NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF SCIENCE AND TECHNOLOGY

COURSE CODE: MTH 416

COURSE TITLE: ALGEBRAIC NUMBER THEORY

COURSE GUIDE

MTH 416: ALGEBRAIC NUMBER THEORY

Course Writer: Prof. Adelodun
Department Of Mathematics,
Babcock University, Ilisan
Ogun State

Course Developer: Dr. S.O Ajibola
School Of Science And Technology
National Open University Of Nigeria,
Lagos.

Course Coordinator: Dr. Disu Babatunde
School Of Science And Technology
National Open University Of Nigeria,
Lagos.

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Annex
245 Samuel Adesujo Ademulegun Street
Central Business District
Opposite Arewa Suites
Abuja

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

First Printed

ISBN:

Printed by ……..
For
National Open University of Nigeria

ACKNOWLEDGEMENT:

I acknowledge the authors whose books I used for this write up. These authors appear in the references**.**

TABLE OF CONTENTS

INTRODUCTION

The course, MTH 416, Titled Algebraic Number Theory mostly belongs to the realm of abstract mathematics. The importance of abstract Mathematics is in folds. Apart from the fact that it sharpens the brain, it is also may real quantities that we use came out of abstract thinking. For example, the invention of electricity might have not been possible; were the idea of complex numbers which involves imaginary numbers (an abstract idea) was not developed. Remember the problem faced when the equation $x^2 + 1 = 0$ was not possible in the real number system. We will in this course study algebraic numbers which are solutions of particular equations. We shall study factorization and the situation when a Polynomial is not factorizable. We will learn of Eisenstein Theorem which tells of the conditions when a polynomial is irreducible, so that one will recognize if solving an equation involving a polynomial can be solved by factorization. The latest of Fermat's last Theorem will be revealed, Dirichilet's Theorem and its applications will be studied.

WHAT YOU WILL LEARN IN THIS COURSE

a) In this course, you will learn what an algebraic number or an algebraic integer is. Using Eisenstein Theorem, you will be able to determine, applying certain conditions, if a polynomial is factorizable. You will, as a learner, be familiar the more, with synthetic division. You will learn of ideals, prime and proper ideals. Class group and class member, very useful topics in Number theory will be learnt. You will learn of the Fermat's last Theorem. You will learn that Fermat's last Theorem that has been a problem for mathematicians for more than 200 years is no longer an open problem but that the Dirichilet's Theorem is still an open problem.

AIM OF THE COURSE

Among other benefits, the course is aimed at preparing you for abstract think that will eventually translate into reality. As one may be aware, many physical facilities that we use arise from abstract thinking. The course may introduce you into specializing in number theory.

OBJECTIVES OF THE COURSE

On successful completing the course, you should be able to:

(i) Say what an algebraic number is.

(ii) Say what an algebraic element is.

(iii) Determine when a polynomial is irreducible by applying Eisenstein criteria of irreducibility

(iv) Perform the operations of addition, subtraction and multiplication on quadratic fields.

(v) Give examples of cyclotomic fields.

(vi) Be better informed of proper and prime ideals.

(vii) Be introduced into the idea of class group and class number.

(viii) Be familiar with Fermat's last Theorem, Dirichlet's theorem with its application and Minkowski's theorem.

COURSE MATERIALS

The following are the requirements, or materials need for a thorough understanding of the course.

(i) Abstract algebra courses like Abstract algebra I and II of the NUC BMAS.

(ii) Text book to be listed later.

(iii) Assignment file.

(iv) Dates of tutorials, Assessment and Examination.

RECOMMENDED TEXT-BOOKS

1. Fraileigh,J.B. A first course in Abstract Algebra.
2. Herstein, I.N. Topics in Algebra.
3. Kuku,A.O. Abstract Algebra.
4. Mollin, R.A. Number Theory with Applications. Ribenboim P. Algebraic Number Theory.

ASSIGNMENT FILE AND TUTOR MARKED ASSIGNMENT (TMA)

There are various exercises given in the course. Some of them are worked in addition to the examples already given. It is very important the exercises are attempted. The exercise given at the end of each unit and at the end of each module should be done and submitted to the course lecturer.

COURSE OVERVIEW

There are 4 modules in the course, comprising 11 units with module I comprising 3 units, module2 comprising 2 units module3 comprising 4 units and module 4 comprising 2 units:

Module 1:	Algebraic Numbers
Unit 1 :	Rings: definitions and example.
Units2.	Field
Units3.	Algebraic numbers
Module 2:	Quqdratic and cyclotomic fields.
Unit: 1:	Quadratic fields
Unit: 2:	Cyclotomic fields
Module 3 :	Factorization into irreducible and ideals.
Units 1:	Factorization of polynomial over a field.
Unit 2:	Factorizating into irreducible
Unit 3:	Ideals
Unit 4:	Class and class number
Module 4:	Fermat's Last Theorem, Dirichilet Theorem and Minkowski's Theorem.
Unit 1:	Fermat"s Last Theorem
Unit 2:	Dirichlet's and Minkowski's Theorems.

NATIONAL OPEN UNIVERSITY OF NIGERIA

COURSE CODE: MTH 416

COURSE TITLE: ALGEBRAIC NUMBER THEORY

COURSE MATERIAL

MTH 416: ALGEBRAIC NUMBER THEORY

Course Writer: Prof. Adelodun

Department Of Mathematics,

Babcock University, Ilisan

Ogun State

Course Developer: Dr. S.O Ajibola
School Of Science And Technology
National Open University Of Nigeria,
Lagos.

Course Coordinator: Dr. Disu Babatunde
School Of Science And Technology
National Open University Of Nigeria,
Lagos.

NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja Annex
245 Samuel Adesujo Ademulegun Street
Central Business District
Opposite Arewa Suites
Abuja

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

First Printed

ISBN:

Printed by ……..
For
National Open University of Nigeria

MTH 416: **Algebraic Number Theory**

Module 1: **Algebraic Numbers**

Unit 1. **Ring**

(This unit gives the fundamentals needed for the module).

1.0 INTRODUCTION

The theory of numbers, or arithmetic, is often called "the queen of mathematics". The simplicity of its subject matter (the ordinary integers and their generalization), attract mathematicians of all classes, whether they be beginners, professional number theorists, or specialists in other branches of mathematics. Emphasis upon the algebraic point-of-view seems to me justifiable for several reasons. First of all, the algebraic point-of-view establishes the context in which number theoretic problems have their most natural formulation. This is true of even those problems which concern only the natural numbers. For example, the problem of finding all integer solutions of the Pell-Fermat equation

$x^2 + dy^2 = \pm 1$ (d: a square-free integer) involves in an essential way the study of the quadratic field of nth roots of unity plays an analogous role. In order to represent an integer as the sum of two (respectively, four) squares, it is advantageous to work in the ring of Gaussian integers (respectively, in a suitably chosen quaternion algebra). The law of quadratic reciprocity involves both quadratic fields and roots of unity. Fields more general than the rational numbers and rings more general than the ordinary integers arise quite naturally when one discusses any of the above problems.

Secondly, although the algebraic approach does not lead to a solution of all number theoretic problems, it does, as the reader will see, nonetheless quickly lead to substantial results. Continuing in the direction of this book, one would reach the deep theorems of class field theory.

Thirdly, even those who prefer analytic number theory will agree that the full generality and power of the analytic approach reveals itself only in the context of number fields and simple algebras, not in investigations involving the rational number alone.

Finally, algebraic number theory provides the student with numerous illustrative examples of notions he has encountered in his algebra courses: groups, rings, fields, ideals, quotient rings and quotient fields, homomorphism and isomorphism, modules and vector spaces. A further benefit to the student lies in the fact that, in studying algebraic number theory, he will meet many new algebraic notions, notions which are fundamental not only for arithmetic but for other branches of mathematics as well, in particular algebraic geometry. Here are some examples: integrality, field extensions, Galois Theory, modules over principal ideal rings, Noetherian rings and modules, Dedekind rings, and rin… gs of fractions.

2.0: Objective

To further teach index knowledge of Abstract algebra

To know the Definition and solve some examples

3.0 Main Content

3.1 Definition.

Let R be a set. Then R is called a ring if two binary operations

(i) $\oplus$ Called addition and (ii) $\odot$ Called multiplication are defined such that:

(a) $(R,\oplus)$ is an ablelian group.

(b) $(R,\odot)$ is a semi group

(c) $\forall, x, y, z \in R$

(i) $x \odot (y \oplus z) = x \odot y \oplus x \odot z,\odot$ is right distributive over $\oplus$.

(ii) $(x \oplus y) \odot z = x \odot z \oplus y \odot c, \odot$ is left distributive over $\oplus$.

A ring R may be denoted $(R, \oplus, \odot)$, indicating the two fundamental operations required to make the set, R a ring. But if there is no confusion of the operations, we just denote the ring, R by R

We should note that it is the multiplicative properties that are used to characterize a ring. Thus, a ring R is called commutative if $\odot$ is commutative in R. Again a ring, R is called a ring with identify if R has the multiplicative identity, 1. That is, $1 \in R$ such that $\forall x \in R, x \odot 1 = 1 \odot x = x;$ then R is called a ring with identity. We, usually, shall write 1 for the additive identity except we state otherwise, If the ring is a commutative one, only one of the distributive laws needs holds for R to be called a ring. Very often too, we denote $\oplus$ by $+$ and $\odot$ by.

Examples

(i) $(\mathbb{Z}, +, \cdot)$ is a commutative ring with 1.

(ii) $(\mathbb{R}, +, \cdot)$ is a commutative ring with 1.

(iii) $(Q, +, \cdot)$ is a commutative ring with 1.

(iv) $(\mathbb{C}, +, \cdot)$ is a commutative ring with 1

(v) $(\mathbb{Z}n, +, \cdot)$, $n \in \mathbb{N}$, is commutative ring with 1.

Counter example

(i) $(\mathbb{N}, +, \cdot)$ (ii) $\left(M_{mn}^{(\mathbb{R})}, +, \cdot\right)$

Example: Show that $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.

Verification

For $(\mathbb{Z}, +, \cdot)$ to be a group, it must be that:

(a) $(\mathbb{Z},+)$ is an abelian group, and certainly $(\mathbb{Z},+)$ is an abelian group.

(b) $(\mathbb{Z},\ \cdot)$ is a semigroup. It is also clear that $(\mathbb{Z},\ \cdot)$ is a semigroup.

(c) The distributing properties of (a) right distributive property of multiplication over addition is obvious and since multiplication is abelian, the right distributive property implies the left distributive property.

Therefore, $(\mathbb{Z},+,\cdot)$ is a ring . Indeed, $(\mathbb{Z},+,\cdot)$ is a commutative ring with, 1.

Exercise

(1) Follow a similar procedure to show that $(Q,+,\cdot)$ and $(\mathbb{R},+,\cdot)$ are Commutative rings with 1.

(2) Show when $(\mathbb{N},+,\cdot)$ is not an abelian group.

Solution to exercise 2

To show that $(\mathbb{N},+,\cdot)$ not a commutative ring with identity is, we show which of the properties of a ring does not hold: For $(\mathbb{N},+,\ \cdot)$ to be a ring, $(\mathbb{N},+,\ \cdot)$ must be:

(i) Abelian group.

(ii) Semigroup with respect to multiplication.

(iii) The distributive properties must hold.

Is $(\mathbb{N},+)$ an abelian group?

If it is, the following holds.

(a) Closure with respect to addition,

(b) Associativity with respect to addition,

(c) $\exists\ 0 \in \mathbb{N}\ \ s.t.\ \ \forall n\ \in \mathbb{N}, n+0=0+n=n.$

(d) $\exists -n \in \mathbb{N}\ \ni \text{for } all\ n \in \mathbb{N}, -n+n=n-n=0.$

Clearly,(c)and (d) does not hold in $\mathbb{N}$. so, $(\mathbb{N},+,\ \cdot)$ is not a group and cannot therefore be a ring.

Zero divisors and proper zero divisors

3.2 Definition.

Let R be a ring and let $x, y \in R$ such that $xy = 0$. Then x is called a left zero divisor and y is called right zero divisor. If it happens that $xy = 0$ with $x \neq 0, y \neq 0$, then x is called a proper left zero divisor and y, a right proper zero divisor. If R is commutative, then the notion of left and right zero divisors or left proper and right proper zero divisors coincide and we just have zero divisors or proper zero divisors.

Examples. (i) in $\mathbb{Z}$, x and y are proper zero divisors.

(i) Let $R = \{M_{22}(\mathbb{R})\}$. If $T \in R$ where

$$S = \left\{X = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix},\ Y = \begin{pmatrix} x & y \\ 0 & o \end{pmatrix}\right\},$$

Then

$$XY = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

So, S has proper zero divisors, since $X \neq 0,\ Y \neq 0$ and $XY = 0$

(iii). $(\mathbb{Z}_6, +, \cdot)$ has proper zero divisors, since $\bar{2}.\bar{3} \in \mathbb{Z}_6$ and

$\bar{2}.\bar{3} = 0$, with $\bar{2} \neq 0, \bar{3} \neq 0$.

Counter examples

(i) $(\mathbb{Z}, +, \cdot)$, has no proper zero divisors.

(ii) $(\mathbb{R}, +, .)$, has no proper zero divisors.

Exercise. Show whether $(\mathbb{Q}, +, \cdot)$ has proper zero divisors.

3.3 Integral Domain

A ring R is called an integral domain (or entire ring) if

(i) R is commutative with 1

(ii) R has no proper zero divisors.

Examples

(i) $(\mathbb{Z}, +, \cdot)$ is an integral domain.

(ii) $(\mathbb{R}, +, \cdot)$ is an integral domain.

(iii) $(\mathbb{Q}, \mathbb{C}, \cdot)$ is an integral domain.

(iv) $(\mathbb{Z}_5, +, \cdot)$ (or indeed $\mathbb{Z}_n$, n prime) is an integral domain.

Counter examples

(i) $\mathcal{S} = \{X, Y\}$ where $X = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}, Y = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ is not an integral domain.

(ii) $(\mathbb{Z}_6, +, \cdot)$ (or indeed $\mathbb{Z}_n, n$ even) is not an integral domain.

Remark

A commutative ring, R with identity is an integral domain iff the cancellation law holds i.e. $ab = ac \Rightarrow b = c$ (or $ac = bc \Rightarrow a = b$).

3.4 Unit or inverse

Definition.

Let R be a ring with 1, and let x, y $\in R$ be any two elements such that $xy = 1$. Then x is called a left unit and y is called a right unit of R. Also we call x a left inverse and y a right inverse of R. We note that the distinction vanishes if R is commutative. A unit

$\in R$. is also called invertible element of R if $xy = yx = 1$, then y is called the inverse of x, inverse of x is written x^{-1}. We denote the set of all unit of R by $U(R)$.

Concrete examples

(i) In the ring, $(\mathbb{Z}, +, .)$, $U(\mathbb{Z}) = \{-1, 1\}$.

(ii) In the ring $M_{22}(\mathbb{Z}), U(M_{22}(\mathbb{Z})) = \begin{pmatrix} 0 & 1 \\ 1 & o \end{pmatrix}$.

Exercise.

Show that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is both left and right units.

Solution to the Exercise

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0\times 0+1\times 1 & 0\times 1+1\times 0 \\ 1\times 0+0\times 1 & 1\times 1+0\times 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

3.5: Division Ring

Definition: A ring D with identity such that every non zero element has a multiplicative inverse (i.e every nonzero element is a unit) is called a division ring (or Skew field)

Concrete Examples

(i) $(Q, +, .)$ is a division Ring.

(ii) $(\mathbb{R}, +, .)$ is a division ring.

Concrete counter examples.

(i) $(\mathbb{Z}, +, .)$ (ii) $(\mathbb{N}, +, .)$

(iii) The Quaternion of Hamilton.

We denote the $\hat{Q}$ as $\hat{Q} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. $\hat{Q}$ is a group under component-wise addition.

We give certain elements of $\hat{Q}$ as follows:

1= $(1,0,0,0), i = (0,1,0,0,)$, j = $(0,0,1,0)$, k =$(0,0,0,1)$

Again, we let

$a_1 = (a_1, 0, 0, 0)$, $a_2 = (0, a_2 0, 0,)$, $a_3 = (0,0, a_3, 0)$

$a_4 = (0,0,0, a_4)$.

By the definition of addition given, $(a_1 a_2 a_3 a_4) = a_1 + a_{2i} + a_{3j} + a_4 k$.

Thus,

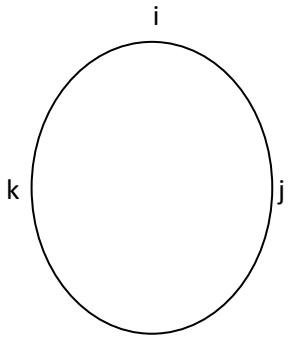
$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k)$$

$$= (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$$

To define multiplication in $\hat{Q}$, we first define

$1a = a1 = a$, for $a \in \hat{Q}, i^2 = j^2 = k^2 = -1$ and

$ij = k, jk = i, ki = j_j\ ji = -k, kj = -i, ki = -j$



Note. Product of two adjacent elements from left to right gives the next while product from right to left gives negative of the next.

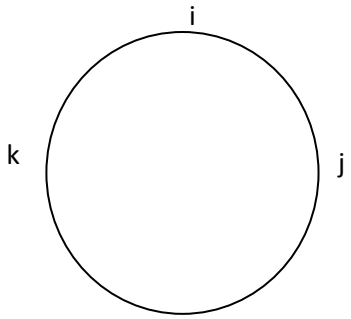
Example: The ring of real quarternons, $(\hat{Q}, +, \ .)$

$\hat{Q}$ has the elements of the form, $a \in \hat{Q}$ and

$a = a_0 + a_i i + a_2 j + a_3 k$, where $a_i \in \mathbb{R}$, and i, j, k

are symbols satisfying $i^2 = j^2 = k^2 = -1$.

$ij = k,\ \ jk = i,\ \ ki = j,\ \ kj = -i,\ \ ki = -j$



Note. Production of two adjacent elements from left to right gives the next one, while product from the left gives the negative of the next one. Suppose that

$a = a_o + a_1 i + a_2 j + a_3 k$

$b = b_o + b_1 i + b_2 j + b_3 k.$

Define $+$ in $\widehat{Q}$ by

$a + b = (a_o + a_1 i + a_2 j + a_3 k) + (b_0 + b_1 i + b_2 j + b_3 k)$

$= (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k$

and multiplication in $\hat{Q}$ by

$$a.b = (a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k)$$

$$= (a_0 b_0 - a_1 b_1 - a_2 b_2 - a_3 b_3) + (a_0 b_1 + a_1 b_0 + a_2 b_3 - a_3 b_2) i$$
$$+ (a_0 b_2 - a_1 b_3 + a_2 b_0 + a_3 b_1) j + (a_0 b_3 + a_1 b_2 - a_2 b_1 + a_3 b_0)$$

Exercise. Verify that $(a + b) + c = a + (b + c)$.

4.0 CONCLUSION

Obviously, it can further, be shown that not all Abelians are rings i.e quotient rings (quarternon)

For instance, Show when $(Z/Q, +, \cdot)$ is not an abelian group

To show that $(Z/Q, +, \cdot)$ not a commutative ring with identity is, we show which of the properties of a ring does not hold: For $(Z/Q, +, \cdot)$ to be a ring, $(Z/Q, +, \cdot)$ must be:

(iv) Abelian group.

(v) Semigroup with respect to multiplication.

(vi) The distributive properties must hold.

Is $(Z/Q, +)$ an abelian group?

If it is, the following holds, hence, it does not hold.

a) Closure with respect to addition,

b) Associativity with respect to addition,

c) $\exists\, 0 \in Z/Q \;\; s.t. \;\forall\, z/q \in Z/Q, z/q + 0 = 0 + z/q = z/q.$

d) $\exists - z/q \in Z/Q \;\ni \text{for } all\; z/q \in Z/Q, -z/q + z/q = z/q - z/q = 0.$

It is clearly shown that the last two axioms does not hold in Z/Q. so, $(Z/Q, +, \cdot)$ is not a group and cannot therefore be a ring.

5.0 SUMMARY

In summary, a ring must be an Abelian group satisfying the following properties:

i) associativity of products i.e (a.b).c = a.(b.c)

ii) associativity of addition i.e (a+b)+c = a+(b+c)

iii) commutativity and identity i.e (1+0)= (0+1) =1

iv) and, also (0.1) = (1.0) = 0

v) must also satisfy the closure properties.

vi) must also satisfy, the distributive properties.

6.0 TUTOR MARK ASSINMENTS

1 .Answer true or false:

(i) A ring is also an abelian group with respect to addition.

(ii) A ring must be a semi group under multiplication.

(iii) $(\mathbb{N}, +, .)$ is a ring.

(iv) $(\mathbb{N}, +, .)$ is an abelian group.

(v) $(\mathbb{Z}, +, .)$ is an integral domain.

(vi) It is the multiplicative property we use to describe a ring.

2. Define a division ring. Hence show if $(\mathbb{R}, +, .)$ is a division ring.?

7.0 REFERENCES AND FURTHER READING

1. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11

MODULE 1

Unit 2. Field.

1.0 INTRODUCTION

The word "field" as used in algebra refers to a certain algebraic structure.

A *field* is a set equipped with two binary operations, one called addition and the other called multiplication, denoted in the usual manner, which are both commutative and associative, both have identity elements (the additive identity denoted 0 and the multiplicative identity denoted 1), addition has inverse elements (the additive inverse of x denoted $-x$ as usual), multiplication has inverses of nonzero elements (the multiplicative inverse of x denoted either $1x$ or $x-1$), multiplication distributes over addition, and $0 \neq 1$.

Important examples of fields are

- the field **R** of real numbers
- the field **C** of complex numbers
- the field **Q** of rational numbers
- the prime field with p elements where p is any prime number.

2.0 OBJECTIVE

To increase the level of abstraction and reasoning of Students,

To solve examples that are related.

3.0 MAIN CONTENTS

Definition: A field is a commutative division ring. The definition of a ring as given implies that the nonzero elements of a field form an abelian group under multiplication.

Examples.

(i) $(\mathbb{R}, +, .)$ is a field, the field of real number

(ii) $(\mathbb{Z}_7, +, .)$ is a field.

(iii) (Q, +, .) is a field, the field of rational numbers.

Exercise: Verify that $(\mathbb{Z}_7, +, .)$ is a field.

Solution

(i) Note that $\mathbb{Z}_7$ is the set of remainders, when $\mathbb{Z}$ is divided by 7. i.e.

$\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

. We make the following tables for $(\mathbb{Z}_7, +)$ and $(\mathbb{Z}_7, .)$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

Table 1: $(\mathbb{Z}_7, +)$

$-$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Table 2: $(\mathbb{Z}_7, .)$

From table 2, In $(\mathbb{Z}_7, \cdot)$, (i) $\exists\, x, y \in \mathbb{Z}_7$ s.t. $xy = 0$ with $x \neq 0, y \neq 0$.

(ii) Every nonzero element in $\mathbb{Z}_7$ has a multiplicative inverse:

(a) The multiplicative inverse of $\bar{2}$ is $\bar{4}$

(b) The multiplicative inverse of $\bar{3}$ is $\bar{5}$

(c)The multiplicative inverse of $\bar{4}$ is $\bar{2}$

Exercises. Write down the multiplicative inverse of

(i) $\bar{5}$ (ii) $\bar{6}$ (iii) $\bar{1}$

Theorem.

Any finite integral domain is a field.

Proof.

To prove the theorem, we just need to show that every nonzero element of a finite integral domain S has a multiplicative inverse. Suppose that $S = \{0, 1, a_3, a_4, \dots, a_n\}$. Let a be any fixed nonzero element of S and let $S* = \{1, a_3, a_4, \dots, a_n\}$, the set of nonzero elements of S. Suppose that $T = \{a, a_3a, a_5a, \dots, a_na\}$

Then the elements of T are distinct, since $a_ia = a_ja \implies a_i = a_j$ by cancellation law. Also since S has no proper zero divisor (as an integral domain), every element of T is nonzero. Moreover, $1 \in T$. So, there exists a_j such that $aa_j = 1$. i.e. a Multiplicative inverse.

Corollary.

For any prime p, $\mathbb{Z}_p$ is a field.

Proof /llustration.

We note that $(\mathbb{Z}_3, +, \cdot)$ $(\mathbb{Z}_5, +, \cdot)$ and $(\mathbb{Z}_7, +, \cdot)$ are fields, for by the tables of $(\mathbb{Z}_7, +,)$ and $(\mathbb{Z}_7, \cdot)$ shown earlier, $\left(\text{and indeed } (\mathbb{Z}_p, +) \text{and } (\mathbb{Z}_p, \cdot)\right)$ for any prime, $(p \in \mathbb{Z},)$, $(\mathbb{Z}_p, +, \cdot)$ has no proper zero divisors and clearly, it is commutative with identity.

Example

Show if $(S, +, .)$ is a field, an integral domain in, or a Skew field.where $S = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, a, b \in \mathbb{R}\right\}$, + is the usual matrix addition and. is the usual matrix multiplication.

Solution

We note that S is the set of a special 2 by 2 matrices over $\mathbb{R}$ and as such it is an abelian group with respect to addition, it is a semi group under multiplication. This special

matrix is commutative since

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix}; \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} ba & 0 \\ 0 & ba \end{pmatrix}$$

Since $a, b \in \mathbb{R}$, $ab = ba$. so the special matrices, S, has identity. Therefore, from the foregone, S, is a field.

5.0 SUMMARY

We can further summarized with this theorem that any finite integral domain is a field.

Proof.

To prove the theorem, we just need to show that every nonzero element of a finite integral domain S has a multiplicative inverse. Suppose that $S = \{0, 1, a_3, a_4, \dots, a_n\}$. Let a be any fixed nonzero element of S and let $S* = \{1, a_3, a_4, \dots, a_n\}$, the set of nonzero elements of S. Suppose that $T = \{a, a_3a, a_5a, \dots, a_na\}$

Then the elements of T are distinct, since $a_ia = a_ja \implies a_i = a_j$ by cancellation law. Also since S has no proper zero divisor (as an integral domain), every element of T is nonzero. Moreover, $1 \in T$. So, there exists a_j such that $aa_j = 1$. i.e. a Multiplicative inverse.

Corollary.

For any prime p, $\mathbb{Z}_p$ is a field.

illustration.

We note that $(\mathbb{Z}_3, +, \cdot)$ $(\mathbb{Z}_5, +, \cdot)$ and $(\mathbb{Z}_7, +, \cdot)$ are fields, for by the tables of $(\mathbb{Z}_7, +,)$ and $(\mathbb{Z}_7, \cdot)$ shown earlier, $\left(\text{and indeed } (\mathbb{Z}_p, +) \text{and } (\mathbb{Z}_p, \cdot)\right)$ for any prime, $(p \in \mathbb{Z},)$, $(\mathbb{Z}_p, +, \cdot)$ has no proper zero divisors and clearly, it is commutative with identity.

5.0: CONCLUSION

The rational numbers, which are the integers and the fractions like [23, -1/3, 355/113], allow you to do the following things with them: you can add and subtract them, you can multiply them, and you can divide them as long as you don't divide by 0.

Those operations satisfy various rules such as $a+b = b+a$, $a\times(b\times c) = (a\times b)\times c$ and $a\times(b+c) = a\times b+a\times c$ for any rational numbers a,b,c. There are "neutral" elements: 0 doesn't do anything when it's added to any number, and 1 doesn't do anything when it's multiplied by any number. Every number a has an inverse: $a + (-a) = 0$, and if it's nonzero it also has a reciprocal $a\times 1a = 1$. There are a few other similar rules, I didn't list them all, but it's a short and familiar list. This is an example of a *field*. In fact this is the model upon which the notion of a field is based. Generally, a field is any set of things (numbers, functions, bicycles, stuffed animals, doesn't matter) which are equipped with operations of "addition" and "multiplication". Each of these is just a machine that takes two things and outputs a thing.

They don't have to resemble ordinary addition and multiplication in any way, they just need to have the same properties I mentioned above. If they do, you have a field.

For example, we can take the two words "Even" and "Odd", and define "addition" and "multiplication" between these words according to the familiar rules of how odd and even numbers behave. So Even + Even = Even, Even + Odd = Odd + Even = Odd, Odd + Odd = Even, Even x Even = Even x Odd = Odd x Even = Even and Odd x Odd = Odd.

This is a field! You may take the time to verify that all the rules apply. "Even" is the neutral element for addition (so it's like the "0" of this field) and "Odd" is neutral for multiplication (so it's like the "1"). In fact this is the smallest field, having just two elements.

6.0: TUTOR MARKED ASSIGNMENTS

1. What do you mean by $\mathbb{Z}_n$? Give the elements of $\mathbb{Z}_7$. Hence show if $(\mathbb{Z}, +, .)$ has proper zero divisors. Deduce if $(\mathbb{Z}, +, \cdot)$ is a field
2. Write true or false for each of the following assertions.

   (a) $(\mathbb{Z}, +, .)$ is a field.

   (b) We can talk of the field of integers.

   (c). the set of integers has a multiplicative inverse for each element.

   (d). $\mathbb{N}$ is not a field.

   (e) $\mathbb{R}$ is a field and so we can talk of the field of real numbers.

   (f) A field is commutative ring.

   (g) Any integral domain is a field.

7.0 REFERENCES AND FURTHER READING

1. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. 175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
8. Pierro Samuel, (1970), Algebraic Theory of Numbers. Dovear Publication, inc Mineola, New York, pp 9.
9. David Joyce, Professor of Mathematics at Clark University definition of Field.
10. Alon Amit, PhD in Mathematics; Mathcircler

MODULE 1

Unit 3: Algebraic Numbers (extension field)

1.0 INTRODUCTION

The extension field degree of an extension field K/F, denoted [K:F], is the dimension of K as a vector space over F, i.e, $[K:F] = \dim_F K$.

Given a field F, there are a couple of ways to define an extension field. If F is contained in a larger field, $F \subset F'$. Then by picking some elements $\alpha_i \in F'$ not in F, one defines $F(\alpha_i)$ to be the smallest subfield of F' containing F and the α_i. For instance, rationals can be extended by the Complex numbers ζ, yielding $\mathbb{Q}(\zeta)$. If there is only one new element, the extension is called a simple extension. The process of adding a new element is called "adjoining." Since elements can be adjoined in any order, it suffices to understand simple extension Because α_i is contained in a larger field, its algebraic operations, such as multiplication and addition, are defined with elements in F. Hence,

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g.are.polynomials.in.F.and.g(\alpha) \neq 0 \in F' \right\}$$

2.0 OBJECTIVES

The objectives are:

To show that every number field is a simple extension of the rationals

To show that naturally, the choice of ζ is not unique.

3.0 MAIN CONTENT

Definitions

(i) Extension field

A field E is called an extension field of a field F if $F \leq E$. Thus $\mathbb{R}$ is an extension field of the field $\mathbb{Q}$,$\mathbb{C}$ is also an extension field of both the field $\mathbb{R}$ and $\mathbb{Q}$ where $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are fields of real numbers, field of rational numbers and field of the complex numbers respectively.

(ii) Algebraic Element.

An element, α of an extension field E of a field F is algebraic over F if $f(\alpha) = 0$

For some nonzero $f(x) \in F[x]$. If α is not algebraic over F,then α is transcendental over F. Note, $F[x]$denotes a ring of polynomials in x. That is,

$$F(x) = \sum_{i=0}^{n} a_i x^i.$$

Examples:

(i) $\mathbb{C}$ is an extension of $\mathbb{Q}$, since $\sqrt{2}$ is a zero of $x^2 - 2$.

Therefore $\sqrt{2}$ is an algebraic element over $\mathbb{Q}$,for, if $f(x) = x^2 - 2$, then $f(\sqrt{2}) = (\sqrt{2})^2 - 2 \Rightarrow 2 - 2 = 0$.

(ii) i is algebraic is an algebraic element of $x^2 + 1$, since $i \in \mathbb{C}$ and for

$f(x) = x^2 + 1, f(i) = i^2 + 1 \Rightarrow -1 + 1 = 0$.

That is, $f(i) = 0$, showing i is algebraic over Q.

Counter Examples.

(i) π is not algebraic over $\mathbb{Q}$, since $\pi \in \mathbb{C}$, and for

$$f(x) = x^2 + 1, f(\pi) \equiv f\left(\frac{22}{7}\right) + 1 \neq 0$$

Therefore π is a transcendental element.

(ii) $e = 2.718$ is not algebraic over Q since, for $f(x) = x^2 + 1$, then

$f(2.718)^2 + 1 \neq 0$

Thus, π and e are transcendental over $\mathbb{Q}$.

(iii) Now $\mathbb{R} \leq \mathbb{R}$, i.e $\mathbb{R}$ is an extension of $\mathbb{R}$. Then π is algebraic over$\mathbb{R}$, since if $f(x) = x - \pi, f(\pi) = \pi - \pi = 0 \in \mathbb{R}$.

Remark.

Just as we do not speak of a vector space but of a vector space over F, in the same way, we do not speak of algebraic number but of algebraic number over F.

Example.

Show that the real number, $\sqrt{1+\sqrt{3}}$ is algebraic over $\mathbb{Q}$.

Solution.

α is algebraic over $\mathbb{Q}$ if $f(\alpha) = 0$, for any $f(x) \in F[x]$.

Now, $\alpha = \sqrt{1+\sqrt{3}}$ then $\alpha^2 = \left(\sqrt{1+\sqrt{3}}\right)^2$

That is, $\alpha^2 = 1 + \sqrt{3}$, that is $\alpha^2 - 1 = \sqrt{3}$.

and $(\alpha^2 - 1)^2 = (\sqrt{3})^2 \Rightarrow (\alpha^2 - 1)^2 = 3$.

$\Rightarrow \alpha^4 - 2\alpha^2 + 1 = 3$,i.e. $\alpha^4 - 2\alpha^2 + 1 - 3 = 0$.

So, $\alpha^4 - 2\alpha^2 - 2 = 0$.

We show that α is a zero of the polynomial.

$\alpha^4 - 2\alpha^2 - 2 = 0$

If $\alpha = \sqrt{1+\sqrt{3}}$, then . $\alpha^4 - 2\alpha^2 + 1 = 3$

becomes

$\left(\sqrt{1+\sqrt{3}}\right)^4 - 2\left(\sqrt{1+\sqrt{3}}\right)^2 + 1 = 3,$

$$\left(\sqrt{1+\sqrt{3}}\right)^4 - 2\left(\sqrt{1+\sqrt{3}}\right)^2 - 2 = 0$$

$$\left(\sqrt{1+\sqrt{3}}\right)^2\left(\sqrt{1+\sqrt{3}}\right)^2 - 2\left(\sqrt{1+\sqrt{3}}\right)^2 - 2 = 0$$

$$(1+\sqrt{3})(1+\sqrt{3}) - 2(1+\sqrt{3}) - 2 = 0$$

$$1+\sqrt{3}+\sqrt{3}+3-2-2\sqrt{3}-2 = 0$$

Therefore α is algebraic over $\mathbb{Q}$, since $f(\alpha) = 0$.

Exercise.

For each of the following given numbers, $\alpha \in \mathbb{C}$, show whether α is algebraic over Q by looking for $f(x) \in Q[x]$ such that $f(\alpha) = 0$.

(i) $1+\sqrt{2}$ (ii) $\sqrt{2}+\sqrt{3}$ (iii) $1+i$

Solutions

(i) For $\alpha = 1+\sqrt{2}$, we try the function

$f(x) = x^2 - 2x - 1$

Now, find $f(\alpha)$ where $\alpha = 1+\sqrt{2}$, and see if $f(\alpha) = 0$.

Now, $f(\alpha) = (1+\sqrt{2})^2 - 2(1+\sqrt{2}) - 1.$

$= 1+2\sqrt{2}+2-2 = -2\sqrt{2}-1$

$= 1+2-2-1$ i.e. $3-3=0.$

Therefore, $1+\sqrt{2}$ is algebraic over $\mathbb{Q}$.

(ii) For $\alpha = \sqrt{2}+\sqrt{3}$, try the function, $f(x) = x^4 - 10x^2 + 1.$

If $f(\alpha) = 0$, then α is an algebraic number over $\mathbb{Q}$.

Now, $f(x) = x^4 - 10x^2 + 1.$

Then $f(\alpha) = \alpha^4 - 10\alpha^2 + 1$

$= (\sqrt{2}+\sqrt{3})^4 - 10(\sqrt{2}+\sqrt{3})^2 + 1$

$= (\sqrt{2}+\sqrt{3})^2(\sqrt{2}+\sqrt{3})^2 - 10(\sqrt{2}+\sqrt{3})^2 + 1$

$= (2 + 2\sqrt{2}\sqrt{3} + 3)(2 + 2\sqrt{2}\sqrt{3} + 3) - 10(2 + 2\sqrt{2}\sqrt{3} + 3) + 1$

$= (5 + 2\sqrt{2}\sqrt{3})(5 + 2\sqrt{2}\sqrt{3}) - 10(5 + 2\sqrt{2}\sqrt{3}) + 1$

$25 + 10\sqrt{2}\sqrt{3} + 10\sqrt{2}\sqrt{3} + 4 \times 2 \times 3 - 50 - 20\sqrt{2}\sqrt{3} + 1$

$25 + 20\sqrt{2}\sqrt{3} + 24 - 50 - 20\sqrt{2}\sqrt{3} + 1$

$25 + 24 - 50 + 1 = 0$

Therefore, $f(\alpha) = 0$, hence α is algebraic over $\mathbb{Q}$.

For $\alpha = 1 + i$, try $f(x) = x^2 - 2x + 2$

$f(x) = x^2 - 2x + 2$

$f(\alpha) = x^2 - 2\alpha + 2$

$= (1 + i)^2 - 2(1 + i) + 2$

$= 1 + 2i - 1 - 2 - 2i + 2$

$= 3 - 3 = 0.$

Therefore $\alpha = 1 + i$ is algebraic over $\mathbb{Q}$.

4.0 SUMMARY

As in conclusion

5.0 CONCLUSION

We conclude with this remark that Just as we do not speak of a vector space but of a vector space over F, in the same way, we do not speak of algebraic number but of algebraic number over F.

6.0 TUTOR MARKED ASSIGNMENT

1. When is a field E called an extension field of a field F? Is $\mathbb{R}$ an extension of $\mathbb{Q}$

2. What do you mean by an algebraic element?

   If $f(x) \in F[x]$ and $f(x) = x^2 - 3$, show if $\sqrt{2}$ is algebraic over F.

3. What is a transcendental element? If $f(x) \in F[x]$, and $f(x) = x^2 - 2$, show if $\sqrt{2}$ is a transcendental element of F.

QUESTION BANKS FOR THE MODULE (exercises)

1. When is a ring said to be a commutative ring with 1. Give 2 examples of a commutative ring with 1. Give an example of a non-commutative ring with identity.
2. List the properties a set must satisfy in order to be called a ring.
3. When will a ring become

   (a) A division ring? (b) an entire ring?

   (c) An integral domain? (d) A field?
4. Give the elements of (a.) $\mathbb{Z}_5$, (b). $\mathbb{Z}_6$.

   If (i). $(\mathbb{Z}_5, +, \cdot)$ is an integral domain. (ii). $(\mathbb{Z}, +, \cdot)$ is a field.
5. Answer true or false for each of the following:

   (a). $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.

   (b). $(\mathbb{Q}, +, \cdot)$ is a division ring.

   (c). $(\mathbb{R}, +, \cdot)$ is a field.

   (d) $(\mathbb{Z}, +, \cdot)$ is a field.

   (e) $(\mathbb{N}, +, \cdot)$ is a field.

6. Let $S = \{X, Y, Z\}$ where $X = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ be a commutative ring with identity. Determine if S is an integral domain.

7(a) Define an algebraic element. Hence show that (i) $\sqrt{2}$ is algebraic element over $\mathbb{Q}$, if $f(x) = x^2 - 2$. Where $\mathbb{C}$ is an extension of $\mathbb{Q}$.

(b) $i \in \mathbb{C}$ is an algebraic element over Q if $f(x) = x^2 + 1$.

(c) If $f(x) = x^2 + 1$, determine if π is an algebraic element over Q, where is an extension of Q.

8. Show that the real number, $\sqrt{1+\sqrt{3}}$ is algebraic over Q.

7.0 REFERENCES AND FURTHER READING

1. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
8. Mathworld contributor Rowland Algebra Field Theory.

Module 2: Quadratic and Cyclotomic Fields.

Unit 1: Quadratic Field.

1.0 INTRODUCTION

We can now say a bit more about the relationship between quadratic fields and cyclotomic fields.

Let $\omega = e^{2\pi/p}$ for an odd prime p. Recall disc $(\omega) = \pm p^{p-2}$ where the sign is positive if and only if p = 1(mod4). Using the definition of the discriminant, we have

$$\left|\sigma_i\left(\omega^j\right)\right| = p^{(p-3)/2}\sqrt{\pm p}$$

where the σ_i are the embeddings of Q[ω] in C. But each embedding simply maps each ω_i to some other ω^j, thus we may compute √±p using field operations on the powers of ω. In other words, $\sqrt{\pm p} \in Q[\omega]$, with the sign positive if and only if p=1(mod4).

For example, for p=3 the above equation becomes

$$\begin{vmatrix} 1 & \omega \\ 1 & \omega^2 \end{vmatrix} = \sqrt{-3}\,|$$

which can be rewritten $\sqrt{-3} = 2\omega + 1$

Similarly for p=5 we obtain $\sqrt{5} = \omega^2 - \omega^4 + \omega^3 - \omega = 1 - 2\omega^4$.

The 8th cyclotomic field contains √2 because in this case we have.

$\omega = \sqrt{2}/2 + i\sqrt{2}/2$, and hence, $\sqrt{2} = \omega + \omega^{-1}$

If the qth cyclotomic field contains Q[p], the 4qth cyclotomic field contains $Q\sqrt{-p}$ because it must contain the fourth root of unity i along with √p.

Now consider any square free $m = p_1.....p_r$. for each p_i take the cyclotomic field containing √p. Then take the smallest cyclotomic field K containing all these fields. Then K contains $Q\sqrt{m}$. Set $d = disc(A \cap Q\sqrt{m})$. It can be easily verified that the desired K is in fact the dth cyclotomic field.

Kronecker and Weber proved that every abelian extension of Q (normal with abelian Galois group) is contained in a cyclotomic field. Hilbert and others studied abelian extensions of general number fields, and their results are known as **class field theory**.

2.0 OBJECTIVE

The objectives are:

To define Quadratic and Cyclotomic Fields

To solve some numerical examples

3.0 MAIN CONTENTS

Definitions

Quadratic fields are subfields of $\mathbb{C}$ generated by $\mathbb{Q}$ and $\sqrt{d}$, where d is a square free integers. A square free integer is an integer that is not divisible by the square of any prime. A quadratic field is denoted by $\mathbb{Q}\sqrt{d}$. A member of $\mathbb{Q}\sqrt{d}$ is of the form $\sigma = r + s\sqrt{d},\ r, s \in \mathbb{Q}$. The operations of $\mathbb{Q}\sqrt{d}$ are

(i) $(r + s\sqrt{d}) + r' + s'^{\sqrt{d}} = (r + r') + (s + s')\sqrt{d}$

(ii) $(r + s\sqrt{d})(r' + s'\sqrt{d}) = (rr' + ss'd) + (rs' + sr')\sqrt{d}$

i.e. $(r + s\sqrt{d})(r' + s'\sqrt{d}) = (r + s\sqrt{d})(r' + s'\sqrt{d})$

$$= r(r' + s'\sqrt{d}) + s\sqrt{d}(r' + s'\sqrt{d})$$

$$= rr' + rs'\sqrt{d} + \quad sr'\sqrt{d} \quad + ss'd.$$

$$= rr' + ss'd + (rs' + sr')\sqrt{d}$$

Numerical Examples

To establish the two operations of addition and multiplication in quadratic fields, we give the following numerical examples.

(A) If addition in $\mathbb{Q}\sqrt{d}$ is defined as follows

$$(r + s\sqrt{d}) + (r' + s'\sqrt{d}) = \quad (r + r') + (s + s')\sqrt{d}$$

then do in $\mathbb{Q}\sqrt{d}$

(1) $\left(\frac{1}{2} + \frac{1}{4}\sqrt{2}\right) + (2 + 3\sqrt{2})$

(2) $(3 + 2\sqrt{2}) + (3 + 2\sqrt{2})$

(3) $(5 + 2\sqrt{5}) + (5 + 2\sqrt{5})$

(4) $(7 + 2\sqrt{2}) + (7 + 2\sqrt{7})$

Solutions

(1) $\left(\frac{1}{2} + \frac{1}{4}\sqrt{2}\right) + (2 + 3\sqrt{2}) = \left(\frac{1}{2} + 2\right) + \frac{1}{4}\sqrt{2} + 3\sqrt{2}$

$$= 2\frac{1}{2} + 3\frac{1}{4}(\sqrt{2} + \sqrt{2}).$$

(2) $(3 + 2\sqrt{2}) + (3 + 2\sqrt{2}) = 6 + 2\sqrt{2} + 2\sqrt{2} = 6 + 4\sqrt{2}$

(3) $(5 + 2\sqrt{5}) + (5 + 2\sqrt{5}) = 10 + 2\sqrt{5} + 2\sqrt{5} + 2\sqrt{5}$

$$= 10 + 4\sqrt{5}$$

Exercise. Do No. (4).

(B) If multiplication in $\mathbb{Q}\sqrt{d}$ is defined by

$$(r + s\sqrt{d})(r' + s'\sqrt{d}) = (rr' + ss'd) + (rs' + sr')\sqrt{d},$$

then do the following multiplication problems.

(1) $\left(\frac{1}{2}+\frac{1}{2}\sqrt{2}\right)(2+3\sqrt{2})$

(2) $(3+2\sqrt{3})(2+3\sqrt{3})$

(3) $(7+7\sqrt{2})(7+\frac{1}{8}\sqrt{2})$

Solutions

(1) $\left(\frac{1}{2}+\frac{1}{2}\sqrt{2}\right)(2+3\sqrt{2}) = \frac{1}{2}(2+3\sqrt{2})+\frac{1}{2}\sqrt{2}(2+3\sqrt{2})$

$$= 1+\frac{3}{2}\sqrt{2}+\sqrt{2}+3$$

$$= 4+\left(\frac{3}{2}+1\right)\sqrt{2}$$

$$= 4+\frac{5}{2}\sqrt{2}$$

(2) $(3+2\sqrt{3})(2+3\sqrt{3}) = 3(2+3\sqrt{3})+2\sqrt{3}(2+3\sqrt{3})$

$$= 6+9\sqrt{3}+4\sqrt{3}+18$$

$$= 24+13\sqrt{3}$$

(3) $(7+7\sqrt{2})\left(7+\frac{1}{8}\sqrt{2}\right) = 7\left(7+\frac{1}{8}\sqrt{2}\right)+7\sqrt{2}\left(7+\frac{1}{8}\sqrt{2}\right)$

$$= 49+\frac{7}{8}\sqrt{2}+49\sqrt{2}+\frac{7}{4}$$

$$= 49\frac{7}{4}+\left(\frac{7}{8}+49\right)\sqrt{2}$$

Exercise. Perform the following multiplication in $Q\sqrt{2}$.

(i) $(3+2\sqrt{5})(2+2\sqrt{5})$

(ii) $\left(\frac{1}{4}+\frac{1}{2}\sqrt{2}\right)(1-3\sqrt{2})$

(iii) $\left(1-\frac{1}{2}\sqrt{2}\right)\left(2-\frac{1}{4}\sqrt{3}\right)$

(iv) $\left(\frac{1}{4}+\frac{1}{8}\sqrt{7}\right)\left(\frac{1}{2}+\frac{1}{3}\sqrt{7}\right)$.

Solutions

(i) $(3+2\sqrt{5})(2+2\sqrt{5}) = 3(2+2\sqrt{5})+2\sqrt{5}(2+2\sqrt{5})$

$$= 6 + 6\sqrt{5} + 4\sqrt{5} + 20$$

$$= 26 + 10\sqrt{5}$$

(ii) $\left(\frac{1}{4} + \frac{1}{2}\sqrt{2}\right)(1 - 3\sqrt{2}) = \frac{1}{4}(1 - 3\sqrt{2}) + \frac{1}{2}\sqrt{2}(1 - 3\sqrt{2})$

$$= \frac{1}{4} - \frac{3}{4}\sqrt{2} + \frac{1}{2} - 3$$

$$= 3\frac{1}{4} - \frac{1}{4}\sqrt{2}$$

(iii) $\left(1 - \frac{1}{2}\sqrt{3}\right)\left(2 - \frac{1}{4}\sqrt{3}\right) = 1\left(2 - \frac{1}{4}\sqrt{3}\right) - \frac{1}{2}\sqrt{3}\left(2 - \frac{1}{4}\sqrt{3}\right)$

$$= 2 - \frac{1}{4}\sqrt{3} = \sqrt{3} + \frac{1}{8} \cdot 3$$

$$= 2 - \frac{1}{4}\sqrt{3} - \sqrt{3} + 3$$

$$= 2\frac{3}{8} - 1\frac{1}{4}\sqrt{3}$$

$$= 2\frac{3}{8} - \frac{5\sqrt{3}}{4}$$

We recall that elements of $\mathbb{Q}\sqrt{d}$ can be denoted by σ and that for any $\sigma \in Q\sqrt{d}, \exists\ \bar{\sigma} \in Q\sqrt{d}$ where for any $\sigma = r + s\sqrt{s},\ \bar{\sigma} = r - s\sqrt{d}.$

Now,

$\sigma\bar{\sigma} = (r + s\sqrt{d})(r - s\sqrt{d})$

$= r(r - s\sqrt{d}) + s\sqrt{d}(r - s\sqrt{d})$

$= rr - rs\sqrt{d} + sr\sqrt{d} - ssd$

$= r^2 - s^2 d$

That is, $\sigma\bar{\sigma} = r^2 - s^2 d;\ \sigma\bar{\sigma}$ is called the norm $N(\sigma)$ of σ. It is clear that $\bar{\sigma}$ is the complex conjugate of σ and $N(\sigma) = \sigma\bar{\sigma} = |\sigma||\bar{\sigma}| = |\sigma|^2$

If $\sigma, \sigma' \in \mathbb{Q}(\sqrt{d})$, then $N(\sigma\sigma') = N(\sigma)N(\sigma')$ and σ is the wit of the monic equation

$$(z-\sigma)(z-\sigma) = z(z-\sigma) - \sigma(z-\sigma)$$
$$= z^2 - z\sigma - z\sigma + \sigma^2$$
$$= z^2 - 2z\sigma + N(\sigma)$$
$$= z^2 - 2rz + N(\sigma) = 0 \qquad (*)$$

Definition. A number $\sigma \in \mathbb{Q}(\sqrt{d})$ is called a quadratic integer if the coefficients $-2r$ and $N(\sigma)$ in the equation $(*)$ are both integers. An easy test for this fact is the following proposition holds:

Proposition. The number $r + s\sqrt{d}$ is a quadratic integer if and only if the following hold:

If $d \equiv 2(mod\ 4)$ or $d \equiv 3(mod\ 4)$, r and s are both integers, or both half integers.

$$\left(r = m + \frac{1}{2},\ \ s = n + \frac{1}{2},\ m, n\ \in \mathbb{Z}\right) \qquad (**)$$

Proof.

Recall the equation

$$(z-\sigma)(z-\bar{\sigma}) = z^2 - \partial rz + N(\sigma). \qquad (*)$$

Where for $\sigma \in \mathbb{Q}\sqrt{d}$ to be a quadratic integer, $-\partial r$ and $N(\sigma)$ in $(*)$ both integers, Since $-2r$ in $(*)$ is an integer, clearly r must be a half integer; hence, r^2 must be an integer or of the form $2k + \frac{1}{4}$, $k \in \mathbb{Z}$.

Since d is a square free integer, S must therefore be an integer or a half integer (whichever r is) to make $N(\sigma) = r^2 - s^2 d$ an integer. In the 2nd case (r and s both half integers) if h is the remainder of $d(mod\ 4)$, then the fractional part of $r^2 - s^2 d$ is $\frac{(1-h)}{4}$, which is an integer precisely when $h = 1$, that is, in the case of $(**)$.

4.0 TUTOR MARKED ASSIGNMENTS (TMAs)

1(a) what do we mean by a square free integer?

(b) Let $\mathbb{Q}\sqrt{d}$ denote a quadratic field, write down a typical elements of $\mathbb{Q}\sqrt{d}$, where d is a square free integer.

2. If $a = (3 - 2\sqrt{5})$, $b = (6 + 3\sqrt{5})$, compute $a + b$.

3. If $a = \frac{1}{4} + \frac{1}{2}\sqrt{2}$ and $b = 1 - 3\sqrt{2}$, computeab.

5.0 SUMMARY

We shall summarize by the re-emphasize the definition and a related proposition thus. A number $\sigma \in \mathbb{Q}(\sqrt{d})$ is called a quadratic integer if the coefficients $-2r$ and $N(\sigma)$ in the equation $(*)$ are both integers. An easy test for this fact is the following proposition holds:

Proposition. The number $r + s\sqrt{d}$ is a quadratic integer if and only if the following hold:

If $d \equiv 2(mod\ 4)$ or $d \equiv 3(mod\ 4)$, r and s are both integers, and both half integers.

$$\left(r = m + \frac{1}{2},\ \ s = n + \frac{1}{2},\ m, n\ \in \mathbb{Z}\right) \qquad (**)$$

6.0 CONCLUSSION

As in the summary.

7.0 REFRENCES AND FURTHER READING

1. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
8. Mathworld contributor Rowland Algebra Field Theory.

MODULE 2

Unit 2.

Cyclotomic Field

1.0 INTRODUCTION

Preamble

(a) Ideal. It is thought fit that certain facts that will help in understanding of cyclotomic fields be established, before going into the topic. The author felt this way because not all the readers may have the prerequisite background.

Let R be a commutative ring with unit element 1. A subset J of R is called an ideal of R if it satisfies the following properties.

(i) If $a, b \in R$, then $a + b \in R$. (ii) If $b \in J, a \in R$, then $ab \in J$. In particular, J is also an additive subgroup of R.

Principal Ideal: If $a \in R$, the ideal, $\{ra | r \in R\}$ of all multiples of a is the principal ideal generated by a, and is denoted by $\langle a \rangle$. An ideal N of R is principal ideal if $N = \langle a \rangle$, for some $a \in R$.

Prime Ideal: An ideal P of R is said to be a prime ideal if satisfies the following properties:

(i) $P \neq R$

(ii) If $ab \in P \Longrightarrow a \in P$ or $b \in P$, for $a, b \in \mathbb{R}$ or equivalently, given two ideals of R, such that $AB \subset D$, then either $A \subset P$ or $B \subset P$.

An idea P of R is said to be maximal if: $P \neq R$ (ii). There exists no ideal J of R such that $P \subset J \subset R$.

2.0 OBJECTIVES

To be taking through what is an ideal, principal ideal, prime ideal, nth root of unity.

To know the definition of Cyclotomic Fields

3.0 MAIN CONTENT

3.1 Primitive nth root of unity.

Let F be a field and, n integer, $n > 0$. An element $x \in F$ such that $x^n = 1 \Longrightarrow x\sqrt[n]{1}$ is called an nth root of unity. The set $W_{n,F}$ of all nth roots of unity in F is a multiplicative group. We denote by W_F the set of all roots of unity in F. That is,

$$W_F = \bigcup_{n \geq 1} W_n, F.$$

Let $x \in W_F$ and let n be the order of x, in the multiplicative group W_F, that is, n is the smallest positive integer such that $x^n = 1$. Then we say that x is a primitive nth root of units.

3.2 Cyclotomic Fields

We shall just give examples of cyclotomic fields so that the reader will understand what is meant by the mathematical structure, cyclotomic fields.

Examples

(i) Let P be a prime number, let $m = P^k > 2$. So if $P = 2$, then $k \geq 2$ since for $P^k > 2$, $k \neq 1$ for $2^1 \not> 2$ i.e. for $m = P^k > 2$, then $k \geq 2$.

(ii) The cyclotomic field, $F = \mathbb{Q}(w)$, generated by a mth root of unity, w, where $m > 2$ is any integer. We can assume that if m is even, then $4/m$ since, $m > 2$. Indeed if $m = 2m'$ where m' is odd, if w' is a primitive m'th root of unity, then $w'^m = 1$, so $w' \in \mathbb{Q}(w)$. On the other hand, $(w'^m)^2 = 1$, so $w'^m = 1$ or $w'^m = -1$. In this case $(-w')^m = -w'^m = 1$ Thus, w or $-w$ belongs to $\mathbb{Q}(w')$.

4.0 TUTOR MARK ASSIGNMENTs (TMAs)

1. Let R be a ring. When is A said to be a left ideal of R? When is A said to be a right ideal of R?
2. Define the terms (a), prime ideal of a ring R, (b), principal ideal of a ring R.
3. Give an example of a cyclotomic field.

5.0 SUMMARY

However, by know you must have been equipped with the following:

The definition of both right and left Ideal of a ring R.

The definition of both prime ideal and principal ideal of a ring R.

and finaly, you must have been aquanted with the definition and example of a cyclotomic field.

6.0 : CONCLUSION

In conclusion, test your comprehension of this module by solving the following QB.

QUESTION BANKS FOR MODULE 2

1. (a) What is a square free integer?

   (b) Give a typical element of a quadratic field.

   (c) If in a quadratic field, $a = \frac{1}{2} + \frac{1}{4}\sqrt{2}$, $b = 2 + 3\sqrt{2}$,

   Compute (i), $a + b$ (ii), ab.

   (d) If in $\mathbb{Q}\sqrt{d}$ multiplication is defined by

$r + s\sqrt{d})(r' + s'\sqrt{d}) = (rr' + ss'd) + (rs' + sr')\sqrt{d}$,

then compute the following:

(i) $(7 + 7\sqrt{d})\left(7 + \frac{1}{8}\sqrt{2}\right)$ (ii) $(3+2\sqrt{3})(2 + 3\sqrt{3})$

2. If the elements of $\mathbb{Q}\sqrt{d}$ can be denoted by σ and that for any $\sigma \in Q\sqrt{d}, \exists\ \bar{\sigma} \in \mathbb{Q}\sqrt{d}$, where for any $\sigma = r + s\sqrt{d}$, $\bar{\sigma} = r - s\sqrt{d}$. Show that $\sigma\bar{\sigma} = r^2 - s^2 d$.

3. (a) What do you mean by an ideal A of a ring, R?

   (b) What do we mean by a principal ideal of a ring, R?

4. (a) Give an example of a cyclotomic field.

   (b) Define each of the following

   (i) nth root of unity. (ii) primitive nth root of unity.

7.0 REFRENCES AND FURTHER READING

1. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
8. Mathworld contributor Rowland Algebra Field Theory.

Module 3: Factorization into irreducible and ideas of Polynomials over a Field

Unit 1: Factorization of Polynomials over a Field

1.0 INTRODUCTION

Polynomials are an extension of quadratics so you may which it useful to review quadratics before reading this section. Also many of the ideas discussed here involve complex numbers so you may want to review those as well.

To create a polynomial imagines carrying out the following steps:

- Start with a variable x.
- Raise x to various integer powers, starting with the power 0 and ending with the power n (where n is a positive integer):

  $1, \quad x, \quad x^2, \quad x^3, \quad \ldots x^n.$

- Multiply each power of x by a coefficient. Let a_3 denote the coefficient of x^3, and so on.
- Add all the terms together.

The result is a **polynomial**. Note that some of the coefficients could be zero so that some of the powers of x could be absent. The formal definition of a polynomial shall be discussed in the main content of this unit.

2.0 OBJECTIVES

(1) Definition of Factorization of polynomials over finite *fields*.

(2) The Primitive element theorem.

(3) Finite separable extensions have a primitive element

3.0 MAIN CONTENTS

3.1 Definition of Polynomial

We begin by defining a polynomial:

Consider an infinite formal sum,

$$a(x) = \sum_{i=1}^{\infty} a_i x^i = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n + \cdots$$

$$= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots$$

with each $a_i \in \mathbb{R}$. This infinite formal sum is called formal power series in x with coefficients in $\mathbb{R}$. The a_i's are called the coefficients of the power series, a_i being called the coefficient of x^i. We denote the set of all such power series, $P[x]$. If we now require that in the infinite formal sum, $a(x) = \sum_{i=1}^{\infty} a_i x^i$, all, but a finite number of the a_i's are zero. Then $a(x)$ is called a polynomial in x with coefficients in $\mathbb{R}$ (it is also called polynomial in x over $\mathbb{R}$), and the element a_i is called the coefficient of x^i. If $a_i = 0$ for $i > n$, $a_n \neq 0$, then $a(x)$ is called a polynomial of degree n and a_n is said to be the leading coefficient of $a(x)$. Then we write, $a(x) = \sum_{i=1}^{n} a_i x^i$ i.e. $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$. a_0 is referred to as the constant of the polynomial. We denote the set of all such polynomials by $P[x]$. The polynomial is called monic if $a_n = 1$.

3.2 Factorization

The basic tool we need to use in this section is Division Algorithm for $f[x]$ where $F[x]$ is the set of polynomials in x over the field, F.

Theorem 3 (Division Algorithm for $F[x]$)

Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + b_{m-2} x^m + \cdots + b_0$$

be two polynomials in $F[x]$, with $a_n \neq 0, b_m \neq 0,$ and $m > n$. Then there exist unique polynomials, $q(x)$, and $r(x)$ in F$[x]$ such that $f(x) = g(x)q(x) + r(x)$, where the degree of r(x) is less than $m =$ degree of $g(x)$.

Remark

(i) We omit the proof as it is found in any standard book in abstract Algebra.

(ii) One can compute $q(x)$ and $r(x)$ in the division algorithm theorem by long division.

We present the following corollaries resulting from the division algorithm theorem

Corollary I: An element $a \in F$ is said to be a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.

Corollary II: A nonzero polynomial, $f(x) \in F[x]$ of degree n can have at most n zeros in a field, F.

Computational Examples

1. Working in $\mathbb{Z}_5[x]$, let $f(x)$, $g(x)$ $\mathbb{Z}_5(x)$ where

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1; g(x) = x^2 - 2x + 3.$$

To find $q(x)$ and $r(x)$ in the theorem, we perform synthetic division: $\frac{f(x)}{g(x)}$

Now,

$$\begin{array}{r} x^2 - x - 3 \\ x^2 - 2x + 3 \quad \overline{)\; x^4 - 3x^3 + 2x^2 + 4x - 1} \\ \underline{x^4 - 2x^3 + 3x^2} \\ -x^3 - x^2 + 4x \\ \underline{-x^3 + x^2 + 4x} \\ -3x^2 + 7x - 1 \\ \underline{-3x^2 + 6x - 9} \\ x + 3 \end{array}$$

$in\ \mathbb{Z}_5[x]$

Thus,

$x^4 - 3x^3 + 2x^2 + 4x - 1 = (x^2 - 2x +)(x^2 - x - 3) + (x + 3)$.

Therefore, $q(x) = x^2 - x - 3$ and $r(x) = x + 3$.

2. Still working in $\mathbb{Z}_5[x]$, we note that 1 is a zero of $x^4 + 3x^3 + 2x + 4 \in \mathbb{Z}_5[x]$.
3. i. e. if

   $f(x) = x^4 + 3x^3 + 2x + 4$,

   Then $f(1) = 0$. i. e. $x = 1$ is a zero which implies that $x - 1$ is a factor of

   $x^4 + 3x^3 + 2x + 4$. **(Corollary I)**

Therefore, to find $q(x)$ and $r(x)$ of the theorem, we divide

$x^4 + 3x^3 + 2x + 4$ by $x - 1$.

$$
\begin{array}{r|l}
 & x^3 + 4x^2 + 4x + 1 = \\
x - 1 & \quad \ldots + 2x + 4 \\
x^4 & -x^3 \\
\hline
 & 4x^3 - 4x^2 \\
\hline
 & \quad 4x^2 - 4x \\
\hline
 & \quad\quad x + 1 \\
 & \quad\quad \underline{} \\
 & 0 \ (in \ \mathbb{Z}_5[x])
\end{array}
$$

Therefore, $x^4 + 3x^3\ 2x + 4 = (x^3 + 4x^2 + 4x + 0)(x - 1) + 0$

Hence, $q(x) = x^3 4x^2 + 4x + 6$, and $r(x) = 0$.

4.0 TUTOR MARK ASSIGNMENT (TMAs)

1. If $f(x)$, of $(x) \in \mathbb{Z}_5[x]$ and $f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$,

   $g(x) = x^2 - 2x + 3$.

   Find polynomials $q(x), r(x) \in \mathbb{Z}_5[x]$ such that

   $x^4 - 3x^3 + 2x^2 + 4x - 1 = g(x)q(x)$ + r(x).

where degree $r(x) <$ degree $g(x)$.

2. When is a polynomials said to be irreducible over $\mathbb{Q}$?
3. State the Eisenstein Theorem with its conditions.

7.0 References and further reading

1. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11

MODULE 2

Unit 2: Factorizing into irreducible

1.0 INTRODUCTION

If F is a field, a non-constant polynomial is **irreducible over F** if its coefficients belong to F and it cannot be factored into the product of two non-constant polynomials with coefficients in F.

A polynomial with integer coefficients, or, more generally, with coefficients in a unique factorisation domain R is sometimes said to be *irreducible over R* if it is an irreducible element of the polynomial ring (a polynomial ring over a unique factorization domain is also a unique factorization domain), that is, it is not invertible, nor zero and cannot be factored into the product of two non-invertible polynomials with coefficients in R. Another definition is frequently used, saying that a polynomial is *irreducible over R* if it is irreducible over the field of fractions of R (the field of rational numbers, if R is the integers). Both definitions generalize the definition given for the case of coefficients in a field, because, in this case, the non constant polynomials are exactly the polynomials that are non-invertible and non zero.

2.0 OBJECTIVE

To know the Define a polynomial in x.

To know Eisenstein Theorem with its conditions

To know when a polynomial is said to be irreducible over Q

3.0 MAIN CONTENT

3.1 Definition: An **irreducible polynomial** may be defined as a non-constant polynomial that cannot be factored into the product of two non-constant polynomials. The property of irreducibility depends on the field and ring to which the coefficients are considered to belong. For example, the polynomial x^2 - 2 is irreducible if the coefficients 1 and -2 are considered as integers, but it factors as [$\left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right)$] if the coefficients are considered as real numbers. One says "the polynomial x^2 - 2 is irreducible over the integers but not over the reals".

A polynomial that is not irreducible is sometimes said to be **reducible**.

Irreducible polynomials appear naturally in polynomial factorisation and algebraic field.

It is helpful to compare irreducible polynomials to prime numbers: prime numbers (together with the corresponding negative numbers of equal magnitude) are the irreducible integers. They exhibit many of the general properties of the concept of 'irreducibility' that equally apply to irreducible polynomials, such as the essentially unique factorization into prime or irreducible factors.

Remark. If $f(x) \in F[x]$ *factors in* $F[x]$ *into* quadratic factors in $F[x]$, then, $f(x)$ has a factorization. If factorization into two quadratic polynomials is not possible, $f(x)$ is said to be irreducible over $\mathbb{Q}$. We state without proof, Eisenstein Theorem which gives conditional criteria for irreducibility.

3.2 Eisenstein Theorem.

Let $p \in \mathbb{Z}$ be a prime. Suppose that

$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_0$ is in $\mathbb{Z}[x]$, and $a_n \neq 0$ (mod p),

but $a_i \equiv 0(modp)$ for $i < n$, with $a_0 \neq 0(modp^2)$. Then $f(x)$ is irreducible over $\mathbb{Q}$. We next give examples, to apply the theorem.

3.3 Examples (application of Eisenstein Theorem)

(i) Show that $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$ is irreducible over $\mathbb{Q}$, taking $p = 3$

Solution

Conditions of the theorem:

(a). $a_n \not\equiv 0(\text{mod}\, p)$

(b). $a_i \equiv 0(\text{mod}\, p^2)$ for, $i < n$,

(c). $a_0 \not\equiv 0(\text{mod}\, p^2)$

Solution

(a) Here $a_n = 25$, and, $25 \not\equiv 0(mod3)$ since $3 \nmid (25 - 3)$.

(b) Here, $a_i < a_n \Longrightarrow a_n \equiv -9, a_3 \equiv 3$

(mod3)

$\Longrightarrow 3 \equiv 0(mod3) since\ 3|(0-3), satisfied.\ a_{0\equiv}\ 0(mod3^2) \Longrightarrow -12 \equiv 0(mod3^2)$

But $a_2 \equiv 0(mod3) \Longrightarrow -9 \equiv 0(mod3) satisfied.$ since 3|3(0 satisfied.

$a_0 \equiv 0(modp^2) \Longrightarrow -12 \equiv 0(mod3^2) \Longrightarrow -12 \not\equiv 0(mod9)$

Because the conditions of the theorem holds, then

$f(x) = 25x^5 - 9x^4 + 3x^2 - 12$

is irreducible over $\mathbb{Q}$.

(ii). Taking $p = 3$, check if $x^2 - 2$ is reducible over Q.

Solution

Here, $a_n = 1, \quad a_0 = -2.$

$a_n \equiv 0(mod3) \Rightarrow 1 \equiv 0(mod3)$, this is not true.

Therefore, $1 \not\equiv 0(mod3)$,

$a_0 \equiv 0(modp^2) \Longrightarrow -2 \equiv 0(mod9)$. This is not true.

Hence $x^2 - 2$ is not reducible over $\mathbb{Q}$.

(iii). Show that through $x^2 - 2$ is irreducible over $\mathbb{Q}[x]$, but reducible over $\mathbb{R}[x]$

Solution (Aliter).

For $(x^2 - 2)$ to be reducible in $\mathbb{Q}$, $x^2 - 2 \in \mathbb{Q}[x]$ has to have zeros in $\mathbb{Q}$.

This shows that $x^2 - 2$ is irreducible over $\mathbb{Q}$. However, $x^2 - 2$ view in $\mathbb{R}[x]$ is reducible over $\mathbb{R}$ since $x^2 - 2$ factors in $\mathbb{R}[x]$ into $(x - \sqrt{2})(x + \sqrt{2})$.

(iv).Theorem cyclotomic polynomial,

$$\mathbb{Q}_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$ for any prime, p.

Proof. We need only to consider factorization in $\mathbb{Z}[x]$.

Let

$$g(x) = \Phi_{(p)}(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + x^{p-2} + \cdots + px}{x}$$

Then,

$$g(x) = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-2} + \cdots + p$$

Satisfies the Eisenstein criterion for any prime p, and is thus irreducible over $\mathbb{Q}$.

But it is clear that if $\Phi_p(x) = h(x)r(x)$ were a nontrivial factorization of $\Phi_p(x)$ in $\mathbb{Z}[x]$. Then $\Phi_p(x+1) = g(x) = h(x+1)r(x+1)$ will give a nontrivial factorization of $g(x)$ in $\mathbb{Z}[x]$. Thus $\Phi_p(x)$ must also be irreducible over $\mathbb{Q}$.

q.e.d

4.0 CONCLUSION

We shall conclude by discussing Schönemann–Eisenstein theorem and the criteria for Direct (without transformation), Indirect (after transformation) and Cyclotomic polynomials in the summary in due course.

5.0 SUMMARY

Suppose we have the following polynomial with integer coefficient.

$$Q = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

If there exists a prime number p such that the following three conditions all applies:

- p divides each a_i for $i \neq n$,
- p does *not* divide a_n, and
- p^2 does *not* divide a_0,

then Q is irreducible over the rational numbers. It will also be irreducible over the integers, unless all its coefficients have a nontrivial factor in common (in which case Q as integer polynomial will have some prime number, necessarily distinct from p, as an irreducible factor). The latter possibility can be avoided by first making Q primitive, by dividing it by the greatest common divisor of its coefficients (the content of Q). This division does not change whether Q is reducible or not over the rational numbers (see primitive part-content factorisation for details), and will not invalidate the hypotheses of the criterion for p (on the contrary it could make the criterion hold for some prime, even if it did not before the division).

Example

Eisenstein's criterion may apply either directly (i.e., using the original polynomial) or after transformation of the original polynomial.

5.1 Direct (without transformation)

Consider the polynomial $Q = 3x^4 + 15x^2 + 10$. In order for Eisenstein's criterion to apply for a prime number p it must divide both non-leading coefficients 15 and 10, which means only $p = 5$ could work, and indeed it does since 5 does not divide the leading coefficient 3, and its square 25 does not divide the constant coefficient 10. One may therefore conclude that Q is irreducible over **Q** (and since it is primitive, over **Z** as well). Note that since Q is of degree 4, this conclusion could not have been established by only checking that Q has no rational roots (which eliminates possible factors of degree 1), since a decomposition into two quadratic factors could also be possible.

5.2 Indirect (after transformation)

Often Eisenstein's criterion does not apply for any prime number. It may however be that it applies (for some prime number) to the polynomial obtained after substitution (for some integer a) of $x + a$ for x. The fact that the polynomial after substitution is irreducible then allows concluding that the original polynomial is as well. This procedure is known as applying a *shift*.

For example consider $H = x^2 + x + 2$, in which the coefficient 1 of x is not divisible by any prime, Eisenstein's criterion does not apply to H. But if one substitutes $x + 3$ for x in H, one obtains the polynomial $x^2 + 7x + 14$, which satisfies Eisenstein's criterion for the prime number 7. Since the substitution is an automorphism of the ring $\mathbf{Q}[x]$, the fact that we obtain an irreducible polynomial after substitution implies that we had an irreducible polynomial originally. In this particular example it would have been simpler to argue that

H (being monic of degree 2) could only be reducible if it had an integer root, which it obviously does not; however the general principle of trying substitutions in order to make Eisenstein's criterion apply is a useful way to broaden its scope.

Another possibility to transform a polynomial so as to satisfy the criterion, which may be combined with applying a shift, is reversing the order of its coefficients, provided its constant term is nonzero (without which it would be divisible by x anyway). This is so because such polynomials are reducible in $R[x]$ if and only if they are reducible in $R[x, x^{-1}]$ (for any integral domain R), and in that ring the substitution of x^{-1} for x reverses the order of the coefficients (in a manner symmetric about the constant coefficient, but a following shift in the exponent amounts to multiplication by a unit). As an example $2x^5 - 4x^2 - 3$ satisfies the criterion for $p = 2$ after reversing its coefficients, and (being primitive) is therefore irreducible in $\mathbf{Z}[x]$.

5.3 Cyclotomic polynomials

An important class of polynomials whose irreducibility can be established using Eisenstein's criterion is that of the cyclotomic polynomials for prime numbers p. Such a polynomial is obtained by dividing the polynomial $x^p - 1$ by the linear factor $x - 1$, corresponding to its obvious root 1 (which is its only rational root if $p > 2$):

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

Here, as in the earlier example of *H*, the coefficients 1 prevent Eisenstein's criterion from applying directly. However the polynomial will satisfy the criterion for p after substitution of $x + 1$ for x: this gives

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

all of whose non-leading coefficients are divisible by p by properties of binomial coefficients, and whose constant coefficient equal to p, and therefore not divisible by p^2. An alternative way to arrive at this conclusion is to use the identity $(a + b)^p = a^p + b^p$ which is valid in characteristic p (and which is based on the same properties of binomial coefficients, and gives rise to the Frobenius endomorphism), to compute the reduction modulo p of the quotient of polynomials:

$$\frac{(x+1)^p - 1}{x} \equiv \frac{x^p + 1^p - 1}{x} = \frac{x^p}{x} = x^{p-1} \pmod{p},$$

which means that the non-leading coefficients of the quotient are all divisible by p; the remaining verification that the constant term of the quotient is p can be done by substituting 1 (instead of $x + 1$) for x into the expanded form $x^{p-1} + \ldots + x + 1$.

6.0 TUTOR MARK ASSIGNMENTs (TMAs)

1. Define a polynomial in x.
2. When is a polynomial said to be irreducible over Q?
3. State the Eisenstein Theorem with its conditions.

4. Define the following**:** Direct (without transformation), Indirect

(after transformation) and Cyclotomic polynomials in the summary in due course.

7.0 **REFERENCES AND FURTHER READING**

8. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
9. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
10. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
11. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
12. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
13. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
14. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
15. wikipedia.org/wiki/Eisenstein's criterion

MODULE 3

Unit 1

Ideals

1.0 INTRODUCTION

An ideal is a subset $\mathrm{I} \in R$ a ring that forms an additive group and has the property such that, whenever $x \in R$ and $y \in \mathrm{I}$, then $xy \in \mathrm{I}$ and $yx \in \mathrm{I}$. For example, the set of even integers is an ideal in the ring of integers Z.

Given an ideal I; it is possible to define a quotient ring(R/I). Ideals are commonly denoted using a Gothic typeface.

2.0: OBJECTIVE

To know the definition of Ideals

To treat the two sided Ideal

3.0 MAIN CONTENT

Definition

Let A be a nonempty subset of a ring, $(R, +, \cdot)$ such that

(i). $(A, +)$ is a subgroup of $(R, +, \cdot)$ i. e. $\forall\, a, b \in A,\ a - b \in A$.

(ii) For any $a \in A, r \in R, ra \in A$.

(iii) For any $a \in A, r \in R, ra \in A$. Then A is called a two sided ideal of R. If only (i) and (ii) hold, A is called a left ideal of R. If (i) and (iii) hold, A is called a right ideal of R. We remark that in a commutative ring, there is no distinction between left and right ideals of a ring R.

A two –sided ideal will just be referred to just as an ideal.

Examples

(i) $\forall\, 0 \in A = \{0\}, 0 - 0 = 0 \in A$. Here $A = \{0\}$ is called a trivial ideal of R.

(ii) R is an ideal of R for $\forall r_1, r_2 \in R, r_1 r_2 \in R$. Again, $r_1 - r_2 \in R$. i. e.,$(R, +)$ is a subgroup of itself. R is also a trivial ideal.

(iii)In $(\mathbb{Z}_n, +, .)$, $3\mathbb{Z}$, is an ideal, for any fixed n $\in \mathbb{Z}$. For if n = 3, $= \{\bar{0}, \bar{1}, \bar{2},\}$ and $\forall$ a, b $\in 3\mathbb{Z}, a - b \in 3\mathbb{Z}$.

(iv)In $M_2(\mathbb{Z})$, let $S = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | a, b \in \mathbb{Z}\right\}$, Check if S is an ideal in $\mathbb{Z}$.

(a) Clearly, S is an additive subgroup of $M_2(\mathbb{Z})$, since $\forall\, s_1, s_2 \in M_2(\mathbb{Z})$, where

$s_1 = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}, s_2 = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}$

Then $s_1 - s_2 \Longrightarrow \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z})$.

(b) Now, in $M_2(\mathbb{Z})$, For any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}), \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in S$,

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ae & ad \\ ce & cd \end{pmatrix} \notin S$ (Not left sided ideal)

But $\begin{pmatrix} e & d \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & f \end{pmatrix} = \begin{pmatrix} ea + dc & eb + df \\ 0 & 0 \end{pmatrix} \in s$ (right sided ideal).

Remark. An ideal is to a ring as a normal subgroup is to a group.

Definition. (Analogue of the definition of a factor group).

If N is an ideal in a ring R, then the ring of cosets, $r + N$ under the induced operations is the quotient ring or factor ring or residue class ring of R modulo N, and is denoted by R/N. The cosets are residue class modulo N.

Consider the ring, $\mathbb{Z}$ of integers. The only additive subgroup of $(\mathbb{Z}, +)$ are the subgroups $n\mathbb{Z}$, since $n\mathbb{Z} \subset \mathbb{Z}$. We next show that this subgroup of $\mathbb{Z}$ is an ideal. If r is any integer, and $m \in n\mathbb{Z}$, then $mr = rm$ is a multiple of n. That is if $m = ns$, then $rm = mr = (ns)^r = n(sr) \in n\mathbb{Z}$. Thus $n\mathbb{Z}$ is an ideal, and the cosets, $a + n\mathbb{Z}$ of $n\mathbb{Z}$ for a ring, $\mathbb{Z}/\, n\mathbb{Z}$ under the induced operations of addition and multiplication.

Example. The subset, $N = \{0,3\}$ of $\mathbb{Z}_6$ is an ideal of $\mathbb{Z}_6$and $\mathbb{Z}_6/N$ has 3 elements:

$0 + N = 0,$

$1 + N = 1, 2 + N = 2.$ (Recall that N is the kernel). We observe that

$\mathbb{Z}_6/N \simeq \mathbb{Z}_3$ with the correspondence$0 + N) \leftrightarrow 0, (1 + N) \leftrightarrow 1, (2 + N) \leftrightarrow 2.$

Theorem: If R is a ring with unity, and N is an ideal of R containing a unit, then $N = R.$

4.0 CONCLUSION

We shall conclude with the following thus:

Definition: Let R be a commutative ring, and Let $a \in R$. The *principal ideal generated by* a is

$$\langle a \rangle = \{ra \mid r \in R\}.$$

Lemma. Let R be a commutative ring, and Let $a \in R$. Then $\langle a \rangle$ is a two-sided ideal in R.

Proof.

First, $0 = 0 \cdot a \in \langle$. If $ra \in \langle a \rangle$, then $-(ra) = (-r)a \in \langle a \rangle$. Finally, if $ra, sa \in \langle a \rangle$, then $ra + sa = (r + s)a \in \langle a \rangle$.

Thus, $\langle a \rangle$ is an additive subgroup of R.

If $ra \in \langle a \rangle$ and $s \in R$, then

$$s(ra) = (sr)a \in \langle a \rangle \quad \text{and} \quad (ra)s = (rs)a \in \langle a \rangle.$$

Therefore, $\langle a \rangle$ is a two-sided ideal.

5.0 SUMMARY

- If R is a ring, an *additive subgroup* of R is a subset of R which is closed under addition, contains 0, and is closed under taking additive inverses.

- A *subring* is a subset S of a ring R which is an additive subgroup of R which is closed under multiplication.

- A *left ideal* is a subset I of a ring R which is an additive subgroup of R such that if $x \in I$ and $r \in R$, then $rx \in I$. A *right ideal* is a subset I of a ring R which is an additive subgroup of R such that if $x \in I$ and $r \in R$, then $xr \in I$. A *two-sided ideal* is a subset I of a ring R which is an additive subgroup of R such that if $x \in I$ and $r \in R$, then $rx, xr \in I$.

- If R is a commutative ring and $x \in R$, the *principal ideal generated by x* is the set

$$\langle x \rangle = \{rx \mid r \in R\}.$$

- An integral domain R is called a *principal ideal domain* (or *PID* for short) if every ideal in R is principal.

  Example.

  (*A principal ideal in the ring of real polynomials*) In $\mathbb{R}[x]$, the following set is an ideal:

  $$\langle x^2 + 4 \rangle = \{(x^2 + 4) \cdot f(x) \mid f(x) \in \mathbb{R}[x]\}.$$

  It's the set consisting of all multiples of $x^2 + 4$. For example, here are some elements of $\langle x^2 + 4 \rangle$:

  $$(2x + 5) \cdot (x^2 + 4), \quad (-\pi x^{50} + \sqrt{2}) \cdot (x^2 + 4), \quad 0 = 0 \cdot (x^2 + 4). \quad \square$$

6.0. TUTOR MARKED ASSIGNMENTs (TMAs)

Let R be a ring. Define an ideal N of R. Hence show that the subset $N = \{0,3\}$ of $\mathbb{Z}_6$ is n ideal of $\mathbb{Z}_6$

7.0 REFRENCES AND FURTHER READING

1. Eynden, C.U. (2001). Elementary Number Theory, McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
8. http://sites.millersville.edu/bikenaga/abstract-algebra-1/ideal/ideal.html

MODULE 3

Unit 2: Class Group and Class Number

1.0 INTRODUCTION

Let K be a number field, then each fractional ideal $I$of K belongs to an equivalence class $[I]$consisting of all fractional ideal Jsatisfying $I = \alpha J$for some nonzero element $\alpha$of K. The number of equivalence classes of fractional ideal of K is a finite number, known as the ''**CLASS NUMBER''** of K. Multiplication of equivalence classes of fractional ideals is defined in the obvious way, i.e., by letting $[I]\,[J] = [I\,J]$. It is easy to show that with this definition, the set of equivalence classes of fractional ideals form an Abelian multiplicative group, known as the ''**CLASS GROUP**'' of K.

2.0 OBJECTIVE

To know the definition of class groups and class numbers.

To know the definition of (Discriminant)

3.0 MAIN CONTENT

3.1 Definition: Class Groups and class Numbers.

We need to give definitions of certain terms in order to be able to define what is meant by class groups and their class numbers.

(a) Definition (Discriminant).

Let $D_0 \neq 1$ be a square free integer and set

$$\Delta_0 = \begin{cases} D_0 & \text{if } D \equiv 1 (\text{mod } 4) \\ 4D_0 & \text{otherwise} \end{cases}$$

Then Δ_0 is called a fundamental discriminant with associated radicand Δ_0. Let $f_\Delta \in N$ and set $\Delta = f^2\Delta$. Then

$$\Delta = \begin{cases} D & \text{if } D \equiv 1 (\text{mod } 4) \\ 4D & \text{otherwise} \end{cases}$$

is a discriminant with conductor f_Δ, and associated radicand

$$\mathrm{D} = \begin{cases} f_\Delta^2 \Delta_0 & \text{if } \Delta \not\equiv 1 \pmod 4 \text{ or } f_\Delta \text{ is odd} \\ 4D & \text{otherwise} \end{cases}$$

having underlying fundamental Δ_0 with associated fundamental radicand D_0.

(b) Let Δ be a discriminant . A fractional $\mathcal{O}_A$-ideal is a set of the form $\alpha I = \{\alpha\beta : \beta \in I\}$, where I is the ideal, for some nonzero $\alpha \in \mathbb{Q}(\sqrt{\Delta})$ and some nonzero $\mathcal{O}_A$-ideal I, fractional $\mathcal{O}_A$-ideals and called invertible if there is another ideal I^{-1} such that $II^{-1} = \mathcal{O}_A$.

Example: If $\Delta = 1234 = 2^3 \cdot 3^2 \cdot 17$, $D = 306 = 2 \cdot 3^2 \cdot 17$, $D_0 = 34$, $\Delta_0 = 2^3 \cdot 17$, $f_\Delta = 3$, the conductor. Also $\mathcal{O}_A = [1 + \sqrt{306} - \text{ideal}$, $I = [9, 6 + \sqrt{306}]$.

Check if the ideal, I is invertible.

Solution. It will be invertible if $\exists$ another ideal I such that $II^{-1} = \mathcal{O}_A$.

We will note that $I^{-1} = \left(\frac{1}{9}\right) I'$ and $II' = \left[3, \sqrt{306}\right) \neq \mathcal{O}_A$.]

Therefore, the ideal $I = [3, 6 + \sqrt{300})]$ is not invertible.

Definition. Let Δ be a discriminant and let $I(\Delta)\mathcal{O}_A$. $I(\Delta)$ forms a group under multiplication. The principal $\mathcal{C}_\Delta = I(\Delta)/P(\Delta)$, called the ideal class group of $\mathcal{O}_A$ with cardinality, h_Δ called the number of $\mathcal{O}_A$.

3.2 Formula for Class Numbers of Quadratic Orders

If $\Delta > 1$is the conductor of an order $\mathcal{O}_A$ with fundamental discriminant Δ_0, class number h_{Δ_0}, are unit index u, then

$h_\Delta = h_{\Delta_0} \psi_{\Delta_0} f(\Delta)/U$, where $f(\Delta)$ is the conductor for associated with Δ,

$$\psi\Delta_0(f\Delta) = f\Delta \prod_{p/f_\Delta} \left(1 - \frac{\Delta_0/P}{P}\right)$$

with $(*/*)$ being the Kronecker symbol, and with the product ranging over all distinct

prime factors of f_Δ. Also if $\Delta < 0$, then $U = 1$ unless $\Delta_0 = -4$, in which case, $U = 2$ or $\Delta_0 = -3$ for which $U = 3$. It also follows that $h_\Delta = h\Delta_0$. Indeed $h_\Delta \geq h\Delta_0 \in \mathbb{Z}$.

Example. If $\Delta = 6317 = 3^2 \cdot 7013$, then $f_\Delta = 3$ and

$$\psi\Delta_0(f\Delta) = 3 \cdot \left(1 - \frac{(7013/3)}{3}\right) = 4.$$

since the Kronecker symbol, $7013/3 = -1$. Also, the fundamental unit

$\varepsilon\Delta_0 = \left(257428 + 3074\sqrt{7013}\right)/2$

and

$\varepsilon\Delta = 219580178991637906729 7 + 87401716233914438 32\sqrt{63117} = \varepsilon_{\Delta_0}^4$

Therefore, the unit index, $U = 4$, since $h_{7013} = 1 = h_{\Delta_0}$, then $h_{\Delta_0}\psi\Delta_0(f\Delta)/U = 1$.

Exercises

1. Distinguish between class group and class number.
2. When is an ideal I called invertible?

4.0 SUMMARY

In mathematics, the **Gauss class number problem** (**for imaginary quadratic fields**), as usually understood, is to provide for each $n \geq 1$ a complete list of imaginary quadratic fields with class number n. It is named after the great mathematician Carl Friedrich Gauss. It can also be stated in terms of discriminants. There are related questions for real quadratic fields and the behavior as $d \to -\infty$.

The difficulty is in effective computation of bounds: for a given discriminant, it is easy to compute the class number, and there are several ineffective lower bounds on class number (meaning that they involve a constant that is not computed), but effective bounds (and explicit proofs of completeness of lists) are harder.

Contents

5.0 CONCLUSION

We shall conclude thus.

Lists of discriminants of class number 1

For more details on this topic, see Heegner number.

For imaginary quadratic number fields, the (fundamental) discriminants of class number 1 are:

$$d = -3, -4, -7, -8, -11, -19, -43, -67, -163.$$

The non-fundamental discriminants of class number 1 are:

$$d = -12, -16, -27, -28.$$

Thus, the even discriminants of class number 1, fundamental and non-fundamental (Gauss's original question) are:

$$d = -4, -8, -12, -16, -28.$$

6.0 TUTOR MARK ASSIGNMENTs (TMAs)

1(a) Distinguish between a polynomial in x and a formal power series in x.

(b) Give an examples of each of the following polynomials in x.

(i) $P_2[x]$ (ii) $P_3[x]$ (iii) $P_5[x]$ (iv) $P_n[x]$

2. Working in $\mathbb{Z}_5[x]$, let $f(x), g(x) \in \mathbb{Z}_5[x]$, where fd []zd l e

$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1;\ g(x) = x^2 - 2x + 3.$

Then find $q(x)$, and $r(x)$ such that

$f(x) = g(x)q(x) + r(x)$, With the degree of $r(x)$ being less than the degree of $g(x)$.

3.0When is a polynomial in x reducible over Q? Hence, state the Eistenstein Theorem

4. Without proof. State the distinguishing conditions of the theorem. Hence, using the distinguishing conditions, show that $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$ is irreducible over Q.
5. Taking $P = 3$ check if $x^2 - 2$ is reducible over Q.
6. Show that the subset $N = \{0, 3\}$ of $\mathbb{Z}_6$ is an ideal of $\mathbb{Z}_6$, and that $\mathbb{Z}_6/N$ has 3 elements.
7. Recall that $\mathbb{Z} + \mathbb{Z}$ is an analogue of $\mathbb{Z} \times \mathbb{Z}$. Then show that $\mathbb{Z} + \mathbb{Z}$ is not an integral domain by showing that (0,1) and (1,0) are proper zero divisors.

7.0: REFERENCES AND FURTHER READINGS

1. Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
2. Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
3. Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
4. Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
5. MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
6. Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
7. Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11

Module 4:

Fermat's Last Theorem, Dirichilet Theorem and Minkowski Theorem

Unit 1.

1.0: INTRODUCTION

In number theory, **Fermat's Last Theorem** (sometimes called **Fermat's conjecture**, especially in older texts) states that no three positive integers *a*, *b*, and *c* satisfy the equation $a^n + b^n = c^n$ for any integer value of *n* greater than two. The cases $n = 1$ and $n = 2$ are known to have infinitely many solutions since antiquity.

This theorem was first conjectured by Pierre de Fermat in 1637 in the margin of a copy of Arithmetica where he claimed he had a proof that was too large to fit in the margin. The first successful proof was released in 1994 by Andrew Wiles, and formally published in 1995, after 358 years of effort by mathematicians. The unsolved problem stimulated the development of algebraic number theory in the 19th century and the proof of the modularity theorem in the 20th century. It is among the most notable theorems in the history of Mathematics and prior to its proof it was in the Guinness Book of Records as the "most difficult mathematical problem", one of the reasons being that it has the largest number of unsuccessful proofs.

2.0: OBJECTIVE

To know the history of Fermat's Last Theorem**,**

To know the definitions of Fermat's Last Theorem**,**

The show that the equation $x^4 + y^4 = z^4$ has no solution in positive integers

3.0: MAIN CONTENT

3.1 Fermat's Last Theorem

Definition

Fermat's Last Theorem says that for $n > 2$, the equation

$$x^n + y^n = z^n \qquad (1)$$

has no solution in positive integers x, y, z. The theorem is an example of a Diophantine equation which is a type of equations in which integral (or sometimes, rational) solutions

are desired. If $n = 2$, we can find solutions to (1), for example, $x = 3, y = 4, z = 5$ satisfy the equation since

$3^2 + 4^2 = 5^2$ *i.e.* $9 + 16 = 25.$

Similarly, $x = 12,\ y = 5,\ z = 13$ satisfy the equation. But when $n > 2$, the story is different. Many attempts of the proof of the Theorem has been made since the problem arose over 200 years ago. Mathematicians proved the theorem for particular values of n and by the 1990s all values up to more than 100,000 had been accounted for. As one of the many proofs that has been offered in the past, we reproduce the following for the case $n = 4$, in the Fermat's Last Theorem. The proof will use the analysis of Pythagorean triples.

Theorem:

The equation,

$x^4 + y^4 = z^4$ (2)

has no solution in positive integers.

This implies that $k = 4$ case of Fermat's Last Theorem, since if (2) had a solution with $k = 4$, then setting $w = z^2$ would satisfy (2).

Proof. We start by showing that if equation (2) has a solution in positive integers x, y and z, then it has another solution X, Y, W in positive integers with $W < w^2$.

Case 1: Some prime p divides all x, y and w.

Then p divides $x^4 + y^4 = w^4\ (*), from$ which we see that p^2 divides w. Thus

$$\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{w}{p^2}\right)^4$$

and so, $X = \frac{x}{p}$, $Y = \frac{y}{p}$, $W = \frac{x}{p^2}$ is another solution with $W < w$.

Lemma 1. If (x, y, z) is a primitive Pythagorean triple, x, y and z are relatively prime in pairs, one of x and y even ands the other odd, and z is odd.

Case 2: No prime divides all of x, y and w. Then, since

$(x^2)^2 + (y^2)^2 = w^2$ (3)

x^2, y^2 and w from a primitive Pythagorean triple. By Lemma 1, we conclude that x^2, y^2 and w (and so x, y and w) are relatively prime in pairs, that exactly one of x^2 and y^2 is even and that w is odd. Let us assume that x^2 is even. So that x is even and y is odd. Then by Pythagorean triple theorem applied to (3), there exists) relatively prime positive integers u and v such that $x^2 = 2uv, y^2 = u^2 - v^2$ and $w = u^2 + v^2$.

We now apply the same theorem to the equation $y^2 + v^2 = u^2$. We see that y, u and v form another primitive Pythagorean triple, and since we know that y is odd, we must have v even and u odd. Thus there exist relatively prime positive integers v and s such that

$y = r^2 - s^2,\ v = \partial rs,$ and $u = r^2 + s^2.$

Now, since $\left(u, \frac{v}{2}\right) = 1$, by considering the prime factorization of both sides of the equation

$\left(\frac{x}{p}\right)^2 = u\left(\frac{v}{2}\right)$, we see that there must exist positive integers W and Z such that $U = W^2$ and $\frac{v}{2} = Z^2$. In the same way, since $(r, s) = 1$ from the equation $rs = \frac{v}{2} = Z^2$. In the same way, positive integers X and Y such that $r = X^2$ and $s = Y^2$.

Now, we have

$$X^4 + Y^4 = r^2 + s^2 = U = W^2 \qquad (4)$$

where X, Y and W are positive integers. Also

$w = u^2 + v^2 = W^4 + V^2 > W^4 \geq W.$

From equation (4), we see we have another solution to equation (*) with $W < w$ as claimed at the beginning of the proof. This concludes Case 2.

So far, our argument has been entirely positive. We showed that given a solution x, y, w to equation (*) in positive integers, then we can find another solution X, Y, W also in positive integers, with $W < w$. But we need not stop there. From X, Y and W, we could create a third solution, say X', Y', W'. In fact, given just one solution, we could find an infinite sequence of solutions with $w > W > W' > W'' > \cdots > 0$.

This is clearly impossible, since one cannot have an infinite decreasing sequence of positive integers. Thus no solution can exist.

Many attempts at solving the problem were successfully made until 1994 when Wiles apparently found s solution. At present, it seems generally accepted that Fermat's Last Theorem has been proved.

4.0 SUMMARY

Around 1637, Fermat wrote in the margin of a book that he could prove this deceptively simple theorem. His claim was discovered after his death some 30 years later. No proof by Fermat was ever found. This claim, Fermat's Last Theorem, stood unsolved in mathematics for the following three and a half centuries.

The claim eventually became one of the most notable unsolved problems of mathematics. Attempts to prove it prompted substantial development in number theory, and over time Fermat's Last Theorem gained prominence as an unsolved problem in Mathematics. It is related to the Pythagorean theorem, which states that $a^2 + b^2 = c^2$, where a and b are the lengths of the legs of a right triangle and c is the length of the hypotenuse.

The Pythagorean equation has an infinite number of positive integer solutions for a, b, and c; these solutions are known as Pythagorean triples. Fermat stated that the more general equation $a^n + b^n = c^n$ had no solutions in positive integer, if n is an integer greater than 2. Although he claimed to have a general proof of his conjecture, Fermat left no details of his proof apart from the special case $n = 4$.

5.0 CONCLUSION

We shall conclude with the Definition of Fermat's Last Theorem says that for $n > 2$, the equation $x^n + y^n = z^n$

has no solution in positive integers x, y, z. The theorem is an example of a Diophantine equation which is a type of equations in which integral (or sometimes, rational) solutions are desired. If $n = 2$, we can find solutions to (1), for example, $x = 3, y = 4, z = 5$ satisfy the equation since

$3^2 + 4^2 = 5^2$ *i.e.* $9 + 16 = 25.$

Similarly, $x = 12,\ y = 5,\ z = 13$ satisfy the equation. But when $n > 2$, the story is different.

7.0 REFERENCES AND FURTHER READING

- Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
- Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
- Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
- Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
- MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
- Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
- Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
- *https://en.wikipedia.org/wiki/**Class_number**_problem* wikipedia

- Singh, pp. 18–20.
- *"Science and Technology". The Guinness Book of World Records. Guinness Publishing Ltd. 1995.*

MODULE 4

Unit 2.

1.0 INTRODUCTION

In number theory, **Dirichlet's theorem on Diophantine approximation**, also called **Dirichlet's approximation theorem**, states that for any real number α and any positive integer N, there exists integers p and q such that $1 \leq q \leq N$ and

$$|q\alpha - p| < \frac{1}{N}$$

This is a fundamental result in **Diophantine approximation**, showing that any real number has a sequence of good rational approximations: in fact an immediate consequence is that for a given irrational α, the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

is satisfied by infinitely many integers p and q. This corollary also shows that the Thue-Siegel- Roth theorem, a result in the other direction, provides essentially the tightest possible bound, in the sense that the limits on rational approximation of algebraic numbers cannot be improved by lowering the exponent 2 + ε beyond 2.

2.0: OBJECTICES

To know the history of **Dirichlet** Theorem**,**

To know the definitions of **Dirichlet and Minkowski's Theorem,**

To know the Diophantine equation,

To know For what values of x, y, z does the equation, $x^2 + y^2 = z^2$ for $x, y, z \in \mathbb{N}$.

3.0 MAIN CONTENTS

3.1: Dirichlet and Minkowski's Theorem

3.1.1 Dirichlet's Theorem.s

Definition

If a and b are relatively prime (i.e. $(a,b)=1$), then the infinite arithmetic progression $a, a+b, a+2b, a+3b, a+4b, \ldots$ contains infinitely many primes. Unlike Fermat's last theorem that has been proved. Dirichlet Theorem is one of the unanswered questions. We can illustrate the theorem with a few examples.

(a) take 2 primes and such that $(a,b)=1$, i.e. a and b are relatively prime or coprime. e.g. $(2,3)=1$. Then the sequence that follows contains infinitely many primes.

$a, a+b,\ a+2b,\ a+3b,\ a+4b, a+5b, \ldots$

(b) Now that $a=2,\ b=3$, we have

$1,\ 5,\ 8, 11, 14, 17, 20, 23, 26, 29, 32, 35, \ldots$

(c) For $(3,10)=1$, the sequence is as follows: $3, 13, 33, 43, 53, 63, 73, 83$.

(d) $a=5, b=7$, then $(a,b)=1 \implies (5,7)=1$. Hence the sequence is as follows:

$5, 12, 19, 26, 33, 44, 47, 54, 61, 68, \ldots$

3.1.2: Minkowski's Theorem

We just state without proof, the Minkowski's Theorem, as the mechanics required of its proof is beyond this course. It may be left for algebraic number theorists.

Minkowski's Theorem. Let Λ be a lattice in $\mathbb{R}^n$ $(n \geq 1)$, and let μ be the volume of the fundamental parallelotope of Λ. If S is a symmetric convex body having volume, $\mathrm{Vol}(s) > 2^n\mu$, it can only be said that there is a point of Λ, distinct from the origin, which is in S (but not necessarily in the interior of S).

4.0: SUMMARY

In summary The simultaneous version of the Dirichlet's approximation theorem states that given real numbers $\alpha_1, \ldots, \alpha_d$ and a natural number N then there are integers $p_1, \ldots, p_d, q \in \mathbb{Z}, 1 \leq q \leq N$ such that $\left|\alpha_i - \frac{p_i}{q}\right| \leq \frac{1}{qN^{1/d}}$.

PROOF

This theorem is a consequence of the pigeonhole principle.Peter Gustav. Lejeune Dirichlet who proved the result used the same principle in other contexts (for example, the Pell equation)) and by naming the principle (in German) popularized its use, though its status in textbook terms comes later.The method extends to simultaneous approximation.

Another simple proof of the Dirichlet's approximation theorem is based on Minkowski's Theorem applied to the set $S = \left\{(x, y) \in \mathbb{R}^2; -N - \frac{1}{2} \leq x \leq N + \frac{1}{2}, |\alpha x - y| \leq \frac{1}{N}\right\}$. Since the volume of S is greater than 4, Minkowski's Theorem establishes the existence of a non-trivial point with integral coordinates. This proof extends naturally to simultaneous approximations by considering the set:

$$S = \left\{(x, y_1, \ldots, y_d) \in \mathbb{R}^{1+d}; -N - \frac{1}{2} \leq x \leq N + \frac{1}{2}, |\alpha_i x - y_i| \leq \frac{1}{N^{1/d}}\right\}$$

5.0: CONCLUSION

In Mathematics, **Minkowski's theorem** is the statement that any convex set in $\mathbf{R}^n$ which is symmetric with respect to the origin and with volume greater than 2^n d(L) contains a non-zero lattice point. The theorem was proved by Hermann Minkowski in 1889 and became the foundation of the branch of number theory called the geometry of numbers.

6.0 TUTOR MARK ASSIGNMENTs (TMAs).

1. State the Fermat's Last Theorem. What is an open problem? Is the Fermat's Last Theorem still an open problem? If not, when and by whom was the theorem proved?
2. What is a Diophantine equation?
3. For what values of x, y, z does the equation, $x^2 + y^2 = z^2$ for $x, y, z \in \mathbb{N}$.
4. (a) State the Dirichlet Theorem. Illustrate with (i) $(2,3) = 1$, (ii) $(3,10) = 1$, (iii) $(3,5) = 1$, (iv) $(4,5) = 1$.

   (b) Is the Dirichlet Theorem an open problem?

7.0 REFERENCES AND FURTHER READING

- Eynden, C.U. (2001). Elementary Number Theory. McGraw-Hill, Madrid, p.202; pp. 252-253.
- Fraileigh, J.B. (1977). First Course in Abstract Algebra. Addison-Wesley, Ibadan. pp. 232-233.
- Herstein, I.N. (1964). Topics in Algebra. Blaisdell. Toronto, pp. 123; 165; 117; 97; 188, 248; 318; 327.
- Kuku, A.O. (1982). Abstract Algebra. Ibadan University Press, Ibadan, pp. 163-175; 178-181; p.317,295.
- MacLane, S. (1967). Algebra. Macmillan London, pp. 118-165.
- Mollin, R.A. (1998). Fundamental Number Theory with Applications. C.R.C. Press, New York, pp. 341-360.
- Ribenbom, P. (1972). Algebraic Number Theory. John Wiley & Sons Inc. New York, pp. 265; 77; 85; 12; 11
- *https://en.wikipedia.org/wiki/**Class_number**_problem* wikipedia