The Transcendence of e

Manuel Eberl

December 14, 2021

Abstract

This work contains a formalisation of the proof that Euler's number e is transcendental. The proof follows the standard approach of assuming that e is algebraic and then using a specific integer polynomial to derive two inconsistent bounds, leading to a contradiction.

This approach can be found in many different sources; this formalisation mostly follows a PlanetMath article [1] by Roger Lipsett.

Contents

1 Proof of the Transcendence of e

theory *E-Transcendental*
  imports
    HOL−Complex-Analysis.Complex-Analysis
    HOL−Number-Theory.Number-Theory
    HOL−Computational-Algebra.Polynomial
begin

1.1 Various auxiliary facts

lemma *fact-dvd-pochhammer*:
  assumes $m \le n + 1$
  shows $fact\ m\ dvd\ pochhammer\ (int\ n - int\ m + 1)\ m$
$\langle proof \rangle$

lemma *of-nat-eq-1-iff* [*simp*]: $of\text{-}nat\ x = (1 :: 'a :: semiring\text{-}char\text{-}0) \longleftrightarrow x = 1$
  $\langle proof \rangle$

lemma *prime-elem-int-not-dvd-neg1-power*:

$prime\text{-}elem\ (p :: int) \Longrightarrow \neg p\ dvd\ (-1)\ \widehat{}\ n$
⟨proof⟩

lemma *nat-fact* [*simp*]: $nat\ (fact\ n) = fact\ n$
⟨proof⟩

lemma *prime-dvd-fact-iff-int*:
$p\ dvd\ fact\ n \longleftrightarrow p \leq int\ n$ **if** $prime\ p$
⟨proof⟩

lemma *filterlim-minus-nat-at-top*:
$filterlim\ (\lambda n.\ n - k :: nat)\ at\text{-}top\ at\text{-}top$
⟨proof⟩

lemma *power-over-fact-tendsto-0*:
$(\lambda n.\ (x :: real)\ \widehat{}\ n\ /\ fact\ n) \longrightarrow 0$
⟨proof⟩

lemma *power-over-fact-tendsto-0'*:
$(\lambda n.\ c * (x :: real)\ \widehat{}\ n\ /\ fact\ n) \longrightarrow 0$
⟨proof⟩

1.2 Lifting integer polynomials

lift-definition *of-int-poly* :: $int\ poly \Rightarrow 'a :: comm\text{-}ring\text{-}1\ poly$ **is** $\lambda g\ x.\ of\text{-}int\ (g\ x)$
⟨proof⟩

lemma *coeff-of-int-poly* [*simp*]: $coeff\ (of\text{-}int\text{-}poly\ p)\ n = of\text{-}int\ (coeff\ p\ n)$
⟨proof⟩

lemma *of-int-poly-0* [*simp*]: $of\text{-}int\text{-}poly\ 0 = 0$
⟨proof⟩

lemma *of-int-poly-pCons* [*simp*]: $of\text{-}int\text{-}poly\ (pCons\ c\ p) = pCons\ (of\text{-}int\ c)\ (of\text{-}int\text{-}poly\ p)$
⟨proof⟩

lemma *of-int-poly-smult* [*simp*]: $of\text{-}int\text{-}poly\ (smult\ c\ p) = smult\ (of\text{-}int\ c)\ (of\text{-}int\text{-}poly\ p)$
⟨proof⟩

lemma *of-int-poly-1* [*simp*]: $of\text{-}int\text{-}poly\ 1 = 1$
⟨proof⟩

lemma *of-int-poly-add* [*simp*]: $of\text{-}int\text{-}poly\ (p + q) = of\text{-}int\text{-}poly\ p + of\text{-}int\text{-}poly\ q$
⟨proof⟩

lemma *of-int-poly-mult* [*simp*]: $of\text{-}int\text{-}poly\ (p * q) = (of\text{-}int\text{-}poly\ p * of\text{-}int\text{-}poly\ q)$
⟨proof⟩

lemma *of-int-poly-sum* [*simp*]: *of-int-poly* (*sum f A*) = *sum* (λx. *of-int-poly* (*f x*)) *A*
⟨*proof*⟩

lemma *of-int-poly-prod* [*simp*]: *of-int-poly* (*prod f A*) = *prod* (λx. *of-int-poly* (*f x*)) *A*
⟨*proof*⟩

lemma *of-int-poly-power* [*simp*]: *of-int-poly* (*p* ^ *n*) = *of-int-poly p* ^ *n*
⟨*proof*⟩

lemma *of-int-poly-monom* [*simp*]: *of-int-poly* (*monom c n*) = *monom* (*of-int c*) *n*
⟨*proof*⟩

lemma *poly-of-int-poly* [*simp*]: *poly* (*of-int-poly p*) (*of-int x*) = *of-int* (*poly p x*)
⟨*proof*⟩

lemma *poly-of-int-poly-of-nat* [*simp*]: *poly* (*of-int-poly p*) (*of-nat x*) = *of-int* (*poly p* (*int x*))
⟨*proof*⟩

lemma *poly-of-int-poly-0* [*simp*]: *poly* (*of-int-poly p*) *0* = *of-int* (*poly p 0*)
⟨*proof*⟩

lemma *poly-of-int-poly-1* [*simp*]: *poly* (*of-int-poly p*) *1* = *of-int* (*poly p 1*)
⟨*proof*⟩

lemma *poly-of-int-poly-of-real* [*simp*]:
poly (*of-int-poly p*) (*of-real x*) = *of-real* (*poly* (*of-int-poly p*) *x*)
⟨*proof*⟩

lemma *of-int-poly-eq-iff* [*simp*]:
of-int-poly p = (*of-int-poly q* :: *'a* :: {*comm-ring-1*, *ring-char-0*} *poly*) $\longleftrightarrow$ *p* = *q*
⟨*proof*⟩

lemma *of-int-poly-eq-0-iff* [*simp*]:
of-int-poly p = (*0* :: *'a* :: {*comm-ring-1*, *ring-char-0*} *poly*) $\longleftrightarrow$ *p* = *0*
⟨*proof*⟩

lemma *degree-of-int-poly* [*simp*]:
degree (*of-int-poly p* :: *'a* :: {*comm-ring-1*, *ring-char-0*} *poly*) = *degree p*
⟨*proof*⟩

lemma *pderiv-of-int-poly* [*simp*]: *pderiv* (*of-int-poly p*) = *of-int-poly* (*pderiv p*)
⟨*proof*⟩

lemma *higher-pderiv-of-int-poly* [*simp*]:
(*pderiv* ^^ *n*) (*of-int-poly p*) = *of-int-poly* ((*pderiv* ^^ *n*) *p*)

$\langle proof \rangle$

lemma *int-polyE*:
assumes $\bigwedge n.\ coeff\ (p :: 'a :: \{comm\text{-}ring\text{-}1,\ ring\text{-}char\text{-}0\}\ poly)\ n \in \mathbb{Z}$
obtains p' **where** $p = of\text{-}int\text{-}poly\ p'$
$\langle proof \rangle$

1.3 General facts about polynomials

lemma *pderiv-power*:
$pderiv\ (p\ \hat{}\ n) = smult\ (of\text{-}nat\ n)\ (p\ \hat{}\ (n - 1) * pderiv\ p)$
$\langle proof \rangle$

lemma *degree-prod-sum-eq*:
$(\bigwedge x.\ x \in A \Longrightarrow f\ x \neq 0) \Longrightarrow$
$degree\ (prod\ f\ A :: 'a :: idom\ poly) = (\sum x{\in}A.\ degree\ (f\ x))$
$\langle proof \rangle$

lemma *pderiv-monom*:
$pderiv\ (monom\ c\ n) = monom\ (of\text{-}nat\ n * c)\ (n - 1)$
$\langle proof \rangle$

lemma *power-poly-const* [*simp*]: $[:c:]\ \hat{}\ n = [:c\ \hat{}\ n:]$
$\langle proof \rangle$

lemma *monom-power*: $monom\ c\ n\ \hat{}\ k = monom\ (c\ \hat{}\ k)\ (n * k)$
$\langle proof \rangle$

lemma *coeff-higher-pderiv*:
$coeff\ ((pderiv\ \hat{}\hat{}\ m)\ f)\ n = pochhammer\ (of\text{-}nat\ (Suc\ n))\ m * coeff\ f\ (n + m)$
$\langle proof \rangle$

lemma *higher-pderiv-add*: $(pderiv\ \hat{}\hat{}\ n)\ (p + q) = (pderiv\ \hat{}\hat{}\ n)\ p + (pderiv\ \hat{}\hat{}\ n)\ q$
$\langle proof \rangle$

lemma *higher-pderiv-smult*: $(pderiv\ \hat{}\hat{}\ n)\ (smult\ c\ p) = smult\ c\ ((pderiv\ \hat{}\hat{}\ n)\ p)$
$\langle proof \rangle$

lemma *higher-pderiv-0* [*simp*]: $(pderiv\ \hat{}\hat{}\ n)\ 0 = 0$
$\langle proof \rangle$

lemma *higher-pderiv-monom*:
$m \leq n + 1 \Longrightarrow (pderiv\ \hat{}\hat{}\ m)\ (monom\ c\ n) = monom\ (pochhammer\ (int\ n - int\ m + 1)\ m * c)\ (n - m)$
$\langle proof \rangle$

lemma *higher-pderiv-monom-eq-zero*:
$m > n + 1 \Longrightarrow (pderiv\ \hat{}\hat{}\ m)\ (monom\ c\ n) = 0$

⟨*proof*⟩

lemma *higher-pderiv-sum*: $(pderiv \ \widehat{}\widehat{} \ n) \ (sum \ f \ A) = (\sum x{\in}A. \ (pderiv \ \widehat{}\widehat{} \ n) \ (f \ x))$
⟨*proof*⟩

lemma *fact-dvd-higher-pderiv*:
$[:fact \ n :: int:] \ dvd \ (pderiv \ \widehat{}\widehat{} \ n) \ p$
⟨*proof*⟩

lemma *fact-dvd-poly-higher-pderiv-aux*:
$(fact \ n :: int) \ dvd \ poly \ ((pderiv \ \widehat{}\widehat{} \ n) \ p) \ x$
⟨*proof*⟩

lemma *fact-dvd-poly-higher-pderiv-aux'*:
$m \le n \Longrightarrow (fact \ m :: int) \ dvd \ poly \ ((pderiv \ \widehat{}\widehat{} \ n) \ p) \ x$
⟨*proof*⟩

lemma *algebraicE'*:
assumes $algebraic \ (x :: 'a :: field\text{-}char\text{-}0)$
obtains p **where** $p \ne 0$ $poly \ (of\text{-}int\text{-}poly \ p) \ x = 0$
⟨*proof*⟩

lemma *algebraicE'-nonzero*:
assumes $algebraic \ (x :: 'a :: field\text{-}char\text{-}0)$ $x \ne 0$
obtains p **where** $p \ne 0$ $coeff \ p \ 0 \ne 0$ $poly \ (of\text{-}int\text{-}poly \ p) \ x = 0$
⟨*proof*⟩

lemma *algebraic-of-real-iff* [*simp*]:
$algebraic \ (of\text{-}real \ x :: 'a :: \{real\text{-}algebra\text{-}1, field\text{-}char\text{-}0\}) \longleftrightarrow algebraic \ x$
⟨*proof*⟩

1.4 Main proof

lemma *lindemann-weierstrass-integral*:
fixes $u :: complex$ **and** $f :: complex \ poly$
defines $df \equiv \lambda n. \ (pderiv \ \widehat{}\widehat{} \ n) \ f$
defines $m \equiv degree \ f$
defines $I \equiv \lambda f \ u. \ exp \ u * (\sum j{\le}degree \ f. \ poly \ ((pderiv \ \widehat{}\widehat{} \ j) \ f) \ 0) -$
$(\sum j{\le}degree \ f. \ poly \ ((pderiv \ \widehat{}\widehat{} \ j) \ f) \ u)$
shows $((\lambda t. \ exp \ (u - t) * poly \ f \ t) \ has\text{-}contour\text{-}integral \ I \ f \ u) \ (linepath \ 0 \ u)$
⟨*proof*⟩

locale *lindemann-weierstrass-aux* =
fixes $f :: complex \ poly$
begin

definition $I :: complex \Rightarrow complex$ **where**
$I \ u = exp \ u * (\sum j{\le}degree \ f. \ poly \ ((pderiv \ \widehat{}\widehat{} \ j) \ f) \ 0) -$

$(\sum j{\leq}\mathit{degree}\ f.\ \mathit{poly}\ ((\mathit{pderiv}\ \widehat{\ \ }\ j)\ f)\ u)$

lemma *lindemann-weierstrass-integral-bound*:
fixes u :: *complex*
assumes $C \geq 0$ $\bigwedge t.\ t \in \mathit{closed\text{-}segment}\ 0\ u \Longrightarrow \mathit{norm}\ (\mathit{poly}\ f\ t) \leq C$
shows $\mathit{norm}\ (I\ u) \leq \mathit{norm}\ u * \mathit{exp}\ (\mathit{norm}\ u) * C$
⟨*proof*⟩

end

lemma *poly-higher-pderiv-aux1*:
fixes c :: $'a$ :: *idom*
assumes $k < n$
shows $\mathit{poly}\ ((\mathit{pderiv}\ \widehat{\ \ }\ k)\ ([:-c,\ 1:]\ \widehat{}\ n * p))\ c = 0$
⟨*proof*⟩

lemma *poly-higher-pderiv-aux1'*:
fixes c :: $'a$ :: *idom*
assumes $k < n$ $[:-c,\ 1:]\ \widehat{}\ n\ \mathit{dvd}\ p$
shows $\mathit{poly}\ ((\mathit{pderiv}\ \widehat{\ \ }\ k)\ p)\ c = 0$
⟨*proof*⟩

lemma *poly-higher-pderiv-aux2*:
fixes c :: $'a$ :: $\{\mathit{idom},\ \mathit{semiring\text{-}char\text{-}0}\}$
shows $\mathit{poly}\ ((\mathit{pderiv}\ \widehat{\ \ }\ n)\ ([:-c,\ 1:]\ \widehat{}\ n * p))\ c = \mathit{fact}\ n * \mathit{poly}\ p\ c$
⟨*proof*⟩

lemma *poly-higher-pderiv-aux3*:
fixes c :: $'a$ :: $\{\mathit{idom},\mathit{semiring\text{-}char\text{-}0}\}$
assumes $k \geq n$
shows $\exists\, q.\ \mathit{poly}\ ((\mathit{pderiv}\ \widehat{\ \ }\ k)\ ([:-c,\ 1:]\ \widehat{}\ n * p))\ c = \mathit{fact}\ n * \mathit{poly}\ q\ c$
⟨*proof*⟩

lemma *poly-higher-pderiv-aux3'*:
fixes c :: $'a$ :: $\{\mathit{idom},\ \mathit{semiring\text{-}char\text{-}0}\}$
assumes $k \geq n$ $[:-c,\ 1:]\ \widehat{}\ n\ \mathit{dvd}\ p$
shows $\mathit{fact}\ n\ \mathit{dvd}\ \mathit{poly}\ ((\mathit{pderiv}\ \widehat{\ \ }\ k)\ p)\ c$
⟨*proof*⟩

lemma *e-transcendental-aux-bound*:
obtains C **where** $C \geq 0$
$\bigwedge x.\ x \in \mathit{closed\text{-}segment}\ 0\ (\mathit{of\text{-}nat}\ n) \Longrightarrow$
$\mathit{norm}\ (\prod k{\in}\{1..n\}.\ (x - \mathit{of\text{-}nat}\ k :: \mathit{complex})) \leq C$
⟨*proof*⟩

theorem *e-transcendental-complex*: $\neg\ \mathit{algebraic}\ (\mathit{exp}\ 1 :: \mathit{complex})$
⟨*proof*⟩

corollary *e-transcendental-real*: $\neg$ *algebraic* (*exp 1* :: *real*)
$\langle proof \rangle$

end

References

[1] R. Lipsett. Planetmath. http://planetmath.org/proofoflindemannweierstrasstheoremandthateandpiaretranscendental, 2007.