Invariant Theory of Finite Groups

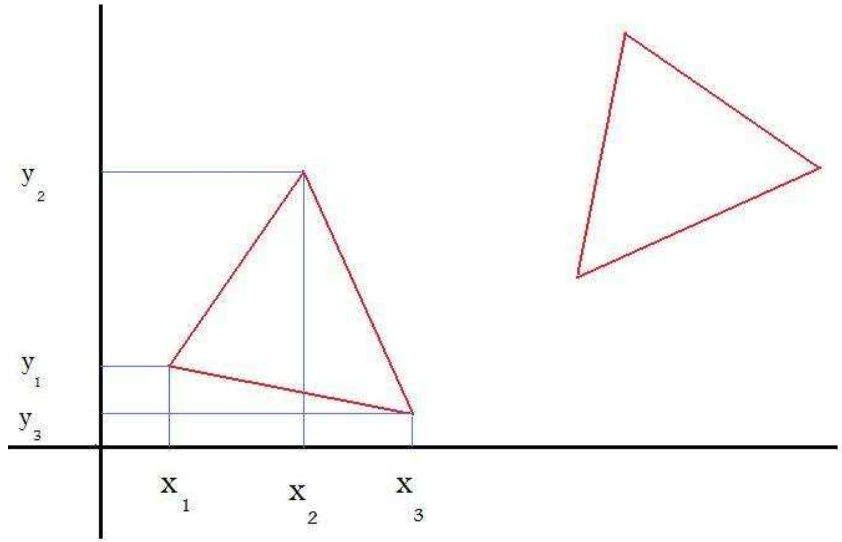
Peter Fleischmann

School of Mathematics, Statistics and Actuarial Science

University of Kent

London, October 2009

Geometric Background



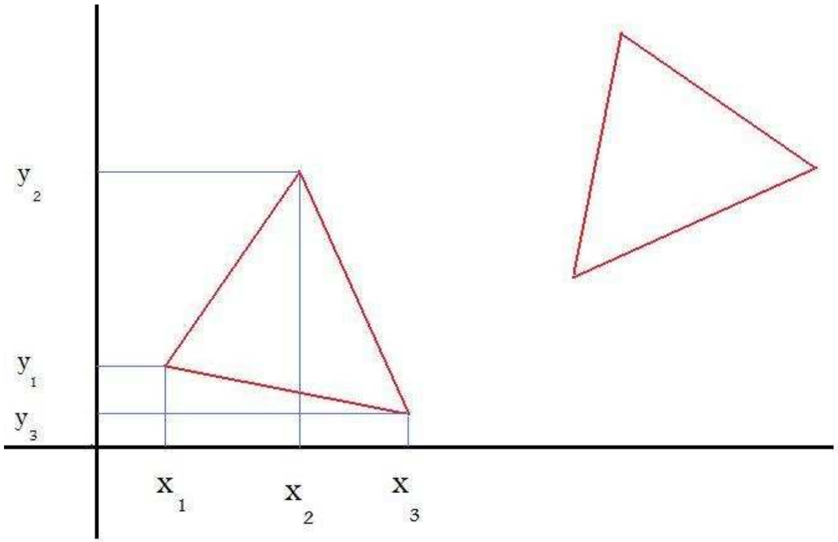
- Description of object by "coordinates";

  "geometric properties" are "invariants" under a group action;

  e.g. translations/rotations.

  described by "invariant functions" e.g.

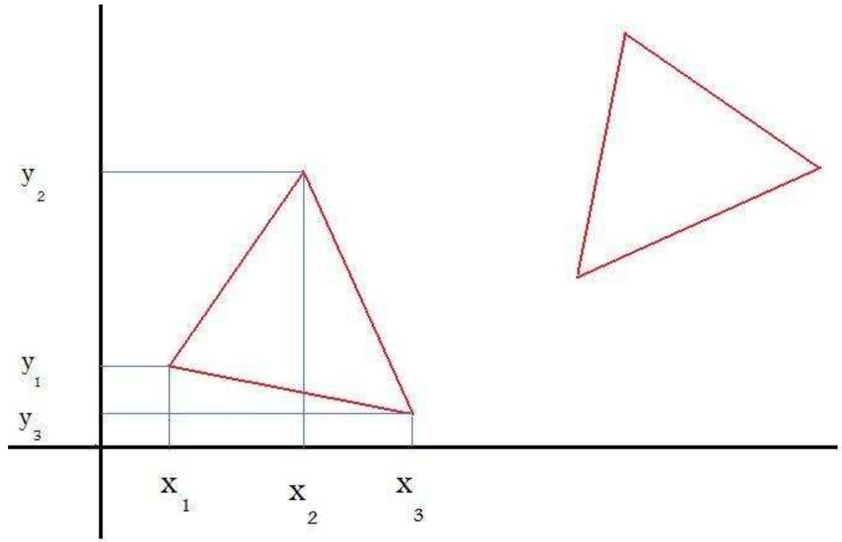
Geometric Background



$$s_{ij}(\mathbf{x},\mathbf{y}) := \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}, \text{ or}$$

$$f(\mathbf{x},\mathbf{y}) = 1/2 \cdot \det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix}.$$

Geometric Background



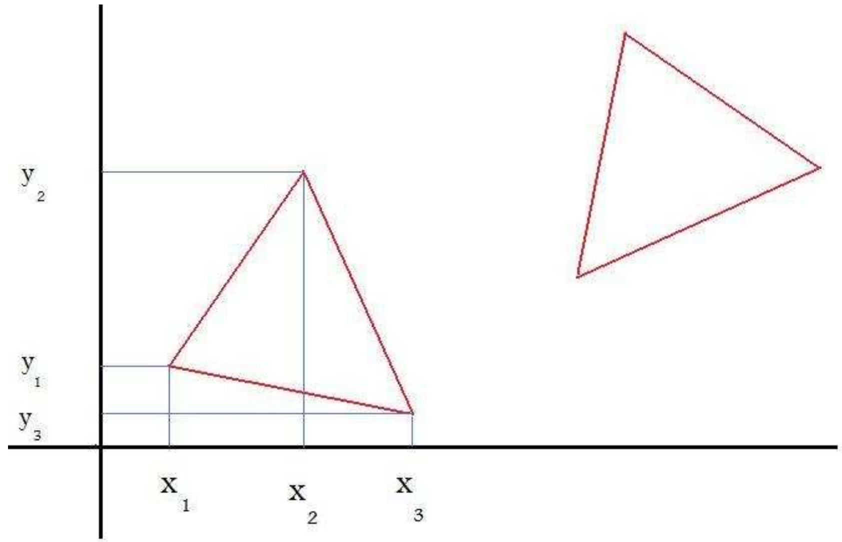
Geometric space described as affine variety:

$\mathbf{V} := \{\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{C}^n \mid f_1(\mathbf{x}) = \cdots = f_m(\mathbf{x}) = 0\}$,

with $f_i \in \mathbb{C}[X_1, \cdots, X_n]$.

Ring of polynomial functions on $\mathbf{V}$:
$A := \mathbb{C}[\mathbf{X}]/(f_1, \cdots, f_m)$, "affine algebra".

Geometric Background

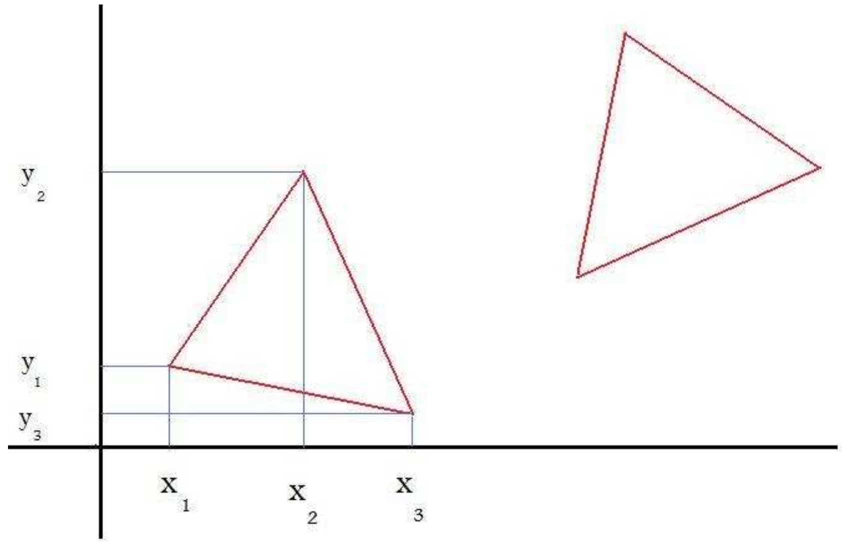


$$\mathbf{V} := \{\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{C}^n \mid f_1(\mathbf{x}) = \cdots = f_m(\mathbf{x}) = 0\},$$

$A := \mathbb{C}[\mathbf{X}]/(f_1, \cdots, f_m)$, "affine algebra".

- $A^G := \{a \in A \mid ga = a \circ g^{-1} = a, \ \forall g \in G\}$.
  Ring of invariants under transformation group G.
  Invariants "measure geometric properties".

Geometric Background



- Algebraic Geometry: dual point of view

  $\mathbf{x} \in \mathbf{V} \leftrightarrow (X_i - x_i \,|i = 1, \cdots, n) \trianglelefteq A$ maximal ideal

  $\mathbf{V} := \max - \mathrm{spec}(A)$

  Geometric objects:

  $\max - \mathrm{spec}(A^G) = V//G$, "categorical quotient".

Geometric Setup

$A :=$ affine algebra over field $\mathbb{F} = \overline{\mathbb{F}}$;

$\mathbf{V} := \mathrm{max} - \mathrm{spec}\ A$, corresponding affine variety;

G group of automorphisms on A with

$$\textbf{ring of invariants}\ A^G := \{a \in A \mid g(a) = a\ \forall\ g \in G\}.$$

Geometric Setup

$A :=$ affine algebra over field $\mathbb{F} = \overline{\mathbb{F}}$;

$\mathbf{V} := \max - \operatorname{spec} A$, corresponding affine variety;

G group of automorphisms on A with

$$\textbf{ring of invariants } A^G := \{a \in A \mid g(a) = a \; \forall \; g \in G\}.$$

When is $\mathbf{V}//G := \max - \operatorname{spec} A^G$ an affine variety?

Geometric Setup

$A :=$ affine algebra over field $\mathbb{F} = \overline{\mathbb{F}}$;

$\mathbf{V} := \mathrm{max} - \mathrm{spec}\ A$, corresponding affine variety;

G group of automorphisms on A with

$$\textbf{ring of invariants } A^G := \{a \in A \mid g(a) = a \;\forall\; g \in G\}.$$

When is $\mathbf{V}//G := \mathrm{max} - \mathrm{spec}\ A^G$ an affine variety?

Necessary condition:

A^G **finitely generated** over $\mathbb{F}$.

Hilbert's 14' th problem

In case $\mathbb{F} = \mathbb{C}$ and $G \leq Gl_n(\mathbb{C})$ this was posed by **Hilbert** (1'st It'l Congress, Paris 1900).

Hilbert's 14' th problem

In case $\mathbb{F} = \mathbb{C}$ and $G \leq Gl_n(\mathbb{C})$ this was posed by **Hilbert** (1'st It'l Congress, Paris 1900).

- Answer **no** in general:
  (1958) Nagata (counter example $G \leq (\mathbb{C}^+)^m$).

Hilbert's 14' th problem

In case $\mathbb{F} = \mathbb{C}$ and $G \leq Gl_n(\mathbb{C})$ this was posed by **Hilbert** (1'st It'l Congress, Paris 1900).

- Answer **no** in general:
  (1958) Nagata (counter example $G \leq (\mathbb{C}^+)^m$).
- Answer **yes** in important special cases
  - 'linear reductive groups' e.g. $Gl_n(\mathbb{C}), SL_n(\mathbb{C}) \ldots$
    (Cayley, Sylvester, Gordan, Hilbert, Weyl.)
  - finite groups, $\mathbb{F}$ arbitrary (Emmy Noether (1926))

Hilbert's 14' th problem

In case $\mathbb{F} = \mathbb{C}$ and $G \leq Gl_n(\mathbb{C})$ this was posed by **Hilbert** (1'st It'l Congress, Paris 1900).

- Answer **no** in general:
  (1958) Nagata (counter example $G \leq (\mathbb{C}^+)^m$).
- Answer **yes** in important special cases
  - 'linear reductive groups' e.g. $Gl_n(\mathbb{C}), SL_n(\mathbb{C}) \ldots$ (Cayley, Sylvester, Gordan, Hilbert, Weyl.)
  - finite groups, $\mathbb{F}$ arbitrary (Emmy Noether (1926))

Theorem:

If G is finite, then A^G is finitely generated and the categorical quotient is in bijection with the orbit space.

$$\mathbf{V}/G \cong \mathbf{V}//G.$$

Notation

From now on always: G **finite group**

V a finite dimensional $\mathbb{F}G$ - module,

V^* dual module with basis $x_1, \cdots, x_n$,

$A = \mathrm{Sym}(V^*) \cong \mathbb{F}[x_1, \cdots, x_n] =: \mathbb{F}[V]$, polynomial ring;

$$A^G := \{a \in A \mid g(a) = a, \ \forall g \in G\}, (\mathbb{N}_0 - \mathrm{graded})$$

ring of polynomial invariants.

Notation

From now on always: G **finite group**

V a finite dimensional $\mathbb{F}G$ - module,

V^* dual module with basis $x_1, \cdots, x_n$,

$A = \mathrm{Sym}(V^*) \cong \mathbb{F}[x_1, \cdots, x_n] =: \mathbb{F}[V]$, polynomial ring;

$$A^G := \{a \in A \mid g(a) = a,\ \forall g \in G\}, (\mathbb{N}_0 - \text{graded})$$

ring of polynomial invariants.

- left/ right - action:

$$g \cdot a := a \cdot g^{-1}.$$

Examples

Symmetric polynomials:
$G := \Sigma_n$, permuting the variables $x_1, \cdots, x_n$,

$A^G = \mathbb{F}[e_1, \cdots, e_n]$, polynomial ring
generated by elementary symmetric functions

$$e_i = \sum_{1 \leq j_1 < j_2 < \cdots < j_i < n} x_{j_1} x_{j_2} \cdots x_{j_i}.$$

Examples

Symmetric polynomials:
$G := \Sigma_n$, permuting the variables $x_1, \cdots, x_n$,

$A^G = \mathbb{F}[e_1, \cdots, e_n]$, polynomial ring
generated by elementary symmetric functions

$$e_i = \sum_{1 \leq j_1 < j_2 < \cdots < j_i < n} x_{j_1} x_{j_2} \cdots x_{j_i}.$$

$G = \langle g \rangle \cong \mathbb{Z}_2$, $A := \mathbb{R}[X, Y]$ with $g(X) = -X, \; g(Y) = -Y.$

$$A^G = \mathbb{R}[X^2, Y^2, XY] \cong \mathbb{F}[S, T, U]/(ST - U^2).$$

Not a polynomial ring! (Why?)

Examples

Symmetric polynomials:
$G := \Sigma_n$, permuting the variables $x_1, \cdots, x_n$,

$A^G = \mathbb{F}[e_1, \cdots, e_n]$, polynomial ring
generated by elementary symmetric functions

$$e_i = \sum_{1 \leq j_1 < j_2 < \cdots < j_i < n} x_{j_1} x_{j_2} \cdots x_{j_i}.$$

$G = \langle g \rangle \cong \mathbb{Z}_2$, $A := \mathbb{R}[X, Y]$ with $g(X) = -X,\ g(Y) = -Y.$

$$A^G = \mathbb{R}[X^2, Y^2, XY] \cong \mathbb{F}[S, T, U]/(ST - U^2).$$

Not a polynomial ring! (Why?) $X^2Y^2 = (XY)^2$

Examples

Symmetric polynomials:
$G := \Sigma_n$, permuting the variables $x_1, \cdots, x_n$,

$A^G = \mathbb{F}[e_1, \cdots, e_n]$, polynomial ring
generated by elementary symmetric functions

$$e_i = \sum_{1 \leq j_1 < j_2 < \cdots < j_i < n} x_{j_1} x_{j_2} \cdots x_{j_i}.$$

$G = \langle g \rangle \cong \mathbb{Z}_2$, $A := \mathbb{R}[X, Y]$ with $g(X) = -X,\ g(Y) = -Y.$

$$A^G = \mathbb{R}[X^2, Y^2, XY] \cong \mathbb{F}[S, T, U]/(ST - U^2).$$

Not a polynomial ring! (Why?) $X^2Y^2 = (XY)^2$
non - unique factorization with irreducibles X^2, Y^2 and XY in $\mathbb{R}[X, Y]^G$.
Hence A^G is not a UFD.

Examples

Symmetric polynomials:
$G := \Sigma_n$, permuting the variables $x_1, \cdots, x_n$,

$A^G = \mathbb{F}[e_1, \cdots, e_n]$, polynomial ring
generated by elementary symmetric functions

$$e_i = \sum_{1 \le j_1 < j_2 < \cdots < j_i < n} x_{j_1} x_{j_2} \cdots x_{j_i}.$$

$G = \langle g \rangle \cong \mathbb{Z}_2$, $A := \mathbb{R}[X, Y]$ with $g(X) = -X,\ g(Y) = -Y$.

$$A^G = \mathbb{R}[X^2, Y^2, XY] \cong \mathbb{F}[S, T, U]/(ST - U^2).$$

Not a polynomial ring! (Why?) $X^2Y^2 = (XY)^2$

However: Let $\mathfrak{P} := \mathbb{R}[X^2, Y^2]$, then $A^G = \mathfrak{P} \cdot 1 \oplus \mathfrak{P} \cdot XY$,
free of rank 2 over polynomial ring $\mathfrak{P}$.

Noether's normalization theorem

Let R be $\mathbb{N}_0$-graded affine algebra, with $R_0 = \mathbb{F}$ (e.g. $R = A^G$).
For $h_1, \cdots, h_d \in R^+$ homogeneous **t.f.a.e.**:

1. $\dim_{\mathbb{F}} (R/(h_1, \cdots, h_d)R) < \infty$ with d minimal;
2. $\mathfrak{P} = \mathbb{F}[h_1, \cdots, h_d]$ is polynomial subring, such that the **module** ${}_{\mathfrak{P}}R$ is finitely generated.

Noether's normalization theorem

Let R be $\mathbb{N}_0$-graded with $R_0 = \mathbb{F}$ (e.g. $R = A^G$).
For $h_1, \cdots, h_d \in R^+$ homogeneous **t.f.a.e.**:

1. $\dim_{\mathbb{F}} (R/(h_1, \cdots, h_d)R) < \infty$ with d minimal;
2. $\mathfrak{P} = \mathbb{F}[h_1, \cdots, h_d]$ is polynomial subring, such that the **module** ${}_{\mathfrak{P}}R$ is finitely generated.

In this case $\{h_1, \cdots, h_d\}$ form a
homogeneous system of parameters (hsop).
$d :=$ **Krull-dimension** of R $(\mathrm{Dim}(R))$.

Noether's normalization theorem

Let R be $\mathbb{N}_0$-graded with $R_0 = \mathbb{F}$ (e.g. $R = A^G$).
For $h_1, \cdots, h_d \in R^+$ homogeneous **t.f.a.e.**:

1. $\dim_{\mathbb{F}} (R/(h_1, \cdots, h_d)R) < \infty$ with d minimal;
2. $\mathfrak{P} = \mathbb{F}[h_1, \cdots, h_d]$ is polynomial subring, such that the **module** ${}_{\mathfrak{P}}R$ is finitely generated.

In this case $\{h_1, \cdots, h_d\}$ form a *homogeneous system of parameters (hsop)*.
$d :=$ **Krull-dimension** of R $(\mathrm{Dim}(R))$.
If $R = \langle s_1, s_2, \cdots, s_k \rangle_{\mathfrak{P}}$, then

- *primary generators*: $h_1, \cdots, h_d$.
- *secondary generators*: $s_1, \cdots, s_k$.

General Questions

I. Constructive Complexity of A^G

generators and relations for algebra A^G
(fundamental systems of invariants)
degree bounds (for generators and/or relations)

General Questions

I. Constructive Complexity of A^G

generators and relations for algebra A^G
(fundamental systems of invariants)
degree bounds (for generators and/or relations)

II. Structural complexity of A^G

when is A^G polynomial ring?
distance of A^G from being a polynomial ring
distance of A^G from being free as module over hsop
cohomological co - dimension: $\mathrm{depth}(A^G)$

General Questions

I. Constructive Complexity of A^G

generators and relations for algebra A^G
(fundamental systems of invariants)
degree bounds (for generators and/or relations)

II. Structural complexity of A^G

when is A^G polynomial ring?
distance of A^G from being a polynomial ring
distance of A^G from being free as module over hsop
cohomological co - dimension: $\mathrm{depth}(A^G)$

As in representation theory:

$\mathrm{char}\,\mathbb{F} \not| \, |G| \iff \mathrm{non-modular\ case}$;
$\mathrm{char}\,\mathbb{F} \mid |G| \iff \mathrm{modular\ case}$.

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g \in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell} T^\ell \in A^G[T]$.

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g \in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell} T^\ell \in A^G[T]$.

Define $B := \mathbb{F}[b_{i,\ell} \mid i = 1, \ldots, d,\ \ell = 0, \ldots, n-1]$.

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g \in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell} T^\ell \in A^G[T]$.

Define $B := \mathbb{F}[b_{i,\ell} \mid i = 1, \ldots, d,\ \ell = 0, \ldots, n-1]$.

- B is a noetherian $\mathbb{F}$ - algebra (Hilbert's theorem)

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g \in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell} T^\ell \in A^G[T]$.

Define $B := \mathbb{F}[b_{i,\ell} \mid i = 1, \ldots, d, \ \ell = 0, \ldots, n-1]$.

- B is a noetherian $\mathbb{F}$ - algebra (Hilbert's theorem)

  $B \leq A$ is finite integral extension;

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g \in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell}T^\ell \in A^G[T]$.

Define $B := \mathbb{F}[b_{i,\ell} \mid i = 1, \ldots, d,\ \ell = 0, \ldots, n-1]$.

- B is a noetherian $\mathbb{F}$ - algebra (Hilbert's theorem)

  $B \leq A$ is finite integral extension;

  $A = \langle \prod_{i=1}^d x_i^{m_i} \mid m_i < n \rangle_B$ (since $f_i(x_i) = 0$);

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g \in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell} T^\ell \in A^G[T]$.

Define $B := \mathbb{F}[b_{i,\ell} \mid i = 1, \ldots, d,\ \ell = 0, \ldots, n-1]$.

- B is a noetherian $\mathbb{F}$ - algebra (Hilbert's theorem)

  $B \leq A$ is finite integral extension;

  $A = \langle \prod_{i=1}^d x_i^{m_i} \mid m_i < n \rangle_B$ (since $f_i(x_i) = 0$);

  $\Rightarrow {}_B A$ is a finitely generated, so a noetherian B - module;

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g\in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell}T^\ell \in A^G[T]$.

Define $B := \mathbb{F}[b_{i,\ell} \mid i = 1, \ldots, d,\ \ell = 0, \ldots, n-1]$.

- B is a noetherian $\mathbb{F}$ - algebra (Hilbert's theorem)

  $B \leq A$ is finite integral extension;

  $A = \langle \prod_{i=1}^d x_i^{m_i} \mid m_i < n\rangle_B$ (since $f_i(x_i) = 0$);

  $\Rightarrow {}_BA$ is a finitely generated, so a noetherian B - module;
- submodules of noetherian modules are finitely generated;

Noether's theorem

Theorem (Emmy Noether (1926)): If G is a finite group, then A^G is a finitely generated $\mathbb{F}$-algebra.

Proof:

Let $A := \mathbb{F}[x_1, \ldots, x_d]$ and $|G| = n$.For $i = 1, \ldots, d$ set $f_i := \prod_{g \in G}(T - gx_i) = T^n + \sum_{\ell=0}^{n-1} b_{i,\ell} T^\ell \in A^G[T]$.

Define $B := \mathbb{F}[b_{i,\ell} \mid i = 1, \ldots, d, \ \ell = 0, \ldots, n-1]$.

- B is a noetherian $\mathbb{F}$ - algebra (Hilbert's theorem)

  $B \leq A$ is finite integral extension;

  $A = \langle \prod_{i=1}^{d} x_i^{m_i} \mid m_i < n \rangle_B$ (since $f_i(x_i) = 0$);

  $\Rightarrow {}_BA$ is a finitely generated, so a noetherian B - module;
- submodules of noetherian modules are finitely generated;

  $A^G \leq \ {}_BA$, hence a finitely generated B-module.

Remarks on Noether's theorem

- The subring B of A^G is generated by the coefficients $b_{i,\ell}$ of the polynomials

  $$(T - g_1(x_i))(T - g_2(x_i)) \ldots (T - g_n(x_i)) \in A^G[T]$$

  having degrees less or equal to $|G|$, and

  $$A = \langle x_1^{b_1} x_2^{b_2} \ldots x_d^{b_d} \mid b_i < \max(2, |G|) \rangle_B.$$

Remarks on Noether's theorem

- The subring B of A^G is generated by the coefficients $b_{i,\ell}$ of the polynomials

$$(T - g_1(x_i))(T - g_2(x_i)) \dots (T - g_n(x_i)) \in A^G[T]$$

having degrees less or equal to $|G|$, and

$$A = \langle x_1^{b_1} x_2^{b_2} \dots x_d^{b_d} \mid b_i < \max(2, |G|) \rangle_B.$$

- We know $A^G = \langle a_1, \cdots, a_m \rangle_B$ with $a_i \in A^G$, so

$$A^G = \mathbb{F}[b_{i,\ell}, a_s \mid i = 1, \dots, d,\ \ell = 0, \dots, g_i - 1,\ s = 1, \dots, m]$$

but the previous arguments do not tell us how to construct the *module-generators* $a_1, \dots, a_m$.

Remarks on Noether's theorem

Suppose $|G| \in \mathbb{F}^*$. Then the **transfer map**

$$\mathrm{tr} : A \longrightarrow A^G, a \mapsto \sum_{g \in G} g(a)$$

is a surjective homomorphism of A^G - modules.

Remarks on Noether's theorem

Suppose $|G| \in \mathbb{F}^*$. Then the **transfer map**

$$\mathrm{tr} : A \longrightarrow A^G, a \mapsto \sum_{g \in G} g(a)$$

is a surjective homomorphism of A^G - modules.
$A = \langle x_1^{b_1} x_2^{b_2} \ldots x_d^{b_d} \mid b_i < \max(2, |G|) \rangle_B$. $\Rightarrow$

$$A^G = \langle \mathrm{tr}(x_1^{b_1} x_2^{b_2} \ldots x_d^{b_d}) \mid b_i < \max(2, |G|), \sum b_i > 0 \rangle_B \ \Rightarrow$$

Remarks on Noether's theorem

Suppose $|G| \in \mathbb{F}^*$. Then the **transfer map**

$$\operatorname{tr} : A \to A^G, a \mapsto \sum_{g \in G} g(a)$$

is a surjective homomorphism of A^G - modules.

$A = \langle x_1^{b_1} x_2^{b_2} \ldots x_d^{b_d} \mid b_i < \max(2, |G|) \rangle_B$. $\Rightarrow$

$$A^G = \langle \operatorname{tr}(x_1^{b_1} x_2^{b_2} \ldots x_d^{b_d}) \mid b_i < \max(2, |G|), \sum b_i > 0 \rangle_B \ \Rightarrow$$

$$A^G = \mathbb{F}[B, \operatorname{tr}(x_1^{b_1} x_2^{b_2} \ldots x_d^{b_d}) \mid b_i < \max(2, |G|)\ ] \ \Rightarrow$$

A^G can be generated in degrees $\leq \max\{|G|, d \cdot (|G| - 1)\}$.

Constructive Aspects

Definition: (Degree bounds, Noether - number)

$$\beta(A^G) := \min\{k \mid A^G \text{ generated in degree } \leq k\} < \infty$$

Constructive Aspects

Definition: (Degree bounds, Noether - number)

$$\beta(A^G) := \min\{k \mid A^G \text{ generated in degree } \leq k\} < \infty$$

Theorem (Emmy Noether (1916)): If $\mathrm{char}\, \mathbb{F} = 0$, then

$$\beta(A^G) \leq |G|; \text{ (Noether bound)}$$

Constructive Aspects

Definition: (Degree bounds, Noether - number)

$$\beta(A^G) := \min\{k \mid A^G \text{ generated in degree } \leq k\} < \infty$$

Theorem (Emmy Noether (1916)): If $\mathrm{char}\, \mathbb{F} = 0$, then

$$\beta(A^G) \leq |G|; \text{ (Noether bound)}$$

- - the Noether bound does not hold if $\mathrm{char}\, \mathbb{F}$ divides $|G|$.

  - Noether's proofs do not work for $\mathrm{char}\, \mathbb{F} \not| \, |G|$ in general ("Noether gap").

  - Generalization to $\mathrm{char}\, \mathbb{F} \not| \, |G|$, (Fl.,Fogarty,(1999)).

Constructive Aspects

$\mathrm{char}\ \mathbb{F}$ appears in two places:

- surjectivity of transfer map

$$\mathrm{tr}:\ A \longrightarrow A^G:\ a \longrightarrow \sum_{g \in G} g(a)$$

Constructive Aspects

$\mathrm{char}\ \mathbb{F}$ appears in two places:

- surjectivity of transfer map

$$\mathrm{tr}:\ A \rightarrow A^G:\ a \rightarrow \sum_{g\in G} g(a)$$

- combinatorics to reduce degrees eg.:

$$x_1 \ldots x_m = \frac{(-1)^m}{m!} \sum_{I\subseteq\{1,\ldots,m\}} (-1)^{|I|} (\sum_{i\in I} x_i)^m$$

(needed for $m = 1, \ldots, |G|$).

Constructive Aspects

Modular counter example to Noether bound:

$G = \Sigma_2$, $A := \mathbb{F}_2[x_1, \ldots, x_k, y_1, \ldots, y_k]$

$g: \; x_i \mapsto y_i, \; \forall i = 1, \ldots, k.$

$$\mathcal{X} := (x_1 \ldots x_k)^+ := x_1 \ldots x_k + y_1 \ldots y_k;$$

indecomposable in A^G (Exercise(!)).

Constructive Aspects

Modular counter example to Noether bound:

$G = \Sigma_2$, $A := \mathbb{F}_2[x_1, \dots, x_k, y_1, \dots, y_k]$

$g: \ x_i \mapsto y_i, \ \forall i = 1, \dots, k.$

$$\mathcal{X} := (x_1 \dots x_k)^+ := x_1 \dots x_k + y_1 \dots y_k;$$

indecomposable in A^G (Exercise(!)).

$\Rightarrow \beta(A^G) \geq k \mapsto \infty.$

Theorem (Richman): If $p = \mathrm{char}(\mathbb{F})$ divides $|G|$, then $\beta_{\mathbb{F}}(G) = \infty$, i.e. $\forall N \in \mathbb{N} \, \exists \, k$ with

$$\beta(\mathbb{F}[x_1, \cdots, x_k]^G) > N.$$