Formalization of transcendence proofs

The omnipresence of Polynomials

Sophie Bernard
supervised by Yves Bertot & Laurence Rideau

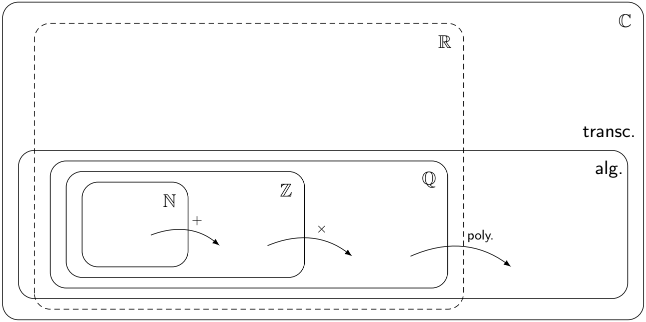
Université Côte d'Azur, Inria, France

May 30th, 2017

Today...

I Introduction
II Transcendence proofs
III Univariate polynomials
IV Multivariate polynomials
V Conclusion

Number hierarchy



Vocabulary

Definition (algebraic)

A number is algebraic if it is the root of a non-zero polynomial whose coefficients lie in $\mathbb{Q}$.

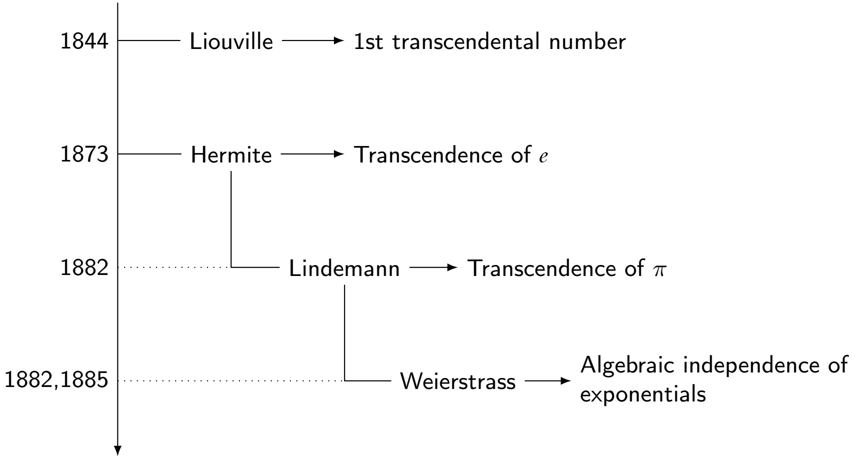
Definition (transcendental)

A number is transcendental if it is not algebraic.

Examples :

- -5 is a root of $X^2 - 25$.
- i is a root of $X^2 + 1$.
- $\sqrt[3]{2}$ is a root of $X^3 - 2$.
- -5 is also a root of $2X^3 - \frac{X^2}{3} - 50X + \frac{25}{3}$.

History


1844
Liouville
1st transcendental number
1873
Hermite
Transcendence of e
1882
Lindemann
Transcendence of π
1882,1885
Weierstrass
Algebraic independence of exponentials

Motivations

- To study the frontier between algebraic and transcendental numbers
- To connect different libraries
- To extend a library for multivariate polynomials (P-Y Strub)
- To formally prove the last big result on number theory of the 19th century

Motivations

- To study the frontier between algebraic and transcendental numbers
- To connect different libraries
- To extend a library for multivariate polynomials (P-Y Strub)
- To formally prove the last big result on number theory of the 19th century
- Analysis for functions $\mathbb{R} \to \mathbb{C}$.
- Fundamental theorem of symmetric polynomials
- Minimal polynomial
- Conjugates of a polynomial

Transcendence of e and π

Definition (algebraic)

A number is algebraic if it is the root of a non-zero polynomial whose coefficients lie in $\mathbb{Q}$.

Algebraic

```
Definition algebraicOver (fFtoE : F → E) u :=
  exists p, p != 0 & root (map_poly fFtoE p) u.
```

Statements

```
Theorem e_transcendental : ~(algebraicOver ratr (exp 1)%:C).
Theorem pi_transcendental : ~(algebraicOver ratr PI%:C).
```

Lindemann-Weierstrass theorem

Theorem (Lindemann-Weierstrass)

For any non-zero natural number n and any algebraic numbers $a_1, \ldots, a_n$, if the set $\{a_1, \ldots, a_n\}$ is linearly independant over $\mathbb{Q}$, then $\{e^{a_1}, \ldots, e^{a_n}\}$ is algebraically independant over $\mathbb{Q}$.

Coq statement

```
Theorem Lindemann (n : nat) (a : complexR ^ n) :
   (n > 0)%N →
   (forall i : 'I_n, a i is_algebraic) →
   (forall (lambda : complexR ^ n),
      (forall i : 'I_n, lambda i \is a Cint) →
      (exists i : 'I_n, lambda i != 0) →
      \sum_(i < n) (lambda i * a i) != 0) →
   forall p, p \is a mpolyOver _ Cint →
   p != 0 →
   p.@[finfun (Cexp \o a)] != 0.
```

Baker's reformulation

Theorem (Baker's reformulation)

For any non-zero natural number l, any distinct algebraic numbers $\alpha_1, \ldots, \alpha_l$ and any non-zero algebraic numbers $\beta_1, \ldots, \beta_l$, we have :

$$\beta_1 e^{\alpha_1} + \ldots + \beta_l e^{\alpha_l} \neq 0.$$

Coq statement

```
Theorem LindemannBaker :
  forall (l : nat) (alpha : complexR ^ l.+1) (a : complexR ^ l.+1),
  injective alpha →
  (forall i : 'I_l.+1, alpha i is_algebraic) →
  (forall i : 'I_l.+1, a i != 0) →
  (forall i : 'I_l.+1, a i is_algebraic) →
  (Cexp_span a alpha != 0).
```

Context

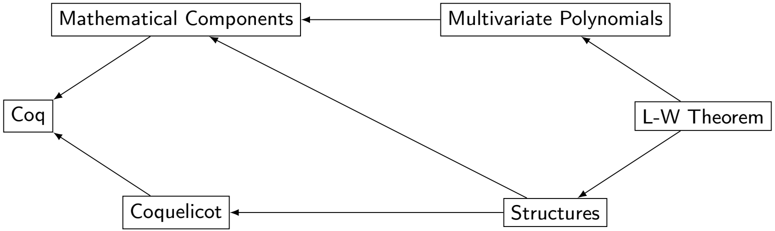


Figure – Link between the different libraries

Transcendence of e

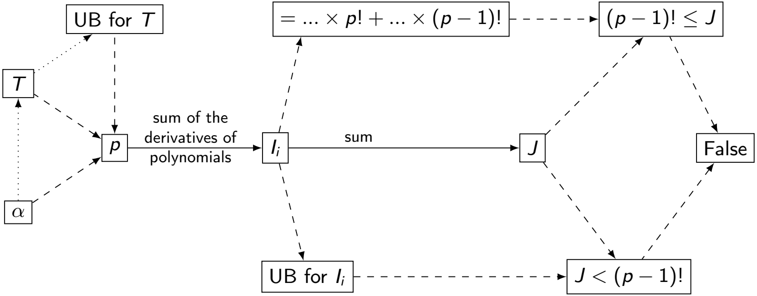


Figure – Proof structure of the transcendence of e

Lindemann-Weierstrass Theorem

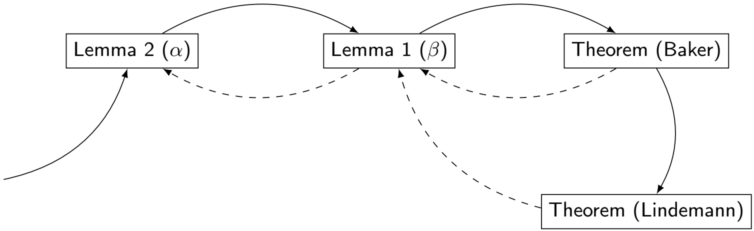


Figure – Implications between the different theorems and lemmas

Lemmas for Baker's reformulation

Theorem (Baker's reformulation)

For any non-zero natural number l, any distinct algebraic numbers $\alpha_1, \ldots, \alpha_l$ and any non-zero algebraic numbers $\beta_1, \ldots, \beta_l$, we have :

$$\beta_1 e^{\alpha_1} + \ldots + \beta_l e^{\alpha_l} \neq 0.$$

Lemma (1)

For any non-zero natural number l, any distinct algebraic numbers $\alpha_1, \ldots, \alpha_l$ and any non-zero integers $\beta_1, \ldots, \beta_l$, we have :

$$\beta_1 e^{\alpha_1} + \ldots + \beta_l e^{\alpha_l} \neq 0.$$

Lemma (2)

For any non-zero natural number l, any distinct algebraic numbers $\alpha_1, \ldots, \alpha_l$ and any non-zero integers $\beta_1, \ldots, \beta_l$, such that the α's can be grouped into a partition A, if for each part in A, the α's form a complete set of conjugates, and on each part in A, the β's are constant, we have :

$$\beta_1 e^{\alpha_1} + \ldots + \beta_l e^{\alpha_l} \neq 0.$$

Proof of Lemma 2

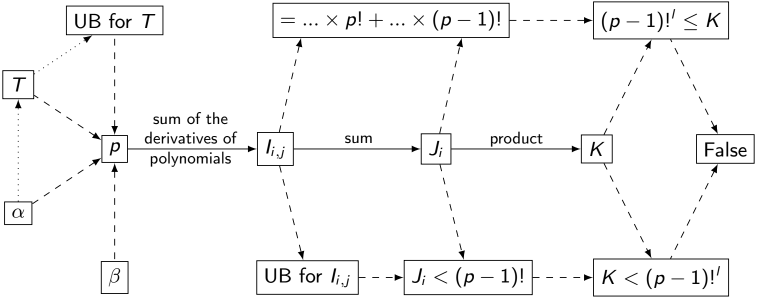


Figure – Proof of Lemma 2

Transcendence of e

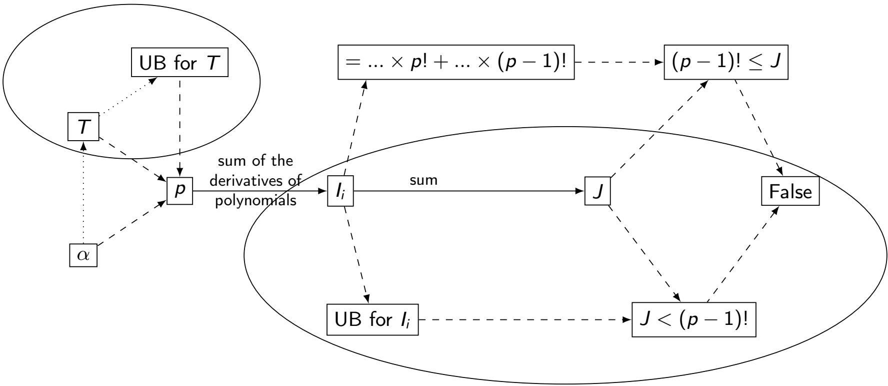


Figure – Proof structure of the transcendence of e

Analysis

- Functions from $\mathbb{R}$ to $\mathbb{C}$
- Goals : integral of a derivative, upper bound on integrals

$$\int_0^1 \alpha e^{-\alpha x} P(\alpha x)\mathrm{d}x = \sum_i P^{(i)}(0) - e^{-\alpha} \sum_i P^{(i)}(\alpha)$$

```
Definition RInt (f : R → R) (a b : R)
```

- Extensions of continuity, derivative and integral
- Not on the Coquelicot complex numbers !

Useful lemmas

Theorem

Let f be a function from $\mathbb{R}$ to $\mathbb{C}$, let a and b be real numbers such that f is differentiable at any point between a and b, and its derivative is continuous at any point between a and b, then

$$\int_a^b f'(t)\mathrm{d}t = f(b) - f(a)$$

```
Lemma RInt_Crderive f a b:
  (forall x, Rmin a b <= x <= Rmax a b → ex_derive f x) →
  (forall x, Rmin a b <= x <= Rmax a b →
        Crcontinuity_pt (Crderive f) x) →
  CrInt (Crderive f) a b = f b - f a.
```

Useful lemmas

Theorem

Let f be a function from $\mathbb{R}$ to $\mathbb{C}$, let a and b be real numbers such that $a \leq b$, and f is continuous at any point between a and b, then

$$\left|\int_a^b f(t)\mathrm{d}t\right| \leq \int_a^b |f(t)|\mathrm{d}t$$

```
Lemma CrInt_norm f a b :
  a <= b →
  (forall x, Rmin a b <= x <= Rmax a b → Crcontinuity_pt f x) →
  norm (CrInt f a b) <= RInt (fun t => norm (f t)) a b.
```

Minimal polynomial

Definition (Minimal polynomial)

The minimal polynomial of a non-zero algebraic number x is the non-zero monic polynomial P over $\mathbb{Q}$ of least degree such that $P(x) = 0$.

But...

- Why ? Uniqueness, Conjugate elements, Many properties, ...
- How ? Existence in `algC` (`minCpoly`), in finite extensions of fields (`minPoly`), in a field with a decidable embedding in a closed field (`minPoly_decidable_closure`).
- So ? Use the existing constructions.

Existence proof of a minimal polynomial

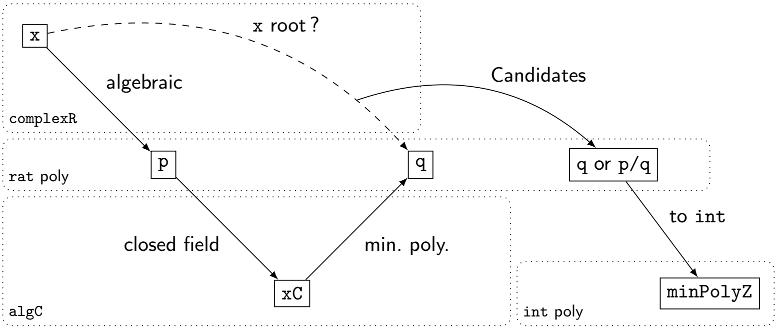


Figure – Existence of a minimal polynomial

Multivariate Polynomials

Definition (Vocabulary)

n-variate polynomial on a ring R

- Indeterminates (ex. $X_1, \ldots, X_n$ or X, Y, Z)
- Monomials : product of indeterminates (ex. $X_1^3 X_3 X_4^2$)
- Multinomials : linear combination of monomials with coefficients in a ring R (ex. $\sqrt{2}i X_1^2 X_6 + \frac{2}{3} X_2^4 X_3$)

How to ?

- Iterated polynomials
- Free abelian group
- Monomials algebra

Symmetric polynomials

Definition (Symmetric polynomials)

A n-variate polynomial P is symmetric if

$$\forall \sigma \in \mathfrak{S}_n, P[X_{\sigma(1)}, \ldots, X_{\sigma(n)}] = P$$

Examples with 3 variables

- $X^3Y^2Z + XY^3Z^2 + X^2YZ^3$ is not symmetric
- $X^3Y^2Z + XY^3Z^2 + X^2YZ^3 + X^3YZ^2 + XY^2Z^3 + X^2Y^3Z$ is symmetric

Basis of symmetric polynomials

- Elementary symmetric polynomials $s_{n,k}$: n-variate polynomial, sum of all distinct products of k distinct variables.
  ex. $s_{3,2} = XY + XZ + YZ$
- Monomial symmetric polynomials m_u (u is a monomial) : polynomial with the same number of variables as u, sum of all distinct monomials obtained when we permute the variables of u.
  ex. 3 variables : $m_{X^2Y} = X^2Y + X^2Z + Y^2X + Y^2Z + Z^2X + Z^2Y$.

Fundamental theorems of symmetric polynomials

Fundamental theorem of symmetric polynomials, v1

Let P be a symmetric n-variate polynomial, with coefficients in a ring R.
There exists a n-variate polynomial Q whose coefficients are in R such that :

$$P = Q[s_{n,1}, \ldots, s_{n,n}]$$

Fundamental theorem of symmetric polynomials, v2

Let P be a symmetric n-variate polynomial, with coefficients in a ring R.
There exists a finite sequence (λ_i) of elements of R, and a finite sequence of monomials (u_i) such that :

$$P = \sum_i \lambda_i m_{u_i}$$

Consequence : the evaluation of a symmetric polynomial on the set of roots of an univariate polynomial is in the ring A if both polynomials have all their coefficients in A.

Subset of variables

All the definitions and lemmas can be extended to allow only a subset A of variables to be considered.

- Symmetric on a subset A : permutations of A.
- Monomial symmetric polynomials on a subset A.
- Evaluation of a multinomial on a subset A.
- Fundamental theorem of symmetric polynomials, v3 ?
- Consequence of the evaluation ?

Conjugates

Definition (Conjugates)

The conjugates of an algebraic number x are the roots of its minimal polynomial.

By extension :

- The conjugates of a non-zero polynomial in $\mathbb{Q}[X]$ are the conjugates of one of its roots.
- A set of complex numbers $\{x_1, \ldots, x_n\}$ is a complete set of conjugates if they are the conjugates of $\prod_{i=1}^{n}(X - x_i)$.
- Two algebraic numbers x and y are conjugates if they have the same minimal polynomial.

Example :

- $X^2 - 2$ has two roots : $\sqrt{2}$ and $-\sqrt{2}$.
- $\sqrt{2}$ and $-\sqrt{2}$ are the conjugates of $\sqrt{2}$, but also of $X^2 - 2$.
- $\{\sqrt{2}, -\sqrt{2}\}$ is a complete set of conjugates

But why ?

Fundamental theorem of symmetric polynomials, v3

- n a non-zero natural number
- Λ a partition of $\{X_1, \ldots, X_n\}$
- P a n-variate polynomial, with coefficients in $\mathbb{Q}$, symmetric on each part of Λ
- $\alpha_1, \ldots, \alpha_n$ distinct complex numbers
- for each part of Λ, the α's are a complete set of conjugates (ex. if $\{X_1, X_2\} \in \Lambda$, $\{\alpha_1, \alpha_2\}$ should be a complete set of conjugates)

Then $P[\alpha_1, \ldots, \alpha_n]$ is a rational number.

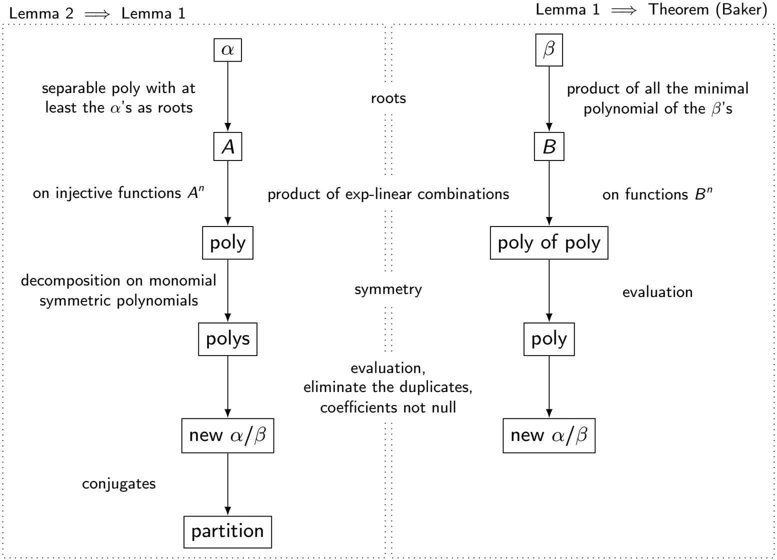


Figure – Comparison of the proofs of L. 2 $\implies$ L. 1 and L. 1 $\implies$ Th. (Baker)

Contributions

- Symmetrized of a monomial, Monomial symmetric polynomials
- Symmetry on a subset, ...
- Partial evaluation of multinomials
- Fundamental theorem of symmetric polynomials
- Conjugates of a polynomial
- Analysis for functions from $\mathbb{R}$ to $\mathbb{C}$
- Structures for archimedean field (`Cint`, `Cnat`)

Future Work

- Use the new multinomials
- Develop more lemmas on the conjugates
- Better real/complex numbers
- Better link between coquelicot/mathcomp
- Morphism between algebraic numbers of `complexR` and `algC`
- Padé approximants ?