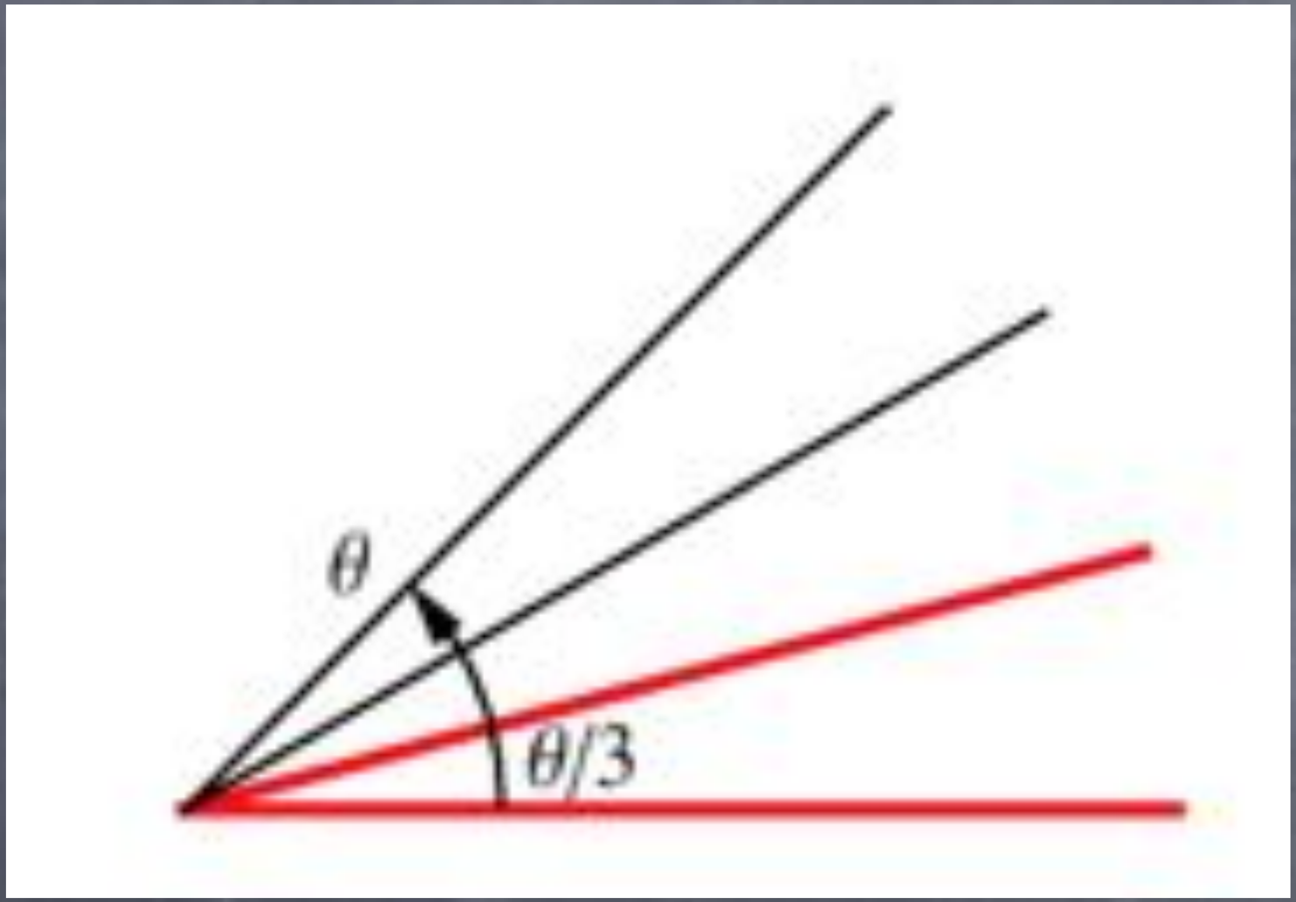
Proving the impossibility of trisecting an angle and doubling the cube

Ralph Romanos and Lawrence Paulson,
University of Cambridge

Duplicating the cube

(using only ruler and compass)

… and trisecting the angle



A brief history

- Posed by classical Greek mathematicians
- Proved impossible in the 19th century (Wantzel, 1837)
- Recently included on a list of 100 well-known theorems
- John Harrison had already formalised a proof using HOL Light.

An elementary proof

- Textbook proofs of the theorem are built upon Galois theory or field extensions.
- The Isabelle formalization follows, but simplifies, Jean-Claude Carrega:

  J. C. Carrega. Theory of fields. Rules and a pair of compasses. Hermann, 1981.

Core concepts

- RADICAL VALUES: those constructed using the operations $+ \; - \; \times \; / \; \sqrt{}$
- CONSTRUCTIBLE POINTS: those having rational coordinates, or defined as the intersection of
  - two lines
  - a line and a circle
  - two circles

Simplifying Wantzel's theorem

- The full theorem refers to a series of field extensions ending in the construction of x — which is constructible iff it is the root of an irreducible polynomial of degree 2^n.
- Therefore, certain regular polygons (e.g. seven-sided) are not constructible.
- Our proof replaces field extensions by radical values and only considers cubic equations.

Lemma 1:

(on a cubic equation with rational coefficients)

$$x^3 + ax^2 + bx + c = 0$$

- If it has a RADICAL root
- ...then it has a RATIONAL root.

Lemma 2

All constructible points
have radical coordinates

Lemmas 3 and 4:

These equations have no rational roots

$$x^3 - 2 = 0$$

$$x^3 - 3x - 1 = 0$$

The first corresponds to duplicating the cube

... and the second to trisecting a 60° angle.

Notes on the Isabelle Formalization

- MANY tedious calculations
- Over 1500 lines; 62 lemmas and theorems
- 3 times the length of the informal mathematics

Formal preliminaries

- points in two dimensions shown to be a metric space
- basic definitions of plane geometry
- radical values (defined inductively)
- radical expressions: an abstract syntax for radical values

Normal forms of radical expressions

- Every nontrivial radical expression e can be written in the form $a+b\sqrt{r}$
- ... where the radicals in a, b, r are only those of e, excluding r itself.

On cubic equations

- Consider a field $F \subseteq \mathbb{R}$ containing the integers.
- If cubic equation over this field has a real root of the form $u+v\sqrt{s}$ (for $u, v, s \in F$)
- ...then it has a root in F.
- Proof: a huge case analysis

Simplifying the roots of cubic equations

- The previous result lets us decrease the number of radicals in a root of a cubic
- (working with formalised expressions)
- Therefore, by induction on the number of radicals...
- if there is a RADICAL root, then there is a RATIONAL root.

Constructible points

- A straightforward inductive definition
- THEOREM: the coordinates of constructible points are radical values
- PROOF: the roots of various quadratic equations are radical values.

Completing the proof: detailed calculations

- the cubic equations for duplicating the cube and trisecting the angle
- ... have no rational solutions
- ... and therefore no constructible ones

Trisecting the angle

- cos 60° equals ½, so a 60° angle is constructible
- cos 20° is the solution of a cubic, and therefore not constructible
- Therefore, a 60° angle cannot be trisected.

Final remarks

- This was the MPhil project of the first author at Cambridge.
- Detailed calculations seem inevitable, but with some effort, the proofs can be simplified.
- A formal theory of field extensions would allow the full result to be reproduced.