Polynomial automorphisms over finite fields and Locally Finite Polynomial Maps

Stefan Maubach

Arpil 2008

 $F: \mathbb{C}^n \longrightarrow \mathbb{C}^n \text{ is a polynomial map if} \\ F = (F_1, \dots, F_n), F_i \in \mathbb{C}[X_1, \dots, X_n].$

 $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ is a polynomial map if $F = (F_1, \dots, F_n), F_i \in \mathbb{C}[X_1, \dots, X_n].$ Examples: all linear maps. $F: \mathbb{C}^n \longrightarrow \mathbb{C}^n \text{ is a polynomial map if}$ $F = (F_1, \dots, F_n), F_i \in \mathbb{C}[X_1, \dots, X_n].$ Examples: all linear maps. Notations:

	Linear	Polynomial
All	$ML_n(\mathbb{C})$	$MA_n(\mathbb{C})$
Invertible	$GL_n(\mathbb{C})$	$GA_n(\mathbb{C})$

BIG STUPID CLAIM:

Why this bold claim?

Why this bold claim?Polynomial maps seem to have similar properties as linear maps (much more so than holomorphic maps for example).

Why this bold claim?Polynomial maps seem to have similar properties as linear maps (much more so than holomorphic maps for example). Well...to be honest, most are conjectures...

Why this bold claim?Polynomial maps seem to have similar properties as linear maps (much more so than holomorphic maps for example). Well...to be honest, most are conjectures... Let's look at a few of these conjectures!

L = (aX + bY, cX + dY) in $ML_2(\mathbb{C})$

$$\begin{split} L &= (aX + bY, cX + dY) \text{ in } ML_2(\mathbb{C}) \\ & \det \left(\begin{array}{c} a & b \\ c & d \end{array} \right) \in \mathbb{C}^* \Longleftrightarrow L \in GL_2(\mathbb{C}) \end{split}$$

$$\begin{split} L &= (aX + bY, cX + dY) \text{ in } ML_2(\mathbb{C}) \\ &\det \left(\begin{array}{c} a & b \\ c & d \end{array} \right) \in \mathbb{C}^* \Longleftrightarrow L \in GL_2(\mathbb{C}) \end{split}$$

 $F = (F_1, F_2) \in MA_2(\mathbb{C})$

$$L = (aX + bY, cX + dY)$$
 in $ML_2(\mathbb{C})$
 $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{C}^* \iff L \in GL_2(\mathbb{C})$

 $F = (F_1, F_2) \in MA_2(\mathbb{C})$

$$\det \begin{pmatrix} \frac{\partial F_1}{\partial X} & \frac{\partial F_1}{\partial Y} \\ \frac{\partial F_2}{\partial X} & \frac{\partial F_2}{\partial Y} \end{pmatrix} \in \mathbb{C}^* \iff F \in GA_2(\mathbb{C})$$

$$\begin{split} L &= (aX + bY, cX + dY) \text{ in } ML_2(\mathbb{C}) \\ &\det \left(\begin{array}{c} a & b \\ c & d \end{array}\right) \in \mathbb{C}^* \Longleftrightarrow L \in GL_2(\mathbb{C}) \end{split}$$

 $F = (F_1, F_2) \in MA_2(\mathbb{C})$

$$\det \left(\begin{array}{cc} \frac{\partial F_1}{\partial X} & \frac{\partial F_1}{\partial Y} \\ \frac{\partial F_2}{\partial X} & \frac{\partial F_2}{\partial Y} \end{array}\right) \in \mathbb{C}^* \iff F \in GA_2(\mathbb{C})$$

Jacobian Conjecture in dimension n (JC(n)): Let $F \in MA_n(\mathbb{C})$. Then

$$det(Jac(F)) \in \mathbb{C}^* \Rightarrow F$$
 is invertible.

Let V be a vector space. Then

$$V \times \mathbb{C} \cong \mathbb{C}^{n+1} \Longrightarrow V \cong \mathbb{C}^n.$$

Let V be a vector space. Then

$$V \times \mathbb{C} \cong \mathbb{C}^{n+1} \Longrightarrow V \cong \mathbb{C}^n.$$

Cancelation Problem:

Let V be a variety. Then

$$V \times \mathbb{C} \cong \mathbb{C}^{n+1} \Longrightarrow V \cong \mathbb{C}^n.$$

$GL_n(\mathbb{C})$ is generated by

 $GL_n(\mathbb{C})$ is generated by

• Permutations $X_1 \longleftrightarrow X_i$

- $GL_n(\mathbb{C})$ is generated by
 - Permutations $X_1 \longleftrightarrow X_i$

▶ Map
$$(aX_1 + bX_j, X_2, \dots, X_n)$$
 $(a \in \mathbb{C}^*, b \in \mathbb{C})$

 $GL_n(\mathbb{C})$ is generated by

• Permutations
$$X_1 \longleftrightarrow X_i$$

▶ Map
$$(aX_1 + bX_j, X_2, \dots, X_n)$$
 $(a \in \mathbb{C}^*, b \in \mathbb{C})$

 $GA_n(\mathbb{C})$ is generated by ???

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

 $(X_1 - f(X_2, ..., X_n), X_2, ..., X_n).$ Triangular map: (X + f(Y, Z), Y + g(Z), Z + c)

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

 $(X_1 - f(X_2, ..., X_n), X_2, ..., X_n).$ Triangular map: (X + f(Y, Z), Y + g(Z), Z + c)

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

 $J_n(\mathbb{C}):=$ set of triangular maps.

 $(X_1 - f(X_2, ..., X_n), X_2, ..., X_n).$ 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) $J_n(\mathbb{C}) := \text{ set of triangular maps.}$ $Aff_n(\mathbb{C}) := \text{ set of compositions of invertible linear maps and translations.}$

 $(X_1 - f(X_2, ..., X_n), X_2, ..., X_n).$ 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) $J_n(\mathbb{C}) := \text{ set of triangular maps.}$ $Aff_n(\mathbb{C}) := \text{ set of compositions of invertible linear maps and translations.}$

 $TA_n(\mathbb{C}) := < J_n(\mathbb{C}), Aff_n(\mathbb{C}) >$

Question: $TA_n(\mathbb{C}) = GA_n(\mathbb{C})$?

Question:
$$TA_n(\mathbb{C}) = GA_n(\mathbb{C})$$
?
 $n = 2$: (Jung-v/d Kulk, 1942)
 $TA_n(\mathbb{C}) = GA_n(\mathbb{C})$

Question: $TA_n(\mathbb{C}) = GA_n(\mathbb{C})$? n = 2: (Jung-v/d Kulk, 1942) $TA_n(\mathbb{C}) = GA_n(\mathbb{C})$

Nagata's map:

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

Question: $TA_n(\mathbb{C}) = GA_n(\mathbb{C})$? n = 2: (Jung-v/d Kulk, 1942) $TA_n(\mathbb{C}) = GA_n(\mathbb{C})$

Nagata's map:

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

n = 3:(Shestakov-Umirbaev, 2004) Nagata's map not tame, i.e. $GA_3(\mathbb{C}) \neq TA_3(\mathbb{C})$ First subject: Polynomial maps over finite fields

Consider $\varphi \in GA_n(\mathbb{F}_q)$. Induces bijection $\mathcal{E}(\varphi) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, i.e. $\mathcal{E}(\varphi) \in Sym(q^n)$. First subject: Polynomial maps over finite fields

Consider $\varphi \in GA_n(\mathbb{F}_q)$. Induces bijection $\mathcal{E}(\varphi) : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, i.e. $\mathcal{E}(\varphi) \in Sym(q^n)$. Question: what is $\mathcal{E}(\mathcal{T}_n(\mathbb{F}_q))$? Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? $T_n(\mathbb{F}_q)$ is generated by $\operatorname{GL}_n(\mathbb{F}_q)$ (for which we have a finite set of generators) and maps of the form

$$\sigma_f := (X_1 + f, X_2, \ldots, X_n)$$

where $f \in \mathbb{F}_q[X_2, \ldots, X_n]$.

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

 $T_n(\mathbb{F}_q)$ is generated by $GL_n(\mathbb{F}_q)$ (for which we have a finite set of generators) and maps of the form

$$\sigma_f := (X_1 + f, X_2, \ldots, X_n)$$

where $f \in \mathbb{F}_q[X_2, ..., X_n]$. Let $\alpha \in \mathbb{F}_q^{n-1}$, $f \in \mathbb{F}_q[X_2, ..., X_n]$, f_α be such that $f(\alpha)(\alpha) = 1$ and 0 otherwise.

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

 $T_n(\mathbb{F}_q)$ is generated by $GL_n(\mathbb{F}_q)$ (for which we have a finite set of generators) and maps of the form

$$\sigma_f := (X_1 + f, X_2, \ldots, X_n)$$

where $f \in \mathbb{F}_q[X_2, \ldots, X_n]$. Let $\alpha \in \mathbb{F}_q^{n-1}$, $f \in \mathbb{F}_q[X_2, \ldots, X_n]$, f_α be such that $f(\alpha)(\alpha) = 1$ and 0 otherwise. Then we can restrict to the

$$\sigma_{\alpha} := \sigma_{f_{\alpha}}.$$

which is a finite set.

Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? Hence, take the following set:
Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? Hence, take the following set:

$$\sigma_{\alpha} := (X_1 + f_{\alpha}, X_2, \ldots, X_n)$$

Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? Hence, take the following set:

$$\sigma_{\alpha} := (X_1 + f_{\alpha}, X_2, \dots, X_n)$$

$$\sigma_i := X_1 \leftrightarrow X_i$$

Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? Hence, take the following set:

$$\sigma_{\alpha} := (X_1 + f_{\alpha}, X_2, \dots, X_n)$$

$$\sigma_i := X_1 \leftrightarrow X_i$$

$$\tau := (aX_1, X_2, \dots, X_n)$$

where $\langle a \rangle = \mathbb{F}_q^*$.

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

Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? (1) $\mathcal{E}(T_n(\mathbb{F}_q))$ is transitive - even stronger, it is *primitive*.

Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? (1) $\mathcal{E}(T_n(\mathbb{F}_q))$ is transitive - even stronger, it is *primitive*. You might know: if H < Sym(m) is transitive + has a 2-cycle then H = Sym(m). Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? (1) $\mathcal{E}(T_n(\mathbb{F}_q))$ is transitive - even stronger, it is *primitive*. You might know: if H < Sym(m) is transitive + has a 2-cycle then H = Sym(m).

If q = 2 or q odd, then indeed we find a 2-cycle! (τ , or σ_i).

Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? (1) $\mathcal{E}(T_n(\mathbb{F}_q))$ is transitive - even stronger, it is *primitive*. You might know: if H < Sym(m) is transitive + has a 2-cycle then H = Sym(m). If q = 2 or q odd, then indeed we find a 2-cycle! $(\tau, \text{ or } \sigma_i)$. Hence if q = 2 or q = odd, then $\mathcal{E}(T_n(\mathbb{F}_q)) = \text{Sym}(q^n)$. Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$?

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

Question: what is $\mathcal{E}(\mathcal{T}_n(\mathbb{F}_q))$? Answer: if q = 2 or q = odd, then $\mathcal{E}(\mathcal{T}_n(\mathbb{F}_q)) = \text{Sym}(q^n)$. If $q = 4, 8, 16, \ldots$ then we can only find a 3-cycle. Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? Answer: if q = 2 or q = odd, then $\mathcal{E}(T_n(\mathbb{F}_q)) = \text{Sym}(q^n)$. If $q = 4, 8, 16, \ldots$ then we can only find a 3-cycle. But: there's another theorem:

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

Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? Answer: if q = 2 or q = odd, then $\mathcal{E}(T_n(\mathbb{F}_q)) = \text{Sym}(q^n)$. If $q = 4, 8, 16, \ldots$ then we can only find a 3-cycle. But: there's another theorem:

Theorem: H < Sym(m) Primitive + 3-cycle $\longrightarrow H = \text{Alt}(m)$ or H = Sym(m). Hence if q = 4, 8, 16, ... then $\mathcal{E}(T_n(\mathbb{F}_q))$ is either Alt(m) or Sym(m). Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$?

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

If $q = 4, 8, 16, \ldots$ then we can only find a 3-cycle. But:

there's another theorem:

Theorem: H < Sym(m) Primitive $+ 3\text{-cycle} \longrightarrow H = \text{Alt}(m)$ or H = Sym(m). Hence if q = 4, 8, 16, ... then $\mathcal{E}(T_n(\mathbb{F}_q))$ is either Alt(m) or Sym(m). But $- \mathcal{E}(\sigma_\alpha, \mathcal{E}(\sigma_i), \mathcal{E}(\tau))$ are all even ! Hence $\mathcal{E}(T_n(\mathbb{F}_q)) = \text{Alt}(m)$! Question: what is $\mathcal{E}(T_n(\mathbb{F}_q))$? Answer: if q = 2 or q = odd, then $\mathcal{E}(T_n(\mathbb{F}_q)) = \text{Sym}(q^n)$. Answer: if $q = 4, 8, 16, 32, \dots$ then $\mathcal{E}(T_n(\mathbb{F}_q)) = \text{Alt}(q^n)$. Question: what is $\mathcal{E}(\mathcal{T}_n(\mathbb{F}_q))$? Answer: if q = 2 or q = odd, then $\mathcal{E}(\mathcal{T}_n(\mathbb{F}_q)) = \text{Sym}(q^n)$. Answer: if q = 4, 8, 16, 32, ... then $\mathcal{E}(\mathcal{T}_n(\mathbb{F}_q)) = \text{Alt}(q^n)$. **Problem:** Do there exist "odd" polynomial automorphisms over \mathbb{F}_4 ?

(1) $\mathsf{T}_n(\mathbb{F}_4) \neq \mathsf{GA}_n(\mathbb{F}_4).$

 $\begin{array}{l} (1) \ \mathsf{T}_n(\mathbb{F}_4) \neq \mathsf{GA}_n(\mathbb{F}_4). \\ (2) \ \mathsf{GA}_n(\mathbb{F}_4) \neq < \mathsf{GLIN}_n(\mathbb{F}_4) >. \end{array}$

(1)
$$T_n(\mathbb{F}_4) \neq GA_n(\mathbb{F}_4).$$

(2) $GA_n(\mathbb{F}_4) \neq \subset GLIN_n(\mathbb{F}_4) >.$
(3) (if $n = 3$:) $GA_3(\mathbb{K}) \neq \subset Aff_3(\mathbb{K}), GA_2(\mathbb{K}[Z]) >.$

If we want to have any hope of applying polynomial maps to the same things we apply linear maps to - then we need to understand them better - give them a better theoretical foundation!

If we want to have any hope of applying polynomial maps to the same things we apply linear maps to - then we need to understand them better - give them a better theoretical foundation!

Now let's be ambitious. What is the strongest theorem in linear algebra. Tell me!

If we want to have any hope of applying polynomial maps to the same things we apply linear maps to - then we need to understand them better - give them a better theoretical foundation!

Now let's be ambitious. What is the strongest theorem in linear algebra. Tell me!

Very good: the Cayley-Hamilton theorem (characteristic polynomials of linear maps etc.).

If we want to have any hope of applying polynomial maps to the same things we apply linear maps to - then we need to understand them better - give them a better theoretical foundation!

Now let's be ambitious. What is the strongest theorem in linear algebra. Tell me!

Very good: the Cayley-Hamilton theorem (characteristic polynomials of linear maps etc.).

Now, let's try to make a Cayley-Hamilton theorem for polynomial maps!

If we want to have any hope of applying polynomial maps to the same things we apply linear maps to - then we need to understand them better - give them a better theoretical foundation!

Now let's be ambitious. What is the strongest theorem in linear algebra. Tell me!

Very good: the Cayley-Hamilton theorem (characteristic polynomials of linear maps etc.).

Now, let's try to make a Cayley-Hamilton theorem for polynomial maps! (Perhaps the constant term can replace that stupid det(Jac(F)) = 1 requirement!)

٠

$$(3X + Y^2, 2Y) = F$$

٠

(27X +	$37Y^{2}$,8Y)	$=F^3$
(9X +	$7Y^{2}$,4Y)	$= F^2$
(3X +	Y^2	,2Y)	= F
(X		, Y)	= 1

.

1	(27X +	$37Y^{2}$,8Y)	$=F^3$
— 9	(9X +	$7Y^2$,4Y)	$= F^2$
26	(3X +	Y^2	,2Y)	= F
- 24	(X		, Y)	= 1

.

- 24	(X		, Y)	= 1
26	(3X +	Y^2	,2Y)	= F
- 9	(9X +	$7Y^{2}$,4Y)	$= F^2$
1	(27X +	$37Y^{2}$,8Y)	$=F^{3}$

.

- 9	(9X +	$7Y^2$,4Y)	$=F^2$
26	(3X +	Y^2	,2Y)	= F
- 24	(X		, Y)	= 1
0	(0		, 0)	

.

F zero of $T^3 - 9T^2 + 26T - 24$

1	(27X +	37 Y ²	,8Y)	$= F^3$	
— 9	(9 <i>X</i> +	$7Y^{2}$,4Y)	$= F^2$	
26	(3X +	Y^2	,2Y)	= F	
- 24	(X		, Y)	= 1	
0	(0		,0)		

F zero of $T^3 - 9T^2 + 26T - 24 = (T - 2)(T - 3)(T - 4)$.

Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

 $P_L(T) := det(TI - L).$

Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

$$P_L(T) := det(TI - L).$$

What about generalizing $ML_n(\mathbb{C}) \longrightarrow MA_n(\mathbb{C})$?

Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

$$P_L(T) := det(TI - L).$$

What about generalizing $ML_n(\mathbb{C}) \longrightarrow MA_n(\mathbb{C})$? EXAMPLE: Let $F = (X^2, Y^2)$.

Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

$$P_L(T) := det(TI - L).$$

What about generalizing $ML_n(\mathbb{C}) \longrightarrow MA_n(\mathbb{C})$? EXAMPLE: Let $F = (X^2, Y^2)$. Then $deg(F^n) = 2^n$.
Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

$$P_L(T) := det(TI - L).$$

What about generalizing $ML_n(\mathbb{C}) \longrightarrow MA_n(\mathbb{C})$? EXAMPLE: Let $F = (X^2, Y^2)$. Then $deg(F^n) = 2^n$. There exists no relation $F^n + a_{n-1}F^{n-1} + \ldots + a_1F + a_0I = 0$.

Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

$$P_L(T) := det(TI - L).$$

What about generalizing $ML_n(\mathbb{C}) \longrightarrow MA_n(\mathbb{C})$? EXAMPLE: Let $F = (X^2, Y^2)$. Then $deg(F^n) = 2^n$. There exists no relation $F^n + a_{n-1}F^{n-1} + \ldots + a_1F + a_0I = 0$. GR! It will not work!

Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

$$P_L(T) := det(TI - L).$$

What about generalizing $ML_n(\mathbb{C}) \longrightarrow MA_n(\mathbb{C})$? EXAMPLE: Let $F = (X^2, Y^2)$. Then $deg(F^n) = 2^n$. There exists no relation $F^n + a_{n-1}F^{n-1} + \ldots + a_1F + a_0I = 0$. GR! It will not work! But...

Let $L: \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a linear map. Then L is a zero of

$$P_L(T) := det(TI - L).$$

What about generalizing $ML_n(\mathbb{C}) \longrightarrow MA_n(\mathbb{C})$? EXAMPLE:

Let
$$F = (X^2, Y^2)$$
. Then $deg(F^n) = 2^n$.

There exists no relation

 $F^n + a_{n-1}F^{n-1} + \ldots + a_1F + a_0I = 0$. GR! It will not work! But... **Definition:** If *F* is a zero of some $P(T) \in \mathbb{C}[T] \setminus \{0\}$, then we will call *F* a Locally Finite Polynomial Endomorphism (short LFPE).

Definition:

If F is a zero of some $P(T) \in \mathbb{C}[T] \setminus \{0\}$, then we will call F a Locally Finite Polynomial Endomorphism (short LFPE).

Definition:

If *F* is a zero of some $P(T) \in \mathbb{C}[T] \setminus \{0\}$, then we will call *F* a Locally Finite Polynomial Endomorphism (short LFPE). Let's be a little less ambitious and study this set.

Definition:

If *F* is a zero of some $P(T) \in \mathbb{C}[T] \setminus \{0\}$, then we will call *F* a Locally Finite Polynomial Endomorphism (short LFPE). Let's be a little less ambitious and study this set. LFPE's should resemble linear maps more than general polynomial maps!

Some Remarks (1/3): $I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$

 $I_f := \{P(T) \in R[T] \mid P(F) = 0\}$ is an ideal of R[T].

 $I_f := \{P(T) \in R[T] \mid P(F) = 0\}$ is an ideal of R[T]. Proof:

 $r_2 f^2 + r_1 f + r_0 = 0$ and $r_4 f + r_5 = 0$ (i.e. $r_2 T^2 + r_1 T + r_0, r_4 T + r_5 \in I_f$)

 $I_f := \{P(T) \in R[T] \mid P(F) = 0\}$ is an ideal of R[T]. Proof:

$$r_2f^2 + r_1f + r_0 = 0$$
 and $r_4f + r_5 = 0$ (i.e.
 $r_2T^2 + r_1T + r_0, r_4T + r_5 \in I_f$) then
0

 $I_f := \{P(T) \in R[T] \mid P(F) = 0\}$ is an ideal of R[T]. Proof:

 $r_2 f^2 + r_1 f + r_0 = 0$ and $r_4 f + r_5 = 0$ (i.e. $r_2 T^2 + r_1 T + r_0, r_4 T + r_5 \in I_f$) then 0 = 0(f)

 $I_f := \{P(T) \in R[T] \mid P(F) = 0\}$ is an ideal of R[T]. Proof:

 $r_2 f^2 + r_1 f + r_0 = 0 \text{ and } r_4 f + r_5 = 0 \text{ (i.e.}$ $r_2 T^2 + r_1 T + r_0, r_4 T + r_5 \in I_f \text{) then}$ $0 = 0(f) = (r_2 f^2 + r_1 f + r_0)(f)$

 $I_f := \{P(T) \in R[T] \mid P(F) = 0\}$ is an ideal of R[T]. Proof:

 $r_2 f^2 + r_1 f + r_0 = 0$ and $r_4 f + r_5 = 0$ (i.e. $r_2 T^2 + r_1 T + r_0, r_4 T + r_5 \in I_f$) then $0 = 0(f) = (r_2 f^2 + r_1 f + r_0)(f) = (r_2 f^3 + r_1 f^2 + r_0 f),$

 $I_f := \{P(T) \in R[T] \mid P(F) = 0\}$ is an ideal of R[T]. Proof:

 $r_2 f^2 + r_1 f + r_0 = 0$ and $r_4 f + r_5 = 0$ (i.e. $r_2 T^2 + r_1 T + r_0, r_4 T + r_5 \in I_f$) then $0 = 0(f) = (r_2 f^2 + r_1 f + r_0)(f) = (r_2 f^3 + r_1 f^2 + r_0 f)$, hence $(r_2 T^2 + r_1 T + r_0)(T) \in I_f$,

$$I_f := \{P(T) \in R[T] \mid P(F) = 0\}$$
 is an ideal of $R[T]$.
Proof:

$$r_2f^2 + r_1f + r_0 = 0$$
 and $r_4f + r_5 = 0$ (i.e.
 $r_2T^2 + r_1T + r_0, r_4T + r_5 \in I_f$) then
 $0 = 0(f) = (r_2f^2 + r_1f + r_0)(f) = (r_2f^3 + r_1f^2 + r_0f)$, hence
 $(r_2T^2 + r_1T + r_0)(T) \in I_f$,
 $0 = r_2f^2 + r_1f + r_0 + r_4f + r_5$,

$$I_f := \{P(T) \in R[T] \mid P(F) = 0\}$$
 is an ideal of $R[T]$.
Proof:

$$r_2f^2 + r_1f + r_0 = 0$$
 and $r_4f + r_5 = 0$ (i.e.
 $r_2T^2 + r_1T + r_0, r_4T + r_5 \in I_f$) then
 $0 = 0(f) = (r_2f^2 + r_1f + r_0)(f) = (r_2f^3 + r_1f^2 + r_0f)$, hence
 $(r_2T^2 + r_1T + r_0)(T) \in I_f$,
 $0 = r_2f^2 + r_1f + r_0 + r_4f + r_5$, hence
 $r_2T^2 + r_1T + r_0 + r_4T + r_5 \in I_f$.

Corollary: if R is a field, there is a unique minimum polynomial

Some Remarks (2/3):

An example:

An example: the permutation $\sigma = (012)$ of \mathbb{F}_3 is a zero of $T^3 - 1$, as $\sigma^3 - I = 0$.

An example: the permutation $\sigma = (012)$ of \mathbb{F}_3 is a zero of $T^3 - 1$, as $\sigma^3 - I = 0$. But even $\sigma^2 + \sigma + I = 0$, just look:

$$(\sigma^2 + \sigma + I) \begin{pmatrix} 0\\1\\2 \end{pmatrix}$$

An example: the permutation $\sigma = (012)$ of \mathbb{F}_3 is a zero of $T^3 - 1$, as $\sigma^3 - I = 0$. But even $\sigma^2 + \sigma + I = 0$, just look:

$$(\sigma^2 + \sigma + I) \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = 0$$

An example: the permutation $\sigma = (012)$ of \mathbb{F}_3 is a zero of $T^3 - 1$, as $\sigma^3 - I = 0$. But even $\sigma^2 + \sigma + I = 0$, just look:

$$(\sigma^2 + \sigma + I) \begin{pmatrix} 0\\1\\2 \end{pmatrix} = \begin{pmatrix} 2\\0\\1 \end{pmatrix} + \begin{pmatrix} 1\\2\\0 \end{pmatrix} + \begin{pmatrix} 0\\1\\2 \end{pmatrix} = 0$$

Note: $T^2 + T + 1$ divides $T^3 - 1$.

An example: the permutation $\sigma = (012)$ of \mathbb{F}_3 is a zero of $T^3 - 1$, as $\sigma^3 - I = 0$. But even $\sigma^2 + \sigma + I = 0$, just look:

$$(\sigma^2 + \sigma + I) \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} = 0$$

Note: $T^2 + T + 1$ divides $T^3 - 1$. Here, $\mathfrak{m}_{\sigma} = T^2 + T + 1$.

Some Remarks (3/3):

$I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$

$I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$

Specific for polynomial maps:

 $I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$ Specific for polynomial maps:

F is LFPE $\iff \{deg(F^n)\}_{n\in\mathbb{N}}$ is bounded.

 $I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$

Specific for polynomial maps:

F is LFPE $\iff \{deg(F^n)\}_{n\in\mathbb{N}}$ is bounded.

 $(F^n = \sum_{i=0}^{n-1} a_i F^i$ is equivalent to $\{I, F, F^2, \ldots\}$ generates a finite dimensional \mathbb{C} -vector space.)

 $I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$

Specific for polynomial maps:

F is LFPE $\iff \{ deg(F^n) \}_{n \in \mathbb{N}}$ is bounded. $(F^n = \sum_{i=0}^{n-1} a_i F^i \text{ is equivalent to } \{I, F, F^2, \ldots\}$ generates a finite dimensional \mathbb{C} -vector space.) *F* is LFPE $\iff G^{-1}FG$ is LFPE

 $I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$

Specific for polynomial maps:

F is LFPE $\iff \{ deg(F^n) \}_{n \in \mathbb{N}}$ is bounded. $(F^n = \sum_{i=0}^{n-1} a_i F^i \text{ is equivalent to } \{I, F, F^2, \ldots\}$ generates a finite dimensional \mathbb{C} -vector space.) *F* is LFPE $\iff G^{-1}FG$ is LFPE

Proof: due to the second remark.

 $I_F := \{P(T) \in \mathbb{C}[T] \mid P(F) = 0\}$ is an ideal of $\mathbb{C}[T]$

Specific for polynomial maps:

F is LFPE $\iff \{deg(F^n)\}_{n \in \mathbb{N}}$ is bounded.

 $(F^n = \sum_{i=0}^{n-1} a_i F^i$ is equivalent to $\{I, F, F^2, \ldots\}$ generates a finite dimensional \mathbb{C} -vector space.)

F is LFPE $\iff G^{-1}FG$ is LFPE

Proof: due to the second remark.

But: the minimum polynomial may change if G is not linear!



$F := (3X + Y^2, Y)$. (Question: Define $F^{\sqrt{2}}$)

Example:

$F := (3X + Y^2, Y).$ (Question: Define $F^{\sqrt{2}}$) $F^2 = (9X + 4Y^2, Y),$

Example:

$$F := (3X + Y^2, Y). \quad (\text{Question: Define } F^{\sqrt{2}})$$

$$F^2 = (9X + 4Y^2, Y),$$
So $F^2 - 4F + 3I = 0$, F zero of
$$T^2 - 4T + 3 = (T - 1)(T - 3).$$

Example:

$$F := (3X + Y^2, Y). \quad (\text{Question: Define } F^{\sqrt{2}})$$

$$F^2 = (9X + 4Y^2, Y),$$
So $F^2 - 4F + 3I = 0$, F zero of
$$T^2 - 4T + 3 = (T - 1)(T - 3).$$
(NOT $(F - I) \circ (F - 3I) = 0.$)
Example:

$$F := (3X + Y^2, Y). \quad (\text{Question: Define } F^{\sqrt{2}})$$

$$F^2 = (9X + 4Y^2, Y),$$
So $F^2 - 4F + 3I = 0, F$ zero of
 $T^2 - 4T + 3 = (T - 1)(T - 3).$
(NOT $(F - I) \circ (F - 3I) = 0.$)
...

$$F^n = (3^n X + \frac{1}{2}(3^n - 1)Y^2, Y)$$

$$F^n = (3^n X + \frac{1}{2}(3^n - 1)Y^2, Y), n \in \mathbb{N}.$$

$$F^n = (3^n X + \frac{1}{2}(3^n - 1)Y^2, Y), n \in \mathbb{N}.$$

We can define
 $F_t = (3^t X + \frac{1}{2}(3^t - 1)Y^2, Y), t \in \mathbb{C}.$

 $F^{n} = (3^{n}X + \frac{1}{2}(3^{n} - 1)Y^{2}, Y), n \in \mathbb{N}.$ We can define $F_{t} = (3^{t}X + \frac{1}{2}(3^{t} - 1)Y^{2}, Y), t \in \mathbb{C}.$ $F_{t}F_{u} = F_{t+u} \text{ so } F_{t} ; t \in \mathbb{C} \text{ is a flow.}$ (Means you can write $F_{t} = F^{t}.$) $F^{n} = (3^{n}X + \frac{1}{2}(3^{n} - 1)Y^{2}, Y), n \in \mathbb{N}.$ We can define $F_{t} = (3^{t}X + \frac{1}{2}(3^{t} - 1)Y^{2}, Y), t \in \mathbb{C}.$ $F_{t}F_{u} = F_{t+u}$ so F_{t} ; $t \in \mathbb{C}$ is a flow. (Means you can write $F_{t} = F^{t}.$)

We (may) get back on that...

 $F^{n} = (3^{n}X + \frac{1}{2}(3^{n} - 1)Y^{2}, Y), n \in \mathbb{N}.$ We can define $F_{t} = (3^{t}X + \frac{1}{2}(3^{t} - 1)Y^{2}, Y), t \in \mathbb{C}.$ $F_{t}F_{u} = F_{t+u} \text{ so } F_{t} ; t \in \mathbb{C} \text{ is a flow.}$ (Means you can write $F_{t} = F^{t}.$)

We (may) get back on that... First some results!

Two essential cases:

Two essential cases: F = (aX + P(Y), bY)

Two essential cases:

$$F = (aX + P(Y), bY)$$

$$F = (aX + YP(X, Y), 0)$$

Two essential cases:

F = (aX + P(Y), bY)

F = (aX + YP(X, Y), 0)Zero of $T^2 - aT$.

Two essential cases:

$$F = (aX + P(Y), bY)$$

Zero of $(T - b)(T - a)(T - a^2) \cdots (T - a^d)$, $d = deg(P)$
 $F = (aX + YP(X, Y), 0)$
Zero of $T^2 - aT$.

Two essential cases:

 $F = (aX + P(Y), bY) \quad (F \text{ invertible})$ Zero of $(T - b)(T - a)(T - a^2) \cdots (T - a^d)$, d = deg(P) $F = (aX + YP(X, Y), 0) \quad (F \text{ not invertible})$ Zero of $T^2 - aT$.

F is LFPE, F(0) = 0.

$$\begin{array}{ll} F \text{ is LFPE, } F(0) = 0 \ . \\ F \text{ invertible} & \Longleftrightarrow & F \text{ is conjugate of} \\ & & (aX + P(Y), bY) \\ & & a, b \in \mathbb{C}^*, P(Y) \in \mathbb{C}[Y]. \end{array}$$

$$\begin{array}{ll} F \text{ is LFPE, } F(0) = 0 \ . \\ F \text{ invertible} & \Longleftrightarrow & F \text{ is conjugate of} \\ & & (aX + P(Y), bY) \\ & & a, b \in \mathbb{C}^*, P(Y) \in \mathbb{C}[Y]. \end{array}$$

 $\begin{array}{ll} F \text{ not invertible} & \Longleftrightarrow & F \text{ is conjugate of} \\ & (aX+YP(X,Y),0) \\ & a, \in \mathbb{C}, P(X,Y) \in \mathbb{C}[X,Y]. \end{array}$

- F is LFPE, and F(0) = 0. Let d = deg(F).
- Let L be the linear part of F.

F is LFPE, and F(0) = 0. Let d = deg(F). Let L be the linear part of F. Then F is a zero of

F is LFPE, and F(0) = 0. Let d = deg(F). Let L be the linear part of F. Then F is a zero of

$$P_F(T) := \prod_{\substack{0 \le k \le d-1 \\ 0 \le m \le d \\ (k,m) \ne (0,0)}} (T^2 - (detL^k)(TrL^m)T + det(L^{2k+m})).$$

Equivalent are:



► *F* is LFPE

Equivalent are:

- ► F is LFPE
- ► deg(F^m) is bounded

Equivalent are:

- ► F is LFPE
- ► deg(F^m) is bounded

•
$$n = 2$$
: $deg(F^2) \le deg(F)$

```
Equivalent are:
```

- ► *F* is LFPE
- ▶ deg(F^m) is bounded

•
$$n = 2$$
: $deg(F^2) \le deg(F)$

Conjecture: in dimension *n*, *F* is LFPE $\iff deg(F^m) \leq deg(F)^{n-1}$ for all $m \in \mathbb{N}$.

Let $D := max_{m \in \mathbb{N}}(deg(F^m))$. (note: conjecture $D = d^{n-1}$)

Let $D := \max_{m \in \mathbb{N}} (deg(F^m))$. (note: conjecture $D = d^{n-1}$) Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of the linear part of F.

Let $D := \max_{m \in \mathbb{N}} (deg(F^m))$. (note: conjecture $D = d^{n-1}$) Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of the linear part of F. Then F is a zero of

Let $D := \max_{m \in \mathbb{N}} (deg(F^m))$. (note: conjecture $D = d^{n-1}$) Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of the linear part of F. Then F is a zero of

(where
$$\lambda^{\alpha} = \lambda_1^{\alpha_1} \cdots \lambda_n^{\alpha_n}$$
)

Let $D := \max_{m \in \mathbb{N}} (deg(F^m))$. (note: conjecture $D = d^{n-1}$) Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of the linear part of F. Then F is a zero of

$$\prod_{\alpha \in \mathbb{N}^n} \quad (T - \lambda^{\alpha})$$

(where $\lambda^{\alpha} = \lambda_1^{\alpha_1} \cdots \lambda_n^{\alpha_n}$)

Let $D := \max_{m \in \mathbb{N}} (deg(F^m))$. (note: conjecture $D = d^{n-1}$) Let $\lambda_1, \ldots, \lambda_n$ be the eigenvalues of the linear part of F. Then F is a zero of

$$\prod_{\substack{\alpha \in \mathbb{N}^n \\ \mathbf{0} < |\alpha| \le D}} (T - \lambda^{\alpha})$$

(where
$$\lambda^{\alpha} = \lambda_1^{\alpha_1} \cdots \lambda_n^{\alpha_n}$$
)
($|\alpha| = \alpha_1 + \ldots + \alpha_n$)

How did we prove that?

How did we prove that?

If
$$F^i = (F_1^{(i)}, \ldots, F_n^{(i)})$$
 and $F_j^{(i)} = \sum F_{j,\alpha}^{(i)} X^{\alpha}$

How did we prove that?

If
$$F^i = (F_1^{(i)}, \dots, F_n^{(i)})$$
 and $F_j^{(i)} = \sum F_{j,\alpha}^{(i)} X^{\alpha}$,
then $\sum a_i F^i = 0 \iff \sum a_i F_{j,\alpha}^{(i)} = 0 \forall j, \alpha$.
How did we prove that?

If
$$F^{i} = (F_{1}^{(i)}, \ldots, F_{n}^{(i)})$$
 and $F_{j}^{(i)} = \sum F_{j,\alpha}^{(i)} X^{\alpha}$,
then $\sum a_{i}F^{i} = 0 \iff \sum a_{i}F_{j,\alpha}^{(i)} = 0 \forall j, \alpha$.
If $\{F_{j,\alpha}^{(i)}\}_{i \in \mathbb{N}}$ is such a sequence, then it is a linear recurrent
sequence belonging to $\sum a_{i}T^{i}$, etc....

A derivation $D : \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}[X_1, \dots, X_n]$

A derivation $D : \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}[X_1, \dots, X_n]$ is a map satisfying (1) \mathbb{C} -linear.

A derivation $D : \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}[X_1, \dots, X_n]$ is a map satisfying (1) \mathbb{C} -linear. (2) D(fg) = D(f)g + fD(g) for all $f, g \in \mathbb{C}[X_1, \dots, X_n]$.

A derivation $D : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$ is a map satisfying (1) \mathbb{C} -linear. (2) D(fg) = D(f)g + fD(g) for all $f, g \in \mathbb{C}[X_1, \ldots, X_n]$. A derivation will have the form:

- A derivation $D: \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}[X_1, \dots, X_n]$ is a map satisfying
- (1) \mathbb{C} -linear.

(2) D(fg) = D(f)g + fD(g) for all $f, g \in \mathbb{C}[X_1, \dots, X_n]$.

A derivation will have the form:

$$a_1rac{\partial}{\partial X_1}+\ldots+a_nrac{\partial}{\partial X_n}$$
 for some $a_i\in\mathbb{C}[X_1,\ldots,X_n]$

- A derivation $D : \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]$ is a map satisfying (1) \mathbb{C} -linear. (2) D(fg) = D(f)g + fD(g) for all $f, g \in \mathbb{C}[X_1, \ldots, X_n]$. A derivation will have the form: $a_1 \frac{\partial}{\partial X_1} + \ldots + a_n \frac{\partial}{\partial X_n}$ for some $a_i \in \mathbb{C}[X_1, \ldots, X_n]$.
- D is called **locally nilpotent** if:

- A derivation $D: \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}[X_1, \dots, X_n]$ is a map satisfying
- (1) \mathbb{C} -linear.

(2) D(fg) = D(f)g + fD(g) for all $f, g \in \mathbb{C}[X_1, \dots, X_n]$.

A derivation will have the form:

 $a_1 \frac{\partial}{\partial X_1} + \ldots + a_n \frac{\partial}{\partial X_n}$ for some $a_i \in \mathbb{C}[X_1, \ldots, X_n]$. *D* is called **locally nilpotent** if:

For all $g \in \mathbb{C}[X_1, \ldots, X_n]$ there exists $m \in \mathbb{N}$ such that $D^m(g) = 0$.

- A derivation $D: \mathbb{C}[X_1, \dots, X_n] \longrightarrow \mathbb{C}[X_1, \dots, X_n]$ is a map satisfying
- (1) \mathbb{C} -linear.

(2) D(fg) = D(f)g + fD(g) for all $f, g \in \mathbb{C}[X_1, \dots, X_n]$.

A derivation will have the form:

 $a_1 \frac{\partial}{\partial X_1} + \ldots + a_n \frac{\partial}{\partial X_n}$ for some $a_i \in \mathbb{C}[X_1, \ldots, X_n]$. *D* is called **locally nilpotent** if:

For all $g \in \mathbb{C}[X_1, ..., X_n]$ there exists $m \in \mathbb{N}$ such that $D^m(g) = 0$. EXAMPLE: $D = \frac{\partial}{\partial X_1}$.

D is called **locally finite** if:

D is called **locally finite** if:

For all $g \in \mathbb{C}[X_1, ..., X_n]$, the vector space $\mathbb{C}g + \mathbb{C}D(g) + \mathbb{C}D^2(g) + ...$ is finite dimensional.

D is called **locally finite** if:

For all $g \in \mathbb{C}[X_1, ..., X_n]$, the vector space $\mathbb{C}g + \mathbb{C}D(g) + \mathbb{C}D^2(g) + ...$ is finite dimensional. EXAMPLE: $D = X_1 \frac{\partial}{\partial X_1}$.

D is called **locally finite** if:

For all $g \in \mathbb{C}[X_1, \ldots, X_n]$, the vector space $\mathbb{C}g + \mathbb{C}D(g) + \mathbb{C}D^2(g) + \ldots$ is finite dimensional. EXAMPLE: $D = X_1 \frac{\partial}{\partial X_1}$. Locally nilpotent \Rightarrow Locally finite

D locally finite derivation, then $exp(D)(g) := g + D(g) + \frac{1}{2!}D^2(g) + \frac{1}{3!}D^3(g) + \dots$ is well-defined.

D locally finite derivation, then $exp(D)(g) := g + D(g) + \frac{1}{2!}D^2(g) + \frac{1}{3!}D^3(g) + \dots$ is well-defined.

Inverse is exp(-D).

D locally finite derivation, then $exp(D)(g) := g + D(g) + \frac{1}{2!}D^2(g) + \frac{1}{3!}D^3(g) + \dots$ is well-defined. Inverse is exp(-D).

EXAMPLE:
$$D = Y^2 \frac{\partial}{\partial X} + Z \frac{\partial}{\partial Y}$$
 on $\mathbb{C}[X, Y, Z]$:

D locally finite derivation, then $exp(D)(g) := g + D(g) + \frac{1}{2!}D^2(g) + \frac{1}{3!}D^3(g) + \dots$ is well-defined. Inverse is exp(-D). EXAMPLE: $D = Y^2 \frac{\partial}{\partial X} + Z \frac{\partial}{\partial Y}$ on $\mathbb{C}[X, Y, Z]$:

$$exp(D) =$$

D locally finite derivation, then $exp(D)(g) := g + D(g) + \frac{1}{2!}D^2(g) + \frac{1}{3!}D^3(g) + \dots$ is well-defined. Inverse is exp(-D). EXAMPLE: $D = Y^2 \frac{\partial}{\partial X} + Z \frac{\partial}{\partial Y}$ on $\mathbb{C}[X, Y, Z]$:

exp(D) = (exp(D)(X), exp(D)(Y), exp(D)(Z))

D locally finite derivation, then $exp(D)(g) := g + D(g) + \frac{1}{2!}D^{2}(g) + \frac{1}{3!}D^{3}(g) + \dots \text{ is}$ well-defined. Inverse is exp(-D). EXAMPLE: $D = Y^{2}\frac{\partial}{\partial X} + Z\frac{\partial}{\partial Y}$ on $\mathbb{C}[X, Y, Z]$: exp(D) = (exp(D)(X), exp(D)(Y), exp(D)(Z)) =

D locally finite derivation, then $exp(D)(g) := g + D(g) + \frac{1}{2!}D^2(g) + \frac{1}{3!}D^3(g) + \dots$ is well-defined.

Inverse is
$$exp(-D)$$
.
EXAMPLE: $D = Y^2 \frac{\partial}{\partial X} + Z \frac{\partial}{\partial Y}$ on $\mathbb{C}[X, Y, Z]$:

exp(D) = (exp(D)(X), exp(D)(Y), exp(D)(Z)) $= (X + Y^2 + YZ + \frac{1}{6}Z^2, Y + Z, Z)$

$$exp(D)^2 = exp(D) \circ exp(D) = exp(2D)$$

$$exp(D)^2 = exp(D) \circ exp(D) = exp(2D)$$

$$F^n = exp(nD) = (X + nY^2 + n^2YZ + \frac{n^3}{6}Z^2, Y + nZ, Z)$$

$$exp(D)^{2} = exp(D) \circ exp(D) = exp(2D)$$

$$F^{n} = exp(nD) = (X + nY^{2} + n^{2}YZ + \frac{n^{3}}{6}Z^{2}, Y + nZ, Z)$$
i.e. $\{deg(exp(nD))\}_{n \in \mathbb{N}}$ is bounded sequence

$$exp(D)^{2} = exp(D) \circ exp(D) = exp(2D)$$

$$F^{n} = exp(nD) = (X + nY^{2} + n^{2}YZ + \frac{n^{3}}{6}Z^{2}, Y + nZ, Z)$$
i.e. $\{deg(exp(nD))\}_{n \in \mathbb{N}}$ is bounded sequence
 $\Rightarrow exp(D)$ is LFPE.

$$exp(D)^{2} = exp(D) \circ exp(D) = exp(2D)$$

$$F^{n} = exp(nD) = (X + nY^{2} + n^{2}YZ + \frac{n^{3}}{6}Z^{2}, Y + nZ, Z)$$
i.e. $\{deg(exp(nD))\}_{n \in \mathbb{N}}$ is bounded sequence
 $\Rightarrow exp(D)$ is LFPE.

So:
$$F = exp(D) \longrightarrow F$$
 is LFPE.

$$exp(D)^{2} = exp(D) \circ exp(D) = exp(2D)$$

$$F^{n} = exp(nD) = (X + nY^{2} + n^{2}YZ + \frac{n^{3}}{6}Z^{2}, Y + nZ, Z)$$
i.e. $\{deg(exp(nD))\}_{n \in \mathbb{N}}$ is bounded sequence
 $\Rightarrow exp(D)$ is LFPE.

So: $F = exp(D) \longrightarrow F$ is LFPE. Even: $F_t := exp(tD)$ is a flow.

$$exp(D)^{2} = exp(D) \circ exp(D) = exp(2D)$$

$$F^{n} = exp(nD) = (X + nY^{2} + n^{2}YZ + \frac{n^{3}}{6}Z^{2}, Y + nZ, Z)$$
i.e. $\{deg(exp(nD))\}_{n \in \mathbb{N}}$ is bounded sequence
 $\Rightarrow exp(D)$ is LFPE.

So: $F = exp(D) \longrightarrow F$ is LFPE. Even: $F_t := exp(tD)$ is a flow. So: we can make many examples of LFPEs!

$F = exp(D) \iff F$ has a flow

 $F = exp(D) \iff F \text{ has a flow}$ (A flow of F is: F_t for each $t \in \mathbb{C}$ $F_1 = F, F_0 = I, F_t F_u = F_{t+u}$.) $F = exp(D) \iff F \text{ has a flow}$ (A flow of F is: F_t for each $t \in \mathbb{C}$ $F_1 = F, F_0 = I, F_t F_u = F_{t+u}$) $F = exp(D) \Rightarrow F \text{ is LFPE.}$ $F = exp(D) \iff F \text{ has a flow}$ (A flow of F is: $F_t \text{ for each } t \in \mathbb{C}$ $F_1 = F, F_0 = I, F_t F_u = F_{t+u}.$ $F = exp(D) \Rightarrow F \text{ is LFPE.}$? \Leftarrow ? D locally finite automorphism, then unique decomposition $D=D_n+D_s \label{eq:D}$

,

D locally finite automorphism, then unique decomposition $D = D_n + D_s$ where D_n is locally nilpotent, D_s is semisimple,

,
,

,

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$ where $F_n = exp(D_n)$ where D_n is locally nilpotent.

,

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$ where $F_n = exp(D_n)$ where D_n is locally nilpotent.

,

an example:

 $F = (2X + 2Y^2, 3Y)$

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$ where $F_n = exp(D_n)$ where D_n is locally nilpotent.

,

$$F = (2X + 2Y^2, 3Y) = (2X, 3Y) \circ (X + Y^2, Y)$$

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$ where $F_n = exp(D_n)$ where D_n is locally nilpotent.

$$F = (2X + 2Y^2, 3Y) = (2X, 3Y) \circ (X + Y^2, Y)$$
$$(2X, 3Y) = \exp(\lambda X \partial_X + \mu Y \partial_Y),$$

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$ where $F_n = exp(D_n)$ where D_n is locally nilpotent.

$$F = (2X + 2Y^2, 3Y) = (2X, 3Y) \circ (X + Y^2, Y)$$

(2X, 3Y) = exp($\lambda X \partial_X + \mu Y \partial_Y$), where
 $\lambda = \log(2), \mu = \log(3).$

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$ where $F_n = exp(D_n)$ where D_n is locally nilpotent.

$$F = (2X + 2Y^2, 3Y) = (2X, 3Y) \circ (X + Y^2, Y)$$

(2X, 3Y) = exp($\lambda X \partial_X + \mu Y \partial_Y$), where
 $\lambda = \log(2), \mu = \log(3).$
(X + Y², Y) = exp(Y² ∂_X).

Given F LFPE, then we find unique decomposition $F = F_n F_s = F_s F_n$ where $F_n = exp(D_n)$ where D_n is locally nilpotent.

an example:

$$F = (2X + 2Y^2, 3Y) = (2X, 3Y) \circ (X + Y^2, Y)$$

(2X, 3Y) = exp($\lambda X \partial_X + \mu Y \partial_Y$), where
 $\lambda = \log(2), \mu = \log(3).$
(X + Y², Y) = exp(Y² ∂_X).

Don't know how to make D_s , given F_s .

 $F = \exp(D_n)$

$$F = \exp(D_n)$$

 F is zero of $(T - 1)^n$ for some n

$$F = \exp(D_n) \iff$$

 F is zero of $(T-1)^n$ for some n

$$F = \exp(D_n) \iff$$

 F is zero of $(T-1)^n$ for some n

Example: $F = exp(Y^2\partial_X) = (X + Y^2, Y)$

$$F = \exp(D_n) \iff$$

 F is zero of $(T-1)^n$ for some n

Example:
$$F = exp(Y^2 \partial_X) = (X + Y^2, Y)$$

 $F^2 - 2F + I = 0$

$$F = \exp(D_n) \iff$$

 F is zero of $(T-1)^n$ for some n

Example:
$$F = exp(Y^2\partial_X) = (X + Y^2, Y)$$

 $F^2 - 2F + I = 0$ i.e. zero of $(T - 1)^2$.

In case F zero of $(T-1)^n$, then F has only eigenvalue 1.

In case F zero of $(T - 1)^n$, then F has only eigenvalue 1. Then there is one natural choice for " $\log(F) = D$ ", only ONE of them is loc. NILPOTENT

In case F zero of $(T-1)^n$, then F has only eigenvalue 1. Then there is one natural choice for " $\log(F) = D$ ", only ONE of them is loc. NILPOTENT Compare to: log(1) = 0.

In case F zero of $(T-1)^n$, then F has only eigenvalue 1. Then there is one natural choice for " $\log(F) = D$ ", only ONE of them is loc. NILPOTENT Compare to: log(1) = 0. But could have been: $log(1) = 2\pi i$. But 0 is natural choice.

In case F zero of $(T-1)^n$, then F has only eigenvalue 1. Then there is one natural choice for " $\log(F) = D$ ", only ONE of them is loc. NILPOTENT Compare to: log(1) = 0. But could have been: $log(1) = 2\pi i$. But 0 is natural choice. if $c \in \mathbb{C}$, then no natural choice $\log(c)$. Recently conjectured: F is LFPE and has no fixed point \Rightarrow $(T-1)^2$ divides $\mathfrak{m}_F(T)$, the minimum polynomial of F. Recently conjectured: F is LFPE and has no fixed point \Rightarrow $(T-1)^2$ divides $\mathfrak{m}_F(T)$, the minimum polynomial of F. Would imply: $F^n = I$ then F has fixed point. Recently conjectured: F is LFPE and has no fixed point \Rightarrow $(T-1)^2$ divides $\mathfrak{m}_F(T)$, the minimum polynomial of F. Would imply: $F^n = I$ then F has fixed point. Only solved so far for n a prime! Recently conjectured: F is LFPE and has no fixed point \Rightarrow $(T-1)^2$ divides $\mathfrak{m}_F(T)$, the minimum polynomial of F. Would imply: $F^n = I$ then F has fixed point. Only solved so far for n a prime!

So there's some funny stuff you might be able to read off \mathfrak{m}_F !

$\mathsf{TA}_n(\mathbb{C}) \subseteq$

 GA_n

$\mathsf{TA}_n(\mathbb{C}) \subseteq$

 GA_n

$$GA_n$$

 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

$$\begin{array}{ll}\mathsf{TA}_n(\mathbb{C}) & \subseteq \mathsf{GLIN}_n(\mathbb{C}) \\ & \subset \end{array}$$



 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

$$\mathsf{TA}_n(\mathbb{C}) \qquad \subseteq \mathsf{GLIN}_n(\mathbb{C}) \\ \subseteq \mathsf{GLND}_n(\mathbb{C}) \subseteq$$

 GA_n

 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

 $\text{GLFD}_n(\mathbb{C})$ is group generated by exponents of LFDs.

$TA_n(\mathbb{C})$	$\subseteq GLIN_n(\mathbb{C})$
	$\subseteq GLND_n(\mathbb{C})$



 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

 $\operatorname{GLFD}_n(\mathbb{C})$ is group generated by exponents of LFDs.

$$\begin{array}{ll} \mathsf{TA}_n(\mathbb{C}) & \subseteq \mathsf{GLIN}_n(\mathbb{C}) \\ & \subseteq \mathsf{GLND}_n(\mathbb{C}) \subseteq \mathsf{GLFD}_n(\mathbb{C}) \subseteq & \mathsf{GA}_n \end{array}$$

 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

 $\operatorname{GLFD}_n(\mathbb{C})$ is group generated by exponents of LFDs. $\operatorname{GLF}_n(\mathbb{C})$ is group generated by locally finite maps.

$$\begin{array}{ll} \mathsf{TA}_n(\mathbb{C}) & \subseteq \mathsf{GLIN}_n(\mathbb{C}) \\ & \subseteq \mathsf{GLND}_n(\mathbb{C}) \subseteq \mathsf{GLFD}_n(\mathbb{C}) \subseteq & \mathsf{GA}_n \end{array}$$

 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

 $\operatorname{GLFD}_n(\mathbb{C})$ is group generated by exponents of LFDs. $\operatorname{GLF}_n(\mathbb{C})$ is group generated by locally finite maps.

$$\begin{array}{ll} \mathsf{TA}_n(\mathbb{C}) & \subseteq \mathsf{GLIN}_n(\mathbb{C}) \\ & \subseteq \mathsf{GLND}_n(\mathbb{C}) \subseteq \mathsf{GLFD}_n(\mathbb{C}) \subseteq \mathsf{GLF}_n(\mathbb{C}) & \subseteq \mathsf{GA}_n \end{array}$$

 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

 $\operatorname{GLFD}_n(\mathbb{C})$ is group generated by exponents of LFDs. $\operatorname{GLF}_n(\mathbb{C})$ is group generated by locally finite maps.

$$\begin{array}{ll} \mathsf{TA}_n(\mathbb{C})(*) & \subseteq \mathsf{GLIN}_n(\mathbb{C})(*) \\ & \subseteq \mathsf{GLND}_n(\mathbb{C}) \subseteq \mathsf{GLFD}_n(\mathbb{C}) \subseteq \mathsf{GLF}_n(\mathbb{C})(*) \subseteq \mathsf{GA}_n \end{array}$$

(*) makes sense for finite fields.
$\operatorname{GLIN}_n(\mathbb{C})$ is group generated by linearizable polynomial automorphisms.

 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

 $\operatorname{GLFD}_n(\mathbb{C})$ is group generated by exponents of LFDs. $\operatorname{GLF}_n(\mathbb{C})$ is group generated by locally finite maps.

$$\begin{array}{ll} \mathsf{TA}_n(\mathbb{C})(*)(**) &\subseteq \mathsf{GLIN}_n(\mathbb{C})(*)(**) \\ &\subseteq \mathsf{GLND}_n(\mathbb{C}) \subseteq \mathsf{GLFD}_n(\mathbb{C}) \subseteq \mathsf{GLF}_n(\mathbb{C})(*) \subseteq \mathsf{GA}_n \end{array}$$

(*) makes sense for finite fields. (**) killed as generators for $GA_n(\mathbb{F}_{2^m})$ for finite fields, if you find an odd polynomial automorphism over \mathbb{F}_{2^m} !

 $\operatorname{GLIN}_n(\mathbb{C})$ is group generated by linearizable polynomial automorphisms.

 $\operatorname{GLND}_n(\mathbb{C})$ is group generated by exponents of LNDs AND linear maps.

 $\operatorname{GLFD}_n(\mathbb{C})$ is group generated by exponents of LFDs. $\operatorname{GLF}_n(\mathbb{C})$ is group generated by locally finite maps.

$$\begin{array}{ll} \mathsf{TA}_n(\mathbb{C})(*)(**) &\subseteq \mathsf{GLIN}_n(\mathbb{C})(*)(**) \\ &\subseteq \mathsf{GLND}_n(\mathbb{C}) \subseteq \mathsf{GLFD}_n(\mathbb{C}) \subseteq \mathsf{GLF}_n(\mathbb{C})(*) \subseteq \mathsf{GA}_n \end{array}$$

(*) makes sense for finite fields. (**) killed as generators for $GA_n(\mathbb{F}_{2^m})$ for finite fields, if you find an odd polynomial automorphism over \mathbb{F}_{2^m} !

*** THANK YOU ***