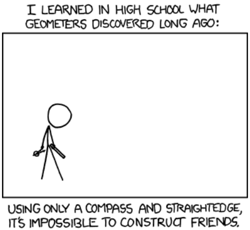
Constructible Numbers

Thomas Desautels

Gatsby Computational Neuroscience Unit, UCL

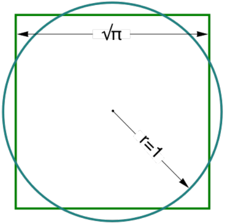
7 May 2015



Squaring the circle

An ancient Greek problem in mathematics:

- Can you construct (using only compass and straightedge) a square of equal area to a reference circle?



This problem (and others) were solved by the work of Pierre Wantzel (1837, this talk) and the Lindemann-Weierstrass Theorem (1882).

Wantzel's Contribution

Definition (Constructible number)

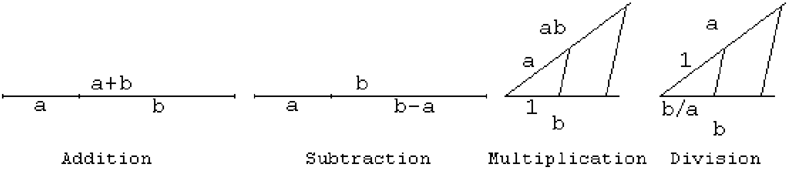
A number which is the length of a line segment which can be constructed in a finite number of steps using a compass and straightedge, beginning from a line segment of unit length.

It turns out that the key question is, “What numbers are constructible?”

Outline

1. Introduction
2. Basic Operations
3. Extension Fields $\mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_n}]$
4. $\exists m_1, \ldots, m_n : a \in \mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_n}] \implies a$ is constructible
5. a is constructible $\implies \exists m_1, \ldots, m_n : a \in \mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_n}]$
6. Capstone

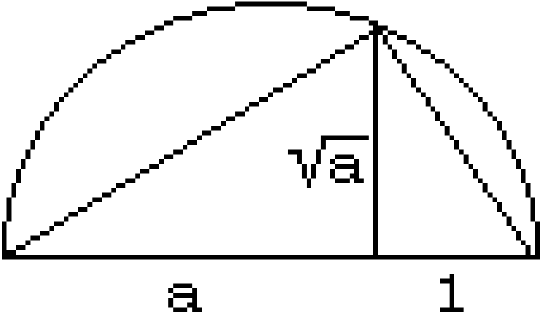
Basic Operations: Arithmetic



Can thus construct any integer multiple of the unit segment we started with ($\mathbb{Z}$) or rational number ($\mathbb{Q}$).

$\mathbb{Q}$ is closed under these operations and is thus a *field*.

Basic Operations: Square Roots



We can also construct the square root of any length we have so far constructed.

These are the only operations we can implement, in terms of the construction of new length line segments.

Extension Fields

For field F, $F' = \{a + bc\}, \forall a, b \in F$, for some particular $c \notin F$.
F' is a field, and is called an *extension field*.
Denote the extension field of F by scalar addition of c as $F[c] = F'$.
Further, for $c' \notin F[c]$, denote the extension with respect to c' as $F[c, c']$.

One step

From $\mathbb{Q}$ we can construct any length $c \in \mathbb{Q}$ or $c = \sqrt{a}, a \in \mathbb{Q}$. If $c \notin \mathbb{Q}$, then we may use c to construct any number in the extension field $\mathbb{Q}[c]$.

$\exists m_1, \ldots, m_n$ constructible: $a \in \mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_n}] \implies a$ is constructible

If $m_1, \ldots, m_n$ are constructible, we can construct them in a finite number of steps.
Then we can sequentially apply the operations above to allow construction of elements in $\mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_i}], \forall i \leq n$, allowing the construction of a after a finite number of additional steps.

a is constructible $\implies \exists m_1, \ldots, m_n : a \in \mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_n}]$

Constructibility of a implies a finite number of applications of our operations to obtain a line segment of length a (take as N). Any line segment constructed in a single one of our operations from a set of lengths in $\mathbb{F}$ must be in $\mathbb{F} \cup \mathbb{F}[c]$ for $c = \sqrt{a}, a \in \mathbb{F}$. Our starting set is $\{1\}$; any length a which can be constructed in N or fewer steps must be contained in the set $\mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_N}]$, where $m_i \in \mathbb{Q}[\sqrt{m_1}, \ldots, \sqrt{m_{i-1}}] \forall i \leq N$.

π is transcendental $\implies$ not constructible

Lindemann-Weierstrass Theorem shows that π is transcendental, i.e., $\nexists$ a set of integer coefficients such that π is a root of a polynomial equation with these coefficients.
Constructible numbers are algebraic, i.e., are the solutions of such integer-coefficient polynomial equations.
Therefore, π is not constructible, so neither is $\sqrt{\pi}$, and thus the circle cannot be squared.

Sources

Proof is (badly) following http://www.cut-the-knot.org/arithmetic/rational.shtml. Some graphics from there.
Some graphics from Wikipedia.
Others from XKCD, drywall-emporium.com, http://www.ck12.org/user%3AamRvdXRoYXRAd2lja2VuYnVyZy5rMT
Geometry/section/1.3/