Representations of reductive groups and invariant theory

Kyo Nishiyama

Graduate School of Science
Kyoto University

International conference on Recent Advances in Mathematics and its applications.
(September 24–30, 2007)

Department of Mathematics, KU Post Graduate Center
Belgaum, Karnataka INDIA

What is invariants?

What is invariants?

Examples of invariants in broader sense

- numbers . . . of finite sets

What is invariants?

Examples of invariants in broader sense

- numbers . . . of finite sets
- dim . . . of finite vector spaces

What is invariants?

Examples of invariants in broader sense

- numbers . . . of finite sets
- dim . . . of finite vector spaces
- rank . . . of matrix (or linear map)

What is invariants?

Examples of invariants in broader sense

- numbers . . . of finite sets
- dim . . . of finite vector spaces
- rank . . . of matrix (or linear map)
- genus . . . of compact 2-dimensional surfaces
  or we should say...
  Euler characteristic . . . of manifolds

What is invariants?

Examples of invariants in broader sense

- numbers . . . of finite sets
- dim . . . of finite vector spaces
- rank . . . of matrix (or linear map)
- genus . . . of compact 2-dimensional surfaces
  or we should say...
  Euler characteristic . . . of manifolds

Classification problem

$\Longrightarrow$ study of equivalence classes

$\Longrightarrow$ invariants

There are more sophisticated invariants...

There are more sophisticated invariants... which I vaguely understand

There are more sophisticated invariants... which I vaguely understand

- Alexander/Jones/Homfly/Kauffman polynomials . . . of knots and links
  Vasiliev invariants
  Chern-Simons invariants
  Now there are so many invariants, quantum invariants, . . .
- Donaldson invariants
  Seiberg-Witten invariants
  Gromov-Witten invariants . . . quantum cohomology
- Iwasawa invariants . . . for class field theory

There are more sophisticated invariants... which I vaguely understand

- Alexander/Jones/Homfly/Kauffman polynomials . . . of knots and links
  Vasiliev invariants
  Chern-Simons invariants
  Now there are so many invariants, quantum invariants, . . .
- Donaldson invariants
  Seiberg-Witten invariants
  Gromov-Witten invariants . . . quantum cohomology
- Iwasawa invariants . . . for class field theory

Study of invariants $\fallingdotseq$ Study of mathematics !

There are more sophisticated invariants... which I vaguely understand

- Alexander/Jones/Homfly/Kauffman polynomials . . . of knots and links
  Vasiliev invariants
  Chern-Simons invariants
  Now there are so many invariants, quantum invariants, . . .
- Donaldson invariants
  Seiberg-Witten invariants
  Gromov-Witten invariants . . . quantum cohomology
- Iwasawa invariants . . . for class field theory

Study of invariants $\fallingdotseq$ Study of mathematics !
. . . Too big subject for us

There are more sophisticated invariants... which I vaguely understand

- Alexander/Jones/Homfly/Kauffman polynomials ... of knots and links
  Vasiliev invariants
  Chern-Simons invariants
  Now there are so many invariants, quantum invariants, ...
- Donaldson invariants
  Seiberg-Witten invariants
  Gromov-Witten invariants ... quantum cohomology
- Iwasawa invariants ... for class field theory

Study of invariants $\fallingdotseq$ Study of mathematics !
... Too big subject for us (at least for me)

So what is invariant theory?

So what is invariant theory?

Examples of classical invariants in invariant theory

1. square of distance $r^2 = x_1^2 + \cdots + x_n^2$: orthogonal invariant

So what is invariant theory?

Examples of classical invariants in invariant theory

1. square of distance $r^2 = x_1^2 + \cdots + x_n^2$: orthogonal invariant

   Or more generally,
   quadratic form of signature (p, q) $(p + q = n)$
   $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$

   $\Longrightarrow$ Sylvester's law of inertia

So what is invariant theory?

Examples of classical invariants in invariant theory

1. square of distance $r^2 = x_1^2 + \cdots + x_n^2$: orthogonal invariant

   Or more generally,
   quadratic form of signature $(p, q) \quad (p + q = n)$
   $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$

   $\Longrightarrow$ Sylvester's law of inertia

2. determinant : $\det X$

   $\det(gXg^{-1}) = \det X \qquad g$: invertible matrix
   $\det(gX) = \det X \qquad g$: unimodular matrix

So what is invariant theory?

Examples of classical invariants in invariant theory

1. square of distance $r^2 = x_1^2 + \cdots + x_n^2$: orthogonal invariant

   Or more generally,
   quadratic form of signature (p, q) $(p + q = n)$
   $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$

   $\Longrightarrow$ Sylvester's law of inertia

2. determinant : $\det X$

   $\det(gXg^{-1}) = \det X$ $\quad g$: invertible matrix
   $\det(gX) = \det X$ $\quad g$: unimodular matrix

   trace : $\operatorname{trace} X$

   $\operatorname{trace}(gXg^{-1}) = \operatorname{trace} X$ $\quad g$: invertible matrix

3. discriminant : $\Delta(f)$ $\cdots \mathrm{SL}_2$-invariant

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$
$$= a_0 \prod_{j=1}^{n} (x - \zeta_j)$$

$$\Delta(f) := a_0^{2n-2} \prod_{i<j} (\zeta_i - \zeta_j)^2 \quad \ldots \text{polynomial in } a = (a_0, a_1, \ldots, a_n)$$

3. discriminant : $\Delta(f)$ $\cdots$ SL_2-invariant

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$
$$= a_0 \prod_{j=1}^{n} (x - \zeta_j)$$

$$\Delta(f) := a_0^{2n-2} \prod_{i<j} (\zeta_i - \zeta_j)^2 \quad \ldots \text{polynomial in } a = (a_0, a_1, \ldots, a_n)$$

4. resultant : $R(f, g)$ $\cdots$ SL_2-invariant

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = a_0 \prod_{i=1}^{n} (x - \zeta_i)$$
$$g(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_{m-1} x + b_m = b_0 \prod_{j=1}^{m} (x - \xi_j)$$

$$R(f, g) := a_0^m b_0^n \prod_{i,j} (\zeta_i - \xi_j) \quad \cdots \text{polynomial in } a \,\&\, b$$

These are all polynomial invariants and

These are all polynomial invariants and
related to some group action

These are all polynomial invariants and related to some group action

Here is a summary:

distance	$O_n \curvearrowright \mathbb{R}^n$: orthogonal group
quadratic form	$O_{p,q} \curvearrowright \mathbb{R}^n$: indefinite orth group
$\det X, \operatorname{trace} X$	$GL_n \curvearrowright M_n$: adjoint action
$\Delta(f), R(f,g)$	$SL_2 \curvearrowright \mathbb{C}[x,y]_n$

Here $GL_n = \{g : n \times n\text{-matrix} \mid \exists g^{-1} \iff \det g \neq 0\}$

$O_{p,q} = \{g \in GL_n \mid \|gx\|_{p,q} = \|x\|_{p,q}\} \quad (n = p + q)$

where $\|x\|_{p,q} = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$

$SL_n = \{g \in GL_n \mid \det g = 1\}$ example of reductive groups

Abstract setting

G : (linear) group $\curvearrowright X \subset \mathbb{C}^N$: algebraic action of G on X

Abstract setting

G : (linear) group $\curvearrowright X \subset \mathbb{C}^N$: algebraic action of G on X

Definition (algebraic action)

$\rho : G \times X \to X$: polynomial function s.t.

1. $\rho(e, x) = x$
2. $\rho(gh, x) = \rho(g, \rho(h, x))$

Notation: $g \cdot x = gx = \rho(g, x)$

Abstract setting

G : (linear) group $\curvearrowright X \subset \mathbb{C}^N$: algebraic action of G on X

Definition (algebraic action)

$\rho : G \times X \to X$: polynomial function s.t.

1. $\rho(e, x) = x$
2. $\rho(gh, x) = \rho(g, \rho(h, x))$

Notation: $g \cdot x = gx = \rho(g, x)$

Polynomial functions and invariants:

$\mathbb{C}[X] := \{f : X \to \mathbb{C} \mid f \text{ is polynomial function}\}$: ring of regular functions

$\mathbb{C}[X]^G := \{f \in \mathbb{C}[X] \mid f(g^{-1} \cdot x) = f(x) \ (\forall g \in G)\}$: ring of invariants

Abstract setting

G : (linear) group $\curvearrowright X \subset \mathbb{C}^N$: algebraic action of G on X

Definition (algebraic action)

$\rho : G \times X \to X$: polynomial function s.t.

1. $\rho(e, x) = x$
2. $\rho(gh, x) = \rho(g, \rho(h, x))$

Notation: $g \cdot x = gx = \rho(g, x)$

Polynomial functions and invariants:

$\mathbb{C}[X] := \{f : X \to \mathbb{C} \mid f \text{ is polynomial function}\}$: ring of regular functions

$\mathbb{C}[X]^G := \{f \in \mathbb{C}[X] \mid f(g^{-1} \cdot x) = f(x)\ (\forall g \in G)\}$: ring of invariants

functions which are constant along orbits

Abstract setting

G : (linear) group $\curvearrowright X \subset \mathbb{C}^N$: algebraic action of G on X

Definition (algebraic action)

$\rho : G \times X \to X$: polynomial function s.t.

1. $\rho(e, x) = x$
2. $\rho(gh, x) = \rho(g, \rho(h, x))$

Notation: $g \cdot x = gx = \rho(g, x)$

Polynomial functions and invariants:

$\mathbb{C}[X] := \{f : X \to \mathbb{C} \mid f \text{ is polynomial function}\}$: ring of regular functions

$\mathbb{C}[X]^G := \{f \in \mathbb{C}[X] \mid f(g^{-1} \cdot x) = f(x) \ (\forall g \in G)\}$: ring of invariants

functions which are constant along orbits

$\Longrightarrow$ $\mathbb{C}[X]^G$ is graded by degree of polynomials, i.e., graded algebra

Why invariants?

Why invariants?

As we saw, invariants are ubiquitos in mathematics

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$
  - orbits,

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$
  - orbits,
  - homogeneous spaces, or prehomogeneous spaces

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$
  - orbits,
  - homogeneous spaces, or prehomogeneous spaces
  - symmetric spaces, symmetric domains, etc.

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$
  - orbits,
  - homogeneous spaces, or prehomogeneous spaces
  - symmetric spaces, symmetric domains, etc.
- Harmonic analysis relative to the action $G \curvearrowright X$

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$
  - orbits,
  - homogeneous spaces, or prehomogeneous spaces
  - symmetric spaces, symmetric domains, etc.
- Harmonic analysis relative to the action $G \curvearrowright X$
  - invariant integral, or Haar measure

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$
  - orbits,
  - homogeneous spaces, or prehomogeneous spaces
  - symmetric spaces, symmetric domains, etc.
- Harmonic analysis relative to the action $G \curvearrowright X$
  - invariant integral, or Haar measure
  - invariant differential operators (Laplacian) and spherical functions

Why invariants?

As we saw, invariants are ubiquitos in mathematics
In particular...

- Classifying mathematical objects
- Understanding the original action $G \curvearrowright X$
  - orbits,
  - homogeneous spaces, or prehomogeneous spaces
  - symmetric spaces, symmetric domains, etc.
- Harmonic analysis relative to the action $G \curvearrowright X$
  - invariant integral, or Haar measure
  - invariant differential operators (Laplacian) and spherical functions
  - Fourier transform, etc.

Fundamental problems of invariant theory

Two classical problems ...

Fundamental problems of invariant theory

Two classical problems ...

1. Find the ring generators $\{\Delta_i\}_{i \in I} \subset \mathbb{C}[X]^G$
   Question : $\exists$ finite number of generators?
   Can choose a good basis?

   FFT = First Fundamental Theorem

Fundamental problems of invariant theory

Two classical problems ...

1. Find the ring generators $\{\Delta_i\}_{i \in I} \subset \mathbb{C}[X]^G$
   Question : $\exists$ finite number of generators?
   Can choose a good basis?

   FFT = First Fundamental Theorem

2. Find all the relations among $\{\Delta_i\}_{i \in I}$
   Question: transcending degree?
   singularities?

   SFT = Second Fundamental Theorem

Fundamental problems of invariant theory

Two classical problems ...

1. Find the ring generators $\{\Delta_i\}_{i\in I} \subset \mathbb{C}[X]^G$
   Question : $\exists$ finite number of generators?
   Can choose a good basis?

   FFT = First Fundamental Theorem

2. Find all the relations among $\{\Delta_i\}_{i\in I}$
   Question: transcending degree?
   singularities?

   SFT = Second Fundamental Theorem

There are many kinds of answers $\cdots$

Fundamental problems of invariant theory

Two classical problems ...

1. Find the ring generators $\{\Delta_i\}_{i\in I} \subset \mathbb{C}[X]^G$
   Question : $\exists$ finite number of generators?
   Can choose a good basis?

   FFT = First Fundamental Theorem

2. Find all the relations among $\{\Delta_i\}_{i\in I}$
   Question: transcending degree?
   singularities?

   SFT = Second Fundamental Theorem

There are many kinds of answers $\cdots$

Final Goal

Better understanding of $\mathbb{C}[X]^G$ in geometric terms.
Understanding of the original action $G \curvearrowright X$ through it.

Basic setting

G : reductive, linear algebraic group

Basic setting

G : reductive, linear algebraic group

Definition (algebraic group)

algebraic group = Zariski closed subgroup in $\mathrm{GL}_N(\mathbb{C})$

Zariski closed = solutions of the system of polynomial equations

Basic setting

G : reductive, linear algebraic group

Definition (algebraic group)

algebraic group = Zariski closed subgroup in $\mathrm{GL}_N(\mathbb{C})$

Zariski closed = solutions of the system of polynomial equations

Definition (reductive)

reductive group = nilpotent radical is trivial

(if $/k$, k being algebraically closed, char $k = 0$)

= $\forall$ finite dim representation is completely reducible

= $\forall$ finite dim repr is decomposed into the direct sum of irreducibles

V : reducible $\iff$ $V = U_1 \oplus U_2$ ($\exists U_i$: subrepresentation)

irreducibles = basi unit (atom) of representation

Reductive groups

Example (reductive groups)

$\mathbb{T} = (\mathbb{C}^\times)^m$: torus

GL_n, SL_n, O_n, $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$, Sp_{2n} : classical groups

G_2, F_4, E_6, E_7, E_8 : exceptional groups

Reductive groups

Example (reductive groups)

$\mathbb{T} = (\mathbb{C}^\times)^m$: torus

GL_n, SL_n, O_n, $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$, Sp_{2n} : classical groups

G_2, F_4, E_6, E_7, E_8 : exceptional groups

Also we have a general machinery to produce reductive groups

Reductive groups

Example (reductive groups)

$\mathbb{T} = (\mathbb{C}^\times)^m$: torus

GL_n, SL_n, O_n, $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$, Sp_{2n} : classical groups

G_2, F_4, E_6, E_7, E_8 : exceptional groups

Also we have a general machinery to produce reductive groups

Theorem

1. *Product of reductive groups is reductive*

Reductive groups

Example (reductive groups)

$\mathbb{T} = (\mathbb{C}^\times)^m$: torus
GL_n, SL_n, O_n, $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$, Sp_{2n} : classical groups
G_2, F_4, E_6, E_7, E_8 : exceptional groups

Also we have a general machinery to produce reductive groups

Theorem

1. *Product of reductive groups is reductive*
2. G : *reductive*, $H \subset G$: *normal* $\Longrightarrow$ G/H *reductive (quotient)*

Reductive groups

Example (reductive groups)

$\mathbb{T} = (\mathbb{C}^\times)^m$: torus

GL_n, SL_n, O_n, $\mathrm{SO}_n = \mathrm{O}_n \cap \mathrm{SL}_n$, Sp_{2n} : classical groups

G_2, F_4, E_6, E_7, E_8 : exceptional groups

Also we have a general machinery to produce reductive groups

Theorem

1. *Product of reductive groups is reductive*
2. G : *reductive*, $H \subset G$: *normal* $\implies$ G/H *reductive (quotient)*
3. G° : *reductive* $\implies$ G : *reductive* (G° : *identity component)*
   Extension by finite group ($\# G/G^\circ < \infty$)

Finite generation of invariants

Here is one of the best answer to FFT

Theorem (D. Hilbert 1990, 1993)

G : *reductive* $\curvearrowright$ $V = \mathbb{C}^n$: *vector space (linear repr)*
$\Longrightarrow$ $\mathbb{C}[V]^G$: *finitely generated algebra* $/\mathbb{C}$

Finite generation of invariants

Here is one of the best answer to FFT

Theorem (D. Hilbert 1990, 1993)

G : *reductive* $\curvearrowright$ $V = \mathbb{C}^n$: *vector space (linear repr)*

$\Longrightarrow$ $\mathbb{C}[V]^G$: *finitely generated algebra* $/\mathbb{C}$

Remark

$\exists$ counter example for non-reductive G

... Nagata (1959) : Hilbert's 14th problem

Recent work by Mukai (2005) ... Rich examples of finite generation even when G is not reductive

Example of actions of finite groups

$\# G < \infty \implies G$: reductive

$$\mathbb{C}[V]^G = \{R(f) \mid R(f)(x) = \frac{1}{\# G} \sum_{g \in G} f(g^{-1}x)\}$$

$R(f)$: Reynolds operator (projection to invariants)

Example of actions of finite groups

$\# G < \infty \implies G$: reductive

$$\mathbb{C}[V]^G = \{R(f) \mid R(f)(x) = \frac{1}{\# G} \sum_{g \in G} f(g^{-1}x)\}$$

$R(f)$: Reynolds operator (projection to invariants)

Theorem (E. Noether 1916)

$\mathbb{C}[V]^G$: *generated by polynomials of degree* $\leq \# G$

Example of actions of finite groups

$\# G < \infty \implies G$: reductive

$$\mathbb{C}[V]^G = \{R(f) \mid R(f)(x) = \frac{1}{\# G} \sum_{g \in G} f(g^{-1}x)\}$$

$R(f)$: Reynolds operator (projection to invariants)

Theorem (E. Noether 1916)

$\mathbb{C}[V]^G$: *generated by polynomials of degree* $\leq \# G$

Molien series : $\sum_{k=0}^{\infty} \dim(\mathbb{C}[V]_k^G)\, t^k = \frac{1}{\# G} \sum_{g \in G} \frac{1}{\det(1 - t\rho(g))}$

Example of actions of finite groups

$\#G < \infty \implies G$: reductive

$$\mathbb{C}[V]^G = \{R(f) \mid R(f)(x) = \frac{1}{\#G} \sum_{g \in G} f(g^{-1}x)\}$$

$R(f)$: Reynolds operator (projection to invariants)

Theorem (E. Noether 1916)

$\mathbb{C}[V]^G$: *generated by polynomials of degree* $\leq \#G$

Molien series : $\displaystyle\sum_{k=0}^{\infty} \dim(\mathbb{C}[V]^G_k)\, t^k = \frac{1}{\#G} \sum_{g \in G} \frac{1}{\det(1 - t\rho(g))}$

Theorem

G : *a finite reflection group*

$\{\Delta_1, \ldots, \Delta_l\} \subset \mathbb{C}[V]^G$: *minimal homogeneous generators*

$\implies \{d_k = \deg \Delta_k \mid 1 \leq k \leq l\}$: *uniquely determined (exponents)*

Rational invariants and Galois theory

Theorem

G : *finite group* $\Longrightarrow$ $\mathbb{C}(V)^G = Q(\mathbb{C}[V]^G)$: *quotient field* &

$$[\mathbb{C}(V) : \mathbb{C}(V)^G] = \# G$$

Rational invariants and Galois theory

Theorem

G : *finite group* $\Longrightarrow$ $\mathbb{C}(V)^G = Q(\mathbb{C}[V]^G)$: *quotient field* &

$$[\mathbb{C}(V) : \mathbb{C}(V)^G] = \# G$$

$\mathbb{C}(V)$: Galois extension of $\mathbb{C}(V)^G$ with Galois group G
i.e.,

Study of $\mathbb{C}[V]^G \leftrightarrow$ Galois theory for rings

Example: symmetric group action

$G = \mathfrak{S}_n \curvearrowright V = \mathbb{C}^n$: action by coordinate change

$\mathbb{C}[V]^G = \{\text{symmetric polynomials}\}$: invariants

Example: symmetric group action

$G = \mathfrak{S}_n \curvearrowright V = \mathbb{C}^n$: action by coordinate change

$\mathbb{C}[V]^G = \{\text{symmetric polynomials}\}$: invariants

Generators of the ring of invariants $\mathbb{C}[V]^G$:

- $\{$elementary symm fun $e_k (1 \leq k \leq n)\}$ $\quad \prod_{i=1}^{n} (1 + tx_i) = \sum_{k=0}^{n} e_k(x) t^k$

Example: symmetric group action

$G = \mathfrak{S}_n \curvearrowright V = \mathbb{C}^n$: action by coordinate change

$\mathbb{C}[V]^G = \{\text{symmetric polynomials}\}$: invariants

Generators of the ring of invariants $\mathbb{C}[V]^G$:

- $\{$elementary symm fun $e_k (1 \leq k \leq n)\}$ $\quad \prod_{i=1}^{n} (1 + t x_i) = \sum_{k=0}^{n} e_k(x) t^k$
- $\{$power sum $p_k (1 \leq k \leq n)\}$ $\quad p_k(x) = \sum_{i=1}^{n} x_i^k$

Example: symmetric group action

$G = \mathfrak{S}_n \curvearrowright V = \mathbb{C}^n$: action by coordinate change

$\mathbb{C}[V]^G = \{\text{symmetric polynomials}\}$: invariants

Generators of the ring of invariants $\mathbb{C}[V]^G$:

- {elementary symm fun $e_k (1 \leq k \leq n)$} $\prod_{i=1}^{n} (1 + tx_i) = \sum_{k=0}^{n} e_k(x) t^k$
- {power sum $p_k (1 \leq k \leq n)$} $p_k(x) = \sum_{i=1}^{n} x_i^k$
- {complete symm fun $h_k (1 \leq k \leq n)$} $\prod_{i=1}^{n} (1 - tx_i)^{-1} = \sum_{k=0}^{\infty} h_k(x) t^k$

Example: symmetric group action

$G = \mathfrak{S}_n \curvearrowright V = \mathbb{C}^n$: action by coordinate change

$\mathbb{C}[V]^G = \{\text{symmetric polynomials}\}$: invariants

Generators of the ring of invariants $\mathbb{C}[V]^G$:

- {elementary symm fun $e_k (1 \leq k \leq n)$} $\prod_{i=1}^{n}(1 + tx_i) = \sum_{k=0}^{n} e_k(x)t^k$
- {power sum $p_k (1 \leq k \leq n)$} $p_k(x) = \sum_{i=1}^{n} x_i^k$
- {complete symm fun $h_k (1 \leq k \leq n)$} $\prod_{i=1}^{n}(1 - tx_i)^{-1} = \sum_{k=0}^{\infty} h_k(x)t^k$

Exponents $\{1, 2, \ldots, n\}$

Gneretors are alegbraically independent

Example: symmetric group action (continued)

Define a qutient map $\Phi : V \to \mathbb{C}^n$ by $\Phi(v) = (e_1(v), e_2(v), \dots, e_n(v))$

Example: symmetric group action (continued)

Define a qutient map $\Phi : V \to \mathbb{C}^n$ by $\Phi(v) = (e_1(v), e_2(v), \ldots, e_n(v))$

Lemma

$\Phi : V \to \mathbb{C}^n$ is surjective & $\mathfrak{S}_n$-invariant
Every fiber $\Phi^{-1}(y)$ ($y \in \mathbb{C}^n$) is a single $\mathfrak{S}_n$-orbit

Example: symmetric group action (continued)

Define a qutient map $\Phi : V \to \mathbb{C}^n$ by $\Phi(v) = (e_1(v), e_2(v), \dots, e_n(v))$

Lemma

$\Phi : V \to \mathbb{C}^n$ is surjective & $\mathfrak{S}_n$-invariant
Every fiber $\Phi^{-1}(y)$ $(y \in \mathbb{C}^n)$ is a single $\mathfrak{S}_n$-orbit

Proof.

Φ surjective $\Leftarrow$ the fundamental theorem of algebra (Gauss's theorem)

i.e., giving $\forall$ coeff of the degree n equation,
$\exists$ n-solutions counting with multiplicity ($\Leftarrow$ fiber) □

Example: symmetric group action (continued)

Define a qutient map $\Phi : V \to \mathbb{C}^n$ by $\Phi(v) = (e_1(v), e_2(v), \ldots, e_n(v))$

Lemma

$\Phi : V \to \mathbb{C}^n$ is surjective & $\mathfrak{S}_n$-invariant
Every fiber $\Phi^{-1}(y)$ $(y \in \mathbb{C}^n)$ is a single $\mathfrak{S}_n$-orbit

Proof.

Φ surjective $\Leftarrow$ the fundamental theorem of algebra (Gauss's theorem)

i.e., giving $\forall$ coeff of the degree n equation,
$\exists$ n-solutions counting with multiplicity $(\Leftarrow$ fiber$)$ □

Thus we conclude $V/\mathfrak{S}_n \simeq \mathbb{C}^n$ via the quotient map Φ

$\Phi : V \to \mathbb{C}^n/\mathfrak{S}_n = \mathbb{C}^n$: generically $[\mathfrak{S}_n : 1]$ map (Galois covering)

Generic fiber $\simeq \mathfrak{S}_n$, inherits regular representation of $\mathfrak{S}_n$

Orthogonal invariants

$G = \mathrm{O}_n \curvearrowright V = \mathbb{C}^n$: vector representation (mult of matrix against vector)

Problem

Describe the invariants for $G \curvearrowright V \oplus \cdots \oplus V = V^{\oplus m}$

$U := \mathbb{C}^m \implies V^{\oplus m} \simeq V \otimes U \simeq \mathrm{M}_{n,m}$ coordinates x_{ij} on $\mathrm{M}_{n,m}$

Orthogonal invariants

$G = \mathrm{O}_n \curvearrowright V = \mathbb{C}^n$: vector representation (mult of matrix against vector)

Problem

Describe the invariants for $G \curvearrowright V \oplus \cdots \oplus V = V^{\oplus m}$

$U := \mathbb{C}^m \implies V^{\oplus m} \simeq V \otimes U \simeq \mathrm{M}_{n,m}$ coordinates x_{ij} on $\mathrm{M}_{n,m}$

FFT for orthogonal invariants:

Theorem (H. Weyl 1939)

$\mathbb{C}[V^{\oplus m}]^{\mathrm{O}_n} = \mathbb{C}[z_{ij} \mid 1 \leq i \leq j \leq m]$ *where* $z_{ij} = \sum_{k=1}^{n} x_{ki} x_{kj}$

$X = (x_{ij}) \in \mathrm{M}_{n,m} \implies Z = (z_{ij}) = {}^t X X \in \mathrm{Sym}_m$

Orthogonal invariants

$G = \mathrm{O}_n \curvearrowright V = \mathbb{C}^n$: vector representation (mult of matrix against vector)

Problem

Describe the invariants for $G \curvearrowright V \oplus \cdots \oplus V = V^{\oplus m}$

$U := \mathbb{C}^m \implies V^{\oplus m} \simeq V \otimes U \simeq \mathrm{M}_{n,m}$ coordinates x_{ij} on $\mathrm{M}_{n,m}$

FFT for orthogonal invariants:

Theorem (H. Weyl 1939)

$\mathbb{C}[V^{\oplus m}]^{\mathrm{O}_n} = \mathbb{C}[z_{ij} \mid 1 \leq i \leq j \leq m]$ *where* $z_{ij} = \sum_{k=1}^{n} x_{ki}x_{kj}$

$X = (x_{ij}) \in \mathrm{M}_{n,m} \implies Z = (z_{ij}) = {}^tXX \in \mathrm{Sym}_m$

Example

$m = 1$: $\mathbb{C}[V]^{\mathrm{O}_n} = \mathbb{C}[\xi]$ $\xi = x_1^2 + \cdots + x_n^2$

Contraction invariants

$G = \mathrm{GL}_n \curvearrowright V = \mathbb{C}^n \implies \mathbb{C}[V^{\oplus m}]^G = \mathbb{C}$: trivial (NO invariants)

Contraction invariants

$G = \mathrm{GL}_n \curvearrowright V = \mathbb{C}^n \implies \mathbb{C}[V^{\oplus m}]^G = \mathbb{C}$: trivial (NO invariants)

Right setting using V^* : contragredient (= dual) of V

Problem

Describe invariants for $G \curvearrowright V^{\oplus p} \oplus V^{*\oplus q}$

$U := \mathbb{C}^p, U' := \mathbb{C}^q \implies V^{\oplus p} \oplus V^{*\oplus q} \simeq V \otimes U \oplus V^* \otimes U' \simeq \mathrm{M}_{n,p} \oplus \mathrm{M}_{n,q}$

coordinates x_{ij} on $\mathrm{M}_{n,p}$, y_{ij} on $\mathrm{M}_{n,q}$

Contraction invariants

$G = \mathrm{GL}_n \curvearrowright V = \mathbb{C}^n \implies \mathbb{C}[V^{\oplus m}]^G = \mathbb{C}$: trivial (NO invariants)

Right setting using V^* : contragredient ($=$ dual) of V

Problem

Describe invariants for $G \curvearrowright V^{\oplus p} \oplus V^{*\oplus q}$

$U := \mathbb{C}^p, U' := \mathbb{C}^q \implies V^{\oplus p} \oplus V^{*\oplus q} \simeq V \otimes U \oplus V^* \otimes U' \simeq \mathrm{M}_{n,p} \oplus \mathrm{M}_{n,q}$

coordinates x_{ij} on $\mathrm{M}_{n,p}$, y_{ij} on $\mathrm{M}_{n,q}$

FFT for contraction invariants:

Theorem (H. Weyl 1939)

$\mathbb{C}[V^{\oplus p} \oplus V^{*\oplus q}]^{\mathrm{GL}_n} = \mathbb{C}[z_{ij} \mid 1 \leq i \leq p, 1 \leq j \leq q]$ *where*

$z_{ij} = \sum_{k=1}^{n} x_{ki} y_{kj}$: *contraction of X and Y*

$X = (x_{ij}) \in \mathrm{M}_{n,p}, Y = (y_{ij}) \in \mathrm{M}_{n,q} \implies Z = (z_{ij}) = {}^t XY \in \mathrm{M}_{p,q}$

Second Fundamental Theorem = SFT

describing relations among generators ...

Second Fundamental Theorem = SFT

describing relations among generators ... easiest case is:

Second Fundamental Theorem = SFT

describing relations among generators ... easiest case is:

Theorem (Shephard-Todd 1954)

Assume $\#G < \infty$, $G \curvearrowright V$: *linear representation*
$\mathbb{C}[V]^G$ *is a polynomial ring (no relations)*
$\iff$ G *is a pseudo-reflection group*

Remark

s : pseudo-reflection $= \exists U \subset V$: $(n-1)$-dim s.t. $s\big|_U = \mathrm{id}_U$
pseudo-reflection group = finite group generated by pseudo-reflections

Second Fundamental Theorem = SFT

describing relations among generators ... easiest case is:

Theorem (Shephard-Todd 1954)

Assume $\#G < \infty$, $G \curvearrowright V$: *linear representation*
$\mathbb{C}[V]^G$ *is a polynomial ring (no relations)*
$\iff$ G *is a pseudo-reflection group*

Remark

s : pseudo-reflection $= \exists U \subset V$: $(n-1)$-dim s.t. $s\big|_U = \mathrm{id}_U$
pseudo-reflection group = finite group generated by pseudo-reflections

If $\exists$ relations, what we can do? Namely

Problem

How to describe relations among generators?

Return to the general situation $G \curvearrowright X \qquad (X \subset \mathbb{C}^N)$
G : reductive ; X : affine variety (solutions of polynomial equations)

$\{\Delta_1, \ldots, \Delta_m\} \subset \mathbb{C}[X]^G$: generators of invariants

Return to the general situation $G \curvearrowright X \qquad (X \subset \mathbb{C}^N)$
G : reductive ; X : affine variety (solutions of polynomial equations)

$\{\Delta_1, \ldots, \Delta_m\} \subset \mathbb{C}[X]^G$: generators of invariants $\Longrightarrow$
Algebra morphism:

$$\Phi^* : \mathbb{C}[y_1, \ldots, y_m] \ni F(\mathbf{y}) \mapsto F(\Delta_1, \ldots, \Delta_m) \in \mathbb{C}[X]^G$$

$\exists$ relation $F(\Delta_1, \ldots, \Delta_m) \equiv 0 \iff F(\mathbf{y}) \in \operatorname{Ker} \Phi^* =: I$
i.e., $I = \operatorname{Ker} \Phi^* \subset \mathbb{C}[\mathbf{y}]$ describes relations completely

Return to the general situation $G \curvearrowright X \qquad (X \subset \mathbb{C}^N)$
G : reductive ; X : affine variety (solutions of polynomial equations)

$\{\Delta_1, \dots, \Delta_m\} \subset \mathbb{C}[X]^G$: generators of invariants $\Longrightarrow$
Algebra morphism:

$$\Phi^* : \mathbb{C}[y_1, \dots, y_m] \ni F(\mathbf{y}) \mapsto F(\Delta_1, \dots, \Delta_m) \in \mathbb{C}[X]^G$$

$\exists$ relation $F(\Delta_1, \dots, \Delta_m) \equiv 0 \iff F(\mathbf{y}) \in \operatorname{Ker} \Phi^* =: I$
i.e., $I = \operatorname{Ker} \Phi^* \subset \mathbb{C}[\mathbf{y}]$ describes relations completely

Theorem (Hilbert's basis theorem)

$\forall$ *ideal* $I \subset \mathbb{C}[\mathbf{y}]$ *admits finite # of generators* $\{F_1, \dots, F_\ell\}$

Notation

$I = (F_1, \dots, F_\ell) = \sum_{j=1}^{\ell} \mathbb{C}[\mathbf{y}] F_j$: ideal generated by $\{F_1, \dots, F_\ell\}$

SFT describes the generators of relations $\{F_1, \dots, F_\ell\}$ completely, which are satisfied by invariants $\{\Delta_1, \dots, \Delta_m\}$

SFT describes the generators of relations $\{F_1, \dots, F_\ell\}$ completely, which are satisfied by invariants $\{\Delta_1, \dots, \Delta_m\}$

Example (orthogonal invariants)

Recall $G = \mathrm{O}_n \curvearrowright V^{\oplus m} \simeq \mathrm{M}_{n,m} \quad (V = \mathbb{C}^n)$
coordinates x_{ij} on $\mathrm{M}_{n,m} \implies$ orthog invariants : $z_{ij} = \sum_{k=1}^{n} x_{ki} x_{kj}$
$X = (x_{ij}) \in \mathrm{M}_{n,m} \implies Z = (z_{ij}) = {}^t XX \in \mathrm{Sym}_m$

1. $m \leq n \implies \{z_{ij}\}$: alg independent (no relation)

SFT describes the generators of relations $\{F_1, \ldots, F_\ell\}$ completely, which are satisfied by invariants $\{\Delta_1, \ldots, \Delta_m\}$

Example (orthogonal invariants)

Recall $G = \mathrm{O}_n \curvearrowright V^{\oplus m} \simeq \mathrm{M}_{n,m} \quad (V = \mathbb{C}^n)$
coordinates x_{ij} on $\mathrm{M}_{n,m} \implies$ orthog invariants : $z_{ij} = \sum_{k=1}^{n} x_{ki} x_{kj}$
$X = (x_{ij}) \in \mathrm{M}_{n,m} \implies Z = (z_{ij}) = {}^t XX \in \mathrm{Sym}_m$

1. $m \leq n \implies \{z_{ij}\}$: alg independent (no relation)
2. $m > n \implies Z = (z_{ij})$ is of rank n
   (i.e., relations are $(n+1)$-th minors in Sym_m)

Geometric point of view

$I \subset \mathbb{C}[\mathbf{y}]$: ideal of relations (prime)

$$\longleftrightarrow Y = \{\mathbf{y} \in \mathbb{C}^m \mid F(\mathbf{y}) = 0 \ (\forall F \in I)\} \subset \mathbb{C}^m$$: variety

Geometric point of view

$I \subset \mathbb{C}[\mathbf{y}]$: ideal of relations (prime)

$$\longleftrightarrow Y = \{\mathbf{y} \in \mathbb{C}^m \mid F(\mathbf{y}) = 0 \ (\forall F \in I)\} \subset \mathbb{C}^m \ : \ \text{variety}$$

Key theorem:

Theorem (Hilbert's Nullstellensatz)

$$(\textit{reduced ideals in } \mathbb{C}[\mathbf{y}]) \ni I \overset{\text{biject}}{\longleftrightarrow} Y \in (\textit{zero pt sets of polynomial equations}) = (\textit{Z closed sets}) \subset \mathbb{C}^m$$

Geometric point of view

$I \subset \mathbb{C}[\mathbf{y}]$: ideal of relations (prime)

$$\longleftrightarrow Y = \{\mathbf{y} \in \mathbb{C}^m \mid F(\mathbf{y}) = 0 \ (\forall F \in I)\} \subset \mathbb{C}^m \ : \text{ variety}$$

Key theorem:

Theorem (Hilbert's Nullstellensatz)

$$(\textit{reduced ideals in } \mathbb{C}[\mathbf{y}]) \ni I \overset{\text{biject}}{\longleftrightarrow}$$
$$Y \in (\textit{zero pt sets of polynomial equations}) = (\textit{Z closed sets}) \subset \mathbb{C}^m$$

- $I = \mathbb{I}(Y) = \{F \in \mathbb{C}[\mathbf{y}] \mid F\big|_Y \equiv 0\} \subset \mathbb{C}[\mathbf{y}]$
- $Y = \mathbb{V}(I) = \{\mathbf{y} \in \mathbb{C}^m \mid F(\mathbf{y}) = 0 \quad (\forall F \in I)\} \subset \mathbb{C}^m$

Geometric point of view

$I \subset \mathbb{C}[\mathbf{y}]$: ideal of relations (prime)

$$\longleftrightarrow Y = \{\mathbf{y} \in \mathbb{C}^m \mid F(\mathbf{y}) = 0 \ (\forall F \in I)\} \subset \mathbb{C}^m \ : \text{variety}$$

Key theorem:

Theorem (Hilbert's Nullstellensatz)

$(\textit{reduced ideals in } \mathbb{C}[\mathbf{y}]) \ni I \overset{\text{biject}}{\longleftrightarrow}$

$$Y \in (\textit{zero pt sets of polynomial equations}) = (\textit{Z closed sets}) \subset \mathbb{C}^m$$

- $I = \mathbb{I}(Y) = \{F \in \mathbb{C}[\mathbf{y}] \mid F\big|_Y \equiv 0\} \subset \mathbb{C}[\mathbf{y}]$
- $Y = \mathbb{V}(I) = \{\mathbf{y} \in \mathbb{C}^m \mid F(\mathbf{y}) = 0 \quad (\forall F \in I)\} \subset \mathbb{C}^m$

I : *prime ideal* $\longleftrightarrow$ Y : *irreducible*

$$(\text{i.e., } Y = Y_1 \cup Y_2 \ (Y_i : \text{Z closed}) \implies Y = Y_1 \text{ or } Y = Y_2)$$

Conclusion:

SFT = describe algebraic variety defined by relations among invariants

To be continued...