Modern Algebra Lecture Notes: Rings and fields set 10, revision 2

Kevin Broughan

University of Waikato, Hamilton, New Zealand

May 27, 2010

Geometric 2D constructions using a ruler and compass

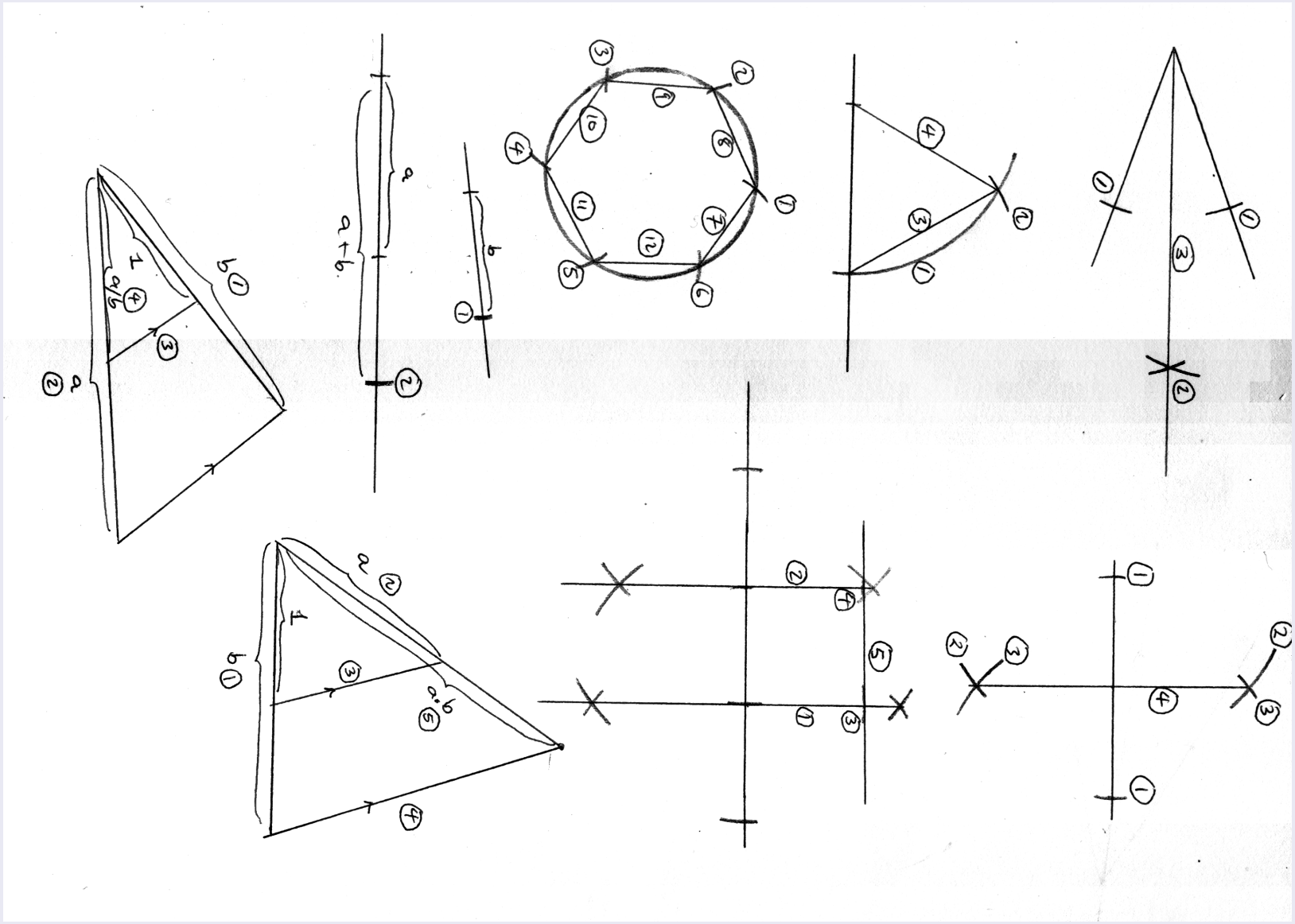
Definitions

The ruler or straight edge is unmarked and the compass of arbitrary size. Typically we have a line segment of length 1, and as much flat paper as required.

Classical tasks for construction

1. The bisector of an angle,
2. A line perpendicular to a given line through a given point on or off the line,
3. An equilateral triangle,
4. A square,
5. A regular hexagon.
6. A line segment of length $a + b$ when a and b have been constructed,
7. A line segment of length $a.b$,
8. A line segment of length a/b,
9. A line segment of any rational length,
10. A line segment of length $\sqrt{2}$.

Methods for the classical tasks



Classical Problems for construction left unsolved

1. A regular polygon with 7 sides,
2. The trisector of a given angle,
3. A square with the same area as a circle of radius 1,
4. The length of the side of a cube so that its volume is twice that of the unit cube,
5. Determining precisely which regular polygons can be constructed and which cannot.

Constructible numbers

Every rational number can be constructed, and so can the irrational $\sqrt{2}$, but what is the set of all numbers which can be constructed from 1 using just the ruler and compass?

Let $C \subset \mathbb{R}$ be the set of all constructible numbers. Then because $a, b \in C$ implies $a + b$, $a.b$ and a/b, when $b \neq 0$ are in C, then C is a subfield of $\mathbb{R}$ which contains $\mathbb{Q}$.

Recursive description of C

Suppose we have constructed some points from $\mathbb{Q}$ and have a set D and we want to use the ruler and compass to construct further points. Use the points in the plain with coordinates from D, drawing lines through two points from $D \times D$ and circles with centers in $D \times D$ and radii from D. Do we get more points assuming D is a field ?

Two lines crossing

Each line has an equation $ax + by + c = 0$ with $a, b, c \in D$. If two such lines cross then the solutions are in D since the solutions are rational functions of the two a, b, c's and D is a field, so we get **no** new points.

Generating new points

Two circles crossing

Each circle has an equation $(x-a)^2+(y-b)^2=r^2$ with $a, b, r \in D$. If two such circles cross then the solutions are on a line with coefficients in D since the quadratic terms vanish when the two equations are subtracted, so again we get **no** new points.

A line and a circle crossing

Let the equation of the line be $ax+by+c=0$ and that of the circle $x^2+y^2+dx+ey+f=0$ where $a, b, c, d, e, f \in D$. Substituting for y from the linear equation into the quadratic and solving for x we get, maybe, a new number of the form $\sqrt{\alpha}$, where $\alpha \in D$. In this manner we generate the field $D(\sqrt{\alpha})$.

Anatomy of a constructible number

If β is constructible starting with 1, we must be able to reach β in a finite number of steps. Hence, following the discussion given above, there must be a finite chain of extension fields $F_1 \subset F_2 \subset F_3 \subset \cdots \subset F_n$ where $F_1 = \mathbb{Q}(\sqrt{\alpha_1}),\ F_2 = F_1(\sqrt{\alpha_2}), \ldots, F_n = F_{n-1}(\sqrt{\alpha_n})$ so that for all i, $[F_{i+1} : F_i] = 1\ or 2$.

But $\beta \in F_n$ and, by the Dimension Theorem, $2^k = [F_n : \mathbb{Q}] = [F_n : \mathbb{Q}(\beta)][\mathbb{Q}(\beta) : \mathbb{Q}]$ for some natural number k. But this shows that $[\mathbb{Q}(\beta) : \mathbb{Q}]$ is a power of 2 also.

Key fact

It is this constrained nature of any field extension by a constructible number β which is typically used to show which entities can **not** be constructed.

Theorem 40: the cube cannot be doubled

Proof

The side of a cube with twice the volume of the unit cube must be $\beta = 2^{\frac{1}{3}}$. But β satisfies $f(x) = x^3 - 2$ which is irreducible over $\mathbb{Z}$ hence over $\mathbb{Q}$ by Eisenstein's method with $p = 2$.

Therefore, since it is monic, it is the minimal polynomial of β and has degree 3 so $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$ which is not a power of 2. Therefore β is not constructible and the cube cannot be doubled in volume in a constructible manner.$\square$

Similarly the cube cannot be tripled.

Theorem 41: an angle of $\pi/3 = 60^o$ cannot be trisected

Proof

Assume, to get a contradiction we can trisect an angle of 60^o and thus get an angle of 20^o and thus construct the value (using a right angled triangle) $\beta = \cos\frac{\pi}{9}$.

Now de Moivre's theorem gives $e^{3i\theta} = (\cos\theta + i\sin\theta)^3$ so expanding the LHS and equating the real parts gives

$$\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta = 4\cos^3\theta - 3\cos\theta.$$

Hence if $\theta = \pi/9$ we get $1/2 = 4\beta^3 - 3\beta$ or $8\beta^3 - 6\beta - 1 = 0$.

The corresponding polynomial $f(x) = 8x^3 - 6x - 1$ is irreducible over $\mathbb{Z}$: any root has to be a factor of -1 so all possible roots can easily be checked. Since it is a cubic, to be reducible it must have a root. Hence the minimum polynomial for β is $x^3 - (3/4)x - (1/8)$ which has degree 3.

Since the corresponding dimension is not a power of 2, the number β is not constructible, so an angle trisector cannot be constructed.$\square$

Squaring the circle

A transcendental example

This does not use the "power of two" criteria, but the deep fact that π is transcendental, i.e. is not an algebraic number.

Let $A = \pi \cdot 1^2 = \pi$ be the area of a circle of radius 1. If we could construct a length a such that a square with that side length had the same area as the circle than we could find a constructible number a such that $a^2 = \pi$, so $f(x) = x^2 - \pi$ would have a constructible root. Constructible numbers are algebraic and the set of all algebraic numbers is a field (Theorem 38), thus we would have π algebraic, but it is not. Hence we cannot square the circle.

Where can this go ?

Constructible polygons

Gauss proved that a regular polygon of n sides was constructible if and only if $n = 2^e p_1 \cdots p_m$ where each p_i was a distinct so called Fermat prime, a prime number of the form $2^{2^m} + 1$. He used cyclotomic polynomials, outside our scope: see the final chapter of Gallian.

Fermat primes

Fermat conjectured that all numbers of this form were prime. But only 5 are known: 3, 5,17, 257, 65537. So the new conjecture is that there are an infinite number of Fermat numbers which are **not** prime!

Equations of the fifth degree

Using the beginnings of Galois Theory, based on the field extension work we have covered, Abel showed that for general polynomial equations of the 5th or higher degree there are no expressions of an algebraic kind describing their roots. This uses group theory quite intensively, where the groups are the automorphism groups of the fields.

The Class Group

When the coefficients of a minimal polynomial for an element algebraic over $\mathbb{Q}$ are integers, we say the element is an algebraic integer, and the set of all such elements is a ring. This ring has ideals and we broaden their class to include "fractional ideals". For example all integer multiples of $(1/3)$ in a type of $\mathbb{Z}$ ideal. We then say two of these ideals A, B are equivalent if there is a principal ideal $\langle\alpha\rangle$ with $A = B\langle\alpha\rangle$. These classes are a group which is finite, called the ideal class group with size $h(\mathbb{K})$ if $\mathbb{K}$ is the given extension of $\mathbb{Q}$. If $h(\mathbb{K}) = 1$ all of the ideals must be principal, so we have a PID and unique factorization in the ring of algebraic integers.

Dangerous curve!

One might suspect that the ring of integers of $\mathbb{Q}(\sqrt{m})$ is always the ring $\mathbb{Z} + \sqrt{m}\mathbb{Z}$ and this is true when $m \not\equiv 1 \bmod 4$, for example $m = -5, -2, -1, 2, 3, 6, 7...$ If $m \equiv 1 \bmod 4$ (e.g. $m = -7, -3, 5$ being some of the examples we have used before on divisibility) then the ring is $\mathbb{Z} + \left(\frac{1+\sqrt{m}}{2}\right)\mathbb{Z}$.

Class number 1 problem

For the imaginary quadratic extensions $\mathbb{Q}(\sqrt{-m}),\ m = 1, 2, ..$ there are only a finite number of values for $-m$ with class number 1, and hence unique factorization:

$$-m = -1,\ -2,\ -3,\ -7,\ -11,\ -19,\ -43,\ -67,\ -163.$$

There are many more with class number 1 for the real extensions $\mathbb{K} = \mathbb{Q}(\sqrt{m}),\ m = 2, 3, 5, ..,$ but proving there are an infinite number is a long outstanding problem, originally stated by Gauss. For example $h(\mathbb{K}) = 1$ for $m = 2, 3, 5, 6, 7$ and $m = 10$ gives the first with $h(\mathbb{K}) = 2$.

Dangerous curve!

One might suspect that the ring of integers of $\mathbb{Q}(\sqrt{m})$ is always the ring $\mathbb{Z} + \sqrt{m}\mathbb{Z}$ and this is true when $m \not\equiv 1 \bmod 4$, for example $m = -5, -2, -1, 2, 3, 6, 7...$ If $m \equiv 1 \bmod 4$ (e.g. $m = -7, -3, 5$ being some of the examples we have used before on divisibility) then the ring is $\mathbb{Z} + \left(\frac{1+\sqrt{m}}{2}\right)\mathbb{Z}$.

Example

So, $\mathbb{Z}[\sqrt{-3}]$ does not have unique factorization, $2.2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, but $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ does! The further development and application of these ideas in the field Algebraic Number Theory.