4 Euclidean Constructions & Constructibility

Euclid's first three postulates specify what are known as *ruler and compass constructions*:

1. Give two points, we may join them with a segment.
2. A segment may be prolonged in either direction.
3. Give a point and a segment, one may construct the circle centered at the point, with radii congruent to the segment.

These constructions were especially important to the ancient Greeks, who approached proof in something of a practical manner. Euclid's postulates 4 and 5 were essentially only used in Book I of the *Elements* in order to prove that certain ruler and compass constructions did what Euclid claimed.

In this section we provide a more modern take on constructions. The entire discussion is embedded inside analytic geometry, indeed we'll work within the complex numbers $\mathbb{C}$.

Definition 4.1. 1. Let S be a set of points in $\mathbb{C}$.

   (a) A line is *constructible in one step from S* if it passes through two distinct points of S.
   (b) A circle is *constructible in one step from S* if it has center in S and radius equal to the distance between two points in S.
   (c) A angle is *constructible in one step from S* if it is the angle between two lines constructible in one step from S.
   (d) A point is *constructible in one step from S* if it is the intersection of two of the above lines or circles.
   (e) A point $P \in \mathbb{C}$ is *constructible from S* if there is a finite sequence of points $P_1, P_2, \ldots, P_n = P$ such that

$$\forall j,\ P_j \text{ is constructible in one step from } S_j = S \cup \{P_1, \ldots, P_{j-1}\}$$

2. (a) A complex number z is *constructible* if it is constructible from the set $\{0, 1\}$.
   (b) A set $S \subseteq \mathbb{C}$ is constructible if every element $z \in S$ is constructible.
   (c) A line, circle or angle is constructible if is constructible in one step from some constructible set S.
3. The symbol $\mathcal{C}$ denotes the set of *constructible numbers.*

The primary goal of this section is to describe the constructible numbers $\mathcal{C}$ as concretely as possible. We can easily summarize the first part of what follows:

Theorem 4.2. *$\mathcal{C}$ is a subfield of $\mathbb{C}$ which is closed under complex conjugation. Otherwise said,*

1. *Every rational number is constructible.*
2. *The constructible numbers are closed under addition, subtraction, multiplication and division.*
3. *If $z \in \mathcal{C}$ then $\overline{z} \in \mathcal{C}$.*

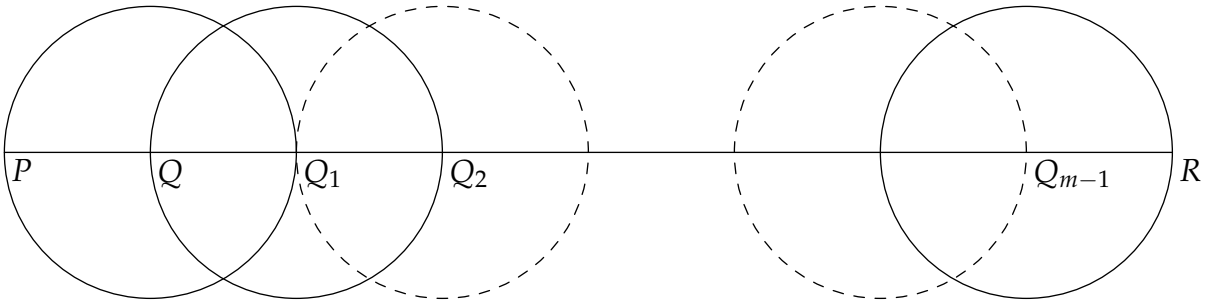
The remaining challenge is to figure out exactly what other constructions are allowed beyond simply the field operations.

Proving Theorem 4.2

We start with a few basic constructions: several of these arguments are almost verbatim from Euclid.

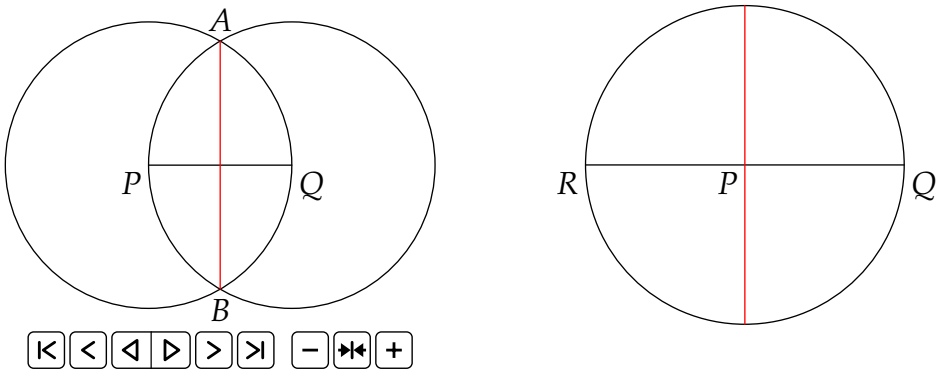
Proposition 4.3. *Let P and Q be distinct points. For any $m \in \mathbb{N}_{\geq 2}$, the point R is constructible where $|PR| = m\,|PQ|$ and Q lies between P and R.*

Proof. This is essentially induction on m: at each step draw a circle of radius $|PQ|$ centered at the previously constructed point Q_i. We obtain a sequence $Q = Q_0, Q_1, Q_2, \ldots, R = Q_m$. ∎



Proposition 4.4. *Let P and Q be distinct points. Then the perpendiculars to $\overline{PQ}$ through P, Q and the midpoint of $\overline{PQ}$ are all constructible from $\{P, Q\}$.*

Proof. For the midpoint, draw circles centered at P and Q respectively, with radius $|PQ|$. The intersection points A, B may be joined, producing the bisector.
The perpendiculars through P and Q may be constructed similarly. For instance, first extend the segment $\overline{PQ}$ and draw a circle centered at P with radius $|PQ|$ to produce the point R. The perpendicular bisector of $\overline{RQ}$ is the desired perpendicular at[1] P. ∎



Corollary 4.5. *The set of Gaussian integers $\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}$ is constructible.*

Proof. Proposition 4.3 applied to $\{P, Q\} = \{0, 1\}$ constructs $\mathbb{N}_0$, now reverse the roles of P, Q to construct the negative integers.
Given $x \in \mathbb{Z}$, Proposition 4.4 builds the perpendicular through x. Draw the circle radius 1 centered at x: one now obtains $x \pm i$. Proposition 4.3 now constructs the values $x \pm iy$ on this vertical line. ∎

[1] Of course we should check that the given construction does the job: if we're assuming a rigorous version of Euclidean geometry, this is easy. Recall that we're working within analytic geometry (indeed within $\mathbb{C}$), so this can be assumed.

Proposition 4.6. *Let P, Q, R be non-collinear. Then the lines through R parallel and perpendicular to $\overleftrightarrow{PQ}$ are both constructible from $\{P, Q, R\}$.*

Proof. Draw the circle with radius $|PR|$ centered at R. Let T be the other intersection of this circle with $\overleftrightarrow{PQ}$.

- If $T = P$ so that there is only one intersection point, then $\overleftrightarrow{PQ}$ is tangent to the circle and thus the radius $\overline{PR}$ is perpendicular to $\overleftrightarrow{PQ}$.
- If $T \neq P$, then the perpendicular bisector of $\overline{PT}$ may be constructed. This passes through R and is therefore the required line.

For the parallel line through R, construct the perpendicular to $\overline{PR}$ at R. ∎

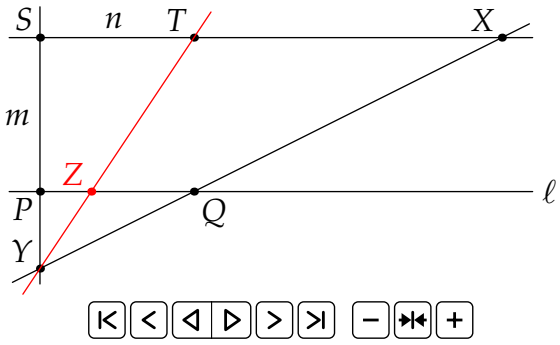
Corollary 4.7. *$z = x + iy \in \mathbb{C}$ is constructible if and only if $x, y \in \mathbb{R}$ are constructible. In particular, $\bar{z}$ is constructible.*

Proof. If $y = 0$ the result is trivial. Otherwise Proposition 4.6 constructs the parallel and perpendicular to $\mathbb{R}$ through z and thus the intersection $x \in \mathbb{R}$ and $y \in i\mathbb{R}$. The circle centered at 0 with radius iy intersects $\mathbb{R}$ at y. The converse follows from Proposition 4.4. ∎

Proposition 4.8. *Let P and Q be distinct points and let $r \in \mathbb{Q}$. Then any point $R \in \overleftrightarrow{PQ}$ for which $|PR| = r\,|PQ|$ is constructible from $\{P, Q\}$.*

Proof.

- Construct m perpendicular to $\ell = \overleftrightarrow{PQ}$ through P.
- The circle center P, radius $\overline{PQ}$ constructs $S \in m$.
- Construct n perpendicular to m through S and $T \in n$ such that $|ST| = |PQ|$.
- Given $q \in \mathbb{N}$, Proposition 4.3 defines X such that $|SX| = q\,|ST|$.
- Define $Y = \overleftrightarrow{XQ} \cap m$.
- Finally define $Z = \overleftrightarrow{YT} \cap \ell$.



By similar triangles,

$$\frac{|PZ|}{|PQ|} = \frac{|PZ|}{|ST|} = \frac{|PY|}{|SY|} = \frac{|PQ|}{|SX|} = \frac{1}{q}$$

Proposition 4.3 now allows us to construct R such that $|PR| = p\,|PZ| = \frac{p}{q}\,|PQ|$ for any $p \in \mathbb{Z}$. ∎

Corollary 4.9. *The rational numbers are constructible. Moreover, so is the extension field of rational complex numbers $\mathbb{Q}(i) = \{x + iy : x, y \in \mathbb{Q}\}$.*

Corollary 4.10. *Suppose that P, Q, A are constructible points on a line ℓ with P distinct from Q and A. Then the product $|PQ|\,|PA|$ and the quotient $\frac{|PQ|}{|PA|}$ are both constructible.*

Proof. Use the above picture: On the perpendicular to ℓ through P, construct S and Y such that $|PY| = 1$ and $|PA| = |YS|$. Then

$$\frac{|SX|}{|SY|} = \frac{|PQ|}{|PY|} \implies |SX| = |PQ|\,|SY| = |PQ|\,|PA|$$

Similarly

$$|PZ| = \frac{|PZ|}{|PY|} = \frac{|ST|}{|SY|} = \frac{|PQ|}{|PA|}$$

■

To complete the proof of Theorem 4.2 we put everything together:

- Addition/subtraction in $\mathbb{R}$: Suppose that x, y are constructible real numbers. Draw the circle centered at x with radius $|y|$. Its intersections with the real line are at $x \pm y$.
- Multiplication/division in $\mathbb{R}$: If x, y are positive constructible real numbers, Corollary 4.10 takes care of things. Otherwise, apply the same construction to $|x|, |y|$ and with suitable reflection to take care of any sign ambiguities.
- In $\mathbb{C}$: If $z = x + iy$ and $w = p + iq$ are constructible, then $z \pm w$, zw and $\frac{z}{w}$ may all be expressed in terms of operations of real numbers. For instance, if $w \neq 0$,

  $$\frac{z}{w} = \frac{x+iy}{p+iq} = \frac{(xp+yq)+i(yp-xq)}{p^2+q^2}$$

  which is constructible since its real and imaginary parts are (Corollary 4.7).

The constructible numbers are closed under the the field operations of $\mathbb{C}$: they are therefore a subfield. We have moreover seen that all rational numbers are constructible: thus $\mathbb{Q} \subseteq \mathcal{C} \subseteq \mathbb{C}$.

Square-roots and Angle-bisectors

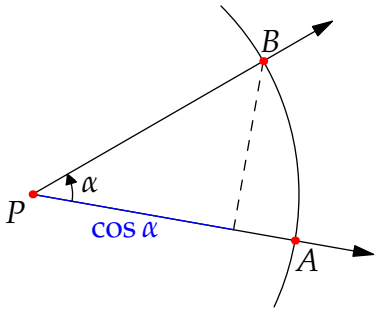
We've shown that all complex rationals $\mathbb{Q}(i)$ are constructible. The first obvious constructible irrationals are *square-roots*. For instance, we can construct a square of side length 1, so we can also construct its hypotenuse of length $\sqrt{2}$. It will transpire that sequences of square roots are essentially the *only* additional numbers we can construct.

To start the discussion, we consider angles.

Proposition 4.11. *An angle with measure α is constructible if and only if $\cos\alpha \in \mathbb{R}$ is constructible.*

Proof. If $\cos\alpha$ is constructible, intersect the perpendicular through $\cos\alpha$ with the unit circle to obtain the point $e^{i\alpha} = \cos\alpha + i\sin\alpha$. Joining this to 0 constructs α.

Conversely, given an angle α at P, draw the circle of radius 1 centered at P, thus producing two intersections A, B with the rays defining α. Drop the perpendicular from B to $\overrightarrow{PA}$ to measure $\cos\alpha$.



■

Proposition 4.12. *Let ℓ and m be constructible lines intersecting at P. Then the line through P bisecting an angle between ℓ and m is constructible.*

Proof. Draw a circle of constructible radius centered at P. Let A, B be intersections of the circle with each the lines ℓ, m respectively. The perpendicular bisector of $\overline{AB}$ (Propostion 4.4) passes through P. SSS congruence forces this to be the angle bisector. ∎

Corollary 4.13. *If $\cos\alpha$ is constructible, then $\pm\cos\frac{\alpha}{2}, \pm\sin\frac{\alpha}{2}$ are also constructible.*

Proposition 4.14. *If $r \in \mathbb{R}^+$ is constructible, so is $\sqrt{r}$.*

A simpler proof is in the homework: here we continue the idea of bisecting angles.

Proof. For any integer n, the number $\frac{2r}{n^2} - 1$ is also constructible. Choose n large enough so that $-1 < \frac{2r}{n^2} - 1 < 1$. Put $\cos\alpha = \frac{2r}{n^2} - 1$. Then,

$$\cos\frac{\alpha}{2} = \sqrt{\frac{1+\cos\alpha}{2}} = \frac{\sqrt{r}}{n}$$

is constructible and hence so is $\sqrt{r}$. ∎

Corollary 4.15. *For any $z \in \mathbb{C}$, the numbers $\sqrt{z}$ is constructible.*

The trick is to recall the form of a complex number in polar form:

$$z = re^{i\theta} \quad \text{where} \quad r = |z| \quad \text{and} \quad \theta = \arg(z)$$

The square-roots is then $\sqrt{z} = \sqrt{r}e^{i\theta/2}$. The upshot is that we are a constructible distance along a constructible angle bisector.

A complete description of the constructible numbers

The remaining discussion may seem a little technical: you don't need to be familiar with field extensions to understand it, though it certainly makes things easier!

Theorem 4.16. *Suppose that a field $\mathbb{F} \subseteq \mathbb{C}$ is constructible from $\{0,1\}$ and closed under complex conjugation. Let $z \in \mathbb{C}$.*

1. *If z is constructible in one step from points in $\mathbb{F}$, then it is a zero of a linear or quadratic polynomial with coefficients in $\mathbb{F}$.*
2. *If z is a zero of a linear or quadratic polynomial with coefficients in $\mathbb{F}$, then z is constructible in a finite number of steps from $\mathbb{F}$.*

Proof. If a line joins two points $\sigma, \tau \in \mathbb{F}$, then it is easily seen to have equation

$$(\overline{\tau} - \overline{\sigma})z - (\tau - \sigma)\overline{z} + \overline{\sigma}\tau - \sigma\overline{\tau} = \alpha z + \overline{\alpha}\overline{z} + \beta = 0$$

with $\alpha, \beta \in \mathbb{F}$. Let $\delta, \eta, \zeta \in \mathbb{F}$: the circle centered at δ with radius $|\eta - \zeta|$ has equation

$$(z - \delta)(\overline{z} - \overline{\delta}) = |\rho|^2$$

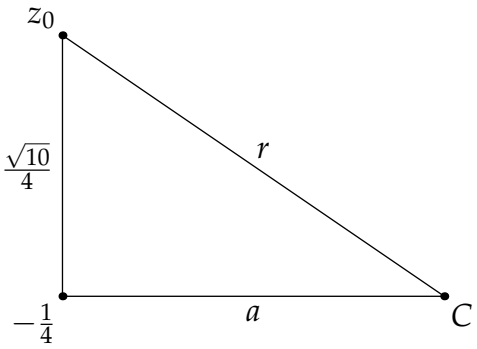
where $|\rho|^2 = (\eta - \zeta)(\overline{\eta} - \overline{\zeta}) \in \mathbb{F}$. We have three options for constructing a point z:

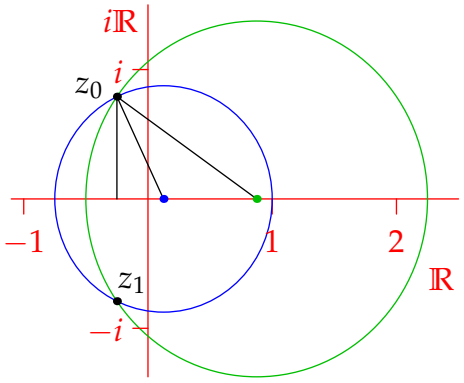
- z is the intersection of two lines. Eliminate $\overline{z}$ and solve for z which lies in $\mathbb{F}$ (depends only on the coefficients and the field operations $+, -, \cdot, \div$).
- z is an intersection of a line and a circle. Substitute the line equation in the circle to obtain a quadratic equation for z with coefficients in $\mathbb{F}$.
- z is the intersection of two circles. Given $(z-\delta)(\overline{z}-\overline{\delta}) = |\rho|^2$ and $(z-\gamma)(\overline{z}-\overline{\gamma}) = |\sigma|^2$, eliminate $\overline{z}$ to again obtain a quadratic equation for z with coefficients in $\mathbb{F}$.

Conversely, if z_0 is a zero of a linear or quadratic polynomial f with coefficients in $\mathbb{F}$, then we may compute z_0 from $\mathbb{F}$ using, at most, the quadratic formula. Since this only requires the field operations and computing a square-root, we see that z_0 is constructible from $\mathbb{F}$ (Corollary 4.15). ■

Example Describe a construction from $\mathbb{Q}$ of the roots of the polynomial $z^2 + \frac{1}{2}z + \frac{11}{16} = 0$.

There are many, many ways to do this. Here is a construction using the intersection of two circles with rational radius centered at a rational point. We have $z_0, z_1 = \frac{1}{4}(-1 \pm \sqrt{10}i)$. Consider the picture, where C is to be the center of a circle passing through $z_0 = \frac{1}{4}(-1 + \sqrt{10}i)$.





If $C \in \mathbb{Q}$, we require a and r to be rational. By Pythagoras', we see that

$$r^2 = a^2 + \frac{10}{16} \implies (r-a)(r+a) = \frac{5}{8}$$

We can easily find many solutions $(a, r) \in \mathbb{Q}^2$ to this equation. For instance

$$\begin{cases} r-a = \frac{1}{4} \\ r+a = \frac{5}{2} \end{cases} \implies (a,r) = (\tfrac{9}{8}, \tfrac{11}{8}) \qquad \text{and} \qquad \begin{cases} r-a = \frac{1}{2} \\ r+a = \frac{5}{4} \end{cases} \implies (a,r) = (\tfrac{3}{8}, \tfrac{7}{8})$$

We therefore choose circles centered at $-\frac{1}{4} + a = \frac{1}{8}$ and $\frac{7}{8}$ with radii $\frac{7}{8}$ and $\frac{11}{8}$ respectively. Indeed one can check that

$$\begin{cases} (z-\frac{1}{8})(\overline{z}-\frac{1}{8}) = \left(\frac{7}{8}\right)^2 \\ (z-\frac{7}{8})(\overline{z}-\frac{7}{8}) = \left(\frac{11}{8}\right)^2 \end{cases} \implies z^2 + \frac{1}{2}z + \frac{11}{16} = 0$$

If complex numbers make this seem too difficult, observe that

$$\begin{cases} (x-\frac{1}{8})^2 + y^2 = \left(\frac{7}{8}\right)^2 \\ (x-\frac{7}{8})^2 + y^2 = \left(\frac{11}{8}\right)^2 \end{cases} \implies x = -\frac{1}{4},\ y = \pm\frac{\sqrt{10}}{4}$$

We make the following observations without proof (take a rings and fields class for details):

- If $\mathbb{F} \subseteq \mathbb{C}$ is a field and $P \in \mathbb{C}$, then the *extension field* $\mathbb{F}(P)$ is the collection of all complex numbers which may be produced from $\mathbb{F}$ and P using only the field operations $(+, -, \cdot, \div)$.
- $\mathbb{F}(P)$ is a vector space of degree n over $\mathbb{F}$ if and only if the lowest-degree polynomial equation with coefficients in $\mathbb{F}$ satisfied by P has degree n. We may write

  $$\mathbb{F}(P) = \{a_0 + a_1 P + \cdots + a_{n-1} P^{n-1} : a_i \in \mathbb{F}\}$$

  When the polynomial in question is *monic* (leading term x^n), we call it the *minimal polynomial of* P. The *index* $[\mathbb{F}(P) : \mathbb{F}] = n$ is the dimension of this vector space.

Examples

1. The minimal polynomial of $P = i$ over $\mathbb{Q}$ is $x^2 + 1$. We can form the index-two extension field $\mathbb{Q}(i) = \{q_0 + q_1 i : q_0, q_1 \in \mathbb{Q}\}$.
2. The minimal polynomial of $P = \sqrt[3]{2}$ over $\mathbb{Q}$ is cubic: $x^3 - 2$, whence the extension field has index $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Corollary 4.17. *1. If $\mathbb{F}$ is a constructible field of finite index over $\mathbb{Q}$, then $[\mathbb{F} : \mathbb{Q}] = 2^n$ for some $n \in \mathbb{N}$. In particular, there exist a tower of fields*

$$\mathbb{Q} = \mathbb{F}_0 \leq \mathbb{F}_1 \leq \cdots \leq \mathbb{F}_n = \mathbb{F}$$

such that $[\mathbb{F}_{k+1} : \mathbb{F}_k] = 2$ for each k.

2. If $z \in \mathbb{C}$ is constructible,[2] then it has minimal polynomial over $\mathbb{Q}$ of degree 2^n for some $n \in \mathbb{N}$.

The impossible problems of antiquity

The early Greek mathematicians took it almost as a point of faith that the solution to every problem could be constructed: all one had to do was to search hard enough and an explicit construction could be found. There were three problems, however, which were simple to state, yet for which no convincing constructions could be found. Mathematicians spent centuries searching for these. It wasn't until the modern advent of field theory that the non-existence of solutions to these problems could be proved.

Theorem 4.18. *The following constructions are impossible with a ruler and compass:*

1. *To duplicate a cube (draw a cube with double the volume of a given cube).*
2. *To trisect a given angle.*
3. *To square a circle[3] (draw a square whose area equals that of a given circle).*

[2]The field $\mathcal{C}$ of constructible numbers is an *infinite algebraic* field extension of $\mathbb{Q}$. Every element thus lies in some finite extension field $\mathbb{F}$ as in part 1.

[3]This expression has become a metaphor for attempting to do something impossible. You might hear it uttered by a politician to rubbish an opponents policy. Interestingly, the metaphor dates from a long time before the first proof of the impossibility, thus suggesting that belief predated proof!

Proof. 1. If we could duplicate the cube, the ratio of the side lengths $\sqrt[3]{2}$ would have to be constructible. As observed above, the minimal polynomial of $\sqrt[3]{2}$ has degree three, whence $\sqrt[3]{2}$ is not constructible.

2. We need a single counter-example. Consider the angle[4] $3\theta = \frac{\pi}{3}$. If the angle $\theta = \frac{\pi}{9}$ were constructible, so would be cosine $x = \cos\frac{\pi}{9}$. The triple-angle formula yields a polynomial equation for x:

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta \implies \frac{1}{2} = 4x^3 - 3x$$

It can be seen that this is the lowest degree polynomial satisfied by x. We have $[\mathbb{Q}(x) : \mathbb{Q}] = 3$ which is not a power of 2.

3. In 1882, Ferdinand von Lindemann proved that π (and consequently $\sqrt{\pi}$) is *transcendental*: there are no polynomials f with coefficients in $\mathbb{Q}$ for which $f(\pi) = 0$. To square a circle of constructible radius r would require construction of a square with side length $\sqrt{\pi}r$. Since $\sqrt{\pi}$ has no minimal polynomial, it is not constructible.

■

[4] This is itself constructible a the angle in an equilateral triangle.