# Affine algebraic geometry over finite fields

Stefan Maubach

December 2010

# Affine algebraic geometry

# Affine algebraic geometry

Study of Affine Varieties

# Affine algebraic geometry

Study of Affine Varieties

Almost always: 1-1 correspondence between *algebra* and *geometry*.

# Affine algebraic geometry

Study of Affine Varieties

Almost always: 1-1 correspondence between *algebra* and *geometry*.

**Example:**

Zero sets of polynomials

$$V := \{x \in k^n \mid f_1(x) = \ldots = f_n(x) = 0\}$$

$$\updownarrow$$

$k$-algebras

$$\mathcal{O}(V) := k[x_1, \ldots, x_n]/(f_1, \ldots, f_n)$$

# Affine algebraic geometry

Almost always: 1-1 correspondence between *algebra* and *geometry*.

**Example:**

Additive group action on $\mathbb{C}^n$

$$\updownarrow$$

Locally nilpotent derivation

$$D : \mathbb{C}[x_1, \ldots, x_n] \longrightarrow \mathbb{C}[x_1, \ldots, x_n].$$

# Affine algebraic geometry

Almost always: 1-1 correspondence between *algebra* and *geometry*.

**Example:**

Polynomial automorphisms $\mathbb{C}^n \longrightarrow \mathbb{C}^n$

(notation: $\mathrm{GA}_n(\mathbb{C})$)

$$\updownarrow$$

Ring automorphisms of $\mathbb{C}[x_1, \ldots, x_n]$.

# 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 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 $g(F_1, \ldots, F_n)$.

Group of polynomial maps having polynomial inverse $=:$ $\mathrm{GA}_n(k)$.

# Finite fields, characteristic $p$, characteristic 0: What is different?

Correspondence

$$\text{ring endomorphisms } \mathbb{F}_q[x_1, \ldots, x_n]$$
$$\longrightarrow$$
$$\text{maps } (\mathbb{F}_q)^n \longrightarrow (\mathbb{F}_q)^n$$

not injective!

$$\pi : \mathrm{GA}_n(\mathbb{F}_q) \longrightarrow \mathrm{Perm}((\mathbb{F}_q)^n)$$

has kernel: $\pi(x + y^q - y, y) = \pi(x, y)$.

# Finite fields, characteristic $p$, characteristic 0: What is different?

Even more:

# Finite fields, characteristic $p$, characteristic 0: What is different?

Even more:

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

# 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

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

$L$ linear map;

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

# Problems in AAG: Jacobian Conjecture

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.

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

# Problems in AAG: Jacobian Conjecture

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

$L$ linear map;

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

$F$ invertible, i.e.

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

# 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;

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

$F$ 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

char$(k) = 0$

$L$ linear map;

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

$F$ invertible, i.e.

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

# 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.

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

# Problems in AAG: Jacobian Conjecture

char$(k) = 0$

$L$ linear map;

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

$F$ invertible, i.e.

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

# Problems in AAG: Jacobian Conjecture

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

$L$ linear map;

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

**Jacobian Conjecture:**

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

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

$L$ linear map;

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

# 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;

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

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

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

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

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

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

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

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

# Linearization problem

Let $F \in \mathsf{GA}_n(k)$.

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$. Important to know if there exists $\varphi \in \mathrm{GA}_n(k)$ such that $\varphi^{-1}F\varphi \in \mathrm{GL}_n(k)$.

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$. Important to know if there exists $\varphi \in \mathrm{GA}_n(k)$ such that $\varphi^{-1}F\varphi \in \mathrm{GL}_n(k)$.
Needed: $F$ has a fixed point $p$. (i.e. $(X+1, Y)$ is not linearizable.)

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$. Important to know if there exists $\varphi \in \mathrm{GA}_n(k)$ such that $\varphi^{-1}F\varphi \in \mathrm{GL}_n(k)$.
Needed: $F$ has a fixed point $p$. (i.e. $(X+1, Y)$ is not linearizable.)
Main question here:
**Linearization Problem:** Let $F^s = I$ some $s$. Is $F$ linearizable?

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$. Important to know if there exists $\varphi \in \mathrm{GA}_n(k)$ such that $\varphi^{-1}F\varphi \in \mathrm{GL}_n(k)$.

Needed: $F$ has a fixed point $p$. (i.e. $(X+1, Y)$ is not linearizable.)

Main question here:

**Linearization Problem:** Let $F^s = I$ some $s$. Is $F$ linearizable?

Proven for $n = 2$.

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$.

Main question here:

**Linearization Problem:** Let $F^s = I$ some $s$. Is $F$ linearizable?

Wrong in characteristic $p$ !

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$.

Main question here:

**Linearization Problem:** Let $F^s = I$ some $s$. Is $F$ linearizable?

Wrong in characteristic $p$ !

$$F := (x + y^2, y) \longrightarrow F^m = (x + my^2, y)$$

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$.

Main question here:

**Linearization Problem:** Let $F^s = I$ some $s$. Is $F$ linearizable?

Wrong in characteristic $p$ !

$$F := (x + y^2, y) \longrightarrow F^m = (x + my^2, y)$$

$$F^p = I$$

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$.

Main question here:

**Linearization Problem:** Let $F^s = I$ some $s$. Is $F$ linearizable?

Wrong in characteristic $p$ !

$$F := (x + y^2, y) \longrightarrow F^m = (x + my^2, y)$$

$$F^p = I$$

So perhaps additional assumption:

# Linearization problem

Let $F \in \mathrm{GA}_n(k)$.

Main question here:

**Linearization Problem:** Let $F^s = I$ some $s$. Is $F$ linearizable?

Assume $p \not| s$.

Wrong in characteristic $p$ !

$$F := (x + y^2, y) \longrightarrow F^m = (x + my^2, y)$$

$$F^p = I$$

So perhaps additional assumption:

# 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:** $(X_1 + f(X_2, \dots, X_n), X_2, \dots, X_n)$,
invertible with inverse

$(X_1 - f(X_2, \dots, X_n), X_2, \dots, X_n)$.
**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.)

Natural map:

$$\begin{tikzcd} \pi_q : & \mathrm{GA}_n(\mathbb{F}_q) \arrow[r] & \mathrm{perm}(q^n) \\ & \arrow[u, hook] & \end{tikzcd}$$

Natural map:

$$\pi_q : \quad \begin{tikzcd} \mathrm{GA}_n(\mathbb{F}_q) \arrow[r] & \mathrm{perm}(q^n) \\ \mathrm{GA}_n(\mathbb{F}_p) \arrow[u, hook] & \end{tikzcd}$$

Natural map:

$$\pi_q : \quad \begin{tikzcd} \mathsf{GA}_n(\mathbb{F}_q) \arrow[r, two heads] & \pi_q(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[r, hook] & \mathrm{perm}(q^n) \\ \mathsf{GA}_n(\mathbb{F}_p) \arrow[r, two heads] \arrow[u, hook] & \pi_q(\mathsf{GA}_n(\mathbb{F}_p)) \arrow[u, hook] & \end{tikzcd}$$

Natural map:

$$\begin{tikzcd}
\pi_q : & \mathsf{GA}_n(\mathbb{F}_q) \arrow[r, two heads] & \pi_q(\mathsf{GA}_n(\mathbb{F}_q)) \arrow[r, hook] & \mathrm{perm}(q^n) \\
& \mathsf{GA}_n(\mathbb{F}_p) \arrow[u, hook] \arrow[r, two heads] & \pi_q(\mathsf{GA}_n(\mathbb{F}_p)) \arrow[u, hook] &
\end{tikzcd}$$

Question 1: wat is $\pi_q(\mathsf{GA}_n(\mathbb{F}_q))$?

Natural map:

$$\begin{tikzcd}
\pi_q : & \mathrm{GA}_n(\mathbb{F}_q) \arrow[r, two heads] & \pi_q(\mathrm{GA}_n(\mathbb{F}_q)) \arrow[r, hook] & \mathrm{perm}(q^n) \\
& \mathrm{TA}_n(\mathbb{F}_q) \arrow[r, two heads] \arrow[u, hook] & \pi_q(\mathrm{TA}_n(\mathbb{F}_q)) \arrow[u, hook] &
\end{tikzcd}$$

Question 1: wat is $\pi_q(\mathrm{GA}_n(\mathbb{F}_q))$?

Question 2: wat is $\pi_q(\mathrm{TA}_n(\mathbb{F}_q))$?

# Theorem:

If $q$ is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n).$$

# Theorem:

If $q$ is odd, or $q = 2$, then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

$$\pi_q(\mathsf{TA}_n(\mathbb{F}_q)) = \mathsf{Alt}(q^n).$$

# Theorem:

If $q$ is odd, or $q = 2$, then

$$\pi_q(\mathrm{TA}_n(\mathbb{F}_q)) = \mathrm{Sym}(q^n).$$

If $q = 4, 8, 16, \ldots$ then

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

**Obvious question:** $\pi_4(\mathrm{GA}_n(\mathbb{F}_4)) = \mathrm{Alt}(4^n)$ or $\mathrm{Sym}(4^n)$? (open since 2000). Would give a *very easy* example which is not tame!

# Proving non-tameness

**Main question:** Does $\mathrm{TA}_n(\mathbb{F}_p)$ differ from $\mathrm{GA}_n(\mathbb{F}_p)$? ($p$ power of a prime)

# Proving non-tameness

**Main question:** Does $\mathrm{TA}_n(\mathbb{F}_p)$ differ from $\mathrm{GA}_n(\mathbb{F}_p)$? ($p$ power of a prime)

**Weaker question:** Does $\pi_q \mathrm{TA}_n(\mathbb{F}_p)$ differ from $\pi_q \mathrm{GA}_n(\mathbb{F}_p)$? ($q = p^m$)

# Proving non-tameness

**Main question:** Does $\mathrm{TA}_n(\mathbb{F}_p)$ differ from $\mathrm{GA}_n(\mathbb{F}_p)$? ($p$ power of a prime)

**Weaker question:** Does $\pi_q \mathrm{TA}_n(\mathbb{F}_p)$ differ from $\pi_q \mathrm{GA}_n(\mathbb{F}_p)$? ($q = p^m$)

Check if for some $p, q$ we have: $\pi_q(N) \notin \mathrm{TA}_3(\mathbb{F}_p)$, and we've negatively answered both questions!

# Proving non-tameness

**Main question:** Does $\mathrm{TA}_n(\mathbb{F}_p)$ differ from $\mathrm{GA}_n(\mathbb{F}_p)$? ($p$ power of a prime)

**Weaker question:** Does $\pi_q \mathrm{TA}_n(\mathbb{F}_p)$ differ from $\pi_q \mathrm{GA}_n(\mathbb{F}_p)$? ($q = p^m$)

Check if for some $p, q$ we have: $\pi_q(N) \notin \mathrm{TA}_3(\mathbb{F}_p)$, and we've negatively answered both questions!

**Theorem:** For all non-tame candidate examples $C \in \mathrm{GA}_n(\mathbb{F}_p)$: for each $m \in \mathbb{N}$, there exists $T_m \in \mathrm{TA}_n(\mathbb{F}_p)$ such that $\pi_{p^m} C = \pi_{p^m} T_m$.

In short, each such map can be *mimicked* by tame maps.

# Another problem in char. $p$: Derksen's Theorem

**Theorem** (Derksen:) Let char. $k$=0. Define

$$\mathrm{DA}_3(k) := < Aff_3(k), (x + y^2, y, z) >$$

Then

$$\mathrm{DA}_3(k) = \mathrm{TA}_3(k).$$

# Another problem in char. $p$: Derksen's Theorem

**Theorem** (Derksen:) Let char. $k$=0. Define

$$\mathrm{DA}_3(k) := < Aff_3(k), (x+y^2, y, z) >$$

Then

$$\mathrm{DA}_3(k) = \mathrm{TA}_3(k).$$

Proof uses following:

Let $m \in \mathbb{N}$. Then the span of $L^m$ where $L$ runs over the polynomials homogeneous of degree 1, is the set of all homogeneous polynomials of degree $m$.

# Another problem in char. $p$: Derksen's Theorem

**Theorem** (Derksen:) Let char. $k$=0. Define

$$\mathrm{DA}_3(k) := < Aff_3(k), (x+y^2, y, z) >$$

Then

$$\mathrm{DA}_3(k) = \mathrm{TA}_3(k).$$

Proof uses following:

Let $m \in \mathbb{N}$. Then the span of $L^m$ where $L$ runs over the polynomials homogeneous of degree 1, is the set of all homogeneous polynomials of degree $m$.

Wrong in char. $k = p$!

# Another problem in char. $p$: Derksen's Theorem

**Proposition:**

$$\mathrm{DA}_3(\mathbb{F}_2) \subsetneq \mathrm{TA}_3(\mathbb{F}_2)$$

Proof:

# Another problem in char. $p$: Derksen's Theorem

**Proposition:**

$$\mathsf{DA}_3(\mathbb{F}_2) \subsetneqq \mathsf{TA}_3(\mathbb{F}_2)$$

Proof:

$$\pi_2(\mathsf{DA}_3(\mathbb{F}_2)) \subsetneqq \pi_2(\mathsf{TA}_3(\mathbb{F}_2))$$

# Another problem in char. $p$: Derksen's Theorem

**Proposition:**

$$\mathrm{DA}_3(\mathbb{F}_2) \subsetneq \mathrm{TA}_3(\mathbb{F}_2)$$

Proof:

$$\pi_2(\mathrm{DA}_3(\mathbb{F}_2)) \subsetneq \pi_2(\mathrm{TA}_3(\mathbb{F}_2))$$

**Repair:** replace $(x + y^2, y, z)$ by $(x + (yz)^{q-1}, y, z)$.

# Another problem in char. $p$: Derksen's Theorem

**Conjecture:**

$$< (x + (yz)^{q-1}, y, z), Aff_3(\mathbb{F}_q) > \neq \mathrm{TA}_3(\mathbb{F}_q)$$

# Another problem in char. $p$: Derksen's Theorem

**Conjecture:**

$$< (x + (yz)^{q-1}, y, z), Aff_3(\mathbb{F}_q) > \neq \mathrm{TA}_3(\mathbb{F}_q)$$

but there is no easy way to show this:

# Another problem in char. $p$: Derksen's Theorem

**Conjecture:**

$$< (x + (yz)^{q-1}, y, z), Aff_3(\mathbb{F}_q) > \neq \mathrm{TA}_3(\mathbb{F}_q)$$

but there is no easy way to show this:

**Theorem:**

$$\pi_{q^m} < (x + (yz)^{q-1}, y, z), Aff_3(\mathbb{F}_q) >= \pi_{q^m}\mathrm{TA}_3(\mathbb{F}_q).$$

Proof is elaborate, here and there technical, and very nontrivial!

# Equivalence of polynomials

Let $p, q \in k[x_1, \ldots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \ldots, x_n)\tau = (q, x_2, \ldots, x_n)$.

**Example:** $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

# Equivalence of polynomials

Let $p, q \in k[x_1, \ldots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \ldots, x_n)\tau = (q, x_2, \ldots, x_n)$.

**Example:** $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

**Lemma:** $p(x) \sim q(x)$ in $k[x, y_1, \ldots, y_n]$ then $p'(x) \sim q'(x)$ in $k[x]$.

# Equivalence of polynomials

Let $p, q \in k[x_1, \dots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \dots, x_n)\tau = (q, x_2, \dots, x_n)$.

**Example:** $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

**Lemma:** $p(x) \sim q(x)$ in $k[x, y_1, \dots, y_n]$ then $p'(x) \sim q'(x)$ in $k[x]$.

If $char k = 0$, this implies $p(x) \sim q(x)$ in $k[x]$.

# Equivalence of polynomials

Let $p, q \in k[x_1, \ldots, x_n]$. Define $p \sim q$ if exists $\varphi, \tau \in \mathrm{GA}_n(k)$ such that $\varphi(p, x_2, \ldots, x_n)\tau = (q, x_2, \ldots, x_n)$.

**Example:** $x^2 \sim (x + y^2)^2 + y$ in $k[x, y]$.

**Lemma:** $p(x) \sim q(x)$ in $k[x, y_1, \ldots, y_n]$ then $p'(x) \sim q'(x)$ in $k[x]$.

If $chark = 0$, this implies $p(x) \sim q(x)$ in $k[x]$.

If $chark = p \ldots$

Are $x^8 + x^4 + x$ and $x^8 + x^2 + x$ equivalent in $\mathbb{F}_2[x, y, z]$?

# Mock automorphisms

$F \in MA_n(\mathbb{F}_q)$ is called a *mock automorphism* if

- $\det(Jac(F)) \in \mathbb{F}_q^*$
- $\pi_q(F)$ is a bijection

$x^8 + x^4 + x$ and $x^8 + x^2 + x$ are mock automorphisms for $\mathbb{F}_{2^m}$ if $7 \nmid m$.

# Equivalence classes of Mock automorphisms

**Theorem:** If $F \in MA_3(\mathbb{F}_2)$ of degree $\leq 2$, then $F$ is equivalent to:

# Equivalence classes of Mock automorphisms

**Theorem:** If $F \in MA_3(\mathbb{F}_2)$ of degree $\leq 2$, then $F$ is equivalent to:

- $(x, y, z)$

# Equivalence classes of Mock automorphisms

**Theorem:** If $F \in MA_3(\mathbb{F}_2)$ of degree $\leq 2$, then $F$ is equivalent to:

- $(x, y, z)$
- $(x^4 + x^2 + x, y, z)$

# Equivalence classes of Mock automorphisms

**Theorem:** If $F \in MA_3(\mathbb{F}_2)$ of degree $\leq 2$, then $F$ is equivalent to:

- $(x, y, z)$
- $(x^4 + x^2 + x, y, z)$
- $(x^8 + x^2 + x, y, z)$
- $(x^8 + x^4 + x, y, z)$

# Equivalence classes of Mock automorphisms

**Theorem:** If $F \in MA_3(\mathbb{F}_2)$ of degree $\leq 2$, then $F$ is equivalent to:

- $(x, y, z)$
- $(x^4 + x^2 + x, y, z)$
- $(x^8 + x^2 + x, y, z)$
- $(x^8 + x^4 + x, y, z)$

. . . but are there 3 or 4 equivalence classes?

# Degree 3 over $\mathbb{F}_2$

| | Representant | Bijection over | # |
|---|---|---|---|
| **1.** | $(x, y, z)$ | all | 400 |
| **2.** | $(x, y, z + x^3z^4 + xz^2)$ | $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{16}, \mathbb{F}_{32}$ | 56 |
| **3.** | $(x, y, z + x^3z^2 + x^3z^4)$ | $\mathbb{F}_2, \mathbb{F}_4$ | 168 |
| **4.** | $(x, y, z + xz^2 + xz^6)$ | $\mathbb{F}_2$ | 336 |
| **5.** | $(x, y, z + x^3z^2 + xy^2z^4 + x^2yz^4 + x^3z^6)$ | $\mathbb{F}_2$ | 336 |
| **6.** | $(x, y, z + x^3z^2 + xy^2z^2 + x^2yz^4 + x^3z^6)$ | $\mathbb{F}_2$ | 168 |
| **7.** | $(x + y^2z, y + x^2z + y^2z, z + x^3 + xy^2 + y^3)$ | $\mathbb{F}_2$ | 56 |

# Additive group actions

Characteristic 0: $(k,+)$-action on $k^n$

Example:

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

# Additive group actions

Characteristic 0: $(k, +)$-action on $k^n$

Example:

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

$$(1 \times (x, y, z) \longrightarrow (x + y + z, y + z, z))$$

# Additive group actions

Characteristic 0: $(k, +)$-action on $k^n$

Example:

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

$$(1 \times (x, y, z) \longrightarrow (x + y + z, y + z, z))$$

Is the same as:

$$t \times (x, y, z) \longrightarrow (\exp(tD)(x), \exp(tD)(y), \exp(tD)(z))$$

where

$$D := (y + \frac{1}{2} z)\frac{\partial}{\partial x} + z\frac{\partial}{\partial y}.$$

(a *locally nilpotent derivation*)

# Additive group actions

Characteristic $p$: $(k, +)$-action on $k^n$

Example:

$$t \times (x, y, z) \longrightarrow (F_1(t, x, y, z), F_2(t, x, y, z), F_3(t, x, y, z))$$

Is the same as:

$$t \times (x, y, z) \longrightarrow (\exp(tD)(x), \exp(tD)(y), \exp(tD)(z))$$

where

$$D$$

(is a *locally finite iterative higher derivation*)

# Additive group actions char. $p$: problems

Characteristic 2: $(k,+)$-action on $k^n$

Example:

$$t \times (x,y,z) \longrightarrow (x + ty + \frac{t^2+t}{2} z, y + tz, z)$$

is NOT a $(k,+)$ action! In particular,

$$(x+y+z, y+z, z)$$

is not the exponent of a locally finite iterative higher derivation. Any $k$-action has order $p$ !

# Additive group actions char. $p$: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

# Additive group actions char. $p$: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

# Additive group actions char. $p$: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

**Theorem:** If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \; ; \; n \in \mathbb{N}\right].$$

# Additive group actions char. $p$: solution

$$t \times (x, y, z) \longrightarrow \left(x + ty + \frac{t^2 + t}{2} z, y + tz, z\right)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

**Theorem:** If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \; ; \; n \in \mathbb{N}\right].$$

**Theorem:** If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \; ; \; n \in \mathbb{N}\right].$$

# Additive group actions char. $p$: solution

$$t \times (x, y, z) \longrightarrow (x + ty + \frac{t^2 + t}{2} z, y + tz, z)$$

Do not consider $\mathbb{F}_2$-actions but consider $\mathbb{Z}$-actions!

**Theorem:** If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}) \subseteq \mathbb{Z}$ then

$$f \in \mathbb{Z}\left[\binom{x}{n} \ ; \ n \in \mathbb{N}\right].$$

**Theorem:** If $f(x) \in \mathbb{Q}[x]$ such that $f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$ then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \ ; \ n \in \mathbb{N}\right].$$

**Corollary:** If $f(x) \in \mathbb{Q}[x]$ such that $f \mod p$ makes sense, then

$$f \in \mathbb{Z}\left[\binom{x}{p^n} \ ; \ n \in \mathbb{N}\right].$$

# Additive group actions char. $p$: solution

Char$= 0$: $(x + ty + \frac{t^2+t}{2}z, y + tz, z) \in k[t][x, y, z]$

# Additive group actions char. $p$: solution

Char$=0$: $(x+ty+\frac{t^2+t}{2}z, y+tz, z)\in k[t][x,y,z]$

Char$=2$: $(x+ty+(Q_1+t)z, y+tz, z)\in k[t,Q_1][x,y,z]$

where $Q_1 := \binom{t}{2}$.

# Additive group actions char. $p$: solution

Char$=0$: $(x+ty+\frac{t^2+t}{2}z, y+tz, z) \in k[t][x,y,z]$
Char$=2$: $(x+ty+(Q_1+t)z, y+tz, z) \in k[t,Q_1][x,y,z]$
where $Q_1 := \binom{t}{2}$.
In general:

$$R := k[Q_i; i \in \mathbb{N}] \text{ where } Q_i := \binom{t}{p^i}.$$

$$F \in GA_n(R)$$

# A puzzling question:

When does a locally nilpotent derivation

$$D : \mathbb{Q}[x_1, \ldots, x_n] \longrightarrow \mathbb{Q}[x_1, \ldots, x_n]$$

induce a polynomial map

$$\exp(D) : \mathbb{Z}[x_1, \ldots, x_n] \longrightarrow \mathbb{Z}[x_1, \ldots, x_n]?$$

# Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1, \ldots, x_n+f_n \,;\; f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

# Strictly upper triangular group

$$B_n(k) := \{(x_1 + f_1, \ldots, x_n + f_n\ ;\ f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

# Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1, \ldots, x_n+f_n \; ; \; f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

$$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n), \quad \#\mathcal{B}_n(\mathbb{F}_p) = v_p(p^n!)$$

# Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1, \ldots, x_n+f_n \; ; \; f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n), \quad \#\mathcal{B}_n(\mathbb{F}_p) = v_p(p^n!)$

$\mathcal{B}_n(\mathbb{F}_p)$ is $p$-sylow subgroup of $\mathrm{sym}(\mathbb{F}_p^n)$ !

# Strictly upper triangular group

$$B_n(k) := \{(x_1+f_1, \ldots, x_n+f_n \ ; \ f_i \in k[x_{i+1}, \ldots, x_n]\} < GA_n(k).$$

$$\mathcal{B}_n(\mathbb{F}_p) := \pi_p(B_n(\mathbb{F}_p))$$

$\mathcal{B}_n(\mathbb{F}_p) < \mathrm{sym}(\mathbb{F}_p^n), \quad \#\mathcal{B}_n(\mathbb{F}_p) = v_p(p^n!)$

$\mathcal{B}_n(\mathbb{F}_p)$ is $p$-sylow subgroup of $\mathrm{sym}(\mathbb{F}_p^n)$ !

$$(x_1 + f_1, \ldots, x_n + f_n) \in \mathcal{B}_n(\mathbb{F}_p)$$

$$f_i \in k[x_{i+1}, \ldots, x_n]/(x_{i+1}^p - x_{i+1}, \ldots, x_n^p - x_n)$$

(Motivation for studying $\mathcal{B}_n(\mathbb{F}_p)$: cryptography)

# What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- To compute $\sigma^m(v)$ easily for any $m \in \mathbb{N}, v \in \mathbb{F}_p^n$.

# What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- To compute $\sigma^m(v)$ easily for any $m \in \mathbb{N}, v \in \mathbb{F}_p^n$.

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

**Proofsketch.** By induction: case $n = 1$ is clear.

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

**Proofsketch.** By induction: case $n = 1$ is clear. So,

$\sigma = (x_1 + f_1, \tilde{\sigma})$.

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

**Proofsketch.** By induction: case $n = 1$ is clear. So,

$\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$.

$\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$.

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

**Proofsketch.** By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$. $\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$. So:

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

**Proofsketch.** By induction: case $n = 1$ is clear. So, $\sigma = (x_1 + f_1, \tilde{\sigma})$. Consider $(c, \alpha) \in \mathbb{F}_p^n$.
$\sigma(c, \alpha) = (c + f_1(\alpha), \sigma(\alpha))$. So:

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

To prove: $\sum_{i=1}^{p^{n-1}} f(\tilde{\sigma}^i \alpha) = 0$ if and only if coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_1$ is nonzero.

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

**Proofsketch.**

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

# Maps having one orbit only

**Theorem 1.**

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

has one orbit if and only if for each $1 \leq i \leq n$: the coefficient of $(x_{i+1} \cdots x_n)^{p-1}$ of $f_i$ is nonzero.

**Proofsketch.**

$$\sigma^{p^{n-1}}(c, \alpha) = (c + \sum_{i=1}^{p^{n-1}} f_1(\tilde{\sigma}^i \alpha), \alpha)$$

## Lemma

*Let* $M(x_1, \ldots, x_n) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ *where* $0 \leq a_i \leq p-1$ *for each* $1 \leq i \leq n$. *Then* $\sum_{\alpha \in \mathbb{F}_p^n} M(\alpha) = 0$ *unless* $a_1 = a_2 = \ldots = a_n = p-1$, *when it is* $(-1)^n$.

# Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

**Theorem 2.** Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

Proof is very elegant but too long to elaborate on in this talk.

# Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

**Theorem 2.** Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

# Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

**Theorem 2.** Let

$$\sigma := (x_1 + f_1, \ldots, x_n + f_n)$$

have only one orbit. Then representants of the conjugacy classes are the $(p-1)^n$ maps where $f_i = \lambda_i (x_{i+1} \cdots x_n)^{p-1}$.

**Theorem 3.** After that, conjugating by a diagonal linear map $D \in \mathrm{GL}_n(\mathbb{F}_p)$ one can get all of them equivalent!

Hence, any $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ having only one orbit can be written as

$$D^{-1}\tau^{-1}\Delta\tau D$$

where $\tau \in \mathcal{B}_n(\mathbb{F}_p)$, $D$ linear diagonal, and $\Delta$ is one particular map you choose in $\mathcal{B}_n(\mathbb{F}_p)$.

# Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- To compute $\sigma^m(v)$ easily for any $m \in \mathbb{N}, v \in \mathbb{F}_p^n$.

# Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- To compute $\sigma^m(v)$ easily for any $m \in \mathbb{N}, v \in \mathbb{F}_p^n$.

Hence, any $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ having only one orbit can be written as

$$D^{-1}\tau^{-1}\Delta\tau D$$

where $\tau \in \mathcal{B}_n(\mathbb{F}_p)$, $D$ linear diagonal, and $\Delta$ is one particular map you choose in $\mathcal{B}_n(\mathbb{F}_p)$.

# Conjugacy classes in $\mathcal{B}_n(\mathbb{F}_p)$

What do we want?

- A criterion to decide when $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ is a permutation of $\mathbb{F}_p^n$ having one orbit,
- To compute $\sigma^m(v)$ easily for any $m \in \mathbb{N}, v \in \mathbb{F}_p^n$.

Hence, any $\sigma \in \mathcal{B}_n(\mathbb{F}_p)$ having only one orbit can be written as

$$D^{-1}\tau^{-1}\Delta\tau D$$

where $\tau \in \mathcal{B}_n(\mathbb{F}_p)$, $D$ linear diagonal, and $\Delta$ is one particular map you choose in $\mathcal{B}_n(\mathbb{F}_p)$.

$$\sigma^m(v) = D^{-1}\tau^{-1}\Delta^m\tau D(v)$$

# What is an easy map $\Delta$?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

# What is an easy map $\Delta$?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then $\Delta$ is very simple:

# What is an easy map $\Delta$?

$$\Delta := (x_1 + g_1, \dots, x_n + g_n)$$

where $g_i(p-1, \dots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then $\Delta$ is very simple:

Let $\zeta : \mathbb{F}_p^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, then

$$\zeta \Delta \zeta^{-1}(a) = a + 1, a \in \mathbb{Z}/p^n\mathbb{Z}$$

i.e. $\Delta^m$ is easy to compute!

# What is an easy map $\Delta$?

$$\Delta := (x_1 + g_1, \ldots, x_n + g_n)$$

where $g_i(p-1, \ldots, p-1) = 1$ and $g_i(\alpha) = 0$ for any other $\alpha \in \mathbb{F}_p^{n-i}$.

Then $\Delta$ is very simple:

Let $\zeta : \mathbb{F}_p^n \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, then

$$\zeta \Delta \zeta^{-1}(a) = a + 1, a \in \mathbb{Z}/p^n\mathbb{Z}$$

i.e. $\Delta^m$ is easy to compute! $\longrightarrow$ Cryptographic application is happy!

# Just one more slide/ conclusions:

# Just one more slide/ conclusions:

Characteristic $p$ different and the same! Some things more easy, some things more difficult.

# Just one more slide/ conclusions:

Characteristic $p$ different and the same! Some things more easy, some things more difficult.

Finite fields in particular are interesting for representing finite groups, and applications in cryptography.

# Just one more slide/ conclusions:

Characteristic $p$ different and the same! Some things more easy, some things more difficult.

Finite fields in particular are interesting for representing finite groups, and applications in cryptography.

**THANK YOU**

(for enduring 136 .pdf slides. . . )