g \in G\}.$$

As we will see in the problem set, R^G itself turns out to be a ring. The problems in invariant theory can be broadly described as:

(i) Finding a (preferably optimal) set of generators for R^G.

(ii) Finding what the "relations" between those generators are.

(iii) Finding what good properties of R are inherited by R^G.

Our results today will focus on the first, with some allusion to the other two.

§3. Classical invariant rings

We shall now see the invariants for the classical actions of the classical groups.

Theorem 3.1. Let $n, m \geqslant 1$ be integers, $R \coloneqq \mathbb{R}[X_{n\times m}]$ a polynomial ring in nm variables, and $G \coloneqq SL_n(\mathbb{R})$. Consider the action of G on R in the manner described earlier. The fixed subring is then given as

$$R^G = \mathbb{R}[\Delta : \Delta \text{ is an } n \times n \text{ minor of } X].$$

Let us parse the above with the help of an example:

Example 3.2. Let us consider $n = 2$ and $m = 2$. Let us denote our variables as

$$\begin{bmatrix} x_1 & x_2 \\ y_1 & y_2 \end{bmatrix}.$$

Then, there is exactly one 2×2 minor, namely $\Delta \coloneqq x_1y_2 - x_2y_1$. The theorem then reads:

$$R^G = \mathbb{R}[x_1y_2 - x_2y_1].$$

This means that any invariant can be written as a polynomial in the Δ. In this case, R^G is particularly nice—it is itself again (isomorphic to) a polynomial ring in one variable.

Example 3.3. Let us now consider $n = 2$ and $m = 4$. Let us denote our variables as

$$\begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{bmatrix}.$$

Now, there are exactly six minors: let $\Delta_{i,j} = x_i y_j - x_j y_i$ denote the determinant of the matrix obtained by considering the columns i and j.

Then, the theorem reads

$$R^G = \mathbb{R}[\Delta_{12}, \Delta_{13}, \Delta_{14}, \Delta_{23}, \Delta_{24}, \Delta_{34}].$$

This means that any invariant can be written as a polynomial in the Δ_{ij}s. However, there are *relations*, that is to say, some invariant possibly be written as a polynomial in the Δ_{ij}s in two different ways. One may verify that

$$\Delta_{12}\Delta_{34} + \Delta_{14}\Delta_{23} = \Delta_{13}\Delta_{24}.$$

In particular, R^G is *not* isomorphic to the polynomial ring in 6 variables.

Note that the inclusion $\mathbb{R}[\{\Delta\}] \subseteq \mathbb{R}^G$ is not too difficult: we saw that elements of $SL_2(\mathbb{R})$ will fix the determinant. The remarkable fact is that these determinants give us all the invariants.

The theme is repeated in the descriptions for the other invariant rings as well: the "obvious" invariants give us all.

Theorem 3.4. Consider the action of $G := O_n(\mathbb{R})$ on $R := \mathbb{R}[X_{n\times m}]$. The invariant ring is given as

$$R^G = \mathbb{R}[X^T X],$$

i.e., the generators are the entries of the matrix $X^T X$.

Once again, let us see a sketch of why the inclusion $\mathbb{R}[X^T X] \subseteq R^G$ is true: consider a matrix $M \in O_n(\mathbb{R})$. Then, we have

$$X^T X \overset{M}{\longmapsto} (MX)^T(MX) = X^T(M^T M)X = X^T X.$$

Example 3.5. Consider the case $n = 2$ and $m = 1$. If we call the variables x and y, then the theorem reads $R^G = \mathbb{R}[x^2 + y^2]$. This matches our geometric intuition of the orthogonal group preserving the norm.

More generally, if $n \geqslant 1$ is arbitrary and $m = 1$, we get the invariant ring as being generated by $x_1^2 + \cdots + x_n^2$.

In the problem set, we will see how in the general case, the entries of X^TX can be interpreted as dot products. Thus, we recover the familiar fact about $O_n(\mathbb{R})$ preserving the dot product.

Similarly, we get the same result for its symplectic cousin.

Theorem 3.6. Consider the action of $G := Sp_{2n}(\mathbb{R})$ on $R := \mathbb{R}[X_{2n\times m}]$. The invariant ring is given as

$$R^G = \mathbb{R}[X^T\Omega X],$$

i.e., the generators are the entries of the matrix $X^T\Omega X$.

For the group $GL_n(\mathbb{R})$, one typically considers a more complicated action. (In the problem set, we will see that for the usual left multiplication action, the ring of invariants is somewhat "boring".)

Theorem 3.7. Consider the action of the general linear group $G := GL_n(\mathbb{R})$ on the polynomial ring $R := \mathbb{R}[X_{m\times n}, Y_{n\times p}]$, where $M \in G$ acts as

$$M\colon \begin{cases} X \mapsto XM^{-1}, \\ Y \mapsto MY. \end{cases}$$

The invariant ring is given as

$$R^G = \mathbb{R}[XY],$$

i.e., the generators are the entries of the matrix XY.

Here's another interesting group action, though usually not under the umbrella of the classical group actions:

Theorem 3.8. Consider the group $G := GL_n(\mathbb{R})$ acting on $R := \mathbb{R}[X_{n\times n}]$ via conjugation, i.e., $M \in G$ acts via $X \mapsto M^{-1}XM$. Then, the invariant ring is given as

$$R^G = \mathbb{R}[\operatorname{trace}(X), \ldots, \det(X)],$$

i.e., the generators are the coefficients of the characteristic polynomial of X.

One question of interest to me is: what if we replace $\mathbb{R}$ with a finite field such as $\mathbb{Z}/5$? What are the rings of invariants in that case?