RULER , COMPASS AND NEUSIS CONSTRUCTIONS

A Dissertation(HMTDS6043D)
submitted in partial fulfilment of the requirements for the award of the degree of
Bachelor of Science
In
Mathematics
by
CHANDRANI SENGUPTA
(Registrtion No.: A01-2112-0503-22)
(Roll No.: 0035)
under the guidance of
PROF. GAURAB TRIPATHI

DEPARTMENT OF MATHEMATICS
ST. XAVIERS COLLEGE (AUTONOMOUS)
KOLKATA-700016

ABSTRACT

Name of the student : Chandrani Sengupta
Registration Number : A01-2112-0503-22
Degree for which submitted : B.Sc.
Dissertation Title : Ruler , Compass and Neusis Constructions
Department : Mathematics
Roll No. : 0035
Dissertation Supervisor : Professor Gaurab Tripathi
Paper Code : HMTDS6043D
Date of Submission : April 1 , 2025

This project explores the concept of **Ruler, Compass, and Neusis Constructions**, addressing the limitations of traditional ruler and compass methods by introducing the Neusis construction process. The objective is to develop a comprehensive theory that integrates these three tools to solve problems that are impossible to resolve with ruler and compass alone.

The foundational concepts begin with field theory and vector spaces, followed by a detailed exploration of **Galois theory**, which provides an algebraic framework for understanding constructibility. Specifically, if K and F are fields with $K \subseteq F$, then F is referred to as an extension field of K. The **degree** of the extension, denoted $[F : K]$, is the dimension of F over K, and the relation $[F : K] = [F : L][L : K]$ holds if L is an intermediate field.

An extension field F over K is algebraic if every element in F is algebraic over K. From this algebraic perspective, I introduce the **Galois group**. If E and F are extension fields of K, a non-zero map $\sigma : E \to F$ that is both a field and K-module homomorphism is called a **K-homomorphism**. A map $\sigma \in \mathrm{Aut}(F)$, which is a K-automorphism of F, forms the **Galois group** of F over K, denoted as $\mathrm{Aut}_K F$.

Building upon these foundational theories, I delve into the topic of constructibility and its inherent limitations. I first explore the basic properties of ruler and compass constructions and then introduce four classical construction problems to motivate the concept of constructibility. A real number c is said to be constructible if the point $(c, 0)$ can be constructed through a finite sequence of ruler and compass constructions. Several well-known constructions are discussed, followed by an exploration of the relationship between constructibility and field extensions. This connection leads to the identification of several impossibilities in ruler and compass constructions, which can be proven algebraically.

In addition to ruler and compass, I introduce the concept of **Neusis construction**, a new geometric tool that extends the range of solvable problems. This method provides geometric solutions to traditionally unsolvable constructions, such as:

1. The trisection of any angle into three equal parts. 2. The doubling of the cube. 3. The construction of certain regular polygons.

Finally, I explore how Neusis construction can be used in combination with ruler and compass to solve specific triangle construction problems. These problems include:

1. Constructing a triangle when its three medians are given (or constructible). 2. Constructing a triangle when its three angle bisectors are given (or constructible). 3. Constructing a triangle when its three perpendicular bisectors are given (or constructible).

Through these topics, this project seeks to broaden the scope of geometric constructions beyond the limitations of traditional methods

DECLARATION

I,Chandrani Sengupta,(Registration No. :A01-2112-0503-22),hereby declare that ,this project entitled "RULER , COMPASS AND NEUSIS CONSTRUCTIONS",submitted to St. Xavier's College (Autonomous),Kolkata towards the partial fulfilments for the requirement of Bachelor of Science in Mathematics , is a research work carried out by me under the supervision of Professor Gaurab Tripathi.I don't claim the entire work to be my own . However ,some theorems and many of the results proved in this project comprises of original work genuinely.I have sincerely tried to uphold academic ethics and honesty.I affirm to have sited all the external sources and no part of my dissertation paper includes unacknowledged materials.

Chandrani Sengupta

CHANDRANI SENGUPTA

CONTENTS

Chapter 1

An Introduction to Field Theory

1.1 Binary Operation

Definition 1.1. A binary operation on a set $\mathbb{F}$ is a mapping $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$, i.e, a correspondence that associates with each ordered pair of elements of $\mathbb{F}$ a uniquely determined element of $\mathbb{F}$.

1.2 Field Axioms

A field is a set $\mathbb{F}$ together with two binary operations on $\mathbb{F}$ called addition and multiplication. The result of the addition of a and b is called the sum of a and b, and is denoted $a+b$. Similarly, the result of the multiplication of a and b is called the product of a and b, and is denoted ab or $a \cdot b$. These operations are required to satisfy the following properties, referred to as field axioms (in these axioms, a, b, and c are arbitrary elements of the field $\mathbb{F}$) :

1. Associativity of addition and multiplication :

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

2. Commutativity of addition and multiplication :

$$a + b = b + a, a \cdot b = b \cdot a$$

3. Additive and multiplicative identity : There exist two different elements 0 and 1 in $\mathbb{F}$ such that

$$a + 0 = a, a \cdot 1 = a.$$

4. Additive inverses : For every $a \in \mathbb{F}, \exists$ an element in $\mathbb{F}$, denoted $-a$, called the additive inverse of a, such that

$$a + (-a) = 0.$$

5. Multiplicative inverses : For every $a \neq 0 \in \mathbb{F}, \exists$ an element in $\mathbb{F}$, denoted by a^{-1} or $\frac{1}{a}$, called the multiplicative inverse of a, such that

$$a \cdot a^{-1} = 1$$

6. Distributivity of multiplication over addition:

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

This may be summarized by saying:

Definition 1.2. A field has two operations, called addition and multiplication; it is an abelian group under addition with 0 as the additive identity; the nonzero elements are an abelian group under multiplication with 1 as the multiplicative identity; and multiplication distributes over addition.

Even more summarized:

Definition 1.3. A field is a commutative ring where $0 \neq 1$ and all nonzero elements are invertible.

Chapter 2

Basics Concepts of Vector Space

2.1 Vector Spaces and Subspaces

Definition 2.1. A vector space (or linear space) consists of the following :

1. a field $\mathbb{F}$ of scalars;

2. a set V of objects, called vectors;

3. a rule (or operation), called vector addition, which associates with each pair of vectors $\alpha, \beta \in V$ a vector $\alpha+\beta \in V$, called the sum of α and β, in such a way that (for the following properties $\alpha, \beta, \gamma \in V$)

(a) addition is commutative, $\alpha+\beta=\beta+\alpha$;

(b) addition is associative, $\alpha+(\beta+\gamma)=(\alpha+\beta)+\gamma$;

(c) $\exists!$ a vector $0 \in V$, called the zero vector, such that $\alpha+0=\alpha, \forall \alpha \in V$;

(d) for each vector $\alpha \in V \exists$! a vector $-\alpha \in V$ such that $\alpha+(-\alpha)=0$;

4. a rule (or operation), called scalar multiplication, which associates with each scalar $c \in \mathbb{F}$ and vector $\alpha \in V$ a vector $c\alpha \in V$, called the product of c and α, in such a way that (for the following properties $\alpha, \beta \in V$ and $c, c_1, c_2 \in \mathbb{F}$)

(a) $1\alpha=\alpha, \forall \alpha \in V$;

(b) $\left(c_1 c_2\right) \alpha=c_1\left(c_2 \alpha\right)$;

(c) $c(\alpha+\beta)=c\alpha+c\beta$;

(d) $\left(c_1+c_2\right) \alpha=c_1 \alpha+c_2 \alpha$;

$\star$ Here, we shall say V is a vector space over the field $\mathbb{F}$.

Definition 2.2. Let V be the vector over the field $\mathbb{F}$. A subspace of V is a subset W of V which itself a vector space over $\mathbb{F}$ with the operations of vector addition and scalar multiplication on V.

2.2 Bases and Dimension

Definition 2.3. Let V be the vector over the field $\mathbb{F}$. A subset S of V is said to be linearly dependent (or simply, dependent) if there exist distinct vectors $a_1, a_2, \cdots, a_n \in S$ and scalars $c_1, c_2, \cdots, c_n \in \mathbb{F}$, not all of which are zero, such that

$$c_1 a_1 + c_2 a_2 + \cdots + c_n a_n = 0$$

A set which is not linearly dependent is called linearly independent.

Definition 2.4. Let V be the vector over the field $\mathbb{F}$. A basis for V is a linearly independent set of vectors in V which spans the space V.

* The dimension of a vector space V is the cardinality (i.e. the number of vectors) of a basis of V over its base field. It is sometimes called Hamel dimension (after Georg Hamel) or algebraic dimension.

* Notationally, the dimension of V over the field $\mathbb{F}$ can be written as $[V : \mathbb{F}]$ or $\dim_{\mathbb{F}}(V)$.

Chapter 3

Field Extensions

Definition: A field extension is a pair of fields K, L such that $K \subseteq L$. We use the notation $L : K$.
Another way of saying this is to say that K is a subfield of L. A subfield is a subset of a field that is itself a field, and therefore it is closed under field operations:addition, multiplication, additive and multiplicative inverses.
The fields that we will work with are all subfields of $\mathbb{C}$. Note that any subfield of $\mathbb{C}$ must contain 0 and 1, and therefore (since it is closed under field operations) it must contain $\mathbb{Q}$.

Definition: Let K be a field and $X \subseteq K$ a subset. The subfield of K generated by X is the intersection of all the subfields of K that contain X.
Equivalently, it is the (unique) smallest subfield of K containing X.

If X contains a nonzero element, this is also equivalent to the set of all elements of $\mathbb{K}$ that can be obtained from elements of X by a finite sequence of field operations (addition, multiplication, additive inverses and multiplicative inverses).
We use the notation Q(X) for the subfield of $\mathbb{C}$ generated by X.

Definition: Let $L : K$ be a field extension and $Y \subseteq L$ a subset of the large field. The subfield of L generated by $K \cup Y$ is denoted by $K(Y)$. When $Y = \{\alpha\}$ or $Y = \{\alpha_1, \ldots, \alpha_n\}$, we write $K(\alpha)$ and $K(\alpha_1, \ldots, \alpha_n)$ respectively, instead of $K(\{\alpha\})$ or $K(\{\alpha_1, \ldots, \alpha_n\})$.

Definition: A *simple extension* is a field extension L/K such that $L = K(\alpha)$ for some $\alpha \in L$. That is, L is obtained from K by adjoining a single element α. Such an element is called a primitive element.

Definition:Let $L : K$ be a field extension and $Y \subseteq L$ be a subset of the large field .The subfield of L generated by $K \cup L$ is denoted by $K(Y)$

When $Y = \{\ \alpha\} or$Y=$\{\alpha_1$,.......,$\alpha_n\}, wewrite$K(α) and $K(\alpha_1, ..., \alpha_n)$ respectively instead of K($\{\alpha\}) or K(\alpha_1, ..., \alpha_n\})$.**Examples:**

$Q(i) = \{p + q \mid p, q \in Q\}$

$Q(\sqrt{2}) = \{p + q\sqrt{2} \mid p, q \in Q\}$

$R(i) = C$

Let $\alpha = 2^{1/3} \in R$. Then $Q(\alpha) = \{p + q + r\alpha^2 \mid p, q, r \in Q\}$

$Q(i, \sqrt{5}) = \{p + q + r\sqrt{5} + s\sqrt{5} \mid p, q, r, s \in Q\}$.

Definition : Let K be a field extension of F. If X is a subset of K, then the ring $F[X]$ generated by F and X is the intersection of all subrings of K that contain F and X. The field $F(X)$ generated by F and X is the intersection of all subfields of K that contain F and X. If $X = \{a_1, \dots, a_n\}$ is finite, we will write $F[X] = F[a_1, \dots, a_n]$ and $F(X) = F(a_1, \dots, a_n)$. If X is finite, we call the field $F(X)$ a finitely generated extension of F.

It is a simple exercise to show that an intersection of subfields or subrings of a field is again a subfield or subring, respectively.
From this definition, it follows that $F(X)$ is the smallest subfield with respect to inclusion of K that contains F and X. We can give more concrete descriptions of $F[X]$ and $F(X)$. Let K be a field extension of F and let $a \in K$. The evaluation homomorphism ev_a is the map $\text{ev}_a : F[x] \to K$ defined by $\text{ev}_a\left(\sum_i a_i x^i\right) = \sum_i a_i d^i$. We denote $\text{ev}_a(f(x))$ by $f(a)$. It is straightforward (see Problem 3) to show that ev_a is both a ring and an F-vector space homomorphism. We use this notion to see what it means for a field to be generated by a set of elements. We start with the easiest case, when K is generated over F by a single element.

Proposition : *Let K be a field extension of F and let $a \in K$. Then $F[a] = \{f(a) : f(x) \in F[x]\}$ (17 Lei $(a) = \{f(a) \mid g(a) : f, g \in F[x], g(a) \neq 0\}$. Moreover, $F(a)$ is the quotient field of $F[a]$.*
Proof. The evaluation map eva : $F[x] \to K$ has image $\{f(a) : f \in F[x]\}$, so this set is a subring of K. If R is a subring of K that contains F and a, then $f(a) \in R$ for any $f(x) \in F[x]$ by closure of addition and multiplication. Therefore, $\{f(a) : f(x) \in F[x]\}$ is contained in all subrings of K that contain F and a. Therefore, $F[a] = \{f(a) : f(x) \in F[x]\}$. The quotient field of $F[a]$ is then the set $\{f(a)/g(a) : f, g \in F[x], g(a) \neq 0\}$. It clearly is contained in any subfield of K that contains $F[a]$; hence, it is equal to $F(a)$.

The notation $F[a]$ and $F(a)$ is consistent with the notation $F[x]$ and $F(x)$ for the ring of polynomials and field of rational functions over F, as the description of $F[a]$ and $F(a)$ shows. By similar arguments, we can describe the ring $F[a_1, \dots, a_n]$ and field $F(a_1, \dots, a_n)$ generated by F and $a_1, \dots, a_n$. The proof of the following proposition is not much different from the proof of the above proposition.

Proposition :*Let K be a field extension of F and let $a_1, \dots, a_n \in K$. Then*

$$F[a_1, \dots, a_n] = \{f(a_1, \dots, a_n) : f \in F[x_1, \dots, x_n]\}$$

and

$$F(a_1,\ldots,a_n)=\left\{\frac{f(a_1,\ldots,a_n)}{g(a_1,\ldots,a_n)}:f,g\in F[x_1,\ldots,x_n],g(a_1,\ldots,a_n)\neq 0\right\}$$

so $F(a_1,\ldots,a_n)$ *is the quotient field of* $F[\alpha_1,.......\alpha_n]$.

For arbitrary subsets X of K we can describe the field $F(X)$ in terms of finite subsets of X. This description is often convenient for turning ques- tions about field extensions into questions about finitely generated field extensions.

Definition : If K is a field extension of F, then an element $a\in K$ is algebraic over F if there is a nonzero polynomial $f(x)\in F[x]$ with $f(a)=0$. If a is not algebraic over F, then a is said to be transcendental over F. If every element of K is algebraic over F, then K is said to be algebraic over F, and $K\mid F$ is called an algebraic extension.

Definition : If a is algebraic over a field F, the minimal polynomial of a over F is the monic polynomial $p(x)$ of least degree in $F[x]$ for which $p(a)=0$; it is denoted $\min(F,a)$. Equivalently, $\min(F,a)$ is the monic generator $p(x)$ of the kernel of the evaluation homomorphism ev_a.

Lemma : *If K is a finite extension of F, then K is algebraic and finitely generated over F.*

Proof. Suppose that $a_1,\ldots,a_n$ is a basis for K over F. Then every element of K is of the form $\sum a_i a_i$ with $a_i\in F$, so certainly we have $K=F(a_1,\ldots,a_n)$; thus, K is finitely generated over F. If $a\in K$, then $\{1,a,\ldots a^n\}$ is dependent over F, since $[K:F]=n$. Thus, there are $c_i\in F$, not all zero, with $\sum c_i a^i=0$. If $f(x)=\sum c_i x^i$, then $f(x)\in F[x]$ and $f(a)=0$. Therefore, a is algebraic over F, and so K is algebraic over F.

The converse of this lemma is also true. In order to give a proof of the converse, we need the following property of degrees. The degree of a field extension is the most basic invariant of an extension. It is therefore important to have some information about this degree. We will use the following transitivity result frequently.

Definition : If K is a field extension of F, then an element $a \in K$ is algebraic over F if there is a nonzero polynomial $f(x) \in F[x]$ with $f(a) = 0$.
If a is not algebraic over F, then a is said to be transcendental over F. If every element of K is algebraic over F, then K is said to be algebraic over F, and K/F is called an algebraic extension.

Definition : If a is algebraic over a field F, the minimal polynomial of a over F is the monic polynomial $p(x)$ of least degree in $F[x]$ for which $p(a) = 0$; it is denoted $\min(F, a)$. Equivalently, $\min(F, a)$ is the monic generator $p(x)$ of the kernel of the evaluation homomorphism ev_a.

Proposition : *Let K be a field extension of F and let $a \in K$ be algebraic over F.*

1. The polynomial $\min(F, a)$ is irreducible over F. 2. If $g(x) \in F[x]$, then $g(a) = 0$ if and only if $\min(F, a)$ divides $g(x)$. 3. If $n = \deg(\min(F, a))$, then the elements $1, a, \ldots, a^{n-1}$ form a basis for $F(a)$ over F, so $[F(a) : F] = \deg(\min(F, a)) < \infty$. Moreover, $F(a) = F[a]$.

Proof. If $p(x) \min(F, a)$, then $F[x]l(p(x))F[a]$ is an integral domain. Therefore, $(p(x))$ is a prime ideal, so $p(x)$ is irreducible. To prove statement 2, if $g(x) \in F[x]$ with $g(a) = 0$, then $g(x) \in \ker(\mathrm{ev}_a)$. But this kernel is the ideal generated by $p(x)$, so $p(x)$ divides $g(x)$. For statement 3, we first prove that $F[a] = F(u)$. To see this, note that $1 - P[a]$ is the image of the evaluation map ev_a. The kernel of ev_a is a prime ideal since ev_a maps $F[x]$ into an integral domain. However, $F[x]$ is a principal ideal domain, so every nonzero prime ideal of $F[x]$ is maximal. Thus, $\ker(\mathrm{ev}_a)$ is maximal, so $F[a]F[x]/\ker(\mathrm{ev}_a)$ is a field. Consequently, $F[a] = F(u)$. To finish the proof of statement 3, let $n = \deg(p(x))$. If $b \in F(u)$, then $b = g(a)$ for some $g(x) \in F[x]$. By the division algorithm, $g(x) = q(x)p(x) + r(x)$, where $r(x) = 0$ or $\deg(r) < n$. Thus, $b = g(a) = r(a)$. Since $r(a)$ is an F-linear combination of $1, a, \ldots, a^{n-1}$, we see that $1, a, \ldots, a^{n-1}$ span $F(a)$ as an F-vector space. If $\sum_{i=0}^{n-1} c_i a^i = 0$, then $f(x) = \sum_{i=0}^{n-1} c_i x^i$ is divisible by $p(x)$, so $f(x) = 0$, or else f is divisible by a polynomial of larger degree than itself. Thus, $1, a, \ldots, a^{n-1}$ is a basis for $F(a)$ over F.

Proposition : *Let $K \subseteq L \subseteq F$ be fields. Then,*

$$[F : K] = [F : L][L : K].$$

Proof : Let, $S_1 \subseteq F/L$ and $S_2 \subseteq L/K$ be bases of corresponding extensions. Now claim,$S = S_1 S_2 = \{\alpha\beta \mid \alpha \in S_1, \beta \in S_2\} \subseteq F$ is a basis of F/K, i.e we need to show, S is a basis of the vector space F over the field K. Firstly, we will show $\mathrm{Span}\{S\} = F$. Let, $v \in F$, then $\exists\{\alpha_1, \alpha_2, \cdots, \alpha_n\} \subseteq S_1$ such that $v = \sum_{i=1}^{n} c_i \alpha_i$ where $c_i \in L$, $1 \leq i \leq n$. Again for each $c_i \in L$, $1 \leq i \leq n$, $\exists\{\beta_{i1}, \beta_{i2}, \cdots, \beta_{im}\} \subseteq S_2$ such that $c_i = \sum_{j=1}^{im} \beta_{ij}$.

Therefore,

$$v = \sum_{i=1}^{n}\sum_{j=1}^{im} \beta_{ij}\alpha_i = \sum_{i=1}^{n}\sum_{j=1}^{im} \beta_{ij}\alpha_i, \text{ where } \alpha_i \in S_1 \& \beta_{ij} \in S_2.$$

$\Rightarrow$ Span$\{S\} = F$. Secondly, we will show S is linearly independent over K. Consider the following equation for $\alpha_i \in S_1$, $\beta_i \in S_2$ and $c_i \in K$,

$$\sum_{i=1}^{n} c_i(\alpha_i\beta_i) = 0, \text{ here } (\alpha_i\beta_i) \in S.$$

$\Rightarrow \sum_{i=1}^{n}(c_i\beta_i)\alpha_i = 0$. Since S_1 is linearly independent over L (according to our assumption), $\Rightarrow c_i\beta_i = 0; 1 \leq i \leq n \Rightarrow c_i = 0; 1 \leq i \leq n$. So, $\sum_{i=1}^{n} c_i(\alpha_i\beta_i) = 0 \Rightarrow c_i = 0; 1 \leq i \leq n$. Hence, S is linearly independent over the field K. Now we have, $|S| = |S_1||S_2|$. [Notation $|X|$ = cardinality of X] Again, $[F : K] = |S|$, $[F : L] = |S_1|$, $[L : K] = |S_2|$.

$$[F : K] = [F : L][L : K].$$

This completes the proof.

Note that, Let $[F : K]$; $S \subseteq F$, 1. $K[S]$ is the smallest subring of F containing K and S. 2. $K(S)$ is the smallest subfield of F containing K and S.

Definition : Let, $U \in F$, $U_1, U_2, \cdots, U_m \in F$ and $K[X]$, $K[X_1X_2 \cdots X_m]$ are the poluno- mial rings over the field K. 1. $K[U] := \{f(U) \mid f(X) \in K[X]\}$.
2. $K(U) := \{\frac{f(U)}{g(U)} \mid f(X), g(X) \in K[X], g(U) \neq 0\}$.
3. $K[U_1U_2 \cdots U_m] := \{f(U_1, U_2, \cdots, U_m) \mid f(X_1X_2 \cdots X_m) \in K[X_1X_2 \cdots X_m]\}$.
4. $K(U_1U_2 \cdots U_m) := \{\frac{f(U_1,U_2,\cdots,U_m)}{g(U_1,U_2,\cdots,U_m)} \mid f(X_1X_2 \cdots X_m), g(X_1X_2 \cdots X_m) \in K[X_1X_2 \cdots X_m], g(U_1, U_2, \cdots, U_m) \neq 0\}$.

Observations:
1. $K[U_1U_2 \cdots U_{m-1}][U_m] = K[U_1U_2 \cdots U_m]$.
2. $K(U_1U_2 \cdots U_{m-1})(U_m) = K(U_1U_2 \cdots U_m)$.

Proposition : *Let K be a field extension of F. If each $a_i \in K$ is algebraic over F, then $F[a_1, \ldots, a_n]$ is a finite dimensional field extension of F with*

$$[F[a_1, \ldots, a_n] : F] < \prod_{i=1}^{n} [F(a_i) : F].$$

Proof. We prove this by induction on n; the case $n = 1$ is trivial. If we set $L = F[c_1, \ldots, a_n]$, then by induction L is a field and $[L : F] < [F(c_1) : F]$. Then $F[a_1, \ldots, a_n] = L[c]$ is a - field since a_n is algebraic over L, and since $\min(L, a_n)$ divides $\min(F, a_n)$ by

Proposition 1.15, we have $[F[a_1, \ldots, a_n] : L] < [F(a_n) : F]$. Hence, by one of the propositions proved previously and the induction hypothesis,

$$[F[a_1, \ldots, a_n] : F] = [F[a_1, \ldots, a_n] : L][L : F] < \prod [F(c) : F].$$

This finishes the proof.

The inequality of the proposition above can be strict. For example, if $a = \sqrt[4]{2}$ and $b = \sqrt[4]{18}$, then $[Q(a) : Q] = [Q(b) : Q] = 4$, since the polynomials $x^4 - 2$ and $x^4 - 18$ are irreducible over Q by an application of the Eisenstein criterion. However, we know that $Q(a, b) = Q(\sqrt[4]{2}, \sqrt{3})$, which has degree 8 over Q. To see this equality, note that $(b/a)^4 = 9$, so $(b/a)^2 = 3$. Thus, $\sqrt{3} \in Q(a, b)$. However, $[Q(a, b) : Q(a)] < 2$ because b satisfies the polynomial $x^2 - 3a^2 \in Q(a)[x]$. Thus, by Proposition proved previously

$$[Q(a, b) : Q] = [Q(a, b) : Q(a)] \cdot [Q(a) : Q] < 8 = [Q(\sqrt[4]{2}, \sqrt{3}) : Q],$$

so since $Q(\sqrt[4]{2}, \sqrt{3})$ is a subfield of $Q(a, b)$, we obtain $Q(a, b) = Q(\sqrt[4]{2}, \sqrt{3})$. The equality $[Q(\sqrt[4]{2}, \sqrt{3}) : Q] = 8$ is left as an exercise.

As a corollary to the previous proposition, we have the following conve- nient criterion for an element to be algebraic over a field. **Corollary** : *If K is a field extension of F, then $a \in K$ is algebraic over F if and only if $[F(a) : F] < \infty$. Moreover, K is algebraic over F if $[K : F] < \infty$.* The converse to the second statement of the corollary is false. There are algebraic extensions of infinite degree. The set of all complex numbers algebraic over $\mathbb{Q}$ is and this field is infinite dimensional over $\mathbb{Q}$.

Proposition . *Let K be a field extension of F, and let X be a subset of K such that each element of X is algebraic over F. Then F(X) is algebraic over F.If $|X| < \infty$, then [F(X):F]*

$< \infty$.

Chapter 4

Automorphisms

The main idea of Galois was to associate to any polynomial f a group of permutations of the roots of f. In this section, we define and study this group and give some numerical information about it. Our description of this group is not the one originally given by Galois but an equivalent description given by Artin.

Let K be a field. A ring isomorphism from K to K is usually called an automorphism of K. The group of all automorphisms of K will be denoted Aut (K). Because we are interested in field extensions, we need to consider mappings of extensions. Let K and L be extension fields of F. An F homomorphism $\tau : K \to L$ is a ring homomorphism such that $\tau(a) = a$ for all $a \in F$; that is, $\tau|_F = \mathrm{id}$. If τ is a bijection, then τ is called an F-isomorphism. An F-isomorphism from a field K to itself is called an F-automorphism.

Let us point out some simple properties of F-homomorphisms. If $\tau : K \to L$ is an F-homomorphism of extension fields of F, then τ is also a linear transformation of F-vector spaces, since $\tau(\alpha a) = \tau(\alpha)\tau(a) = \alpha\tau(a)$ for $\alpha \in F$ and $a \in K$. Furthermore, $\tau \neq 0$, so τ is injective since K is a field. Also, if $[K : F] = [L : F] < \infty$, then τ is automatically surjective by dimension counting. In particular, any F-homomorphism from K to itself is a bijection, provided that $[K : F] < \infty$.

Definition : Let K be a field extension of F. The Galois group $\mathrm{Gal}(K/F)$ us the set of all F-automorphisms of K.

If $K = F(X)$ is generated over F by a subset X, we can determine the F-automorphisms of K in terms of their action on the generating set X. For instance, if K is an extension of F that is generated by the roots of a polynomial $f(x) \in F[x]$, the following two lemmas will allow us to interpret the Galois group $\mathrm{Gal}(K/F)$ as a group of permutations of the roots of f. This type of field extension obtained by adjoining to a base field roots of a polynomial is extremely important. One use of these two lemmas will be to help calculate Galois groups, as shown in the examples below.

Lemma : Let $K = F(X)$ be a field extension of F that is generated by a subset X

of K. If $\sigma, \tau \in \operatorname{Gal}(K/F)$ with $\left.\sigma\right|_X = \left.\tau\right|_X$, then $\sigma = \tau$. Therefore, F-automorphisms of K are determined by their action on a generating set.

Proof. Let $a \in K$. Then there is a finite subset $\{\alpha_1, \ldots, \alpha_n\} \subseteq X$ with $a \in F(\alpha_1, \ldots, \alpha_n)$. This means there are polynomials $f, g \in F[x_1, \ldots, x_n]$ with $a = f(\alpha_1, \ldots, \alpha_n) / g(\alpha_1, \ldots, \alpha_n)$; say

$$\begin{aligned} f(x_1, \ldots, x_n) &= \sum b_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}, \\ g(x_1, \ldots, x_n) &= \sum c_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}, \end{aligned}$$

where each coefficient is in F. Since σ and τ preserve addition and multiplication, and fix elements of F, we have

$$\begin{aligned} \sigma(a) &= \sum \frac{b_{i_1 i_2 \cdots i_n} \sigma(\alpha_1)^{i_1} \sigma(\alpha_2)^{i_2} \cdots \sigma(\alpha_n)^{i_n}}{i_{i_1 i_2 \cdots i_n} \sigma(\alpha_1)^{i_1} \sigma(\alpha_2)^{i_2} \cdots \sigma(\alpha_n)^{i_n}} \\ &= \sum \frac{b_{i_1 i_2 \cdots i_n} \tau(\alpha_1)^{i_1} \tau(\alpha_2)^{i_2} \cdots \tau(\alpha_n)^{i_n}}{c_{i_1 i_2 \cdots i_n} \tau(\alpha_1)^{i_1} \tau(\alpha_2)^{i_2} \cdots \tau(\alpha_n)^{i_n}} \\ &= \tau(a). \end{aligned}$$

Thus, $\sigma = \tau$, so F-automorphisms are determined by their action on generators.

Lemma : Let $\tau : K \to L$ be an F-homomorphism and let $\alpha \in K$ be algebraic over F. If $f(x)$ is a polynomial over F with $f(\alpha) = 0$, then $f(\tau(\alpha)) = 0$. Therefore, τ permutes the roots of $\min(F, \alpha)$. Also, $\min(F, \alpha) = \min(F, \tau(\alpha))$.

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$. Then

$$0 = \tau(0) = \tau(f(\alpha)) = \sum_i \tau(a_i) \tau(\alpha)^i.$$

But, since each $a_i \in F$, we have $\tau(a_i) = a_i$. Thus, $0 = \sum_i a_i \tau(\alpha)^i$, so $f(\tau(\alpha)) = 0$. In particular, if $p(x) = \min(F, \alpha)$, then $p(\tau(\alpha)) = 0$, so $\min(F, \tau(\alpha))$ divides $p(x)$. Since $p(x)$ is irreducible, $\min(F, \tau(\alpha)) = p(x) = \min(F, \alpha)$.

Corollary : If $[K : F] < \infty$, then $|\operatorname{Gal}(K/F)| < \infty$.

Proof. We can write $K = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_i \in K$. Any F automorphism of K is determined by what it does to the α_i. By Lemma 2.3 , there are only finitely many possibilities for the image of any α_i; hence, there are only finitely many automorphisms of K/F.

Example: The Galois group of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is $\langle\mathrm{id}\rangle$. To see this, if σ is a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[3]{2})$, then $\sigma(\sqrt[3]{2})$ is a root of $\min(\mathbb{Q}, \sqrt[3]{2}) = x^3 - 2$. If $\omega = e^{2\pi i/3}$, then the roots of this polynomial are $\sqrt[3]{2}, \omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$. The only root of $x^3 - 2$ that lies in $\mathbb{Q}(\sqrt[3]{2})$ is $\sqrt[3]{2}$, since if another root lies in this field, then $\omega \in \mathbb{Q}(\sqrt[3]{2})$, which is false since $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Therefore, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, and since σ is determined by its action on the generator $\sqrt[3]{2}$, we see that $\sigma = \mathrm{id}$.

Lemma : Let K be a field. 1. If $L_1 \subseteq L_2$ are subfields of K, then $\operatorname{Gal}(K/L_2) \subseteq \operatorname{Gal}(K/L_1)$. 2. If L is a subfield of K, then $L \subseteq \mathcal{F}(\operatorname{Gal}(K/L))$. 3. If $S_1 \subseteq S_2$ are subsets of $\operatorname{Aut}(K)$, then $\mathcal{F}(S_2) \subseteq \mathcal{F}(S_1)$. 4. If S is a subset of $\operatorname{Aut}(K)$, then $S \subseteq \operatorname{Gal}(K/\mathcal{F}(S))$. 5. If $L = \mathcal{F}(S)$ for some $S \subseteq \operatorname{Aut}(K)$, then $L = \mathcal{F}(\operatorname{Gal}(K/L))$. 6. If $H = \operatorname{Gal}(K/L)$ for some subfield L of K, then $H = \operatorname{Gal}(K/\mathcal{F}(H))$.

Proof. The first four parts are simple consequences of the definitions. We leave the proofs of parts 2,3 , and 4 to the reader and prove part 1 for the sake of illustration. If $\sigma \in \operatorname{Gal}(K/L_2)$, then $\sigma(a) = a$ for all $a \in L_2$. Thus, $\sigma(a) = a$ for all $a \in L_1$, as $L_1 \subseteq L_2$, so $\sigma \in \operatorname{Gal}(K/L_1)$.

To prove part 5 , suppose that $L = \mathcal{F}(S)$ for some subset S of $\operatorname{Aut}(K)$. Then $S \subseteq \operatorname{Gal}(K/L)$, so $\mathcal{F}(\operatorname{Gal}(K/L)) \subseteq \mathcal{F}(S) = L$. But $L \subseteq \mathcal{F}(\operatorname{Gal}(K/L))$, so $L = \mathcal{F}(\operatorname{Gal}(K/L))$. For part 6, if $H = \operatorname{Gal}(K/L)$ for some subfield L of K, then $L \subseteq \mathcal{F}(\operatorname{Gal}(K/L))$, so

$$\operatorname{Gal}(K/\mathcal{F}(\operatorname{Gal}(K/L))) \subseteq \operatorname{Gal}(K/L) = H$$

However, by part 4 we have $H \subseteq \operatorname{Gal}(K/\mathcal{F}(H))$, so $H = \operatorname{Gal}(K/\mathcal{F}(H))$.

Corollary : If K is a field extension of F, then there is $1-1$ inclusion reversing correspondence between the set of subgroups of $\operatorname{Gal}(K/F)$ of the form $\operatorname{Gal}(K/L)$ for some subfield L of K containing F and the set of subfields of K that contain F of the form $\mathcal{F}(S)$ for some subset S of $\operatorname{Aut}(K)$. This correspondence is given by $L \mapsto \operatorname{Gal}(K/L)$, and its inverse is given by $H \mapsto \mathcal{F}(H)$.

Proof. This follows immediately from the lemma. If $\mathcal{G}$ and $\mathcal{F}$ are respectively the set of groups and fields in question, then the map that sends a subfield L of K to the subgroup $\operatorname{Gal}(K/L)$ of $\operatorname{Aut}(K)$ sends $\mathcal{F}$ to $\mathcal{G}$. This map is injective and surjective by part 5 of the lemma. Its inverse is given by sending H to $\mathcal{F}(H)$ by part 6 .

If K/F is a finite extension, under what circumstances does the association $L \mapsto \operatorname{Gal}(K/L)$ give an inclusion reversing correspondence between the set of all subfields of K containing F and the set of all subgroups of $\operatorname{Gal}(K/F)$? A necessary condition from part 5 is that $F = \mathcal{F}(\operatorname{Gal}(K/F))$. We shall see in Section 5 that this is actually a sufficient condition.

The next three results aim at getting more precise numerical information on $|\operatorname{Gal}(K/F)|$ for a finite extension K/F. We first need a definition.

Definition : If G is a group and if K is a field, then a character is a group homomorphism from G to K^*.

By setting $G = K^*$, we see that F-automorphisms of K can be viewed as characters from G to K^*. The next lemma will lead to a bound on $|\operatorname{Gal}(K/F)|$.

Lemma : (Dedekind's Lemma) Let $\tau_1, \ldots, \tau_n$ be distinct characters from G to K^*. Then the τ_i are linearly independent over K; that is, if $\sum_i c_i \tau_i(g) = 0$ for all $g \in G$, where the $c_i \in K$, then all $c_i = 0$.

Proof. Suppose that the lemma is false. Choose k minimal (relabeling the τ_i if necessary) so that there are $c_i \in K$ with $\sum_i c_i \tau_i(g) = 0$ for all $g \in G$. Then all $c_i \neq 0$. Since $\tau_1 \neq \tau_2$, there is an $h \in G$ with $\tau_1(h) \neq \tau_2(h)$. We have $\sum_{i=1}^k (c_i \tau_1(h)) \tau_i(g) = 0$ and

$$\sum_{i=1}^k c_i \tau_i(hg) = \sum_i (c_i \tau_i(h)) \tau_i(g) = 0$$

for all g. Subtracting gives $\sum_{i=1}^k (c_i (\tau_1(h) - \tau_i(h))) \tau_i(g) = 0$ for all g. This is an expression involving $k-1$ of the τ_i with not all of the coefficients zero. This contradicts the mimimality of k, so the lemma is proved.

There is a vector space interpretation of Dedekind's lemma. If V is the set of all functions from G to K, then V is a K-vector space under usual function addition and scalar multiplication, and Dedekind's lemma can be viewed as showing that the set of characters from G to K^* forms a linearly independent set in V.

$Proposition : If\ K is\ a\ finite\ field\ extension\ of$ F, $then$—$\operatorname{Gal}(K/F)| \leq [K : F]$.

Proof. The group $\operatorname{Gal}(K/F)$ is finite . Let $\operatorname{Gal}(K/F) = \{\tau_1, \ldots, \tau_n\}$, and suppose that $[K : F] < n$. Let $\alpha_1, \ldots, \alpha_m$ be a basis for K as an F-vector space. The matrix

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \cdots & \tau_1(\alpha_m) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \cdots & \tau_2(\alpha_m) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \cdots & \tau_n(\alpha_m) \end{pmatrix}$$

over K has $\operatorname{rank}(A) \leq m < n$, so the rows of A are linearly dependent over K. Thus, there are $c_i \in K$, not all zero, such that $\sum_i c_i \tau_i(\alpha_j) = 0$ for all j. If we set $G = K^*$, then for $g \in G$ there are $a_i \in F$ with $g = \sum_j a_j \alpha_j$. Thus,

$$\begin{aligned} \sum_i c_i \tau_i(g) &= \sum_i c_i \tau_i \left(\sum_j a_j \alpha_j \right) = \sum_i c_i \left(a_j \sum_j \tau_j(\alpha_j) \right) \\ &= \sum_j a_j \left(\sum_i c_i \tau_i(\alpha_j) \right) = 0 \end{aligned}$$

All the c_i are then 0 by Dedekind's lemma. This contradiction proves that $\operatorname{Gal}(K/F) \leq [K : F]$.

The following question arises naturally from this proposition: For which field extensions K/F does $|\operatorname{Gal}(K/F)| = [K : F]$?

The next proposition determines when $|\operatorname{Gal}(K/F)| = [K : F]$, provided that the group $\operatorname{Gal}(K/F)$ is finite.

Proposition : Let G be a finite group of automorphisms of K with $F = \mathcal{F}(G)$. Then $|G| = [K : F]$, and so $G = \operatorname{Gal}(K/F)$.

Proof. By the previous proposition, $|G| \leq [K : F]$ since $G \subseteq \operatorname{Gal}(K/F)$. Suppose that $|G| < [K : F]$. Let $n = |G|$, and take $\alpha_1, \ldots, \alpha_{n+1} \in K$ linearly independent over F. If $G = \{\tau_1, \ldots, \tau_n\}$, let A be the matrix

$$A = \begin{pmatrix} \tau_1(\alpha_1) & \tau_1(\alpha_2) & \cdots & \tau_1(\alpha_{n+1}) \\ \tau_2(\alpha_1) & \tau_2(\alpha_2) & \cdots & \tau_2(\alpha_{n+1}) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_n(\alpha_1) & \tau_n(\alpha_2) & \cdots & \tau_n(\alpha_{n+1}) \end{pmatrix}.$$

Then the columns of A are linearly dependent over K. Choose k minimal so that the first k columns of A are linearly dependent over K (relabeling if necessary). Thus, there are $c_i \in K$ not all zero with $\sum_{i=1}^{k} c_i \tau_j(\alpha_i) = 0$ for all j. Minimality of k shows all $c_i \neq 0$. Thus, by dividing we may assume that $c_1 = 1$. If each $c_i \in F$, then $0 = \tau_j\left(\sum_{i=1}^{k} c_i \alpha_i\right)$ for each j, so $\sum_{i=1}^{k} c_i \alpha_i = 0$. This is false by the independence of the α_i over F. Take $\sigma \in G$. Since σ permutes the elements of G, we get $\sum_{i=1}^{k} \sigma(c_i)\, \tau_j(\alpha_i) = 0$ for all j. Subtracting this from the original equation and recalling that $c_1 = 1$ gives $\sum_{i=2}^{k} (c_i - \sigma(c_i))\, \tau_j(\alpha_i) = 0$ for all j. Minimality of k shows that $c_i - \sigma(c_i) = 0$ for each i. Since this is true for all $\sigma \in G$, we get all $c_i \in \mathcal{F}(G) = F$. But we have seen that this leads to a contradiction. Thus $|G| = [K : F]$. In particular, $G = \operatorname{Gal}(K/F)$, since $G \subseteq \operatorname{Gal}(K/F)$ and $|G| = [K : F] \geq |\operatorname{Gal}(K/F)|$.

The field extensions described in the above proposition are those of particular interest to us, as they were to Galois in his work on the solvability of polynomials.

Definition : Let K be an algebraic extension of F. Then K is Galois over F if $F = \mathcal{F}(\operatorname{Gal}(K/F))$.

If $[K : F] < \infty$, then the above proposition gives us a numerical criterion for when K/F is Galois.

Corollary : Let K be a finite extension of F. Then K/F is Galois if and only if $|\operatorname{Gal}(K/F)| = [K : F]$.

Proof. If K/F is a Galois extension, then $F = \mathcal{F}(\operatorname{Gal}(K/F))$, so by the above proposition, $|\operatorname{Gal}(K/F)| = [K : F]$. Conversely, if $|\operatorname{Gal}(K/F)| = [K : F]$, let $L = \mathcal{F}(\operatorname{Gal}(K/F))$. Then $\operatorname{Gal}(K/L) = \operatorname{Gal}(K/F)$ by Proposition 2.14, and so $|\operatorname{Gal}(K/F)| = [K : L] \leq [K : F]$. Since $|\operatorname{Gal}(K/F)| = [K : F]$, this forces $[K : L] = [K : F]$, so $L = F$.

Corollary : Let K be a field extension of F, and let $a \in K$ be algebraic over F. Then $|\operatorname{Gal}(F(a)/F)|$ is equal to the number of distinct roots of $\min(F, a)$ in $F(a)$. Therefore, $F(a)$ is Galois over F if and only if $\min(F, a)$ has n distinct roots in $F(a)$, where $n = \deg(\min(F, a))$.

Proof. If $\tau \in \operatorname{Gal}(F(a)/F)$, we have seen that $\tau(a)$ is a root of $\min(F, a)$. Moreover, if $\sigma, \tau \in \operatorname{Gal}(F(a)/F)$ with $\sigma \neq \tau$, then $\sigma(a) \neq \tau(a)$, since F automorphisms on $F(a)$ are determined by their action on a. Therefore, $|\operatorname{Gal}(F(a)/F)| \leq n$. Conversely, let b be a root in $F(a)$ of $\min(F, a)$. Define $\tau : F(a) \to F(a)$ by $\tau(f(a)) = f(b)$ for any $f(x) \in F[x]$. This map is well defined precisely because b is a root of $\min(F, a)$. It is straightforward to show that τ is an F-automorphism, and $\tau(a) = b$ by the definition of τ. Thus, $|\operatorname{Gal}(F(a)/F)|$ is equal to the number of distinct roots of $\min(F, a)$ in $F(a)$. Since $[F(a) : F] = \deg(\min(F, a))$, we see that $F(a)$ is Galois over F if and only if $\min(F, a)$ has n distinct roots in $F(a)$.

There are two ways that a field extension $F(a)/F$ can fail to be Galois. First, if $p(x) = \min(F, a)$, then p could fail to have all its roots in $F(a)$. Second, $p(x)$ could have repeated roots. The next two sections will address these concerns. We finish this section with a number of examples of extensions for which we determine whether or not they are Galois. Here and elsewhere in this book, we use the idea of the characteristic of a field (or a ring with identity). For the reader unfamiliar with this notion, the characteristic $\operatorname{char}(F)$ of a field F is the order of the multiplicative identity 1 as an element of the additive group $(F, +)$, provided that this order is finite, or else $\operatorname{char}(F) = 0$ if this order is infinite. Note that the characteristic of a field is either 0 or is a prime number.

Example : The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois, for we have seen that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ but $|\operatorname{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1$. The polynomial $x^3 - 2$ has three distinct roots, but only one of them lies in $\mathbb{Q}(\sqrt[3]{2})$.

Chapter 5

Ruler and Compass Constructions

In the days of the ancient Greeks, some of the major mathematical questions involved constructions with ruler and compass. In spite of the ability of many gifted mathematicians, a number of questions were left unsolved. It was not until the advent of field theory that these questions could be answered. We consider in this section the idea of constructibility by ruler and compass, and we answer the following four classical questions:

1. Is it possible to trisect any angle?
2. Is it possible to double the cube? That is, given a cube of volume V, a side of which can be constructed, is it possible to construct a line segment whose length is that of the side of a cube of volume $2V$?
3. Is it possible to square the circle? That is, given a constructible circle of area A, is it possible to construct a square of area A?
4. For which n is it possible to construct a regular n-gon?

The notion of ruler and compass construction was a theoretical one to the Greeks. A ruler was taken to be an object that could draw perfect, infinitely long lines with no thickness but with no markings to measure distance. The only way to use a ruler was to draw the line passing through two points. Similarly, a compass was taken to be a device that could draw a perfect circle, and the only way it could be used was to draw the circle centered at one point and passing through another. The compass was sometimes referred to as a "collapsible compass"; that is, after drawing a circle, the compass could not be lifted to draw a circle centered at another point with the same radius as that of the previous circle. Likewise, given two points a distance d apart, the ruler cannot be used to mark a point on another line a distance d from a given point on the line. The assumptions of constructibility are as follows. Two points are given and are taken to be the initial constructible points. Given any two constructible points, the line through these points can be constructed, as can the circle centered at one point passing through the other. A point is constructible if it is the intersection of constructible lines and circles.

The first thing we note is that the collapsibility of the compass is not a problem, nor is not being able to use the ruler to mark distances. Given two constructible points a distance d apart, and a line *l*with a point P on £, we can construct a point Q on *l* a distance d from P. Also, if we can construct a circle of radius r, given any constructible point P, we can construct the circle of radius r centered at P.

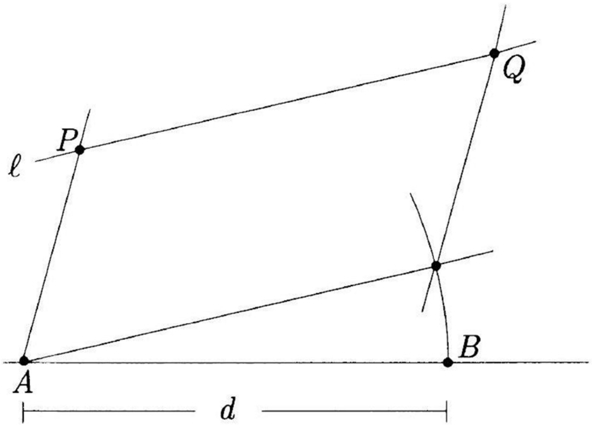
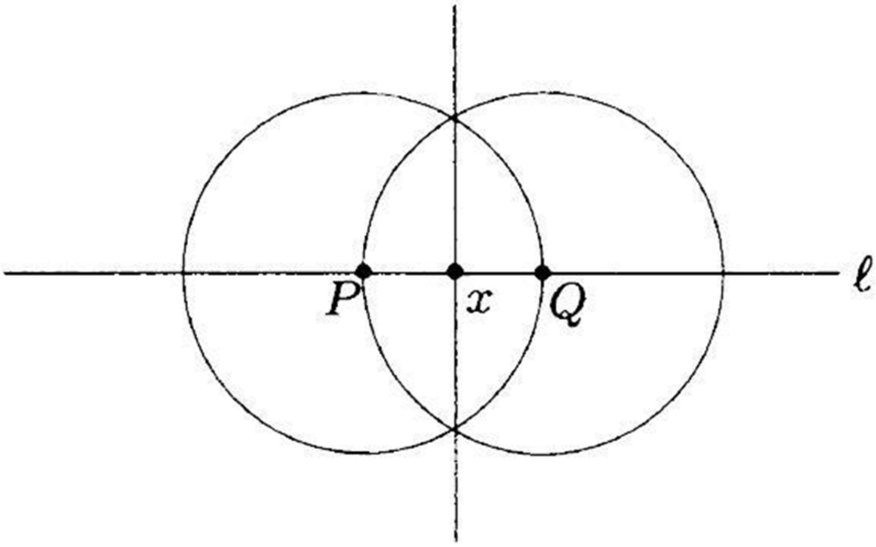


FIGURE 4.1.*Construction of Q on l a distance d from P.*

There are some standard constructions from elementary geometry that we recall now. Given a line and a point on the line, it is possible to construct a second line through the point perpendicular to the original line. Also, given a line and a point not on the line, it is possible to construct a second line parallel to the original line and passing through the point.



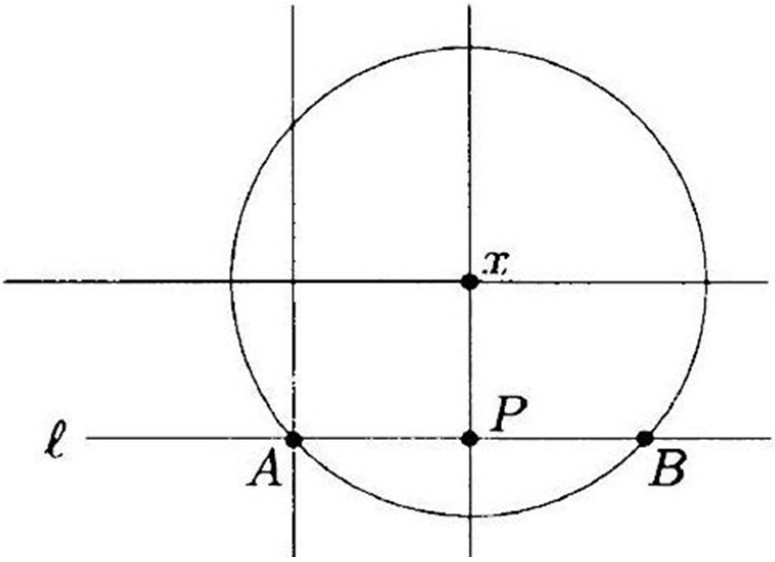


FIGURE 4.2.*Construction of lines perpendicular and parallel to l passing through x.*

So far, our discussion has been purely geometric. We need to describe ruler and compass constructions algebraically in order to answer our four questions. To do this, we turn to the methods of analytic geometry. Given

our original two points, we set up a coordinate system by defining the x- axis to be the line through the points, setting one point to be the origin and the other to be the point $(1, 0)$. We can draw the line perpendicular to the x-axis through the origin to obtain the y-axis. Let $a \in \mathbb{R}$. We say that a is a constructible number if we can construct two points a distance $|a|$ apart. Equivalently, a is constructible if we can construct either of the points $(a, 0)$ or $(0, a)$. If a and b are constructible numbers, elementary geometry tells us that $a + b$, $a - b$, ab, and a/b (if $b \neq 0$) are all constructible. Therefore, the set of all constructible numbers is a subfield of $\mathbb{R}$. Furthermore, if $a > 0$ is constructible, then so is $\sqrt{a}$. These facts are illustrated in Figures later.

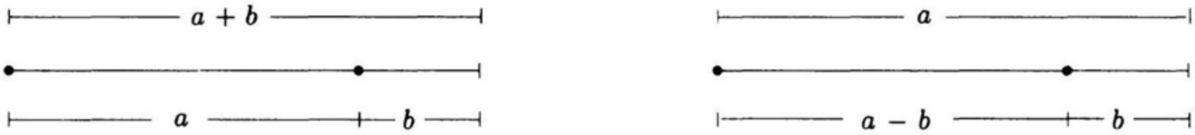


FIGURE 4.3. *Construction of* $a + b$ *and* $a - b$.

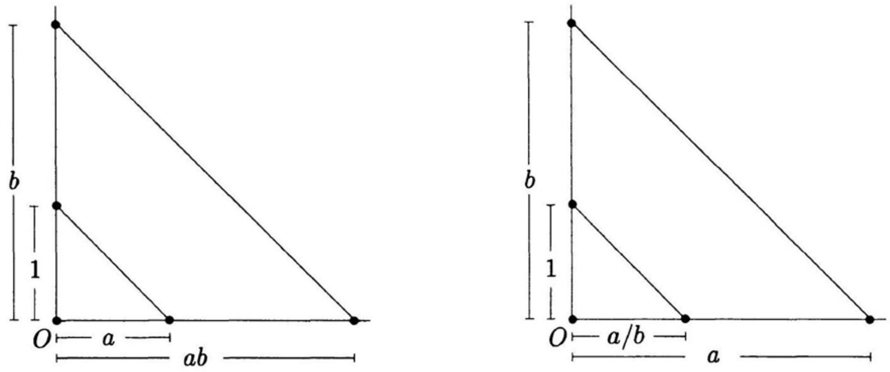


FIGURE 4.4. *Construction of ab and a/b.*

Suppose that P is a constructible point, and set $P = (a, b)$ in our coordinate system. We can construct the lines through P perpendicular to the x-axis and y-axis; hence, we can construct the points $(a, 0)$ and $(0, b)$. Therefore, a and b are constructible numbers. Conversely, if a and b are constructible numbers, we can construct $(a, 0)$ and $(0, b)$, so we can construct P as the intersection of the line through $(a, 0)$ parallel to the y-axis with the line through $(0, b)$ parallel to the x-axis. Thus, $P = (a, b)$ is constructible if and only if a and b are constructible numbers. In order to construct a number e, we must draw a finite number of lines and circles in such a way that $|e|$ is the distance between two points of intersection. Equivalently, we must draw lines and circles so that $(e, 0)$ is a point of intersection. If we let K be the field generated over $\mathbb{Q}$ by all the numbers obtained in some such construction, we obtain a subfield of the field of constructible numbers. To give a criterion for when a number is constructible, we need to relate constructibility to properties of the field extension $K/\mathbb{Q}$. We do this with analytic geometry. Let K be a subfield of $\mathbb{R}$. Given any two points in the plane of K, we obtain a line through these points. This will be called a line in K. It is not hard to show that a line in K has an equation of the form $ax + by + c = 0$ with $a, b, c \in K$. If P and Q are points in the plane of K, the circle with center P passing through Q is called a circle in K. Again, it is not hard to show that the equation of a circle in K can be written in the form $x^2 + y^2 + ax + by + c = 0$ for some $a, b, c \in K$. The next lemma gives us a connection between constructibility and field extensions.

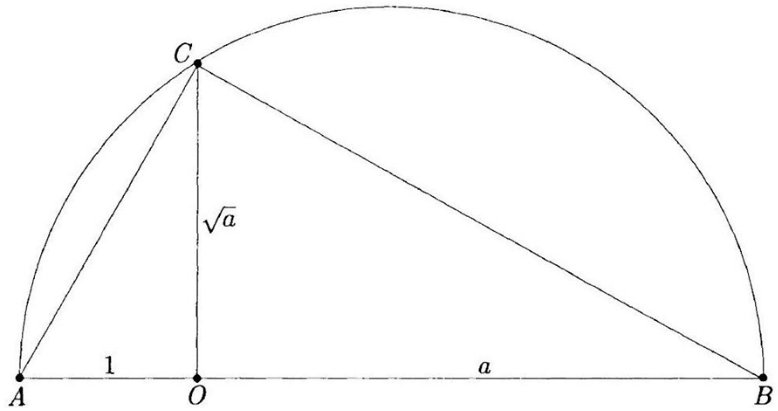


FIGURE 4.5 *Construction of* $\sqrt{a}$.

Lemma Let K be a subfield of $\mathbb{R}$.
1. The intersection of two lines in K is either empty or is a point in the plane of K.
2. The intersection of a line and a circle in K is either empty or consists of one or two points in the plane of $K(..JU)$ for some $u \in K$ with $u \geq 0$.
3. The intersection of two circles in K is either empty or consists of one or two points in the plane of $K(..JU)$ for some $u \in K$ with $u \geq 0$. *Proof.* The first statement is an easy calculation. For the remaining two statements, it suffices to prove statement 2, since if $x^2+y^2+ax+by+c=0$ and $x^2+y^2+a'x+b'y+c'=0$ are the equations of circles C and C', respectively, then their intersection is the intersection of C with the line $(a-a')x+(b-b')y+(c-c')=0$. So, to prove statement 2, suppose that our line L in K has the equation $dx+ey+f=0$. We assume that $d \neq 0$, since if $d=0$, then $e \neq 0$. By dividing by d, we may then assume that $d=1$. Plugging $-x = ey+f$ into the equation of C, we obtain $(e^2+1)y^2+(2ef-ae+b)y+(J^2-af+c)=0$. Writing this equation in the form $\alpha y^2+\beta y+\gamma=0$, if $\alpha=0$, then $y \in K$. If $\alpha \neq 0$, then completing the square shows that either $L \cap C = 0$ or $y \in K(\sqrt{\beta^2-4\alpha\gamma})$ with $\beta^2-4\alpha\gamma \geq 0$.

From this lemma, we can turn the definition of constructibility into a property of field extensions of $\mathbb{Q}$, and in doing so obtain a criterion for when a number is constructible. **Theorem .***A real number c is constructible if and only if there is a tower of fields* $\mathbb{Q} = K_0 \sim K_1 \sim \cdots \sim K_r$ *such that* $c \in K_r$ *and* $[K_{i+1} : K_i] \leq 2$ *for each i. Therefore, if c is constructible, then c is algebraic over* $\mathbb{Q}$*, and* $[\mathbb{Q}(c) : \mathbb{Q}]$ *is a power of 2.*

Proof. If c is constructible, then the point $(c, 0)$ can be obtained from a finite sequence of constructions starting from the plane of $\mathbb{Q}$. We then obtain a finite sequence of points, each an intersection of constructible lines and circles, ending at $(c, 0)$. By Lemma 1, the first point either lies in $\mathbb{Q}$ or in $\mathbb{Q}(\sqrt{U})for\,some\,u$. This extension has degree either 1 or 2. Each time we construct a new point, we obtain a field extension whose degree over the previous field is either 1 or 2 by the lemma. Thus, we obtain a sequence of fields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_r$ with $[K_{i+l} : K_i] \leq 2$ and $c \in K_r$. Therefore, $[K_r : \mathbb{Q}] = 2^n$ for some n. However, $[\mathbb{Q}(c) : \mathbb{Q}]$ divides $[K_r : \mathbb{Q}]$, so $[\mathbb{Q}(c) : \mathbb{Q}]$ is also a power of 2.

For the converse, suppose that we have a tower $Q = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$ with $c \in K_r$ and $[K_{i+1} : K_i] \leq 2$ for each i. We show that c is constructible by induction on r. If $r = 0$, then $c \in Q$, so c is constructible.
Assume then that $r > 0$ and that elements of K_{r-1} are constructible. Since $[K_r : K_{r-1}] \leq 2$, the quadratic formula shows that we may write
$K_r = K_{r-1}(\sqrt{a})$ for some $a \in K_{r-1}$. Since a is constructible by assump- tion, so is $\sqrt{a}$. Therefore, $K_r = K_{r-1}(\sqrt{a})$ lies in the field of constructible numbers; hence, c is constructible.

With this theorem, we are now able to answer the four questions posed earlier. We first consider trisection of angles. An angle of measure θ is constructible if we can construct two intersecting lines such that the angle between them is θ. For example, a 60° angle can be constructed because the point $(\frac{3}{2}, \frac{1}{2})$ is constructible, and the line through this point and (0,0) makes an angle of 60° with the x-axis. Suppose that P is the point of intersection on two constructible lines. By drawing a circle of radius 1 centered at P,now if θ is the angle between the two lines, then $\sin(\theta)$ and $\cos(\theta)$ are constructible numbers. Conversely, if $\sin(\theta)$ and $\cos(\theta)$ are constructible, then θ is a constructible angle . In order to trisect an angle of measure θ, we would need to be able to construct an angle of $\theta/3$.

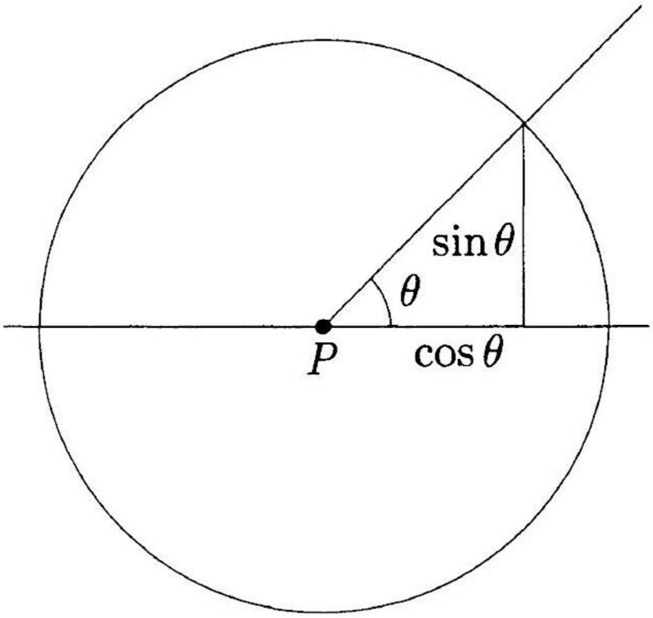


FIGURE 4.6. *Construction of sines and cosines.*

Theorem *It is impossible to trisect a* 60° *angle by ruler and compass construction.*

Proof. As noted above, a 60° angle can be constructed. If a 60° angle can be trisected, then it is possible to construct the number $\alpha = \cos 20°$. However, the triple angle formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ gives $4\alpha^3 - 3\alpha = \cos 60° = 1/2$. Thus, α is algebraic over $\mathbb{Q}$. The polynomial $8x^3 - 6x - 1$ is irreducible over $\mathbb{Q}$ because it has no rational roots. Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, so α is not constructible. A 20° angle cannot then be constructed, so a 60° degree angle cannot be trisected.

This theorem does not say that no angle can be trisected. A 90° angle can be trisected, since a 30° angle can be constructed. This theorem only says that not all angles can be trisected, so there is no method that will trisect an arbitrary angle.

The second classical impossibility we consider is the doubling of a cube.

Theorem . *It is impossible to double a cube of length 1 by ruler and compass construction.*

Proof. The length of a side of a cube of volume 2 is $\sqrt[3]{2}$. The minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $x^3 - 2$. Thus, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of 2 , so $\sqrt[3]{2}$ is not constructible.

The third of the classical impossibilities is the squaring of a circle. For this, we need to use the fact that π is transcendental over $\mathbb{Q}$.

Theorem. *It is impossible to square a circle of radius 1.*

Proof. We are asking whether we can construct a square of area π. To do so requires us to construct a line segment of length $\sqrt{\pi}$, which is impossible since $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$ by the Lindemann-Weierstrauss theorem; hence, $\sqrt{\pi}$ is not algebraic of degree a power of 2 .

Our last question concerns construction of regular n-gons. To determine which regular n-gons can be constructed, we will need information about cyclotomic extensions. Recall from Section 7 that if ω is a primitive nth root of unity, then $[\mathbb{Q}(\omega):\mathbb{Q}]=\phi(n)$, where ϕ is the Euler phi function.

Theorem. *A regular n-gon is constructible if and only if $\phi(n)$ is a power of 2.*
Proof. We point out that a regular n-gon is constructible if and only if the central angles $2\pi/n$ are constructible, and this occurs if and only if $\cos(2\pi/n)$ is a constructible number. Let $\omega = e^{2\pi i/n} = \cos(2\pi/n)+\ i\sin(2\pi/n)$, a primitive nth root of unity. Then $\cos(2\pi/n)=\frac{1}{2}\left(\omega+\omega^{-1}\right)$, since $\omega^{-1}=\cos(2\pi/n)-i\sin(2\pi/n)$. Thus, $\cos(2\pi/n)\in\mathbb{Q}(\omega)$. However, $\cos(2\pi/n)\in\mathbb{R}$ and $\omega\notin\mathbb{R}$, so $\mathbb{Q}(\omega)\neq\mathbb{Q}(\cos(2\pi/n))$. But ω is a root of $x^2-\ 2\cos(2\pi/n)x+1$, as an easy calculation shows, so $[\mathbb{Q}(\omega):\mathbb{Q}(\cos(2\pi/n))]=2$. Therefore, if $\cos(2\pi/n)$ is constructible, then $[\mathbb{Q}(\cos(2\pi/n)):\mathbb{Q}]$ is a power of 2. Hence, $\phi(n)=[\mathbb{Q}(\omega):\mathbb{Q}]$ is also a power of 2.

Conversely, suppose that $\phi(n)$ is a power of 2 . The field $\mathbb{Q}(\omega)$ is a Galois extension of $\mathbb{Q}$ with Abelian Galois group by Proposition 7.2. If $H=\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\cos(2\pi/n)))$, by the theory of finite Abelian groups there is a chain of subgroups

$$H_0\subseteq H_1\subseteq\cdots\subseteq H_r=H$$

with $|H_{i+1}:H_i|=2$. If $L_i=\mathcal{F}(H_i)$, then $[L_i:L_{i+1}]=2$; thus, $L_i=L_{i+1}\left(\sqrt{u_i}\right)$ for some u_i. Since $L_i\subseteq\mathbb{Q}(\cos(2\pi/n))\subseteq\mathbb{R}$, each of the $u_i\geq 0$. Since the square root of a constructible number is constructible, we see that everything in $\mathbb{Q}(\cos(2\pi/n))$ is constructible. Thus, $\cos(2\pi/n)$ is constructible, so a regular n-gon is constructible.

This theorem shows, for example, that a regular 9-gon is not constructible and a regular 17-gon is constructible. An explicit algorithm for constructing a regular 17-gon was given by Gauss in 1801. If $n=p_1^{m_1}\cdots p_r^{m_r}$ is the prime factorization of n, then $\phi(n)=\prod_i p^{m_i-1}\left(p_i-1\right)$. Therefore, $\phi(n)$ is a power of 2 if and only if $n=2^s q_1\cdots q_r$, where $r,s\geq 0$, and the q_i are primes of the form 2^m+1. In order to determine which regular n-gons are constructible, it then reduces to determining the primes of the form 2^m+1.

Chapter 6

Neusis Construction

Definition 5.1. The neusis is a geometric construction method that was generally used in antiquity by greek mathematicians .

Definition 5.2. A neusis ruler is a marked ruler that can be rotated around a constructible point P.

Motivation and Uses

The study of methods that accomplish trisections is vast and extends back in time approximately 2300 years. A very interesting method of trisection from the Ancients is due to

Archimedes, who performed a "neusis" between a circle and line. Basically a neusis (or use of a marked ruler) allows the marking of points on constructed objects of unit distance apart using a ruler placed so that it passes through some known (constructed) point P. The Greek word "neusis" means "verging" and the process is to verge from line 1 to line 2 through point P.

Uses of neusis :

1. It can trisect any angle into three equal parts

2. We can double a cube using neusis construction

3. The construction of a regular heptagon, nonagon, hendecagon, or tridecagon (poly- gons with 7, 9, or 11, 13 sides).

4. Sir Isaac Newton followed their line of thought, and also used neusis constructions.

Chapter 7

Application of constructibility

Prove that length of three bisectors determine triangle.

Let the sides of the triangle be a,b,c and let the lengths of the three angle bisectors be l,m,n . We show first that

$$l = \frac{2}{b+c}\sqrt{bcs(s-a)}(*)$$

where $2s = a+b+c$.

Let the bisector AD have length l (and sides BC, CA, AB have lengths a, b, c respectively). Then area $ABD+$ area $ADC =$ area ABC. So we have $bc\sin A = bl\sin\frac{A}{2} + cl\sin\frac{A}{2}$ and hence $l = \frac{2bc}{b+c}\cos\frac{A}{2}$. The cosine formula gives $\cos A = \frac{b^2+c^2-a^2}{2bc}$, so $2\cos^2\frac{A}{2} = 1+\cos A = \frac{(b+c)^2-a^2}{2bc}$ and hence $\cos\frac{A}{2} = \frac{\sqrt{s(s-a)}}{bc}$ which gives (*).

Taking $4(*)^2$ we have $4l^2 = \frac{4}{(b+c)^2}bc(b+c+a)(b+c-a) = 4bc - \frac{4a^2bc}{(b+c)^2}$. Adding $a^2+(b-c)^2$ to both sides we get

$4l^2 + a^2 + (b-c)^2 = a^2 + (b+c)^2 - \frac{4a^2bc}{(b+c)^2} = (b+c)^2 + \frac{a^2(b-c)^2}{(b+c)^2}$. We now add $\pm 2a(b-c)$ to both sides to get

$$4l^2 + (a \pm (b-c))^2 = \left(b + c \pm \frac{a(b-c)}{b+c}\right)^2$$

Taking the square root for each choice of sign and adding we get

$$b+c = \sqrt{l^2+(s-b)^2} + \sqrt{l^2+(s-c)^2}$$

$\left[\text{note that } \frac{1}{2}(a+(b-c)) = s-c \text{ and } \frac{1}{2}(a-(b-c)) = s-b\right]$. Putting $x = s-a, y = s-b, z = s-c$ and defining $f(u,v) = \frac{1}{2}\left(\sqrt{u^2+v^2} - u\right)$, we can write this as

$$x = f(y,l) + f(z,l)$$

We obviously get also the corresponding equations

Now fix l, m, n and regard x, y, z simply as real variables. Let $K = [0,l] \times [0,m] \times [0,n] \subset \mathbb{R}^3$ and define $F : K \to \mathbb{R}^3$ by

$$F(x,y,z) = (f(y,l) + f(z,l), f(z,m) + f(x,m), f(x,n) + f(y,n))$$

The preceding work shows that (x,y,z) is a fixed point of F iff the triangle with side lengths $a = y+z, b = z+x, c = x+y$ has angle bisector lengths l, m, n.

Note that $0 \leq f(u,v) \leq \frac{1}{2}v$, so $F(x,y,z) \in K$ for $(x,y,z) \in K$. So by the Brouwer fixed point theorem, F must have a fixed point.

We have now established that some triangle has the given bisector lengths. It remains to show that it is unique. Fortunately only a little more work is required. We show that if $(x,y,z) \neq (x',y',z')$ then the distance between (x,y,z) and (x',y',z') is strictly less than the distance between $F(x,y,z)$ and $F(x',y',z')$. It follows that they cannot both be fixed points.

Note that $\left(\sqrt{y^2+l^2} - \sqrt{y'^2+l^2}\right)\left(\sqrt{y^2+l^2} + \sqrt{y'^2+l^2}\right) = y^2 - y'^2 = (y-y')(y+y')$, so we have $2\left|f(y,l) - f(y',l)\right| = \left|\sqrt{y^2+l^2} - y - \sqrt{y'^2+l^2} + y'\right| = |y-y'|\left|1 - \frac{y+y'}{\sqrt{y^2+l^2}+\sqrt{y^2+l^2}}\right| \leq | y$ with the inequality strict for $y \neq y'$.

So we have

$$\begin{aligned}
&|F(x,y,z) - F(x',y',z')|^2 \leq |f(y,l) - f(y',l) + f(z,l) - f(z',l)|^2 + |\ f(z,m) - f(z',m)\,.\\
&+ f(x,m) - f(x',m)|^2 + |f(x,n) - f(x',n) + f(y,n) - f(y',n)|^2\\
&< \left(\frac{1}{2}|y-y'| + \frac{1}{2}|z-z'|\right)^2 + \left(\frac{1}{2}|z-z'| + \frac{1}{2}|x-x'|\right)^2 + \left(\frac{1}{2}|x-x'| + \frac{1}{2}|y-y'|\right)^2
\end{aligned}$$

Note that the inequality is strict because at least one of $|x-x'|, |y-y'|, |z-z'|$ is non-zero.

Adding the non-negative quantity

$\left(\frac{1}{2}|y-y'| - \frac{1}{2}|z-z'|\right)^2 + \left(\frac{1}{2}|z-z'| - \frac{1}{2}|x-x'|\right)^2 + \left(\frac{1}{2}|x-x'| - \frac{1}{2}|y-y'|\right)^2$ the rhs becomes $|x-x'|^2 + |y-y'|^2 + |z-z'|^2$ and we have established $|F(x,y,z) - F(x',y',z')| < |(x,y,z) - (x',y',z')|$ as promised.

THEOREM . It is impossible to construct an isosceles triangle given the lengths of its 2 different bisectors (again, apart from the equilateral triangle). It is sufficient to prove this and it follows that the general triangle is also impossible to construct.

PROOF:

Isosceles triangle $\triangle ABC$, angles at vertices A and B equal, denote α. I is the incenter, i.e., the intersection of angle bisectors. $I_a = I_b, I_c$ are the bisector lengths. L_a, L_b, L_c are the intersections of sides a, b, c with the bisectors.

Consider triangle $\triangle ABC$ (or ΔAL_cC):

$$\mathrm{c/a} = 2\cos(\ \mathrm{d})$$

Consider triangle $\triangle \mathrm{ABL_a}$:

angle $\angle BL_aA = \pi - \alpha - \alpha/2 = \pi - 3/2\alpha$

$\mathrm{I}_a/C = \sin(\alpha)/\sin(3/2\alpha)$ Consider triangle $\Delta \mathrm{AL_cC}$:

$$I_c/a = \sin(\alpha)$$

Combining: $1/A_a = a/c\sin(3/2\alpha) = \sin(3/2\alpha)/(2\cos(\alpha))$

$$\sin(3/2\alpha) = \sin(\alpha)\cos(\alpha/2) + \cos(\alpha)\sin(\alpha/2)$$
$$\sin^2(3/2\alpha) = \sin^2(\alpha)\cos^2(\alpha/2) + \cos^2(\alpha)\sin^2(\alpha/2) + 2\sin(\alpha)\cos(\alpha)\sin(\alpha/2)\cos(\alpha/2)$$

Using $\sin^2(\alpha/2) = (1-\cos(\alpha))/2$ and $\cos^2(\alpha/2) = (1+\cos(\alpha))/2$,

$$\sin^2(3/2\alpha) = 1/2 + \left(3/2\sin^2(\alpha) - 1/2\cos^2(\alpha)\right)\cos(\alpha) = 1/2 + \left(3/2 - 2\cos^2(\alpha)\right)\cos(\alpha)$$

Let us denote $x = \cos(\alpha)$ and $k = I_C/l_a$. The problem is reduced to determining (constructing) $\cos(\alpha)$ from the bisector length ratio. This is equivalent to the following cubic equation

$$k^2 = \left(1/2 + 3/2x - 2x^3\right)/4x^2 \text{ or}$$
$$2x^3 + 4k^2x^2 - 3/2x - 1/2 = 0 \text{ or}$$
$$4x^3 + 8k^2x^2 - 3x - 1 = 0$$

It is easy to see that for $k = 1$ (equilateral triangle), the equation has rational root $x = \cos(\alpha) = 1/2, \alpha = \pi/3$. Suppose that the quadratic coefficient is some positive integer (of course, except 8), for example some prime number:

$$8k^2 = q > 0$$

Then the ratio k is always constructible (as a square root of rational number q/8). We can construct the bisector lengths $\mathrm{I_a}$ and $\mathrm{I_c}$ and try to construct $\cos(\alpha)$ to solve the problem for these particular lengths. This is generally impossible. It is sufficient to show that for some integer quadratic coefficient the above cubic equation has no rational root. Then no roots are constructible.

By the rational root theorem for polynomials with integer coefficients, the possible rational roots are $r = p/q$, where p is a divider of the absolute term (1 for our equation) and q is a divider of the highest power term coefficient (4 for our equation). The possible rational roots are $-1, +1, -1/2, +1/2, -1/4, +1/4$ and no others.

It is easy to find a positive integer for the quadratic term, for which our cubic equation has none of the above roots (almost any integer will do). Indeed, by calculating the value of $4x^3 - 3x - 1$ for all possible rational roots, which must be compensated by the quadratic term, we can quickly convince ourselves that the above cubic equation has rational root(s) for the following integer values of q only:

$$\begin{aligned}
&q = 0 : r_1 = +1, r_2 = -1/2, r_3 = -1/2\\
&q = 2 : r = -1\\
&q = 5 : r = -1/4\\
&q = 8 : r = +1/2\\
&q = 27 : r = +1/4
\end{aligned}$$

Therefore, $\cos(\alpha)$ is not constructible for all possible bisector length ratios.

REFERENCES

1] Patrick Morandi, Field and Galois Theory, Springer 1996.

2] R. C. Alperin, A mathematical theory of origami constructions and numbers, New York J. Math. 6 (2000) 119–133; also available at http://nyjm.albany.edu.

3] An origamic view of Alhazen's optical problem, in Proceedings of O3-Science, Education and Mathematics, T. Hull, ed., A. K. Peters, Natick, MA, 2002, pp. 83–93.

4] D. Auckly and J. Cleveland, Totally real origami and impossible paper folding, this MONTHLY 102 (1995) 215–226.

5] A. Baragar, Constructions using a compass and a twice-notched straightedge, this MONTHLY 109 (2002) 151–164.

6] J. W. Emert, K. I. Meeks, and R. B. Nelson, Reflections on a Mira, this MONTHLY 101 (1994) 544–549.

7] A. M. Gleason, Angle trisection, the heptagon, and the triskaidecagon, this MONTHLY 95 (1988) 185–194.

8] D. Hilbert, Foundations of Geometry, 10th ed. (trans. L. Unger), Open Court, La Salle, IL, 1971.

9] T. Hull, A note on “impossible” paper folding, this MONTHLY 103 (1996) 240–241.

10] N. Jacobson, Basic Algebra, 2 vols., W. H. Freeman, New York, 1985.

11] W. R. Knorr, The Ancient Tradition of Geometric Problems, Birkhǻuser, Boston, 1986.

12] A. I. Sabra, Ibn al-Haytham's lemmas for solving “Alhazen's problem,” Archive for History of Exact Sciences 26 (1982) 299–324.

13] C. R. Videla, On points constructible from conics, Math. Intelligencer 19 (1997) 53–57.

14] F. Vi`ete, The Analytic Art (1591) (transl. T. R. Witmer), Kent State University Press, Kent, OH, 1983.

ACKNOWLEDGEMENT

Here , in this paper , I ,Chandrani Sengupta , Roll No.:0035(MTMA) , Semester VI (3rd Year), have tried to construct a complete theory of **RULER , COMPASS AND NEUSIS CONSTRUCTIONS**. It would have been an onerous work to do the project without the assistance and encouragement of my respected supervisor , Professor Gaurab Tripathi. I am really thankful to our Head of Department, Professor Sucharita Roy, and St. Xavier's College(Autonomous) , Kolkata for giving me this extremely important opportunity, which furnished my knowledge with a professional taste of higher mathematics.

Prof.Gaurab Tripathi
Assistant Professor
Department of Mathematics
St. Xavier's College(Autonomous),Kolkata

THANKYOU