Computational methods in the study of symplectic quotients

Hans-Christian Herbig, UFRJ and Christopher Seaton, Rhodes College

Instituto de Matemática Aplicado, Universidade Federal do Rio de Janeiro

January 11–12th, 2016

Minicourse Abstract

Let G be a compact Lie group and let V be a unitary G-representation. Then there is a quadratic moment map $J : V \to \mathfrak{g}^*$ with respect to which V is a Hamiltonian manifold. Letting Z denote the zero fiber $J^{-1}(0)$ of the moment map, the corresponding *symplectic quotient* is given by $M_0 = Z/G$. It has the structure of a symplectic stratified space as well as a semialgebraic set, and it is equipped with an *algebra of regular functions* $\mathbb{R}[M_0]$, a Poisson subalgebra of its algebra of smooth functions.

In these lectures, we will introduce methods of computing the algebra $\mathbb{R}[M_0]$ of regular functions on such a symplectic quotient using methods from invariant theory and computational algebraic geometry. In addition, we will explain how these computations can be used to observe and verify properties of the symplectic quotient. Topics will include using Groebner bases to compute invariant polynomials, elimination theory, and methods of computing Hilbert series of Cohen-Macaulay algebras. In addition, we will introduce the software packages *Mathematica* and *Macaulay2* for these kinds of computations.

Minicourse Lectures

1. **Invariant theory and Gröbner bases**
2. Singular symplectic reduction and regular functions on symplectic quotients
3. The Hilbert series of the regular functions on a symplectic quotient
4. Elimination theory and the nonabelian case

Lecture 1: Invariant Theory and Groebner Bases

Affine varieties and ideals of polynomials

Affine Varieties

Let $\mathbb{K}$ denote either $\mathbb{R}$ or $\mathbb{C}$.

To fix notation:

- $\mathbb{K}^n$ is **affine space**, the vector space $\{(a_1, \ldots, a_n) : a_i \in \mathbb{K}\}$ under component-wise addition and $\mathbb{K}$-multiplication.
- A **monomial** in the variables $x_1, \ldots, x_n$ is an expression of the form $x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$ where each p_i is a nonnegative integer. The **degree** of $x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$ is $p_1 + \cdots + p_n$.
- $\mathbb{K}[x_1, \ldots, x_n]$ is the set of polynomials in $x_1, \ldots, x_n$ with coefficients in $\mathbb{K}$, i.e. finite linear combinations of monomials in $x_1, \ldots, x_n$.

We identify $\mathbb{K}[x_1, \ldots, x_n]$ with a subset of the continuous functions $\mathbb{K}^n \to \mathbb{K}$ in the obvious way.

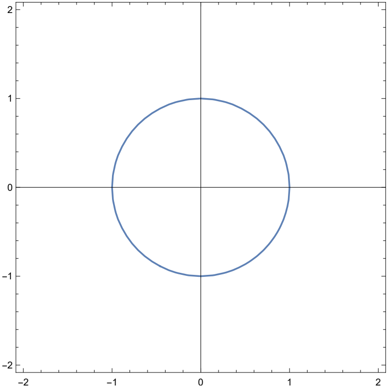
A subset V of $\mathbb{K}^n$ is an **affine variety** if there is a *finite* subset $\mathcal{F} \subset \mathbb{K}[x_1, \ldots, x_n]$ such that V can be described as

$$V = \mathcal{V}(\mathcal{F}) := \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f(a_1, \ldots, a_n) = 0 \ \ \forall f \in \mathcal{F}\}.$$

Affine Varieties: Examples

Example

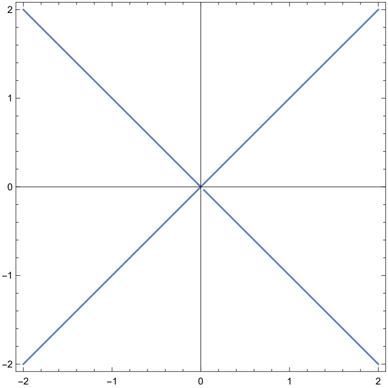
In $\mathbb{R}^2$, the unit circle is the vanishing set of $\mathcal{F} = \{x^2 + y^2 - 1\}$, hence an affine variety.



Affine Varieties: Examples

Example

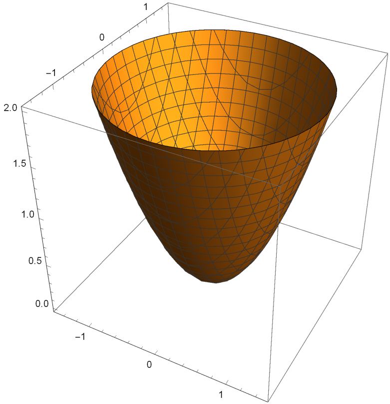
In $\mathbb{R}^2$, the variety corresponding to $\mathcal{F} = \{x^2 - y^2\}$ consists of the lines $y = x$ and $y = -x$.



Affine Varieties: Examples

Example

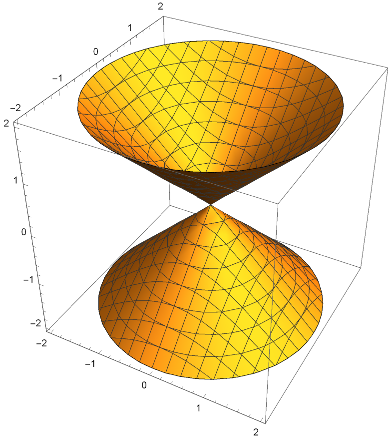
In $\mathbb{R}^3$, the variety corresponding to $\mathcal{F} = \{x^2 + y^2 - z\}$ is a paraboloid:



Affine Varieties: Examples

Example

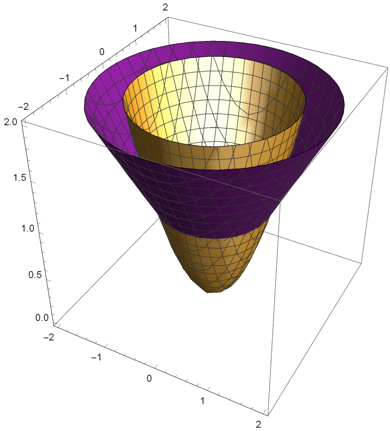
In $\mathbb{R}^3$, the variety corresponding to $\mathcal{F} = \{x^2 + y^2 - z^2\}$ is a cone:



Affine Varieties: Examples

Example

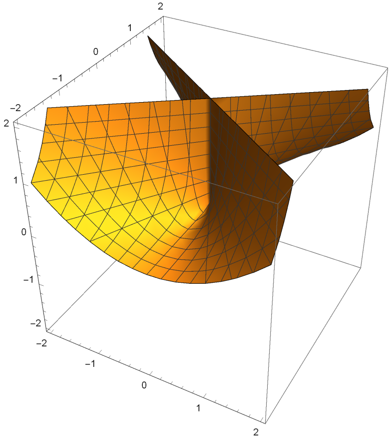
In $\mathbb{R}^3$, the variety corresponding to $\mathcal{F} = \{x^2 + y^2 - z^2, x^2 + y^2 - z\}$ the intersection of the cone and paraboloid:



Affine Varieties: Examples

Example

In $\mathbb{R}^3$, the *Whitney umbrella* is the variety of $\mathcal{F} = \{x^2 - y^2 z\}$:



Ideals: Motivation

Let $V = \mathcal{V}(\mathcal{F})$ be the variety of $\mathbb{K}^n$ described by the subset $\mathcal{F} \subset \mathbb{K}[x_1, \dots, x_n]$.

If $f \in \mathcal{F}$ and $g \in \mathbb{K}[x_1, \dots, x_n]$, then

$$(fg)(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in V.$$

For instance, in $\mathbb{R}[x, y]$, any polynomial of the form $(x^2 + y^2 - 1)g(x, y)$ must vanish on the unit circle.

Hence, the subset of $\mathbb{K}[x_1, \dots, x_n]$ that vanishes on V is much larger than $\mathcal{F}$.

Ideals

Definition

Let I be a subset of $\mathbb{K}[x_1, \ldots, x_n]$. Then I is an **ideal** if

- $0 \in I$,
- $\forall f_1, f_2 \in I$, $f_1 + f_2 \in I$, and
- $\forall f \in I, g \in \mathbb{K}[x_1, \ldots, x_n]$, $fg \in I$.

If $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$, the **ideal generated by** $f_1, \ldots, f_r$ is

$$\langle f_1, \ldots, f_r \rangle = \left\{ \sum_{i=1}^{r} h_i f_i : h_i \in \mathbb{K}[x_1, \ldots, x_n] \right\}.$$

It is the smallest ideal containing $f_1, \ldots, f_r$.

Exercise: Show that $\langle f_1, \ldots, f_r \rangle$ is in fact an ideal.

Ideals

Definition

Let S be any subset of $\mathbb{K}^n$. The **ideal of** S is

$$\mathcal{I}(S) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(c_1, \ldots, c_n) = 0 \quad \forall (c_1, \ldots, c_n) \in S\}.$$

i.e. the set of polynomials that vanish on S.

To see that $\mathcal{I}(S)$ is in fact an ideal, let S be an arbitrary subset of $\mathbb{K}^n$.

- 0 vanishes on all of $\mathbb{K}^n$ so $0 \in \mathcal{I}(S)$ is obvious.
- If $f_1, f_2 \in \mathcal{I}(S)$, then for each $(c_1, \ldots, c_n) \in S$, $f_1(c_1, \ldots, c_n) = f_2(c_1, \ldots, c_n) = 0$. Therefore $(f_1 + f_2)(c_1, \ldots, c_n) = 0 + 0 = 0$ and $f_1 + f_2 \in \mathcal{I}(S)$.
- If $f \in \mathcal{I}(S)$ and $g \in \mathbb{K}[x_1, \ldots, x_n]$, then for each $(c_1, \ldots, c_n) \in S$, $f(c_1, \ldots, c_n) = 0$. Therefore $(fg)(c_1, \ldots, c_n) = f(c_1, \ldots, c_n)g(c_1, \ldots, c_n) = 0 \cdot g(c_1, \ldots, c_n) = 0$ and $fg \in \mathcal{I}(S)$.

Ideals and Varieties

So we have:

$$\text{subsets of } \mathbb{K}^n \quad \xrightarrow{\mathcal{I}} \quad \text{ideals of } \mathbb{K}[x_1, \ldots, x_n]$$

and

$$\text{subsets of } \mathbb{K}[x_1, \ldots, x_n] \quad \xrightarrow{\mathcal{V}} \quad \text{varieties in } \mathbb{K}^n.$$

Lemma

If $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$, then

$$\langle f_1, \ldots, f_r \rangle \subseteq \mathcal{I}(\mathcal{V}(f_1, \ldots, f_r)).$$

Ideals and Varieties

Proof.

Given $\sum_{i=1}^{r} h_i f_i \in \langle f_1, \dots, f_r \rangle$, pick $(c_1, \dots, c_n) \in \mathcal{V}(f_1, \dots, f_r)$.
Then for each i, $f_i(c_1, \dots, c_n) = 0$ by definition. Hence

$$\begin{aligned}\left(\sum_{i=1}^{r} h_i f_i\right)(c_1, \dots, c_n) &= \sum_{i=1}^{r} h_i(c_1, \dots, c_n) f_i(c_1, \dots, c_n) \\ &= \sum_{i=1}^{r} h_i(c_1, \dots, c_n) \cdot 0 = 0.\end{aligned}$$

So $\sum_{i=1}^{r} h_i f_i \in \mathcal{I}(\mathcal{V}(f_1, \dots, f_r))$. $\square$

Ideals and Varieties

However, $\mathcal{I}(\mathcal{V}(f_1, \dots, f_r))$ is often larger than $\langle f_1, \dots, f_r \rangle$.

Example

In $\mathbb{R}[x]$, the ideal $I = \langle x^2 \rangle$ contains all polynomials with no constant or linear terms.

Then $\mathcal{V}(I) = \{0\}$.

However, $\mathcal{I}(\mathcal{V}(I))$ contains x.

Ideals and Varieties

Lemma

If $S \subseteq \mathbb{K}^n$, then

$$S \subseteq \mathcal{V}(\mathcal{I}(S)).$$

Exercise: Prove this lemma.

Again, equality need not hold.

Example

If $S = \mathbb{Q} \subset \mathbb{R}$, any function that vanishes on $\mathbb{Q}$ must vanish on $\mathbb{R}$ by continuity, so $\mathcal{I}(S) = \{0\}$ and $\mathcal{V}(\mathcal{I}(S)) = \mathbb{R}$.

Radical Ideals

Definition

($\mathbb{K} = \mathbb{C}$) The **radical** of an ideal I of $\mathbb{C}[x_1, \ldots, x_n]$ is

$$\sqrt{I} := \{f \in \mathbb{C}[x_1, \ldots, x_n] : f^m \in I \text{ for some } m > 0\}.$$

An ideal I of $\mathbb{C}[x_1, \ldots, x_n]$ is **radical** if $I = \sqrt{I}$, i.e. for any $f \in \mathbb{C}[x_1, \ldots, x_n]$, if $f^m \in I$ for a positive integer m, then $f \in I$.

($\mathbb{K} = \mathbb{R}$) The **real radical** of an ideal I of $\mathbb{R}[x_1, \ldots, x_n]$ is

$$\sqrt[\mathbb{R}]{I} := \{f \in \mathbb{R}[x_1, \ldots, x_n] : \exists g_1, \ldots, g_r \in \mathbb{R}[x_1, \ldots, x_n], \\ f^{2m} + g_1^2 + \cdots g_r^2 \in I \text{ for some } m > 0\}$$

An ideal I of $\mathbb{R}[x_1, \ldots, x_n]$ is **real** if $I = \sqrt[\mathbb{R}]{I}$, i.e. for any $f_1, \ldots, f_r \in \mathbb{R}[x_1, \ldots, x_n]$, $f_1^2 + \cdots + f_r^2 \in I$ for a positive integer m implies $f_1, \ldots, f_r \in I$.

Correspondence between Ideals and Varieties

Theorem (Hilbert's Nullstellensatz)

If I is an ideal of $\mathbb{C}[x_1, \dots, x_n]$, then $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.

Hence, there is a bijection between affine varieties in $\mathbb{C}^n$ and **radical** *ideals in $\mathbb{C}[x_1, \dots, x_n]$.*

If I is an ideal of $\mathbb{R}[x_1, \dots, x_n]$, then $\mathcal{I}(\mathcal{V}(I)) = \sqrt[\mathbb{R}]{I}$.

Hence, there is a bijection between affine varieties in $\mathbb{R}^n$ and **real** *ideals in $\mathbb{C}[x_1, \dots, x_n]$.*

Proofs can be found in Cox–Little–O'Shea [2] (over $\mathbb{C}$) and Bochnak–Coste–Roy [1] (over $\mathbb{R}$).
In the correspondence, the ideals of $\mathbb{K}[x_1, \dots, x_n]$ that are **maximal** (contained in no larger ideal except $\mathbb{K}[x_1, \dots, x_n]$ itself) correspond to points in the variety.

The Polynomial Functions on a Variety

If I is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, define the equivalence class $\equiv \mod I$ on $\mathbb{K}[x_1, \ldots, x_n]$ by

$$g_1 \equiv g_2 \mod I \qquad \text{iff} \qquad g_1 - g_2 \in f.$$

The equivalence class of g is denotes $g + I$.
The **quotient algebra** $\mathbb{K}[x_1, \ldots, x_n]/I$ is defined to be the set of equivalence classes in $\mathbb{K}[x_1, \ldots, x_n]$.
It can be shown that the operations

$$(g_1 + I) + (g_2 + I) := (g_1 + g_2) + I \quad \text{and} \quad (g_1 + I)(g_2 + I) := (g_1 g_2) + I$$

are well defined on $\mathbb{K}[x_1, \ldots, x_n]/I$.
If $I = \mathcal{I}(V)$ is the ideal of a variety V, then $\mathbb{K}[x_1, \ldots, x_n]/I$ is thought of as the polynomial functions on V.
Two elements of $\mathbb{K}[x_1, \ldots, x_n]$ represent the same element of $\mathbb{K}[x_1, \ldots, x_n]/I$ if and only if they have the same value at every point in V.

Invariant polynomials

Invariant Polynomials

Let $\mathrm{GL}_n(\mathbb{K})$ denote the group of invertible $n \times n$ matrices with entries in $\mathbb{K}$.

Definition

A subset $G \subseteq \mathrm{GL}_n(\mathbb{K})$ is a **subgroup**, written $G \leq \mathrm{GL}_n(\mathbb{K})$, if

- The identity $\mathrm{Id} \in G$,
- If $A, B \in G$, then the matrix product $AB \in G$, and
- If $A \in G$, then $A^{-1} \in G$.

If, $G \leq \mathrm{GL}_n(\mathbb{K})$ and $f \in \mathbb{K}[x_1, \ldots, x_n]$, then f is G-**invariant** if $f \circ A = f$ for each $A \in G$.

The collection of all G-invariant polynomials is denoted $\mathbb{K}[x_1, \ldots, x_n]^G$.

Invariant Polynomials: Basic Examples

Let $G = \{1, -1\} \subset \mathsf{GL}_1(\mathbb{R})$.

For $f \in \mathbb{R}[x]$, it is easy to see that $f(x) = f(-x)$ if and only if $f(x)$ is even, i.e. $f(x) = g(x^2)$ for some $g \in \mathbb{R}[w]$.

Hence,

$$\mathbb{R}[x]^G = \{g(x^2) : g \in \mathbb{R}[w]\}.$$

Invariant Polynomials: Basic Examples

Let $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and let $G = \{\mathrm{Id}, A\} \subset \mathrm{GL}_2(\mathbb{C})$.

For $f \in \mathbb{C}[x, y]$, we have $(f \circ A)(x, y) = f(y, x)$.

Exercise: For $f \in \mathbb{C}[x, y]$, $f \circ A = f$ if and only if $f(x, y) = g(x + y, xy)$ for some $g \in \mathbb{C}[w_1, w_2]$.

Hint: If h is a monomial of degree d, then $g \circ A$ is a monomial of degree d. So f is G-invariant if and only if it is the sum of **homogeneous** G-invariant polynomials (i.e. all terms have the same degree).

Hence,

$$\mathbb{C}[x, y]^G = \{g(x + y, xy) : g \in \mathbb{C}[w_1, w_2]\}.$$

Elements of $\mathbb{C}[x, y]^G$ are called **symmetric polynomials in two variables**.

Hilbert Bases

The set $\mathbb{K}[x_1, \ldots, x_n]^G$ is closed under addition, multiplication, and scalar multiplication of polynomials, and hence is a **subalgebra** or **subring** of $\mathbb{K}[x_1, \ldots, x_n]$.

This is easy to see, e.g. $(f+g) \circ A = (f \circ A) + (g \circ A)$ so that $(f \circ A) = f$ and $(g \circ A) = g$ implies $(f+g) \circ A = f + g$.

Note that $\mathbb{K}[x_1, \ldots, x_n]^G$ is **not** an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

We refer to $\{g(x^2) : g \in \mathbb{C}[w]\}$ as the **subalgebra generated by** x^2, written $\mathbb{C}[x^2]$.

Similarly, $\{g(x+y, xy) : g \in \mathbb{C}[w_1, w_2]\} = \mathbb{C}[x+y, xy]$ is the **subalgebra generated by** $\{x+y, xy\}$.

In general, the **subalgebra generated by** $f_1, \ldots, f_r \in \mathbb{K}[x_1, \ldots, x_n]$ is $\{g(f_1, \ldots, f_r) : g \in \mathbb{K}[w_1, \ldots, w_r]\}$. We refer to $\{f_1, \ldots, f_r\}$ as a **Hilbert basis** for the subalgebra.

Hilbert basis (even minimal Hilbert bases) are often not unique.

Invariant Polynomials: Another Example

Let $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, and let $G = \{\mathrm{Id}, B\} \subset \mathrm{GL}_2(\mathbb{R})$.

For $f \in \mathbb{R}[x, y]$, we have $(f \circ B)(x, y) = f(-x, -y)$. Hence, each monomial of degree d is multiplied by $(-1)^d$.

For $f \in \mathbb{R}[x, y]$, $f \circ B = f$ if and only if $f(x, y) = g(x^2, y^2, xy)$ for some $g \in \mathbb{R}[w_1, w_2, w_3]$.

Hence, $\{x^2, y^2, xy\}$ is a Hilbert basis for $\mathbb{R}[x, y]^G$, i.e.

$$\mathbb{R}[x, y]^G = \mathbb{R}[x^2, y^2, xy].$$

In this example, however, the elements of the Hilbert basis satisfy a relation:

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

Algebraic Dependence

Definition

We say that a finite set $\{f_1, \ldots, f_r\} \subset \mathbb{K}[x_1, \ldots, x_n]$ is **algebraically independent** if $g(f_1, \ldots, f_r) = 0$ implies $g = 0$.

If there is a nonzero $g \in \mathbb{K}[w_1, \ldots, w_r]$ such that $g(f_1, \ldots, f_r) = 0$, then $\{f_1, \ldots, f_r\}$ is **algebraically dependent**.

If a subalgebra has an algebraically independent Hilbert basis $\{f_1, \ldots, f_r\}$, then the subalgebra has the same properties as $\mathbb{K}[w_1, \ldots, w_r]$.

We can think of it as "the same as" polynomial functions on $\mathbb{K}^r$.

Algebraic Dependence

If $\{f_1, \ldots, f_r\}$ is algebraically dependent, define

$$\mathcal{R}(f_1, \ldots, f_r) = \{g \in \mathbb{K}[w_1, \ldots, w_r] : g(f_1, \ldots, f_r) = 0\}.$$

Then $\mathcal{R}(f_1, \ldots, f_r)$ is an ideal, the **ideal of relations** of $\{f_1, \ldots, f_r\}$.
It is easy to see that $\mathcal{R}(f_1, \ldots, f_r)$ is an ideal:

- Obviously, $0 \in \mathcal{R}(f_1, \ldots, f_r)$.
- If $g_1, g_2 \in \mathcal{R}(f_1, \ldots, f_r)$, then $g_1(f_1, \ldots, f_r) = g_2(f_1, \ldots, f_r) = 0$, so $(g_1 + g_2)(f_1, \ldots, f_r) = 0 + 0 = 0$ and $(g_1 + g_2) \in \mathcal{R}(f_1, \ldots, f_r)$.
- If $g \in \mathcal{R}(f_1, \ldots, f_r)$ and $h \in \mathbb{K}[w_1, \ldots, w_r]$, then

  $$(gh)(f_1, \ldots, f_r) = g(f_1, \ldots, f_r)h(f_1, \ldots, f_r) = 0 \cdot h(f_1, \ldots, f_r) = 0,$$

  and $gh \in \mathcal{R}(f_1, \ldots, f_r)$.

If a subalgebra has an algebraically dependent Hilbert basis $\{f_1, \ldots, f_r\}$, then the subalgebra is "the same as" the polynomial functions on the variety $\mathcal{V}(\mathcal{R}(f_1, \ldots, f_r))$.

Invariant Polynomials: Example Revisited

For $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ and $G = \{\mathrm{Id}, B\} \subset \mathrm{GL}_2(\mathbb{R})$,

$$\mathbb{R}[x, y]^G = \mathbb{R}[x^2, y^2, xy].$$

The Hilbert basis $\{x^2, y^2, xy\}$ is algebraically dependent, with relation

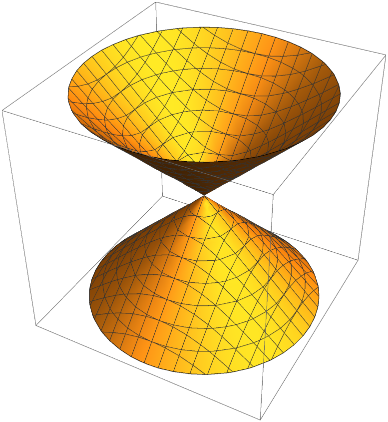
$$(x^2)(y^2) = (xy)^2, \quad \text{i.e.} \quad w_1 w_2 - w_3^2 = 0.$$

The ideal of relations is $\mathcal{R}(x^2, y^2, xy) = \langle w_1 w_2 - w_3^2 \rangle$.

Hence, $\mathbb{R}[x, y]^G$ is the "same as" the polynomial functions on the affine variety in $\mathbb{R}^3$ defined by $w_1 w_2 - w_3^2$.

Invariant Polynomials: Example Revisited

The affine variety in $\mathbb{R}^3$ defined by $w_1 w_2 - w_3^2$:



Invariant Polynomials: Some Facts

- For an arbitrary subgroup $G \leq \mathrm{GL}_n(\mathbb{K})$, $\mathbb{K}[x_1, \ldots, x_n]^G$ might not have a Hilbert basis.
  For *many* subgroups (**reductive subgroups**) it does.
- If G is a *closed* subgroup of $\mathrm{GL}_n(\mathbb{K})$ then it is an example of a **Lie group**. Compact (bounded) Lie groups are always reductive by a theorem of Hilbert and Weyl.
- If $\{f_1, \ldots, f_r\}$ is a Hilbert basis for $\mathbb{K}[x_1, \ldots, x_n]^G$, the variety $\mathcal{V}(\mathcal{R}(f_1, \ldots, f_r))$ plays the role of the *quotient* of $\mathbb{K}^n$ by G, and is written $\mathbb{K}^n/\!\!/G$. It is called the **affine GIT quotient**.
- When $\mathbb{K} = \mathbb{C}$, there is a bijection between the *closed G-orbits* in $\mathbb{C}^n$ and $\mathbb{C}^n/\!\!/G$.
- When $\mathbb{K} = \mathbb{R}$, there is a bijection between the *closed G-orbits* in $\mathbb{K}^n$ and a *subset* of $\mathbb{R}^n/\!\!/G$.
- When G is a compact Lie group, all orbits are closed.

An Example with Non-Closed Orbits

Let $G = \mathrm{GL}_1(\mathbb{C})$. This is the group of nonzero complex numbers, denoted $\mathbb{C}^\times$.

For $f \in \mathbb{C}[x]$, it is easy to see that $f(x) = f(zx)\ \forall z \in \mathbb{C}^\times$ if and only if $f(x) = c$ for some $c \in \mathbb{C}$. That is,

$$\mathbb{C}[x]^{\mathbb{C}^\times} = \mathbb{C}.$$

Hence, $\mathbb{C}[x]^{\mathbb{C}^\times}$ is the polynomial functions on a point (no variables).

In terms of this action, $\mathbb{C}$ has two orbits: $\{0\}$ and all other points.

The variety of $\mathbb{C}[x]^{\mathbb{C}^\times}$, a single point, corresponds to the closed orbit $\{0\}$.

Gröbner Bases

Ideal Membership

Ideal Membership Problem: Given an ideal

$$I = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{K}[x_1, \dots, x_n]$$

and a polynomial $g \in \mathbb{K}[x_1, \dots, x_n]$, decide whether $g \in \langle f_1 \dots, f_r \rangle$.

If $n = r = 1$, then we can use polynomial division to find the answer.

Example

In $\mathbb{R}[x]$, the polynomial $x^5 - 3x^2 + 2$ is not an element of $\langle x^2 + 1 \rangle$.

This can be seen by dividing $x^5 - 3x^2 + 2$ by $x^2 + 1$ and seeing that the remainder is $x + 5$.

Ideal Membership

Example

In $\mathbb{R}[x]$, the polynomial $x^5 - 3x^2 - x - 3$ is an element of $\langle x^2 + 1 \rangle$.

Dividing $x^5 - 3x^2 - x - 3$ by $x^2 + 1$, we see that

$$x^5 - 3x^2 - x - 3 = (x^3 - x - 3)(x^2 + 1) \in \langle x^2 + 1 \rangle.$$

In fact, it can be shown that when $n = 1$ (one variable), every ideal is of the form $\langle f \rangle$, so $r = 1$ in every case.

Ideal Membership

Ideal Membership Problem: Given an ideal

$$I = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{K}[x_1, \dots, x_n]$$

and a polynomial $g \in \mathbb{K}[x_1, \dots, x_n]$, decide whether $g \in \langle f_1 \dots, f_r \rangle$.

A natural idea to try is to divide g by f_1, then the remainder by f_2, then the remainder by f_3, etc. to try to express g in the form $\sum_{i=1}^{r} h_i f_i$ for some $h_i \in \mathbb{K}[x_1, \dots, x_n]$.

But polynomial division depends on how you order the terms of g, and if we fix this, the answer depends on the order of $f_1, \dots, f_r$, etc.

Monomial Orders

Definition

A **monomial order** on $\mathbb{K}[x_1, \ldots, x_n]$ is a linear order on the set of monomials such that

- $1 \preceq m$ for each monomial m, and
- $m_1 \prec m_2$ implies $m_1 m_3 \prec m_2 m_3$ for monomials m_1, m_2, m_3.

Example

In $\mathbb{K}[x]$, the only monomial order is $1 \prec x \prec x^2 \prec x^3 \prec \cdots$.

With more than one variable, it is typical to assume that $x_1 \succ x_2 \succ \cdots$.

Example

Lexicographic order: $m_1 = x_1^{p_1} \cdots x_n^{p_n} \prec m_2 = x_1^{q_1} \cdots x_n^{q_n}$ if the first nonzero entry of $p_1 - q_1, p_2 - q_2, \ldots, p_n - q_n$ is negative.

Monomial Orders

Example

Degree lexicographic order: $m_1 = x_1^{p_1} \cdots x_n^{p_n} \prec m_2 = x_1^{q_1} \cdots x_n^{q_n}$ if $\deg m_1 < \deg m_2$ or $\deg m_1 = \deg m_2$ and the first nonzero entry of $p_1 - q_1, p_2 - q_2, \ldots, p_n - q_n$ is negative.

Example

Degree reverse lexicographic order: $m_1 = x_1^{p_1} \cdots x_n^{p_n} \prec m_2 = x_1^{q_1} \cdots x_n^{q_n}$ if $\deg m_1 < \deg m_2$ or $\deg m_1 = \deg m_2$ and the last nonzero entry of $p_1 - q_1, p_2 - q_2, \ldots, p_n - q_n$ is positive.

Gröbner Bases

Definition

Given a monomial order $\prec$ on $\mathbb{K}[x_1, \ldots, x_n]$, let $f \in \mathbb{K}[x_1, \ldots, x_n]$, and let I be an ideal of $\mathbb{K}[x_1, \ldots, x_n]$.

- The **initial monomial** $\operatorname{init}(f)$ of f is the largest monomial in f with respect to $\prec$.
- The **initial ideal** of the ideal I is the ideal generated by the initial monomials of the elements of I.
- A finite set $\{g_1, \ldots, g_s\}$ of I is a **Gröbner basis for** I if $\{\operatorname{init}(g_1), \ldots, \operatorname{init}(g_s)\}$ generates the initial ideal of I.
- A Gröbner basis $\{g_1, \ldots, g_s\}$ for I is **reduced** if, for $i \neq j$, $\operatorname{init}(g_i)$ does not divide any monomial in g_j.

Properties of Gröbner Bases

Gröbner bases have properties that can be used to solve problems like the Ideal Membership Problem.

There is a division algorithm that allows one to divide a polynomial g by a Gröbner basis for an ideal I, yielding a unique remainder.
(The remainder is zero if and only if $g \in I$).

Gröbner bases generalize the Euclidean algorithm for polynomials to the multivariable case, and Gaussian elimination to polynomials of degree larger than 1.

Buchberger's algorithm is an algorithm for computing a Gröbner basis for an ideal of $\mathbb{K}[x_1, \ldots, x_n]$, and is implemented on many computer algebra systems.

More information can be found in Cox–Little–O'Shea [2].

Computing Gröbner bases on *Mathematica*

To compute the Gröbner basis of the ideal $I = \langle f_1, \dots, f_r \rangle$ in $\mathbb{K}[x_1, \dots, x_n]$ on *Mathematica*, the command is

```
GroebnerBasis[{f1,f2,...,fr}, {x1,x2,...,xr}]
```

The monomial order is lexicographic (and based on the order in which the variables are listed).

```
GroebnerBasis[{f1,f2,...,fr}, {x1,x2,...,xr},
  MonomialOrder->DegreeReverseLexicographic]
```

changes the monomial order.

```
GroebnerBasis[{f1,f2,...,fr}, {x1,x2,...,xr},
  {x1,x2}
```

eliminates x_1 and x_2 in the Gröbner basis (i.e. removes any elements involving these variables).

Representations of Tori

Compact Tori

Let $\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$, considered with the operation of multiplication.

This is the unit circle in the complex plane, and it is closed under multiplication and inversion.

We define the ℓ-**dimensional (compact) torus** to be

$$\mathbb{T}^\ell := (\mathbb{S}^1)^\ell$$

with the operation

$$(t_1, \ldots, t_\ell) \cdot (t_1', \ldots, t_\ell') = (t_1 t_1', \ldots, t_\ell t_\ell').$$

Compact Tori as Subgroups of $\mathrm{GL}_n(\mathbb{C})$

There are many subgroups of $\mathrm{GL}_n(\mathbb{C})$ that can be identified with $\mathbb{T}^\ell$.

- $\mathbb{T}^1 = \mathbb{S}^1$ is a subgroup of $\mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$.
- We can identify $\mathbb{T}^1$ with

$$\left\{ \begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix} : t \in \mathbb{T}^1 \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

- We can also identify $\mathbb{T}^1$ with

$$\left\{ \begin{pmatrix} t^{-1} & 0 \\ 0 & t^2 \end{pmatrix} : t \in \mathbb{T}^1 \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

- We can identify $\mathbb{T}^2$ with

$$\left\{ \begin{pmatrix} t_1 & 0 \\ 0 & t_1^{-1} t_2 \end{pmatrix} : (t_1, t_2) \in \mathbb{T}^2 \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

Compact Tori as Subgroups of $\mathrm{GL}_n(\mathbb{C})$

A **weight matrix** A is an $\ell \times n$ matrix with integer entries.

It describes a specific subgroup of $\mathrm{GL}_n(\mathbb{C})$ that can be identified with the torus $\mathbb{T}^r$ where r is the rank of A (which we usually assume is ℓ).

The subgroup is given by diagonal matrices with diagonal entries

$$(t_1^{a_{1,1}} t_2^{a_{2,1}} \cdots t_\ell^{a_{\ell,1}}, t_1^{a_{1,2}} t_2^{a_{2,2}} \cdots t_\ell^{a_{\ell,2}}, \ldots, t_1^{a_{1,n}} t_2^{a_{2,n}} \cdots t_\ell^{a_{\ell,n}})$$

where $(t_1, \ldots, t_\ell) \in \mathbb{T}^\ell$.

Note that Gaussian elimination (over $\mathbb{Z}$) and permuting columns of the weight matrix doesn't really change the subgroup, just expresses it using different coordinates.

Up to equivalence, every subgroup of $\mathrm{GL}_n(\mathbb{C})$ that can be identified with $\mathbb{T}^\ell$ can be expressed by a weight matrix.

Compact Tori as Subgroups of $\mathrm{GL}_n(\mathbb{C})$, Examples

- The weight matrix (1) describes $\mathbb{T}^1$ as it is defined in $\mathrm{GL}_1(\mathbb{C})$, i.e. matrices (t) with $|t| = 1$.
- The weight matrix $(-2, 3)$ describes $\mathbb{T}^1$ as the subgroup

$$\left\{ \begin{pmatrix} t^{-2} & 0 \\ 0 & t^3 \end{pmatrix} : t \in \mathbb{T}^1 \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

- The weight matrix $\begin{pmatrix} -2 & 3 \\ 0 & 4 \end{pmatrix}$ describes $\mathbb{T}^2$ as the subgroup

$$\left\{ \begin{pmatrix} t_1^{-2} & 0 \\ 0 & t_1^3 t_2^4 \end{pmatrix} : (t_1, t_2) \in \mathbb{T}^2 \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

Invariants of Compact Tori

Let A be an $\ell \times n$ weight matrix and G the corresponding subgroup of $\mathrm{GL}_n(\mathbb{C})$.

A polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$ is G-invariant if and only if each of its monomial terms is invariant.

The monomial $x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$ is invariant if and only if

$$A \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} = 0.$$

Invariants of Compact Tori, Examples

For $A = \begin{pmatrix} -1 & 1 & 1 \end{pmatrix}$, the monomial $f(x_1, x_2) = x_1^2 x_2 x_3$ is invariant, as, for any $t_1 \in \mathbb{T}^1$,

$$\begin{aligned} f(t_1^{-1}x_1, t_1x_2, t_1x_3) &= (t_1^{-1}x_1)^2(t_1x_2)(t_1x_3) \\ &= x_1^2x_2x_3 \\ &= f(x_1, x_2, x_3). \end{aligned}$$

The monomial $f(x_1, x_2) = x_2x_3$ is not invariant, as

$$\begin{aligned} f(t_1^{-1}x_1, t_1x_2, t_1x_3) &= (t_1x_2)(t_1x_3) \\ &= t_1^2x_2x_3 \\ &\neq f(x_1, x_2, x_3) \end{aligned}$$

unless $t_1 = 1$.

Invariants of Compact Tori, Examples

$A = \begin{pmatrix} -1 & 1 & 1 \end{pmatrix}$

A Hilbert basis for $\mathbb{C}[x_1, x_2, x_3]^G$ is given by

$$\{x_1x_2, \quad x_1x_3\},$$

i.e.

$$\mathbb{C}[x_1, x_2, x_3]^G = \mathbb{C}[x_1x_2, x_1x_3].$$

Invariants of Compact Tori, Examples

For $A = \begin{pmatrix} -2 & 0 & 1 \\ -3 & 1 & 0 \end{pmatrix}$, the monomial $f(x_1, x_2, x_3) = x_1 x_2^3 x_3^2$ is invariant, as, for any $(t_1, t_2, t_3) \in \mathbb{T}^2$,

$$\begin{aligned} f(t_1^{-2} t_2^{-3} x_1, t_2 x_2, t_1 x_3) &= (t_1^{-2} t_2^{-3} x_1)(t_2 x_2)^3 (t_1 x_3)^2 \\ &= x_1 x_2^3 x_3^2 \\ &= f(x_1, x_2, x_3). \end{aligned}$$

A Hilbert basis for $\mathbb{C}[x_1, x_2, x_3]^G$ is given by

$$\{x_1 x_2^3 x_3^2\}.$$

Compact Vs. Algebraic Tori

The ℓ-**dimensional algebraic torus** is $(\mathbb{C}^\times)^\ell$ with the same operation as the compact torus.

A weight matrix A can also be used to describe a subgroup of $\mathrm{GL}_n(\mathbb{C})$ that can be identified with $(\mathbb{C}^\times)^\ell$ (just remove the requirement that $|t_i| = 1$).

- The weight matrix (1) describes $\mathbb{C}^\times$ as it is defined, i.e. matrices (t) with $t \neq 0$.
- The weight matrix $(-2, 3)$ describes $\mathbb{C}^\times$ as the subgroup

$$\left\{ \begin{pmatrix} t^{-2} & 0 \\ 0 & t^3 \end{pmatrix} : t \in \mathbb{C}^\times \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

- The weight matrix $\begin{pmatrix} -2 & 3 \\ 0 & 4 \end{pmatrix}$ describes $(\mathbb{C}^\times)^2$ as the subgroup

$$\left\{ \begin{pmatrix} t_1^{-2} & 0 \\ 0 & t_1^3 t_2^4 \end{pmatrix} : (t_1, t_2) \in (\mathbb{C}^\times)^2 \right\} \subset \mathrm{GL}_2(\mathbb{C}).$$

Compact Vs. Algebraic Tori

- Let A be an $\ell \times n$ weight matrix.
- Let G denote the corresponding subgroup of $\mathrm{GL}_n(\mathbb{C})$ identified with $\mathbb{T}^\ell$.
- Let $G_\mathbb{C}$ denote the corresponding subgroup of $\mathrm{GL}_n(\mathbb{C})$ identified with $(\mathbb{C}^\times)^\ell$.

The subgroup $G_\mathbb{C}$ is a kind of algebraic completion of G called the **Zariski closure**.

We say that $G_\mathbb{C}$ is the **complexification** of the Lie group G, as G is a maximal compact (closed and bounded) subgroup of $G_\mathbb{C}$.

It is not hard to show (using the descriptions of the matrices) that a monomial in $\mathbb{C}[x_1, \dots, x_n]$ is G-invariant if and only if it is $G_\mathbb{C}$-invariant. Hence,

$$\mathbb{C}[x_1, \dots, x_n]^G = \mathbb{C}[x_1, \dots, x_n]^{G_\mathbb{C}}.$$

Compact Tori as Subgroups of $\mathrm{GL}_n(\mathbb{R})$

We can also realize $\mathbb{T}^\ell$ as a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

For instance, $\mathbb{S}^1$ can be identified with the group of rotations of the plane:

$$\left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\} \subset \mathrm{GL}_2(\mathbb{R}).$$

However, this is the same as $\mathbb{S}^1 \leq \mathrm{GL}_1(\mathbb{C})$, identifying $(x, y) \in \mathbb{R}^2$ with $x + iy \in \mathbb{C}$.

In general, any subgroup of $\mathrm{GL}_n(\mathbb{R})$ that is a torus arises from a subgroup of $\mathrm{GL}_m(\mathbb{C})$ for some $m \leq n/2$.

Real Invariants of Compact Tori

If A is an $\ell \times n$ weight matrix describing a subgroup of $\mathrm{GL}_n(\mathbb{C})$, and hence a subgroup G of $\mathrm{GL}_{2n}(\mathbb{R})$, we can describe the point

$$(z_1, \dots, z_n) \in \mathbb{C}^n$$

with coordinates

$$(x_1, \dots, x_n,\ y_1, \dots, y_n) \in \mathbb{R}^2$$

as above, $z_j = x_j + iy_j$, or we can use

$$(z_1, \dots, z_n,\ \overline{z_1}, \dots, \overline{z_n}),$$

where $\overline{z_j} = x_j - iy_j$.

The group operation in real coordinates is much easier to describe using these coordinates.

Real Invariants of Compact Tori

If A is an $\ell \times n$ weight matrix describing a subgroup of $\mathrm{GL}_n(\mathbb{C})$, and hence a subgroup G of $\mathrm{GL}_{2n}(\mathbb{R})$, a Hilbert basis for

$$\mathbb{R}[x_1, \dots, x_n,\ y_1, \dots, y_n]^G = \mathbb{R}[z_1, \dots, z_n,\ \overline{z_1}, \dots, \overline{z_n}]^G$$

is the same as a Hilbert basis of

$$\mathbb{C}[z_1, \dots, z_n,\ w_1, \dots, w_n]^H$$

where H is the subgroup of $\mathrm{GL}_{2n}(\mathbb{C})$ corresponding to the weight matrix

$$[A| - A].$$

Real Invariants of Compact Tori, Example

The weight matrix $A = \begin{pmatrix} -2 & 0 & 1 \\ -3 & 1 & 0 \end{pmatrix}$ describes a subgroup of $\mathrm{GL}_3(\mathbb{C})$ but also a subgroup G of $\mathrm{GL}_6(\mathbb{R})$.

To find a Hilbert basis for the G-invariants, we need only find a Hilbert basis for the invariants of the subgroup of $\mathrm{GL}_6(\mathbb{C})$ associated to

$$\left(\begin{array}{ccc|ccc} -2 & 0 & 1 & 2 & 0 & -1 \\ -3 & 1 & 0 & 3 & -1 & 0 \end{array}\right).$$

Finding invariants using Gröbner bases

Algorithm for Torus Invariants

This algorithm is from Sturmfels [5, Algorithm 1.4.5]

Given an $\ell \times n$ weight matrix A:

Give $\mathbb{C}[t_1, \ldots, t_\ell, x_1, \ldots, x_n, y_1, \ldots, y_n]$ a monomial order $\prec$ such that for any i, j, k, $t_i \succ x_j \succ y_k$.

For each column j of A, define

$$q_j = x_j - y_j t_1^{a_{1,j}} t_2^{a_{2,j}} \cdots t_\ell^{a_{\ell,j}}.$$

If q_j is not a polynomial (as some $a_{i,j}$ is negative), multiply by $t_i^{-a_{i,j}}$ so that it is.

Compute the reduced Gröbner basis for $\langle q_1, \ldots, q_n \rangle$ with respect to $\prec$.

The Hilbert basis of the invariants is the set of all $x_1^{p_1} \cdots x_n^{p_n}$ such that $x_1^{p_1} \cdots x_n^{p_n} - y_1^{p_1} \cdots y_n^{p_n}$ appears in the Gröbner basis.

Algorithm for Torus Invariants on *Mathematica*

On *Mathematica*, we can compute this Gröbner basis with the command

```
GroebnerBasis[ideal, variables, t-variables]
```

where

- `ideal` is the list of the q_j (in brackets $\{\}$),
- `variables` is the list of the all variables (t_i's, then x_j's, then y_j's, all in brackets $\{\}$), and
- `t-variables` is the list of t_i's (in brackets $\{\}$).

Algorithm for Torus Invariants on *Mathematica*, Example

For the weight matrix $\begin{pmatrix}-2 & 3 & 5\end{pmatrix}$, we work in $\mathbb{C}[t_1,\ x_1, x_2, x_3,\ y_1, y_2, y_3]$.

We start with

$$\begin{aligned} q_1 &= x_1 - y_1 t_1^{-2}, \\ q_2 &= x_2 - y_2 t_1^{3}, \\ q_3 &= x_3 - y_3 t_1^{5}. \end{aligned}$$

But q_1 is not a polynomial, so we redefine $q_1 = x_1 t_1^2 - y_1$.

Hence, we enter:

```
GroebnerBasis[{x1*t1^2-y1, x2-y2*t1^3, x3-y3*t1^5},
  {t1,x1,x2,x3,y1,y2,y3}, {t1}]
```

Algorithm for Torus Invariants on *Mathematica*, Example

$\begin{pmatrix} -2 & 3 & 5 \end{pmatrix}$:

The output of

```
GroebnerBasis[{x1*t1^2-y1, x2-y2*t1^3, x3-y3*t1^5},
  {t1,x1,x2,x3,y1,y2,y3}, {t1}]
```

is

```
-x3^3 y2^5 + x2^5 y3^3, x1 x3 y2 - x2 y1 y3,
 -x3^2 y1 y2^4 + x1 x2^4 y3^2, -x3 y1^2 y2^3 + x1^2 x2^3 y3,
 x1^3 x2^2 - y1^3 y2^2, x1^4 x2 x3 - y1^4 y2 y3,
 x1^5 x3^2 - y1^5 y3^2
```

Hence, the Hilbert basis is

$$\{x_1^3 x_2^2, \quad x_1^4 x_2 x_3, \quad x_1^5 x_3^2\}.$$

Algorithm for Torus Invariants on *Mathematica*, Example

For the weight matrix $\begin{pmatrix} -1 & 0 & 2 & 3 \\ 0 & -2 & 3 & 4 \end{pmatrix}$, we work in $\mathbb{C}[t_1, , t_2\ x_1, x_2, x_3, x_4,\ y_1, y_2, y_3, y_4]$.
We start with

$$q_1 = x_1 - y_1 t_1^{-1},$$
$$q_2 = x_2 - y_2 t_2^{-2},$$
$$q_3 = x_3 - y_3 t_1^2 t_2^3,$$
$$q_4 = x_4 - y_4 t_1^3 t_2^4,$$

and redefine $q_1 = x_1 t_1 - y_1$ and $q_2 = x_2 t_2^2 - y_2$.

Hence, we enter:

```
GroebnerBasis[{x1*t1 - y1, x2*t2^2 - y2,
    x3 - y3*t1^2*t2^3, x4 - y4*t1^3*t2^4},
  {t1, t2, x1, x2, x3, x4, y1, y2, y3, y4},
  {t1, t2}]
```

Algorithm for Torus Invariants on *Mathematica*, Example

$$\begin{pmatrix} -1 & 0 & 2 & 3 \\ 0 & -2 & 3 & 4 \end{pmatrix}:$$

The output of

```
GroebnerBasis[{x1*t1 - y1,    x2*t2^2 - y2,
               x3 - y3*t1^2*t2^3,    x4 - y4*t1^3*t2^4},
  {t1, t2, x1, x2, x3, x4, y1, y2, y3, y4},   {t1, t2}]
```

is

```
-x4^4 y2 y3^6 + x2 x3^6 y4^4, x1 x4^3 y3^4 - x3^4 y1 y4^3,
 -x4 y1 y2 y3^2 + x1 x2 x3^2 y4,
 x1^2 x2 x4^2 y3^2 - x3^2 y1^2 y2 y4^2,
 x1^3 x2^2 x4 - y1^3 y2^2 y4,
 x1^4 x2^3 x3^2 - y1^4 y2^3 y3^2
```

Hence, the Hilbert basis is

$$\{x_1^3 x_2^2 x_4, \quad x_1^4 x_2^3 x_3^2\}.$$

Algorithm for Torus Invariants on *Mathematica*, Example

For the weight matrix $\begin{pmatrix} -1 & -1 & 2 & 7 \end{pmatrix}$, we use

$$\begin{aligned} q_1 &= x_1 t_1 - y_1, \\ q_2 &= x_2 t_1 - y_2, \\ q_3 &= x_3 - y_3 t_1^2, \\ q_4 &= x_4 - y_4 t_1^7. \end{aligned}$$

The input is

```
GroebnerBasis[{
    x1*t1^1 - y1, x2*t1^1 - y2,
    x3 - y3*t1^2, x4 - y4*t1^7},
  {t1, x1, x2, x3, x4, y1, y2, y3, y4}, {t1}]
```

Algorithm for Torus Invariants on *Mathematica*, Example

$\begin{pmatrix}-1 & -1 & 2 & 7\end{pmatrix}$:

The output is

```
-x4^2 y3^7 + x3^7 y4^2,    x2 x4 y3^3 - x3^3 y2 y4,    -x4 y2 y3^4 + x2 x3^4 y4,
 x2^2 x3 - y2^2 y3,    x2^3 x4 y3^2 - x3^2 y2^3 y4,    x2^5 x4 y3 - x3 y2^5 y4,
 x2^7 x4 - y2^7 y4,    -x2 y1 + x1 y2,    x1 x4 y3^3 - x3^3 y1 y4,
 -x4 y1 y3^4 + x1 x3^4 y4,    x1 x2 x3 - y1 y2 y3,
 x1 x2^2 x4 y3^2 - x3^2 y1 y2^2 y4,    x1 x2^4 x4 y3 - x3 y1 y2^4 y4,
 x1 x2^6 x4 - y1 y2^6 y4,    x1^2 x3 - y1^2 y3,
 x1^2 x2 x4 y3^2 - x3^2 y1^2 y2 y4,    x1^2 x2^3 x4 y3 - x3 y1^2 y2^3 y4,
 x1^2 x2^5 x4 - y1^2 y2^5 y4,    x1^3 x4 y3^2 - x3^2 y1^3 y4,
 x1^3 x2^2 x4 y3 - x3 y1^3 y2^2 y4,    x1^3 x2^4 x4 - y1^3 y2^4 y4,
 x1^4 x2 x4 y3 - x3 y1^4 y2 y4,    x1^4 x2^3 x4 - y1^4 y2^3 y4,
 x1^5 x4 y3 - x3 y1^5 y4,    x1^5 x2^2 x4 - y1^5 y2^2 y4,
 x1^6 x2 x4 - y1^6 y2 y4,    x1^7 x4 - y1^7 y4
```

Hence, the Hilbert basis is

$$\{x_2^2x_3,\quad x_2^7x_4,\quad x_1x_2x_3,\quad x_1x_2^6x_4,\quad x_1^2x_3,\quad x_1^2x_2^5x_4,$$
$$x_1^3x_2^4x_4,\quad x_1^4x_2^3x_4,\quad x_1^5x_2^2x_4,\quad x_1^6x_2x_4,\quad x_1^7x_4\}.$$

Other Kinds of Groups

There are similar algorithms using Gröbner bases to compute Hilbert bases of invariants of finite groups, general compact Lie groups, etc.

See Cox–Little–O'Shea [2], Derksen and Kemper [3], and Sturmfels [5].

Finding Relations Using Gröbner Bases

Algorithm for Relations

This algorithm is from Cox–Little–O'Shea [2, Proposition 7.4.3].

Given generators $f_1, \ldots, f_r$ for a subalgebra of $\mathbb{K}[x_1, \ldots, x_n]$ (e.g. a Hilbert basis):

Give $\mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_r]$ a monomial order such that for each i, j, $x_i \succ y_j$.

Compute a Gröbner basis for the ideal

$$I = \langle f_1 - y_1, f_2 - y_2, \ldots, f_r - y_r \rangle.$$

A Gröbner basis for the ideal of relations of $\langle f_1, \ldots, f_r \rangle$ is given by intersecting the result with $\mathbb{K}[y_1, \ldots, y_m]$, i.e. removing the elements that involve the x_i.

Algorithm for Relations on *Mathematica*

On *Mathematica*, we can compute this Gröbner basis with the command:

```
GroebnerBasis[ideal, variables, x-variables]
```

where

- `ideal` is the list of $f_j - y_j$, $j = 1, \ldots, r$ (in brackets $\{\}$),
- `variables` is the list of the all variables (x_j's, then y_j's, all in brackets $\{\}$), and
- `x-variables` is the list of x_j's (in brackets $\{\}$).

Algorithm for Relations on *Mathematica*, Example

Recall that the weight matrix $\begin{pmatrix} -2 & 3 & 5 \end{pmatrix}$ had Hilbert basis

$$\{x_1^3 x_2^2, \quad x_1^4 x_2 x_3, \quad x_1^5 x_3^2\}.$$

We work in $\mathbb{C}[x_1, x_2, x_3, \ y_1, y_2, y_3]$ and enter:

```
GroebnerBasis[{
    x1^3*x2^2-y1, x1^4*x2*x3-y2, x1^5*x3^2-y3},
  {x1,x2,x3,y1,y2,y3}, {x1,x2,x3}]
```

The output is:

```
-y2^2 + y1 y3
```

So the ideal of relations is

$$\langle f_1 f_3 - f_2^2 \rangle.$$

Algorithm for Relations on *Mathematica*, Example

Recall that the weight matrix $\begin{pmatrix} -1 & 0 & 2 & 3 \\ 0 & -2 & 3 & 4 \end{pmatrix}$ had Hilbert basis

$$\{x_1^3 x_2^2 x_4, \quad x_1^4 x_2^3 x_3^2\}.$$

We work in $\mathbb{C}[x_1, x_2, x_3, x_4,\ y_1, y_2]$ and enter:

```
GroebnerBasis[{
    x1^3*x2^2^2*x4-y1, x1^4*x2^3*x3^2-y2},
  {x1,x2,x3,x4,y1,y2}, {x1,x2,x3,x4}]
```

The output is empty, so there are no relations.

Algorithm for Relations on *Mathematica*, Example

Recall that the weight matrix $\begin{pmatrix} -1 & -1 & 2 & 7 \end{pmatrix}$ had Hilbert basis

$$\{x_2^2x_3, \quad x_2^7x_4, \quad x_1x_2x_3, \quad x_1x_2^6x_4, \quad x_1^2x_3, \quad x_1^2x_2^5x_4, \\ x_1^3x_2^4x_4, \quad x_1^4x_2^3x_4, \quad x_1^5x_2^2x_4, \quad x_1^6x_2x_4, \quad x_1^7x_4\}.$$

We work in $\mathbb{C}[x_1, x_2, x_3, x_4,\ y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}, y_{11}]$ and enter:

```
GroebnerBasis[{
    x2^2*x3-y1,  x2^7*x4-y2,  x1*x2*x3-y3,
    x1*x2^6*x4-y4,  x1^2*x3-y5,
    x1^2*x2^5*x4-y6,  x1^3*x2^4*x4-y7,
    x1^4*x2^3*x4-y8,  x1^5*x2^2*x4-y9,
    x1^6*x2*x4-y10,  x1^7*x4-y11
  },
{x1,x2,x3,x4,y1,y2,y3,y4,y5,y6,y7,
  y8,y9,y10,y11}, {x1,x2,x3,x4}]
```

Algorithm for Relations on *Mathematica*, Example

The output is

```
-y10^2 + y11 y9, y11 y8 - y10 y9, y10 y8 - y9^2,
 y11 y7 - y9^2, y10 y7 - y8 y9, -y8^2 + y7 y9,
 y11 y6 - y8 y9, y10 y6 - y8^2, -y7 y8 + y6 y9,
 -y7^2 + y6 y8, y11 y4 - y8^2, y10 y4 - y7 y8,
 -y7^2 + y4 y9, -y6 y7 + y4 y8, -y6^2 + y4 y7,
 y11 y3 - y10 y5, y10 y3 - y5 y9, -y5 y8 + y3 y9,
 -y5 y7 + y3 y8, -y5 y6 + y3 y7, -y4 y5 + y3 y6,
 y11 y2 - y7 y8, y10 y2 - y7^2, -y6 y7 + y2 y9,
 -y6^2 + y2 y8, -y4 y6 + y2 y7, -y4^2 + y2 y6,
 -y3 y4 + y2 y5, y1 y11 - y5 y9, y1 y10 - y5 y8,
 -y5 y7 + y1 y9, -y5 y6 + y1 y8, -y4 y5 +
 y1 y7, -y3 y4 + y1 y6, -y3^2 + y1 y5,
 -y2 y3 + y1 y4
```

Algorithm for Relations on *Mathematica*, Example

Hence, there are 36 relations.

$$
\begin{gathered}
-f_{10}^2+f_{11}f_9,\quad f_{11}f_8-f_{10}f_9,\quad f_{10}f_8-f_9^2,\quad f_{11}f_7-f_9^2,\quad f_{10}f_7-f_8f_9,\\
-f_8^2+f_7f_9,\quad f_{11}f_6-f_8f_9,\quad f_{10}f_6-f_8^2,\quad -f_7f_8+f_6f_9,\quad -f_7^2+f_6f_8,\\
f_{11}f_4-f_8^2,\quad f_{10}f_4-f_7f_8,\quad -f_7^2+f_4f_9,\quad -f_6f_7+f_4f_8,\quad -f_6^2+f_4f_7,\\
f_{11}f_3-f_{10}f_5,\quad f_{10}f_3-f_5f_9,\quad -f_5f_8+f_3f_9,\quad -f_5f_7+f_3f_8,\quad -f_5f_6+f_3f_7,\\
-f_4f_5+f_3f_6,\quad f_{11}f_2-f_7f_8,\quad f_{10}f_2-f_7^2,\quad -f_6f_7+f_2f_9,\quad -f_6^2+f_2f_8,\\
-f_4f_6+f_2f_7,\quad -f_4^2+f_2f_6,\quad -f_3f_4+f_2f_5,\quad f_1f_{11}-f_5f_9,\quad f_1f_{10}-f_5f_8,\\
-f_5f_7+f_1f_9,\quad -f_5f_6+f_1f_8,\quad -f_4f_5+f_1f_7,\quad -f_3f_4+f_1f_6,\quad -f_3^2+f_1f_5,\\
-f_2f_3+f_1f_4
\end{gathered}
$$

Thank you!

References:

Jacek Bochnak, Michel Coste, and Marie-Françoise Roy, *Real algebraic geometry*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 36, Springer-Verlag, Berlin, 1998, Translated from the 1987 French original, Revised by the authors. MR 1659509 (2000a:14067)

David A. Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms*, fourth ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015, An introduction to computational algebraic geometry and commutative algebra.

Harm Derksen and Gregor Kemper, *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, Encyclopaedia of Mathematical Sciences, 130.

V. L. Popov and È. B. Vinberg, *Invariant theory*, Algebraic geometry. IV, Encyclopaedia of Mathematical Sciences, vol. 55, Linear algebraic groups. Invariant theory, A translation of ıt Algebraic geometry. 4 (Russian), Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989, Translation edited by A. N. Parshin and I. R. Shafarevich.

Bernd Sturmfels, *Algorithms in invariant theory*, second ed., Texts and Monographs in Symbolic Computation, SpringerWienNewYork, Vienna, 2008.