

A formalisation of transcendence of e

Jujian Zhang (CID: 01803812)

Supervisor: Prof. Kevin Buzzard

2020

Declaration

I declare that this report was composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text.

ZuR

Acknowledgement

I would like to thanks professor Kevin Buzzard for supervising this project whose advise has helped me to write more idiomatic `Lean` codes. He introduced me to the area of formalisation, hence I owe this unique experience to him. I am also thankful for the `Lean` community for providing `library_search` without which this project could not possibly make any noticeable progress.

Abstract

The objective of this report is to present formalization of some basic theorems from transcendental number theory with **Lean** and **mathlib** in the hope that it will motivate and inspire other mathematicians, by igniting their curiosity about interactive theorem proving. The following theorems are formalized:

1. the set of algebraic numbers is countable, hence transcendental number exists:

```
1 theorem algebraic_set_countable : set.countable algebraic_set
2 theorem transcendental_number_exists :
3    $\exists x : \mathbb{R}, \text{transcendental } x$ 
```

2. all Liouville numbers are transcendental:

```
1 theorem liouville_numbers_transcendental :
2    $\forall x : \mathbb{R}, \text{liouville\_number } x \rightarrow \text{transcendental } x$ 
```

3. $\alpha := \sum_{i=0}^{\infty} \frac{1}{10^{i!}}$ is a Liouville number hence α is transcendental.

```
1 theorem liouville_alpha : liouville_number alpha
2 theorem transcendental_alpha : transcendental alpha :=
3   liouville_numbers_transcendental alpha liouville_alpha
```

4. e is transcendental:

```
1 theorem e_transcendental : transcendental e
```

Contents

1	Overview	2
1.1	Interactive theorem proving	2
1.2	History of transcendental numbers	3
2	Brief introduction to Lean	5
2.1	Simple type theory	5
2.1.1	Proposition as type	6
2.2	Lean and mathlib	7
2.2.1	prove a conjunction	11
2.2.2	prove a disjunction	11
2.2.3	prove an implication	11
2.2.4	prove an equivalence	12
2.2.5	prove a negation	12
2.2.6	prove a proposition with \forall	12
2.2.7	prove a proposition with \exists	13
2.3	An example	13
3	Formalisation using Lean	16
	Logistics of the formalisation	16
3.1	Countability argument	17
3.2	Liouville's theorem and Liouville numbers	23
	General theory about Liouville number	23
	Construction of a Liouville number	29
3.3	Hermite's theorem	32
	Transcendence of e	36
	Conclusion and future work	50
	Bibliography	51

Chapter 1

Overview

1.1 Interactive theorem proving

Around 1920s, the German mathematician David Hilbert put forward a programme to seek:

1. an axiomatic foundation of mathematics;
2. a proof of consistency of the said foundation;
3. Entscheidungsproblem: an algorithm to determine if any proposition is universally valid given a set of axioms.

The first two aims were later proved to be impossible by Gödel and his celebrated incompleteness theorems. Via the completeness of first order logic, the Entscheidungsproblem can also be interpreted as an algorithm for producing proofs using deduction rules. Even without a panacea approach for mathematics, a computer still bears advantages against a carbon-based mathematician. Perhaps the most manifested advantage is the accuracy of a computer with which it execute its command and to recall its memories. Thus came the idea of **interactive theorem proving** — instead of hoping a computer algorithm can spit out some unfathomable proofs, assuming computers are given the ability to check the correctness of proofs, so human-comprehensible proofs can be verified by machines and thus guaranteed to be free of errors. With a collective effort, all theorems verified this way can be collected in an error-free library such that all mathematicians can utilise to prove further theorems, which can then be added to the collection, ad infinitum [Boy+94]. Curry-Howard isomorphism provided the crucial relationship between mathematical proofs and computer programmes, more specifically relationship between propositions and types, to make such project feasible [KK11]. The idea will be explained in section 2 along with `Lean`.

The proof of “Kepler’s conjecture¹” illustrates and exemplifies the utility of

¹the most efficient way to pack spheres should be hexagonally

interactive theorem proving. As early as 1998, Thomas Hales had claimed a proof [Hal98; HUW14], however the proof is controversial in the sense that other mathematician even after great effort could not guarantee its correctness. A collaborative project using `Isabelle`² and `HOL Light`³ verified the proof around 2014, hence settled the controversy in 2017 [Hal+17]. There is also Georges Gonthier with his teams using `Coq`⁴ who formalised the four colour theorem and Feit-Thompson theorem where the latter is a step closer to the classification of simple groups [Gon08; Gon+13]. Additionally, using `Lean`⁵, Buzzard, Commelin, and Massot were able to formalise the modern notion of perfectoid spaces [BCM20].

1.2 History of transcendental numbers

“Transcendence” as a mathematical jargon first appeared in a Leibniz’s 1682 paper where he proved that sine is a transcendental function in the sense that for any natural number n there does not exist polynomials p_0, \dots, p_n such that

$$p_0(x) + p_1(x) \sin(x) + p_2(x) \sin(x)^2 + \dots + p_n(x) \sin(x)^n = 0$$

holds for all $x \in \mathbb{R}$ [Bou98]. The Swiss mathematician Johann Heinrich Lambert in his 1768 paper proved the irrationality of e and π and he also conjectured their transcendence [Lam04]. It is not until 1844 that Joseph Liouville proved the existence of any transcendental number and until 1851 an explicit example of transcendental number was actually given by its decimal expansion:[Kem16]

$$\sum_{i=1}^{\infty} \frac{1}{10^{i!}} = 0.11000100000\dots$$

However, this construction is still artificial in nature. The first example of a real number proven to be transcendental that is not constructed for the purpose of being transcendental was e . Charles Hermite proved the transcendence of e in 1873 with a method applicable (with help of symmetric polynomial) to π in 1882 and later to be generalised to Lindemann-Weierstrass theorem in 1885 stating that if $\alpha_1, \dots, \alpha_n$ are distinct algebraic numbers then $e^{\alpha_1}, \dots, e^{\alpha_n}$ are linearly independent over the algebraic numbers [Bak90]. The transcendence of π was particularly celebrated because it immediately implied the impossibility of the ancient greek challenge of squaring the circle, i.e. it is not possible to construct a square, using compass and ruler only, with equal area to a circle. This question is plainly equivalent to construct $\sqrt{\pi}$, which is not possible for otherwise π is algebraic. Georg Cantor in 1874 proved that algebraic numbers are countable hence not only do transcendental numbers exist, they exist in

²a theorem prover relies extensively on dependent type theory and Curry-Howard correspondence.

³ibid.

⁴ibid.

⁵ibid.

a ubiquitous manner – there is a bijection from the set of all transcendental numbers to \mathbb{R} [Can32; Can78].

In 1900, Hilbert proposed twenty-three questions, the 7th of which is regarding transcendental numbers: Is a^b transcendental, for any algebraic number a that is not 0 or 1 and any irrational algebraic number b ? The answer is yes provided by Gelfond-Schneider theorem in 1934 [Gel34]. This led to some immediate consequences such that

1. $2^{\sqrt{2}}$ and its square root $\sqrt{2^{\sqrt{2}}}$ are transcendental;
2. e^π is transcendental for $e^\pi = (e^{i\pi})^{-i} = (-1)^{-i}$;
3. $i^i = e^{-\frac{\pi}{2}}$ is transcendental etc.

In contrast, none of $\pi \pm e$, πe , $\frac{\pi}{e}$, π^π , π^e , etc were proven to be transcendental. It was also conjectured by Stephen Schanuel that given any n \mathbb{Q} -linearly independent $z_1, \dots, z_n \in \mathbb{C}$, then $\text{trdeg}(\mathbb{Q}(z_1, \dots, z_n, e^{z_1}, \dots, e^{z_n})/\mathbb{Q})$ is at least n [Lan66]. If this was proven, the algebraic independence of e and π would follow immediately by setting $z_1 = 1$ and $z_2 = \pi i$ with Euler's identity.

Chapter 2

Brief introduction to Lean

Lean was developed by Leonardo de Moura at Microsoft Research Redmond in 2013 using dependent type theory and calculus of inductive constraint [AMK15]. In this chapter, basic ideas of Curry-Howard isomorphism will be demonstrated by some basic examples of mathematical theorem expressed in Lean using dependent type theory.

2.1 Simple type theory

Unlike set theory where everything from basic things like natural numbers to complex constructions like modular forms is essentially a set, type theory associate every expression with a **type**. In set theory, an element can belong to different sets, for example 0 is simultaneously in $\mathbb{N} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. However an expression can only have one type. 0 without any context will have type \mathbb{N} and, to specify the zero with type \mathbb{R} we write $(0 : \mathbb{R})$. If a has type α , we write $a : \alpha$. By a universe of types we mean a collection of types. Types can be combined to form new types in the following way:

- let α and β be types then $\alpha \rightarrow \beta$ is the type of functions from α to β : the element of type $\alpha \rightarrow \beta$ is a function that for any element of α gives an element of β . For mathematicians this loosely means that for any two classes α and β , there is a new class $\text{hom}(\alpha, \beta)$. Sometimes we are not bothered to give a function a name, we can use the λ notation: the expression $(\lambda x : \alpha, \text{expression})$ has type $\alpha \rightarrow \dots$ depending on the content of expression. For example $(\lambda x : \mathbb{N}, x + 1) : \mathbb{N} \rightarrow \mathbb{N}$ is the function from natural numbers to natural numbers that add 1 to any input.
- let α and β be types then $\alpha \times \beta$ is the cartesian product of α and β : the element of type $\alpha \times \beta$ is an ordered tuple (a, b) where $a : \alpha$ and $b : \beta$.
- Let α be a type in universe \mathcal{U} and $\beta : \alpha \rightarrow \mathcal{U}$ be a family of type that for

any $a : \alpha$, $\beta(a)$ is a type in \mathcal{U} . Then we can form the Π -type

$$\prod_{a:\alpha} \beta(a)$$

whose element is of the form $f : \prod_{a:\alpha} \beta(a)$ such that for any $x : \alpha$, $f(x) : \beta(x)$. Note that function type is actually an example of Π -type where β is a constant family of types. For this reason, we also call Π -types dependent functions. For example if $\text{Vec}(\mathbb{R}, n)$ is the type of \mathbb{R}^n , then

$$n \mapsto (\underbrace{1, \dots, 1}_{n \text{ times}}) : \prod_{m:\mathbb{N}} \text{Vec}(\mathbb{R}, m)$$

- We also have dependent cartesian product or Σ -type: Let α be a type in universe \mathcal{U} and $\beta : \alpha \rightarrow \mathcal{U}$ be a family of types in \mathcal{U} , then the Σ -type

$$\sum_{a:\alpha} \beta(a)$$

whose element is of the form $(x, y) : \sum_{a:\alpha} \beta(a)$ such that $x : \alpha$ and $y : \beta(x)$.

Similarly

$$\left(n, (\underbrace{1, \dots, 1}_{n \text{ times}}) \right) : \sum_{m:\mathbb{N}} \text{Vec}(\mathbb{R}, m)$$

2.1.1 Proposition as type

In type theory, a proposition p can be regarded as a type whose elements is a proof of p .

Example 1. $1 + 1 = 2$ is a proposition. `rfl` is an element of type $1 + 1 = 2$ where `rfl` is the assertion that every term equals to itself.

Example 2. For two propositions p and q , the implication $p \implies q$ then can be interpreted as function $p \rightarrow q$. To say `imp` : $p \rightarrow q$ is to say for any `hp` : p we have `imp(hp)` : q , or equivalently given any `hp`, a *proof* of proposition p , `imp(hp)` is a *proof* of proposition q .

Example 3. If $p : \alpha \rightarrow \text{proposition}$, the proposition $\forall x : \alpha, p(x)$ can be interpreted as a Π -type $\prod_{x:\alpha} p(x)$. To prove $\forall x : \alpha, p(x)$, we need to find an element

of type $\prod_{x:\alpha} p(x)$; equivalently for any $x : \alpha$, we need to find an element of type $p(x)$; equivalently for any $x : \alpha$, we need to find a proof of $p(x)$.

Similarly, $\exists x : \alpha, p(x)$ can be interpreted as a Σ -type $\sum_{x:\alpha} p(x)$. To prove $\exists x : \alpha, p(x)$ is to find an element x of type α and prove $p(x)$, equivalent to find an element $x : \alpha$ and an element of type $p(x)$ and this is precisely $(x, p(x)) : \sum_{a:\alpha} p(a)$.

Theorems are true propositions. Using the interpretation above, theorems are inhabited types and to prove a theorem is to find an element of the required type.

2.2 Lean and mathlib

`mathlib` is the collection of mathematical definitions, theorems, lemmas built on `Lean`. `mathlib` includes topics in algebra, topology, manifolds and combinatorics etc. The following section will briefly explain how to use `Lean` with `mathlib`.

In `Lean`, new definition can be introduced with the following syntax:

```
1 def name (arg1:type1) ... (argn:typen) : return_type := contents
2
3 def name' {arg1:type1} ... (argn:typen) : return_type := contents
```

`return_type` is optional when it can be inferred from `contents`. If an argument is enclosed by curly brackets instead of round brackets, then when the definition is invoked the said argument is implicit, i.e. `name' a2 ... an` where `ai:typei`. To explicitly mention the said argument, one needs to use `@name' a1 ... an` where `ai:typei`. One can use “if then else” to introduce a function whose value depends on the value of the arguments:

```
1 def name args : return_type :=
2   if (h args)
3   then contents1
4   else contents2
5
6 def name args : return_type :=
7   ite (h args) contents1 contents2
```

New notations are introduced with the following syntax:

```
1 notation _`lhs`_ := _rhs_
```

so that `Lean` will treat every occurrence of `_`lhs`_` as `_rhs_` verbatim. For example `notation $\mathbb{Z}[X]$:= polynomial \mathbb{Z}` will replace `polynomial \mathbb{Z}` with a more familiar notation of `$\mathbb{Z}[X]$` .

For any type of α , we can introduce a subtype of α by:

```
1 def  $\alpha'$  := {x :  $\alpha$  // property_satisfied_by_x}
```

An element of type α' is of the form $\langle x, hx \rangle$ where $x : \alpha$ and hx is a proof that x satisfies the given property.

Theorems or lemmas are introduced with the following syntax:

```

1 theorem name (arg1:type1) ... (argn:typen) : content :=
2 begin
3   -- proof of the theorem
4 end

```

To write a proof understandable to Lean, one needs to use *tactic mode*. In Lean, one can use

- proof by induction: if the goal is a proposition about natural number n , `induction n with n IH` is to prove the proposition by induction. This command will change the current goal to two goals. The first is to prove the proposition for $n = 0$ and the second to prove the proposition for $n + 1$ with the additional inductive hypothesis `IH`;

```

1 theorem awesome_theorem_about_natural_number (n : ℕ) :
2   ↔ propositionn :=
3 begin
4   induction n with n IH,
5
6   a_proof_of_proposition0
7
8   -- (IH : propositionn) is now in context
9   a_proof_of_propositionn+1
10 end

```

- proof by contradiction: if the goal is to prove proposition H , `by_contra absurdum` will add `absurdum : ¬H` into the current context and turn the goal into proving `false`;

```

1 theorem awesome_theorem : awesome_proposition :=
2 begin
3   by_contra absurdum,
4
5   -- Now (absurdum : ¬ awesome_proposition) is in context and
6   ↔ the goal is to prove falsehood.
7   a_proof_of_falsehood
8 end

```

- proof in a forward manner i.e. introduce new theorem into the current context or convert known theorem in the current context to approach the goal:

- `have H := content` will introduce a new proposition whose proof is given by `content`.
- `have H : some_proposition` will add one more goal of proving the proposition then introduce the proved proposition to the current context.

- If H is in context then `replace H := content` will change H to (a proof of) the proposition that `content` is proving.
`replace H : some_proposition` will add one more goal of proving `some_proposition` and then replace H to the proposition proven.
 - If H is in context, `simp at H` will simplify H to using small lemmas¹.
`simp only [h1,...,hn]` is to simplify only using $h1 \dots hn$.
 - `rw` is for term rewriting. If we have $h : lhs = rhs$ or $h : lhs \leftrightarrow rhs$ and another H in context, then `rw h at H` will replace every occurrence of `lhs` with `rhs` in H and `rw ←h` will replace every occurrence of `rhs` with `lhs` in H .
`rw [h1, h2, ..., hn] at H` is the same as `rw h1 at H, rw h2 at H, ..., rw hn at H`.
 - The fact that `rw` and `simp` change all term occurrences sometimes creates an inconvenience. If H is in context, `conv_lhs at H {tactics}` will confine the scope of `tactics` only to the left hand side of H ; similarly `conv_rhs at H {tactics}` will confine the scope to the right hand side of H .
 - `generalise H : lhs = var_name` will set `var_name` to `lhs` and add (proof of) the proposition $H : lhs = var_name$ to the current context.
 - If $H : \exists x : type, property_about_x$ is in the current context, `choose x hx using H` will introduce $x : type$ with the assumption $hx : property_about_x$ to the current context.
 - If $H : p \wedge q$ is in the current context, then $H.1$ is (a proof of) p and $H.2$ is (a proof of) q .
 - If $H : ite\ h1\ h2\ h3$ is in the current context, then `split_ifs at H` will turn the current goal into two goals, the first one is to prove the original goal with the additional assumption $h1$ and $h2$; the second one is to prove the original with goal with the additional assumption $\neg h1$ and $h3$.
- proof in a backward manner i.e. convert or replace the goal so that it is closer to what is known in context:
 - `unfold definition` is to unfold a definition to what is explicitly defined when the definition is introduced.
 - `simp, rw, conv_lhs {tactics}` and `conv_rhs {tactics}` is the same as above except now they change at goal.
 - Given (a proof of) proposition $H : h1 \rightarrow h2$, then `apply H` will change the goal of proving $h2$ to prove $h1$.

¹to be more precise, lemma with `@[simp]` tag, i.e. lemmas declared in the following syntax `@[simp] lemma lemma_name args : Prop`. These lemma are usually trivial in nature such as `nat.add_zero` which asserts that $\forall n : \mathbb{N}, n + 0 = n$.

- `suffices H : some_proposition` ask for a proof of the current goal with additional `H`, then ask for a proof of `H`.
 - `norm_cast` converts the type of numbers. For example the current goal is $(x : \mathbb{R}) < (y : \mathbb{R})$ where x and y are of type \mathbb{N} , then after `norm_cast` the goal will become $x < y$. This should be simpler because \mathbb{R} in `Lean` is defined as equivalent classes of Cauchy sequence of \mathbb{Q} while natural number is much easier to work with.
`norm_num` is equivalent to `norm_cast`, `simp`.
 - `ext` will convert the current goal with axioms of extensionality. For example if the goal is to prove equality of polynomial then after `ext` the goal would become to prove that every coefficient is equal; or if the goal is to prove equality of sets of type α $A = B$, then after `ext`, an arbitrary element `x` of type α will be introduced into context then the goal will become to prove $x \in A \iff x \in B$. `ext var_name` will force `Lean` to introduce a new variable under the identifier `var_name`.
 - If the goal is to prove `ite h1 h2 h3` (or `ite h1 h2 lhs = rhs`), then `split_ifs at H` will turn the current goal into two goals, the first one is to prove `h2 (lhs = rhs` resp.) with the additional assumption `h1`; the second one is to prove `h3 (lhs = rhs` resp.) with the additional assumption `¬h1`.
- when the goal is easily provable, one can use the following to finish a goal:
 - `refl` (for reflexive) is used to prove propositions of the form `lhs = rhs` when `lhs` is **definitionally** equal to `rhs`. Definitional equality is more general than two string being literally identical but is less general than being (canonically) isomorphic. For example

$$\sum_{i=0}^{\infty} \frac{1}{2^i} = \sum_{j=0}^{\infty} \frac{1}{2^j}$$

is a definitional equality but

$$\mathbb{R}^n = \text{Func}(\{0, \dots, n-1\}, \mathbb{R})$$

is not a definitional equality (strictly speaking perhaps not an equality at all).

- `exact H` will prove the current goal if the goal is definitionally equal to `H`.
- `ring` will try to prove the current goal using associativity and commutativity of addition and multiplication.
- `linarith` is used when proving inequality from context. `linarith` is semi-automated, so it can work with inequalities with symbols or variables but only to a degree. If `linarith` fails, one has to either

provide `linarith` with more propositions or use other tactics to change the goal into something more manageable the use `linarith`. `linarith [h1, ..., hn]` is equivalent to use `linarith` with additional (proofs of) propositions `h1 ... hn`.

– `tidy` is to ask `Lean` to try different tactics and finishes the goal if it possible.

- If there is multiple goals, one can use `{ }` to focus on the first one.
- If the entirety of proof is one line, one can replace `begin contents end` with `by contents`.

A proposition if not atomic is either a conjunction, a disjunction, an implication, an equivalence, a negation or a proposition with universal quantifier or existential quantifier.

2.2.1 prove a conjunction

If the goal is to prove a conjunction of the form $h_1 \wedge h_2$, `split` is used. It will change the current goal to two goals of proving h_1 and h_2 respectively. Then the general pattern is

```
1 theorem how_to_prove_conjunction (h1 : Prop) (h2 : Prop) : h1 ∧ h2 :=
2 begin
3   split,
4
5   proof_of_h1
6
7   proof_of_h2
8 end
```

2.2.2 prove a disjunction

If the goal is to prove a disjunction of the form $h_1 \vee h_2$, one can use `left` to change the goal to prove h_1 or `right` to change the goal to prove h_2 . Let us assume h_1 is a true proposition :

```
1 theorem how_to_prove_disjunction (h1 : Prop) (h2 : Prop) : h1 ∨ h2 :=
2 begin
3   left,
4
5   proof_of_h1
6 end
```

2.2.3 prove an implication

If the goal is to prove an implication of the form $p \implies q$, one can use `intro` `hp` to add `hp:p` a proof of p into the context and convert the goal to proving q .

```

1 theorem how_to_prove_implication (p : Prop) (q : Prop) : p → q :=
2 begin
3 intro hp,
4
5 proof_of_q
6 end

```

If the goal is of the form $p_1 \rightarrow p_2 \rightarrow \dots p_n$, one can use `intros hp1 ... hpn` as an abbreviation of `intro hp1, intro hp2, ..., intro hpn`.

2.2.4 prove an equivalence

An equivalence of the form $p \iff q$ is by definition $p \implies q \wedge q \implies p$. Thus `split` will change the goal to two goals, one to prove $p \implies q$, the other to prove $q \implies p$. Then use section 2.2.3.

2.2.5 prove a negation

A negation of the form $\neg p$ is by definition $p \implies \perp$. Thus `intro hp` will add `hp:p` to the current context and convert the goal to proving a falsehood.

```

1 theorem how_to_prove_negation (p : Prop) : ¬p :=
2 begin
3 intro hp,
4
5 proof_of_falsehood
6 end

```

2.2.6 prove a proposition with \forall

A proposition of the form $\forall a : \alpha, p(a)$ where α is a type and $p : \alpha \rightarrow \mathbf{Prop}$ can be proved also using `intro x0`. This will add an arbitrary $x_0 : \alpha$ to the current context and change the goal to proving $p(x_0)$.

```

1 theorem how_to_proposition_with_universal_quantifier {α : Type} (p
2   ↪ : α → Prop) : ∀ a : α, p a :=
3 begin
4 intro x0,
5
6 a_proof_of_p(x0)
7 end

```

If the goal is the form $\forall a_1 : \alpha_1, \forall a_2 : \alpha_2, \dots, \forall a_n : \alpha_n, p \ a_1 \ a_2 \ \dots \ a_n$ can be proved using `intros a1 a2 ... an` as an abbreviation of `intro a1, intro a2, ..., intro an`.

2.2.7 prove a proposition with \exists

A proposition of the form $\exists a : \alpha, p(a)$ where α is a type and $p : \alpha \rightarrow \text{Prop}$ can be proved by `use x_0` . This will convert the goal to proving $p(x_0)$.

```
1 theorem how_to_proposition_with_universal_quantifier { $\alpha$  : Type} ( $p$ 
   $\hookrightarrow$  :  $\alpha \rightarrow \text{Prop}$ ) :  $\exists a : \alpha, p\ a :=$ 
2 begin
3   a_construction_of_ $x_0$ 
4
5   use  $x_0$ ,
6
7   a_proof_of_ $p(x_0)$ 
8 end
```

2.3 An example

To illustrate the above syntax and patterns, an example is presented here of defining mean value of two real numbers and proving some basic properties thereof.

```
1 import data.real.basic
2 import tactic
3
4 noncomputable theory
5 open_locale classical
6
7 def mean ( $x\ y : \mathbb{R}$ ) :  $\mathbb{R} := (x + y) / 2$ 
8
9 theorem min_le_mean :  $\forall x\ y : \mathbb{R}, \min x\ y \leq (\text{mean } x\ y) :=$ 
10 begin
11   intros  $x\ y$ ,
12   have ineq1 :  $\min x\ y \leq x := \text{min\_le\_left } x\ y$ ,
13   have ineq2 :  $\min x\ y \leq y := \text{min\_le\_right } x\ y$ ,
14
15   unfold mean, rw le_div_iff, rw mul_two,
16   apply add_le_add,
17   exact ineq1, exact ineq2,
18
19   linarith,
20 end
21
22 theorem mean_le_max :  $\forall x\ y : \mathbb{R}, (\text{mean } x\ y) \leq \max x\ y :=$ 
23 begin
24   intros  $x\ y$ ,
25   have ineq1 :  $x \leq \max x\ y := \text{le\_max\_left } x\ y$ ,
26   have ineq2 :  $y \leq \max x\ y := \text{le\_max\_right } x\ y$ ,
27
28   unfold mean, rw div_le_iff, rw mul_two,
29   apply add_le_add,
30   exact ineq1, exact ineq2,
31
32   linarith,
```

```

33 end
34
35 theorem a_number_in_between :
36    $\forall x y : \mathbb{R}, x \leq y \rightarrow \exists z : \mathbb{R}, x \leq z \wedge z \leq y :=$ 
37 begin
38   intros x y hxy,
39   have ineq1 := min_le_mean x y,
40   have ineq2 := mean_le_max x y,
41   have min_eq_x := min_eq_left hxy,
42   have max_eq_y := max_eq_right hxy,
43   use mean x y,
44   split,
45
46   { conv_lhs {rw <-min_eq_x}, exact ineq1, },
47   { conv_rhs {rw <-max_eq_y}, exact ineq2, },
48 end

```

Line 1 makes basic properties of real available to use and line 2 makes all the tactics we discussed amongst other more advanced tactics available to use. We add line 4 so that `lean` would ignore the issue of computability and line 5 so that we can use proof by contradiction².

We define the mean value of two real numbers on line 7. Then `mean`³ has the type $\mathbb{R} \rightarrow \mathbb{R} \rightarrow \mathbb{R}$, `mean 1` has the type $\mathbb{R} \rightarrow \mathbb{R}$ and `mean 1 2` has the type \mathbb{R} .

We can introduce and prove theorems about `mean` stating that the mean value of two numbers is greater than or equal to the minimum of the two numbers but less than the maximum. This is from line 9 to line 33 where

- `min_le_left` is a proof of the proposition $\forall(x y : \alpha), \min(x, y) \leq x$ where α is an implicit argument with a linear order. In this case, `Lean` infers from context that α is \mathbb{R} . Thus `min_le_left x y` is a proof of $\min x y \leq x$.
- `min_le_right` is a proof of the proposition $\forall(x y : \alpha), \min(x, y) \leq y$ In this case, `min_le_right x y` is a proof of $\min x y \leq y$.
- Similarly, `le_max_left` is a proof of the proposition $\forall(x y : \alpha), x \leq \max(x, y)$ where α is an implicit argument with a linear order. In this case, `le_max_left` is a proof of $x \leq \max x y$.
- Similarly, `le_max_right` is a proof of the proposition $\forall(x y : \alpha), y \leq \max(x, y)$ where α is an implicit argument with a linear order. In this case, `le_max_right` is a proof of $y \leq \max x y$.
- `le_div_iff` is a proof that $0 < c \rightarrow (a \leq \frac{b}{c} \iff a \times c \leq b)$ where a, b, c are elements of a type with a linear ordered field structure. So by

²`Lean` by default use constructivism where $\neg\neg p \implies p$ is not an axiom of deduction. Thus the law of excluded middle is not by default a tautology.

³`mean` is not a function $\mathbb{R}^2 \rightarrow \mathbb{R}$ but a function $\mathbb{R} \rightarrow \text{Func}(\mathbb{R}, \mathbb{R})$. This is called currying.

`rw le_div_iff`, the goal would change from $\min x y \leq (x + y) / 2$ to $\min x y * 2 \leq x + y$. Since `le_div_iff` requires the assumption that $0 < c$, a new goal to prove that $0 < 2$ is created after the original goal. This goal is proved by the final `linarith`.

- `div_le_iff` is proof that $0 < b \implies (\frac{a}{b} \leq c \iff a \leq c \times b)$ where a, b, c are elements of a type with a linear ordered field structure. So by `rw div_le_iff` the goal would change from $(x + y) / 2 \leq \max x y$ to $x + y \leq \max x y * 2$. Since `div_le_iff` requires the assumption that $0 < b$, a new goal to prove $0 < 2$ is created after the original goal. This goal is proved by the final `linarith`.
- `mul_two` proves the lemma that $\forall n : \alpha, n \times 2 = n + n$ where α is a semiring. Thus `rw mul_two` would change the goal of proving $\min x y * 2 \leq x + y$ ($x + y \leq \max x y * 2$ resp.) to $\min x y + \min x y \leq x + y$ ($x + y \leq \max x y + \max x y$ resp.).
- `add_le_add` proves the lemma that $a \leq b \rightarrow c \leq d \rightarrow a + c \leq b + d$ where a, b, c and d are elements of an ordered additive commutative monoid. Since the goal now is to prove $\min x y + \min x y \leq x + y$, by apply `add_le_add`, goal will be replaced by two goals of proving $\min x y \leq x$ and $\min x y \leq y$. These are *exactly* `ineq1` and `ineq2`.

Chapter 3

Formalisation using Lean

Logistics of the formalisation

There are five main files in this project where

1. `small_things.lean` formalised results about the trivial embedding of $\mathbb{Z}[X] \subset \mathbb{R}[X]$ and manipulation of inequality in real numbers common to all three parts;
2. `algebraic_over_Z.lean` formalised countability of algebraic numbers with help of Schröder-Berstein theorem.
3. `liouville.lean` formalised Liouville's theorem and a construction of a Liouville's number;
4. `e_trans_helpers2.lean` formalised some results about differentiation and integration. Especially the formalisations of

$$\frac{d^n}{dx^n} uv = \sum_{i=0}^n \binom{n}{i} \frac{d^i u}{dx^i} \frac{d^{n-i} v}{dx^{n-i}}$$

where u and v are differentiable function from \mathbb{R} to \mathbb{R} and

$$\int_0^t e^{t-x} f(x) dx = e^t \sum_{i=0}^m f^{(i)}(0) - \sum_{i=0}^m f^{(i)}(t)$$

where $f(X) \in \mathbb{Z}[X]$;

5. `e_transcendental.lean` formalised transcendence of e by assuming the algebraicity of e which resulted in two contradictory bounds using the results from `e_trans_helpers2.lean`.

3.1 Countability argument

The main caveat in this part is the internal specification of `mathlib`. A real number x in `Lean` is algebraic over \mathbb{Z} if and only if there exists a nonzero polynomial $p(X) \in \mathbb{Z}[X]$ such that p is in the kernel of the unique \mathbb{Z} -algebra homomorphism $\mathbb{Z}[X] \rightarrow \mathbb{R}$ given by $X \mapsto x$.

```
1  ∃ (p : ℤ[X]), p ≠ 0 ∧ ↑(polynomial.aeval ℤ ℝ x) p = 0
```

Here the \mathbb{Z} -algebra homomorphism is `polynomial.aeval ℤ ℝ x`. `↑` is to convert the homomorphism to a function applicable to `p`. The reason that a conversion is necessary is because an algebra homomorphism contains more information than a function, it is a structure containing the map and other fields containing (proofs of) the properties of algebra homomorphism. However in polynomial library of `mathlib`, the definition of root is as following :

```
1  def is_root (p : polynomial R) (a : R) : Prop := p.eval a = 0
```

Thus the first part of this formalisation is to unify the two evaluation methods – denote ι_x to be the unique \mathbb{Z} -algebra homomorphism $\iota_x : \mathbb{Z}[X] \rightarrow \mathbb{R}$ given by $X \mapsto x$ then for all polynomial $p(X) \in \mathbb{Z}[X]$ and for all $x \in \mathbb{R}$, $\text{eval}_p(x) = \iota_x p$:

```
1  -- the trivial embedding ℤ[X] ⊆ ℝ[X]
2  def poly_int_to_poly_real (p : ℤ[X]) : polynomial ℝ :=
3    ↪ polynomial.map Zembℝ p
4
5  def poly_int_to_poly_real_wd (p : ℤ[X]) :=
6    ∀ x : ℝ, polynomial.aeval ℤ ℝ x p = (poly_int_to_poly_real
7      ↪ p).eval x
8
9  theorem poly_int_to_poly_real_well_defined
10    (x : ℝ) (p : ℤ[X]) : poly_int_to_poly_real_wd p :=
11    begin
12      proof_omitted
13    end
```

Source Code 3.1: unifying two ways of evaluation

For any $p \in \mathbb{Z}[X]$, we can define the set of roots to be $\{x \in \mathbb{R} \mid \text{eval}_p(x) = 0\}$ or $\{x \in \mathbb{R} \mid \iota_x p = 0\}$ where the former is builtin as `↑(poly_int_to_poly_real p).roots`¹ and the latter is defined as line 1 in source code 3.2. By line 7 in source code 3.1, the two sets must be equal, hence they have finite cardinality for a none-zero polynomial:

¹`_.roots` in fact has type `finset ℝ`. The type `finset` is a `set` with a proof of finite cardinality. Here `↑` is used to convert a `finset` to `set` by discarding the proof of finite cardinality.

```

1 def roots_real (p :  $\mathbb{Z}[X]$ ) : set  $\mathbb{R}$  :=
2   {x | polynomial.aeval  $\mathbb{Z}$   $\mathbb{R}$  x p}
3
4 theorem roots_real_eq_roots (p :  $\mathbb{Z}[X]$ ) (hp : p  $\neq$  0) :
5   roots_real p =  $\uparrow$ (poly_int_to_poly_real p).roots :=
6 begin
7   proof_omitted
8 end
9
10 theorem roots_finite (p :  $\mathbb{Z}[X]$ ) (hp : p  $\neq$  0) :
11   set.finite (roots_real p) :=
12 begin
13   proof_omitted
14 end

```

Source Code 3.2: two ways of defining roots

We define the set of all algebraic numbers over \mathbb{Z} to be

```

1 def algebraic_set : set  $\mathbb{R}$  := {x | is_algebraic  $\mathbb{Z}$  x}

```

To investigate the countability of `algebraic_set`, we compare it with

$$\bigcup_{n \in \mathbb{N}} \bigcup_{\substack{p \in \mathbb{Z}[X] \\ p \neq 0 \\ \deg p < n+1}} \{x \in \mathbb{R} \mid \iota_x p = 0\}. \quad (3.1)$$

To this end, we introduce some types of interest:

```

1 notation `int_n` n := fin n  $\rightarrow$   $\mathbb{Z}$ 
2 notation `nat_n` n := fin n  $\rightarrow$   $\mathbb{N}$ 
3 notation `poly_n` n := {p :  $\mathbb{Z}[X]$  // p  $\neq$  0  $\wedge$  p.nat_degree < n}
4 notation `int_n` n := {f : fin n  $\rightarrow$   $\mathbb{Z}$  // f  $\neq$  0}
5 notation `int` := {r :  $\mathbb{Z}$  // r  $\neq$  0}

```

where $\langle m, hm \rangle$ is an element of `fin n` if and only if m is a natural number and hm is a proof of $m < n$. Then `fin n` is the type of only n elements. Thus

- `int_n n` is \mathbb{Z}^n ;
- `int_n' n` is $\mathbb{Z}^n - \{(0, \dots, 0)\}$;
- `int'` is $\mathbb{Z} - \{0\}$;
- `nat_n n` is \mathbb{N}^n ;
- `poly_n' n` is the type of non-zero integer polynomials with degree less than n .

Then $\mathbb{Z} \simeq \mathbb{Z} - \{0\}$ by the bijective function $s : \mathbb{Z} \rightarrow \mathbb{Z} - \{0\}$:

$$m \mapsto \begin{cases} m & \text{if } m < 0 \\ m + 1 & \text{if } m \geq 0 \end{cases}$$

```

1 def strange_fun : ℤ → int' :=
2   λ m, if h : m < 0
3     then ⟨m, by linarith⟩
4     else ⟨m + 1, by linarith⟩
5
6 theorem strange_fun_inj :
7   function.injective strange_fun :=
8   begin
9     proof_omitted
10  end
11
12 theorem strange_fun_sur :
13   function.surjective strange_fun :=
14   begin
15     proof_omitted
16  end
17
18 theorem int_equiv_int' : ℤ ≃ int' :=
19   begin
20     apply equiv.of_bijective strange_fun,
21     split,
22     exact strange_fun_inj,
23     exact strange_fun_sur,
24   end

```

Source Code 3.3: $\mathbb{Z} \simeq \mathbb{Z} - \{0\}$

Then we prove that for all non-zero $n : \mathbb{N}$, non-zero integer polynomials of degree less than n bijectively correspond to $\mathbb{Z}^n - \{(0, \dots, 0)\}$ via the function: $p \mapsto \mathbf{z}$ where the i -th coordinate of \mathbf{z} is the i -th coefficient of p .

```

1 def identify (n : nat) : (poly_n' n) → (int_n' n) :=
2   λ p, ⟨λ m, p.1.coeff m.1, a_proof_z_is_not_zero⟩
3
4 theorem sur_identify_n (n : nat) (hn : n ≠ 0) :
5   function.surjective (identify n) :=
6   begin
7     proof_omitted
8   end
9
10 theorem inj_identify_n (n : nat) (hn : n ≠ 0) :
11   function.injective (identify n) :=
12   begin
13     proof_omitted
14   end
15
16 theorem poly_n'_equiv_int_n' (n : nat) :
17   (poly_n' n.succ) ≃ (int_n' n.succ) :=
18   begin

```

```

19   apply equiv.of_bijective (identify n.succ),
20   split,
21   exact inj_identify_n n.succ (nat.succ_ne_zero n),
22   exact sur_identify_n n.succ (nat.succ_ne_zero n),
23 end

```

†: $n.succ$ means $n + 1$.

Source Code 3.4: non-zero integer polynomials with degree less than n has the same cardinality as $\mathbb{Z}^n - \{(0, \dots, 0)\}$

Then we define two injective functions $F : \mathbb{Z}^{n+1} \rightarrow \mathbb{Z}^{n+1} - \{(0, \dots, 0)\}$ and $G : \mathbb{Z}^{n+1} - \{(0, \dots, 0)\} \rightarrow \mathbb{Z}^{n+1}$ by:

$$F(m_0, \dots, m_n) = (s(m_0), \dots, s(m_n))$$

$$G(m_0, \dots, m_n) = (m_0, \dots, m_n)$$

where $s : \mathbb{Z} \rightarrow \mathbb{Z} - \{0\}$ is defined previously. By Schröder-Berstein theorem, there is then a bijection $\mathbb{Z}^{n+1} \rightarrow \mathbb{Z}^{n+1} - \{(0, \dots, 0)\}$ and thus $\mathbb{Z}^{n+1} \simeq \mathbb{Z}^{n+1} - \{(0, \dots, 0)\}$:

```

1  def F (n : nat) : (int_n n.succ) → (int_n' n.succ) :=
2    λ f, ⟨λ m, (strange_fun (f m)).1,
3      a_proof_of_(s(m_0), ..., s(m_n))_non-zero⟩
4  theorem F_inj (n : nat) : function.injective (F n) :=
5  begin
6    proof_omitted
7  end
8
9  def G (n : nat) : (int_n' n.succ) → (int_n n.succ) :=
10   λ f m, (f.1 m)
11  theorem G_inj (n : nat) : function.injective (G n) :=
12  begin
13    proof_omitted
14  end
15
16  theorem int_n_equiv_int_n' (n : nat) :
17    (int_n n.succ) ≃ int_n' n.succ :=
18  begin
19    choose B HB using function.embedding.schroeder_bernstein (F_inj
20      ↪ n) (G_inj n),
21    apply equiv.of_bijective B HB,
22  end

```

Source Code 3.5: $\mathbb{Z}^{n+1} \simeq \mathbb{Z}^{n+1} - \{(0, \dots, 0)\}$

For any natural number $n \geq 1$, we then construct two injective function $f_n : \mathbb{Z}^{n+2} \rightarrow \mathbb{Z}^{n+1} \times \mathbb{Z}$ and $g_n : \mathbb{Z}^{n+1} \times \mathbb{Z} \rightarrow \mathbb{Z}^{n+2}$:

$$f_n((m_0, \dots, m_{n+1})) = ((m_0, \dots, m_n), m_{n+1})$$

$$g_n(((m_0, \dots, m_n), m_{n+1})) = (m_0, \dots, m_{n+1})$$

Then by Schröder-Berstein theorem $\mathbb{Z}^{n+2} \simeq \mathbb{Z}^{n+1} \times \mathbb{Z}$ for all $n \geq 1$.


```

1 def fn (n : nat) :
2   (int_n n.succ.succ) → (int_n n.succ) × ℤ := λ r,
3   ⟨λ m, r (⟨m.1, nat.lt_trans m.2 (nat.lt_succ_self n.succ))),
4     r (⟨n.succ, nat.lt_succ_self n.succ⟩)⟩
5 theorem fn_inj (n : ℕ) : function.injective (fn n) :=
6 begin
7   proof_omitted
8 end
9
10 def gn (n : nat) : (int_n n.succ) × ℤ → (int_n n.succ.succ) := λ r
11   ↪ m,
12 begin
13   by_cases (m.1 = n.succ),
14     exact r.2,
15     exact r.1 (⟨m.1, lt_of_le_of_ne (fin.le_last m) h⟩),
16 end
17 theorem gn_inj (n : nat) : function.injective (gn n) :=
18 begin
19   proof_omitted
20 end
21
22 theorem aux_int_n (n : nat) :
23   (int_n n.succ.succ) ≃ (int_n n.succ) × ℤ :=
24 begin
25   choose B HB using function.embedding.schroeder_bernstein (fn_inj n)
26   ↪ (gn_inj n),
27   apply equiv.of_bijective B HB,
28 end

```

Source Code 3.6: $\mathbb{Z}^{n+2} \simeq \mathbb{Z}^{n+1} \times \mathbb{Z}$ for all $n \geq 1$

Now we are finally in the position of using equation 3.1 to prove the countability of all algebraic numbers. We first define the set of real roots of non-zero integer polynomials of degree less than n to be:

```

1 def algebraic_set'_n (n : ℕ) : set ℝ :=
2   ⋃ p : (poly_n' n.succ), roots_real p.1

```

Hence by taking union over all natural numbers we can obtain an equivalent definition of all algebraic number over \mathbb{Z} :

```

1 def algebraic_set' : set real :=
2   ⋃ n : ℕ, algebraic_set'_n n.succ
3
4 theorem algebraic_set'_eq_algebraic_set :
5   algebraic_set' = algebraic_set :=
6 begin
7   proof_omitted
8 end

```

We prove by induction that for any $n \in \mathbb{N}$, \mathbb{Z}^{n+1} is denumerable (i.e. countably infinite) where the base case is $\mathbb{Z}^1 \simeq \mathbb{Z}$ and the inductive step is to prove

\mathbb{Z}^{n+2} is denumerable using the denumerability of \mathbb{Z}^{n+1} . Since non-zero integer polynomials of degree less than $n + 1$ bijectively corresponds to \mathbb{Z}^{n+1} , we infer that non-zero integer polynomials of degree less than $n + 1$ are denumerable hence countable. Then the result of taking union over the countable set \mathbb{N}

$$\bigcup_{n \in \mathbb{N}} \bigcup_{\substack{p \in \mathbb{Z}[X] \\ p \neq 0 \\ \deg p < n+1}} \{x \in \mathbb{R} \mid \iota_x p = 0\}$$

is still countable. Then finally the set of all algebraic numbers over \mathbb{Z} is conclude to be countable. Since \mathbb{R} is uncountable, transcendental number must exist:

```

1  theorem int_1_equiv_int : (int_n 1)  $\simeq$   $\mathbb{Z}$  :=
2  begin
3    proof_omitted
4  end
5
6  theorem int_n_denumerable {n : nat} :
7    denumerable (int_n n.succ) :=
8  begin
9    proof_omitted
10 end
11
12 theorem poly_n'_denumerable (n : nat) :
13   denumerable (poly_n' n.succ) :=
14 begin
15   proof_omitted
16 end
17
18 theorem algebraic_set'_n_countable (n : nat) :
19   set.countable (algebraic_set'_n n) :=
20 begin
21   proof_omitted
22 end
23
24 theorem algebraic_set'_countable :
25   set.countable algebraic_set' :=
26   set.countable_Union
27     ( $\lambda$  n, algebraic_set'_n_countable n.succ)
28
29 theorem algebraic_set_countable :
30   set.countable algebraic_set :=
31 begin
32   rw  $\leftarrow$  algebraic_set'_eq_algebraic_set,
33   exact algebraic_set'_countable
34 end
35
36 theorem transcendental_number_exists :
37    $\exists$  x :  $\mathbb{R}$ , transcendental x :=
38 begin
39   proof_omitted
40 end

```

Source Code 3.7: algebraic numbers are countable, hence transcendental numbers exists.

3.2 Liouville's theorem and Liouville numbers

General theory about Liouville numbers

A Liouville number is a real number that is “almost rational”, i.e. for any $n \in \mathbb{N}$ there is a rational number² $\frac{a}{b} \in \mathbb{Q}$ such that $b > 1$ and $0 < |x - \frac{a}{b}| < \frac{1}{b^n}$.

```

1 def liouville_number (x : ℝ) :=
2   ∀ n : ℕ, ∃ a b : ℤ,
3     b > 1 ∧
4     0 < abs(x - a / b) ∧ abs(x - a / b) < 1/b^n

```

Source Code 3.8: Definition of Liouville number

We first prove a lemma about irrational roots of an integer polynomial:

Lemma 3.2.1. if f is an integer polynomial with degree $m > 1$ and α is an irrational root for $i(f)$ where $i : \mathbb{Z}[X] \rightarrow \mathbb{R}[X]$ is the trivial embedding, then there is a positive real number A such that for every rational number $\frac{a}{b}$,

$$\left| \alpha - \frac{a}{b} \right| > \frac{A}{b^m}:$$

```

1 lemma about_irrational_root (α : ℝ)
2   (hα : irrational α) (f : ℤ[X])
3   (f_deg : f.nat_degree > 1)
4   (α_root : f.eval_on_ℝ f α = 0) :
5   ∃ A : ℝ, A > 0 ∧ ∀ a b : ℤ, b > 0 → abs(α - a/b) >
    ↪ (A/b^(f.nat_degree)) :=

```

Proof. We will abuse the notation to denote f both as the integer polynomial and the real polynomial via trivial embedding.

```

6 begin
7   have f_nonzero : f ≠ 0,
8     proof_omitted
9   generalize hfℝ: f.map Zembℝ = f_ℝ,
10  have hfℝ_nonzero : f_ℝ ≠ 0,
11    proof_omitted
12  generalize hDf: f_ℝ.derivative = Df_ℝ,

```

²Without losing generality, we are always assuming, for any rational number, the denominator is a strictly positive natural number.

Since $\text{abs} \circ Df : \mathbb{R} \rightarrow \mathbb{R}$ given by $x \mapsto \left| \frac{d}{dt} \Big|_{t=x} f(t) \right|$ is a continuous function and $[\alpha - 1, \alpha + 1]$ is a non-empty compact subset of \mathbb{R} , $\text{abs} \circ Df$ attains a maximum on $[\alpha - 1, \alpha + 1]$, denote it by M . Then $M > 0$ for otherwise $M = 0$ then $Df(x) = 0$ for all $x \in [\alpha - 1, \alpha + 1]$ implying that f is constant contradicting the degree of f .

```

13   have H := is_compact.exists_forall_ge
14         a_proof_of_[α-1,α+1]_compact
15         a_proof_of_[α-1,α+1]_not_empty
16         a_proof_of_abs ∘ Df_continuous,
17
18   choose x_max hx_max using H,
19   generalize M_def: abs (Df_ℝ.eval x_max) = M,
20   have hM := hx_max.2, rw M_def at hM,
21   have M_non_zero : M ≠ 0,
22     proof_omitted
23   have M_pos : M > 0,
24     proof_omitted

```

Let us consider the smallest element B of the set $\left\{1, \frac{1}{M}\right\} \cup \{|\alpha - x| \mid f(x) = 0 \wedge x \neq \alpha\}$, then $B > 0$.

```

25   generalize roots_def : f_ℝ.roots = f_roots,
26   generalize roots'_def : f_roots.erase α = f_roots',
27   generalize roots_distance_to_α : f_roots'.image (λ x, abs (α -
28     ↪ x)) = distances,
29   generalize hdistances' : insert (1/M) (insert (1:ℝ) distances) =
30     ↪ distances',
31   have hnon_empty: distances'.nonempty,
32     proof_omitted
33   generalize hB : finset.min' distances' hnon_empty = B,
34   have allpos : ∀ x : ℝ, x ∈ distances' → x > 0,
35     proof_omitted
36   have B_pos : B > 0,
37     proof_omitted

```

Let $A = \frac{B}{2}$ then $A > B > 0$. We claim that A satisfies the lemma, i.e. $A > 0$ and for every rational number $\frac{a}{b}$, $|\alpha - a/b| > \frac{A}{b^m}$ where m is the degree of f .

```

36   generalize hA : B / 2 = A,
37   use A, split,
38   a_proof_of_A > 0

```

We proceed by assuming that there exists a rational number $\frac{a}{b}$ such that $\left| \alpha - \frac{a}{b} \right| \leq \frac{A}{b^m}$ for a contradiction. Since $b \geq 1$, we have $\left| \alpha - \frac{a}{b} \right| \leq A < B$. Then $\frac{a}{b}$ is not a root of f because otherwise $B \leq \left| \alpha - \frac{a}{b} \right|$.

```

39 by_contra absurd,
40 simp only [gt_iff_lt, classical.not_forall, not_lt,
41   ↪ classical.not_imp] at absurd,
42 choose a ha using absurd,
43 choose b hb using ha,
44 have hb2 : b ^ f.nat_degree ≥ 1,
45   proof_omitted
46 have hb21 : abs (α - a / b) ≤ A,
47   proof_omitted
48 have hb22 : abs (α - a/b) < B,
49   proof_omitted
50 have hab0 : (a/b:ℝ) ∈ set.Icc (α-1) (α+1),
51   proof_omitted
52 have hab1 : (a/b:ℝ) ≠ α,
53   proof_omitted
54 have hab2 : (a/b:ℝ) ∉ f_roots,
55   proof_omitted

```

Since $\alpha \neq \frac{a}{b}$, we can assume without losing generality that $\frac{a}{b} < \alpha$. Since $\text{eval}_f : \mathbb{R} \rightarrow \mathbb{R}$ given by $x \mapsto f(x)$ is differentiable, we can use mean value theorem to find $x_0 \in \left(\frac{a}{b}, \alpha\right)$ such that

$$\begin{aligned}
Df(x_0) &= \frac{\text{eval}_f(\alpha) - \text{eval}_f(\frac{a}{b})}{\alpha - \frac{a}{b}} \quad [\text{Mean value theorem}] \\
&= -\frac{\text{eval}_f(\frac{a}{b})}{\alpha - \frac{a}{b}} \quad [\alpha \text{ is a root of } i(f)]
\end{aligned}$$

```

55 have hab3 := ne_iff_lt_or_gt.1 hab1,
56 cases hab3,
57 have H :=
58   exists_deriv_eq_slope (λ x, f_ℝ.eval x) hab3 _ _,
59 choose x0 hx0 using H,
60 have hx0r := hx0.2,
61 rw [polynomial.deriv, hDf, ←hfℝ] at hx0r,
62 rw [f_eval_on_ℝ] at α_root, rw [α_root, hfℝ] at hx0r, simp only
   ↪ [zero_sub] at hx0r,

```

Then $|Df(x_0)| > 0$ hence $\left|\alpha - \frac{a}{b}\right| = \left|\frac{\text{eval}_f(\frac{a}{b})}{Df(x_0)}\right|$ is non-zero. Since M is the maximum of $\text{abs} \circ Df$ on $[\alpha - 1, \alpha + 1]$. We have $|Df(x_0)| \leq M$ and thus $\left|\alpha - \frac{a}{b}\right| \geq \frac{|\text{eval}_f(\frac{a}{b})|}{M}$. If we write $f(X)$ as $\sum_{j=0}^m \lambda_j X^j$ then

$$\left|\text{eval}_f\left(\frac{a}{b}\right)\right| = \left|\sum_{j=0}^m \lambda_j \frac{a^j}{b^j}\right| = \frac{1}{b^m} \left|\sum_{j=0}^m \lambda_j a^j b^{m-j}\right| \geq \frac{1}{b^m}$$

Hence we have $\left| \alpha - \frac{a}{b} \right| \geq \frac{1}{Mb^m} > \frac{A}{b^m}$. But we assumed $\left| \alpha - \frac{a}{b} \right| < \frac{A}{b^m}$ to start with, this is the desired contradiction.

```

63   have Df_x0_nonzero : Df_ℝ.eval x0 ≠ 0,
64     proof_omitted
65   have H2 : abs(α - a/b) = abs((f_ℝ.eval (a/b:ℝ)) / (Df_ℝ.eval
66     ↪ x0)),
67     proof_omitted
68   have ineq' : polynomial.eval (a/b:ℝ) (polynomial.map Zembℝ f) ≠
69     ↪ 0,
70     proof_omitted
71   have ineq : abs (α - a/b) ≥ 1/(M*b^(f.nat_degree)),
72     proof_omitted
73   have ineq2 : 1/(M*b^(f.nat_degree)) > A / (b^f.nat_degree),
74     proof_omitted
75   have ineq3 : abs (α - a / b) > A / b ^ f.nat_degree,
76     proof_omitted
77   have ineq4 : abs (α - a / b) > abs (α - a / b),
78     proof_omitted
79   linarith,
80   We omit the proof of differentiability of eval_f, continuity of abs ∘ Df and the case when
81     ↪ a/b > α
82   rest_omitted
end

```

□

We then prove the irrationality of Liouville numbers.

Lemma 3.2.2. Every Liouville number is irrational

```

1 lemma liouville_numbers_irrational:
2   ∀ (x : ℝ), (liouville_number x) → irrational x :=

```

Proof. Let x be an arbitrary Liouville number and suppose for a contradiction that $x = \frac{a}{b}$, write $n = b + 1$ then $2^{n-1} > b$.

```

3 begin
4   intros x liouville_x a b hb rid,
5   replace rid : x = ↑a / ↑b, linarith,
6   generalize hn : b.nat_abs + 1 = n,
7   have b_ineq : 2 ^ (n-1) > b,
8     proof_omitted

```

Since $x = \frac{a}{b}$ is a Liouville number we can find a rational number $\frac{p}{q}$ such that $q > 1$ and $0 < \left| \frac{a}{b} - \frac{p}{q} \right| < \frac{1}{q^n}$ or equivalently $0 < \frac{|aq - bp|}{bq} < \frac{1}{q^n}$. If $aq - bp = 0$, then $0 < 0$ is the desired contradiction.

```

9   choose p hp using liouville_x n,
10  choose q hq using hp, rw rid at hq,
11  have q_pos : q > 0 := by linarith,
12  rw [div_sub_div at hq, abs_div at hq],
13
14  by_cases (abs (a*q-b*p:ℝ) = 0),
15  intermediate_step_omitted
16  linarith,

```

If $aq - bp \neq 0$ then $\frac{1}{bq} \leq \frac{|aq - bp|}{bq}$. But we also have $b < 2^{n-1}$ and $2^{n-1}q \leq q^n$ because $q \geq 2$. Hence $bq < q^n$, then $\frac{|aq - bp|}{bq} > \frac{1}{q^n}$. This is the desired contradiction.

```

17  have ineq4 : 1 / (b * q : ℝ) ≤ (abs(a * q - b * p:ℝ)) / (b * q),
18    proof_omitted
19  have b_ineq'' : (b*q:ℝ) < (2:ℝ)^(n-1)*(q:ℝ),
20    proof_omitted
21  have q_ineq3 : 2 ^ (n - 1) * q ≤ q ^ n,
22    proof_omitted
23  have b_ineq2 : b * q < q ^ n, linarith,
24  have rid'' :
25    abs (a*q-b*p:ℝ) / (b*q:ℝ) > 1/q^n,
26    proof_omitted,
27
28  have hq22 := hq2.2,
29  linarith,
30
31  We manipulated inequalities involving division and multiplication hence we need to prove
32  ↪ several things to be positive.
33  proofs_omitted
34  end

```

□

With the above lemmas, we are ready to prove the transcendence of Liouville numbers.

Theorem 3.2.1. Every Liouville number is transcendental

```

1  theorem liouville_numbers_transcendental : ∀ x : ℝ,
   ↪ liouville_number x → transcendental x :=

```

Proof. Let x be an arbitrary Liouville number then x is irrational. Assume for a contradiction that x is algebraic, let f be the non-zero integer polynomial admitting x as root as a \mathbb{R} -polynomial. Then since x is irrational, f has degree at least 2.

```

2 begin
3   intros x liouville_x,
4   have irrational_x : irrational x := liouville_numbers_irrational
    ↪ x liouville_x,
5   intros rid, rw is_algebraic at rid,
6   choose f hf using rid,
7   have f_deg : f.nat_degree > 1,
8   proof_omitted

```

By using lemma 3.2.1 we can find a real number $A > 0$ such that for any rational number $\frac{p}{q}$, $\left|x - \frac{p}{q}\right| > \frac{A}{q^n}$ where n is the degree of f .

```

9   have about_root : f_eval_on_ℝ f x = 0,
10   proof_omitted
11   choose A hA using about_irrational_root x irrational_x f f_deg
    ↪ about_root,
12   have A_pos := hA.1,

```

Since \mathbb{R} is an Archimedean field, we can find an $r \in \mathbb{N}$ such that $\frac{1}{A} \leq 2^r$. Then consider $m := r + n$. Since x is a Liouville number, there is a rational number $\frac{a}{b}$ such that $b > 1$ and $0 < \left|x - \frac{a}{b}\right| < \frac{1}{b^m} = \frac{1}{b^r b^n}$.

```

13   have exists_r := pow_big_enough A A_pos,
14   choose r hr using exists_r,
15   have hr' : 1/(2^r) ≤ A,
16   proof_omitted
17   generalize hm : r + f.nat_degree = m,
18   replace liouville_x := liouville_x m,
19   choose a ha using liouville_x,
20   choose b hb using ha,
21
22   have ineq : abs (x - a/b : ℝ) < 1/((b : ℝ)^r) * (1/(b : ℝ)^f.nat_degree),
23   proof_omitted

```

Since $b \geq 2$, we have $\frac{1}{b^r} \leq \frac{1}{2^r} \leq A$. Thus $\left|x - \frac{a}{b}\right| < \frac{1}{b^r b^n} \leq \frac{A}{b^n}$. This contradicts lemma 3.2.1 stating that $\left|x - \frac{a}{b}\right| > \frac{A}{q^n}$.

```

24   have ineq3 : 1/(b : ℝ)^r ≤ A,
25   proof_omitted,
26   have ineq4 : 1 / (b : ℝ)^r * (1/(b : ℝ)^f.nat_degree) ≤ (A /
    ↪ (b : ℝ)^f.nat_degree),
27   proof_omitted
28   have ineq5 : abs (x - a/b : ℝ) < A/(b : ℝ)^f.nat_degree, linarith,
29   have rid := hA.2 a b _, linarith, linarith,
30   end

```

□

Construction of a Liouville number

Knowing that all Liouville numbers are transcendental, we now focus on constructing a Liouville number

$$\alpha = \sum_{j=0}^{\infty} \frac{1}{10^{j!}}$$

hence obtain a concrete example of transcendental number α .

Lemma 3.2.3. α converges.

Proof. Since for any $n \in \mathbb{N}$ we have $\frac{1}{10^n}$ is none-negative and $\frac{1}{10^n} \leq \frac{1}{10^{n!}}$, we can use comparison test against $\sum_{j=0}^{\infty} \frac{1}{10^j}$ to deduce the convergence of α .

```

1 def ten_pow_n_fact_inverse (n : ℕ) : ℝ :=
2   (1/10)^n.fact
3 def ten_pow_n_inverse (n : ℕ) : ℝ :=
4   (1/10)^n
5
6 lemma summable_ten_pow_n_fact_inverse : summable
7   ↪ ten_pow_n_fact_inverse :=
8   begin
9     exact @summable_of_nonneg_of_le _
10      ten_pow_n_inverse
11      ten_pow_n_fact_inverse
12      a_proof_of_1_10^n ≥ 0
13      a_proof_of_1_10^n ≤ 1/10^n!
14      a_proof_of_∑_{j=0}^∞ 1/10^j converges,
15
16 end
17
18 def α := ∑' n, ten_pow_n_fact_inverse n

```

†: In Lean, \sum' is to indicate infinite sum while \sum is for finite sum. \square

Lemma 3.2.4. For every $k \in \mathbb{N}$, there exists some $p_k \in \mathbb{N}$ such that

$$\sum_{j=0}^k \frac{1}{j^{k!}} = \frac{p_k}{10^{k!}}$$

```

1 notation `α_k` k := ∑ ii in finset.range(k+1),
2   ↪ ten_pow_n_fact_inverse ii
3 notation `α_k_rest` k :=

```

```

4   ∑ ii, ten_pow_n_fact_inverse (ii+(k+1))
5
6   theorem α_k_rat (k:ℕ) :
7   ∃ (p:ℕ), α_k k = (p:ℝ)/((10:ℝ)^k.fact) :=

```

Proof. We prove by induction on k . For $k = 0$, the zeroth partial sum is $\frac{1}{10^0!} = \frac{1}{10}$. Thus we can pick $p_0 = 1$.

```

8   begin
9     induction k with k IH,
10
11     simp only [ten_pow_n_fact_inverse, pow_one, finset.sum_singleton,
12               ↪ finset.range_one, nat.fact_zero],
13     use 1, norm_cast,

```

Assuming that $\sum_{j=0}^k \frac{1}{10^j!} = \frac{p_k}{10^{k!}}$, let $m := 10^{(k+1)!-k!}$, then we can set $p_{k+1} := p_k m + 1$ then

$$\sum_{j=0}^{k+1} \frac{1}{10^j!} = \frac{p_k}{10^{k!}} + \frac{1}{10^{(k+1)!}} = \frac{p_k m + 1}{10^{(k+1)!}} = \frac{p_{k+1}}{10^{(k+1)!}}$$

```

13   choose pk hk using IH,
14   rw α_k at hk ⊢,
15   generalize hm : 10^((k+1).fact - k.fact) = m,
16   generalize hp : pk * m + 1 = p,
17   use p,
18   proof_omitted
19 end

```

† : In line 1 and 4 above, we use `ii` as indexing variable is to avoid clashes.

‡ : `finset.range n` ranges over $\{0, \dots, n-1\}$. \square

Theorem 3.2.2. α is a Liouville number

```

1 theorem liouville_α : liouville_number α :=

```

Proof. We need to prove that for an arbitrary $n \in \mathbb{N}$, there exists a rational number $\frac{p(n)}{q(n)}$ such that $p(n) > 1$ and $0 < \left| \alpha - \frac{p(n)}{q(n)} \right| < \frac{1}{q(n)^n}$. By lemma 3.2.4 We know that for some $p \in \mathbb{N}$,

$$\alpha = \sum_{j=0}^n \frac{1}{10^j!} + \sum_{j=0}^{\infty} \frac{1}{10^{(j+n+1)!}} = \frac{p}{10^{n!}} + \sum_{j=0}^{\infty} \frac{1}{10^{(j+n+1)!}}.$$

We take $p(n)$ to be p and $q(n)$ to be $10^{n!}$. Then $10^{n!} > 1$, thus it suffices to prove $0 < \left| \sum_{j=0}^{\infty} \frac{1}{10^{(j+n+1)!}} \right| < \left(\frac{1}{10^{n!}} \right)^n$

```

2 begin
3   intro n,
4   have lemma1 :=  $\alpha\_k\_rat$  n,
5   have lemma2 : ( $\alpha\_k\_rest$  n) =  $\alpha - \alpha\_k$  n,
6     proof_omitted
7   choose p hp using lemma1,
8   use p, use  $10^{(n.fact)}$ ,
9   suffices :  $0 < \text{abs } (\alpha\_k\_rest \text{ n}) \wedge$ 
10      $\text{abs } (\alpha\_k\_rest \text{ n}) < 1/(10^{n.fact})^n$ ,
11     split,
12     a_proof_of_ $10^{n!} > 1$ ,
13     tidy,
14     split,

```

Since each summand is strictly positive, $\left| \sum_{j=0}^{\infty} \frac{1}{10^{(j+n+1)!}} \right| = \sum_{j=0}^{\infty} \frac{1}{10^{(j+n+1)!}} > 0$. Then we prove $\left| \sum_{j=0}^{\infty} \frac{1}{10^{(j+n+1)!}} \right| < \left(\frac{1}{10^{n!}} \right)^n$, or equivalently $\sum_{j=0}^{\infty} \frac{1}{10^{(j+n+1)!}} < \left(\frac{1}{10^{n!}} \right)^n$ instead. Because for all $j \in \mathbb{N}$, $10^j \times 10^{(n+1)!} \leq 10^{(j+(n+1))!}$, we have

$$\begin{aligned} \sum_{j=0}^{\infty} \frac{1}{10^{(j+(n+1))!}} &\leq \sum_{j=0}^{\infty} \left(\frac{1}{10^j} \frac{1}{10^{(n+1)!}} \right) = \frac{1}{10^{(n+1)!}} \sum_{j=0}^{\infty} \frac{1}{10^j} \\ &= \frac{10}{9} \frac{1}{10^{(n+1)!}} < \frac{2}{10^{(n+1)!}} < \left(\frac{1}{10^{n!}} \right)^n \end{aligned}$$

```

15 rw [ $\alpha\_k\_rest$ , abs_of_pos ( $\alpha\_k\_rest\_pos$  n)],
16
17 have ineq2 :
18    $(\sum_{j:\mathbb{N}} (j:\mathbb{N}), \text{ten\_pow\_n\_fact\_inverse } (j+(n+1))) \leq$ 
19    $(\sum_{i:\mathbb{N}} (i:\mathbb{N}), (1/10:\mathbb{R})^i * (1/10:\mathbb{R})^{(n+1).fact})$ ,
20   proof_omitted
21 have ineq3 :
22    $(\sum_{i:\mathbb{N}} (i:\mathbb{N}), (1/10:\mathbb{R})^i * (1/10:\mathbb{R})^{(n.fact*n.succ)}) \leq$ 
23    $(2/10^{n.succ.fact}:\mathbb{R})$ ,
24   proof_omitted
25 have ineq4 :  $(2 / 10 ^ (n.fact*n.succ):\mathbb{R}) <$ 
26    $(1/((10:\mathbb{R})^{n.fact})^n)$ ,
27   proof_omitted,
28 have ineq5 :

```

```

27   (∑ (j : ℕ), ten_pow_n_fact_inverse (j+(n+1))) <
    ↪ (1/((10:ℝ)^n.fact)^n),
28   proof_omitted
29   tidy,
30 end

```

□

The transcendence of α follows immediately from theorem 3.2.1 and theorem 3.2.2.

Corollary 3.2.1. α is a transcendental number.

```

1 theorem transcendental_α : transcendental α :=
  ↪ liouville_numbers_transcendental α liouville_α

```

3.3 Hermite's theorem

Throughout this section f will be an integer polynomial with degree d , and t is a none-negative real number.

Definition 3.3.1. we define

$$I(f, t) := \int_0^t e^{t-x} \text{eval}_f(x) dx$$

```

1 def II (f : ℤ[X]) (t : ℝ) (ht : t ≥ 0) : ℝ :=
2   ∫ x in set.Icc 0 t, real.exp(t-x)*(f_eval_on_ℝ f x)

```

If $f(X) = \sum_{j=0}^d \lambda_j X^j$, we define $\bar{f}(X) := \sum_{j=0}^d |\lambda_j| X^j$

```

1 def f_bar (f : ℤ[X]) : ℤ[X] :=
2   { support      := f.support,
3     to_fun       := λ n, abs (f.coeff n),
4     mem_support_to_fun := proof_omitted }

```

†: In **Lean**, an integer polynomial is a function $\mathbb{N} \rightarrow \mathbb{Z}$ with finite support such that for any $n \in \mathbb{N}$ the value of the said function at n is not zero if and only if n is in the support of the said function. Thus to define \bar{f} , not only need we to specify the support and the function, a proof of n -th coefficient being non-zero if and only if n being in the support is needed as well.

Let us estimate an upper bound for $|I(f, t)|$ using \bar{f} .

Lemma 3.3.1. If $x \in [0, t]$, then $|\text{eval}_f(x)| \leq \text{eval}_{\bar{f}}(t)$

```

1 lemma f_bar_ineq (f : ℤ[X]) (t : ℝ) (ht : t ≥ 0) :
2   ∀ x ∈ set.Icc 0 t, abs (f_eval_on_ℝ f x) ≤ f_eval_on_ℝ (f_bar f)
   ↪ t :=

```

Proof. If we write $f(X) = \sum_{j=0}^d \lambda_j X^j$, then for any $x \in [0, t]$, we have $|\text{eval}_f(x)| =$

$$\left| \sum_{j=0}^d \lambda_j x^j \right| \leq \sum_{j=0}^d |\lambda_j x^j|.$$

```

3 intros x hx,
4 have lhs : f_eval_on_ℝ f x = ∑ i in f.support, (f.coeff i : ℝ) *
   ↪ x ^ i,
   proof_omitted
5 rw lhs,
6
7
8 have ineq1 : abs (∑ (i : ℕ) in f.support, (f.coeff i : ℝ) * x ^ i)
   ↪ ≤ ∑ i in f.support, (abs (f.coeff i : ℝ) * (x ^ i)),
   proof_omitted
9

```

On the right hand side, $\text{eval}_{\bar{f}}(t) = \sum_{j=0}^d |\lambda_j| t^j$. We conclude by noting that for any $n \in \mathbb{N}$, $x^n \leq t^n$.

```

10 have rhs : f_eval_on_ℝ (f_bar f) t = ∑ i in (f_bar f).support,
   ↪ abs (f.coeff i : ℝ) * t ^ i,
   proof_omitted
11 rw rhs,
12
13
14 have ineq2 : ∑ (i : ℕ) in f.support, abs (f.coeff i : ℝ) * x ^ i ≤
   ↪ ∑ i in (f_bar f).support, abs (f.coeff i : ℝ) * t ^ i,
   {
15     suffices : x ^ n ≤ t ^ n,
16     proof_omitted
17   },
18 exact le_trans ineq1 ineq2,
19

```

□

Theorem 3.3.1.

$$|I(f, t)| \leq t e^t \text{eval}_{\bar{f}}(t)$$

```

1 theorem abs_II_le2 (f : ℤ[X]) (t : ℝ) (ht : t ≥ 0) :
2   abs (II f t ht) ≤ t * t.exp * (f_eval_on_ℝ (f_bar f) t)

```

Proof.

$$\begin{aligned} |I(f, t)| &= \left| \int_0^t e^{t-x} \text{eval}_f(x) dx \right| \\ &\leq \int_0^t |e^{t-x} \text{eval}_f(x)| dx \\ &\leq t e^t \text{eval}_{\bar{f}}(t) \end{aligned}$$

where the last inequality is due to $e^{t-x} \leq e^t$ for all $x \in [0, t]$ and lemma 3.3.1.

```

3 begin
4   have ineq1 :
5     abs (II f t ht) ≤ ∫ (x : ℝ) in set.Icc 0 t, abs ((t-x).exp *
6       ↪ f_eval_on_ℝ f x),
7     proof_omitted
8   have ineq2 :
9     (∫ (x : ℝ) in set.Icc 0 t,
10      abs ((t-x).exp * f_eval_on_ℝ f x)) ≤
11      t * t.exp * f_eval_on_ℝ (f_bar f) t,
12      proof_omitted
13   exact le_trans ineq1 ineq2,
end

```

□

Lemma 3.3.2.

$$I(f, t) := \int_0^t e^{t-x} \text{eval}_f(x) dx = e^t \text{eval}_f(0) - \text{eval}_f(t) + I(f', t)$$

```

1 lemma II_integrate_by_part
2   (f : ℤ[X]) (t : ℝ) (ht : t ≥ 0) :
3   (II f t ht) = (real.exp t) * (f_eval_on_ℝ f 0) - (f_eval_on_ℝ f
4     ↪ t) + (II f.derivative t ht)

```

Proof. Since $e^{t-x} = \frac{d}{dx} (-e^{t-x})$, we can use integration by part.

```

4   rw II,
5   have eq :
6     (∫ x in set.Icc 0 t,
7      (t-x).exp * f_eval_on_ℝ f x) =
8     (∫ x in set.Icc 0 t,
9      f_eval_on_ℝ f x * (deriv (λ x, -(real.exp (t-x))) x)),
10    proof_omitted
11   rw eq,
12   replace eq := integrate_by_part (f_eval_on_ℝ f) (λ (x : ℝ), -(t -
13     ↪ x).exp) 0 t ht,
14   intermediate_steps_omitted
15   rw eq, ring,

```

□

Lemma 3.3.3. For any $m \in \mathbb{N}$,

$$I(f, t) := \int_0^t e^{t-x} \text{eval}_f(x) dx = e^t \sum_{j=0}^m \text{eval}_{f^{(j)}}(0) - \sum_{j=0}^m \text{eval}_{f^{(j)}}(t) + I(f^{(m+1)}, t)$$

```

1 lemma II_integrate_by_part_m (f : ℤ[X]) (t : ℝ)
2   (ht : t ≥ 0) (m : ℕ) :
3   II f t ht = t.exp * (∑ i in finset.range (m+1), (f_eval_on_ℝ
   ↪ (deriv_n f i) 0)) - (∑ i in finset.range (m+1), f_eval_on_ℝ
   ↪ (deriv_n f i) t) + (II (deriv_n f (m+1)) t ht) :=

```

Proof. We prove by induction on m . The base case is lemma 3.3.2

```

4 begin
5   induction m with m ih,
6   rw [deriv_n, II_integrate_by_part],
7   simplification_steps_omitted

```

The inductive step is to apply lemma 3.3.2 to $f^{(m+1)}$ and regroup.

```

8   rw [ih, II_integrate_by_part],
9   simplification_steps_omitted
10 end

```

□

By the previous lemma, we obtain an alternative formulation of $I(f, t)$

Theorem 3.3.2.

$$I(f, t) = e^t \left(\sum_{j=0}^d \text{eval}_{f^{(j)}}(0) \right) - \sum_{j=0}^d \text{eval}_{f^{(j)}}(t)$$

```

1 def I (f : ℤ[X]) (t : ℝ) (ht : t ≥ 0) : ℝ :=
2   t.exp * (∑ i in finset.range f.nat_degree.succ, (f_eval_on_ℝ
   ↪ (deriv_n f i) 0)) - (∑ i in finset.range f.nat_degree.succ,
   ↪ (f_eval_on_ℝ (deriv_n f i) t))
3
4 theorem II_eq_I (f : ℤ[X]) (t : ℝ) (ht : t ≥ 0) :
5   II f t ht = I f t ht

```

Proof. We use lemma 3.3.3 with $m := d$, the degree of f . Then we get

$$I(f, t) := \int_0^t e^{t-x} \text{eval}_f(x) dx = e^t \sum_{j=0}^d \text{eval}_{f^{(j)}}(0) - \sum_{j=0}^d \text{eval}_{f^{(j)}}(t) + I(f^{(d+1)}, t)$$

together with $f^{(d+1)}$ is the zero polynomial so that $I(f^{(d+1)}, t) = 0$.

```

6 begin
7   have II_integrate_by_part_m :=
8     II_integrate_by_part_m f t ht f.nat_degree,
9   have triv : deriv_n f (f.nat_degree + 1) = 0,
10    proof_omitted
11    rw I, rw [triv, II_0, add_zero] at II_integrate_by_part_m,
12    assumption,
13 end

```

□

Transcendence of e

To prove the transcendence of e , we will assume the algebraicity for the hope of a contradiction.

Definition 3.3.2. For any prime number p and natural number n , we define an integer polynomial $f_{p,n}(X) := X^{p-1} \prod_{i=1}^n (X-i)^p$. For any integer polynomial g with degree n whose i -th coefficient is denoted by g_i , we define $J_p(g) = \sum_{j=0}^n g_j I(f_{p,n}, j)$

```

1 def f_p (p : ℕ) (hp : nat.prime p) (n : ℕ): ℤ[X] :=
2   polynomial.X ^ (p - 1) *
3   (∏ i in finset.range n,
4     (polynomial.X - (polynomial.C (i+1:ℤ)))^p)
5
6 def J (g : ℤ[X]) (p : ℕ) (hp : nat.prime p) : ℝ :=
7   ∑ i in finset.range g.nat_degree.succ,
8   (g.coeff i : ℝ) * (II (f_p p hp g.nat_degree) i (nonneg_nat i))

```

Let us evaluate an upper bound for $J_p(g)$

Theorem 3.3.3. Let g and $f_{p,n}$ be as above. Define

$$M := (d+1) \left(\max\{1, |g_0|, \dots, |g_m|\} (n+1) e^{n+1} (2(n+1))^{1+n} \right).$$

Then

$$|J_p(g)| \leq M^p$$

```

1 def M (g : ℤ[X]) : ℝ :=
2   g.nat_degree.succ * ((max_abs_coeff_1 g) * (g.nat_degree+1) *
3     ↪ ((g.nat_degree:ℝ)+1).exp *
4     ↪ (2*(g.nat_degree+1))^(1+g.nat_degree))

```



```

4 | theorem abs_J_upper_bound
5 |   (g :  $\mathbb{Z}[X]$ ) (p :  $\mathbb{N}$ ) (hp : nat.prime p) :
6 |   abs (J g p hp) ≤ (M g)^p :=
7 |

```

Proof.

$$\begin{aligned}
|J_p(g)| &= \left| \sum_{j=0}^n g_j I(f_{p,n}, j) \right| && \text{[by definition]} \\
&\leq \sum_{j=0}^n |g_j I(f_{p,n}, j)| \\
\text{ineq1} &\leq \sum_{j=0}^n |g_j| j e^j \text{eval}_{\bar{f}_{p,d}}(j) && \text{[by theorem 3.3.1]} \\
&\leq \sum_{j=0}^n \max\{1, |g_0|, \dots, |g_m|\} \cdot (d+1) e^{d+1} \left(j^{p-1} \prod_{i=1}^n (j-i)^p \right) \\
&\leq \sum_{j=0}^n \max\{1, |g_0|, \dots, |g_m|\} \cdot (d+1) e^{d+1} \left((2d+1)^p \prod_{i=1}^n (2d+1)^p \right) \\
\text{ineq2} &= (n+1) \left(\max\{1, |g_0|, \dots, |g_m|\} \cdot (n+1) e^{n+1} (2n+1)^{p(1+n)} \right) \\
\text{ineq3} &\leq (n+1)^p \left(\max\{1, |g_0|, \dots, |g_m|\}^p \cdot (n+1)^p e^{p(n+1)} (2n+1)^{p(1+n)} \right) \\
&= M^p
\end{aligned}$$

```

1 | theorem abs_J_upper_bound (g :  $\mathbb{Z}[X]$ ) (p :  $\mathbb{N}$ ) (hp : nat.prime p) :
2 |   ↪ abs (J g p hp) ≤ (M g)^p :=
3 | begin
4 |   have ineq1 := abs_J_ineq1'' g p hp,
5 |   have ineq2 := sum_ineq_1 g p hp,
6 |   have ineq3 := sum_ineq_2 g p hp,
7 |   have ineq4 := le_trans (le_trans ineq1 ineq2) ineq3,
8 |   rw [M, mul_pow, mul_pow, mul_pow, mul_pow, ←pow_mul, add_mul,
9 |     ↪ one_mul],
10 |   have eq1 : g.nat_degree * p = p * g.nat_degree, rw mul_comm, rw
11 |     ↪ eq1, exact ineq4,
12 | end

```

†: Later we will see that as long as there exists for some $c > 0$, $|J_p(g)| < c^p$, we can prove the transcendence of e . Thus here M is chosen to be quite rough on purpose to trivialise the small inequalities needing to be proved such as $j^{p-1} < (2(n+1))^p$ for any $j = 0, \dots, d$. \square

For lower bound of $J_p(g)$ where $\text{eval}_g(e) = 0$, we need to work with more precision.

Lemma 3.3.4. For any prime number p and natural number n , $f_{p,n}(X)$ has degree $(n+1)p - 1$.

```

1 lemma deg_f_p (p : ℕ) (hp : nat.prime p) (n : ℕ) : (f_p p hp
  ↪ n).nat_degree = (n+1)*p - 1 :=
2 begin
3   proof_omitted
4 end

```

Theorem 3.3.4. Let $g \in \mathbb{Z}[X]$ with degree n whose i -th coefficient is denoted by g_i such that $\text{eval}_g(e) = 0$. Let $m = (n+1)p - 1$. Then

$$J_p(g) = - \sum_{j=0}^m \sum_{k=0}^n g_k \text{eval}_{f_{p,n}^{(j)}}(k) \quad (3.2)$$

```

1 theorem J_eq' (g : ℤ[X])
2   (e_root_g : (polynomial.aeval ℤ ℝ e) g = 0) (p : ℕ) (hp :
  ↪ nat.prime p) :
3   (J g p hp) =
4   - ∑ j in finset.range (f_p p hp g.nat_degree).nat_degree.succ,
5     (∑ k in finset.range g.nat_degree.succ,
6       (g.coeff k : ℝ) * (f_eval_on_ℝ (deriv_n (f_p p hp)
  ↪ g.nat_degree) j) (k:ℝ))) :=

```

Proof. We consider the following equalities

$$J_p(g) = \sum_{k=0}^n g_k I(f_{p,n}, k) \quad [\text{definition}]$$

$$J_{\text{eq1}} = \sum_{k=0}^n g_k \left[e^k \left(\sum_{j=0}^m \text{eval}_{f_{p,n}^{(j)}}(0) \right) - \sum_{j=0}^m \text{eval}_{f_{p,n}^{(j)}}(k) \right] \quad [\text{by lemma 3.3.2}]$$

$$\begin{aligned}
J_{\text{eq2}} &= \sum_{k=0}^n g_k e^k \left(\sum_{j=0}^m \text{eval}_{f_{p,n}^{(j)}}(0) \right) - \sum_{k=0}^n g_k \sum_{j=0}^m \text{eval}_{f_{p,n}^{(j)}}(k) \\
&= \left(\sum_{j=0}^m \text{eval}_{f_{p,n}^{(j)}}(0) \right) \sum_{k=0}^n g_k e^k - \sum_{k=0}^n g_k \sum_{j=0}^m \text{eval}_{f_{p,n}^{(j)}}(k)
\end{aligned}$$

$$\begin{aligned}
J_{\text{eq3}} &= - \sum_{k=0}^n g_k \sum_{j=0}^m \text{eval}_{f_{p,n}^{(j)}}(k) \quad [\text{eval}_g(e) = 0] \\
&= - \sum_{j=0}^m \sum_{k=0}^n g_k \text{eval}_{f_{p,n}^{(j)}}(k)
\end{aligned}$$

```

7 begin
8   rw [J_eq1, J_eq2, J_eq3, finset.sum_comm],

```

```

9   simp only [zero_sub, neg_inj],
10  apply congr_arg, ext, rw finset.mul_sum,
11  assumption,
12  end

```

†: Types too long to be displayed with clarity, thus the information about $\mathbf{J_eqi}$ was moved to the start of the proof. \square

The summation in 3.2 actually starts at $j = p - 1$ because of the following lemmas.

Lemma 3.3.5. Let $g, p, n, f_{p,n}$ be like above. If $j < p - 1$, then $\text{eval}_{f_{p,n}^{(j)}}(0) = 0$.

```

1  lemma deriv_f_p_k_eq_zero_k_eq_0_when_j_lt_p_sub_one
2    (p : ℕ) (hp : nat.prime p) (n j : ℕ) (hj : j < p-1):
3    polynomial.eval 0 (deriv_n (f_p p hp n) j) = 0 :=

```

Proof. Let us agree to write $f_{p,n}(X) = X^{p-1}\Pi_{p,n}$ as a short hand. Then

$$\begin{aligned}
 f_{p,n}^{(j)}(X) &= \sum_{i=0}^j \binom{j}{i} (X^{p-1})^{(j-i)} \Pi_{p,n}^{(i)} \\
 \text{eval}_{f_{p,n}^{(j)}}(0) &= \sum_{i=0}^j \binom{j}{i} \text{eval}_{(X^{p-1})^{(j-i)}}(0) \text{eval}_{\Pi_{p,n}^{(i)}}(0)
 \end{aligned} \tag{3.3}$$

We prove that for all $i = 0, \dots, j$, since $j - i < p - 1$,

$$(X^{p-1})^{(j-i)} = \left(\prod_{k=0}^{j-i-1} (p-1) - k \right) X^{p-1-(j-i)}. \tag{3.4}$$

Thus by substituting 0, we get $\text{eval}_{f_{p,n}^{(j)}}(0) = \sum_{i=0}^j \binom{j}{i} 0 = 0$

```

4  begin
5    corresponding to equation (3.3)
6    rw [deriv_n_poly_prod, eval_sum', polynomial.eval_mul],
7    intermediate_steps_omitted
8
9    corresponding to equation (3.4)
10   rw deriv_X_pow',
11   rest_omitted
12  end

```

\square

Similarly, we have the following lemma:

Lemma 3.3.6. Let $g, p, n, f_{p,n}$ be like above. If $j < p$, then $\text{eval}_{f_{p,n}^{(j)}}(x) = 0$ for all $1 \leq x \leq n$.

```

1 lemma deriv_f_p_when_j_lt_p (p : ℕ) (hp : nat.prime p) (n : ℕ) :
2   ∀ x : ℕ, ∀ j : ℕ, j < p → x > 0 → x < n.succ →
3     polynomial.eval (x : ℤ) (deriv_n (f_p p hp n) j) = 0 :=

```

Proof. We prove this by induction on n . For $n = 0$, there is no $1 \leq x \leq 0$, there is nothing to prove.

```

4 begin
5   induction n with n hn,
6   intros x j hj hx1 hx2,
7   linarith,

```

For the inductive step, assume $\text{eval}_{f_{p,n}^{(j)}}(k) = 0$ for all $1 \leq k \leq n$. Then for any $1 \leq x \leq n+1$

$$\begin{aligned}
 f_{p,n+1} &= f_{p,n}(X - (n+1))^p \\
 f_{p,n+1}^{(j)} &= \sum_{i=0}^j \binom{j}{i} f_{p,n}^{(j-i)} ((X - (n+1))^p)^{(i)} \\
 \text{eval}_{f_{p,n+1}^{(j)}}(x) &= \sum_{i=0}^j \binom{j}{i} \text{eval}_{f_{p,n}^{(j-i)}}(x) \text{eval}_{((X - (n+1))^p)^{(i)}}(x).
 \end{aligned}$$

We will prove that for any $0 \leq y \leq j$,

$$\text{eval}_{f_{p,n}^{(j-y)}}(x) \text{eval}_{((X - (n+1))^p)^{(y)}}(x) = 0$$

```

8 intros x j hj hx1 hx2,
9 rw [f_p_n_succ, deriv_n_poly_prod, eval_sum'],
10 apply finset.sum_eq_zero, intros y hy,

```

Here we have that either $x \leq n$ or $x = n+1$. For $x \leq n$, by inductive hypothesis we have $\text{eval}_{f_{p,n}^{(j-y)}}(x) = 0$ then of course $\text{eval}_{f_{p,n}^{(j-y)}}(x) \text{eval}_{((X - (n+1))^p)^{(y)}}(x) = 0$

```

11 cases hx2,
12 simp only [int.cast_coe_nat, int.cast_add,
13   ↪ ring_hom.eq_int_cast, gt_iff_lt, int.coe_nat_eq_zero,
14   ↪ int.cast_one, mul_eq_zero] at *,
13 rw IH x (j-y) (gt_of_gt_of_ge hj (nat.sub_le j y)) hx1 hx2,
14 tauto,

```

For $x = n+1$, we show $\text{eval}_{((X - (n+1))^p)^{(y)}}(x) = 0$. This is true because

$$((X - (n+1))^p)^{(y)} = \left(\prod_{i=0}^y (p-i) \right) (X - (n+1))^{p-y}$$

and $p - y > 0$ hence $0^{p-y} = 0$.

```

15 intermediate_steps_omitted
16 rw [hx2, deriv_X_sub_pow, polynomial.eval_mul,
    ↪ polynomial.eval_pow],
17 simp only [polynomial.eval_X, polynomial.eval_C,
    ↪ int.coe_nat_succ, polynomial.eval_sub, sub_self,
    ↪ mul_eq_zero],
18 right, apply zero_pow (nat.sub_pos_of_lt (gt_of_ge_of_gt hj hy))
19 exact le_of_lt (gt_of_ge_of_gt hj hy),

```

□

Combining the previous lemmas 3.3.5 and 3.3.6, we have the following corollary.

Corollary 3.3.1. Let $g, p, n, f_{p,n}$ be like above. If $j < p-1$, then $\text{eval}_{f_{p,n}^{(j)}}(k) = 0$ for all $0 \leq k \leq n$.

Thus

$$\sum_{j=0}^{p-2} \sum_{k=0}^n g_k \text{eval}_{f_{p,n}^{(j)}}(k) = 0$$

```

1 theorem deriv_f_p_k_eq_zero_when_j_lt_p_sub_one
2 (p : ℕ) (hp : nat.prime p) (n j : ℕ)
3 (hj : j < p - 1) (k : ℕ)
4 (hk : k ∈ finset.range n.succ):
5 polynomial.eval (k:ℤ) (deriv_n (f_p p hp n) j) = 0 :=
6 begin
7   cases k,
8   exact deriv_f_p_k_eq_zero_k_eq_0_when_j_lt_p_sub_one p hp n j hj,
9   apply deriv_f_p_when_j_lt_p p hp n k.succ j (nat.lt_of_lt_pred
    ↪ hj) (nat.succ_pos k) (finset.mem_range.mp hk),
10 end
11
12 theorem J_partial_sum_from_one_to_p_sub_one
13 (g : ℤ[X]) (p : ℕ) (hp : nat.prime p) :
14   ∑ (j : ℕ) in finset.range (p - 1),
15   ∑ (k : ℕ) in finset.range g.nat_degree.succ,
16   g.coeff k * polynomial.eval ↑k (deriv_n (f_p p hp g.nat_degree)
    ↪ j) = 0 :=
17 begin
18   rw finset.sum_eq_zero, intros, rw finset.sum_eq_zero, intros,
19   rw mul_eq_zero, right,
20   rw deriv_f_p_k_eq_zero_when_j_lt_p_sub_one, simp only
    ↪ [finset.mem_range] at H, exact H, exact H_1,
21 end

```

When $j = p - 1$, we can express $\text{eval}_{f_{p,n}^{(p-1)}}(0)$ in a closed form.

Theorem 3.3.5. Let $g, p, n, f_{p,n}$ be like above. Then

$$\text{eval}_{f_{p,n}^{(p-1)}}(0) = (p-1)!(-1)^{np}(n!)^p$$

```

1 theorem deriv_f_p_zero_when_j_eq_p_sub_one
2   (p : ℕ) (hp : nat.prime p) (n : ℕ) :
3   polynomial.eval 0 (deriv_n (f_p p hp n) (p-1)) =
4   (p-1).fact * (-1)^(n*p)*(n.fact)^p :=

```

Proof. We have the following equalities:

$$\begin{aligned}
f_{p,n}^{(p-1)}(X) &= \sum_{i=0}^{p-1} \binom{p-1}{i} (X^{p-1})^{(p-1-i)} \Pi_{p,n}^{(i)} \\
\text{eval}_{f_{p,n}^{(p-1)}}(0) &= \sum_{i=0}^{p-1} \binom{p-1}{i} \text{eval}_{(X^{p-1})^{(p-1-i)}}(0) \text{eval}_{\Pi_{p,n}^{(i)}}(0) \\
&= \binom{p-1}{0} \text{eval}_{(X^{p-1})^{(p-1)}}(0) \text{eval}_{\Pi_{p,n}}(0)
\end{aligned}$$

where the last equality is due to $\text{eval}_{(X^{p-1})^{(p-1-i)}}(0) = 0$ for $i \neq 0$.

```

5 begin
6   rw [f_p, deriv_n_poly_prod, eval_sum'],
7   rw finset.sum_eq_single 0,
8
9   a_proof_of_  $\binom{p-1}{0} \text{eval}_{(X^{p-1})^{(p-1)}}(0) \text{eval}_{\Pi_{p,n}}(0) = (p-1)!(-1)^{np}(n!)^p$ 
10
11   a_proof_of_eval  $\text{eval}_{(X^{p-1})^{(p-1-i)}}(0) = 0$  for all  $i \neq 0$ 
12 end

```

□

Combine theorem 3.3.5 with lemma 3.3.6, we get the following corollary:

Corollary 3.3.2. Let $g, p, n, f_{p,n}$ be like above. Then

$$\sum_{k=0}^n g_k \text{eval}_{f_{p,n}^{(p-1)}}(k) = g_0 (p-1)! (-1)^{np} (n!)^p$$

```

1 theorem J_partial_sum_from_p_sub_one_to_p
2   (g : ℤ[X]) (e_root_g : (polynomial.aeval ℤ ℝ e) g = 0)
3   (p : ℕ) (hp : nat.prime p) :
4    $\sum (k : ℕ) \text{in } \text{finset.range } g.\text{nat\_degree}.\text{succ}, g.\text{coeff } k * \text{polynomial.eval } \uparrow k (\text{deriv\_n } (f\_p \ p \ hp \ g.\text{nat\_degree}) \ (p-1))$ 
5    $= g.\text{coeff } 0 * (\uparrow((p-1).\text{fact}) * (-1) ^ (g.\text{nat\_degree} * p) * \uparrow(g.\text{nat\_degree}.\text{fact}) ^ p) :=$ 
6 begin
7   rw finset.sum_eq_single 0,
8
9   simp only [int.coe_nat_zero],

```

```

10   rw deriv_f_p_zero_when_j_eq_p_sub_one p hp g.nat_degree,
11
12   intros i hi1 hi2, rw mul_eq_zero, right,
13   apply deriv_f_p_when_j_lt_p p hp g.nat_degree,
14   rest_omitted
15 end

```

The final piece of the puzzle is to evaluate $f_{p,n}^j$ when $j \geq p$. We first consider when $k = 0$:

Lemma 3.3.7. Let $g, p, n, f_{p,n}$ be like above. Then if $j \geq p$ then $p! \mid \text{eval}_{f_{p,n}^{(j)}}(0)$.

```

1 lemma k_eq_0_case_when_j_ge_p (p : ℕ) (hp : nat.prime p) (n:ℕ) :
2   ∀ j : ℕ, j ≥ p → (p.fact:ℤ) ∣ polynomial.eval 0 (deriv_n (f_p p
   ↪ hp n) j) :=

```

Proof. Using equation 3.3, we need to prove that for all $0 \leq x \leq j$,

$$p! \mid \binom{j}{x} \text{eval}_{(X^{p-1})^{(j-x)}}(0) \text{eval}_{\Pi_{p,n}^{(x)}}(0)$$

```

3 begin
4   rw f_p, intros j j_ge_p, rw [deriv_n_poly_prod, eval_sum'],
5   apply finset.dvd_sum, intros x hx,
6   simp only [polynomial.eval_C, polynomial.C_add, polynomial.C_1,
   ↪ polynomial.eval_mul, nat.fact],

```

If $j - x = p - 1$, then $\text{eval}_{(X^{p-1})^{(j-x)}}(0) = (p - 1)!$, so it suffices to prove that $p \mid \text{eval}_{\Pi_{p,n}^{(x)}}(0)$. In this case, $x \neq 0$, otherwise $j = p - 1 > p$. For $x \geq 1$,

$$\Pi_{p,n}^{(x)} = \left(\left(\prod_{i=1}^n (X - i) \right)^p \right)^{(x)} = p \left(\left(\prod_{i=1}^n (X - i) \right)^{p-1} \left(\prod_{i=1}^n (X - i) \right)' \right)^{(x-1)} \quad (3.5)$$

```

7   by_cases j - x = p - 1,
8   rw [h, deriv_X_pow'], simp only [mul_one, polynomial.eval_C,
   ↪ nat.sub_self, pow_zero],
9   rw ← fact_eq_prod',
10  suffices :
11    (p:ℤ) ∣ polynomial.eval 0 (deriv_n (∏ (x : ℕ) in finset.range
   ↪ n, (polynomial.X - (polynomial.C ↑ x + 1)) ^ p) x),
12  proof_omitted
13  cases x,
14  simplification_omitted, linarith,
15  rw finset.prod_pow,
16  apply dvd_poly_pow_deriv, corresponding to equation 3.5

```

If $j - x \neq p - 1$, either $j - x < p - 1$ or $j - x > p - 1$. If $j - x < p - 1$ then $\text{eval}_{(X^{p-1})^{j-x}}(0) = 0$; if $j - x > p - 1$, $(X^{p-1})^{j-x}$ is the zero polynomial.

```

17  replace h : j - x < p - 1 ∨ j - x > p - 1, exact lt_or_gt_of_ne
    ↪ h,
18  cases h,
19    rw [(deriv_X_pow' (p-1) (j-x) (le_of_lt h)),
        ↪ polynomial.eval_mul],
20    simp only [polynomial.eval_X, polynomial.eval_C,
        ↪ polynomial.eval_pow],
21    rw (rw (zero_pow (nat.sub_pos_of_lt h))),
22    simp only [zero_mul, mul_zero, dvd_zero],
23
24    rw deriv_X_pow_too_much,
25    simp only [zero_mul, mul_zero, polynomial.eval_zero, dvd_zero],
26    assumption,

```

□

Lemma 3.3.8. Let $g, p, n, f_{p,n}$ be like above. Then $p! \mid \text{eval}_{\Pi_{p,n}^{(j)}}(k)$ for any $0 < k \leq n$ and any $p > 0$, prime or composite.

```

1  lemma p_fact_dvd_prod_part (n : ℕ) :
2  ∀ j : ℕ, ∀ k : ℕ, ∀ p : ℕ, p > 0 → k > 0 → k < n.succ →
3  (p.fact : ℤ) ∣ polynomial.eval (k : ℤ) (deriv_n (∏ i in finset.range
    ↪ n, (polynomial.X - polynomial.C (↑i + 1))^p) j) :=

```

Proof. We proceed by using strong induction on j . For $j = 0$ we need to prove $p! \mid \text{eval}_{\Pi_{p,n}^{(0)}}(k) = \text{eval}_{\Pi_{p,n}}(k)$ for any $0 < k \leq n$. This is true because $\text{eval}_{\Pi_{p,n}}(k) = 0$

```

4  intros j,
5  apply nat.case_strong_induction_on j,
6  intros k p hp hk1 hk2,
7  rw zeroth_deriv, simp only [int.cast_coe_nat, int.cast_add,
    ↪ ring_hom.eq_int_cast, int.cast_one, nat.fact],
8  suffices : polynomial.eval (k : ℤ) (∏ (i : ℕ) in finset.range n,
    ↪ (polynomial.X - (↑i + 1))^p) = 0,
9  rw this, exact dvd_zero ↑(nat.fact p),
10 a_proof_of_eval_{\Pi_{p,n}}(k) = 0

```

For inductive case, we assume $p! \mid \text{eval}_{\Pi_{p,n}^{(m)}}(k)$ for all $m \leq j$, $p > 0$ and $0 < k \leq$

n . This is certainly true for $p = 1$, for $p! = 1$. For $p > 1$,

$$\begin{aligned}\Pi_{p,n}^{(j+1)} &= \left(\left(\left(\prod_{i=0}^n (X - (i+1)) \right)^p \right)' \right)^{(j)} \\ &= p \left(\left(\prod_{i=0}^n (X - (i+1)) \right)^{p-1} \left(\prod_{i=0}^n (X - (i+1)) \right)' \right)^{(j)} \\ &= p \sum_{i=0}^j \binom{j}{i} \Pi_{p-1,n}^{(j-i)} (\Pi'_{1,n})^{(i)}\end{aligned}$$

By inductive hypothesis $(p-1)! \mid \Pi_{p-1,n}^{j-i}$ for any $i = 0, \dots, j$. Thus $p! \mid \Pi_{p,n}^{(j+1)}$

```

11 intros j IH k p hp hk1 hk2,
12 rw [deriv_n, function.iterate_succ_apply, ←deriv_n,
    ↪ finset.prod_pow, poly_pow_deriv, deriv_n_poly_prod,
    ↪ eval_sum'],
13 apply finset.dvd_sum,
14 intros x hx,
15 by_cases (p=1), rw h, norm_num,
16
17 replace IH := IH (j-x) _ k (p-1) _ hk1 hk2,
18 intermediate_steps_omitted,
19 exact IH,
```

□

Immediately by lemma 3.3.7, 3.3.8 and equation 3.3, we have:

Corollary 3.3.3. Let $g, p, n, f_{p,n}$ be like above. If $j \geq p$ then for all $0 \leq k \leq n$ we have $p! \mid \text{eval}_{f_{p,n}^{(j)}}(k)$. Then

$$p! \mid \sum_{j=p}^m \sum_{k=0}^n g_k \text{eval}_{f_{p,n}^{(j)}}(k)$$

```

1 lemma k_ge_1_case_when_j_ge_p (p : ℕ) (hp : nat.prime p) (n:ℕ) :
2   ∀ j : ℕ, j ≥ p → ∀ k : ℕ, k < n.succ → k > 0 → (p.fact:ℤ) |
    ↪ polynomial.eval (k:ℤ) (deriv_n (f_p p hp n) j) :=
3 begin
4   intros j hj k hk1 hk2,
5   rw [f_p, deriv_n_poly_prod, eval_sum'], apply finset.dvd_sum,
6   intros x hx,
7   rw polynomial.eval_mul, rw polynomial.eval_mul,
8   apply dvd_mul_of_dvd_right,
9   apply p_fact_dvd_prod_part n _ _ (nat.prime.pos hp) hk2 hk1,
10 end
11
12 theorem when_j_ge_p_k (p : ℕ) (hp : nat.prime p) (n:ℕ) :
```

```

13  ∀ j : ℕ, j ≥ p → ∀ k : ℕ, k ∈ finset.range n.succ → (p.fact:ℤ)
    ↪ | polynomial.eval (k:ℤ) (deriv_n (f_p p hp n) j) :=
14  begin
15    intros j j_ge_p k hk,
16    simp only [finset.mem_range] at hk,
17    cases k,
18    exact k_eq_0_case_when_j_ge_p p hp n j j_ge_p,
19    exact k_ge_1_case_when_j_ge_p p hp n j j_ge_p k.succ hk
    ↪ (nat.succ_pos k),
20  end
21
22  theorem J_partial_sum_rest (g : ℤ[X]) (e_root_g : (polynomial.aeval
    ↪ ℤ ℝ e) g = 0) (p : ℕ) (hp : nat.prime p) :
23    (p.fact:ℤ) |
24    ∑ (j : ℕ) in finset.Ico p (f_p p hp
    ↪ g.nat_degree).nat_degree.succ,
25    ∑ (k : ℕ) in finset.range g.nat_degree.succ, g.coeff k *
    ↪ polynomial.eval (k:ℤ) (deriv_n (f_p p hp g.nat_degree) j)
    ↪ :=
26  begin
27    apply finset.dvd_sum, intros x hx,
28    apply finset.dvd_sum, intros y hy,
29    apply dvd_mul_of_dvd_right,
30    apply when_j_ge_p_k, simp only [finset.Ico.mem] at hx,
31    exact hx.1, exact hy,
32  end

```

We finally have everything we need to evaluate equation 3.2: by previous corollaries 3.3.1 3.3.2 we have:

Corollary 3.3.4. Let $g, p, n, f_{p,n}$ be like above, there is some $M \in \mathbb{Z}$,

$$J_p(g) = -g_0(p-1)!(-1)^{np}(n!)^p + p! \cdot M$$

```

1  theorem J_eq_final
2    (g : ℤ[X]) (e_root_g : (polynomial.aeval ℤ ℝ e) g = 0)
3    (p : ℕ) (hp : nat.prime p) :
4    ∃ M : ℤ, (J g p hp) = ℤembℝ ((-(g.coeff 0 * (↑((p - 1).fact) *
    ↪ (-1) ^ (g.nat_degree * p) * ↑(g.nat_degree.fact) ^ p))) +
    ↪ (p.fact:ℤ) * M) :=
5  begin
6    have J_eq := J_eq'' g e_root_g p hp, rw J_eq, rw
    ↪ ←ring_hom.map_neg,
7    have seteq : finset.range (f_p p hp g.nat_degree).nat_degree.succ
    ↪ = finset.range (p-1) ∪ {p-1} ∪ finset.Ico p (f_p p hp
    ↪ g.nat_degree).nat_degree.succ,
8    proof_omitted
9    rw seteq, rw finset.sum_union, rw finset.sum_union,
10   rw J_partial_sum_from_one_to_p_sub_one g, rw zero_add, rw
    ↪ finset.sum_singleton,
11   rw J_partial_sum_from_p_sub_one_to_p g e_root_g,
12
13   have H3 := J_partial_sum_rest g e_root_g p hp,
14   rw dvd_iff_mul at H3,

```

```

15 choose c eq3 using H3,
16 rw eq3, rw neg_add, use -c, rw neg_mul_eq_mul_neg ↑(p.fact),
17
18 rest_omitted
19 end

```

We are now ready to prove a lower bound for $|J_p(g)|$.

Theorem 3.3.6. Let $g, p, n, f_{p,n}$ be like above, if we further assume $g_0 \neq 0$, $p > n$ and $p > |g_0|$. Then $(p-1)! \leq |J_p(g)|$

```

1 theorem abs_J_lower_bound
2   (g : ℤ[X]) (e_root_g : (polynomial.aeval ℤ ℝ e) g = 0)
3   (coeff_nonzero : (g.coeff 0) ≠ 0)
4   (p : ℕ) (hp : nat.prime p)
5   (hp2 : p > g.nat_degree ∧ p > (g.coeff 0).nat_abs) :
6   ((p-1).fact:ℝ) ≤ (abs (J g p hp)) :=

```

Proof. By the previous theorem, for some $c \in \mathbb{Z}$

$$|J_p(g)| = (p-1)! |(-g_0(-1)^{np}(n!)^p) + pc|.$$

Thus to prove $|J_p(g)| > (p-1)!$, we prove $|(-g_0(-1)^{np}(n!)^p) + pc| \geq 1$, equivalently, $(-g_0(-1)^{np}(n!)^p) + pc \neq 0$. Let us assume otherwise, i.e. assume $(-g_0(-1)^{np}(n!)^p) + pc = 0$

```

7 simplification_steps_omitted
8 intro rid,

```

Then since $p \mid 0$, we have $p \mid (-g_0(-1)^{np}(n!)^p) + pc$ then $p \mid (-g_0(-1)^{np}(n!)^p)$.

```

9 have rid2 : (p:ℤ) | g.coeff 0 * ((-1) ^ (g.nat_degree * p)) *
  ↪ -↑(g.nat_degree.fact ^ p) + ↑p * c,
10 rw rid, exact dvd_zero ↑p,
11
12 replace rid2 : (p:ℤ) | g.coeff 0 * ((-1) ^ (g.nat_degree * p)) *
  ↪ -↑(g.nat_degree.fact ^ p),
13 refine (dvd_add_iff_left _).2 rid2, exact dvd.intro c rfl,

```

Assume $(-1)^{np} = 1$, then we have $p \mid g_0(n!)^p$, then either $p \mid |g_0|$ or $p \mid (n!)^p$. If $p \mid |g_0|$ then $p \leq |g_0|$.

```

14 have triv : (-1:ℤ) ^ (g.nat_degree * p) = 1 ∨ (-1:ℤ) ^
  ↪ (g.nat_degree * p) = -1 := neg_one_pow_eq_or _,
15 cases triv,
16 simplification_steps_omitted
17 rw nat.prime.dvd_mul at rid2,
18 cases rid2,
19 simplification_steps_omitted
20 have hm : p * m = (g.coeff 0).nat_abs, proof_omitted,
21 replace hm : p ≤ (g.coeff 0).nat_abs, proof_omitted,

```

If $p \mid (n!)^p$, since p is a prime number, $p \mid n!$ implies $p \leq n$.

```

22 intermediate_steps_omitted
23 have H : p | ↑(g.nat_degree.fact).nat_abs,
24 rw nat.prime.dvd_fact at H,

```

For $(-1)^{np} = -1$, the same proof works mutatis mutandis,

```

25 rest_omitted
26 end

```

□

To fulfill the requirement of g having a non-zero coefficient, we divide g by a suitable power of X as following:

```

1 def min_degree_term (f : ℤ[X]) (hf : f ≠ 0) : ℕ :=
2   finset.min' (f.support) (non_empty_supp f hf)
3 def make_const_term_nonzero (f : ℤ[X]) (hf : f ≠ 0) : ℤ[X] :=
4   { support := finset.image (λ i : ℕ, i-(min_degree_term f hf))
5     ↪ f.support,
6     to_fun := (λ n, (f.coeff (n+(min_degree_term f hf)))),
7     mem_support_to_fun := begin
8       intro n, split, intro hn, rw finset.mem_image at hn, choose a
9       ↪ ha using hn, rw ←ha.2, rw nat.sub_add_cancel,
10      have eq2 := (f.3 a).1 ha.1, exact eq2,
11      rw min_degree_term, exact finset.min'_le f.support
12      ↪ (non_empty_supp f hf) a ha.1,
13      intro hn, rw finset.mem_image, use n + min_degree_term f hf,
14      split,
15      exact (f.3 (n + min_degree_term f hf)).2 hn, simp only
16      ↪ [nat.add_sub_cancel],
17    end, }

```

In other words, we divide g by X^m where m is the degree of the lowest non-zero monomial of g .

Because for any $x \geq 0$, $\lim_{n \rightarrow \infty} \frac{x^n}{n!} = 0$ and there is an infinite amount of primes, we have the following theorem serving the coup de grace of attacking the algebraicity of e .

Theorem 3.3.7. For any integer z and non-negative real number M , there is some prime number $p > z$ such that $(p-1)! > M^p$

```

1 theorem coup_de_grace (M : ℝ) (hM : M ≥ 0) (z : ℤ) : ∃ p :
  ↪ nat.primes, (p.val:ℤ) > z ∧ ((p.val-1).fact:ℝ) > M^p.val

```

Theorem 3.3.8. e is transcendental.

```

1 theorem e_transcendental : transcendental e :=

```

Proof. We prove by contradiction. Assume e is algebraic then there is an integer polynomial g such that $\text{eval}_g(e) = 0$. Divide g by some suitable power of X if necessary, we can assume that g has a non-zero constant coefficient.

```

2 begin
3   by_contra e_algebraic,
4   rw is_algebraic at e_algebraic,
5   choose g' g'_def using e_algebraic,
6   have g'_nonzero := g'_def.1,
7   have e_root_g' := g'_def.2,
8   generalize g_def : make_const_term_nonzero g' g'_nonzero = g,
9   have coeff_zero_nonzero : (g.coeff 0) ≠ 0,
10  rw ←g_def, apply coeff_zero_after_change,
11  have e_root_g : (polynomial.aeval ℤ ℝ e) g = 0,
12  rw ←g_def,
13  apply non_zero_root_same, rw e, exact (1:ℝ).exp_ne_zero, exact
    ↪ e_root_g',

```

There is a prime number p such that $p > n$, $p > |g_0|$ and $(p-1)! > M^p$ where M is defined as in theorem 3.3.3. Then $(p-1)! > M^p \geq |J_p(g)| > (p-1)!$ is the desired contradiction.

```

14 have contradiction := contradiction (M g) _ (max g.nat_degree
    ↪ (abs (g.coeff 0))),
15 choose p Hp using contradiction,
16 have abs_J_lower_bound := abs_J_lower_bound g e_root_g
    ↪ coeff_zero_nonzero p.val p.property _,
17 have rid := le_trans abs_J_lower_bound abs_J_upper_bound,
18 simplification_steps_omitted

```

□

Conclusion and future work

This project lives in an interdisciplinary area between mathematics and computer science. Even interactive theorem proving is not necessarily suitable for every mathematician, its pedagogical value is enormous because by formalising theorems the logic of proofs are disentangled and one is forced to be precise and explicit. Hence a proof in `Lean` often challenge users to prove intuitions in a rigorous manner. For example, Alan Baker deemed the evaluation of $J_p(g)$ in equation 3.2 to be clear, but by formalising one has to get hands dirty by actually performing the evaluation [Bak90]. Then anyone else interested in the proof can choose to read or discard relevant sections depending on whether she/he shares the same intuitions with the author.

This is perhaps both a blessing and a curse – by forbidding to use words like “trivial” or “clearly”, one often finds her/himself proving truly trivial propositions as well, for example to prove that $\mathbb{Z}^1 \simeq \mathbb{Z}$. Hence there are at least two directions in which future works could take. One is to formalise more theorems of interest for example the transcendence of π ; the other is to use the (meta-)programming facilities of `Lean` to make more tactics so that learning and using `Lean` could be more effortless.

Bibliography

- [AMK15] Jeremy Avigad, Leonardo de Moura, and Soonho Kong. *Theorem proving in Lean*. 2015.
- [AMR16] Jeremy Avigad, Leonardo de Moura de Moura, and Jared Roesch. *Programming in Lean*. 2016.
- [Bak90] Alan Baker. *Transcendental number theory*. Cambridge university press, 1990.
- [BCM20] Kevin Buzzard, Johan Commelin, and Patrick Massot. “Formalising perfectoid spaces”. In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*. 2020, pp. 299–312.
- [Bou98] Nicolas Bourbaki. *Elements of the History of Mathematics*. Springer Science & Business Media, 1998.
- [Boy+94] Robert Boyer et al. “The QED manifesto”. In: *Automated Deduction—CADE 12* (1994), pp. 238–251.
- [Can32] G Cantor. *Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen*. *Crelles J.* 77 (1874), 258-262; also in *Gesammelte A bhandlungen*. 1932.
- [Can78] Georg Cantor. “Ein beitrage zur mannigfaltigkeitslehre”. In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1878.84 (1878), pp. 242–258.
- [Gel34] Aleksandr Gelfond. “Sur le septieme probleme de Hilbert”. In: *Известия Российской академии наук. Серия математическая* 4 (1934), pp. 623–634.
- [Gon+13] Georges Gonthier et al. “A machine-checked proof of the odd order theorem”. In: *International Conference on Interactive Theorem Proving*. Springer. 2013, pp. 163–179.
- [Gon08] Georges Gonthier. “Formal proof—the four-color theorem”. In: *Notices of the AMS* 55.11 (2008), pp. 1382–1393.
- [Hal+17] Thomas Hales et al. “A formal proof of the Kepler conjecture”. In: *Forum of mathematics, Pi*. Vol. 5. Cambridge University Press. 2017.

- [Hal98] Thomas C Hales. “The kepler conjecture”. In: *arXiv preprint math.MG/9811078* (1998).
- [HUW14] John Harrison, Josef Urban, and Freek Wiedijk. “History of Interactive Theorem Proving.” In: *Computational Logic*. Vol. 9. 2014, pp. 135–214.
- [Kem16] Aubrey J. Kempner. “On Transcendental Numbers”. In: *Transactions of the American Mathematical Society* 17.4 (1916), pp. 476–482. ISSN: 00029947. URL: <http://www.jstor.org/stable/1988833>.
- [KK11] Juliette Kennedy and Roman Kossak. *Set Theory, Arithmetic, and Foundations of Mathematics: Theorems, Philosophies*. Vol. 36. Cambridge University Press, 2011.
- [Lam04] M Lambert. “Mémoire sur quelques propriétés remarquables des quantités transcendentes circulaires et logarithmiques”. In: *Pi: A Source Book*. Springer, 2004, pp. 129–140.
- [Lan66] Serge Lang. *Introduction to transcendental numbers*. Addison-Wesley Pub. Co., 1966.
- [Zha20] Jujian Zhang. *e is a transcendental number*. 2020. URL: https://jjaassoonn.github.io/e_transcendence_doc.html.
- [Zor00] Vladimir A Zorich. *Mathematical Analysis I, volume 1. Universitext*. 2000.