Constructions with ruler and compass

An application of algebra to geometry

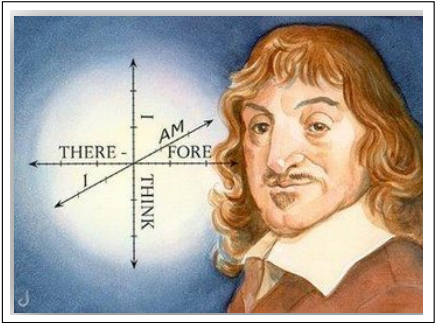
K. N. Raghavan
http://www.imsc.res.in/~knr/

IMSc, Chennai

July 2013

Coordinate geometry following Descartes

Well known is the revolutionary idea of translating problems of geometry to algebra by means of the use of co-ordinates: we are all familiar with such terms as *Cartesian plane* and *Cartesian co-ordinates* in honour of René Descartes (1596–1650), to whom this idea is attributed.



The manipulative power of algebra can thus be brought to bear upon geometry. And, conversely, algebraic equations can be interpreted as representing geometric shapes—the loci of their solutions—whose properties reflect those of the equations.

What is this talk about?

Not so well known is another equally revolutionary instance of the introduction of algebra into geometry, due to Carl Friedrich Gauss (1777–1855), dating from circa 1795, which lead to spectacular solutions of certain long standing problems of geometry:

- Can regular polygons be constructed?
- Can angles be trisected?

and which illuminated certain other long standing problems:

- Can the circle be squared?

thereby contributing to their eventual solution.

Always using only ruler and compass.

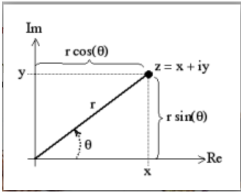
This lecture is about this second instance of the application of algebra to geometry.

GAUSS'S BASIC IDEA

- Descartes: represent points in the plane by ordered pairs (x, y) of real numbers
- Gauss: represent points in the plane by complex numbers:

$$\boxed{(x,y) \leftrightarrow x+iy}$$

where $i^2 = -1$



Thus points in the plane that are *constructible* (in the sense to be presently defined) can be considered as a subset of the complex numbers. And, as such, we can add, subtract, multiply, divide, extract roots, and generally perform algebraic operations on them.

Gauss's basic idea (continued)

We are thus lead to ask:

Can the subset of constructible numbers be characterized algebraically?

When Gauss posed and answered this, half the battle was won (towards the solution of those long standing problems of geometry).

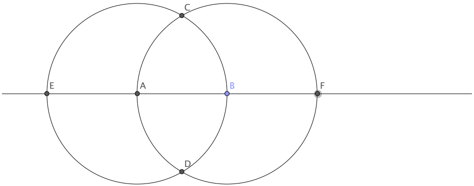
Formulation of the problem

We are given two tools (a ruler and a compass) and two initial points:

- Ruler (or straight-edge): using which we can draw the straight line through two given points in the plane.
- Compass: using which, given two points on the plane, we can draw the circle with centre one of them and passing through the other.
- Initial data: We are given two distict points on the plane, which we may assume to be those with co-ordinates $(0, 0)$ and $(1, 0)$, or, equivalently, those corresponding to the complex numbers 0 and 1.

Drawing lines and circles, generating more points

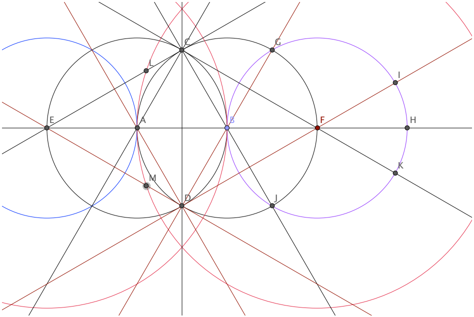
To begin with, we can draw, using the ruler, the line through the two given points, the x-axis. We can draw two circles, one with centre the origin and passing through $(1, 0)$, the other with centre $(1, 0)$ and passing through the origin.



We get points other than A and B: the intersections of the circles (C and D), and the intersections of the line with each of the circles (E and F).

More lines, circles, and points

Using these extra points we can now draw more lines and circles:



We obtain more points as intersections: $G, H, I, J, K, L, M, \ldots$ as in the picture above.

Constructible points and other objects

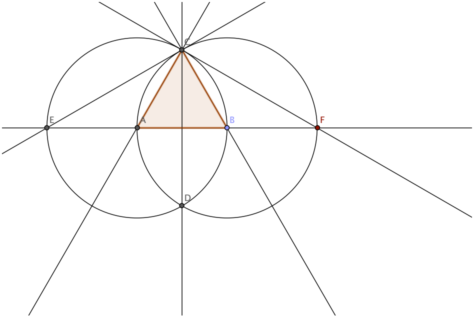
All points so obtained as intersections are called *constructible*: the original two points are by definition *constructible*. It is also convenient to apply the term *constructible* to the lines and circles that we can draw by this process. We will extend the term further to other objects as well: a triangle is *constructible* if all its vertices are, in other words, if its sides are constructible lines; an angle is *constructible* if it is the angle between two constructible lines, etc.

We can now pose the big questions:

> *Which points of the plane are constructible? Which regular polygons are constructible? More precisely, for which integers n can we find constructible points $p_1, \ldots, p_n$ such that they form the vertices of a regular polygon?*

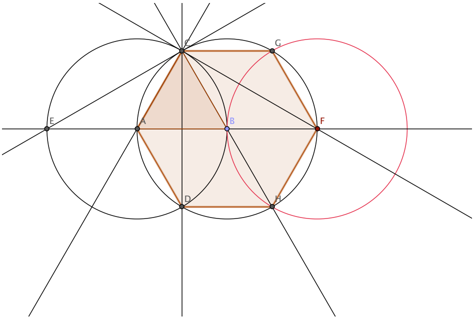
Which regular n-gons are constructible?

The equilateral triange is constructible:



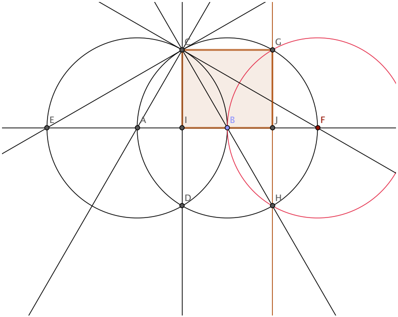
Which regular n-gons are constructible?

The regular hexagon is constructible:



WHICH REGULAR n-GONS ARE CONSTRUCTIBLE?

The square is constructible:



WHICH REGULAR n-GONS ARE CONSTRUCTIBLE?

What about the regular pentagon, heptagon, etc.? Are they constructible?

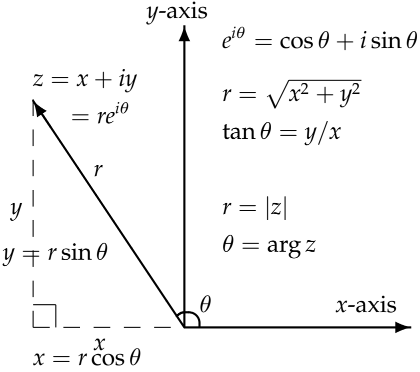
It was known since antiquity that the regular pentagon is constructible. Later in this talk, we will give a construction. But it was not known at the time of Gauss whether even the regular heptagon was constructible or not. We will shortly state precisely what the state of the art was before Gauss.

Gauss answered the question completely. His answer was not only comprehensive, it was also surprisingly simple and stunningly elegant.

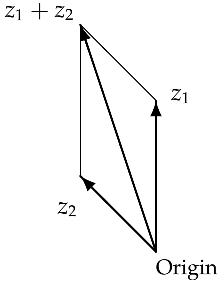
Our goal is to state his theorem and to understand the basic idea of his proof.

Preliminary: geometric representation of complex numbers

Rectangular and polar co-ordinates



Addition of complex numbers



Multiplication of complex numbers

$$z_1 z_2 = r_1 e^{i\theta_1} r_2 e^{i\theta_2} = r_1 r_2 e^{i(\theta_1 + \theta_2)}$$

i.e., moduli multiply, arguments add

Problem translated into algebra

The question of constructibility of regular polygons is clearly of a geometric nature. Gauss translated it into algebra by

- first extending the notion of constructibility to numbers—a complex number is *constructible* if and only if its corresponding point on the Cartesian plane is constructible in the sense just defined.
- then observing that the regular n-gon is constructible if and only if the complex number $e^{2\pi i/n}$ is constructible.

It is clear that if the number is constructible then so is the regular polygon. The converse requires a bit of routine work—we have to show that if we find a regular n-gon somewhere (with vertices being constructible points),then we can actually construct THE regular n-gon with centre the origin and $(1, 0)$ a vertex—this will become clear presently.

Preliminary: Basic constructions with ruler and compass

Let p and q be two distinct constructible points. We can construct:

- ✓ The line ℓ through p and q
- ✓ The perpendicular to ℓ at p (or q)

Let r be a constructible point not on ℓ. We can construct

- ✓ The perpendicular to ℓ through r
- ✓ The parallel to ℓ through r
- ✓ The parallelogram of which pq and pr are the two sides

Given a constructible point s at a distance d from r, we can construct

- ✓ The circle with centre p and radius d (that is, we can "transfer distances")

Preliminary: Basic constructions with ruler and compass (continued)

Let ℓ and ℓ' be two constructible lines that meet. We can construct

- ✓ the line that bisects the angle between ℓ and ℓ'

(We have at least two constructible points each on ℓ and ℓ'.)

We can also transfer angles. That is, given another constructible line ℓ'' and a constructible point u on ℓ'' we con construct

- ✓ The line through u that is at the same angle to ℓ'' as ℓ' is to ℓ.

In particular, the sum of two constructible angles is constructible.

Corollary

A complex number $z = x + iy = re^{i\theta}$ is constructible if and only if both x and y are constructible; also if and only if both r and θ are constructible.

The first crucial observation

A subset of the complex numbers is said to be a *field* if it contains the elements 0 and 1, and is closed under the operations of addition, subtraction, multiplication, and division by non-zero elements.

Proposition (Gauss)

The constructible numbers form a field closed under taking square roots.

Proof: That the constructible numbers form a field follows from the basic constructions that we have just made. For the second part of the assertion, note that the square roots of $z = re^{i\theta}$ are $z = \pm\sqrt{r} \cdot e^{i\theta/2}$. Since we can bisect angles, we need only show that $\sqrt{r}$ is constructible. We know that r is constructible.

Proof that $\sqrt{r}$ is constructible if r is

ABC is a straight line with |AB|=r and |BC|=1

D is the Midpoint of A and C

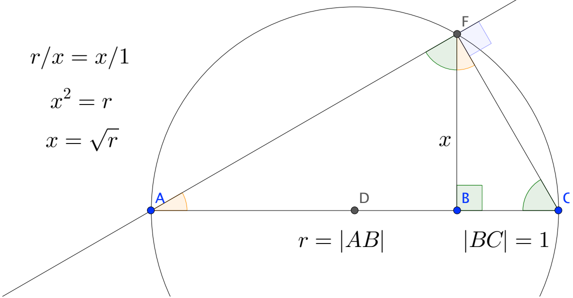
Circle has centre D and passes through A and C

F is the intersection of the circle and the perpendicular at B to ABC

$$r/x = x/1$$

$$x^2 = r$$

$$x = \sqrt{r}$$



CONSTRUCTIBILITY OF THE PENTAGON

Corollary

If a, b, and c are constructible, then so are the roots of the quadratic equation

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

Proof: The well known formula for the roots involves only the field operations (addition, subtraction, multiplication, and division) and extracting square roots.

Corollary

The regular pentagon is constructible.

Proof: Put $\zeta = e^{2\pi i/5}$. Consider $\alpha = \zeta + \zeta^4$ and $\beta = \zeta^2 + \zeta^3$. Their sum and product are both -1:

$$\alpha + \beta = \alpha\beta = -1$$

Thus they are roots of the quadratic equation $(x - \alpha)(x - \beta) = x^2 + x - 1 = 0$, and so constructible.

Now observe that $(x - \zeta)(x - \zeta^4) = x^2 - \alpha x + 1 = 0$ has constructible coefficients, and so constructible roots. $\square$

THE STATE OF THE ART AT GAUSS'S TIME

The equilateral triangle is easily constructed. We have just now seen that the regular pentagon is constructible, a fact which was known to the ancients.

- Since angles can be bisected, if the regular n-gon is constructible, so is the regular $2n$-gon.
- Suppose that m and n are coprime, and that the regular m-gon and the regular n-gon are constructible, then the regular mn-gon is constructible. To see this, observe that there exist integers a and b such that

  $$am + bn = 1 \qquad \text{and so} \qquad a\frac{2\pi i}{n} + b\frac{2\pi i}{m} = \frac{2\pi i}{mn} \qquad (\text{multiply by } \frac{2\pi i}{mn})$$

  . Exponentiating both sides, we get

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

  Since $e^{2\pi i/m}$ and $e^{2\pi i/n}$ are constructible by hypothesis, so is the right hand side. $\square$

The state of the art at Gauss's time (Continued)

Putting all this together, we see that the regular n-gon is constructible if n has any of the following forms:

$$2^m \qquad 2^m \cdot 3 \qquad 2^m \cdot 5 \qquad 2^m \cdot 15$$

The numbers less than 100 of this form (excluding 1 and 2) are:

$$3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30, 32, 40, 48, 60, 64, 80, 96$$

Such was the state of knowledge at the time of Gauss. For any number n not in the list above, e.g., 7, 9, 11, 13, 14, 17, 18, 19, 21, 22, 23, 25, etc., it was *not* known whether the regular n-gon is constructible.

Gauss's theorem on constructibility of regular polygons

As a teenager, Gauss succeeded in constructing the regular 17-gon. In fact, he settled the problem of constructibility of regular polygons for good:

Theorem (Gauss)

The regular n-gon is constructible if and only if the factorization of n into primes has the following form

$$n = 2^r \cdot p_1 \cdot \ldots \cdot p_k$$

where r is a non-negative integer, and $p_1, \ldots, p_k$ are distinct odd primes such that $p_1 - 1, \ldots, p_k - 1$ are all powers of 2.

In the above, k could be 0, in which case n is a power of 2.

Here is the full list of numbers up to 100 for which the regular n-gon is constructible: 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96.

Corollary

Since the 18-gon is not constructible, neither is the 20° angle, which means that the 60° angle cannot be trisected. In particular, angles in general cannot be trisected.

TOWARDS THE PROOF: A COMPLEMENT TO THE FIRST OBSERVATION

We have seen that the constructible numbers form a field closed under taking square roots. In fact,

Theorem (Gauss)

The constructible numbers constitute the smallest subfied of the complex numbers that is closed under taking square roots.

A unique smallest such subfields exists: it is just the interesection of all such subfields.

Proof: The proof is surprisingly simple. Let us denote by C the subfield of constructible numbers and by F the smallest subfield closed under taking square roots. Since F is contained in every subfield closed under taking square roots, clearly $F \subseteq C$.

To show that $C \subseteq F$, we divide C into layers. The zeroth layer consists just of the original two points 0 and 1. This layer is contained in F by definition (of a subfield).

The proof of the theorem continued: the induction step

At every stage, the next layer consists of those obtained as intersections of lines and circles constructed from points of the previous layer. The points of the previous layer have constructible co-ordinates by induction. Therefore the equations of the lines and circles have constructible coefficients.

To get the co-ordinates of the points of the next layer, we do algebraic operations on these equations, and solve the resulting linear or quadratic equations. Since these equations have constructible coefficients, the roots are also constructible. This means the points in the next layer are constructible. $\square$

END OF THE PROOF

Recall that the constructibility of the regular n-gon is equivalent to the constructibility of the number $\zeta = e^{2\pi i/n}$. The latter in turn is equivalent to the condition that ζ belongs to the smallest subfield F of the complex numbers that is closed under taking square roots.

Gauss observed further:

- The smallest subfield of the complex numbers containing ζ has dimension $\phi(n)$ over the rational field, where $\phi(n)$ is the number of positive integers less than or equal to n (including 1) that are coprime to n.
- If a subfield of F has finite dimension over the rational field, then that dimension is a power of 2.

Now it follows that the regular n-gon is constructible if and only if $\phi(n)$ is a power of 2. And it is an easy exercise to show that this last condition is equivalent to n having the form described in the theorem. $\square$

SUMMARY OF THE TALK

Following Gauss, we've answered the following:

- Which regular polygons are constructible? Answer: Those n-gons with $\phi(n)$ a power of 2.
- Can angles be trisected? Answer: No. E.g., the 60° angle cannot be trisected, for the 20° is not constructible (the 18-gon isn't constructible).
- Can the circle be squared? Answer: No. This will follow once we know π is "transcendental" (proved by Lindemann in the 1880s).
- Always using only ruler and compass.

Note on Fermat primes: Suppose that p is a prime with $\phi(p) = p - 1$ a power of 2. As can be easily seen, for $2^n + 1$ to be prime, it is necessary that n be a power of 2. Thus p is of the form $2^{2^k} + 1$. Such primes are called *Fermat primes*. Fermat conjectured that $2^{2^k} + 1$ is always a prime, but $2^{2^5} + 1$ is not prime—691 divides it—as noted by Euler.

It is not known whether the number of Fermat primes is infinite; in other words, whether there are infinitely many primes p such that the regular p-gon is constructible.