

The Hermite–Lindemann–Weierstraß Transcendence Theorem

Manuel Eberl

March 12, 2021

Abstract

This article provides a formalisation of the Hermite–Lindemann–Weierstraß Theorem (also known as simply Hermite–Lindemann or Lindemann–Weierstraß). This theorem is one of the crowning achievements of 19th century number theory.

The theorem states that if $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ are algebraic numbers that are linearly independent over \mathbb{Z} , then $e^{\alpha_1}, \dots, e^{\alpha_n}$ are algebraically independent over \mathbb{Q} .

Like the previous formalisation in Coq by Bernard [2], I proceeded by formalising Baker’s alternative formulation of the theorem [1] and then deriving the original one from that. Baker’s version states that for any algebraic numbers $\beta_1, \dots, \beta_n \in \mathbb{C}$ and distinct algebraic numbers $\alpha_1, \dots, \alpha_n \in \mathbb{C}$, we have:

$$\beta_1 e^{\alpha_1} + \dots + \beta_n e^{\alpha_n} = 0 \quad \text{iff} \quad \forall i. \beta_i = 0$$

This has a number of immediate corollaries, e.g.:

- e and π are transcendental
- e^z , $\sin z$, $\tan z$, etc. are transcendental for algebraic $z \in \mathbb{C} \setminus \{0\}$
- $\ln z$ is transcendental for algebraic $z \in \mathbb{C} \setminus \{0, 1\}$

Contents

1	Divisibility of algebraic integers	3
2	Auxiliary facts about univariate polynomials	6
3	The minimal polynomial of an algebraic number	10
4	The lexicographic ordering on complex numbers	12
5	Additional facts about multivariate polynomials	13
5.1	Miscellaneous	13
5.2	Converting a univariate polynomial into a multivariate one	14
6	More facts about algebraic numbers	15
6.1	Miscellaneous	15
6.2	Turning an algebraic number into an algebraic integer	18
6.3	Multiplying an algebraic number with a suitable integer turns it into an algebraic integer.	18
7	Miscellaneous facts	18
8	The Hermite–Lindemann–Weierstraß Transcendence Theorem	20
8.1	Main proof	21
8.2	Removing the restriction of full sets of conjugates	22
8.3	Removing the restriction to integer coefficients	22
8.4	The final theorem	23
8.5	The traditional formulation of the theorem	23
8.6	Simple corollaries	24
8.7	Transcendence of the trigonometric and hyperbolic functions	25

1 Divisibility of algebraic integers

```
theory Algebraic-Integer-Divisibility
imports Algebraic-Numbers.Algebraic-Numbers
begin
```

In this section, we define a notion of divisibility of algebraic integers: y is divisible by x if y / x is an algebraic integer (or if x and y are both zero).

Technically, the definition does not require x and y to be algebraic integers themselves, but we will always use it that way (in fact, in our case x will always be a rational integer).

```
definition alg-dvd :: 'a :: field  $\Rightarrow$  'a  $\Rightarrow$  bool (infix alg'-dvd 50) where
  x alg-dvd y  $\longleftrightarrow$  (x = 0  $\longrightarrow$  y = 0)  $\wedge$  algebraic-int (y / x)
```

```
lemma alg-dvd-imp-algebraic-int:
fixes x y :: 'a :: field-char-0
shows x alg-dvd y  $\Longrightarrow$  algebraic-int x  $\Longrightarrow$  algebraic-int y
 $\langle$ proof $\rangle$ 
```

```
lemma alg-dvd-0-left-iff [simp]: 0 alg-dvd x  $\longleftrightarrow$  x = 0
 $\langle$ proof $\rangle$ 
```

```
lemma alg-dvd-0-right [iff]: x alg-dvd 0
 $\langle$ proof $\rangle$ 
```

```
lemma one-alg-dvd-iff [simp]: 1 alg-dvd x  $\longleftrightarrow$  algebraic-int x
 $\langle$ proof $\rangle$ 
```

```
lemma alg-dvd-of-int [intro]:
assumes x dvd y
shows of-int x alg-dvd of-int y
 $\langle$ proof $\rangle$ 
```

```
lemma alg-dvd-of-nat [intro]:
assumes x dvd y
shows of-nat x alg-dvd of-nat y
 $\langle$ proof $\rangle$ 
```

```
lemma alg-dvd-of-int-iff [simp]:
  (of-int x :: 'a :: field-char-0) alg-dvd of-int y  $\longleftrightarrow$  x dvd y
 $\langle$ proof $\rangle$ 
```

```
lemma alg-dvd-of-nat-iff [simp]:
  (of-nat x :: 'a :: field-char-0) alg-dvd of-nat y  $\longleftrightarrow$  x dvd y
 $\langle$ proof $\rangle$ 
```

```
lemma alg-dvd-add [intro]:
fixes x y z :: 'a :: field-char-0
shows x alg-dvd y  $\Longrightarrow$  x alg-dvd z  $\Longrightarrow$  x alg-dvd (y + z)
```

<proof>

lemma *alg-dvd-uminus-right* [*intro*]: $x \text{ alg-dvd } y \implies x \text{ alg-dvd } -y$
<proof>

lemma *alg-dvd-uminus-right-iff* [*simp*]: $x \text{ alg-dvd } -y \iff x \text{ alg-dvd } y$
<proof>

lemma *alg-dvd-diff* [*intro*]:
fixes $x \ y \ z :: 'a :: \text{field-char-0}$
shows $x \text{ alg-dvd } y \implies x \text{ alg-dvd } z \implies x \text{ alg-dvd } (y - z)$
<proof>

lemma *alg-dvd-triv-left* [*intro*]: $\text{algebraic-int } y \implies x \text{ alg-dvd } x * y$
<proof>

lemma *alg-dvd-triv-right* [*intro*]: $\text{algebraic-int } x \implies y \text{ alg-dvd } x * y$
<proof>

lemma *alg-dvd-triv-left-iff*: $x \text{ alg-dvd } x * y \iff x = 0 \vee \text{algebraic-int } y$
<proof>

lemma *alg-dvd-triv-right-iff*: $y \text{ alg-dvd } x * y \iff y = 0 \vee \text{algebraic-int } x$
<proof>

lemma *alg-dvd-triv-left-iff'* [*simp*]: $x \neq 0 \implies x \text{ alg-dvd } x * y \iff \text{algebraic-int } y$
<proof>

lemma *alg-dvd-triv-right-iff'* [*simp*]: $y \neq 0 \implies y \text{ alg-dvd } x * y \iff \text{algebraic-int } x$
<proof>

lemma *alg-dvd-trans* [*trans*]:
fixes $x \ y \ z :: 'a :: \text{field-char-0}$
shows $x \text{ alg-dvd } y \implies y \text{ alg-dvd } z \implies x \text{ alg-dvd } z$
<proof>

lemma *alg-dvd-mono* [*simp*]:
fixes $a \ b \ c \ d :: 'a :: \text{field-char-0}$
shows $a \text{ alg-dvd } c \implies b \text{ alg-dvd } d \implies (a * b) \text{ alg-dvd } (c * d)$
<proof>

lemma *alg-dvd-mult* [*simp*]:
fixes $a \ b \ c :: 'a :: \text{field-char-0}$
shows $a \text{ alg-dvd } c \implies \text{algebraic-int } b \implies a \text{ alg-dvd } (b * c)$
<proof>

lemma *alg-dvd-mult2* [*simp*]:
fixes $a \ b \ c :: 'a :: \text{field-char-0}$
shows $a \text{ alg-dvd } b \implies \text{algebraic-int } c \implies a \text{ alg-dvd } (b * c)$

<proof>

A crucial theorem: if an integer x divides a rational number y , then y is in fact also an integer, and that integer is a multiple of x .

lemma *alg-dvd-int-rat*:

fixes $y :: 'a :: \text{field-char-0}$

assumes $\text{of-int } x \text{ alg-dvd } y$ **and** $y \in \mathbb{Q}$

shows $\exists n. y = \text{of-int } n \wedge x \text{ dvd } n$

<proof>

lemma *prod-alg-dvd-prod*:

fixes $f :: 'a \Rightarrow 'b :: \text{field-char-0}$

assumes $\bigwedge x. x \in A \Longrightarrow f x \text{ alg-dvd } g x$

shows $\text{prod } f A \text{ alg-dvd } \text{prod } g A$

<proof>

lemma *alg-dvd-sum*:

fixes $f :: 'a \Rightarrow 'b :: \text{field-char-0}$

assumes $\bigwedge x. x \in A \Longrightarrow y \text{ alg-dvd } f x$

shows $y \text{ alg-dvd } \text{sum } f A$

<proof>

lemma *not-alg-dvd-sum*:

fixes $f :: 'a \Rightarrow 'b :: \text{field-char-0}$

assumes $\bigwedge x. x \in A - \{x'\} \Longrightarrow y \text{ alg-dvd } f x$

assumes $\neg y \text{ alg-dvd } f x'$

assumes $x' \in A \text{ finite } A$

shows $\neg y \text{ alg-dvd } \text{sum } f A$

<proof>

lemma *fact-dvd-pochhammer*:

assumes $m \leq n + 1$

shows $\text{fact } m \text{ dvd } \text{pochhammer } (\text{int } n - \text{int } m + 1) m$

<proof>

lemma *coeff-higher-pderiv*:

$\text{coeff } ((\text{pderiv } \widetilde{m}) f) n = \text{pochhammer } (\text{of-nat } (\text{Suc } n)) m * \text{coeff } f (n + m)$

<proof>

lemma *fact-alg-dvd-poly-higher-pderiv*:

fixes $p :: 'a :: \text{field-char-0} \text{ poly}$

assumes $\bigwedge i. \text{algebraic-int } (\text{poly.coeff } p i) \text{ algebraic-int } x \text{ } m \leq k$

shows $\text{fact } m \text{ alg-dvd } \text{poly } ((\text{pderiv } \widetilde{k}) p) x$

<proof>

end

2 Auxiliary facts about univariate polynomials

theory *More-Polynomial-HLW*

imports

HOL-Computational-Algebra.Computational-Algebra
Polynomial-Factorization.Gauss-Lemma
Power-Sum-Polynomials.Power-Sum-Polynomials-Library
Algebraic-Numbers.Algebraic-Numbers

begin

instance *poly* :: (*{ idom-divide, normalization-semidom-multiplicative, factorial-ring-gcd, semiring-gcd-mult-normalize }*) *factorial-semiring-multiplicative*
 ⟨*proof*⟩

lemma *lead-coeff-prod-mset*:

fixes *A* :: 'a :: *{ comm-semiring-1, semiring-no-zero-divisors }* *poly multiset*
shows *Polynomial.lead-coeff (prod-mset A) = prod-mset (image-mset Polynomial.lead-coeff A)*
 ⟨*proof*⟩

lemma *content-normalize [simp]*:

fixes *p* :: 'a :: *{ factorial-semiring, idom-divide, semiring-gcd, normalization-semidom-multiplicative }*
poly
shows *content (normalize p) = content p*
 ⟨*proof*⟩

lemma *rat-to-normalized-int-poly-exists*:

fixes *p* :: *rat poly*
assumes *p ≠ 0*
obtains *q lc* **where** *p = Polynomial.smult lc (of-int-poly q) lc > 0 content q = 1*
 ⟨*proof*⟩

lemma *irreducible-imp-squarefree*:

assumes *irreducible p*
shows *squarefree p*
 ⟨*proof*⟩

lemma *squarefree-imp-rsquarefree*:

fixes *p* :: 'a :: *idom poly*
assumes *squarefree p*
shows *rsquarefree p*
 ⟨*proof*⟩

lemma *squarefree-imp-coprime-pderiv*:

fixes *p* :: 'a :: *{ factorial-ring-gcd, semiring-gcd-mult-normalize, semiring-char-0 }*
poly
assumes *squarefree p and content p = 1*
shows *Rings.coprime p (pderiv p)*
 ⟨*proof*⟩

lemma *irreducible-imp-coprime-pderiv*:

fixes $p :: 'a :: \{\text{idom-divide, semiring-char-0}\}$ *poly*

assumes *irreducible p Polynomial.degree p $\neq 0$*

shows *Rings.coprime p (pderiv p)*

<proof>

lemma *poly-gcd-eq-0I*:

assumes *poly p x = 0 poly q x = 0*

shows *poly (gcd p q) x = 0*

<proof>

lemma *poly-eq-0-coprime*:

assumes *Rings.coprime p q p $\neq 0$ q $\neq 0$*

shows *poly p x $\neq 0 \vee$ poly q x $\neq 0$*

<proof>

lemma *coprime-of-int-polyI*:

assumes *Rings.coprime p q*

shows *Rings.coprime (of-int-poly p) (of-int-poly q :: 'a :: \{field-char-0, field-gcd\}*
poly)

<proof>

lemma *irreducible-imp-rsquarefree-of-int-poly*:

fixes $p :: \text{int poly}$

assumes *irreducible p and Polynomial.degree p > 0*

shows *rsquarefree (of-int-poly p :: 'a :: \{field-gcd, field-char-0\}*
poly)

<proof>

lemma *squarefree-of-int-polyI*:

assumes *squarefree p content p = 1*

shows *squarefree (of-int-poly p :: 'a :: \{field-char-0, field-gcd\}*
poly)

<proof>

lemma *higher-pderiv-pcompose-linear*:

$(\text{pderiv } \overset{\sim}{\sim} n) (\text{pcompose } p \text{ } [:0, c:]) =$

$\text{Polynomial.smult } (c \overset{\sim}{\sim} n) (\text{pcompose } ((\text{pderiv } \overset{\sim}{\sim} n) p) \text{ } [:0, c:])$

<proof>

lemma *poly-poly-eq*:

poly (poly p [:x:]) y = poly (eval-poly ($\lambda p. [:poly p y:]$) p [:0, 1:]) x

<proof>

lemma *poly-poly-poly-y-x [simp]*:

fixes $p :: 'a :: \text{idom poly poly}$

shows *poly (poly (poly-y-x p) [:y:]) x = poly (poly p [:x:]) y*

<proof>

lemma (**in** *idom-hom*) *map-poly-higher-pderiv [hom-distrib]*:

$map\text{-}poly\ hom ((pderiv \hat{\sim} n) p) = (pderiv \hat{\sim} n) (map\text{-}poly\ hom\ p)$
 $\langle proof \rangle$

lemma *coeff-prod-linear-factors*:

fixes $f :: 'a \Rightarrow 'b :: comm\text{-}ring\text{-}1$

assumes $[intro]: finite\ A$

shows $Polynomial.coeff (\prod_{x \in A}. [-f\ x, 1] \hat{\sim} e\ x)\ i =$
 $(\sum X \mid X \in Pow (SIGMA\ x:A. \{..<e\ x\}) \wedge i = sum\ e\ A - card\ X.$
 $(-1) \hat{\sim} card\ X * (\prod_{x \in X}. f\ (fst\ x)))$

$\langle proof \rangle$

lemma $(in\ comm\text{-}ring\text{-}hom)$ *synthetic-div-hom*:

$synthetic\text{-}div\ (map\text{-}poly\ hom\ p)\ (hom\ x) = map\text{-}poly\ hom\ (synthetic\text{-}div\ p\ x)$

$\langle proof \rangle$

lemma *synthetic-div-altdef*:

fixes $p :: 'a :: field\ poly$

shows $synthetic\text{-}div\ p\ c = p\ div\ [-c, 1]$

$\langle proof \rangle$

lemma $(in\ ring\text{-}closed)$ *poly-closed* $[intro]$:

assumes $\bigwedge i. poly.coeff\ p\ i \in A\ x \in A$

shows $poly\ p\ x \in A$

$\langle proof \rangle$

lemma $(in\ ring\text{-}closed)$ *coeff-pCons-closed* $[intro]$:

assumes $\bigwedge i. poly.coeff\ p\ i \in A\ x \in A$

shows $poly.coeff\ (pCons\ x\ p)\ i \in A$

$\langle proof \rangle$

lemma $(in\ ring\text{-}closed)$ *coeff-poly-mult-closed* $[intro]$:

assumes $\bigwedge i. poly.coeff\ p\ i \in A\ \bigwedge i. poly.coeff\ q\ i \in A$

shows $poly.coeff\ (p * q)\ i \in A$

$\langle proof \rangle$

lemma $(in\ ring\text{-}closed)$ *coeff-poly-prod-closed* $[intro]$:

assumes $\bigwedge x\ i. x \in X \implies poly.coeff\ (f\ x)\ i \in A$

shows $poly.coeff\ (prod\ f\ X)\ i \in A$

$\langle proof \rangle$

lemma $(in\ ring\text{-}closed)$ *coeff-poly-power-closed* $[intro]$:

assumes $\bigwedge i. poly.coeff\ p\ i \in A$

shows $poly.coeff\ (p \hat{\sim} n)\ i \in A$

$\langle proof \rangle$

lemma $(in\ ring\text{-}closed)$ *synthetic-div-closed*:

assumes $\bigwedge i. poly.coeff\ p\ i \in A\ x \in A$

shows $poly.coeff\ (synthetic\text{-}div\ p\ x)\ i \in A$

$\langle proof \rangle$

lemma *pcompose-monom*: $pcompose (Polynomial.monom\ c\ n)\ p = Polynomial.smult\ c\ (p \wedge n)$
 ⟨proof⟩

lemma *poly-roots-uminus* [simp]: $poly-roots\ (-p) = poly-roots\ p$
 ⟨proof⟩

lemma *poly-roots-normalize* [simp]:
 fixes $p :: 'a :: \{normalization-semidom, idom-divide\}$ poly
 shows $poly-roots\ (normalize\ p) = poly-roots\ p$
 ⟨proof⟩

lemma *poly-roots-of-int-normalize* [simp]:
 $poly-roots\ (of-int-poly\ (normalize\ p)) :: 'a :: \{idom, ring-char-0\}$ poly =
 $poly-roots\ (of-int-poly\ p)$
 ⟨proof⟩

lemma *poly-roots-power* [simp]: $poly-roots\ (p \wedge n) = repeat-mset\ n\ (poly-roots\ p)$
 ⟨proof⟩

lemma *poly-roots-conv-sum-prime-factors*:
 $poly-roots\ q = (\sum\ p \in \#prime-factorization\ q.\ poly-roots\ p)$
 ⟨proof⟩

lemma *poly-roots-of-int-conv-sum-prime-factors*:
 $poly-roots\ (of-int-poly\ q :: 'a :: \{idom, ring-char-0\}$ poly) =
 $(\sum\ p \in \#prime-factorization\ q.\ poly-roots\ (of-int-poly\ p))$
 ⟨proof⟩

lemma *dvd-imp-poly-roots-subset*:
 assumes $q \neq 0\ p\ dvd\ q$
 shows $poly-roots\ p \subseteq \# poly-roots\ q$
 ⟨proof⟩

lemma *abs-prod-mset*: $|prod-mset\ (A :: 'a :: idom-abs-sgn\ multiset)| = prod-mset\ (image-mset\ abs\ A)$
 ⟨proof⟩

lemma *content-1-imp-nonconstant-prime-factors*:
 assumes $content\ (p :: int\ poly) = 1$ and $q \in prime-factors\ p$
 shows $Polynomial.degree\ q > 0$
 ⟨proof⟩

end

3 The minimal polynomial of an algebraic number

theory *Min-Int-Poly*

imports

Algebraic-Numbers.Algebraic-Numbers

HOL-Computational-Algebra.Computational-Algebra

More-Polynomial-HLW

begin

Given an algebraic number x in a field, the minimal polynomial is the unique irreducible integer polynomial with positive leading coefficient that has x as a root.

Note that we assume characteristic 0 since the material upon which all of this builds also assumes it.

definition *min-int-poly* :: 'a :: field-char-0 \Rightarrow int poly **where**

min-int-poly $x =$

(if algebraic x then THE p . p represents $x \wedge$ irreducible $p \wedge$ Polynomial.lead-coeff $p > 0$

else [:0, 1:])

lemma

fixes $x :: 'a :: \{field-char-0, field-gcd\}$

shows *min-int-poly-represents* [intro]: algebraic $x \implies$ *min-int-poly* x represents x

and *min-int-poly-irreducible* [intro]: irreducible (*min-int-poly* x)

and *lead-coeff-min-int-poly-pos*: Polynomial.lead-coeff (*min-int-poly* x) > 0

\langle proof \rangle

lemma

fixes $x :: 'a :: \{field-char-0, field-gcd\}$

shows *degree-min-int-poly-pos* [intro]: Polynomial.degree (*min-int-poly* x) > 0

and *degree-min-int-poly-nonzero* [simp]: Polynomial.degree (*min-int-poly* x) $\neq 0$

\langle proof \rangle

lemma *min-int-poly-squarefree* [intro]:

fixes $x :: 'a :: \{field-char-0, field-gcd\}$

shows *squarefree* (*min-int-poly* x)

\langle proof \rangle

lemma *min-int-poly-primitive* [intro]:

fixes $x :: 'a :: \{field-char-0, field-gcd\}$

shows *primitive* (*min-int-poly* x)

\langle proof \rangle

lemma *min-int-poly-content* [simp]:

fixes $x :: 'a :: \{field-char-0, field-gcd\}$

shows *content* (*min-int-poly* x) = 1

\langle proof \rangle

lemma *ipoly-min-int-poly* [*simp*]:
 $\text{algebraic } x \implies \text{ipoly } (\text{min-int-poly } x) (x :: 'a :: \{\text{field-gcd}, \text{field-char-0}\}) = 0$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-nonzero* [*simp*]:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
shows $\text{min-int-poly } x \neq 0$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-normalize* [*simp*]:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
shows $\text{normalize } (\text{min-int-poly } x) = \text{min-int-poly } x$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-prime-elem* [*intro*]:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
shows $\text{prime-elem } (\text{min-int-poly } x)$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-prime* [*intro*]:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
shows $\text{prime } (\text{min-int-poly } x)$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-unique*:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
assumes p represents x irreducible p $\text{Polynomial.lead-coeff } p > 0$
shows $\text{min-int-poly } x = p$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-of-int* [*simp*]:
 $\text{min-int-poly } (\text{of-int } n :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}) = [:-\text{of-int } n, 1:]$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-of-nat* [*simp*]:
 $\text{min-int-poly } (\text{of-nat } n :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}) = [:-\text{of-nat } n, 1:]$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-0* [*simp*]: $\text{min-int-poly } (0 :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}) = [:-0, 1:]$
 $\langle \text{proof} \rangle$

lemma *min-int-poly-1* [*simp*]: $\text{min-int-poly } (1 :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}) = [:-1, 1:]$
 $\langle \text{proof} \rangle$

lemma *poly-min-int-poly-0-eq-0-iff* [*simp*]:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
assumes $\text{algebraic } x$

shows $\text{poly } (\text{min-int-poly } x) \ 0 = 0 \longleftrightarrow x = 0$
 ⟨proof⟩

lemma *min-int-poly-conv-Gcd*:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
assumes *algebraic* x
shows $\text{min-int-poly } x = \text{Gcd } \{p. p \neq 0 \wedge p \text{ represents } x\}$
 ⟨proof⟩

lemma *min-int-poly-eqI*:
fixes $x :: 'a :: \{\text{field-char-0}, \text{field-gcd}\}$
assumes p *represents* x *irreducible* p $\text{Polynomial.lead-coeff } p \geq 0$
shows $\text{min-int-poly } x = p$
 ⟨proof⟩

end

4 The lexicographic ordering on complex numbers

theory *Complex-Lexorder*
imports *Complex-Main HOL-Library.Multiset*
begin

We define a lexicographic order on the complex numbers, comparing first the real parts and, if they are equal, the imaginary parts. This ordering is of course not compatible with multiplication, but it is compatible with addition.

definition *less-eq-complex-lex* (**infix** $\leq_{\mathbb{C}}$ 50) **where**
 $\text{less-eq-complex-lex } x \ y \longleftrightarrow \text{Re } x < \text{Re } y \vee \text{Re } x = \text{Re } y \wedge \text{Im } x \leq \text{Im } y$

definition *less-complex-lex* (**infix** $<_{\mathbb{C}}$ 50) **where**
 $\text{less-complex-lex } x \ y \longleftrightarrow \text{Re } x < \text{Re } y \vee \text{Re } x = \text{Re } y \wedge \text{Im } x < \text{Im } y$

interpretation *complex-lex*:
 $\text{linordered-ab-group-add } (+) \ 0 \ (-) \ \text{uminus } \text{less-eq-complex-lex } \text{less-complex-lex}$
 ⟨proof⟩

lemmas [*trans*] =
 $\text{complex-lex.order.trans } \text{complex-lex.less-le-trans}$
 $\text{complex-lex.less-trans } \text{complex-lex.le-less-trans}$

lemma (**in** *ordered-comm-monoid-add*) *sum-mono-complex-lex*:
 $(\bigwedge i. i \in K \implies f \ i \leq_{\mathbb{C}} \ g \ i) \implies (\sum i \in K. f \ i) \leq_{\mathbb{C}} (\sum i \in K. g \ i)$
 ⟨proof⟩

lemma *sum-strict-mono-ex1-complex-lex*:
fixes $f \ g :: 'i \Rightarrow \text{complex}$
assumes *finite* A

and $\forall x \in A. f x \leq_{\mathbb{C}} g x$
and $\exists a \in A. f a <_{\mathbb{C}} g a$
shows $\text{sum } f A <_{\mathbb{C}} \text{sum } g A$
 $\langle \text{proof} \rangle$

lemma *sum-list-mono-complex-lex*:
assumes *list-all2* $(\leq_{\mathbb{C}}) xs ys$
shows $\text{sum-list } xs \leq_{\mathbb{C}} \text{sum-list } ys$
 $\langle \text{proof} \rangle$

lemma *sum-mset-mono-complex-lex*:
assumes *rel-mset* $(\leq_{\mathbb{C}}) A B$
shows $\text{sum-mset } A \leq_{\mathbb{C}} \text{sum-mset } B$
 $\langle \text{proof} \rangle$

lemma *rel-msetI*:
assumes *list-all2* $R xs ys$ $\text{mset } xs = A$ $\text{mset } ys = B$
shows *rel-mset* $R A B$
 $\langle \text{proof} \rangle$

lemma *mset-replicate [simp]*: $\text{mset } (\text{replicate } n x) = \text{replicate-mset } n x$
 $\langle \text{proof} \rangle$

lemma *rel-mset-replicate-mset-right*:
assumes $\bigwedge x. x \in \# A \implies R x y$ $\text{size } A = n$
shows *rel-mset* $R A (\text{replicate-mset } n y)$
 $\langle \text{proof} \rangle$

end

5 Additional facts about multivariate polynomials

theory *More-Multivariate-Polynomial-HLW*
imports *Power-Sum-Polynomials.Power-Sum-Polynomials-Library*
begin

5.1 Miscellaneous

lemma *Var-altdef*: $\text{Var } i = \text{monom } (\text{Poly-Mapping.single } i 1) 1$
 $\langle \text{proof} \rangle$

lemma *Const-conv-monom*: $\text{Const } c = \text{monom } 0 c$
 $\langle \text{proof} \rangle$

lemma *smult-conv-mult-Const*: $\text{smult } c p = \text{Const } c * p$
 $\langle \text{proof} \rangle$

lemma *mpoly-map-vars-Var [simp]*: $\text{bij } f \implies \text{mpoly-map-vars } f (\text{Var } i) = \text{Var } (f i)$

<proof>

lemma *symmetric-mpoly-symmetric-prod'*:

assumes $\bigwedge \pi. \pi \text{ permutes } A \implies g \pi \text{ permutes } X$

assumes $\bigwedge x \pi. x \in X \implies \pi \text{ permutes } A \implies \text{mpoly-map-vars } \pi (f x) = f (g \pi x)$

shows *symmetric-mpoly* $A (\prod_{x \in X}. f x)$

<proof>

5.2 Converting a univariate polynomial into a multivariate one

lift-definition *mpoly-of-poly-aux* :: $\text{nat} \Rightarrow 'a :: \text{zero poly} \Rightarrow (\text{nat} \Rightarrow_0 \text{nat}) \Rightarrow_0 'a$ is

$\lambda i c m. \text{if } \text{Poly-Mapping.keys } m \subseteq \{i\} \text{ then } c (\text{Poly-Mapping.lookup } m i) \text{ else } 0$
<proof>

lift-definition *mpoly-of-poly* :: $\text{nat} \Rightarrow 'a :: \text{zero poly} \Rightarrow 'a \text{ mpoly}$ is
mpoly-of-poly-aux *<proof>*

lemma *mpoly-of-poly-0* [simp]: *mpoly-of-poly* $i 0 = 0$
<proof>

lemma *coeff-mpoly-of-poly1* [simp]:
 $\text{coeff } (\text{mpoly-of-poly } i p) (\text{Poly-Mapping.single } i n) = \text{poly.coeff } p n$
<proof>

lemma *coeff-mpoly-of-poly2* [simp]:
assumes $\neg \text{keys } x \subseteq \{i\}$
shows $\text{coeff } (\text{mpoly-of-poly } i p) x = 0$
<proof>

lemma *coeff-mpoly-of-poly*:
 $\text{coeff } (\text{mpoly-of-poly } i p) m =$
 $(\text{poly.coeff } p (\text{Poly-Mapping.lookup } m i) \text{ when } \text{keys } m \subseteq \{i\})$
<proof>

lemma *poly-mapping-single-eq-0-iff* [simp]: $\text{Poly-Mapping.single } i n = 0 \iff n = 0$
<proof>

lemma *mpoly-of-poly-pCons* [simp]:
fixes $p :: 'a :: \text{semiring-1 poly}$
shows $\text{mpoly-of-poly } i (\text{pCons } c p) = \text{Const } c + \text{Var } i * \text{mpoly-of-poly } i p$
<proof>

lemma *mpoly-of-poly-1* [simp]: *mpoly-of-poly* $i 1 = 1$
<proof>

lemma *mpoly-of-poly-uminus* [simp]: $mpoly\text{-of-poly } i (-p) = -mpoly\text{-of-poly } i p$
(proof)

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

lemma *mpoly-of-poly-diff* [simp]: $mpoly\text{-of-poly } i (p - q) = mpoly\text{-of-poly } i p - mpoly\text{-of-poly } i q$
(proof)

lemma *mpoly-of-poly-smult* [simp]:
 $mpoly\text{-of-poly } i (Polynomial.smult c p) = smult c (mpoly\text{-of-poly } i p)$
(proof)

lemma *mpoly-of-poly-mult* [simp]:
fixes $p q :: 'a :: comm\text{-semiring-1 } poly$
shows $mpoly\text{-of-poly } i (p * q) = mpoly\text{-of-poly } i p * mpoly\text{-of-poly } i q$
(proof)

lemma *insertion-mpoly-of-poly* [simp]: $insertion f (mpoly\text{-of-poly } i p) = poly p (f i)$
(proof)

lemma *mapping-of-mpoly-of-poly* [simp]: $mapping\text{-of } (mpoly\text{-of-poly } i p) = mpoly\text{-of-poly- aux } i p$
(proof)

lemma *vars-mpoly-of-poly*: $vars (mpoly\text{-of-poly } i p) \subseteq \{i\}$
(proof)

lemma *mpoly-map-vars-mpoly-of-poly* [simp]:
assumes $bij f$
shows $mpoly\text{-map-vars } f (mpoly\text{-of-poly } i p) = mpoly\text{-of-poly } (f i) p$
(proof)

end

6 More facts about algebraic numbers

theory *More-Algebraic-Numbers-HLW*
imports *Algebraic-Numbers.Algebraic-Numbers*
begin

6.1 Miscellaneous

lemma *in-Ints-imp-algebraic* [simp, intro]: $x \in \mathbb{Z} \implies algebraic x$
(proof)

lemma *in-Rats-imp-algebraic* [*simp, intro*]: $x \in \mathbb{Q} \implies \text{algebraic } x$
(*proof*)

lemma *algebraic-uminus-iff* [*simp*]: $\text{algebraic } (-x) \iff \text{algebraic } x$
(*proof*)

lemma *algebraic-0* [*simp*]: $\text{algebraic } (0 :: 'a :: \text{field-char-0})$
and *algebraic-1* [*simp*]: $\text{algebraic } (1 :: 'a :: \text{field-char-0})$
(*proof*)

lemma *algebraic-sum* [*intro*]:
 $(\bigwedge x. x \in A \implies \text{algebraic } (f x)) \implies \text{algebraic } (\text{sum } f A)$
(*proof*)

lemma *algebraic-prod* [*intro*]:
 $(\bigwedge x. x \in A \implies \text{algebraic } (f x)) \implies \text{algebraic } (\text{prod } f A)$
(*proof*)

lemma *algebraic-sum-list* [*intro*]:
 $(\bigwedge x. x \in \text{set } xs \implies \text{algebraic } x) \implies \text{algebraic } (\text{sum-list } xs)$
(*proof*)

lemma *algebraic-prod-list* [*intro*]:
 $(\bigwedge x. x \in \text{set } xs \implies \text{algebraic } x) \implies \text{algebraic } (\text{prod-list } xs)$
(*proof*)

lemma *algebraic-sum-mset* [*intro*]:
 $(\bigwedge x. x \in \# A \implies \text{algebraic } x) \implies \text{algebraic } (\text{sum-mset } A)$
(*proof*)

lemma *algebraic-prod-mset* [*intro*]:
 $(\bigwedge x. x \in \# A \implies \text{algebraic } x) \implies \text{algebraic } (\text{prod-mset } A)$
(*proof*)

lemma *algebraic-power* [*intro*]: $\text{algebraic } x \implies \text{algebraic } (x \wedge n)$
(*proof*)

lemma *algebraic-csqr*t [*intro*]: $\text{algebraic } x \implies \text{algebraic } (\text{csqr}t x)$
(*proof*)

lemma *algebraic-csqr*t-iff [*simp*]: $\text{algebraic } (\text{csqr}t x) \iff \text{algebraic } x$
(*proof*)

lemmas [*intro*] = *algebraic-plus algebraic-times algebraic-uminus algebraic-div*

lemma *algebraic-power-iff* [*simp*]:
assumes $n > 0$
shows $\text{algebraic } (x \wedge n) \iff \text{algebraic } x$
(*proof*)

lemma *algebraic-ii* [*simp*]: *algebraic* i
⟨*proof*⟩

lemma *algebraic-int-fact* [*simp*, *intro*]: *algebraic-int* (*fact* n)
⟨*proof*⟩

lemma *algebraic-minus* [*intro*]: *algebraic* x \implies *algebraic* y \implies *algebraic* (x - y)
⟨*proof*⟩

lemma *algebraic-add-cancel-left* [*simp*]:
 assumes *algebraic* x
 shows *algebraic* (x + y) \longleftrightarrow *algebraic* y
⟨*proof*⟩

lemma *algebraic-add-cancel-right* [*simp*]:
 assumes *algebraic* y
 shows *algebraic* (x + y) \longleftrightarrow *algebraic* x
⟨*proof*⟩

lemma *algebraic-diff-cancel-left* [*simp*]:
 assumes *algebraic* x
 shows *algebraic* (x - y) \longleftrightarrow *algebraic* y
⟨*proof*⟩

lemma *algebraic-diff-cancel-right* [*simp*]:
 assumes *algebraic* y
 shows *algebraic* (x - y) \longleftrightarrow *algebraic* x
⟨*proof*⟩

lemma *algebraic-mult-cancel-left* [*simp*]:
 assumes *algebraic* x x \neq 0
 shows *algebraic* (x * y) \longleftrightarrow *algebraic* y
⟨*proof*⟩

lemma *algebraic-mult-cancel-right* [*simp*]:
 assumes *algebraic* y y \neq 0
 shows *algebraic* (x * y) \longleftrightarrow *algebraic* x
⟨*proof*⟩

lemma *algebraic-inverse-iff* [*simp*]: *algebraic* (*inverse* y) \longleftrightarrow *algebraic* y
⟨*proof*⟩

lemma *algebraic-divide-cancel-left* [*simp*]:
 assumes *algebraic* x x \neq 0
 shows *algebraic* (x / y) \longleftrightarrow *algebraic* y
⟨*proof*⟩

lemma *algebraic-divide-cancel-right* [*simp*]:

```

assumes algebraic y y ≠ 0
shows algebraic (x / y) ↔ algebraic x
⟨proof⟩

```

6.2 Turning an algebraic number into an algebraic integer

6.3 Multiplying an algebraic number with a suitable integer turns it into an algebraic integer.

```

lemma algebraic-imp-algebraic-int:
fixes x :: 'a :: field-char-0
assumes ipoly p x = 0 p ≠ 0
defines c ≡ Polynomial.lead-coeff p
shows algebraic-int (of-int c * x)
⟨proof⟩

```

```

lemma algebraic-imp-algebraic-int':
fixes x :: 'a :: field-char-0
assumes ipoly p x = 0 p ≠ 0 Polynomial.lead-coeff p dvd c
shows algebraic-int (of-int c * x)
⟨proof⟩

```

end

7 Miscellaneous facts

theory Misc-HLW

imports

Complex-Main

HOL-Library.Multiset

HOL-Library.Permutations

HOL-Library.FuncSet

HOL-Library.Groups-Big-Fun

HOL-Library.Poly-Mapping

HOL-Library.Landau-Symbols

HOL-Computational-Algebra.Computational-Algebra

begin

```

lemma set-mset-subset-singletonD:
assumes set-mset A ⊆ {x}
shows A = replicate-mset (size A) x
⟨proof⟩

```

```

lemma image-mset-eq-replicate-msetD:
assumes image-mset f A = replicate-mset n y
shows ∀ x ∈ #A. f x = y
⟨proof⟩

```

```

lemma bij-betw-permutes-compose-left:

```

assumes π permutes A
shows $\text{bij-betw } (\lambda\sigma. \pi \circ \sigma) \{ \sigma. \sigma \text{ permutes } A \} \{ \sigma. \sigma \text{ permutes } A \}$
 $\langle \text{proof} \rangle$

lemma *bij-betw-compose-left-perm-Pi*:
assumes π permutes B
shows $\text{bij-betw } (\lambda f. (\pi \circ f)) (A \rightarrow B) (A \rightarrow B)$
 $\langle \text{proof} \rangle$

lemma *bij-betw-compose-left-perm-PiE*:
assumes π permutes B
shows $\text{bij-betw } (\lambda f. \text{restrict } (\pi \circ f) A) (A \rightarrow_E B) (A \rightarrow_E B)$
 $\langle \text{proof} \rangle$

lemma *bij-betw-image-mset-set*:
assumes $\text{bij-betw } f A B$
shows $\text{image-mset } f (\text{mset-set } A) = \text{mset-set } B$
 $\langle \text{proof} \rangle$

lemma *finite-multisets-of-size*:
assumes $\text{finite } A$
shows $\text{finite } \{ X. \text{set-mset } X \subseteq A \wedge \text{size } X = n \}$
 $\langle \text{proof} \rangle$

lemma *sum-mset-image-mset-sum-mset-image-mset*:
 $\text{sum-mset } (\text{image-mset } g (\text{sum-mset } (\text{image-mset } f A))) =$
 $\text{sum-mset } (\text{image-mset } (\lambda x. \text{sum-mset } (\text{image-mset } g (f x))) A)$
 $\langle \text{proof} \rangle$

lemma *sum-mset-image-mset-singleton*: $\text{sum-mset } (\text{image-mset } (\lambda x. \{ \#f x \# \}) A)$
 $= \text{image-mset } f A$
 $\langle \text{proof} \rangle$

lemma *sum-mset-conv-sum*:
 $\text{sum-mset } (\text{image-mset } f A) = (\sum x \in \text{set-mset } A. \text{of-nat } (\text{count } A x) * f x)$
 $\langle \text{proof} \rangle$

lemma *sum-mset-conv-Sum-any*:
 $\text{sum-mset } (\text{image-mset } f A) = \text{Sum-any } (\lambda x. \text{of-nat } (\text{count } A x) * f x)$
 $\langle \text{proof} \rangle$

lemma *Sum-any-sum-swap*:
assumes $\text{finite } A \wedge y. \text{finite } \{ x. f x y \neq 0 \}$
shows $\text{Sum-any } (\lambda x. \text{sum } (f x) A) = (\sum y \in A. \text{Sum-any } (\lambda x. f x y))$
 $\langle \text{proof} \rangle$

lemma (in *landau-pair*) *big-power*:
assumes $f \in L F g$
shows $(\lambda x. f x \wedge n) \in L F (\lambda x. g x \wedge n)$

<proof>

lemma (in *landau-pair*) *small-power*:

assumes $f \in l F g n > 0$

shows $(\lambda x. f x \wedge n) \in l F (\lambda x. g x \wedge n)$

<proof>

lemma *pairwise-imp-disjoint-family-on*:

assumes *pairwise* $R A$

assumes $\bigwedge m n. m \in A \implies n \in A \implies R m n \implies f m \cap f n = \{\}$

shows *disjoint-family-on* $f A$

<proof>

lemma (in *comm-monoid-set*) *If-eq*:

assumes $y \in A$ *finite* A

shows $F (\lambda x. g x (if x = y then h1 x else h2 x)) A = f (g y (h1 y)) (F (\lambda x. g x (h2 x)) (A - \{y\}))$

<proof>

lemma *prod-nonzeroI*:

fixes $f :: 'a \Rightarrow 'b :: \{semiring-no-zero-divisors, comm-semiring-1\}$

assumes $\bigwedge x. x \in A \implies f x \neq 0$

shows *prod* $f A \neq 0$

<proof>

lemma *frequently-prime-cofinite*: *frequently* (*prime* :: *nat* \Rightarrow *bool*) *cofinite*

<proof>

lemma *frequently-eventually-mono*:

assumes *frequently* $Q F$ *eventually* $P F \bigwedge x. P x \implies Q x \implies R x$

shows *frequently* $R F$

<proof>

lemma *bij-betw-Diff*:

assumes *bij-betw* $f A B$ *bij-betw* $f A' B' A' \subseteq A B' \subseteq B$

shows *bij-betw* $f (A - A') (B - B')$

<proof>

lemma *bij-betw-singleton*: *bij-betw* $f \{x\} \{y\} \longleftrightarrow f x = y$

<proof>

end

8 The Hermite–Lindemann–Weierstraß Transcendence Theorem

theory *Hermite-Lindemann*

imports

Pi-Transcendental.Pi-Transcendental
Algebraic-Numbers.Algebraic-Numbers
Algebraic-Integer-Divisibility
Min-Int-Poly
Complex-Lexorder
More-Polynomial-HLW
More-Multivariate-Polynomial-HLW
More-Algebraic-Numbers-HLW
Misc-HLW

begin

The Hermite–Lindemann–Weierstraß theorem answers questions about the transcendence of the exponential function and other related complex functions. It proves that a large number of combinations of exponentials is always transcendental.

A first (much weaker) version of the theorem was proven by Hermite. Lindemann and Weierstraß then successively generalised it shortly afterwards, and finally Baker gave another, arguably more elegant formulation (which is the one that we will prove, and then derive the traditional version from it).

To honour the contributions of all three of these 19th-century mathematicians, I refer to the theorem as the Hermite–Lindemann–Weierstraß theorem, even though in other literature it is often called Hermite–Lindemann or Lindemann–Weierstraß. To keep things short, the Isabelle name of the theorem, however, will omit Weierstraß’s name.

8.1 Main proof

Following Baker, We first prove the following special form of the theorem: Let $m > 0$ and $q_1, \dots, q_m \in \mathbb{Z}[X]$ be irreducible, non-constant, and pairwise coprime polynomials. Let β_1, \dots, β_m be non-zero integers. Then

$$\sum_{i=1}^m \beta_i \sum_{q_i(\alpha)=0} e^\alpha \neq 0$$

The difference to the final theorem is that

1. The coefficients β_i are non-zero integers (as opposed to arbitrary algebraic numbers)
2. The exponents α_i occur in full sets of conjugates, and each set has the same coefficient.

In a similar fashion to the proofs of the transcendence of e and π , we define some number J depending on the α_i and β_i and an arbitrary sufficiently

large prime p . We then show that, on one hand, J is an integer multiple of $(p - 1)!$, but on the other hand it is bounded from above by a term of the form $C_1 \cdot C_2^p$. This is then clearly a contradiction if p is chosen large enough.

lemma *Hermite-Lindemann-aux1:*

fixes $P :: \text{int poly set}$ **and** $\beta :: \text{int poly} \Rightarrow \text{int}$
assumes *finite* P **and** $P \neq \{\}$
assumes *distinct: pairwise Rings.coprime* P
assumes *irred:* $\bigwedge p. p \in P \Longrightarrow \text{irreducible } p$
assumes *nonconstant:* $\bigwedge p. p \in P \Longrightarrow \text{Polynomial.degree } p > 0$
assumes $\beta\text{-nz:}$ $\bigwedge p. p \in P \Longrightarrow \beta p \neq 0$
defines $\text{Roots} \equiv (\lambda p. \{\alpha :: \text{complex. poly (of-int-poly } p) \alpha = 0\})$
shows $(\sum p \in P. \text{of-int } (\beta p) * (\sum \alpha \in \text{Roots } p. \text{exp } \alpha)) \neq 0$
 $\langle \text{proof} \rangle$

8.2 Removing the restriction of full sets of conjugates

We will now remove the restriction that the α_i must occur in full sets of conjugates by multiplying the equality with all permutations of roots.

lemma *Hermite-Lindemann-aux2:*

fixes $X :: \text{complex set}$ **and** $\beta :: \text{complex} \Rightarrow \text{int}$
assumes *finite* X
assumes *nz:* $\bigwedge x. x \in X \Longrightarrow \beta x \neq 0$
assumes *alg:* $\bigwedge x. x \in X \Longrightarrow \text{algebraic } x$
assumes *sum0:* $(\sum x \in X. \text{of-int } (\beta x) * \text{exp } x) = 0$
shows $X = \{\}$
 $\langle \text{proof} \rangle$

8.3 Removing the restriction to integer coefficients

Next, we weaken the restriction that the β_i must be integers to the restriction that they must be rationals. This is done simply by multiplying with the least common multiple of the demoninators.

lemma *Hermite-Lindemann-aux3:*

fixes $X :: \text{complex set}$ **and** $\beta :: \text{complex} \Rightarrow \text{rat}$
assumes *finite* X
assumes *nz:* $\bigwedge x. x \in X \Longrightarrow \beta x \neq 0$
assumes *alg:* $\bigwedge x. x \in X \Longrightarrow \text{algebraic } x$
assumes *sum0:* $(\sum x \in X. \text{of-rat } (\beta x) * \text{exp } x) = 0$
shows $X = \{\}$
 $\langle \text{proof} \rangle$

Next, we weaken the restriction that the β_i must be rational to them being algebraic. Similarly to before, this is done by multiplying over all possible permutations of the β_i (in some sense) to introduce more symmetry, from which it then follows by the fundamental theorem of symmetric polynomials that the resulting coefficients are rational.

lemma *Hermite-Lindemann-aux4*:
fixes $\beta :: \text{complex} \Rightarrow \text{complex}$
assumes *[intro]*: *finite X*
assumes *alg1*: $\bigwedge x. x \in X \implies \text{algebraic } x$
assumes *alg2*: $\bigwedge x. x \in X \implies \text{algebraic } (\beta x)$
assumes *nz*: $\bigwedge x. x \in X \implies \beta x \neq 0$
assumes *sum0*: $(\sum_{x \in X}. \beta x * \text{exp } x) = 0$
shows $X = \{\}$
<proof>

8.4 The final theorem

We now additionally allow some of the β_i to be zero:

lemma *Hermite-Lindemann'*:
fixes $\beta :: \text{complex} \Rightarrow \text{complex}$
assumes *finite X*
assumes $\bigwedge x. x \in X \implies \text{algebraic } x$
assumes $\bigwedge x. x \in X \implies \text{algebraic } (\beta x)$
assumes $(\sum_{x \in X}. \beta x * \text{exp } x) = 0$
shows $\forall x \in X. \beta x = 0$
<proof>

Lastly, we switch to indexed summation in order to obtain a version of the theorem that is somewhat nicer to use:

theorem *Hermite-Lindemann*:
fixes $\alpha \beta :: 'a \Rightarrow \text{complex}$
assumes *finite I*
assumes $\bigwedge x. x \in I \implies \text{algebraic } (\alpha x)$
assumes $\bigwedge x. x \in I \implies \text{algebraic } (\beta x)$
assumes *inj-on* αI
assumes $(\sum_{x \in I}. \beta x * \text{exp } (\alpha x)) = 0$
shows $\forall x \in I. \beta x = 0$
<proof>

The following version using lists instead of sequences is even more convenient to use in practice:

corollary *Hermite-Lindemann-list*:
fixes $xs :: (\text{complex} \times \text{complex}) \text{ list}$
assumes *alg*: $\forall (x,y) \in \text{set } xs. \text{algebraic } x \wedge \text{algebraic } y$
assumes *distinct*: *distinct (map snd xs)*
assumes *sum0*: $(\sum (c,\alpha) \leftarrow xs. c * \text{exp } \alpha) = 0$
shows $\forall c \in (\text{fst } \text{' set } xs). c = 0$
<proof>

8.5 The traditional formulation of the theorem

What we proved above was actually Baker's reformulation of the theorem. Thus, we now also derive the original one, which uses linear independence

and algebraic independence.

It states that if $\alpha_1, \dots, \alpha_n$ are algebraic numbers that are linearly independent over \mathbf{Z} , then $e^{\alpha_1}, \dots, e^{\alpha_n}$ are algebraically independent over \mathbf{Q} .

Linear independence over the integers is just independence of a set of complex numbers when viewing the complex numbers as a \mathbf{Z} -module.

definition *linearly-independent-over-int* :: 'a :: field-char-0 set \Rightarrow bool **where**
linearly-independent-over-int = *module.independent* ($\lambda r x. \text{of-int } r * x$)

Algebraic independence over the rationals means that the given set X of numbers fulfils no non-trivial polynomial equation with rational coefficients, i.e. there is no non-zero multivariate polynomial with rational coefficients that, when inserting the numbers from X , becomes zero.

Note that we could easily replace ‘rational coefficients’ with ‘algebraic coefficients’ here and the proof would still go through without any modifications.

definition *algebraically-independent-over-rat* :: nat \Rightarrow (nat \Rightarrow 'a :: field-char-0) \Rightarrow bool **where**
algebraically-independent-over-rat n a \longleftrightarrow
 $(\forall p. \text{vars } p \subseteq \{..<n\} \wedge (\forall m. \text{coeff } p \ m \in \mathbf{Q}) \wedge \text{insertion } a \ p = 0 \longrightarrow p = 0)$

corollary *Hermite-Lindemann-original*:
fixes n :: nat **and** α :: nat \Rightarrow complex
assumes *inj-on* α {.. n }
assumes $\bigwedge i. i < n \implies \text{algebraic } (\alpha \ i)$
assumes *linearly-independent-over-int* (α ‘{.. n }’)
shows *algebraically-independent-over-rat* n ($\lambda i. \text{exp } (\alpha \ i)$)
<proof>

8.6 Simple corollaries

Now, we derive all the usual obvious corollaries of the theorem in the obvious way.

First, the exponential of a non-zero algebraic number is transcendental.

corollary *algebraic-exp-complex-iff*:
assumes *algebraic* x
shows *algebraic* (exp x :: complex) $\longleftrightarrow x = 0$
<proof>

More generally, any sum of exponentials with algebraic coefficients and exponents is transcendental if the exponents are all distinct and non-zero and at least one coefficient is non-zero.

corollary *sum-of-exp-transcendentalI*:
fixes xs :: (complex \times complex) list
assumes $\forall (x,y) \in \text{set } xs. \text{algebraic } x \wedge \text{algebraic } y \wedge y \neq 0$
assumes $\exists x \in \text{fst}' \text{set } xs. x \neq 0$
assumes *distinct*: *distinct* (map snd xs)

shows $\neg\text{algebraic } (\sum (c,\alpha)\leftarrow xs. c * \exp \alpha)$
(proof)

Any complex logarithm of an algebraic number other than 1 is transcendental (no matter which branch cut).

corollary *transcendental-complex-logarithm*:
assumes *algebraic x exp y = (x :: complex) x ≠ 1*
shows $\neg\text{algebraic } y$
(proof)

In particular, this holds for the standard branch of the logarithm.

corollary *transcendental-Ln*:
assumes *algebraic x x ≠ 0 x ≠ 1*
shows $\neg\text{algebraic } (\text{Ln } x)$
(proof)

The transcendence of e and π , which I have already formalised directly in other AFP entries, now follows as a simple corollary.

corollary *exp-1-complex-transcendental*: $\neg\text{algebraic } (\exp 1 :: \text{complex})$
(proof)

corollary *pi-transcendental*: $\neg\text{algebraic } \pi$
(proof)

8.7 Transcendence of the trigonometric and hyperbolic functions

In a similar fashion, we can also prove the transcendence of all the trigonometric and hyperbolic functions such as \sin , \tan , \sinh , \arcsin , etc.

lemma *transcendental-sinh*:
assumes *algebraic z z ≠ 0*
shows $\neg\text{algebraic } (\sinh z :: \text{complex})$
(proof)

lemma *transcendental-cosh*:
assumes *algebraic z z ≠ 0*
shows $\neg\text{algebraic } (\cosh z :: \text{complex})$
(proof)

lemma *transcendental-sin*:
assumes *algebraic z z ≠ 0*
shows $\neg\text{algebraic } (\sin z :: \text{complex})$
(proof)

lemma *transcendental-cos*:
assumes *algebraic z z ≠ 0*
shows $\neg\text{algebraic } (\cos z :: \text{complex})$

<proof>

lemma *tan-square-neq-neg1*: $\tan (z :: \text{complex})^2 \neq -1$
<proof>

lemma *transcendental-tan*:
 assumes *algebraic* $z \neq 0$
 shows $\neg \text{algebraic} (\tan z :: \text{complex})$
<proof>

lemma *transcendental-cot*:
 assumes *algebraic* $z \neq 0$
 shows $\neg \text{algebraic} (\cot z :: \text{complex})$
<proof>

lemma *transcendental-tanh*:
 assumes *algebraic* $z \neq 0$ *cosh* $z \neq 0$
 shows $\neg \text{algebraic} (\tanh z :: \text{complex})$
<proof>

lemma *transcendental-Arcsin*:
 assumes *algebraic* $z \neq 0$
 shows $\neg \text{algebraic} (\text{Arcsin } z)$
<proof>

lemma *transcendental-Arccos*:
 assumes *algebraic* $z \neq 1$
 shows $\neg \text{algebraic} (\text{Arccos } z)$
<proof>

lemma *transcendental-Arctan*:
 assumes *algebraic* $z \notin \{0, i, -i\}$
 shows $\neg \text{algebraic} (\text{Arctan } z)$
<proof>

end

References

- [1] A. Baker. *Transcendental Number Theory*. Cambridge Mathematical Library. Cambridge University Press, 1975.
- [2] S. Bernard. Formalization of the Lindemann-Weierstrass theorem. In M. Ayala-Rincón and C. A. Muñoz, editors, *Interactive Theorem Proving - 8th International Conference, ITP 2017, Brasília, Brazil, September 26-29, 2017, Proceedings*, volume 10499 of *Lecture Notes in Computer Science*, pages 65–80. Springer, 2017.

- [3] R. Steinberg and R. M. Redheffer. Analytic proof of the Lindemann theorem. *Pacific Journal of Mathematics*, 2(2):231–242, 1952.