Fields and Galois Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Ruler and Compasses Constructions

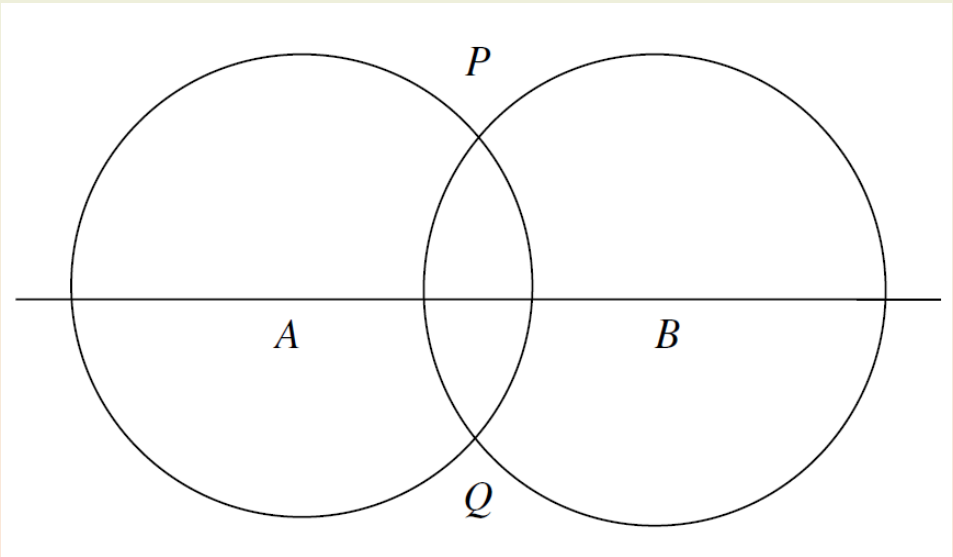
Perpendicular Bisector of a Line Segment

- Let A, B be distinct points on the plane. Construct the perpendicular bisector of AB.

  Draw a circle with center A passing through B.

  Draw a circle with center B passing through A.

  The two circles meet in points P and Q.

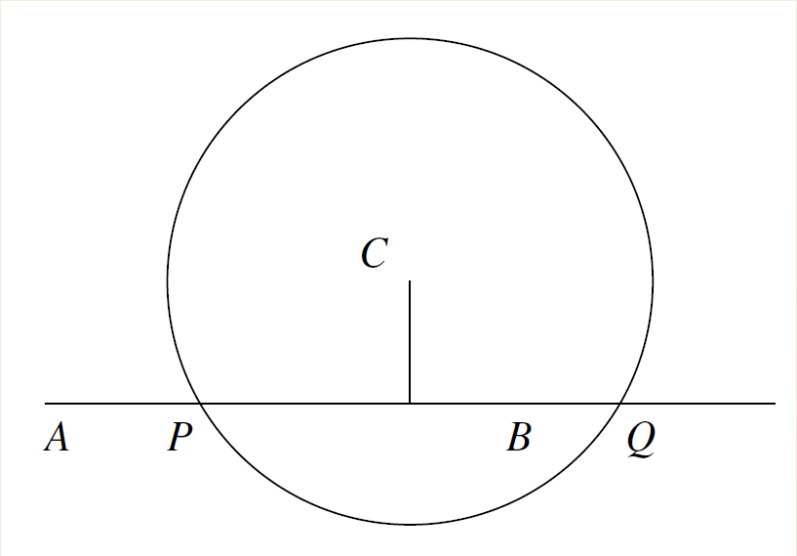


The line PQ is the required perpendicular bisector.

Dropping a Perpendicular From a Point to a Line

- Let A, B be distinct points on the plane, and let C be a point not on the line segment AB. Draw a line through C perpendicular to AB.

  Draw a circle with center C meeting the line AB in points P and Q.



  Then, draw the perpendicular bisector of PQ.

  This construction works just as well if C lies on the line AB.

A Square With a Given Side

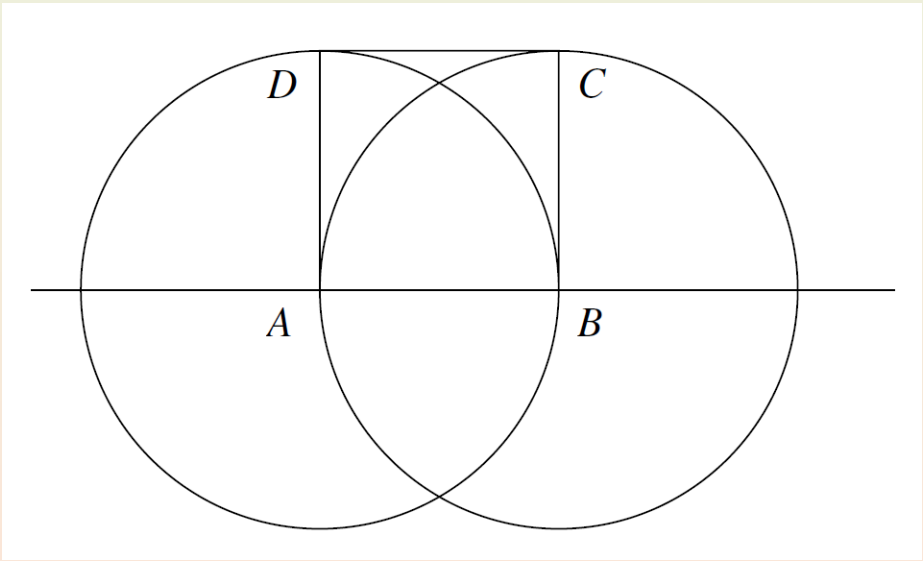
- Let A, B be distinct points on the plane. Construct a square on AB.

  Let $\mathscr{K}_1$ be a circle with center A passing through B.

  Let $\mathscr{K}_2$ be a circle with center B passing through A.

  Draw a line though A perpendicular to AB, meeting $\mathscr{K}_1$ in D.

  Draw a line through B perpendicular to AB, meeting $\mathscr{K}_2$ in C.



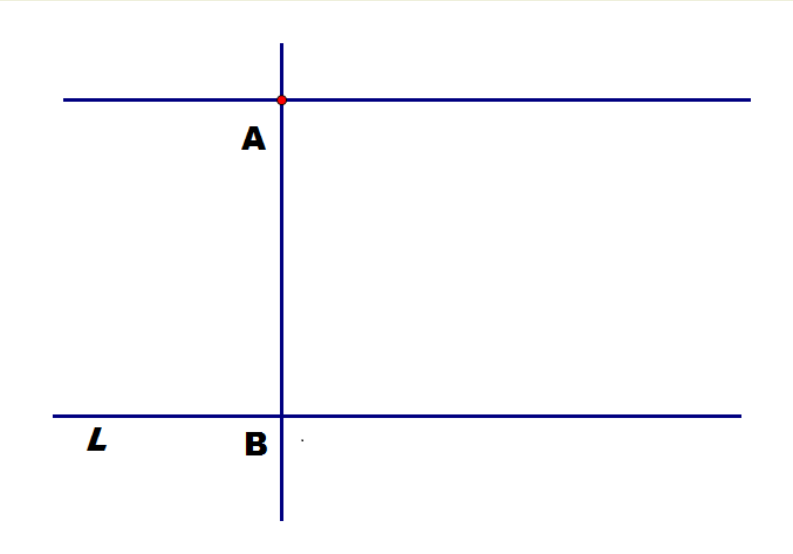
Then $ABCD$ is the required square.

Line Through a Given Point Parallel to a Given Line

- Let L be a line and A a point not on L. Construct a line through A parallel to L.

  Drop a perpendicular from A on to L, meeting L at the point B.

  Then draw the perpendicular to the line AB at the point A.



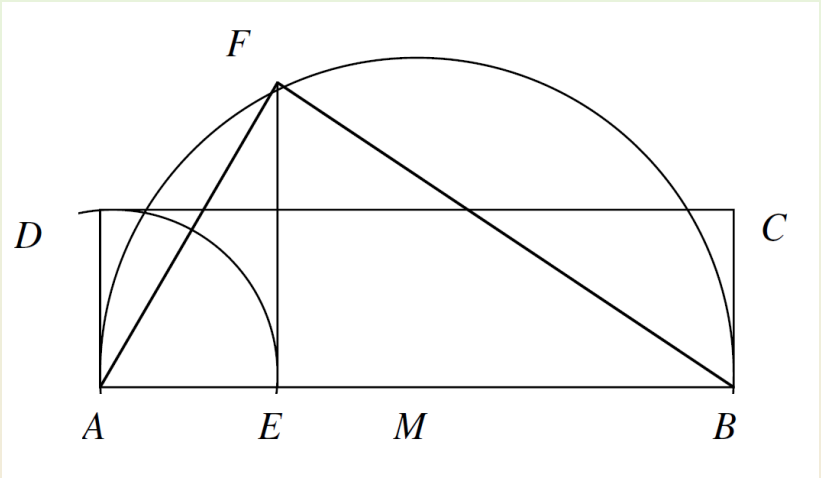
Square Equal in Area to a Given Rectangle

- Construct a square equal in area to a given rectangle $ABCD$.

Suppose that $AD < AB$.

Draw a circle with center A passing through D, meeting AB in E.

Let M be the midpoint of AB.
Draw a circle $\mathscr{K}$ with AB as diameter.



Draw the line through E perpendicular to AB, meeting $\mathscr{K}$ in F.

The angle AFB is a right angle, and the triangles AFB and AEF are similar. Hence $\frac{AE}{AF} = \frac{AF}{AB}$. So

$$AF^2 = AE \cdot AB = AD \cdot AB.$$

The square constructed on AF has the same area as $ABCD$.

Classic Challenges in Geometry

- A classic challenge in Geometry was this:

  Squaring the Circle: Construct, using ruler and compasses only, a square equal in area to a given circle.

  No construction was ever found.
- Other classical challenges were:

  Duplication of the Cube: Construct a cube double the volume of a given cube.
  Trisection of the Angle: Given an angle θ, construct the angle $\frac{\theta}{3}$.

Subsection 2

An Algebraic Approach

Ruler an Compass Operations

- A **cartesian coordinate system** in the plane is specified by:
  - (i) Two axes at right angles to each other, meeting at a point O, the **origin**;
  - (ii) A point I, distinct from O, on one of the axes, given coordinates (1,0).
- Let B_0 be a set of points in the plane.
- There are two permitted operations on the points of B_0.
  - (1) (**Ruler**) Through any two points of B_0, draw a straight line.
  - (2) (**Compass**) Draw a circle whose center is a point in B_0, and whose radius is the distance between two points in B_0.

Constructible Points

- A point is said to be **constructed from B_0 in one step** if it is one of the following types:
  - An intersection of two lines obtained by (Ruler) and (Compass);
  - An intersection of two circles obtained by (Ruler) and (Compass);
  - An intersection of a line and a circle obtained by (Ruler) and (Compass).
- Denote the set of such points by $\mathscr{C}(B_0)$.
- Let $B_1 = B_0 \cup \mathscr{C}(B_0)$.
- By iterating this process, define

$$B_n = B_{n-1} \cup \mathscr{C}(B_{n-1}), \quad n = 1, 2, 3, \ldots.$$

- A point is said to be **constructible from B_0** if it belongs to B_n, for some n.
- A point that is constructible from $\{O, I\}$ is said to be **constructible**.

Example: Constructibility of the Midpoint

- To construct the midpoint of OI from the set $B_0 = \{O, I\}$, we carry out the following steps:
  (1) Join O and I.
  (2) Draw a circle with center O, passing through I.
  (3) Draw a circle with center I, passing through O.
  (4) Mark the points P, Q in which the circles intersect.
  Thus, $B_1 = \{O, I, P, Q\}$.
  (5) Join P and Q.
  (6) Mark the point M in which OI and PQ meet.
  Thus, $B_2 = \{O, I, P, Q, M\}$.

  So the point M is constructible (from $\{O, I\}$).

Associating a Subfield of $\mathbb{R}$ with B_i

- The connection with algebra comes if we associate each B_i with the subfield of $\mathbb{R}$ generated by the coordinates of the points in B_i.

  Example (Cont'd): The field K_0 generated by $B_0 = \{(0,0),(1,0)\}$ is $\mathbb{Q}$.

  The circles $x^2+y^2=1$ and $x^2+y^2=2x$ intersect in $(\frac{1}{2}, \pm\frac{\sqrt{3}}{2})$.

  So the field K_1 generated by $B_1 = \{(0,0),(1,0),(\frac{1}{2},\pm\frac{\sqrt{3}}{2})\}$ is $\mathbb{Q}[\sqrt{3}]$.

  Finally, M is the point $(\frac{1}{2},0)$.

  So the field K_2 generated by

$$B_2 = \left\{(0,0),(1,0),\left(\frac{1}{2},\pm\frac{\sqrt{3}}{2}\right),\left(\frac{1}{2},0\right)\right\}$$

  is still $\mathbb{Q}[\sqrt{3}]$.

Constructibility Theorem

Theorem

Let P be a constructible point, belonging to B_n, where $B_0 = \{(0,0),(1,0)\}$. For $n = 0,1,2,\ldots$, let K_n be the field generated over $\mathbb{Q}$ by B_n. Then $[K_n : Q]$ is a power of 2.

- It is clear that $[K_0 : \mathbb{Q}] = 1 = 2^0$.

  We suppose inductively that $[K_{n-1} : \mathbb{Q}] = 2^k$, for some $k \geq 0$.

  We must show that $[K_n : K_{n-1}]$ is a power of 2.

  New points in B_n are obtained by:

  (1) The intersection of two lines;
  (2) The intersection of a line and a circle;
  (3) The intersection of two circles.

Constructibility Theorem Case (1)

- Case (1). Suppose that we have lines AB and CD, where $A = (a_1, a_2)$, $B = (b_1, b_2)$, $C = (c_1, c_2)$, $D = (d_1, d_2)$, and that all these coordinates are in K_{n-1}.

  The equations of the lines are

$$\begin{aligned} (y - b_2)(a_1 - b_1) &= (x - b_1)(a_2 - b_2); \\ (y - d_2)(c_1 - d_1) &= (x - d_1)(c_2 - d_2). \end{aligned}$$

  The coordinates of their intersection are obtained by solving these two simultaneous linear equations.

  The crucial observation is that the solution process involves only rational operations (addition, subtraction, multiplication and division).

  So it takes place entirely within the field K_{n-1}.

  It follows that the coordinates of the intersection of AB and CD lie inside the field K_{n-1}.

Constructibility Theorem Case (2)

- Case (2). Consider a line AB intersecting a circle with center C and radius PQ, where all points have coordinates in K_{n-1}.

  Taking again $A=(a_1,a_2)$, $B=(b_1,b_2)$, $C=(c_1,c_2)$, we must solve the equations

$$\begin{aligned}(y-b_2)(a_1-b_1) &= (x-b_1)(a_2-b_2);\\ (x-c_1)^2+(y-c_2)^2 &= r^2, \text{ where } r^2\in K_{n-1}.\end{aligned}$$

  We have to solve two simultaneous equations, one linear and one quadratic, with coefficients in K_{n-1}.
  - We express y in terms of x using the linear equation;
  - We substitute in the equation of the circle, obtaining a quadratic equation in x, with coefficients in K_{n-1}.

  The solution involves $\sqrt{\Delta}$, where Δ is the discriminant of the quadratic.

  So the coordinates of the points of intersection belong to $K_{n-1}[\sqrt{\Delta}]$.

  If $\sqrt{\Delta}$ happens to be in K_{n-1}, then $K_{n-1}[\sqrt{\Delta}]=K_{n-1}$.

Constructibility Theorem Case (3)

- Case (3). Suppose that we have a circle with center A and radius r and a circle with center B and radius s, where $r, s \in K_{n-1}$.
  If $A = (a_1, a_2)$, $B = (b_1, b_2)$, we must solve the system

$$\begin{aligned} (x - a_1)^2 + (y - a_2)^2 &= r^2; \\ (x - c_1)^2 + (y - c_2)^2 &= s^2. \end{aligned}$$

  By subtraction we obtain a linear equation (the equation of the chord connecting the points of intersection of the circles).
  This reduces this case to Case (2).
- The conclusion is that the elements in K_n are either in K_{n-1} or in $K_{n-1}[\sqrt{\Delta}]$, for some Δ in K_{n-1}.
  Hence, for some $k \geq 0$,

$$K_n = K_{n-1}(\sqrt{\Delta_1}, \sqrt{\Delta_2}, \ldots, \sqrt{\Delta_k}).$$

  This shows that $[K_n : K_{n-1}]$ is a power of 2.

Duplicating the Cube

- **Duplication of the Cube**: Construct a cube double the volume of a given cube.

  Suppose, without loss of generality, that the original cube has side of length 1.

  We must extend the field $\mathbb{Q}$, using the construction rules, to a field K containing an element α, such that $\alpha^3 = 2$.

  The polynomial $X^3 - 2$ is irreducible, by the Eisenstein criterion.

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

  Hence $[K : \mathbb{Q}]$ is divisible by 3.

  This is impossible, by the Constructibility Theorem.

Trisecting the Angle

- **Trisection of the Angle**: Given an angle θ, construct the angle $\frac{\theta}{3}$.
  Suppose that we have an angle 3θ, which is "known", in the sense that we know its cosine, say $\cos 3\theta = c$.
  We need to construct the number $\cos\theta$.
  Recall that $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$.
  Indeed, we have

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

  So $\frac{1}{2}\cos 3\theta = 2\cos^3\theta - \frac{3}{2}\cos\theta$ or $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$.
  We need find a root α of $4X^3 - 3X - c = 0$.
  We show that this depends on the value of 3θ (or c).
  So there is no construction that works for any angle.

Trisecting the Angle (Cont'd)

- Recall that we need find a root α of $4X^3 - 3X - c = 0$.
- Suppose, for example, $3\theta = \frac{\pi}{2}$, so that $c = \cos 3\theta = 0$.
  Then $4X^3 - 3X$ factorizes as $X(4X^2 - 3)$.
  So $[\mathbb{Q}[\alpha] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$.
  In this case we can construct a trisector.
- On the other hand, suppose, e.g., $3\theta = \frac{\pi}{3}$, so that $c = \cos 3\theta = \frac{1}{2}$.
  Then we are looking at $f(X) = 8X^3 - 6X - 1$.
  It factorizes if and only if $g(X) = f(\frac{X}{2}) = X^3 - 3X - 1$ factorizes.
  If $g(X)$ factorizes over $\mathbb{Q}$, then, by Gauss's Lemma, it does so over $\mathbb{Z}$.
  One of the factors must be linear, and must be either $X - 1$ or $X + 1$.
  However, $g(1) = -3 \neq 0$ and $g(-1) = 1 \neq 0$.
  So $g(X)$, and hence $f(X)$, is irreducible.
  Thus, $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$.
  So no ruler and compass construction is possible.

Squaring the Circle

- **Squaring the Circle**: Construct, using ruler and compasses only, a square equal in area to a given circle.

  Suppose that we have a circle of radius 1.

  Its area is π.

  So we need to construct the number $\sqrt{\pi}$.

  As mentioned earlier, the number π is transcendental.

  Since $\mathbb{Q}(\pi) \subseteq \mathbb{Q}(\sqrt{\pi})$, the degree $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ is certainly infinite.

  So $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ is certainly not a power of 2.

  This shows that the construction is not possible.
- This very brief proof is concealing the real issue, which is the transcendentality of π.