

SOME IMPORTANT USES OF PRIME NUMBERS IN ABSTRACT ALGEBRA

By

MARY OSEI FOKUO

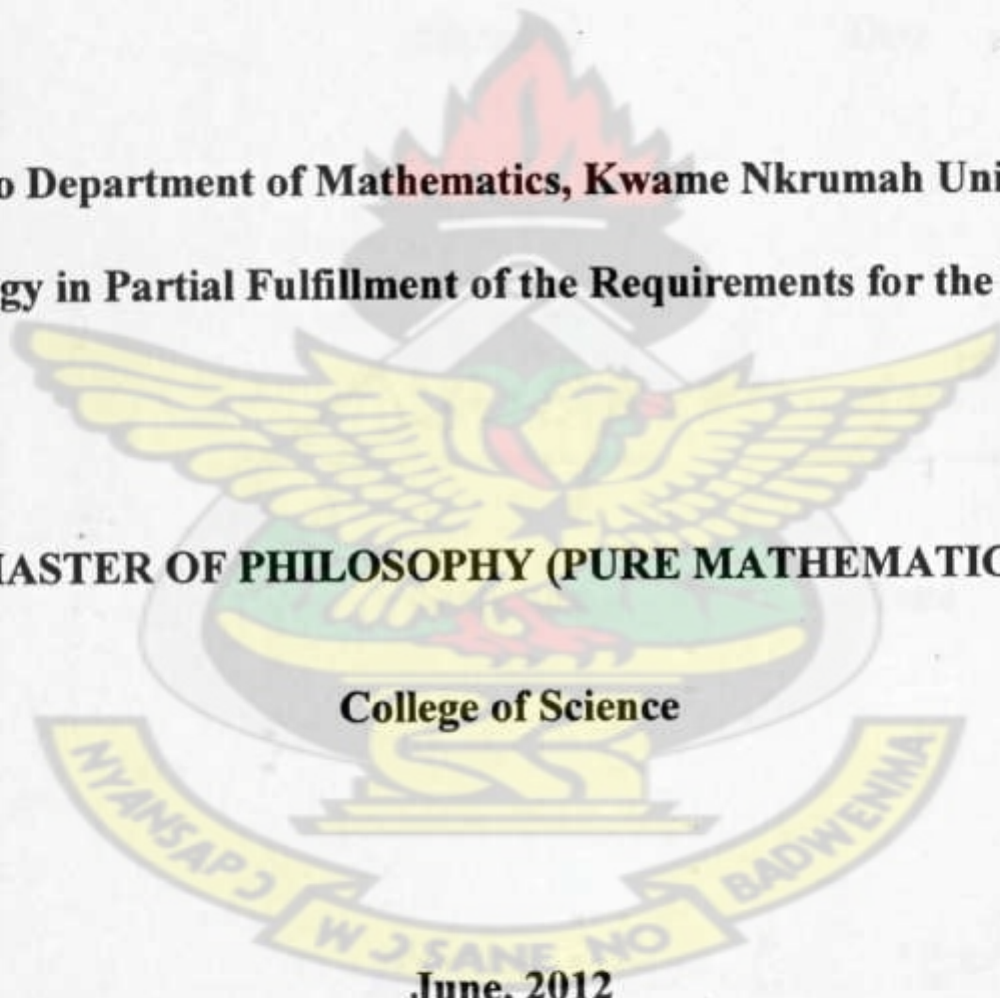
KNUST

**A Thesis Submitted to Department of Mathematics, Kwame Nkrumah University of Science and
Technology in Partial Fulfillment of the Requirements for the Degree of**

MASTER OF PHILOSOPHY (PURE MATHEMATICS)

College of Science

June, 2012



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 other degree of the university, except where due acknowledgement has been made in the text.

Mary Osei Fokuo (PG5074110)



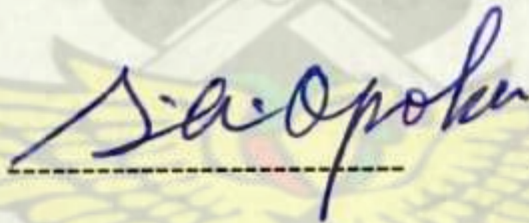
24th July, 2012

Signature

Date

Certified by:

Dr. S. A. Opoku



24th July, 2012

Supervisor

Signature

Date

Certified by:

Mr. F. K. Darkwah



20/07/2012

Head of Department

Signature

Date

DEDICATION

I dedicate this thesis to God Almighty.

KNUST



ACKNOWLEDGEMENT

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

To my supervisor Dr. S. A. Opoku for his supervision throughout the study.

I also acknowledge my friend Patience Ahiaku for her support and encouragement.

Lastly, it goes to my husband Elias Boakye for his support and love and all my family members.

KNUST



ABSTRACT

A prime number is a natural number greater than 1 which has only two factors among natural numbers, namely, 1 and itself. That is equivalent to the assertion "a positive integer p is prime if, and only if $p > 1$ and every positive integer which divides p is either 1 or p ". Prime numbers have been used to formulate many useful principles in Abstract Algebra. In fact there are many useful theorems in Abstract Algebra which are based on prime numbers.

Prime numbers have been used to produce many useful theorems, especially on finite fields, irreducibility of certain polynomial of the field of rational numbers and in group theory, to define p -groups and sylow p -subgroup.

This thesis seeks to provide some of the most commonly used results which have prime numbers in their background.

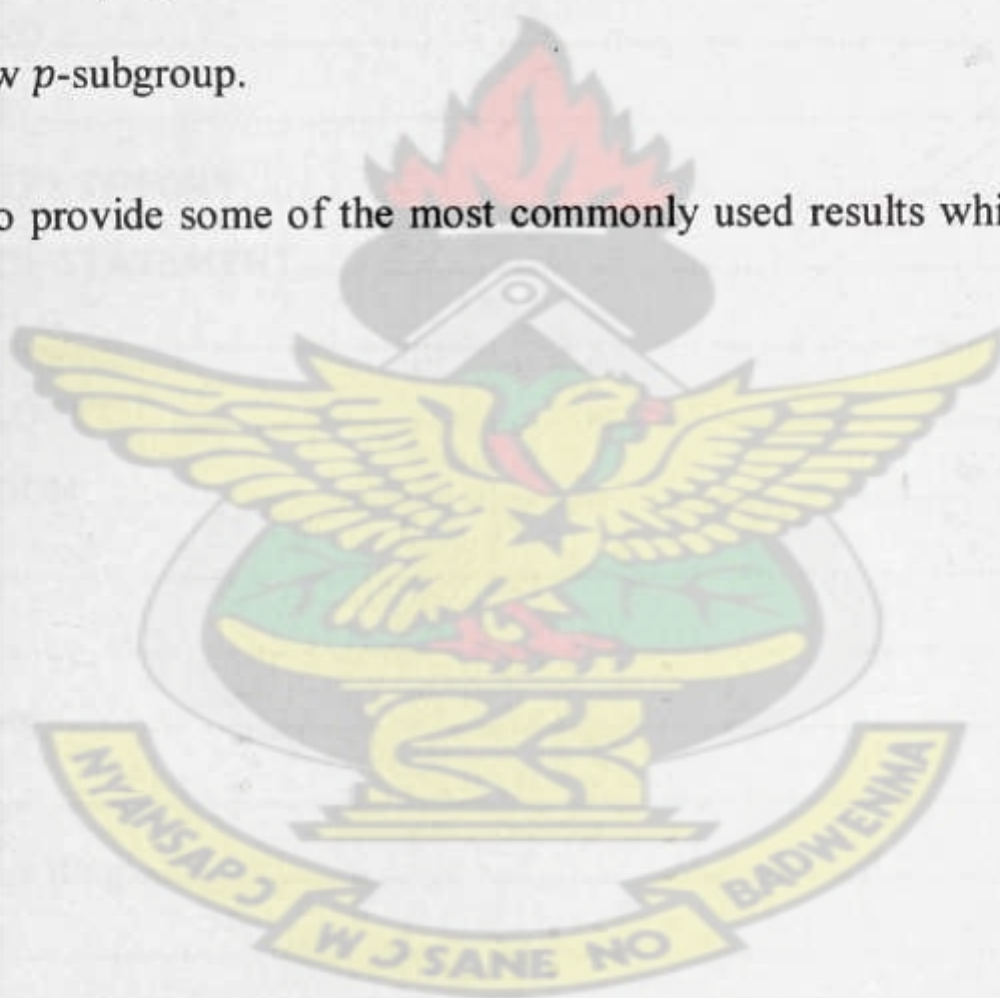


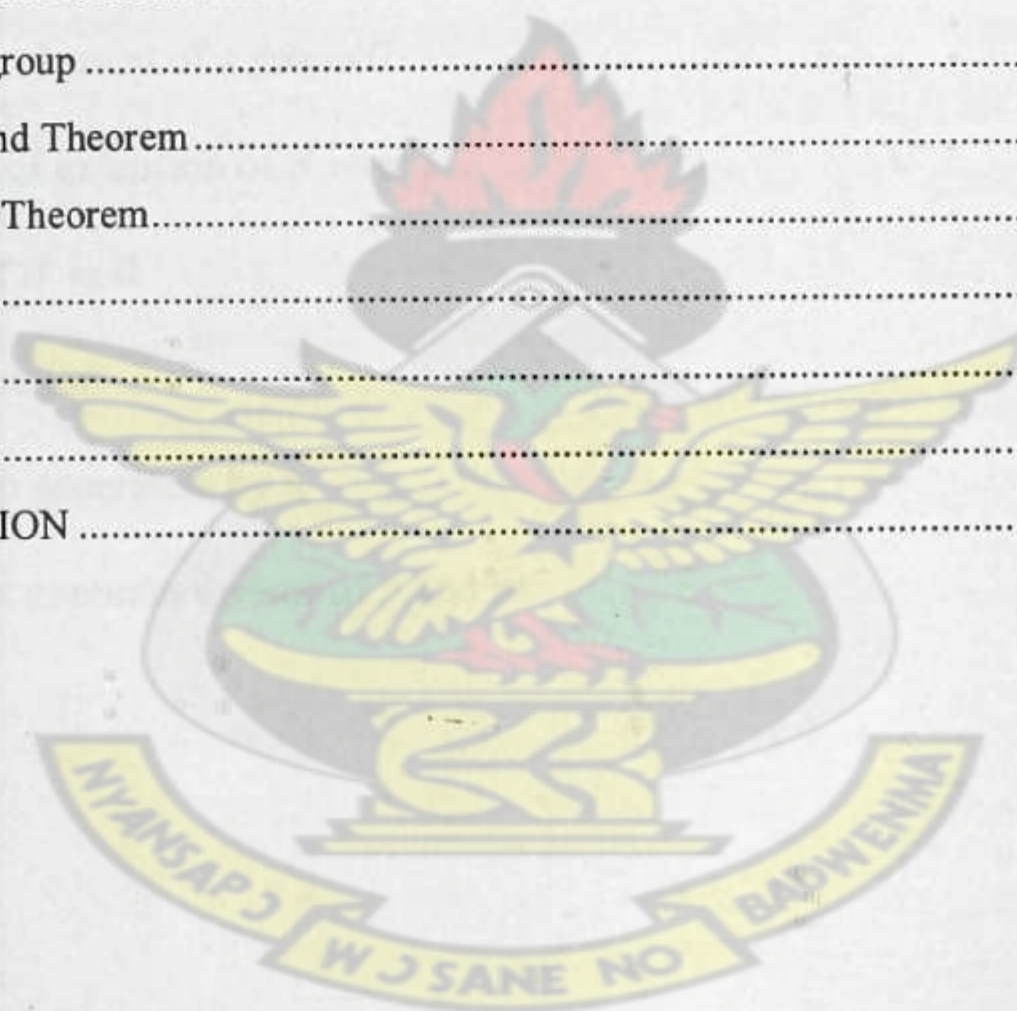
TABLE OF CONTENTS

Table of Contents

DECLARATION.....	ii
DEDICATION.....	iii
ACKNOWLEDGEMENT.....	iv
ABSTRACT.....	v
TABLE OF CONTENTS.....	vi
NOTATION.....	ix
CHAPTER 1.....	1
INTRODUCTION.....	1
1.1 BACKGROUND.....	1
1.2 DEFINITION.....	2
1.2.1 EUCLID'S THEORY.....	3
1.3 PROBLEM OF STATEMENT.....	3
1.4 OBJECTIVE.....	4
1.5 METHODOLOGY.....	4
1.6 JUSTIFICATION.....	4
CHAPTER 2.....	5
RING.....	5
2.1 Basic Concepts.....	5
2.1.1 Definition.....	5
2.1.2 Commutative Ring.....	6
2.2 Ideal.....	6
2.2.1 Maximal Ideal.....	7
2.2.2 Prime Ideal.....	8
2.3 Quotient Ring.....	9
2.4 Integral Domain.....	9
2.5 Euclidean Algorithm.....	11
2.6 Definition on Factors.....	11
2.6.1 Associates.....	12
2.6.2 Relatively Prime.....	14

2.6.3 Prime element	14
2.6.4 Unique Factorization Domain (U.F.D).....	15
2.7 Principal Ideal Domain (P.I.D).....	16
2.8 Some Useful Results On Principal Ideal Domain.....	19
CHAPTER 3	21
FIELD.....	21
3.1 DEFINITION	21
3.2 Subfield.....	21
3.3 Finite Characteristic.....	23
3.4 Vector Space.....	26
3.5 Extension of a Field	26
3.6 Primitive Polynomial	28
3.6.1 Gauss Lemma	30
3.6.2 Eisenstein's Irreducibility Criterion.....	31
3.6.3 Cyclotomic Polynomial.....	32
3.6.4 The p th Cyclotomic Polynomial.....	33
3.7 Splitting Field.....	33
3.8 Finite Field	34
CHAPTER 4	38
EXERPTS ON THE USE OF PRIME NUMBERS IN GROUP THEORY.....	38
4.1 GROUP	38
4.1.1 Axioms of a group.....	38
4.1.2 Commutative Group.....	39
4.1.3 Subgroup.....	39
4.1.4 Normal Subgroup.....	39
4.1.5 Center of a Group.....	40
4.1.6 Cyclic Group.....	41
4.1.7 Homomorphism	41
4.1.8 Isomorphism	42
4.2 Automorphisms of a Group	42
4.2.1 Kernel of a Group	42
4.2.2 Left Cosets and Right Cosets of a Subgroup	43

4.3	Finite Group	43
4.3.1	Lagrange Theorem	43
4.3.2	Normaliser and Centraliser	44
4.3.3	Cauchy Theorem	45
4.4	p -Group	46
4.4.1	Nilpotent	48
4.5	Finite p -group	48
4.6	Fratini subgroup	50
4.7	p -subgroup	51
4.8	Sylow's Theorem	55
4.8.1	Sylow's First Theorem	55
4.8.2	Sylow p -Subgroup	56
4.8.3	Sylow's Second Theorem	57
4.8.4	Sylow's Third Theorem	59
4.9	Simple Group	60
CHAPTER 5	62
5.1	CONCLUSION	62
5.2	RECOMMENDATION	62



NOTATION

$Z_a(G)$: Conjugate Class of a in G

$C_G(a)$: Centralizer of a in G

$N_G(H)$: the normalizer of H in G

$C(G)$: Center of G

$\text{Ker } h$: Kernel of h

$|G|$: Order of a group G

e : Identity element of a group G

$[K:F]$: Degree of extension of K over F

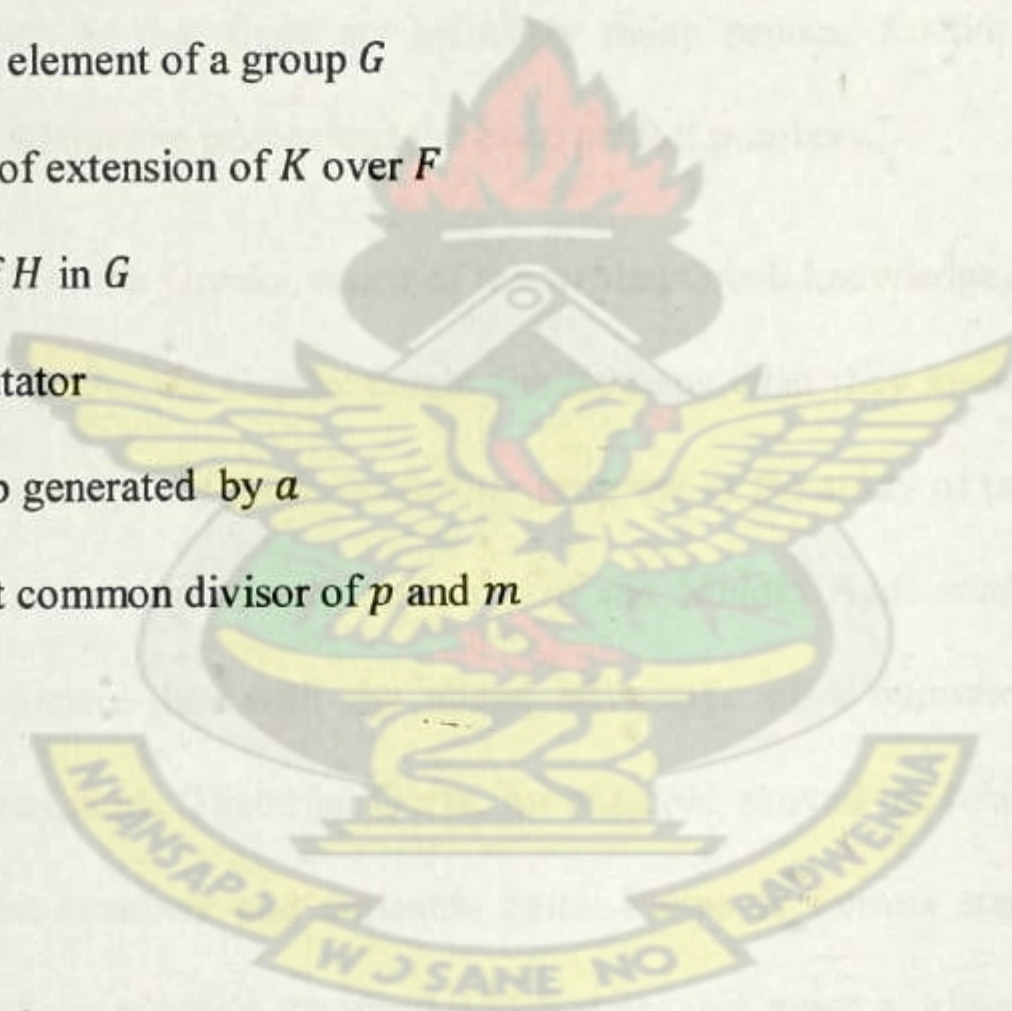
$[G:H]$: Index of H in G

$[G,H]$: Commutator

$\langle a \rangle$: A group generated by a

(p,m) : greatest common divisor of p and m

KNUST



LIBRARY
KWAME NKROMAN UNIVERSITY OF
SCIENCE AND TECHNOLOGY
KUMASI-GHANA

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Prime numbers and their properties were first studied extensively by the ancient Greek Mathematicians. About twenty-five hundred years ago, the ancient Greek often got credit for being the first to study prime numbers for their own sake. Eratosthenes came up with the sieve of Eratosthenes, and Euclid proved many important basic facts about prime numbers which today we take for granted, such as that there are infinitely many primes. Euclid also proved the relationship between the Mersenne primes and the even perfect numbers.

With the Roman conquest of the Greeks, much of the written Greek knowledge was translated to Latin, or at least preserved. As the Greeks taught the Romans what they knew, they preserved Greek mathematical knowledge but made no further progress in the study of pure mathematics, such as prime numbers. The Arab mathematicians of the Middle Ages studied the work of ancient Greek mathematicians but with the added advantage of a numerical system more amenable to computational work. Thabit ibn Qurra, for example, proved the relationship between consecutive prime Thabit numbers and amicable pairs. Pierre de Fermat stated an important theorem (now known as Fermat's little theorem) which states that given a prime p and a coprime base b , the congruence $b^{p-1} \equiv 1 \pmod{p}$ holds true.

In the 20th century, computers gradually became important in calculating data for theorists to ponder; from the 13th Mersenne prime on all the largest primes since the middle of the century have been found with the help of computers. The invention of public key cryptography in the late 1970s has precipitated the need for larger prime numbers and motivated many advances in

integer factorization algorithms. From the 1990s onwards, distributed computing projects like the Great Internet Mersenne Prime Search and Seventeen or Bust have discovered some of the largest known prime numbers.

An integer greater than one is called a prime number, if it's only positive divisors (factors) are one and itself. For example, the prime divisors of 10 are 2 and 5; and the first six primes are 2, 3, 5, 7, 11, and 13. The Fundamental Theorem of Arithmetic shows that the primes are the building blocks of the positive integers: every positive integer is a product of prime numbers in one and only one way, except for the order of the factors. On the other hand, in the nineteenth century it was shown that the number of primes less than or equal to n^{th} prime is approximately equal to $\frac{n}{\log n}$.

1.2 DEFINITION

A prime number is a natural number greater than 1 which has only two factors among natural numbers, namely, 1 and itself. Examples of prime numbers are 2, 3, 5, 7, 11 etc.

For larger natural numbers, prime number can be determined by using the primality testing. Since prime numbers do not follow any pattern. The primality testing is of two tests. The first is deterministic primality test and the second is probabilistic primality test.

Deterministic primality test determine whether a number is prime. It is mostly based on factorization techniques.

Probabilistic primality test determine whether a number is prime or not with a given degree of confidence. Many important basic facts about prime numbers were proved by Euclid. For example, there are infinitely many prime numbers.

1.2.1 EUCLID'S THEORY

There are infinitely many prime numbers

Proof

Suppose that there were only finitely many prime numbers. Then we could list all of them

p_1, p_2, \dots, p_n . Then consider the number $M = p_1 p_2 \dots p_{n-1} p_n + 1$.

That is, M is the product of all the primes plus 1. Choose $p \in \{p_1, \dots, p_n\}$ such that p is a factor of M .

Then p cannot be in the list p_1, p_2, \dots, p_n , since if it were in that list, then p would divide $M - (p_1 p_2 \dots p_n) = 1$. Then there is a contradiction p divides 1 and p cannot divide 1 since $p > 1$. Thus, there are infinitely many prime numbers.

1.3 PROBLEM OF STATEMENT

Prime number is one of the important numbers used in Mathematics. Even back in our primary school days, prime numbers were featuring in factorization. Prime numbers play a vital role when we talk about characteristics of a field.

With the definition of prime number, prime field is an example of how prime number has been used. It also leads to the studying of all finite fields.

The study of p -groups, sylow p -subgroup and Sylow theorem of a finite field will also be considered.

This thesis seeks to examine the role of prime numbers in abstract algebra.

1.4 OBJECTIVE

Prime numbers are used widely in both abstract algebra and number theory. The aim of this thesis is to identify the main uses of prime number in abstract algebra and its importance. Also to know how prime number helps to formulate certain theorems and prove them. Examples are using prime numbers to describe all finite fields and using prime numbers to describe certain important subgroups of finite groups like p -groups and sylow p -subgroup.

1.5 METHODOLOGY

To present an overview of the uses of prime numbers in abstract algebra considering the following topics such as rings, commutative rings, fields, integral domain, finite fields, characteristic of a field, groups, Cauchy's theorem, p -subgroup, sylow p -subgroup, sylow theorem, and Galois theory. Every finite integral domain is a field.

1.6 JUSTIFICATION

The study will be such that it will be easy to study it without going to look through any text book. It will also help you to learn more about prime numbers. That is deduced from the definition, how to identify that a number is prime and looking at its application in various accept of abstract algebra.

CHAPTER 2

RING

2.1 Basic Concepts

2.1.1 Definition

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.

R₁: For every pair $a, b \in R$ $a + b \in R$

R₂: Addition is commutative

$$a + b = b + a \quad \forall a, b \in R$$

R₃: Addition is associative

$$(a + b) + c = a + (b + c) \quad \forall a, b, c \in R$$

R₄: There is an element 0 in R such that

$$a + 0 = a \quad \forall a \in R$$

R₅: There exist an element $-a$ in R such that

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

R₆: For every pair $a, b \in R$ $a \cdot b \in R$

R₇: Multiplication is associative

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in R$$

R₈: Distributive law

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

and $(b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in R$

2.1.2 Commutative Ring

If the multiplication of a ring R is such that $a \cdot b = b \cdot a$ for every $a, b \in R$ then R is a commutative ring.

Ring with unit 1: A ring R is said to be a ring with unity 1 if R contains at least two distinct elements and there exist $1 \in R$ such that $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$.

Example

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

2.2 Ideal

Let R be a ring and S a nonempty subset of R that is closed under the operations of addition and multiplication in R . If S is itself a ring under these operations then S is called a subring of R . A

nonempty subset I of a ring R is a left ideal if and only if for all $x, y \in I$ and $r \in R$

i) $x, y \in I \Rightarrow x - y \in I$

ii) $x \in I, r \in R \Rightarrow rx \in I$

Similarly, I is a right ideal if and only if for all $x, y \in I$ and $r \in R$

i) $x, y \in I \Rightarrow x - y \in I$

ii) $x \in I, r \in R \Rightarrow xr \in I$

If I is both a left and a right ideal then I is called ideal.

Example

1: For an integer Z , $I = \{2k | k \in Z\}$

2: For each integer n the cyclic subgroup $\langle n \rangle = \{kn | k \in Z\}$ is an ideal in Z .

3: Let R be any commutative ring with unity 1. If $a \in R$, let $\langle a \rangle = \{xa | x \in R\}$, then $\langle a \rangle$ is an ideal.

Proof

Suppose that $u, v \in \langle a \rangle$: thus $u = xa$, $v = ya$ where $x, y \in R$. Hence

$$\begin{aligned} u + v &= xa + ya \\ &= (x + y)a \in \langle a \rangle \end{aligned}$$

Also if $u \in \langle a \rangle$ and $r \in R$ then $u = xa$. $ru = rxa = (rx)a \in \langle a \rangle$. Thus $\langle a \rangle$ is an ideal of R .

2.2.1 Maximal Ideal

An ideal M in a ring R is said to be a maximal ideal of R if $M \neq R$ and whenever I is an ideal of R such that $M \subset I \subset R$ then either $R = I$ or $M = I$.

Theorem 2.2.1

If R is a commutative ring such that $R^2 = R$, then every maximal ideal M in R is prime.

Proof

Suppose $M \neq R$ and $ab \in M$ but $a \notin M$ and $b \notin M$. Then each $M + \langle a \rangle$ and $M + \langle b \rangle$ properly contains M . $M + \langle a \rangle = R = M + \langle b \rangle$, since R is commutative and $ab \in M$, it implies

$$\langle a \rangle \langle b \rangle \subset \langle ab \rangle \subset M$$

$$\therefore R = R^2 = (M + \langle a \rangle)(M + \langle b \rangle) \subset M^2 + \langle a \rangle M + M \langle b \rangle + \langle a \rangle \langle b \rangle \subset M.$$

This contradicts the fact that $M \neq R$. Therefore $a \in M$ or $b \in M$. Hence M is prime.

2.2.2 Prime Ideal

An ideal P in a ring R is said to be prime if $P \neq R$ and for any ideal A, B in R

$$AB \subset P \Rightarrow A \subset P \text{ or } B \subset P. \text{ For example } a \in A, b \in B \text{ and } ab \in P \Rightarrow a \in P \text{ or } b \in P$$

Theorem 2.2.2

If P is an ideal in a ring R such that $P \neq R$ and for all $a, b \in R$ $ab \in P \Rightarrow b \in P$ or $a \in P$ then P is a prime.

Proof

If A and B are ideals such that $AB \subset P$ and $A \not\subset P$, then there exist an element $a \in A - P$.

For every $b \in B$, $ab \in AB \subset P$. Hence $a \in P$ or $b \in P$. Since $a \notin P$, we must have $b \in P$ for all $b \in B$: thus $B \subset P$. Therefore P is prime.

Conversely, if P is any ideal and $ab \in P$, then the principal ideal $\langle ab \rangle$ is contained in P . If R is commutative implies that $\langle a \rangle \langle b \rangle \subset \langle ab \rangle$ hence $\langle a \rangle \langle b \rangle \subset P$. If P is prime then either $\langle a \rangle \subset P$ or $\langle b \rangle \subset P$. Hence $a \in P$ or $b \in P$.

2.3 Quotient Ring

Let S be a multiplicative subset of a commutative ring R and let $S^{-1}R$ be the set of equivalence classes of $R \times S$ under the equivalence relation then

i) $S^{-1}R$ is a commutative ring with identity, where addition and multiplication are defined by

$$r/s + r'/s' = (rs' + r's)/ss' \text{ and } (r/s)(r'/s') = rr'/ss'$$

ii) If R is a nonzero ring with no zero divisors and $0 \notin S$, then $S^{-1}R$ is an integral domain.

iii) If R is a nonzero ring with no zero divisors and S is set of all nonzero element of R , then

$S^{-1}R$ is a field. Therefore $S^{-1}R$ is a quotient ring.

2.4 Integral Domain

An integral domain is a commutative ring with unity 1 such that $1 \neq 0$ and it has no zero divisors. That is, a commutative ring K with unity $1 \neq 0$ is an integral domain is an integral domain, 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 irreducible element is an element which cannot be written as a product of two non units.

Example: The ring Z of all integers is an integral domain. Examples of finite integral domain are

Z_2, Z_3, Z_5, \dots There are some finite commutative rings with unity which are not integral domain

such as Z_4, Z_6, Z_8, \dots

Theorem 2.4.1

In a commutative ring R with identity $1_R \neq 0$ an ideal P is prime if and only if the quotient ring R/P is an integral domain.

Proof

R/P is a commutative ring with identity $1_R + P$ and zero element $0 + P = P$. If P is prime, then

$1_R + P \neq P$ since $P \neq R$.

Furthermore, R/P has no zero divisors since

$$(a + P)(b + P) = P$$

$$\Rightarrow ab + P = P$$

Therefore $ab \in P \Rightarrow a \in P$ or $b \in P$. So $a + P = P$ or $b + P = P$.

Hence R/P is an integral domain.

Conversely, if R/P is an integral domain, then $1_R + P \neq 0 + P$,

hence $1_R \notin P$.

$\therefore P \neq R$. Since R/P has no zero divisors,

$$ab \in P \Rightarrow ab + P = P$$

$$(a + P)(b + P) = P$$

$$\Rightarrow a + P = P \text{ or } b + P = P, a \in P \text{ or } b \in P$$

Hence P is Prime

Therefore, in a commutative ring R with identity $1_R \neq 0$ an ideal P is prime if and only if the quotient ring R/P is an integral domain.

2.5 Euclidean Algorithm

If m and n are integers with $n > 0$, then there exist integer q and r with $0 \leq r < n$ such that

$$m = qn + r.$$

Proof

Let $W = \{m - tn \mid t \in \mathbb{Z}\}$. We claim that W contains some nonnegative integers, for if t is large enough and negative, then $m - tn > 0$. Let $v = \{v \in W \mid v \geq 0\}$ by the well-ordering principle v has a smallest element, r since $r \in v, r \geq 0$ and $r = m - qn$ for some q . We claim that $r < n$ if not $r = m - qn \geq n$. Hence $m - (q + 1)n \geq 0$.

But $m - (q + 1)n \in v$ yet $m - (q + 1)n < r$. Contradicting the minimal nature of r in v .

Hence the Euclidean Algorithm.

Well-ordering principle: Any nonempty set of nonnegative integers has a smallest element.

This is the well-ordering principle for nonnegative integers.

2.6 Definition on Factors

Let a and b be integers. Then a is said to be a **factor** of b if there is an integer k such that

$$b = ak.$$

Let x and y be integers, then an integer c is called a **common factor** of x and y if c is a factor of x and c is a factor of y .

Let a and b be integers. Then an integer c is said to be **highest common factor** of a and b if:

Theorem 2.6.1

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 exist 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 $uv = 1$

$$\text{then } va = vub = b$$

$$\text{then } a = ub \text{ and } b = va$$

$\therefore a$ and b are associate

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

2.6.2 Relatively Prime

A pair of integers x, y are said to be relatively prime if 1 is the only positive integer which divides both of x and y . For example 24 and 35 are relatively prime.

Corollary

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

KNUST

Lemma 2.6.2

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 .

2.6.3 Prime element

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

- i) p is a nonzero nonunit
- ii) if p/ab then p/a or p/b where $a, b \in D$.

2.6.4 Unique Factorization Domain (U.F.D)

A unique factorization domain is any integral domain in which every nonzero noninvertible element has a unique factorization.

Thus an integral domain R is a unique factorization domain provided that

- i) every nonzero nonunit element a of R can be written $a = c_1 c_2 \dots c_n$, with $c_1 c_2 \dots c_n$, irreducible.
- ii) If $a = c_1 c_2 \dots c_n$, and $b = d_1 d_2 \dots d_m$ (c_i, d_i irreducible) then $n = m$ and for some permutation α of $(1, 2, \dots, n)$, c_i and d_i are associates for every i .

Theorem 2.6.4

In a unique factorization domain every irreducible element is prime.

Proof

Let D be a U.F.D. Let a be an irreducible element of D . Suppose x divides b ($a, b \in D$). Suppose there exists $y \in D$ such that $xy = ab$. Now y, a and b are products of irreducible elements, say, $y = r_1 r_2 \dots r_t$, $a = c_1$, $b = d_1 d_2 \dots d_m$, $y = r_1 r_2 \dots r_t$

where $c_1, c_2, \dots, c_n, d_1, d_2, \dots, d_m$ and r_1, r_2, \dots, r_t are irreducible elements.

Then $xy = ab$, $x(r_1 r_2 \dots r_t) = (c_1 c_2 \dots c_n)(d_1 d_2 \dots d_m)$. But these are two factorizations into irreducible elements and so, as D is a U.F.D, we must have $1 + t = n + m$ and, more importantly, every irreducible element on the left-hand side must be an associate of an irreducible element on the right-hand side. Thus x is an associate of some c_i or some d_j .

But this implies that x divides a or x divides b .

2.7 Principal Ideal Domain (P.I.D)

An integral domain D is called a principal ideal domain if every ideal I in D is of the form

$$I = \{xa \mid x \in D\} \text{ for some } a \in I.$$

If K is a commutative ring with unity 1 then the ring $K[X]$ of all polynomials over K in indeterminate X is a principal ideal. Also an integral domain in which every ideal is principal is called a principal ideal domain.

Lemma 2.7.1

Let D be a Principal Ideal Domain (P.I.D). Any two non-zero elements a and b of D have a highest common factor given by $Da + Db = Dd$.

Proof

Da and Db are ideals of D and so $Da + Db$ is also an ideal. Hence as D is a P.I.D there exist $d \in D$ such that $Da + Db = Dd$. Certainly $Da \subseteq Dd$ and so d divides a and similarly d divides b . Thus d is a common divisor of a and b . Suppose $c \in D$ is also a common divisor of a and b . Now $d \in Da + Db$ and so there exist $x, y \in D$ such that $d = xa + yb$. But now if c divides a and c divides b , we must know that c divides d . Thus d is a highest common factor of a and b .

Theorem 2.7.2

A principal ideal domain is also a unique factorization domain.

Proof

Let D be a principal ideal domain and every non-zero element of D which is not a unit is a finite product of irreducible elements. Let $a \in D$ and let a be expressed as

$a = c_1 c_2 \dots c_n = d_1 d_2 \dots d_m$ where c_1, c_2, \dots, c_n and d_1, d_2, \dots, d_m are irreducible elements of D .

Then c_1 divides $d_1 d_2 \dots d_m$ and so divides one of d_1, d_2, \dots, d_m . Suppose c_1 divides d_1 . Then c_1 and d_1 are irreducible elements which are associates and so $d_1 = uc_1$ where u is a unit of D .

Then $c_1 c_2 \dots c_n = d_1 d_2 \dots d_m = uc_1 d_2 \dots d_m$ which implies that

$c_2 c_3 \dots c_n = ud_2 d_3 \dots d_m = d'_2 d_3 \dots d_m$ where $d'_2 = ud_2$ is an irreducible element.

Hence by induction, the theorem is proof.

Theorem 2.7.3

In a principal ideal domain (P.I.D), every irreducible element is prime.

Proof

Let D be P.I.D. Let P be an irreducible element of D . Let p divides ab where $a, b \in D$. Suppose p does not divide a , let $c \in D$ be such that c divides p and c divides a . Since p is irreducible c is a unit or an associate of p . If c is an associate of p then as c divides a so also does p divides a which is false. Hence c is a unit. Hence by lemma 2.7.1

$Da + Dp = Dd$ where d is necessarily a unit and so $Dd = D$, giving $Da + Dp = D$.

Hence there exist $x, y \in D$ such that $xa + yp = 1$.

But then $xab + ybp = b$ from which p divides b . Hence p is a prime.

Theorem 2.7.4

The ring Z of all integers is an example of a principal ideal domain.

Proof

$0 \in I$. If $I \neq 0$, choose any $x \in I$ such that $x \neq 0$ then $|x|$ is a positive integer and $|x| \in I$. Using the well-ordering principle, for positive integers let a be the smallest positive integer in I .

If $x \in I$ use the Euclidean Algorithm to write $x = qa + r$ where q, r are integers and

$0 \leq r < a$. Then, $r = x - qa \in C(a)$. $C(a)$ is the principal ideal in Z . This implies $C(a) \subset I$.

Hence r cannot be positive integer. Hence $r = 0$, thus $x = qa$.

Theorem 2.7.5

If p is a prime then the square root of p is not a rational number.

Proof

To prove that if p is prime number then there is no rational number r such that $r^2 = p$; assume that r is a rational number and $r^2 = p$. Let $r = \frac{m}{n}$ where m and n are positive integers such that m and n are relatively prime. Then $m^2 = n^2p$. It follows that $m = pk$, where k is a positive integer. That also implies $n^2 = k^2p$. Hence $n = gp$, where g is a positive integer. This contradicts the assertion that m and n are relatively prime since $p \leq 2$. The assumption is false.

Hence there is no rational number r such that $r^2 = p$.

Theorem 2.7.6

If R is a principal ring and $I_1 \subset I_2 \subset \dots$ is a chain of ideals in R , then for some positive integer

$$n, \quad I_j = I_n \forall j \geq n$$

Proof

Let $A = \bigcup_{i \geq 1} I_i$. We claim that A is an ideal. If $a, b \in A$ then $a \in I_i$ and $b \in I_i$. Either $i \leq j$ or

$i \geq j$. Consequently $I_j \subset I_i$ and $a, b \in I_i$ since I_i is an ideal $a - b \in I_i \subset A$. Therefore, A is an

ideal. By hypothesis A is principal. Say $A = I$, since $a \in A = \bigcup I_i$ and $a \in I_n$ for some n .

Therefore, for every $j \geq n, I \subset I_n \subset I_j \subset A \subset I$

Hence $I_j = I_n$.

Theorem 2.7.7

If a is an element in a principal ideal domain D such that $a \neq 0$ and a is not invertible then there exist a prime element such that p divides a .

2.8 Some Useful Results On Principal Ideal Domain

If a, b are elements in a principal ideal domain D then there exist $\gamma, \eta \in D$ such that $a\gamma + b\eta$ is a highest common factor of a and b . If c is a highest common factor of a and b in D . Then there exist $\gamma_1, \eta_1 \in D$ such that $c = a\gamma_1 + b\eta_1$.

Corollary 1: let a, b be elements of a principal ideal domain D . Then a and b are relatively prime if and only if there exist $u, w \in D$ such that $au + bw = 1$

Corollary 2: let p be a prime element in a principal ideal domain D . If x, y are elements of D such that p divides xy then either p divides x or p divides y .

Corollary 3: If a is an element in a principal Ideal domain D such that $a \neq 0$ and a is not invertible then there exist a prime element p in D such that p divides a .

Corollary 4: If a is an element in a principal ideal domain D such that $a \neq 0$ and a is not invertible element v in D . There are finitely many prime elements p_1, \dots, p_k in D and positive integers v_1, \dots, v_t such that $a = vp_1^{v_1} \dots p_k^{v_t}$

KNUST



CHAPTER 3

FIELD

3.1 DEFINITION

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

F_1 : F is an additive Abelian group. That is $a + b = b + a$ where $a, b \in F$

F_2 : $F - \{0\}$ is a multiplicative Abelian group.

F_3 : The distributive laws hold.

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

and $(b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a, b, c \in F$

3.2 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: R is a subfield of the field C of all complex numbers

Theorem 3.2.1

Every field is an integral domain

Proof

Let F be a field. Then F is a commutative ring with an identity 1. 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

$$\begin{aligned} b &= 1 \cdot b \\ &= (a^{-1} \cdot a) \cdot b \\ &= a^{-1}(a \cdot b) \\ &= a^{-1} \cdot 0 = 0 \end{aligned}$$

$$\therefore b = 0$$

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

$$\begin{aligned} a &= 1 \cdot a \\ &= (b^{-1} \cdot b) \cdot a \\ &= b^{-1}(b \cdot a) \\ &= b^{-1} \cdot 0 = 0 \end{aligned}$$

$$\therefore a = 0$$

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

Theorem 3.2.2

Every finite integral domain is a field.

Proof

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

Then $n \geq 2$ and $F = \{a_1, a_2, \dots, a_n\}$. If $a \in F$ and $a \neq 0$ then a, \dots, a^n cannot be all distinct elements. Choose $q \in \{1, \dots, n\}$ and $r \in \{1, \dots, n\}$ such that $q < r$ and $a^q = a^r$.

If $r - q = 1$ then $a = 1$. 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 $a^{r-q-1} \in F$ and $a^{-1} \cdot a = 1$ if $a^{-1} = a^{r-q-1}$.

Thus in all cases a has an inverse. Hence every finite integral domain is a field.

Example

Let Z be the set of all integers. Also Z is an integral domain. If p is a prime number then Z_p ,

$Z_p = \{0, 1, \dots, p - 1\}$ is an integral domain. Since Z_p is finite integral domain then it is field.

3.3 Finite Characteristic

Let D be an integral domain and is said to have finite characteristic if there exist an integer n ($n > 0$) such that $0 = 1 + 1 + \dots + 1$ (n terms) or equivalently that $n1 = 0$.

Lemma 3.3.1

Let D be an integral domain with an identity 1 . Let D have finite characteristic and suppose that $n1 = 0$ ($n > 0$). Then for all elements a of D , $na = 0$.

Proof

$$\begin{aligned}
 na &= a + a + \cdots + a \text{ (} n \text{ terms)} \\
 &= 1a + 1a + \cdots + 1a \\
 &= (1 + 1 + \cdots + 1)a \\
 &= (n1)a \\
 &= 0
 \end{aligned}$$

Theorem 3.3.2

Let D be an integral domain with identity 1 and of finite characteristic. Then there exists a unique prime p such that $p1 = 0$.

Proof

By assumption there exist an integer n where $n > 0$ such that $n1 = 0$. Let P be chosen to be the least positive integer such that $P1 = 0$. we claim that P is a prime. Suppose P is not a prime and let $P = p_1 p_2$ where $1 < p_1 < p_1 1 < p_2 < P$ where $p_1, p_2 \in \mathbb{N}$.

$$\text{Then } (p_1)(p_2) = (1 + 1 + \cdots + 1)(1 + 1 + \cdots + 1)$$

where we have p_1 terms in the first bracket and p_2 terms in the second bracket.

Expanding by distributive and collecting terms we have $p_1 p_2$ term of the form $11=1$.

Thus $(p_1 1)(p_2 1) = (p_1 p_2) 1 = P 1 = 0$.

But D is an integral domain and so $p_1 1 = 0$ or $p_2 1 = 0$. But conclusion contradicts the choice of P as least integer such that $P 1 = 0$. Hence P is a prime and is unique.

Theorem 3.3.3

Let D be an integral domain of prime characteristic p and let $a, b \in D$.

Then $(a + b)^p = a^p + b^p$

Proof

Let p be a prime number. By using binomial theorem to expand

$$(a + b)^p = a^p + p a^{p-1} b + \frac{p(p-1)}{1 \cdot 2} a^{p-2} b^2 + \dots + b^p$$

Now the middle term which is $\frac{p(p-1)\dots(p-r+1)}{1 \cdot 2 \dots r} a^{p-r} b^r$ where $1 \leq r \leq p - 1$ is strictly positive

integer and so $1 \cdot 2 \dots r$ must divide $p(p-1) \dots (p-r+1)$. But p is a prime and $p > r$ so none

of $1, 2, \dots, r$ can divide p but each must divide the product $(p-1)(p-2) \dots (p-r+1)$. In

consequence $\frac{p(p-1)\dots(p-r+1)}{1 \cdot 2 \dots r}$ is an integer. Thus p divides $\frac{p(p-1)\dots(p-r+1)}{1 \cdot 2 \dots r}$

Hence $\frac{p(p-1)\dots(p-r+1)}{1 \cdot 2 \dots r} a^{p-r} b^r = 0$

Thus, finally, $(a + b)^p = a^p + b^p$

3.4 Vector Space

A vector space V over a field F is an Abelian group under the operation $+$ such that every

$\alpha \in F$ and every $v \in V$ there is an element $\alpha v \in V$, and such that :

1. $\alpha(v_1 + v_2) = \alpha v_1 + \alpha v_2$, for $\alpha \in F$ and $v_1, v_2 \in V$
2. $(\alpha + \beta)v = \alpha v + \beta v$, for $\alpha, \beta \in F$ and $v \in V$
3. $\alpha(\beta v) = (\alpha\beta)v$, for $\alpha, \beta \in F$ and $v \in V$
4. $1v = v$, for all $v \in V$, where 1 is a the unit element of F .

3.5 Extension of a Field

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

K is a finite dimensional vector space over F then K is called a finite extension of F . Let $[K:F]$

denote the degree of extension of K over F .

Example 1: The field R of all real numbers is an extension of the field Q of all rational numbers.

Example 2: C is a 2-dimensional vector space over R . Hence C is an extension of degree 2 over R .

Theorem 3.5

Let F, K, L be fields. If K is a finite extension of F , the degree $[K:F] = m$ and L is a finite extension of K with degree $[L:K] = n$ then L is a finite extension of F and $[L:F] = mn$. Thus

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

Proof

K is an m -dimensional vector space over F and so choose a basis $\{a_1, \dots, a_m\}$ for K over F .

Also L is an n -dimensional vector space over K and so choose a basis $\{b_1, \dots, b_n\}$ for L over K .

Suppose $\lambda_{jk}, j = 1, \dots, m, k = 1, \dots, n$ are elements of F such that

$$\sum_{j=1}^m \sum_{k=1}^n \lambda_{jk} a_j b_k = 0$$

$$\text{then } \sum_{k=1}^n \left\{ \sum_{j=1}^m \lambda_{jk} a_j \right\} b_k = 0$$

$$\text{it follows that } \sum_{j=1}^m \lambda_{jk} a_j = 0 \quad \forall k \in \{1, \dots, n\}$$

$$\Rightarrow \lambda_{jk} = 0 \quad \forall j \in \{1, \dots, m\} \text{ and } \forall k \in \{1, \dots, n\}$$

since a_1, \dots, a_m are linearly independent over F .

This proves the set $\{a_j b_k \mid 1 \leq j \leq m, 1 \leq k \leq n\}$ is linearly independent over F .

Finally, suppose $z \in L$. Choose $\gamma_1, \dots, \gamma_n \in K$ such that $z = \sum_{k=1}^n \gamma_k b_k$.

Then for each $k \in \{1, \dots, n\}, \gamma_k = \sum_{j=1}^m \eta_{jk} a_j$ where $\eta_{jk} \in F \forall j \in \{1, \dots, m\}$ and $\forall k \in \{1, \dots, n\}$.

Hence $z = \sum_{k=1}^n \sum_{j=1}^m \eta_{jk} a_j b_k$ and so $\{a_j b_k \mid 1 \leq j \leq m, 1 \leq k \leq n\}$ spans L over F .

That prove that mn elements $\{a_j b_k \mid 1 \leq j \leq m, 1 \leq k \leq n\}$ form a basis of L over F .

$$\text{Hence } [L:F] = [L:K][K:F]$$

3.6 Primitive Polynomial

A polynomial $f(x) = a_0 + a_1x + \dots + a_r x^r \in Z[X]$ where a_0, a_1, \dots, a_r are integers, is said to be *primitive* if 1 is the positive integer which is a highest common factor of a_0, a_1, \dots, a_r .

Examples: $5 + 18x - 2x^2 + 30x^3$ and $x^5 - 6x + 1$

Monic Polynomial

A polynomial $a_0 + a_1x + \dots + a_n x^n$ over a ring R is called monic if $a_n = 1$.

Theorem 3.6

If $f, g \in Z[X]$ and both of f and g are primitive, then the product fg is primitive.

Proof

let $f = a_0x^0 + a_1x^1 + \dots + a_mx^m$ and

$g = b_0x^0 + b_1x^1 + \dots + b_nx^n$ where 1 the highest common factor of is a_0, a_1, \dots, a_m and 1 is the highest common factor of b_0, b_1, \dots, b_n .

Then $fg = \sum_{k=0}^{m+n} C_k x^k$ where $C_k = \sum_{i+j=k} a_i b_j$ i.e. $C_0 = a_0 b_0, C_1 = a_0 b_1 + a_1 b_0$

Assume that fg is not primitive. Choose an integer $t \geq 2$ such that t divides every one of

C_0, C_1, \dots, C_{m+n}

Next choose a prime number p such that p divides t , and then p divides every one of $C_0,$

C_1, \dots, C_{m+n} . Assume that p does not divide b_0 then p divides a_0 . Since p divides C_1 and p

divides $a_0 b_1$, it follows that p divides $a_1 b_0$. That implies p divides a_1 , since p does not divide

b_0 . Continuing the process, we find that p divides each of a_0, a_1, \dots, a_m .

This contradicts the fact that f is primitive. The assumption is false.

Hence fg is primitive.

Lemma

Let $f(x)$ and $g(x)$ be primitive polynomial in $Z[x]$. Suppose there exist

$c_1, c_2 \in Z, c_1 \neq 0$ and $c_2 \neq 0$ such that $c_1f(x) = c_2g(x)$. Then $c_1 = \pm c_2$ and $f(x) = \pm g(x)$

Proof

Let $f(x) = a_0 + a_1x + \dots + a_nx^n$ ($a_n \neq 0$). Then the highest common factor of

a_0, a_1, \dots, a_n is 1 and so there exist $t_0, t_1, \dots, t_n \in Z$ such that

$$t_0a_0 + t_1a_1 + \dots + t_na_n = 1$$

since $c_1f(x) = c_2g(x)$, c_2 divides $c_1a_0, c_1a_1, \dots, c_1a_n$ and so

c_2 divides

$$\begin{aligned} & t_0c_1a_0 + t_1c_1a_1 + \dots + t_nc_1a_n \\ &= c_1(t_0a_0 + t_1a_1 + \dots + t_na_n) = c_1. \end{aligned}$$

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

3.6.1 Gauss Lemma

If $f \in Z[X]$ and f has a factorization $f = gh$ where $g, h \in Q[X]$ $\deg g \geq 1$ and $\deg h \geq 1$.

Then f has a factorization $f = gh$ where $g, h \in Z[X]$, $\deg g \geq 1$ and $\deg h \geq 1$.

Proof

Let f be a primitive polynomial in $Z[X]$. Let $f = gh$ where $g, h \in Q[X]$. Choose integers m, n such that mg is primitive and nh is primitive, then mnh is primitive. Hence mnf is primitive. That implies mn is an invertible integer that is $mn = \pm 1$. Therefore $g \in Z[X]$ and $h \in Z[X]$

Theorem 3.6.1

Let $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} + x^n \in Z[x]$ be a monic polynomial. If $f(x)$ has a root $a \in Q$, then $a \in Z$ and $a \mid a_0$.

Proof

Let $a = \alpha/\beta$, where $\alpha, \beta \in Z$ and $(\alpha, \beta) = 1$. Then

$$a_0 + a_1 \frac{\alpha}{\beta} + \dots + a_{n-1} \left(\frac{\alpha^{n-1}}{\beta^{n-1}} \right) + \frac{\alpha^n}{\beta^n} = 0$$

Multiply the above equation by β^{n-1} to obtain

$$a_0\beta^{n-1} + a_1\alpha\beta^{n-2} + \dots + a_{n-1}\alpha^{n-1} = -\frac{\alpha^n}{\beta}$$

Because $\alpha, \beta \in Z$, it follows that $\alpha^n/\beta \in Z$, so β must be ± 1 . The last equation also shows α/a_0 . Hence, $a = \pm\alpha \in Z$ and $a \mid a_0$.

3.6.2 Eisenstein's Irreducibility Criterion

Let $f = a_0 + a_1x + \dots + a_nx^n \in Z[X]$ where $n \geq 1$. Suppose there exist a prime number p such that:

1. p divides a_0, a_1, \dots, a_{n-1}
2. p does not divide a_n and
3. p^2 does not divide a_0 ,

Then f is irreducible over Q .

Proof

Assume that f is not irreducible over Q . Let $f = gh$ and $g, h \in Q[X]$, then f has a factorization $f = gh$ where $g, h \in Z[X]$, $\deg g \geq 1$ and $\deg h \geq 1$ by Gauss' Lemma.

Let $g = C_0x^0 + C_1x^1 + \dots + C_r x^r$ and $h = d_0x^0 + d_1x^1 + \dots + d_q x^q$ in $Z[X]$. Then $a_0 = C_0d_0$ and so either p divides C_0 and p does not divide d_0 or p divides d_0 and p does not divide C_0 . We say without loss of generality consider the case where p divides C_0 and p does not divide d_0 .

Then from $a_1 = C_0d_1 + C_1d_0$ we conclude that p divides C_1d_0 and since p does not divide d_0 then p divides C_1 . Continuing the process we find that p divides each of C_0, C_1, \dots, C_r . This leads to a contradiction p divide each of a_0, a_1, \dots, a_n and p does not divide $a_n = C_r d_q$. The assumption is false. Hence f is irreducible over Q .

Example

1. Let $f(x) = x^5 - 4x + 22$, Since $2/22, 2^2 \nmid 22$ and 2 divides the other relevant coefficients of $f(x)$. Thus by Eisenstein Criterion, $f(x)$ is irreducible in $Q[x]$.
2. Let $f(x) = x^{11} - 6x^4 + 12x^3 + 30$, since $3/30, 3^2 \nmid 30$ and 3 divides the other relevant coefficients of $f(x)$. Thus by Eisenstein Criterion, $f(x)$ is irreducible in $Q[x]$.

KNUST

3.6.3 Cyclotomic Polynomial

The polynomial $\varphi_n(x)$ are defined inductively by:

(a) $\varphi_1(x) = x - 1$

(b) If $n > 1$, then $\varphi_n(x) = \frac{(x^n - 1)}{\prod \varphi_d(x)}$,

where in the product in the denominator d runs over all the divisors of n except for n itself.

These polynomials are called the *Cyclotomic Polynomials* and $\varphi_n(x)$ is called the *n th Cyclotomic Polynomial*.

Example

1. $\varphi_2(x) = \frac{(x^2 - 1)}{\varphi_1} = \frac{(x^2 - 1)}{(x - 1)} = x + 1$

2. $\varphi_4(x) = \frac{(x^4 - 1)}{(\varphi_1(x)\varphi_2(x))}$

$$= \frac{(x^4 - 1)}{((x - 1)(x + 1))}$$

$$= \frac{(x^4 - 1)}{(x^2 - 1)} = (x^2 + 1)$$

3.6.4 The p th Cyclotomic Polynomial

If p is a prime number then the polynomial $1 + x + \dots + x^{p-1}$ is called the p th Cyclotomic Polynomial. It is irreducible over Q .

Proof

Consider,
$$(1 + x + \dots + x^{p-1})(x - 1) = x^p - 1$$

$$1 + x + \dots + x^{p-1} = \frac{x^p - 1}{x - 1}$$

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

$$\text{then } 1 + x + \dots + x^{p-1} = \frac{(y+1)^{p-1}}{y}$$

$$= y^{p-1} + py^{p-2} + \dots + p$$

if $p > 2$, $y^{p-1} + py^{p-2} + \dots + p$ is irreducible over Q by Eisenstein's irreducible criterion.

Hence, $1 + x + \dots + x^{p-1}$ is irreducible over Q .

3.7 Splitting Field

Let F be a field and $f \in F[x]$ a polynomial such that $\deg f = m \geq 1$. A field K is called a splitting field of f over F if K is a finite extension of F , f has m roots $\alpha_1, \alpha_2, \dots, \alpha_m \in K$ and the degree of extension $[K:F]$ is the smallest possible.

3.8 Finite Field

A field F is finite if there exist a positive integer q such that F contains exactly q distinct elements a_1, a_2, \dots, a_q . The commonest examples of finite fields are $Z_p = \{0, 1, \dots, p-1\}$ where p is a prime number.

KNUST

Theorem 3.8.1

Let F be a finite field with q elements and suppose that $F \subset K$ where K is also a finite field.

Then K has q^m elements where $m = [K:F]$.

Proof

K is a vector space over F and since K is finite it is certainly finite dimensional as a vector space over F . Suppose that $[K:F] = m$; then K has a basis of m elements over F . Let such a basis be

v_1, v_2, \dots, v_m . Then every element in K has a unique representation in the form

$\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m$ where $\alpha_1, \alpha_2, \dots, \alpha_m$ are all in F . Thus the number of elements in K

is the number of $\alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_m v_m$ as the $\alpha_1, \alpha_2, \dots, \alpha_m$ range over F . Since each

coefficient can have q values K must clearly have q^m elements.

Corollary 1

Let F be a finite field, then F has p^m elements where the prime number p is the characteristic of F .

Proof

Since F has a finite number of elements, then $f1 = 0$ where f is the number of elements in F .

Thus F has characteristics p for some prime number p .

Therefore F contains a field F_0 isomorphic to Z_p (ring of integers with modulo prime p). Since F_0 has elements p , F has p^m elements where $m = [F:F_0]$ by theorem 3.7.1. Hence let F be a finite field, then F has p^m elements where the prime number p is the characteristic of F .

Corollary 2

If the finite field F has p^m elements then every $a \in F$ satisfies $a^{p^m} = a$.

Proof

If $a = 0$ the assertion of the corollary is trivially true. On the other hand, the nonzero elements of F form a group under multiplication of order $p^m - 1$ thus this corollary $a^{p^m-1} = 1$ for $a \neq 0$ in F . Multiplying this relation by a we obtain $a^{p^m} = a$.

LIBRARY
SWAMI VIDYAMAN UNIVERSITY OF
SCIENCE AND TECHNOLOGY
MUMBAI-CHANA

Corollary 3

If the field F has p^m elements then F is the splitting field of the polynomial $x^{p^m} - x$.

Proof

By lemma 3.3.1, $x^{p^m} - x$ certainly splits in F . However, it cannot split in any smaller field for that field would have to have all the roots of this polynomial and so would have to have at least p^m elements. Thus F is the splitting field of $x^{p^m} - x$.

KNUST

Lemma 3.8.1

If the finite field F has p^m elements then the polynomial $x^{p^m} - x$ in $F[x]$ factors in $F[x]$ as

$$x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda).$$

Proof

The polynomial $x^{p^m} - x$ has at most p^m roots in F . However, by corollary 2 we know p^m such roots, namely all the elements of F . Therefore, we conclude that $x^{p^m} - x = \prod_{\lambda \in F} (x - \lambda)$.

Theorem 3.8.2

For every prime number p and every positive integer m there exist a field having p^m elements.

Proof

Consider the polynomial $x^{p^m} - x$ in $Z_p[x]$, the ring of polynomials in x over Z_p , the field of integers mod p . Let K be the splitting field of this polynomial.

In K let $F = \{a \in K \mid a^{p^m} = a\}$. The elements of F are thus the roots of $x^{p^m} - x$, which by corollary 2 are distinct whence F has p^m elements. We now claim that F is a field.

If $a, b \in F$ then $a^{p^m} = a$, $b^{p^m} = b$

and so $(ab)^{p^m} = a^{p^m} b^{p^m} = ab$; thus $ab \in F$.

Also since the characteristic is p , $(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m} = a \pm b$, hence $a \pm b \in F$.

Consequently F is a subfield of K and so is a field.

KNUST



CHAPTER 4

EXERPTS ON THE USE OF PRIME NUMBERS IN GROUP THEORY

4.1 GROUP

A nonempty set G is said to be a group, if there is a defined binary operation $(*)$ and it must satisfies the condition of a group or group axioms.

4.1.1 Axioms of a group

Axiom 1

The binary operation $(*)$ is closed, if $a, b \in G$ 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 is an existence of an identity element 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

$$a * a^{-1} = a^{-1} * a = e$$

4.1.2 Commutative Group

A group G is called a commutative or Abelian group if for every $a, b \in G$ then $a * b = b * a$.

4.1.3 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.

$$H_1: a, b \in H \Rightarrow a * b \in H$$

$$H_2: a \in H \Rightarrow a^{-1} \in H$$

4.1.4 Normal Subgroup

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

Example

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

Proof

If $a \in A$ and $h \in H$

$$\text{then } a^{-1} h a = h a^{-1} a = h I = h \in H$$

Therefore H is a normal subgroup of A .

Theorem 4.1.4

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 $ah = \eta a \in Ha \therefore aH \subset Ha \therefore Ha = aH \quad \forall a \in G$

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

$$hg \in Hg = gH \quad \Rightarrow hg = gf \quad \text{where } f \in H$$

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.

4.1.5 Center of a Group

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

Then $C(G)$ is called the centre of a group G .

Theorem 4.1.5

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

Proof

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

If $a \in C(G)$ then $ag = ga, \forall g \in G$

$\Rightarrow aga^{-1} = g \quad \forall g \in G \therefore a^{-1} \in C(G)$ if $a \in C(G)$

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

if $a \in C(G)$ and $b \in C(G)$

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

Finally for every $g \in G$ and every $h \in C(G)$ $g^{-1}hg = g^{-1}gh = Ih = h \in C(G)$

$\therefore C(G)$ is a normal subgroup of G .

4.1.6 Cyclic Group

If G is a group and there exists an element $a \in G$ such that G is the same as the subgroup of G generated by $\langle a \rangle$ 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, \dots, a^{n-1}, I where $a^n = I$, the identity. Such a group C_n is called a cyclic group of order n . For example, where $n=2$, then $C_2 = \{-1, 1\}$ then C_2 is a cyclic group of order 2.

4.1.7 Homomorphism

Let G and B be group under binary operation o and $*$ respectively. A mapping $h : G \rightarrow B$ is called a homomorphism if $h(a o b) = h(a) * h(b)$ for every pair $a, b \in G$.

4.1.8 Isomorphism

If $h : G \rightarrow B$ 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.

If $h : G \rightarrow B$ for every $g_1, g_2 \in G$ such that

$h(g_1) = h(g_2) \Rightarrow g_1 = g_2$ then h is **injective** and h is said to be a *monomorphism*.

Also if $h : G \rightarrow B$ for every $b \in B$ there exist $g \in G$ such that $h(g) = b$ then, h is **surjective** and h is said to be an *epimorphism*.

4.2 Automorphisms of a Group

Let G be a group. If $h : G \rightarrow G$ is an isomorphism then h is called an automorphism of G .

Characteristic subgroup of G : a subgroup H of G is said to be a characteristic subgroup of G if

$(H)^T \subset H$ for all automorphisms T of G .

4.2.1 Kernel of a Group

Given groups G and B with identities 1 and e respectively and homomorphism $h : G \rightarrow B$. Let

$\ker h = \{x \in G \mid h(x) = e\}$ then $\ker h$ is called the kernel of h .

4.2.2 Left Cosets and Right Cosets of a Subgroup

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

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

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

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

4.3 Finite Group

A group whose underlying set G has finitely many elements is known as finite group. The order of a group is the number of elements in the group.

For example, the number of elements in G is called the order of G and is denoted by $|G|$. A group having finite group order is also called a finite group.

4.3.1 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, \dots, g_k in G such that $G = \bigcup_j^k H_{g_j}$ and $H_r \cap H_j = \emptyset$ where

$$\text{every } r \neq j \text{ then } n = v_1 + \dots + v_k = qk \quad \text{for each } j \in \{1, \dots, k\}$$

where V_j is the number of elements in H_{g_j}

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

NOTE: The integer $k = \frac{n}{q}$ is called the index of H in G . We write $[G; H]$ as the index.

4.3.2 Normaliser and Centraliser

Definitions:

- i. Let H be a subset of G . The subset $g^{-1}Hg = \{g^{-1}hg: h \in H\}$ is called the *conjugate* of H by g in G . We denote $g^{-1}Hg$ by H^g .
- ii. If H, K are subsets of G we say that K is conjugate to H in G if there exist in G an element g such that $H^g = K$. It follows that $K^{g^{-1}} = H$.
i.e. $g^{-1}Kg = g^{-1}\{g^{-1}Hg\}g = g^{-1}gHgg^{-1} = H$. Hence we conclude that H and K are conjugate in G .
- iii. If $H^g = K$ where H and K have exactly one element say $H = \{x\}, K = \{y\}$. Then for $g \in G, x^g = y$ which implies y is conjugate to x in G . By the preceding definition, we deduce that x is a conjugate to y in G . Therefore x and y are conjugate in G .
- iv. The subset $N_G(H) = \{g: g \in G \text{ and } H^g = H\}$ is called the *normaliser* of H in G .
- v. If H contains exactly one element x , we have
 $N_G(\{x\}) = \{g: g \in G \text{ and } g^{-1}xg = x\} = \{g: g \in G \text{ and } xg = gx\}$. Then $N_G(\{x\})$ is called the *centraliser* of x in G . Let us denote the centraliser of $x \in G$ by
 $C_G(x) = \{x \in G | xg = gx\}$.
- vi. Conjugacy determines an equivalence relation on the set of all subsets of G and also on the set of all subgroups of G . In each equivalence relation there corresponds an equivalence class. These equivalence classes are called *conjugacy classes*.

Class Equation

Let G be a group. Suppose $a \in G$ and let $C_G(a)$ be the centralizer of a in G , $Z_a(G)$ the conjugate class of a in G , K_a the set of all right coset of in G . Then there exists a bijective mapping

$$\psi_a: Z_a(G) \rightarrow K_a$$

defined by

$$\psi_a(g^{-1}ag) = C_G(a)g$$

Corrollary: If G is a finite group, then the number of elements in $Z_a(G)$ is the index $[G; C_G(a)]$

Definition of Class Equation

If G is a finite group of order n , then there exist elements a_1, \dots, a_r in G such that

$$n = \sum_{j=1}^r [G; C_G(g_j)]$$

This equation is termed as Class equation.

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

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 invisible by p and whose 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 $\psi: G \rightarrow G/H$ be the projection of G onto.

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, let k be the order of the centre $C(G)$ and the order of G be $p\lambda$ where λ is a positive integer. Then we can choose elements $a_1 \dots a_r \in G - C(G)$ such that the class equation of G is $p\lambda = k + \sum_{j=1}^r [G; Z_{a_j}(G)]$

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

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

Then the theorem is proved in all cases.

4.4 p -Group

Let p be a prime. p -group is a periodic group which its elements has a power p as its order. In this each element has a prime power order. A p -group is also defined as a group in which every element has finite order and these orders are powers of p . A finite group can also be defined as p -group if the order is a of a prime p .

In fact, every finite group has subgroup which is a p -group by the Sylow theorems in which they are called sylow p -subgroup. p -group can arise as subgroup and as subgroup for a given prime p one has the sylow p -subgroup.

Theorem

A finite group G is a p -group if and only if the order of G , $|G|$, is a power of p .

Proof

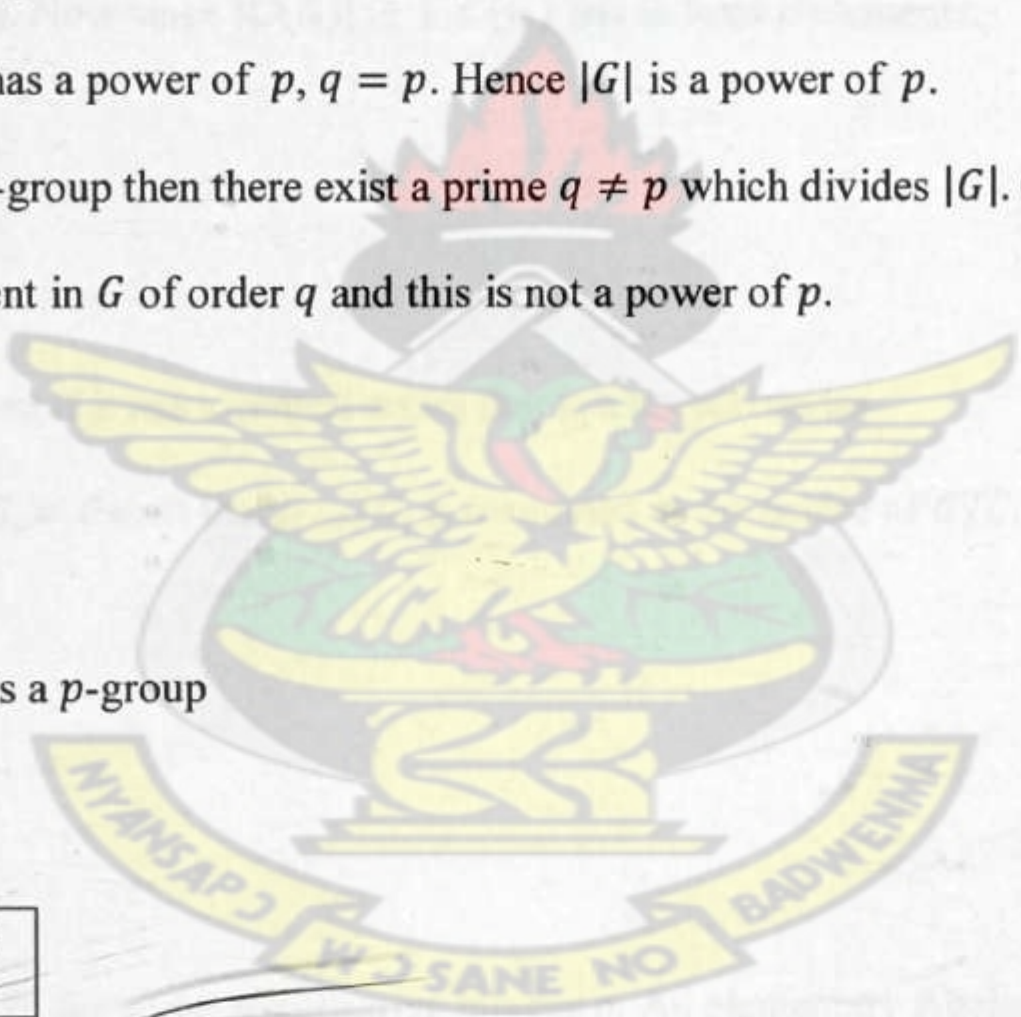
If G is a p -group and q is a prime which divides $|G|$, then G contains an element of order q .

Since every element of G has a power of p , $q = p$. Hence $|G|$ is a power of p .

Conversely, if G is not a p -group then there exist a prime $q \neq p$ which divides $|G|$. Cauchy's theorem provides an element in G of order q and this is not a power of p .

Example

Cyclic group of order 4 is a p -group



GROUP	ORDER
I	$2^0 = 1$
U	$2^2 = 4$
U^2	$2^1 = 2$
U^3	$2^2 = 4$

Corollary

The center $C(G)$ of a nontrivial finite p -group G contains more than one element.

Proof

Consider the class equation of G

$$|G| = |C(G)| + \sum [G; C_G(x_i)]$$

since each $[G; C_G(x_i)] > 1$ and divides $|G| = p^n$ ($n \geq 1$), p divides each $[G; C_G(x_i)]$ and $|G|$.

Therefore p divides $|C(G)|$. Now since $|C(G)| \geq 1$, $C(G)$ has at least p elements.

4.4.1 Nilpotent

A group G is called nilpotent if it has a central series that is a normal series

$1 = G_0 \subset G_1 \subset G_2 \subset \dots \subset G_n = G$ such that G_{i+1}/G_i is contained in the centre of G/G_i for all $i \in \{0, 1, \dots, n\}$.

4.5 Finite p -group

A finite p -group has order p^n for some nonnegative integer n . An elementary Abelian group p -group is a finite abelian p -group in which the p -th power of every element is 1. Such a group is a direct product of cyclic group of order p and it may be considered to be a vector space over field \mathbb{Z}_p of integers modulo p . Equivalently, let G be a group such that every element of G has a p -power order for some fixed prime p , then G is called a p -group. By Lagrange's theorem any finite group of order p^n where $n \in \mathbb{N}$ is a finite p -group.

Properties about finite p -group are

Let F be a nontrivial finite p -group

a) The center of F is nontrivial

b) Every proper subgroup of F is contained in a subgroup of index p and all subgroup of index p are normal.

c) F is nilpotent.

Proof of F is nilpotent

Let F be a finite p -group of order > 1 . Then by (a) the center of F is nontrivial shows that

$\tau F \neq 1$. Hence $F/\tau F$ is nilpotent by induction on $|F|$. By forming the preimages of the terms of a central series of $F/\tau F$ under the natural homomorphism $F \rightarrow F/\tau F$ and adjoining 1, we arrive at a central series of F .

Lemma 4.5.1

Let A be a finite Abelian group. Let p be a prime such that every element of A has an order which is a power of p . Then A is a p -group.

Proof

Let A be a finite Abelian group as given. Assume the result is true for all groups of order strictly less than $|A|$. Suppose A is not cyclic and let $a \in A$, $a \neq 0$. Then the subgroup $\langle a \rangle$ generated by a has an order which is a power of p . Further $A/\langle a \rangle$ has the property that every element has an order which is a power of p since if $x \in A$ and x has order p^a then

$$\begin{aligned}
 p^a(x + \langle a \rangle) &= p^a x + \langle a \rangle \\
 &= 0 + \langle a \rangle \\
 &= \langle a \rangle
 \end{aligned}$$

and so $x + \langle a \rangle$ has order dividing p^a . By the induction assumption $A/\langle a \rangle$ is a p -group and so, as $|A| = |\langle a \rangle| = |\langle a \rangle| |A/\langle a \rangle|$, A is a p -group

4.6 Frattini subgroup

Let H be a group, the intersection of all maximal subgroup of H is defined as the Frattini subgroup of a group of H . the Frattini subgroup of H is denoted by $\Phi(H)$.

Critical subgroup: A critical subgroup of G is a characteristic subgroup H of G such that $\Phi(H) \subset C(H)$, $[G, H] \subset C(H)$ and $C_G(H) = C(H)$.

Theorem 4.6.1

Each p -group possess a critical subgroup.

Proof

let S be the set of characteristic subgroup H of G with $\Phi(H) \subset C(H)$ and $[G, H] \subset C(H)$.

Let H be a maximal member of S .

Claim H is a critical subgroup of G . Assume not and let $K = C_G(H)$, $C = C(H)$ and X

by $C = \alpha_1(C(G/C)) \cap K/C$. Then $K \not\subset H$ and $C = H \cap K$, so, as K normal subgroup of G ,

$X \neq Z$.

Hence $XH \in S$, contradicting the maximality of H . Therefore p -group possess a critical subgroup.

A p -group is *special* if $\Phi(G) = C(G) = G^{(1)}$. A *special* p -group is said to be *extraspecial* if its center is *cyclic*.

Theorem 4.6.2

The center of a special p -group is elementary Abelian.

Proof

Let G be special and $g, h \in G$. Then $g^p \in \Phi(G) = C(G)$, so $1 = [g^p, h] = [g, h]^p$.

Hence $G^{(1)}$ is elementary.

4.7 p -subgroup

If H is a subgroup of a finite group G and H is a p -group. H is said to be a p -subgroup of G . In particular $\langle e \rangle$ is a p -subgroup of G for every prime p , since $|\langle e \rangle| = 1 = p^0$.

Lemma 4.7.1

If H is a p -subgroup of a finite group G , then $[N_G(H); H] \equiv [G; H] \pmod{p}$.

Proof

let S be the set of the left cosets of H in G and let H act on S by left translation.

Then $|S| = [G; H]$, also

$$xH \in S_0 \Leftrightarrow hxH = xH \text{ for all } h \in H$$

$$\Leftrightarrow x^{-1}hxH = H \text{ for all } h \in H \Leftrightarrow x^{-1}hx \in H \text{ for all } h \in H$$

$$\Leftrightarrow x^{-1}Hx = H \Leftrightarrow xHx^{-1} = H \Leftrightarrow x \in N_G(H).$$

Therefore $|S_0|$ is the number of cosets xH with $x \in N_G(H)$; that is,

$$|S_0| = [N_G(H); H] \equiv |S| = [G; H] \pmod{p}$$

Remarks: If a group H of order p^n (where p is prime) is on a finite set S and if $S_0 = \{x \in S | hx = x \text{ for all } h \in H\}$ then $|S| \equiv |S_0| \pmod{p}$.

Corollary 4.7.2

If H is p -subgroup of a finite group G such that p divides $[G; H]$, then $N_G(H) \neq H$

Proof

$0 \equiv [G; H] \equiv [N_G(H); H] \pmod{p}$. Since $[N_G(H); H] \geq 1$ in any case, we must have $[N_G(H); H] > 1$. Therefore $N_G(H) \neq H$

Lemma 4.7.3

Let G be a group and let P and Q be p -subgroups. Suppose that Q normalizes P .

Then PQ is also a p -subgroup.

Proof

Since Q normalizes P , then PQ is a subgroup. Now $|PQ| = \frac{|P||Q|}{|P \cap Q|}$ and so PQ is p -group.

Theorem 4.7.4

A group of order p^n for any positive integer n and every prime index has non-trivial centre.

Proof

Let C_1, C_2, \dots, C_r be the equivalence classes of conjugate elements of G where C_1 is the class containing just the identity elements of G . Let C_2, \dots, C_t ($t \leq r$) denote the remaining equivalence classes, if any, which contains just one element. Then $\bigcup_{1 \leq i \leq t} C_i = C(G)$ the centre of G , and C_i are pairwise disjoint. That implies $|G| = |C(G)| + \sum_{j=1}^k [G:C(a_j)]$ (this is called the class equation of G).

But each of the $[G:C(a_j)]$ divides $|G|$ by Lagrange, and hence is a power of p .

Now $p \nmid |G|$ and $p \nmid [G:C(a_j)]$ for $l = t + 1, \dots, r$. Thus $p \nmid \sum_{j=1}^k [G:C(a_j)] = t$. It follows that $t > 1$ and hence that G has non-trivial centre.

Example

Let G be a group of order p^2 where p is a prime. Then we may prove that G is Abelian as follows. Certainly we now know that the centre $C(G)$ of G is non-trivial and so must be of order p or p^2 . But if $C(G)$ is of order p then $G/C(G)$ is also of order p and so is cyclic.

Theorem 4.7.5

If p is a prime then all groups of order p^2 are Abelian.

Proof

Let $|G| = p^2$ and $C = \tau G$. Then the $|C| = p$ or p^2 and $|G:C| = p$ or 1 . Hence G/C is cyclic generated by xC . Then $G = \langle x, C \rangle$ which implies that G is Abelian.

Proposition

Let p and q be primes such that $p > q$. If $q \nmid p - 1$, then every group of order pq is isomorphic to the cyclic group Z_{pq} . If $q \mid p - 1$, then there are exactly two distinct groups of order pq : the cyclic group Z_{pq} and a non Abelian group k generated by elements c and d such that $|c| = p$, $|d| = q$ and $dc = c^s d$ where $s \not\equiv 1 \pmod{p}$ $s^q \equiv 1 \pmod{p}$.

Theorem 4.7.6

If p is a prime number such that $p > 2$, then every finite group of order $2p$ is isomorphic either to the cyclic group Z_{2p} or the dihedral group D_p .

Proof

Apply above proposition with $q = 2$. Let G be a finite group. If G is not cyclic, then conditions on s imply

$s = -1 \pmod{p}$. Hence $G = \langle c, d \rangle$, $|d| = 2$, $|c| = p$ and $dc = c^{-1}d$. Therefore $G \cong D_p$

4.8 Sylow's Theorem

There are some results that serve as a partial converse to the theorem of Lagrange results which establish the existence of subgroup corresponding to certain divisors of the order of the group.

These results are collected in what is known as Sylow's theorem.

4.8.1 Sylow's First Theorem

Let G be a group of order $p^n m$ with $n \geq 1$, p prime and $(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i ($i < n$) is normal in some subgroup of order p^{i+1}

Proof

Since $p \mid |G|$, G contains an element a , and therefore, a subgroup $\langle a \rangle$ of order p by Cauchy's theorem. By induction, assume H is a subgroup of G of order p^i ($1 \leq i \leq n$). Then $p \mid [G; H]$ and by lemma 4.7.1 and corollary 4.7.2, H is normal in $N_G(H)$, $H \neq N_G(H)$ and $1 < |N_G(H)/H| = [N_G(H); H] \equiv [G; H] \equiv 0$.

Hence $p \mid |N_G(H)/H|$ and $N_G(H)/H$ contains a subgroup of order p as above. This group is of the form H_1/H where H_1 is a subgroup of $N_G(H)$ containing H . Since H is normal in $N_G(H)$, it is necessarily normal in H_1 .

Finally $|H_1| = |H||H_1/H| = p^i p = p^{i+1}$

4.8.2 Sylow p -Subgroup

A Sylow p -subgroup of G is a subgroup of G which has its order been the highest power of p dividing $[G; 1]$. For example, A can be a Sylow p -subgroup of G if it is a p -group and its index in G is prime p . In other words, if p^k is the highest power of a prime p dividing the order of a finite group G , then a subgroup of G of order p^k is called a Sylow p -subgroup of G .

Also a subgroup H of a group G is said to be a Sylow p -subgroup (p is prime) if H is a maximal p -subgroup of G . That is $H \subset S \subset G$ with S a p -group implies $H = S$.

Example

A group G of order $8897850 = 2 \cdot 3^4 \cdot 5^2 \cdot 13^3$ has Sylow subgroups corresponding to primes 2, 3, 5 and 13. These Sylow subgroups have orders 2, 81, 25 and 2197 respectively.

Lemma 4.8.2

Let P be a normal Sylow p -subgroup of the finite group G . Let Q be a p -subgroup of G . Then $Q \subset P$.

Proof

Since P is normal in G , PQ is a subgroup of G . Since PQ/P is isomorphic to $Q/(P \cap Q)$ it follows that $|PQ/P| = |Q/(P \cap Q)|$ and so $|PQ/P|$ is a power of p . Thus PQ is a p -subgroup of G . But $P \subset PQ$ and P is a Sylow p -subgroup of G . Thus $P = PQ$ and hence $Q \subset P$.

Corollary 4.8.2

Let P be a Sylow p -subgroup of the finite group G . Let Q be a p -subgroup of the normalizer $N_G(P)$ of P . Then $Q \subset P$.

Proof

Let P is a normal Sylow p -subgroup of $N_G(P)$. Since $Q \subset N_G(P)$ we deduce from lemma 4.8.2 that $Q \subset P$.

KNUST

4.8.3 Sylow's Second Theorem

If H is p -subgroup of a finite group G and B is any Sylow p -subgroup of G , then there exists $x \in G$ such that $H \subset xBx^{-1}$. In particular, any two Sylow p -subgroups of G are conjugate.

Proof

Let S be the set of left cosets of B in G and let H act on S by left translation,

$|S_0| \equiv |S| = [G; B]$. But $p \nmid [G; B] \therefore |S_0| \neq 0$ and there exists $xB \in S_0$.

$xB \in S_0 \Leftrightarrow hxB = xB$ for all $h \in H$

$\Leftrightarrow x^{-1}hxB = B$ for all $h \in H \Leftrightarrow x^{-1}Hx \subset B \Leftrightarrow H \subset xBx^{-1}$.

If H is a Sylow p -subgroup then $|H| = |B|$. Hence $H = xBx^{-1}$.

Theorem

If P is a Sylow p -subgroup of a finite group G , then $N_G(N_G(P)) = N_G(P)$

Proof

Every conjugate of P is a Sylow p -subgroup of G and of any subgroup of G that contains it.

Since P is normal in $N = N_G(P)$, P is the only Sylow p -subgroup of N .

$$x \in N_G(N) \Rightarrow xNx^{-1} = N$$

$$\Rightarrow xPx^{-1} \subset N$$

$$\Rightarrow xPx^{-1} = P$$

$$\Rightarrow x \in N.$$

Hence $N_G(N_G(P)) \subset N$

Example

Let G be a finite group and let P be a sylow p -subgroup of G . Let H be a subgroup of G such that $N_G(P) \subset H$. Therefore $N_G(H) = H$.

Proof

Let $x \in G$ be such that $x^{-1}Hx = H$. Then we wish to prove that $x \in H$. Certainly

$$x^{-1}Px \subset x^{-1}N_G(P)x \subset x^{-1}Hx = H$$

Then P and $x^{-1}Px$ are both sylow p -subgroup of H . Thus we have $h \in H$ such that

$$h^{-1}Ph = x^{-1}Px$$

But then

$$P = hx^{-1}P_xh^{-1} = (xh^{-1})^{-1}P(xh^{-1})$$

and so $xh^{-1} \in N_G(P) \subset H$ from which $x \in Hh = H$. Hence $N_G(H) = H$.

4.8.4 Sylow's Third Theorem

If G is a finite group and p is a prime number which divides the $|G|$, then the number of Sylow p -subgroups of G divides $|G|$ and is of the form $kp + 1$ for some $k \geq 0$.

Proof

By the second Sylow Theorem the number of Sylow p -subgroup is the number of conjugates of any one of them, say P . But this number is $[G; N_G(P)]$, a divisor of $|G|$. Let S be the set of all Sylow p -subgroups of G and let U act on S by conjugation. Then $Q \in S_0$ if and only if

$xQx^{-1} = Q$ for all $x \in U$. The latter condition holds if and only if $U \subset N_G(Q)$. Both U and Q are Sylow p -subgroups of G and hence of $N_G(Q)$ and are therefore conjugate in $N_G(Q)$. But since Q is normal in $N_G(Q)$, this can only occur if $Q = U$. Therefore, $Q = U$ and $|S| \equiv |S_0| = 1$.

Hence $|S| = kp + 1$

Example

A group G of order 175 is necessarily Abelian. From the factorization, $175 = 5^2 \cdot 7$, the group G has sylow 5-subgroup of order 25 and sylow 7-subgroup of order 7.

Proof

Suppose there are m sylow 5-subgroup and n sylow 7-subgroup.

Then m divides $5^2 \cdot 7$ and $m = 1 + 5r$ for some $r \in \{0,1,2, \dots\}$. If $r > 0$ then m must divide 7 which is impossible. Thus $r = 0$ and $m = 1$.

Also n divides $5^2 \cdot 7$ and $n = 1 + 7s$ for some $s \in \{0,1,2, \dots\}$. If $s > 0$ then n must divide 5^2 which is impossible. Hence the slow 5-subgroup P and the sylow 7-subgroup Q are both unique.

Thus G is isomorphic to the direct product $P \times Q$ and is therefore Abelian as P and Q are Abelian.

4.9 Simple Group

A simple group is one with no proper nontrivial normal subgroups. A group G is said to be simple if and only if it has exactly two normal subgroups, namely $\{e\}$ and G .

KNUST

Theorem 4.9.1

A nontrivial group G is simple if and only if any nontrivial group homomorphism out of G is an embedding.

Proof

Suppose G is simple. Let $f: G \rightarrow H$ be a homomorphism, with $f(g) \neq e$ for some g . Then the kernel of f is a proper normal subgroup of G . Since G is simple, its only proper normal subgroup is trivial, so the kernel of f is trivial, which means f is an embedding.

Conversely, suppose all nontrivial homomorphism out of G are embeddings. If N is a normalizer G and $N \neq G$ then the reduction map $G \rightarrow G/N$ is a homomorphism with kernel N .

The image is not just the identity, so by hypothesis this is embedding. Therefore, the kernel N is trivial so G is simple.

Theorem 4.9.2

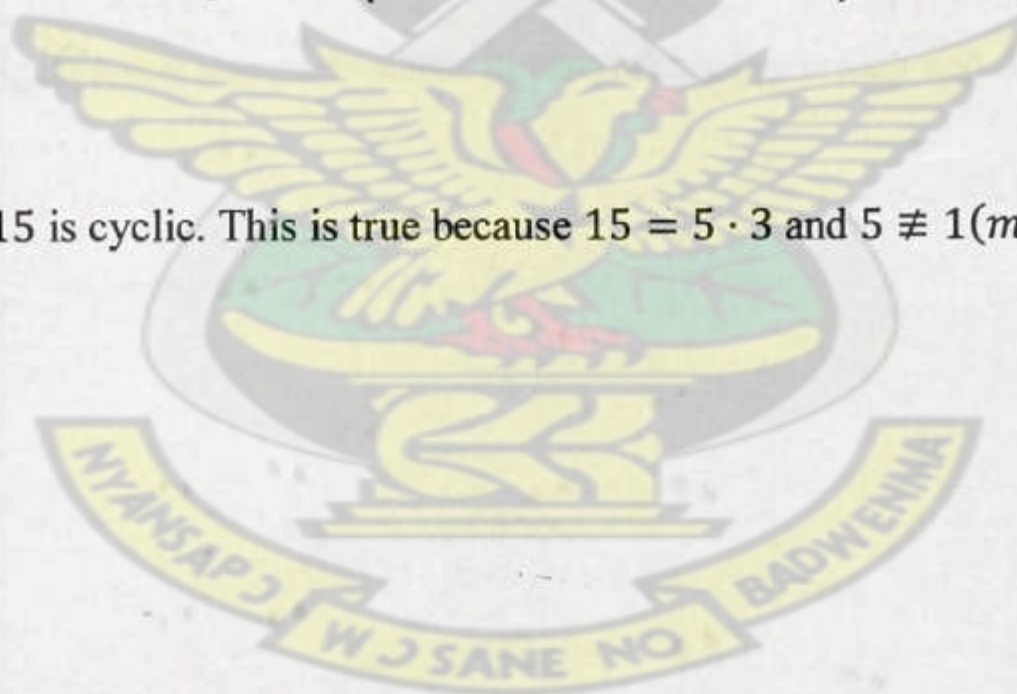
If p and q are distinct primes with $p < q$ then every group G of order pq has a single subgroup of order q and this subgroup is normal in G . Hence G cannot be simple. Furthermore, if $q \not\equiv 1 \pmod{p}$, then G is cyclic.

Proof

Given that G contains a subgroup H of order p . The number of conjugates of H divides pq and is equal to $1 + kq$ for $k = 0, 1, \dots$. However, $1 + q$ is already too large to divide the order of the group. Hence H can only be conjugates to itself. That is, H must be normal in G . The group G also has a Sylow p -subgroup, say K . The number of conjugates of K must divide q and be equal to $1 + kp$ for $k = 0, 1, \dots$ since q is prime, either $1 + kp = q$ or $1 + kp = 1$. If $1 + kp = 1$, then K is normal in G . Since H is isomorphic to Z_p and K is isomorphic to Z_q , $G \cong Z_p \times Z_q \cong Z_{pq}$.

Example

Every group of order 15 is cyclic. This is true because $15 = 5 \cdot 3$ and $5 \not\equiv 1 \pmod{3}$



CHAPTER 5

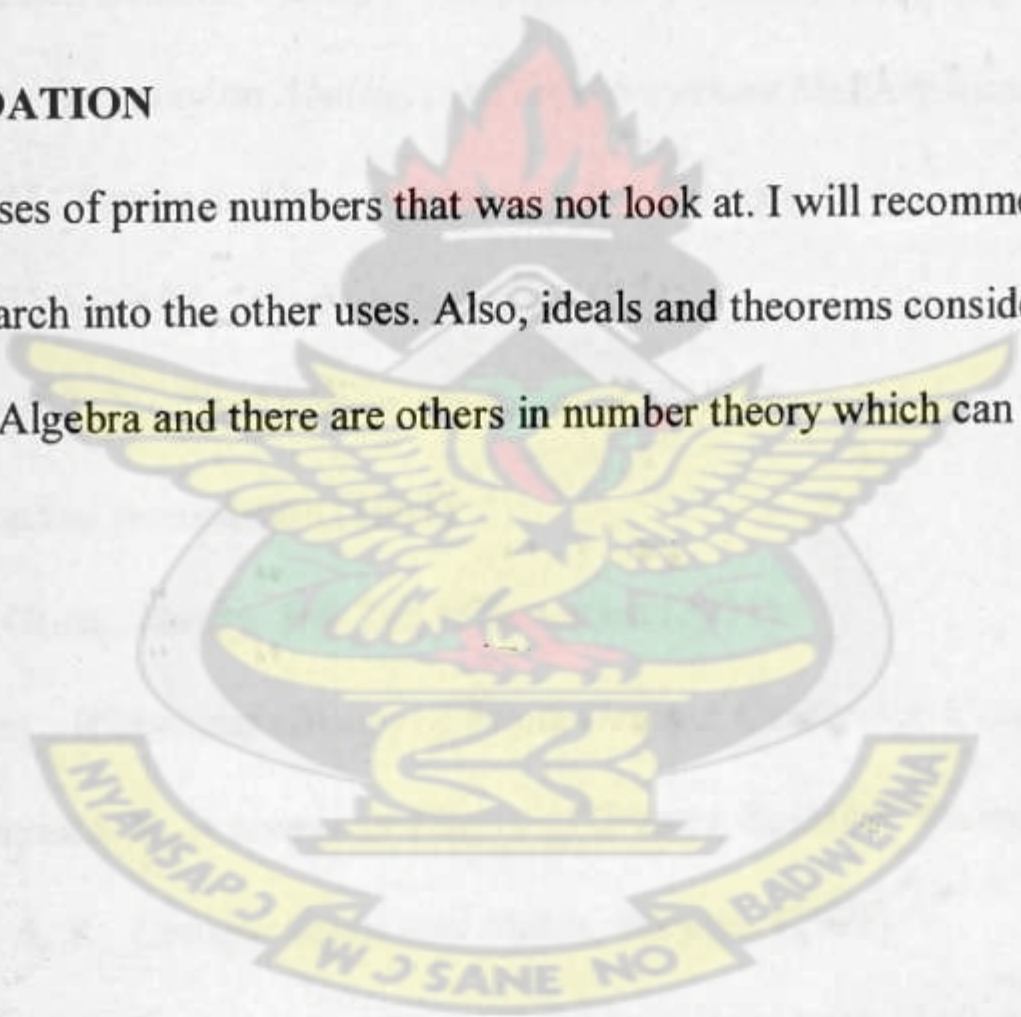
5.1 CONCLUSION

The definition of prime number was clearly stated. There are so many uses of prime numbers, especially prime numbers help in proving certain theories in abstract algebra. With the help of prime number, a new group was discovered that is the p -group.

KNUST

5.2 RECOMMENDATION

There are so many uses of prime numbers that was not look at. I will recommend that other students should research into the other uses. Also, ideals and theorems considered in this thesis were all in Abstract Algebra and there are others in number theory which can be consider.



REFERENCES

1. Aschbacher, M, *Finite Group Theory*, Cambridge University Press
2. Austin, Stephen F. and Judson, Thomas W. , *Abstract Algebra (Theory and Application)*, GNU Free Documentation License (2009)
3. Beezer, Robert A., *A supplement to Abstract Algebra (Theory and Application)*, GNU Free Documentation License (2011)
4. Cohn, Paul , *Free Ideal Rings and Localization in General Rings*, Cambridge (2006)
5. Hausen, Jutta and Schultz, Phillip , *The Maximal Normal p -subgroup of the Automorphism Group of an Abelian p -Group*, American Mathematical Society (1998)
6. Herstein, I. N., *Topics in Algebra*, Blaisdell Publishing (1964)
7. Hungerford, Thomas W., *Algebra*, Springer (1974)
8. Malone, Joseph J. Jr., *The Mathematical Gazette vol. 51*, The Mathematical Association (1967)
9. Milne, J. S., *Group Theory*, Bib Tex Information (2011)
10. Oliver, Robert , *Whitehead Groups of Finite Groups*, Cambridge University Press, (1988)
11. Robinson, Derek J. S., *A course in Theory of Groups*, Springer-Verlag (1982)
12. Wallace, D. A. R., *Groups, Rings and Fields*, Springer (1998)
13. Walter, John H. , *The characterization of Finite Groups with Abelian Sylow 2-subgroups*, Annals of Mathematics (1969)