Proving the Impossibility of Trisecting an Angle and Doubling the Cube

Ralph Romanos and Lawrence Paulson

September 19, 2015

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 2
2 Formal Proof 2
   2.1 Definition of the set of Points 2
   2.2 Subtraction 2
   2.3 Metric Space 4
   2.4 Geometric Definitions 4
   2.5 Reals definable with square roots 5
   2.6 Introduction of the datatype expr which represents radical expressions 6
   2.7 Important properties of the roots of a cubic equation 10
   2.8 Important properties of radicals 11
   2.9 Important properties of geometrical points which coordinates are radicals 12
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. ∃ x ∈ R. ∃ y ∈ 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] ==> M = N
(proof)

lemma point-eq-iff:
M = N <-> abscissa M = abscissa N ∧ 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:
\[
\begin{align*}
0 &= \text{Point } 0 \ 0 \\
\text{definition } \text{point-one-def}: & \quad \text{point-one} = \text{Point } 1 \ 0 \\
\text{definition } \text{point-add-def}: & \quad A + B = \text{Point } (\text{abscissa } A + \text{abscissa } B) (\text{ordinate } A + \text{ordinate } B) \\
\text{definition } \text{point-minus-def}: & \quad - A = \text{Point } (- \text{abscissa } A) (- \text{ordinate } A) \\
\text{definition } \text{point-diff-def}: & \quad A - (B::\text{point}) = A + - B \\
\text{lemma } \text{Point-eq-0 } [\text{simp}]: & \quad \text{Point } xA \ yA = 0 \iff (xA = 0 \land yA = 0) \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-abscissa-zero } [\text{simp}]: & \quad \text{abscissa } 0 = 0 \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-ordinate-zero } [\text{simp}]: & \quad \text{ordinate } 0 = 0 \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-add } [\text{simp}]: & \quad \text{Point } xA \ yA + \text{Point } xB \ yB = \text{Point } (xA + xB) (yA + yB) \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-abscissa-add } [\text{simp}]: & \quad \text{abscissa } (A + B) = \text{abscissa } A + \text{abscissa } B \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-ordinate-add } [\text{simp}]: & \quad \text{ordinate } (A + B) = \text{ordinate } A + \text{ordinate } B \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-minus } [\text{simp}]: & \quad - (\text{Point } xA \ yA) = \text{Point } (-xA) (-yA) \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-abscissa-minus } [\text{simp}]: & \quad \text{abscissa } (-A) = - \text{abscissa } (A) \\
& \quad \langle \text{proof} \rangle \\
\text{lemma } \text{point-ordinate-minus } [\text{simp}]: & \quad \text{ordinate } (-A) = - \text{ordinate } (A) \\
& \quad \langle \text{proof} \rangle 
\end{align*}
\]
lemma \textit{point-diff} [simp]:
\[ \text{Point } xA \ yA - \text{Point } xB \ yB = \text{Point } (xA - xB) \ (yA - yB) \]
\langle \text{proof} \rangle

lemma \textit{point-abscissa-diff} [simp]:
\[ \text{abscissa } (A - B) = \text{abscissa } (A) - \text{abscissa } (B) \]
\langle \text{proof} \rangle

lemma \textit{point-ordinate-diff} [simp]:
\[ \text{ordinate } (A - B) = \text{ordinate } (A) - \text{ordinate } (B) \]
\langle \text{proof} \rangle

instance \langle \text{proof} \rangle \end

2.3 Metric Space

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

\textit{instantiation} \textit{point} :: \textit{metric-space}

\textit{begin}

definition \textit{point-dist-def}:
\[ \text{dist } A \ B = \sqrt{(\text{abscissa } (A - B))^2 + (\text{ordinate } (A - B))^2} \]

definition \textit{open-point-def}:
\[ \text{open } (S :: \text{point set}) <\rightarrow> (\forall \ A \in S. \exists \epsilon > 0. \forall \ B. \text{dist } B \ A < \epsilon \rightarrow \ B \in S) \]

lemma \textit{point-dist} [simp]:
\[ \text{dist } (\text{Point } xA \ yA) \ (\text{Point } xB \ yB) = \sqrt{(xA - xB)^2 + (yA - yB)^2} \]
\langle \text{proof} \rangle

lemma \textit{real-sqrt-diff-squares-triangle-ineq}:
\[ \text{fixes } a \ b \ c \ d :: \text{real} \]
\[ \text{shows } \sqrt{(a - c)^2 + (b - d)^2} \leq \sqrt{(a^2 + b^2)} + \sqrt{(c^2 + d^2)} \]
\langle \text{proof} \rangle

instance \langle \text{proof} \rangle \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 \( B \)) \( \ast \) (ordinate \( C \) – ordinate \( D \)) = (ordinate \( A \) – ordinate \( B \)) \( \ast \) (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 \( A M B \) \( \land \) collinear \( C M D \))

2.5 Reals definable with square roots

The inductive set \( \text{radical-sqrt} \) 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 \( \text{radical-sqrt} \) because it is only defined with rationals and square roots of radicals.

inductive-set \( \text{radical-sqrt} :: \text{real set} \) where
  \( x \in Q \Rightarrow x \in \text{radical-sqrt} \)
  \( x \in \text{radical-sqrt} \Rightarrow -x \in \text{radical-sqrt} \)
  \( x \in \text{radical-sqrt} \Rightarrow x \neq 0 \Rightarrow 1/x \in \text{radical-sqrt} \)
  \( x \in \text{radical-sqrt} \Rightarrow y \in \text{radical-sqrt} \Rightarrow x+y \in \text{radical-sqrt} \)
  \( x \in \text{radical-sqrt} \Rightarrow y \in \text{radical-sqrt} \Rightarrow x*y \in \text{radical-sqrt} \)
  \( x \in \text{radical-sqrt} \Rightarrow x \geq 0 \Rightarrow \sqrt{x} \in \text{radical-sqrt} \)

Here, we list some rules that will be used to prove that a given real is in \( \text{radical-sqrt} \).

Given two reals in \( \text{radical-sqrt} \) \( x \) and \( y \), the subtraction \( x - y \) is also in \( \text{radical-sqrt} \).

lemma radical-sqrt-rule-subtraction:
  \( x \in \text{radical-sqrt} \Rightarrow y \in \text{radical-sqrt} \Rightarrow x+y \in \text{radical-sqrt} \)
  \( \langle proof \rangle \)
Given two reals in $\text{radical-sqrt } x$ and $y$, and $y \neq 0$, the division $x/y$ is also in $\text{radical-sqrt}$.

**Lemma** radical-sqrt-rule-division:
\[
x \in \text{radical-sqrt} \Rightarrow y \in \text{radical-sqrt} \Rightarrow y \neq 0 \Rightarrow x/y \in \text{radical-sqrt}
\]

(proof)

Given a positive real $x$ in $\text{radical-sqrt}$, its square $x^2$ is also in $\text{radical-sqrt}$.

**Lemma** radical-sqrt-rule-power2:
\[
x \in \text{radical-sqrt} \Rightarrow x \geq 0 \Rightarrow x^2 \in \text{radical-sqrt}
\]

(proof)

Given a positive real $x$ in $\text{radical-sqrt}$, its cube $x^3$ is also in $\text{radical-sqrt}$.

**Lemma** radical-sqrt-rule-power3:
\[
x \in \text{radical-sqrt} \Rightarrow x \geq 0 \Rightarrow x^3 \in \text{radical-sqrt}
\]

(proof)

### 2.6 Introduction of the datatype expr which represents radical expressions

An expression $\text{expr}$ is either a rational constant: $\text{Const}$ 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** $\text{expr} = \text{Const } \text{rat} | \text{Negation } \text{expr} | \text{Inverse } \text{expr} | \text{Addition } \text{expr} \ \text{expr} | \text{Multiplication } \text{expr} \ \text{expr} | \text{Sqrt } \text{expr}$

The function $\text{translation}$ translates a given expression into its equivalent real.

**Fun** translation :: $\text{expr} => \text{real } ((2\{\frac{1}{2}\}))$

where
\[
\text{translation} (\text{Const } x) = \text{of-rat } x |
\text{translation} (\text{Negation } e) = - \text{translation } e |
\text{translation} (\text{Inverse } e) = (1::\text{real}) / \text{translation } e |
\text{translation} (\text{Addition } e1 \ e2) = \text{translation } e1 + \text{translation } e2 |
\text{translation} (\text{Multiplication } e1 \ e2) = \text{translation } e1 * \text{translation } e2 |
\text{translation} (\text{Sqrt } e) = (\text{if } \text{translation } e < 0 \ \text{then } 0 \ \text{else } \text{sqr } (\text{translation } e))
\]

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

**Fun** radicals :: $\text{expr} => \text{expr set}$
where
radicals $\{\text{Const } x\} = \{\}$
radicals $\{\text{Negation } e\} = (\text{radicals } e)\$
radicals $\{\text{Inverse } e\} = (\text{radicals } e)\$
radicals $\{\text{Addition } e1 e2\} = ((\text{radicals } e1) \cup (\text{radicals } e2))\$
radicals $\{\text{Multiplication } e1 e2\} = ((\text{radicals } e1) \cup (\text{radicals } e2))\$
radicals $\{\text{Sqrt } e\} = (\text{if } \|e\| < 0 \text{ then radicals } e \text{ else } \{e\} \cup (\text{radicals } e))$

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:** $r \in \text{radicals } e \implies \text{radicals } r \subset \text{radicals } e$

*(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:**

$x \in \text{radical-sqrt} \implies (\exists e. \|e\| = x)$

*(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: $\text{expr} = \text{Addition} (\text{Sqrt} (\text{Addition} (\text{Const } a) \text{ Sqrt} (\text{Const } b))) (\text{Sqrt} (\text{Addition} (\text{Const } c) (\text{Sqrt} (\text{Sqrt} (\text{Const } d)))))$, where $a$, $b$, $c$ and $d$ are rationals and which can be translated as follows: $\|expr\|$

$= \sqrt{a + \sqrt{b} + \sqrt{c + \sqrt{d}}}$. The order of $expr$ is $\text{max}(2, 3) = 3$.

**fun order :: expr => nat**

where
order $\{\text{Const } x\} = 0$
order $\{\text{Negation } e\} = \text{order } e$
order $\{\text{Inverse } e\} = \text{order } e$
order $\{\text{Addition } e1 e2\} = \text{max } (\text{order } e1) (\text{order } e2)$
order $\{\text{Multiplication } e1 e2\} = \text{max } (\text{order } e1) (\text{order } e2)$
order $\{\text{Sqrt } e\} = 1 + \text{order } e$

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:**

$s \in \text{radicals } r \implies (\text{order } s) < (\text{order } r)$

*(proof)*

The following theorem is the converse of the previous lemma.

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

$(\text{order } s) \geq (\text{order } r) \implies \neg (s \in \text{radicals } r)$

*(proof)*
An expression $r$ cannot be one of its own radicals.

**lemma** not-in-own-radicals:
\[ \neg (r \in \text{radicals } r) \]

(proof)

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

**lemma** radicals-empty-rational: radicals $e = \{\}$ $\implies \{e\} \in \mathbb{Q}$

(proof)

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

**lemma** finite-set-has-max:
\[ \text{finite } (s::\text{nat set}) \implies s \neq \{\} \implies \exists k \in s. \forall p \in s. p \leq k \]

(proof)

There is a finite number of radicals in an expression.

**lemma** finite-radicals: finite (radicals $e$)

(proof)

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: $\{expr\} = \sqrt{a + \sqrt{b + \sqrt{c + \sqrt{d}}}}$. The set radicals of expr is $\{\text{Addition (Const } a) \text{ Sqrt (Const } b), \text{Addition (Const } c) \text{ (Sqrt (Sqrt (Const } d)))}, \text{Sqrt (Const } d), \text{Const } d\}$; therefore, the set order-radicals of this set is $\{1, 0, 2, 1, 0\}$.

**fun** order-radicals:: expr set $\Rightarrow$ nat set

**where** order-radicals $s = \{y. \exists x \in s. y = \text{order } x\}$

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.

**lemma** finite-order-radicals:
\[ \text{radicals } e \neq \{\} \implies \text{finite } (\text{radicals } e) \implies \text{order-radicals } (\text{radicals } e) \neq \{\} \land \text{finite } (\text{order-radicals } (\text{radicals } e)) \]

(proof)

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:
\[ \text{order-radicals } (\text{radicals } e) \neq \{\} \implies \text{finite } (\text{order-radicals } (\text{radicals } e)) \implies \exists r. (r \in \text{radicals } e) \land (\forall s \in (\text{radicals } e). (\text{order } r \geq \text{order } s)) \]
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:

\[
e = \text{Addition} \left( \text{Sqrt} \left( \text{Addition} \left( \text{Const} \ a \right) \right) \right) \left( \text{Sqrt} \left( \text{Addition} \left( \text{Const} \ c \right) \right) \right),
\]

where \( a, b, c \) and \( d \) are rationals and which can be translated as follows:

\[
\| e \| = \sqrt{a} + \sqrt{b} + \sqrt{c + \sqrt{d}}.
\]

The possible upmost radicals in this expression are \( \text{Addition} \left( \text{Const} \ a \right) \left( \text{Sqrt} \left( \text{Const} \ b \right) \right) \) or \( \text{Addition} \left( \text{Const} \ c \right) \left( \text{Sqrt} \left( \text{Sqrt} \left( \text{Const} \ d \right) \right) \right) \).

**Lemma** upmost-radical-sqrt2:

\[
\text{radicals } e \neq \{\} \implies \exists r \in \text{radicals } e. \forall s \in \text{radicals } e. r \not\in \text{radicals } s
\]

**Proof**

The following 7 lemmas are used to prove the main lemma radial-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 \( \text{Sqrt} \ r \) is not necessarily the term of highest order.

**Lemma** radial-sqrt-normal-form-sublemma:

\[
(x::\text{real}) - b) \ast (a + b) = a \ast a - b \ast b
\]

**Proof**

**Lemma** eq-sqrt-squared:

\[
(x::\text{real}) \geq 0 \implies (\text{sqrt} x) \ast (\text{sqrt} x) = x
\]

**Proof**

**Lemma** radical-sqrt-normal-form-lemma4:

assumes \( z \geq 0 \ x \neq y \ast \text{sqrt} \ z \)

shows

\[
1 / (x + y \ast \text{sqrt} \ z) = \\
(x \ast x - y \ast y \ast z) / (x \ast x - y \ast y \ast z)
\]

**Proof**

**Lemma** radical-sqrt-normal-form-lemma:

fixes \( e::\text{expr} \)

assumes radicals \( e \neq \{\} \)

and \( \forall s \in \text{radicals } e. r \not\in \text{radicals } s \)

and \( r : \text{radicals } e \)

shows \( 3 \ a, b, 0 \leq \| r \| \text{ & } \| e \| = \| a \| + \| b \| \sqrt{\| r \|} \text{ & } \text{radicals } a \cup \text{radicals } b \cup \text{radicals } r \subseteq \text{radicals } e \text{ & } \)

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

**Theorem** `radical-sqrt-normal-form`:

\[
\text{radicals } e \neq \{\} \implies \\
\exists r \in \text{radicals } e. \\
\forall a, b. \{e\} = \{\text{Addition } a \text{ (Multiplication } b \text{ (Sqrt } r))\} \land \{r\} \geq 0 \land \\
\text{radicals } a \cup \text{radicals } b \cup \text{radicals } r \subseteq \text{radicals } e \land \\
r \notin \text{radicals } a \cup \text{radicals } b \cup \text{radicals } r
\]

(\text{proof})

### 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 (\textit{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-step-lemma`:

\[
\text{fixes } P :: \text{real set} \\
\text{assumes } Nats [\text{THEN set-mp, intro}]: Nats \subseteq P \\
\text{and } \text{Neg}: \forall x \in P. -x \in P \\
\text{and } \text{Inv}: \forall x \in P. x \neq 0 \implies 1/x \in P \\
\text{and } \text{Add}: \forall x \in P. \forall y \in P. x+y \in P \\
\text{and } \text{Mult}: \forall x \in P. \forall y \in P. x*y \in P \\
\text{and } a: (a \in P) \text{ and } b: (b \in P) \text{ and } c: (c \in P) \\
\text{and eq0: } z^3 + a*z^2 + b*z + c = 0 \\
\text{and u: (a \in P)} \\
\text{and v: (v \in P)} \\
\text{and s: ((s * s) \in P)} \\
\text{and z: (z = u + v * s)} \\
\text{shows } \exists w \in P. w^3 + a*w^2 + b*w + c = 0
\]

(\text{proof})

**Lemma** `cubic-root-radical-sqrt-step-lemma-sqrt`:

\[
\text{assumes } Nats [\text{THEN set-mp, intro}]: Nats \subseteq P \\
\text{and } \text{Neg}: \forall x \in P. -x \in P \\
\text{and } \text{Inv}: \forall x \in P. x \neq 0 \implies 1/x \in P \\
\text{and } \text{Add}: \forall x \in P. \forall y \in P. x+y \in P \\
\text{and } \text{Mult}: \forall x \in P. \forall y \in P. x*y \in P \\
\text{and } a: (a \in P) \text{ and } b: (b \in P) \text{ and } c: (c \in P) \\
\text{and eq0: } z^3 + a*z^2 + b*z + c = 0 \\
\text{and u: (u \in P)} \\
\text{and v: (v \in P)} \\
\text{and s: (s \in P)}
\]

(\text{proof})
and \( s \) Positive: \( s \geq 0 \)
and \( z \): \( z = u + v \times \sqrt{s} \)
shows \( \exists w \in P. w^3 + a \times w^2 + b \times w + c = 0 \)
⟨proof⟩

lemma cubic-root-radical-sqrt-lemma:
fixes \( c :: \text{expr} \)
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: \( \{e\}^3 + a \times \{e\}^2 + b \times \{e\} + c = 0 \)
shows \( \exists e1. \) radicals \( e1 \subset \text{radicals } e \) & \( ( \{e1\}^3 + a \times \{e1\}^2 + b \times \{e1\} + c = 0 ) \)
⟨proof⟩

lemma cubic-root-radical-sqrt:
assumes \( abc : a \in \mathbb{Q} \ b \in \mathbb{Q} \ c \in \mathbb{Q} \)
shows \( \text{card } ( \text{radicals } e ) = n \implies \{e\}^3 + a \times \{e\}^2 + b \times \{e\} + c = 0 \implies \exists x \in \mathbb{Q}. x^3 + a \times x^2 + b \times x + c = 0 \)
⟨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 \( b \in \mathbb{Q} \) and \( c \in \mathbb{Q} \)
and \( x : x \in \text{radical-sqrt} \)
and \( x-eqn: x^3 + a \times x^2 + b \times x + c = 0 \)
shows \( c : \exists x \in \mathbb{Q}. x^3 + a \times x^2 + b \times x + c = 0 \)
⟨proof⟩

2.8 Important properties of radicals

lemma sqrt-roots:
\( y^2=x \implies x \geq 0 \) & \( (\sqrt{x})=y \mid \sqrt{(-y)}=-y \)
⟨proof⟩

lemma radical-sqrt-linear-equation:
assumes \( a : a \in \text{radical-sqrt} \)
and \( b : b \in \text{radical-sqrt} \)
and \( abNotNull: \neg (a = 0 \& b = 0) \)
and \( eq0: a \times x + b = 0 \)
shows \( x \in \text{radical-sqrt} \)
⟨proof⟩

lemma radical-sqrt-simultaneous-linear-equation:
assumes \( a : a \in \text{radical-sqrt} \)
and \( b : b \in \text{radical-sqrt} \)
and \( c : c \in \text{radical-sqrt} \)
and \( d : d \in \text{radical-sqrt} \)
and \( e \in \text{radical-sqrt} \)
and \( f \in \text{radical-sqrt} \)
and \( \text{NotNull} \): \( \neg \left( a + e - b + d = 0 \land a + f - c + d = 0 \land e + c = b + f \right) \)
and \( \text{eq0} \): \( a + x + b + y = c \)
and \( \text{eq1} \): \( d + x + e + y = f \)
shows \( x \in \text{radical-sqrt} \) & \( y \in \text{radical-sqrt} \)

\( \langle \text{proof} \rangle \)

**lemma radical-sqrt-quadratic-equation:**

assumes \( a \in \text{radical-sqrt} \)
and \( b \in \text{radical-sqrt} \)
and \( c \in \text{radical-sqrt} \)
and \( \text{eq0} \): \( a \cdot x^2 + b \cdot x + c = 0 \)
and \( \text{NotNull} \): \( \neg \left( a = 0 \land b = 0 \land c = 0 \right) \)
shows \( x \in \text{radical-sqrt} \)

\( \langle \text{proof} \rangle \)

**lemma radical-sqrt-simultaneous-linear-quadratic:**

assumes \( a \in \text{radical-sqrt} \)
and \( b \in \text{radical-sqrt} \)
and \( c \in \text{radical-sqrt} \)
and \( d \in \text{radical-sqrt} \)
and \( e \in \text{radical-sqrt} \)
and \( f \in \text{radical-sqrt} \)
and \( \text{NotNull} \): \( \neg \left( d = 0 \land e = 0 \land f = 0 \right) \)
and \( \text{eq0} \): \( (x-a)^2 + (y-b)^2 = c \)
and \( \text{eq1} \): \( d \cdot x + e \cdot y = f \)
shows \( x \in \text{radical-sqrt} \) & \( y \in \text{radical-sqrt} \)

\( \langle \text{proof} \rangle \)

**lemma radical-sqrt-simultaneous-quadratic-quadratic:**

assumes \( a \in \text{radical-sqrt} \)
and \( b \in \text{radical-sqrt} \)
and \( c \in \text{radical-sqrt} \)
and \( d \in \text{radical-sqrt} \)
and \( e \in \text{radical-sqrt} \)
and \( f \in \text{radical-sqrt} \)
and \( \text{NotEqual} \): \( \neg \left( a = d \land b = e \land c = f \right) \)
and \( \text{eq0} \): \( (x-a)^2 + (y-b)^2 = c \)
and \( \text{eq1} \): \( (x-d)^2 + (y-e)^2 = f \)
shows \( x \in \text{radical-sqrt} \) & \( y \in \text{radical-sqrt} \)

\( \langle \text{proof} \rangle \)

2.9 Important properties of geometrical points which coordinates are radicals

**lemma radical-sqrt-line-line-intersection:**
\textbf{assumes} \(\text{absA: } (\text{abscissa } A) \in \text{radical-sqrt}\) \\
and \(\text{ordA: } (\text{ordinate } A) \in \text{radical-sqrt}\) \\
and \(\text{absB: } (\text{abscissa } B) \in \text{radical-sqrt}\) \\
and \(\text{ordB: } (\text{ordinate } B) \in \text{radical-sqrt}\) \\
and \(\text{absC: } (\text{abscissa } C) \in \text{radical-sqrt}\) \\
and \(\text{ordC: } (\text{ordinate } C) \in \text{radical-sqrt}\) \\
and \(\text{absD: } (\text{abscissa } D) \in \text{radical-sqrt}\) \\
and \(\text{ordD: } (\text{ordinate } D) \in \text{radical-sqrt}\) \\
and \(\text{notParallel: } \neg (\text{parallel } A B C D)\) \\
and \(\text{isIntersec: } \text{is-intersection } X A B C D\) \\
\textbf{shows} (\(\text{abscissa } X\) \(\in \text{radical-sqrt}\) \\
& (\(\text{ordinate } X\) \(\in \text{radical-sqrt}\)) \\
\langle \text{proof} \rangle

\textbf{lemma} \text{radical-sqrt-line-circle-intersection:} \\
\textbf{assumes} \(\text{absA: } (\text{abscissa } A) \in \text{radical-sqrt}\) \\
and \(\text{ordA: } (\text{ordinate } A) \in \text{radical-sqrt}\) \\
and \(\text{absB: } (\text{abscissa } B) \in \text{radical-sqrt}\) \\
and \(\text{ordB: } (\text{ordinate } B) \in \text{radical-sqrt}\) \\
and \(\text{absC: } (\text{abscissa } C) \in \text{radical-sqrt}\) \\
and \(\text{ordC: } (\text{ordinate } C) \in \text{radical-sqrt}\) \\
and \(\text{absD: } (\text{abscissa } D) \in \text{radical-sqrt}\) \\
and \(\text{ordD: } (\text{ordinate } D) \in \text{radical-sqrt}\) \\
and \(\text{absE: } (\text{abscissa } E) \in \text{radical-sqrt}\) \\
and \(\text{ordE: } (\text{ordinate } E) \in \text{radical-sqrt}\) \\
and \(\text{notEqual: } A \neq B\) \\
and \(\text{colin: } \text{collinear } A X B\) \\
and \(\text{eqDist: } (\text{distance } C X = \text{distance } D E)\) \\
\textbf{shows} (\(\text{abscissa } X\) \(\in \text{radical-sqrt}\) \\
& (\(\text{ordinate } X\) \(\in \text{radical-sqrt}\)) \\
\langle \text{proof} \rangle

\textbf{lemma} \text{radical-sqrt-circle-circle-intersection:} \\
\textbf{assumes} \(\text{absA: } (\text{abscissa } A) \in \text{radical-sqrt}\) \\
and \(\text{ordA: } (\text{ordinate } A) \in \text{radical-sqrt}\) \\
and \(\text{absB: } (\text{abscissa } B) \in \text{radical-sqrt}\) \\
and \(\text{ordB: } (\text{ordinate } B) \in \text{radical-sqrt}\) \\
and \(\text{absC: } (\text{abscissa } C) \in \text{radical-sqrt}\) \\
and \(\text{ordC: } (\text{ordinate } C) \in \text{radical-sqrt}\) \\
and \(\text{absD: } (\text{abscissa } D) \in \text{radical-sqrt}\) \\
and \(\text{ordD: } (\text{ordinate } D) \in \text{radical-sqrt}\) \\
and \(\text{absE: } (\text{abscissa } E) \in \text{radical-sqrt}\) \\
and \(\text{ordE: } (\text{ordinate } E) \in \text{radical-sqrt}\) \\
and \(\text{eqDist0: } \text{distance } A X = \text{distance } B C\) \\
and \(\text{eqDist1: } \text{distance } D X = \text{distance } E F\) \\
and \(\text{notEqual: } \neg (A = D \& \text{distance } B C = \text{distance } E F)\) \\
\textbf{shows} (\(\text{abscissa } X\) \(\in \text{radical-sqrt}\) \\
& (\(\text{ordinate } X\) \(\in \text{radical-sqrt}\)) \\
\langle \text{proof} \rangle

\textbf{2.10 Definition of the set of constructible points} \\
\textbf{inductive-set} \text{constructible :: point set} \\
\textbf{where} \\
(\(M \in \text{points} \& (\text{abscissa } M) \in \mathbb{Q} \& (\text{ordinate } M) \in \mathbb{Q}\) \(\implies M \in \text{constructible}\)) \\
(\(A \in \text{constructible} \& B \in \text{constructible} \& C \in \text{constructible} \& D \in \text{constructible} \& \neg \text{parallel } A B C D \& \text{is-intersection } M A B C D\) \(\implies M \in \text{constructible}\)) \\
(\(A \in \text{constructible} \& B \in \text{constructible} \& C \in \text{constructible} \& D \in \text{constructible} \& \neg \text{A} = B \& \text{collinear } A M B \& \text{distance } C M = \text{distance } D\))
\[ E \implies M \in \text{constructible} \]
\[ (A \in \text{constructible} \land B \in \text{constructible} \land C \in \text{constructible} \land D \in \text{constructible} \land E \in \text{constructible} \land F \in \text{constructible} \land \neg (A = D \land \text{distance } B C = \text{distance } E F) \land \text{distance } A M = \text{distance } B C \land \text{distance } D M = \text{distance } E F) \implies M \in \text{constructible} \]

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

\text{lemma} \ constructible-radical-sqrt:
\text{assumes} \ h: M \in \text{constructible}
\text{shows} (\text{abscissa } M) \in \text{radical-sqrt} \land (\text{ordinate } M) \in \text{radical-sqrt}
\langle \text{proof} \rangle

2.12 Proving the impossibility of duplicating the cube

\text{lemma} \ impossibility-of-doubling-the-cube-lemma:
\text{assumes} \ x: x \in \text{radical-sqrt}
\text{and} \ x\text{-eqn: } x^3 = 2
\text{shows} False
\langle \text{proof} \rangle

\text{theorem} \ impossibility-of-doubling-the-cube:
\[ x^3 = 2 \implies (\text{Point } x 0) \notin \text{constructible} \]
\langle \text{proof} \rangle

2.13 Proving the impossibility of trisecting an angle

\text{lemma} \ impossibility-of-trisecting-pi-over-3-lemma:
\text{assumes} \ x: x \in \text{radical-sqrt}
\text{and} \ x\text{-eqn: } x^3 - 3 * x - 1 = 0
\text{shows} False
\langle \text{proof} \rangle

\text{theorem} \ impossibility-of-trisecting-angle-pi-over-3:
\text{Point } (\cos (\pi / 9)) 0 \notin \text{constructible}
\langle \text{proof} \rangle

end

References