الفصل الاول

" Ring Theorey "

Concents

Chapter One _ Rings

Rings (Definition - Example and general properties of rings).
Direct sum of rings and some remarks.
Integral domain - Division ring - Field - Boolean rings - Center of a ring.

Chapter two _ Subrings

Subrings (Definition - Characterization of subring - Examples).
some operations on subrings - subfields (Definition and examples).

Chapter three _ Ideals

Ideals (Definitions and examples) - operations on ideals (addition of ideal, multiplication of ideals, intersection of ideal, union of ideal).
finitely generated ideal - Principle ideal ring - finitely generated ring - rings as direct sum of ideals.

Chapter four - factor ring

Factor ring (definition and examples) - some relationships between a ring R and its factor ring.

Chapter five - Ring homomorphism

Ring homomorphism (definition and examples).
- Kernel and image of ring homomorphism - some basic properties of ring homomorphism - Fundamental theorems of ring homomorphism - Embedding of ring and theorem of embedding.

Chapter six - Certain special types of ideals

Certain special types of ideals : maximal ideals, prime ideal, semiprime ideal, Primary ideal and radical of ideals (definitions and example and basic properties)

Chapter seven - (Polynomial rings)

Polynomial ring (definition and examples, some relationships between a ring R and polynomial ring over R) - degree of polynomial with some theorems related with this Concept - Division Algorithm - factor theorem - remainder theorem - irreducible polynomail - polynomial ring over field (F[x], where F is a field) - the quotient of polynomial ring over field.

Chapter eight _ Extension of fields

Extension of fields (definitions) _ some example to Calculate extension field of Certain field.

Chapter nine _ Modules

Modules _ Submodules _ factor modules _ homomorphism of Modules.

Refernces : المصادر

1. Introduction to abstract and linear algebra by David. M. Burton.

2- مقدمة في الجبر المجرد : تأليف د. ليلى سلمان محمود و د. محمد عبد الرزاق

3- ملزمة نظرية الحلقات : تأليف د. عادل غسان نعوم و د. باسل الهاشمي

Definition

(Chapter one)

let R be a non-empty set and let $+$, $\cdot$ be two binary operations on R. Then $(R,+,\cdot)$ is a ring if:

1. $(R,+)$ is an abelain group, that is

a. $+$ is closed on R

b. $+$ is associative

c. $\forall a \in R$, $\exists$ an element $0 \in R$ s.t. $a+0=a$, 0 is Called the zero element.

d. $\forall a \in R$, $\exists\, -a \in R$ s.t. $a+(-a)=0$, $-a$ is Called the additive inverse of a.

e. $+$ is Commutative.

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

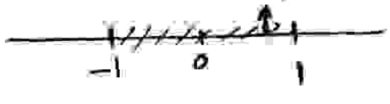
3. $a \cdot (b+c) = a \cdot b + a \cdot c$, $(b+c) \cdot a = b \cdot a + c \cdot a$ $\forall a,b,c \in R$.

Examples

1. $(\mathbb{R},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{Z},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are rings

2. $((-1,1),+,\cdot)$ is not ring, for example

$0.7 \in (-1,1)$



, but $0.7+0.7=1.4 \notin (-1,1)$

3. $(Z_e,+,\cdot)$ be a ring, where $Z_e = \{x : x = 2k \text{ for some } k \in \mathbb{Z}\}$

4. let n be a fixed positive integer and $n \neq 1$.

Definition (chapter one)

let R be a non-empty set and let $+ , \cdot$ be two binary operations on R. Then $(R, +, \cdot)$ is a ring if:

1. $(R, +)$ is an abelain group, that is
   a. $+$ is closed on R
   b. $+$ is associative
   c. $\forall a \in R$, $\exists$ an element $0 \in R$ s.t. $a + 0 = a$, 0 is Called the zero element.
   d. $\forall a \in R$, $\exists -a \in R$ s.t. $a + (-a) = 0$, $-a$ is Called the additive inverse of a.
   e. $+$ is Commutative.

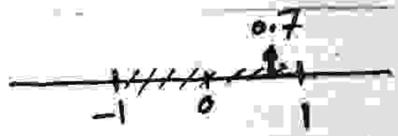
2. $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b \in R$
3. $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$ $\forall a, b, c \in R$.

Examples

1. $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings

2. $((-1, 1), +, \cdot)$ is not ring, for example

$0.7 \in (-1, 1)$



, but $0.7 + 0.7 = 1.4 \notin (-1, 1)$

3. $(Z_e, +, \cdot)$ be a ring, where $Z_e = \{x : x = 2k \text{ for some } k \in Z\}$

4. let n be a fixed positive integer and $n \neq 1$.

let $A=\{x : x=nk$ for some $k\in Z\}$. Then $(A,+,\cdot)$ is a ring. show that (H.W.)

Definition:

let R be a ring. R is said to be Commutative ring, if $a.b=b.a \quad \forall a,b\in R$.

Definition:

let R be a ring. Then if $\exists\, 1\in R$ such that $a.1=1.a=a \quad \forall a\in R$. R is Called a ring with identity (or unitary ring). Also, let $a\in R$. Then a is Called invertible element, if $\exists\, a^{-1}\in R$ st $a.a^{-1}=a^{-1}.a=1$

Examples:

1. $(Z,+,\cdot)$, $(Q,+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are a Commutative ring with identity.

2. let $R=M_{n\times n}(\mathbb{R})=\left\{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn}\end{bmatrix} ; a_{ij}\in\mathbb{R} \quad \forall i,j=1,\dots,n\right\}$

be the set of all metrices $n\times n$ with usual addition and multiplicative for matrices. Then $(R,+,\cdot)$ is a non Commutative ring with identity

Since, let $A=(a_{ij})_{n\times n}$ and $B=(b_{ij})_{n\times n}$. Then

1. $A+B=(a_{ij}+b_{ij})\in M_{n\times n}(\mathbb{R})$ is Comm. gp.

2. $A.B=\left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)_{n\times n}$, Then • associative and • distributive over +

$$I_n=\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1\end{pmatrix}_{n\times n}\in M_{n\times n}(\mathbb{R})$$

$A.I_n = I_n.A = A \qquad \forall A \in M_{n\times n}$

$\therefore (M_{n\times n}, +, .)$ is a ring with unity, but $(M_{n\times n}, +, .)$ is not Comm. ingeneral.

3. $(Z_e, +, .)$ is Comm. ring without identity

4. let X be a non-empty set. Then $(P(x), \Delta, \cap)$ is a ring, where $A\Delta B = (A\cup B)-(A\cap B)$
$= (A-B)\cup(B-A)$.

This ring is Comm. with identity X. For example:

let $X=\{1,2\}$. Then $P(x) = \{\emptyset, \{1\}, \{2\}, X\}$
Δ is closed on $P(x)$ and $\cap$ is Comm. and associa.

$\emptyset$ = identity with respect to Δ and every element in $P(x)$ has inverse, also Δ is associative, then $(P(x), \Delta)$ is Comm. gp.

Now, $\cap$ is asso. and $\cap$ distributed over Δ.

Therefore $(P(x), \Delta, \cap)$ is a Comm. ring with identity X. {since, $X\cap\{1\} = \{1\}$, $X\cap\{2\}=\{2\}$, $X\cap\emptyset = \emptyset$ and $X\cap X = X$}

5. let $Z[\sqrt{3}] = \{a+b\sqrt{3} : a,b\in Z\}$. Define $+, .$ on $Z[\sqrt{3}]$ by

$$(a+b\sqrt{3})+(c+d\sqrt{3}) = (a+c)+(b+d)\sqrt{3}$$

$$(a+b\sqrt{3}).(c+d\sqrt{3}) = (ac+3bd)+(bc+ad)\sqrt{3}$$

$A.I_n = I_n.A = A \quad \forall A \in M_{n\times n}$

$\therefore (M_{n\times n}, +, .)$ is a ring with unity, but $(M_{n\times n}, +, .)$ is not Comm. ingeneral.

3. $(Z_e, +, .)$ is Comm. ring without identity

4. let X be a non-empty set. Then $(\mathbb{P}(x), \Delta, \cap)$ is a ring, where $A \Delta B = (A \cup B) - (A \cap B)$
$= (A - B) \cup (B - A)$.

This ring is Comm. with identity X. For example:

let $X = \{1, 2\}$. Then $\mathbb{P}(x) = \{\emptyset, \{1\}, \{2\}, X\}$
Δ is closed on $\mathbb{P}(x)$ and $\cap$ is Comm. and associa.

$\emptyset$ = identity with respect to Δ and every element in $\mathbb{P}(x)$ has inverse, also Δ is associative, then $(\mathbb{P}(x), \Delta)$ is Comm. gp.

Now, $\cap$ is asso. and $\cap$ distributed over Δ.

Therefore $(\mathbb{P}(x), \Delta, \cap)$ is a Comm. ring with identity X. $\{$since, $X \cap \{1\} = \{1\}$, $X \cap \{2\} = \{2\}$, $X \cap \emptyset = \emptyset$ and $X \cap X = X \}$

5. let $Z[\sqrt{3}] = \{a + b\sqrt{3} : a, b \in Z\}$. Define $+, .$ on $Z[\sqrt{3}]$ by

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c) + (b + d)\sqrt{3}$$

$$(a + b\sqrt{3}).(c + d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3}$$

Then $(\mathbb{Z}[\sqrt{3}], +, \cdot)$ be a Comm. ring with identity $1 = 1 + 0.\sqrt{3}$

6. let $x \oplus y = x+y \quad \forall x, y \in \mathbb{Z}$ and
$x \odot y = 0 \quad \forall x, y \in \mathbb{Z}$

defined on $\mathbb{Z}$. Then $(\mathbb{Z}, \oplus, \odot)$ is Comm. ring without unity.

Since, $(\mathbb{Z}, \oplus)$ is Comm. gp.

① Now, To prove well-defined, if $x = x_1$ and $y = y_1$, implies $x \odot y = 0$ and $x_1 \odot y_1 = 0$

Therefore $x \odot y = x_1 \odot y_1$ and hence $\odot$ well-defined

②. $\forall x, y \in \mathbb{Z}$, $x \odot y = 0 \in \mathbb{Z}$
$\therefore \odot$ is closed on $\mathbb{Z}$

③. $x \odot y = y \odot x = 0$ which implies $\odot$ is Comm.

④. $\forall x, y, z \in \mathbb{Z}$, $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z) = 0 \oplus 0 = 0$
Then $\odot$ distributive over $\oplus$.

Thus $(\mathbb{Z}, \oplus, \odot)$ is Comm. ring and $\nexists\, b \in \mathbb{Z}$ s.t. $a \odot b = a \quad \forall a \in \mathbb{Z}$ and $a \neq 0$. Hence the ring has no unity.

7. let $C[0,1] = \{f: [0,1] \longrightarrow \mathbb{R}\}$ which are Countinuas s.t. $(f+g)_{(x)} = f(x) + g(x)$ and
$$(f.g)_{(x)} = f(x) . g(x)$$

Then $(C[0,1], +, \cdot)$ is a Comm. ring with unity $I(x)$ [identity function].

8. let $Z_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$. Then $(Z_n, +_n, \cdot_n)$ is Comm. ring with identity 1

special Case : $(Z_4, +_4, \cdot_4)$ is Comm. ring with identity 1.

Properties of Rings "مبرهنات الحلقات"

let $(R, +, \cdot)$ be a ring. Then for all $a, b, c \in R$.

1. $a \cdot 0 = 0 = 0 \cdot a$
2. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$
3. $-(-a) = a$
4. $(-a) \cdot (-b) = a \cdot b$
5. $-(a+b) = -a - b$
6. $a \cdot (b - c) = a \cdot b - b \cdot c$
7. $(a - b) \cdot c = a \cdot c - b \cdot c$
8. If R has unity 1, then
   (i) $(-1) a = -a$
   (ii) $(-1)(-1) = 1$

Proofs

1. To prove : $a \cdot 0 = 0$

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

4. $(-a)(-b) = -(a(-b))$ by (2)

$= -(-(ab))$ by (2)

$= ab$ by (3)

8. $(-1)a = -(1.a)$ by (2)

$= -a$

Direct Sum of Rings and Some Remarks

الجمع المباشر للحلقات مع بعض الخواص

Definition:

let $(R,+,.)$ and $(R',+',.')$ be any two rings.
let $X = R \times R' = \{(a,b) : a \in R \wedge b \in R'\}$
Define $\oplus, \odot$ on X by:

$(a,b) \oplus (c,d) = (a+c,\ b+'d)$

$(a,b) \odot (c,d) = (a.c,\ b.'d)$.

Then $(X, \oplus, \odot)$ is a ring.

This ring is called the direct sum of R with R'

From above example, we have the following remarks:

Remarks:

1. If $(R,+,.)$, $(R',+',.')$ are Comm. ring, then the ring of direct sum of R, R' is Comm. ring

2. If the ring $(R,+,.)$ has unity 1 and the ring $(R',+',.')$ has unity $\bar{1}$, then the ring $R \times R'$ has

unity $(1,1')$

3. If rings $(R,+,\cdot)$, $(R',+',\cdot')$ have unities $1, 1'$ and $a\in R \wedge b\in R'$ such that a is an invertible in $R\times R'$ and $(a^{-1}, b^{-1}) = (a,b)^{-1}$.

Example:

let $\mathbb{Z}_2\times\mathbb{Z}_3 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2})\}$

and $(\bar{a},\bar{b}) \oplus (\bar{c},\bar{d}) = (\bar{a}+_2\bar{c}, \bar{b}+_3\bar{d})$

$(\bar{a},\bar{b}) \odot (\bar{c},\bar{d}) = (\bar{a}\cdot_2\bar{c}, \bar{b}\cdot_3\bar{d})$

Then $(\mathbb{Z}_2\times\mathbb{Z}_3, \oplus, \odot)$ is a ring.

$\oplus$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$
$(\bar{0},\bar{2})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{0},\bar{2})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{2},\bar{0})$	$(\bar{0},\bar{0})$
$(\bar{1},\bar{2})$	$(\bar{1},\bar{2})$	$(\bar{1},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{2})$	$(\bar{0},\bar{0})$	$(\bar{0},\bar{1})$

النظائر الجمعيه

$-(\bar{0},\bar{0}) = (\bar{0},\bar{0})$

$-(\bar{0},\bar{1}) = (\bar{0},\bar{2})$ $\qquad -(\bar{1},\bar{1}) = (\bar{1},\bar{2})$

$-(\bar{0},\bar{2}) = (\bar{0},\bar{1})$ $\qquad -(\bar{1},\bar{2}) = (\bar{1},\bar{1})$

$-(\bar{1},\bar{0}) = (\bar{1},\bar{0})$

Definition :- let $(R,+,\cdot)$ be a ring and $a,b \in R$, $a \neq 0$, $b \neq 0$. If $a.b = 0$, then a is called left zero divisor and b is called right zero divisor.

In Comm. ring, every left zero divisor is right zero divisor and conversely.

Examples :

1. In $(Z_3, +_3, \cdot_3)$, $\bar{0}, \bar{1}, \bar{2}$ are not zero divisors

2. In $(Z_4, +_4, \cdot_4)$, $\bar{0}, \bar{1}, \bar{3}$ are not zero divisors, but $\bar{2}$ is zero divisor, (since $\bar{2} \cdot_4 \bar{2} = \bar{0}$).

3. In $(Z_6, +_6, \cdot_6)$, $\bar{0}, \bar{1}, \bar{5}$ are not zero divisors. But $\bar{2}, \bar{3}, \bar{4}$ are zero divisors.

Remark :- let $(R,+,\cdot)$ be a Comm. ring with unity 1. If $a \in R$, $a \neq 0$, a is an invertible element, then a is not zero divisor.

That is, a is invertible element $\Rightarrow$ a is not zero divisor

Proof :- If $a \in R$, $a \neq 0$ and a is an invertible element.

$\therefore \exists\, a^{-1} \in R$ s.t. $a^{-1}.a = a.a^{-1} = 1$

Suppose a is a zero divisor.

Then $\exists\ b \in R,\ b \neq 0$ s.t. $a.b = 0$

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

$\Rightarrow 1.b = 0 \Rightarrow b = 0$ C! (since $b \neq 0$).

Thus a is not zero divisor.

والعلاقة العكسية صحيحة أيضاً

a is zero divisor $\Rightarrow$ a is not invertible.

Now, we have the following example:

Example :-

Consider the direct sum of $(\mathbb{R}, +, .)$ with $(\mathbb{R}, +, .)$

$$(a,0) \odot (0,b) = (0,0) \quad \forall a \neq 0,\ \forall b \neq 0$$

Then all element of the form $(a,0)$, $(0,b)$ where $a \neq 0$, $b \neq 0$ are zero divisors.

Theorem :-

let R be a comm. ring. Then R has no zero divisor $\Leftrightarrow$ $\forall a \in R$, $a \neq 0$, $a.b = a.c$ which implies $b = c$.

The cancellation law holds with respect to multiplication operation

proof: $\Rightarrow$ If R has no zero divisor

let $a.b = a.c$ and $a \neq 0$

$a.b + (-ac) = ac + (-ac)$

$a.b - ac = 0 \Rightarrow a(b-c) = 0$

but $a \neq 0$ and R has no Zero divisor.
Then $b - c = 0$ and hence $b = c$.

$\Leftarrow$ suppose R has Zero divisor, so

$\exists\, a \neq 0, b \neq 0$ s.t. $a.b = 0$

let $a.0 = 0$ (by properties of ring)
Then $a.b = a.0$ and hence $b = 0$ C!

Therefore R has no Zero divisor.

Theorem: let R be a comm. ring with unity 1 and R has no zero divisor. Then the equation $a^2 = a$ has only two slution $a = 0$ or $a = 1$.

"Integral domain" (تامة)

Definition: let $(R, +, \cdot)$ be a comm. ring with unity 1. Then R is called an integral domain $\Leftrightarrow$ R has no Zero divisor.

Example: ① All rings $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ have no Zero divisors. Then all these rings are integral domains.

② $(\mathbb{Z}_3, +_3, \cdot_3)$, $(\mathbb{Z}_5, +_5, \cdot_5)$ are integral domains
③ $(\mathbb{Z}_4, +_4, \cdot_4)$, $(\mathbb{Z}_6, +_6, \cdot_6)$ are not integral domains

Class

Theorem: $(Z_n, +_n, \cdot_n)$ is an integral domain $\Leftrightarrow$ n is prime number.

Proof: $\Rightarrow$ If $(Z_n, +_n, \cdot_n)$ is an integral domain

To prove n is a prime number
suppose n is not prime number
$\therefore \exists\, m, k \in Z_+$ s.t. $\quad n = m.k \quad 1 < m < n$, $\quad 1 < k < n$

$\Rightarrow \bar{0} = \bar{m} \cdot_n \bar{k}$ and $\bar{m}, \bar{k}$ are no zero element.

Then $\bar{m}, \bar{k}$ are zero divisors in Z_n.
which is contradiction since Z_n is an integral domain.
Thus n is prime number.

$\Leftarrow$ $(Z_n, +_n, \cdot_n)$ is comm. ring with unity 1
To prove $(Z_n, +_n, \cdot_n)$ is an integral domain,
we must prove that Z_n has no zero divisor
suppose Z_n has zero divisor
$\exists\, \bar{m}, \bar{k} \in Z_n$ s.t. $\bar{m} \neq \bar{0}$ and $\bar{k} \neq \bar{0}$, $\bar{m} \cdot \bar{k} = 0$

اعتيادي اعتيادي

$\Rightarrow \bar{m} \cdot \bar{k} = n \cdot r$ for some $r \in Z_+$

$\Rightarrow n / mk$. Then n/m or $n \backslash k$ (since n is prime)

If $n/m \Rightarrow m =$ multiply of $n \Rightarrow \bar{m} = \bar{0}$ C!
If $n/k \Rightarrow k =$ multiply of $n \Rightarrow \bar{k} = \bar{0}$ C!

Thus Z_n has no zero divisor.

Definition: let $(R, +, \cdot)$ be a comm. ring with unity 1. Then $(R, +, \cdot)$ is called field $\Leftrightarrow$ $\forall a \in R$, $a \neq 0$, a

is an invertible.

Example:

1. $(Q,+,\cdot)$, $(R,+,\cdot)$, $(C,+,\cdot)$ are fields

2. $(Z,+,\cdot)$, $(Ze,+,\cdot)$ is not a field.

3. direct sum of $(R,+,\cdot)$ with $(R,+,\cdot)$ is not a field.
Since all elements of the form $(a,0)$ and $(0,b)$ $a \neq 0$, $b \neq 0$ are not invertible elements.

problems:

1. let $S = R \times R$, Define $\oplus$, $\boxdot$

$(a,b) \oplus (c,d) = (a+c, b+d)$
$(a,b) \boxdot (c,d) = (ac-bd, ad+bc)$.

Show that $(S, \oplus, \boxdot)$ is field.

2. IS $(Z[\sqrt{3}], +, \cdot)$ field?

let $x = 1+3\sqrt{3} \in Z[\sqrt{3}]$

$$\frac{1}{x} = \frac{1}{1+3\sqrt{3}} = \frac{1-3\sqrt{3}}{(1+3\sqrt{3})\cdot(1-3\sqrt{3})} = \frac{1-3\sqrt{3}}{-26} = \frac{-1}{26} + \frac{3}{26}\sqrt{3}$$

$\notin Z[\sqrt{3}]$

$\therefore Z[\sqrt{3}]$ is not field.

Theorem: Every field is an integral domain. But the Converse is not true ingeneral for example $(Z,+,\cdot)$ is an integral domain but it is not field.

Theorem

Every finite integral domain is a field.

Proof :-

let $(R, +, \cdot)$ be a finite integral domain and let $R = \{a_1, a_2, \ldots, a_n\}$ من العناصر المختلفة n

Since, R is Comm. ring with unity 1

let a_k be a non-Zero element of R ;

$S = \{a_k \cdot a_1, a_k \cdot a_2, \ldots a_k \cdot a_k, \ldots a_k \cdot a_n\} \subseteq R$

Now, if $a_k \cdot a_t = a_k \cdot a_s$, $t \neq s$

$\Longrightarrow a_t = a_s$ (Since R is an integral domain)

أي أن S ليس فيها عناصر مكررة

Then S has exactly n elements and hence

$S \subseteq R$, also R has n elements. Then

$S = R$.

$1 \in R \Longrightarrow 1 \in S$. Thus $1 \in S \Longrightarrow 1 = a_k \cdot a_r$

for some r, $1 \leq r < n$

$\Longrightarrow a_k$ is an invertible element, $a_k^{-1} = a_r$

Therefore R is field.

□ ——— □

Definition

A division ring is a ring with identity in which every non-Zero element has invertible.

Remark

Every field is a division ring, but the Converse is not true, ingeneral. For example:

let $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$ with usual addition and multiplication operations on matrices. Then $(R, +, \cdot)$ is a ring with identity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Since, for example:

$$\begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 2 \\ 1 & 3 \end{bmatrix}$$

That is $(R, +, \cdot)$ is not Comm. ring, but every element in R has inverse

Therefore, R is division ring but not field.

Definition

let $(F, +, \cdot)$, $(K, +, \cdot)$ be two fields s.t. $F \subseteq K$. Then F is Called a subfield of K.

Remark

let $(F, +, \cdot)$ be a field and let $\emptyset \neq S \subseteq F$. Then $(S, +, \cdot)$ is a subfield of $F \Leftrightarrow$

1. $a - b \in S \quad \forall a, b \in S$
2. $a \cdot b^{-1} \in S \quad \forall a, b \in S$

Example

$Q[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in Q \}$

Then $(Q[\sqrt{2}],+,\cdot)$ is a subfield of $\mathbb{R}$.

let $a+b\sqrt{2}$, $c+d\sqrt{2} \in Q[\sqrt{2}]$. Then

1. $(a+b\sqrt{2})-(c+d\sqrt{2}) = (a-c)+(b-d)\sqrt{2} \in Q[\sqrt{2}]$

2. $(a+b\sqrt{2})\cdot(c+d\sqrt{2})^{-1} = (a+b\sqrt{2})\cdot\dfrac{1}{c+d\sqrt{2}}$

$$= \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}}\cdot\frac{c-d\sqrt{2}}{c-d\sqrt{2}}$$

$$= \frac{ac+ad\sqrt{2}+cb\sqrt{2}-2bd}{c^2-2d^2} = \frac{(ac-2bd)+(ad+cb)\sqrt{2}}{c^2-2d^2}$$

$$= \underbrace{\frac{ac-2bd}{c^2-2d^2}}_{\in Q} + \underbrace{\frac{ad+cb}{c^2-2d^2}}_{\in Q}\sqrt{2} \in Q[\sqrt{2}].$$

Remark:

let F be a fied and let $\{S_\alpha\}$ be any Collection of subfield of F. Then $\cap S_\alpha$ is a subfield of F.

Proof:

Since, $0 \in S_\alpha \quad \forall\alpha \implies \cap S_\alpha \neq \emptyset$

let $a,b \in \cap S_\alpha$

$\implies a,b \in S_\alpha \quad \forall\alpha$

But S_α is a subfield of F $\forall\alpha$

$\therefore a-b \in S_\alpha$, $ab^{-1} \in S_\alpha \quad \forall\alpha$

$\therefore\ a-b \in \bigcap S_\alpha \quad , \quad ab^{-1} \in \bigcap S_\alpha$

$\therefore \bigcap S_\alpha$ is a subfield of F.

المرحله الثالثه/قسم الرياضيات

الماده الحلقات

الفصل الثاني

Chapter Two