Exponential Algebra and Schanuel's Conjecture

Giuseppina Terzo

Seconda Università degli Studi di Napoli

30 November 2009, Paris

Goals

- **Exponential rings, exponential fields and exponential polynomial ring**
- **Schanuel's Conjecture, its variants and some consequences**
- **O-minimal structures**

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 $r \in S$

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

Free object

Definition: The free E-ring on $\overline{X} = X_1, \ldots, X_n$, denoted by $[\overline{X}]^E$, is an E-ring containing $\overline{X}$ as elements such that for each E-ring R and any $r_1, \ldots, r_n \in R$ there is exactly one E-ring morphism:

$$f : [X_1, \ldots, X_n]^E \to (R, E)$$

such that $f(X_i) = r_i$ for $i = 1, \ldots n$.

Construction of the free object by recursion

Construction

$$\underset{\text{rings}}{([\overline{X}]_k, +, \cdot)_{k\geq -1}}, \quad \underset{\text{ab groups}}{(B_k, +)_{k\geq 0}} \quad \text{and} \quad \underset{E\text{-morphisms}}{(E_k)_{k\geq -1}}$$

Step 0:

$[\overline{X}]_{-1} = \{0\}$

$[\overline{X}]_0 = (\mathbb{Z}[\overline{X}], +, \cdot)$, $B_0 = (\mathbb{Z}[\overline{X}], +)$, and $E_{-1}(0) = 1$.

Construction

Inductive step:

Suppose $k \geq 0$ and $[\overline{X}]_{k-1}$, $[\overline{X}]_k$, B_k and E_{k-1} have been defined in such a way that:

$$[\overline{X}]_k = [\overline{X}]_{k-1} \oplus B_k, \;\; E_{k-1} : ([\overline{X}]_{k-1}, +) \to (\mathcal{U}([\overline{X}]_k), \cdot)$$

Let

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

an isomorphism. Define

$$[\overline{X}]_{k+1} = [\overline{X}]_k[t^{B_k}] \text{ (group ring construction).}$$

Therefore

$$[\overline{X}]_k \text{ is a subring of } [\overline{X}]_{k+1}$$

and

$$[\overline{X}]_{k+1} = [\overline{X}]_k \oplus B_{k+1}.$$

Construction

Define

$$E_k : ([\overline{X}]_k, +) \to (\mathcal{U}([\overline{X}]_{k+1}), \cdot) \text{ s.t.}$$

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

$$[\overline{X}]_0 \subset [\overline{X}]_1 \subset [\overline{X}]_2 \cdots \subset [\overline{X}]_k \subset \cdots$$

Then the free E-ring is:

$$[\overline{X}]^E = \lim_k [\overline{X}]_k = \bigcup_{k=0}^{\infty} [\overline{X}]_k$$

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

$$E(x) = E_k(x) \textbf{ if } x \in [\overline{X}]_k, \ \ k \in \mathbb{N}.$$

Free object

Let $P(\overline{X}) \in [\overline{X}]^E$, then $P(\overline{X}) \in [\overline{X}]_k$ for some $k \in \mathbb{N}$,

$$P(\overline{X}) = p_0 + p_1 + \cdots + p_k \text{ where } p_i \in [\overline{X}]_i$$

$$p_i = \sum_{d_i \in B_{i-1}} c_i E(d_i), \text{ where } c_i \in [\overline{X}]_{i-1}.$$

Example:

Let $P(x, y) \in [x, y]^E$

$$P(x,y) = -3x^2y - x^5y^7 + (2xy + 5y^2 - x^5)\mathbf{e}^{(-7x^3+11x^5y^4)} +$$

$$+ (6 - 2xy^5)\mathbf{e}^{(5x+2y^2)\mathbf{e}^{5x-10y^2}} - 3xy\mathbf{e}^{(-2x+y^5)\mathbf{e}^{(x^3y^5+3)\mathbf{e}^{(9xy+y^2-5)}}}$$

Exponential ideals

Definition: Let R be an E-ring, and I be an ideal of R (as a ring). I is an E-ideal:

$$\text{if } \alpha \in I \text{ then } E(\alpha) - 1 \in I.$$

Remark:

- R Noetherian $\Rightarrow$ $R[\overline{X}]$ Noetherian.
- (R, E) Noetherian $\not\Rightarrow$ $R[\overline{X}]^E$ Noetherian.

$(\mathbb{C}, E)$ is Noetherian, $\mathbb{C}[X]^E$ **is not Noetherian.**

Schanuel's Conjecture

Schanuel's Conjecture (SC) 1960

Let $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ 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 $\mathbb{Q}$.

Theorem (Lindemann-Weierstrass 1885)

If $\alpha_1, \ldots, \alpha_n$ are algebraic numbers which are linearly independent over $\mathbb{Q}$, then $e^{\alpha_1}, \ldots, e^{\alpha_n}$ are algebraically independent over $\mathbb{Q}$.

Known cases

- $\lambda = 1$ transcendence of e; **[Hermite (1873)]**
- $\lambda = 2\pi i$ transcendence of π; **[Lindemann (1882)]**
- $\overline{\lambda} = \pi, i\pi$, then π and e^{π} are algebraically independent over $\mathbb{Q}$; **[Nesterenko (1996)]**

The Schanuel's machine

- $\overline{\lambda} = (1, i\pi)$,

$$\mathbf{SC} \Rightarrow t.d(1, \pi, e, e^{i\pi}) \geq l.d.(1, i\pi).$$

Then e, π are algebraically independent over $\mathbb{Q}$;

- $\overline{\lambda} = (1, \pi, \pi i)$,

$$\mathbf{SC} \Rightarrow t.d(1, \pi, i\pi, e, e^{\pi}, e^{i\pi}) \geq l.d.(1, \pi, i\pi).$$

Then e, π, e^{π} are algebraically independent over $\mathbb{Q}$;

- $\overline{\lambda} = (1, i\pi, e)$

$$\mathbf{SC} \Rightarrow t.d(1, i\pi, e, e, e^{i\pi}, e^{e}) \geq l.d.(1, i\pi, e).$$

Then π, e, e^{e} are algebraically independent over $\mathbb{Q}$;

The Schanuel's machine

- $\overline{\lambda} = (1, i\pi, i\pi^2, e, e^e, e^{i\pi^2})$,

$$\textbf{SC} \Rightarrow t.d(1, i\pi, i\pi^2, e, e^e, e^{i\pi^2}, e, e^{i\pi}, e^{i\pi^2}, e^e, e^{e^e}, e^{e^{i\pi^2}})$$

$$\geq l.d.(1, i\pi, i\pi^2, e, e^e, e^{i\pi^2}).$$

Then $\pi, e, e^e, e^{e^e}, e^{i\pi^2}, e^{e^{i\pi^2}}$ are algebraically independent over $\mathbb{Q}$;

- $\overline{\lambda} = (1, 2i\pi, \log\pi, e\log\pi)$,

$$\textbf{SC} \Rightarrow t.d(1, 2i\pi, \log\pi, e\log\pi, e, e^{2i\pi}, e^{\log\pi}, e^{e\log\pi}) \geq$$

$$l.d.(1, 2i\pi, \log\pi, e\log\pi).$$

Then $e, \pi, \log\pi, \pi^e$ are algebraically independent over $\mathbb{Q}$.

First consequences of Schanuel's Conjecture

Theorem (Macintyre and Wilkie 1990) (SC) $Th(\mathbb{R}, e^x)$ is decidable.

Theorem (Macintyre 1991): Suppose (S, E) satisfies Schanuel's Condition, and S_0 is the E-subring of S generated by 1. Then the natural E-morphism

$$\varphi : [\emptyset]^E \to S_0$$

is an isomorphism.

Corollary: (SC) There exists an algorithm which decides if two exponential constants coincide.

Main results

Theorem (T.): (SC) Let $[x, y]^E$ be the free E-ring generated by $\{x, y\}$ and let ψ be the E-morphism:

$$\psi : [x, y]^E \to (\mathbb{C}, E)$$

defined by $\psi(x) = \pi$ and $\psi(y) = i$. Then there exists a unique isomorphism

$$f : [x, y]^E / Ker\psi \to \langle i, \pi \rangle^E$$

s. t.

$$Ker\psi = \langle e^{xy} + 1, y^2 + 1 \rangle^E.$$

Corollary (T.): (SC) The only algebraic relations among π, e and i in $\mathbb{C}$ are

$$e^{i\pi} = -1 \textbf{ and } i^2 = -1$$

Corollary (D'Aquino and T.): (SC) There exists an algorithm which decides if two exponential polynomials in π and i are equal in $\mathbb{C}$.

Non principal E-ideal

Theorem (T.): The E-ideal

$$\langle e^{xy} + 1, y^2 + 1 \rangle^E$$

in $[x, y]^E$ is not principal.

Proof: Uses augmentation maps and augmentation ideals.

Algebraic relations over $(\mathbb{R}, e^x)$

Theorem (T.): (SC) Let $[x]^E$ be the free E-ring generated by $\{x\}$ and let R be the E-subring of $(\mathbb{R}, E)$ generated by π. Then the E-morphism φ

$$\varphi : [x]^E \to (R, E)$$

$$x \mapsto \pi$$

is an E-isomorphism.

Corollary (D'Aquino and T.): (SC) There exists an algorithm which decides if two exponential polynomials in π are equal in $\mathbb{R}$.

Variants of Schanuel's Conjecture: SC for the E-polynomial ring

Theorem (D'Aquino, Macintyre and T.): Let K be an E-field. Suppose that $\gamma_1, \ldots, \gamma_n \in K[\overline{X}]^E - K$ are linearly independent over $\mathbb{Q}$. Then

$$t.d._K K(\gamma_1, \ldots, \gamma_n, E(\gamma_1), \ldots, E(\gamma_n)) \geq n + 1.$$

Schanuel's Conjecture for the power series

Theorem (Ax 1971): Let $y_1, \ldots, y_n \in t\mathbb{C}[[t]]$ linearly independent over $\mathbb{Q}$. Then

$$t.d._{\mathbb{C}(t)}\mathbb{C}(y_1, \ldots, y_n, e^{y_1}, \ldots, e^{y_n}) \geq n.$$

Schanuel's Conjecture for differential algebra

Theorem (Ax 1971): (SD) Let K be a field and D a derivation of K with constants $C \supseteq \mathbb{Q}$. Let $y_1, \ldots, y_n, z_1, \ldots, z_n \in K^*$ such that:

- $Dy_j = \frac{Dz_j}{z_j}$ for $j = 1, \ldots, n$;
- $Dy_1, \ldots, Dy_n$ are linearly independent over $\mathbb{Q}$.

Then

$$t.d._C C(y_1, \ldots, y_n, z_1, \ldots, z_n) \geq n + 1.$$

O-minimality

Definition: An expansion $\mathcal{R} = (R, <, \ldots)$ of a totally ordered, dense set $(R, <)$ and without end points is an **o-minimal structure** if every subset of R which is definable in $\mathcal{R}$ is a finite union of intervals and points.

Denote by $\mathbb{R}_{exp} = \langle \mathbb{R}, +, \cdot, 0, 1, <, exp \rangle$.

Theorem: $\mathbb{R}_{exp}$ is an o-minimal structure.

Notions

Let τ be a real number not definable in $\mathbb{R}_{exp}$ over $\mathbb{Q}$:

- For any $a \in \mathbb{R}$ there exists $\theta : \mathbb{R} \to \mathbb{R}$ such that $\theta(\tau) = a$.
- Let $\delta_\tau : \mathbb{R} \to \mathbb{R}$, such that $\delta_\tau(a) = \frac{d\theta}{dx}(\tau)$.
- δ_τ is a derivation over $\mathbb{R}$ and we denote by C the field of constants.

Theorem (Edmundo, T.): Let τ and C be as above. Let $\alpha_1, \ldots, \alpha_n$ be real numbers such that $\delta_\tau(\alpha_1), \ldots, \delta_\tau(\alpha_n)$ are linear independent over $\mathbb{Q}$. Then

$$t.d._C C(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}) \geq n + 1.$$

Proof: We apply (SD), where $y_i = \alpha_i$ and $z_i = e^{\alpha_i}$ for each $i = 1, \ldots, n$. Then

- $\delta_\tau(y_i) = \frac{\delta_\tau(z_i)}{z_i}$ for all $i = 1, \ldots, n$;
- the $\delta_\tau(y_i)$ are $\mathbb{Q}$-linearly independent.

Thus the conditions of (SD) hold and so the conclusion follows.

E-subrings freely generated

Theorem (Edmundo, T.): Let $[x]^E$ be the free E-ring generated by $\{x\}$ and let R be the E-subring of $\mathbb{R}$ generated by τ, where τ is a real number not definable in $\mathbb{R}_{\exp}$. Then the E-morphism φ,

$$\varphi : [x]^E \to R$$

$$x \mapsto \tau$$

is an E-isomorphism.

O-minimality

We denote by $\mathbb{R}_{an,exp} = \langle \mathbb{R}, +, \cdot, 0, 1, <, exp, f \rangle$, with f are analytic functions restricted to a compact.

Theorem: $\mathbb{R}_{an,exp}$ is o-minimal.

Notions

Let τ be a real number not definable in the o-minimal structure $\mathcal{M} = \langle \mathbb{R}, +, \cdot, exp, \sin \restriction [-2, 2], <, 0, 1 \rangle$.

- Let C and δ_τ be as above.
- $$\partial_\tau : \mathbb{C} \to \mathbb{C}$$
$$z \mapsto \delta_\tau(Rez) + i\delta_\tau(Imz).$$
- The constants field is $K = C(i)$.

Complex version of SC

Theorem (Edmundo, T.): Let τ be a real number not definable in $\mathcal{M} = \langle \mathbb{R}, +, \cdot, exp, \sin \restriction [-2, 2], <, 0, 1 \rangle$, and K as above. Let $\alpha_1, \ldots \alpha_n$ be complex numbers such that $\partial_\tau(\alpha_1), \ldots, \partial_\tau(\alpha_n)$ are linearly independent over $\mathbb{Q}$. Then

$$t.d._K K(\alpha_1, \ldots \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n}) \geq n + 1.$$

Proof: We apply (SD), where $y_i = \alpha_i$ and $z_i = e^{\alpha_i}$ for each $i = 1, \ldots, n$. Then

- $\partial_\tau(y_i) = \frac{\partial_\tau(z_i)}{z_i}$ for all $i = 1, \ldots, n$;
- the $\partial_\tau(y_i)$ are $\mathbb{Q}$-linearly independent.

Thus the conditions of (SD) hold and so the conclusion follows.

E-subrings freely generated

Theorem (Edmundo, T.): Let $[x, y]^E$ be the free E-ring generated by $\{x, y\}$. Let τ be a real number not definable in $\mathcal{M}$. Then the E-morphism:

$$\psi : [x, y]^E \to (\mathbb{C}, +, \cdot, \exp)$$

$$x \mapsto \tau$$

$$y \mapsto i\tau$$

is an E-monomorphism.

The complex exponential field

Let $(\mathbb{C}, exp)$ be the complex exponential field

Open question

- Is $\mathbb{R}$ definable in $(\mathbb{C}, exp)$?
- Is every definable set countable or co-countable?
- Is there an automorphism of $(\mathbb{C}, exp)$ other than the identity and complex conjugation?