SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Field Extensions and Straightedge and Compass Constructions

av

Manuel Hemström

2024 - No K12

Field Extensions and Straightedge and Compass Constructions

Manuel Hemström

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Gregory Arone

2024

Abstract

This bachelor thesis explores the use of Field Extensions on Straightedge and Compass Constructions in order to refute the Three Classical Problems: (1) Doubling the Cube, (2) Trisecting the Angle, (3) Squaring the Circle. By applying the theory of Field Extensions, we demonstrate that these age-old conjectures are inherently unsolvable within the framework of constructible numbers.

Abstrakt

Detta kandidatarbete undersöker användningen av kroppsutvidningar vid linjal- och passarkonstruktioner för att motbevisa de tre klassiska problemen: (1) Fördubbling av kuben, (2) Tredelning av vinkeln, (3) Kvadratur av cirkeln. Genom att tillämpa teorin om kroppsutvidningar visar vi att dessa uråldriga hypoteser är fundamentalt olösbara inom ramen för konstruktibla tal.

Contents

1 Introduction

Straightedge and compass constructions have been a subject of fascination for mathematicians throughout history, dating back to ancient Greece. In pursuit of geometric perfection, mathematicians sought to explore the limitations and possibilities of constructing shapes using only a straightedge (an unmarked ruler) and compass.

The origins of straightedge and compass constructions can be traced back to the work of ancient Greek mathematicians such as Euclid, who laid the foundations of geometry in his seminal work Elements. Here, Euclid introduced the fundamental principles of geometry and provided a systematic approach to constructing geometric figures using straightedge and compass.

Among the many legacies of ancient Greek mathematics are three classical construction problems, known for their intriguing impossibility:

- Doubling the Cube: Given a cube, construct a cube with twice the volume.
- Trisecting the Angle: Given an angle, divide it into three equal segments.
- Squaring the Circle: Given a circle, construct a square with the same area.

The pursuit of solutions to these problems has led mathematicians to explore the limits of straightedge and compass constructions. Despite numerous attempts over the centuries, these problems have remained unsolved.

These problems have challenged mathematicians for centuries, leading to significant advancements in understanding the limitations of straightedge and compass constructions. Despite numerous attempts, these have been proven impossible to solve using these tools only.

In this thesis, we explore the limitations of straightedge and compass constructions, focusing primarily on disproving the three classical problems. Our approach involves employing the tools of field theory and algebraic extensions to demonstrate that these problems are inherently unsolvable within the realm of constructible numbers.

2 Straightedge and Compass Constructions

In this section we introduce the fundamental notions of geometric constructions. We will delve into straightedge and compass constructions, illustrating the tools and methods used to construct geometric figures. We will also show that the set of constructible numbers form a field.

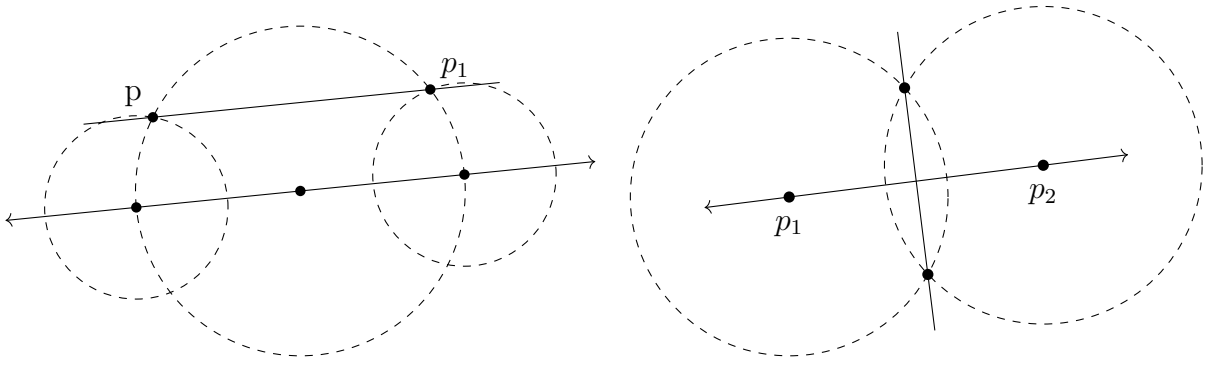
2.1 Tools for Constructions

A *straightedge*, sometimes referred to as a *Euclidean ruler*, is used to draw straight lines through two points or to extend existing line. It has no markings, rendering it unusable for measurement. A *compass* is used to draw circles or arcs given a center and set radius.

2.2 Constructions

We will now explore some of the elementary constructions using straightedge and compass.

First, we will demonstrate how to construct a parallel line through a point p off of a given line l. Begin by drawing a circle passing through p and with its center somewhere on l. Then at one of the intersection points of l and the circle, draw a circle intersecting with p. Next, draw a circle with the same radius from the other intersection point of l and the circle. This circle will intersect the first circle at a point p_0 on the same side of the line as p. By drawing a line between p and p_0, we have successfully constructed a line parallel to l. Refer to Figure (1a) for visualization.



(a) Parallel line (b) Perpendicular line

Figure 1

We will also demonstrate the construction of a perpendicular bisector. Pick two points p_1 and p_2 on a line. With these points as centers, draw two circles with the same radius such that the two circles intersect at two points on each side of the line. Connect them, and we are done. Refer to Figure (1b) for visualization.

Given two lengths α and β and a unit distance 1, it is possible to construct the lengths $\alpha \pm \beta$, $\alpha\beta$, α/β (when $\beta \neq 0$), and $\sqrt{\alpha}$. These operations are hereby presented:

First, let's show the construction for $\alpha+\beta$ and $\alpha-\beta$. See Figure 2. If $\alpha, \beta > 0$ are two given lengths, we can extend α, using the straightedge, from its endpoint to a point at length β from the endpoint. This is the construction for $\alpha+\beta$. Additionally, we can if $\alpha > \beta$, we can find the point on α that is at length β from its endpoint, constructing $\alpha - \beta$.

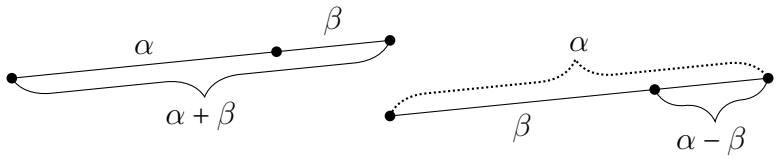


Figure 2: Addition and subtraction

Next, let's show the construction for $\alpha\beta$ in Figure 3. First, construct a segment of length α, and from one endpoint, mark the unit distance 1 on the same segment. From the same endpoint construct a segment of length β while also extending the line. Connect the endpoint of β to the endpoint of 1. Label this line $\mathcal{L}$. From the other endpoint of the α segment, construct a line parallel to $\mathcal{L}$ until the intersection of the extended segment. The length from the first endpoint to this intersection has the length $\alpha\beta$. To construct α/β, interchange the length from the first endpoint to the intersection with β.

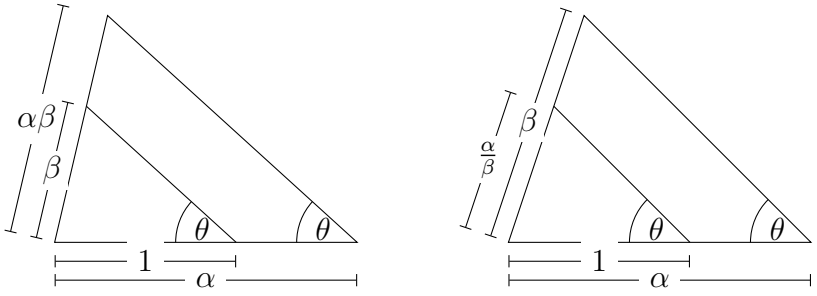


Figure 3: Multiplication and division

To prove the construction of $\alpha\beta$, notice that since the triangles are similar, the length $\alpha\beta$ is proportional to α as β is proportional to 1, i.e., $\alpha\beta/\alpha = \beta/1$. From this we are able to derive $\alpha\beta$. To construct α/β, just change $\alpha\beta$, in the first figure, to β.

Lastly, let's show the construction of $\sqrt{\alpha}$ as shown in Figure 4.

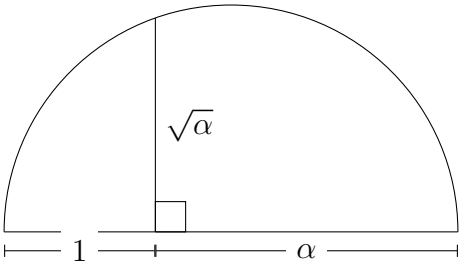


Figure 4: Square root

Given a segment of length $\alpha + 1$, find its midpoint and draw a semicircle using the midpoint as the center and the segment as the diameter. On the segment, find the point between α and 1. From this point, construct a perpendicular to the arc of the semicircle. This perpendicular segment has length $\sqrt{\alpha}$.

Thus, we have demonstrated the constructions of $\alpha \pm \beta$, $\alpha\beta$, α/β (when $\beta \neq 0$), and $\sqrt{\alpha}$ using straightedge and compass.

Now, lets formalize exactly what is meant by constructing points with a straightedge and compass. Initially, we assume that we are given two points in the plane, with the distance between them defined as the unit length. We introduce a coordinate system on the plane, such that the two points have coordinates $(0, 0)$ and $(1, 0)$. Using only straightedge and compass, the points we can construct must fall into one of the following categories:

1. the intersection point of two lines,
2. the intersection point(s) of a line and a circle,
3. the intersection point(s) of two circles.

Definition 2.1. A point is *constructible* by straightedge and compass if it is either (1) the intersection of two lines that both pass through two already constructible points, (2) the intersection of a line and a circle of which the line passes through an already constructible points and the circle passes through an already constructible point with a constructible points as a center, or (3) the intersection of two circles

that both pass through some already constructible points with constructible points as their centers. The initial constructible points are $(0,0),(1,0)$.

Definition 2.2. A length x is constructible if the point $(x,0)$ is constructible. The term constructible number is used interchangeably.

Definition 2.3. A *sequence* of constructible points is a set of points $\{p_1,p_2,...,p_n\}$ with $n \geq 2$, wherein the last point has been constructed using the earlier points.

Here are some examples of sequences of constructible points:

$\{(0,0),(1,0)\}$ are the trivial constructions,
$\{(0,0),(1,0),(2,0),(2,2)\}$,
$\{(0,0),(1,0),(2,0),(3,0),(-3,0)\}$,
$\{(0,0),(1,0),(1/2,0),(1/4,0),(1/8,0)\}$,
$\{(0,0),(1,0),(2,0),(3,0),(1,\sqrt{2})\}$.

Note that in order to construct, say, the point $(1,\sqrt{2})$, we must first construct $(2,0)$, and then $(3,0)$ and only then can we construct $(1,\sqrt{2})$.

We will now also consider the construction of angles.

Definition 2.4. An angle θ is constructible if there exists points A,B,C, such that $\angle ABC = \theta$.

Proposition 2.5. *The following are equivalent:*

1. *The angle θ is constructible.*
2. *The length $\cos\theta$ is constructible.*
3. *The length $\sin\theta$ is constructible.*

Proof. If an angle is constructible, there exists three constructible point A,B,C such that $\angle ABC = \theta$. Then, we can draw a line perpendicular from A to the line BC, and let P be the point of intersection. Then $\sin\theta = AP/AB$, and $\cos\theta = BP/AB$.

Conversely, suppose $\sin\theta$ is constructible. From one endpoint of a segment of length $\sin\theta$, draw a perpendicular line. From the other endpoint, draw an arc with radius 1 to intersect the perpendicular. Connecting this endpoint and the intersection point forms the angle θ.

An similiar method can be used to show that if $\cos\theta$ is constructible, then the angle θ is also constructible. □

2.3 Field of Straightedge and Compass Constructions

Geometric constructions can be reformulated in field-theoretic terms. A field is a set of numbers equipped with the operations of addition, subtraction, multiplication, and division, satisfying certain axioms. We conclude that the set of numbers obtainable by straightedge and compass constructions forms a field.

Theorem 2.6. *The set F of all lengths constructible by straightedge and compass, and a unit distance* 1*, together with their negatives, form a subfield of* $\mathbb{R}$*.*

Proof. Let F be the set of *constructible numbers*. Since F contains the unit distance, it is non-empty, i.e., $1 \in F$. As we have seen, for two lengths $\alpha, \beta > 0$, we can construct $\alpha \pm \beta$, $\alpha\beta$, and α/β (when $\beta \neq 0$), using a straightedge and compass. Therefore, F is closed under the field operations. □

Remark 2.7. Additionally, the field F has the property that if $\alpha > 0$ is an element of F, then $\sqrt{\alpha}$ is also an element of F.

Notice that F is a subfield of $\mathbb{R}$. We will later see that it is a proper subfield. Also, notice that $\mathbb{Q}$ is a proper subfield of F, since we can construct numbers $\sqrt{\alpha}$ which are not in $\mathbb{Q}$.

2.4 Moving forward

In this section, we have explored some basic geometric constructions, including those corresponding to arithmetic operations. While these examples provide a foundational understanding, geometric constructions extend far beyond these operations. Additional constructions include angle bisections, constructing parallelograms, and constructing some regular polygons like pentagons and hexagons. However, we will now shift our focus to field theory, developing the tools necessary for algebraically analyzing straightedge and compass constructions.

Moving forward, we will assume the reader is familiar with fundamental concepts of ring theory, specifically, the definitions of *rings* and *fields*. Additionally, the reader should have a basic understanding of linear algebra, particularly the concept of a *basis*.

3 Field Extensions

3.1 Basic definitions

We begin by recalling the definition of a field extensions, and of a subfield generated by a set of elements.

Definition 3.1. A field K containing a subfield F is said to be an *extension* of the *base field* F, denoted as K/F. Let α, β, ... be elements of K. The field $F(\alpha, \beta, ...)$ is defined to be the intersection of all subfields of K containing F and α, β, ... etc. This is the smallest subfield of K containing both F and the elements $\alpha, \beta, ...$ from K. This field is said to be generated by $\alpha, \beta, ...$ over F.

Example 3.2. It is well-known that $\sqrt{2}$ is not rational, so we can extend $\mathbb{Q}$ by it. We obtain the extension $\mathbb{Q}(\sqrt{2})$ generated by $\sqrt{2}$ over $\mathbb{Q}$. This field consists of all numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$. In other words, it is the set obtained by combining rational numbers with multiples of $\sqrt{2}$. For instance, $\frac{1}{3} - 2\sqrt{2}$ or $\frac{\sqrt{2}}{7}$ are both elements of $\mathbb{Q}(\sqrt{2})$.

Lets check that this in fact is a field. It has an additive identity $0 + 0\sqrt{2}$, and a multiplicative identity $1 + 0\sqrt{2}$. It is closed under addition and subtraction since, for $a, b, c, d \in \mathbb{Q}$,

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}.$$

It is closed under multiplication since

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}.$$

For every $a + b\sqrt{2}$, there exists an additive inverse $-a - b\sqrt{2}$. If $a + b\sqrt{2} \neq 0$, there exists a multiplicative inverse $1/(a+b\sqrt{2})$. We can see that this is indeed an element of $\mathbb{Q}(\sqrt{2})$ by multiplying with the conjugate:

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

Example 3.3. The extension $\mathbb{Q}(\sqrt[3]{2})$ generated by $\sqrt[3]{2}$ over $\mathbb{Q}$. It is obvious that $\mathbb{Q}(\sqrt[3]{2})$ contains all numbers of the form $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$, where $a, b, c \in \mathbb{Q}$. One sees that this set forms a field, and in fact this field is $\mathbb{Q}(\sqrt[3]{2})$.

Lets again check that this is a field. It has the additive identity $(0+0\sqrt[3]{2}+0\sqrt[3]{2}^2)$, and the multiplicative identity $(1+0\sqrt[3]{2}+0\sqrt[3]{2}^2)$. We can see that it is closed under

addition since, for $a, b, c, d, e, f \in \mathbb{Q}$,

$$(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) + (d + e\sqrt[3]{2} + f\sqrt[3]{2}^2) = (a + d) + (b + e)\sqrt[3]{2} + (c + f)\sqrt[3]{2}^2.$$

It is closed under multiplication since

$$\begin{aligned}&(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2) \cdot (d + e\sqrt[3]{2} + f\sqrt[3]{2}^2) = \\ &(ad + 2bf + 2ce) + (ae + bd + 2cf)\sqrt[3]{2} + (af + be + cd)\sqrt[3]{2}^2.\end{aligned}$$

For every $(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)$ there exists an additive inverse $(-a - b\sqrt[3]{2} - c\sqrt[3]{2}^2)$. There also exists a multiplicative inverse $1/(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)$ for every non-zero $(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)$. While the proof of this property is more difficult to show and outside the scope of this discussion, it can in fact be shown that

$$\frac{1}{(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2)} = \frac{(a^2 - 2bc) + (2c^2 - ab)\sqrt[3]{2} + (b^2 - ac)\sqrt[3]{2}^2}{a^3 + 2b^3 + 4c^3 - 6abc}.$$

These examples show how we can extend the rational field $\mathbb{Q}$ by adding certain irrational numbers to it, allowing us to form new fields with richer algebraic structures.

3.2 Degree of Field Extensions

We can view a field extension as a vector space by considering the extension field as a vector space over the base field. Let K be an extension field of a base field F. Then, since K contains F, we can consider the elements of K as vectors, and the elements of F as scalars. The vector space structure will be defined as:

1. For any α, β in K, $\alpha + \beta$ is also in K,
2. For any α in K and c in F, $c \cdot \alpha$ is also in K.

With this observation, with can apply concepts from linear algebra to field-theory. This leads us to the following definition:

Definition 3.4. The degree of an extension K/F, denoted as $[K : F]$, is the dimension of K over F as a vector space.

The degree of a field extension therefore quantifies the "size" of an extension in terms of how many elements are added to the base field.

Example 3.5. The degree of the extension $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ is 2. This means that any element in the field can be expressed by two rationals a and b, and the base $\{1, \sqrt{2}\}$ spans a two-dimensional vector space over $\mathbb{Q}$.

Example 3.6. For the extension $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$, any element can be expressed as $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$, where $a, b, c \in \mathbb{Q}$. To demonstrate that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is linearly independent, we will show that there are no non-trivial rational coefficients a, b, c such that $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 = 0$.

First, observe that $\sqrt[3]{2}$ is irrational, and clearly 1 and $\sqrt[3]{2}$ are linearly independent. Suppose for contradiction that $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is linearly dependent. This would imply that there exists $a, b \in \mathbb{Q}$ such that $a + b\sqrt[3]{2} = \sqrt[3]{2}^2$. Cubing both sides, we get

$$a^3 + 2b^3 + 3a^2b\sqrt[3]{2} + 3ab^2\sqrt[3]{4} = 4.$$

For this equation to hold, the rational and irrational parts on both sides must be equal. Thus, we have the two equations

$$\begin{aligned} a^3 + 2b^3 &= 4, \\ 3a^2b\sqrt[3]{2} + 3ab^2\sqrt[3]{4} &= 0. \end{aligned}$$

For the irrational part to hold, either $a = 0$ or $b = 0$. Substituting $a = 0$ in the rational part, we get $b^3 = 2$. But since b is rational, this is a contradiction. If $b = 0$ in the rational part, then $a^3 = 4$. A contradiction for the same reason.

Therefore, no non-trivial solutions exists, and $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ is indeed linearly independent over $\mathbb{Q}$. Consequently, the basis spans a three-dimensional vector space over $\mathbb{Q}$, and the degree of the extension $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ is 3.

Example 3.7. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, where any element can be expressed as $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, where $a, b, c, d \in \mathbb{Q}$.

To show that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is linearly independent over $\mathbb{Q}$, we start by assuming a linear combination of these elements are equal to zero:

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0.$$

By factoring $\sqrt{2}$ we get

$$(a + b\sqrt{2}) + (c + d\sqrt{2})\sqrt{3} = 0.$$

This is then equivalent to showing that $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$. Suppose by contradiction that there exists rationals a and $b \neq 0$ such that $a + b\sqrt{2} = \sqrt{3}$. Squaring both sides gives and

$$a^2 + 2ab\sqrt{2} + 2b^2 = 3$$

Separating the rational and irrational parts, we get

$$a^2 + 2b^2 = 3$$
$$2ab\sqrt{2} = 0.$$

For the irrational part to hold, $a = 0$ since, by assumption $b \neq 0$. Substituting $a = 0$ in the rational part, we get $b^2 = 3/2$, which contradicts the assumption that b is rational. Therefore, $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$.

Thus, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ spans a four-dimensional vector space over $\mathbb{Q}$, and the degree of the extension $[\mathbb{Q}(\sqrt{2}, \sqrt{3} : \mathbb{Q}]$ is 4.

As we adjoin more algebraic elements to a base field, the degree of the resulting field extension will increase. We state this as a theorem shortly.

A quadratic extension arises when we add the square root of an element to a given field. Specifically, for a field F and an element α in F such that$\sqrt{\alpha} \notin F$, the extension $F(\sqrt{\alpha})$ is a quadratic extension. Such a field will be of the form

$$\{a + b\sqrt{\alpha} \mid a, b \in F\},$$

which is spanned by its basis $\{1, \sqrt{\alpha}\}$. If, however, $\sqrt{\alpha} \in F$, the extension does not add any new element that was not already in F, i.e., $F(\sqrt{\alpha}) = F$. This proves the next proposition:

Proposition 3.8. *Any quadratic extension $F(\sqrt{\alpha})$ where α is an element of F, but $\sqrt{\alpha} \notin F$, has degree 2 over F, i.e., $[F(\alpha) : F] = 2$.*

Proposition 3.9. *Suppose E is a subfield of the real numbers, and we have the quadratic equation*

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

where a, b, c are elements of E. Then the solutions to this equation are either in E or in a quadratic extension of E.

Proof. By the quadratic formula, the solutions to the equation is given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

It is trivially clear that $b^2 - 4ac$ is in E. Now, if $\sqrt{b^2 - 4ac}$ is in E, then the solutions are in E. If not, $\sqrt{b^2 - 4ac}$ is in a quadratic extension of E, and the solutions will be in the same quadratic extension. □

Another important result:

Theorem 3.10. *Extension degrees are multiplicative, i.e., if $F \subseteq K \subseteq L$, then $[L : F] = [L : K][K : F]$.*

Proof. Let $[K : F] = n$ and let K have a basis $u_1, u_2, ..., u_n$ over F. Then for any element $k \in K$, we can express it as a linear combination

$$k = f_1u_1 + f_2u_2 + ... + f_nu_n,$$

where $f_1, f_2, ..., f_n$ are elements of F. Also let $[L : K] = m$ and let L have a basis $v_1, v_2, ..., v_m$ over K. Then for any element $l \in L$:

$$l = k_1v_1 + k_2v_2 + ... + k_mv_m,$$

where $k_1, k_2, ..., k_m$ are elements in K. We can then express any element k_i as

$$f_{i1}u_1 + f_{i2}u_2 + ... + f_{in}u_n,$$

and thereby, any element in L can be expressed as a linear combination

$$\begin{aligned}\varphi = (f_{11}u_1 + ... + f_{1n}u_n)v_1 + (f_{21}u_1 + ... + f_{2n}u_n)v_2 + ... \\ ... + (f_{m1}u_1 + ... + f_{mn}u_n)v_m \\ = \sum_{\substack{i=1,2,...,m \\ j=1,2,...,n}} f_{ij}u_jv_i,\end{aligned}$$

where each element f_{ij} is in F. It follows that the elements u_iv_j span L as the vector space over F. We still have to show that they are linearly independent.

Now, suppose that

$$\sum_{\substack{i=1,2,...,m \\ j=1,2,...,n}} f_{ij}u_jv_i = 0.$$

This is equivalent to the following

$$(f_{11}u_1 + ... + f_{1n}u_n)v_1 + ... + (f_{m1}u_1 + ... + f_{mn}u_n)v_m = 0.$$

Since $v_1, v_2, ..., v_m$ is a basis for L over K, it follows that the coefficients v_i must be 0. Then, really

$$f_{i1}u_1 + f_{i2}u_2 + ... + f_{in}u_n = 0,$$

for $i = 1, 2, ..., m$ in K. Now, since u_j, $j = 1, 2, ..., n$ forms a basis for K over F, it must be $f_{ij} = 0$, for all i, j. Thereby, the elements $u_j v_i$ in L are linearly independent over F, and form a basis. Therefore $[L : F] = nm$, which is the degrees of $[L : K]$ multiplied with $[K : F]$. □

Recall Example 3.7, where we established that the degree $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ is 4. We can further understand this result using the multiplicativity of extension degrees:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

First extend $\mathbb{Q}$ by $\sqrt{2}$, yielding $\mathbb{Q}(\sqrt{2})$, Then, we extend $\mathbb{Q}(\sqrt{2})$ by $\sqrt{3}$, yielding $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Next, we want to determine $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$. Since $\sqrt{3}$ is not in $\mathbb{Q}(\sqrt{2})$, the extension has degree 2. This follows from the fact that any element in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written as $a + b\sqrt{3}$, where $a, b \in \mathbb{Q}(\sqrt{2})$. Thus, we confirm that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

As we have seen, algebraic field extensions have finite dimensions. However, when extending the rational field by non-algebraic numbers, the situation becomes more complicated.

Definition 3.11. An element $\alpha \in K$ is algebraic over F if it is the root of some monic polynomial $f(x) \in F[x]$. If this is not the case, i.e., if the degree is infinite, α is transcendental over F.

Theorem 3.12. *The number π is transcendental.*[1]

[1]This was proved by Ferdinard Lindemann in 1882. We will not go into the proof since it is quite long. It is not too difficult to find.

4 Impossible Constructions

Continuing, we will use the results above on field extensions, especially the multiplicativity of extension degrees, to algebraize the straightedge and compass constructions and find some interesting results about the impossible constructions mentioned in Section (1). Lets first prepare some lemmas about the characteristics of constructible points.

Lemma 4.1. *Suppose a line passes through two constructible points* (x_1, y_1) *and* (x_2, y_2)*. Then the equation for the line can be written in the form*

$$ax + by + c = 0,$$

where a, b, c *are constructible numbers.*

Proof. It is well known that the equation for the line can be expressed as

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

which, in turn, can be simplified as

$$(y_2 - y_1)x + (x_1 - x_2)y + (x_1y_2) + (x_2y_1) = 0.$$

Letting $a = (y_2 - y_1)$, $b = (x_1 - x_2)$, and $c = (x_1y_2) + (x_2y_1)$, it follows that the line is constructible. □

Lemma 4.2. *Suppose a circle has its center at a constructible point and passes through another constructible point. Then its equation can be written in the form*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

where a, b, c, d, e, f *are constructible numbers.*

Proof. The equation for a circle with center (p, q) passing through a point (s, t) can be described by

$$(x - p)^2 + (y - q)^2 = (s - p)^2 + (t - q)^2.$$

Expanding, we get

$$\begin{aligned} x^2 - 2px + p^2 + y^2 - 2qy + q^2 &= s^2 - 2ps + p^2 + t^2 - 2qt + q^2 \\ x^2 + y^2 + (-2p)x + (-2q)y + (s(2p - s) + t(2q - t)) &= 0, \end{aligned}$$

which is of the desired form. □

These two lemmas provide essential tools for algebraically describing lines and circles, enabling us to precisely characterize geometric constructions using straightedge and compass.

Now, let's delve into the properties of intersection points:

Lemma 4.3. *Suppose we are given two lines described by the equations*

$$\begin{aligned} a_1x + b_1y + c_1 &= 0, \\ a_2x + b_2y + c_2 &= 0, \end{aligned}$$

where $a_1, b_1, c_1, a_2, b_2, c_2$ belong to a field E. Assuming the lines are not parallel, they intersect at a single point (x_1, y_1), where x_1 and y_1 are also in E.

Proof. We determine the intersection point using Cramer's rule:

$$(x_1, y_1) = \left(\frac{c_2b_1 - c_1b_2}{a_1b_2 - a_2b_1}, \frac{a_2c_1 - a_1c_2}{a_1b_2 - a_2b_1} \right).$$

It is then evident that the coordinates for the point (x_1, y_1) are in E. □

From the above lemma, we infer that if we are given points on a plane, whose coordinates are in a field E, constructions solely using straightedge will not yield points with coordinates outside E. It becomes more intriguing when circles are introduced:

Lemma 4.4. *Suppose we have a line and a circle by the equations*

$$\begin{aligned} y &= kx + m, \\ ax^2 + bxy + cy^2 + dx + ey + f &= 0, \end{aligned}$$

where k, m, a, b, c, d, e, f are all in the field E. If the line and the circle intersect at a point (x_1, y_1), then x_1 and y_1 belong to either E or a quadratic extension of E.

Proof. By substituting $kx + m$ for y in the second equation, we obtain a quadratic equation

$$(a + bk + k^2)x^2 + (d + bm + 2km + ek)x + (f + m^2 + em) = 0,$$

whose coefficients all belong to E. By Proposition 3.9, the solutions to this equation are either in E or in a quadratic extension of E. □

Lemma 4.5. *Suppose we have two circles with the equations*

$$(x - h_1)^2 + (y - k_1)^2 = r_1^2,$$
$$(x - h_2)^2 + (y - k_2)^2 = r_2^2,$$

where $h_1, k_1, r_1, h_2, k_2, r_2$ are in the field E. If the circles intersect at a point (x_1, y_1), then x_1 and y_1 belong either to E or a quadratic extension of E.

Proof. By subtracting the second equation from the first, we obtain the equation of a line:

$$2(h_2 - h_1)x + 2(k_2 - k_1)y + r_2^2 - h_2^2 - k_2^2 - r_1^2 + h_1^2 + k_1^2 = 0.$$

This, then, amounts to identifying the point(s) of intersection between a line and a circle, reducing the proof to Lemma 4.4. □

Proposition 4.6. *Let (x, y) be a constructible point. Then there exists a field extension F of $\mathbb{Q}$ such that x and y are in F, and $[F : \mathbb{Q}] = 2^n$, for some $n \geq 0$.*

Proof. According to the Definition 2.1, a constructible point (x, y) can be obtained by a sequence of points:

$$\{p_1 = (0, 0), p_2 = (1, 0), p_3, p_4, ..., p_k = (x, y)\},$$

where each p_i is obtained by finding the intersection point of either two lines, a line and a circle, or two circles.

For each $i = 1, 2, ..., k$, let E_i be the field generated over $\mathbb{Q}$ by the coordinates $p_1, p_2, ..., p_i$. It follows from the previous lemmas that for each i, either $E_{i+1} = E_i$ or $[E_{i+1} : E_i] = 2$.

It now follows from induction and Theorem (3.10) that $[E_k : \mathbb{Q}] = 2^n$, for some $n \geq 0$. □

This leads us to the next theorem:

Theorem 4.7. *Suppose α is a constructible number. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2.*

Proof. A constructible number is the coordinate of a constructible point. It follows from the previous proposition that α is in some field E with $[E : \mathbb{Q}] = 2^k$, for some $k \geq 0$. But then $[E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]$, and therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is also a power of 2. □

We can now use this result to examine the three following constructions:

4.1 Doubling the Cube

Doubling the cube seeks to construct a cube with twice the volume of a given cube.

Let the volume of the cube be 1. We then want to construct a cube with volume 2, requiring us to find the side length $\sqrt[3]{2}$. However, as demonstrated in Example (3.6), the degree $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, which is not a power of 2. Thus, doubling the cube is not achievable.

4.2 Trisecting the Angle

Trisecting an angle seeks to divide an angle into three equal parts.

Recall that an angle α is constructible if and only if $\cos\alpha$ is constructible. While it is possible to trisect certain angles, such as the right angle $90°$, where we can construct $\sin 30° = \frac{1}{2}$ and $\cos 60° = \frac{1}{2}$, this construction is not universally applicable. We will demonstrate this by proving the impossibility of trisecting a $60°$ angle.

Let $\theta = 20°$. We know that $\cos 3\theta$ is constructible. By the triple angle formula,

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

Let $x = \cos\theta$, and we can rewrite the equation as

$$\begin{aligned} \frac{1}{2} &= 4x^3 - 3x \\ 8x^3 - 6x - 1 &= 0. \end{aligned} \tag{1}$$

If this polynomial is irreducible, then it is the minimal polynomial of $\cos\theta$. In such a case, we conclude that $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 3$, and by Theorem (4.7), $\cos\theta$ is not constructible.

We now show that $8x^3 - 6x - 1 = 0$ is irreducible over $\mathbb{Q}$. Suppose $\frac{p}{q}$ is a root of this polynomial with $(p, q) = 1$. Then

$$8\frac{p^3}{q^3} - 6\frac{p}{q} - 1 = 0$$
$$8p^3 - 6pq^2 - q^3 = 0.$$

We find that $2|(8p^3 - 6pq^2)$ implying $2|q$. Let $q = 2k$, and $(p, k) = 1$. Then

$$8p^3 - 24pk^2 - 8k^3 = 0$$
$$p^3 - 3pk^2 - k^3 = 0,$$

which implies $p|k^3$ and $k|p^3$, forcing p and k to be ± 1, which is not a solution. Hence, there can be no rational roots for $8x^3 - 6x - 1 = 0$, proving it irreducible over $\mathbb{Q}$.

Therefore, we have shown that it is impossible to trisect a constructible 60° angle using only a straightedge and compass.

4.3 Squaring the Circle

Squaring the circle seeks to construct a square with the same area as a given circle.

The area for a circle is given by πr^2. If we consider a square with the same area, its side length would be $\sqrt{\pi r^2}$. Therefore, the construction of $\sqrt{\pi}$ is necessary.

According to Theorem 3.12, π is transcendental. This implies that the field extension $\mathbb{Q}(\pi)$ over $\mathbb{Q}$ has infinite degree, meaning π is non-constructible by Theorem (4.7). However, we aim to determine whether $\sqrt{\pi}$ is constructible.

Suppose $\sqrt{\pi}$ is algebraic over $\mathbb{Q}$. Then $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = n$ for some finite n. But we can write

$$n = [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}(\pi)] \cdot [\mathbb{Q}(\pi) : \mathbb{Q}],$$

which implies that n is divisible by $[\mathbb{Q}(\pi) : \mathbb{Q}]$. Since π is transcendental, $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is infinite. Consequently, $[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}]$ must also be infinite, contradicting the assumption that n is finite.

Thus, by Theorem (4.7), we conclude that $\sqrt{\pi}$ is impossible to construct. Therefore, squaring the circle is impossible.

5 Constructions using Ruler and Compass

As we have seen, constructions using a straightedge and compass are limited in their applications. However, by introducing alternative tools, we can solve at least some of these classical problems. In this section, without developing the algebraic framework, we will explore constructions using a marked ruler and compass to address the problems of trisecting the angle and doubling the cube.

While the classical straightedge is unmarked, a marked ruler, also known as a neusis ruler, allows for more versatile constructions. The *neusis construction*, also refereed to as *verging*, provides additional flexibility that can solve problems otherwise impossible with a straightedge and compass.

5.1 Neusis Construction

The neusis construction involves the following steps: Given two intersecting lines n and m, and a point p, position the ruler at p, pivoting around p until the distance between the lines is a desired distance d (e.g., the unit distance 1). For reference, see Figure 5.

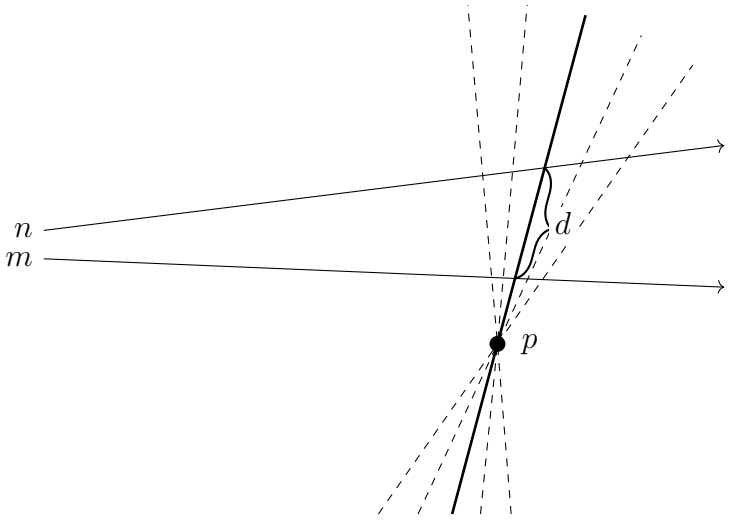


Figure 5: Neusis construction

With this additional flexibility in the construction process, we can solve the problems of angle trisection and cube duplication. Let's delve into each of these problems.

5.2 Trisecting the Angle using Neusis

Using the neusis construction, we can achieve angle trisection as follows:

Theorem 5.1 (Trisecting the Angle using Neusis)**.** *Given an acute angle $\angle AOB$ with $AO = d$, draw a line AC perpendicular to BO through A, and draw a line AE through A parallel to BO. Then, use the neusis construction to draw a line OS such that IS is twice the length of d. The line OS trisects $\angle AOB$.*

Proof. Let $\angle SOB = t$. Thus, $\angle ASO = t$ as well. Since $\angle CAS$ is a right angle, A lies on a circle centered at M with radius d. Therefore, $\triangle AMO$ and $\triangle AMS$ are both isosceles triangles. By the Exterior Angle Theorem, since $\angle MAS = t$, it follows that $\angle OMA = 2t$ and $\angle AOM = 2t$. Consequently, OM trisects $\angle AOB$. See figure 6 for reference. □

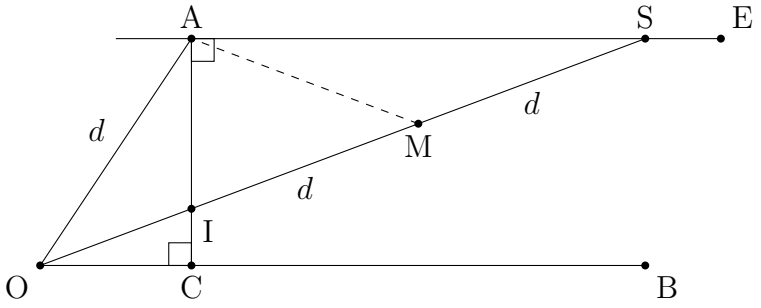


Figure 6: Construction for trisecting the angle, due to Pappus

5.3 Doubling the Cube using Neusis

Another classical problem is doubling the volume of a cube. Using the neusis construction, we can find a solution:

Theorem 5.2 (Doubling the Cube using Neusis)**.** *Let the isosceles triangle $\triangle ABC$ have sides $1, 1, k/4$ such that $AB = k/4$. Extend AD from AC by the same length. Extend AB to AE and DB to DF, and use the neusis construction to draw a line CI intersecting DF at P such that $PI = 1$. Then $BI = k^{1/3}$.*

Proof. Let the parallel to AE through C intersect DB at O. The triangles $\triangle ADB$ and $\triangle CDO$ are similar. Since $CD = 2AD$, we have $CO = 2AB = k/2$. Additionally,

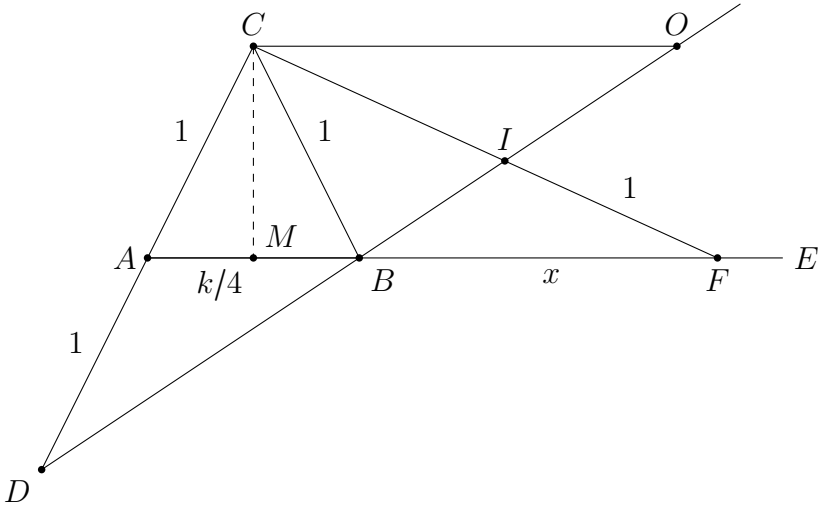


Figure 7: Construction for Cube root, due to Nicomedes

the triangles $\triangle CIO$ and $\triangle FIB$ are similar, leading to

$$\frac{CO}{CI} = \frac{BF}{IF} \iff \frac{k/2}{CI} = \frac{x}{1} \iff CI = \frac{k}{2x}.$$

Let M be the midpoint of AB, and $CM = \sqrt{1^2 - (k/2)^2}$. By the Pythagorean Theorem,

$$\begin{aligned}(CI + IF)^2 &= (CM)^2 + (MF)^2 \\ (k/2x + 1)^2 &= (1^2 - (k/8)^2) + (k/8 + x)^2,\end{aligned}$$

which simplifies to the polynomial $4x^4 - kx^3 + 4kx + k^2 = 0$. Factoring this yields $(4x + k)(x^3 - k) = 0$. Since $4x + k > 0$, we must have $(x^3 - k) = 0$, giving us $x = \sqrt[3]{k}$. See Figure 7 for reference. □

References

G.E. Martin. *Geometric Constructions*. Undergraduate Texts in Mathematics. Springer New York, 1997. ISBN 9780387982762. URL https://books.google.se/books?id=ABLtD3IE_RQC.

D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004. ISBN 9780471452348. URL https://books.google.se/books?id=QkAxJgAACAAJ.