Lecture 15: Introduction to Invariant Theory

Rafael Oliveira

University of Waterloo
Cheriton School of Computer Science

rafael.oliveira.teaching@gmail.com

March 8, 2021

Overview

- Group Actions on Vector Spaces
- Ring of Invariant Polynomials
- Fundamental Theorems
- Conclusion
- Acknowledgements

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space

$$SL(n) = \{A \in \mathbb{C}^{n \times n} \mid \det(A) = 1\}$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

$$(gh) \circ v = g \circ (h \circ v)$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n$, $V = \mathbb{C}^n$ permuting coordinates

$\sigma : [n] \longrightarrow [n]$ bijection

$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$ $\sigma v = \begin{pmatrix} v_{\sigma(1)} \\ v_{\sigma(2)} \\ \vdots \\ v_{\sigma(n)} \end{pmatrix}$

$n = 3$

$\sigma = (1\ 2\ 3)$ $v = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ $\sigma v = \begin{pmatrix} b \\ c \\ a \end{pmatrix}$

$\sigma(1) = 2$ $\sigma(2) = 3$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

$$\sigma\left(\begin{pmatrix}\alpha\\ \beta\\ \gamma\end{pmatrix}+\begin{pmatrix}a\\ b\\ c\end{pmatrix}\right)=\begin{pmatrix}\beta\\ \gamma\\ \alpha\end{pmatrix}+\begin{pmatrix}b\\ c\\ a\end{pmatrix}$$

$$\| \text{ sum}$$

$$\begin{pmatrix}\alpha+a\\ \beta+b\\ \gamma+c\end{pmatrix}\xrightarrow{\text{group}}\begin{pmatrix}\beta+b\\ \gamma+c\\ \alpha+a\end{pmatrix}$$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates

permutations of even sign

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^{d+1}$ linear transformations of curves

bivariate homogeneous polynomials of degree d

$$P(x,y) = a_d x^d + a_{d-1} x^{d-1} y + \cdots + a_0 y^d$$

$$\longleftrightarrow (a_d, a_{d-1}, \ldots, a_0)$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

$$\underline{a'} = \underline{a \cdot \alpha^2 + b\alpha\gamma + \gamma^2 \cdot c}$$ linear combination $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2)$$

$$p(x,y) = ax^2 + bxy + cy^2$$

$$(a,b,c) \in \mathbb{C}^3$$

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \beta y \\ \gamma x + \delta y \end{pmatrix}$$

$$q(x,y) = p(\alpha x + \beta y, \gamma x + \delta y)$$

$$= \underline{a(\alpha x + \beta y)^2} + b\underline{(\alpha x + \beta y)(\gamma x + \delta y)} +$$

$$\underline{c(\gamma x + \delta y)^2} = a'x^2 + b'xy + c'y^2$$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n$, $V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n$, $V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2)$, $V = \mathbb{C}^{d+1}$ — linear transformations of curves
  4. $G = \mathbb{SL}(n)$, $V = \mathrm{Mat}(n)$ — left multiplication

elementary row operations

$$g \circ A = g \cdot A$$

$$\underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{\in G} \cdot \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\mathrm{Mat}(n)} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^{d+1}$ — linear transformations of curves
  4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication
  5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ — conjugation

$g \in GL(n)$ $A \in Mat(n)$ changes of bases of $\mathbb{C}^n$

$A \xmapsto{g} gAg^{-1}$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^{d+1}$ — linear transformations of curves
  4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication
  5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ — conjugation
  6. $G = \mathbb{ST}(n) \times \mathbb{ST}(n),\ V = \mathrm{Mat}(n)$ — row/column scaling

$$ST(n) = \left\{ \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix} \,\middle|\, \prod_{i=1}^{n} \alpha_i = 1 \right\}$$ diagonal w/ determinant 1

$$\begin{pmatrix} x_1 & 0 \\ 0 & x_2 \end{pmatrix}\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} c_1 & 0 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1c_1 & a_{12}x_1c_2 \\ a_{21}x_2c_1 & a_{22}x_2c_2 \end{pmatrix}$$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$

Group Actions

- Let G be a nice[1] group and V be a $\mathbb{C}$-vector space
- G acts *linearly* on V if

$$g \circ (\alpha u + \beta v) = \alpha(g \circ u) + \beta(g \circ v)$$

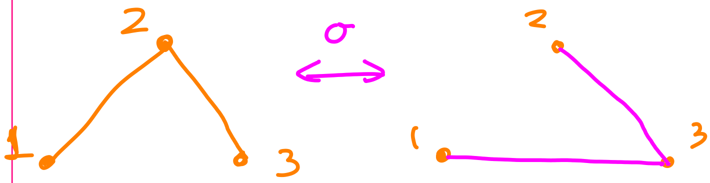
- Examples:
  1. $G = S_n,\ V = \mathbb{C}^n$ — permuting coordinates
  2. $G = A_n,\ V = \mathbb{C}^n$ — permuting coordinates
  3. $G = \mathbb{SL}(2),\ V = \mathbb{C}^{d+1}$ — linear transformations of curves
  4. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ — left multiplication
  5. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ — conjugation
  6. $G = \mathbb{ST}(n) \times \mathbb{ST}(n),\ V = \mathrm{Mat}(n)$ — row/column scaling
  7. $G = S_n,\ V = \mathbb{C}^{\binom{n}{2}}$ — graph isomorphism

$A([n], E_A) \quad B([n], E_B) \quad \{i, j\} \in E_A$

$\updownarrow$

$\sigma : [n] \to [n] \quad (\sigma A)([n], \sigma E_A) \quad \{\sigma(i), \sigma(j)\} \in \sigma E_A$

[1] The definition of nice is a bit technical, so we will stick to finite groups and $\mathbb{SL}(n)$



$$\sigma = (1\ 2\ 3)$$

$$\{1, 2\} \xrightarrow{\sigma} \{2, 3\}$$

$$\{2, 3\} \xrightarrow{\sigma} \{3, 1\}$$

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G, \; v \in V$$

$f : V \to \mathbb{C}$

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

Invariant Functions

$g \circ f = f(g^{-1}x)$

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G, \ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n, \ V = \mathbb{C}^n$ permuting coordinates

Symmetric polynomials.

$e_1 = \sum_{i=1}^{n} x_i$ invariant

$\sigma : [n] \to [n]$ bijective

$$\sigma e_1 = e_1\left(\sigma^{-1}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = \sum_{i=1}^{n} x_{\sigma^{-1}(i)}$$

$$= \sum_{i=1}^{n} x_i$$

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G,\ v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n,\ V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials.

2. $G = A_n,\ V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials (and more)

$$\Delta = \prod_{i<j} (x_i - x_j) \qquad \text{discriminant}$$

Invariant Functions

- In this setup, important to study functions which are *invariant* under the group action, that is:

$$f(v) = f(g \circ v) \quad \text{for all} \quad g \in G, \; v \in V$$

- Algebraically, would like to understand *polynomial invariant* functions

1. $G = S_n, \; V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials.

2. $G = A_n, \; V = \mathbb{C}^n$ permuting coordinates

   Symmetric polynomials (and more)

3. $G = \mathbb{SL}(2), \; V = \mathbb{C}^d$ linear transformations of curves

   Discriminants, Catalecticants (and more)

$d = 3$ (quadratic polynomials)

$(a, b, c) \longleftrightarrow ax^2 + bxy + cy^2$ $\quad \boxed{b^2 - 4ac}$

Examples, Continued

1. $G = \mathbb{SL}(n)$, $V = \text{Mat}(n)$ left multiplication

Determinant

$$\det(g \cdot A) = \det(g) \cdot \det(A)$$
$$= \det(A)$$

Examples, Continued

1. $G = \mathbb{SL}(n)$, $V = \mathrm{Mat}(n)$ left multiplication

   Determinant

2. $G = \mathbb{GL}(n)$, $V = \mathrm{Mat}(n)$ conjugation

   Trace polynomials.

$$A \xmapsto{g} gAg^{-1}$$

$$\mathrm{Tr}[A^k]$$

$$\mathrm{Tr}[(gAg^{-1})^k] = \mathrm{Tr}[gA^kg^{-1}] = \mathrm{Tr}[A^kg^{-1}g]$$

$$= \mathrm{Tr}[A^k]$$

Examples, Continued

1. $G = \mathbb{SL}(n)$, $V = \operatorname{Mat}(n)$ — left multiplication

   Determinant

2. $G = \mathbb{GL}(n)$, $V = \operatorname{Mat}(n)$ — conjugation

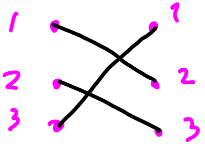
   Trace polynomials.

3. $G = \underline{\mathbb{ST}(n)} \times \underline{\mathbb{ST}(n)}$, $V = \operatorname{Mat}(n)$ — row/column scaling

   Matching/Permutation monomials.

$\begin{pmatrix} r_1 & & \\ & \ddots & \\ & & r_n \end{pmatrix} \quad \begin{pmatrix} c_1 & & \\ & \ddots & \\ & & c_n \end{pmatrix}$

$\sigma : [n] \longrightarrow [n]$



$\underline{\prod A_{i\sigma(i)}}$

$\sigma(1\ 2\ 3)$

$$\prod_{i=1}^{n} A_{i\sigma(i)}\, r_i\, c_{\sigma(i)} = \underline{\left(\prod_{i=1}^{n} A_{i\sigma(i)}\right)} \cancel{\left(\prod_{i=1}^{n} r_i\right)} \cancel{\left(\prod_{i=1}^{n} c_{\sigma(i)}\right)}$$

Examples, Continued

1. $G = \mathbb{SL}(n),\ V = \mathrm{Mat}(n)$ left multiplication

   Determinant

2. $G = \mathbb{GL}(n),\ V = \mathrm{Mat}(n)$ conjugation

   Trace polynomials.

3. $G = \mathbb{ST}(n) \times \mathbb{ST}(n),\ V = \mathrm{Mat}(n)$ row/column scaling

   Matching/Permutation monomials.

4. $G = S_n,\ V = \mathbb{C}^{\binom{n}{2}}$ graph isomorphism

   Open.

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$

α

$e_1(x_1, \ldots, x_n) = x_1 + x_2 + \cdots + x_n$

$e_2(x_1, \ldots, x_n) = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n$

$e_1 e_2$ $\qquad \alpha e_1 + \beta e_2$

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$
- For the ring of symmetric polynomials, we know that

$$\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[\underline{e_1}, \underline{e_2}, \ldots, \underline{e_n}]$$

where

$$e_d(x_1, \ldots, x_n) = \sum_{\substack{S \subset [n] \\ |S| = d}} \prod_{i \in S} x_i$$

$p(\bar{x}) \in \mathbb{C}[\bar{x}]$ symmetric.

$$p(\bar{x}) = q(e_1, \ldots, e_n)$$

$$\underline{x_1^2 + x_2^2} = \underbrace{(x_1 + x_2)^2}_{} - 2x_1x_2$$

$$\boxed{e_1^2 - 2e_2}$$

$x_1^3 + x_2^3$

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$
- For the ring of symmetric polynomials, we know that

$$\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[e_1, e_2, \ldots, e_n]$$

where

$$e_d(x_1, \ldots, x_n) = \sum_{\substack{S \subset [n] \\ |S| = d}} \prod_{i \in S} x_i$$

- Every symmetric polynomial is itself a <u>polynomial function</u> of the *elementary symmetric polynomials*

Ring of Invariant Polynomials

- G acts linearly on $V = \mathbb{C}^N$, let $\mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_N]$ be the polynomial ring over $\mathbb{V}$
- Invariant polynomials form a *subring* of $\mathbb{C}[\mathbf{x}]$, denoted $\mathbb{C}[\mathbf{x}]^G$
- For the ring of symmetric polynomials, we know that

$$\mathbb{C}[x_1, \ldots, x_n]^{S_n} = \mathbb{C}[e_1, e_2, \ldots, e_n]$$

  where

$$e_d(x_1, \ldots, x_n) = \sum_{\substack{S \subset [n] \\ |S| = d}} \prod_{i \in S} x_i$$

- Every symmetric polynomial is itself a <u>polynomial function</u> of the *elementary symmetric polynomials*
- Elementary symmetric polynomials are a *fundamental system of invariants*

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*

$\bar{a} \succ \bar{b}$ if $\deg(\bar{a}) > \deg(\bar{b})$

or $\deg(\bar{a}) = \deg(\bar{b})$

$\bar{a} \succ_{lex} \bar{b}$

$(\underline{2}, 3, 1) \succ (\underline{2}, 1, 3)$

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*
- Every symmetric polynomial $p(x)$ has a non-zero **leading term**

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

with $a_1 \geq a_2 \geq \cdots \geq a_n$

$$x_1^{a_{12}} x_2^{a_1} x_3^{a_3} \cdots x_n^{a_n} + x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots x_n^{a_n}$$

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*
- Every symmetric polynomial $p(x)$ has a non-zero **leading term**

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

with $a_1 \geq a_2 \geq \cdots \geq a_n$

$a_i - a_{i+1} \geq 0$

- Then

$$p(x) - LC(p) \cdot \boxed{e_1^{a_1 - a_2} \cdot e_2^{a_2 - a_3} \cdots e_{n-1}^{a_{n-1} - a_n} \cdot e_n^{a_n}}$$

has *smaller* leading monomial! division algorithm!

monomial over $e_1, \dots, e_n$

$$P(x) = LC(p) \cdot x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} + \cdots$$

$$P(x) - LC(p)\, \underbrace{e_1^{a_1-a_2}\, e_2^{a_2-a_3} \cdots e_{n-1}^{a_{n-1}-a_n}\, e_n^{a_n}}$$

$$x_1^{a_1-a_2} (x_1 x_2)^{a_2-a_3} (x_1 x_2 x_3)^{a_3-a_4} \cdots (x_1 \cdots x_n)^{a_n}$$

$$= x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

Cancelling the leading term of $p(x)$!

Proof of Invariant Ring of Symmetric Polynomials

- Proof due to van der Waerden using monomial ordering!
- Use *degree lexicographic order*
- Every symmetric non zero polynomial $p(x)$ has a non-zero **leading term**

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

with $a_1 \geq a_2 \geq \cdots \geq a_n$

- Then

$$p(x) - LC(p) \cdot e_1^{a_1 - a_2} \cdot e_2^{a_2 - a_3} \cdots e_{n-1}^{a_{n-1} - a_n} \cdot e_n^{a_n}$$

has *smaller* leading monomial! division algorithm!

- Procedure must terminate because of well-ordering of monomial ordering!

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!

$$xy = \frac{(x+y)^2 - (x^2+y^2)}{2}$$

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants!

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants!
- The complete symmetric polynomials are also a fundamental system of invariants!

$$h_d(x_1,\dots,x_n) = \sum_{\substack{S\subset[n] \\ \text{multiset} \\ |S|=d}} \prod_{i\in S} x_i$$

$$h_2(x,y,z) = x^3 + x^2y + x^2z + xy^2 + xyz + xz^2 + \cdots + z^3$$

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants!
- The complete symmetric polynomials are also a fundamental system of invariants!
- Relations between these bases is very important in algebraic combinatoric and representation theory!

Other Fundamental Invariants

- It turns out that the fundamental system of invariants may not be unique (an are generally far from being unique)
- The power sum polynomials $p_d(x) = x_1^d + \cdots + x_n^d$ are also a fundamental system of invariants!
- The Schur polynomials are also a fundamental system of invariants!
- The complete symmetric polynomials are also a fundamental system of invariants!
- Relations between these bases is very important in algebraic combinatoric and representation theory!
- More generally, fundamental systems of invariants give us great properties and connections between many areas of mathematics!

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

Matching/Permutation monomials.

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

Matching/Permutation monomials.

- Action is: $\underline{A_{ij}} = \underline{A_{ij}} \cdot \underline{x_i} \cdot \underline{y_j}$ $= B_{ij}$

invariants are generated by monomials

$$\prod_{i,j=1}^{n} B_{ij}^{e_{ij}} = \prod_{i,j=1}^{n} A_{ij}^{e_{ij}} x_i^{e_{ij}} y_j^{e_{ij}}$$

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Action is: $A_{ij} = A_{ij} \cdot x_i \cdot y_j$

  invariants are generated by monomials

- Equations that exponents must satisfy: monomial $\prod_{i,j} A_{i,j}^{e_{i,j}}$ is invariant iff:

$$\prod_{i,j=1}^{n} A_{ij}^{e_{ij}} = \prod_{i,j=1}^{n} (A_{ij} x_i y_j)^{e_{ij}}$$

$$= \left(\prod_{i,j=1}^{n} A_{ij}^{e_{ij}}\right) \boxed{\prod_{i=1}^{n} x_i^{\boxed{\sum_{j=1}^{n} e_{ij}}} \prod_{i=1}^{n} y_j^{\boxed{\sum_{i=1}^{n} e_{ij}}}}$$

$$\sum_{j=1}^{n} e_{1j} = \sum_{j=1}^{n} e_{2j} = \cdots = \sum_{j=1}^{n} e_{nj} = \underline{m} = \sum_{i=1}^{n} e_{ij} \quad \forall j$$

$$\prod x_i^{\sum_j e_{ij}} = \prod x_i^{m} = \underbrace{\left(\prod x_i\right)^{m}}_{=1}$$

because $\det\begin{pmatrix} x_1 & & \\ & \ddots & \\ & & x_n \end{pmatrix} = \underline{1}$

matrix of exponents

$$\begin{array}{cc} \begin{bmatrix} e_{11} & e_{12} & e_{13} \\ e_{21} & e_{22} & e_{23} \\ e_{31} & e_{32} & e_{33} \end{bmatrix} & \begin{array}{c} m \\ m \\ m \end{array} \\ \begin{array}{ccc} m & m & m \end{array} & \end{array}$$

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Action is: $A_{ij} = A_{ij} \cdot x_i \cdot y_j$

  invariants are generated by monomials

- Equations that exponents must satisfy: monomial $\prod_{i,j} A_{i,j}^{e_{i,j}}$ is invariant iff:
- Permutation/matching monomials are definitely invariant

$$\begin{array}{cc} \begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix} & \begin{array}{c} 1 \\ 1 \\ 1 \end{array} \\ \begin{array}{ccc} 1 & 1 & 1 \end{array} & \end{array}$$

Fundamental System of Invariants – Another Example

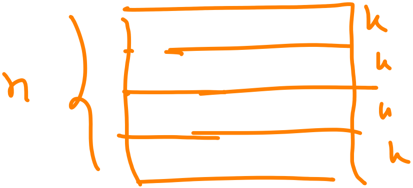
- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Action is: $A_{ij} = A_{ij} \cdot x_i \cdot y_j$

  invariants are generated by monomials

- Equations that exponents must satisfy: monomial $\prod_{i,j} A_{i,j}^{e_{i,j}}$ is invariant iff:
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$



$k \cdot n$

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Action is: $A_{ij} = A_{ij} \cdot x_i \cdot y_j$

  invariants are generated by monomials

- Equations that exponents must satisfy: monomial $\prod_{i,j} A_{i,j}^{e_{i,j}}$ is invariant iff:
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$
- Birkhoff-von Neumann theorem, must be in convex hull of permutations

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Action is: $A_{ij} = A_{ij} \cdot x_i \cdot y_j$

  invariants are generated by monomials

- Equations that exponents must satisfy: monomial $\prod_{i,j} A_{i,j}^{e_{i,j}}$ is invariant iff:
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$
- Birkhoff-von Neumann theorem, must be in convex hull of permutations
- Relation to combinatorics: if matrix A is adjacency matrix of a bipartite graph H, then A has *no perfect matching* iff A *vanishes on all invariants*!

perfect matching

$\prod A_{i\sigma(i)} \leftarrow$ one must be zero $\Rightarrow = 0$

Fundamental System of Invariants – Another Example

- $G = \mathbb{ST}(n) \times \mathbb{ST}(n)$, $V = \mathrm{Mat}(n)$ row/column scaling

  Matching/Permutation monomials.

- Action is: $A_{ij} = A_{ij} \cdot x_i \cdot y_j$

  invariants are generated by monomials

- Equations that exponents must satisfy: monomial $\prod_{i,j} A_{i,j}^{e_{i,j}}$ is invariant iff:
- Permutation/matching monomials are definitely invariant
- Any invariant monomial must have degree kn for some $k \in \mathbb{Z}$
- Birkhoff-von Neumann theorem, must be in convex hull of permutations
- Relation to combinatorics: if matrix A is adjacency matrix of a bipartite graph H, then A has *no perfect matching* iff A *vanishes on all invariants*!
- It is no coincidence that polytopes appear naturally with torus actions. For the interested folks, see moment polytopes.

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by

$$\underline{g^{-1} \circ p} = p\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by

$$g^{-1} \circ p = p\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

- If (a', b', c') is the image $g^{-1} \circ p$, we have

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2 \cdot (a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma) \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$

$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$

- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by

$$g^{-1} \circ p = p\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

- If (a', b', c') is the image $g^{-1} \circ p$, we have

$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2 \cdot (a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma) \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$

- The discriminant is an *invariant*!

$$\underline{b^2 - 4ac} = \underline{(b')^2 - 4a'c'}$$

Discriminant & Invariant Theory

- Let $\mathbb{SL}(2)$ act on the space of quadratic polynomials $\mathbb{C}^3$
$$p(x) = ax^2 + bxy + cy^2 \leftrightarrow p := (a, b, c)$$
- $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on p by
$$g^{-1} \circ p = p\left(g\begin{pmatrix} x \\ y \end{pmatrix}\right)$$
- If (a', b', c') is the image $g^{-1} \circ p$, we have
$$\begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2 \cdot (a\alpha\beta + c\gamma\delta) + b(\alpha\delta + \beta\gamma) \\ c' &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$
- The discriminant is an *invariant*!
$$b^2 - 4ac = (b')^2 - 4a'c'$$
- It captures exactly the quadratic polynomials which have a double root! We may see why this is the case in the end of the course.

- Group Actions on Vector Spaces
- Ring of Invariant Polynomials
- **Fundamental Theorems**
- Conclusion
- Acknowledgements

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?

$$\mathbb{C}[\bar{x}]^G = \mathbb{C}[\underbrace{f_1, \dots, f_t}]$$

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.

$$\mathbb{C}[\bar{x}]^{A_n} = \mathbb{C}[\underbrace{e_1, \ldots, e_n, \Delta}_{\Delta^2 - (\cdots)}]$$

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

Δ^2 symmetric $\in \mathbb{C}[e_1, \ldots, e_n]$

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.
- Give an algorithm which writes an invariant $p(x)$ as a polynomial in the fundamental invariants.

$$\mathbb{C}[\bar{x}]^G = \mathbb{C}[f_1, \ldots, f_t]$$

$$p(\bar{x}) = q(f_1, \ldots, f_t)$$

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.
- Give an algorithm which writes an invariant $p(x)$ as a polynomial in the fundamental invariants.

These were the problems Hilbert was trying to solve when he developed the **Hilbert Basis Theorem**, **Nullstellensatz** and **Syzygy** theorem - cornerstones of modern commutative algebra and algebraic geometry.

Fundamental Problems in Invariant Theory

- Is the invariant ring *finitely generated* as a $\mathbb{C}$-algebra?
- Can we describe the algebraic *relations* among the fundamental invariants from the previous question? These algebraic relations are called *syzygies*.
- Give an algorithm which writes an invariant $p(x)$ as a polynomial in the fundamental invariants.

  These were the problems Hilbert was trying to solve when he developed the **Hilbert Basis Theorem**, **Nullstellensatz** and **Syzygy** theorem - cornerstones of modern commutative algebra and algebraic geometry.

- Answer to third problem can be done via Gröbner basis methods

Examples of Invariants with Syzygies

- Cyclic group of order 4:

$$G = \left\{ \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{id}, \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{x}, \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{y}, \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{xy} \right\}$$

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

Examples of Invariants with Syzygies

- Cyclic group of order 4:

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

- Invariant ring equals set of polynomials $p(x, y)$ such that

$$p(x, y) = p(-y, x)$$

Examples of Invariants with Syzygies

- Cyclic group of order 4:

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

- Invariant ring equals set of polynomials $p(x, y)$ such that

$$p(x, y) = p(-y, x)$$

- Three fundamental invariants:

$$f_1 = x^2 + y^2, \ f_2 = x^2 y^2, \ f_3 = x^3 y - x y^3$$

Examples of Invariants with Syzygies

- Cyclic group of order 4:

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

- Invariant ring equals set of polynomials $p(x, y)$ such that

$$p(x, y) = p(-y, x)$$

- Three fundamental invariants:

$$f_1 = x^2 + y^2, \;\; f_2 = x^2y^2, \;\; f_3 = x^3y - xy^3$$

- Syzygy:

$$f_3^2 - f_2 f_1^2 + 4f_2^2 \quad = 0$$

Conclusion

- Today we learned the basics about the algebraic side of invariant theory
- Some history
- Many examples of important rings of invariants
- Connections to other areas of mathematics
- Fundamental problems in invariant theory

Acknowledgement

- Lecture based entirely on the wonderful book by Sturmfels: Algorithms in Invariant Theory