On Shapiro's Conjecture in a Zilber field

Giuseppina Terzo

Seconda Università degli Studi di Napoli

Bedlewo 9-14 August 2009

*joint work with Paola D'Aquino and Angus Macintyre

Goals

- Exponential rings, exponential fields and exponential polynomial ring
- Factorization Theorem for exponential polynomials
- Shapiro's Conjecture in $\mathbb{C}$ and in a Zilber field

Goals

- **Exponential rings, exponential fields and exponential polynomial ring**
- **Factorization Theorem for exponential polynomials**
- **Shapiro's Conjecture in $\mathbb{C}$ and in a Zilber field**

Goals

- **Exponential rings, exponential fields and exponential polynomial ring**
- **Factorization Theorem for exponential polynomials**
- **Shapiro's Conjecture in $\mathbb{C}$ and in a Zilber field**

Goals

- **Exponential rings, exponential fields and exponential polynomial ring**
- **Factorization Theorem for exponential polynomials**
- **Shapiro's Conjecture in $\mathbb{C}$ and in a Zilber field**

Exponential rings

Definition: An exponential ring, or E-ring, is a pair (R, E) with R a ring (commutative with 1) and

$$E : (R, +) \to (\mathcal{U}(R), \cdot)$$

a map of the additive group of R into the multiplicative group of units of R satisfying

1. $E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$
2. $E(0) = 1$.

(K, E) is an E-field if K is a field.

Exponential rings

Definition: An exponential ring, or E-ring, is a pair (R, E) with R a ring (commutative with 1) and

$$E : (R, +) \to (\mathcal{U}(R), \cdot)$$

a map of the additive group of R into the multiplicative group of units of R satisfying

1. $E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$
2. $E(0) = 1.$

(K, E) is an E-field if K is a field.

Exponential rings

Definition: An exponential ring, or E-ring, is a pair (R, E) with R a ring (commutative with 1) and

$$E : (R, +) \to (\mathcal{U}(R), \cdot)$$

a map of the additive group of R into the multiplicative group of units of R satisfying

1. $E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$
2. $E(0) = 1$.

(K, E) is an E-field if K is a field.

Exponential rings

Definition: An exponential ring, or E-ring, is a pair (R, E) with R a ring (commutative with 1) and

$$E : (R, +) \to (\mathcal{U}(R), \cdot)$$

a map of the additive group of R into the multiplicative group of units of R satisfying

1. $E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$
2. $E(0) = 1$.

(K, E) is an E-field if K is a field.

Exponential rings

Definition: An exponential ring, or E-ring, is a pair (R, E) with R a ring (commutative with 1) and

$$E : (R, +) \to (\mathcal{U}(R), \cdot)$$

a map of the additive group of R into the multiplicative group of units of R satisfying

1. $E(x + y) = E(x) \cdot E(y)$ for all $x, y \in R$
2. $E(0) = 1$.

(K, E) is an E-field if K is a field.

Examples

Examples:

1. $(\mathbb{R}, e^x)$; $(\mathbb{C}, e^x)$;
2. (R, E) where R is any ring and $E(x) = 1$ for all $x \in R$.
3. $(S[t], E)$ where S is E-field of characteristic 0 and $S[t]$ the ring of formal power series in t over S. Let $f \in S[t]$, where $f = r + f_1$ with $r \in S$

$$E(f) = E(r) \cdot \sum_{n=0}^{\infty} (f_1)^n / n!$$

Examples:

1. $(\mathbb{R}, e^x)$; $(\mathbb{C}, e^x)$;
2. (R, E) where R is any ring and $E(x) = 1$ for all $x \in R$.
3. $(S[t], E)$ where S is E-field of characteristic 0 and $S[t]$ the ring of formal power series in t over S. Let $f \in S[t]$, where $f = r + f_1$ with $r \in S$

$$E(f) = E(r) \cdot \sum_{n=0}^{\infty} (f_1)^n / n!$$

Examples

Examples:

1. $(\mathbb{R}, e^x)$; $(\mathbb{C}, e^x)$;
2. (R, E) where R is any ring and $E(x) = 1$ for all $x \in R$.
3. $(S[t], E)$ where S is E-field of characteristic 0 and $S[t]$ the ring of formal power series in t over S. Let $f \in S[t]$, where $f = r + f_1$ with $r \in S$

$$E(f) = E(r) \cdot \sum_{n=0}^{\infty} (f_1)^n / n!$$

Examples

Examples:

1. $(\mathbb{R}, e^x)$; $(\mathbb{C}, e^x)$;
2. (R, E) where R is any ring and $E(x) = 1$ for all $x \in R$.
3. $(S[t], E)$ where S is E-field of characteristic 0 and $S[t]$ the ring of formal power series in t over S. Let $f \in S[t]$, where $f = r + f_1$ with $r \in S$

$$E(f) = E(r) \cdot \sum_{n=0}^{\infty} (f_1)^n / n!$$

Examples:

1. $(\mathbb{R}, e^x)$; $(\mathbb{C}, e^x)$;
2. (R, E) where R is any ring and $E(x) = 1$ for all $x \in R$.
3. $(S[t], E)$ where S is E-field of characteristic 0 and $S[t]$ the ring of formal power series in t over S. Let $f \in S[t]$, where $f = r + f_1$ with $r \in S$

$$E(f) = E(r) \cdot \sum_{n=0}^{\infty} (f_1)^n / n!$$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings **ab groups** **E-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings **ab groups** **E-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \dots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings **ab groups** ***E*-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings **ab groups** **E-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings **ab groups** **E-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$,	$(B_k, +)_{k \geq 0}$	and	$(E_k)_{k \geq -1}$
rings	**ab groups**		**E-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings **ab groups** E-**morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings **ab groups** ***E*-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$,	$(B_k, +)_{k \geq 0}$	and	$(E_k)_{k \geq -1}$
rings	**ab groups**		***E*-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Exponential polynomial ring

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$,	$(B_k, +)_{k \geq 0}$	and	$(E_k)_{k \geq -1}$
rings	**ab groups**		E**-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$, $(B_k, +)_{k \geq 0}$ and $(E_k)_{k \geq -1}$

rings — ab groups — E-morphisms

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Construction

Let (K, E) be an E-field, the ring of E-polynomials in the indeterminates $\overline{X} = X_1, \ldots, X_n$, denoted by $K[\overline{X}]^E$, is an E-ring constructed by recursion:

$(R_k, +, \cdot)_{k \geq -1}$,	$(B_k, +)_{k \geq 0}$	and	$(E_k)_{k \geq -1}$
rings	**ab groups**		***E*-morphisms**

Step 0:

$R_{-1} = K$

$R_0 = (K[\overline{X}], +, \cdot)$, $B_0 = (\overline{X})$, $R_0 = R_{-1} \oplus B_0$ $E_{-1} : R_{-1} \longrightarrow R_0$

Construction

Inductive step:

Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k, \ E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring).}$$

So

$$R_k \text{ is a subring of } R_{k+1}$$

and

$$R_{k+1} = R_k \oplus B_{k+1}.$$

Inductive step:

Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k, \ E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring).}$$

So

$$R_k \text{ is a subring of } R_{k+1}$$

and

$$R_{k+1} = R_k \oplus B_{k+1}.$$

Inductive step:

Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k,\ E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring).}$$

So

$$R_k \text{ is a subring of } R_{k+1}$$

and

$$R_{k+1} = R_k \oplus B_{k+1}.$$

Construction

Inductive step:

Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k,\ E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring).}$$

So

$$R_k \text{ is a subring of } R_{k+1}$$

and

$$R_{k+1} = R_k \oplus B_{k+1}.$$

Construction

Inductive step:

Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k,\ \ E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring).}$$

So

$$R_k \text{ is a subring of } R_{k+1}$$

and

$$R_{k+1} = R_k \oplus B_{k+1}.$$

Construction

Inductive step:

Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k,\ \ E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring).}$$

So

$$R_k \text{ is a subring of } R_{k+1}$$

and

$$R_{k+1} = R_k \oplus B_{k+1}.$$

Inductive step:

Suppose $k \geq 0$ and R_{k-1}, R_k, B_k and E_{k-1} have been defined in such a way that:

$$R_k = R_{k-1} \oplus B_k,\ \ E_{k-1} : (R_{k-1}, +) \to (\mathcal{U}(R_k), \cdot)$$

Let

$$t : (B_k, +) \to (t^{B_k}, \cdot)$$

an isomorphism. Define

$$R_{k+1} = R_k[t^{B_k}] \text{ (group ring).}$$

So

$$R_k \text{ is a subring of } R_{k+1}$$

and

$$R_{k+1} = R_k \oplus B_{k+1}.$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \cdots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \textbf{ if } x \in R_k,\ \ k \in \mathbb{N}$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \cdots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \textbf{ if } x \in R_k, \; k \in \mathbb{N}$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \cdots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \textbf{ if } x \in R_k, \; k \in \mathbb{N}$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \cdots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \textbf{ if } x \in R_k, \ k \in \mathbb{N}$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \cdots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \textbf{ if } x \in R_k,\ \ k \in \mathbb{N}$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \cdots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \textbf{ if } x \in R_k,\ \ k \in \mathbb{N}$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \ldots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \text{ if } x \in R_k, \ k \in \mathbb{N}$$

Construction

Define

$$E_k : (R_k, +) \to (\mathcal{U}(R_{k+1}), \cdot) \text{ s.t.}$$

$E_k(x) = E_{k-1}(r) \cdot t^b$, for $x = r + b$, $r \in R_{k-1}$ and $b \in B_k$.

$$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_k \subset \cdots$$

Then the E-polynomial ring is:

$$K[\overline{X}]^E = \lim_k R_k = \bigcup_{k=0}^{\infty} R_k = K[\overline{X}][t^{B_0 \oplus B_1 \oplus \ldots \oplus B_k \ldots}]$$

and the E-ring morphism on $K[\overline{X}]^E$ is the following:

$$E(x) = E_k(x) \textbf{ if } x \in R_k, \;\; k \in \mathbb{N}$$

Invertible elements

Theorem (Folklore): Let (R, E) be an exponential domain. Then $R[\overline{X}]^E$ is an integral domain whose units are $u \cdot E(f)$, where u is invertible in R and $f \in R[\overline{X}]^E$.

Invertible elements

Theorem (Folklore): Let (R, E) be an exponential domain. Then $R[\overline{X}]^E$ is an integral domain whose units are $u \cdot E(f)$, where u is invertible in R and $f \in R[\overline{X}]^E$.

Factorization theorem

Let K be an ACF, where $char(K) = 0$, if $f \in K[X_1, \ldots, X_n]$ is an irreducible polynomial over K, it can happen that for some $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$, $f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$ becomes reducible.

Ritt (1927) and Gourin (1930) studied factorizations of

$$\beta_1 e^{\alpha_1 x} + \ldots + \beta_k e^{\alpha_k x}$$

Definition: A polynomial $f(\overline{X})$ is power irreducible (over K) if for each $\overline{\mu} \in \mathbb{N}^n$, $f(\overline{X}^{\overline{\mu}})$ is irreducible.

monomial: $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$.

Definition: A polynomial $f(\overline{X})$ is effectively **1-variable** or **simple** if $f = \tau_1 \cdot g(\tau_2)$, where τ_1, τ_2 are monomials (possibly with negative exponents), and g is a polynomial with constant term different from zero.

Factorization theorem

Let K be an ACF, where $char(K) = 0$, if $f \in K[X_1, \ldots, X_n]$ is an irreducible polynomial over K, it can happen that for some $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$, $f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$ becomes reducible.

Ritt (1927) and Gourin (1930) studied factorizations of

$$\beta_1 e^{\alpha_1 x} + \ldots + \beta_k e^{\alpha_k x}$$

Definition: A polynomial $f(\overline{X})$ is power irreducible (over K) if for each $\overline{\mu} \in \mathbb{N}^n$, $f(\overline{X}^{\overline{\mu}})$ is irreducible.

monomial: $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$.

Definition: A polynomial $f(\overline{X})$ is effectively **1-variable** or **simple** if $f = \tau_1 \cdot g(\tau_2)$, where τ_1, τ_2 are monomials (possibly with negative exponents), and g is a polynomial with constant term different from zero.

Factorization theorem

Let K be an ACF, where $char(K) = 0$, if $f \in K[X_1, \ldots, X_n]$ is an irreducible polynomial over K, it can happen that for some $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$, $f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$ becomes reducible.

Ritt (1927) and Gourin (1930) studied factorizations of

$$\beta_1 e^{\alpha_1 x} + \ldots + \beta_k e^{\alpha_k x}$$

Definition: A polynomial $f(\overline{X})$ is power irreducible (over K) if for each $\overline{\mu} \in \mathbb{N}^n$, $f(\overline{X}^{\overline{\mu}})$ is irreducible.

monomial: $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$.

Definition: A polynomial $f(\overline{X})$ is effectively **1-variable** or **simple** if $f = \tau_1 \cdot g(\tau_2)$, where τ_1, τ_2 are monomials (possibly with negative exponents), and g is a polynomial with constant term different from zero.

Factorization theorem

Let K be an ACF, where $char(K) = 0$, if $f \in K[X_1, \ldots, X_n]$ is an irreducible polynomial over K, it can happen that for some $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$, $f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$ becomes reducible.

Ritt (1927) and Gourin (1930) studied factorizations of

$$\beta_1 e^{\alpha_1 x} + \ldots + \beta_k e^{\alpha_k x}$$

Definition: A polynomial $f(\overline{X})$ is power irreducible (over K) if for each $\overline{\mu} \in \mathbb{N}^n$, $f(\overline{X}^{\overline{\mu}})$ is irreducible.

monomial: $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$.

Definition: A polynomial $f(\overline{X})$ is effectively **1-variable** or **simple** if $f = \tau_1 \cdot g(\tau_2)$, where τ_1, τ_2 are monomials (possibly with negative exponents), and g is a polynomial with constant term different from zero.

Factorization theorem

Let K be an ACF, where $char(K) = 0$, if $f \in K[X_1, \ldots, X_n]$ is an irreducible polynomial over K, it can happen that for some $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$, $f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$ becomes reducible.

Ritt (1927) and Gourin (1930) studied factorizations of

$$\beta_1 e^{\alpha_1 x} + \ldots + \beta_k e^{\alpha_k x}$$

Definition: A polynomial $f(\overline{X})$ is power irreducible (over K) if for each $\overline{\mu} \in \mathbb{N}^n$, $f(\overline{X}^{\overline{\mu}})$ is irreducible.

monomial: $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$.

Definition: A polynomial $f(\overline{X})$ is effectively **1-variable** or **simple** if $f = \tau_1 \cdot g(\tau_2)$, where τ_1, τ_2 are monomials (possibly with negative exponents), and g is a polynomial with constant term different from zero.

Factorization theorem

Let K be an ACF, where $char(K) = 0$, if $f \in K[X_1, \ldots, X_n]$ is an irreducible polynomial over K, it can happen that for some $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$, $f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$ becomes reducible.

Ritt (1927) and Gourin (1930) studied factorizations of

$$\beta_1 e^{\alpha_1 x} + \ldots + \beta_k e^{\alpha_k x}$$

Definition: A polynomial $f(\overline{X})$ is power irreducible (over K) if for each $\overline{\mu} \in \mathbb{N}^n$, $f(\overline{X}^{\overline{\mu}})$ is irreducible.

monomial: $X_1^{m_1} \cdot \ldots \cdot X_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$.

Definition: A polynomial $f(\overline{X})$ is effectively **1-variable** or **simple** if $f = \tau_1 \cdot g(\tau_2)$, where τ_1, τ_2 are monomials (possibly with negative exponents), and g is a polynomial with constant term different from zero.

Factorization theorem

van der Poorten (1995) gives a uniform bound for the number of irreducible factors of

$$f(X_1^{\mu_1}, \dots, X_n^{\mu_n})$$

for $f(X_1, \dots, X_n)$ not effectively 1-variable, and arbitrary $\mu_1, \dots, \mu_n \in \mathbb{N}_+$. The bound depends only on

$$M = max\{d_{X_1}, \dots, d_{X_n}\}$$

Factorization theorem

van der Poorten (1995) gives a uniform bound for the number of irreducible factors of

$$f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$$

for $f(X_1, \ldots, X_n)$ not effectively 1-variable, and arbitrary $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$. The bound depends only on

$$M = max\{d_{X_1}, \ldots, d_{X_n}\}$$

Factorization theorem

van der Poorten (1995) gives a uniform bound for the number of irreducible factors of

$$f(X_1^{\mu_1}, \dots, X_n^{\mu_n})$$

for $f(X_1, \dots, X_n)$ not effectively 1-variable, and arbitrary $\mu_1, \dots, \mu_n \in \mathbb{N}_+$. The bound depends only on

$$M = max\{d_{X_1}, \dots, d_{X_n}\}$$

Factorization theorem

van der Poorten (1995) gives a uniform bound for the number of irreducible factors of

$$f(X_1^{\mu_1}, \ldots, X_n^{\mu_n})$$

for $f(X_1, \ldots, X_n)$ not effectively 1-variable, and arbitrary $\mu_1, \ldots, \mu_n \in \mathbb{N}_+$. The bound depends only on

$$M = max\{d_{X_1}, \ldots, d_{X_n}\}$$

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \cdots \oplus B_n \cdots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \ldots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \ldots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \ldots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \ldots, \omega_l$ for $t^{\beta_1}, \ldots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \ldots, \omega_l]$.

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \cdots \oplus B_n \cdots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \ldots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \ldots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \ldots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \ldots, \omega_l$ for $t^{\beta_1}, \ldots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \ldots, \omega_l]$.

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \dots \oplus B_n \dots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \dots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \dots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \dots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \dots, \omega_l$ for $t^{\beta_1}, \dots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \dots, \omega_l]$.

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \cdots \oplus B_n \cdots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \ldots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \ldots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \ldots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \ldots, \omega_l$ for $t^{\beta_1}, \ldots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \ldots, \omega_l]$.

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \dots \oplus B_n \dots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \dots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \dots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \dots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \dots, \omega_l$ for $t^{\beta_1}, \dots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \dots, \omega_l]$.

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \dots \oplus B_n \dots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \dots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \dots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \dots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \dots, \omega_l$ for $t^{\beta_1}, \dots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \dots, \omega_l]$.

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \cdots \oplus B_n \cdots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \ldots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \ldots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \ldots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \ldots, \omega_l$ for $t^{\beta_1}, \ldots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \ldots, \omega_l]$.

The basic idea

We denote by $U[G] = K[\overline{X}][t^{B_0 \oplus \dots \oplus B_n \dots}]$. Let $f(\overline{X}) \in U[G]$, so

$$f(\overline{X}) = \sum_{m=1}^{h} a_m t^{b_m},$$

where $a_m \in U$ and $b_m \in G$

Let Γ be the abelian additive group generated by $b_1, \dots, b_h$.

$supp(f) = \mathbb{Q}$-vector space generated by Γ.

Let $\{\beta_1, \dots, \beta_l\}$ a $\mathbb{Z}$-base of Γ.

We can consider f as polynomial in $t^{\beta_1}, \dots, t^{\beta_l}$, with coefficients in $U = K[\overline{X}]$. We use formally $\omega_1, \dots, \omega_l$ for $t^{\beta_1}, \dots, t^{\beta_l}$, and we consider f as an element of $U[\omega_1, \dots, \omega_l]$.

Almost Unique Factorization Theorem

Theorem (DMT):

Let $f(\overline{X}) \in K[\overline{X}]^E$, where (K, E) is an algebraically closed E-field of *char* 0 and $f \neq 0$. Then f factors, uniquely up to units and associates, as finite product of irreducibles of $K[\overline{X}]$, a finite product of irreducible polynomials F_i in $K[\overline{X}]^E$ with support of dimension bigger than 1, and a finite product of polynomials G_j where $supp(G_{j1}) \neq supp(G_{j2})$, for $j_1 \neq j_2$ and whose supports are of dimension 1.

Remark:

1. If a polynomial f factors as $f_1 \cdot f_2$ then $supp(f_i) \subseteq supp(f)$, where $i = 1, 2$.
2. If a polynomial f divides a polynomial with support of dimension 1 then the dimension of support of f is 1.

Almost Unique Factorization Theorem

Theorem (DMT):

Let $f(\overline{X}) \in K[\overline{X}]^E$, where (K, E) is an algebraically closed E-field of *char* 0 and $f \neq 0$. Then f factors, uniquely up to units and associates, as finite product of irreducibles of $K[\overline{X}]$, a finite product of irreducible polynomials F_i in $K[\overline{X}]^E$ with support of dimension bigger than 1, and a finite product of polynomials G_j where $supp(G_{j1}) \neq supp(G_{j2})$, for $j_1 \neq j_2$ and whose supports are of dimension 1.

Remark:

1. If a polynomial f factors as $f_1 \cdot f_2$ then $supp(f_i) \subseteq supp(f)$, where $i = 1, 2$.
2. If a polynomial f divides a polynomial with support of dimension 1 then the dimension of support of f is 1.

Almost Unique Factorization Theorem

Theorem (DMT):

Let $f(\overline{X}) \in K[\overline{X}]^E$, where (K, E) is an algebraically closed E-field of *char* 0 and $f \neq 0$. Then f factors, uniquely up to units and associates, as finite product of irreducibles of $K[\overline{X}]$, a finite product of irreducible polynomials F_i in $K[\overline{X}]^E$ with support of dimension bigger than 1, and a finite product of polynomials G_j where $supp(G_{j1}) \neq supp(G_{j2})$, for $j_1 \neq j_2$ and whose supports are of dimension 1.

Remark:

1. If a polynomial f factors as $f_1 \cdot f_2$ then $supp(f_i) \subseteq supp(f)$, where $i = 1, 2$.
2. If a polynomial f divides a polynomial with support of dimension 1 then the dimension of support of f is 1.

Almost Unique Factorization Theorem

Theorem (DMT):

Let $f(\overline{X}) \in K[\overline{X}]^E$, where (K, E) is an algebraically closed E-field of *char* 0 and $f \neq 0$. Then f factors, uniquely up to units and associates, as finite product of irreducibles of $K[\overline{X}]$, a finite product of irreducible polynomials F_i in $K[\overline{X}]^E$ with support of dimension bigger than 1, and a finite product of polynomials G_j where $supp(G_{j1}) \neq supp(G_{j2})$, for $j_1 \neq j_2$ and whose supports are of dimension 1.

Remark:

1. If a polynomial f factors as $f_1 \cdot f_2$ then $supp(f_i) \subseteq supp(f)$, where $i = 1, 2$.
2. If a polynomial f divides a polynomial with support of dimension 1 then the dimension of support of f is 1.

Almost Unique Factorization Theorem

Theorem (DMT):

Let $f(\overline{X}) \in K[\overline{X}]^E$, where (K, E) is an algebraically closed E-field of *char* 0 and $f \neq 0$. Then f factors, uniquely up to units and associates, as finite product of irreducibles of $K[\overline{X}]$, a finite product of irreducible polynomials F_i in $K[\overline{X}]^E$ with support of dimension bigger than 1, and a finite product of polynomials G_j where $supp(G_{j1}) \neq supp(G_{j2})$, for $j_1 \neq j_2$ and whose supports are of dimension 1.

Remark:

1. If a polynomial f factors as $f_1 \cdot f_2$ then $supp(f_i) \subseteq supp(f)$, where $i = 1, 2$.
2. If a polynomial f divides a polynomial with support of dimension 1 then the dimension of support of f is 1.

Pseudo exponential fields or Zilber fields

Zilber's programme: Look for a canonical algebraically closed field of characteristic 0 with exponentiation.

K is a Zilber field if:

- K is an algebraically closed field of characteristic 0;
- $E : (K, +) \longrightarrow (K^\times, \cdot)$ is a surjective homomorphism and there is $\omega \in K$ transcendental over $\mathbb{Q}$ such that $\ker E = \mathbb{Z}\omega$;
- **Schanuel's Conjecture (SC)** Let $\lambda_1, \ldots, \lambda_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, E(\lambda_1), \ldots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$;
- Axioms giving criteria for solvability of systems of exponential equations.

Pseudo exponential fields or Zilber fields

Zilber's programme: Look for a canonical algebraically closed field of characteristic 0 with exponentiation.

K is a Zilber field if:

- K is an algebraically closed field of characteristic 0;
- $E : (K, +) \longrightarrow (K^{\times}, \cdot)$ is a surjective homomorphism and there is $\omega \in K$ transcendental over $\mathbb{Q}$ such that $\ker E = \mathbb{Z}\omega$;
- **Schanuel's Conjecture (SC)** Let $\lambda_1, \ldots, \lambda_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, E(\lambda_1), \ldots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$;
- Axioms giving criteria for solvability of systems of exponential equations.

Pseudo exponential fields or Zilber fields

Zilber's programme: Look for a canonical algebraically closed field of characteristic 0 with exponentiation.

K is a Zilber field if:

- K is an algebraically closed field of characteristic 0;
- $E : (K, +) \longrightarrow (K^{\times}, \cdot)$ is a surjective homomorphism and there is $\omega \in K$ transcendental over $\mathbb{Q}$ such that $\ker E = \mathbb{Z}\omega$;
- **Schanuel's Conjecture (SC)** Let $\lambda_1, \ldots, \lambda_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, E(\lambda_1), \ldots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$;
- Axioms giving criteria for solvability of systems of exponential equations.

Pseudo exponential fields or Zilber fields

Zilber's programme: Look for a canonical algebraically closed field of characteristic 0 with exponentiation.

K is a Zilber field if:

- K is an algebraically closed field of characteristic 0;
- $E : (K, +) \longrightarrow (K^{\times}, \cdot)$ is a surjective homomorphism and there is $\omega \in K$ transcendental over $\mathbb{Q}$ such that $\ker E = \mathbb{Z}\omega$;
- **Schanuel's Conjecture (SC)** Let $\lambda_1, \ldots, \lambda_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, E(\lambda_1), \ldots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$;
- Axioms giving criteria for solvability of systems of exponential equations.

Pseudo exponential fields or Zilber fields

Zilber's programme: Look for a canonical algebraically closed field of characteristic 0 with exponentiation.

K is a Zilber field if:

- K is an algebraically closed field of characteristic 0;
- $E : (K, +) \longrightarrow (K^{\times}, \cdot)$ is a surjective homomorphism and there is $\omega \in K$ transcendental over $\mathbb{Q}$ such that $\ker E = \mathbb{Z}\omega$;
- **Schanuel's Conjecture (SC)** Let $\lambda_1, \ldots, \lambda_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, E(\lambda_1), \ldots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$;
- Axioms giving criteria for solvability of systems of exponential equations.

Pseudo exponential fields or Zilber fields

Zilber's programme: Look for a canonical algebraically closed field of characteristic 0 with exponentiation.

K is a Zilber field if:

- K is an algebraically closed field of characteristic 0;
- $E : (K, +) \longrightarrow (K^{\times}, \cdot)$ is a surjective homomorphism and there is $\omega \in K$ transcendental over $\mathbb{Q}$ such that $\ker E = \mathbb{Z}\omega$;
- **Schanuel's Conjecture (SC)** Let $\lambda_1, \dots, \lambda_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \dots, \lambda_n, E(\lambda_1), \dots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$;
- Axioms giving criteria for solvability of systems of exponential equations.

Pseudo exponential fields or Zilber fields

Zilber's programme: Look for a canonical algebraically closed field of characteristic 0 with exponentiation.

K is a Zilber field if:

- K is an algebraically closed field of characteristic 0;
- $E : (K, +) \longrightarrow (K^{\times}, \cdot)$ is a surjective homomorphism and there is $\omega \in K$ transcendental over $\mathbb{Q}$ such that $\ker E = \mathbb{Z}\omega$;
- **Schanuel's Conjecture (SC)** Let $\lambda_1, \ldots, \lambda_n \in K$ be linearly independent over $\mathbb{Q}$. Then $\mathbb{Q}(\lambda_1, \ldots, \lambda_n, E(\lambda_1), \ldots, E(\lambda_n))$ has transcendence degree (t.d.) at least n over $\mathbb{Q}$;
- Axioms giving criteria for solvability of systems of exponential equations.

Categoricity

Theorem (Zilber):

The class of pseudo exponential fields has a unique model in every uncountable cardinality.

Zilber's Conjecture:

The unique model of cardinality $2^{\aleph_0}$ is $(\mathbb{C}, E)$.

Categoricity

Theorem (Zilber):

The class of pseudo exponential fields has a unique model in every uncountable cardinality.

Zilber's Conjecture:

The unique model of cardinality $2^{\aleph_0}$ is $(\mathbb{C}, E)$.

Categoricity

Theorem (Zilber):

The class of pseudo exponential fields has a unique model in every uncountable cardinality.

Zilber's Conjecture:

The unique model of cardinality $2^{\aleph_0}$ is $(\mathbb{C}, E)$.

Categoricity

Theorem (Zilber):

The class of pseudo exponential fields has a unique model in every uncountable cardinality.

Zilber's Conjecture:

The unique model of cardinality $2^{\aleph_0}$ is $(\mathbb{C}, E)$.

Categoricity

Theorem (Zilber):

The class of pseudo exponential fields has a unique model in every uncountable cardinality.

Zilber's Conjecture:

The unique model of cardinality $2^{\aleph_0}$ is $(\mathbb{C}, E)$.

Compare $(\mathbb{C}, E)$ and (K, E)

- Does $(\mathbb{C}, E)$ satisfy properties which will follow directly from Zilber's axioms?
- Does (K, E) satisfy properties which are known for $(\mathbb{C}, E)$?

Compare $(\mathbb{C}, E)$ and (K, E)

- Does $(\mathbb{C}, E)$ satisfy properties which will follow directly from Zilber's axioms?
- Does (K, E) satisfy properties which are known for $(\mathbb{C}, E)$?

Compare $(\mathbb{C}, E)$ and (K, E)

- Does $(\mathbb{C}, E)$ satisfy properties which will follow directly from Zilber's axioms?
- Does (K, E) satisfy properties which are known for $(\mathbb{C}, E)$?

Questions

1. When does the polynomial $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$ has no solutions in $\mathbb{C}$?
2. If $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_n, c_1, \ldots, c_m, d_1, \ldots, d_n \in \mathbb{C}$, when does the system

$$\begin{cases} c_1 exp(\lambda_1) + \ldots c_n exp(\lambda_n) & = 0 \\ d_1 exp(\mu_1) + \ldots d_m exp(\mu_m) & = 0 \end{cases}$$

have infinitely many solutions in $\mathbb{C}$?

Questions

1. When does the polynomial $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$ has no solutions in $\mathbb{C}$?
2. If $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_n, c_1, \ldots, c_m, d_1, \ldots, d_n \in \mathbb{C}$, when does the system

$$\begin{cases} c_1 exp(\lambda_1) + \ldots c_n exp(\lambda_n) & = 0 \\ \\ d_1 exp(\mu_1) + \ldots d_m exp(\mu_m) & = 0 \end{cases}$$

have infinitely many solutions in $\mathbb{C}$?

Questions

1. When does the polynomial $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$ has no solutions in $\mathbb{C}$?
2. If $\lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_n, c_1, \ldots, c_m, d_1, \ldots, d_n \in \mathbb{C}$, when does the system

$$\begin{cases} c_1 exp(\lambda_1) + \ldots c_n exp(\lambda_n) & = 0 \\ d_1 exp(\mu_1) + \ldots d_m exp(\mu_m) & = 0 \end{cases}$$

have infinitely many solutions in $\mathbb{C}$?

Questions

1. When does the polynomial $F(z_1, \dots, z_n) \in \mathbb{C}[z_1, \dots, z_n]^E$ has no solutions in $\mathbb{C}$?
2. If $\lambda_1, \dots, \lambda_m, \mu_1, \dots, \mu_n, c_1, \dots, c_m, d_1, \dots, d_n \in \mathbb{C}$, when does the system

$$\begin{cases} c_1 exp(\lambda_1) + \dots c_n exp(\lambda_n) & = 0 \\ d_1 exp(\mu_1) + \dots d_m exp(\mu_m) & = 0 \end{cases}$$

have infinitely many solutions in $\mathbb{C}$?

Answers to first question

1. **Theorem (Henson and Rubel 1984):**

   Let $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

   $F(z_1, \ldots, z_n)$ has no solution in $\mathbb{C}$ iff $F(z_1, \ldots, z_n) = e^{G(z_1, \ldots, z_n)}$

   where $G(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

1. **Theorem (DMT):**

   Let $F(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$, where K is a Zilber field, then

   $F(z_1, \ldots, z_n)$ has no root in K iff $F(z_1, \ldots, z_n) = e^{H(z_1, \ldots, z_n)}$,

   where $H(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$.

   Proof:

   We use algebraic methods

Answers to first question

1. **Theorem (Henson and Rubel 1984):**

   Let $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

   $F(z_1, \ldots, z_n)$ has no solution in $\mathbb{C}$ iff $F(z_1, \ldots, z_n) = e^{G(z_1, \ldots, z_n)}$

   where $G(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

1. **Theorem (DMT):**

   Let $F(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$, where K is a Zilber field, then

   $F(z_1, \ldots, z_n)$ has no root in K iff $F(z_1, \ldots, z_n) = e^{H(z_1, \ldots, z_n)}$,

   where $H(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$.

   Proof:

   We use algebraic methods

1. **Theorem (Henson and Rubel 1984):**

   Let $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

   $F(z_1, \ldots, z_n)$ has no solution in $\mathbb{C}$ iff $F(z_1, \ldots, z_n) = e^{G(z_1, \ldots, z_n)}$

   where $G(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

1. **Theorem (DMT):**

   Let $F(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$, where K is a Zilber field, then

   $F(z_1, \ldots, z_n)$ has no root in K iff $F(z_1, \ldots, z_n) = e^{H(z_1, \ldots, z_n)}$,

   where $H(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$.

   Proof:

   We use algebraic methods

Answers to first question

1. **Theorem (Henson and Rubel 1984):**

   Let $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

   $F(z_1, \ldots, z_n)$ has no solution in $\mathbb{C}$ iff $F(z_1, \ldots, z_n) = e^{G(z_1, \ldots, z_n)}$

   where $G(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

1. **Theorem (DMT):**

   Let $F(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$, where K is a Zilber field, then

   $F(z_1, \ldots, z_n)$ has no root in K iff $F(z_1, \ldots, z_n) = e^{H(z_1, \ldots, z_n)}$,

   where $H(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$.

   Proof:

   We use algebraic methods

Answers to first question

1. **Theorem (Henson and Rubel 1984):**

   Let $F(z_1, \dots, z_n) \in \mathbb{C}[z_1, \dots, z_n]^E$.

   $F(z_1, \dots, z_n)$ has no solution in $\mathbb{C}$ iff $F(z_1, \dots, z_n) = e^{G(z_1, \dots, z_n)}$

   where $G(z_1, \dots, z_n) \in \mathbb{C}[z_1, \dots, z_n]^E$.

1. **Theorem (DMT):**

   Let $F(z_1, \dots, z_n) \in K[z_1, \dots, z_n]^E$, where K is a Zilber field, then

   $F(z_1, \dots, z_n)$ has no root in K iff $F(z_1, \dots, z_n) = e^{H(z_1, \dots, z_n)}$,

   where $H(z_1, \dots, z_n) \in K[z_1, \dots, z_n]^E$.

   Proof:

   We use algebraic methods

Answers to first question

1. **Theorem (Henson and Rubel 1984):**

   Let $F(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

   $F(z_1, \ldots, z_n)$ has no solution in $\mathbb{C}$ iff $F(z_1, \ldots, z_n) = e^{G(z_1, \ldots, z_n)}$

   where $G(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]^E$.

1. **Theorem (DMT):**

   Let $F(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$, where K is a Zilber field, then

   $F(z_1, \ldots, z_n)$ has no root in K iff $F(z_1, \ldots, z_n) = e^{H(z_1, \ldots, z_n)}$,

   where $H(z_1, \ldots, z_n) \in K[z_1, \ldots, z_n]^E$.

   Proof:

   We use algebraic methods

Answers to first question

1. **Theorem (Henson and Rubel 1984):**

   Let $F(z_1, \dots, z_n) \in \mathbb{C}[z_1, \dots, z_n]^E$.

   $F(z_1, \dots, z_n)$ has no solution in $\mathbb{C}$ iff $F(z_1, \dots, z_n) = e^{G(z_1, \dots, z_n)}$

   where $G(z_1, \dots, z_n) \in \mathbb{C}[z_1, \dots, z_n]^E$.

1. **Theorem (DMT):**

   Let $F(z_1, \dots, z_n) \in K[z_1, \dots, z_n]^E$, where K is a Zilber field, then

   $F(z_1, \dots, z_n)$ has no root in K iff $F(z_1, \dots, z_n) = e^{H(z_1, \dots, z_n)}$,

   where $H(z_1, \dots, z_n) \in K[z_1, \dots, z_n]^E$.

   Proof:

   We use algebraic methods

Answer to second question

2. Unknown, but there is a nice conjecture:

   Shapiro's Conjecture (1958): If two exponential polynomials f, g of the form

   $$f = c_1 e^{\lambda_1 z} + \ldots + c_n e^{\lambda_n z}, g = b_1 e^{\mu_1 z} + \ldots + b_m e^{\mu_m z},$$

   where $c_i, b_j, \lambda_i, \mu_j \in \mathbb{C}$ have infinitely many zeros in common they are both multiples of some exponential polynomial of the same kind.

Answer to second question

2. Unknown, but there is a nice conjecture:

   Shapiro's Conjecture (1958): If two exponential polynomials f, g of the form

   $$f = c_1 e^{\lambda_1 z} + \ldots + c_n e^{\lambda_n z}, g = b_1 e^{\mu_1 z} + \ldots + b_m e^{\mu_m z},$$

   where $c_i, b_j, \lambda_i, \mu_j \in \mathbb{C}$ have infinitely many zeros in common they are both multiples of some exponential polynomial of the same kind.

Answer to second question

2. Unknown, but there is a nice conjecture:

   Shapiro's Conjecture (1958): If two exponential polynomials f, g of the form

   $$f = c_1 e^{\lambda_1 z} + \ldots + c_n e^{\lambda_n z}, g = b_1 e^{\mu_1 z} + \ldots + b_m e^{\mu_m z},$$

   where $c_i, b_j, \lambda_i, \mu_j \in \mathbb{C}$ have infinitely many zeros in common they are both multiples of some exponential polynomial of the same kind.

Answer to second question

2. Unknown, but there is a nice conjecture:

   Shapiro's Conjecture (1958): If two exponential polynomials f, g of the form

   $$f = c_1 e^{\lambda_1 z} + \ldots + c_n e^{\lambda_n z}, g = b_1 e^{\mu_1 z} + \ldots + b_m e^{\mu_m z},$$

   where $c_i, b_j, \lambda_i, \mu_j \in \mathbb{C}$ have infinitely many zeros in common they are both multiples of some exponential polynomial of the same kind.

Answer to second question

2. Unknown, but there is a nice conjecture:

Shapiro's Conjecture (1958): If two exponential polynomials f, g of the form

$$f = c_1 e^{\lambda_1 z} + \ldots + c_n e^{\lambda_n z}, g = b_1 e^{\mu_1 z} + \ldots + b_m e^{\mu_m z},$$

where $c_i, b_j, \lambda_i, \mu_j \in \mathbb{C}$ have infinitely many zeros in common they are both multiples of some exponential polynomial of the same kind.

Answer to second question

2. Unknown, but there is a nice conjecture:

   Shapiro's Conjecture (1958): If two exponential polynomials f, g of the form

   $$f = c_1 e^{\lambda_1 z} + \ldots + c_n e^{\lambda_n z}, g = b_1 e^{\mu_1 z} + \ldots + b_m e^{\mu_m z},$$

   where $c_i, b_j, \lambda_i, \mu_j \in \mathbb{C}$ have infinitely many zeros in common they are both multiples of some exponential polynomial of the same kind.

Special case of Shapiro's Conjecture in $\mathbb{C}$

Theorem (A.J. van der Poorten, R. Tijdeman) (1):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, with $\alpha_j, \beta_j \in \mathbb{C}$, be a simple exponential polynomial and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomial.

Remark:

The factorization theorem implies that we need to consider only two cases of the Shapiro problem.

Special case of Shapiro's Conjecture in $\mathbb{C}$

Theorem (A.J. van der Poorten, R. Tijdeman) (1):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, with $\alpha_j, \beta_j \in \mathbb{C}$, be a simple exponential polynomial and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomial.

Remark:

The factorization theorem implies that we need to consider only two cases of the Shapiro problem.

Special case of Shapiro's Conjecture in $\mathbb{C}$

Theorem (A.J. van der Poorten, R. Tijdeman) (1):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, with $\alpha_j, \beta_j \in \mathbb{C}$, be a simple exponential polynomial and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomial.

Remark:

The factorization theorem implies that we need to consider only two cases of the Shapiro problem.

Theorem (A.J. van der Poorten, R. Tijdeman) (1):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, with $\alpha_j, \beta_j \in \mathbb{C}$, be a simple exponential polynomial and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomial.

Remark:

The factorization theorem implies that we need to consider only two cases of the Shapiro problem.

Integers solutions

Theorem (Skolem, Malher, Lech):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, be an exponential polynomial, where $\alpha, \beta \in K$ where K is a field of characteristic 0. If $f(z)$ vanishes for infinitely many integers $z = z_i$, then there exists an integer d and certain set of least residues modulo $d, d_1, \ldots, d_l$ such that $f(z)$ vanishes for all integers $z \equiv d_i (mod\ d)$, for $i = 1, \ldots, l$, and $f(z)$ vanishes only finitely often on other integers.

Theorem (A.J. van der Poorten, R. Tijdeman):

Theorem (1) is equivalent to the Skolem-Malher-Lech Theorem

Integers solutions

Theorem (Skolem, Malher, Lech):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, be an exponential polynomial, where $\alpha, \beta \in K$ where K is a field of characteristic 0. If $f(z)$ vanishes for infinitely many integers $z = z_i$, then there exists an integer d and certain set of least residues modulo $d, d_1, \ldots, d_l$ such that $f(z)$ vanishes for all integers $z \equiv d_i (mod\ d)$, for $i = 1, \ldots, l$, and $f(z)$ vanishes only finitely often on other integers.

Theorem (A.J. van der Poorten, R. Tijdeman):

Theorem (1) is equivalent to the Skolem-Malher-Lech Theorem

Theorem (Skolem, Malher, Lech):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, be an exponential polynomial, where $\alpha, \beta \in K$ where K is a field of characteristic 0. If $f(z)$ vanishes for infinitely many integers $z = z_i$, then there exists an integer d and certain set of least residues modulo $d, d_1, \ldots, d_l$ such that $f(z)$ vanishes for all integers $z \equiv d_i (mod \ d)$, for $i = 1, \ldots, l$, and $f(z)$ vanishes only finitely often on other integers.

Theorem (A.J. van der Poorten, R. Tijdeman):

Theorem (1) is equivalent to the Skolem-Malher-Lech Theorem

Theorem (DMT):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, with $\alpha_j, \beta_j \in K$, where K is a Zilber Field, be a simple exponential polynomial and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomial.

Theorem (DMT):

Let $f(z) = \sum \alpha_j e^{\beta_j z}$, with $\alpha_j, \beta_j \in K$, where K is a Zilber Field, be a simple exponential polynomial and let $g(z)$ be an arbitrary exponential polynomial such that $f(z)$ and $g(z)$ have infinitely many common zeros. Then there exists an exponential polynomial $h(z)$, with infinitely many zeros, such that h is a common factor of f and g in the ring of exponential polynomial.