College of Natural and Computational Sciences

Department of Mathematics

Senior Project on Field

Prepared by: Getahun Hordofa(NCSR/190/10)

Advisor: Kassahun Tesfaye (Ass. Prof.)

A Senior project submitted to the Department of Mathematics, Wolkite University in partial fulfillment of the requirements of the Bachelor of Science Degree in Mathematics

December, 2020

Contents

Wolkite University

Department of Mathematics

The undersigned hereby certify that they have read and recommend to the Department of Mathematics for acceptance of a project entitled **Field** by Student Getahun Hordofa in partial fulfillment of the requirements for the degree of Bachelor of Science.

Dated: December, 2020

Advisor: _____

Advisor name

Examining committee: _____

_____

December, 2020

Acknowledgment

First of all, I would like to thank our almighty Gog for the success of my project work.Actually, my project comes in to its present look with the help of different people. I would like to thank all those who help me in my project work first and for most, my deep and heartfelt appreciation goes to my advisor Kassahun Tesfaye(Ass.Prof.);for incessant support and assistance. Especially their suggestion were priceless and helpful. Next to this, I would like to express my great and acknowledgment to my families for their support by financially and in my manner. I am also extending heartfelt to thank all mathematics teachers especially Algebra streams in Wolkite University for their cooperation and accepting student's idea for their helping with guidance great deal of support in order to make successful completion of this project work.

Abstract

This project contains two chapters,the first chapter is about preliminary concepts, the second chapter is about field. more general the first chapter contains specially definition terms, the second chapter contains basic definition of field with axioms,examples and its properties, theorem and corollary with their proof. finally this paper contains the general conclusion and reference.

Notations(Symbols)

F	Non empty set
R	The set of real number
Z	Set of integers number
Q	Set of rational number
C	Set of complex number
E	Field extension
$\neq$	Not equal to
$\in$	Elements of
$\cdot$	Multiplication
$+$	Addition
*	Any binary operation

Introduction

In mathematics, a Field is a set on which addition, subtraction, multiplication, and division are defined and behave as the corresponding operations on rational and real numbers satisfying certain axioms. A field is thus a fundamental algebraic structure which is widely used in algebra, number theory, and many other areas of mathematics. The best known fields are the field of rational numbers, the field of real numbers and the field of complex numbers. Many other fields, such as field of rationals functions, algebraic function fields, algebraic number fields, are commonly used and studied in mathematics, particularly in number theory and geometry. Most cryptographic protocols rely on finite fields, such that fields with finitely many elements. field serves as foundational notions in several mathematical domains.this includes different branches of mathematical analysis,which are based on fields with additional structure.basic theorems in analysis hinge on the structural properties or the field or real numbers.most importantly for algebraic purposes,any field may be used as the scalars for a vector space,which is the standard general context for linear algebra.number fields,the siblings of the field of rational numbers,are studied in depth in number theory.function fields can help describe properties of geometric objects.

Chapter 1

Preliminaries

We can see here that is some basic definition terms.

1.1 Binary Operation

Binary operation :A word "binary" means composed of two pieces.

Binary operation is an operation that applies to two quantities or expressions.

Definition (1.0)

A binary operation on a set is a calculation involving two elements of the set to produce another element of the set.

Note: A binary operation $*$ on a set S is a function mapping S $\times$ S into S. For each (a, b) $\in S \times S$, we denote the element $*$((a, b)) of S by $a * b$.

Closed

A binary operation $*$ on S is closed if for each pair of elements of S the element assigned to it is again in S.

Such that, $\forall$ a, b $\in S$, then $a * b \in S$.

Associativity

A binary operation $*$ on S is associative if $\forall$a, b, c $\in$ S,then $(a * b) * c = a * (b * c)$

Commutativity

A binary operation $*$ on S is commutative if $\forall$a, b $\in$ S, then $a * b = b * a$

Identity

If $*$ is a binary operation on S, an element e $\in$ S is an identity element of A with respect to $*$ if $\forall$a $\in$S,then

$a * e = e * a = a$

Inverse

Let $*$ be a binary operation on S with identity e, and let a$\in$ S. We say that a is invertible with respenct to $*$ if $\exists$ b$\in$ S such that $a * b = b * a = e$ If b exists, we say that b is an inverse of a with respect to $*$ and write b = a^{-1}.

Distribution of multiplication over addition

Note that:i. If a binary operation is addition (+), then the identity element is zero(0).
ii. If a binary operation is multiplication ($\cdot$), then the identity element is one(1).

1.2 Ring

: A ring $(R, \bigoplus, \bigodot)$ is a set R together with binary operations + and $\cdot$, which we call addition and multiplication,defined on R such that the following axioms are satisfied:

1. $(R, \bigoplus)$ is an abelian group.

   i. Closed

   $\forall$ a,b$\in$ $R, then\ sum\ of\ a + b$ is contained in R.

   ii. Associativity

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

   iii. Existence of Identity

   There exists an element $0 \in R, such\ that\ a + 0 = 0 + a = a\ for\ all\ a \in R$.

   iv.Existence of Inverses

   For any a $\in$ $F, there\ exists\ b \in R\ such\ that\ a + b = b + a = 0$.The element b is called the additive inverse of a and written a^{-1}

   v. Commutativity

   For all a,b $\in$ $R, a + b = b + a$

2. Multiplication is associative.

   For any a,b,e $\in$ $R, then (a + b) + c = a + (b + c)$

3. $\forall$ a,b,c $\in R$, then the distribution law is holds.

   i. $a \cdot (b + c) = a \cdot b + a \cdot c$ Left distribution and

   ii. $(a + b) \cdot c = a \cdot c + b \cdot c$ Right distribution.

   A ring in which the multiplication is a commutative is a commutative ring.

   A ring with a multiplicative identity element is a ring with unity; the multiplicative element 1 is called Unity.

Example 1,

Show that $(Z, \bigoplus, \bigodot)$ is a ring.

Solution

Axiom(1)

first I show that,if it is an abelian group.

i. $\forall$ a,b$\in Z$, then

a+b $\in Z$ is closed.

ii. $\forall$ a,b,c $\in Z$, then

(a+b)+c=a + (b + c) is associativity.

iii. $\forall$ 0 $\in Z$, then

a+0 =a=0+a such that $a \in Z$, existence of identity.

iv. $\forall$ a $\in Z$, then

$\exists b \in Z$,such that a+b=0=b+a existence of inverses

The element b is called the additive inverse of a and written a^{-1}

v. $\forall$ a,b$\in Z$, then

a+b=b+a is commutativity.

Form (i) to (v) Z is an abelian group.

Axiom(2)

$\forall$ a,b,c $\in Z$, then

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ is a multiplication associative.

Axiom(3)

$\forall$ a,b,c $\in Z$, then the distribution law is holds.

i. $a \cdot (b + c) = a \cdot b + a \cdot c$ Left distribution and

ii. $(a + b) \cdot c = a \cdot c + b \cdot c$ Right distribution.

Therefore, form axioms(1) to axioms(3) above $(Z, \bigoplus, \bigodot)$ is a Ring.
In short $(Z, \bigoplus, \bigodot)$, $(Q, \bigoplus, \bigodot)$, $(R, \bigoplus, \bigodot)$, $(Z_5, \bigoplus_5, \bigodot_5)$, and $(C, \bigoplus, \bigodot)$ is a ring.

1.3 Types of Ring

Some types of ring are:

1. **Null ring**:The singleton (0) with binary operation addition and multiplication is defined by 0+0 and $0 \cdot 0 = 0$ is a ring called the zero ring or null ring.

2. **Commutative ring**:A ring in which the multiplication is commutative is called commutative ring.

3. **Ring with unity**:A ring with a multiplicative identity element is a ring with unity; the multiplicative identity element 1 is called "unity."

4. **Ring with zero divisor**:Let R be a ring with unity $1 \neq 0$. An element u in R is a unit of R if it has a multiplicative inverse in R. If every nonzero element of R is a unit, then R is a division ring.

Integral Domain

Definition (1.1)

A commutative ring R with unity $1 \neq 0$ that has no zero divisors is an Integral Domain.

Examples 2,

Solution

$(Z_2, \bigoplus_2, \bigodot_2)$ is a an integral domain.

because, for $1 \in Z_2$ such that, $1 \cdot 1 = 1$

1 is the unity element of Z_2.

$\implies$ Z_2 has no zero divisors

Therefore, Z_2 is integral domain under binary operation addition and multiplication.

Theorem (1.0)

If R is a ring with additive identity 0, then for any a,b $\in R$ we have

1. 0a = a0 = 0
2. a(-b) = (-a)b = -(ab)
3. (-a)(-b) = ab

proof

For Property 1, note that by axioms 1 and 2,

a0 + a0 = a(0 + 0) = a0 = 0 + a0.

Then by the cancellation law for the additive group (R,+), we have a0 = 0. Likewise,

0a + 0a = (0 + 0)a = 0a = 0 + 0a

$\Longrightarrow$ 0a = 0

For Property 2,

we must remember that, by definition, —(ab) is the element that when added to ab gives 0. Thus to show that a(—b) = —(ab),

we must show precisely that a(—b) + ab = 0. By the left distributive law,

a(-b) + ab = a(-b + b) = a0 = 0,

since a0 = 0 by Property (1) Likewise,

(-a)b + ab = (-a + a)b = 0b = 0.

For Property 3, note that

(-a)(-b) = -(a(-b))

by Property (2),

-(a(-b)) = -(-(ab)),

and —(—(ab)) is the element that when added to —(ab) gives 0.

This is ab by definition of —(ab) and by the uniqueness of an inverse in a ring.

Thus, (—a)(—b) = ab.

1.4 Algebraic and Transcendental numbers

Definition (1.2)

• A number $\alpha \in$C is called algebraic number if there is a non-zero polynomial f(x) for any f(x) $\in$Q[X] with f(α) = 0.

• A transcendental number is a number that is not an algebraic number is, or not a root (such that, solution) of a nonzero polynomial equation with integer coefficients.

Chapter 2

Field

2.1 Definition and Example of Field

Informally

Field is a set, along two operations defined on the set:an addition operation written as $a+b$, and a multiplication operation written as $a \cdot b$, both of which behave similarly as they be have for rational numbers and real numbers.

Formally

Field is nonempty set F, containing at least two operations, which denoted by + and $\cdot$ (called addition and multiplication, respectively) are defined, which satisfy the following axioms.

1. **Closure under Addition**

   $\forall$x,y$\in F, the\ sum\ x+y$ is contained in F.

2. **Associativity of Addition**

   $\forall$ x,y,z $\in F, (x+y)+z = x+(y+z)$.

3. **Additive Identity**

   There exists an element $0 \in F, such\ that\ x+0=0+x=x\ for\ all\ x \in F$.

4. **Additive Inverses**

   $\forall$ x $\in F, there\ exists\ y \in F\ such\ that\ x+y=y+x=0$, The element y is called

the additive inverse of x and written x^{-1}.

5. **Commutativity of Addition**

   $\forall$ x,y $\in F, x + y = y + x$

6. **Closure under Multiplication**

   $\forall$x,y $\in F, [the\ product] x \cdot y$ is contained in F.

7. **Associativity of Multiplication**

   $\forall$ x,y,z $\in F, (x \cdot y) \cdot z = x \cdot (y \cdot z)$

8. **Commutativity of Multiplication**

   $\forall$ x,y $\in F, x \cdot y = y \cdot x$

9. **Multiplicative Identity**

   $\forall$ x$\in F$ there exists 1$\in F$ such that$1 \neq 0$, then $x \cdot 1 = x = 1 \cdot x$ where 1 is identity element of multiplication.

10. **Multiplicative Inverses**

    $\forall$ x $\in F such\ that x \neq 0$ there exists y $\in F$ *such that* $x \cdot y = y \cdot x = 1$. The element y is called the multiplicative inverse of x and denoted x^{-1}.

11. **Distribution of Multiplication over Addition**

    $\forall$ x, y ,z $\in F, x \cdot (y + z) = x \cdot y + x \cdot z$ Left distribution

    $\forall$ x, y, z$\in F, (x + y) \cdot z = x \cdot z + y \cdot z$ Right distribution

Example 1,

Show that (R,$\bigoplus$,$\bigodot$), is a field.

The set of real numbers are a field, under binary operation addition and multiplication. Because of,

1. for any a,b $\in R, a + b\ an \in R$.closure under addition

2. for any a,b,c$\in R, a + (b + c) = (a + b) + c\ an \in R$. associativity properties of addition

3. There exists an element $0 \in R \, such \; that \; a + 0 = a = 0 + a \; for \; a \in R.$ identity properties of addition

4. for any a$\in R there \; exists \; b \in R, \; such \; that \; a + b = 0 = b + a \; an \; \in R.$ where b is the inverse element of a. inverse properties of addition

5. for any a,b $\in R, a + b = b + a \; an \in R.$ Commutativity properties of addition

6. for any a,b $\in R, a \cdot b \; an \in R.$ closure under multiplication

7. for any a,b,c$\in \; R, \; a \cdot (b \cdot c) = (a \cdot b) \cdot c \; an \; \in R.$ associativity properties of multiplication

8. for any a,b $\in R; a \cdot b = b \cdot a$ commutative properties of multiplication

9. for any a $\in$ R, there exists $1 \in$ R such that $1 \neq 0$, then a $\cdot 1 = a = 1 \cdot a$ where 1 is the identity element of multiplication.

10. for any a$\in R, \; such \; that \; a \neq 0, \; there \; exists \; b \in R, then \; a \cdot b = 1 = b \cdot a,$ where b is the multiplicative inverse of a. multiplication inverse properties

11. $\forall$ a,b,c$\in R, then$

    i. $a \cdot (b + c) = a \cdot b + a \cdot c$ left distribution of multiplication

    ii. $(a + b) \cdot c = a \cdot c + b \cdot c$ right distribution of multiplication.is the distribution properties of multiplication over addition

    Now, from 1 to 11 above the set of real numbers is a Field, under binary operation of addition and multiplication.

Similarly,The set of Rational numbers and Complex numbers are a Field, under binary operation addition and multiplication.

Prime Field

Corollary: If p is prime, then $Z_p$is a Field.

Proof

Suppose a,b $\in Z_p$, and ab = 0.

Then ab = pk for some k$\in Z$.

$p|a$ *or* $p|b$. by definition of congruence

$\implies a = 0 \ mod \ p \ or b = 0 \ mod \ p$

$\implies a = 0 \ or \ b = 0.$

Thus Z_p is an integral domain.

Since, p is prime and $p \neq 0$, then Z_p is also a field.

Example 2,

Show that $(Z_7, \bigoplus_7, \bigodot_7)$ is a field.

Solution

1. $\forall$ a,b $\in Z_7, a + b$ an $\in Z_7$.closure under addition
2. $\forall$ a,b,c$\in Z_7, (a + b) + c = a + (b + c)$ an $\in Z_7$. associativity properties of addition
3. $\exists$ an elements 0$\in Z_7, such \ that \ a + 0 = 0 = 0 + a \ for \ a \in Z_7$. identity properties of addition
4. $\forall \ a \in Z_7, there \ exists \ b \in Z_7, such \ that \ a + b = 0 = b + a \ is \ in \ Z_7$. inverse properties of addition
5. $\forall$ a,b $\in Z_7, a + b = b + a$ an $\in Z_7$. commutativity properties of addition
6. $\forall$ a,b, $\in F_7, a \cdot b$ an $\in Z_7$. closure under multiplication
7. $\forall$ a,b,c$\in Z_7, a \cdot (b \cdot c) = (a \cdot b) \cdot c$. associative properties of multiplication
8. $\forall$ a,b$\in Z_7, a \cdot b = b \cdot a$ commutative properties of multiplication
9. $\forall$ a $\in Z_7$, there exists $1 \in Z_7$ such that 1 1 $\neq 0$, then a $\cdot 1 = a = 1 \cdot a$ where 1 is the identity element of multiplication.
10. $\forall$ a$\in Z_7, such \ that \ a \neq 0 \ there \ exists \ b \in Z_7, \ then \ a \cdot b = 1 = b \cdot a$ for b is the multiplicative inverse a.
    such that: $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ then
    the inverse of 1 is 1 because $1 \cdot 1 = 1 \neq 0$

the inverse of 2 is 4 because $2 \cdot 4 = 1 \neq 0$

the inverse of 3 is 5 because $3 \cdot 5 = 1 \neq 0$

the inverse of 4 is 2 because $4 \cdot 2 = 1 \neq 0$

the inverse of 5 is 3 because $5 \cdot 3 = 1 \neq 0$

the inverse of 6 is 6 because $6 \cdot 6 = 1 \neq 0$. is inverse properties of multiplicative. since 1 is the identities inverse of multiplication.

11. $\forall$ a,b,c $\in Z_7, a \cdot (b + c) = a \cdot b + a \cdot c$.left distribution

    for any a,b,c $\in Z_7, (a+b) \cdot c = a \cdot c + b \cdot c$.right distribution. distribution properties of multiplication over addition

    Therefore, from 1 to 11 above of $(Z_7, \bigoplus_7, \bigodot_7)$ is a field.

Definition (2.0)

Field is a commutative division ring.

Since, If every non-zero element of R is a unit, then R is a division ring.

Definition (2.1)

A Field F is a commutative ring F with identity in which every nonzero element has an inverse.

Examples 3,

• the rational numbers Q with the usual addition and multiplication

• the real numbers R with the usual addition and multiplication

• the complex numbers C with the usual addition and multiplication

• the set mod p where p is a prime number is a Field under addition and multiplication mod p

2.2 Properties of Field

1. The multiplicative identity of field F is unique.

   proof

   Suppose that $1 \in F$ and $\alpha \in F$ are multiplicative identities.

   Since 1 is a multiplicative identity, by property (9), $x \cdot 1 = xforallx \in F$.

Setting $x = \alpha$,

we get $\alpha \cdot 1 = \alpha$.

On the other hand, since α is a multiplicative identity, by property (9),

$x \cdot \alpha = x \; for \; all \; x \in F$. If we take x = 1, we get $1 \cdot \alpha = 1$.

But $1 \cdot \alpha = \alpha \cdot 1$ by property (5).

So we have $\alpha = \alpha \cdot 1 = 1 \cdot \alpha = 1$.

2. The additive inverse of an element of field F is unique.

   proof

   suppose b and b'both additive inverses of a. then:

   b=b+0 by additive identity.

   b=b+(a+b') as b' is an additive inverse of a.

   b=(b+a)+b' by associativity of addition.

   b=0+b' as b is an additive inverse of a.

   b=b' by additive identity.

   Therefore, the additive inverse of field F is unique.

3. The multiplicative inverse of a nonzero element of F is unique.

4. In a Field, a product of two nonzero elements is nonzero, or equivalently.

   $a \cdot b = 0 \implies a = 0$ or b = 0

   proof

   Suppose ab = 0.

   If $a \neq 0$, then a has an inverse a^{-1}

   so $ab = 0$

   $\implies a^{-1}ab = a^{-1}0$

   $\implies$ 1b = 0

   $\implies$ b = 0.

Example 4,

Let F be a Field. Using the axioms in the definition of Field, prove that $-1 \cdot x = -x \; for \; all \; x \in F$. State which axioms are used in your proof.

Solution

We must show that $-1 \cdot x$ *is an additive inverse of* x, that is, x + $(-1) \cdot x = 0$.

$$
\begin{aligned}
x + (-1) \cdot x &= x + x \cdot (-1) \text{ by axioms commutativity of multiplication.} \\
&= x \cdot 1 + x \cdot (-1) \text{ by axioms of existence multiplicative identity.} \\
&= x \cdot (1 + (-1)) \text{ by axioms of distibutivity properties over addition} \\
&= x \cdot 0 \text{ by axioms of existence additive} \\
&= x \cdot 0 + 0 \text{ by axioms of additive indentity} \\
&= x \cdot 0 + (x \cdot 0 + -(x \cdot 0)) \text{ byaxioms of associative multiplication} \\
&= (x \cdot 0 + x \cdot 0) + -(x \cdot 0) \text{ by axioms of assoiative addition} \\
&= x \cdot (0 + 0) + -(x \cdot 0) \text{ by axioms of distribution over addition} \\
&= x \cdot 0 + -(x \cdot 0) \text{ by axioms of existence an additive} \\
&= 0 \text{ by axioms of existence of additive inverse}
\end{aligned}
$$

Definition (2.2)

Theorem 2.0

Cancellation Laws Holds on Field.

Let a, b, and c be elements of a Field F.

1. If a+ b = a + c, then b = c.
2. If ab = cb and $b \neq 0$, then a = c.

   Proof

1, suppose that $a \cdot b = a \cdot$ then, we have

$$\begin{aligned} &= b = 0 + b \text{ by additive identity} \\ &= (-a + a) + b \text{ by additive inverse of a} \\ &= -a + (a + b) \text{ by associativity of addition} \\ &= -a + (a + c) \text{ by assumption} \\ &= (-a + a) + c \text{ by associativity of addition} \\ &= 0 + c \text{ by additive inverse of a} \\ &= c \text{ by additive identity} \end{aligned}$$

so that $b = c$ as desired.

This implies, if $a + b = a + c$, then $b = c$

Proof

2, suppose that $b \neq 0$. Then, according to multiplicative inverse properties,
there exists $b^{-1} \in F$ *such that* $b \cdot b^{-1} = 1$.
Multiplying both sides of the equation $a \cdot b = c \cdot b$ on the right by b^{-1}, we get
$(ab)b^{-1} = (cb)b^{-1}$.
Applying associativity of multiplication properties on both sides, we get
$a(bb^{-1}) = c(bb^{-1})$
Now applying identities multiplication inverse properties $a \cdot 1 = c \cdot 1$.
we obtain a = c.

2.3 Sub-Field

A sub-Field of a field F is a subset of F which is itself a field with the same operations as F.
Examples 5,

1. Q is a sub-field of R.
2. R is a sub-field of C.

3. Z_p has no sub-fields (other than itself).

Theorem 2.1

Every Field F is an Integral Domain

Proof

Suppose that a,b $\in Fa \neq 0$ then, if ab=0 we have:

We need to show that if $a \neq 0$, then b = 0.

$a^{-1}(ab) = 0$

By the associativity of multiplication, we have:

$(a^{-1}a)b = 0$

$1 \cdot b = 0$

$b = 0$

$\Longrightarrow$ there is no zero divisors in F.

Therefor, every field F is an integral domain.

Theorem 2.2

Every finite Integral Domain is a Field.

Proof

let $0, 1, a_1, a_2, ..., a_n$ be all the elements of a finite integral domain.

we need to show that for $a \in D$,where $a \neq 0$,there exists $b \in D$ such that ab=1

$a1, aa_1, aa_2, ..., aa_n$

We claim that all these elements of D are distinct, for $aa_i = aa_j$ This:

$\Longrightarrow$ $a_i = aj$, by cancellation laws that hold in an integral domain.

Also, since D has no zero divisors,none of these elements is 0.

Hence by counting, we find that $a1, aa_1, aa_2, ..., aa_n$ are elements $1, a_1, a_2, ..., a_n$ in some order.

so that either $a_1 = 1$, *that is*, $a = 1$, *or* $aa_i = 1$ for some i.

Thus, a has a multiplicative inverse.

Therefore, every finite integral domain is a Field.

Remark: Every integral domain is not a field.

Example 6,

$(Z, \bigoplus, \bigodot)$ is integral domain, but its not a field.

Because, it is not division ring. the only invertible element is 1 and -1

2.4 Type of Field

2.4.1 Prime Field

Corollary: If p is prime, then $Z_p$is a Field.

Proof Suppose a,b $\in Z_p$, and ab = 0.

Then ab = pk for some k$\in Z$.

$p|a$ *or* $p|b$. by definition of congruence

$\implies a = 0 \ mod \ p \ or b = 0 \ mod \ p$

$\implies a = 0 \ or \ b = 0.$

Thus Z_p is an integral domain.

Since, p is prime and $p \neq 0$, then Z_p is also a field.

Example 2,

Show that $(Z_7, \bigoplus_7, \bigodot_7)$ is a field.

Solution

1. $\forall$ a,b $\in Z_7, a + b$ an $\in Z_7$.closure under addition
2. $\forall$ a,b,c$\in Z_7, (a + b) + c = a + (b + c)$ an $\in Z_7$. associativity properties of addition
3. $\exists$ an elements 0$\in Z_7, such \ that \ a + 0 = 0 = 0 + a \ for \ a \in Z_7$. identity properties of addition
4. $\forall \ a \in Z_7, there \ exists \ b \in Z_7, such \ that \ a + b = 0 = b + a \ is \ in \ Z_7$. inverse properties of addition
5. $\forall$ a,b $\in Z_7, a + b = b + a$ an $\in Z_7$. commutativity properties of addition
6. $\forall$ a,b, $\in F_7, a \cdot b$ an $\in Z_7$. closure under multiplication
7. $\forall$ a,b,c$\in Z_7, a \cdot (b \cdot c) = (a \cdot b) \cdot c$. associative properties of multiplication
8. $\forall$ a,b$\in Z_7, a \cdot b = b \cdot a$ commutative properties of multiplication

9. $\forall$ a $\in Z_7$, there exists $1 \in Z_7$ such that 1 1 $\neq 0$, then a $\cdot 1 = a = 1 \cdot a$ where 1 is the identity element of multiplication.

10. $\forall$ a$\in Z_7, \textit{such that } a \neq 0 \textit{ there exists } b \in Z_7, \textit{ then } a \cdot b = 1 = b \cdot a$ for b is the multiplicative inverse a.
    such that: $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ then
    the inverse of 1 is 1 because $1 \cdot 1 = 1 \neq 0$
    the inverse of 2 is 4 because $2 \cdot 4 = 1 \neq 0$
    the inverse of 3 is 5 because $3 \cdot 5 = 1 \neq 0$
    the inverse of 4 is 2 because $4 \cdot 2 = 1 \neq 0$
    the inverse of 5 is 3 because $5 \cdot 3 = 1 \neq 0$
    the inverse of 6 is 6 because $6 \cdot 6 = 1 \neq 0$. is inverse properties of multiplicative. since 1 is the identities inverse of multiplication.

11. $\forall$ a,b,c $\in Z_7, a \cdot (b + c) = a \cdot b + a \cdot c$.left distribution
    for any a,b,c $\in Z_7, (a+b) \cdot c = a \cdot c + b \cdot c$.right distribution. distribution properties of multiplication over addition
    Therefore, from 1 to 11 above of $(Z_7, \bigoplus_7, \bigodot_7)$ is a field.

2.4.2 Extension Field

Definition Of Extension Field

A Field E is an extension field of a field F if $F \leq E$.

Thus the graph show that R is an extension field of Q, and C is an extension field of both R and Q.

2.4.3 Algebraic and Transcendental Elements

Definition (2.3)

An element α of an extension field E of a field F is algebraic over F if f(α) = 0 for some non-zero f(x) ∈F[x].

If α is not algebraic over F, thenα is transcendental over F.

Example 7,

Show that $\sqrt{3}$ is algebraic over Q.

Solution:

Let $\alpha = \sqrt{3}$,then by squaring both side, we get that is

α^2=3

α^2-3=0

$\Longrightarrow$ there exists f(x)= $x^2 - 3 = 0 \in Q[x]$.

$\Longrightarrow$ $\sqrt{3}$ is algebraic over Q.

Example 8,

Show that π is Transcendental over Q.

Solution:

Let $\alpha = \pi$

$\alpha - \pi = 0$

$\Longrightarrow$ f(x)=x- π

But, f(x)=x- π is not element of Q[x].

$\Longrightarrow$ π is Transcendental over Q.

Definition (2.4)

An element of C that is algebraic over Q is an algebraic number. A transcendental number is an element of C that is transcendental over Q.

Theorem (2.3)

Let E be an extension field of a field F and let a $\alpha \in$ E. Let $\phi_\alpha : F[x] \to E$ be the evaluation homomorphism of F[x] into E such that $\phi_\alpha(a) = a$ $\forall$ a ∈ F and $\phi_\alpha(x) = \alpha$. Then α is transcendental over F if and only if ϕ_α gives an isomorphism of F[x] with a subdomain of E, that is, if and only if ϕ_α is a one-to-one map.

proof

The element α is transcendental over F if and only if $f(\alpha) \neq 0$ for all nonzero f(x) ∈

F[x].

which is true (by definition) if and only if $\phi_\alpha(f(x)) \neq 0$ for all nonzero f(x) $\in F[x]$.

which is true if and only if the kernel of ϕ_α is 0, that is, if and only if ϕ_α is a one-to-one map.

2.4.4 The Irreducible Polynomial For α Over Field(F)

Theorem (2.4)

Let E be an extension field of F, and let $\alpha \in E$, where a is algebraic over F. Then there is an irreducible polynomial px) $\in F[x]$ such that $p(\alpha) = 0$. This irreducible polynomial p(x) is uniquely determined up to a constant factor in F and is a polynomial of minimal degree $\geq$1 in F[x] having a as a zero. If $f(\alpha) = 0$ for f(x) $\in F[x]$, with f(x) = 0. then p(x) divides f(x).

Proof

Let ϕ_α be the evaluation homomorphism of F[x] into E, given by the evaluation of homomorphisms for field theory. The kernel of ϕ_α is an ideal and by Theorem (if F is a field, every ideal in F[x] is principal.) it must be a principal ideal generated by some px) $\in$ F[x]. Now (p(x) consists precisely of those elements of F[x] having a as a zero. Thus, if f(α) = 0 for f(x) $\neq$ 0, then f(x) $\in$ (p(x), so p(x) divides f(x). Thus p(x) is a polynomial of minimal degree $\geq$1 having α as a zero,and any other such polynomial of the same degree as p(x) must be of the form (a)p(x) for some a $\in$ F. It only remains for us to show that p(x) is irreducible.If p(x)=r(x)s(x) were a factorization of px) into polynomials of lower degree, then p(α) = 0 would imply that r(α)s(α) = 0, so either r(α) = 0 or s(α) = 0, since E is a field. This would contradict the fact that p(x) is of minimal degree $\geq$1 such that p(α) = 0. Thus p(x) is irreducible.

Example 9,

$\sqrt{2}$ is algebraic over Q.

There exists x^2 -2 $\in$Q[x], such that p(x)= x^2 -2

Let f(x)= x^3 -2x,

since, f($\sqrt{2}$)= $(\sqrt{2})^3$ -2$\sqrt{2}$=0

$\Longrightarrow$ x^2 -2 $|x^3$ -2x,

because, x^3 - 2x=x(x^2 - 2)

$\Longrightarrow$ $f(x)|p(x)$, for all p(x)$\neq$ 0

Definition (2.5)

Let E be an extension field of a field F, and let α E be algebraic over F. The unique monic polynomial p(x) having the property described in Theorem above is the irreducible polynomial for a over F and will be denoted by irr(α, F). The degree of irr(α, F) is the degree of a over F, denoted by deg(α, F).

Example 10,

Show that $\sqrt{1+\sqrt{3}}$ is irreducible over Q.

Solution:

Let α= $\sqrt{1+\sqrt{3}}$ where $\sqrt{1+\sqrt{3}} \in R$

α= $\sqrt{1+\sqrt{3}}$ by square both side of the equation, we get that.

$\alpha^2 = 1+\sqrt{3}$

α^2-1 = $\sqrt{3}$ by square both side of the equation also, we get that.

$\alpha^4 - 2\alpha^2+1 = 3$

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

Then, f(x)= $x^4 - 2x^2 - 2 = 0 \in Q[x]$

$\Longrightarrow$ $\sqrt{1+\sqrt{3}}$ is irreducible over Q.

Therefore, irr($\sqrt{1+\sqrt{3}}$, Q)= $x^4 - 2x^2 - 2 = 0$

deg($\sqrt{1+\sqrt{3}}$, Q) =4

2.5 Simple Extension

An extension field E of a field F is a simple extension of F if E = F (α) for some $\alpha \in$E.

Theorem (2.5)

Let E be a simple extension F(α) of a field F, and let α be algebraic over F. Let the degree of irr(α, F) be n $\geq$ 1. Then every element β of E = F(α) can be uniquely expressed in the form

$\beta = \beta_0 + \beta_1\alpha + \beta_2\alpha^2 + ... + \beta_{n-1}\alpha^{n-1}$, where the βi are in F.

proof

For the usual evaluation homomorphism ϕ_α, every element of

F(α) = ϕ_α[F[x]]

is of the form ϕ_α(f(x)) = f(α), a formal polynomial in a with coefficients in F.

Let irr(α, F) = p(x) = $x^n + a_{n-1}x^{n-1} + ... + a_0$.

Then p(α) = 0, so

$\alpha^n = -a_{n-1}\alpha^{n-1} - a_{n-2}\alpha^{n-2} - ... - a_0$.

This equation in F(α) can be used to express every monomial α^m for m $\geq$n in terms of powers of α that are less than n.

For example,

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

$= a_{n-1}(a_{n-1}\alpha^{n-1} - ... - a_0) - a_{n-2}\alpha^{n-1} - ... - a_0\alpha$.

Thus, if $\beta \in F(\alpha), \beta$ can be expressed in the required form

$\beta = b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}$.

For uniqueness, if $b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1} = b'_0 + b'_1\alpha + ...b'_{n-1}\alpha^{n-1}$

For $b'_i \in F$, then

$(b_0 - b'_0) + (b_1 - b'_1)x + ... + (b_{n-1} - b'_{n-1} = g(x)$

is in F[x] and g(α) = 0.

Also, the degree of g(x) is less than the degree of irr(α, F).

Since irr(α, F) is a nonzero polynomial of minimal degree in F[x] having α as a zero, we must have g(x) = 0.

Therefore, $b_i - b'_i$= 0, so

$b_i = b'_i$, and the uniqueness of the b_i is established.

2.5.1 Algebraic Extensions

I saw that if E is an extension field of a field F and $\alpha \in$ E is algebraic of F, then every element of F(α),then every element of F(α), is algebraic over F.

Definition (2.6)

An extension field E of a field F is an algebraic extension of F if every element in E is algebraic over F.

Example 11,

1. Q($\sqrt{2}$) *and* $Q(\sqrt{3})$ are algebraic extension.

2. R is not an algebraic extensions of Q.

2.5.2 Finite Extensions

Definition(2.7)

If an extension field E of a field F is of finite dimension n as a vector space over F, then E is a finite extension of degree n over F.

We shall let [E : F] be the degree n of over F.

To say that a field E is a finite extension of a field F does not mean that E is finite field. It just asserts that £ is a finite-dimensional vector space over F, that is, that [E : F] is finite.

Theorem (2.6)

A finite extension field E of a field F is an algebraic extension of F.

Proof

We must show that for $\alpha \in$ E, α is algebraic over F. By Theorem ($if B = \beta_1, ..., \beta_n$ is any basis for V over F,then $r \leq n$). if [E:F] = n,

then $1, \alpha, ...\alpha^n$ can not be linearly independent elements.

so there exist $\alpha_i \in$ F, such that

$a_n\alpha_n + ... + a_1\alpha + a_0 = 0$ and not all $\alpha_i = 0$.

Then $f(x) = a_n\alpha_n + ... + a_1\alpha + a_0$ is a nonzero polynomial in F[x].and $f(\alpha) = 0$

Therefore, α is algebraic over F.

Remark: i.To say that a field F is a finite extension of a field F, k does not mean E is finite.

ii. If is a finite extension of F then [E:F] =1 if and only if E=F.

2.5.3 Algebraically Closed and Algebraic Closures

Theorem (2.7)

Let E be an extension field of F. Then $\bar{F}_E = \{\alpha \in E | \alpha \; is \; algebraic \; over \; F\}$ is a subfield of E, the algebraic closure of F in E.

A finite extension field £ of a field £ is an algebraic extension of £. Let $\alpha, \beta \in \bar{F}_E$.If F (α, β) is a finite extension of F, and if every element of F(α, β) is algebraic over F. that is,F$(\alpha, \beta) \subseteq \bar{F}_E$.

Thus, $\bar{F}_E$ contains $\alpha + \beta$, $\alpha\beta$, $\alpha - \beta$, and also contains $\frac{\alpha}{\beta}$ for $\beta \neq 0$, so $\bar{F}_E$ is a subfield of E.

Corollary:

The set of all algebraic numbers forms a field.because the set of all algebraic numbers is the algebraic closure of Q in C.

Definition (2.8):

A field F is algebraically closed if every non constant polynomial in F[x] has a zero in F.

Note that a field F can be the algebraic closure of F in an extension field E with out F being algebraically closed.

Example 12,

1. Q is the algebraic closure of Q in Q(x), but
2. Q is not algebraically closed because $x^2 + 1$ has no zero in Q.

Theorem (2.8)

A field F is algebraically closed if and only if every non constant polynomial in F[x] factors in F[x] into linear factors.

Proof

Let F be algebraically closed, and let f(x) be a non constant polynomial in F[x].

Then f(x) has a zero a ∈F. By Corollary above x-a is a factor of f(x).

so f(x) = (x - a)g(x).

Then if g(x) is non constant, it has a zero b ∈ F, and we have

f(x) = (x — a)(x — b)h(x).

Continuing, we get a factorization of f(x) in F[x] into linear factors.

Conversely, suppose that every non constant polynomial of F[x] has a factorization into linear factors.

If ax - b is a linear factor of f(x), then

$\frac{b}{a}$ is a zero of f(x).

Thus F is algebraically closed.

corollary:

An algebraically closed field F has no proper algebraic extensions, that is, no algebraic extensions E with F $<$ E.

Theorem (2.9)

Every field F has an algebraic closure, that is, an algebraic extension $\bar{F}$ that is algebraically closed.

Example 13,

1. C is an algebraically closed field.
2. No finite field F algebraically closed. since if $a_1, ..., a_n$ are all the elements of F, then the polynomial $(X - a_1)...(X - a_n) + 1$ has no zero in F.
3. The field R is not algebraically closed. since $x^2 + 1 = 0$ has no root in R.

Conclusion

Generally, from this project we understand the definition of basic terms to defined field, definition of field, and its axioms and properties,types of field, and with some example of field and also proof some of its properties, theorem,corollary that can be helps when we defined a field.

References

1. Fraleigh J.B.A first course in abstract algebra.

2. Schaum's outline abstract algebra. pdf.

3. Blyth, T.S.; Robertson, E. F. (1985), Groups, rings and fields: Algebra through practice, Cambridge University.

4. www. com Google