SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Geometric constructions and solutions of cubic equations

av

Lisa Nicklasson

2014 - No 8

Geometric constructions and solutions of cubic equations

Lisa Nicklasson

Självständigt arbete i matematik 30 högskolepoäng, Avancerad nivå

Handledare: Christian Gottlieb

2014

Geometric constructions and solutions of cubic equations

Lisa Nicklasson

April 24, 2014

Abstract

It is well known that, using ruler and compass, the angle can not be trisected in general, and the regular p-gon, where p is an odd prime, can be constructed if and only if p is a Fermat prime. Also, cubic equations can generally not be solved. But what happens if we allow angle trisection? Which p-gons can be constructed, and what cubic equations can be solved? These questions shall be answered, and we shall also see what can be constructed with a marked ruler, and what cubic equations can be solved using a parabola in addition to the classical tools.

Contents

1 Introduction

Ruler and compass constructions is a classical, and well studied subject in mathematics. It is well known what is constructible, and what is not. As an example, we can bisect angles, but not trisect them, in general. Using Galois theory one can prove that the regular p-gon, where p is an odd prime, is constructible when p is a Fermat prime, that is a prime of the form $2^{2^n} + 1$. We also know that quadratic equations can be solved by ruler and compass, but the cubic equation is in general unsolvable. In this thesis we shall study what more can be constructed with a few different improvements of our tools. Especially we shall see which regular polygons can be constructed, and which cubic equations can be solved.
The reader is supposed to be familiar with the fundamentals of Galois theory.

The points we construct shall be defined as complex numbers $x + yi$, instead of points (x, y) in $\mathbb{R}^2$ as conventional in modern literature.

Our first modification of the tools is to use an angle trisector together with the ruler and compass. We shall see that the regular p-gon is constructible when p is a Pierpont prime, which is a prime of the form $2^n 3^m + 1$. We shall also see that an irreducible cubic equation is solvable if and only if it has three real roots. This section is my own work, although some of the results can also be found in Gleason [3].

Better than to add the angle trisector to our toolbox is to replace the ruler and compass by one single tool, namely the marked ruler. The marked ruler is a ruler with only two markings on it, one unit apart. With this single tool we can solve any cubic equation. Here I follow Martins book Geometric Constructions [5].

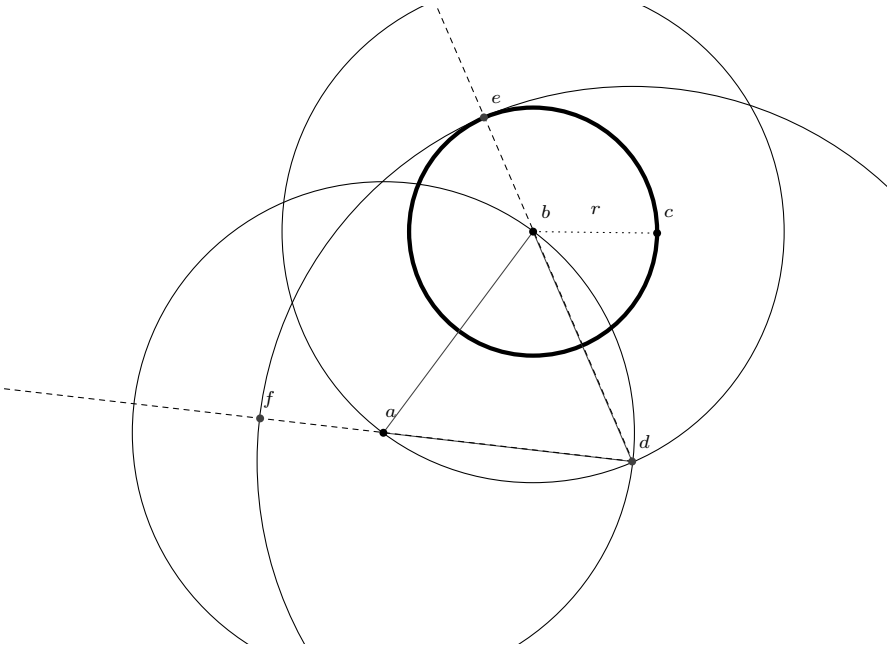
Last we shall see how cubic equations can be solved using a parabola. Here I was inspired by Khayyam and did some improvements of his original method, which is found in Kline [4].

But before doing any of these things we shall study the classical ruler and compass constructions, and see how they relate to field extensions.

2 Ruler and compass constructions

The theory of ruler and compass constructions goes all the way back to Euclid's time. The question is what we can construct given a compass and an unmarked ruler. Formally, we are allowed to draw a straight line between two given points, and draw a circle that goes through a given point and has its center in another given point.
This definition does not allow us to draw a circle, move the compass (without closing it), and draw a circle with the same radius at some other place. However, Euclid showed in his book Elementa that it is possible "move" a circle, without cheating. This is how he did it.

Assume we have a circle with center in a point b and that goes through a point c. Say the radius is r. We want to draw a circle with radius r with center in some given point a. To do this, first draw a circle with center in a that goes through b, and a circle with center in b that goes through a. Call one of the intersection points of these two circles d. This point d, together with a and b form a equilateral triangle. The line through b and d intersects the original circle in some point e. Draw a circle with center in d that goes through e. The line that goes through a and d intersects this circle in a point f. Then the distance between a and f is equal to the distance between b and e, which is r.



Now we can draw a circle with center in a and radius r.

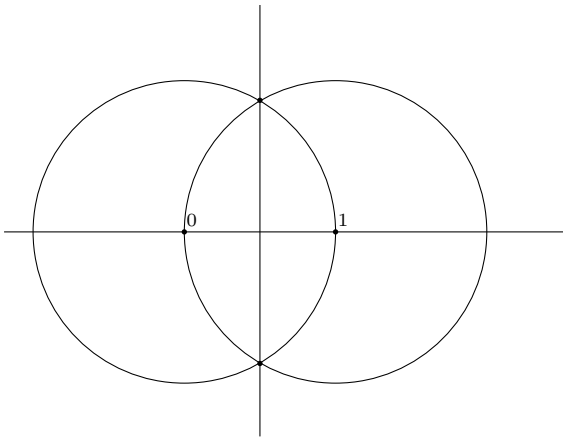
From now on we shall consider our points as numbers in the complex plane, which is not exactly what Euclid did since complex numbers appeared in mathematics much later. Assume we are given a set of points in the complex plane. From these points we can draw lines and circles. We say that a point in the plane is *contructible in one step* if it is the intersection of two such lines, a line and a circle, or two circles. Such a point we can use to draw new lines and

circles, just as we did above, and from these construct new points. Any point that can be constructed in a finite number of steps is called *constructible*.

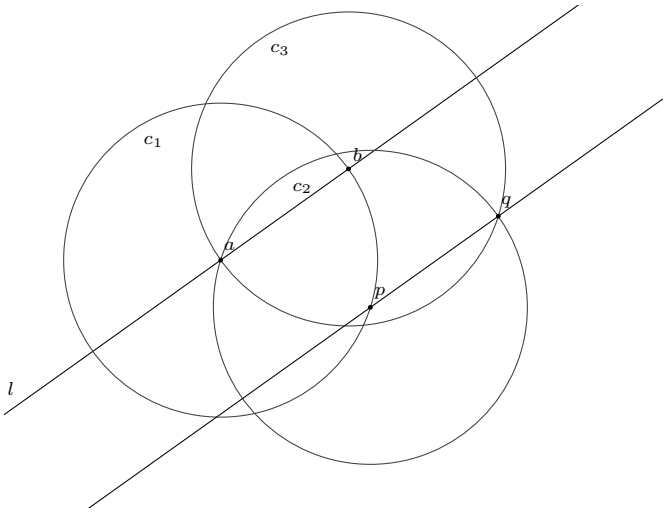
2.1 Possible constructions

Now, what kind of things can we do with the ruler and compass?

To get started we need at least two points. But of course, if we are given an empty paper we could just mark two arbitrary points. We may also choose these points to be 0 and 1 in the complex plane. Then we can draw a line between these two points. This will be the real axis in the complex plane.
One nice thing we can do now is to construct a right angle. To do this we draw two circles, one that goes through 1 and with center in 0, and the other goes through 0 and has center in 1. These circles intersect in two points. A line that goes through these two points is orthogonal to the real axis.

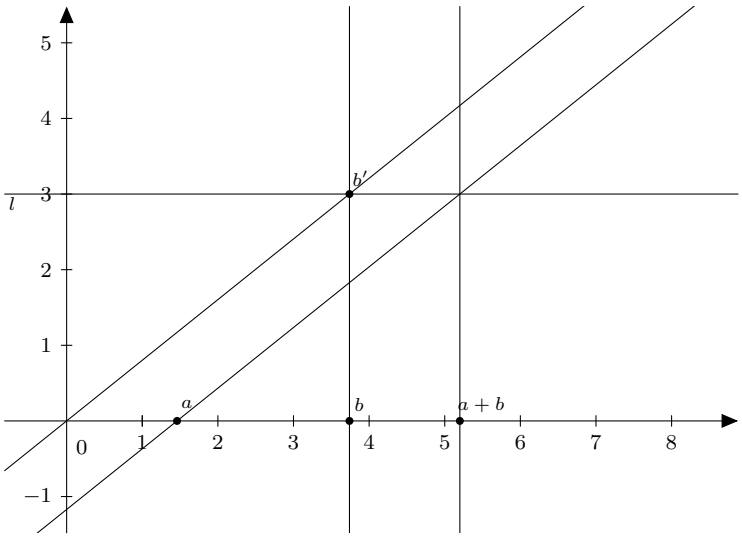


Note that this line intersects the real line exactly midway between 0 and 1, so this is also a method for dividing a distance in half.
Since we can construct orthogonal lines we can also draw parallel lines. But in fact we can do even better. Given a line l and a point p, we can draw a line parallel to l that goes through p. Here is one way to do this:
Draw a circle c_1 that goes through p and with center at a point a on l. The circle c_1 intersects l at some point b. Draw a circle c_2 with center in p that goes through a, and a third circle c_3 with center in b that also goes through a. Note that these three circles all have the same radius. The circles c_2 and c_3 intersects in a and in some point q. Then the line that goes through p and q is parallel to the line that goes through a and b, which is l.



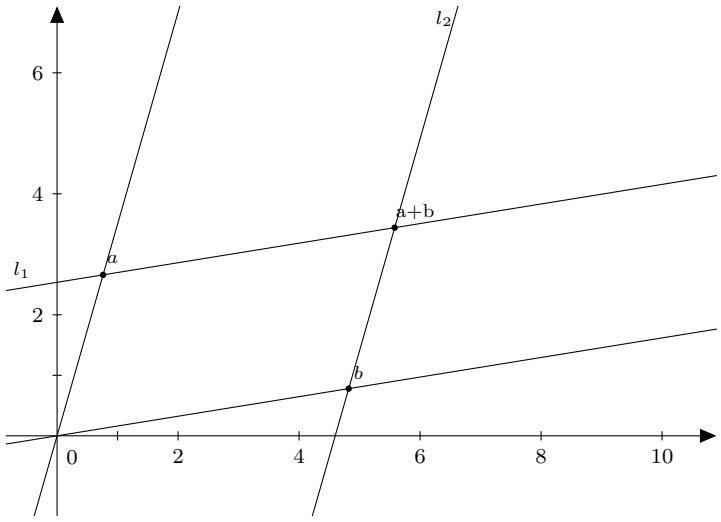
It follows that we also can draw a line that goes through a given point and is orthogonal to a given line. Especially, we can draw the imaginary axis. These facts will be useful in the task to construct numbers.

Given two real numbers a and b, say $a \leq b$. To add these two we start with drawing a line l parallel to the real line. Then we draw a line orthogonal to the real line that goes through b. This gives us a point b' right above b, on the line l. We draw a line that goes through 0 and b', and a line parallel to this one that goes through a. This line intersects l in a point right above $a + b$. Finally we project this point (i.e. we draw a line through this point orthogonal to the real line) on the real line and we have constructed the point $a + b$.



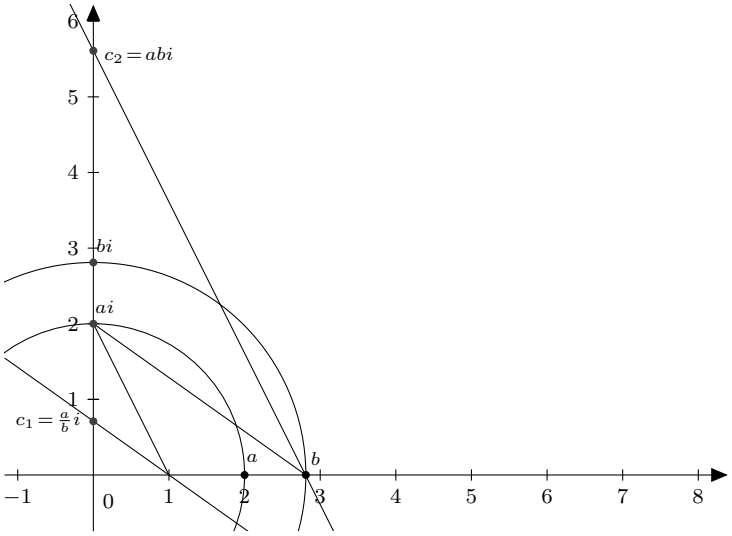
For any complex numbers a and b such that $b = \lambda a$, where λ is real, we can perform addition in a similar way. We just use the line that goes through the origin, a, and b, instead of the real line.
Complex numbers a and b that does not possess this property can be added in another (easier) way. First draw the line that goes through the origin and a,

and draw another line l_1 that goes through b and is parallel to this one. Second, draw a line that goes through the origin and b, and a line l_2 that is parallel to this one and goes through a. The point where l_1 and l_2 intersect is $a + b$.



Multiplication and division of real numbers can also be performed with ruler and compass.

Assume we have two real numbers a and b, say $a \leq b$. Start with drawing a circle with center in the origin and radius a, to get the point ai on the imaginary axis. Draw a line l_1 between 1 and ai, and a line l_2 between ai and b. Then draw a line parallel to l_1 that goes through b, and a line parallel to l_2 that goes through 1. The line parallel to l_1 intersects the imaginary axis in some point c_1. The line parallel to l_2 intersects the imaginary axis in some point c_2.



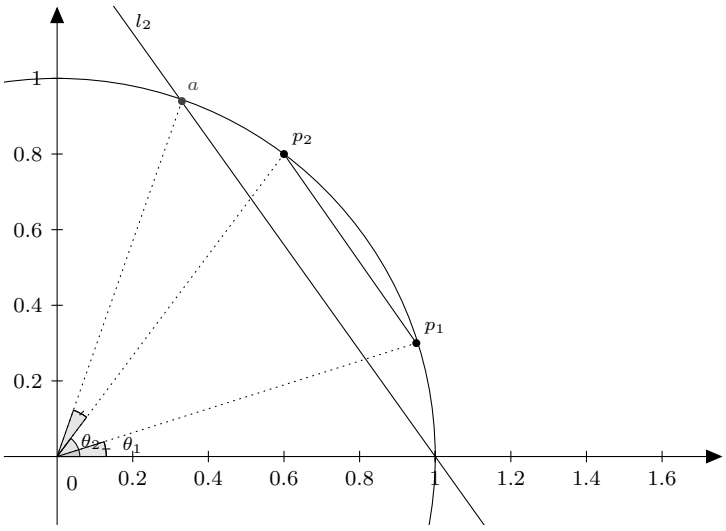
Now consider the four right-angled triangles with a corner in the origin that we have drawn.

Note that the triangle with corners in b and c_2 is similar to the triangle with

corners in 1 and ai. The side with length 1 in the smaller triangle corresponds to the side with length b in the bigger triangle, so the side with length a must correspond to a side with length ab. Hence $c_2 = abi$.
Also, the triangle with corners in 1 and c_1 is similar to the triangle with corners in b and ai. Then we get $c_1 = \frac{a}{b}i$ with a similar argument as above.
Now, since we have abi and $\frac{a}{b}i$ we can use the compass to get ab and $\frac{a}{b}$.

Recall that we started with just the numbers 0 and 1. Now, since we can perform addition, multiplication, and division, we can construct all rational numbers.

Multiplying complex numbers is slightly more complicated. For this matter it will be convenient to write the numbers in polar form. Say we want to multiply the numbers $r_1e^{\theta_1 i}$ and $r_2e^{\theta_2 i}$, i.e. we want to construct $r_1r_2e^{(\theta_1+\theta_2)i}$. We know how to multiply real numbers, so we can construct r_1r_2. The question is how to add angles.
Let $p_1 = e^{\theta_1 i}$ and $p_2 = e^{\theta_2 i}$ be points on the unit circle, and let us assume $\theta_1 \leq \theta_2$. Draw a line between p_1 and p_2, and a line l parallel to this one that goes through 1. The line l intersects the unit circle in a point a. Because of the symmetry the distance between 1 and p_1 is the same as the distance between p_2 and a. Hence the polar angle for a is $\theta_1 + \theta_2$, and $a = p_1p_2$.

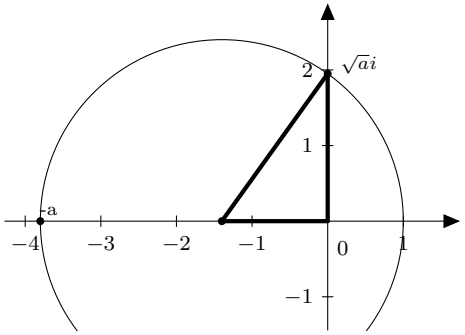


Now draw a circle with radius r_1r_2 and center in the origin, and a line that goes through the origin and $e^{\theta_1+\theta_2}$. The point where these two intersect is $r_1r_2e^{(\theta_1+\theta_2)i}$, so we can conclude that is is possible to multiply complex numbers using ruler and compass.

It follows from this that we can construct the number $-a$, given a. Since we can add numbers, we can now also perform subtraction.

We might want to construct multiplicative inverses of complex numbers as well. As above, we can construct the inverse $\frac{1}{r}e^{-\theta i}$ to the number $re^{\theta i}$ if we can construct the angle $-\theta$. Given the angle θ on the unit circle we just need to draw a line orthogonal to the real axis and pick the other point where the line meets the unit circle.
Note that this also allows us to construct the conjugate of a complex number.

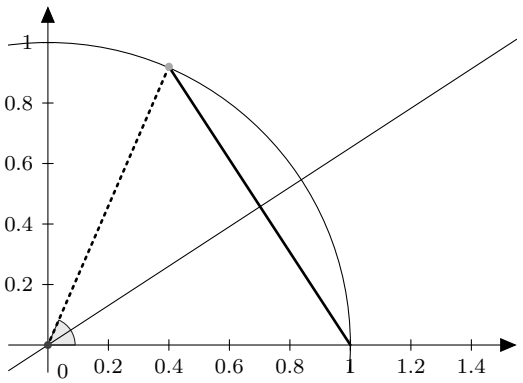
Another nice thing we can do is to take square roots of real numbers. To construct the square root of the real number a, draw a circle that goes through 1 and $-a$ (i.e. has its center $\frac{1-a}{2}$). The point where this circle meets the imaginary axis is $\sqrt{a}i$.



This can easily be verified by the Pythagorean Theorem. The right triangle with corners in the origin, the center of the circle, and $\sqrt{a}i$ has catheti $\frac{a-1}{2}$ and $\sqrt{a}$, and hypotenuse $\frac{a+1}{2}$ (the radius of the circle). Indeed

$$\left(\frac{a-1}{2}\right)^2 + \left(\sqrt{a}\right)^2 = \frac{1-2a+a^2}{4} + a = \frac{1+2a+a^2}{4} = \left(\frac{a+1}{2}\right)^2.$$

To construct the square root $\sqrt{r}e^{\frac{\theta}{2}i}$ of the complex number $re^{\theta i}$ we need to divide an angle in half. This is possible: Draw a line between the point $p = e^{\theta i}$, on the unit circle, and 1. As we noted in the beginning, we can draw an orthogonal line exactly midway between p and 1. This line divides the angle in half.



With all these operations possible we can conclude that the set of constructible complex numbers is a subfield of $\mathbb{C}$ which is closed under taking conjugates and square roots.

2.2 Quadratic equations

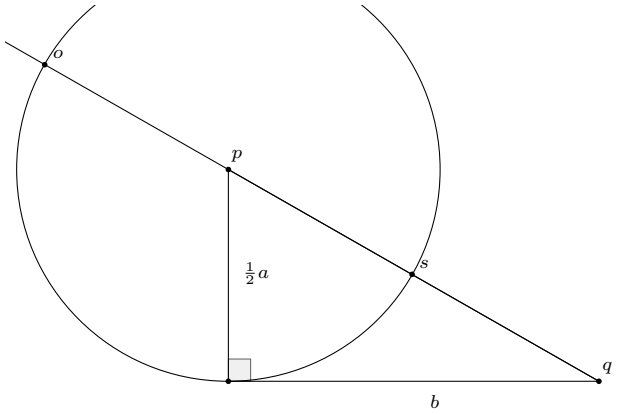
Recall that the solutions to a quadratic equation $x^2 + px + q = 0$ are

$$\pm\sqrt{\left(\frac{p}{2}\right)^2 - q} - \frac{p}{2}.$$

Since we can add, multiply, and take square roots, we can hence solve any quadratic equation.

The fact that quadratic equations with positive real roots can be solved geometrically was originally proved in another way. Here we shall see how Descartes did it.
Descartes considered three cases of quadratic equations: $z^2 = az + b^2$, $z^2 = -az + b^2$, and $z^2 = az - b^2$, where a and b are positive numbers. We shall have a look at his geometric solution to these three equations.

1. $z^2 = az + b^2$
   Draw a right triangle with catheti $\frac{1}{2}a$ and b. Also draw a circle with radius equal to the side $\frac{1}{2}a$, and with center p at the acute corner of the triangle, as in the figure below. Call the other acute corner q. The hypotenuse of the triangle intersects the circle at some point s. Prolong the hypotenuse to a line that intersects the circle a second time, in a point o.



   Then the distance between o and q is

$$\frac{1}{2}a + \sqrt{\frac{1}{4}a^2 + b^2},$$

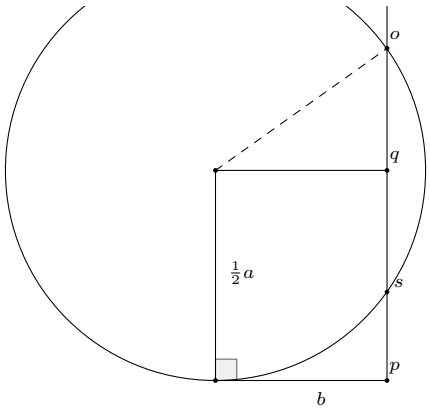
   which is a solution to the equation. The other solution $\frac{1}{2}a - \sqrt{\frac{1}{4}a^2 + b^2}$ is negative, and was ignored by Descartes.

2. $z^2 = -az + b^2$
   To solve this equation we use the same construction. The distance between q and s is

$$-\frac{1}{2}a + \sqrt{\frac{1}{4}a^2 + b^2},$$

and this is the positive solution to the equation. The negative solution is ignored.

3. $z^2 = az - b^2$
   We draw a rectangle with height $\frac{1}{2}a$ and base b. Call the lower right corner p and the upper left corner q. Draw also a circle with center at the upper left corner and radius $\frac{1}{2}a$. The circle intersects the rectangle in some point s between p and q. Prolong the line between p and q so that in intersects the circle in a second point o.



   Note that the center of the circle together with the points q and o form a right triangle. We see that distance between q and o is $\sqrt{\frac{1}{4}a^2 - b^2}$. The distance between p and q is $\frac{1}{2}a$, so the distance between p and o is

$$\frac{1}{2}a + \sqrt{\frac{1}{4}a^2 - b^2},$$

   which is a solution to the equation. In a similar way we see that the distance between p and s is

$$\frac{1}{2}a - \sqrt{\frac{1}{4}a^2 - b^2},$$

   which is the other solution to the equation. Note that this only works when $b \leq \frac{1}{2}a$, and this is exactly when the equation has real roots.

Descartes did not consider the case $z^2 = -az - b^2$ since this equation never has real solutions.

2.3 Relation to field extensions

Given some set of points we have seen how to construct new ones with the ruler and compass. In this section we will see how this relates to field extensions.

Theorem 1. *Let K be some subfield of $\mathbb{C}$ which contains i and is closed under complex conjugation. Let p be a complex number constructible in one step from*

K. Then p is a zero of a quadratic or linear polynomial with real coefficients, and hence

$$[K(p) : K] = 1 \text{ or } 2.$$

Also, $K(p)$ is closed under complex conjugation.

Proof. Note that if K contains some point $x + yi$ it also contains the conjugate $x - yi$ and hence

$$x = \frac{(x + yi) + (x - yi)}{2}$$

lies in K. Since K contains i we also have

$$y = -i((x + yi) - x)$$

in K.
Since p is constructible in one step from K there are three cases to consider. The point p could be the intersection between two lines, a line and a circle, or two circles.

1. **The intersection of two lines:**
   Let's say we have a line that goes through two points $x_1 + y_1 i$ and $x_2 + y_2 i$ in K, and a line that goes through two points $x_3 + y_3 i$ and $x_4 + y_4 i$ in K, none of them vertical. As noted above, the real numbers x_1, x_2, x_3, x_4, y_1, y_2, y_3, and y_4 also belongs to K. The point $p = x + yi$ lie on both lines.
   The first line gives us the equation

   $$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$

   or

   $$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1.$$

   In the same way the other line gives us

   $$y = \frac{y_4 - y_3}{x_4 - x_3}(x - x_3) + y_3,$$

   so we have

   $$\frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1 = \frac{y_4 - y_3}{x_4 - x_3}(x - x_3) + y_3.$$

   Hence, x is the solution to a linear equation. That is, x actually lie in K. Then the same holds for y.
   Since i also belongs to K we have $p = x + yi \in K$ and hence $K(p) = K$. Then $K(p)$ is obviously closed under complex conjugation and $[K(p) : K] = 1$.

   We must also consider the case when one line is vertical. Assume that the first line is given by

   $$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1$$

as before, and the second one is vertical

$$x = a$$

for some real number a. Then $a \in K$, and y can be calculated as

$$y = \frac{y_2 - y_1}{x_2 - x_1}(a - x_1) + y_1.$$

As before we can conclude that $K(p) = K$.

2. **The intersection of a circle and a line:**
Assume we have a non-vertical line that goes through some points $x_1 + y_1 i$ and $x_2 + y_2 i$, and a circle with center in $x_3 + y_3 i$ and radius r. The circle has some point $a + bi$ that lies in K (since we were allowed to draw it), so $r^2 = (a - x_3)^2 + (b - y_3)^2$ lies in K.
The line can be described with the equation

$$y = \frac{x - x_1}{x_2 - x_1}(y_2 - y_1) + y_1$$

and the circle

$$(x - x_3)^2 + (y - y_3)^2 = r^2.$$

To find an x that satisfies both equations we place the linear expression for y in the equation of the circle. This gives

$$(x - x_3)^2 + \left(\frac{x - x_1}{x_2 - x_1}(y_2 - y_1) + y_1 - y_3\right)^2 = r^2.$$

Hence x is the solution to a quadratic equation over K, so $[K(x) : K] = 2$ (assuming x was not already in K). From the equation of the line see that $y \in K(x)$. Then we also have $p = x + yi \in K(x)$, so in fact $K(p) = K(x)$. This field is closed under complex conjugation and we have that $[K(p) : K] = 2$.

If the line is vertical, say $y = a$, the proof is the same, except the quadratic equation becomes

$$(x - x_3)^2 + (a - y_3)^2 = r^2.$$

3. **The intersection of two circles:**
Assume we have two intersecting circles, one with center $x_1 + y_1 i$ and radius r_1, and the other with center $x_2 + y_2 i$ and radius r_2. Then we have the equations

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = r_1^2 \\ (x - x_2)^2 + (y - y_2)^2 = r_2^2. \end{cases}$$

If we expand the parenthesis we get

$$\begin{cases} x^2 - 2xx_1 + x_1^2 + y^2 - 2yy_1 + y_1^2 = r_1^2 \\ x^2 - 2xx_2 + x_2^2 + y^2 - 2yy_2 + y_2^2 = r_2^2. \end{cases}$$

As we saw in the previous case, r_1^2 and r_2^2 both lie in K.
We subtract the second equation from the first and get

$$x_1^2 - 2xx_1 + y_1^2 - 2yy_1 - x_2^2 + 2xx_2 - y_2^2 + 2yy_2 = r_1^2 - r_2^2.$$

From this we can solve out y

$$y = \frac{r_1^2 - r_2^2 - x_1^2 + 2xx_1 - y_1^2 + x_2^2 - 2xx_2 + y_2^2}{2(y_2 - y_1)}.$$

If we place this in one of the original equations we see that x is the solution to a quadratic equation over K. We can also see from the above expression that $y \in K(x)$. As in the previous case we can conclude that $[K(p) : K] = 2$, and $K(p)$ is closed under complex conjugation.

□

Note that if K consists only of real numbers, the requirement of K being closed under complex conjugation is trivial. If p is also a real number we do not need the field K to contain i.

We need also to note that $K(p)$ is the splitting field of p's minimal polynomial over K. Let $f(x)$ be the minimal polynomial for p over K, and let Σ be the splitting field of f over K. The case when f is linear is trivial, so let us assume that f is quadratic. Then f has one other root q, so we have

$$f(x) = (x - p)(x - q) = x^2 - (p + q)x + pq.$$

The coefficients lie in K, which is a subfield of $K(p)$. Hence

$$(p + q) - p = q \in K(p).$$

Since both p and q belongs to $K(p)$ this must be the splittingfield, i.e. $K(p) = \Sigma$.

In fact, any quadratic normal extension of a subfield of $\mathbb{C}$ comes from a geometric construction. Recall that a finite normal extension field is the same as a splitting field of some polynomial. A quadratic normal extension field is hence the splitting field of some quadratic polynomial. The zeroes of a quadratic polynomial are constructible, as we saw earlier.

In the continuation we would like to start with the field $\mathbb{Q}$ (which we can construct, as noted in the prevoius section). This is, as required, closed under complex conjugation, but does not contain i.

Theorem 2. *A complex number z is constructible if and only if there is a tower*

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n \subseteq \mathbb{C}$$

of field extensions such that $z \in K_n$ and $[K_{j+1} : K_j] \leq 2$ for all $j = 0, 1, 2, \ldots, n-1$. Hence $[K_n : \mathbb{Q}]$ is a power of 2.

Proof. Since i is of degree 2 over $\mathbb{Q}$ we can let $K_1 = \mathbb{Q}(i)$. This is a field that contains i and is closed under complex conjugation, so the conditions in Theorem 1 are satisfied. Since z is constructible there is a sequence of points $p_1, \ldots, p_n$ such that p_1 is constructible in one step from $\mathbb{Q}(i)$, the point p_2 is constructible in one step from $\mathbb{Q}(i) \cup \{p_1\}$, and so on.
Now let $K_{i+1} = K_i(p_i)$ for $i = 1, 2, \ldots n$. Assume K_i is closed under complex conjugation. The field K_i will contain all the points $p_1, \ldots, p_{i-1}$, so p_i is constructible in one step from K_i. Then $[K_{i+1} : K_i] \leq 2$ and K_{i+1} is closed under

complex conjugation, by Theorem 1. By induction we can conclude that we have a tower

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{n+1} \subseteq \mathbb{C}$$

of field extensions such that $z \in K_n$ and $[K_{i+1} : K_i] \leq 2$ for all $i = 0, 2, \ldots, n$. □

2.4 Impossible constructions

We have seen that we can do a lot of things with the ruler and compass. However, there are some things we can't do. There are three famous "impossible constructions", namely

- *duplicating the cube*
- *squaring the circle.*
- *trisecting the angle*

To duplicate a cube is to construct a new cube with twice the volume. In terms of constructions in the complex plane, this is constructing the length of the side of the cube. Assuming the given cube has side 1, we are to construct the number $\sqrt[3]{2}$. But this number has degree 3 over $\mathbb{Q}$, and is not constructible by ruler and compass.

To square a circle is to construct a square with the same area as a given circle. Let the circle be the unit circle. Since the unit circle has area π, we are supposed to construct a square with side $\sqrt{\pi}$. If we can construct the number $\sqrt{\pi}$ we can also construct π. But π is transcendental, which makes the construction impossible.

We shall take a closer look at the third "impossibility".

Theorem 3. *Not all angles can be trisected using ruler and compass.*

Proof. To show this we need to find one angle which is impossible to trisect with ruler and compass. We shall prove that $\frac{\pi}{3}$ is such an angle.
Given the point $\cos\left(\frac{\pi}{3}\right) + i\sin\left(\frac{\pi}{3}\right)$ on the unit circle we try to construct the point $\cos\left(\frac{\pi}{9}\right) + i\sin\left(\frac{\pi}{9}\right)$. If this point is constuctible, then its real part $\cos\left(\frac{\pi}{9}\right)$ is constructible as well.
Recall the trigonometric formula

$$\cos(3\theta) = 4\cos^3\theta - 3\cos\theta.$$

If we apply this to $\theta = \frac{\pi}{9}$ we get

$$\frac{1}{2} = 4\cos^3\left(\frac{\pi}{9}\right) - 3\cos\left(\frac{\pi}{9}\right)$$

since $\cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$. Hence $\alpha = \cos\left(\frac{\pi}{9}\right)$ is a solution to the equation

$$4x^3 - 3x - \frac{1}{2} = 0$$

or over the integers

$$8x^3 - 6x - 1 = 0.$$

Since 3 is a prime and

$$3 \nmid 8, \quad 3 \mid 6, \quad \text{and } 9 \nmid 1$$

the polynomial $8x^3 - 6x - 1$ is irreducible, by Eisenstein's criterion [1, p. 214]. Hence

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3.$$

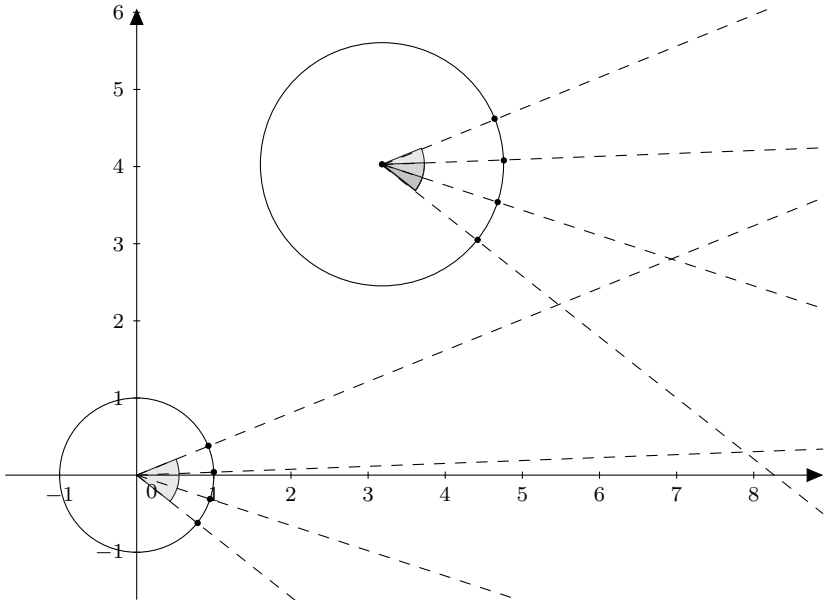
But this is not a power of two, so α is not constructible and the angle $\frac{\pi}{3}$ can not be trisected. □

3 The angle trisector

We saw above that angles can not be trisected using ruler and compass, in general. But assume now that we have an additional tool that allows us to trisect angles, an "angle trisector".

3.1 Constructible numbers and field extensions

First we need a formal definition of the angle trisector. Say we are given a circle, and two points on the circle. These two points, together with the center of the circle, defines some angle θ. The angle trisector allows us to mark the two points on the circle that divides the angle θ in three.
We now extend out definition of constructible points, by also allowing points to be constructed in this way.
We may now draw lines between the center of the circle and the four points on the circle. The angles θ and $\frac{\theta}{3}$ can now be moved to any other circle by drawing lines parallel to these four, but that goes through the center of the new circle. Hence it is enough to be able to trisect angles on the unit circle.

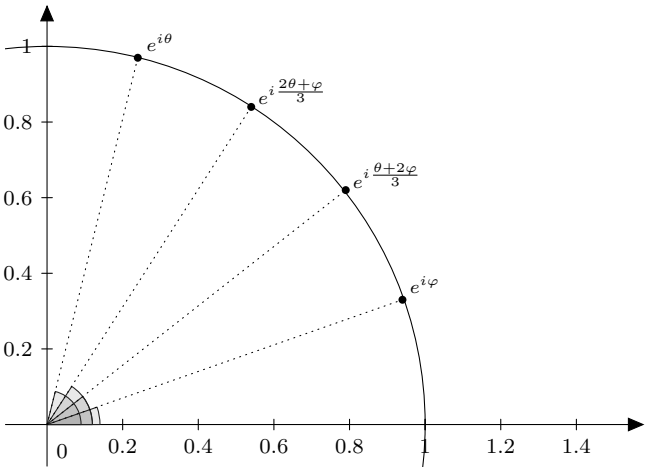


Given two points $e^{i\theta}$ and $e^{i\varphi}$, say $\varphi < \theta$, on the unit circle. With the angle trisector we can construct

$$e^{i\left(\varphi+\frac{\theta-\varphi}{3}\right)} = e^{i\left(\frac{\theta+2\varphi}{3}\right)} = e^{i\frac{\theta}{3}}\left(e^{i\frac{\varphi}{3}}\right)^2$$

and

$$e^{i\left(\varphi+2\frac{\theta-\varphi}{3}\right)} = e^{i\left(\frac{2\theta+\varphi}{3}\right)} = \left(e^{i\frac{\theta}{3}}\right)^2 e^{i\frac{\varphi}{3}}.$$



Since we can multiply complex numbers it is enough to be able to construct $e^{i\frac{\theta}{3}}$ and $e^{i\frac{\varphi}{3}}$.
So far we have concluded that we can trisect angles if we can construct $e^{i\theta}$ given $e^{i3\theta}$.
Note that a point is constructible if and only if its real and imaginary parts are

constructible. By Euler's formula we have

$$\begin{aligned}
&\cos(3\theta) + i\sin(3\theta) = e^{i3\theta} = (e^{i\theta})^3 = (\cos\theta + i\sin\theta)^3 = \\
&= \cos^3\theta + 3i\cos^2\theta\sin\theta - 3\cos\theta\sin^2\theta - i\sin^3\theta \\
&= \cos^3\theta + 3i(1-\sin^2\theta)\sin\theta - 3\cos\theta(1-\cos^2\theta) - i\sin^3\theta \\
&= 4\cos^3\theta - 3\cos\theta + i(-4\sin^3\theta + 3\sin\theta).
\end{aligned}$$

If we consider the real and imaginary parts we get the two equalities

$$\begin{aligned}
\cos 3\theta &= 4\cos^3\theta - 3\cos\theta \\
-\sin 3\theta &= 4\sin^3\theta - 3\sin\theta.
\end{aligned}$$

We see that the real and imaginary parts of the point we wanted to construct is both solutions to equations of the form

$$4x^3 - 3x = A$$

where A is a real (constructible) number with $|A| \leq 1$. Hence being able to trisect angles is equivalent to being able to solve this kind of equations.

Note that if we solve the equation for $\cos\theta$ the number $e^{i\theta}$ is the intersection of the unit circle and a vertical line that goes through $\cos\theta$. In terms of field extensions we start with some field K containing $\cos(3\theta)$, and consider the field extension $K(\cos\theta)$. Then $e^{i\theta}$ lies in a quadratic extension of this field. As we saw above $\cos\theta$ is a root of the equation

$$4x^3 - 3x = \cos(3\theta).$$

We also have

$$\cos(3\theta) = \cos(3\theta + 2\pi) = 4\cos^3\Big(\theta + \frac{2\pi}{3}\Big) - 3\cos\Big(\theta + \frac{2\pi}{3}\Big)$$

and

$$\cos(3\theta) = \cos(3\theta - 2\pi) = 4\cos^3\Big(\theta - \frac{2\pi}{3}\Big) - 3\cos\Big(\theta - \frac{2\pi}{3}\Big),$$

so the equation has the three roots

$$\cos(\theta),\ \cos\Big(\theta + \frac{2\pi}{3}\Big),\ \cos\Big(\theta - \frac{2\pi}{3}\Big).$$

If $4x^3 - 3x - \cos(3\theta)$ is reducible over K, it can be factorized as a product of one quadratic and one linear polynomial, or three linear polynomials. But then we could have constructed $\cos\theta$ with only the ruler and compass, so let us assume $4x^3 - 3x - \cos(3\theta)$ is irreducible over K. Then the extension $K \subset K(\cos\theta)$ is of degree three.

As before, we usually want to start with the field $\mathbb{Q}$ when constructing numbers.

Theorem 4. *Let $z \in \mathbb{C}$ be constructible by ruler, compass, and angle trisector. Then there is a tower*

$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n \subset \mathbb{C}$$

of field extensions, with $z \in K_n$ and $[K_n : \mathbb{Q}] = 2^k \cdot 3^l$.

Proof. This is proved the same way as Theorem 2. What is diffrent here is that the extension $K_{i+1} = K_i(p) \subset K_i$ might come from trisecting an angle. We need to verify that K_{i+1} is closed under complex conjugation also in this case. As we have seen above trisecting an angle corresponds to a series of ruler and compass operations, and adjoining the real part of the cuberoot of a number on the unit circle. We may therefore assume that $K_{i+1} = K_i(\cos\theta)$ and $\cos(3\theta) \in K_i$. If K_i is closed under complex conjugation, so is $K_i(\cos\theta)$. We get a tower

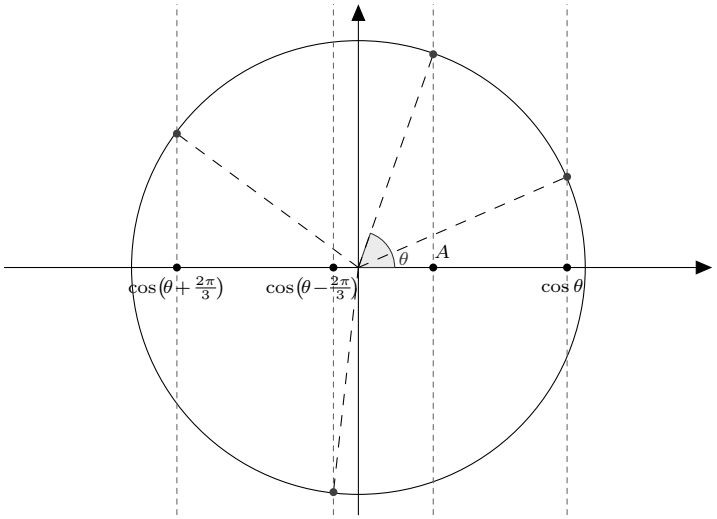
$$\mathbb{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$$

where each extension is of degree 2 or 3. Hence $[K_n : \mathbb{Q}] = 2^k \cdot 3^l$, where k is the number of degree 2 extensions, and l the number of degree 3 extensions. □

The converse statement might not be true here; A normal degree 3 field extension might be the splitting field of a cubic polynomial that can not be solved by ruler, compass, and angle trisector. In the next section we shall investigate what kind of polynomial equations can be solved with these tools.

3.2 Cubic equations

We have seen that any quadratic polynomial equation can be solved using ruler and compass. With the angle trisector we can also solve some cubic equations. Given an equation of the form $4x^3 - 3x = A$, where $|A| \leq 1$, we may assume that $A = \cos(3\theta)$ for some angle θ. But given only $\cos(3\theta)$ there are two possible choices for the angle 3θ (when $|A| \neq 1$). The choice of angle should not affect the solution, and this can easily be verified. Say we make a choice of the angle 3θ, and get the solutions $\cos(\theta)$, $\cos(\theta + \frac{2\pi}{3})$, and $\cos(\theta - \frac{2\pi}{3})$. The other possible choice of the angle is -3θ. This gives the same solutions since $\cos(-\theta) = \cos(\theta)$, $\cos(-\theta + \frac{2\pi}{3}) = \cos(\theta - \frac{2\pi}{3})$, $\cos(-\theta - \frac{2\pi}{3}) = \cos(\theta + \frac{2\pi}{3})$. Hence, to solve the equation geometrically, we make an appropriate choice of angle, trisect it, and add the angles $\frac{2\pi}{3}$ and $-\frac{2\pi}{3}$. We project these angles on the real axis to get the three solutions to the equations.



But the question is now, when can a cubic equation be written of the form

$$4x^3 - 3x = A$$

for some real number A where $|A| \leq 1$?

3.2.1 Rewriting equations, a condition on the coefficients

Any third degree equation

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

can be written as

$$t^3 + pt + q = 0$$

by the substitution $x = t - \frac{a}{3}$ of variables. When can such an equation be written as

$$4x^3 - 3x = A$$

where A is a real number with $|A| \leq 1$?

Assume we have the equation

$$x^3 + px + q = 0.$$

There are two things we can do that preserves the degree:

- A substitution $x = \alpha_1 t + \alpha_2$ of variables, where α_1 and α_2 are complex numbers.
- Multiply the equation by some complex number β.

But a substitution $x = \alpha_1 t + \alpha_2$ where $\alpha_2 \neq 0$ would give us the quadratic term back, and we don't want that. Therefore we do a substitution $x = \alpha t$, and multiply by β, for some $\alpha, \beta \in \mathbb{C}$. This gives us

$$\beta\alpha^3 t^3 + \beta\alpha pt + \beta q = 0.$$

Now we want to choose the numbers α and β such that

$$\beta\alpha^3 = 4, \quad \beta\alpha p = -3, \quad \beta q \in \mathbb{R} \text{ and } |\beta q| \leq 1.$$

We may rewrite the first equality as

$$\beta = \frac{4}{\alpha^3}.$$

If we put this into the second we get

$$\frac{4}{\alpha^2} p = -3$$

and

$$\alpha^2 = -\frac{4}{3} p.$$

Here we see that p must be non-zero. We can solve out α as

$$\alpha = \pm 2\sqrt{-\frac{p}{3}}.$$

We now have the following expression for β

$$\beta = \frac{4}{\alpha^3} = \frac{4}{\pm\left(2\sqrt{-\frac{p}{3}}\right)^3} = \frac{1}{\pm 2\sqrt{-\frac{p}{3}}^3} = \frac{1}{\mp\frac{2p}{3}\sqrt{-\frac{p}{3}}} = \mp\frac{3}{2p}\sqrt{-\frac{3}{p}}.$$

We also wanted $\beta q \in \mathbb{R}$, and $|\beta q| \leq 1$. That is,

$$A = q\frac{3}{2p}\sqrt{-\frac{3}{p}} \in \mathbb{R}, \text{ and } |A| \leq 1.$$

Note that, if p and q are real, p must be negative for A to be real (we take the square root of $-\frac{3}{p}$). In this case the condition on A can be formulated as

$$q \leq \frac{2p}{3}\sqrt{-\frac{p}{3}}$$

or if we want

$$q^2 \leq -4\left(\frac{p}{3}\right)^3.$$

We now have a condition on the coefficients for reformulation of the equation to be possible. To summarize:
The equation

$$x^3 + px + q = 0$$

can be rewritten as

$$4x^3 - 3x = A$$

where $A \in \mathbb{R}$ and $|A| \leq 1$ if $p \neq 0$ and the number

$$q\frac{3}{2p}\sqrt{-\frac{3}{p}}$$

satisfies the conditions on A. In the real case the two conditions becomes

$$p < 0, \text{ and } \; q^2 \leq -4\left(\frac{p}{3}\right)^3.$$

We do this by substituting

$$x = 2\sqrt{-\frac{p}{3}}t,$$

and multiplying the equation by the number

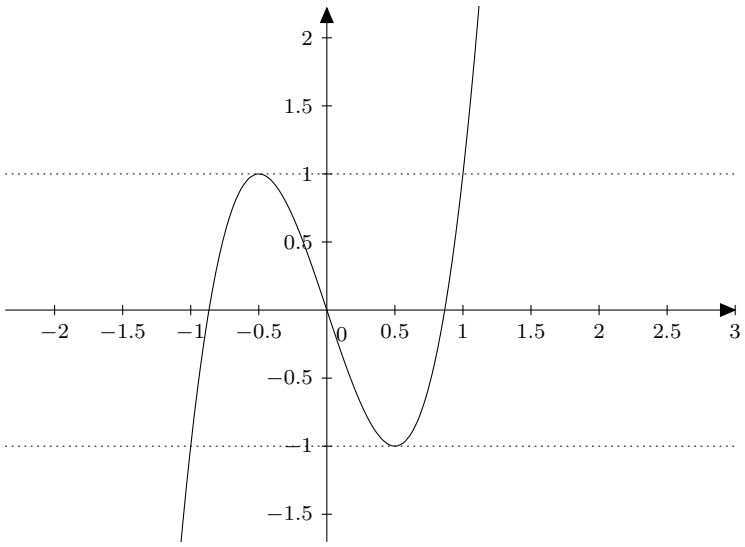
$$-\frac{3}{2p}\sqrt{-\frac{3}{p}}.$$

3.2.2 Rewriting equations, a condition on the roots

We shall now study the roots of the equation $4x^3-3x = A$, where $A \in \mathbb{R}$. When $|A| \leq 1$ we can find an angle θ such that $A = \cos 3\theta$. Then we know that the equation has the roots

$$\cos(\theta),\ \cos\Big(\theta + \frac{2\pi}{3}\Big),\ \cos\Big(\theta - \frac{2\pi}{3}\Big).$$

But what happens when $|A| > 1$?
The function $f(x) = 4x^3-3x$ has the derivative $f'(x) = 12x^2-3$. The derivative has its zeroes in $\frac{1}{2}$ and $-\frac{1}{2}$. The second derivative, $f''(x) = 24x$, is positive in $\frac{1}{2}$, and negative $-\frac{1}{2}$. Hence the function $f(x)$ has a local minimum in $\frac{1}{2}$, and a local maximum in $-\frac{1}{2}$. Note also that $f(x) \longrightarrow \pm\infty$ when $x \longrightarrow \pm\infty$. We see that $f(x)$ has the upper bound $f(-\frac{1}{2}) = 1$, but now lower bound, on $(-\infty, 0]$. On $[0, \infty)$ the function has the lower bound $f(\frac{1}{2}) = -1$, and no upper bound.



Hence the equation $f(x) = A$ has three real roots if and only if $|A| \leq 1$.

Assume now that we have an equation

$$x^3 + px + q = 0$$

with three real roots $x_1,\ x_2$ and x_3. Then

$$\begin{aligned} x^3 + px + q &= (x - x_1)(x - x_2)(x - x_3) \\ &= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

From this we get the equalities

$$x_1 + x_2 + x_3 = 0, \tag{1}$$

$$p = x_1x_2 + x_1x_3 + x_2x_3 \tag{2}$$

and

$$q = -x_1x_2x_3. \tag{3}$$

We also have

$$(x_1 + x_2 + x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3 = 0$$

and hence

$$p = x_1x_2 + x_1x_3 + x_2x_3 = -\frac{x_1^2 + x_2^2 + x_3^2}{2}.$$

We see that $p < 0$, except when all the roots are zero, then of course $p = 0$. This is one of the properties on the coefficients we had before.
Actually, the second property is satisfied as well. To show this, we start with considering the discriminant of the polynomial, which is given by

$$\Delta = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

Since all the roots are real $\Delta \geq 0$, with equality only if two of the roots are equal. From (1) we get $x_3 = -x_1 - x_2$. We use this and expand the expression for the

$$\begin{aligned}\Delta &= (x_1 - x_2)^2(2x_1 + x_2)^2(x_1 + 2x_2)^2 \\ &= 4x_1^6 + 12x_1^5x_2 - 3x_1^4x_2^2 - 26x_1^3x_2^3 - 3x_1^2x_2^4 + 12x_1x_2^5 + 4x_2^6 \geq 0.\end{aligned}$$

The property

$$q^2 \leq -4\left(\frac{p}{3}\right)^3$$

becomes

$$(x_1x_2x_3)^2 \leq -4\frac{(x_1x_2 + x_1x_3 + x_2x_3)^3}{27}$$

here. We shall show that this gives us the same expression as the one we got from the discriminant above. The left hand side is expanded as

$$(x_1x_2x_3)^2 = (x_1x_2(x_1 + x_2))^2 = x_1^4x_2^2 + 2x_1^3x_2^3 + x_1^2x_2^4,$$

and the right hand side

$$\begin{aligned}&-\frac{4}{27}(x_1x_2 + x_1x_3 + x_2x_3)^3 \\ =&-\frac{4}{27}(x_1x_2 - x_1(x_1 + x_2) - x_2(x_1 + x_2))^3 \\ =&\frac{4}{27}(x_1^2 + x_2^2 + x_1x_2)^3 \\ =&\frac{4}{27}(x_1^6 + 3x_1^5x_2 + 6x_1^4x_2^2 + 7x_1^3x_2^3 + 6x_1^2x_2^4 + 3x_1x_2^5 + x_2^6),\end{aligned}$$

so we have the inequality

$$27(x_1^4x_2^2 + 2x_1^3x_2^3 + x_1^2x_2^4) \leq 4(x_1^6 + 3x_1^5x_2 + 6x_1^4x_2^2 + 7x_1^3x_2^3 + 6x_1^2x_2^4 + 3x_1x_2^5 + x_2^6).$$

If we collect all the terms on one side we get

$$4x_1^6 + 12x_1^5x_2 - 3x_1^4x_2^2 - 26x_1^3x_2^3 - 3x_1^2x_2^4 + 12x_1x_2^5 + 4x_2^6 \geq 0.$$

This is the same expression as the one we got from the discriminant. Hence the equation satisfies both our conditions.

This could also be deduced directly from the formula, [6, p. 256]

$$\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2$$

for the discriminant of the polynomial $ax^3 + bx^2 + cx + d$. In our case, with the polynomial $x^3 + px^2 + q$, this becomes

$$\Delta = -4p^3 - 27q^2.$$

The discriminant is positive if and only if all roots are real, so this would also give us the second condition.

Note also that the roots to

$$t^3 + pt + q = 0$$

are real if and only if the roots to the original equation

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

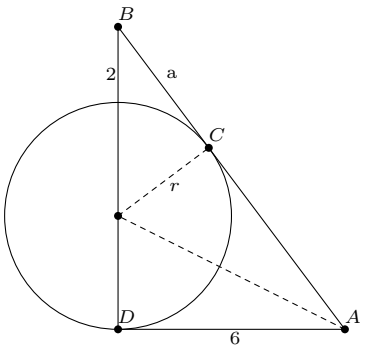
are real, since the reformulation was done by the substitution $x = t - \frac{a}{3}$. We have shown the following theorem.

Theorem 5. *A cubic polynomial equation can be written as*

$$4x^3 - 3x = A$$

where and $|A| \leq 1$, if and only if it has three real roots. Hence any cubic polynomial with three real roots can be solved geometrically by ruler, compass, and angle trisector.

We finish this section with an example, inspired by an old Chinese riddle.
There is a circular castle with two gates, one to the north and one to the south. Two *li* (a Chinese unit, approximately 500 meters) outside the north gate there is a large tree. This tree can be seen standing at a point no less than six *li* east of the south gate. What is the radius of the castle?
We call the point where the tree is B, and the point from where the tree is visible A. We draw a straight line from A to B, and call the point where it tangents the circle of the castle C. Let a denote the distance from B to C.



Note that we have three right triangles with one corner in the centre of the castle. The one with corners in A and D (the south gate) is in fact the congruent to the one with corners in A and C. Hence the distance between A and C is 6. The smaller triangle, with a corner in B, together with the big triangle with corners in A, B and D gives us the equations

$$\begin{cases} a^2 + r^2 = (r+2)^2 \\ 36 + (2r+2)^2 = (a+6)^2 \end{cases}.$$

The first one is simplified as

$$a^2 = 4(r+1).$$

We know that a is positive, since it is a distance, so we insert $a = 2\sqrt{(r+1)}$ in the second equation and get

$$36 + (2r+2)^2 = (2\sqrt{(r+1)} + 6)^2,$$

which (after some elementary algebraic operations) becomes

$$r^2 + r = 6\sqrt{r+1}.$$

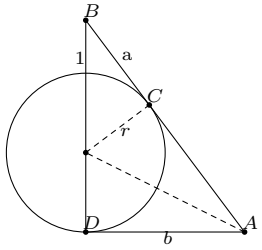
We square both sides to get a polynomial equation

$$r^4 + 2r^3 + r^2 = 36(r+1).$$

The left hand side factorizes as $r^2(r+1)^2$, and since $r = -1$ is not a solution to our problem (we do not want a negative radius), we cancel the factor $(r+1)$. We now have the cubic polynomial equation

$$r^2(r+1) = 36.$$

This equation has the root $r = 3$, and is hence reducible, so we do not need our angle trisector here. But let us generalize the problem a bit. Instead of the distances two and six *li* we define the distance from the north gate to the tree to be one (and forget about the unit *li*), and call the distance from the south



gate to the point where the tree is visible b.
For which b can this be solved geometrically with the angle trisector? Our two equations now becomes

$$\begin{cases} a^2 + r^2 = (r+1)^2 \\ b^2 + (2r+1)^2 = (a+b)^2 \end{cases}.$$

The first equation gives us $a^2 = 1 + 2r$, and placing this in the second one gives

$$a^4 = a^2 + 2ab,$$

and hence

$$a^3 - a = 2b.$$

We factorize the left hand side

$$a(a^2 - 1) = 2b$$

and note that $a = \sqrt{1 + 2r}$, and $a^2 - 1 = 2r$. Hence, in terms of r the equation becomes

$$2r\sqrt{1 + 2r} = 2b$$

or

$$r^2(1 + 2r) = b^2.$$

We write this as a monic polynomial equation

$$r^3 + \frac{r^2}{2} - \frac{b^2}{2} = 0$$

and try to solve it with the method from section 3.2.1. The first step is the substitution $r = t - \frac{1}{6}$, to eliminate the quadratic term. This gives the equation

$$t^3 - \frac{t}{12} - \frac{b^2}{2} + \frac{1}{108} = 0.$$

The next step is the substitution $t = 2\sqrt{-\frac{p}{3}}x$, where p is the coefficient of the linear term. In this case $p = -\frac{1}{12}$, so we get

$$t = 2\sqrt{\frac{1}{36}}x = \frac{x}{3}.$$

The equation becomes

$$\frac{x^3}{27} - \frac{x}{36} - \frac{b^2}{2} + \frac{1}{108} = 0.$$

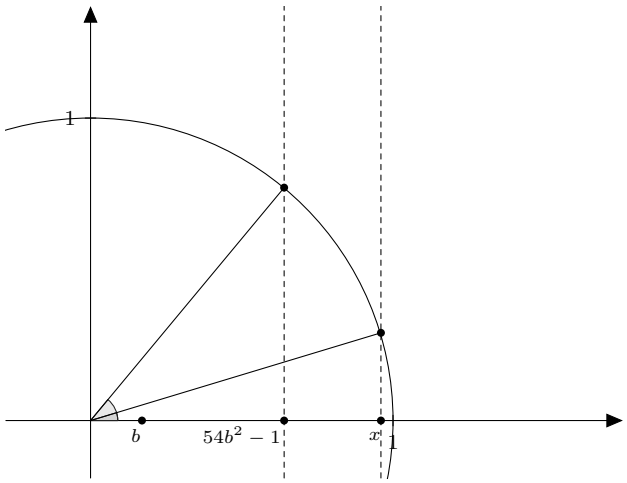
Last we multiply by $4 \cdot 27 = 108$ and get

$$4x^3 - 3x = 54b^2 - 1.$$

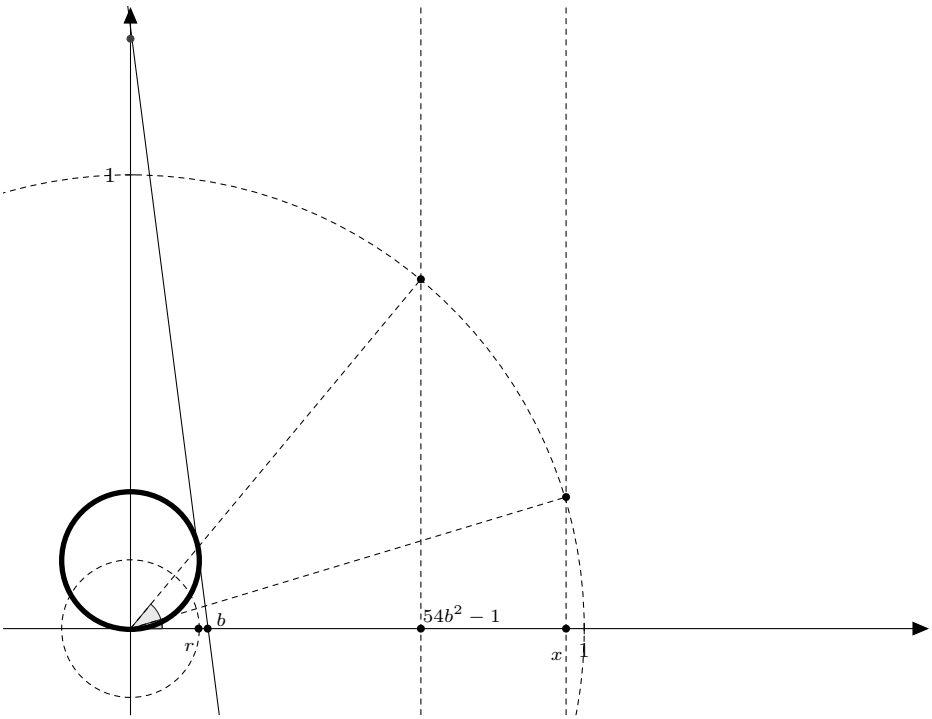
For this to be solvable by angle trisection we need

$$b^2 \leq \frac{2}{54} = \frac{1}{27}.$$

Assume now that our distance b satisfies this condition. How do we draw the castle?
The number $54b^2 - 1$ is $\cos 3\theta$, for some angle 3θ, which we find by drawing the unit circle. Then we use our angle trisector to get the angle θ, and the number $x = \cos\theta$.

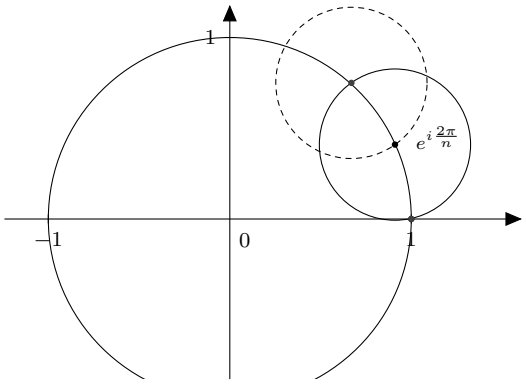


To get the radius r we must now construct the number $r = t - \frac{1}{6} = \frac{x}{3} - \frac{1}{6}$. The south gate of the castle will in this picture be at the origin, so we draw a circle with radius r that goes through the origin. We mark the place of the tree (which is the complex number $(2r + 1)i$) as well, and see that it should be visible from the point b.



4 Regular polygons

A particularly interesting kind of construction is the construction of regular polygons. A regular n-gon will in this case have its corners at the n:th roots of unity. The essential part is to construct the number $\omega = e^{i\frac{2\pi}{n}}$. Once this is done we have two adjacent corners (1 and ω), and we can use the compass to draw a circle with center in ω that goes through 1. This circle intersects the unit circle in the next corner of the n-gon, and we proceed in the same way to construct the other corners.



Not all regular polygons can be constructed. In the next section we shall se which n-gons are constructible by ruler and compass.

4.1 Construction of regular polygons using ruler and compass

Assume that the regular n-gon, and the regular m-gon are constructible, and that n and m are relatively prime. Then there are some integers a and b such that $an + bm = 1$. We have

$$\frac{1}{mn} = \frac{a}{m} + \frac{b}{n},$$

and

$$e^{i\frac{2\pi}{mn}} = \left(e^{i\frac{2\pi}{m}}\right)^a \left(e^{i\frac{2\pi}{n}}\right)^b.$$

Hence the regular mn-gon is constructible.

The regular 2^k-gon is constructible. This can easily be proved by induction. If $k = 2$ (smaller k does not give an actual polygon), we get a square with corners in $1,\ i,\ -1$ and $-i$. This is obviously constructible. If the 2^k-gon is constructible we get the 2^{k+1}-gon by bisecting the angle $\frac{2\pi}{2^k}$.

However, we shall see that the regular p^a-gon is not constructible, when $a > 1$ and p is an odd prime.
Assume, for a contradiction, that the regular p^a-gon is constructible, for some $a > 1$. Then the number

$$\left(e^{i\frac{2\pi}{p^a}}\right)^{p^{a-2}} = e^{i\frac{2\pi}{p^2}},$$

and hence the regular p^2-gon, is constructible. Geometrically, we can get the p^2-gon by adjoining every p^{a-2}th corner in the p^a-gon. We shall now prove that the minimal polynomial of $e^{i\frac{2\pi}{p^2}}$ is

$$f(x) = 1 + x^p + x^{2p} + \cdots + x^{(p-1)p}.$$

Note that

$$f(x) = \frac{x^{p^2} - 1}{x^p - 1}$$

and

$$f\left(e^{i\frac{2\pi}{p^2}}\right) = \frac{0}{e^{i\frac{2\pi}{p}} - 1} = 0.$$

We need to show that $f(x)$ is irreducible. The polynomial $f(x)$ is irreducible if and only if $f(1+t)$ is irreducible. We have

$$f(1+t) = 1 + (1+t)^p + (1+t)^{2p} + \cdots + (1+t)^{(p-1)p}.$$

This polynomial has the constant term p. We also have

$$f(1+t) = \frac{(1+t)^{p^2} - 1}{(1+t)^p - 1}.$$

Recall that $(x+y)^{p^n} \equiv x^{p^n} + y^{p^n} \mod p$. Hence

$$f(1+t) \equiv \frac{1 + t^{p^2} - 1}{1 + t^p - 1} = \frac{t^{p^2}}{t^p} = t^{(p-1)p} \mod p.$$

Then

$$f(1+t) = t^{(p-1)p} + p \cdot tk(t) + p$$

for some polynomial $k(t)$ with integer coefficients. By Eisensteins criterion, with the prime p, the polynomial $f(x)$ is irreducible. Hence $e^{i\frac{2\pi}{p^2}}$ has degree $(p-1)p$ over $\mathbb{Q}$. This is obviously not a power of 2, and by Theorem 2 the number $e^{i\frac{2\pi}{p^2}}$ is not constructible. This contradicts our assumption, and hence the regular p^a-gon is not constructible, when $a > 1$.

We have now proved that the regular n-gon is constructible if and only if $n = 2^k p_1 \cdots p_l$, where $p_1, \ldots, p_l$ are distinct odd primes and the regular p_i-gons are constructible. The question is, for which primes p is the regular p-gon constructible?

For the regular p-gon to be constructible we need the degree of $\omega = e^{i\frac{2\pi}{p}}$ over $\mathbb{Q}$ to be a power of 2. We shall first prove that the minimal polynomial of ω is

$$f(x) = 1 + x + x^2 + \cdots + x^{p-1}.$$

We do this in a similar way as above. Note that

$$f(x) = \frac{x^p - 1}{x - 1}$$

and

$$f(\omega) = \frac{\omega^p - 1}{\omega - 1} = 0.$$

The polynomial

$$f(1+t) = 1 + (1+t) + (1+t)^2 + \cdots + (1+t)^{p-1}$$

has the constant term p. Since

$$f(1+t) = \frac{(1+t)^p - 1}{1+t-1} = \frac{(1+t)^p - 1}{t} \equiv \frac{t^p}{t} = t^{p-1} \mod p$$

we can use Eisensteins criterion as before, and hence $f(x)$ is irreducible. Then ω has the degree $p-1$ over $\mathbb{Q}$. Hence the regular p-gon is constructible when $p-1$ is a power of 2. That is, when $p = 2^k + 1$, for some integer k.
The number $2^k + 1$ can only be prime when $k = 2^n$ for some integer n, because if $k = ab$ where b is odd

$$2^k + 1 = 2^{ab} + 1 = (2^a)^b + 1 \equiv (-1)^b + 1 = -1 + 1 = 0 \mod 2^a - 1.$$

This was originally proved by Fermat, and primes of this form are called Fermat primes. However, not all numbers of the form $2^{2^n} + 1$ are prime. Fermat himself found that the first five numbers in the sequence, which is

$$\begin{aligned} 2^{2^0} + 1 &= 3 \\ 2^{2^1} + 1 &= 5 \\ 2^{2^2} + 1 &= 17 \\ 2^{2^3} + 1 &= 257 \\ 2^{2^4} + 1 &= 65537, \end{aligned}$$

are prime. These are believed to be the only Fermat primes, but no one has been able provide a proof.

The results of this section summarizes to the following theorem.

Theorem 6. *The regular n-gon is constructible by ruler and compass if and only if*

$$n = 2^k p_1 \cdots p_l$$

where $p_1, \ldots, p_l$ are distinct Fermat primes.

4.2 Construction of regular polygons using ruler, compass, and angle trisector

We now ask ourselves what new regular polygons can be constructed when we allow angle trisecting. An immediate result is that the 3^k-gon is constructible. The regular triangle with corners in the third roots of unity, that is $-\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$ and 1, is obviously constructible. We get the 3^k-gon inductively by trisecting angles, as with the 2^k-gon. Hence any regular $2^k 3^l p_1 \cdots p_m$-gon, where $p_1, \ldots, p_m$ are Fermat primes, are constructible. But can we construct a regular p-gon, for some prime p that is not a Fermat prime? A guess would be that this works for primes of the form $2^n 3^m + 1$, which are called Pierpont primes after the

mathematician James Pierpont. But this is not obvious, since not all field extensions of degree three are allowed. We shall start with a special case of the Pierpont primes, the primes of the form $2^n 3 + 1$. The first two are $2 \cdot 3 + 1 = 7$ and $4 \cdot 3 + 1 = 13$. It turns out that the regular heptagon (7-gon), and tridecagon (13-gon) are constructible.

4.2.1 The regular heptagon

Let $\omega = e^{i\frac{2\pi}{7}}$. This is then the first corner in the heptagon, and the others are given by ω^2, $\omega^3, \ldots, \omega^7$. These are the seventh roots of unity, that is the roots of the polynomial $x^7 - 1$. This polynomial is factorized as

$$x^7 - 1 = (x - 1)(1 + x + \cdots + x^6).$$

As we saw above, the polynomial $(1 + x + \cdots + x^6)$ is irreducible, and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$. To find out more about this extension we shall use some Galois theory. The Galois group Γ corresponding to the extension $[\mathbb{Q}(\omega) : \mathbb{Q}]$ has six elements. As we know, the Galois group consists of permutations of the zeroes of the polynomial, or equivalently of all automorphisms on $\mathbb{Q}(\omega)$ that fixes $\mathbb{Q}$. Since all the zeroes are powers of ω every $\tau \in \Gamma$ is completely determined by $\tau(\omega)$. There are six possible automorphisms, since ω can be mapped to itself or any of the other zeroes. Since Γ should have six elements, all these occur. That is

$$\Gamma = \{\tau_i\}_{i=1}^6, \text{ where } \tau_i(\omega) = \omega^i.$$

The automorphism τ_3 generates the group since

$$\begin{aligned}
\tau_3(\omega) &= \omega^3 \\
\tau_3^2(\omega) &= \tau_3(\omega^3) = \omega^9 = \omega^2 \\
\tau_3^3(\omega) &= \tau_3(\omega^2) = \omega^6 \\
\tau_3^4(\omega) &= \tau_3(\omega^6) = \omega^{18} = \omega^4 \\
\tau_3^5(\omega) &= \tau_3(\omega^4) = \omega^{12} = \omega^5 \\
\tau_3^6(\omega) &= \tau_3(\omega^5) = \omega^{15} = \omega
\end{aligned}$$

(recall that $\omega^7 = 1$). Let $\tau = \tau_3$. Then $\Gamma = \langle\tau\rangle$, and we have a subgroup

$$\langle\tau^3\rangle = \{\tau^3, \tau^6\}$$

By Galois theory this tells us that there is a field K such that $\mathbb{Q} \subset K \subset \mathbb{Q}(\omega)$, where $[\mathbb{Q}(\omega) : K] = 2$, and $[K : \mathbb{Q}] = 3$. The field K consists of everything that is fixed under τ^3. So we need to find out what elements that are, other than the rational numbers. As a start, note that

$$\tau^3(\omega) = \omega^{3^3} = \omega^{27} = \omega^6 = \overline{\omega}$$

and then

$$\tau^3(\omega^k) = \overline{\omega}^k = \overline{\omega^k}.$$

That is, τ^3 maps every element to its complex conjugate. Since

$$\overline{\omega} = \omega^6, \quad \overline{\omega^2} = \omega^5, \text{ and } \overline{\omega^3} = \omega^4,$$

we have

$$\begin{aligned}\tau^3(\omega+\omega^6) =& \omega+\omega^6\\ \tau^3(\omega^2+\omega^5) =& \omega^2+\omega^5\\ \tau^3(\omega^3+\omega^4) =& \omega^3+\omega^4.\end{aligned}$$

Put

$$x_1=\omega+\omega^6,\quad x_2=\omega^2+\omega^5,\ \text{and}\ x_3=\omega^3+\omega^4.$$

Note that these are real numbers, since they are sums of complex conjugates. We also have

$$x_1+x_2+x_3=\sum_{j=1}^{6}\omega^j=-1,$$

$$\begin{aligned}x_1x_2+&x_1x_3+x_2x_3 =\\ &=(\omega+\omega^6)(\omega^2+\omega^5)+(\omega+\omega^6)(\omega^3+\omega^4)+(\omega^2+\omega^5)(\omega^3+\omega^4)\\ &=\omega^3+\omega^6+\omega+\omega^4+\omega^4+\omega^5+\omega^2+\omega^3+\omega^5+\omega^6+\omega+\omega^2=-2\end{aligned}$$

and

$$\begin{aligned}x_1x_2x_3 =&(\omega+\omega^6)(\omega^2+\omega^5)(\omega^3+\omega^4)\\ =&(\omega^3+\omega^6+\omega+\omega^4)(\omega^3+\omega^4)\\ =&\omega^6+\omega^2+\omega^4+1+1+\omega^3+\omega^5+\omega+1=1.\end{aligned}$$

Hence the numbers $x_1,\ x_2$ and x_3 are roots of the polynomial equation

$$\begin{aligned}(x-x_1)(x-&x_2)(x-x_3) =\\ &=x^3-(x_1+x_2+x_3)x^2+(x_1x_2+x_1x_3+x_2x_3)x-x_1x_2x_3\\ &=x^3+x^2-2x-1=0\end{aligned}$$

This equation has rational coefficients and real roots, so it should be solvable by ruler, compass, and angle trisector. But to see how the construction goes we need to rewrite the equation on the form $4x^3-3x=A$. The first step is the substitution $x=t-\frac{1}{3}$, to eliminate the quadratic term. We get

$$\begin{aligned}x^3+x^2-2x-1&=\left(t-\frac{1}{3}\right)^3+\left(t-\frac{1}{3}\right)^2-2\left(t-\frac{1}{3}\right)-1\\ &=t^3-\frac{7}{3}t-\frac{7}{27}=0.\end{aligned}$$

The we substitute

$$t=2\sqrt{\frac{7}{9}}u=2\frac{\sqrt{7}}{3}u,$$

which gives

$$8\frac{7\sqrt{7}}{27}u^3-2\frac{7\sqrt{7}}{9}u-\frac{7}{27}=0.$$

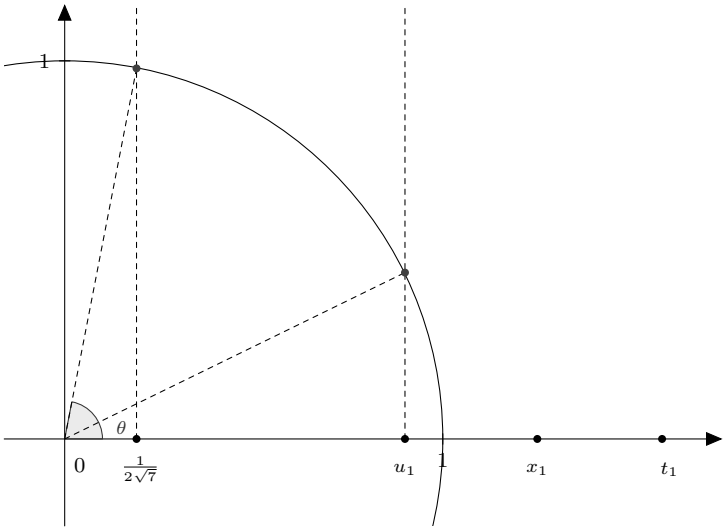
Last we multiply by $\frac{27}{14\sqrt{7}}$, and get

$$4u^3-3u-\frac{1}{2\sqrt{7}}=0.$$

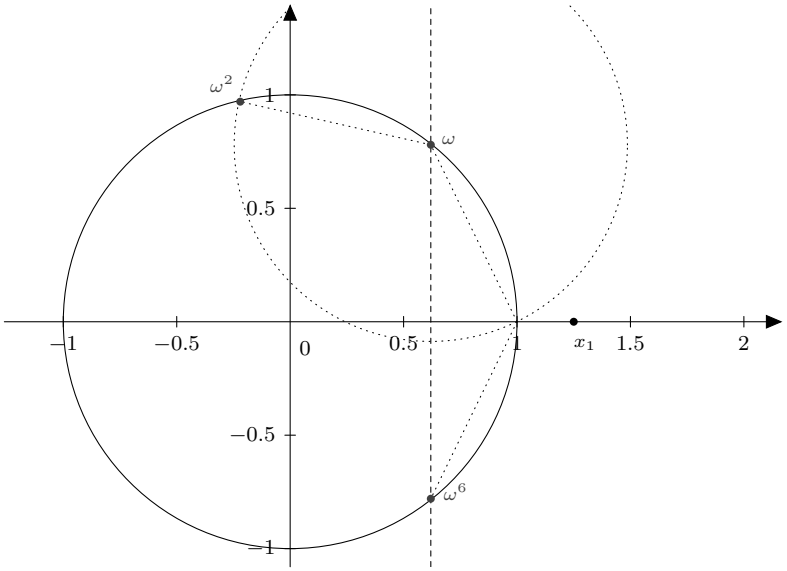
as desired. That is,

$$A = \frac{1}{2\sqrt{7}} = \cos(3\theta),$$

so we need to construct the number $\frac{1}{2\sqrt{7}}$ (which is possible by ruler and compass). Then we draw a vertical line through this point and take the intersection with the unit circle to get the angle 3θ. We trisect the angle to get the solution $u_1 = \cos\theta$. From this we get $t_1 = 2\frac{\sqrt{7}}{3}u_1$ (after constructing $2\frac{\sqrt{7}}{3}$) and $x_1 = t_1 - \frac{1}{3}$. Note that we already defined x_1 in terms of ω, so it is not obvious that this root is x_1, it might equally well be x_2 or x_3. But if we actually perform the construction (or use a computer to approximate the numbers), we see that it is correct.



In the same way we can use u_2 and u_3 given by $\cos\left(\theta \pm \frac{2\pi}{3}\right)$ to get x_2 and x_3. This is not necessary however, we will get all we need from x_1. Recall that $x_1 = \omega + \overline{\omega}$. We draw a vertical line midways between x_1 and the origin. This line intersects the unit circle in ω and $\overline{\omega}$, and as noted earlier we can now use the compass to get the other corners.



4.2.2 The regular tridecagon

Let now $\omega = e^{i\frac{2\pi}{13}}$. Then $1, \omega, \omega^2, \ldots, \omega^{12}$ are the 13th roots of unity, and the corners in the regular tridecagon. These are the zeroes of the irreducible polynomial

$$1 + x + x^2 + \cdots + x^{12}.$$

As with the heptagon, we shall study the Galois group corresponding to the field extension $\mathbb{Q}(\omega) \supset \mathbb{Q}$, which is given by

$$\Gamma = \{\tau_i\}_{i=1}^{12} \text{ where } \tau_i(\omega) = \omega^i.$$

Note that $\tau_i \circ \tau_j = \tau_r$ where r is the remainder of ij when divided by 13, since $\tau_j(\tau_i(\omega)) = \omega^{ij}$ and $\omega^{13} = 1$. Hence τ_n generates Γ when n generates $\mathbb{Z}_{13}^*$. One can easily check that the number 2 generates $\mathbb{Z}_{13}^*$, and hence $\tau = \tau_2$ generates Γ. The automorphism τ^3 generates a subgroup

$$\langle \tau^3 \rangle = \{\mathrm{id}, \tau^3, \tau^6, \tau^9\}$$

since

$$\begin{aligned}
\tau^3(\omega) &= \omega^{2^3} = \omega^8 \\
\tau^6(\omega) &= \tau^3 \circ \tau^3(\omega) = \tau^3(\omega^8) = (\omega^8)^8 = \omega^{64} = \omega^{12} = \omega^{-1} \\
\tau^9(\omega) &= \tau^6 \circ \tau^3(\omega) = (\omega^{-1})^8 = \omega^{-8} = \omega^5 \\
\tau^9 \circ \tau^3(\omega) &= (\omega^5)^8 = \omega^{40} = \omega.
\end{aligned}$$

Note that τ^6 is of order 2, and generates the subgroup

$$\langle \tau^6 \rangle = \{\mathrm{id}, \tau^6\} \subset \langle \tau^3 \rangle.$$

Galois theory then tells us there are fields K_1 and K_2 such that

$$\mathbb{Q} \underset{3}{\subset} K_1 \underset{2}{\subset} K_2 \underset{2}{\subset} \mathbb{Q}(\omega)$$

where the indexed numbers are the degrees of the extensions. K_1 is the fixed field under $\langle\tau^3\rangle$, so we need to find out what is fixed under τ^3. Since

$$\begin{aligned}\tau^3(\omega) =&\omega^8,\\ \tau^3(\omega^8) =&\omega^{12},\\ \tau^3(\omega^{12}) =&\omega^5,\\ \tau^3(\omega^5) =&\omega\end{aligned}$$

we have

$$\tau^3(\omega+\omega^5+\omega^8+\omega^{12}) = \omega+\omega^5+\omega^8+\omega^{12}.$$

In a similar way we see that $\omega^2+\omega^3+\omega^{10}+\omega^{11}$ and $\omega^4+\omega^6+\omega^7+\omega^9$ are fixed under τ^3. Put

$$\begin{aligned}x_1 &= \omega+\omega^5+\omega^8+\omega^{12},\\ x_2 &= \omega^2+\omega^3+\omega^{10}+\omega^{11},\end{aligned}$$

and

$$x_3 = \omega^4+\omega^6+\omega^7+\omega^9.$$

Note that $\overline{\omega}=\omega^{12}$, $\overline{\omega}^2=\omega^{11}$, $\overline{\omega}^3=\omega^{10}$, and so on. Hence

$$x_1 = \omega+\omega^5+\overline{\omega}^5+\overline{\omega},$$

$$x_2 = \omega^2+\omega^3+\overline{\omega}^3+\overline{\omega}^2,$$

and

$$x_3 = \omega^4+\omega^6+\overline{\omega}^6+\overline{\omega}^4.$$

The numbers x_1, x_2, and x_3 are sums of complex conjugates, and hence real. They are not rational though, since

$$\tau(x_1) = \omega^2+\omega^{10}+\overline{\omega}^{10}+\overline{\omega}^2 = \omega^2+\overline{\omega}^3+\omega^3+\overline{\omega}^2 = x_2,$$

$$\tau(x_2) = \omega^4+\omega^6+\overline{\omega}^6+\overline{\omega}^4 = x_3$$

and

$$\tau(x_3) = \tau^2(x_2) = \tau^3(x_1) = x_1,$$

and rational numbers should be fixed under τ.
This means that $K_1 = \mathbb{Q}(x_1,x_2,x_3)$.
In a similar way as for the heptagon we can calculate

$$x_1+x_2+x_3 = \omega+\omega^2+\cdots+\omega^{12} = -1,$$

$$x_1x_2+x_1x_3+x_2x_3 = -4,$$

and

$$x_1x_2x_3 = -1$$

using that $\sum_{i=1}^{12}\omega^i = -1$ repeatedly. Hence x_1, x_2 and x_3 are the roots of the polynomial equation

$$(x-x_1)(x-x_2)(x-x_3) = x^3+x^2-4x+1 = 0.$$

This is a cubic polynomial with rational coefficients and real zeroes, and hence x_1, x_2 and x_3 can be constructed using angle trisection. When this is done we

can construct ω using ruler and compass, since the other two field extensions are of degree two.

We have now proved that the regular tridecagon is constructible. Next, we shall see how this is done geometrically.
First we need to write the equation $x^3+x^2-4x+1=0$ on the form $4x^3-3x=A$. The first substitution, $x=t-\frac{1}{3}$, gives

$$t^3-\frac{13}{3}t+\frac{65}{27}=0,$$

and the second, $t=\frac{2}{3}\sqrt{13}s$, gives

$$\frac{8\cdot 13}{27}\sqrt{13}s^3-\frac{2\cdot 13}{9}\sqrt{13}s+\frac{65}{27}=0.$$

We multiply by $\frac{27}{2\cdot 13\sqrt{13}}$, which gives us the equation

$$4s^3-3s+\frac{5}{2\cdot\sqrt{13}}=0.$$

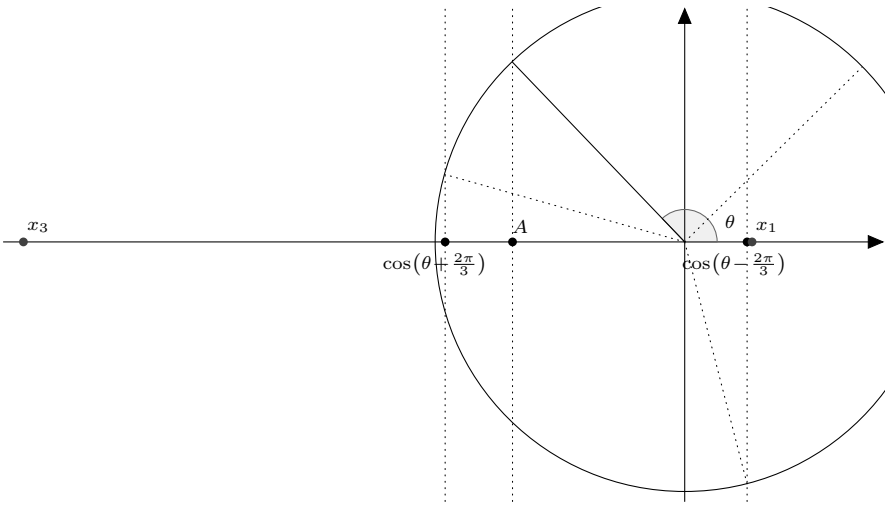
Hence

$$A=-\frac{5}{2\cdot\sqrt{13}}=\cos(3\theta),$$

and the solutions to the equation $x^3+x^2-4x+1=0$ is given by

$$\begin{aligned}
x_1&=\frac{2}{3}\sqrt{13}\cos\left(\theta-\frac{2\pi}{3}\right)-\frac{1}{3}\\
x_2&=\frac{2}{3}\sqrt{13}\cos\theta-\frac{1}{3}\\
x_3&=\frac{2}{3}\sqrt{13}\cos\left(\theta+\frac{2\pi}{3}\right)-\frac{1}{3}
\end{aligned}$$

which we get by angle trisecting, and some ruler and compass operations. One can check that x_i is actually equal to the x_i expressed in terms of ω, for $i=1$, 2 and 3. We shall also see that it is enough to construct x_1 and x_3.



Let us now define the real numbers $y_1 = \omega + \overline{\omega}$ and $y_2 = \omega^5 + \overline{\omega}^5$. Recall that

$$x_1 = \omega + \omega^5 + \overline{\omega}^5 + \overline{\omega} = y_1 + y_2.$$

We also have that

$$y_1 y_2 = \omega^6 + \overline{\omega}^4 + \omega^4 + \overline{\omega}^6 = x_3.$$

Hence y_1 and y_2 are the roots to the quadratic polynomial equation

$$(x - y_1)(x - y_2) = x^2 - x_1 x + x_3 = 0$$

with coefficients in K_1. Note also that

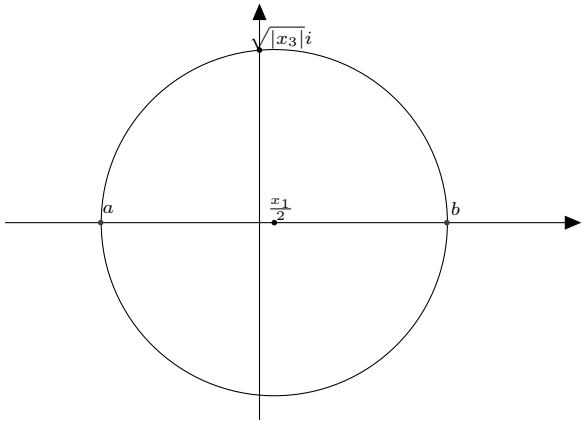
$$y_1 = \omega + \overline{\omega} = 2\cos\left(\frac{2\pi}{13}\right) > 0,$$

$$y_2 = \omega^5 + \overline{\omega}^5 = 2\cos\left(\frac{10\pi}{13}\right) < 0,$$

and hence

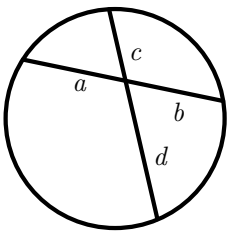
$$x_3 = y_1 y_2 < 0.$$

The points y_1 and y_2 can be constructed by ruler and compass by drawing a circle with center in $\frac{x_1}{2}$ that goes through the point $\sqrt{|x_3|}i$. Call the points where this circle intersects the real axis a and b. We may assume $a < 0$ and $b > 0$.



Now recall the Intersecting Chords Theorem.

Theorem 7 (Intersecting Chords Theorem)**.**



Assume we have two intersecting chords in a circle. The point where the chords intersect splits the first chord into two segments of length a and b. In the same way the second chord splits into two segments of length c and d. Then $ab = cd$.

Applied to this case, where the cords are given by the real and imaginary axes, the theorem says that $-ab = |x_3| = -x_3$ and hence $ab = x_3$. Since we also have $a + b = x_1$, the numbers a and b must be the solutions to the equation $x^2 - x_1 x + x_3 = 0$. Hence $y_1 = b$ and $y_2 = a$.
Now the number $y_1 = \omega + \overline{\omega}$ is constructed, and from this we get the first corner of the tridecagon.

4.2.3 The regular $2^n 3+1$-gon

With a few results from Group Theory we will be ready to consider the regular p-gon, when $p = 2^n \cdot 3 + 1$. This shall later be generalized to the case when p is a Pierpont prime.

Theorem 8. *The multiplicative group $\mathbb{Z}_p^*$, where p is prime, is cyclic.*

Theorem 9. *The subgroups of a cyclic group all have different order.*

For proofs see [1, p. 136] and [1, p. 347].

Theorem 10. *The regular p-gon, where p is a prime on the form $2^n \cdot 3 + 1$, is constructible.*

Proof. Let p be a prime such that $p = 2^n \cdot 3 + 1$, for some integer n, and let $\omega = e^{i\frac{2\pi}{p}}$. As before, we note that $\omega,\ \omega^2, \ldots, \omega^{p-1}$ are the zeroes of the polynomial

$$f(x) = 1 + x + x^2 + \ldots + x^{p-1},$$

and we consider the corresponding Galois group Γ. The group Γ is given by

$$\Gamma = \{\tau_i\}_{i=1}^{p-1}$$

where τ_i is an automorphism on $\mathbb{Q}(\omega)$ that fixes the rational numbers and maps ω to ω^i. As noted in the construction of the tridecagon, τ_m generates Γ when m generates $\mathbb{Z}_p^*$. By the theorem above, such an m exists. Let $\tau = \tau_m$. Hence $\Gamma = \langle\tau\rangle$ is a cyclic group, and all subgroups have different order.

Complex conjugation is an automorphism on $\mathbb{Q}(\omega)$ that leaves $\mathbb{Q}$ fixed, and hence an element in the Galois group Γ. Complex conjugation has order two, and generates a subgroup of order two. But $\langle\tau^{\frac{p-1}{2}}\rangle$ is also a subgroup of order two, hence $\tau^{\frac{p-1}{2}} = \tau^{3\cdot 2^{n-1}}$ must be complex conjugation.

Now consider the chain of subgroups

$$\Gamma = \langle\tau\rangle \supset \langle\tau^3\rangle \supset \langle\tau^{3\cdot 2}\rangle \supset \cdots \supset \langle\tau^{3\cdot 2^{n-1}}\rangle,$$

and the corresponding tower of field extensions

$$\mathbb{Q} \subset K_1 \subset \cdots \subset K_n \subset \mathbb{Q}(\omega),$$

where K_1 is the fixed field of τ^3, K_2 the fixed field of $\tau^{3\cdot 2}$, and so on. The field K_n is the fixed field of $\tau^{3\cdot 2^{n-1}}$. Since this automorphism was complex conjugation the field K_n, and all the other K_i's, consists of real numbers. The

non-real complex numbers appears first in $\mathbb{Q}(\omega)$.
By the Fundamental Theorem of Galois Theory the field K_1 is normal over $\mathbb{Q}$, since $\langle\tau^3\rangle$ is a normal subgroup of Γ. Let $\alpha \in K_1 \setminus \mathbb{Q}$. Then

$$3 = [K_1 : \mathbb{Q}] = [K_1 : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Since 3 is prime we must have $K_1 = \mathbb{Q}(\alpha)$. Let now $f(x)$ be the minimal polynomial of α over $\mathbb{Q}$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ the degree of $f(x)$ must be 3. The field K_1 was normal over $\mathbb{Q}$, so all the zeroes of $f(x)$ lies in K_1, and are hence real. This means that the field K_1 is constructible by ruler, compass, and angle trisector. The other field extensions were of degree 2, thus we have now proved that the regular p-gon is constructible. □

4.2.4 A closer look at the field K_1

Before generalizing this, we shall take a closer look at the field K_1.
Let $\sigma = \tau^3$. Then K_1 is the fixed field of σ, and we want to find out what is fixed under σ. Note that

$$\sigma(\omega + \sigma(\omega) + \sigma^2(\omega) + \cdots + \sigma^{2^n-1}(\omega)) = \omega + \sigma(\omega) + \sigma^2(\omega) + \cdots + \sigma^{2^n-1}(\omega),$$

since

$$\sigma^{2^n-1} \circ \sigma = \sigma^{2^n} = \tau^{3\cdot 2^n} = \mathrm{id}\,.$$

This also holds if we replace ω by ω^i for any i. So how many different sums, fixed by σ, can we get in this way? We shall see that if two such sums are different then they have no terms in common. Assume we have two sums $\sum_{k=0}^{2^n-1} \sigma^k(\omega^i)$ and $\sum_{k=0}^{2^n-1} \sigma^k(\omega^j)$, where $i \neq j$, with a common term

$$\sigma^a(\omega^i) = \sigma^b(\omega^j).$$

We may assume $a \leq b$. Then

$$\omega^i = \sigma^{b-a}(\omega^j),$$

and

$$\omega^i + \sigma(\omega^i) + \sigma^2(\omega^i) + \cdots + \sigma^{2^n-1}(\omega^i) =$$
$$\sigma^{b-a}(\omega^j) + \cdots + \sigma^{2^n-1}(\omega^j) + \omega^j + \cdots + \sigma^{b-a-1}(\omega^j) =$$
$$\omega^j + \sigma(\omega^j) + \cdots + \sigma^{2^n-1}(\omega^j).$$

Note also that each sum consists of 2^n terms, and all the terms are different powers of ω. Since there are $3 \cdot 2^n$ powers of ω (before we reach 1), we can form three different sums of this type.
Recall that we had $\tau(\omega) = \omega^m$, where m generates $\mathbb{Z}_p^*$. That is $\sigma(\omega) = \omega^{m^3}$, and

$$\mathbb{Z}_p^* = \{1, m, \ldots, m^{3\cdot 2^n-1}\}.$$

Let

$$\begin{aligned}
x_1 =&\omega + \sigma(\omega) + \sigma^2(\omega) + \cdots + \sigma^{2^n-1}(\omega) \\
=&\omega + \omega^{m^3} + \omega^{m^{2\cdot 3}} + \omega^{m^{3\cdot 3}} + \cdots + \omega^{m^{(2^n-1)3}}, \\
x_2 =&\omega^m + \sigma(\omega^m) + \ldots + \sigma^{2^n-1}(\omega^m) \\
=&\omega^m + \omega^{m^4} + \cdots + \omega^{m^{3\cdot 2^n-2}}, \\
&\text{and} \\
x_3 =&\omega^{m^2} + \sigma(\omega^{m^2}) + \ldots + \sigma^{2^n-1}(\omega^{m^2}) \\
=&\omega^{m^2} + \omega^{m^5} + \cdots + \omega^{m^{3\cdot 2^n-1}}.
\end{aligned}$$

We have now found three elements that are fixed under σ. These numbers are of course real, since they belongs to K_1. Another way to see this is the following. Recall that $\sigma^{2^{n-1}} = \tau^{3\cdot 2^{n-1}}$ is complex conjugation. Then

$$\sigma^i(\omega) = \sigma^{2^{n-1}}(\sigma^{i-2^{n-1}}(\omega)) = \overline{\sigma^{i-2^{n-1}}(\omega)},$$

and

$$\sigma^{2^n-1}(\omega) = \overline{\sigma^{2^{n-1}-1}(\omega)}$$

since

$$2^n - 1 - 2^{n-1} = 2^{n-1}(2-1) - 1 = 2^{n-1} - 1.$$

For x_1, this means that

$$x_1 = \omega + \sigma(\omega) + \cdots + \sigma^{2^{n-1}-1}(\omega) + \overline{\omega} + \overline{\sigma(\omega)} + \cdots + \overline{\sigma^{2^{n-1}-1}(\omega)}.$$

In the same way we see that x_2, and x_3 are also sums of complex conjugates, and hence real. Note that the x_i's in the construction of the heptagon and the tridecagon corresponds to the x_i's here.

These numbers are not rational, since $\tau(x_1) = x_2$ and $\tau^2(x_1) = x_3$. As be saw before $K_1 = \mathbb{Q}(\alpha)$ for any $\alpha \in K_1 \setminus \mathbb{Q}$. Especially, $K_1 = \mathbb{Q}(x_1)$. Let $m(x)$ be the minimal polynomial of x_1 over $\mathbb{Q}$. Then

$$m(x_2) = m(\tau(x_1)) = \tau(m(x_1)) = \tau(0) = 0$$

and

$$m(x_3) = m(\tau^2(x_1)) = \tau^2(m(x_1)) = \tau^2(0) = 0,$$

hence x_2, and x_3 are the other two zeroes of the polynomial $m(x)$. We can then describe $m(x)$ as

$$\begin{aligned}
m(x) =& \\
&= (x - x_1)(x - x_2)(x - x_3) \\
&= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3,
\end{aligned}$$

and we shall try to compute these coefficients. We have

$$x_1 + x_2 + x_3 = \sum_{i=1}^{p-1} \omega^i = -1,$$

so the coefficient for x^2 is 1.
Next, note that if ω^a is a term in x_1, so is $\omega^{-a} = \overline{\omega^a}$. The same holds for x_2 and x_3. We know that the sums x_1, x_2 and x_3 does not contain any common terms. Hence, when multiplying a term in x_i by a term in x_j we know that we are multiplying two numbers that are not each others inverses, when $i, j = 1, 2, 3$ and $i \neq j$. This means that the product $x_i x_j$ is a sum of powers of ω not equal to 1, no term is ever multiplied by its inverse. Hence

$$x_1x_2 + x_1x_3 + x_2x_3 = g(\omega)$$

where $g(x)$ is a polynomial with positive integer coefficients and no constant term. Since all powers of omega can be reduced so that the exponent is less than p we can say that $g(x)$ has degree at most $p-1$. Also, we know that $x_1x_2 + x_1x_3 + x_2x_3$ is rational, so $g(w) = r$ for some rational number r. Now put $h(x) = g(x) - r$. Then $h(\omega) = 0$, and $h(x)$ must be divisible by the minimal polynomial

$$f(x) = \sum_{i=0}^{p-1} x^i$$

of ω. But $h(x)$ is also of degree at most $p-1$, and since $h(x)$ is not constant we must have $h(x) = c \cdot f(x)$, for some rational number c. In fact, c must be equal to the constant term in $h(x)$, which is $-r$, so we have $h(x) = -r \cdot f(x)$. Since the leading coefficient in $h(x)$ is a positive integer, r must be a negative integer. Moreover, each power of ω must occur the same number of times, and this number is $-r$.
When expanding $x_1x_2 + x_1x_3 + x_2x_3$ we get $3 \cdot 2^{2n}$ terms, since each x_i has 2^n terms. On the other hand, the above expression there is $r \cdot 3 \cdot 2^n$ terms. Hence $r = 2^n$, and

$$x_1x_2 + x_1x_3 + x_2x_3 = 2^n.$$

Let now $x_1x_2x_3 = s$, for some rational number s. With the same argument as above we get that

$$x_1x_2x_3 = q(\omega)$$

where $q(x)$ is a polynomial such that $q(x) - s = a \cdot f(x)$ for some integer a. The problem is that, in this case we can not say anything about the constant term in $q(x)$. All we know is that when expanding $x_1x_2x_3$ we get a sum of powers of ω and 1's. From $q(x) - s = a \cdot f(x)$ we see that

$$q(\omega) = a \cdot f(\omega) + s = a \sum_{i=1}^{p-1} \omega^i + a + s,$$

and $a + s$ must be the number of 1's. We also know that the number of terms in the expansion of $x_1x_2x_3$ is 2^{3n}, and we can use this to approximate a. Obviously, a must be at least 1. If $a = 2^{2n-1}$ the number of omegas in the sum is

$$2^{2n-1}(p-1) = 2^{2n-1} \cdot 3 \cdot 2^n = 2^{3n-1} \cdot 3 > 2^{3n}.$$

Since the number of terms is 2^{3n}, this is a contradiction, and we deduce that $a < 2^{2n-1}$.

Note that the number of 1's in the expansion of $x_1x_2x_3$ must be $2^{3n} - a \cdot (p-1)$. But the number of 1's is also given by $a + s$, so we have

$$a + s = 2^{3n} - a \cdot (p-1),$$

and hence

$$s = 2^{3n} - a \cdot (p-1) - a = 2^{3n} - a \cdot p.$$

The polynomial $m(x)$ can now be expressed as

$$x^3 + x^2 - 2^n x - 2^{3n} + a \cdot p \quad \text{where } a \in \mathbb{Z} \text{ and } 1 \leq a < 2^{2n-1},$$

and K_1 is the splitting field of this polynomial.

We compare this with the polynomials we got for the heptagon and tridecagon. When $p = 7$ and $n = 1$ we get the polynomial

$$x^3 + x^2 - 2x - 8 + 7a, \quad \text{where } 1 \leq a < 2.$$

The only possibility is $a = 1$, and hence the polynomial is $x^3 + x^2 - 2x - 1$, which is consistent with the result from section 4.2.1.
When $p = 13$ and $n = 2$ we get the polynomial

$$x^3 + x^2 - 4x - 64 + 13a, \quad \text{where } 1 \leq a < 8.$$

From section 4.2.2 we know that the polynomial should be $x^3 + x^2 - 4x + 1$, and hence $a = 5$ in this case.

4.2.5 The regular 2^n3^m+1-gon

We shall now generalize Theorem 10 to the case when p is a Pierpont prime.

Theorem 11. *The regular p-gon, where p is a Pierpont prime, is constructible.*

Proof. Let p be a Pierpont prime, say $p = 2^n3^m + 1$. We let $\omega = e^{i\frac{2\pi}{p}}$, and define the Galois group $\Gamma = \langle\tau\rangle$ as before. The chain of subgroups now looks like

$$\langle\tau\rangle \supset \langle\tau^3\rangle \supset \langle\tau^{3^2}\rangle \supset \ldots \langle\tau^{3^m}\rangle \supset \langle\tau^{3^m\cdot 2}\rangle \supset \cdots \supset \langle\tau^{3^m\cdot 2^{n-1}}\rangle$$

and we have a corresponding tower of field extensions

$$\mathbb{Q} \underset{3}{\subset} K_1 \underset{3}{\subset} \ldots \underset{3}{\subset} K_m \underset{2}{\subset} \ldots \underset{2}{\subset} K_{m+n-1} \underset{2}{\subset} \mathbb{Q}(\omega).$$

The fact that $\tau^{\frac{p-1}{2}}$ is complex conjugation still holds, so all the fields, except $\mathbb{Q}(\omega)$ consists of real numbers.
In the case when $p = 3 \cdot 2^n + 1$ we showed that K_1 was the splitting field of an irreducible cubic polynomial over the rationals, and this holds here as well. The same holds for $K_{i+1} \underset{3}{\supset} K_i$, if we can show that the extension is normal. We know that all the K_i's are normal over $\mathbb{Q}$, since the corresponding groups are normal in Γ (since Γ is Abelian).

In general, assume that we have fields $K \subset F \subset E$, such that E is normal over K. We want to show that E is normal over F.

Let $a \in E \setminus F$, and let $m(x)$ be the minimal polynomial of a over F. Let $p(x)$ be the minimal polynomial of a over K. Then $m(x)$ must divide $p(x)$, say

$$p(x) = f(x)m(x),$$

for some polynomial $f(x)$. Assume that b is another zero of $m(x)$. We want to show that $b \in E$. We have

$$p(b) = f(b)m(b) = 0,$$

and since E is normal over K we must have $b \in E$.

From this we can conclude that K_{i+1} is normal over K_i, for all $i = 1, 2, \ldots, m-1$. Then all the extensions of degree 3 can be constructed by ruler, compass and angle trisection. The other extensions are of degree 2, and can be constructed by ruler and compass. Thus we have showed that the regular p-gon is constructible when p is a Pierpont prime. □

As in section 4.1, this now implies the following theorem.

Theorem 12. *The regular n-gon is constructible by ruler, compass, and angle trisector if and only if*

$$n = 2^k 3^l p_1 \cdots p_m$$

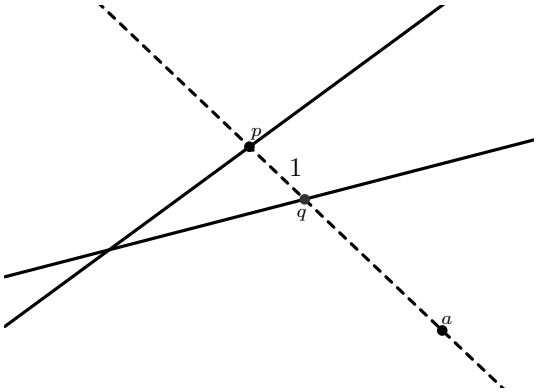
where $p_1, \ldots, p_m$ are distinct Pierpont primes.

The number of Pierpont primes is unknown, but the general conjecture is that there are infinitely many.

5 Marked ruler constructions

Instead of constructions using ruler, compass, and angle trisector we shall now consider constructions using only one tool, namely a marked ruler. A marked ruler is a ruler with two marks on it, one unit apart. This may seem like a restriction compared to our previous set of tools, but we will see that this in fact allows us to construct more points than before.

As before, a point is considered constructible if it is the intersection between two lines. Of course, the marked ruler may be used as the unmarked ruler, to draw lines between two given points. But we may also draw a line that goes through a given point a, and intersects two other lines at points p and q (not yet constructed) exactly one unit apart.

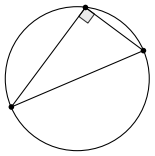


We allow the special case when a and q coincide. Then, obviously, q is already constructed and we are constructing p. Say now that we choose a as the origin. Any point that lies on a line and is at distance one from the origin is constructible in this way. This is the same as allowing to draw the unit circle. The following famous theorem implies that we can construct any point constructible by ruler and compass.

Theorem 13 (Poncelet-Steiner)**.** *Any point constructible by ruler and compass can be constructed by the ruler alone, given one circle and its center.*

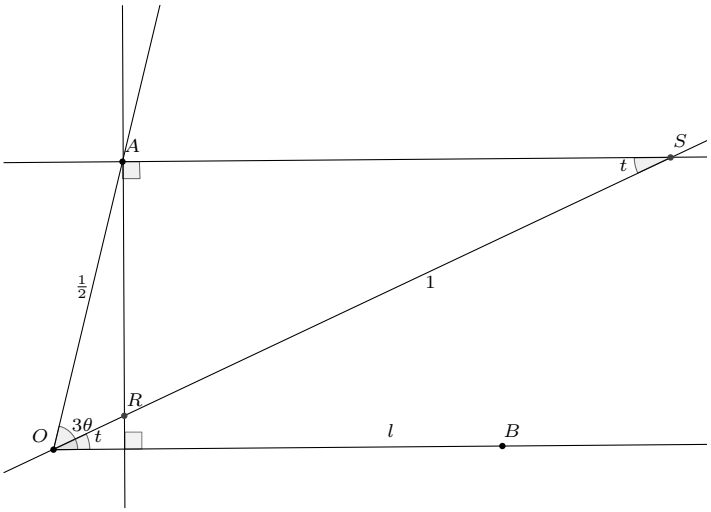
Next we shall see that the marked ruler can trisect angles. In this construction we will use the Converse theorem of Thales.

Theorem 14 (Converse Theorem of Thales)**.**

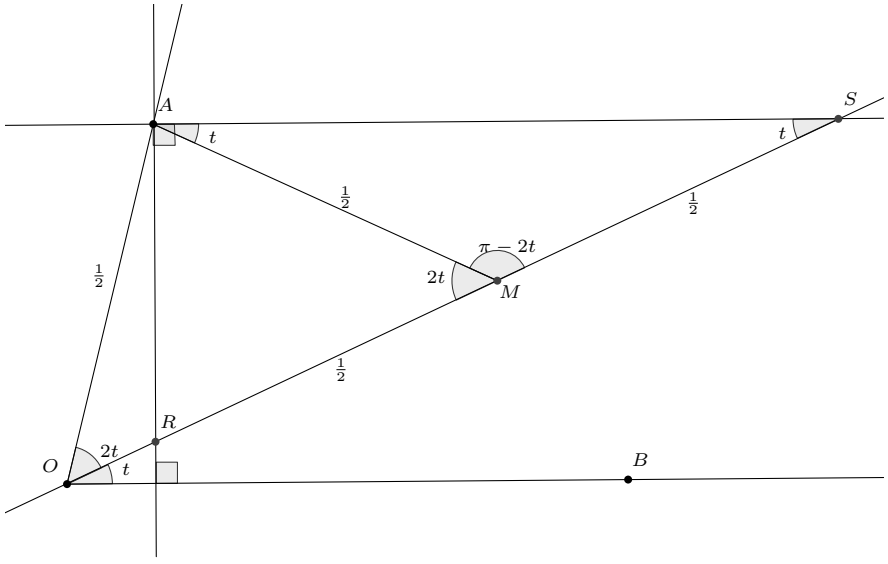


Any right triangle has its corners on a circle, where the hypotenuse of the triangle is the diameter of the circle.

Assume we are given points A, O, and B that form an acute angle 3θ. Without loss of generality we can assume that the distance between A and O is $\frac{1}{2}$. If A were at some other distance from O we could use our marked ruler to construct a point at distance $\frac{1}{2}$ from O, on the line between A and O. Let l denote the line between O and B. Draw two lines through A, one orthogonal to l, and one parallel to l. With the marked ruler we now draw a line that goes through O and intersects these two lines at points R and S, one unit apart.
The points B, O, and R form an angle t. We shall prove that $t = \theta$. Note that the angle at S, given by the points R and A, forms the same angle, t.



Now mark the point that lies midways between R and S, and call it M. Note that the points R, A, and S form a right triangle. By the Converse Theorem of Thales these points lie on a circle with center M and radius $\frac{1}{2}$. Hence the distance between A and M is $\frac{1}{2}$.
Now consider the triangle with corners in A, M and S. This triangle is isosceles. Hence the angle at the corner A, in this triangle, is the same as the angle at the corner S, which is t. The angle at the corner M is then $\pi - 2t$. Then the angle at M given by the points A and O is $2t$. The triangle with corners in A, M, and O is also isosceles. As the angle at the point M, in this triangle, is $2t$, the angle at the corner O is also $2t$.

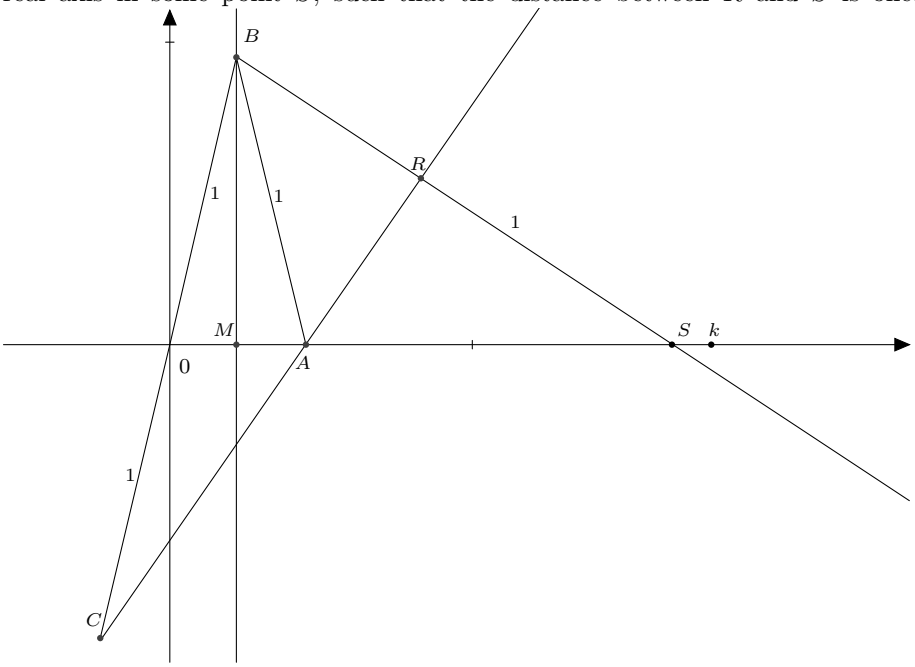


Now we see that $2t + t = 3t = 3\theta$, and hence $t = \theta$, and we have trisected the angle 3θ.

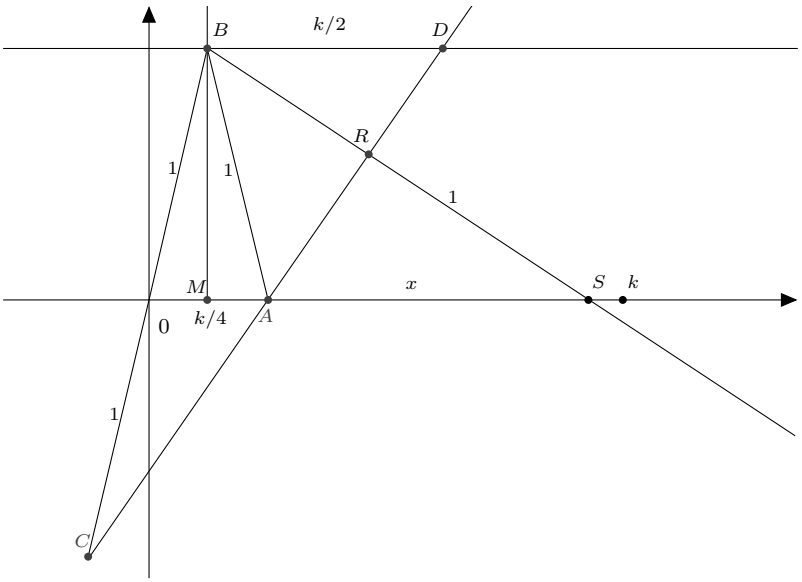
For obtuse angles we can first bisect the angle (which is possible with ruler and compass, and hence with marked ruler), one or two times, into acute angles.

Then we trisect these angles separately. To get the trisection of the original angle we need to add angles, which we have seen can be done with ruler and compass.

We have now seen that with the marked ruler we can do the same constructions as with ruler, compass, and angle trisector. As promised, we shall now see that we can do even more.
Let k be a real number, such that $0 < k < 8$. We shall construct the real number $\sqrt[3]{k}$.
Start with marking the point A at $\frac{k}{4}$. Call the point midways between A and the origin (at $\frac{k}{8}$, that is) M, and draw a vertical line through this point. Then we use the marked ruler to find a point B on this line, with the distance one from A and the origin. Note that this would be impossible for $k > 8$, because then the distance between A and M is greater than one. In the case $k = 8$ the points B and M coincide, which would also fail our construction, so this explains the upper bound for k. Extend the line through B and the origin to a point C at the distance one from the origin, in the other direction. Next, draw a line through C and A. We use the marked ruler to draw a line through B that intersects this line in some point R, and the real axis in some point S, such that the distance between R and S is one.



Let x be the distance between A and S. We shall now prove that $x = \sqrt[3]{k}$.
Draw a line through B parallel to the real axis. This intersects the line through A and C at some point D.
Now note that the triangle with corners in A, C, and the origin is similar to the triangle with corners in D, C and B. The side of the smaller triangle is half the side of the bigger one. Since the distance between A and the origin is $\frac{k}{4}$, the distance between B and D is $\frac{k}{2}$.



The triangle with corners in B, D, and R is similar to the triangle with corners in A, S, and R. This gives us the equality

$$x = \frac{x}{1} = \frac{k/2}{BR},$$

where BR denotes the distance from B to R. We rewrite this as

$$BR = \frac{k}{2x}.$$

Then

$$BS = BR + 1 = \frac{k}{2x} + 1.$$

Now consider the right triangle with corners in B, M, and S. Pythagoras gives

$$BS^2 = BM^2 + MS^2,$$

and hence

$$\left(\frac{k}{2x} + 1\right)^2 = BM^2 + \left(x + \frac{k}{8}\right)^2.$$

Since B, M, and A also are the corners of a right triangle we can calculate the length of the side BM by

$$BM^2 = 1 - \left(\frac{k}{8}\right)^2.$$

If we put this into the above expression we get the equation

$$\left(\frac{k}{2x} + 1\right)^2 = 1 - \left(\frac{k}{8}\right)^2 + \left(x + \frac{k}{8}\right)^2.$$

This factorizes to

$$(4x + k)(x^3 - k) = 0,$$

which has the only real positive solution $x = \sqrt[3]{k}$.

This was only for real k in the range $0 < k < 8$, but it easily extends to any complex number. Assume that $k \geq 8$. Then we can choose some sufficiently large n, such that $\frac{k}{8^n} < 8$. Since 2^n is constructible, the number

$$\sqrt[3]{k} = \sqrt[3]{\frac{k}{8^n}} \cdot 2^n$$

is also constructible. This is, with the marked ruler we can construct the cube root of positive real numbers. Since we can trisect angles the cube root $\sqrt[3]{r}e^{i\frac{\theta}{3}}$ of a complex number $re^{i\theta}$, is also constructible.
Especially the number $\sqrt[3]{2}$ is constructible. Hence the marked ruler does not only trisect angles, but also solves another of the impossible constructions, namely duplicating the cube.
In fact, this means that we can solve any cubic polynomial equation. By Cardano's formula, the roots to the equation

$$x^3 + px + q = 0$$

is given by

$$u + v, \quad \omega u + \omega^2 v, \text{ and } \omega^2 u + \omega v,$$

where

$$u = \sqrt[3]{-\frac{p}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$
$$v = \sqrt[3]{-\frac{p}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

and ω is the number $e^{i\frac{2pi}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, a primitive third root of unity. Since we can construct cube roots, these numbers are constructible.

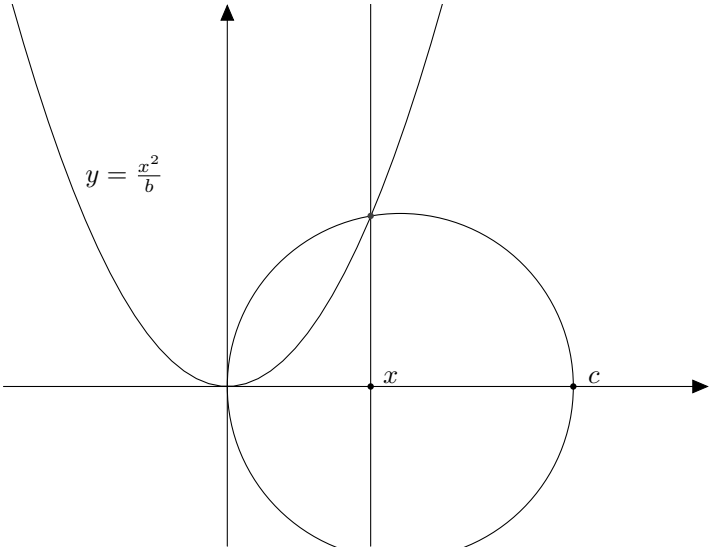
6 Solving cubic equations using a parabola

We have now seen that the angle trisector can solve cubic equations with real roots, and that the marked ruler solve any cubic equation. We shall now consider a third way of solving cubic equations geometrically.

In the 12's century the Persian mathematician Omar Khayyam solved cubic equations $x^3 + Ax = B$ where A and B are positive numbers, geometrically using ruler, compass, and a parabola. Khayyam wrote the equation of the form

$$x^3 + b^2 x = b^2 c$$

and used the parabola $y = \frac{x^2}{b}$. To solve the equation we draw the parabola, and the circle with center at $\frac{c}{2}$ that goes through the origin. The solution is the intersection of the parabola and the circle, projected on the real axis.



To prove that this is actually a solution to the equation $x^3 + b^2x = b^2c$, we consider the equation of the circle, which is given by

$$\left(x - \frac{c}{2}\right)^2 + y^2 = \left(\frac{c}{2}\right)^2.$$

Since we shall intersect this circle with the parabola $y = \frac{x^2}{b}$ we insert this into the equation of the circle, and get

$$\left(x - \frac{c}{2}\right)^2 + \frac{x^4}{b^2} = \left(\frac{c}{2}\right)^2.$$

Simplifying this we get

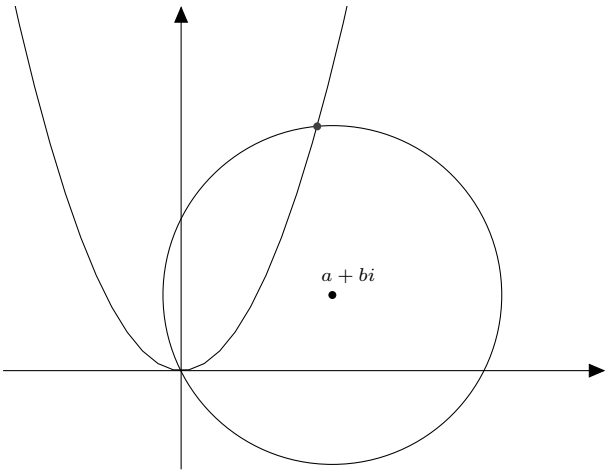
$$\frac{x^4}{b^2} + x^2 = cx.$$

Obviously $x = 0$ is a solution. But we are interested in the other one, i.e. the solution to

$$\frac{x^3}{b^2} + x = c.$$

If we multiply b^2 we get the exact equation we wanted to solve. Hence the real part (or x-coordinate) of the intersection of the circle and the parabola is a solution to the equation $x^3 + b^2x = b^2c$.

We shall now try to generalize Khayyam's method. Instead of using the parabola $y = \frac{x^2}{b}$ which depends on the equation we want to solve, we shall consider the fixed parabola $y = x^2$. We shall also allow the center of the circle to be some point $a + bi$, not necessarily a positive real number.



Such a circle has the equation

$$(x-a)^2 + (y-b)^2 = a^2 + b^2.$$

Replacing y by x^2 and simplifying the expression gives

$$x^4 + (1-2b)x^2 - 2ax = 0.$$

Hence real solutions to this equation are real parts of the intersections of the parabola and the circle. As before, $x = 0$ is a solution, but we are interested in the other ones. Therefore we consider the equation

$$x^3 + (1-2b)x - 2a = 0.$$

Say now that we have some equation $x^3 + px + q = 0$ with real coefficients that we want to solve. We put

$$\begin{cases} a = -\frac{q}{2} \\ b = \frac{1-p}{2} \end{cases}$$

This gives precisely the equation $x^3 + (1-2b)x - 2a = 0$, and we can solve it geometrically by intersecting the parabola $y = x^2$, and the circle with center in $a+bi$ that goes through the origin. Note that this works for any cubic equation, when written on the form without quadratic term. As we know, cubic equation can have one or three real roots. When the equation has three real roots, this method gives all the roots right away. If the equation has one real α roots and two complex roots the intersection with the parabola only gives the real root, but the complex roots are not that hard to find. Say the complex roots are c and $\overline{c}$. Then we have

$$(x-\alpha)(x-c)(x-\overline{c}) = x^3 + px + q.$$

Hence

$$q = -ac\overline{c} = -a|c|^2,$$

and

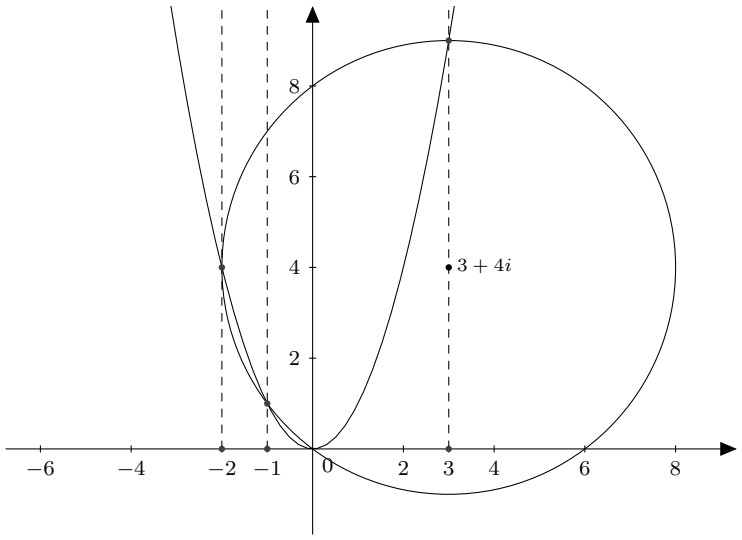
$$0 = a + c + \overline{c} = a + 2\,\mathrm{Re}(c).$$

From this we see that the absolute value, and the real part of the complex roots are constructible. From this the numbers c and $\overline{c}$ themselves can also be constructed.

As an example we consider the equation $x^3 - 7x - 6 = 0$. This equation has three real roots, namely -1, -2, and 3, and is not solvable by Khayyam's original method. We calculate

$$a = \frac{6}{2} = 3, \quad \text{and } b = \frac{1+7}{2} = 4,$$

and draw the circle with center at $3 + 4i$ that goes through the origin, together with the parabola.



We see that this gives us all the three solutions.

With the angle trisector we could solve any cubic equation with three real roots. Using the parabola we can solve any cubic equation with real coefficients. Hence both the parabola, in addition to the ruler and compass, and the marked ruler alone contributes more than to allow angle trisection.

References

[1] John A. Beachy, William D. Blair *Abstract Algebra*. Waveland press, inc., Third edition, 2006.

[2] Rene Descartes, English translation by D. Eugene Smith and M. Latham, *The Geometry*. Dover Publications, 1954.

[3] Andrew M. Gleason, *Angle Trisection, the Heptagon, and the Triskaidecagon*. The American Mathematical Monthly, Vol. 95. No. 3, Mathematical Association of America, 1988.

[4] Morris Kline, *Mathematical Thought from Ancient to Modern Times*. Oxford University press, 1972.

[5] George E. Martin, *Geometric Constructions*. Springer, First Edition, 1998.

[6] Ian Stewart, *Galois Theory*. Chapman & Hall / crc, Third Edition, 2004.