Refrences

1- Introduction to modren abstract algebra by D.M. Burton, 1967

2- A First course in abstract algebra by John B. Iraleigh, 1982.

3- A First course in Module theory by M.E. Keating 1998

Course

1- Rings and Subrings

2- Ideals

3- The rings Homomorphism

4- Polynomial rings

5- The series

6- Modules

chapter one: The Rings

Def. 1.1

A nonempty set R with two binary operation $*$ and $\circ$ is said to be ring if:

1- $(R,*)$ is a commutative group, 2- $(R,\circ)$ is semigroup.

3- $a\circ(b*c)=(a\circ b)*(a\circ c)$ (left distribution law)

$(a*b)\circ c=(a\circ c)*(b\circ c)$ (right distribution law)

and will be denoted by $(R,*,\circ)$

Note: we use $+=*$, $\cdot=\circ$ then $(R,+,\cdot)=(R,*,\circ)$

Def. 1.2

A nonempty set $(R,+,\cdot)$ is a ring if

① $(R,+)$ is a commutative group i.e

a- R closed under +

b- + is associative on R

c- R has an identity

d- for each $a\in R$ then $\exists -a$ s.t $a+(-a)=-a+a=0$

e- $a+b=b+a$, $\forall a,b\in R$

② $(R,\cdot)$ is a semigroup i.e

a- R is closed under multi.

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

③ $a\cdot(b+c)=a\cdot b+a\cdot c$ and

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

Ex. 1.6

① $(R,+,\cdot)$ is a ring

② $(Z,+,\cdot)$ // //

③ $(Q,+,\cdot)$ // //

④ $(Z_n,+_n,\cdot_n)$ // //

Def: 1.3
A ring $(R,+,\cdot)$ is said to be commutative ring if
$a \cdot b = b \cdot a \quad \forall a,b \in R$

~~Exam~~
~~Examples:~~

Ex.2: Some examples 1
Def:
A ring $(R,+,\cdot)$ is said to be ring with identity or (with 1) iff R has an identity with mult. i.e if $\exists$ $1 \in R$ s.t $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

Ex3:
$(\mathbb{R},+,\cdot), (\mathbb{Z},+,\cdot), (\mathbb{Q},+,\cdot), (\mathbb{Z}_n,+_n,\cdot_n), (\mathbb{Z}_4,+_4,\cdot_4)$

Ex4:
$(\mathbb{Z}_e,+,\cdot)$ is commutative ring without identity

Ex5:
$(M,+,\cdot)$ is a ring where $M = \{A : A \text{ is } n \times n \text{ matrices}\}$ with the usual added and multi of matrices. $(M,+,\cdot)$ is ring with identity $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ which which not commutative since If $A,B \in M$ then $AB = BA$ ingeneral

Theorem: 1.1
In any ring $(R,+,\cdot)$ if $a \in R$ then $a \cdot 0 = 0 \cdot a = 0$ where 0 is identity with added
Proof:
$a \cdot 0 + a \cdot 0 = a(0+0) = a \cdot 0 = a \cdot 0 + 0$

$\Rightarrow a \cdot 0 + a \cdot 0 - a \cdot 0 = 0 \Rightarrow a \cdot 0 = 0$ (Canslution law

Theorem 1.2:
If $(R,+,\cdot)$ is a ring, $a,b \in R$ then
$(a\cdot b) = a\cdot(-b) = (-a)\cdot b$
Proof:
① T.P $(a\cdot b) = a(-b)$
$a\cdot(-b) + ab = a(-b+b) = a(0) = 0$
$\Rightarrow a(-b) = -(ab)$
② T.P $-(a\cdot b) = (-a)\cdot b$
H.W
③ Since inverse of (ab) is $(-a)b$ by ① and $a(-b)$ by ② and by the uniqueness of an inverse in a group.
Thus $(-a)b = a(-b)$

Def: 1.4
A ring $(R,+,\cdot)$ is said to be have divisor of zero if there exists a non-zero elements $a,b \in R$ s.t $a\cdot b = 0$
(i.e $\exists\, a,b \in R, a \neq 0 \wedge b \neq 0$ but $a\cdot b = 0$)

EX6:
$(Z_{12}, +_{12}, \cdot_{12})$ has divisors of zero since $2 \neq 0$, $6 \neq 0 \in Z_{12}$ and $2 \cdot_{12} 6 = 0$
also $3,4 \in Z_{12} \Rightarrow 3 \cdot_{12} 4 = 12$
$4,6 \in Z_{12} \Rightarrow 4 \cdot_{12} 6 = 24$
$3,8 \in Z_{12} \Rightarrow 3 \cdot_{12} 8 = 24$, $6,10 \in Z_{12} \Rightarrow 6 \cdot_{12} 10 = 0$
Thus 2,3,4,6,8,10 are divisors of zero.

EX7:
$(\mathbb{R},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(Z,+,\cdot)$ has no divisor of zero
EX8:
$(\mathbb{Z},+,\cdot)$ has no divisor of zero.

Remark:
Integral $(\mathbb{Z}_p, +_p, \cdot_p)$ where p is prime has no divisors of zero

Def: 1.5
An integral domain is a commutative ring with identity which does not have divisors of zero

Examples:
- $(\mathbb{R}, +, \cdot)$ is an integral domain
- $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$ is not integral domain since $\mathbb{Z}_{12}$ has divisors of zero, $2, 6 \neq 0$ of belong to $\mathbb{Z}_{12}$ but $2 \cdot_{12} 6 = 0_{12}$
- $(\mathbb{Z}_7, +_7, \cdot_7)$ is an integral domain.

Remark: In general $(\mathbb{Z}_p, +_p, \cdot_p)$ is an integral domain when p is a prime.

Theorem 1.3: A ring $(R, +, \cdot)$ is without divisors of zero iff the cancellation law for multiplication hold in R

Proof: $\Rightarrow$ Suppose that R has no divisors of zero T.p the cancellation law holds in R
If $a, b, c \in R$, $a \neq 0$ and $a \cdot b = a \cdot c$, let $a \neq 0$
$a \cdot b - ac = 0 \Rightarrow a(b-c) = 0$, $\because$ R has no divisors of zero and $a \neq 0$
$b - c = 0 \Rightarrow b = c$
suppose the cancellation law holds in R
s.t $a \cdot b = 0$, if $a \neq 0 \Rightarrow a \cdot b = a \cdot 0 \Rightarrow$
$a, b \in R$

~~~~ let $(R,+,\cdot)$ be a ring with identity which has no divisors of zero, then the only solution of the equation $a^2=a$ are $a=0$ and $a=1$.

proof:

~~~ If $a\neq 0 \Rightarrow a^2=a\cdot a=a \Rightarrow a\cdot a=a\cdot 1$

$\therefore R$ has no divisors of zero by th1.3

the cancel law hold in $R \Rightarrow a=1$

But if $a=0 \Rightarrow a^2=a\cdot a=a\cdot 0=0$

Def 1.6:

~~~ let $(R,+,\cdot)$ be a ring then $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ iff:

① $(S,+)$ is subgroup of $(R,+)$

② $(S,\cdot)$ is a subsemigroup of $(R,\cdot)$

This def is equivalent to the following

Def 1.7:

~~~ let $\phi\neq S\subseteq R$, then $(S,+,\cdot)$ is subring of $(R,+,\cdot)$ iff

① $a-b\in S, \forall a,b\in S$

② $a\cdot b\in S, \forall a,b\in S$

Ex 1.11:

~~~ $(2\mathbb{Z},+,\cdot)$ is subring of $(\mathbb{Z},+,\cdot)$ but $(2\mathbb{Z}_0,+,\cdot)$ is not subring of $(2\mathbb{Z},+,\cdot)$.

Ex 1.12:

~~~ consider the ring $(\mathbb{Z}_{12},+_{12},\cdot_{12})$ let $H_1=\{0,2,4,6,8,10\}$ then $(H_1,+_{12},\cdot_{12})$ is subring of $(\mathbb{Z}_{12},+_{12},\cdot_{12})$

$H_2=\{0,4,8\}$ // N // N

$H_3=\{0,6\}$ // // N N

Remark 1.3:

~~~~ Every ring $(R,+,\cdot)$ have at least two subr[ings] $(R,+,\cdot)$ and $(\{0\},+,\cdot)$ are called the trivial subr
~~~~

Def 1.8:

A ring $(F,+,\cdot)$ is said to be field iff

① $(F,+)$ is comm group

② $(F-\{0\},\cdot)$ is comm group

③ $\cdot$ distribution on the addition

i.e $\forall a,b,c \in F$ the $a\cdot(b+c)=ab+ac$ and So $(a+b)\cdot c = ac+bc$

Theorem 1.4:

A Field has no zero divisors.

proof:

let R be a field and $a,b \in R$ s.t $a\cdot b=0$

let $a\neq 0 \Rightarrow \exists a^{-1} \in R$

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

Similary $b\neq 0$

Corollary:

Every Field is integral domain

proof:

let R be a fielet

$\therefore$ R is comm ring with 1 and by th 1.4

R has no zero divisors

$\therefore$ R is an integral domain

Th 1.5:

A finite integral domain is field

proof:

Let be a finite integral domain containing n elements

i.e: D is comm with identity and without zero divisors

Let $a \in D$ s.t $a\neq 0$

Consider the set $D^* = \{ax : x \in D \text{ and } x\neq 0\}$

$\forall y \in D^* \Rightarrow y \neq 0$ [D without zero divisors]

and $ax=ay \Rightarrow x=y$ [by cancl. law]

Thus all elements of D^* are distinct

$|D^*| = n-1$, nonzero element of D

and $1 \in D$ [D is an int. domain]

oof:
The only thing we need to show is that a typical element $a \neq 0$ has a multiplicative inverse.
Consider $a, a^2, a^3, \ldots$ Since there are only finitly many elements we must have $a^m = a^n$ for some $m < n$ (say). Then $0 = a^m - a^n = a^m(1 - a^{n-m})$. Since there are no zero-divisors we must have $a^m \neq 0$ and hence $a^{n-m} = 0$ and so $1 = a(a^{n-m-1})$ and we have found a multiplicative inverse for a.

Then, each de of D has/mult.inverse

Th 1.6:

A finite commutative ring without zero divisors is a field.

Def 1.9:

Let $(R,+,.)$ be a ring the center of R denoted by $C(R)$ is the set

$C(R)=\{x\in R : x.y=y.x, \forall y\in R\}$

Ex 1.13:

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

$C(\mathbb{R})=\mathbb{R}$

Ex 1.14:

$(M,+,.)$ is a ring whose $M=\{A : A \text{ is } n\times n \text{ matrix}$

$C(M)=I_n$

Th 1.7:

In any ring $(R,+,.)$ then $(C(R),+,.)$ is a subring of $(R,+,.)$.

proof:

$C(R)\subseteq R$ and $\exists\, 0\in C(R)$ s.t $a.0=0.a=0\ \forall a$

$\therefore 0\in C(R) \Rightarrow C(R)\neq\emptyset$.

① let $a,b\in C(R)$

T.p $a-b\in C(R)$

let $x\in R$

$(a-b)x=(a+(-b))x=ax+(-b)x=xa+(-x)b=xa+(-x)(-b)$

$=x(a-b)$

$\therefore a-b\in C(R)$

② T.p $a.b\in C(R)$

let $x\in R$ then $(a.b).x=a.(b.x)=a(x.b)=(ax).b=(xa).b$

$=x(ab)$

subring of $(R,+,.)$

positive integer n, such that $na=0$, $\forall a \in R$.
In case, such an n does not exist, we say that the ring R is of characteristic zero.

Ex 1.15

: a ring $(\mathbb{Z}_7, +_7, \cdot_7)$, the characteristic of $\mathbb{Z}_7$ is 7 since 7 is least positive integer such that $7_7 a = 0$, $\forall a \in \mathbb{Z}_7$

Ex 1.16:

a ring $(\mathbb{Z}, +, \cdot)$ then characteristic of $\mathbb{Z}$ is zero since there exist no positive integer for which $na=0$ $\forall a \in \mathbb{Z}$

Ex 1.17:

$(\mathbb{R}, +, \cdot)$ then the characteristic of $\mathbb{R}$ is zero

Ex 1.18:

the ring $(P(X), \Delta, \cap)$ is of characteristic 2 since 2 since

$2A = A \Delta A = (A-A) \cup (A-A) = \emptyset \cup \emptyset = \emptyset$ for every subset A of X

Th 1.8:

let $(R, +, \cdot)$ be a ring with identity. then $(R, +, \cdot)$ has characteristic $n > 0$ iff n is the least positive integer for which $n.1 = 0$

Proof:

If the ring $(R, +, \cdot)$ is of characteristic $n > 0$, $n.1 = 0$

let $m.1 = 0$ where, $0 < m < n$ then

$m.a = m(1.a) = (m.1)a = 0.a = 0$ $\forall a \in R$

then the characteristic of R is $m \Rightarrow$ C!

since the characteristic of R is n

$n \cdot 1 = 0$

T.p characteristic of R is n

$n \cdot a = n \cdot (1 \cdot a) = (n \cdot 1) \cdot a = 0 \cdot a = 0$, $\forall a \in R$

then characteristic of R is n

Corollary:

The characteristic of an integral domain $(R, +, \cdot)$ is either zero or a prime number.

proof:

let $(R, +, \cdot)$ be of positive characteristic n and assume that n is not prime, then $n = n_1 n_2$

$1 < n_i < n \quad (i = 1, 2)$

$\therefore 0 = n \cdot 1 = (n_1 \cdot n_2) \cdot 1 = (n_1 \cdot 1) \cdot (n_2 \cdot 1)$

since by hopythesis $(R, +, \cdot)$ is without zero divisors, either $n_1 \cdot 1 = 0$ or $n_2 \cdot 1 = 0 \Rightarrow$ C!

since n is the least positive integer such that $n \cdot 1 = 0$

$\therefore$ the characteristic must be prime.

Def 1.11:

In a ring $(R, +, \cdot)$ with identity, we say an element $a \in R$ is invertible if it possesses an inverse relative to multiplication

i.e. $R^* = \{y^{-1} \in R : \exists y \in R \text{ s.t } y^{-1} * y = 1\}$

Ex 1.14:

$(\mathbb{R}, +, \cdot)$

$\mathbb{R}^* = \mathbb{R} - \{0\}$

The Ideal

Def 2.1: A subring $(I,+,\cdot)$ of the ring $(R,+,\cdot)$ is an ideal of $(R,+,\cdot)$ iff $\forall r \in R$ and $a \in I$ then $ra \in I$ and $ar \in I$

This def. is equivalent to the following

Def 2.2:

Let $(R,+,\cdot)$ be a ring and $\phi \neq I \subseteq R$ then $(I,+,\cdot)$ is an ideal of $(R,+,\cdot)$ iff:

1) $a-b \in I \quad \forall a,b \in I$

2) $\forall r \in R$ and $\forall a \in I$ then $ar \in I$ and $ra \in I$

If for each $r \in R, a \in I \Rightarrow ar \in I$ then I is called right ideal. If for each $r \in R, a \in I \Rightarrow ra \in I$ then I is called left ideal.

If I is both right and left then I is called two-sided ideal.

Ex 2.1:

: the ring $(\mathbb{Z},+,\cdot)$ and $I = 2\mathbb{Z}$. show that $(2\mathbb{Z},+,\cdot)$ is an ideal of $(\mathbb{Z},+,\cdot)$

Sol:

let $a,b \in 2\mathbb{Z}$ then $a = 2n, b = 2m$

① $a-b = 2n-2m = 2(n-m)$

$\therefore a-b \in 2\mathbb{Z}$

② let $a \in 2\mathbb{Z}$ and $c \in \mathbb{Z}$

$ac = (2n)c = 2(nc) \Rightarrow ac \in 2\mathbb{Z}$

$ca = c(2n) = (c2)n = (2c)n = 2(cn)$ ($\mathbb{Z}$ is comm.)

$\therefore (2\mathbb{Z},+,\cdot)$ is an ideal of $(\mathbb{Z},+,\cdot)$

Ex 2.2:

Is $(\mathbb{Z},+,\cdot)$ an ideal of $(\mathbb{Q},+,\cdot)$?

Sol:

① let $a,b \in \mathbb{Z}$ then $a-b \in \mathbb{Z}$ and $a \cdot b \in \mathbb{Z}$

$\therefore (\mathbb{Z},+,\cdot)$ is subring of $(\mathbb{Q},+,\cdot)$

2) $3 \in \mathbb{Z}$ and $\frac{2}{5} \in \mathbb{Q}$ but $3 \cdot \frac{2}{5} = \frac{6}{5} \notin \mathbb{Z}$ and $\frac{2}{5}(3) = \frac{6}{5} \notin \mathbb{Z}$

then $(\mathbb{Z}, +, \cdot)$ is not ideal of $(\mathbb{Q}, +, \cdot)$

Ex 2.3: H.W:

Is $(\mathbb{Q}, +, \cdot)$ an ideal of $(\mathbb{R}, +, \cdot)$?

Ex 2.4:

Let M be ring of all 2x2 matrices with their elements as integers.

Let $I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in \mathbb{Z} \right\}$ then

let $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} \in I$

① $A - B = \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \in I$ [since $a_1 - a_2, b_1 - b_2 \in \mathbb{Z}$]

② $A \cdot B = \begin{bmatrix} a_1 a_2 & 0 \\ b_1 a_2 & 0 \end{bmatrix} \in I$ (since $a_1, a_2, b_1, a_2 \in \mathbb{Z}$)

③ if $A = \begin{bmatrix} p & 0 \\ q & 0 \end{bmatrix} \in I$ and $T = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M$ then

$$TA = \begin{bmatrix} ap + bq & 0 \\ cp + dq & 0 \end{bmatrix} \in I$$

Hence, I is a left ideal but not a right ideal of M.

Ex 2.5:

Let $(M, +, \cdot)$ be a ring whose

$M = \{ A : A$ is an 2x2 matrices $\}$

1) let $A=\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}, B=\begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix}$

$A-B=\begin{bmatrix} a_1-a_2 & b_1-b_2 \\ 0 & 0 \end{bmatrix} \in I$ [since $(a_1-a_2)(b_1-b_2) \in Z$]

2) Let

$A=\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, C=\begin{bmatrix} x & y \\ z & t \end{bmatrix}$

$CA=\begin{bmatrix} xa & xb \\ za & zb \end{bmatrix} \notin I$ but $AC=\begin{bmatrix} ax+bz & ay+bt \\ 0 & 0 \end{bmatrix}$

$\in I$. Hence I is a right ideal but not a left ideal.

In any ring $(R,+,\cdot)$ the trivial subrings $(R,+,\cdot)$ and $(\{0\},+,\cdot)$ are both ideals. A ring which contains no ideals except these two is said to be simple.

Th 2.1:

Let $(I_i,+,\cdot)$ be a collection of ideals of $(R,+,\cdot)$ then $(\cap I_i,+,\cdot)$ is also ideal of $(R,+,\cdot)$.

proof:

I_i are ideal $\forall i$ then $0 \in I_i \ \forall i$

$\Rightarrow 0 \in \cap I_i \Rightarrow \cap I_i \neq \emptyset$

① let $x,y \in \cap I_i \Rightarrow x,y \in I_i \ \forall i \Rightarrow x-y \in I_i \ \forall i \Rightarrow x-y \in \cap I_i$

② let $x \in \cap I_i \Rightarrow x \in I_i \ \forall i \Rightarrow$ but I_i is ideal $\forall i$

$\Rightarrow rx \in I_i \ \forall i$ al $\forall r \in R$

$\Rightarrow rx \in \cap I_i$ al $x,r \in \cap I_i$ since I_i is ideal

$\therefore (\cap I_i,+,\cdot)$ is an ideal of $(R,+,\cdot)$

Def: 2.3

Let $(R,+,\cdot)$ be a ring, an ideal $(I,+,\cdot)$ is said to be proper ideal iff $I \neq \{0\}$ and $I \subset R$

Ex 2.6:

$(2\mathbb{Z},+,\cdot)$ is an proper ideal of $(\mathbb{Z},+,\cdot)$

Th 2.2:

If $(I,+,\cdot)$ is a proper ideal of a ring $(R,+,\cdot)$ with identity then no element of I has a multiplicative inverse; that is $I \cap R^* = \emptyset$

proof:

suppose that $I \cap R^* \neq \emptyset \Rightarrow a \in I$ and $a \in R^*$

$\therefore a^{-1} \in R$ then $a \cdot a^{-1} = 1 \in I$ since I is ideal

then $\forall x \in R \quad x \cdot 1 = x \in I \Rightarrow R \subseteq I \Rightarrow I = R \Rightarrow$ C!

$\therefore I \cap R^* = \emptyset$

A field has no proper ideals.

proof:

suppose that I be an ideal of a field F s.t $I \neq \{0\}$

let $0 \neq a \in I$ since $I \subseteq F$

$\therefore a \in I \Rightarrow a \in F$ but $a^{-1} \in F$

$\Rightarrow a \cdot a^{-1} \in I \Rightarrow 1 \in I$

$\therefore \forall x \in F, 1 \cdot x \in I \Rightarrow x \in I$

$\therefore F \subseteq I$ but $I \subseteq F \Rightarrow I = F$

Therefore the only ideals of F are $\{0\}$ and F.

Def 2.4:

let $(R,+,\cdot)$ be a ring and S be a nonempty subset of R. Define the set $(S) = \bigcap \{I : S \subseteq I;$ $(I,+,\cdot)$ is an ideal of $(R,+,\cdot)\}$ the ideal generated by set S.

Ex 2.7:

$(Z'_{12}, +_{12}, \cdot_{12})$ is a ring

$H_1 = Z'_{12}$, $H_2 = \{2,4,6,8,10,0\}$, $H_3 = \{0,4,8\}$

let $S = \{6\}$

$H_1 \cap H_2 = \{0,6\} = (S)$

Th 2.4:

$(S), +, \cdot)$ is smallest ideal of $(R,+,\cdot)$

proof:

Let $\{S_\alpha : \alpha \in \Lambda\}$ be the collection of all ideals of R which containing S

Then $\bigcap \{S_\alpha : \alpha \in \Lambda\}$ is an ideal by (Th 2.1)

if M is any ideal of R contining S then $M \in \{S_\alpha : \alpha \in \Lambda\}$

and therefore $\bigcap \{S_\alpha : \alpha \in \Lambda\} \subseteq M$

Hence $\bigcap \{S_\alpha : \alpha \in \Lambda\}$ is the smallest ideal of R containing R.

Th 2.5:

If $(R,+,\cdot)$ is a commutative ring and $a \in R$ then $Ra = \{ra : r \in R\}$ is an ideal of R

① let $r_1a, r_2a \in Ra$, $r_1, r_2 \in R$
$\therefore r_1a - r_2a = (r_1 - r_2)a \in Ra$ since $r_1 - r_2 \in R$
② let $r_1a \in Ra$
then $r(r_1a) = (rr_1)a \in Ra$ [since $rr_1 \in R$]
$(r_1a)r = r_1(ar) = r_1(ra) = (r_1r)a \in Ra$ [$r_1, r \in R$]
Hence Ra is an ideal of R.

Th 2.6:
A commutative ring with identity is a field if it has no proper ideals

proof:
since R has no proper ideals then R has only R and $\{0\}$
let $a \in R \Rightarrow Ra$ is a non zero ideal of R.
$\Rightarrow Ra = R$
$1 \in R \Rightarrow 1 \in Ra \Rightarrow 1 = ba$ for some $b \in R$
$\therefore ab = 1$ Thus $a^{-1} = b$
$\therefore$ every non-zero element in R has its multiplicative inverse in R, Hence R is a field

Def 2.5:
An ideal of a ring R generated by a single element $a \in R$, is called a principle ideal of the ring and we write $I = (a) = Ra$

Ex 2.8:
~~A ring $(Z, +, \cdot)$ an ideal (~~
Let $(Z, +, \cdot)$ be a ring then $(2Z, +, \cdot)$ is principle ideal of ring $(Z, +, \cdot)$ since $(2) = 2Z$

Remark 2.2:
The principle ideal generated by 0 is the ring $(\{0\}, +, \cdot)$ while the principle ideal generated by the identity element 1 is the ring $(R, +, \cdot)$

A commutative ring $(R,+,.)$ without zero divisors and with unity is called a principle ideal ring if every ideal of R is a principle ideal.

Ex2.8:

Th2.7:

Let $(R,+,.)$ be a commutative ring with unity and let $a \in R$ then, Ra is a principle ideal of R generated by a.

Proof:

$\because 1 \in R \Rightarrow 1.a \in Ra \Rightarrow a \in Ra$

$\therefore Ra$ is an ideal of R containing a

Let S be any ideal of R containing a

$\text{if } r \in R \Rightarrow ra \in Ra$

$\because a \in S, r \in R \Rightarrow ra \in S$ [since S is an ideal containing a]

Therefore $Ra \subseteq S$

Thus, Ra is contained in every ideal containing a and therefore, it is smallest ideal containing a. Hence, Ra is the principle ideal generated by a.

Th2.8: Lijo J.

The ring of integers is a principle ideal ring

Def 2.6:

A nonzero ideal $(I,+,.)$ of a ring $(R,+,.)$ such that $I \neq R$ is called a maximal ideal of R if there exist no proper ideal of R containing I.

i.e I is Max if $I \subset M \subseteq R \rightarrow M = R$

Ex2.9:

$(Z_6, +_6, .6)$ is a ring

$I_1 = \{0,2,4\}, I_2 = \{0,3\}$ then I_1 and I_2 are maximal ideals

$\{0, 2, 4, 6, 8\}$ is a ring
$I_1 = \{0, 2, 4, 6\}$, ~~$I_2 = \{0, 4\}$ are maximal~~ $I_2 = \{0, 4\}$ is maximal but I_2 is not maximal

Th 2.9:

An ideal $(I, +, \cdot)$ of the ring $(\mathbb{Z}, +, \cdot)$ of all integers is a maximal ideal if and only if I is generated by some prime integer.

proof: $\Rightarrow$

let I be an ideal of $\mathbb{Z}$, generated by a prime integer p.

$\Rightarrow I = \mathbb{Z}p = (p)$

If T be an ideal of $\mathbb{Z}$ containing I and generated by some positive integer q, then $T = \mathbb{Z}q = (q)$

$\because I \subseteq T \Rightarrow p = aq$ for some $a \in \mathbb{Z}$

But p is a prime $\Rightarrow q = 1$ or $q = p$

when $q = 1 \Rightarrow T = \mathbb{Z}$

when $q = p \Rightarrow T = I$

Thus the ideal of $\mathbb{Z}$ generated by prime is a maximal ideal of $\mathbb{Z}$

$\Leftarrow$ Let I be a maximal ideal of $\mathbb{Z}$, generated by a positive integer p

T.P p is prime

Suppose that p is composite $\Rightarrow p = mn$, $m \neq 1$ and $n \neq 1$

let $(T, +, \cdot)$ be an ideal of $(\mathbb{Z}, +, \cdot)$ generated by m

i.e $T = (m) = \mathbb{Z}m \Rightarrow I \subseteq T \subseteq \mathbb{Z}$

But, I is maximal $\Rightarrow T = I$ or $T = \mathbb{Z}$

if $T = \mathbb{Z} \Rightarrow T$ is an ideal generated by 1

$\Rightarrow m = 1 \Rightarrow$ C!

if $T = I \Rightarrow m = ap$ for some $a \in \mathbb{Z}$

$\Rightarrow mn = apn \Rightarrow pan = mn$

$\Rightarrow pan = p$

$\Rightarrow an = 1 \Rightarrow n = 1 \Rightarrow$ C!

ideal generated by $S_1 \cup S_2$ ... $S_1 + S_2$ is the ideal

proof:

$0 = 0 + 0 \in S_1 + S_2 \Rightarrow S_1 + S_2 \neq \emptyset$

Let $a_1 + a_2, b_1 + b_2 \in S_1 + S_2$ s.t $a_1, b_1 \in S_1$ and $a_2, b_2 \in S_2$

$\Rightarrow (a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \in S_1 + S_2$

Let $a_1 + a_2 \in S_1 + S_2$, $a_1 \in S_1$ & $a_2 \in S_2$ and $r \in R$ then

$r(a_1 + a_2) = ra_1 + ra_2 \in S_1 + S_2$ [since S_1 & S_2 are ideals]

$(a_1 + a_2) \cdot r = a_1 r + a_2 r \in S_1 + S_2$

$\therefore S_1 + S_2$ is an ideal of R.

Now, we will prove $S_1 + S_2$ generated by $S_1 \cup S_2$

Since $a_1 \in S_1 \Rightarrow a_1 + 0 \in S_1 + S_2 \Rightarrow S_1 \subseteq S_1 + S_2$

$\because a_2 \in S_2 \Rightarrow 0 + a_2 \in S_1 + S_2 \Rightarrow S_2 \subseteq S_1 + S_2$

$\therefore S_1 \cup S_2 \subseteq S_1 + S_2$

If I is an ideal of R s.t $S_1 \cup S_2 \subseteq I$

$\Rightarrow S_1 \subseteq I$ and $S_2 \subseteq I \Rightarrow S_1 + S_2 \in I$

$\therefore S_1 + S_2$ is the smallest ideal containing $S_1 \cup S_2$

$\therefore (S_1 \cup S_2) = S_1 + S_2$

Th 2.11:

Let $(I, +, \cdot)$ be a proper ideal of $(R, +, \cdot)$ then I is a maximal ideal of R iff $I + (a) = R$, $\forall a \notin I$

proof:

$\Rightarrow$ T.P $I + (a) = R$

$\because a \notin I \Rightarrow I \subset I + (a) \subset R$

But I is maximal ideal $\Rightarrow I + (a) = R$

$\Leftarrow$ suppose that $I + (a) = R$, $\forall a \notin I$

T.P I is maximal ideal

let $(J, +, \cdot)$ be an ideal of R

s.t $I \subset J \subseteq R \Rightarrow \exists a \in J, a \notin I \Rightarrow I \subset I + (a)$

$\ast = R \subseteq J \Rightarrow J = R \Rightarrow I$ is maximal

ple ideal (n), $n>1$ is maximal ideal in $\mathbb{Z}$ iff n is prime numbers.
proof: H.w
Zorn's lemma:
Let G be a nonempty family of subsets of some fixed set with the property that for each chain C in G the union $\cup C$ also belongs to G. Then G contains a set which is maximal in the sense that it is not property contained in any members of G.
Th 2.12: Krull-Zorn
In a commutative ring with identity each proper ideal is contained in a maximal ideal
proof:
Let $(I,+,\cdot)$ be any proper ideal of comm ring with identity $(R,+,\cdot)$. Define a family $G=\{J : I \subseteq J ; J \text{ is proper ideal of } R\}$
$\because I \in G \Rightarrow$ let $\{J_i\}$ chain in G
$\because \cup J_i \neq R$ since $1 \notin J_i$, $\forall i$ and $1 \in R$
let $a,b \in \cup J_i$
$\Rightarrow \exists J_i, J_j$ s.t $a \in J_i, b \in J_j$
but $\{J_i\}$ is chain $\Rightarrow$ either $J_i \subseteq J_j$ or $J_j \subseteq J_i$ then
let $J_i \subseteq J_j \Rightarrow a-b \in J_j \Rightarrow a-b \in \cup J_i$
let $a \in \cup J_i$ and $r \in R$
then $\exists j$ s.t $a \in J_j$ but J_j is ideal
$\Rightarrow ar \in J_j \Rightarrow ar \in J_j$ also $ra \in \cup J_i \Rightarrow ar \in \cup J_i$
$\therefore \cup J_i$ is proper ideal of R
and since $I \subseteq \cup J_i \Rightarrow \cup J_i \in G$
By Zorn's lemma then G contains a maximal element $M \in G$ therefore $I \subseteq M$ and M is maximal ideal
$M \subset I \subseteq R$

Th 2.13:

In a commutative ring with identity $(R,+,\cdot)$ an element $a \in R$ is invertible iff it belongs to no maximal ideal of R.

Proof:

$\Rightarrow$ suppose that $a \in R$, a is invertible
$\Rightarrow a$ belongs to no proper ideal of R then by (krull-Zorn) Th 2.12 a belong to no maximal ideal.

$\Leftarrow$ Suppose that $a \notin M$, M is maximal ideal of R
T.P a is invertible
let $a \in R$, $a \notin M$
$\Rightarrow (a)$ is an ideal of R
either $(a) \subset R$ or $(a) = R$
If $(a) \subset R \Rightarrow$ by th 2.12 $(a) \subset M \Rightarrow a \in M$ (maxim
$\because (a) = R \Rightarrow 1 \in (a) = \{ra : r \in R\}$
$\Rightarrow 1 = ra, r \in R \Rightarrow a^{-1} = r$
$\therefore a$ is invertible.