APPLICATION OF EULER'S PHI-FUNCTION IN ABSTRACT ALGEBRA

BY

PATIENCE AHIAKU (BSc. Mathematics)

A Thesis Submitted to the department of Mathematics, Kwame Nkrumah University of Science and Technology in Partial Fulfillment of the Degree of

MASTER OF PHILOSOPHY (PURE MATHEMATICS)

College of Science

April, 2014

DECLARATION

I hereby declare that this submission is my own work towards the MPhil and that, to the best of my knowledge, it contains no material previously published by another person nor material, which has been accepted for the award of any degree of the university, except where due acknowledgement has been made in the text.

Patience Ahiaku (PG5069510) ---------- ----------

Signature Date

Certified by:

Dr. S. A. Opoku ---------- ----------

Signature Date

Supervisor

Certified by:

Prof. Samuel K. Amponsah ---------- ----------

Head of Department Signature Date

DEDICATION

I dedicate this thesis to the Almighty God and my mother Mrs Matilda Ahiaku

ACKNOWLEDEMENT

My deepest gratitude goes to the Almighty God for seeing me through this work successfully.

I could not but say, God bless my Supervisor Dr. S. A. Opoku for his supervision throughout the study. Also I am grateful to Mrs Mary Osei Fokuo Boakye and Dr. R.Y. Tamakloe of Department of Physics for their support and encouragement.

My heartfelt appreciation goes to my family for their support and prayers.

Finally, to all, who have contributed in diverse ways in ensuring the successful completion of this work. I say God richly bless you all.

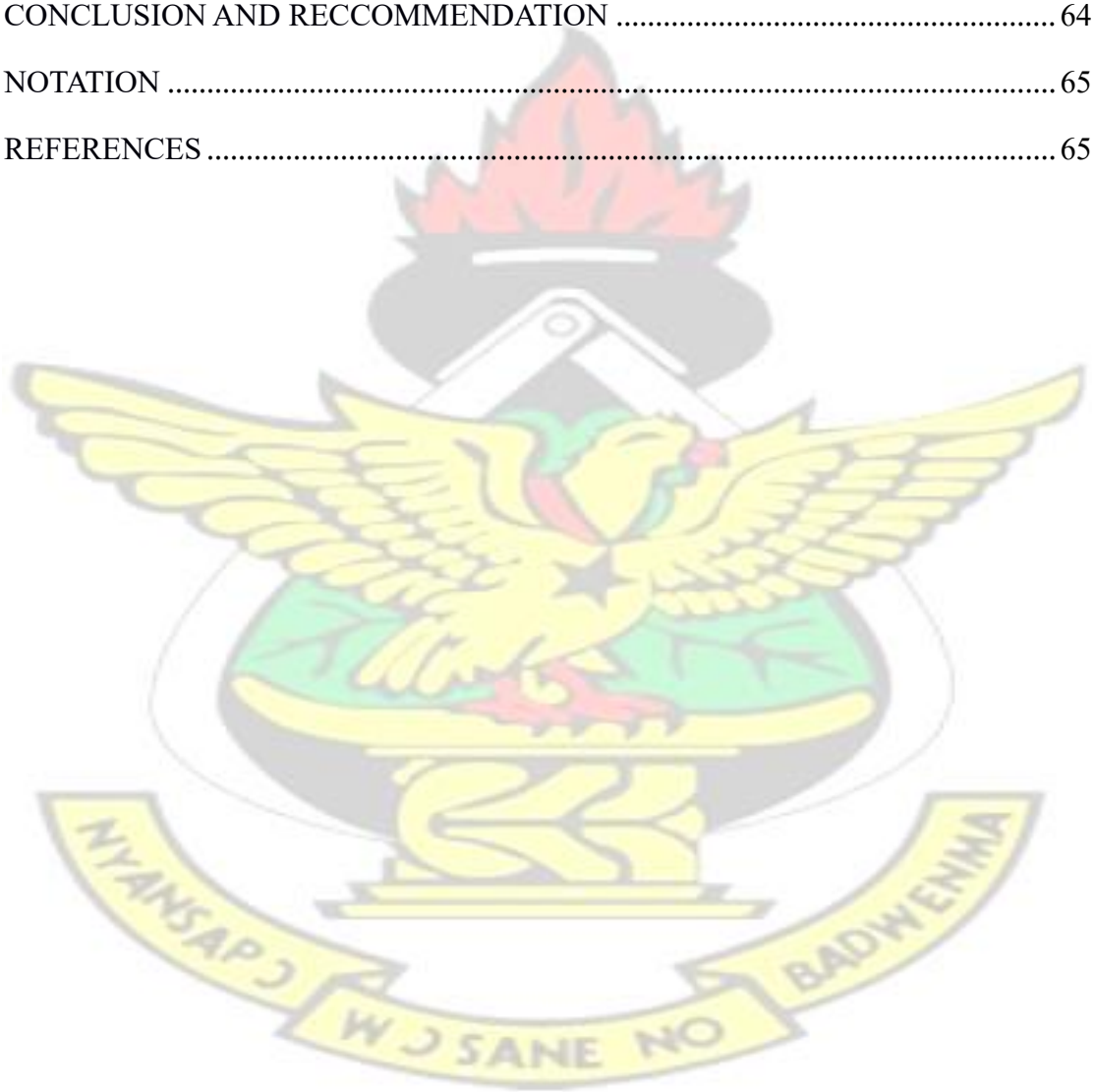
ABSTRACT

Euler's phi – function $\phi(n)$ is defined for every positive integer n as follows:

$\phi(1) = 1$ and when $n \geq 2$ then $\phi(n)$ is the number of distinct integers $k \in \{1,2,\dots,n-1\}$ such that k and n are relatively prime.

This thesis seeks to examine the application of Euler's phi-function in the study of cyclic groups, field extensions and cyclotomic polynomials of a finite field.

TABLE OF CONTENTS



CHAPTER 1

INRODUCTION

A fundamental difficulty for beginning students is often the axiomatic nature of abstract algebra and the exacting need to follow the axioms precisely. To this end particular and extensive attention is paid to the integers, which are familiar objects of knowledge, and which, together with some simple properties of polynomials, are used to give motivation for the introduction of more abstract algebraic concepts. The aim here is to provide an appropriate, interesting and entertaining text for those who require a rounded knowledge in application of Euler's phi-function in Abstract Algebra as well as for those who wish to continue with further studies in algebra.

1.1 BACKGROUND OF STUDY

Leonhard Euler's father was Paul Euler. Paul Euler had studied theology at the University of Basel and had attended Jacob Bernoulli's lectures there. Leonhard was sent to school in Basel. Euler's father wanted his son to follow him into the church and sent him to the University of Basel to prepare for the ministry.

He entered the University in 1720, at the age of 14, where, Johann Bernoulli soon discovered Euler's great potential for mathematics in private tuition that Euler himself engineered. Euler obtained his father's consent to change to mathematics after Johann Bernoulli had used his persuasion. Euler completed his studies at the University of Basel in 1726.

In 1726, Euler now had to find himself an academic appointment when Nicolaus (II) Bernoulli died in St Petersburg; Euler was offered the post which would involve him in teaching applications of mathematics and mechanics to physiology.

He had studied many mathematical works during his time in Basel. They include works by Varignon, Descartes, Newton, Galileo, van Schooten, Jacob Bernoulli, Hermann, Taylor and Wallis. By 1726 Euler had already a paper in print, a short article on isochronous curves in a resisting medium. In 1727 he published another article on reciprocal trajectories and submitted an entry for the 1727 Grand Prize of the Paris Academy on the best arrangement of masts on a ship. The Prize of 1727 went to Bouguer, an expert on mathematics relating to ships, but Euler's essay won him second place which was a fine achievement for the young graduate. By 1740 Euler had a very high reputation, having won the Grand Prize of the Paris Academy in 1738 and 1740. On both occasions he shared the first prize with others.

Euler's reputation was to bring an offer to go to Berlin. Accepting an offer, Euler, at the invitation of Frederick the Great, went to Berlin's Academy of Science. He left St Petersburg on 19 June 1741, arriving in Berlin on 25 July. Even while in Berlin Euler continued to receive part of his salary from Russia. For this remuneration he bought books and instruments for the St Petersburg Academy, he continued to write scientific reports for them, and he educated young Russians.

Maupertuis was the president of the Berlin Academy when it was founded in 1744 with Euler as director of mathematics. He deputised for Maupertuis in his absence and the two became great friends. Euler undertook an unbelievable amount of work for the Academy. During the twenty-five years spent in Berlin, Euler wrote around 380 articles.

He wrote books on the calculus of variations; on the calculation of planetary orbits; on artillery and ballistics (extending the book by Robins); on analysis; on shipbuilding and navigation; on the motion of the moon; lectures on the differential calculus; and many more.

In 1766 Euler returned to St Petersburg and Frederick was greatly angered at his departure. Soon after his return to Russia, Euler became almost entirely blind after an illness. Shortly, he became totally blind. Because of his remarkable memory he was able to continue with his work on optics, algebra, and lunar motion. Amazingly after his return to St Petersburg (when Euler was 59) he produced almost half his total works despite the total blindness. Euler died on 18 September 1783, after his death in 1783 the St Petersburg Academy continued to publish Euler's unpublished work for nearly 50 more years.

He made large bounds forward in the study of modern analytic geometry and trigonometry where he was the first to consider *sin, cos*, etc. as functions rather than as chords as Ptolemy had done.

He made decisive and formative contributions to geometry, calculus and number theory. He integrated Leibniz's differential calculus and Newton's method of fluxions into mathematical analysis. He introduced beta and gamma functions, and integrating factors for differential equations. He studied continuum mechanics, lunar theory with Clairaut, the three body problem, elasticity, acoustics, and the wave theory of light, hydraulics, and music. He laid the foundation of analytical mechanics, especially in his Theory of the Motions of Rigid Bodies (1765). We owe to Euler the notation $f(x)$ for a function (1734), e for the base of natural logs (1727), i for the square root of -1 (1777), π for pi, ∑ for summation (1755), the notation for finite

differences Δy and $\Delta^2 y$ and many others.

1.2 STATEMENT OF PROBLEM

Euler's phi – function $\phi(n)$ is defined for every positive integer n as follows:

$\phi(1) = 1$ and when $n \geq 2$ then $\phi(n)$ is the number of distinct integers $k \in \{1,2, \dots, n-1\}$such that$kandn$are relatively prime. The ϕ function has many interesting properties which among other things greatly simplify the problem of computing$\phi(n)$. The one obvious property is that if p is a prime$\phi(p) = p - 1$.

The problem of the thesis is to establish some useful application of Euler's phi – function $\phi(n)$ in Abstract Algebra

Let n be any positive integer. Then by definition there are $\phi(n)$ numbers in $Z_n$that are relatively prime to$n$. If a and b are two of these numbers, then so isab. This follows from Euclid's lemma by contradiction. Suppose ab was not relatively prime to n.Then there is some Prime p that divides ab and divides n.

By Euclid's lemma, p must divide a or b.Suppose for example that p divides a, then a and n both have p as a factor and are not relatively prime. This contradicts our assumptions. Hence ab is relatively prime to n.

This thesis also seeks to examine the study of field extensions and cyclotomic polynomials of a finite field.

1.3 OBJECTIVE OF STUDY

The aim of the project is to identify some properties and uses of Euler's phi function in abstract algebra. In particular in the determination of Automorphisms of Cyclic group as well as cyclotomic polynomials and related field extensions.

1.4 METHODOLOGY

To present an overview of the application of Euler's phi function in group and field theory with particular attention to the following subjects: homomorphism,

isomorphism, automorphism of cyclic groups, fields, field extensions and cyclotomic polynomials.

1.5 JUSTIFICATION OF THE OBJECTIVES

The thesis deals extensively with the use of $\phi(n)$ to describe the group of automorphisms of C_n where C_n is a cyclic group of order n . It also makes it easy to write the cyclotomic polynomial $\Phi(n)$ and show that it's splitting field over the field of all rational numbers is an extension of degree $\phi(n)$. It will also help you learn about some properties of Euler's phi – function $\phi(n)$, as well as Group and Field automorphisms.

1.6 ORGANIZATION OF THESIS

The Chapter one of the thesis comprises the statement of problem. The Chapter two looks at the preliminary concepts of integers, some properties of Euler's phi-function. The application of Euler's phi-function in the determination of the order and structure of the Automorphisms of Cyclic Groups with the properties of Groups, Rings and Fields is outlined in the Chapter three. The Chapter four outlines Ring of Polynomials, Galois group and Cyclotomic polynomials.

CHAPTER 2

BASIC CNCEPTS

In Mathematics, it is always possible to regard any object as a set with some additional structure-preserving bijective function from the set to itself. Composition of functions provides an operation on this set and it is not hard to show that the group axioms are satisfied.

The theory of Euler's phi function is concerned with group theory and number theory with probably more of the latter than the former. This chapter looks at some properties and theorems of Euler's phi-function.

2.1 Principle of Well-ordering

Let$\mathbb{N}$be the set of natural numbers. Every non-empty subset $S$of$\mathbb{N}$has a least element integer in$S$. It frequently happens that we have some assertion, proposition or statement $P(n)$which depends on the particular integer$n$.

The proposition may itself be true or false.

Examples

1. $1 + 2 + \cdots + n = \frac{n}{2}(n+1)\ where\ n \in \mathbb{N}$

2. $2n + 1 \leq 2^n\ where\ n \in \mathbb{N}$

3. $n^2 \leq 2^n\ where\ \ n \in \mathbb{N}$

In each of these examples we have a statement that depends on$n$. We are not asserting the truth or falsity of the statement. Naturally, however, we wish to know whether the particular statement is true for all$n \in \mathbb{N}$or, possibly, for all $n \in$

$\mathbb{N}$greater than some fixed integer.

We are led to the Principle of Induction and to an obvious and convenient variant of this principle. We may derive the Principle of Induction from the Principle of Wellordering but both, for present purposes, may be regarded as simply axiomatic or, indeed, as 'obvious'.

2.1.1 Principle of Induction

Let$P(n)$be a proposition depending on the integer$n$. Suppose that

1. $P(1)$is true and

2. If$P(k)$is true then $P(k+1)$is true (induction assumption).

Then$P(n)$is true for all$n \in \mathbb{N}$.

Proof

Let Sbe the subset of $\mathbb{N}$ of those integers$n$ for which$P(n)$is true.

Then certainly$1 \epsilon S$and so$S$is a nonempty set. Let$X = \mathbb{N}/S$.

We wish to show that $X$is an empty set and then$S = \mathbb{N}$.

For the sake of argument suppose $X$is a nonempty.

We apply the Principle of Well-ordering to X. Let N be the least integer in$X$.

Now$N \neq 1$since $1 \in S$and so$N > 1$.

Since $N$is the least integer in X, $N-1$is an integer not in$X$and so $N-1 \in S$.

But then$P(N-1)$is true and so, by hypothesis 2, $P(N)$is also true and$N \in S$. Z But this is a contradiction as $X \cap S = \emptyset$(is an empty set).

Hence $X$is empty and$S = \mathbb{N}$. (Wallace, D. A. R., 1998)

The Principle of Induction is often used in a modified version which we may also deem to be axiomatic.

2.1.2.Principle of Induction (Modified Version)

Let$P(n)$be a proposition depending on the integer$n$.

Suppose that

1. $P(1)$is true and

2. If for each$m \leq k$, $P(m)$is true, then $P(k+1)$is true (induction assumption).

Then$P(n)$is true for all$n \in \mathbb{N}$. (Wallace, D. A. R., 1998)

Examples

1. $P(n)$is the statement $1 + 2 + \cdots + n = \frac{n}{2}(n+1)\ for\ n \in \mathbb{N}$.

   Certainly $P(1)$is true since$1 = \frac{1}{2}(1+1)$.

   If we now make the induction assumption that$P(k)$is true, then we suppose that

$1 + 2 + \cdots + k = \frac{k}{2}(k+1)$.

But this implies that

$$1 + 2 + \cdots + k + (k+1) = \frac{k}{2}(k+1) + (k+1)$$

$$= \frac{(k+1)}{2}(k+2)$$

$$= \frac{(k+1)}{2}[(k+1)+1]$$

and so we may assert that $P(k)$ implies $P(k+1)$. Hence we have for all $n \in \mathbb{N}$

$$1 + 2 + \cdots + n = \frac{n}{2}(n+1)$$

2. $P(n)$ is the statement that $2n + 1 \leq 2^n \; where \; n \in \mathbb{N}$ Now $P(1)$ and $P(2)$ are, in fact, false since $2(1) + 1 > 2^1$ and $2(2) + 1 > 2^2$. However, $P(3)$ is true since $2(3) + 1 = 7 \leq 2^3$.

   Let us suppose that $P(k)$ is true for all $k \geq 3$. Then we suppose $2k + 1 \leq 2^k$. But this implies

   $$2(k+1) + 1 = 2k + 3 = 2k + 1 + 2 \leq 2^k + 2 = 2^{k+1} \; for \; k \geq 3$$

   and so $P(k+1)$ is true.

   Hence we conclude that for all $n \in \mathbb{N}$, $n \geq 3$: $2n + 1 \leq 2^n$

2.1.3 Euclidean Algorithm

The Euclidean Algorithm is a very important and non-obvious systematic procedure to find the greatest common divisor d of two integers m, n, and also to find integers x, y so that $xm + yn = d$

Each step in the Euclidean Algorithm is an instance of the Division algorithm. One important aspect of the Euclidean Algorithm is that it avoids factorization of integers into primes, and at the same time is a reasonably fast algorithm to accomplish its purpose. This is true at the level of hand calculations and for machine calculations, too.

2.1.4 The Division Algorithm

For a non-zero positive integer$m$, there is the process of reduction modulo m, which can be applied to arbitrary integers$N$.

This is exactly the division-with remainder process of elementary arithemetic, with the quotient discarded: the reduction modulo m of N is the remainder when N is divided by n. This procedure is also called the Division Algorithm, for that reason. More precisely, the reduction modulo m of N is the unique integer $r$such that N can be written as

$$N = qm + r$$

with an integer q and with$0 \leq r < m$.

2.2 FACTORS

An integer$d$ is a *common divisor* of a family of integers$n_1, \cdots, n_m$if d divides each one of the integersn_i.

An integer N is a *common multiple* of a family of integers$n_1, \cdots, n_m$if N is a multiple of each of the integersn_i.

Theorem 2.1

Letm, nbe integers, both not zero. Among all common divisors of m, nthere is a unique one, call it$d$, so that for every other common divisor e of m, nwe have$e|d$, and also$d > 0$.

This divisor d is the *greatest common divisor* (gcd)ofm, n. The greatest common divisor of two integers m, n(both not zero) is the *least positive integer* of the form $dxm + yn$with $x, y \in \mathbb{Z}$.

Remark: The greatest common divisor of m, n is denoted$gcd(m, n)$.

Lemma 2.1

If a and b are integers, not both zero then, the greatest common divisor exist is unique. Moreover, we can find integers$m$ and n such that the greatest common divisor c of a and b is $c = ma + nb$.

Proof

Let β be the set of all integers of the form $ma + nb$,where $m, n \in Z$and $a \neq 0, b \neq 0$. If d/a and d/b then $d/(ma + nb)$ hence d/c. Given $x = m_1a + n_1b$in β, then by the Euclidean algorithm, $x = tc + r$where $0 \leq r < c$.

Now $m_1a + n_1b = t(ma + nb) + r \Rightarrow r = (m_1 - tm)a + (n_1 - tn)b$ since $0 \leq r$ and $r < c$ by the choice of $c, r = 0$. Thus $x = tc$. Hence c/x for any $x \in \beta$. Hence c/a and c/b.

2.2.1 Relatively Prime

Two integers are relatively prime or coprime if their greatest common divisor is 1. Also we may say that m is prime to n if they are relatively prime.

For example 24 and 35 are relatively prime.

Corollary 2.1

If a and b are relatively prime, we can find integers m and n such that $ma + nb = 1$.

Lemma 2.2

If a is relatively prime to b but a/bc, then a/c Proof

Since a and b are relatively prime, by the corollary, we find integers m and n such that $ma + nb = 1$.

Thus $mac + nbc = c$. Now a/mac and by assumption a/nbc. Consequently, $a/(mac + nbc)$ since $mac + nbc = c$. We conclude that a/c.

Hence, if a is relatively prime to b but a/bc then a/c.

2.2.2 Associates

A nonzero element a of a commutative ring R is said to divide an element $b \in R$ if there exist $x \in R$ such that $ax = b$,where $a, b \in R$ are said to be associates if $a/b \ and \ b/a$.

Invertible: An element is said to be invertible if $a \in R$ and $b \in R$ then $a \cdot b = 1$

2.2.3 Prime element

A non-zero element p of an integral domain D with unity is called prime element if

1. p is a nonzero and non-unit
2. if p/ab then p/a or p/b where $a, b \in D$.

2.3 INTEGERS MODULO *m*

If two integers $x, y \in \mathbb{Z}$ differ by a multiple of a non-zero integer$m \in Z$we say that $x$is congruent to $y$to modulo $m$written$x \equiv y \ mod \ m$.

Any relation such as this is called a *congruence* modulo$m$and $m$is the modulus.

Equivalently, $x \equiv y \ mod \ m$if and only if$m|(x - y)$.

Example $3 \equiv 18 \ mod \ 5$because$5|(18 - 3)$.

Theorem 2.2

For a fixed integer$m$, congruence modulo$m$ is an equivalence relation. That is;

1. Reflexivity: always $x \equiv x \ mod \ m$for any integer$x$

2. Symmetry: if $x \equiv y \mod m$ then $y \equiv x \mod m$.
3. Transitivity: if $x \equiv y \mod m$ and $y \equiv z \mod m$ then $x \equiv z \mod m$.

Proof

1. Since $x - x = 0$ and always $m|0$, we have reflexivity.
2. If $m|(x-y)$ then $m|(y-x)$ since $y - x = -(x-y)$ thus we have symmetry
3. Suppose that $m|(x-y)$ and $m|(y-z)$. Then there exists integers $k, l \in \mathbb{Z}$ such that $mk = x - y$ and $ml = y - z$. Then, $x - z = (x-y) + (y-z) = mk + ml = m(k+l)$. This proves the transitivity.

2.3.1 EULER'S PHI-FUNCTION

Definition

For $n \geq 1$. The number $\phi(n)$ denotes is the number of distinct integers $k \in Q(n) = \{1,2,\dots,n-1\}$ such that k and n are relatively prime, that is $\phi(n) = |Q(n)|$ the order of $Q(n)$.

Examples

$Q(1) = \{1\}$, $Q(2) = \{1\}$, $Q(3) = \{1,2\}$, $Q(4) = \{1,3\}$,

$Q(7) = \{1,2,3,4,5,6\}$, $Q(10) = \{1,3,7,9\}$,

$Q(30) = \{1,7,11,13,17,19,23,29\}$

Therefore

$$\phi(1) = |Q(1)| = 1,\ \phi(2) = |Q(2)| = 1,\ \phi(3) = |Q(3)| = 2,\ \phi(4) = |Q(4)| = 2,\ \phi(7) = |Q(7)| = 6,\ \phi(10) = |Q(10)| = 4,\ \phi(30) = |Q(30)| = 8$$

Definition

For $n \geq 1$, $\phi(n)$ can be characterized as the number of positive integers less than n and relatively prime to n. The function $\phi(n)$ is usually called the Euler phi-function after its originator. The functional notation $\phi(n)$ however is credited to Gauss,

that is $\phi(n) = |\phi(n)|$,

where $\phi(n) = \{m_i | 0 < m_i \leq n, where\ m_i\ are\ relatively\ prime\ to\ n\}$

Remark: We know $\phi(1) = 1$, for $n > 1$. Since the greatest common divisor, $gcd(1,1) = 1,\ gcd(n,n) = n \neq 1 \Longrightarrow n$ is not relatively prime to n.

If n is prime then every number less than n is relatively prime to it, that is $\phi(n) = n - 1$.

Theorem 2.3

If p is a prime number and $k > 1$, then $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$, integers relatively prime to p^k.

Proof

The $gcd(n, p^k) = 1$ if and only if p does not divide n. There are p^{k-1} integers between $1\ and\ p^k$ which are divisible by p namely $p, 2p, 3p, \ldots, (p^{k-1})p$. Thus the set $\{1,2, \ldots, p^k\}$ contains exactly $p^k - p^{k-1}$ integers which are relatively prime to p^k so by the definition of ϕ, $\phi(p^k) = p^k - p^{k-1}$ integers relatively prime to p^k.

Example

i. $\phi(9) = \phi(3^2) = 3^2 - 3 = 6\ elements \Longrightarrow\ Q(9) = \{1,2,4,5,7,8\}$ ii.

$\phi(16) = \phi(4^2) = 2^4 - 2^3 = 8\ elements \Longrightarrow Q(16) = \{1,3,5,7,9,11,13,15\}$

Theorem 2.4

The function ϕ is a multiplicative function, $\phi(mn) = \phi(m)\phi(n)$ when ever $m\ \ and\ \ n$ are relatively prime i.e. $gcd(m,n) = 1$.

Theorem 2.5

If an integer $n > 1$has the prime factorization $n = P_1^{k_1}.P_2^{k_2} \ldots P_r^{k_r}$

Then,$\phi(n) = \left(P_1^{k_1} - P_1^{k_1-1}\right)\left(P_2^{k_2} - P_2^{k_2-1}\right) \ldots \left(P_r^{k_r} - P_r^{k_r-1}\right)$ and hence

$\phi(n) = n\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right) \ldots \left(1 - \frac{1}{P_r}\right)$elements.

Proof

By induction on r, the number of distinct prime factors of n. It is true for$r = 1$.

Then$\phi\left(P_1^{k_1}\right) = \left(P_1^{k_1} - P_1^{k_1-1}\right)$.

Let it hold for $r = i$ since the$gcd\left(P_1^{k_1}P_2^{k_2} \ldots P_i^{k_i}P_{i+1}^{k_{i+1}}\right) = 1$.

Now by the definition of multiplicative function;

$$\phi(P_1^{k_1}P_2^{k_2} \ldots P_i^{k_i})(P_{i+1}^{k_{i+1}}) = \phi\left(P_1^{k_1}P_2^{k_2} \ldots P_i^{k_i}\right)\phi\left(P_{i+1}^{k_{i+1}}\right)$$

$$= \phi\left(P_1^{k_1}P_2^{k_2} \ldots P_i^{k_i}\right)\left(P_{i+1}^{k_{i+1}} - P_{i+1}^{k_{i+1}-1}\right)$$

Invoking the induction assumption, the first factor on the right hand side becomes

$$\phi\left(P_1^{k_1}P_2^{k_2}\cdot\ldots P_{i+1}^{k_{i+1}}\right)=\left(P_1^{k_1}-P_1^{k_1-1}\right)\left(P_2^{k_2}-P_2^{k_2-1}\right)\ldots\left(P_{i+1}^{k_{i+1}}-P_{i+1}^{k_{i+1}-1}\right)$$

This serves to complete the induction step as well as the proof.

Hence $\phi(n)=\left(P_1^{k_1}-P_1^{k_1-1}\right)\left(P_2^{k_2}-P_2^{k_2-1}\right)\ldots\left(P_{i+1}^{k_{i+1}}-P_{i+1}^{k_{i+1}-1}\right)$

Therefore

$$\phi(n)=n\left(1-\frac{1}{P_1}\right)\left(1-\frac{1}{P_2}\right)\ldots\left(1-\frac{1}{P_r}\right)$$ elements

Example

To find $\phi(360)$. We know that the prime factors of $360=2^3 3^2 5$.

so $\phi(360)=360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=96$

Thus $Q(360)$ has 96 elements, each relatively prime 360.

Theorem 2.6

For $n>2$, $\phi(n)$ is an even integer.

Proof

Consider two cases when n is a power of 2 and when n is not a power of 2.

1. Let n be a power of 2 that is $n=2^k,\ k\geq 2$.

   Hence $\phi(n)=\phi(2^k)=2^k(1-1/2)=2^{k-1}$, therefore $\phi(n)$ is even.

2. When n is not a power of 2. Then it is divisible by an odd prime number p,

   then $n=p^k m$ where $k\geq 1$ and $gcd(p^k,m)=1$.

   By the multiplicative nature of phi-function,

   $$\phi(n)=\ \phi(p^k m)=\ \phi(p^k)\,\phi(m)=p^{k-1}(p-1)\,\phi(m)$$

Hence $\phi(n)$is even, because2 is divisible by$p-1$.

2.3.2 Fermat's Little Theorem

Let$p$ be a prime number. Then for any integer x

$$x^p \equiv x \mod p$$

Proof

We will first prove that prime $p$divides the binomial coefficients $\binom{p}{i}$ with

$1 \leq i \leq p-1$, keeping in mind that the ‘”extreme" cases $i = 0$ and $i = p$ cannot possibly also have this property, since$\binom{p}{0} = 1 \binom{p}{p} = 1$

Indeed, from its definition,$\binom{p}{i} = \frac{p!}{i!(p-i)!}$

Certainly $p$divides the numerator. Since $0 < i < p$, the prime$p$ divides none of the factors in the factorials in the denominator. By unique factorization into primes, this means that$p$ does not divide the denominator at all.

From the Binomial Theorem,

$$(x+y)^p = \sum_{0 \leq i \leq p} \binom{p}{i} x^i y^{p-i}$$

In particular, since the coefficients of the left-hand side are integers the same must be true of the right-hand side. Thus, all the binomial coefficients are integers.

Thus, the binomial coefficients with$0 < i < p$are integers expressed as fractions whose numerators are divisible by p and whose denominators are not divisible by$p$. Thus, when all cancellation is done in the fraction, there must remain a factor of p in the numerator. This proves the desired fact about binomial coefficients.

Now we prove Fermat's Little Theorem (for$positive \ \ x$) by induction on$x$.

First, certainly,$1^p \equiv 1 \mod p$.

For the induction step, suppose that we already know for some particular x that

$$x^p \equiv x \ mod \ p$$

Then

$$(x+1)^p = \sum_{0 \le i \le p} \binom{p}{i} x^i 1^{p-i} = x^p + \sum_{0<i<p} \binom{p}{i} x^i + 1$$

All the coefficients in the sum in the middle of the last expression are divisible by p.

Therefore,

$$(x+1)^p \equiv x^p + 0 + 1 \equiv x + 1 \ mod \ p$$

since our induction hypothesis is that $x^p \equiv x \ mod \ p$.

This proves the theorem for positive x.

To prove the theorem for $x < 0$ we use the fact that $-x$ is then positive. For $p = 2$, we can just treat the two cases, $x \equiv 0 \ mod \ 2$ and $x \equiv 1 \ mod \ 2$ separately and directly.

For $p > 2$ we use the fact that such a prime is odd. Thus,

$$x^p = -(-x)^p \equiv -(-x) \ mod \ p = x \ mod \ p$$

by using the result for positive integers.

Definition

Let n be a positive integer. An integer g is a *primitive root modulo* n if the smallest positive integer *l*so that $g^l = 1 \ mod \ n \ \ is \ \ \ \phi(n)$.

Theorem 2.7

The only integers n for which there is a primitive root modulo n are those of the forms

1. $n = p^e$ with an odd prime p, and $e \geq 1$ 2.

$n = 2p^e$ with an odd prime p, and $e \geq 1$

3. $n = 2\,;4$

It is useful to make clear one important property of primitive roots.

Corollary 2.2

Let$g$ be a primitive root modulo$n$. Let$l$be an integer so that

$$g^l \equiv 1 \ mod \ n$$

Then $\phi(n)$divides l.

Proof

Using the Division Algorithm, we may write $l = q.\ \phi(n) + r$ with $0 \leq r <$ $\phi(n)$. Then

$$1 = g^l = g^{q.\phi(n)+r} = \left(g^{\,\phi(n)}\right)^q . g^r = 1^q . g^r = g^r \ mod \ n$$

Since g is a primitive root, $\phi(n)$ is the least positive exponent so that $g$raised to that power is $1 \ mod \ n$.

Thus, since$1 = g^r \ mod \ n$, it must be that $r = 0$. That is, $\phi(n)|l$.

2.3.3 Euler's Theorem

Let n be a positive integer. For $x \in \mathbb{Z}$relatively prime to$n$,

$$x^{\,\phi(n)} \equiv 1 \ mod \ n$$

Proof:

The set $\mathbb{Z}/n^x$ of integers$mod \ n$which are relatively prime to$n$ has $\phi(n)$elements. By Lagrange's theorem, this implies that the order $k \ of \quad g \in \mathbb{Z}/n^x \mid \phi(n)$.

Therefore,

$\phi\,(n)/k$is an integer, and

$$g^{\,\phi(n)} = (g^k)^{\,\phi(n)/k} = e^{\,\phi(n)/k} = e$$

Applied to $x \ mod \ n$ this is the desired result.

Theorem 2.8

Let n be a positive integer. For $x \in \mathbb{Z}$ relatively prime to n, the smallest exponent l so that

$$x^l \equiv 1 \ mod \ n$$

is a divisor of $\phi(n)$. That is, the order of x in the multiplicative group $\mathbb{Z}/n^x$ is a divisor of $\phi(n)$.

Proof:

The order x is equal to the order of the subgroup $< x >$, which by Lagrange's theorem is a divisor of the order of the whole group $\mathbb{Z}/n^x$.

CHAPTER THREE

GROUPS, RINGS AND FIELDS

This chapter looks at Groups, Rings and Field and also Polynomials. Also looks at the use of Euler's phi-function, in the determination of the order and structure of automorphisms of cyclic groups under multiplication.

The evolution of the concept of an abstract group owes much to the labours of many mathematicians of whom only a few will be mentioned here. The origins of the concept may be traced from the work of P. Ruffini (1765-1822) and E. Galois (181132) through to that of L. Kronecker who developed ideas for what we now call an Abelian group ('Abelian' after N.H. Abel, 1802-29). The abstract concept of a finite group was first formulated in 1854 by A. Cayley (1821-95) but its significance was not properly appreciated until 1878. W. von Dyck (1856-1934) and H. Weber (18421913) were influential in the development of group theory, the latter giving the first definition of an infinite group in 1893.

3.1 GROUP

A group $(G,*)$ is an ordered pair such that G is nonempty set, a binary operation $(*)$ defined on G and it satisfies the axioms of a group.

3.1.1 Axioms of a group

Axiom 1: The binary operation $(*)$ is closed, if for every pair $a, b \in G$ then $a * b \in G$

Axiom 2: The binary operation $(*)$satisfies the associative law.

If $a, b, c \in G$ then $a * (b * c) = (a * b) * c$

Axiom 3: There exists an identity element (e) under the binary operation.

If $\exists\ e \in G$such that $a * e = e * a = a$for all $a \in G$.

Axiom 4: The existence of inverse in G. For every $a \in G$ there exist an element $a^{-1} \in G$such that $a * a^{-1}a^{-1}a = e$

Terminology: If $(G,*)$ is a group, will from hence forth denoted as G is a group or G a group under$(*)$.

Some Useful Properties of a Group

Suppose G is a group under a binary operation$(*)$and without any ambiguity

$ab = a * b$ for every pair$a, b \in G$. Then the following results:

1. Left cancellation
2. Right cancellation
3. A left identity is also a right identity
4. Uniqueness of an identity
5. A left inverse of an element $g \in G$ is also a right inverse of g
6. Uniqueness of the inverse of an element
7. The inverse of the inverse of an element
8. For every pair of elements $a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$

Examples

1. Group of numbers $\mathbb{Z}, \mathbb{Q}, \mathbb{R}\ and\ \mathbb{C}$ under multiplication
2. Group of matrices; let R be a ring with an identity element and let

$GL(n, R)$denote the set of all $n \times n$matrices with coefficients in Rwhich have inverses, taking matrix multiplication, $GL(n, R)$ is a group with identity $1_n, n \times n$ identity matrix.

3. Groups of linear transformation; if V is an $n - dimensional$ vector space over a field F, let GLV denote the set of all bijective linear transformations, then GLV is a group under composition
4. Group of Permutations

3.1.2 Commutative Group

A group G under a binary operation$(*)$ is called a *commutative* or *Abelian* group if $(*)$is commutative that is for every$a, b \in G$then$a * b = b * a$.

3.1.3 Subgroup

Let H be a nonempty subset of a group$G$. A nonempty subset H is defined as a subgroup of G under a binary operation $(*)$ defined in G , if it satisfies these conditions.

- $a, b \in H \Longrightarrow a * b \in H$
- $a \in H \Longrightarrow a^{-1} \in H$
- the identity $e \in H$

Examples

1. $\mathbb{Q}^* = \{\frac{p}{q} : p \; and \; q \;\; are \;\; nonzero \;\; integers\}$ is a subgroup of $\mathbb{R}^*$
2. $H = \{1, -1, \; i, -i\}$ is a subgroup of $\mathbb{C}^*$

3.1.3.1 Left Cosets and Right Cosets of a Subgroup

Given a group$G$, a subgroup H of G and an element$a \in G$. Let

$aH = \{ah | h \in H\}$ and $Ha = \{ha | h \in H\}$

then aH is called a left coset of H in G and Ha is called a right coset of Hin G.

In the case where $H$is a normal subgroup of$G$. Then$aH = Ha$.

3.1.4 Normal Subgroup

A subgroup$H$ of a group$G$ is a normal subgroup of$G$ if$g^{-1}hg \in H$for every $g \in G$ and every$h \in H$.

Proof

If$a \in A$and$h \in H$then $a^{-1}ha = ha^{-1}a = hI = h \in H$

Therefore$H$is a normal subgroup of$A$.

Example

IfA is an Abelian group and$H$ is a subgroup of$A$ then$H$ is a normal subgroup of$A$.

Theorem 3.1

These two statements about a group$G$and a subgroup$H$ of$G$ are equivalent.

1. $H$is a normal subgroup of$G$.
2. $Ha = aH$ for every $a \in G$.

Proof

Suppose$H$ is a normal subgroup of$G$ is true. If $a \in G$ then $\forall\ h \in H, aha^{-1} \in H$

and $a^{-1}ha \in H$

Let $a^{-1}ha = \gamma \in H$, then $ha = a\gamma \in aH \therefore Ha \subset aH$ Let
$aha^{-1}\eta \in H$then $ah = \eta a \in Ha \therefore aH \subset Ha \therefore Ha = aH \quad \forall \quad a \in G$

Thus$H$ is a normal subgroup of$G$ implies $Ha = aH$ for every $a \in G$.

On the other hand, suppose $Ha = aH$ for every $a \in G$ is true. If $g \in G$ and $h \in H$ then $hg \in Hg = gH \Longrightarrow hg = gf$ where $f \in H$ then $g^{-1}hg = f \in H$

Therefore $Ha = aH$ for every $a \in G$ implies$H$ is a normal subgroup of$G$.

Hence, the two statements are equivalent.

3.1.5 Center of a Group

Let$G$ be a group and $Z(G)$be the set of all elements $a \in G$ such that $ga = ag, \forall\, g \in G$.

Then $Z(G)$ is called the centre of a group$G$, $Z(G) = \{a \in G \mid ag = ga, \forall\, g \in G\}$

Theorem 3.2

The centre of a group $Z(G)$ is a normal subgroup of$G$.

Proof

Let I be the identity in G. Then $Ig = gI = g, \forall g \in G \therefore I \in Z(G)$.

If$a \in Z(G)$then$ag = ga, \forall g \in G$Hence $aga^{-1}g \forall g \in G \therefore a^{-1} \in Z(G)$

Ifa and$b$are elements of $Z(G)$ then$abg = agb = gab, \forall g \in G \therefore ab \in Z(G)$,

That show that$Z(G)$ is a subgroup of$G$.

Finally for every,$g \in G$and every $h \in Z(G)$ $g^{-1}hg = g^{-1}gh = Ih = h \in Z(G) \therefore$ $Z(G)$ is a normal subgroup of$G$.

3.2 FINITE GROUP

A group whose underlying set G has finite number of elements is known as *finite group*.

The order of a group is the number of elements in the group. A group G consisting of an

infinite number of elements is said to be an *infinite group*, for example the set $\mathbb{Z}$ of all integers is an infinite group under the addition composition.

The number of elements in$G$ is called the *order of* the *group*G and is denoted by $G||$. The infinite group is said to be of an infinite order. Example; the set $\{1, -1\}$ under multiplication composition is a group of order2.

Examples

1. For every integer $n \geq 2$ there is a *dihedral group* of order$2n$, let Dn denote a dihedral group of order $2n$. Then $Dn = \{I, A, \dots, A^{n-1}, B, AB, \dots, A^{n-1}B^n\}$where I is the identity, A, B are elements such that $A^n = I$for, $A^k \neq I$for$1 \leq k < n$, $B^2 = I$and $BA = A^{n-1}B$.
2. For every positive integer n there exists a group C_n comprising of exactly n elements: $a^1, a^2, \dots, a^{n-1}, \ I$ where$a^n = I$, the identity. Such a group is called a *cyclic group* of order$n$.

3.2.1The Order of an Element

A group element$x$has finite order if the cyclic subgroup $< x >$has order$n$. If $< x >$is infinite then $x$has infinite order. Let$|x|$ denote the order of$x$. Elements of order2are often called *involutions*.

A periodic group (or torsion group) is a group all of whose elements have finite order. If the orders of the elements of a group are finite and bounded, the group is said to have *finite exponent (or index)*. The exponent of the group is then the least common multiple of all the orders.

However, a group is said to be aperiodic (torsion-free) if apart from the identity$I$, all its elements have infinite order.

Theorem 3.3

Let $x$be an element of a group$G$. Then the following statements are equivalent.

1. If $x$has infinite order if and only if all powers of $x$are distinct.
2. If $x$has finite order$n$, then $x^m = 1$if and only if$n|m$. Moreover $< x >$ consists of the distinct elements$1, x, x^2, \dots, x^{n-1}$.
3. If$x$has finite order$n$, the order of$x^k \ \ equals \ \ n/(n,k)$.

Proof

If all powers of$x$are distinct,$< x >$is infinite. Conversely suppose that two powers of$x$are equal, say$x^l = x^m \ \ where \ \ l < m: then \ \ x^{m-l} = 1$. Thus we can choose the least positive integer$n$such that$x^n = 1$. Using the division algorithm we may write an arbitrary integer$m$in the form$m = qn + r \ \ where \ \ q, r$are integers and$0 \leq r < n$.

Then$x^m = (x^n)^q x^r = x^r$, which shows that$< x >= \{1, x, \dots, x^{n-1}\}$.

Hence$x$has finite order. Also$x^m = 1$if and only if$r = 0$, that is, if$n|m$: this is by minimality of$m$.

Next suppose that$x^i = x^j \ where \ 0 \leq i \leq j < n$. Then$x^{j-i} = 1, so \ \ that \ \ n|j - i$: but this can only mean that$i = j$. Hence the elements$1, x, \dots, x^{n-1}$are all distinct and$|x| = n$.

Thus1and2are established.

To prove3, observe that $(x^k)^{n/(n,k)} = (x^n)^{k/(n,k)} = 1$,

which implies that $m = |x^k|$ divides $n/(n,k)$. Also since $(x^k)^m = 1$, one has that $n|km$ and hence that $n/(n,k)$ divides $(k/(n,k))m$.

By Euclid's lemma $n/(n,k)$ divides m, so $m = n/(n,k)$.

3.2.2 Lagrange Theorem

If G is a finite group and H is a finite subgroup of G then the order of H divides the order of G.

Proof

Let n be the order of G and q be the order of H.

Choose finitely many elements $g_1, \cdots, g_k$ in G such that $G = \bigcup_j^k H_{gj}$ and $H_r \cap H_j = \emptyset$ where every $r \neq j$ then $n = v_1 + \cdots + v_k = qk$ for each $j \in \{1, \ldots, k\}$ where V_j is the number of elements in H_{gj}

Since each right coset of H contains exactly q elements. Hence q divides n.

Therefore, if G is a finite group and H is a finite subgroup of G then the order of H divides the order of G

3.2.3 Cauchy Theorem

If G is a finite group and p is a prime number such that p divides the order of G then there exists $a \in G$ such that the order of a is p.

Proof

First suppose G is Abelian. Choose an element $b \in G$ such that b is not the identity.

If order of b is p^r where r is positive. In this case let $a = b^r$ then the order of a is $\emptyset$

On the other hand if p does not divide the order of b.

Let H be the subgroup generated by the G/H is a group whose order is indivisible by p and whose order is less than the order of G.

If the hypothesis is true for all group whose orders are less than that of G and are divisible by $p$then there exist $t \in G/H$ such that the order of t is p. Let $\psi: G \longrightarrow G/H$ be the projection of G onto$H$.

Choose $a \in G$ such that$\psi(u) = t$. Then the order of u is $p\alpha$ where α is a positive integer.

In this case let $a = u^{\alpha}$ then the order of $a$is$p$.

On the other hand if p does not divide the order of b. This proves Cauchy's theorem if G is Abelian.

If G is not Abelian, then let $k$be the order of the centre$Z(G)$ and the order of G be$p\lambda$, where $\lambda$is a positive integer. Then we can choose elements $a_1 \ldots a_r \in G - Z(G)$ such that the class equation of G is $p\lambda = k + \sum_{j=1}^{r}[G: Z_{aj}(G)]$

If there exist $a \in Z(G)$ such that the order of a is p then the result is done. If k and p are relatively prime then there exist $j \in \{1, \ldots r\}$ such that the index $[G: Z_{aj}(G)]$ is not divisible by p.

That implies the order of $Z_{aj}(G)$ is divisible by p and the order of $Z_{aj}(G)$ is less than the order of G using induction hypothesis we choose$a \in Z_{aj}(G)$ such that the order of a is p. Then the theorem is proved in all cases.

3.3 CYCLIC GROUP

Definition 1

The group G is said to be cyclic if every element of G is a power of some given element of G. This given element is said to generate, or to be a generator of, the group G.

Thus if G is cyclic we may write $G = \{a^n : n = 0,1,2 \ldots\}$ for some $a \in G$. A cyclic group is necessarily Abelian.

Definition 2

If G is a finite group and there exists an element $a \in G$ such that G is the same as the subgroup of G generated by $< a >$ then G is called a cyclic group.

It is denoted by C_n, where n is a positive integer. For every positive integer n there exist a group C_n comprising exactly n elements $a, \ldots a^{n-1}, I$ where $a^n = I$, the identity. Such a group C_n is called a cyclic group of order n.

Examples

1. When $n = 1$, let $I = \{1\}$. Then I is a cyclic group of order 1 and I is also called the *trivial group*.
2. When $n = 2$, then $C_2 = \{-1,1\}$ then C_2 is a cyclic group of order 2
3. When $n = 3$, let $\omega = cos\frac{2\pi}{3} + isin\frac{2\pi}{3}$. Then $C_3 = \{I, \omega, \omega^2\}$ is a cyclic group of order 3.
4. When $n = 4$, let $C_4 = \{i, -i, -1,1\}$ or $C_4 = \{a, a^2, a^3, I\}$ where $a^4 = i$, is cyclic group of order 4.
5. For all $n \geq 1$, let $\omega = cos\frac{2\pi}{n} + isin\frac{2\pi}{n}$. Then $\omega^n = 1$ and $C_n = \{1, \omega, \ldots, \omega^{n-1}\}$ is a cyclic group of order n.

3.3.1 Subgroup of Cyclic Groups

Theorem 3.4

Let $G =< x >$ and let H be a subgroup of G.

1. If G is infinite, H is either infinite cyclic or trivial.
2. If G has finite order n, then H is cyclic of order dividing n.

   Conversely, to each positive divisor d of n there corresponds exactly one subgroup of order d, namely $< x^{n/d} >$.

Proof

We prove first that H is cyclic. If $H = 1$, let $H \neq 1$: then H contains some positive power $x^s \neq 1$ such that s is the smallest positive integer. Clearly $< x^s > \subseteq H$. Choose a positive integer t, if $x^t \in H$, write $t = sq + r \ \ where \ \ 0 \leq r < s$. Then $x^r = (x^s)^{-q} x^t \in H$, so the minimality of s shows that $r = 0$ and $s|t$.

Hence $x^t \in < x^s >$ and $H =< x^s >$. If G is infinite, x has infinite order, as does x^s.

Hence H is an infinite cyclic subgroup.

Now let $|x| = n < \infty$. Then $|H|$ divides n, as we see at once from Lagrange's theorem.

Conversely suppose that $d|n$: then $|x^{n/d}| = d$ by theorem 3.3 and $< x^{n/d} >= d$.

Finally suppose that $< x^k >$ is another subgroup of order d.

Then $x^{kd} = 1$ and $n|kd$: consequently n/d divides k and $< x^k > \leq < x^{n/d} >$.

But these subgroups both have order d, so they coincide.

3.4 HOMOMORPHISM

Let G and B be groups under binary operations $(\circ)$and$(*)$respectively. A mapping

$h : G \longrightarrow B$ is called a homomorphism if $h(a \circ b) = h(a) * h(b)$ for every pair $a, b \in G$.

Example

1. Let$h(x) = e, for\ \ all\ \ e \in G$, then $h(x)$ is a trival homomorphism.
2. Let $h(x) = x, for\ \ every\ \ x \in G$ is a homomorphism.
3. Let $h(a) = 2^a\ \ for\ \ all\ \ a \in G$hence$h(ab) = 2^{a+b} = 2^a 2^b = h(a)h(b)$. Therefore $h(a)$ is a homomorphism.

Some result of homomorphism

1. If $h : G \longrightarrow B \ \forall\ g_1,\ g_2 \in G$such that$h(g_1)h(g_2) \Longrightarrow g_1 g_2$ then$h$ is injective and$h$is said to be a *monomorphism*.
2. If $h : G \longrightarrow B \ \forall\ \ b \in B,\ \exists\ \ g \in G$ such that $h(g) = b$ then, h is surjective and$h$ is said to an *epimorphism*.
3. If $h : G \longrightarrow B$ is a homomorphism and$h$ is bijective then h is called an *isomorphism*. When$h$ is bijective, it means$h$ is both injective and surjective.

Theorem 3.5

Let G and B be groups with identities I, e respectively and h: $G \longrightarrow B$ a homomorphism.

Then these results are important.

1. $h(I) = e$
2. $h(g^{-1}) = \{h(g)\}^{-1}$ for every $g \in G$

3. $h(S)$ is a subgroup of B for every subgroup S of G.

3.4.1 Kernel of a Group

Let G and H be groups and let $f: G \to H$ be a homomorphism. Then the subgroup

$K = \{x \in G | f(x) = I_H\}$ is a normal subgroup of G which is called the kernel of f, denoted $Ker\ f$.

Lemma 3.1

Let G and H be groups and let $f: G \to H$ be a homomorphism with kernel K.

Let a and b be elements of G. Then, $f(a) = f(b)$ if and only if $Ka = Kb$.

Proof

Suppose $f(a) = f(b)$. Then

$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} = f(b)[f(b)]^{-1} = I_H$.

Hence $ab^{-1} \in K$ and so $Ka = Kb$.

Conversely if $Ka = Kb$ then $b = ka$ for some $h \in K$ and

so $f(b) = f(ka) = (fk)f(a) = I_H f(a) = f(a)$.

Theorem 3.6

Let G and H be groups and let $f: G \to H$ be a homomorphism.

Then the following statements hold.

1. If I_G and I_H are the identities of G and H respectively, then $f(I_G) = I_H$

2. For all $x \in G, [f(x)]^{-1} = f(x^{-1})$where $[f(x)]^{-1}$ is the inverse of $f(x)$ in$H$and x^{-1} is the inverse of $x$in G.
3. $f(G)$is a subgroup of H.
4. Let$K = \{x \in G | f(x) = I_H\}$. Then K is a normal subgroup of$G$.

Proof

We note the necessity of distinguishing the identities in the two groups$G$ and$H$.

1. Since$f(I_G)f(I_G) = f(I_G I_G) = f(I_G)$, we conclude that$f(I_G) = I_H$.

2. Since$f(x^{-1})f(x) = f(x^{-1}x) = f(I_G) = I_H \ \ where \ \ x \in G$, we have

$f(x^{-1}) = [f(x)]^{-1}$

3. $f(G)$is closed under multiplication in$H$. Let $a \in f(G)$.

Then $a = f(x)$ for some $x \in G$and $a^{-1} = [f(x)]^{-1} = f(x^{-1}) \in f(G)$.

Thus $f(G)$ is a subgroup of H.

4. Since $f(I_G) = I_H$, K is non-empty. Let $x, y \in K$, then $f(x) = f(y) = I_H$.

Hence

$f(xy) = f(x)f(y) = I_H I_H = I_H$.

and

$f(x^{-1}) = [f(x)]^{-1} = [I_H]^{-1} = I_H$.

Consequently K is a subgroup of G.

To prove that $K$is a normal subgroup let

$a \in K, x \in G$. Then $f(x^{-1}ax) = f(x^{-1})f(ax) = f(x^{-1})f(a)f(x)$

$[f(x)]^{-1}I_H f(x) = [f(x)]^{-1}f(x) = I_H$, and so $x^{-1}ax \in K$.

Hence K is a normal subgroup of G.

SOME APPLICATIONS OF EULER'S PHI-FUNCTION IN GROUP THEORY

3.5 AUTOMORPHISMS OF A GROUP

Let G be a group. If $h : G \longrightarrow G$ is an isomorphism then h is called an *automorphism* of G. For every pair $f, g \in Aut\ G$, let $f \circ g$ be the composite map. Then $AutG$ the set of all automorphisms of G is also a group under the binary operation $(\circ)$ and the identity in $Aut\ G$ is I.

The composite of two automorphisms is again an automorphism; composition of maps is always associative; an automorphism is a bijection and therefore has an inverse, which is again an automorphism.

Example

1. Let $I: G \to G$ be a mapping of G such that every element of G maps to itself, that is $I(x) = x$ for all $x \in G$. We say I is a trivial automorphism of G.
2. Given an element, $a \in G$ a group. Define $f(a): G \to G \ \ by \ \ f(a)x = axa^{-1}$. Then $f(a)$ is an automorphism of G called then *inner automorphism* of G determined by a. The remaining automorphisms are said to be *outer automorphism*.

Notation

Denote by G the set of all inner automorphisms of G. Then G is also a group under the binary operation $(\circ)$.

3.5.1 Automorphism of Cyclic Group

Theorem 3.7

Let G be a cyclic group

1. If G is infinite, $AutG$ consists of the identity automorphism and the automorphism $\alpha: g \mapsto g^{-1}$. Thus $AutG$ is cyclic of order 2.
2. If G has finite order n then $AutG$ consists of all automorphisms $\alpha_k: g \mapsto g^k \ where\ 1 \leq k \leq n\ and\ gcd(k,n) = 1$. $AutG$ is Abelian and has order $\phi(n) \ \ where \ \ \phi \ \ is\ Euler's\ function$.

Proof

Let $G = < x >$ and let $\alpha: g \to g^{-1} \ \ \forall \ g \in G\ such\ that\ \ \alpha \in AutG$. Since $(x^n)^\alpha = (x^\alpha)^n$, the automorphism α is completely determined by x^α. If G is infinite, x and x^{-1} are the only generators, so $x^\alpha = x \ \ or\ x^{-1}$ which implies that x^α generates G. Both possibilities clearly give rise to automorphisms. Hence $AutG$ is cyclic of order 2

Next, let $G =< x >= \{1, x, \dots, x^{n-1}\}$ where $1, x, \dots, x^{n-1}$ are distinct elements of $< x >$ which implies $|G| = n < \infty$.

From 1, $G =< x^\alpha >$. Since x^α must have order n, by theorem 3.3, x^k has order $m = n/(n,k)$.

We conclude that $x^\alpha = x^k \ where\ 1 \leq k < n\ and\ gcd(k,n) = 1$. Let $\alpha_k: g \to g^k$ for a positive integer k, such that $0 \leq \ k < n, gcd\ (k,n) = 1$ where $\alpha_k \in Aut\ G$.

Observe that $(x^k)^{n/(n,k)} = \ (x^n)^{k/(n,k)} = 1$ if the order of $|G| = n$ than this implies the order of $Aut\ G = n/(n,k) = \ \phi(n)$ by definition.

Example 1:

Let $C_5 = \{a, a^2, a^3, a^4, I\}$. Find $AutC_5$

Solution:

The order of $Aut\ C_5 = \ \phi(5) = 4$.

Choose $\tau : C_5 \to C_5$ where $\tau \in AutC_5$.

Suppose $\tau(a) = a^2$

Then $\tau^2(a) = \tau(\tau(a)) = \tau(a)\tau(a) = a^2.a^2 = a^4$. Thus $\tau^2 \neq I$.

Therefore the order τ of is 4 hence the same order as $Aut\ C5$ by Lagrange's theorem

Hence $AutC_5 = \{\tau, \tau^2, \tau^3, \tau^4\}$

Example 2:

Let $C_8 = \{b, b^2, b^3, b^4, b^5, b^6, b^7, I\}$. Find $AutC_8$

Solution:

The order of $AutC_8 = \ \phi(8) = 4$.

Choose $\gamma : C_8 \to C_8$ where $\gamma \in AutC_8$

Suppose $\gamma(b) = b^3$

Then $\gamma^2(b) = \ \gamma\left(\gamma\ (b)\right) = \gamma\ (b^3) = \ \gamma\ (b)\gamma\ (b)\gamma\ (b) = b^3b^3b^3 = b^9 = I.b = b$

It implies γ has order 2.

Choose $\delta : C_8 \to C_8$ where $\delta \in AutC_8$

Suppose $\delta(b) = b^5$

Then $\delta^2(b) = \delta\left(\delta(b)\right) = \delta(b^5) = \delta(b)\delta(b)\delta(b)\delta(b)\delta(b) = b^5b^5b^5b^5b^5$

$$= b^{25} = I.b = b$$

Henceδ has order 2. Therefore $AutC_8 = \{\gamma, \delta, \gamma\delta, I\}$.

Because the generatorsγ, δ are both of order2, $AutC_8$ is Klein four group.

3.6 RING

A nonempty set *R* is said to be a Ring if there are two defined binary operation namely addition$(+)$ and multiplication$(\cdot)$ such that the following conditions are satisfied.

1. For every pair $a, b \in R$ $a \cdot b \in R$
2. Multiplication is associative$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ $\forall$ $a, b, c \in R$
3. Distributive law $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot$

   $a \; \forall \; a, b, c \in R$
4. For every pair $a, b \in R$ $a + b \in R$
5. Addition is commutative $a + b = b + a$ $\forall$ $a, b \in R$
6. There is an element 0 in*R* such that $a + 0 = a$ $\forall$ $a \in R$
7. There exist an element – a in R such that $a + (-a) = 0$
8. Addition is associative $(a + b) + c = a + (b + c) \; \forall \; a, b, c \in R$

3.6.1 Commutative Ring / A Ring with unity 1

A ring*R*is said to be a commutative ring, if the multiplication on a ring*R* is such that $a \cdot b = b \cdot a$ for every $a, b \in R$ then *R* is.

A Ring with unity1: A ring *R* is said to be a ring with unity1 if *R* contains at least two distinct elements and there exist $1 \in R$ such that

$$1 \cdot a = a \cdot 1 = a \ \ for \ \ all \ \ a \in R.$$

Example

1. Let $\mathbb{Z}$ be the set of all integers. Then$\mathbb{Z}$is commutative ring with unity 1 under the usual binary operation of addition and multiplication.
2. Let$\mathbb{Q}$be the set of all rational numbers then$\mathbb{Q}$is a commutative ring under the usual binary operation of addition and multiplication
3. Let $\mathbb{C}$ be the set of all complex numbers. Then $\mathbb{C}$ is a commutative ring under the usual binary operation of addition and multiplication.

3.6.2 Subring

Let R be a ring and S a nonempty subset of$R$. Then S is a subring of R if and only if the following conditions are satisfied.

1. $rs \in S \ \ for \ all \ \ r, s \in S$
2. $r - s \in S \ \ for \ \ all \ \ r, s \in S$

3.6.3 Integral Domain

A commutative ring is an integral domain if it has no zero divisors. That is, if for every pair $a, b \in k$ such that $a \cdot b = 0$ either $a = 0$ or $b = 0$ then k is called an integral domain.

An integral domain with identity is a commutative domain with identity. An irreducible element is an element which cannot be written as a product of two non units.

Example: The ring $\mathbb{Z}$ of all integers is an integral domain. Examples of finite integral domain are$\mathbb{Z}_2$.

3.6.7 Zero Divisor

A nonzero element a in a ring R is called a zero divisor if there is a nonzero element b in R such that $ab = 0$.

Example

Let the product of two elements a and b in Z_n be defined by $a.b(mod\ n)$.

For instance, in the ring Z_{12}, the product of $5 . 7 = 11\ (mod\ 12)$.

This product makes the Abelian group Z_{12} into a commutative ring.

If we consider $3, 4 \in Z_{12}\ then\ 3.4 = 0\ (mod\ 12)$.

It is easy to see that a product of two nonzero elements in the ring can be equal to zero.

Hence Z_{12} is not an integral domain.

Theorem 3.7

Let D be an integral domain and $a, b \in D$. Then these two statements are equivalent

1. a and b are associates
2. There exists an invertible element $u \in D$ such that $a = ub$

Proof

Suppose a and b are associates is true. Let $a = ub$ where $u \in D$ or $b = va$ where $v \in D$ then $a = uva,\ a(uv - 1) = 0$, if $a = 0$ then $b = 0$ and so $a = 1 \cdot b$.

Let $u = 1$ if $a \neq 0$ then from $a(uv - 1) = 0$ then we get $uv - 1 = 0 \therefore uv = 1$

Thus u is invertible.

Therefore a and b are associates implies there exist an invertible element $u \in D$ such that

$a = ub$.

Suppose there exists an invertible element $u \in D$ such that $a = ub$ is true. Let $a = ub$ where u an invertible element in D.

Choose $v \in D$ such that $uv = 1$ then

$va = vub = b$ then $a = ub$ and $b = va \therefore a$ and b are associate.

Hence, there exist, an invertible element $u \in D$ such that $a = ub$ implies a and b are associates

3.7 FIELD

A commutative ring with an identity in which every non-zero element is invertible is called a field. Also a non-empty set F with two binary operation; addition and multiplication is said to be a field if the following conditions hold;

1. F is an additive Abelian group. That is $a + b = b + a$ where $a, b \in F$
2. F without zero is a multiplicative Abelian group.
3. The distributive laws hold. That is $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a \ \forall \ a, b, c \in F$

Examples

1. $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.
2. Z_5 is a field.
3. $\mathbb{Z}$ is not a field.

3.7.1 Subfield

Let F be a field. A subring S of F is called a subfield if S is also a field under the same binary operation of multiplication and addition.

Example $\mathbb{R}$ is a subfield of the field $\mathbb{C}$ of all complex numbers

Theorem 3.8

Every field is an integral domain

Proof

Let$F$ be a field. Then F is a commutative ring with an identity1.

Suppose there exist $a, b \in F$ such that $a \cdot b = 0$.

Now as $a \neq 0$ there exist a^{-1} such that $a^{-1} \cdot a = 1$ and so write

$$\mathrm{b} = 1 \cdot b = (a^{-1}.a).\mathrm{b} \implies \mathrm{b} = a^{-1}(a \cdot b) = a^{-1} \cdot 0 = 0 \quad \therefore b = 0$$

Similarly if $b \neq 0$ there exist b^{-1} such that $b^{-1} \cdot b = 1$ so write

$$a = 1.a = (b^{-1} \cdot b) \cdot a \Longrightarrow b^{-1}(b \cdot a) = b^{-1} \cdot 0 = 0 \therefore a = 0$$

Hence we show that F is an integral domain. Thus every finite field is an integral domain.

Theorem 3.9

Every finite integral domain is a field.

Proof

Let F be a finite integral domain. Suppose Fcontains exactly n distinct elements.

Then $F = \{0,1,2, \ldots x_n\}$ If $a \in F$ and $a \neq 0$ then $a \ldots a^n$ cannot be all distinct elements.

Choose $q \in \{1, \ldots, n\}$ and $r \in \{1, \ldots, n\}$ such that $q < r$and $a^q = a^r$.

Then $a^q(1-a^{r-q})=0$ and $a^q \neq 0$ therefore $1-a^{r-q}=0$ and $1=a^{r-q}=a^{-1}\cdot a=a^{r-q}$. If $r-q \geq 2$ then $a^{r-q-1} \in F$ where $q<r$. If $r=q=1$ then, $a=1$. Let $a^{-1}\cdot a=1, a^{-1}=1,\ a^{-1}=a^{r-q-1}$. Thus in all cases a has an inverse.

Hence every finite integral domain is a field.

Example

Let $\mathbb{Z}$ be the set of all integers. Also $\mathbb{Z}$ is an integral domain. If p is a prime number then Z_p, $Z_p=\{0,1,\ldots,p-1\}$ is an integral domain.

Since Z_p is finite integral domain then is a field.

3.7.2 Polynomials

When we talk about polynomials, we think of algebraic expressions such as $2x+1$ *or*

x^2+5x+6 *or* $2x^3+x^2-2x-1$ etc. We say these are 'polynomials in x' and say that $2x+1$ has 'degree' 1, x^2+5x+6 has 'degree' 2 and $2x^3+x^2-2x-1$ has 'degree' 3.

We know how to add, subtract and multiply such polynomials:

- $(3x+5)+(4x^2-2x-1)=4x^2+x+4$,
- $(2x^2-6)-(x^2-5x-1)=x^2+5x-5$,
- $(x^2+2x+2)(3x+1)=x^2(3x+1)+2x(3x+1)+2(3x+1)$

$$=(3x^3+x^2)+(6x^2+2x)+(6x+4)$$

$$=3x^3+7x^2+8x+4.$$

As in the case of the integers we may perform long division, for example $3x + 1$does not divide $9x^3 - 3x^2 + 6x + 4$but leaves a remainder when we employ long division as follows:

$$
\begin{array}{r}
3x^2 - 2x + \frac{8}{3} \\
3x + 1\overline{)\,9x^3 - 3x^2 + 6x + 4} \\
\underline{9x^3 + 3x^2} \\
-6x^2 + 6x \\
\underline{-6x^2 - 2x} \\
8x + 4 \\
\underline{8x + \frac{8}{3}} \\
\frac{4}{3}
\end{array}
$$

Thus we write

$$\frac{9x^3 - 3x^2 + 6x + 4}{3x + 1} = 3x^2 - 2x + \frac{8}{3} + \frac{\frac{4}{3}}{3x + 1}$$

or, more usefully,

$$9x^3 - 3x^2 + 6x + 4 = (3x + 1)\left(3x^2 - 2x + \frac{8}{3}\right) + \frac{4}{3}$$

CHAPTER 4

RING OF POLYNOMIALS

4.1 Ring of Polynomials

Let$R$ be a commutative ring with unity1. Then the ring of polynomials in indeterminate $x$with coefficients in$R$ is the collection of all polynomials in indeterminate$x$ denoted by$R[x]$.

When a polynomial in indeterminate$x$ is written as

$p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} + c_nx^n$, the coefficients$c_0, c_1, \ldots, c_n$ are in the ring$R$.

The constant coefficient isc_0. If$c_n \neq 0$, then$c_nx^n$is said to be the highest-order term or leading term andc_n is the highest-order coefficient or leading coefficient. The order of the highest non-zero coefficient is the degree of the polynomial. A polynomial is said to be ***monic*** if its leading or highest-order coefficient is 1

We have looked at polynomial rings in indeterminate$x$ in which the polynomials have coefficients from $\mathbb{Z}, \mathbb{Q}\ or\ \mathbb{R}$, yielding $\mathbb{Z}[x], \mathbb{Q}[x]\ or\ \mathbb{R}[x]$ respectively. But similarly we may have a polynomial ring in$x$ in which the coefficients belong to an integral domain$D$yielding$D[x]$. We have the following result.

Theorem 4.1

Let$D$ be an integral domain. Then the polynomial ring $D[x]$is an integral domain.

Proof

Certainly $D[x]$is a commutative ring with the identity of$D$ as the identity of $D[x]$, Thus we have to show that$D[x]$ has no proper divisors of zero.

Let

$$f(x) = a_0 + a_1x + \ldots + a_mx^m \quad (a_m \neq 0),$$

$$g(x) = b_0 + b_1x + \ldots + b_nx^n \quad (b_n \neq 0),$$

be two non-zero polynomials in $D[x]$, Then $f(x)g(x)$ is a polynomial of highest term $a_mb_nx^{m+n}$. But since$D$ is an integral domain $a_mb_n \neq 0$. Thus $f(x)g(x) \neq 0$ and $D[x]$ is an integral domain.

Corollary 4.1

Let $f(x)$ and $g(x)$ be non-zero polynomials in $D[x]$. Then

$\deg f(g(x)) = \deg f(x) + deg\ g(x)$.

Definition 4.1

Let F be a field and let $f(x)$ be a polynomial in $F[x]$. Then the greatest common divisor of the coefficients of $f(x)$ is called the **content** of $f(x)$. A polynomial of content 1 is said to be ***primitive***.

Let $f(x) \in \mathbb{Q}[x], f(x) \neq 0$. Then we may write

$$f(x) = \frac{d}{c} h(x)$$

where c, d are integers, $h(x) \in F[x]$ and $h(x)$ has content 1.

Lemma 4.1

Let $f(x)$ and $g(x)$ be primitive polynomials in $F[x]$. Suppose there exist $c_1, c_2 \in F$, $c_1 \neq 0, c_2 \neq 0$, such that $c_1 f(x) = c_2 g(x)$. Then $c_1 = \pm c_2$ and $f(x) = \pm g(x)$

Proof

Let $f(x) = a_0 + a_1 x + \ldots + a_n x^n (a_n \neq 0)$. Then the gcd of $a_0, a_1, \ldots, a_n$ is 1 and so there exist $t_0, t_1, \ldots, t_n \in F$ such that

$$t_0 a_0 + t_1 a_1 + \cdots + t_n a_n = 1$$

Since $c_1 f(x) = c_2 g(x)$, c_2 divides $c_0 a_0, c_1 a_1, \ldots, c_n a_n$ and so c_2 divides

$$t_0 c_1 a_0 + t_1 c_1 a_1 + \ldots + t_n c_1 a_n = c_1(t_0 a_0 + t_1 a_1 + \cdots + t_n a_n) = c_1$$

Similarly c_1 divides c_2. Thus $c_1 = \pm c_2$ and so $f(x) = \pm g(x)$

4.1.1 Gauss theorem

Let $f(x)$ and $g(x)$ be primitive polynomials in $\mathbb{Z}[x]$. Then $f(x)g(x)$ is primitive.

Proof

Let $f(x) = a_0 + a_1 x + \ldots + a_m x^m \quad (a_m \neq 0)$,

$g(x) = b_0 + b_1 x + \ldots + b_n x^n \quad (b_n \neq 0)$,

$f(x)g(x) = h(x) = c_0 + c_1 x + \ldots + c_{m+n} x^{m+n} \quad (c_{m+n} \neq 0)$.

If $h(x)$ is not primitive there exists a prime $p \in \mathbb{Z}$ such that p divides each of $c_0, c_1, \ldots, c_{m+n}$. Now p cannot divide all of the coefficients of $f(x)$ or all of the coefficients of $g(x)$ since $f(x)$ and $g(x)$ are primitive.

Suppose therefore that p divides $a_0, a_1, \ldots, a_{r-1}$ but p does not divide a_r where $0 \leq r < m$ and that p divides $b_0, b_1, \ldots, b_{s-1}$ but p does not divide b_s where $0 \leq s < n$.

Considering c_{r+s} we have

$$c_{r+s} = a_0 b_{r+s} + a_1 b_{r+s-1} + \cdots + a_{r-1} b_{s+1} + a_r b_s + a_{r+1} b_{s-1} + \cdots + a_{r+s} b_0$$

Now p divides $c_{r+s}; a_0, a_1, \ldots, a_{r-1}; b_0, b_1, \ldots, b_{s-1}$ and hence it follows that p divides $a_r b_s$ and so divides a_r or b_s.

But this is a contradiction and so $f(x)g(x)$ is primitive.

4.1.2 Gauss lemma

If $f \in \mathbb{Z}[x]$ and f has a factorization $f = gh$ where $g, h \in \mathbb{Q}[x]$, $deg\ g > 1$ and $deg\ h > 1$. Then f has a factorization $f = gh$ where $g, h \in \mathbb{Z}[x], deg\ g > 1$ and $deg\ h > 1$.

Proof

Let f be a primitive polynomial in $\mathbb{Z}[x]$. Let $f = gh$ choose integers m, n such that mg is primitive and nh is primitive. Hence mnf is primitive.

That implies mn is an invertible integer that is $mn = 1$.

Therefore $g \in \mathbb{Z}[x]$ and $h \in \mathbb{Z}[x]$.

4.1.3 Eisenstein's Irreducibility Criterion

Let $f(x) \in \mathbb{Z}[x]$ and let $f(x) = a_0 + a_1x + \ldots + a_mx^m \quad (a_m \neq 0)$.

Suppose there exists a prime p such that:

1. p divides $a_0, a_1, \ldots, a_{m-1}$,
2. p does not divide a_m and
3. p^2 does not divide a_0.

Then $f(x)$ is an irreducible polynomial in $\mathbb{Q}[x]$.

Proof

We prove by contradiction.

If $f(x)$ is not irreducible in $\mathbb{Q}[x]$ then $f(x)$ is not prime in $\mathbb{Q}[x]$ and so $f(x)$ may be factorized in $\mathbb{Q}[x]$ into two polynomials of $degrees\ r\ and\ s$ where $0 < r < n$,

$0 < s < n, r + s = n$. There is necessarily a corresponding factorization of $f(x)$ in $\mathbb{Z}[x]$.

Hence we may suppose that $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ of degrees r and s respectively.

Let

$$g(x) = b_0 + b_1x + \ldots + b_rx^r \quad (b_r \neq 0),$$

$$h(x) = c_0 + c_1x + \ldots + c_sx^s \quad (c_s \neq 0).$$

Now $a_0 = b_0c_0$ and since p divides a_0 but p^2 does not divide a_0, either b_0 or c_0 but not both b_0 and c_0, is divisible by p.

Suppose p divides b_0 but p does not divide c_0. If p were to divide $b_0, b_1, \ldots, b_r$ then all the coefficients of $f(x)$ would also be divisible by p and that is false. We suppose therefore that p divides $b_0, b_1, \ldots, b_{k-1}$ but p does not divide b_k for some k where $0 < k \leq r < n$.

Since $a_k = b_kc_0 + b_{k-1}c_1 + \cdots + b_0c_k$, we have that p divides $a_k; b_0, b_1, \ldots, b_{k-1}$ and so p divides b_kc_0. But p does not divide c_0 and so p divides b_k which is false.

Hence our initial assumption was wrong and consequently $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example

1. Let p be a prime. Then $x^m - p \in \mathbb{Q}[x]$ is irreducible by the criterion.
2. $24 + 6x^2 + 9x^3 + 4x^4$ is irreducible in $\mathbb{Q}[x]$ on applying the criterion with $p = 3$.

4.2 Characteristic of a Field

Let F be a field with unity 1_F. Let $\mathbb{Z}$ be the ring of all integers with unity 1. We define a homomorphism $h: \mathbb{Z} \longrightarrow F$ as

follows $h(1) = 1_F, h(0) = 0.1_F \; that \; is \; the \; \; zero \in F$.

For every positive integer m, $h(m) = 1_F + 1_F + \cdots + 1_F (m \; terms) \; and$

$h(-m) = -h(m)$; for every pair $m, n \in Z \quad h(m+n) = h(m) + h(n)$

and $h(mn) = h(m)h(n)$.

1. If the $Ker \; h = 0$, then h is a homomorphism and F is isomorphic to $h(\mathbb{Z})$. in this case F is said to be of characteristic ∞ (others say F is of characteristic 0)
2. If $Ker \; h = 0$, then $h(w) = 0$ for some positive integers, let p be the smallest positive integer such that $h(p) = 0$ where $p = 0$. Then p is a prime number and F is said to be of characteristic p.

Examples

1. $p = 2, \; Z_2 = \{0,1\}$ and Z_2 is of characteristic 2
2. $p = 3, \; Z_3 = \{0,1,2\}$ and Z_3 is of characteristic 3
3. for all $p \geq 2$ such that p is prime $Z_p = \{0,1,2, \ldots, p-1\}$ is a field with characteristic p.
4. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields with characteristic ∞.

Theorem 4.2

Let F be a field of positive characteristic p then for any polynomial

$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n$ in $F[x]$ we have

$$f(x)^p = a_0^p + a_1^p x^p + \cdots + a_{n-1}^p x^{p(n-1)} + a_n^p x^{pn}$$

Theorem 4.3

For two polynomials f, g in the ring $F[x]$ of polynomials in indeterminate x with coefficients in F, and for $r \in F$,

- $(r, f)' = r.f'$
- $(f + g)' = f' + g'$
- $(fg)' = f'g + fg'$

Definition 4.2

Let F and K be fields. If F is a subfield of K, then K is called an ***extension*** of the field F.

Theorem 4.4

If K is a field and K is an extension of a field F, then K is a vector space over F.

Definition 4.3

Let K and F be fields, such that K is an extension of F. If K is a finite dimensional vector space over F then K is called a ***finite extension*** of F. We let $[K:F]$ denote the dimension of K over F, then $[K:F]$ is called the degree of extension of K over F.

Definition 4.4

Suppose K and F are fields and K is an extension of F.

1. An element $\alpha \in K$ is said to ***algebraic*** over F, if there exists $g \in F[x]$ such that $g(\alpha) = 0$.
2. An element $\beta \in K$ is said to be ***transcendental*** over F if β is not algebraic over F.

Definition 4.5

Let K and F be fields, such that K is an extension of F. Suppose $\alpha \in K$ and α is algebraic over F. Let p be a polynomial in $F[x]$ such that the degree of p is a positive integer.

We say α is a root of p if $p(\alpha) = 0$. Given that α is a root of p, then p is said to be a ***minimum polynomial*** of degree α over F.

Theorem 4.4

Let F be a field and $p \in F[x]$ an irreducible polynomial of degree $n \geq 1$ over F. Then there exists a finite extension K of F such that $[K:F] = n$ and $\alpha \in K$ such that $p(\alpha) = 0$

Corollary 4.2

If F is a field, $f \in F[x]$ and $deg\ f \geq 1$ then there exists a field K such that K is a finite extension of F, $[K:F] \leq m!$ and f has m roots that is $\alpha_1, \alpha_2, \ldots, \alpha_m$ not necessarily distinct (some may be repeated). That is $f = \lambda(x - \alpha_1) \ldots (x - \alpha_m)$

4.3 Splitting Field

Let K be a field, and a polynomial $f(x) \in K$, we need to construct the smallest possible extension field F of K that contains all of the roots of $f(x)$. This is called a splitting field for $f(x)$ over K. Note that any two splitting fields are isomorphic.

Let F be an extension field of K and let $u \in F$. If there exists a nonzero polynomial $f(x) \in K[x]$ such that $f(u) = 0$, then u is said to be *algebraic* over K.

If not, then u is said to be *transcendental* over K.

Corollary 4.3

If F is an extension field of K, and $u \in F$ is algebraic over K, then there exists a unique monic irreducible polynomial $p(x) \in K[x]$ such that $p(u) = 0$. It is the monic polynomial of minimal degree that has u as a root, and if $f(x)$ is any polynomial in $K[x]$ with

$f(u) = 0$, then $p(x)|f(x)$.

Proof

Assume that $u \in F$ is algebraic over K, and let I be the set of all polynomials $f(x) \in K[x]$ such that $f(u) = 0$. The division algorithm for polynomials can be used to show that if $p(x)$ is a nonzero monic polynomial in I of minimal degree, then $p(x)$ is a generator for I, and thus

$p(x)|f(x)$ whenever $f(u) = 0$.

Furthermore, $p(x)$ must be an irreducible polynomial, since

if $p(x) = g(x)h(x) f\ or\ g(x); h(x) \in K[x]$, then $g(u)h(u) = p(u) = 0$, and so

either $g(u) = 0\ or\ h(u) = 0$ since F is a field.

From the choice of $p(x)$ as a polynomial of minimal degree that has u as a root, we see that either $g(x)$ or $h(x)$ has the same degree as $p(x)$, and so $p(x)$ must be irreducible.

Corollary 4.4

Let F be an extension field of K and let $u \in F$ be an element algebraic over K.

a) $K(u) \cong K[x]/< p(x) >$, where $p(x)$ is the *minimal* polynomial of u over K.

b) If the minimal polynomial of u over K has degree n, then $K(u)$ is an n-dimensional vector space over K.

Proof

Define a homomorphism $\delta: K[x]/<p(x)> \rightarrow K(u)$ by $\delta[f(x)] = f(u)$, for all congruence classes $[f(x)]$ of polynomials ($modulo \ \ p(x)$).

This mapping makes sense because $K(u)$ contains u, together with all of the elements of K, and so it must contain any expression of the form $a_0 + a_1u + \cdots + a_mu^m$, where $a_i \in K$, for each $i \in \{0,1,2, \ldots m\}$.

The function δ is well-defined, since it is also independent of the choice of a representative of $[f(x)]$. In fact, if $g(x) \in K[x]$ and $f(x)$ is equivalent to $g(x)$, then $f(x) - g(x) = q(x)p(x)$ for some $q(x) \in K[x]$, and so $f(u) - g(u) = q(u)p(u) = 0$, showing that $\delta([f(x)]) = \delta([g(x)])$.

Since the function δ simply substitutes u into the polynomial $f(x)$, and it is not difficult to show that it preserves addition and multiplication. It follows from the definition of $p(x)$ that δ is one-to-one.

Suppose that $f(x)$ represents a nonzero congruence class in $K[x] =< p(x) >$. Then $p(x) \nmid f(x)$, and so $f(x)$ is relatively prime to $p(x)$ since it is irreducible. Therefore there exist polynomials $a(x)$ and $b(x)$ in $K[x]$ such that $a(x)f(x) + b(x)p(x) = 1$.

It follows that $[a(x)][f(x)] = [1]$ for the corresponding equivalence classes, and this shows that $K[x]/<p(x)>$ is a field. Thus the image E of δ in F must be subfield of F. On the one hand, E contains u and K, and on the other hand, we have already shown that E must contain any expression of the form $a_0 + a_1u + \cdots + a_mu^m$, where $a_i \in K$, for each $i \in \{0,1,2, \ldots m\}$. It follows that $E = K(u)$, and we have the desired isomorphism.

(b) It follows from the description of $K(u)$ in part (a) that if $p(x)$ has degree n,

then the set $B = \{1, u, u^2, \dots, u^{n-1}\}$ is a basis for $K(u)$ over K.

Theorem 4.5

Let F be an extension field of K. The dimension of F as a vector space over K is called the degree of extension of F over K, denoted by $[F: K]$.

If the dimension of F over K is finite, then F is said to be a finite extension of K. Let F be an extension field of K and let $u \in F$. The following conditions are equivalent:

1. u is algebraic over K;
2. $K(u)$ is a finite extension of K;
3. u belongs to a finite extension of K.

Let K be a field and let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $K[x]$ of degree $n > 0$. An extension field F of K is called a splitting field for $f(x)$ over K if there exist elements $r_1, r_2, \dots, r_n \in F$ such that

(i) $f(x) = a_n(x - r_1)(x - r_2) \dots (x - r_n)$ and (ii) $F = K(r_1, r_2, \dots, r_n)$

4.4 GALOIS GROUP

We use the notation $Aut(F)$ for the group of all automorphisms of F, that is, all one-to-one functions from F onto F that preserve addition and multiplication.

The smallest subfield containing the identity element 1 is called the prime subfield of F. If F has characteristic zero, then its prime subfield is isomorphic to $\mathbb{Q}$ and if F has characteristic p, for some prime number p, then its prime subfield is isomorphic to Z_p.

In either case, for any automorphism σ of F we must $\sigma(x) = x$ for all elements in the prime subfield of F.

To study solvability by radicals of a polynomial equation $f(x) = 0$, we let K be the field generated by the coefficients of $f(x)$, and let F be a splitting field for $f(x)$ over K. Galois considered permutations of the roots that leave the coefficient field fixed. The modern approach is to consider the automorphisms determined by these permutations. The first result is that if F is an extension field of K, then the set of all automorphisms $\sigma: F \to F$ such that $\sigma(a) = a$ for all $a \in K$ is a group under composition of functions.

This justifies the following definitions

Definition

Let F be an extension field of K. The set $\{\theta \in Aut(F) | \theta(a) = a \ for\ all\ a \in K\}$ is called the Galois group of F over K, denoted by Gal (F/K).

Definition

Let K be a field, let $f(x) \in K[x]$, and let F be a splitting field for $f(x)$ over K. Then Gal (F/K) is called the Galois group of $f(x)$ over K, or the Galois group of the equation $f(x) = 0$ over K.

Theorem 4.6

Let K be a field, let $f(x) \in K[x]$ have positive degree, and let F be a splitting field for $f(x)$ over K. If no irreducible factor of $f(x)$ has repeated roots, then

$|Gal(F = K)| = [F: K]$.

Theorem 4.7

Let K be a finite field and let F be an extension of K with $[F: K] = m$. Then

Gal(F/K) is a cyclic group of order$m$.

Definition 4.6

A polynomial$f(x)$over the field$K$ is called ***separable*** if its irreducible factors have only simple roots.

An algebraic extension field$F$ of$K$ is called ***separable*** over$K$ if the minimal polynomial of each element of$F$ is separable.

The field$F$ is called ***perfect*** if every polynomial over$F$ is separable.

Any field of characteristic zero is perfect, and a field of characteristic$p > 0$ is perfect if and only if each of its elements has a *pth* root in the field. It follows immediately that any finite field is perfect.

The extension field F of K is called a ***simple*** extension if there exists an element$u \in F$ such that$F = K(u)$. In this case,u is called a primitive element.

Note that if $F$is a finite field, then the multiplicative group F^* is cyclic. If the generator of this group is a, then it is easy to see that$F = K(a)$for any subfield$K$.

Definition 4.7

An extension field$F$ of $K$is called a ***radical extension*** of$K$ if there exist elements $u_1, u_2, \dots, u_m \in F$ such that

(i) $F = K(u_1, u_2, \dots, u_m)$, and

(ii) $u_1^{n_1} \in K$ and $u_i^{n_i} \in K(u_1, u_2, \dots, u_{i-1})$ for $i = 2, \dots, m$ and $n_1, n_2, \dots, n_m \in Z$.

For$f(x) \in K[x]$, the polynomial equation$f(x) = 0$is said to be solvable by radicals if there exists a radical extension$F$ of$K$that contains all roots of$f(x)$.

Corollary 4.5

If F is the splitting field of $x^n - 1$ over a field K of characteristic zero, then Gal(F/K) is an Abelian group.

The roots of the polynomial $x^n - 1$ are called the *nth* roots of unity. Any generator of the group of all *nth* roots of unity is called a *primitive nth root of unity*.

Definition 4.8

The complex roots of the polynomial $x^n - 1$ are the ***nth roots of unity***. If we let θ be the complex

number $\alpha = cos\theta + isin\theta,\ where\ \ \theta = \frac{2\pi}{n}, then\ \ 1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ are each roots of $x^n - 1$, and since they are distinct they must constitute the set of all nth roots of unity. Thus we have $x^n - 1 = \prod_{k=0}^{n-1}(x - \alpha^k)$

The set of *nth* roots of unity is a cyclic subgroup of C^* of order n. Thus there are $\phi(n)$ primitive nth roots of unity, the generators of the group.

Choose a positive integer d. If $d|n$, then any element of order d generates a subgroup of order d, which has $\phi(d)$ generators.

Thus there are precisely $\phi(d)$ complex numbers of order d, all living in the group of nth roots of unity.

If p is prime, then every nontrivial $\boldsymbol{pth}$ ***root of unity is primitive***. And is a root of the irreducible polynomial $x^{p-1} + x^{p-2} + \cdots + x + 1$, which is a factor of $x^p - 1$.

Theorem 4.8

If p is a prime number and n is a positive integer, then there exists a finite field K containing exactly p^n distinct elements. K is the splitting field of the

polynomial$x^{p^n} - x$overZ_p.

Proof let$K$be the splitting field of $x^{p^n} - x$ overZ_p. The proof is done if we show that the set of all $\alpha \in K$such that$\alpha$is a root of $x^{p^n} - x$ is a field .let$f = x^{p^n} - x$and L be the set of all $\alpha \in K$such that $f(\alpha) = 0$.

Then $f(0) = 0 \Longrightarrow 0 \in L, f(1) = 0 \Longrightarrow 1 \in L$.

If$\alpha, \beta \in L$, then$(\alpha + \beta)^{p^n} = \alpha^{p^n} + \cdots . + \beta^{p^n} = \alpha + \beta \Longrightarrow \alpha + \beta \in L$.

And$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta \Longrightarrow \alpha\beta \in L$

Finally if $\eta \in L\ and\ \eta \neq 0$. Then $(\eta^{-1})^{p^n} = (\eta^{p^n})^{-1} = \eta^{-1}$ and so $\eta^{-1} \in L\ if\ \eta \in L$.

The conclusion is that$L$ is a subfield of$K$ and$L$ contains all the roots of$f$.

Therefore$L = F$this implies Kcontains exactlyp^ndistinct element and they are the roots of$x^{p^n} - x \in Z_p[x]$

4.5 CYCLOTOMIC POLYNOMIALS

Let$U_n = \{z \in C | z^n = 1\}$. Note that $U_n = < e^{2\pi i/n} > = < e^{2\pi ik/n} >$for all k such that gcd$(k, n) = 1$ where$n, k \in \mathbb{Z}\ and\ i \in \{0,1,2, \ldots, n-1\}$.

Any cyclic generator of $U_n$is called a primitive nth root of unity.

There are$\phi(n)$primitive nth roots of unity.

Definition 4.9

The nth cyclotomic polynomial is

$$\Phi_n(x) = \prod_{1 \leq i \leq n, gcd(i,n)=1} (x - \alpha^i)$$

where α is any primitive root of unity.

Definition by induction

1. Given $n = 1$, then $\Phi_1(x) = x - 1$
2. If $n > 1$ then $\Phi_n(x) = \frac{(x^n - 1)}{\prod \Phi_d(x)}$,

   where in the product in the denominator d runs over all the divisors of n except n itself.
3. When $n = p$ a prime number, then

$$\Phi_p(x) = \frac{(x^p - 1)}{(x - 1)} = x^{p-1} + x^{p-2} + \_\_\_ + x + 1$$

This implies that $(x^{p-1} + x^{p-2} + \_\_\_ + x + 1)(x - 1) = x^p - 1$

Examples

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = \frac{(x^2-1)}{\Phi_1} = \frac{(x-1)(x+1)}{(x-1)} = x + 1$
- $\Phi_3(x) = \frac{(x^3-1)}{\Phi_1} = \frac{(x^3-1)}{(x-1)} = x^2 + x + 1$
- $\Phi_4(x) = \frac{(x^4-1)}{\Phi_1\Phi_2} = \frac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = x^2 + 1 = (x - i)(x + i)$
- $\Phi_5(x) = \frac{(x^5-1)}{\Phi_1} = \frac{(x^5-1)}{(x-1)} = x^4 + x^3 + x^2 + x + 1$
- $\Phi_6(x) = x^2 - x + 1$
- $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
- $\Phi_8(x) = x^4 + 1$
- $\Phi_9(x) = x^6 + x^3 + 1$
- $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$

Remarks

1. $x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i)$
2. $x^n - 1 = \prod_{d|n,d>0} \Phi_d(x)$ since $x^n - 1 = \prod_{d|n}(\prod_{\alpha \text{ has order } d}(x - \alpha^i))$
3. $\deg \Phi_n(x) = \phi(n)$

Lemma 4.3

The nth cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$

Proof

Induction on n: when $n = 1$ the case is trivial.

Let $n > 1$ and assume $\Phi_d(x) \in \mathbb{Z}[x]$ for all $d < n$ by remark 2,

$x^n - 1 = \prod_{d|n,d>0} \Phi_d(x) = f(x)\Phi_n(x)$ where $f(x) \in \mathbb{Z}[x]$ by induction.

Note that $f(x)$ is monic, so by the Division Algorithm,

$x^n - 1 = f(x)q(x) + r(x)$ where $q(x), r(x) \in \mathbb{Z}[x]$

Thus it is also true in $\mathbb{C}[x]$; where we know $x^n - 1 = f(x)\Phi_n(x)$

By the uniqueness of quotients and remainders, $r(x) = 0$ and $\Phi_n(x) = q(x) \in \mathbb{Z}[x]$:

Theorem 4.9

The *nth* cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.

Proof

Suppose the assumption is false. Then by Gauss's Lemma, since $\Phi_n(x) \in \mathbb{Z}[x]$ there exists $f, g \in \mathbb{Z}[x]$ such that $\Phi_n(x) = fg$ where f, g are monic and f is irreducible over $\mathbb{Q}$ (if not, take an irreducible factor of f and group the other factors into g).

Let α be a root of f (and therefore of $\Phi_n(x)$) and p any prime such that $p \nmid n$. Since $gcd(p, n) = 1$ we see α^p is also a primitive nth root of unity and thus is a root of Φ_n

Claim: α^p is a root of f.

If the claim is false, then $g(\alpha^p) = 0$ which says α is a root of $g(x^p)$.

Since f is monic and irreducible, $f = Irred(\alpha, \mathbb{Q})$.

Thus $f | g(x^p)$ in $\mathbb{Q}[x]$ (and thus, in $\mathbb{Z}[x]$ as it is monic) and, so $g(x^p) = fh$ for some

$h \in \mathbb{Z}[x]$. In $\mathbb{Z}_p[x]$ we see $\acute{g}(x))^p = \acute{g}(x^p) = \acute{f}h$. Let β be any root of $f(x)$ in $\mathbb{Z}_p$, then $\acute{G}(\beta) = 0$ as we are in an Integral Domain.

Then $\Phi_n(x)$ has multiple roots, which says $\overline{x^n - 1} = x^n - 1$ has multiple roots in $\mathbb{Z}_p[x]$. But $gcd\ (x^n - 1,\ nx^{n-1}) = 1$, a contradiction. Thus α^p is a root of f.

Thus every primitive nth root of unity is a root of f which is enough to say $f = \Phi_n$ and since f is irreducible, $\Phi_n(x)$ is irreducible.

Corollary 4.6

If $\alpha \in \mathbb{C}$ is a primitive nth root of unity, then $[\mathbb{Q}(\alpha): \mathbb{Q}] = \phi(n)$ and $Irred(\alpha, \mathbb{Q}) = \Phi_n$.

Note. The above extension is normal as it is the splitting field for $\Phi_n(x)$.

Example.

Let α be a primitive $9th$ root of unity. Then $[\mathbb{Q}(\alpha): \mathbb{Q}] = \phi(9) = 6$.

To find the minimal polynomial, note that

$x^9 - 1 = \Phi_1\Phi_3\Phi_9 = (x^3 - 1)\Phi_9$

Thus $Irred\ (\alpha, \mathbb{Q}) = \Phi_9(x) = x^6 + x^3 + 1$.

Definition 4.10

An extension $\mathbb{Q}\,(\alpha)/\mathbb{Q}$ where α is a root of unity is called a *cyclotomic extension*.

Theorem 4.10

If p is a prime number then the polynomial$1 + x + \cdots + x^{p-2} + x^{p-1}$ is called the***p^{th} Cyclotomic polynomial***.

Thep^{th}Cyclotomic polynomial is irreducible over$\mathbb{Q}$. Proof

$(1 + x + \cdots + x^{p-2} + x^{p-1})(x - 1) = x^p - 1 \Rightarrow \frac{x^p-1}{x-1}$.

We change the indeterminate x by writing$x = y + 1$.

Then

$$1 + x + \cdots + x^{p-2} + x^{p-1} = \frac{(y+1)-1}{y}$$

By binomial expansion

$y^{p-1} + py^{p-2} + \cdots + py + p$if $p > 2$.

Therefore $y^{p-1} + py^{p-2} + \cdots + py + p$ is irreducible over $\mathbb{Q}$ by Eisenstein's irreduciblity criterion.

Hence $1 + x + \cdots + x^{p-2} + x^{p-1}$is irreducible over$\mathbb{Q}$.

Lemma 4.4

Let$n$be a positive integer not divisible by the characteristic of the field$F$.

Then the polynomial$x^n - 1$ has no repeated roots.

CHAPTER FIVE

CONCLUSION AND RECCOMMENDATION

5.1 CONCLUSION

The definition of Euler's phi-function is clearly stated as well as some of its important properties. There are so many uses of Euler's phi-function in abstract algebra, especially in the determination of the order and structure of automorphisms of cyclic group, Galois groups and cyclotomic polynomials.

5.2 RECOMMENDATION

I will recommend that other students take up research in other uses of the Euler phifunction in all aspects of the study of mathematics for instance, Number Theory.

NOTATION

1.	$\mathbb{N}$	-	Set of Natural numbers
2.	$\mathbb{Z}$	-	Set of Integers
3.	$\mathbb{Q}$	-	Set of Rational numbers
4.	$\mathbb{R}$	-	Set of Real numbers
5.	$\mathbb{C}$	-	Set of Complex numbers
6.	$(G,*), G$	-	A Group
7.	S, H, A, B	-	Subgroups
8.	$C_n, < a >$	-	Cyclic group
9.	$D,\ Z_n, Z_p$	-	Integral Domain
10.	R	-	A Ring
11.	F, E, K	-	A Field
12.	$\phi(n)$	-	Euler's phi function
13.	$h(x), g(x), f(x)$	-	Functions and polynomials
14.	$Gal\ (F/K)$	-	Galois group of F over K
15.	$\Phi_n(x)$	-	Cyclotomic polynomial
16.	$Aut\ G$	-	Automorphism of a Group G

REFERENCES

1. Aschbacher, M (2011) *Finite Group Theory*, Cambridge University Press

2. Austin, S. F. and Judson, T W., (2009) *Abstract Algebra (Theory and Application)*, GNU Free Documentation License
3. Beachy J. A. and Blair William D., (2006) *Abstract Algebra*, Waveland Press-Illinois-city
4. Beezer, R. A., (2011) *A Supplement to Abstract Algebra (Theory and Application)*, GNU Free Documentation License
5. Cohn, P., (2006) *Free Ideal Rings and Localization in General Rings*, Cambridge University Press
6. Garrett, P.(1997-8) *Intro to Abstract Algebra*, http://www.math.umn.edu/garret
7. Hernstien, I. N., (1964) *Topics in Algebra*, Blaisdell Publishing
8. Hungerford, T. W., (1974) *Algebra*, Springer –Verlag, New York
9. Judson T.W., (1997) *Abstract Algebra Theory and Applications* GNU Free Documentation License
10. Lang Serge, (2002) *Algebra*, Springer
11. Malone, Joseph J. Jr., (1967) *The Mathematical Gazette vol.51*, the Mathematical Association
12. Milne, J.S., (2011) *Group Theory*, Bib Tex Information
13. Oliver, R., (1998) *Whitehead Groups, Rings and Fields,* Springer –Verlag, New York
14. Robinson, D. J. S., (1982) *A course in Theory of Groups*, Springer-Verlag , New York
15. Wallace, D. A. R., (1998) *Groups, Rings and Fields*, Springer –Verlag, London