Geometrical Constructions

Tanveer Sabir  Aamir Muneer
Tanveer Sabir Aamir Muneer

Trisecting the Angle, Doubling the Cube, Squaring the Circle and Construction of n-gons

Master thesis

Mathematics

2009
Abstract

In this thesis, we are dealing with following four problems
(i) Trisecting the angle;
(ii) Doubling the cube;
(iii) Squaring the circle;
(iv) Construction of all regular polygons;
With the help of field extensions, a part of the theory of abstract algebra, these problems seems to be impossible by using unmarked ruler and compass. 
First two problems, trisecting the angle and doubling the cube are solved by using marked ruler and compass, because when we use marked ruler more points are possible to construct and with the help of these points more figures are possible to construct.
The problems, squaring the circle and Construction of all regular polygons are still impossible to solve.
Key-words:
Acknowledgments

We are obliged to our supervisor Per-Anders Svensson for accepting and giving us chance to do our thesis under his kind supervision. We are also thankful to our Programme Manager Marcus Nilsson for his work that set up a road map for us. We wish to thank Astrid Hilbert for being in Växjö and teaching us, She is really a cool, calm and knowledgeable, as an educator should. We also want to thank of our head of department and teachers who time to time supported in different subjects. We are also expressing our deepest gratitude to our parents and elders who supported and encouraged us during our study. At the end we are very much thankful to Swedish Government for providing the great opportunity by granting the permission to stay and study in Sweden.
Contents

1 Introduction 1
   1.1 Four Major Mathematical Problems 1
   1.2 Straightedge and Compass Constructions 2
   1.3 Impossibility of the Constructions 2

2 Preliminaries 3
   2.1 Fields and Vector Spaces 3
   2.2 Polynomials 6

3 Algebraic Numbers and Their Polynomials 9
   3.1 Algebraic Numbers 9
   3.2 Monic Polynomials 10
   3.3 Monic Polynomials of least Degree 10

4 Extending Fields 12
   4.1 An Illustration: $\mathbb{Q}(\sqrt{3})$ 12
   4.2 Construction of $G(\beta)$ 14
   4.3 Iterating the construction 18
   4.4 Towers of Fields 19

5 Irreducible Polynomials 21
   5.1 Irreducible Polynomials 21
   5.2 Reducible Polynomials and zeros 21
   5.3 Finite-dimensional Extensions 23

6 Compass and Unmarked Ruler Constructions 24
   6.1 Unmarked Ruler and Compass Constructions 24
   6.2 Products, Quotients, Square Roots 28
   6.3 Rules for Unmarked Ruler and Compass Constructions 30
   6.4 Constructible Numbers and Fields 33

7 Proofs of the Impossibilities 36
   7.1 Proving the "All constructibles Come From Square Roots"Theorem 36
   7.2 The Three Constructions are Impossible 39
   7.3 Construction of Regular Polygons with unmarked ruler and compass 41
   7.4 Algebraic description of the set of all numbers that are constructible with marked ruler and compass 42

References 54
1 Introduction

In this dissertation, four of the oldest problems in mathematics have been discussed which arose about 2,000 years ago. These problems are: (1) Trisecting an arbitrary angle; (2) Doubling the cube (duplicating the cube); (3) Squaring the circle (quadrature of the circle); (4) Constructing the regular polygon; Problem 1 describes how every angle can be trisected. Problem 2 is about constructing a cube having twice the volume of a given cube. Problem 3 is that of constructing a square whose area is equal to that of a given circle. The last construction problem is that of subdividing the circumference of a circle in \( n \) equal parts.

In all cases, the construction is to be carried out using only a ruler and a compass. The origins of Problem 1 are obscure. The Greeks were concerned with the problem of constructing regular polygons, and it is likely that the trisection problem arose in this context. This is so because the construction of a regular polygon with nine sides necessitates the trisection of an angle.

The dissertation has been divided into seven sections. The first section deals with the literature review of the four major ancient mathematical problems. The section two is about the preliminaries. Third section is about Algebraic Numbers and Their Polynomials. Forth section explains extending fields. In the fifth section, Irreducible Polynomials have been discussed. Sixth section deals with Compass and Unmarked ruler Constructions. The last section shows the results and proofs of the Impossibilities.

1.1 Four Major Mathematical Problems

Reference to Problem 1 occurs in the following ancient document supposedly written by Eratosthenes to King Ptolemy III about the year 240 B.C.: To King Ptolemy, Eratosthenes sends greetings. It is said that one of the ancient tragic poets represented Minos as preparing a tomb for Glaucus and as declaring, when he learnt it was a hundred feet each way: "Small indeed is the tomb thou hast chosen for a royal burial. Let it be double (in volume). And thou shalt not miss that fair from if thou quickly doublest each side of the tomb." But he was wrong. For when the sides are doubled, the surface(area)becomes four times as big, and the volume eight times. It became a subject of inquiry among geometers in what manner one might double the given volum without changing the shape. And this problem was called the duplication of the cube, for given a cube they sought to double it. The history of Problem 3 is linked to that of calculating the area of a circle. Information about this is contained in the Rhind Papyrus, perhaps the best known ancient mathematical manuscript, which was brought by A.H. Rhind to the British Museum in the nineteenth century. The manuscript was copied by the scribe Ahmes about 1650 B.C. from an even older work. It states that the area of a circle is equal to that of a square whose side is the diameter diminished by one ninth; that is,

\[
A = \left(\frac{8}{9}\right)^2 d^2
\]

Comparing this with the formula

\[
A = \pi r^2 = \pi \frac{d^2}{4}
\]

gives

\[
\pi = 4 \left(\frac{8}{9}\right)^2 = \frac{256}{81} = 3.1604\cdots
\]
The Papyrus does not show any explanation of how this formula was obtained. Nearly fifteen centuries later, Archimedes showed the following inequalities \(\frac{223}{71} < \pi < \frac{22}{7} = 3\frac{1}{7} \).

Many renowned mathematicians have been trying to tackle these problems. Amateur mathematicians also found these problems fascinating. In the period of the 1, a Greeks word to describe people who tried to solve Problem 3 "tetragonidzein" which means to occupy oneself with the quadrature. The Paris Academy, in 1775, advised their amateur mathematicians not to waste their time on these unsolved problems. They made a law that no more time would be taken to find out solutions for the problems of doubling the cube, trisecting an arbitrary angle, and squaring the circle and that the same resolution should apply to machines for exhibiting perpetual motion. These problems were, at last, solved in the nineteenth century. In 1837, Wantzel found the solution of problems 1 and 2, in 1882, Lindemann solved Problem 3.

Another problem about the circle is the problem of dividing a circle into equal arcs. Joining the successive points of division by chords produces a regular polygon. The Greeks could easily construct some regular polygon, but wanted to know whether it was possible to construct all regular \(n\)-gons with compass and straightedge. If not, which \(n\)-gons are constructible and which are not?

In 1796, Carl Friedrich Gauss found a way for the constructibility of the regular 17-gon. A few years later, he presented the theory of Gaussian periods in his Disquisitiones Arithmeticae. This theory led him to formulate a enough condition for the constructibility of regular polygons: [3, Page 2]

### 1.2 Straightedge and Compass Constructions

Construction problems have been a favourite topic in geometry. With the help of a ruler and compass, a large variety of constructions is possible. A line segment can be bisected; any angle can be bisected; a line can be drawn from a given point perpendicular to a given line; etc. In all of these constructions the ruler was used only to draw lines but not for measurement. This ruler is called a straightedge. Problem 1 is to produce a construction of trisecting any given angle. Problem 2 is that of constructing a cube having twice the volume of a given cube with a compass and a straightedge. If the side of the given cube has length 1 unit, then the volume of the given cube is \(1^3 = 1\). So the volume of the larger cube should be 2, and its sides should thus have length \(\sqrt[3]{2}\). Hence the problem is reduced to that of constructing, from a segment of length 1, a segment of length \(\sqrt[3]{2}\). Problem 3 relates constructing a square of area equal to that of a given circle with compass and straightedge. If the radius of the circle is taken as one unit, the area of the circle is \(\pi\); that is, the side of the square should be \(\sqrt{\pi}\), so the problem is reduced to that of constructing, from a segment of length 1, a segment of length \(\sqrt{\pi}\).

### 1.3 Impossibility of the Constructions

Why did it take so many centuries for these problems to be solved? The reasons are (1) the required constructions are impossible, and (2) a full understanding of these problems comes not from geometry but from abstract algebra (a subject not born until the nineteenth century). In our thesis, we introduce this algebra and show how it is used to prove the impossibility of these constructions. A real number \(\alpha\) is said to be constructible if, starting from a line segment of length 1, we can construct a line segment of length \(|\alpha|\) in a finite number of steps using straightedge and compass.

A real number is constructible if and only if it can be obtained from the number 1 by successive applications of the operations of addition, subtraction, multiplication, and tak-
ing square roots. Thus, for example, the number \(3 + \sqrt{5 + 9\sqrt{3}}\) is constructible. Now \(\sqrt{2}\) does not appear to have this form. Appearances can be deceiving, however. How can we be sure? The answer turns out to be that if \(\sqrt{2}\) did have this form, then a certain vector space would have the wrong dimension! This settles Problem 1.

As for Problem 2, note that it is sufficient to give just one example of an angle which cannot be trisected. One such example is the angle of \(60^\circ\). It can be shown that this angle can be trisected only if \(\cos 20^\circ\) is a constructible number. But, the number \(\cos 20^\circ\) is solution of the cubic equation

\[
8y^3 - 6y - 1 = 0
\]

which does not factorize over the rational numbers. Hence it seems likely that cubic roots, rather than square roots, will be involved in its solution, so we would not expect \(\cos 20^\circ\) to be constructible. Once again this can be made into a rigorous proof by considering the possible dimensions of a certain vector space. Problem 3 is impossible because \(\pi\) is not an algebraic number.

2 Preliminaries

2.1 Fields and Vector Spaces

In this section we summarize the main ideas and terminology of groups, fields, rings, and vector spaces which we shall use throughout our thesis.

**Definition 2.1** (Group). A set \(F\) is said to be group under a binary operation \(+\) if it satisfies the following properties

\(a\) if for all \(a_1, a_2 \in F\) then \(a_1 + a_2 \in F\)

\(b\) if for all \(a_1, a_2, a_3 \in F\), then

\[a_1 + (a_2 + a_3) = (a_1 + a_2) + a_3\]

\(c\) there is an element \(0 \in F\) such that \(a + 0 = 0 + a = a\) for all \(a \in F\)

\(d\) for each element \(a \in F\) there exists an element \(b\) such that

\[a + b = b + a = 0\]

The element 0 is called the identity of the group \(F\) and \(b\) is called the inverse of \(a\).

The group \(F\) is said to be abelian if \(a_1 + a_2 = a_2 + a_1\) for all \(a_1, a_2 \in F\)

**Definition 2.2** (Ring). A set \(R\) is said to be ring under two binary operations \(+\) and \(\cdot\) if it satisfies the following properties

\(a\) \(R\) together with the operation \(+\) is an abelian group;

\(b\) if for all \(a_1, a_2 \in R\) then \(a_1 \cdot a_2 \in R\)

\(c\) if for all \(a_1, a_2, a_3 \in R\) then

\[a_1 \cdot (a_2 \cdot a_3) = (a_1 \cdot a_2) \cdot a_3\]

\(d\) if for all \(a_1, a_2, a_3 \in R\) then

\[a_1 \cdot (a_2 + a_3) = a_1 \cdot a_2 + a_1 \cdot a_3\]

and

\[(a_2 + a_3) \cdot a_1 = a_2 \cdot a_1 + a_3 \cdot a_1\]

Identity of \(R\) with respect to addition is denoted by 0.
Definition 2.3. A subset $F$ of a ring $(R, +)$ is said to be a subring of $R$ if $F$ is itself a ring under the same binary operations.

Thus the set $Z$ of all integers is an example of a ring, whereas the set $N$ of all natural numbers is not a ring.

Definition 2.4 (Field). A field is a set $F$ together with two operations, usually called addition and multiplication, and denoted by $+$ and $\cdot$, respectively, such that the following axioms hold:

(i) For all $a, b \in F$, both $a + b$ and $a \cdot b$ are in $F$.

(ii) For all $a, b, c \in F$, the following equalities hold:

$$a + (b + c) = (a + b) + c$$

and

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) For all $a, b \in F$ the following equalities hold: $a + b = b + a$ and $a \cdot b = b \cdot a$.

(iv) There exists an element of $F$, called the additive identity element and denoted by 0, such that for all $a \in F$, $a + 0 = a$. Likewise, there is an element, called the multiplicative identity element and denoted by 1, such that for all $a \in F$, $a \cdot 1 = a$.

(v) For every $a \in F$, there exists an element $-a \in F$, such that $a + (-a) = 0$. Similarly, for any $a \in F$ other than 0, there exists an element $a^{-1} \in F$, such that $a \cdot a^{-1} = 1$.

(vi) For all $a, b, c \in F$, the following equality holds:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Example 2.1. The set of rational number $Q$ is an example of a field.

Example 2.2. If $M$ is the set of all $2 \times 2$ matrices with entries from $R$, then $M$ is a ring with the ring operations being matrix addition and matrix multiplication. However, $M$ is not a field since if

$$A = \begin{pmatrix} 6 & 9 \\ -4 & -6 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 1 & 2 \\ -1 & 0 \end{pmatrix}$$

then

$$AB = \begin{pmatrix} -3 & 12 \\ 2 & -8 \end{pmatrix} \neq BA = \begin{pmatrix} -2 & -3 \\ -6 & -9 \end{pmatrix}$$

Also note that this ring $M$ has zero-divisors, for example, if

$$C = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

$$D = \begin{pmatrix} 0 & 0 \\ 8 & 9 \end{pmatrix}$$

then

$$CD = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

[6, Page 464]
**Theorem 2.1.** $Q$ is the smallest subfield of set of complex numbers $C$.

**Proof.** For this we have to prove that if $M$ is any subfield of $C$ then $Q \subseteq M$. So we let $M$ be any subfield of $C$. To show that $Q \subseteq M$ we shall show that If $y \in Q$ then $y \in M$. Let $y \in Q$; that is, $y = \frac{a}{b}$, where $a, b$ are integers and $b \neq 0$. We have to prove that $y \in M$. To prove this we use the field properties of $M$. As $M$ is a field, multiplicative identity 1 must be in $M$. Therefore each positive integer is in $M$, as closure property holds in $M$ with respect to addition. Also each negative integer is in $M$, as $M$ is closed under subtraction. Also 0 $\in M$ as $M$ is a field. Hence the integers $a$ and $b$ are in $M$. Since $M$ is closed under division and $b \neq 0$, the quotient $a/b \in M$. So $y \in M$, as required.

There are lots of fields which lie between $Q$ and $C$. Also not all fields are subfields of $C$. To see this, consider the following.

$$Z_m = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 \cdots, m - 1\}$$

Where $m$ is any prime. We define addition of elements $c$ and $d$ in $Z_m$ by

$$c \oplus_m d = c + d \mod m$$

that is, add $c$ and $d$ in the usual way and then subtract multiples of $m$ until the answer lies in the set $Z_m$. We define multiplication similarly:

$$c \otimes_m d = c \cdot d \mod m$$

**Definition 2.5** (Vector Space). A set $V$ together with a field $M$ is said to be *vector space* under two operations $+$ and $\cdot$ over the field $M$ if it satisfies the following properties

(i) $V$ together with the operation $+$ is an abelian group;
(ii) If $a \in M$ and $v \in V$, then $a.v \in V$;
(iii) if $a_1, a_2 \in M$ and $v \in V$ then $(a_1 + a_2).v = a_1.v + a_2.v$;
(iv) if $v_1, v_2 \in V$ and $a \in M$ then $a.(v_1 + v_2) = a.v_1 + a.v_2$;
(v) if 1 is the multiplicative identity of $M$, then $1.v = v$ for all $v \in V$;
(vi) if $a_1, a_2 \in M$ and $v \in V$, then

$$(a_1a_2).v = a_1(a_2.v)$$
2.2 Polynomials

The most simplest way of describing a polynomial is to say that it is an "expression" of the form

\[ b_0 + b_1 y + b_2 y^2 + \cdots + b_m y^m \]

The coefficients \( b_0, b_1, \cdots, b_m \) are in any ring \( R \). The above expression is then called a \textit{polynomial} over the ring \( R \). There are, in fact, two distinct ways of interpreting this symbol. One of these ways leads to the concept of a polynomial form, the other to that of a polynomial function.

**Polynomial Forms** To arrive at the concept of a polynomial form, we say as little as possible about the symbol \( y \). We regard \( y \) and its various powers as simply performing the role of "makers" to indicate the position of the various coefficients in the expression.

For example, we have two polynomials

\[ 4 + 5y + 3y^5 \]

and

\[ 5y + 4 + 3y^5 \]

these two polynomials are equal because in each expression the coefficients of the same powers of \( y \) are equal. When we add two polynomials, for example

\[ (5 + 7y + 5y^2) + (5 + 3y^2) = 10 + 7y + 8y^2 \]

powers of \( y \) simply inform us which coefficients to add, although more complicated, role when we multiply two polynomials. Although \( y \) is regarded as obeying the same algebraic rules as the elements of the ring \( R \), we do not think of it as assuming values from \( R \). For this reason it is called an \textit{indeterminate}.

**Definition 2.6.** Suppose we are given a polynomial \( b_0 + b_1 y + b_2 y^2 + \cdots + b_m y^m \) with coefficient \( b_m \neq 0 \), then we can say the polynomial has degree \( m \). If all the coefficients are zero, we say that the polynomial is the \textit{zero polynomial} and leave its degree undefined. When we do not wish to state the coefficients explicitly we shall use symbols like \( g(y), h(y), k(y) \) to denote polynomials in \( y \). The degree of a nonzero polynomial \( g(y) \) is denoted by

\[ \deg g(y) \]

If in the above polynomial form \( b_n \neq 0 \), we call \( b_n \) the \textit{leading coefficient}. The collection of all polynomials over the ring \( R \) in the indeterminate \( y \) will be denoted by \( R[y] \).

**Polynomial Functions.** Suppose we have a polynomial \( b_0 + b_1 y + b_2 y^2 + \cdots + b_m y^m \). An alternative way to regard the symbol "\( y \)" is as a variable standing for a typical element of the ring \( R \). Thus the expression \( b_0 + b_1 y + b_2 y^2 + \cdots + b_m y^m \) may be used to assign to each element \( y \in R \) another element in \( R \). In this way we get a function \( f : R \longrightarrow R \) with values assigned by the formula

\[ f(y) = a_0 + a_1 y + a_2 y^2 + \cdots + a_n y^n \]  \hspace{1cm} (2.1)

Such a function \( f \) is called a \textit{polynomial function} on the ring \( R \). Thus if we regard polynomials as functions, emphasis shifts from the coefficients to the values of the function. In particular, equality of two polynomial functions \( f : R \longrightarrow R \) and \( g : R \longrightarrow R \) means that

\[ f(y) = g(y) \]
for all $y \in R$ which is just the standard definition of equality for functions. Clearly each polynomial form $f(y)$ determines a unique polynomial function $f : \mathbb{R} \rightarrow \mathbb{R}$ (because we can read off the coefficients from $f(y)$ and use them to generate the values of $f$ via the formula (1)).

**Example 2.3.** Let $g(y)$ and $h(y)$ be the polynomial forms over the ring $\mathbb{Z}_4$ given by $g(y) = 2y$ and $h(y) = 2y^2$. These two polynomial forms are different, yet they determine the same polynomial function.

**Proof.** These polynomial forms determine functions $g : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ and $h : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ with values given by

$$g(y) = 2y \text{ and } h(y) = 2y^2$$

Hence calculation in $\mathbb{Z}_4$ shows that

$$
\begin{align*}
g(0) &= 0 = h(0) \\
g(1) &= 2 = h(1) \\
g(2) &= 0 = h(2) \\
g(3) &= 2 = h(3)
\end{align*}
$$

So

$$g(y) = h(y)$$

for all $y \in \mathbb{Z}_4$. Thus the functions $g$ and $h$ are equal.

We have produced an example of a ring $R$ and two polynomial forms $g(y), h(y) \in R[y]$ such that $g(y) \neq h(y)$ and yet $g = h$. The only rings which are relevant to our geometrical construction problems are those which are subfields of the complex number field, $\mathbb{C}$. For such rings it can be shown that the above phenomenon cannot occur and we get a one-to-one correspondence

$$g(y) \leftrightarrow g$$

between polynomial forms $g(y) \in R[y]$ and polynomial functions

$$g : R \rightarrow R$$
The Rational Roots Test This simple test has great importance in mathematics. It will enable us to prove very easily that certain numbers, such as $\sqrt{5}$, $\sqrt{7}$ and $\sqrt{11} + \sqrt{2}$ are irrational. The test illustrates how we use polynomials to the study the numbers. A zero of a polynomial $g(y)$ is a number $\alpha$ such that $g(\alpha) = 0$. The test works by narrowing down to a short list the possible zeros in $Q$ of a polynomial in $Q[y]$. A preliminary observation is that every polynomial in $Q[y]$ can be written as a rational multiple of a polynomial in $Z[y]$. This is achieved by multiplying the given polynomial in $Q[y]$ by a suitable integer. For example

$$1 + \frac{1}{2}y + \frac{3}{8}y^2 + \frac{1}{64}y^3 = \frac{1}{64} (64 + 32y + 24y^2 + y^3)$$

In looking for zeros in $Q$ of polynomials in $Q[y]$ we may as well, therefore, look for zeros in $Q$ of polynomials in $Z[y]$. The Rational Roots Test uses some terminology which we now record. By saying that an integer $a$ is a factor of an integer $b$, we mean that there is an integer $n$ such that $b = na$. By saying that a rational number $\alpha$ is expressed in lowest terms by

$$\alpha = \frac{s}{r}$$

we mean that $r$ and $s$ are in $Z$ with $r \neq 0$ and $r$ and $s$ have no common factors except 1 and $-1$.

Theorem 2.2 (Rational Roots Test). Let $g(y) \in Z[y]$ be a polynomial of degree $m$ so that

$$g(y) = b_0 + b_1y + \cdots + b_my^m$$

for some $b_0, b_1, b_2, \cdots, b_m \in Z$ with $b_m \neq 0$. If $\alpha$ is a rational number, written in its lowest terms as $\alpha = \frac{s}{r}$ and $\alpha$ is a zero of $g(y)$ then

(i) $s$ is a factor of $b_0$

(ii) $r$ is a factor of $b_m$.

Proof. Suppose $g(\alpha) = 0$ so that

$$b_0 + b_1\left(\frac{s}{r}\right) + b_2\left(\frac{s}{r}\right)^2 + \cdots + b_m\left(\frac{s}{r}\right)^m = 0$$

and hence

$$b_0r^m + b_1sr^{m-1} + b_2s^2r^{m-2} + \cdots + b_ms^m = 0$$

This gives

$$b_0r^m = -s (b_1r^{m-1} + b_2sr^{m-2} + \cdots + b_ms^{m-1})$$

so that $s$ is a factor of $b_0r^m$. But since $s$ and $r$ have no common factors except 1 and $-1$, there can be no common prime numbers in the prime factorizations of $s$ and $r$. This implies that $s$ is a factor of $b_0$. Similarly on writing

$$b_ms^m = -r (b_0r^{m-1} + b_1sr^{m-2} + \cdots + b_{m-1}s^{m-1})$$

We see that $r$ is a factor of $b_ms^m$ and therefore $r$ is a factor of $b_m$. \hfill \square

Example 2.4. The real number $\sqrt{3}$ irrational.

Proof. As $\sqrt{3}$ is a zero of the polynomial $3 - X^2$ in $Q[y]$. This polynomial also lies in $Z[y]$, and hence we can use the Rational Roots Test to see if it has a zero in $Q$. Let $\frac{s}{r}$ is a zero of $3 - X^2$, where $r, s \in Z$ with $r \neq 0$ is expressed in lowest terms. By the Rational Roots Test, $s$ is a factor of 3 and $r$ is a factor of $-1$. This means that only possible values of $s$ are 1, $-1$, 3 and $-3$ while the only possible values of $r$ are 1 and $-1$. Hence $\frac{s}{r}$ must be 1, $-1$, 3 and $-3$. This means that $\pm 1$ and $\pm 3$ are the only possible zeros in $Q$. Substitutions shows, however, that none of $\pm 1$ and $\pm 3$ is a zero of $3 - X^2$. Hence $\sqrt{3}$, being a zero, is not in $Q$. \hfill \square
3 Algebraic Numbers and Their Polynomials

3.1 Algebraic Numbers

Numbers which lie in \( \mathbb{R} \) but not in \( \mathbb{Q} \) are said to be irrational. Some famous examples are \( \sqrt{2} \), \( e \), and \( \pi \). Ancient Greeks proved that \( \sqrt{2} \) is not rational whereas that of \( e \) and \( \pi \) was proved much later. Although these three numbers are all irrational, there is a fundamental distinction between \( \sqrt{2} \) and the other two numbers. While \( \sqrt{2} \) satisfies a polynomial equation

\[
y^2 - 2 = 0
\]

with coefficients in \( \mathbb{Q} \), no such equation is satisfied by \( e \) or \( \pi \). For this reason \( \sqrt{2} \) is said to be an algebraic number over \( \mathbb{Q} \) whereas \( e \) and \( \pi \) are said to be transcendental numbers over \( \mathbb{Q} \).

**Definition 3.1.** A number \( \beta \in \mathbb{C} \) is said to be algebraic over a field \( G \subseteq \mathbb{C} \) if there exist a nonzero polynomial \( g(y) \in G[y] \) such that \( \beta \) is a zero of \( g(y) \); that is there is a

\[
f(y) = b_0 + b_1y + \cdots + b_my^m
\]

where \( b_0, b_1, \cdots, b_m \) are in \( G \), at least one of \( b_i \neq 0 \) such that

\[
g(\beta) = 0.
\]

For each field \( G \), every number \( \beta \) in \( G \) is algebraic over \( G \) because \( \beta \) is a zero of the polynomial \( y - \beta \in G[y] \) This shows that \( e \) and \( \pi \) are algebraic over \( \mathbb{R} \) even though they are transcendental over \( \mathbb{Q} \).

**Example 3.1.** (a) The number \( \sqrt{3} \) is algebraic over \( \mathbb{Q} \) as it is a zero of the polynomial \( y^2 - 3 \), which is nonzero and its coefficients belong to \( \mathbb{Q} \).

(b) The number \( \sqrt[4]{5} \) is algebraic over \( \mathbb{Q} \) because it is a zero of the polynomial \( y^4 - 5 \), its coefficients are in \( \mathbb{Q} \).

**Example 3.2.** The real number \( 1 + \sqrt{2} \) is algebraic over \( \mathbb{Q} \)

**Proof.** Let \( \beta = 1 + \sqrt{2} \). We want to find a polynomial, with \( \beta \) as a zero, which has coefficients in \( \mathbb{Q} \). Squaring \( \beta \) yields

\[
\beta^2 = 1 + 2\sqrt{2} + 2
\]

After some more calculation we get

\[
\beta^2 - 1 = \sqrt{2}.
\]

Then squaring both sides \((\beta^2 - 1)^2 = 2\) yields

\[
\beta^4 - 2\beta^2 - 1 = 0
\]

So we can say that \( \beta \) is a zero of the polynomial \( y^4 - 2y^2 - 1 \), which is nonzero and has coefficients in \( \mathbb{Q} \). Hence \( \beta \) is algebraic over \( \mathbb{Q} \).
3.2 Monic Polynomials

We know that algebraic number such as \( \sqrt{5} \) can be satisfied of many different polynomials \( i.e \) it is a zero of many polynomials. Ultimately we need to take from all these polynomials one which is, in some sense, the best. Here we make a start in this direction by restricting attention to monic polynomials, defined as follows:

**Definition 3.2.** A polynomial 
\[
g(y) = b_0 + b_1 y + \cdots + b_n y^n
\]
in \( G[y] \) is said to be monic if its leading coefficient \( b_n \) is 1.

For example \( y^2 - 3 \) is a monic polynomial where as \( 2y^2 - 6 \) is not monic. Note that both these polynomials have \( \sqrt{3} \) as a zero and, for our purposes, the polynomial \( y^2 - 3 \) is some what nicer than \( 2y^2 - 6 \).

**Proposition.** If a complex number \( \beta \) is a zero of a nonzero polynomial \( g(y) \in G(y) \) then \( \beta \) is a zero of a monic polynomial \( h(y) \in G[y] \) with
\[
\deg h(y) = \deg g(y)
\]

*Proof.* Assume that \( \beta \) is a zero of a polynomial \( g(y) \neq 0 \). Since \( g(y) \neq 0 \), some coefficient must be nonzero and (because there are only finitely many coefficient \( b_i \) there must be a largest \( i \) such that \( b_i \neq 0 \). Let \( m \) be the largest such \( i \). Hence
\[
g(y) = b_0 + b_1 y + b_2 y^2 + \cdots + b_m y^m
\]
where \( b_m \neq 0 \). We choose
\[
h(y) = \frac{1}{b_m} g(y).
\]
Thus \( h(y) \) is monic, has \( \beta \) as a zero and the same degree \( m \) as \( g(y) \). All the coefficients of \( h(y) \) are in \( G \), moreover, since \( G \) is a field.

\[ \square \]

3.3 Monic Polynomials of least Degree

Even if we study monic polynomials, we see that there are still a lot of polynomials which have \( \sqrt{2} \) as a zero. For example, \( \sqrt{2} \) is a zero of each of the following polynomials
\[
y^2 - 2, y^4 - 4, (y^2 - 2)^2, (y^2 - 2)(y^5 + 3), (y^2 - 2)(y^{100} + 84y^3 + 73),
\]
all of which belong to \( Q(y) \). What distinguishes \( y^2 - 2 \) from the remaining polynomials is that it has the least degree.

**Proposition.** If \( \beta \in \mathbb{C} \) is algebraic over a field \( G \subseteq \mathbb{C} \) then among all monic polynomials \( g(y) \in G[y] \) with \( g(\beta) = 0 \) there is a unique one of least degree.
Proof. Since $\beta$ is algebraic, there is a monic polynomial $g(y) \in G[y]$ with $g(\beta) = 0$. Hence there is one such polynomial of least possible degree. To prove that only one such polynomial exist, suppose there are two of them, say $g_1(y)$ and $g_2(y)$, each having the least degree $m$, say. Thus

$$g_1(y) = b_0 + b_1y + b_2y^2 + \cdots + b_{n-1}y^{m-1} + y^m$$

$$g_2(y) = c_0 + c_1y + c_2y^2 + \cdots + c_{n-1}y^{m-1} + y^m$$

Hence if we put $g(y) = g_1(y) - g_2(y)$ we get

$$g(y) = d_0 + d_1y + \cdots + d_{m-1}y^{m-1}$$

we want to prove that $g_1(y) = g_2(y)$ to do this we show that $g(y) = 0$

Clearly $g(y) \in G[y], g(\beta) = 0$ and either $g(y)$ is zero or $g(y)$ has degree $< n$ then there is a monic polynomial which has the same degree as $g(y)$ and which has $\beta$ as a zero. But this is impossible since $m$ is the least degree for which there is a monic polynomial having $\beta$ as a zero. It follows that $g(y) = 0$ and hence

$$g_1(y) = g_2(y).$$

\qed

**Definition 3.3.** Let $\beta \in C$ be algebraic over a field $G \subseteq C$. The unique polynomial of least degree among those polynomials $g(y)$ in $G[y]$ satisfying

(a) $g(\beta) = 0$ and

(b) $g(y)$ is monic

is called the *minimal polynomial*. This polynomial is denoted by

$$\text{irr}(\beta, G)$$

Its degree is called the *degree of $\beta$ over $G$* and is denoted by

$$\deg(\beta, G)$$

**Example 3.3.** The minimal polynomial of $\sqrt{3}$ over $Q$ is $y^2 - 3$.

*Proof.* We see that $\sqrt{3}$ is a zero of $y^2 - 3$, moreover its coefficients are in $Q$ and it is monic. It remains to show there is no polynomial of smaller degree with these properties. If there were such a polynomial it would be $b + y$, for some $b \in Q$, then we would have $b + \sqrt{3} = 0$ so that $\sqrt{3} = -b \in Q$, a contradiction. Hence

$$\text{irr}(\sqrt{3}, Q) = y^2 - 3$$

therefore

$$\deg(\sqrt{3}, Q) = 2.$$
4 Extending Fields

4.1 An Illustration: $Q(\sqrt{3})$

If $G$ is a subfield of $C$ and $\beta$ is a complex number which is algebraic over $G$, we show how to construct a certain vector space $G(\beta)$ which contains $\beta$ and which satisfies $G \subseteq G(\beta) \subseteq C$.

This vector space is then shown to be a subfield of $C$. Thus, from the field $G$ and the number $\beta$, we have produced a larger field $G(\beta)$. Fields of the form $G(\beta)$ are essential to our analysis of the lengths of those line segments which can be constructed with straightedge and compass.

An Illustration: $Q(\sqrt{3})$

As $Q$ is a subfield of $C$, we can consider $C$ as vector space over $Q$, taking the elements of $C$ as the vectors and the elements of $Q$ as the scalars.

Definition 4.1. The set $Q(\sqrt{3}) \subseteq C$ is defined as

$$Q(\sqrt{3}) = \{ c + d\sqrt{3} : c, d \in Q \}.$$ 

Thus $Q(\sqrt{3})$ is the linear span of the set of vectors $\{1, \sqrt{3}\}$ over $Q$ and is therefore a vector subspace of $C$ over $Q$. Hence $Q(\sqrt{3})$ is a vector space over $Q$.

Theorem 4.1. The set of vectors

$$\{1, \sqrt{3}\}$$

is a basis for the vector space $Q(\sqrt{3})$ over $Q$.

Proof. This set of vectors spans $Q(\sqrt{3})$. Now we have to prove linear independence over $Q$. For this, suppose $c, d \in Q$ with

$$c + d\sqrt{3} = 0. \quad (4.1)$$

If $d \neq 0$ then

$$\sqrt{3} = -\frac{c}{d},$$

which is again in $Q$ as $Q$ is a field. This contradicts the fact that $\sqrt{3}$ is irrational; hence $d = 0$. It now follows from (4.1) that also $c = 0$. Thus (4.1) implies $c = 0$ and $d = 0$ so that the set of vectors

$$\{1, \sqrt{3}\}$$

is linearly independent over $Q$. The dimension of the vector space $Q(\sqrt{3})$ over $Q$ is 2, this being the number of vectors in the basis.

\[\square\]

Proposition. $Q(\sqrt{3})$ is a ring as it is closed under multiplication as well as addition.

Theorem 4.2. $Q(\sqrt{3})$ is a field.
Proof. To prove this subring of \( C \) is a subfield, it is sufficient to prove that it contains the multiplicative inverse of each of its nonzero elements. So let \( y \in Q(\sqrt{3}) \) be such that \( y \neq 0 \). Thus \( x = c + d\sqrt{3} \) where \( c, d \in Q \) and \( c \neq 0 \) or \( d \neq 0 \). It follows that \( c - d\sqrt{3} \neq 0 \) by the linear independence of the set \( \{1, \sqrt{3}\} \). Thus

\[
\frac{1}{y} = \frac{1}{c + d\sqrt{3}}
\]

\[
= \frac{1}{c + d\sqrt{3}} \times \frac{c - d\sqrt{3}}{c - d\sqrt{3}}
\]

\[
= \left( \frac{c}{c^2 - 3d^2} \right) + \left( \frac{-d}{c^2 - 3d^2} \right) \sqrt{3}
\]

which is again an element of \( Q(\sqrt{3}) \), since \( \frac{c}{c^2 - 3d^2} \) and \( \frac{-d}{c^2 - 3d^2} \) are both in \( Q \).

The following theorem gives a way of describing \( Q(\sqrt{3}) \) as a field with a certain property.

**Theorem 4.3.** \( Q(\sqrt{3}) \) is the smallest field containing all the numbers in the field \( Q \) and the number \( \sqrt{3} \).

**Proof.** Let \( G \) be any field containing \( Q \) and \( \sqrt{3} \). It is obvious that \( Q(\sqrt{3}) \) is a field which contains both \( Q \) and \( \sqrt{3} \). To show it is the smallest such field we shall prove that

\[
Q(\sqrt{3}) \subseteq G.
\]

To prove that \( Q(\sqrt{3}) \subseteq G \) we have to prove that if \( y \in Q(\sqrt{3}) \), then \( y \in G \). For this let \( y \in Q(\sqrt{3}) \); that is,

\[
y = c + d\sqrt{3}
\]

for some \( c, d \in Q \). Our aim is to prove that \( y \in G \). To do this we shall use the fact that \( G \) is a field. By assumption, \( \sqrt{3} \in G \). Also \( c, d \in G \) as \( G \) is assumed to contain \( Q \). Hence \( d\sqrt{3} \in G \) as \( G \) is closed under multiplication. So \( c, d\sqrt{3} \in G \) as \( G \) is closed under addition. Thus \( y \in G \), as required. Because \( Q(\sqrt{3}) \) is field, the theory developed in Chapter 2 for a field \( G \subseteq C \) can now be applied in the case

\[
G = Q(\sqrt{3})
\]

**Example 4.1.** The real number \( \sqrt{7} \) is algebraic over \( Q(\sqrt{5}) \) and has degree 2 over this field.

**Proof.** The polynomial \( y^2 - 7 \) has coefficients in \( Q \), and hence also in \( Q(\sqrt{5}) \). It is monic, moreover, and has \( \sqrt{7} \) as a zero. Hence \( \sqrt{7} \) is algebraic over \( Q(\sqrt{5}) \). Suppose \( y^2 - 7 \) is not the minimal polynomial of \( \sqrt{7} \) over \( Q(\sqrt{5}) \). Then the minimal polynomial is a monic first degree polynomial \( a + y \) for some \( a \in Q(\sqrt{5}) \). Hence

\[
a + \sqrt{7} = 0
\]

13
and $\sqrt{7} = -a$, which implies

$$\sqrt{7} = e + f\sqrt{5}$$

for some $e, f \in Q$. Squaring both sides gives

$$7 = e^2 + 2\sqrt{5}ef + 5f^2$$

If $e = 0$ we have $5f^2 = 7$ which leads to the contradiction that $\sqrt{5}$ is rational, while if $f = 0$ we get the contradiction that $\sqrt{7}$ is rational. Hence $ef \neq 0$, which gives

$$\sqrt{5} = \frac{7 - e^2 - f^2}{2ef} \in Q$$

which is also contradiction. Thus our original assumption that $y^2 - 7$ is not the minimal polynomial of $\sqrt{7}$ over $Q\left(\sqrt{5}\right)$ has led to a contradiction. Hence $y^2 - 7$ is the minimal polynomial of $\sqrt{7}$ over $Q\left(\sqrt{5}\right)$; that is,

$$\text{Irr}\left(\sqrt{7}, Q\left(\sqrt{5}\right)\right) = y^2 - 7$$

and hence

$$\deg \left(\sqrt{7}, Q\left(\sqrt{5}\right)\right) = 2$$

\[ \square \]

### 4.2 Construction of $G(\beta)$

In the previous section we discussed vector subspace $Q\left(\sqrt{3}\right)$ of $C$ which was constructed from the field $Q$ and number $\sqrt{3}$ by putting

$$Q\left(\sqrt{3}\right) = \left\{ c + d\sqrt{3} : c, d \in Q \right\}.$$  

In this section we generalize the construction of $Q\left(\sqrt{3}\right)$ by constructing a subset $G(\beta)$ of $C$ for any subfield $G$ of $C$ and any number $\beta \in C$ which is algebraic over $G$. We begin by defining $G(\beta)$ and then showing that this set is in turn a vector subspace, a subring, and then a subfield of $C$. Our final goal is to prove that $G(\beta)$ is the smallest subfield of $C$ containing $\beta$ and all the numbers in $G$. Throughout this section, we assume that $\beta$ is algebraic over $G$.

**Definition 4.2.** Let $G$ be a subfield of $C$ and let $\beta$ be algebraic over $G$ with

$$\deg(\beta, G) = n$$

The extension of $G$ by $\beta$ is the set $G(\beta) \subseteq C$ where

$$G(\beta) = \left\{ a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1} : a_0, a_1, \cdots, a_{n-1} \in G \right\}$$

Thus $G(\beta)$ is the linear span over $G$ of the powers

$$1, \beta, \beta^2, \cdots, \beta^{n-1},$$

and so is a vector subspace of $C$ over $G$. In this section we show that $G(\beta)$ is field - indeed it is the smallest field containing $G$ and $\beta$. 

14
Theorem 4.4. The set $G(\beta)$ contains all the remaining positive powers of $\beta$:

$$\beta^n, \beta^{n+1}, \beta^{n+2}, \ldots$$

Proof. Since $n = \deg(\beta, G)$, $\beta$ is a zero of monic polynomial of degree $n$ in $G[y]$. Hence

$$a_0 + a_1 \beta + \cdots + a_{n-1} \beta^{n-1} + \beta^n = 0$$

for some coefficients

$$a_0, a_1, \ldots, a_{n-1} \in G.$$ 

Thus

$$\beta^n = -a_0 - a_1 \beta - \cdots - a_{n-1} \beta^{n-1},$$

(4.2)

And each $-a_i \in G$, as $G$ is a field. Hence, by the definition of $G(\beta)$

$$\beta^n \in G(\beta).$$

If we multiply both sides of (4.2) by $\beta$ we see that

$$\beta^{n+1} = -a_0 \beta - \cdots - a_{n-2} \beta^{n-1} - a_{n-1} \beta^n.$$  

(4.3)

Now $\beta, \ldots, \beta^{n-1}$ are all in $G(\beta)$ (by definition). We have just shown that

$$\beta^n \in G(\beta).$$

Thus, because $G(\beta)$ is a vector subspace of $C$, it follows from (4.3) that

$$\beta^{n+1} \in G(\beta)$$

Now multiply both sides of (4.2) by $\beta^2$ and then proceed in the same way, thereby showing that

$$\beta^{n+2} \in G(\beta).$$

It is clear that by proceeding in this way we can show that the powers

$$\beta^n, \beta^{n+1}, \beta^{n+2}, \ldots$$

all belong to $G(\beta)$. Thus, in our definition of $G(\beta)$ we have, in some sense, included "enough" powers of $\beta$. Have we included "too many"? An answer can be deduced from the following result.

Theorem 4.5. If $n$ is the degree of $\beta$ over $G$, then the set of vectors

$$\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}$$

is linearly independent over $G$.

Proof. Suppose on the contrary that this set is linearly dependent; so there are scalars

$$a_0, a_1, a_2, \ldots, a_{n-1} \in G$$

not all zero, such that

$$a_0 + a_1 \beta + \cdots + a_{n-1} \beta^{n-1} = 0$$
Among the coefficients
\[ a_0, a_1, a_2, \ldots, a_{n-1} \]
pick the one, say \( a_i \), farthest down the list which is nonzero. Dividing by this coefficient gives
\[
\left( \frac{a_0}{a_i} \right) + \left( \frac{a_1}{a_i} \right) \beta + \cdots + \left( \frac{a_{i-1}}{a_i} \right) \beta^{i-1} + \beta^i = 0,
\]
where \( i \leq n - 1 \), and the coefficients are still in the field \( G \). Hence \( \beta \) is a zero of a monic polynomial in \( G[y] \) with degree smaller than \( n \) (which was the least possible degree for such polynomials). This contradiction shows that our initial assumption was false. \( \square \)

**Theorem 4.6** (Basis for \( G(\beta) \) Theorem). Let \( G \) be a subfield of \( C \) and let \( \beta \in C \) be algebraic over \( G \) with
\[
\text{deg}(\beta, G) = n.
\]
Then the set of vectors
\[
\{1, \beta, \beta^2, \ldots, \beta^{n-1}\}
\]
is a basis for the vector space \( G(\beta) \) over \( G \). In particular this vector space has dimension \( n \), the degree of \( \beta \) over \( G \).

**Proof.** By definition 4.2 this set of vectors spans the vector space \( G(\beta) \) over \( G \) and, by theorem 4.5, the set of vectors is linearly independent. Hence it is a basis for the vector space and the number \( n \) of elements in the basis is the dimension of the vector space. \( \square \)

As \( G(\beta) \) is a subset of \( C \), its elements can be multiplied together. This leads to the following theorem.

**Theorem 4.7.** \( G(\beta) \) is a ring.

**Proof.** To show \( G(\beta) \) is a subring of \( C \), it is sufficient to show it is closed under addition and multiplication. The former is obvious while the latter will now be shown. Consider any two elements in \( G(\beta) \), say
\[
p = d_0 + d_1 \beta + d_2 \beta^2 + \cdots + d_{n-1} \beta^{n-1} \in G(\beta)
\]
And
\[
q = e_0 + e_1 \beta + e_2 \beta^2 + \cdots + e_{n-1} \beta^{n-1} \in G(\beta)
\]
Where the \( d' \)s and \( e' \)s belong to \( G \). If we multiply these two elements together, we get a linear combination of powers of \( \beta \), with coefficients still in the field \( G \). Because all positive powers of \( \beta \) are in \( G(\beta) \) and because \( G(\beta) \) is closed under addition and scalar multiplication, it follows that the product \( pq \) is also in \( G(\beta) \). \( \square \)

At long last we are in a position to establish that \( G(\beta) \) is a field.

**Theorem 4.8.** Let \( G \) be a subfield of \( C \) and let \( \beta \in C \) be algebraic over \( G \).Then \( G(\beta) \) is a field.

**Proof.** In view of theorem 4.7, what remains to be shown is that \( 1/\alpha \) is in \( G(\beta) \) for every nonzero \( \alpha \) in \( G(\beta) \). So let \( \alpha \) be a nonzero number in \( G(\beta) \).Firstly note that
\[
\{1, \alpha, \alpha^2, \cdots, \alpha^n\}
\]
is a set of \( n+1 \) numbers which are all in \( G(\beta) \), since \( G(\beta) \) is closed under multiplication. Because \( G(\beta) \) is an \( n - \text{dimensional} \) vector space over \( G \), this set must be linearly
dependent, which means that there are scalars $a_0, a_1, \ldots, a_k \in G$ (not all zero) with $k \leq n$ such that

$$a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + d_k \alpha^k = 0$$

(4.4)

in $G$. If $a_0 = 0$ in (4.4), we could divide by $\alpha$ (or multiply by $1/\alpha$) to reduce the number of terms in (4.4). By repeating this if necessary, we see that (4.4) can be assumed to hold with $a_0 \neq 0$. If we multiply (3) by $-1/a_0$ we have

$$-1 + c_1 \alpha + c_2 \alpha^2 + \cdots + c_k \alpha^k = 0$$

Where each

$$c_i = -a_i/a_0$$

is in $G$ since $G$ is a field. Thus

$$1 = c_1 \alpha + c_2 \alpha^2 + \cdots + c_k \alpha^k = \alpha \left( c_1 + c_2 \alpha + \cdots + c_k \alpha^{k-1} \right)$$

It follows that

$$1/\alpha = c_1 + c_2 \alpha + \cdots + c_k \alpha^{k-1}$$

which is in $G(\beta)$ since the $c_i$ and $\alpha^i$ are in $G(\beta)$ and $G(\beta)$ is a ring. □

In simple cases the method used to prove Theorem 4.8 can be used to find a formula for $1/\alpha$, as the following example shows.

**Example 4.2.** In $Q(\sqrt{2})$, if $\alpha = 1 + 2\sqrt{2}$ then $\alpha^2 = 9 + 4\sqrt{2}$ and it is easy to see that

$$\alpha^2 - 2\alpha - 7 = 0$$

This can be rewritten as

$$\alpha (\alpha - 2) = 7$$

so that

$$1/\alpha = (\alpha - 2)/7 = -1/7 + 2\sqrt{2}.$$ 

**Example 4.3.** $G(\beta^2) \subseteq G(\beta)$ for each subfield $G$ of $C$ and each $\beta \in C$.

**Proof.** Let $G$ be a subfield of $C$ and let $\beta \in C$. By the Smallest Field Theorem, $G(\beta)$ contains $\beta$ and $G$. Hence $G(\beta)$ contains

$$\beta \cdot \beta = \beta^2$$

since, being a field, $G(\beta)$ is closed under multiplication. This shows that $G(\beta)$ is a field containing $\beta^2$ and $G$. But $G(\beta)$ is the smallest such field. Therefore

$$G(\beta^2) \subseteq G(\beta)$$

as required. □
4.3 Iterating the construction

Suppose we have a field \( G \subseteq C \) and a number \( \beta \in C \) which is algebraic over \( G \). From these ingredients a new field can be constructed,

\[ G(\beta) \subseteq C. \]

We can now take the field \( G(\beta) \) and a number \( \alpha \in C \) which is algebraic over \( G(\beta) \) as the starting point for a further application of the construction process to get a further new field.

\[ G(\beta)(\alpha) \subseteq C. \]

This process can be repeated as often as we like to give a "tower" of fields, each inside the next,

\[ Q \subseteq G \subseteq G(\beta) \subseteq G(\beta)(\alpha) \subseteq G(\beta)(\alpha)(\gamma) \subseteq \cdots \subseteq C. \]

**Example 4.4.** \( Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) \) is the linear span over \( \sqrt{5} \) of the set of vectors \( \{1, \sqrt{7}\} \).

This set, furthermore, is a basis for the vector space \( Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) \) over \( Q\left(\sqrt{5}\right) \).

**Proof.** We can write,

\[ \text{irr}\left(\sqrt{7}, Q\left(\sqrt{5}\right)\right) = x^2 - 7 \]

and hence

\[ \text{deg}\left(\sqrt{7}, Q\left(\sqrt{5}\right)\right) = 2 \]

also

\[ Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) = \{a + \sqrt{7}b : a, b \in Q\left(\sqrt{5}\right)\} \]

Which is just the linear span of the set of vectors \( \{1, \sqrt{7}\} \) over \( Q\sqrt{5} \). This set of vectors forms a basis. The tower of fields

\[ Q \subseteq Q\left(\sqrt{5}\right) \subseteq Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) \]

This shows that we may consider \( Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) \) as a vector space over \( Q \) also. \( \Box \)

**Example 4.5.** \( Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) \) is the linear span \( Q \) of the set of vectors

\[ \{1, \sqrt{5}, \sqrt{7}, \sqrt{5}\sqrt{7}\} \]

**Proof.** If we use previous example

\[ Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) = \{x + \sqrt{7}y : x, y \in Q\left(\sqrt{5}\right)\} \]

\[ = \{a + b\sqrt{5} + \sqrt{7}(c + d\sqrt{5}) : a, b, c, d \in Q\} \]

\[ = \{a + b\sqrt{5} + c\sqrt{7} + d\sqrt{5}\sqrt{7} : a, b, c, d \in Q\} \]

Which expresses it as the required linear span. \( \Box \)

One might say by seeing above example that the set of vectors \( \{1, \sqrt{5}, \sqrt{7}, \sqrt{5}\sqrt{7}\} \) is in fact a basis for the vector space \( Q\left(\sqrt{5}\right)\left(\sqrt{7}\right) \) over \( Q \).
4.4 Towers of Fields

Here in this section we discuss a theorem which has importance in problems involving a tower

\[ L \subseteq M \subseteq N, \]

consisting of three distinct subfields \( L, M, \) and \( N \) of \( C \). Implicit in this set-up are three different vector spaces and the theorem to be proved will give a precise relationship between their dimensions. The three vector spaces arising from the tower are as follows. Since \( L \) is a subfield of \( M \), we may take \( M \) as the vectors and \( L \) as the scalars to give the vector space

(i) \( M \) over \( L \).

Likewise there are the vector spaces

(ii) \( N \) over \( M \), and

(iii) \( N \) over \( L \).

**Theorem 4.9** (Basis for a Tower Theorem). Consider a tower of subfields of \( C \),

\[ L \subseteq M \subseteq N. \]

If the vector space \( M \) over \( L \) has a basis

\[ \{a_1, a_2, \ldots, a_m\} \]

and the vector space \( N \) over \( M \) has a basis

\[ \{b_1, b_2, \ldots, b_n\} \]

then the set of vectors

\[ a_1b_1, a_1b_2, \ldots, a_1b_n \]
\[ a_2b_1, a_2b_2, \ldots, a_2b_n \]
\[ \ldots \]
\[ a_mb_1, a_mb_2, \ldots, a_mb_n \]

forms a basis for the vector space \( N \) over \( L \).

**Proof.** As \( L \subseteq M \subseteq N \) where \( a_j \in L, a_jb_i \in N \) and \( b_i \in N \). Firstly we show that the given set of vectors spans the vector space \( N \) over \( L \). To do this, let \( k \in N \). Our aim is to prove that \( k \) is a linear combination of the \( a_jb_i \)'s with coefficients in \( L \). Because the \( b \)'s form a basis for \( N \) over \( M \), there exist \( n \) scalars

\[ f_1, f_2, \ldots, f_n \in M \]

such that

\[ k = \sum_{i=1}^{n} f_i b_i. \quad (4.5) \]

But since the \( a \)'s form a basis for \( M \) over \( L \), there exist scalars \( e_{ij} \) (\( 1 \leq i \leq n, 1 \leq j \leq m \)) in \( L \) such that

\[ f_i = \sum_{j=i}^{m} e_{ij} a_j. \quad (4.6) \]

Substituting (4.6) in (4.5) gives

\[ k = \sum_{i=1}^{n} \left( \sum_{j=i}^{m} e_{ij} a_j \right) b_j \]
Thus the \(a_j b_i\)'s spans the vector space \(N\) over \(L\). Secondly we show that these vectors are linearly independent over \(L\). Suppose \(e_{ij}\) (\(1 \leq i \leq n, 1 \leq j \leq m\)) are elements of \(L\) such that

\[
\sum_{i=1}^{n} \sum_{j=1}^{m} e_{ij} a_j b_i = 0. \tag{4.7}
\]

our aim is to prove that all the \(e\)'s are zero. We can rewrite (4.7) as

\[
\sum_{i=1}^{n} \left( \sum_{j=1}^{m} e_{ij} a_j \right) b_i = 0.
\]

But in this sum, the coefficients of the \(b_i\)'s are elements of \(M\) and the \(b\)'s are linearly independent over \(M\). Hence, for \(1 \leq i \leq n\),

\[
\sum_{j=1}^{m} e_{ij} a_j = 0.
\]

But the \(a\)'s are linearly independent over \(L\), which means that, for \(1 \leq j \leq m\), \(e_{ij} = 0\). This establishes the required linear independence. Thus the \(a_j b_i\)'s span the vector space \(N\) over \(M\) and are linearly independent over \(L\). Hence they form a basis for the vector space \(N\) over \(L\). \(\square\)

**Example 4.6.** The vector space

\[ Q(\sqrt{5}) (\sqrt{7}) \]

over \(Q\) has the set of vectors

\[ \{ 1, \sqrt{5}, \sqrt{7}, \sqrt{5} \sqrt{7} \} \]

as basis.
5 Irreducible Polynomials

5.1 Irreducible Polynomials

Definition 5.1 (Reducible polynomial). Let $G$ be a field. A polynomial $g(y) \in G[y]$ is said to be reducible over $G$ if there are polynomials $k(y)$ and $m(y)$ in $G[y]$ such that

(a) each has degree less than that of $g(y)$, and
(b) $g(y) = k(y)m(y)$

Example 5.1. The polynomial $y^2 - 3$ is reducible over $R$.

Proof. We can write $y^2 - 3 = (y - \sqrt{3})(y + \sqrt{3})$, where each of the factors belongs to $R[y]$ and has degree less than that of $y^2 - 3$. \qed

Example 5.2. The polynomial $y^2 - 3$ is not reducible over $Q$.

Proof. To prove this, suppose, on the contrary, that $y^2 - 3$ is reducible over $Q$. This means that

$$y^2 - 3 = (by + c)(dy + e)$$

where $b, c, d, e \in Q$. Clearly neither $b$ nor $d$ can be zero. Evaluating both sides at $\sqrt{3}$ gives.

$$0 = \left( b\sqrt{3} + c \right) \left( d\sqrt{3} + e \right).$$

Hence $\sqrt{3} = -c/b$ or $-e/d$, which is contradicts that $\sqrt{3}$ is rational. Thus it is proved that $y^2 - 3$ is not reducible over $Q$. \qed

Example 5.3. Constant polynomials and polynomials of degree 1 are never reducible.

Definition 5.2. Let $G$ be a field. A polynomial $g(y) \in G[y]$ is said to be irreducible over $G$ if it is not factorized over $G$ and it is not a constant. [4, Page 277]

We can say that a polynomial is irreducible if it cannot be factorized suitably. The reason for excluding constant polynomials in this definition is that, without this exclusion certain theorems which appear later would need to be stated in a more cumbersome way. In terms of "irreducible", the examples given earlier show that $y^2 - 3$ is not irreducible over $R$, but that $y^2 - 3$ is irreducible over $Q$. Note that if a polynomial is irreducible over a field, then it is irreducible over all subfields of that field. More precisely, if $E$ is a subfield of $G$ and $g(y) \in E[y]$ is irreducible over $G$, then $g(y)$ is irreducible over $E$. Also constant polynomials are neither reducible nor irreducible; but all other polynomials are either reducible or irreducible over a given field.

5.2 Reducible Polynomials and zeros

In this section the relationship between a polynomial having a zero and being reducible will be explored. This relationship will form the basis of our technique for proving the irreducibility of certain polynomials. As a first step in this direction, the relationship between having a zero and having a factor of degree 1 will be explored.

Definition 5.3. Let $G$ be a field. A polynomial $g(y) \in G[y]$ is said to have a factor of degree 1 in $G(y)$ if

$$g(y) = (by + c)h(y)$$

Where $b, c \in G$ with $b \neq 0$ and where $h(y) \in G[y]$. 21
**Theorem 5.1** (Factor Theorem). Let $G$ be a field. A polynomial $g(y) \in G[y]$ has a factor of degree 1 in $G[y]$ if and only if $g(y)$ has a zero in $G$.

**Proof.** Assume firstly that $g(y)$ has a factor of degree 1. (definition 5.3) It follows $-c/b \in G$ is a zero of $g(y)$ since

$$g\left(-\frac{c}{b}\right) = \left(b\left(-\frac{c}{b}\right) + c\right)h\left(-\frac{c}{b}\right) = 0$$

Conversely, assume that $\beta \in G$ is a zero of $g(y)$. We want to show that $y - \beta$ is a factor of $g(y)$. If we divide $g(y)$ by $y - \beta$ then (by the Division Theorem) there exist $q(y), r(y)$ in $G[y]$ with

$$g(y) = (y - \beta)q(y) + r(y) \quad (5.1)$$

Either $r(y) = 0$ or $\deg r(y) < \deg (y - \beta) = 1$ Since $r(y) = 0$ or its degree is less than 1, $r(y)$ must be a constant polynomial $c \in G \subseteq G[y]$, which means we can rewrite (5.1) as

$$g(y) = (y - \beta)q(y) + c \quad (5.2)$$

If we substitute $y = \beta$ into this and use the fact that $g(\beta) = 0$, we have

$$0 = g(\beta) = (\beta - \beta)q(\beta) + c = 0 + c = c.$$

Thus, from (5.2),

$$g(y) = (y - \beta)q(y)$$

which means $g(y)$ has the factor $y - \beta$ of degree 1 in $G[y]$.

**Theorem 5.2** (Small Degree Irreducibility Theorem). Let $G$ be any field. Let $g(y) \in G[y]$ have degree 2 or 3. If $g(y)$ is reducible over $G$ then $g(y)$ has a zero in $G$.

**Proof.** Let $g(y) \in G[y]$ have degree 2 or 3. Assume firstly that $g(y)$ is reducible over $G$, so that

$$g(y) = k(y)h(y)$$

For some non constant polynomials $k(y), h(y) \in G[y]$. Since the degrees of $k(y)$ and $h(y)$ must add up to 2 or 3, one (or both) of these degrees must be 1. Hence, one of them must have a zero in $G$; hence $g(y)$ must also have a zero in $G$.

**Example 5.4.** The polynomial $5y^3 - 7$ is irreducible over $Q$.

**Proof.** By the Rational Roots Test the only possible zeros in $Q$ of the polynomial are

$$\pm 1, \pm \frac{1}{5}, \pm \frac{7}{5}, \pm 7$$

Among these values none gives zero when substituted into $5y^3 - 7$. Thus the polynomial has no zeros in $Q$. Since its degree is 3, the Small Degree Irreducibility Theorem is applicable and shows that $g(y)$ is irreducible over $Q$. It is important to observe that the Small Degree Irreducibility Theorem would not be true if we removed the restriction about degree 2 or 3. For example, the quartic

$$(y^2 + 1)(y^2 + 4)$$

Is reducible over $Q$ but has no zero in $Q$.

Fortunately we do not need to worry about the irreducibility of quartics (or higher degree polynomials) in order to prove the impossibility of the three famous geometri constructions.
5.3 Finite-dimensional Extensions

Suppose we have an extension field $E$ of $G$ such that the vector space $E$ over $G$ is finite-dimensional. Numbers in $E$ be algebraic over $G$ and, if so, What can we say about $\deg(\alpha, G)$? The following theorem answers these questions.

**Theorem 5.3.** Let $G$ be a subfield of a field $E$ with $[E : G] = m$. Then every number $\beta$ in $E$ is algebraic over $G$ and $\deg(\beta, G) \leq m$.

**Proof.** Let $\beta \in E$. Because $[E : G] = m$, every set of $m + 1$ numbers in $K$ must be linearly dependent over $G$. Now

$$1, \beta, \cdots, \beta^m$$

is such a set and thus there exist $a_0, a_1, a_2, \cdots, a_m \in G$, not all zero, such that $a_0 1 + a_1 \beta + \cdots + a_m \beta^m = 0$. If we let

$$P(y) = a_0 + a_1 y + \cdots + a_m \beta^m$$

then $P(y)$ is a nonzero polynomial in $G[y]$ which has $\beta$ as a zero. Thus by definition $\beta$ is algebraic over $G$. It follows $\deg(\beta, G) \leq m$ since $\deg P(y) \leq m$.

**Theorem 5.4.** Let $G$ be a subfield of a field $E$. The set of numbers in $E$ which are algebraic over $G$ is a subfield of $E$.

**Proof.** Let $\vartheta, \beta \in E$ be algebraic over $G$. We must show that $\vartheta + \beta, \vartheta - \beta, \vartheta \beta$ and provided ($\beta \neq 0$) $\vartheta / \beta$ are all algebraic over $G$. We consider the tower

$$G \subseteq G(\vartheta) \subseteq G(\vartheta)(\beta).$$

Since $\vartheta$ is algebraic over $G$, $G(\vartheta)$ is a finite-dimensional extension of $G$. Since $\beta$ is algebraic over $G$ it is also algebraic over $G(\vartheta)$ and hence $G(\vartheta)(\beta)$ is a finite dimensional extension of $G(\vartheta)$. Thus, by the Dimension for a Tower Theorem, we see that $G(\vartheta)(\beta)$ is a finite-dimensional extension of $G$ and so, every element of $G(\vartheta)(\beta)$ is algebraic over $G$. This completes the proof since $\vartheta + \beta, \vartheta - \beta$ and $\vartheta / \beta$ are all in $G(\vartheta)(\beta)$.

**Corollary 1.** The algebraic numbers are a subfield of $C$. 

---

23
6 Compass and Unmarked Ruler Constructions

In the previous discussion we used the algebraic machinery for proving that the classical geometric problems are unsolvable. In this chapter we discuss some geometry and try to show the relation between algebra and the geometry of constructions. We begin by showing how to do some basic geometrical constructions with unmarked ruler and compass, and then how to construct line segments whose lengths are products, quotients or square roots of ones already constructed. We conclude the chapter by showing that there is a connection between geometric constructions and fields of the form \( k(\sqrt{\eta}) \).

6.1 Unmarked Ruler and Compass Constructions

In this section we show how to do some basic constructions with straightedge and compass. In each of these constructions, we are given some points and some lines passing through these points. We can construct new circles and lines using the unmarked ruler and compass as described in \((i)\) and \((ii)\) below.

**Definition 6.1. type \((i)\) and \((ii)\) operation**

\( (i) \) The unmarked ruler may be used to draw a line, bisect line, trisect line and extend as far as we like, through any two points already in the figure.

\( (ii) \) The compass may be used to draw new circles in two ways.

\( (a) \) Put the compass on one point in the figure and the pencil on another such point and draw a circle.

\( (b) \) Place the compass point and pencil as in \((a)\) but then move the compass point to a third point in the figure before drawing the circle with this third point as centre.

Now we shall show how straightedge and compass are used to construct several constructions by using above two rules. These constructions will be used later as building blocks for other constructions. All compass and straightedge constructions consist of repeated application of five basic constructions using the points, lines and circles that have already been constructed. These are:

1. Creating the line through two existing points
2. Creating the circle through one point with centre at another point
3. Creating the point which is the intersection of two existing, non-parallel lines
4. Creating the one or two points in the intersection of a line and a circle (if they intersect)
5. Creating the one or two points in the intersection of two circles (if they intersect)

**Bisecting a line segment**

**Purpose.** To construct the midpoint \( O \) of a given line segment \( AB \).

**Methods.**

(i) Put the compass point on \( P \) and extend the compass until its pencil is exactly on \( Q \). Now draw an arc above \( PQ \) and another arc below \( PQ \).

(ii) Put the compass point on \( Q \) and extend the compass until its pencil is exactly on \( P \). Now draw an arc above \( PQ \) and another arc below \( PQ \). These arcs intersect previous arcs at two points. These points of intersection are said to be \( A \) and \( B \).

(iii) Join \( A \) and \( B \) with the straightedge. Then \( AB \) meets \( PQ \) at point \( O \).
where \( O \) is midpoint of line \( AB \)

**Transferring a length**

**Purpose.** Given a line segment \( OP \) and a (longer) line segment \( CD \), to construct a point \( L \) on \( CD \) such that line segment \( OP \) and \( CL \) have equal lengths.

![Figure 6.4:](image)

**Method.**

1. Put the compass point on \( O \) and extend the compass until its pencil is exactly on \( P \).
2. Put the compass point on \( C \) and with the same radius as in (i), draw an arc to cut \( CD \) at \( L \). Then \( L \) is the required point.

**Bisecting an angle.**

**Purpose.** To construct a line \( OA \) which bisects a given angle \( BOP \).

![Figure 6.5:](image)

**Method.**
(i) With centre $O$ and radius $OP$, draw an arc to meet $OB$ at $C$.
(ii) Draw arcs with centres $C$ and $P$, and radius $PA$, to meet at a point $A$. Then $OA$ bisects angle $BOP$.

**Constructing an angle of 60°**

**Purpose.** Given a line segment $AD$, to construct a line $AP$ so that angle $DAP = 60°$.

![Figure 6.6](image_url)

Figure 6.6:

**Method.**
Draw arcs with center $A$ and $D$, and radius $AD$, which meet at a point $P$. Then angle $DAP = 60°$.

**Constructing an angle of 90°**

**Purpose.** Given a line segment $OP$, to construct a line $OC$ so that angle $POC = 90°$.

**Method.**

![Figure 6.7](image_url)

Figure 6.7:

(i) With center $O$ draw an arc of radius $OP$ which meets the extended segment $PO$ at the
(ii) With centre \( P \) and radius \( AP \), draw arcs, one above the segment \( AP \) and the other below \( AP \).

(iii) At centre \( A \) and the same radius as in (ii), draw arcs to meet those in (ii) at points \( C \) and \( D \) respectively.

(iv) Join \( C \) and \( D \), using the straightedge. This line passes through \( O \) and angle \( POC = 90^\circ \).

6.2 Products, Quotients, Square Roots

Constructing a product.

Purpose. Given line segments of lengths \( a \) and \( b \), to construct a line segment of length \( ab \).

![Figure 6.8:](image)

Method

(i) Draw two lines which intersect in a single point \( X \).

(ii) On one of these lines, construct a point \( O \) such that the length of \( XO \) is \( a \).

(iii) On the other line construct a point \( U \) such that the length of \( XU \) is 1, and a point \( B \) such that the length of \( XB \) is \( b \).

(iv) Construct a line through \( B \) parallel to \( UO \) and meeting the line \( XO \), extended if necessary, at \( A \)

Result. The line segment \(XA\) has length \( ab \).

Proof. Let \( x \) be the length of \(XA\). Because the triangles \( XOU \) and \( XAB \) are similar,

\[
\frac{x}{a} = \frac{b}{1}.
\]

And so

\[
x = ab.
\]
Constructing a quotient

Purpose. Given line segments of lengths $d$ and $c \neq 0$ to construct a line segment of length $d/c$.

![Diagram](image)

Figure 6.9:

Method (i) Draw two lines which intersect in a single point $X$.
(ii) On one of these lines, construct a point $O$ such that the length of $XO$ is $d$.
(iii) On the other line construct a point $U$ such that the length of $XU$ is $c$, and a point $B$ such that the length of $XB$ is 1.
(iv) Construct a line through $B$ parallel to $UO$ and meeting $XO$ (extended, if necessary) at $A$.

Result. The line segment $XA$ has length $d/c$.

Proof. Let $x$ the length of $XA$. By similar triangles,

$$\frac{x}{d} = \frac{1}{c}.$$ 

And so

$$x = \frac{d}{c}.$$ 

Constructing square roots

Purpose. Given a line segment of length $a \geq 0$ to construct a segment of length $\sqrt{a}$.

Method

(i) Draw a line segment $CD$ of length $a$ and extend it backwards to $B$ so that $BC$ has length 1.
(ii) Bisect the line segment $BD$ and construct a semicircle with the midpoint as centre and radius half the length of $BD$.
(iii) Erect a perpendicular to $BD$ at $C$ which intersects the semicircle at a point $A$, say.

Result. The line segment $CA$ has length $\sqrt{a}$.
Proof. Let $x$ be the length of $CA$. The angle $BAD$ is a right angle, being the angle subtended by a diameter of the circle at a point on the circumference. Hence the triangles $BCA$ and $ACD$ are similar. It follows that

$$\frac{x}{a} = \frac{1}{x},$$

which gives

$$x = \sqrt{a}.$$

\[ \square \]

6.3 Rules for Unmarked Ruler and Compass Constructions

The purpose of this section is to spell out in complete detail the very precise rules which must be followed in these constructions. In each of these construction problems, a set of points is given at the start, say

$$a_0, a_1, a_2, \ldots, a_n$$

which we shall call the initial set of points for the construction. Some lines and circles may also be given. Finitely many new points

$$a_{n+1}, a_{n+2}, \ldots, a_{n+m}$$

(and extra lines and circles) may be added, using straightedge and compass, to achieve the desired result. We are not permitted to put points, lines and circles randomly on the page-rather we must base new lines and circles on points given at the start or already constructed. New points are where these lines and circles meet other lines and circles. Thus the precise rules are that, at any stage of the construction process, we may add new points (and lines and circles) to the old ones already in existence by performing an operation of one of the following two types:

Construction Rules.

(i) Draw a line which passes through two old points $Q_i$ and $Q_j$ to get new points where this line, intersects other lines and circles.
(ii) Draw a circle with centre at an old point \(Q_i\) and has radius equal to the distance between two old points \(Q_j\) and \(Q_k\) to get new points where this circle intersects other lines and circles.

Rule (i) tells us very precisely how the unmarked ruler is to be used, while rule (ii) does the same for the compass. These rules tell us the only ways we are allowed to enlarge the set of points, lines and circles. A special case, \(Q_j\) may be the same as \(Q_i\) in rule (ii). This permits us to draw a circle with centre at an old point \(Q_i\) and radius equal to the distance between \(Q_i\) and another old point \(Q_k\).

Thus rule (ii) does allow us to use the compass in the two ways 2(a) and 2(b) described at the start of this chapter. Case ii(a) is when \(Q_i = Q_j\) and ii(b) is when \(Q_i\) and \(Q_j\) are different.

**Example 6.1.** The construction "bisect a line segment".
**Proof.** The initial set of points for the construction is \( \{A, B\} \). Hence, in the notation above we may put \( Q_0 = A \) and \( Q_1 = B \). The construction proceeds by the drawing of two circles with centres \( A \) and \( B \) respectively, and radius equal to the distance between the points \( A \) and \( B \). Thus these circles are of the type permitted by rule \((\text{ii})\), and so the new points \( D \) and \( E \), being points where the circles intersect, can be obtained by two operations of type \((\text{ii})\). Hence we may put \( P_2 = D \) and \( P_3 = E \). The final stage in the construction involves drawing the line \( DE \) joining these two points to get the point \( C \) where this line intersects the line \( AB \). Hence \( C \) can be obtained by an operation of type \((\text{i})\), and so we may choose \( Q_4 = C \). The desired midpoint \( C \) has thus been obtained from the set of initial points by successive operations of the types \((\text{i})\) and \((\text{ii})\).

We conclude this section by re-examining the famous construction problems in the light of the construction rules which are used above.

**Doubling the Cube.** We are given a cube and asked to construct a cube with double the volume. We first translate this into the following equivalent problem in two dimensions. Given two points \( Q_i \) and \( Q_j \) whose distance apart is equal to one side of the original cube, we are asked to construct two points \( Q_k \) and \( Q_l \) whose distance apart is exactly \( \sqrt{2} \) times the distance between \( Q_i \) and \( Q_j \).

The question is whether or not this is possible using operations of types \((\text{i})\) and \((\text{ii})\) only.

**Squaring the Circle.** Squaring the circle means to construct square whose area is equal to that of given circle. This is equivalent to being given just two points \( Q_i \) and \( Q_j \) (distance apart equal to the radius of the circle) and being asked to construct two points \( Q_k \) and \( Q_o \) whose distance apart is exactly \( \sqrt{\pi} \) times the distance between \( Q_i \) and \( Q_j \).

As always, the question is whether or not this is possible using only finitely many operations of types \((\text{i})\) and \((\text{ii})\).

**Trisecting an Angle.** Trisecting an angle means to construct a angle which is one third the given angle. We are given the points \( Q_i, Q_o \) and \( Q_k \), which determine the angle. We are then asked to construct (using only operations of types \((\text{i})\) and \((\text{ii})\) a point \( Q_j \) such that angle \( Q_jQ_oQ_k \) is exactly one third of angle \( Q_kQ_oQ_i \).
6.4 Constructible Numbers and Fields

In analysing construction problems, it often helps to introduce a convenient unit of length. For example, in analysing the problem of doubling the cube, a convenient unit of length is the length of one side of the given cube. Doubling the cube is then possible if, given points $Q_i$ and $Q_j$ one unit apart, we can construct points $Q_k$ and $Q_l$ whose distance apart is $3\sqrt{2}$, using only operations of types (i) and (ii) definition 6.1. This leads to the following definition.

**Definition 6.2.** Let $\alpha$ be a real number with absolute value $|\alpha|$. Then $\alpha$ is said to be *constructible* if we can construct points $Q_k$ and $Q_l$ whose distance apart is $|\alpha|$ units by starting from an initial set of points $\{Q_i, Q_j\}$ whose distance apart is 1 unit and then performing a finite number of operations of types (i) and (ii). Clearly, doubling the cube is possible if and only if the number $3\sqrt{2}$ is constructible, while squaring the circle is possible if and only if $\sqrt{\pi}$ is constructible. The following two theorems and the related
discussion make it clear that the set of constructible numbers is quite large. They also mark the place where geometry and algebra begin to overlap.

**Theorem 6.1** (Field with Square Roots Theorem). The set $K$ of all constructible numbers is a subfield of $R$. Furthermore
\[(a) \text{ all rational numbers are in } K, \text{ and} \]
\[(b) \text{ if } \gamma \in K \text{ and } \gamma > 0 \text{ then } \sqrt[4]{\gamma} \in K. \]

**Proof.** Now we have to show that $K$ is a subfield of $R$; that is, the operations of addition, subtraction, multiplication and division (except by 0) can be performed without restriction in $K$. Let $\gamma$ and $\alpha$ be in $K$. Hence line segments of lengths $|\gamma|$ and $|\alpha|$ can be constructed by successive operations of types (i) and (ii) definition 6.1, starting from a segment of length 1 unit. Because we can transfer lengths, it is easy to see that segments of lengths $|\gamma + \alpha|$ and $|\gamma - \alpha|$ can be constructed from the above two segments. (If, for example, the segment $AB$ has length $\gamma$ and segment $CD$ has length $\alpha$ we can extend $AB$ and construct a point $E$ so that $BE$ has length $\alpha$ and $AE$ has the desired length $(\gamma + \alpha)$. We can also construct, using operations of types (i) and (ii), segments of lengths $|\gamma \alpha|$ and $|\gamma/\alpha|$ (if $\alpha \neq 0$), by section 6.2. Thus the numbers $\gamma + \alpha$, $\gamma - \alpha$, $\gamma \alpha$ and $\gamma/\alpha$ (if $\alpha \neq 0$) are all constructible and so are in $K$. Hence $K$ is a field. We now prove that all rational numbers are in $K$. Since we are given a segment of length 1, we can construct segments of lengths $1 + 1 = 2$, $2 + 1 = 3$ and so on, from which we see that we can construct segments of length equal to any positive integer. Hence, by section 6.2 we can construct a segment of length equal to any desired positive rational number $p/q$ (with $p, q \in N$). Because of the use of $|\alpha|$ in definition 6.1, it follows that all rational numbers (negative as well as positive) are in $K$. (Alternatively, the result that $Q \subseteq K$ follow from theorem 2.1 and the fact that $K$ is a field. Finally by section 6.2 if $\gamma \in K$ and $\gamma > 0$, then $\sqrt[4]{\gamma}$ is constructible.

By applying this theorem repeatedly we see that each of the numbers $1 + 1 = 2$, $5$, $\frac{2}{3} + \sqrt{2}$, $3 + \sqrt{\frac{2}{3} + \sqrt{2}}$, is constructible. Thus we see that every real number which is obtained from $Q$ by performing successive field operations and taking square roots is constructible. \[\Box\]

The following theorem expresses this precisely, in the notation of field extensions.

**Theorem 6.2** (Successive Square Roots Give Constructibles). A real number $\alpha$ is constructible if there exist positive real numbers
\[\alpha_1, \alpha_2, \ldots, \alpha_m\]
such that $\alpha_1 \in G_1$, where $G_1 = Q$ $\alpha_2 \in G_2$, where $G_2 = G_1(\sqrt[4]{\alpha_1}) \cdots \alpha_m \in G_m$ where $G_{m+1} = G_m(\sqrt[4]{\alpha_m})$.

There is a $Q \subseteq G_1 \subseteq G_2 \subseteq G_3 \cdots \subseteq G_m \subseteq G_{m+1}$ implicit in this theorem. This tower will play an important role in the impossibility proofs. In the following example, the fields $G_1, G_2, \ldots$ and the numbers $\alpha_1, \alpha_2, \ldots$ relevant to a particular $\alpha$ are indicated.

**Example 6.2.** Let
\[\alpha = 9\sqrt{3} + \frac{\sqrt{8 - 5\sqrt{3}}}{1 - \sqrt{3}}\]

Prove that $\alpha$ is constructible by using the “Successive Square Roots Give Constructibles” Theorem.
Proof. We must produce a positive integer \( m \) and positive real numbers 
\[ \alpha_1, \alpha_2, \ldots, \alpha_m \]
as in the statement of the "Successive Square Roots Give Constructibles" Theorem such that 
\[ \alpha \in G_{m+1} = G_m (\sqrt{\alpha_m}) \]
Put \( \alpha_1 = 3 \in G_1 \) where \( G_1 = \mathbb{Q} \),
\[ \alpha_2 = 8 - 5\sqrt{3} \]
\[ = 8 - 5\sqrt{\alpha_1} \in G_2 \]
where 
\[ G_2 = G_1 (\sqrt{\alpha_1}) \]
Hence
\[ \alpha = 9\sqrt{\alpha_1} + \frac{\sqrt{\alpha_2}}{1 - \sqrt{\alpha_1}} \in G_3 \]
where 
\[ G_3 = G_2 (\sqrt{\alpha_2}) \]
Thus we have produced positive real numbers \( \alpha_1, \alpha_2 \) which satisfy the hypothesis of the "Successive square Roots Give Constructibles" Theorem. Hence \( \alpha \) is constructible.
7 Proofs of the Impossibilities

In this chapter finally we are going to clearly illustrate about the impossibility of these classical constructions. Because after going in detailed discussion now we are able to understand the solutions of these classical problems. As we have discussed that since over two thousand years the world’s best mathematicians discussed about these classical problems but they could not find solution. About the connection of algebra with geometry we have already discussed in previous chapters. We have also discussed the constructible numbers, on which any construction is based. After knowing the notion of constructible numbers now we can find any constructible number by checking that if it is algebraic over \( \mathbb{Q} \) and its irreducible polynomial has a degree some power of 2. On behalf of this theory now we can prove that doubling the cube and trisecting the angle are impossible because there were no existence of such constructible numbers which are algebraic and whose irreducible polynomial has degree of a power of 2. We will also illustrate the impossibility of squaring the circle due to the reason that \( \pi \) is not algebraic over \( \mathbb{Q} \).

7.1 Proving the "All Construtibles Come From Square Roots" Theorem

In order to discuss the points and associated lines and circles which appear when the operations (i) and (ii) (by section 6.1) are applied, we work with the coordinates of these points. To do so, we introduce the following definitions.

Definition 7.1. Suppose that \( G \) is a subfield of \( R \).
A point is a \( G \)-point if both of its coordinates are in \( G \).
A circle is a \( G \)-circle if its centre is an \( G \)-point and its radius is the distance between two \( G \)-points. A line is a \( G \)-line if it passes through two \( G \)-points.

Example 7.1.
(i) \((3, 4)\) is a \( \mathbb{Q} \)-point, because both its coordinates belong to \( \mathbb{Q} \).
(ii) \((4, \sqrt{5})\) is a \( \mathbb{Q} \left( \sqrt{5} \right) \)-point.
(iii) \(\{(p, q) : p = q\}\) is a \( \mathbb{Q} \)-line, because it contains the two \( \mathbb{Q} \)-points \((3, 3)\) and \((5, 5)\).
(iv) \(\{(p, q) : q = \sqrt{3}p\}\) is a \( \mathbb{Q} \left( \sqrt{3} \right) \)-line but not a \( \mathbb{Q} \)-line.
(v) \(\{(r, s) : r^2 + s^2 = 4\}\) is a \( \mathbb{Q} \)-circle, because it has the \( \mathbb{Q} \)-point \((0, 0)\) as its centre while its radius is the distance between the \( \mathbb{Q} \)-points \((0, 0)\) and \((0, 2)\).
(vi) \(\{(l, m) : l^2 + m^2 = 2\}\) is a \( \mathbb{Q} \left( \sqrt{2} \right) \)-circle.

Example 7.2. The \( \mathbb{Q} \)-line \(\{(l, m) : m = l\}\) intersects the \( \mathbb{Q} \)-circle \(\{(l, m) : l^2 + m^2 = 4\}\) at the two points \(\sqrt{2}, \sqrt{2}\) and \(-\sqrt{2}, -\sqrt{2}\). These points are no \( \mathbb{Q} \)-points. However, they are \( \mathbb{Q} \left( \sqrt{2} \right) \)-points.

Remark. Assume that we are performing a construction. We have already obtained points \(q_0, q_1, \cdots, q_n\). Let \( G \) be a subfield of \( R \) containing the coordinates of all points \(q_0, q_1, \cdots, q_n\), so that these points are all \( G \)-points. If we perform an operation of type (i) or (ii) (section 6.1), we might obtain several new points \(q_{n+1}, \cdots, q_{n+t}\). The lines and circles which appear in (i) and (ii) are \( G \)-lines and \( G \)-circles, and so each of the new points obtained is at the intersection of
(1) two \( G \)-lines, or
(2) a \( G \)-line and an \( F \)-circle, or
(3) two \( G \)-circles.
Lemma 7.1. Let $G$ be a subfield of $R$.

(i) If two $G$-lines intersect in a single point, then this point is a $G$-point.
(ii) Given a $G$-line and a $G$-circle, there exists a positive number $\beta \in G$ such that the points of intersection (if any) of this line and circle are $G\left(\sqrt{\beta}\right)$-points.
(iii) Given two $G$-circles, there exists a positive number $\beta \in G$ such that any points of intersection of these two circles are $G\left(\sqrt{\beta}\right)$-points.

Proof. $G$-lines have equations of the form
\[ ax + by + c = 0 \] (7.1)
for $a, b, c$ in $G$, while $G$-circles have equations of the form
\[ x^2 + y^2 + lx + my + n = 0, \] (7.2)
for $l, m, n$ in $G$.

(i) To find where two $G$-lines meet, we solve two simultaneous equations of the form (7.1). This can be done just using field operations $+, -, \cdot, /$. So the solutions are both in $G$.

(ii) Finding where a line and a circle meet amounts to solving two equations, one of the form (7.1) and the other like (7.2). This is easily done by using the
\[ y = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \]
formula for solving the quadratic $ay^2 + by + c = 0$. Since, at worst, square roots are introduced, we obtain $F\left(\sqrt{\beta}\right)$ points for some positive $\beta \in G$.

(iii) The two $G$-circles
\[ x^2 + y^2 + a_1x + b_1y + c_1 = 0 \]
\[ x^2 + y^2 + a_2x + b_2y + c_2 = 0 \]
meet where the first of these and the $G$-line
\[ (a_1 - a_2)x + (b_1 - b_2)y + (c_1 - c_2) = 0 \]
meet. So this case follows from (ii).

With these preliminaries out of the way, we can now prove the "all constructibles come from square roots" theorem.

Theorem 7.2 (All Constructibles come from square roots). If the real number $\alpha$ is constructible, then there exist positive real numbers $\alpha_1, \alpha_2, \cdots, \alpha_n$ such that
- $\alpha_1 \in G_1$ where $G_1 = Q$.
- $\alpha_2 \in G_2$ where $G_2 = G_1\left(\sqrt{\alpha_1}\right)$
- $\vdots$
- $\alpha_n \in G_n$ where $G_n = G_{n-1}\left(\sqrt{\alpha_{n-1}}\right)$
and finally $\alpha \in G_{n+1}$ where $G_{n+1} = G_n\left(\sqrt{\alpha_n}\right)$
Proof. Suppose that \( \alpha \) is constructible so that, by the definition of constructible number, there exists a set of points

\[ q_0, q_1, q_2, \ldots, q_n \]

with \( |\alpha| \) equal to the distance between two of these points. Because the initial points \( q_0 \) and \( q_1 \) are at a distance 1 unit apart, we can introduce coordinate axes so that \( q_0 = (0, 0) \) and \( q_1 = (1, 0) \). Note that the coordinates of \( q_0 \) and \( q_1 \) are in \( Q \). Initially, the points \( q_0, q_1 \) are \( Q \)-points. Put \( G_1 = Q \). Assume that for some \( k \) satisfying \( 1 \leq k \leq n - 1 \), the points \( q_0, q_1, \ldots, q_k \) are \( G_k \)-points, where \( G_k \) is a subfield of \( R \). It follows from the construction rules that the next point \( q_{k+1} \) will be at the intersection of (1) a pair of \( G_k \)-lines, (2) a \( G_k \)-lines and a \( G_k \)-circle, (3) a pair of \( G_k \)-circles. Hence, by lemma 7.1, \( P_{k+1} \) is a \( G_{k+1} \)-point where

\[ G_{k+1} = G_k(\sqrt{\alpha_k}), \quad (7.3) \]

for some positive \( \alpha_k \) in \( G_k \). Since \( G_k \subseteq G_{k+1} \), this implies further that

\[ q_0, q_1, \ldots, q_s, q_{s+1} \]

are \( G_{k+1} \)-points. From above statement and equation (7.3), it now follows by mathematical induction on \( k \) that the numbers \( \alpha_1, \alpha_2, \ldots, \alpha_n \) are as described in this theorem. It also follows that \( |\alpha| \), being the distance between two of the points

\[ q_0, q_1, q_2, \ldots, q_n \]

(which are \( G_n \)-points), will be the square root of an element of \( G_n \). Thus for some \( \alpha_n \in G_n \) with \( \alpha_n > 0 \)

\[ \alpha \in G_n(\sqrt{\alpha_n}). \]

\[ \square \]

Example 7.3. Start from two points. \( A = (0, 0) \) and \( B = (1, 0) \), at a distance 1 apart, as in the definitions of a constructible number (Definition 6.2). Draw two circles with centres at \( A \) and \( B \) respectively, each with radius \( AB \). Then the coordinates of each of the points of intersection, \( D \) and \( C \), of the two circles involve a single square root.

Proof. The circles have equations

\[ l^2 + m^2 = 1 \quad (7.4) \]

\[ (l - 1)^2 + m^2 = 1 \quad (7.5) \]

The points of intersection satisfy both equations. Subtracting (7.4) from (7.5) gives \( l = 1/2 \) and substituting in (7.4) gives \( m = \pm \sqrt{3}/2 \). Thus the two points of intersection are \( D = \left( \frac{1}{2}, \frac{\sqrt{3}}{2} \right) \) and \( C = \left( \frac{1}{2}, -\frac{\sqrt{3}}{2} \right) \), which involve nothing worse than square root, \( \sqrt{3} \).

\[ \square \]

We now apply the "all constructibles come from square roots" theorem to show that every constructible number must be algebraic over \( Q \) and must have degree over \( Q \) which is a power of 2. This result, which is the key to the impossibility proofs, enables us to be certain that many numbers are not constructible.
Theorem 7.3 (Degree of a constructible number theorem). If a real number $\alpha$ is constructible, then $\alpha$ is algebraic over $\mathbb{Q}$ and $\deg(\alpha, \mathbb{Q}) = 2^r$ for some integer $r \geq 0$.

Proof. Let $\alpha$ be constructible and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be as in the "all constructibles come from square roots" theorem. The number $\sqrt{\alpha_i}$ is a zero of the polynomial $y^2 - \alpha_i$ which is in $G_i[y]$ since $\alpha_i \in G_i$. $\deg(\sqrt{\alpha_i}, G_i) = 1$ or $2$ and since $G_{i+1} = G_i(\sqrt{\alpha_i})$ it follows that $[G_{i+1} : G_i] = 1$ or $[G_{i+1} : G_i] = 2$ $(1 \leq i \leq n)$.

Repeated application of the dimension for a tower theorem

$$Q = G_1 \subseteq G_2 \subseteq G_3 \subseteq \cdots \subseteq G_{n+1}$$

show that

$$[G_{n+1} : Q] = [G_{n+1} : G_n][G_n : G_{n-1}] \cdots [G_2 : G_1] = 2^v,$$

for some integer $v \geq 0$. It follows from theorem (7.3) that $\alpha$ is algebraic over $\mathbb{Q}$. Also, by considering the tower

$$Q \subseteq Q(\alpha) \subseteq G_{n+1}$$

we see that $\deg(\alpha, \mathbb{Q})$ is factor of $[G_{n+1} : Q]$. □

7.2 The Three Constructions are Impossible

At long last, we are in a position to see why the old classical constructions are impossible.

Theorem 7.4. A real number $\beta \in \mathbb{R}$ is constructible if and only if there is a tower of subfields of $\mathbb{R}$.

$$Q = G_0 \subseteq G_1 \subseteq G_2 \cdots \subseteq G_m \subseteq \mathbb{R}$$

such that $\beta \in G_m$ and each

$$G_j = G_{j-1}(\sqrt{b_j})$$

for some $b_j \in G_{j-1}$. 

39
Dubling the Cube  Given the edge of the cube, it is not possible to construct with a unmarked ruler and compass the edge of the cube that has twice the volume of the original cube. Suppose the given cube has an edge of length $a$ and, therefore, a volume of $a^3$. If we could construct a cube having a volume of $2a^3$, then this new cube would have an edge of length $\sqrt[3]{2}a$. However, $\sqrt[3]{2}$ is a zero of the irreducible polynomial $y^3 - 2$ over $\mathbb{Q}$; hence,

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

This is impossible, since 3 is not a power of 2.

Problem II - Trisecting an arbitrary angle  The problem is, given an angle in the plane, to construct by ruler and compass a new angle equal to one-third of the given angle. This problem is a bit more complicated because some angles can be trisected. For example, if the given angle is a right angle, we can construct an angle equal to one-third of it. However there are some angles which cannot be trisected by unmarked ruler and compass. For example an angle of $60^\circ$ cannot be trisected by ruler and compass.

Theorem 7.5. Let $K$ be the field of constructible numbers. Then the real number

$$\beta = \cos 20^\circ$$

is not in $K$. Hence an angle of $60^\circ$ cannot be trisected by ruler and compass.

Proof. Since by the triple-angle formulas for sin and cos we find for any angle $\theta$ that

$$\cos 3\phi = 4\cos^3 \phi - 3\cos \phi$$

since $\cos 60^\circ = \frac{1}{2}$, the real number $\beta = \cos 20^\circ$ satisfies

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

In other words, $\beta$ is a root of the equation

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

We will show that this equation has no roots in $K$. Making the substitution $l = 2y$, it is sufficient to show that the equation

$$l^3 - 3l - 1 = 0$$

has no roots in $K$. First we show that it has no roots in $Q$. If it has, let the root be $b/c$ with $b, c \in \mathbb{Z}$, relatively prime. Then

$$b^3 - 3bc^2 - c^3 = 0$$

Consequently any prime factor $p$ of $b$ also divides $c$, and conversely, any prime factor of $c$ divides $b$. Since $b, c$ are relatively prime, we conclude that $b, c = \pm 1$, so $b/c = \pm 1$. But by inspection we see that neither $+1$ nor $-1$ is a root of the equation. Hence $l^3 - 3l - 1$ is an irreducible polynomial over $Q$, also it is of degree 3 with no rational roots. We conclude that $Q(\beta)$ is an extension of degree 3 of $Q$. We conclude that $\beta \notin K$, so the angle of $20^\circ$ is not constructible.
Problem III - Squaring the circle
The problem is, given a circle, to construct by ruler and compass a square of area equal to the area enclosed by the circle. If the circle has radius \( s \), its area is \( \pi s^2 \), so we need a square of side \( b \) with \( b^2 = \pi s^2 \). Thus \( b = \sqrt{\pi s} \). If \( b \) were constructible from \( s \), then \( \sqrt{\pi} \) and hence \( \pi \) would be constructible. In 1882, the problem squaring the circle was proven to be impossible, by Lindemmann Weierstrass’s theorem that proved that \( \pi \) is a transcendental, rather than an algebraic irrational number; that is, it is not the root of any polynomial with rational coefficients.

7.3 Construction of Regular Polygons with unmarked ruler and compass
Another intractable problem concerning the circle which occupied the efforts and attention of the greatest mathematicians from antiquity to the nineteenth century is the problem of dividing a circle into equal arcs. Joining the successive points of division by chords produces a regular polygon. The Greeks were able to construct a regular polygon of \( 2^n \) sides, where \( n \) is an integer greater than 1. They were also able to construct regular polygons of 3 sides and 5 sides. Since an arc of a circle can be bisected using straight edge and compass, regular polygons of \( 3 \cdot 2^n \) and \( 5 \cdot 2^n \) sides can be constructed, where \( n \) is any positive integer. Furthermore, the Greeks had proved that, if a regular polygon of \( p \) sides and one of \( q \) sides can be constructed and \( p \) and \( q \) are relatively prime, then a regular polygon of \( p \cdot q \) sides can be constructed. Since 3 and 5 are relatively prime, a regular polygon of 15 sides can be constructed, as well as regular polygons of \( 15 \cdot 2^n \) sides, where \( n \) is a positive integer. We can summarize the achievement of the Greeks by stating a general formula which indicates which regular polygons the ancient mathematicians could construct. The Greeks could construct a regular polygon of \( m \) sides if \( m \) is an integer of the form \( 2^n \cdot p_1^{r_1} \cdot p_2^{r_2} \) where \( n \) is any non-negative integer and \( p_1 \) and \( p_2 \) are the distinct primes 3 and 5, and \( r_i = 0 \) or 1. [2, Page 49]

The regular \( n \)-gons constructible with a ruler and a compass in antiquity. [1, Page 18] Values for \( n \):
- 3, 6, 12, 24, 48, 96, \ldots ,
- 4, 8, 16, 32, 64, 128, \ldots ,
- 5, 10, 20, 40, 80, 160, \ldots ,
- 15, 30, 60, 120, 240, 480, \ldots ,
For more than 2,000 years the problem of dividing a circle into equal parts remained as left by the ancient mathematicians. Despite the fact that such eminent mathematicians as Fermat and Euler worked on the problem, no further progress was made until in 1796 then nineteen year old Carl Friederich Gauss amazed the mathematical world by constructing a regular polygon with 17 sides. He did this by showing that the equation \( y^{17} - 1 = 0 \) can be reduced to a finite set of quadratic equations. So the regular polygon with 17 sides can be constructed with straightedge and compass. Gauss showed, furthermore, that a regular polygon with \( n \) sides can be constructed if and only if

\[ n = 2^r q_1 q_2 \cdots q_j \]

where \( r \geq 0 \) is an integer and \( q_1, q_2, \ldots, q_j \) are distinct Fermat primes. What if \( n \) does not have this form? The answer was provided by Pierre Wantzel in 1837, who proved that, for \( n \) not of this form, the construction of a regular polygon with \( m \) sides is impossible. Only
five Fermat primes are known: \( q_0 = 3, q_1 = 5, q_2 = 17, q_3 = 257, \) and \( q_4 = 65537 \). The next seven Fermat numbers, \( q_5 \) to \( q_{11} \), are known to be composite. Thus an \( n \)-gon is constructible if \( n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, \ldots \) while an \( n \)-gon is not constructible with compass and straightedge if

\[
n = 7, 9, 11, 13, 14, 18, 19, 21, 22, 23, 25, \ldots
\]

**Theorem 7.6.** The regular polygon of \( n \) sides is constructible by unmarked ruler and compass if and only if \( n \) is a number of the form

\[
n = 2^r p_1 p_2 \cdots p_s,
\]

where \( r, s \geq 0 \) and the \( p_i \) are distinct odd primes, each of which is a prime of the form

\[
p = 2^{2^k} + 1.
\]

[5, Page 258]

### 7.4 Algebraic description of the set of all numbers that are constructible with marked ruler and compass

In this section we are going to discuss set of all those numbers which are constructed with marked ruler and compass. We will also discuss fields, field extensions of these constructed numbers, and will relate these numbers with the roots of cubic and quartic equations. So far, we have studied the classical ruler and compass constructions of Euclid’s Elements. We have found that there are some problems that cannot be solved by ruler and compass, such as the duplication of the cube, the trisection of the angle, or construction of a regular 7-gons. Although Euclid uses only ruler and compass, other classical authors used a variety of other methods to solve more complicated problems. With the use of marked ruler, it is easy to trisect angles and extract cubic roots. Moreover, we will see that, analytically, the use of the marked ruler between lines corresponds to finding a root of a certain quartic equation. We will describe the associated field theory and show that the geometrical use of the compass and marked ruler is same to the algebraic solution of
cubic and quartic equation.
Firstly, it will be made clear what a marked ruler can do. Two marks are made on the ruler corresponding to given distance, Then the ruler is rotated along in a way that the marks come on two different lines, whereas at the same time the ruler passes through a given point. In other words, given two lines \( r, q \), given a distance \( d \), and given a point \( G \), we can draw a line \( GFE \) with \( E \in r, F \in q \) in figure 7.2, and such that \( FE = d \). This will count as one marked ruler step.

**Definition 7.2.** In the cartesian plane a point is said to be a **marked ruler point** if it lies in the last of a finite sequence \( q_1, q_2, q_3, \ldots, q_n \) of points such that each point is either in \( \{(0,0), (0,1), (1,0)\} \) or is obtained in one of two ways:

(i) As the result of intersection of two lines, such that both of them passes through two points that appear earlier in the sequence;

(ii) As either of two points that are one unit apart, that are collinear with a point that appears earlier in the sequence.

With two marked ruler points make, a marked ruler line can be constructed. A marked ruler circle is a circle through a marked ruler point with a marked ruler point as center. If \((x,0)\) is a marked ruler point then \( x \) is said to be **marked ruler number**.

**The intersection of two marked ruler lines is a marked ruler point.**
Suppose we have a ruler, we mark two points \( R \) and \( S \) on it such that distance between these two points is one unit. Now we use marked ruler such that points \( R \) and \( S \) are on different marked ruler lines and are collinear with a marked ruler point \( V = (a,b) \), then \( R \) and \( S \) are marked ruler points. Let,s look at verging algebraically, with reference to Figure 7.3, where we have verged through point \( V = (a,b) \) with respect to the lines with equations \( Y = mX \) and \( Y = 0 \). Now \( R \) and \( S \) have coordinates \( R = (x_1,y_1) \) and \( S = (s,0) \) respectively. We would like to express \( s \) in terms of the given numbers \( a, b, m \).

![Diagram](image)

**Figure 7.3:**
First we would like to find \((x_1,y_1)\). As \( R \) lies on line \( L \) it satisfies its equation \( i.e. y = mx \). Thus

\[ y_1 = mx_1. \]
As the slop of line $SV$ is $m_1 = \frac{b-0}{a-s}$, equation of line $SV$ becomes

$$y - 0 = \frac{b}{a-s} (x - s).$$

The point $R = (x_1, y_1)$ lies on line $VS$, so

$$y_1 = \frac{b}{a-s} (x_1 - s).$$

If we put value of $y_1$ into this equation, we obtain

$$mx_1 = \frac{b}{a-s} (x_1 - s).$$

Also

$$|RS| = (x_1 - s)^2 + (y_1 - 0)^2 \iff 1 = \left( \frac{bs}{ms-ma+b} - s \right)^2 + \left( \frac{bms}{ms-ma+b} \right)^2$$

$$\iff 1 = \frac{(mas - s^2m)^2}{(ms-ma+b)^2} + \frac{(bms)^2}{(ms-ma+b)^2}$$

$$\iff (ms-ma+b)^2 = m^2a^2s^2 + s^2m^2 - 2m^2s^3a + b^2m^2s^2$$

$$s^4 - 2as^3 + (b^2 + a^2 - 1)s^2 + 2\left( \frac{m-b}{m} \right)s^{\frac{3}{2}} - \left( \frac{2mab - m^2a^2 - b^2}{m^2} \right) = 0,$$

We have a fourth degree polynomial in $s$ with coefficients in terms of $a, b, m$. So verging allows us to solve some quartic equations. In this case we have four solutions, as in Figure 7.3, where two ways to verge through $V$ with respect to lines $L$ and $F$ are shown.

**Cubic and Quartic Equations**

Here in this section we will discuss the roots of cubic and quartic equations. As a result of this, we will be able to show relations between successive real roots of cubic and quartic equation, and the geometrical constructions which we make with the help of the compass and marked ruler. In the quadratic case, there is a coincidence among these three elements: solving quadratic equations, adjoining square roots of field elements, and considering degree-2 field extensions. But, the situation is more complicated with cubic and quartic equations. A real root of a cubic equation, sometimes may or may not be satisfy this cubic root field extension. A root of a quartic equation may give a degree-4 field extension that has no intermediate degree-2 subfield, and so may not be expressible by square and fourth roots only. We can not use successive square roots and cube roots of complex numbers as we are working in geometry, we are more interested in what happens in the real cartesian plane. Therefore, we will discuss real roots of these equations. We will show that real roots of cubic and quartic equations can be expressed by three types of field extensions of a subfield $G \subseteq \mathbb{R}$:

1. $G(\sqrt{b})$ where $b \in G$, $b > 0$. 
(2) $G\left(\sqrt[3]{b}\right)$ where $b \in G$.
(3) $G\left(\cos \frac{1}{3}\phi\right)$ where $\cos \phi \in G$

We will say that cubic and quartic equation can be solved by taking square roots, cubic roots, and trisecting angles. Suppose we have polynomial $f(y) = y^2 - 2$ over $Q$ which is irreducible, then for the equation of the form $y^3 - 2 = 0$, we will use field extension of the form $G\left(\sqrt[3]{2}\right)$. Each root of the equation lie in this field extension. If we have equation of the form $y^3 - 2$, then we will use field extension of the form $G\left(\sqrt[3]{2}\right)$. And if we have cubic equation of the form $y^3 - 3y - b = 0$ then we will use field extension of the form $G\left(\cos \frac{1}{3}\phi\right)$.

**Proposition 7.3** If $\beta$ is a real root of a quartic polynomial with coefficients in $G$, where $G$ is subfield of $R$ then the root of quartic polynomial can be found by first adjoining a real root of a cubic polynomial with coefficients in $G$ (called the cubic resolvent of the quartic equation), followed by successive real square roots.

**Proof.** Consider a quartic function

$$f(y) = ay^4 + by^3 + cy^2 + dy + e$$

where $a$ is nonzero, and $a, b, c$ and $d$ are in $G$. Such a function is sometimes called a biquadratic function. We can also write it product of two quadratic factors, having the form

$$(by^2 + my^2 + n)(py^2 + qy^2 + r).$$

We can write a quartic equation as

$$f(y) = ay^4 + by^3 + cy^2 + dy + e = 0,$$

where $a \neq 0$.

$$y^4 + \frac{b}{a}y^3 + \frac{c}{a}y^2 + \frac{d}{a}y + \frac{e}{a} = 0.$$

To eliminate the $y^3$ we have to change variables from $y$ to $u$ such that $y = u + \frac{b}{4a}$. Then

$$\left(u - \frac{b}{4a}\right)^4 + \frac{b}{a}\left(u - \frac{b}{4a}\right)^3 + \frac{c}{a}\left(u - \frac{b}{4a}\right)^2 + \frac{d}{a}\left(u - \frac{b}{4a}\right) + \frac{e}{a} = 0.$$

The resulting equation is

$$u^4 + \alpha u^2 + \beta u + \gamma = 0 \quad (7.6)$$

This equation is said to be **depressed quartic equation**. To get square on both sides, adding and subtracting $w^2 + 2u^2w$ in (7.6)

$$\iff u^4 + \alpha u^2 + \beta u + \gamma + w^2 + 2u^2w = w^2 + 2u^2w$$

$$\iff (u^2 + w)^2 = (2w - \alpha)u^2 - \beta u - \gamma + w^2$$

$$\iff (u^2 + w)^2 = (2w - \alpha)\left(u^2 - \frac{\beta}{2w - \alpha}u - \frac{\gamma - w^2}{2w - \alpha}\right)$$

$$\iff (u^2 + w)^2 = (2w - \alpha)\left(u - \frac{\beta}{2(2w - \alpha)}\right)^2 - \frac{\beta^2}{4(2w - \alpha)^2} - \frac{\gamma - w^2}{2w - \alpha}. \quad (7.7)$$
For finding roots we have to put
\[ -\beta^2 - 4 (\gamma - w^2) (2w - \alpha) = 0 \]
\[ 8w^3 - 4\alpha w^2 + 8\gamma w + 4\gamma\alpha - \beta^2 = 0. \]

After solving cubic equation we get three roots and, then we put real root of cubic equation in equation (7.7). Hence equation (7.7) becomes
\[ (u^2 + w)^2 = (2w - \alpha) \left( u - \frac{\beta}{2(2w - \alpha)} \right)^2 \] (7.8)

There are two cases.
(i). If the root of cubic equation is rational or square root and it satisfies the equation (7.8) then this root can be constructible by unmarked ruler and compass.
(ii). If the root of cubic equation is cube root and it satisfies the equation (7.8) then this root can be constructible by marked ruler and compass.

**Theorem 7.7.** Consider
\[ y^3 - 3y - c = 0 \]
with \( c \in G \) and \( |c| \leq 2 \). Let \( \phi \) be an angle with \( \cos \phi = \frac{1}{2}c \). Then \( \beta = 2 \cos \frac{1}{3}\phi \) is a root of the equation.

**Proof.** We know that we can write this trigonometric identity
\[ \cos 3\theta = 4\cos^3 \theta - 3\cos \theta, \]
where we put \( \phi = 3\theta \), \( y = 2\cos \theta \), and \( c = 2\cos 3\theta \). Then restriction \( |c| < 2 \) is necessary to find a \( \phi \) with \( \cos \phi = \frac{1}{2}c \). □

**Theorem 7.8.** We will use method of Cardano to solve cubic equation.

**Proof.** Consider a general cubic
\[ y^3 + by^2 + cy + d = 0 \]
This can be simplified by the putting \( y = x - \frac{b}{3} \) so as to eliminate the \( y^2 \). So it will be sufficient to consider the equation
\[ y^3 + qy + p = 0. \]
We look for a solution of the form \( y = w + h \)
\[ w^3 + 3w^2h + 3wh^2 + h^3 + q(w + h) + p = 0 \]
This can be accomplished by setting \( q = -3wh \) and \( p = -w^3 - h^3 \).then
\[ w^3 + h^3 = -p \]
\[ w^3 h^3 = -\left(\frac{q}{3}\right)^3, \]

so \( w^3 \) and \( h^3 \) are roots of the quadratic equation
\[ x^2 + px - \left(\frac{q}{3}\right)^3 = 0. \]

We solve this by the quadratic formula to obtain
\[ x = -\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3} \]

since \( w \) and \( h \) are the cube roots of these two values of \( x \), we get
\[ y = 3\sqrt{\sqrt{\left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3} - \frac{p}{2} - 3\sqrt{\left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3} + \frac{p}{2}} \]

This is Cardano formula. In order for the roots to be real, we need
\[ \left(\frac{p}{2}\right)^2 + \left(\frac{q}{3}\right)^3 \geq 0 \]

Thus we have proved the following result: \( \square \)

**Remark** Although it appears that we need two cube roots, since \( q = -3wh \), we have \( h = -q/(3w) \), so \( y = w - q/(3w) \) can be expressed using one square root and one cube root.

**Proposition 7.2** If \((p/2)^2 + (q/3)^3 < 0\), then a real root of the equation \( y^3 + qy + p = 0 \) can be found by taking a square root and trisecting an angle.

**Proof.** The hypothesis implies that \( q < 0 \) so we adjoin \( \sqrt{-3q} \) to our field and make a change of variables \( y = \frac{1}{3} \sqrt{-3qt} \). This gives the equation
\[ t^3 - 3t + c = 0 \]

where
\[ c = p \sqrt{-\frac{27}{q^3}} \]

Now, our hypothesis \((p/2)^2 + (q/3)^3 < 0\) implies \( |c| < 2 \), so we can use theorem 7.7 to solve the equation by trisecting an angle.

\( \square \)

**Theorem 7.9.** Let \( G \) be a subfield of \( R \) and let \( \beta \in R \). The following conditions are equivalent:

(i) There exists a tower of subfields \( G = G_0 \subseteq G_1 \subseteq \cdots G_k \subseteq R \) with \( \beta \in G_k \), and for each \( i \), \( G_i \) is obtained from \( G_{i-1} \) by adjoining an element \( \alpha_i = \alpha \), where either

(1) \( \alpha = \sqrt{\beta} \) with \( \beta \in G_{i-1}, \beta > 0 \), or

(2) \( \alpha = 3\sqrt{\beta} \) with \( \beta \in G_{i-1}, \) or

(3) \( \alpha = \cos \frac{1}{3} \phi \) with \( \cos \phi \in G_{i-1} \).

(ii) There exists a tower of subfields \( G = G_0 \subseteq G_1 \subseteq \cdots G_n \subseteq R \) with \( \beta \in G_n \), and each \( G_i \) is obtained from \( G_{i-1} \) by adjoining a root of a quadratic, a cubic, or a quartic
polynomial.

(iii) The quantity $\beta$ can be constructed by compass and marked ruler from data with coordinates in $G$.

Proof. $(i) \Rightarrow (iii)$. The three types of extensions are constructible with compass and marked ruler, the first by ordinary ruler and compass construction, the second by theorem (7.8) and third by theorem (7.7). (Note that $\cos \phi \in G$ does not necessarily imply that the angle $\phi$ can be realized by lines in the cartesian plane over $G$. We may have to make a quadratic extension to obtain $\sin \phi$ first, before we have an actual angle to trisect.)

$(iii) \Rightarrow (ii)$. Regular ruler and compass constructions correspond to quadratic equations, and each use of the marked ruler between lines can be accomplished by solving a quartic equation section (7.4).

$(ii) \Rightarrow (i)$. A quartic polynomial can be reduced to cubic and quadratic equations by section (7.4), and cubic and quadratic polynomials can be solved by the three types of extensions, by (theorem 7.8) and section (7.4).
**Proposition 7.3** (Menelaus’ theorem) Suppose we are given a triangle $ABC$, and also consider a line $L$ which cuts the side $AB$ of triangle at points $D$ and $E$ respectively. Extend the side $DE$ on both sides. Then

$$\frac{AD}{BD} \cdot \frac{BF}{CF} \cdot \frac{CE}{AE} = 1.$$  

![Figure 7.4:](image)

**Proof.** Parallel to $CB$ draw a line which passes through $A$ and intersect the line $ED$ at point $G$. Then the triangle $ADG$ is congruent to $BDF$, and the triangle $AEG$ is congruent to $CEF$. From this we obtain

$$\frac{AD}{AG} = \frac{BD}{BF}$$

and

$$\frac{AE}{AG} = \frac{CE}{CF}.$$  

Eliminating $AG$ from above equations and rearranging gives the result. [5, Page 180] □

**Proposition 7.4** If a point $A$ lies outside a circle, and if $AB$ is tangent to the circle at $B$, and if $ACD$ cuts the circle at $C$ and $D$, then the rectangle formed by $AC$ and $AD$ has area equal to the square on $AB$ as shown in figure 7.5. [5, Page 47]

**Theorem 7.10.** Using compass and marked ruler, it is possible to trisect any angle.

**Proof.** To trisect an arbitrary angle by a "small" step outside the Greek framework is via a ruler with two marks a set distance apart. Suppose we are given an angle $OAC$. From point $O$ we drop a perpendicular $OB$ on line $AC$. And then we draw a line $l$ which passes through $O$ parallel to $AC$. Now we use marked ruler to draw a line $AEG$ such that $E \in OB$, $G \in l$, $EG = 2OA$. This line will be the trisector of the original angle. Suppose mid point of $EG$ be the $D$, and let mid point of $OG$ be the $F$. Then $DF$ and $OG$ are perpendicular to each other, the triangles $GDF$ and $ODF$ are congruent (because two sides and a angle of triangle $GDF$ is equal to two sides and a angle of triangle $ODF$). Now the new angle $GAC = \phi$ is equal to $\angle OGA$ by parallel lines and to $\angle GOD$ by congruent triangles. So
\[ \angle ODA = 2\phi, \text{ since it is an exterior angle to the triangle } OGD. \text{ But } EG \text{ was equal to } 2OA, \text{ so } OA = GD = OD. \text{ Hence the triangle } OAD \text{ is isosceles, and so } \angle OAE = 2\phi. \text{ Thus the original angle } OAC \text{ is equal to } 3\phi, \text{ and } \phi \text{ is one-third of it, as required.} \]

**Theorem 7.11.** Using compass and marked ruler, it is possible to construct \( \sqrt[k]{k} \), with \( 0 < k < 8 \).

**Proof.** Consider the triangle \( ABC \) with sides \( 1, 1, k/4 \). \( AB=k/4 \). Extend side \( CB \) by one unit to form the line segment \( CBD \). Extend side \( BA \) to form the ray \( BAL \) and draw the ray \( DAZ \). Also \( M \) is the midpoint of \( BA \). Now take the marked ruler and place it so that it passes through vertex \( C \) and intersects \( DAZ \) at \( R \) and \( BAL \) at \( S \) such that the distance \( RS \) is exactly 1. Let the parallel to \( AB \) that passess through \( C \) intersect \( DA \) at \( E \). So triangles \( ABD \) and \( ECD \) are congruent. Then, since \( B \) bisects \( DC \), we have \( CE = 2BA = k/2 \). Also, since triangle \( ECR \) congruent to Triangle \( ASR \), we have \( (k/2)/CR = AS/1 \). with \( x = AS \).
then $CR = k/2x$. With $M$ the mid point of $A$ and $B$,
By pythagorean theorem
\[
[1 + k/(2x)]^2 = CS^2 = CM^2 + MS^2
\]
\[
= [CB^2 + BM^2] + MS^2
\]
\[
= [1^2 - (k/8)^2] + [x + (k/8)^2]
\]
\[
\iff 4x^4 + kx^3 - 4kx - k^2 = 0
\]
\[
\iff (4x + k)(x^3 - k) = 0
\]
Since $4x + k > 0$, then we must have $x^3 - k = 0$. Therefore, $x$ is the real cube root of $k$ i.e $x = \sqrt[3]{k}$.

Figure 7.7:

\[\text{\begin{tikzpicture}
\end{tikzpicture}}\]

**Theorem 7.12.** Given segments of lengths 1 and $b$, it is possible with compass and marked ruler to construct a segment of length $\sqrt[3]{b}$.

**Proof.** Suppose we are given a line segment $BA$ of length $b$. With the help of segment of length 1, choose $a = 2^{3l-1}$ for suitable $l$ such that $a > b$. Construct an triangle $BAE$ with $EB = EA = a$, and extend side $EB$ by $a$ units to form the line segment $EBF$. Draw the ray $FAN$ which intersect line segment $BD$ at $A$. Now use the marked ruler to draw $ECD$ with $C \in FN$ and $CD = a$. Let $AD = x$. Then $\sqrt[3]{2} = x/2^l$. To see this, we first apply Menelaus’s theorem Proposition 7.3 to the triangle $BED$ and the transversal line $FAC$. Letting $EC = y$, starting with vertex $B$, and going clockwise, it says that
\[
a \frac{y}{2a} \cdot \frac{x}{a} \cdot \frac{1}{b} = 1
\]
This gives us
\[
yx = 2ba.
\]
Then we apply proposition 7.4 to the circle with center $E$ and radius $a$, and the point $D$ outside, and the two line segment $DAB$ and $DGO$. Note that $EC = a$, so by subtraction, $DC = y$. Thus we obtain

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

Removing $y$ from equations

$$x^3 = 4ba^2.$$ 

Since $a = 2^{3l−1}$

$$x^3 = 2^{6l}·b.$$ 

Hence, $\sqrt[3]{2} = x/2^{2l}$. \hfill $\Box$

**Corollary 2.** A regular polygon of $n$ sides can be constructed with compass and marked ruler (between lines only) if and only if $n$ is of the form

$$n = 2^k3^l p_1 \cdots p_s,$$

where $p_1, p_2, p_3, \cdots, p_s$ are Pierpont primes.

**Definition 7.3.** A prime number of the form $2^u3^v + 1$ for some nonnegative integers $u$ and $v$ is said to be a Pierpont prime. They are named after the mathematician James Pierpont. It is possible to prove that if $v = 0$ and $u > 0$, then $u$ must be a power of 2, making the prime a Fermat prime. If $v$ is positive then $u$ must also be positive, and the Pierpont prime is of the form $6k + 1$ (because if $u = 0$ and $v > 0$ then $2^u3^v + 1$ is an even number greater than 2 and therefore composite). The first few Pierpont primes are: 2, 3, 5, 7, 13, 17, 19, 37, 73, 97, 109, 163, 193, 257, 433, 487, 577, 769.

All constructible number which are obtained by using unmarked ruler and compass

**Theorem 7.13.** A real number $\alpha$ is constructible with unmarked ruler and compass if and only if a tower of subfields $Q = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_m$ of $R$ exists such that $\alpha \in G_m$ and $[G_k: G_{k−1}] = 1$ or 2 for each $K$. 

52
Example 7.4. Suppose $Q$ is a subfield of $R$ and $\alpha = \sqrt{2} + \sqrt{3} \in R$, we want to check either $\alpha$ is constructible or not with unmarked ruler. Since for this $\alpha$ there is irreducible polynomial $p(y) = y^4 - 10y^2 + 1$ over $Q$ such that $p(\alpha) = 0$ and $\deg p(y) = 2^2$. Also for $\alpha$ there exist a tower of subfields with $\alpha \in Q(\alpha)$; and

$$Q \subseteq Q\left(\sqrt{2}\right) \subseteq Q\left(\sqrt{2}\right)\left(\sqrt{3}\right) = Q(\alpha).$$

Hence we can extend this definition to all real numbers.

**All constructible points which are obtained by using marked ruler and compass**

**Theorem 7.14.** A real number $\alpha$ is constructible with marked ruler and compass if and only if a tower of subfields $Q = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_m$ of $R$ exists such that $\alpha \in G_m$ and $[G_k : G_{k-1}] = 1$ or 2 or 3 for each $K$.

**Example 7.5.** Suppose $Q$ is a subfield of $R$ and $\alpha = \sqrt[3]{2} \cdot \sqrt{2} \in R$, we want to check either $\alpha$ is constructible or not with marked ruler. Since for this $\alpha$ there is irreducible polynomial $p(y) = y^6 - 32$ over $Q$ such that $p(\alpha) = 0$ and $\deg p(y) = 2^1 3^1$, also for $\alpha$ there exist a tower of subfields with $\alpha \in Q(\alpha)$, and

$$Q \subseteq Q\left(\sqrt{2}\right) \subseteq Q\left(\sqrt{2}\right)\left(\sqrt[3]{2}\right) = Q(\alpha).$$

Hence in this way we can explain algebraically all those real numbers which are constructible with marked ruler and compass and so we can solve all those geometric problems which are attached to these constructible numbers.

**Conclusion** With the help of field extensions, a part of the theory of abstract algebra, we conclude that these four problems trisecting the angle, doubling the cube, squaring the circle, and construction of all regular polygons are impossible by using unmarked ruler and compass.

First two problems, trisecting the angle and doubling the cube are solved by using marked ruler and compass, because when we use marked ruler more points are possible to construct and with the help of these points more figures are possible to construct. The problems, squaring the circle and construction of all regular polygons are still impossible to solve.
References


