Affine algebraic geometry

Stefan Maubach

April 2010

How this talk is organised:

- What is affine algebraic geometry?
- What are its big problems?
- $\longrightarrow$ Polynomial automorphism group
- $\longrightarrow$ $\longrightarrow$ over finite fields

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Geometrically sometimes "more difficult" than projective geometry (affine spaces are rarely compact).

Algebraically, more simple! (There's always a *ring*.)

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Geometrically sometimes "more difficult" than projective geometry (affine spaces are rarely compact).

Algebraically, more simple! (There's always a *ring*.)

Subtopic - but of *fundamental importance* to the whole of Algebraic geometry.

What is affine algebraic geometry?

Subfield of Algebraic Geometry (duh!).

Typical objects:

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Geometrically sometimes “more difficult” than projective geometry (affine spaces are rarely compact).

Algebraically, more simple! (There's always a *ring*.)

Subtopic - but of *fundamental importance* to the whole of Algebraic geometry.

We do all kinds of advanced things with algebraic geometry, but still we don't understand affine n-space k^n !

A Very Brief History

“Originally”: geometry and algebra different things.

Zariski $\longrightarrow$ Grothendieck $\longrightarrow$ etc.: **algebraic geometry**.

$+$- 1970: What if we apply algebraic geometry to the original simple objects, like $\mathbb{C}^n$, or $\mathbb{C}[X_1, X_2, \ldots, X_n]$?

(“Birth” of the field and many of its current questions.)

Since then: steady growth of the field.

(2000: separate AMS classification.)

$$
\begin{aligned}
k^n &\leftrightarrow k[X_1, \ldots, X_n] \\
V &\leftrightarrow \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V)
\end{aligned}
$$

Objects, hence morphisms!

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Objects, hence morphisms!

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.

$$\begin{array}{rcl} k^n & \leftrightarrow & k[X_1, \ldots, X_n] \\ V & \leftrightarrow & \mathcal{O}(V) := k[X_1, \ldots, X_n]/I(V) \end{array}$$

Objects, hence morphisms!

$$F : k^n \longrightarrow k^n$$

polynomial map if $F = (F_1, \ldots, F_n)$, $F_i \in k[X_1, \ldots, X_n]$.

Example: $F = (X + Y^2, Y)$ is polynomial map $\mathbb{C}^2 \longrightarrow \mathbb{C}^2$.

Set of polynomial automorphisms of k^n:

$Aut_n(k)$, also denoted by $\mathrm{GA}_n(k)$ - similarly to $\mathrm{GL}_n(k)$!

A topic is defined by its problems.

Many problems in AAG: inspired by linear algebra!
(In some sense: AAG most "natural generalization of linear algebra"...)

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$L \in \mathrm{GL}_n(k) \text{ invertible} \iff \det(L) = \quad \det(\mathrm{Jac}(L)) \in k^*$$

Problems in AAG: Jacobian Conjecture

$\text{char}(k) = 0$

L linear map;

$$\begin{array}{rclr} L \in \text{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\text{Jac}(L)) \in k^* \\ F \in \text{GA}_n(k) \text{ invertible} & ?? & & \det(\text{Jac}(F)) \in k^* \end{array}$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$L \in \mathrm{GL}_n(k)$ invertible	$\Longleftrightarrow$	$\det(L) =$	$\det(\mathrm{Jac}(L)) \in k^*$
$F \in \mathrm{GA}_n(k)$ invertible	??		$\det(\mathrm{Jac}(F)) \in k^*$

F invertible, i.e.

$$G \circ F = (X_1, \ldots, X_n).$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$L \in \mathrm{GL}_n(k)$ invertible	$\Longleftrightarrow$	$\det(L) =$	$\det(\mathrm{Jac}(L)) \in k^*$
$F \in \mathrm{GA}_n(k)$ invertible	??		$\det(\mathrm{Jac}(F)) \in k^*$

F invertible, i.e.

$$\mathrm{Jac}(G \circ F) = \mathrm{Jac}(X_1, \ldots, X_n).$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$L \in \mathrm{GL}_n(k)$ invertible	$\Longleftrightarrow$	$\det(L) =$	$\det(\mathrm{Jac}(L)) \in k^*$
$F \in \mathrm{GA}_n(k)$ invertible	??		$\det(\mathrm{Jac}(F)) \in k^*$

F invertible, i.e.

$$\mathrm{Jac}(G \circ F) = I.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rclr} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\mathrm{Jac}(F) \cdot (\mathrm{Jac}(G) \circ F) = I.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \cdot \det(\mathrm{Jac}(G) \circ F) = \det I = 1.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rclcl} L \in \mathrm{GL}_n(k) \text{ invertible} & \iff & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & ?? & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \cdot \det(blabla) = \det I = 1.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$L \in \mathrm{GL}_n(k)$ invertible	$\Longleftrightarrow$	$\det(L) =$	$\det(\mathrm{Jac}(L)) \in k^*$
$F \in \mathrm{GA}_n(k)$ invertible	??		$\det(\mathrm{Jac}(F)) \in k^*$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \in k[X_1, \ldots, X_n]^* = k^*.$$

Problems in AAG: Jacobian Conjecture

$\mathrm{char}(k) = 0$

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & \Longleftarrow & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

F invertible, i.e.

$$\det(\mathrm{Jac}(F)) \in k[X_1, \ldots, X_n]^* = k^*.$$

Problems in AAG: Jacobian Conjecture

$\text{char}(k) = 0$

L linear map;

$$L \in \text{GL}_n(k) \text{ invertible} \iff \det(L) = \det(\text{Jac}(L)) \in k^*$$

$$F \in \text{GA}_n(k) \text{ invertible} \Longleftarrow \det(\text{Jac}(F)) \in k^*$$

Jacobian Conjecture:

$$F \in \text{GA}_n(k) \textit{invertible} \Longrightarrow \det(\text{Jac}(F)) \in k^*$$

“Visual” version of Jacobian Conjecture

Volume-preserving polynomial maps are invertible.

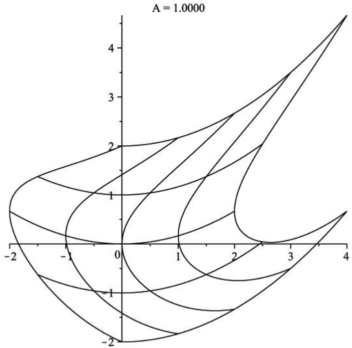

Figure: Image of raster under $(X + \frac{1}{2}Y^2, Y + \frac{1}{6}(X + \frac{1}{2}Y^2)^2)$.

Jacobian Conjecture very particular for *polynomials:*

$$F : (x, y) \longrightarrow (e^x, ye^{-x})$$

$$\mathrm{Jac}(F) = \begin{pmatrix} e^x & 0 \\ -ye^{-x} & e^{-x} \end{pmatrix}$$

$$\det(\mathrm{Jac}(F)) = 1$$

Jacobian Conjecture in $\text{char}(k) = p$:

L linear map;

$$\begin{array}{rcll} L \in \text{GL}_n(k) \text{ invertible} & \iff & \det(L) = & \det(\text{Jac}(L)) \in k^* \\ F \in \text{GA}_n(k) \text{ invertible} & \Rightarrow & & \det(\text{Jac}(F)) \in k^* \end{array}$$

Jacobian Conjecture in $\mathrm{char}(k) = p$:

L linear map;

$$
\begin{array}{rcll}
L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\
F \in \mathrm{GA}_n(k) \text{ invertible} & \Rightarrow & & \det(\mathrm{Jac}(F)) \in k^*
\end{array}
$$

$$
\begin{aligned}
F: \quad k^1 &\longrightarrow k^1 \\
X &\longrightarrow X - X^p
\end{aligned}
$$

$Jac(F) = 1$ but $F(0) = F(1) = 0$.

Jacobian Conjecture in $\mathrm{char}(k) = p$:

L linear map;

$$\begin{array}{rcll} L \in \mathrm{GL}_n(k) \text{ invertible} & \Longleftrightarrow & \det(L) = & \det(\mathrm{Jac}(L)) \in k^* \\ F \in \mathrm{GA}_n(k) \text{ invertible} & \Rightarrow & & \det(\mathrm{Jac}(F)) \in k^* \end{array}$$

$$\begin{array}{rl} F: & k^1 \longrightarrow k^1 \\ & X \longrightarrow X - X^p \end{array}$$

$Jac(F) = 1$ but $F(0) = F(1) = 0$.

Jacobian Conjecture in char$(k) = p$**:** Suppose $\det(Jac(F)) = 1$ and $p \not| [k(X_1, \ldots, X_n) : k(F_1, \ldots, F_n)]$. Then F is an automorphism.

Jacobian Conjecture in $\mathrm{char}(k) = p$:

$\mathrm{char}(k) = 0$:

$F = (X + a_1X^2 + a_2XY + a_3Y^2, Y + b_1X^2 + b_2XY + b_3Y^2)$

$$
\begin{aligned}
1 = \;& \det(Jac(F)) \\
= \;& 1+ \\
& (2a_1 + b_2)X+ \\
& (a_2 + 2b_3)Y+ \\
& (2a_1b_2 + 2a_2b_1)X^2+ \\
& (2b_2a_2 + 4a_1b_3 + 4a_3b_1)XY+ \\
& (2a_2b_3 + 2a_3b_2)Y^2
\end{aligned}
$$

In char(k)=2 : (parts of) equations vanish. **Question:** What are the right equations in $\mathrm{char}(k) = 2$? (or p?)

Enough about the Jacobian Problem! Another problem:

Cancellation problem

Cancellation problem: introduction

V, W vector spaces, if $V \times k \cong W \times k$ then $V \cong W$.

V vector space, then $V \times k \cong k^{n+1}$ implies $V \cong k^n$.

Cancellation problem: introduction

V, W vector spaces, if $V \times k \cong W \times k$ then $V \cong W$.
V vector space, then $V \times k \cong k^{n+1}$ implies $V \cong k^n$.

V, W varieties, if $V \times k \cong W \times k$ then $V \cong W$?

Cancellation problem: introduction

V, W vector spaces, if $V \times k \cong W \times k$ then $V \cong W$.
V vector space, then $V \times k \cong k^{n+1}$ implies $V \cong k^n$.

V, W varieties, if $V \times k \cong W \times k$ then $V \cong W$?
Cancellation problem: V variety. $V \times k \cong k^{n+1}$, is $V \cong k^n$?

Cancellation $V \times k \cong W \times k$

counterexamples

1972(?): Hoechster: over $\mathbb{R}$

Cancellation $V \times k \cong W \times k$ counterexamples

1972(?): Hoechster: over $\mathbb{R}$

1986(?): Danielewski: $V : xz + y^2 + 1 = 0$, $W : x^2z + y^2 + 1$

(over $\mathbb{C}$)

(Not a UFD)

Cancellation $V \times k \cong W \times k$ counterexamples

1972(?): Hoechster: over $\mathbb{R}$

1986(?): Danielewski: $V : xz + y^2 + 1 = 0$, $W : x^2z + y^2 + 1$ (over $\mathbb{C}$)

(Not a UFD)

2008: Finston & M. : "Best" counterexamples so far (UFD, over $\mathbb{C}$, lowest possible dimension):

$$V_{n,m} := \{(x, y, z, u, v) \mid x^2 + y^3 + z^7 = 0, x^m u - y^n v - 1 = 0\}$$

Cancellation $V \times k \cong W \times k$ counterexamples

1972(?): Hoechster: over $\mathbb{R}$

1986(?): Danielewski: $V : xz + y^2 + 1 = 0$, $W : x^2z + y^2 + 1$ (over $\mathbb{C}$)

(Not a UFD)

2008: Finston & M. : "Best" counterexamples so far (UFD, over $\mathbb{C}$, lowest possible dimension):

$$V_{n,m} := \{(x, y, z, u, v) \mid x^2 + y^3 + z^7 = 0, x^m u - y^n v - 1 = 0\}$$

Still looking for an example where $V = k^n$!

Understanding polynomial automorphisms

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.
- A list of n polynomials: $F \in (k[X_1, \ldots, X_n])^n$.

Understanding polynomial automorphisms

A map $F : k^n \longrightarrow k^n$ given by n polynomials:

$$F = (F_1(X_1, \ldots, X_n), \ldots, F_n(X_1, \ldots, X_n)).$$

Example: $F = (X + Y^2, Y)$.

Various ways of looking at polynomial maps:

- A map $k^n \longrightarrow k^n$.
- A list of n polynomials: $F \in (k[X_1, \ldots, X_n])^n$.
- A ring automorphism of $k[X_1, \ldots, X_n]$ sending $g(X_1, \ldots, X_n)$ to $g(F_1, \ldots, F_n)$.

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.

Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.

Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\ &= (X - Y^2 + Y^2, Y) \\ &= (X, Y).\end{aligned}$$

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \ldots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$\begin{aligned}(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\ &= (X - Y^2 + Y^2, Y) \\ &= (X, Y).\end{aligned}$$

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!

Understanding polynomial automorphisms

A polynomial map F is a polynomial automorphism if there is a polynomial map G such that $F(G) = (X_1, \dots, X_n)$.
Example: $(X + Y^2, Y)$ has inverse $(X - Y^2, Y)$.

$$
\begin{aligned}
(X + Y^2, Y) \circ (X - Y^2, Y) &= ([X - Y^2] + [Y]^2, [Y]) \\
&= (X - Y^2 + Y^2, Y) \\
&= (X, Y).
\end{aligned}
$$

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!
$(X^3, Y) : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{R}$!

Understanding polynomial automorphisms

Remark: If k is algebraically closed, then a polynomial endomorphism $k^n \longrightarrow k^n$ which is a bijection, is an invertible polynomial map.

$(X^p, Y) : \mathbb{F}_p^2 \longrightarrow \mathbb{F}_p^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{F}_p$!
$(X^3, Y) : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ is not a polynomial automorphism, even though it induces a bijection of $\mathbb{R}$!

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$
- Map $(aX_1 + bX_j, X_2, \ldots, X_n)$ $(a \in k^*, b \in k)$

The Automorphism Group

(This whole talk: $n \geq 2$)

$GL_n(k)$ is generated by

- Permutations $X_1 \longleftrightarrow X_i$
- Map $(aX_1 + bX_j, X_2, \ldots, X_n)$ $(a \in k^*, b \in k)$

$GA_n(k)$ is generated by ???

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n)$.

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$

$J_n(k)$:= set of triangular maps.

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

$J_n(k)$:= set of triangular maps.

$Aff_n(k)$:= set of compositions of invertible linear maps and translations.

Elementary map: $(X_1 + f(X_2, \ldots, X_n), X_2, \ldots, X_n)$, invertible with inverse

$$(X_1 - f(X_2, \ldots, X_n), X_2, \ldots, X_n).$$

Triangular map: $(X + f(Y, Z), Y + g(Z), Z + c)$

$$= (X, Y, Z + c)(X, Y + g(Z), Z)(X + f(X, Y), Y, Z)$$

$J_n(k)$:= set of triangular maps.

$Aff_n(k)$:= set of compositions of invertible linear maps and translations.

$TA_n(k) := < J_n(k), Aff_n(k) >$

In dimension 1: we understand the automorphism group.

(They are linear.)

In dimension 1: we understand the automorphism group. (They are linear.)
In dimension 2: famous Jung-van der Kulk-theorem:

$$\mathrm{GA}_2(\mathbb{K}) = \mathrm{TA}_2(\mathbb{K}) = \mathit{Aff}_2(\mathbb{K}) \ltimes \mathrm{J}_2(\mathbb{K})$$

Jung-van der Kulk is the reason that we can do a lot in dimension 2 !

What about dimension 3?

What about dimension 3? Stupid idea: everything will be tame?

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: “I cannot tame the following map:”

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: “I cannot tame the following map:”

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata’s map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!!

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: “I cannot tame the following map:”

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata’s map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!!

(Difficult and technical proof.) (2007 AMS Moore paper award.)

What about dimension 3? Stupid idea: everything will be tame?

1972: Nagata: "I cannot tame the following map:"

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z)$ where $\Delta = XZ + Y^2$.

Nagata's map is the historically most important map for polynomial automorphisms. It is a very elegant but complicated map.

AMAZING result: Umirbaev-Shestakov (2004)

N is not tame!! ...in characteristic ZERO...

(Difficult and technical proof.) (2007 AMS Moore paper award.)

AMS E.H. Moore Research Article Prize


Ivan Shestakov (center) and Ualbai Umirbaev (right) with Jim Arthur.

How did Nagata make Nagata's map?

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X, Y + z^2 X)$$

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$
$$= (X - 2(Xz + Y^2)Y - (Xz + Y^2)^2 z, Y + (Xz + Y^2)z)$$

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$
$$= (X - 2(Xz + Y^2)Y - (Xz + Y^2)^2 z, Y + (Xz + Y^2)z)$$

Thus: N is tame over $k[z, z^{-1}]$, i.e. N in $\mathrm{TA}_2(k[z, z^{-1}])$.

How did Nagata make Nagata's map?

Study maps over $k[z, z^{-1}]$:

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X)(X + z^{-1}Y^2, Y)$$
$$= (X - 2(Xz + Y^2)Y - (Xz + Y^2)^2 z, Y + (Xz + Y^2)z)$$

Thus: N is tame over $k[z, z^{-1}]$, i.e. N in $\mathrm{TA}_2(k[z, z^{-1}])$.

Nagata proved: N is NOT tame over $k[z]$, i.e. N not in $\mathrm{TA}_2(k[z])$.

Stably tameness

N tame in one dimension higher:

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z, W)$ where $\Delta = XZ + Y^2$.

Stably tameness

N tame in one dimension higher:

$N := (X - 2Y\Delta - Z\Delta^2, Y + Z\Delta, Z, W)$ where $\Delta = XZ + Y^2$.

$$\begin{aligned}
&(X + 2YW - ZW^2, Y - ZW, Z, W)\circ \\
&(X, Y, Z, W - \tfrac{1}{2}\Delta)\circ \\
&(X - 2YW - ZW^2, Y + ZW, Z, W)\circ \\
&(X, Y, Z, W + \tfrac{1}{2}\Delta) \\
&= N
\end{aligned}$$

Intermezzo 1: public key crytography by tame automorphisms

(By T.T. Moh - called it Tame Transformation Method, or TTM. . .)

Intermezzo 1: public key crytography by tame automorphisms

(By T.T. Moh - called it Tame Transformation Method, or TTM. . .)

Public key.

Intermezzo 1: public key crytography by tame automorphisms

(By T.T. Moh - called it Tame Transformation Method, or TTM. . .)

$$(\text{complicated map}) \longleftarrow \text{Public key.}$$

Intermezzo 1: public key crytography by tame automorphisms

(By T.T. Moh - called it Tame Transformation Method, or TTM. . .)

Secret key: decomposition

(complicated map) $\longleftarrow$ Public key.

Intermezzo 1: public key crytography by tame automorphisms

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

Secret key: decomposition

(elementary) $\times$ (affine) $\times$ (elementary) $\times \ldots \times$ (elementary)

$=$ (complicated map) $\longleftarrow$ Public key.

Intermezzo 1: public key crytography by tame automorphisms

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

Secret key: decomposition

(elementary) $\times$ (affine) $\times$ (elementary) $\times \ldots \times$ (elementary)

$=$ (complicated map) $\longleftarrow$ Public key.

Nice idea - basic idea still uncracked, but: a lot of attacks on implementations (Goubin, Courtois, etc.)

Intermezzo 1: public key crytography by tame automorphisms

(By T.T. Moh - called it Tame Transformation Method, or TTM...)

Secret key: decomposition

(elementary) $\times$ (affine) $\times$ (elementary) $\times \ldots \times$ (elementary)

$=$ (complicated map) $\longleftarrow$ Public key.

Nice idea - basic idea still uncracked, but: a lot of attacks on implementations (Goubin, Courtois, etc.)

(End intermezzo 1.)

Intermezzo 2: why characteristic p?

The “characteristic p case” has been neglected mostly - up until recently!

What are reasons to study especially $\mathbb{F}_q$?

Intermezzo 2: why characteristic p?

The "characteristic p case" has been neglected mostly - up until recently!

What are reasons to study especially $\mathbb{F}_q$?

- Reduction-mod-p techniques (recent work of Belov-Kontsevich).

Intermezzo 2: why characteristic p?

The "characteristic p case" has been neglected mostly - up until recently!

What are reasons to study especially $\mathbb{F}_q$?

- Reduction-mod-p techniques (recent work of Belov-Kontsevich).
- Many new connections: finite Group Theory, Number Theory!

Intermezzo 2: why characteristic p?

The "characteristic p case" has been neglected mostly - up until recently!

What are reasons to study especially $\mathbb{F}_q$?

- Reduction-mod-p techniques (recent work of Belov-Kontsevich).
- Many new connections: finite Group Theory, Number Theory!
- Almost virgin research subject! (Brainstorming 30 minutes $\longrightarrow$ new accessible problem!)

Intermezzo 2: why characteristic p?

The "characteristic p case" has been neglected mostly - up until recently!

What are reasons to study especially $\mathbb{F}_q$?

- Reduction-mod-p techniques (recent work of Belov-Kontsevich).
- Many new connections: finite Group Theory, Number Theory!
- Almost virgin research subject! (Brainstorming 30 minutes $\longrightarrow$ new accessible problem!)
- Applications? (Cryptography)

Intermezzo 2: why characteristic p?

The "characteristic p case" has been neglected mostly - up until recently!

What are reasons to study especially $\mathbb{F}_q$?

- Reduction-mod-p techniques (recent work of Belov-Kontsevich).
- Many new connections: finite Group Theory, Number Theory!
- Almost virgin research subject! (Brainstorming 30 minutes $\longrightarrow$ new accessible problem!)
- Applications? (Cryptography)
- Quite accessible for students.

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

What about $\mathsf{TA}_n(k) \subseteq \mathsf{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?
Denote $\mathsf{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map
$\mathsf{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathsf{Bij}_n(\mathbb{F}_q)$.

What about $\mathrm{TA}_n(k) \subseteq \mathrm{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

Denote $\mathrm{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map

$\mathrm{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathrm{Bij}_n(\mathbb{F}_q)$.

What is $\pi_q(\mathrm{GA}_n(\mathbb{F}_q))$? Can we make every bijection on $\mathbb{F}_q^n$ as an *invertible* polynomial map?

What about $\mathsf{TA}_n(k) \subseteq \mathsf{GA}_n(k)$ if $k = \mathbb{F}_q$ is a finite field?

Denote $\mathsf{Bij}_n(\mathbb{F}_q)$ as set of bijections on $\mathbb{F}_q^n$. We have a natural map

$\mathsf{GA}_n(\mathbb{F}_q) \xrightarrow{\pi_q} \mathsf{Bij}_n(\mathbb{F}_q)$.

What is $\pi_q(\mathsf{GA}_n(\mathbb{F}_q))$? Can we make every bijection on $\mathbb{F}_q^n$ as an *invertible* polynomial map?

Simpler question: what is $\pi_q(\mathsf{TA}_n(\mathbb{F}_q))$?

Why simpler? Because we have a set of generators!

Question: what is $\pi_q(\mathsf{TA}_n(\mathbb{F}_q))$?

See $\mathsf{Bij}_n(\mathbb{F}_q)$ as $\mathsf{Sym}(q^n)$.

Question: what is $\pi_q(\mathsf{TA}_n(\mathbb{F}_q))$?

See $\mathsf{Bij}_n(\mathbb{F}_q)$ as $\mathsf{Sym}(q^n)$.

$\mathsf{TA}_n(\mathbb{F}_q) =< \mathsf{GL}_n(\mathbb{F}_q), \sigma_f >$ where f runs over $\mathbb{F}_q[X_2, \ldots, X_n]$ and $\sigma_f := (X_1 + f, X_2, \ldots, X_n)$.

Question: what is $\pi_q(\mathsf{TA}_n(\mathbb{F}_q))$?

See $\mathsf{Bij}_n(\mathbb{F}_q)$ as $\mathsf{Sym}(q^n)$.

$\mathsf{TA}_n(\mathbb{F}_q) =< \mathsf{GL}_n(\mathbb{F}_q), \sigma_f >$ where f runs over $\mathbb{F}_q[X_2, \ldots, X_n]$ and $\sigma_f := (X_1 + f, X_2, \ldots, X_n)$.

We make finite subset $\mathcal{S} \subset \mathbb{F}_q[X_2, \ldots, X_n]$ and define

$$\mathcal{G} :=< \mathsf{GL}_n(\mathbb{F}_q), \sigma_f \ ; \ f \in \mathcal{S} >$$

such that

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \pi_q(\mathcal{G}).$$

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

(1) $\pi_q(T_n(\mathbb{F}_q)) = \pi_q(\mathcal{G})$ is 2-transitive, hence primitive.

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

(1) $\pi_q(T_n(\mathbb{F}_q)) = \pi_q(\mathcal{G})$ is 2-transitive, hence primitive.

You might know: if $H < \mathrm{Sym}(m)$ is primitive + a 2-cycle then $H = \mathrm{Sym}(m)$.

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

(1) $\pi_q(T_n(\mathbb{F}_q)) = \pi_q(\mathcal{G})$ is 2-transitive, hence primitive.

You might know: if $H < \mathrm{Sym}(m)$ is primitive + a 2-cycle then $H = \mathrm{Sym}(m)$.

If $q = 2$ or q odd, then indeed we find a 2-cycle!

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

(1) $\pi_q(T_n(\mathbb{F}_q)) = \pi_q(\mathcal{G})$ is 2-transitive, hence primitive.

You might know: if $H < \mathrm{Sym}(m)$ is primitive + a 2-cycle then $H = \mathrm{Sym}(m)$.

If $q = 2$ or q odd, then indeed we find a 2-cycle!

Hence if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n)$.

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q = \text{odd}$, then $\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle.

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle. In fact-all generators of $\mathrm{TA}_n(\mathbb{F}_q)$ turn out to be even, i.e.

$\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) \subseteq \mathrm{Alt}(q^n)$!

But: there's another theorem:

Theorem: $H < \mathrm{Sym}(m)$ Primitive $+$ 3-cycle $\longrightarrow H = \mathrm{Alt}(m)$ or $H = \mathrm{Sym}(m)$.

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle. In fact- all generators of $\mathrm{TA}_n(\mathbb{F}_q)$ turn out to be even, i.e. $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) \subseteq \mathrm{Alt}(q^n)$!

But: there's another theorem:

Theorem: $H < \mathrm{Sym}(m)$ Primitive $+$ 3-cycle $\longrightarrow H = \mathrm{Alt}(m)$ or $H = \mathrm{Sym}(m)$.

We find a 3-cycle!

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

If $q = 4, 8, 16, \ldots$ we don't succeed to find a 2-cycle. In fact- all generators of $\mathrm{TA}_n(\mathbb{F}_q)$ turn out to be even, i.e.

$\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) \subseteq \mathrm{Alt}(q^n)$!

But: there's another theorem:

Theorem: $H < \mathrm{Sym}(m)$ Primitive + 3-cycle $\longrightarrow H = \mathrm{Alt}(m)$ or $H = \mathrm{Sym}(m)$.

We find a 3-cycle!

Hence, if $q = 4, 8, 16, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(m)$!

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Suppose $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi(F)$ odd permutation, then $\pi(F) \notin \pi(\mathrm{TA}_n(\mathbb{F}_4))$, so $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$!

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?
Answer: if $q = 2$ or $q =$ odd, then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.
Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.
Suppose $F \in \mathrm{GA}_n(\mathbb{F}_4)$ such that $\pi(F)$ odd permutation, then $\pi(F) \notin \pi(\mathrm{TA}_n(\mathbb{F}_4))$, so $\mathrm{GA}_n(\mathbb{F}_4) \neq \mathrm{TA}_n(\mathbb{F}_4)$!
So: Start looking for an odd automorphism!!! (Or prove they don't exist)

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$?

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X - 2(XZ + Y^2)Y - (XZ + Y^2)^2 Z, \\ Y + (XZ + Y^2)Z, \\ Z \end{pmatrix}$$

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X - 2(XZ + Y^2)Y - (XZ + Y^2)^2 Z, \\ Y + (XZ + Y^2)Z, \\ Z \end{pmatrix}$$

...drumroll...

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X - 2(XZ + Y^2)Y - (XZ + Y^2)^2 Z, \\ Y + (XZ + Y^2)Z, \\ Z \end{pmatrix}$$

...drumroll... Nagata is EVEN if and only if $q = 4, 8, 16, \ldots$ and ODD otherwise...

Question: what is $\pi_q(T_n(\mathbb{F}_q))$?

Answer: if $q = 2$ or $q =$ odd, then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n)$.

Answer: if $q = 4, 8, 16, 32, \ldots$ then $\pi_q(T_n(\mathbb{F}_q)) = \mathrm{Alt}(q^n)$.

Problem: Do there exist "odd" polynomial automorphisms over $\mathbb{F}_4$? Exciting! Let's try Nagata!

$$N = \begin{pmatrix} X - 2(XZ + Y^2)Y - (XZ + Y^2)^2 Z, \\ Y + (XZ + Y^2)Z, \\ Z \end{pmatrix}$$

...drumroll... Nagata is EVEN if and only if $q = 4, 8, 16, \ldots$ and ODD otherwise... so far: no odd example found!

Different approach?

Is there perhaps a combinatorial reason why $\pi(\mathrm{GA}_n(\mathbb{F}_4)$ has only even permutations??

Losing less information: embedding $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

$$\mathsf{GA}_n(\mathbb{F}_q) \subset \mathsf{GA}_n(\mathbb{F}_{q^m}) \xrightarrow{\pi_{q^m}} \mathsf{sym}(q^{mn}).$$

Losing less information: embedding $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

$$\mathsf{GA}_n(\mathbb{F}_q) \subset \mathsf{GA}_n(\mathbb{F}_{q^m}) \xrightarrow{\pi_{q^m}} \mathsf{sym}(q^{mn}).$$

$$\begin{array}{c} \mathsf{GA}_n(\mathbb{F}_q) \\ \bigcup| \\ \mathsf{TA}_n(\mathbb{F}_q) \end{array}$$

Losing less information: embedding $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

$$\mathsf{GA}_n(\mathbb{F}_q) \subset \mathsf{GA}_n(\mathbb{F}_{q^m}) \xrightarrow{\pi_{q^m}} \mathsf{sym}(q^{mn}).$$

$$\begin{array}{ccccc} \mathsf{GA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathsf{GA}_n(\mathbb{F}_q)) & \subset \mathsf{sym}(q^{mn}) \\ \bigcup\!| & & \bigcup\!| & \\ \mathsf{TA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathsf{TA}_n(\mathbb{F}_q)) & \subset \mathsf{sym}(q^{mn}) \end{array}$$

Losing less information: embedding $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

$$\mathsf{GA}_n(\mathbb{F}_q) \subset \mathsf{GA}_n(\mathbb{F}_{q^m}) \xrightarrow{\pi_{q^m}} \mathrm{sym}(q^{mn}).$$

$$\begin{array}{ccccc}
\mathsf{GA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathsf{GA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn}) \\
\bigcup\vert & & \bigcup\vert & \\
\mathsf{TA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathsf{TA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn})
\end{array}$$

(1) Compute $\pi_{q^m}(\mathsf{TA}_n(\mathbb{F}_q))$,

Losing less information: embedding $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

$$\mathrm{GA}_n(\mathbb{F}_q) \subset \mathrm{GA}_n(\mathbb{F}_{q^m}) \xrightarrow{\pi_{q^m}} \mathrm{sym}(q^{mn}).$$

$$\begin{array}{ccccc} \mathrm{GA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn}) \\ \bigcup\vert & & \bigcup\vert & \\ \mathrm{TA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn}) \end{array}$$

(1) Compute $\pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$,

(2) check if $\pi_{q^m}(N) \notin \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$,

Losing less information: embedding $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

$$\mathrm{GA}_n(\mathbb{F}_q) \subset \mathrm{GA}_n(\mathbb{F}_{q^m}) \xrightarrow{\pi_{q^m}} \mathrm{sym}(q^{mn}).$$

$$\begin{array}{ccccc}
\mathrm{GA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn}) \\
\bigcup| & & \bigcup| & \\
\mathrm{TA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn})
\end{array}$$

(1) Compute $\pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$,

(2) check if $\pi_{q^m}(N) \notin \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$,

and hop, (3) $\mathrm{TA}_n(\mathbb{F}_q) \neq \mathrm{GA}_n(\mathbb{F}_q)$ and immortal fame!

Losing less information: embedding $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$.

$$\mathrm{GA}_n(\mathbb{F}_q) \subset \mathrm{GA}_n(\mathbb{F}_{q^m}) \xrightarrow{\pi_{q^m}} \mathrm{sym}(q^{mn}).$$

$$\begin{array}{ccccc}
\mathrm{GA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathrm{GA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn}) \\
\bigcup\!| & & \bigcup\!| & \\
\mathrm{TA}_n(\mathbb{F}_q) & \longrightarrow & \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q)) & \subset \mathrm{sym}(q^{mn})
\end{array}$$

(1) Compute $\pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$,

(2) check if $\pi_{q^m}(N) \notin \pi_{q^m}(\mathrm{TA}_n(\mathbb{F}_q))$,

and hop, (3) $\mathrm{TA}_n(\mathbb{F}_q) \neq \mathrm{GA}_n(\mathbb{F}_q)$ and immortal fame!

However:

Mimicking Nagata's map:

Theorem: (M) [- general stuff -]

Corollary: For every extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, there exists $T_m \in \mathrm{TA}_3(\mathbb{F}_{q^m})$ such that T_m "mimicks" N, i.e.

$$\pi_{q^m}(T_m) = \pi_{q^m}(N).$$

Mimicking Nagata's map:

Theorem: (M) [- general stuff -]

Corollary: For every extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$, there exists $T_m \in \mathrm{TA}_3(\mathbb{F}_{q^m})$ such that T_m "mimicks" N, i.e.

$$\pi_{q^m}(T_m) = \pi_{q^m}(N).$$

Theorem states: for *practical* purposes, tame is almost always enough!

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$.

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X), (X + z^{-1}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_p)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

$$(X - z^{-1}Y^2, Y)(X, Y + z^2X), (X + z^{-1}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Do the Big Trick, since for $z \in \mathbb{F}_q$ we have $z^q = z$:

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_q)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

$$(X - z^{q-2}Y^2, Y)(X, Y + z^2X), (X + z^{q-2}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Do the Big Trick, since for $z \in \mathbb{F}_q$ we have $z^q = z$:

Nagata can be mimicked by a tame map for every $q = p^m$ - i.e. exists $F \in TA_3(\mathbb{F}_q)$ such that $\pi_q N = \pi_q F$. Proof is easy once you realize where to look... Remember Nagata's way of making Nagata map?

$$(X - z^{q-2}Y^2, Y)(X, Y + z^2 X), (X + z^{q-2}Y^2, Y)$$
$$= (X - 2\Delta Y - \Delta^2 z, Y + \Delta z)$$

Do the Big Trick, since for $z \in \mathbb{F}_q$ we have $z^q = z$:

This almost works - a bit more wiggling necessary (And for the general case, even more work.)

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \mid deg(F) \leq d\}$.
If $k = \mathbb{F}_q$, then this is finite.

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \mid deg(F) \leq d\}$. If $k = \mathbb{F}_q$, then this is finite. Now compute $\mathrm{GA}_n^d(\mathbb{F}_q) := \mathrm{GA}_n(\mathbb{F}_q) \cap MA_n^d(\mathbb{F}_q)$ by checking all $F \in MA_n^d(k)$! We find ALL automorphisms of degree $\leq d$. Will we find new ones we didn't know before?

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \mid deg(F) \leq d\}$.
If $k = \mathbb{F}_q$, then this is finite. Now compute
$\mathrm{GA}_n^d(\mathbb{F}_q) := \mathrm{GA}_n(\mathbb{F}_q) \cap MA_n^d(\mathbb{F}_q)$ by checking all $F \in MA_n^d(k)$!
We find ALL automorphisms of degree $\leq d$. Will we find new ones we didn't know before?

Let's not be too ambitious: $n = 3$. And $q = 2, 3, 4, 5$.

Computable is (R. Willems):
$\mathrm{GA}_3^2(\mathbb{F}_{2,3,4,5})$ and main part of $\mathrm{GA}_3^3(\mathbb{F}_2)$. Surprisingly, results seem to be intersting!

Another idea: define $MA_n^d(k) := \{F \in MA_n(k) \, | deg(F) \leq d\}$.
If $k = \mathbb{F}_q$, then this is finite. Now compute
$\mathrm{GA}_n^d(\mathbb{F}_q) := \mathrm{GA}_n(\mathbb{F}_q) \cap MA_n^d(\mathbb{F}_q)$ by checking all $F \in MA_n^d(k)$!
We find ALL automorphisms of degree $\leq d$. Will we find new ones we didn't know before?
Let's not be too ambitious: $n = 3$. And $q = 2, 3, 4, 5$.
Computable is (R. Willems):
$\mathrm{GA}_3^2(\mathbb{F}_{2,3,4,5})$ and main part of $\mathrm{GA}_3^3(\mathbb{F}_2)$. Surprisingly, results seem to be intersting!
(Work in progress. Also bijective endomorphisms are interesting.)

Another topic: additive group actions

$\mathcal{G}$ group, acting on $\mathbb{C}^n$ means:

Another topic: additive group actions

$\mathcal{G}$ group, acting on $\mathbb{C}^n$ means:

$\varphi_g \in \mathrm{GA}_n(\mathbb{C})$ such that $\varphi_g \varphi_h = \varphi_{g+h}$ (in a "continuous way").

Another topic: additive group actions

$\mathcal{G}$ group, acting on $\mathbb{C}^n$ means:

$\varphi_g \in \mathrm{GA}_n(\mathbb{C})$ such that $\varphi_g \varphi_h = \varphi_{g+h}$ (in a "continuous way").

Special example: $\mathcal{G} =< \mathbb{C}, + >$. Denoted by $\mathcal{G}_a$.

Another topic: additive group actions

$\mathcal{G}$ group, acting on $\mathbb{C}^n$ means:

$\varphi_g \in \mathrm{GA}_n(\mathbb{C})$ such that $\varphi_g\varphi_h = \varphi_{g+h}$ (in a "continuous way").

Special example: $\mathcal{G} =< \mathbb{C}, + >$. Denoted by $\mathcal{G}_a$.

Example: $t \in \mathcal{G}_a \longrightarrow \varphi_t := (X_1 + t, X_2, \ldots, X_n)$.

Another topic: additive group actions

$\mathcal{G}$ group, acting on $\mathbb{C}^n$ means:

$\varphi_g \in \mathrm{GA}_n(\mathbb{C})$ such that $\varphi_g \varphi_h = \varphi_{g+h}$ (in a "continuous way").

Special example: $\mathcal{G} =< \mathbb{C}, + >$. Denoted by $\mathcal{G}_a$.

Example: $t \in \mathcal{G}_a \longrightarrow \varphi_t := (X_1 + t, X_2, \ldots, X_n)$.

Define $D : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$ as the 'log' of the action:

$$D(P) := \frac{\partial}{\partial t} \varphi_t(P)|_{t=0}$$

Another topic: additive group actions

$\mathcal{G}$ group, acting on $\mathbb{C}^n$ means:

$\varphi_g \in \mathrm{GA}_n(\mathbb{C})$ such that $\varphi_g \varphi_h = \varphi_{g+h}$ (in a "continuous way").

Special example: $\mathcal{G} =< \mathbb{C}, + >$. Denoted by $\mathcal{G}_a$.

Example: $t \in \mathcal{G}_a \longrightarrow \varphi_t := (X_1 + t, X_2, \ldots, X_n)$.

Define $D : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$ as the 'log' of the action:

$$D(P) := \frac{\partial}{\partial t} \varphi_t(P)|_{t=0}$$

Example:

$$\begin{aligned} & \tfrac{\partial}{\partial t} P(X_1 + t, X_2, \ldots, X_n)|_{t=0} \\ = \; & \tfrac{\partial P}{\partial X_1}(X_1, X_2, \ldots, X_n) \end{aligned}$$

Additive group actions

Define $D : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$ as the 'log' of the action:

$$D(P) := \frac{\partial}{\partial t}\varphi_t(P)|_{t=0}$$

Example:

$$\begin{aligned} & \tfrac{\partial}{\partial t} P(X_1 + t, X_2, \ldots, X_n)|_{t=0} \\ = \quad & \tfrac{\partial P}{\partial X_1}(X_1, X_2, \ldots, X_n) \end{aligned}$$

Additive group actions

Define $D : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$ as the 'log' of the action:

$$D(P) := \frac{\partial}{\partial t} \varphi_t(P)|_{t=0}$$

Example:

$$\begin{aligned} & \tfrac{\partial}{\partial t} P(X_1 + t, X_2, \ldots, X_n)|_{t=0} \\ = \; & \tfrac{\partial P}{\partial X_1}(X_1, X_2, \ldots, X_n) \end{aligned}$$

$$D := \frac{\partial}{\partial X_1}$$

Additive group actions

Define $D : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$ as the 'log' of the action:

$$D(P) := \frac{\partial}{\partial t}\varphi_t(P)|_{t=0}$$

Example:

$$\begin{aligned} & \tfrac{\partial}{\partial t} P(X_1 + t, X_2, \ldots, X_n)|_{t=0} \\ = \quad & \tfrac{\partial P}{\partial X_1}(X_1, X_2, \ldots, X_n) \end{aligned}$$

$$D := \frac{\partial}{\partial X_1}$$

and indeed:

$$\exp(tD)(P) = P(X_1 + t, X_2, \ldots, X_n)$$

Additive group actions

D is a locally nilpotent derivation:

$D(fg) = fD(g) + D(f)g$, $D(f+g) = D(f) + D(g)$

(derivation)

For all f, there exists an m_f such that $D^{m_f}(f) = 0$. (locally nilpotent)

Example:

$$\begin{aligned} & \tfrac{\partial}{\partial t} P(X_1 + t, X_2, \ldots, X_n)|_{t=0} \\ = \quad & \tfrac{\partial P}{\partial X_1}(X_1, X_2, \ldots, X_n) \end{aligned}$$

$$D := \frac{\partial}{\partial X_1}$$

and indeed:

$$\exp(tD)(P) = P(X_1 + t, X_2, \ldots, X_n)$$

Another example:

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y}$$

is locally nilpotent derivation.

Another example:

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y}$$

is locally nilpotent derivation.

$$\delta(XZ) = \quad \delta(X)Z + X\delta(Z) = -2Y \cdot Z.$$

Another example:

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y}$$

is locally nilpotent derivation.

$$\begin{aligned} \delta(XZ) = &\quad \delta(X)Z + X\delta(Z) = -2Y \cdot Z. \\ \delta(Y^2) = &\quad 2Y\delta(Y) = 2Y \cdot Z. \end{aligned}$$

Another example:

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y}$$

is locally nilpotent derivation.

$$\begin{aligned} \delta(XZ) = &\quad \delta(X)Z + X\delta(Z) = -2Y \cdot Z. \\ \delta(Y^2) = &\quad 2Y\delta(Y) = 2Y \cdot Z. \\ \hline \delta(XZ + Y^2) = &\quad 0 \end{aligned}$$

Another example:

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y}$$

is locally nilpotent derivation.

$$\begin{aligned}
\delta(XZ) = &\quad \delta(X)Z + X\delta(Z) = -2Y \cdot Z. \\
\delta(Y^2) = &\quad 2Y\delta(Y) = 2Y \cdot Z. \\
\hline
\delta(XZ + Y^2) = &\quad 0
\end{aligned}$$

Hence,

$\delta(\Delta) = 0$ where $\Delta = XZ + Y^2$.

Another example:

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y}$$

is locally nilpotent derivation.

$$\begin{aligned}
\delta(XZ) = &\quad \delta(X)Z + X\delta(Z) = -2Y \cdot Z. \\
\delta(Y^2) = &\quad 2Y\delta(Y) = 2Y \cdot Z. \\
\hline
\delta(XZ + Y^2) = &\quad 0
\end{aligned}$$

Hence,

$\delta(\Delta) = 0$ where $\Delta = XZ + Y^2$.

Hence: $D := \Delta\delta$ is also an LND:

$D^3(X) = D^2(\Delta \cdot -2Y) = \Delta \cdot -2 \cdot D^2(Y) = \Delta \cdot -2 \cdot D(Z) = 0$

etc.

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y},$$

$$D := \Delta\delta, \quad \Delta := XZ + Y^2$$

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y},$$

$$D := \Delta\delta, \quad \Delta := XZ + Y^2$$

Now compute:

$$\varphi_t := \exp(tD) := (\exp(tD)(X), \exp(tD)(Y), \exp(tD)(Z))$$

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y},$$
$$D := \Delta\delta, \quad \Delta := XZ + Y^2$$

Now compute:

$$\varphi_t := \exp(tD) := (\exp(tD)(X), \exp(tD)(Y), \exp(tD)(Z))$$

$$\exp(tD)(X) = X + tD(X) + \frac{1}{2}t^2D^2(X)$$
$$\exp(tD)(Y) = Y + tD(Y)$$
$$\exp(tD)(Z) = Z$$

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y},$$

$$D := \Delta\delta, \quad \Delta := XZ + Y^2$$

Now compute:

$$\varphi_t := \exp(tD) := (\exp(tD)(X), \exp(tD)(Y), \exp(tD)(Z))$$

$$\exp(tD)(X) = X + tD(X) + \frac{1}{2}t^2 D^2(X)$$

$$\exp(tD)(Y) = Y + t\Delta Z$$

$$\exp(tD)(Z) = Z$$

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y},$$

$$D := \Delta\delta, \quad \Delta := XZ + Y^2$$

Now compute:

$$\varphi_t := \exp(tD) := (\exp(tD)(X), \exp(tD)(Y), \exp(tD)(Z))$$

$$\exp(tD)(X) = X + t(-2Y\Delta) + \frac{1}{2}t^2 D(-2Y\Delta)$$

$$\exp(tD)(Y) = Y + t\Delta Z$$

$$\exp(tD)(Z) = Z$$

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y},$$

$$D := \Delta\delta, \quad \Delta := XZ + Y^2$$

Now compute:

$$\varphi_t := \exp(tD) := (\exp(tD)(X), \exp(tD)(Y), \exp(tD)(Z))$$

$$\exp(tD)(X) = X + t(-2Y\Delta) + \frac{1}{2}t^2(-2Z\Delta^2)$$

$$\exp(tD)(Y) = Y + t\Delta Z$$

$$\exp(tD)(Z) = Z$$

$$\delta := -2Y\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y},$$

$$D := \Delta\delta, \quad \Delta := XZ + Y^2$$

Now compute:

$$\varphi_t := \exp(tD) := (\exp(tD)(X), \exp(tD)(Y), \exp(tD)(Z))$$

$$\exp(tD)(X) = X - 2t\Delta Y - t^2\Delta^2 Z)$$

$$\exp(tD)(Y) = Y + t\Delta Z$$

$$\exp(tD)(Z) = Z$$

$$\exp(tD)(X) = X - 2t\Delta Y - t^2\Delta^2 Z$$

$$\exp(tD)(Y) = Y + t\Delta Z$$

$$\exp(tD)(Z) = Z$$

$$\exp(tD)(X) = X - 2t\Delta Y - t^2\Delta^2 Z$$

$$\exp(tD)(Y) = Y + t\Delta Z$$

$$\exp(tD)(Z) = Z$$

Examine $t = 1$:

$$\exp(D)(X) = X - 2\Delta Y - \Delta^2 Z)$$

$$\exp(D)(Y) = Y + \Delta Z$$

$$\exp(D)(Z) = Z$$

Examine $t = 1$:

$$\exp(D)(X) = X - 2\Delta Y - \Delta^2 Z)$$

$$\exp(D)(Y) = Y + \Delta Z$$

$$\exp(D)(Z) = Z$$

Examine $t = 1$: Nagata's automorphism!

$\mathsf{GA}_n(k)$

$\mathsf{TA}_n(k)$

$\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{LF}_n(k) \quad := < F \in \mathrm{GA}_n(k) \mid deg(F^m) \text{ bounded} >$

$\cup|$

$\mathrm{ELFD}_n(k) \quad := < \exp(D) \mid D \text{ locally finite derivation} >$

$\cup|$

$\mathrm{TA}_n(k)$

$\mathrm{GA}_n(k)$

$\cup|$

$\mathrm{LF}_n(k) \quad := < F \in \mathrm{GA}_n(k) \mid deg(F^m) \text{ bounded} >$

$\cup|$

$\mathrm{ELFD}_n(k) \quad := < \exp(D) \mid D \text{ locally finite derivation} >$

$\cup|$

$\mathrm{GLIN}_n(k) \quad := \text{normal closure of } \mathrm{GL}_n(k)$

$?\cup|?$

$\mathrm{TA}_n(k)$

$$
\begin{array}{ll}
\mathrm{GA}_n(k) & \\
\cup| & \\
\mathrm{LF}_n(k) & := < F \in \mathrm{GA}_n(k) \mid deg(F^m) \text{ bounded} > \\
\cup| & \\
\mathrm{ELFD}_n(k) & := < \exp(D) \mid D \text{ locally finite derivation} > \\
\cup| & \\
\mathrm{GTAM}_n(k) & := \text{normal closure of } \mathrm{TA}_n(k) \\
\cup| & \\
\mathrm{GLIN}_n(k) & := \text{normal closure of } \mathrm{GL}_n(k) \\
?\cup|? & \\
\mathrm{TA}_n(k) &
\end{array}
$$

Where in these groups is Nagata?

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Theorem: (M., Poloni) Nagata is *shifted linearizable:*

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Theorem: (M., Poloni) Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Theorem: (M., Poloni) Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$(s \exp(D))$$

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Theorem: (M., Poloni) Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp\left(\frac{-s^2}{1-s^2}D\right)(s\exp(D))\exp\left(\frac{s^2}{1-s^2}D\right)$$

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Theorem: (M., Poloni) Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp\left(\frac{-s^2}{1-s^2}D\right)(s\exp(D))\exp\left(\frac{s^2}{1-s^2}D\right) = sI$$

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Theorem: (M., Poloni) Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp(\frac{-s^2}{1-s^2}D)(s\exp(D))\exp(\frac{s^2}{1-s^2}D) = sI$$

Hence: Nagata map is in $\mathrm{GLIN}_3(k)$!

Where in these groups is Nagata?

No conjugate of Nagata is in $\mathrm{GL}_n(k)$ for any field k !

Theorem: (M., Poloni) Nagata is *shifted linearizable:* choose $s \in k$ such that $s \neq 0, 1, -1$.

$$\exp(\frac{-s^2}{1-s^2}D)(s\exp(D))\exp(\frac{s^2}{1-s^2}D) = sI$$

Hence: Nagata map is in $\mathrm{GLIN}_3(k)$! - If $k \neq \mathbb{F}_2, \mathbb{F}_3$, that is !!

How does $\mathsf{GLIN}_n(k)$ compare to $\mathsf{GTAM}_n(k)$?

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$.

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(aX, Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(X - bf(Y), Y)(aX, Y)(X + bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(X - bf(Y), Y)(aX, Y)(X + bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?
As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(X - bf(Y), Y)(a(X + bf(Y)), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(X - bf(Y), Y)(aX + abf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(a^{-1}X, Y)(aX + abf(Y) - bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(X + bf(Y) - a^{-1}bf(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$

$$\vdots$$

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$.

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?

As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$.

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?
As soon as $(X_1 + f(X_2), X_2, \dots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$. Then $(X + f(Y), Y))$ in $\mathrm{GLIN}_2(k)$!

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?
As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$. Then $(X + f(Y), Y))$ in $\mathrm{GLIN}_2(k)$!
... if $k \neq \mathbb{F}_2$...

How does $\mathrm{GLIN}_n(k)$ compare to $\mathrm{GTAM}_n(k)$?
As soon as $(X_1 + f(X_2), X_2, \ldots, X_n) \in \mathrm{GLIN}_n(k)$ for any $f \in k[X_2]$, then $\mathrm{GLIN}_n(k) = \mathrm{GTAM}_n(k)$. Choose some $a \neq 0$ $a \neq 1$:

$$(X + b(1 - a^{-1})f(Y), Y)$$

Choose $b = (1 - a^{-1})^{-1}$. Then $(X + f(Y), Y))$ in $\mathrm{GLIN}_2(k)$!
$\ldots$ if $k \neq \mathbb{F}_2 \ldots$

Question: How does $\mathrm{GLIN}_n(\mathbb{F}_2)$ and $\mathrm{GTAM}_n(\mathbb{F}_2)$ relate?

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Theorem:

$\mathsf{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathsf{GTAM}_n(\mathbb{F}_2)$.

Proof.

Theorem:

$\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathrm{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathrm{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Theorem:

$\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathrm{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL}_n(\mathbb{F}_2)$ is even.

Theorem:

$\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneqq \mathrm{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathrm{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL}_n(\mathbb{F}_2)$ is even. Hence $\pi_2(\mathrm{GLIN}_n(\mathbb{F}_2)) \subseteq \mathrm{Alt}(2^n)$. If $n = 2$, then $(X + Y, Y)$ is odd, unfortunately.

Theorem:

$\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathrm{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL}_n(\mathbb{F}_2)$ is even. Hence $\pi_2(\mathrm{GLIN}_n(\mathbb{F}_2)) \subseteq \mathrm{Alt}(2^n)$. If $n = 2$, then $(X + Y, Y)$ is odd, unfortunately. However, in dimension 2 we understand the automorphism group, and can do a computer calculation

Theorem:

$\mathrm{GLIN}_n(\mathbb{F}_2) \subsetneq \mathrm{GTAM}_n(\mathbb{F}_2)$.

Proof. Remember, $\pi_2(TA_n(\mathbb{F}_2)) = \mathrm{Sym}(2^n)$, as $\mathbb{F}_2$ was the exception to the exception.

Now, notice that if $n \geq 3$, then any element of $\mathrm{GL}_n(\mathbb{F}_2)$ is even. Hence $\pi_2(\mathrm{GLIN}_n(\mathbb{F}_2)) \subseteq \mathrm{Alt}(2^n)$. If $n = 2$, then $(X + Y, Y)$ is odd, unfortunately. However, in dimension 2 we understand the automorphism group, and can do a computer calculation to see that

$$\frac{\#\pi_4(\mathrm{GLIN}_2(\mathbb{F}_2))}{\#\pi_4(\mathrm{GTAM}_2(\mathbb{F}_2))} = 2.$$

End proof.

Just one more slide:

Just one more slide:

I hope you got an impression of the beauty of

Affine Algebraic Geometry!

Just one more slide:

I hope you got an impression of the beauty of

Affine Algebraic Geometry!

THANK YOU

(for enduring 189 slides. . .)