Proving the Impossibility of Trisecting an Angle and Doubling the Cube

Ralph Romanos and Lawrence Paulson

March 17, 2025

Abstract

Squaring the circle, doubling the cube and trisecting an angle, using a compass and straightedge alone, are classic unsolved problems first posed by the ancient Greeks. All three problems were proved to be impossible in the 19th century. The following document presents the proof of the impossibility of solving the latter two problems using Isabelle/HOL, following a proof by Carrega [Car81]. The proof uses elementary methods: no Galois theory or field extensions. The set of points constructible using a compass and straightedge is defined inductively. Radical expressions, which involve only square roots and arithmetic of rational numbers, are defined, and we find that all constructive points have radical coordinates. Finally, doubling the cube and trisecting certain angles requires solving certain cubic equations that can be proved to have no rational roots. The Isabelle proofs require a great many detailed calculations.

Contents

1 Proving the impossibility of trisecting an angle and doubling the cube

theory *Impossible-Geometry*
imports *Complex-Main*
begin

2 Formal Proof

2.1 Definition of the set of Points

datatype *point* = *Point real real*

definition *points-def*:
  $points = \{M.\ \exists\ x \in \mathbb{R}.\ \exists\ y \in \mathbb{R}.\ (M = Point\ x\ y)\}$

primrec *abscissa* :: *point* => *real*
  where *abscissa*: *abscissa* (*Point x y*) = *x*

primrec *ordinate* :: *point* => *real*
  where *ordinate*: *ordinate* (*Point x y*) = *y*

lemma *point-surj* [*simp*]:
  Point (*abscissa M*) (*ordinate M*) = *M*
  ⟨*proof*⟩

lemma *point-eqI* [*intro?*]:
  $[\![abscissa\ M = abscissa\ N;\ ordinate\ M = ordinate\ N]\!] \Longrightarrow M = N$
  ⟨*proof*⟩

lemma *point-eq-iff*:
  $M = N \longleftrightarrow abscissa\ M = abscissa\ N \wedge ordinate\ M = ordinate\ N$
  ⟨*proof*⟩

2.2 Subtraction

Datatype point has a structure of abelian group

instantiation *point* :: *ab-group-add*
begin

definition *point-zero-def*:

$0 = Point\ 0\ 0$

definition *point-one-def*:
$point\text{-}one = Point\ 1\ 0$

definition *point-add-def*:
$A + B = Point\ (abscissa\ A + abscissa\ B)\ (ordinate\ A + ordinate\ B)$

definition *point-minus-def*:
$-\ A = Point\ (-\ abscissa\ A)\ (-\ ordinate\ A)$

definition *point-diff-def*:
$A - (B{::}point) = A + -\ B$

lemma *Point-eq-0* [*simp*]:
$Point\ xA\ yA = 0 \longleftrightarrow (xA = 0 \wedge yA = 0)$
⟨*proof*⟩

lemma *point-abscissa-zero* [*simp*]:
$abscissa\ 0 = 0$
⟨*proof*⟩

lemma *point-ordinate-zero* [*simp*]:
$ordinate\ 0 = 0$
⟨*proof*⟩

lemma *point-add* [*simp*]:
$Point\ xA\ yA + Point\ xB\ yB = Point\ (xA + xB)\ (yA + yB)$
⟨*proof*⟩

lemma *point-abscissa-add* [*simp*]:
$abscissa\ (A + B) = abscissa\ A + abscissa\ B$
⟨*proof*⟩

lemma *point-ordinate-add* [*simp*]:
$ordinate\ (A + B) = ordinate\ A + ordinate\ B$
⟨*proof*⟩

lemma *point-minus* [*simp*]:
$-\ (Point\ xA\ yA) = Point\ (-\ xA)\ (-\ yA)$
⟨*proof*⟩

lemma *point-abscissa-minus* [*simp*]:
$abscissa\ (-\ A) = -\ abscissa\ (A)$
⟨*proof*⟩

lemma *point-ordinate-minus* [*simp*]:
$ordinate\ (-\ A) = -\ ordinate\ (A)$
⟨*proof*⟩

lemma *point-diff* [*simp*]:
Point xA yA − *Point xB yB* = *Point* (*xA* − *xB*) (*yA* − *yB*)
⟨*proof*⟩

lemma *point-abscissa-diff* [*simp*]:
abscissa (*A* − *B*) = *abscissa* (*A*) − *abscissa* (*B*)
⟨*proof*⟩

lemma *point-ordinate-diff* [*simp*]:
ordinate (*A* − *B*) = *ordinate* (*A*) − *ordinate* (*B*)
⟨*proof*⟩

instance
⟨*proof*⟩

end

2.3 Metric Space

We can also define a distance, hence point is also a metric space

instantiation *point* :: *metric-space*
begin

definition *point-dist-def*:
dist A B = *sqrt* ((*abscissa* (*A* − *B*))^2 + (*ordinate* (*A* − *B*))^2)

definition
(*uniformity* :: (*point* × *point*) *filter*) = (*INF e*∈{*0* <..}. *principal* {(*x*, *y*). *dist x y* < *e*})

definition
open (*S* :: *point set*) = (∀ *x*∈*S*. $\forall_F$ (*x'*, *y*) *in uniformity*. *x'* = *x* ⟶ *y* ∈ *S*)

lemma *point-dist* [*simp*]:
dist (*Point xA yA*) (*Point xB yB*) = *sqrt* ((*xA* − *xB*)^2 + (*yA* − *yB*)^2)
⟨*proof*⟩

lemma *real-sqrt-diff-squares-triangle-ineq*:
fixes *a b c d* :: *real*
shows *sqrt* ((*a* − *c*)^2 + (*b* − *d*)^2) ≤ *sqrt* (*a*^2 + *b*^2) + *sqrt* (*c*^2 + *d*^2)
⟨*proof*⟩

instance
⟨*proof*⟩
end

2.4 Geometric Definitions

These geometric definitions will later be used to define constructible points

The distance between two points is defined with the distance of the metric space point

definition *distance-def*:
 distance A B = *dist* A B

parallel A B C D is true if the lines AB and CD are parallel. If not it is false.

definition *parallel-def*:
 parallel A B C D = ((*abscissa* A − *abscissa* B) ∗ (*ordinate* C − *ordinate* D) = (*ordinate* A − *ordinate* B) ∗ (*abscissa* C − *abscissa* D))

Three points A B C are collinear if and only if the lines AB and AC are parallel

definition *collinear-def*:
 collinear A B C = *parallel* A B A C

The point M is the intersection of two lines AB and CD if and only if the points A, M and B are collinear and the points C, M and D are also collinear

definition *is-intersection-def*:
 is-intersection M A B C D = (*collinear* A M B ∧ *collinear* C M D)

2.5 Reals definable with square roots

The inductive set *radical-sqrt* defines the reals that can be defined with square roots. If x is in the following set, then it depends only upon rational expressions and square roots. For example, suppose x is of the form : $x = (\sqrt{a+\sqrt{b}} + \sqrt{c+\sqrt{d*e+f}})/(\sqrt{a}+\sqrt{b}) + (a+\sqrt{b})/\sqrt{g}$, where a, b, c, d, e, f and g are rationals. Then x is in *radical-sqrt* because it is only defined with rationals and square roots of radicals.

inductive-set *radical-sqrt* :: *real set*
 where
  Rat: $x \in \mathbb{Q} \Longrightarrow x \in$ *radical-sqrt*
 | *Neg*: $x \in$ *radical-sqrt* $\Longrightarrow -x \in$ *radical-sqrt*
 | *Inverse*: $x \in$ *radical-sqrt* $\Longrightarrow x \neq 0 \Longrightarrow 1/x \in$ *radical-sqrt*
 | *Plus*: $x \in$ *radical-sqrt* $\Longrightarrow y \in$ *radical-sqrt* $\Longrightarrow x+y \in$ *radical-sqrt*
 | *Times*: $x \in$ *radical-sqrt* $\Longrightarrow y \in$ *radical-sqrt* $\Longrightarrow x*y \in$ *radical-sqrt*
 | *Sqrt*: $x \in$ *radical-sqrt* $\Longrightarrow x \geq 0 \Longrightarrow$ *sqrt* $x \in$ *radical-sqrt*

Here, we list some rules that will be used to prove that a given real is in *radical-sqrt*.

Given two reals in *radical-sqrt* x and y, the subtraction $x - y$ is also in *radical-sqrt*.

lemma *radical-sqrt-rule-subtraction*:
$x \in$ *radical-sqrt* $\Longrightarrow y \in$ *radical-sqrt* $\Longrightarrow x-y \in$ *radical-sqrt*
⟨*proof*⟩

Given two reals in *radical-sqrt* x and y, and $y \neq 0$, the division x/y is also in *radical-sqrt*.

lemma *radical-sqrt-rule-division*:
$[\![x \in$ *radical-sqrt*; $y \in$ *radical-sqrt*; $y \neq 0]\!] \Longrightarrow x/y \in$ *radical-sqrt*
⟨*proof*⟩

Given a positive real x in *radical-sqrt*, its square x^2 is also in *radical-sqrt*.

lemma *radical-sqrt-rule-power2*:
$x \in$ *radical-sqrt* $\Longrightarrow x \geq 0 \Longrightarrow x\hat{\ }2 \in$ *radical-sqrt*
⟨*proof*⟩

Given a positive real x in *radical-sqrt*, its cube x^3 is also in *radical-sqrt*.

lemma *radical-sqrt-rule-power3*:
$x \in$ *radical-sqrt* $\Longrightarrow x \geq 0 \Longrightarrow x\hat{\ }3 \in$ *radical-sqrt*
⟨*proof*⟩

2.6 Introduction of the datatype expr which represents radical expressions

An expression expr is either a rational constant: Const or the negation of an expression or the inverse of an expression or the addition of two expressions or the multiplication of two expressions or the square root of an expression.

datatype *expr* = *Const rat* | *Negation expr* | *Inverse expr* | *Addition expr expr* | *Multiplication expr expr* | *Sqrt expr*

The function *translation* translates a given expression into its equivalent real.

fun *translation* :: *expr* => *real* (‹(2{|-|})›)
where
translation (*Const x*) = *of-rat x*|
translation (*Negation e*) = − *translation e*|
translation (*Inverse e*) = (*1*::*real*) / *translation e*|
translation (*Addition e1 e2*) = *translation e1* + *translation e2*|
translation (*Multiplication e1 e2*) = *translation e1* ∗ *translation e2*|
translation (*Sqrt e*) = (*if translation e* < *0 then 0 else sqrt* (*translation e*))

Define the set of all the radicals of a given expression. For example, suppose *expr* is of the form : expr = Addition (Sqrt (Addition (Const a) Sqrt (Const b))) (Sqrt (Addition (Const c) (Sqrt (Sqrt (Const d))))), where a, b, c and d are rationals. This can be translated as follows: $\{\!|expr|\!\} = \sqrt{a + \sqrt{b}} + \sqrt{c + \sqrt{\sqrt{d}}}$. Moreover, the set *radicals* of this expression is : {|Addition

(Const a) (Sqrt (Const b)), Const b, Addition (Const c) (Sqrt (Sqrt (Const d))), Sqrt (Const d), Const d⦄.

fun *radicals* :: *expr* => *expr set*
  where
  radicals (*Const x*) = {}|
  radicals (*Negation e*) = (*radicals e*)|
  radicals (*Inverse e*) = (*radicals e*)|
  radicals (*Addition e1 e2*) = ((*radicals e1*) ∪ (*radicals e2*))|
  radicals (*Multiplication e1 e2*) = ((*radicals e1*) ∪ (*radicals e2*))|
  radicals (*Sqrt e*) = (*if* ⦃*e*⦄ < *0 then radicals e else* {*e*} ∪ (*radicals e*))

If r is in *radicals* of e then the set *radical-sqrt* of r is a subset (strictly speaking) of the set *radicals* of e.

lemma *radicals-expr-subset*: $r \in$ *radicals* $e \Longrightarrow$ *radicals* $r \subset$ *radicals* e
  ⟨*proof*⟩

If x is in *radical-sqrt* then there exists a radical expression e which translation is x (it is important to notice that this expression is not necessarily unique).

lemma *radical-sqrt-correct-expr*:
  $x \in$ *radical-sqrt* $\Longrightarrow \exists\ e.$ ⦃e⦄ $= x$
⟨*proof*⟩

The order of an expression is the maximum number of radicals one over another occurring in a given expression. Using the example above, suppose *expr* is of the form : expr = Addition (Sqrt (Addition (Const a) Sqrt (Const b))) (Sqrt (Addition (Const c) (Sqrt (Sqrt (Const d))))), where a, b, c and d are rationals and which can be translated as follows: ⦃*expr*⦄ $= \sqrt{a+\sqrt{b}+\sqrt{c+\sqrt{\sqrt{d}}}}$. The order of *expr* is $max(2,3) = 3$.

fun *order* :: *expr* => *nat*
  where
  order (*Const x*) = *0*|
  order (*Negation e*) = *order e*|
  order (*Inverse e*) = *order e*|
  order (*Addition e1 e2*) = *max* (*order e1*) (*order e2*)|
  order (*Multiplication e1 e2*) = *max* (*order e1*) (*order e2*)|
  order (*Sqrt e*) = *1* + *order e*

If an expression s is one of the radicals (or in *radicals*) of the expression r, then its order is smaller (strictly speaking) then the order of r.

lemma *in-radicals-smaller-order*:
  $s \in$ *radicals* $r \Longrightarrow$ (*order* s) < (*order* r)
  ⟨*proof*⟩

The following theorem is the converse of the previous lemma.

lemma *in-radicals-smaller-order-contrap*:

$(order\ s) \geq (order\ r) \Longrightarrow \neg\ (s \in radicals\ r)$
$\langle proof \rangle$

An expression r cannot be one of its own radicals.

lemma *not-in-own-radicals*:
$\neg\ (r \in radicals\ r)$
$\langle proof \rangle$

If an expression e is a radical expression and it has no radicals then its translation is a rational.

lemma *radicals-empty-rational*: $radicals\ e = \{\} \Longrightarrow \{\!|e|\!\} \in \mathbb{Q}$
$\langle proof \rangle$

A finite non-empty set of natural numbers has necessarily a maximum.

lemma *finite-set-has-max*:
$finite\ (s{::}\ nat\ set) \Longrightarrow s \neq \{\} \Longrightarrow \exists\, k \in s.\ \forall\ p \in s.\ p \leq k$
$\langle proof \rangle$

There is a finite number of radicals in an expression.

lemma *finite-radicals*: $finite\ (radicals\ e)$
$\langle proof \rangle$

We define here a new set corresponding to the orders of each element in the set *radicals* of an expression *expr*. Using the example above, suppose *expr* is of the form : expr = Addition (Sqrt (Addition (Const a) Sqrt (Const b))) (Sqrt (Addition (Const c) (Sqrt (Sqrt (Const d))))), where a, b, c and d are rationals and which can be translated as follows: $\{\!|expr|\!\} = \sqrt{a + \sqrt{b}} + \sqrt{c + \sqrt{\sqrt{d}}}$. The set *radicals* of *expr* is {Addition (Const a) Sqrt (Const b), Const b, Addition (Const c) (Sqrt (Sqrt (Const d))), Sqrt (Const d), Const d}; therefore, the set *order-radicals* of this set is $\{1, 0, 2, 1, 0\}$.

fun *order-radicals*:: *expr set* => *nat set*
where $order\text{-}radicals\ s = \{y.\ \exists\ x \in s.\ y = order\ x\}$

If the set of radicals of an expression e is not empty and is finite then the set *order-radicals* of the set of radicals of e is not empty and is also finite.

The following lemma states that given an expression e, if the set *order-radicals* of the set *radicals* e is not empty and is finite, then there exists a radical r of e which is of highest order among the radicals of e.

lemma *finite-order-radicals-has-max*:
$[\![order\text{-}radicals\ (radicals\ e) \neq \{\};$
$finite\ (order\text{-}radicals\ (radicals\ e))]\!]$
$\Longrightarrow \exists\, r.\ r \in radicals\ e \wedge (\forall\, s{\in}radicals\ e.\ order\ s \leq order\ r)$
$\langle proof \rangle$

This important lemma states that in an expression that has at least one radical, we can find an upmost radical r which is not radical of any other term of the expression e. It is also important to notice that this upmost radical is not necessarily unique and is not the term of highest order of the expression e. Using the example above, suppose e is of the form : $e =$ Addition (Sqrt (Addition (Const a) Sqrt (Const b))) (Sqrt (Addition (Const c) (Sqrt (Sqrt (Const d))))), where a, b, c and d are rationals and which can be translated as follows: $\{\!|e|\!\} = \sqrt{a + \sqrt{b}} + \sqrt{c + \sqrt{\sqrt{d}}}$. The possible upmost radicals in this expression are Addition (Const a) (Sqrt (Const b)) or Addition (Const c) (Sqrt (Sqrt (Const d))).

lemma *finite-order-radicals*:
$\mathit{radicals}\ e \neq \{\} \Longrightarrow \mathit{finite}\ (\mathit{radicals}\ e) \Longrightarrow$
$\mathit{order\text{-}radicals}\ (\mathit{radicals}\ e) \neq \{\} \wedge \mathit{finite}\ (\mathit{order\text{-}radicals}\ (\mathit{radicals}\ e))$
$\langle \mathit{proof} \rangle$

lemma *upmost-radical-sqrt2*:
$\mathit{radicals}\ e \neq \{\} \Longrightarrow$
$\exists\, r \in \mathit{radicals}\ e.\ \forall\ s \in \mathit{radicals}\ e.\ r \notin \mathit{radicals}\ s$
$\langle \mathit{proof} \rangle$

The following 7 lemmas are used to prove the main lemma *radical-sqrt-normal-form* which states that if an expression e has at least one radical then it can be written in a normal form. This means that there exist three radical expressions a, b and r such that $\{\!|e|\!\} = \{\!|a|\!\} + \{\!|b|\!\} * \sqrt{\{\!|r|\!\}}$ and the radicals of a are radicals of e but are not r, and the same goes for the radicals of b and r. It is important to notice that a, b and r are not unique and *Sqrt r* is not necessarily the term of highest order.

lemma *eq-sqrt-squared*:
$(x{::}\mathit{real}) \geq 0 \Longrightarrow (\mathit{sqrt}\ x) * (\mathit{sqrt}\ x) = x$
$\langle \mathit{proof} \rangle$

lemma *radical-sqrt-normal-form-inverse*:
assumes $z \geq 0\ x \neq y * \mathit{sqrt}\ z$
shows
$1\ /\ (x + y * \mathit{sqrt}\ z) =$
$x\ /\ (x * x - y * y * z) - (y * \mathit{sqrt}\ z)\ /\ (x * x - y * y * z)$
$\langle \mathit{proof} \rangle$

lemma *radical-sqrt-normal-form-lemma*:
fixes $e{::}\mathit{expr}$
assumes $\mathit{radicals}\ e \neq \{\}$
and $\forall\, s \in \mathit{radicals}\ e.\ r \notin \mathit{radicals}\ s$
and $r \in \mathit{radicals}\ e$
shows $\exists\, a\ b.\ 0 \leq \{\!|r|\!\} \wedge \{\!|e|\!\} = \{\!|a|\!\} + \{\!|b|\!\} * \mathit{sqrt}\ \{\!|r|\!\}\ \&$
$\mathit{radicals}\ a \cup \mathit{radicals}\ b \cup \mathit{radicals}\ r \subseteq \mathit{radicals}\ e\ \&$
$r \notin \mathit{radicals}\ a \cup \mathit{radicals}\ b$

($\mathbf{is}$ $\exists\, a\ b.\ ?concl\ e\ a\ b$)
$\langle proof \rangle$

This main lemma is essential for the remaining part of the proof.

theorem *radical-sqrt-normal-form*:
$radicals\ e \neq \{\} \Longrightarrow$
$\exists\ r \in radicals\ e.$
$\exists\ a\ b.\ \{\!|e|\!\} = \{\!|Addition\ a\ (Multiplication\ b\ (Sqrt\ r))|\!\} \wedge \{\!|r|\!\} \geq 0 \wedge$
$radicals\ a \cup radicals\ b \cup radicals\ r \subseteq radicals\ e\ \&$
$r \notin radicals\ a \cup radicals\ b \cup radicals\ r$
$\langle proof \rangle$

2.7 Important properties of the roots of a cubic equation

The following 7 lemmas are used to prove a main result about the properties of the roots of a cubic equation (*cubic-root-radical-sqrt-rational*) which states that assuming that a b and c are rationals and that x is a radical satisfying $x^3 + ax^2 + bx + c = 0$ then there exists a rational root. This lemma will be used in the proof of the impossibility of trisection an angle and of duplicating a cube.

lemma *cubic-root-radical-sqrt-steplemma*:
fixes $P :: real\ set$
assumes $Nats\ [THEN\ subsetD,\ intro]$: $Nats \subseteq P$
and Neg: $\forall x \in P.\ -x \in P$
and Inv: $\forall x \in P.\ x \neq 0 \longrightarrow 1/x \in P$
and Add: $\forall x \in P.\ \forall y \in P.\ x+y \in P$
and $Mult$: $\forall x \in P.\ \forall y \in P.\ x*y \in P$
and a: $a \in P$ **and** b: $b \in P$ **and** c: $c \in P$
and $eq0$: $z\hat{}3 + a * z\hat{}2 + b * z + c = 0$
and u: $u \in P$
and v: $v \in P$
and s: $s * s \in P$
and z: $z = u + v * s$
shows $\exists\, w \in P.\ w\hat{}3 + a * w\hat{}2 + b * w + c = 0$
$\langle proof \rangle$

lemma *cubic-root-radical-sqrt-steplemma-sqrt*:
assumes $Nats\ [THEN\ subsetD,\ intro]$: $Nats \subseteq P$
and $\forall x \in P.\ -x \in P$
and $\forall x \in P.\ x \neq 0 \longrightarrow 1/x \in P$
and $\forall x \in P.\ \forall y \in P.\ x+y \in P$
and $\forall x \in P.\ \forall y \in P.\ x*y \in P$
and $(a \in P)$ **and** b: $(b \in P)$ **and** c: $(c \in P)$
and $z\hat{}3 + a * z\hat{}2 + b * z + c = 0$
and $u \in P\ v \in P\ s \in P$
and $s \geq 0$
and $z = u + v * sqrt\ s$
shows $\exists\, w \in P.\ w\hat{}3 + a * w\hat{}2 + b * w + c = 0$

⟨*proof*⟩

lemma *cubic-root-radical-sqrt-lemma*:
fixes *e::expr*
assumes *a*: $a \in \mathbb{Q}$ **and** *b*: $b \in \mathbb{Q}$ **and** *c*: $c \in \mathbb{Q}$
and *notEmpty*: *radicals* $e \neq \{\}$
and *eq0*: $\{\!|e|\!\}\hat{\ } 3 + a * \{\!|e|\!\}\hat{\ }2 + b * \{\!|e|\!\} + c = 0$
shows $\exists$ *e1*. *radicals e1* $\subset$ *radicals e* $\wedge$ $(\{\!|e1|\!\}\hat{\ }3 + a * \{\!|e1|\!\}\hat{\ }2 + b * \{\!|e1|\!\} + c = 0)$
⟨*proof*⟩

lemma *cubic-root-radical-sqrt*:
assumes *abc*: $a \in \mathbb{Q}$ $b \in \mathbb{Q}$ $c \in \mathbb{Q}$
shows *card* (*radicals e*) $= n \Longrightarrow \{\!|e|\!\}\hat{\ }3 + a * \{\!|e|\!\}\hat{\ }2 + b * \{\!|e|\!\} + c = 0 \Longrightarrow$
$\exists x \in \mathbb{Q}.\ x\hat{\ }3 + a * x\hat{\ }2 + b * x + c = 0$
⟨*proof*⟩

Now we can prove the final result about the properties of the roots of a cubic equation.

theorem *cubic-root-radical-sqrt-rational*:
assumes *a*: $a \in \mathbb{Q}$ **and** *b*: $b \in \mathbb{Q}$ **and** *c*: $c \in \mathbb{Q}$
and *x*: $x \in$ *radical-sqrt*
and *x-eqn*: $x\hat{\ }3 + a * x\hat{\ }2 + b * x + c = 0$
shows *c*: $\exists x \in \mathbb{Q}.\ x\hat{\ }3 + a * x\hat{\ }2 + b * x + c = 0$
⟨*proof*⟩

2.8 Important properties of radicals

lemma *sqrt-roots*:
$y\hat{\ }2=x \Longrightarrow x\geq 0 \wedge (sqrt\ (x) = y \mid sqrt\ (x) = -y)$
⟨*proof*⟩

lemma *radical-sqrt-linear-equation*:
assumes $a \in$ *radical-sqrt* $b \in$ *radical-sqrt*
and $\neg\ (a = 0 \wedge b = 0)$
and $a * x + b = 0$
shows $x \in$ *radical-sqrt*
⟨*proof*⟩

lemma *radical-sqrt-simultaneous-linear-equation*:
assumes $a \in$ *radical-sqrt*
and $b \in$ *radical-sqrt*
and $c \in$ *radical-sqrt*
and $d \in$ *radical-sqrt*
and $e \in$ *radical-sqrt*
and $f \in$ *radical-sqrt*
and *NotNull*: $\neg\ (a*e - b*d = 0 \wedge a*f - c*d = 0 \wedge e*c = b*f)$
and *eq*: $a*x + b*y = c$ $d*x + e*y = f$

shows $x \in$ *radical-sqrt* $\wedge$ $y \in$ *radical-sqrt*
$\langle proof \rangle$

lemma *radical-sqrt-quadratic-equation*:
assumes $a \in$ *radical-sqrt*
and $b \in$ *radical-sqrt*
and $c \in$ *radical-sqrt*
and *eq0*: $a{*}x\hat{}2{+}b{*}x{+}c = 0$
and *NotNull*: $\neg$ $(a = 0 \wedge b = 0 \wedge c = 0)$
shows $x \in$ *radical-sqrt*
$\langle proof \rangle$

lemma *radical-sqrt-simultaneous-linear-quadratic*:
assumes $a \in$ *radical-sqrt*
and $b \in$ *radical-sqrt*
and $c \in$ *radical-sqrt*
and $d \in$ *radical-sqrt*
and $e \in$ *radical-sqrt*
and $f \in$ *radical-sqrt*
and *NotNull*: $\neg(d{=}0 \wedge e{=}0 \wedge f{=}0)$
and *eq*: $(x{-}a)\hat{}2 + (y{-}b)\hat{}2 = cd{*}x{+}e{*}y = f$
shows $x \in$ *radical-sqrt* $\wedge$ $y \in$ *radical-sqrt*
$\langle proof \rangle$

lemma *radical-sqrt-simultaneous-quadratic-quadratic*:
assumes $a \in$ *radical-sqrt*
and $b \in$ *radical-sqrt*
and $c \in$ *radical-sqrt*
and $d \in$ *radical-sqrt*
and $e \in$ *radical-sqrt*
and $f \in$ *radical-sqrt*
and *NotEqual*: $\neg$ $(a = d \wedge b = e \wedge c = f)$
and *eq*: $(x - a)\hat{}2 + (y - b)\hat{}2 = c$ $(x - d)\hat{}2 + (y - e)\hat{}2 = f$
shows $x \in$ *radical-sqrt* $\wedge$ $y \in$ *radical-sqrt*
$\langle proof \rangle$

2.9 Important properties of geometrical points which coordinates are radicals

lemma *radical-sqrt-line-line-intersection*:
assumes *absA*: (*abscissa* (A)) $\in$ *radical-sqrt*
and *ordA*: (*ordinate* A) $\in$ *radical-sqrt*
and *absB*: (*abscissa* B) $\in$ *radical-sqrt*
and *ordB*: (*ordinate* B) $\in$ *radical-sqrt*
and *absC*: (*abscissa* C) $\in$ *radical-sqrt*
and *ordC*: (*ordinate* C) $\in$ *radical-sqrt*
and *absD*: (*abscissa* D) $\in$ *radical-sqrt*

and *ordD*: (*ordinate D*) ∈ *radical-sqrt*
and *notParallel*: ¬ (*parallel A B C D*)
and *isIntersec*: *is-intersection X A B C D*
shows (*abscissa X*) ∈ *radical-sqrt* ∧ (*ordinate X*) ∈ *radical-sqrt*
⟨*proof*⟩

lemma *radical-sqrt-line-circle-intersection*:
assumes *absA*: (*abscissa A*) ∈ *radical-sqrt* **and** *ordA*: (*ordinate A*) ∈ *radical-sqrt*
and *absB*: (*abscissa B*) ∈ *radical-sqrt* **and** *ordB*: (*ordinate B*) ∈ *radical-sqrt*
and *absC*: (*abscissa C*) ∈ *radical-sqrt* **and** *ordC*: (*ordinate C*) ∈ *radical-sqrt*
and *absD*: (*abscissa D*) ∈ *radical-sqrt* **and** *ordD*: (*ordinate D*) ∈ *radical-sqrt*
and *absE*: (*abscissa E*) ∈ *radical-sqrt* **and** *ordE*: (*ordinate E*) ∈ *radical-sqrt*
and *notEqual*: $A \neq B$
and *colin*: *collinear A X B*
and *eqDist*: (*distance C X* = *distance D E*)
shows (*abscissa X*) ∈ *radical-sqrt* ∧ (*ordinate X*) ∈ *radical-sqrt*
⟨*proof*⟩

lemma *radical-sqrt-circle-circle-intersection*:
assumes *absA*: (*abscissa A*) ∈ *radical-sqrt* **and** *ordA*: (*ordinate A*) ∈ *radical-sqrt*
and *absB*: (*abscissa B*) ∈ *radical-sqrt* **and** *ordB*: (*ordinate B*) ∈ *radical-sqrt*
and *absC*: (*abscissa C*) ∈ *radical-sqrt* **and** *ordC*: (*ordinate C*) ∈ *radical-sqrt*
and *absD*: (*abscissa D*) ∈ *radical-sqrt* **and** *ordD*: (*ordinate D*) ∈ *radical-sqrt*
and *absE*: (*abscissa E*) ∈ *radical-sqrt* **and** *ordE*: (*ordinate E*) ∈ *radical-sqrt*
and *absF*: (*abscissa F*) ∈ *radical-sqrt* **and** *ordF*: (*ordinate F*) ∈ *radical-sqrt*
and *eqDist0*: *distance A X* = *distance B C*
and *eqDist1*: *distance D X* = *distance E F*
and *notEqual*: ¬ (*A* = *D* ∧ *distance B C* = *distance E F*)
shows (*abscissa X*) ∈ *radical-sqrt* ∧ (*ordinate X*) ∈ *radical-sqrt*
⟨*proof*⟩

2.10 Definition of the set of contructible points

inductive-set *constructible* :: *point set*
where
(*M* ∈ *points* ∧ (*abscissa M*) ∈ $\mathbb{Q}$ ∧ (*ordinate M*) ∈ $\mathbb{Q}$) ⟹ *M* ∈ *constructible*|
(*A* ∈ *constructible* ∧ *B* ∈ *constructible* ∧ *C* ∈ *constructible* ∧ *D* ∈ *constructible* ∧ ¬ *parallel A B C D* ∧ *is-intersection M A B C D*) ⟹ *M* ∈ *constructible*|
(*A* ∈ *constructible* ∧ *B* ∈ *constructible* ∧ *C* ∈ *constructible* ∧ *D* ∈ *constructible* ∧ *E* ∈ *constructible* ∧ ¬ *A* = *B* ∧ *collinear A M B* ∧ *distance C M* = *distance D E*) ⟹ *M* ∈ *constructible*|
(*A* ∈ *constructible* ∧ *B* ∈ *constructible* ∧ *C* ∈ *constructible* ∧ *D* ∈ *constructible* ∧ *E* ∈ *constructible* ∧ *F* ∈ *constructible* ∧ ¬ (*A* = *D* ∧ *distance B C* = *distance E F*) ∧ *distance A M* = *distance B C* ∧ *distance D M* = *distance E F*) ⟹ *M* ∈ *constructible*

2.11 An important property about constructible points: their coordinates are radicals

lemma *constructible-radical-sqrt*:
  assumes $M \in constructible$
  shows $(abscissa\ M) \in radical\text{-}sqrt \land (ordinate\ M) \in radical\text{-}sqrt$
  ⟨*proof*⟩

2.12 Proving the impossibility of duplicating the cube

lemma *impossibility-of-doubling-the-cube-lemma*:
  assumes *x*: $x \in radical\text{-}sqrt$
  and *x-eqn*: $x\hat{}3 = 2$
  shows *False*
⟨*proof*⟩

theorem *impossibility-of-doubling-the-cube*:
  $x\hat{}3 = 2 \Longrightarrow (Point\ x\ 0) \notin constructible$
  ⟨*proof*⟩

2.13 Proving the impossibility of trisecting an angle

lemma *impossibility-of-trisecting-pi-over-3-lemma*:
  assumes *x*: $x \in radical\text{-}sqrt$
  and *x-eqn*: $x\hat{}3 - 3 * x - 1 = 0$
  shows *False*
⟨*proof*⟩

theorem *impossibility-of-trisecting-angle-pi-over-3*:
  $Point\ (cos\ (pi\ /\ 9))\ 0 \notin constructible$
⟨*proof*⟩

end

References

[Car81] J. C. Carrega. *Théorie des corps : la règle et le compas*. Hermann, 1981.