

Irrational numbers from THE BOOK

Lawrence C. Paulson

February 6, 2026

Abstract

An elementary proof is formalised: that $\exp r$ is irrational for every nonzero rational number r . The mathematical development comes from the well-known volume *Proofs from THE BOOK* [1, pp. 51–2], by Aigner and Ziegler, who credit the idea to Hermite. The development illustrates a number of basic Isabelle techniques: the manipulation of summations, the calculation of quite complicated derivatives and the estimation of integrals. We also see how to import another AFP entry (Stirling’s formula) [2].

As for the theorem itself, note that a much stronger and more general result (the Hermite–Lindemann–Weierstraß transcendence theorem) is already available in the AFP [3].

Contents

1	Some irrational numbers	3
1.1	Basic definitions and their consequences	3
1.2	Towards the main result	6

Acknowledgements The author was supported by the ERC Advanced Grant ALEXANDRIA (Project 742178) funded by the European Research Council.

1 Some irrational numbers

From Aigner and Ziegler, *Proofs from THE BOOK* (Springer, 2018), Chapter 8, pp. 50–51.

theory *Irrationals-From-THEBOOK* **imports** *Stirling-Formula.Stirling-Formula*
begin

1.1 Basic definitions and their consequences

definition *hf* **where** $hf \equiv \lambda n. \lambda x::real. (x^n * (1-x)^n) / fact\ n$

definition *cf* **where** $cf \equiv \lambda n\ i. \text{if } i < n \text{ then } 0 \text{ else } (n \text{ choose } (i-n)) * (-1)^{i-n}$

Mere knowledge that the coefficients are integers is not enough later on.

lemma *hf-int-poly*:

fixes $x::real$

shows $hf\ n = (\lambda x. (1 / fact\ n) * (\sum_{i=0..2*n}. \text{real-of-int } (cf\ n\ i) * x^i))$

proof

fix x

have *inj*: *inj-on* $((+)n) \{..n\}$

by (*auto simp: inj-on-def*)

have [*simp*]: $((+)n) \text{ ' } \{..n\} = \{n..2*n\}$

using *nat-le-iff-add* **by** *fastforce*

have $(x^n * (-x + 1)^n) = x^n * (\sum_{k \leq n}. \text{real } (n \text{ choose } k) * (-x)^k)$

unfolding *binomial-ring* **by** *simp*

also have $\dots = x^n * (\sum_{k \leq n}. \text{real-of-int } ((n \text{ choose } k) * (-1)^k) * x^{n+k})$

by (*simp add: mult.assoc flip: power-minus*)

also have $\dots = (\sum_{k \leq n}. \text{real-of-int } ((n \text{ choose } k) * (-1)^k) * x^{n+k})$

by (*simp add: sum-distrib-left mult-ac power-add*)

also have $\dots = (\sum_{i=n..2*n}. \text{real-of-int } (cf\ n\ i) * x^i)$

by (*simp add: sum.reindex [OF inj, simplified] cf-def*)

finally have $hf\ n\ x = (1 / fact\ n) * (\sum_{i=n..2*n}. \text{real-of-int } (cf\ n\ i) * x^i)$

by (*simp add: hf-def*)

moreover have $(\sum_{i=0..<n}. \text{real-of-int } (cf\ n\ i) * x^i) = 0$

by (*simp add: cf-def*)

ultimately show $hf\ n\ x = (1 / fact\ n) * (\sum_{i=0..2*n}. \text{real-of-int } (cf\ n\ i) * x^i)$

using *sum.union-disjoint* [*of* $\{0..<n\} \{n..2*n\}$] $\lambda i. \text{real-of-int } (cf\ n\ i) * x^i$

by (*simp add: ivl-disj-int-two(7) ivl-disj-un-two(7) mult-2*)

qed

Lemma (ii) in the text has strict inequalities, but that's more work and is less useful.

lemma

assumes $0 \leq x \leq 1$

shows *hf-nonneg*: $0 \leq hf\ n\ x$ **and** *hf-le-inverse-fact*: $hf\ n\ x \leq 1 / fact\ n$

using *assms* **by** (*auto simp: hf-def divide-simps mult-le-one power-le-one*)

lemma *hf-differt* [*iff*]: *hf n differentiable at x*
unfolding *hf-int-poly differentiable-def*
by (*intro derivative-eq-intros exI | simp*)+

lemma *deriv-sum-int*:

deriv ($\lambda x. \sum i=0..n. \text{real-of-int } (c\ i) * x^{\wedge}i$) *x*
= (*if* $n=0$ *then* 0 *else* ($\sum i=0..n-1. \text{of-int}((i+1) * c(\text{Suc } i)) * x^{\wedge}i$))
(*is deriv* $?f\ x = (\text{if } n=0 \text{ then } 0 \text{ else } ?g)$)

proof –

have (*?f has-real-derivative* $?g$) (*at x*) **if** $n > 0$

proof –

have ($\sum i = 0..n. i * x^{\wedge}(i - \text{Suc } 0) * (c\ i)$)
= ($\sum i = 1..n. (\text{real } (i-1) + 1) * \text{of-int } (c\ i) * x^{\wedge}(i-1)$)
using *that by* (*auto simp: sum.atLeast-Suc-atMost intro!: sum.cong*)
also have ... = *sum* ($(\lambda i. (\text{real } i + 1) * c(\text{Suc } i) * x^{\wedge}i) \circ (\lambda n. n-1)$)
 $\{1..\text{Suc } (n-1)\}$

using *that by* *simp*

also have ... = $?g$

by (*simp flip: sum.atLeast-atMost-pred-shift* [**where** $m=0$])

finally have \S : ($\sum a = 0..n. a * x^{\wedge}(a - \text{Suc } 0) * (c\ a) = ?g$.

show *?thesis*

by (*rule derivative-eq-intros* \S | *simp*)+

qed

then show *?thesis*

by (*force intro: DERIV-imp-deriv*)

qed

We calculate the coefficients of the k th derivative precisely.

lemma *hf-deriv-int-poly*:

(*deriv* $\wedge k$) (*hf n*) = ($\lambda x. (1/\text{fact } n) * (\sum i=0..2*n-k. \text{of-int } (\text{int}(\prod \{i<..i+k\}) * \text{cf } n\ (i+k)) * x^{\wedge}i)$)

proof (*induction k*)

case 0

show *?case*

by (*simp add: hf-int-poly*)

next

case (*Suc k*)

define *F* **where** $F \equiv \lambda x. (\sum i = 0..2*n - k. \text{real-of-int } (\text{int}(\prod \{i<..i+k\}) * \text{cf } n\ (i+k)) * x^{\wedge}i)$

have *Fd*: *F field-differentiable at x* **for** *x*

unfolding *field-differentiable-def F-def*

by (*rule derivative-eq-intros exI | force*)+

have [*simp*]: $\text{prod int } \{i<..\text{Suc } (i+k)\} = (1 + \text{int } i) * \text{prod int } \{\text{Suc } i<..\text{Suc } (i+k)\}$ **for** *i*

by (*metis Suc-le-mono atLeastSucAtMost-greaterThanAtMost le-add1 of-nat-Suc prod.head*)

have *deriv* ($\lambda x. F\ x / \text{fact } n$) *x*

= ($\sum i = 0..2 * n - \text{Suc } k. \text{of-int } (\text{int}(\prod \{i<..i+ \text{Suc } k\}) * \text{cf } n\ (\text{Suc } (i+k))) * x^{\wedge}i$) / *fact n* **for** *x*

unfolding *deriv-cdivide-right* [*OF Fd*]
by (*fastforce simp add: F-def deriv-sum-int cf-def simp flip: of-int-mult intro: sum.cong*)
then show *?case*
by (*simp add: Suc F-def*)
qed

lemma *hf-deriv-0*: $(\text{deriv} \sim^k) (hf\ n)\ 0 \in \mathbf{Z}$
proof (*cases n ≤ k*)
case *True*
then obtain *j where* $(\text{fact } k :: \text{real}) = \text{real-of-int } j * \text{fact } n$
by (*metis fact-dvd dvd-def mult.commute of-int-fact of-int-mult*)
moreover have $\text{prod real } \{0 <..k\} = \text{fact } k$
by (*simp add: fact-prod atLeastSucAtMost-greaterThanAtMost*)
ultimately show *?thesis*
by (*simp add: hf-deriv-int-poly dvd-def*)
next
case *False*
then show *?thesis*
by (*simp add: hf-deriv-int-poly cf-def*)
qed

lemma *deriv-hf-minus*: $\text{deriv } (hf\ n) = (\lambda x. - \text{deriv } (hf\ n) (1-x))$
proof
fix *x*
have $hf\ n = hf\ n \circ (\lambda x. (1-x))$
by (*simp add: fun-eq-iff hf-def mult.commute*)
then have $\text{deriv } (hf\ n)\ x = \text{deriv } (hf\ n \circ (\lambda x. (1-x)))\ x$
by *fastforce*
also have $\dots = \text{deriv } (hf\ n)\ (1-x) * \text{deriv } ((-) 1)\ x$
by (*intro real-derivative-chain auto*)
finally show $\text{deriv } (hf\ n)\ x = - \text{deriv } (hf\ n)\ (1-x)$
by *simp*
qed

lemma *deriv-n-hf-diffr* [*iff*]: $(\text{deriv} \sim^k) (hf\ n)$ *field-differentiable at x*
unfolding *field-differentiable-def hf-deriv-int-poly*
by (*rule derivative-eq-intros exI | force*)**+**

lemma *deriv-n-hf-minus*: $(\text{deriv} \sim^k) (hf\ n) = (\lambda x. (-1) \sim^k * (\text{deriv} \sim^k) (hf\ n) (1-x))$
proof (*induction k*)
case *0*
then show *?case*
by (*simp add: fun-eq-iff hf-def*)
next
case (*Suc k*)
have $o: (\lambda x. (\text{deriv} \sim^k) (hf\ n) (1-x)) = (\text{deriv} \sim^k) (hf\ n) \circ (-) 1$
by *auto*

```

show ?case
proof
  fix x
  have [simp]: ((deriv  $\hat{\sim}$  k) (hf n)  $\circ$  (-) 1) field-differentiable at x
    by (force intro: field-differentiable-compose)
  have (deriv  $\hat{\sim}$  Suc k) (hf n) x = deriv ( $\lambda$ x. (-1)  $\hat{\sim}$  k * (deriv  $\hat{\sim}$  k) (hf n)
(1-x)) x
    by simp (metis Suc)
  also have ... = (-1)  $\hat{\sim}$  k * deriv ( $\lambda$ x. (deriv  $\hat{\sim}$  k) (hf n) (1-x)) x
    using o by fastforce
  also have ... = (-1)  $\hat{\sim}$  Suc k * (deriv  $\hat{\sim}$  Suc k) (hf n) (1-x)
    by (subst o, subst deriv-chain, auto)
  finally show (deriv  $\hat{\sim}$  Suc k) (hf n) x = (-1)  $\hat{\sim}$  Suc k * (deriv  $\hat{\sim}$  Suc k) (hf
n) (1-x) .
qed
qed

```

1.2 Towards the main result

lemma *hf-deriv-1*: (deriv $\hat{\sim}$ k) (hf n) 1 \in \mathbb{Z}

by (smt (verit, best) Ints-1 Ints-minus Ints-mult Ints-power deriv-n-hf-minus hf-deriv-0)

lemma *hf-deriv-eq-0*: $k > 2*n \implies$ (deriv $\hat{\sim}$ k) (hf n) = (λ x. 0)

by (force simp add: cf-def hf-deriv-int-poly)

The case for positive integers

lemma *exp-nat-irrational*:

assumes $s > 0$ shows \exp (real-of-int s) \notin \mathbb{Q}

proof

assume \exp (real-of-int s) \in \mathbb{Q}

then obtain a b where $ab: a > 0$ $b > 0$ coprime a b and \exp -s: \exp s = of-int a / of-int b

by (smt (verit) Rats-cases' divide-nonpos-pos exp-gt-zero of-int-0-less-iff)

define n where $n \equiv \text{nat} (\max (a^2) (3 * s^3))$

then have ns3: $s^3 \leq \text{real } n / 3$

by linarith

have $n > 0$

using $\langle a > 0 \rangle$ by (simp add: n-def max.strict-coboundedI1)

then have $s^{2*n+1} \leq s^{3*n}$

using $\langle a > 0 \rangle$ assms by (intro power-increasing) auto

also have ... = real-of-int(s^3) \wedge n

by (simp add: power-mult)

also have ... $\leq (n / 3) \wedge$ n

using assms ns3 by (simp add: power-mono)

also have ... $\leq (n / \exp 1) \wedge$ n

using \exp -le $\langle n > 0 \rangle$ by (auto simp: divide-simps)

finally have s-le: $s^{2*n+1} \leq (n / \exp 1) \wedge$ n

by presburger

have a-less: $a < \text{sqrt} (2*pi*n)$

```

proof –
  have  $2 * \pi > 1$ 
    using pi-ge-two by linarith
  have  $a \leq \sqrt[n]{n}$ 
    using  $\langle 0 < n \rangle$  n-def of-nat-nat real-le-rsqrt by fastforce
  also have  $\dots < \sqrt[n]{2 * \pi * n}$ 
    by (simp add: <0 < n> <1 < 2 * pi>)
  finally show ?thesis .
qed
have  $\sqrt[n]{2 * \pi * n} * (n / \exp 1) ^ n > a * s ^ (2 * n + 1)$ 
  using mult-strict-right-mono [OF a-less] mult-left-mono [OF s-le]
by (smt (verit, best) s-le ab(1) assms of-int-1 of-int-le-iff of-int-mult zero-less-power)
then have  $n : \text{fact } n > a * s ^ (2 * n + 1)$ 
  using fact-bounds(1) by (smt (verit, best) <0 < n> of-int-fact of-int-less-iff)
define  $F$  where  $F \equiv \lambda x. \sum_{i \leq 2 * n} (-1) ^ i * s ^ (2 * n - i) * (\text{deriv } ^ i) (hf\ n)\ x$ 
have  $F\text{der} : (F\ \text{has-real-derivative } -s * F\ x + s ^ (2 * n + 1) * hf\ n\ x)\ (\text{at } x)$  for  $x$ 
proof –
  have  $*$ :  $\text{sum } f\ \{..n+n\} = \text{sum } f\ \{..<n+n\}$  if  $f\ (n+n) = 0$  for  $f :: \text{nat} \Rightarrow \text{real}$ 
    by (smt (verit, best) lessThan-Suc-atMost sum.lessThan-Suc that)
  have [simp]:  $(\text{deriv } ((\text{deriv } ^ (n+n)) (hf\ n))\ x) = 0$ 
    using hf-deriv-eq-0 [where k= Suc(n+n)] by simp
  have  $\S$ :  $(\sum_{k \leq n+n} (-1) ^ k * ((\text{deriv } ^ (\text{Suc } k)) (hf\ n)\ x * \text{of-int } s ^ (n+n - k)))$ 
     $+ s * (\sum_{j=0..n+n} (-1) ^ j * ((\text{deriv } ^ j) (hf\ n)\ x * \text{of-int } s ^ (n+n - j)))$ 
     $= s * (hf\ n\ x * \text{of-int } s ^ (n+n))$ 
    using  $\langle n > 0 \rangle$ 
    apply (subst sum-Suc-reindex)
    apply (simp add: algebra-simps atLeast0AtMost)
    apply (force simp add: * mult.left-commute [of of-int s] minus-nat.diff-Suc sum-distrib-left)
    simp flip: sum.distrib intro: comm-monoid-add-class.sum.neutral split: nat.split-asm)
  done
show ?thesis
  unfolding  $F\text{-def}$ 
  apply (rule derivative-eq-intros field-differentiable-derivI | simp)+
  using  $\S$  by (simp add: algebra-simps atLeast0AtMost eval-nat-numeral)
qed
have  $F01\text{-Ints} : F\ 0 \in \mathbb{Z}\ F\ 1 \in \mathbb{Z}$ 
  by (simp-all add: F-def hf-deriv-0 hf-deriv-1 Ints-sum)
define  $sF$  where  $sF \equiv \lambda x. \exp (\text{of-int } s * x) * F\ x$ 
define  $sF'$  where  $sF' \equiv \lambda x. \text{of-int } s ^ (\text{Suc } (2 * n)) * (\exp (\text{of-int } s * x) * hf\ n\ x)$ 
have  $sF\text{-der} : (sF\ \text{has-real-derivative } sF'\ x)\ (\text{at } x)$  for  $x$ 
  unfolding  $sF\text{-def } sF'\text{-def}$ 
  by (rule refl Fder derivative-eq-intros | force simp: algebra-simps)+
let  $?N = b * \text{integral } \{0..1\}\ sF'$ 
have  $sF'\text{-integral} : (sF'\ \text{has-integral } sF\ 1 - sF\ 0)\ \{0..1\}$ 
  by (smt (verit) fundamental-theorem-of-calculus has-real-derivative-iff-has-vector-derivative)

```

has-vector-derivative-at-within sF-der)

then have $?N = a * F 1 - b * F 0$
using $\langle b > 0 \rangle$ **by** (*simp add: integral-unique exp-s sF-def algebra-simps*)
also have $\dots \in \mathbb{Z}$
using *hf-deriv-1* **by** (*simp add: F01-Ints*)
finally have *N-Ints: ?N ∈ ℤ .*
have $sF' (1/2) > 0$ **and** $ge0: \bigwedge x. x \in \{0..1\} \implies 0 \leq sF' x$
using *assms* **by** (*auto simp: sF'-def hf-def*)
moreover have *continuous-on {0..1} sF'*
unfolding *sF'-def hf-def* **by** (*intro continuous-intros*) *auto*
ultimately have *False* **if** (*sF' has-integral 0*) $\{0..1\}$
using *has-integral-0-cbox-imp-0* [*of 0 1 sF' 1/2*] **that by** *auto*
then have *integral {0..1} sF' > 0*
by (*metis ge0 has-integral-nonneg integral-unique order-le-less sF'-integral*)
then have $0 < ?N$
by (*simp add: 0*)
have *integral {0..1} sF' = of-int s ^ Suc(2*n) * integral {0..1} (λx. exp (s*x)*
** hf n x)*
unfolding *sF'-def* **by** *force*
also have $\dots \leq of-int s ^ Suc(2*n) * (exp s * (1 / fact n))$
proof (*rule mult-left-mono*)
have *integral {0..1} (λx. exp (s*x) * hf n x) ≤ integral {0..1} (λx::real. exp s*
** (1/fact n))*
proof (*intro mult-mono integral-le*)
show $(λx. exp (s*x) * hf n x)$ *integrable-on {0..1}*
using $\langle 0 < ?N \rangle$ *not-integrable-integral sF'-def* **by** *fastforce*
qed (*use assms hf-nonneg hf-le-inverse-fact in auto*)
also have $\dots = exp s * (1 / fact n)$
by *simp*
finally show *integral {0..1} (λx. exp (s*x) * hf n x) ≤ exp s * (1 / fact n) .*
qed (*use assms in auto*)
finally have $?N \leq b * of-int s ^ Suc(2*n) * exp s * (1 / fact n)$
using $\langle b > 0 \rangle$ **by** (*simp add: sF'-def mult-ac divide-simps*)
also have $\dots < 1$
using *n apply* (*simp add: field-simps exp-s*)
by (*metis of-int-fact of-int-less-iff of-int-mult of-int-power*)
finally show *False*
using $\langle 0 < ?N \rangle$ *Ints-cases N-Ints* **by** *force*
qed

theorem *exp-irrational:*

fixes $q::real$ **assumes** $q \in \mathbb{Q} \ q \neq 0$ **shows** $exp\ q \notin \mathbb{Q}$

proof

assume $q: exp\ q \in \mathbb{Q}$

obtain $s\ t$ **where** $s \neq 0 \ t > 0 \ q = of-int\ s / of-int\ t$

by (*metis Rats-cases' assms div-0 of-int-0*)

then have $(exp\ q) ^ (nat\ t) = exp\ s$

by (*smt (verit, best) exp-divide-power-eq of-nat-nat zero-less-nat-eq*)

```

moreover have  $\exp q ^{\wedge} (\text{nat } t) \in \mathbf{Q}$ 
  by (simp add: q)
ultimately show False
  by (smt (verit, del-insts) Rats-inverse ‹s ≠ 0› exp-minus exp-nat-irrational
of-int-of-nat)
qed

```

corollary *ln-irrational*:

```

fixes q::real assumes  $q \in \mathbf{Q} \quad q > 0 \quad q \neq 1$  shows  $\ln q \notin \mathbf{Q}$ 
using assms exp-irrational [of ln q] exp-ln-iff [of q] by force

```

end

References

- [1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer, 6th edition, 2018.
- [2] M. Eberl. Stirling’s formula. *Archive of Formal Proofs*, Sept. 2016. https://isa-afp.org/entries/Stirling_Formula.html, Formal proof development.
- [3] M. Eberl. The Hermite–Lindemann–Weierstraß transcendence theorem. *Archive of Formal Proofs*, Mar. 2021. https://isa-afp.org/entries/Hermite_Lindemann.html, Formal proof development.