Ring & Field

by

Waseem Akram

https://www.mathcity.org/people/waseem-akram

Lectures 2026

Ms. Arsla Afzal

Department of Mathematics
Govt Islamia College
Sargodha Road, Faisalabad

Collected and composed by Waseem Akram

Available at https://www.MathCity.org

Ring & Field

by

Waseem Akram

Ring :

The structure $(R,+,\times)$ consisting of non void set R with two binary composition denoted by $+$ and $\times$ is said to be a ring if the following axiom are satisfied

$[\mathbf{R}_1]$ $(R,+)$ is an abelian group.

$[\mathbf{R}_2]$ $(R,\times)$ is a semi group .

$[\mathbf{R}_3]$ R hold distributavie law.

i.e $\forall\ a,b,c \in R\ \ a(b+c) = a.b + a.c$ (left distributive law)

$(a+b)\times c = a\times c + b\times c$ (Right distributavie law)

Examples :

(1) $(\mathbb{Z},+,\times),(\mathbb{R},+,\times),(\mathbb{C},+,\times),(m\mathbb{Z},+,\times),(\mathbb{Q},+,\times)$.

(2) The set M of all $n\times n$ matrices with real numbers as their element is ring.

(3) The algebraic structure $(Z_n,+_n,\times_n)$ is a is ring .

Example : $Q\left(\sqrt{2}\right) = \left\{a+b\sqrt{2}; a,b\in Q\right\}$ .Prove that it is a ring with operation addition and multiplication.

Solution :

Let $x = a+b\sqrt{2}; y = c+d\sqrt{2}$ where $a,b,c,d \in Q$

Closure under addition :

$$\begin{aligned} x+y &= (a+b\sqrt{2})+(c+d\sqrt{2}) \\ &= (a+c)+(b+d)\sqrt{2} \end{aligned}$$

Since, $a+c\in Q, b+d\in Q$

$\Longrightarrow x+y \in Q\left(\sqrt{2}\right)$

Additive Identity :

$$O = 0+0\sqrt{2} \in Q\left(\sqrt{2}\right) \text{ and } A = a+b\sqrt{2}$$

$$\begin{aligned} \Longrightarrow\ O+A &= (0+0\sqrt{2})+(a+b\sqrt{2}) \\ &= a+b\sqrt{2} \end{aligned}$$

Additive Inverse:

For

$$\begin{aligned} x &= a+b\sqrt{2} \\ -x &= -a-b\sqrt{2} \end{aligned}$$

Since,

$$\begin{aligned} -a,-b\sqrt{2} &\in \mathbb{Q} \\ &\Rightarrow -x \in \mathbb{Q}\sqrt{2} \end{aligned}$$

Commutative Under Addition :

$$\begin{aligned} x+y &= y+x \\ a+b\sqrt{2}+c+d\sqrt{2} &= c+d\sqrt{2}+a+b\sqrt{2} \\ (a+c)+(b+d)\sqrt{2} &= (c+d)+(b+d)\sqrt{2} \end{aligned}$$

Associativity of addition:

$$(x+y)+z = x+(y+z)$$

L.H.S

$$\begin{aligned} x &= a+b\sqrt{2} \\ y &= c+d\sqrt{2} \\ z &= e+f\sqrt{2} \end{aligned}$$

$\Rightarrow$

$$\begin{aligned} &= \left(a+b\sqrt{2}+c+d\sqrt{2}\right)+e+f\sqrt{2} \\ &= \left((a+c)+(b+d)\sqrt{2}\right)+e+f\sqrt{2} \\ &= (a+c+e)+(b+d+f)\sqrt{2} \end{aligned}$$

R.H.S

$$\begin{aligned} &= a+b\sqrt{2}+\left(\left(c+d\sqrt{2}\right)+\left(e+f\sqrt{2}\right)\right) \\ &= \left(a+b\sqrt{2}\right)+(c+e)+(d+f)\sqrt{2} \\ &= (a+c+e)+(b+d+f)\sqrt{2} \end{aligned}$$

Closure under Multiplication:

$$x = a+b\sqrt{2}; y = c+d\sqrt{2}$$

$$\begin{aligned} x.y &= \left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right) \\ &= ac+ad\sqrt{2}+bc\sqrt{2}+bd\left(\sqrt{2}\right)^2 \\ &= (ac+2bd)+(ad+bc)\sqrt{2} \end{aligned}$$

As $ac+2bd \in \mathbb{Q}, ad+bc \in \mathbb{Q}$
Hence, $xy \in \mathbb{Q}$
Associativity of Multiplication :

$$\begin{aligned} (xy)\,z &= x\,(yz) \\ L.H.S &= \left(\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)\right)\left(e+f\sqrt{2}\right) \\ &= \left(ac+ad\sqrt{2}+bc\sqrt{2}+bd\,(2)\right)\left(e+f\sqrt{2}\right) \\ &= \left((ac+2bd)+(ad+bc)\sqrt{2}\right)\left(e+f\sqrt{2}\right) \\ &= (ac+2bd)\left(e+f\sqrt{2}\right)+(ad+bc)\sqrt{2}\left(e+f\sqrt{2}\right) \\ &= ace+acf\sqrt{2}+2bde+2bdf\sqrt{2}+ade\sqrt{2}+2adf+bce\sqrt{2}+2bcf \\ &= (ace+2bde+2adf+2bcf)+(acf+2bdf+ade+bce)\sqrt{2} \end{aligned}$$

$$\begin{aligned} R.H.S &= \left(a+b\sqrt{2}\right)\left(\left(c+d\sqrt{2}\right)\left(e+f\sqrt{2}\right)\right) \\ &= \left(a+b\sqrt{2}\right)\left(ce+cf\sqrt{2}+de\sqrt{2}+2df\right) \\ &= \left(a+b\sqrt{2}\right)\left((ce+2df)+(cf+de)\sqrt{2}\right) \\ &= \left(a+b\sqrt{2}\right)(ce+2df)+\left(a+b\sqrt{2}\right)(cf+de)\sqrt{2} \\ &= (ace+2bde+2adf+2bcf)+(acf+2bdf+ade+bce)\sqrt{2} \end{aligned}$$

Distributive Laws :

Multiplication distribution over addition over addition in R .Since, $\mathbb{Q}$ is a subset of R so ,it also holds in $\mathbb{Q}$

$$\begin{aligned} x(y+z) &= xy+xz \\ &= xz+yz \end{aligned}$$

for all $x, y, z \in \mathbb{Q}\sqrt{2}$
$So, that\ \mathbb{Q}\left(\sqrt{2}\right)$ is a ring .

Commutative ring :

If for all $a, b \in R$ if $ab = ba$ OR If commutative law w.r.t multiplication holds for all elements of R then R is called commutative ring .More ever,If miltiplication identity exists in R is called Ring with unity .

Unit element of Ring :

For any $a \in R$ if there is $a^{-1} \in R$ s.t $a.a^{-1} = a^{-1}.a = 1$ then a is called unit element of R.

Division Ring (Skew field) :

A ring R is said to be division ring if all non zero elements of R have their multiplicative inverses in R . OR each non zero element of R is unit in R .

Note :

Every field is also a division ring but only commutative division ring is field .

Field :

A commutative division ring is known as field OR A set F is said to be field if it satisfies
(1) $(F, +)$ is abelian group.
(2) $(F, \times)$ is abelian group.
(3) Distributive law hold for all elements of F.

Zero divisor :

A non zero element a a of a commutative ring R is called zero divisor if there is a non zero element b s.t $ab = 0$

Example# :

$Z_6 = \{0, 1, 2, 3, 4, 5\}$
$2.3 = 0 = 3.2$,3 and 2 are zero divisor .

Theorem :

A ring R is without zerodivisor iff the cancellation law holds in R.
Pr**oof** : Let R is without zerodivisor

Suppose that $a \neq 0$

$$\begin{aligned} ab &= ac \\ &\Longrightarrow ab - ac = ac - ac \\ &\Longrightarrow ab - ac = 0 \\ &\Longrightarrow a(b-c) = 0 \ \because a \neq 0 \\ &\Longrightarrow b - c = 0 \\ &\Longrightarrow b = c \end{aligned}$$

Similary,$a \neq 0$

$$\begin{aligned} ba &= ca \\ &\Longrightarrow ba - ca = ca - ca \\ &\Longrightarrow ba - ca = 0 \\ &\Longrightarrow a(b-c) = 0 \quad \because a \neq 0 \\ &\Longrightarrow b - c = 0 \\ &\Longrightarrow b = c \end{aligned}$$

$\Longrightarrow$ If R is without zero divisor then the cancellation law holds.
Conversly,

Suppose that the cancellation law holds in R if $a \in R$ and $a \neq 0$

$$\begin{aligned} ab &= 0 \\ &\Longrightarrow ab = a0 \, (\because a0 = 0) \\ &\Longrightarrow b = 0 \ \because a \neq 0 \end{aligned}$$

$\Longrightarrow R$ is a ring without zero divisors.■
Theorem : **A skew field has no zero divisors.**
Pr**oof**

Let D be a skew field .Then D is a ring with unity and has multiplicative inverse of every non-zero elements .Let $a, b \in D$ with $a, b \neq 0$ Now, as $a \neq 0$ so a^{-1} exists
Now suppose

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

Again if $b \neq 0$ so, b^{-1}exists

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

So, a skew field has no zero divisor.■

Integral domain :

A commutative ring without zero divisor is called integral domain.

Example#

$\mathbb{Z}$ = set of integers is integral domain

Note : For integral domian D if $ab = 0$ either $a = 0$ or $b = 0$ $\forall a, b \in D$.

Lemma :

A commutative ring R is called integral domain iff it holds cancellation law .

Pr**oof** :

let R be an integral domain .Let $ab = ac$ $(a \neq 0)$

$$\begin{aligned} ab &= ac \\ ab - ac &= ac - ac \\ ab - ac &= 0 \\ a(b - c) &= 0 \end{aligned}$$

Since,$a \neq 0$

$$\begin{aligned} &\Rightarrow \quad b - c = 0 \\ &\Rightarrow \quad b = c \end{aligned}$$

Conversly,

Let the given condition holds .Let $a, b \in R$ be any elements with $a \neq 0$ .Suppose

$$\begin{aligned} ab &= 0 \\ ab &= a.0 \\ &\Rightarrow \quad b = 0 \end{aligned}$$

using the given condition

$Hence$, $ab = 0$

$\Rightarrow b = 0$ whenever $a \neq 0$ OR that R is an integral domain.■

Characteristic of a ring :

If for any ring $(R, +, \times)$ there exists a least $+ve$ integer n s.t $(a + a + a \cdots\cdots + a)_{n \text{ times}} = na = 0$ $\forall a \in R$ then n is called characteristics of R.

If possible there does not exists any $+ve$ interger n such that $na = 0$ $\forall a \in R$ then we say $n = 0$ i.e the given R is of characteristic of 0.

Example:

Set of integer, set of rational number, set of Real number Set of complex number ,Set of even integers has characteristics zero.

Remark:

If n is the least positive integers such that $na = 0$ $\forall a \in R$ then $O(a) = n$ it means that order of any elements is equal to ch of R i.e $O(a) = ch(R)$ $\forall a \in R$

Idempotent Element :

For any $x \in R$ if $x^2 = x$ then x is called idempotent element.

Nilpotent Elements :

For any $x \in R$ if $x^n = 0$ for some integer n then x is called a nilpotent element .

Bolean Ring :

If each element of ring is idempotent then ring is bolean ring

Lemma: If R is bolean ring then

(1) $2a = 0$

$\forall a \in R$

(2) $ab = ba$ i.e R is commutative.

Proof :

$$\begin{aligned} 2a &= a + a = (a+a)^2 \\ &= a^2 + a^2 + a^2 + a^2 = 4a^2 \\ 2a &= 4a^2 = 4a \\ &\Longrightarrow 4a - 2a = 0 \\ 2a &= 0 \end{aligned}$$

$(ii)\, ab = ba$

Let $(R, +, \cdot)$ is a boolian ring $\forall a \in R \Rightarrow a^2 = a$

let $a \in R \Rightarrow a + a \in R$

$$\begin{aligned} \left(a + a^2\right) &= a + a \\ &\Rightarrow (a+a)(a+a) = a + a \\ &\Rightarrow a^2 + a^2 + a^2 + a^2 = a + a \\ &\Rightarrow a + a + a + a = a + a \\ &\Rightarrow a + a = 0 \\ &\Rightarrow a = -a \cdots\cdots (i) \end{aligned}$$

Now ,Let $a, b \in R$

$$\begin{aligned} (a+b)^2 &= (a+b)(a+b) \\ a + b &= a^2 + ab + ba + b^2 \\ a + b &= a + b + ab + ba \\ &\Rightarrow ab + ba = 0 \\ &\Rightarrow ab = -ba \\ &\Rightarrow ab = -b(-a) \quad \text{using } (i) \\ &\Rightarrow ab = ba \end{aligned}$$

hence, commutative hold.■

Subring :

A subset S of ring R is said to be subring .If it satisfies all the axiom of R .

Theorem:

A subset S of a ring R is subring of R iff S satisfies $\forall a, b \in S$

(i) $a - b \in S$

(ii) $ab \in S$

Pr**oof** : First suppose S is a subring of R.

$\Longrightarrow$ S satifies all properties of R for $a, b \in S$ so $a, -b \in S$

and hence $a - b \in S$ ($\because$ S is abelian group under addition)

also for $a, b \in S, ab \in S$ ($\because$ S is semi group under multiplication) .

Hence, (i) and (ii) holds

Conversly,

Let (i) and (ii) holds for all $a, b \in S \because S \subset R$ and R is abelian under addition so by subgroup test $\because a - b \in S$ for all $a, b \in S$.

$\Longrightarrow S$ is subgroup under addition .Moreover,commutative property under addition holds for all elements of R so it does holds for all elements of S $(i.e\ S \subset R)$.

$\Longrightarrow S$ is abelian under addition .Next $\because \forall a, b \in S$ that implies $ab \in S$.

S is closed under multiplication .Also since associative property under multiplication holds for all elements of R so it does holds for all elements of S .

$\Longrightarrow S$ is semi group under multiplication .

Further, Since distributivity holds for all elements of R so, it holds for all the element of S because $S \subset R$.Combining all three results,we obtain

(i) S is abelian group under addition .

(ii) S is semi group under multiplication

(iii) Distributive law holds for S .

Hence, S is ring .($\because S \subset R$ so S is subring of R) .

Theorem :

Intersection of any two subring is again a subring .

Pr**oof** :

let S_1 and S_2be two subrings of a ring R .

$$\begin{aligned} 0 \quad &\in \quad S_1 \text{ and } 0 \in S_2 \Longrightarrow 0 \in S_1 \cap S_2 \\ &\Longrightarrow \quad S_1 \cap S_2 \neq 0 \end{aligned}$$

Now ,Let

$$\begin{aligned} a, b \quad &\in \quad S_1 \cap S_2 \\ &\Longrightarrow \quad ab \in S_1 \text{and } ab \in S_2 \\ &\Longrightarrow \quad a - b \in S_1, ab \in S_1 \text{ and } a - b \in S_2, ab \in S_2 \\ &\Longrightarrow \quad a - b \in S_1 \cap S_2 \text{ and } ab \in S_1 \cap S_2 \end{aligned}$$

$\Longrightarrow S_1 \cap S_2$ is a subring of R.

corollary :

Arbitrary intersection of subring is again a subring.

Center of Ring :

Let R be a ring The set of elements of R is said to be center of ring $C(R)$ if each element of this set commute with all the elements of R. OR $C(R) = \{x | x \in R, xa = ax\ \forall x \in R\}$

Theorem :

Center of a ring is subring of ring.

Pr**oof** :

Let R be ring and $C(R) = \{x | x \in R, xa = ax \ \forall x \in R\}$ for any $x_1, x_2 \in C(R)$;$x_1 a = a x_1, x_2 a = a x_2$

$$\begin{aligned} (x_1 - x_2)\, a &= x_1 a - x_2 a \quad \textit{Associativity} \\ &= a x_1 - a x_2 \quad (\text{by def } C(R)) \\ &= a(x_1 - x_2) \quad \text{Distributivity} \\ &\Longrightarrow x_1 - x_2 \in C(R) \end{aligned}$$

similarliy ,

$$\begin{aligned} (x_1 x_2) &\in a = x_1 (x_2 a) \quad \text{Associativity} \\ &= x_1 (a x_2) \quad (\text{by def } C(R)) \\ &= (a x_1) x_2 \quad \text{Associativity} \\ &= a(x_1 x_2) \quad (\text{by def } C(R)) \\ &\Longrightarrow x_1 x_2 \in C(R) \end{aligned}$$

Hence, $C(R)$ is subring of R.

Theorem :

Every finite integral domain is field .

Pr**oof** :

Let $D = \{x_1, x_2, \cdots x_n\}$ be a finite integral domian .To prove D is field we have to show

(i) $1 \in D$

(ii) For any nonzero element of D its multiplicative inverse also belongs to D.

For this consider $a \neq 0, a \in D$ and form the set $\{x_1 a, x_2 a \cdot \cdot x_n a\}$ .Since D being integral domian is closed under multiplication so, $\{x_1 a, x_2 a \cdots \cdot x_n a\} \subseteq D$. Let

$$\begin{aligned} x_i a &= x_j a \quad i \neq j \\ &\Longrightarrow x_i a - x_j a = 0 \\ &\Longrightarrow (x_i - x_j)\, a = 0 \end{aligned}$$

Since ,$a \neq 0$ and D is integral domian so,

$$\begin{aligned} x_i - x_j &= 0 \\ &\Longrightarrow x_i = x_j \end{aligned}$$

$\Longrightarrow$ each element of set $\{x_1 a, x_2 a \cdots x_n a\}$ is distinic OR $\{x_1 a, x_2 a \cdots x_n a\} = D$ .Next let

$$y \in D \quad y \neq 0$$

$\Longrightarrow$

$$\begin{aligned} y &= x_i a \qquad \text{But } a \neq 0, a \in D \\ &\Longrightarrow a = x_j \ \text{ for some } j \\ &\Longrightarrow y = x_i (x_j a) \\ &= x_i (a x_j) \quad \because D \text{ is commutative} \\ &= (x_i a) x_j \\ y &= y x_j = 1 \in D \end{aligned}$$

Also for $a \neq 0 \in D$ and $1 \in D$ there must exist $a, b \neq 0, b \in D$ s.t $a, b = 1$.
$\Longrightarrow$ Each non zero element of D has its multiplicative inverse in D.
Hence, D is field.

Theorem :

Z_p is field where p is prime.

Pr**oof** :

$Z_p = \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{p-1}\right\}$. we have to show that Z_p is integral domain .For this let $a, b \in Z_p$ s.t $a.b = 0$ Since, p is prime .Now in Z_p $a.b = 0$

$$\begin{aligned} &\Longrightarrow ab \equiv 0 \bmod p \quad \text{OR } P|ab \\ &\Longrightarrow \text{either } p|a \text{ or } \ p|b \end{aligned}$$

if $p|a$ that implies $a \equiv 0 \bmod p$ OR if $p|b$ that implies $b \equiv 0 \bmod p$
$\Longrightarrow$ either $a = 0$or $\ b = 0$.
$\Longrightarrow$ Z_p is integral domian also it is finite .So, Z_p is field.

Ring Homomorphism :

A ring homomorphism Φ from a ring $< R, +, \times >$ to a ring $< R^{'}, +, \times >$ is a mapping from to $R^{'}$ that preserve the the two ring operation $i.e$ $\forall$ $a, b \in R$
$(i)\ \Phi(a + b) = \Phi(a) + \Phi(b)$
$(ii)\ \Phi(a.b) = \Phi(a)\ .\ \Phi(b)$

Ring Isomorphism:

A ring homomorphism that is both one-one and onto is called ring homomorphism .

Example: $< \mathbb{C}, +, . >$ be a ring .

Define a maping $\Phi : \mathbb{C} \to \mathbb{C}$ s.t $\Phi(a + ib) = a - ib \qquad \forall a, b \in R \ \ \Phi(Z) = \overline{Z}$ where $Z = a + ib \in \mathbb{C}$
Let $Z_1, Z_2 \in \mathbb{C}$ Where $Z_1 = a + ib$ and $Z_2 = c + id$
$(i)\ \Phi(Z_1 + Z_2) = \Phi(Z_1) + \Phi(Z_2)$
$L.H.S$

$$\begin{aligned} \Phi(Z_1 + Z_2) &= \Phi(a + ib + c + id) \\ &= \Phi((a + c) + i(b + d)) \\ &= (a + c) - i(b + d) \\ &= a - ib + c - id \\ &= \Phi(Z_1) + \Phi(Z_1) = R.H.S \end{aligned}$$

$(ii)\,\Phi(Z_1Z_2) = \Phi(Z_1).\Phi(Z_2)$

$$\begin{aligned} L.H.S = \Phi(Z_1Z_2) &= \Phi((a+ib)(c+id)) \\ &= \Phi(ac-bd+iad+ibc) \\ &= \Phi(ac-bd+i(ad+bc)) \\ &= ac-bd-i(ad+bc) \\ &= ac-bd-iad-ibc \\ &= ac-iad-bd-ibc \\ &= a(c-id)-ib(c-id) \\ &= (c-id)(a-ib) \\ &= \Phi(Z_1)\Phi(Z_2) \end{aligned}$$

$\Rightarrow \Phi$ is a ring homomorphism.

Example $< Z, +, . >$ and $< Z_n, +_n, \times_n >$ are two rings

$\Phi : Z \to Z_n$ s.t $\Phi(x) = x \bmod n \quad \forall x \in Z$

Let $xy \in Z$ to show

$(i)\,\Phi(x+y) = \Phi(x) +_n \Phi(y)$

$$\begin{aligned} \Phi(x+y) &= (x+y) \bmod n \\ &= (x \bmod n + y \bmod n) \bmod n \\ &= x \bmod n +_n y \bmod n \\ &= \Phi(x) +_n \Phi(y) \end{aligned}$$

$(ii)\,\Phi(xy) = \Phi(x) \times_n \Phi(y)$

$$\begin{aligned} \Phi(xy) &= (xy) \bmod n \\ &= [(x \bmod n).(y \bmod n)] \bmod n \\ &= x \bmod n \times_n y \bmod n \\ &= \Phi(x) \times_n \Phi(y) \end{aligned}$$

$\Rightarrow \Phi$ is a ring homomorphism

Theorem :

If $\Phi : R \to R'$ is a ring homomorphism .The image of Φ is a subring of R' also $\ker \Phi$ is subring of R.

Proof:

Let $\Phi : R \to R'$ be a ring homomorphism ,Clearly$\Phi(R) \subseteq R'$ .For any two

$$\begin{aligned} r_1, r_2 \quad &\in \quad R, \Phi(r_1), \Phi(r_2) \in R' \text{ where } \Phi(r_1) = r_1', \Phi(r_2) = r_2' \\ &\Longrightarrow \quad \Phi(r_1) - \Phi(r_2) = \Phi(r_1) + \Phi(-r_2) \qquad \because \Phi \text{ is homomorphism} \end{aligned}$$

And

$$\begin{aligned} r_1', r_2' &= \Phi(r_1).\Phi(r_2) \\ &= \Phi(r_1r_2) \qquad \because \Phi \text{ is homomorphism} \\ &= \Phi(r_1r_2) \in \Phi(R) \end{aligned}$$

Hence, $\Phi(R)$ is subring of R.

Now, we prove $\ker\Phi$ is subring of R.

$$\begin{aligned}
\ker\Phi &= \{r\in R|\Phi(r)=0\} \text{ is subset of } R \text{ for any}\\
\text{two elements } r_1,r_2 &\in \ker\Phi\\
\Phi(r_1) &= 0, \Phi(r_2)=0\\
(i)\qquad \Phi(r_1-r_2) &= \Phi(r_1)-\Phi(r_2) \qquad \because \Phi \text{ is homomorphism}\\
&= 0-0\\
&\Longrightarrow (r_1-r_2)\in\ker\Phi\\
(ii)\quad \Phi(r_1r_2) &= \Phi(r_1)\Phi(r_2) \qquad \because \Phi \text{ is homomorphism}\\
&= 0.0\\
&= 0\\
&\Longrightarrow r_1r_2\in\ker\Phi
\end{aligned}$$

Hence, $\ker\Phi$ is subring of R.

Ideal of a Ring :

Left Ideal :

A subset I of a ring R is said to be an left ideal if it satisfies two axioms:

(1) For $a,b\in I$
$a-b\in I$

(2) For $a\in I, r\in R; ar\in R$

and subset I of R is said to be right ideal i

Right ideal :

A subset I of R is said to be right ideal if

(i) $\forall a,b\in I, r\in R, a-b\in I$

(ii) $\forall a\in I, r\in R\Longrightarrow ar\in I$

A subset I of R is said to be ideal of R if it is both left and right ideal $i.e$

(i) $\forall a,b\in I\Longrightarrow a-b\in I$

(ii) $\forall r\in R, a\in I\Longrightarrow ar\in I$ and $ra\in I$

Example :

For Ring$(\mathbb{Z},+,\cdot)$ the subset $2\mathbb{Z}$ of $\mathbb{Z}$ is ideal of $\mathbb{Z}$

Solution :

$\mathbb{Z}=\{0,\pm1,\pm2,\cdots\cdot\}$

$2\mathbb{Z}=\{0,\pm2,\pm4,\cdots\}$

For any $a,b\in 2\mathbb{Z}$

(i) $a=2x, b=2y$ where $x,y\in\mathbb{Z}$

$$\begin{aligned}
a-b &= 2x-2y\\
&= 2(x-y)\in 2\mathbb{Z}
\end{aligned}$$

(ii) For any $n\in\mathbb{Z}, a\in 2\mathbb{Z}, a=2x$

$$\begin{aligned}
n.a &= n(2x)\\
&= 2(nx)\in 2\mathbb{Z}
\end{aligned}$$

Hence,$2\mathbb{Z}$ is an ideal .

Example :

For any Ring of all 2×2 matrices.
$M_{2\times 2} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $a, b, c, d \in \mathbb{Z}$ .The following subset $I = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ where $a, b \in \mathbb{Z}$ .Prove that it is left ideal but not right ideal .

Solution :

Let $A = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ $R = \begin{bmatrix} a^{'} & b^{'} \\ c^{'} & d^{'} \end{bmatrix}$.To prove it is left ideal we prove two Properties

(i) $A, B \in I \Longrightarrow A - B \in I$

(ii) *For* any $R \in M, A \in I \Longrightarrow RA \in I$

(i)

$$\begin{aligned} A - B &= \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a_1 - a_1 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \\ &\Longrightarrow A - B \in I \end{aligned}$$

(ii)

$$\begin{aligned} RA &= \begin{bmatrix} a^{'} & c^{'} \\ b^{'} & d^{'} \end{bmatrix} \times \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a^{'}a_1 + c^{'}b_1 & 0+0 \\ b^{'}a_1 + d^{'}b_1 & 0+0 \end{bmatrix} \\ &= \begin{bmatrix} a^{'}a_1 + c^{'}b_1 & 0 \\ b^{'}a_1 + d^{'}b_1 & 0 \end{bmatrix} \\ &\Longrightarrow RA \in I \end{aligned}$$

Hence ,it is left ideal .Now, we check it is right ideal or not ?

(i)

$$\begin{aligned} A - B &= \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a_1 - a_1 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \\ &\Longrightarrow A - B \in I \end{aligned}$$

(ii)

$$\begin{aligned} AR &= \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \times \begin{bmatrix} a^{'} & c^{'} \\ b^{'} & d^{'} \end{bmatrix} \\ &= \begin{bmatrix} a_1a^{'} + 0 & a_1c^{'} + 0 \\ b_1a^{'} + 0 & b_1c^{'} + 0 \end{bmatrix} \\ AR &= \begin{bmatrix} a_1a^{'} & a_1c^{'} \\ b_1a^{'} & b_1c^{'} \end{bmatrix} \\ &\Longrightarrow AR \notin I \end{aligned}$$

Hence, it is not an right ideal.
Note :
(i) For a commutative ring any ideal of ring is both left and right.
(ii) Every ideal of R is subring of R but every subring of R need not to be ideal of R
(iii) The trivial subring $\{0\}$ and R (itself) are also trivial ideal.
Theorem :

Let $\Phi : R \to R^{'}$ **be a ring homomorphism then** $\ker \Phi$ **is ideal of** R.

Pr**oof**

Let $a, b \in \ker \Phi \Longrightarrow \Phi(a) = 0, \Phi(b) = 0$

(i)

$$\begin{aligned} \Phi(a-b) &= \Phi(a) - \Phi(b) \\ &= 0 - 0 \\ &= 0 \\ &\Longrightarrow a - b \in \ker \Phi \end{aligned}$$

(ii) For any $r \in R, a \in \ker \Phi, \Phi(a) = o$

$$\begin{aligned} \Phi(ar) &= \Phi(a)\Phi(r) \\ &= 0 \cdot \Phi(r) \\ &= 0 \end{aligned}$$

Similarliy,

$$\begin{aligned} \Phi(ra) &= \Phi(r)\Phi(a) \\ &= 0 \end{aligned}$$

$\Longrightarrow ar, ra \in \ker \Phi$ and hence, $\ker \Phi$ is ideal of R.
Theorem :
Let R be ring and I, J be two ideals of R then
(i) $I \cap J$ is ideal
(ii) $I + J$ is ideal
(ii) IJ is ideal
Pr**oof** :

(i) Let

$$\begin{aligned} a, b &\in I \cap J \\ &\Longrightarrow a, b \in I \text{ and } a, b \in J \\ &\Longrightarrow a - b \in I \text{ and } a - b \in J \because I \text{ and } J \text{ both are ideal} \\ &\Longrightarrow a - b \in I \cap J \end{aligned}$$

Further, For any

$$a \in I \cap J \text{ and } r \in R, a \in I, b \in J$$

Since, IJ are ideals So, there is $r \in R$ s.t $ar, ra \in I$ and $ra, ar \in J$ So, that $ar, ra \in I \cap J$. $Hence, I \cap J$ is an ideal

(ii) $I+J=\{a+b; a\in I, b\in J\}$ .Let $x,y\in I+J$ where $x=a_1+b_1; y=a_2+b_2$

$$\begin{aligned} x-y &= (a_1+b_1)-(a_2+b_2) \\ &= (a_1-a_2)+(b_1-b_2) \end{aligned}$$

Here,

$$\begin{aligned} a_1-a_2 &\in I \text{ and } b_1-b_2\in J \\ &\Longrightarrow x-y\in I+J \quad \text{because } I \text{ and } J \text{ are ideal} \end{aligned}$$

For any $r\in R$ and $x\in I+J$ wher $x=a_1+b_1$

$$\begin{aligned} rx &= r(a_1+b_1) \\ &= ra_1+rb_1 \because ra_1\in I \text{ and } rb_1\in J \\ &\Longrightarrow ra_1+rb_1\in I+J \end{aligned}$$

Similarly,$(a_1+b_1)\, r\in I+J$.
$Hence, I+J$ is an ideal
(iii) $IJ=\{a_1b_1+a_2b_2+\cdots a_nb_n \;\; ; a_i\in I, b_i\in J\}$

Let $xy\in IJ$ where $x=a_1b_1+a_2b_2+\cdot\cdot$ and $y=a_1^{'}b_1^{'}+a_2^{'}b_2^{'}+\cdots$

$$\begin{aligned} x-y &= (a_1b_1+a_2b_2+\cdots a_nb_n)-\left(a_1^{'}b_1^{'}+a_2^{'}b_2^{'}+\cdots+a_n^{'}b_n^{'}\right) \\ &= a_1b_1+a_2b_2+\cdots a_nb_n+\left(-a_1^{'}\right)b_1^{'}+\left(-a_2^{'}\right)b_2^{'}+\cdots+\left(-a_n^{'}\right)b_n^{'}\in IJ \end{aligned}$$

$\because I$ is an ideal and for any $r\in R, x\in IJ$ for $a_1^{'}\in I, \left(-a_1^{'}\right)\in I$

$$\begin{aligned} rx &= r(a_1b_1+a_2b_2+\cdots a_nb_n) \\ &= (ra_1)\,b_1+(ra_2)\,b_2+\cdot\cdot+(ra_n)\,b_n\in IJ \end{aligned}$$

because I is an ideal so $ra\in IJ$
Similarliy, $xr\in IJ$.Hence, IJ is an ideal.

Principla ideal :

Let R be ring and I be an ideal of R I is called principal ideal if

$$I=aR; \forall a\in R$$

Principal ideal Ring :

If each ideal of ring is principal then tthe ring is khown as principal ideal ring

Example :

Z is an principal ideal ring.

Theorem :

The set of integers is a principal Ideal ring

Proof

Consider an ideal I of Z and let $n \in I$ be least positive integer for any other $g \in I$ By division algorthim we can write as

$$\begin{aligned} g &= nq + r \qquad 0 \leq r < n \\ &\Rightarrow \quad r = g - nq \end{aligned}$$

Hence,q and r both are integers for $q \in Z, n \in I$

$$\Rightarrow nq \in I$$

and $nq \in I, g \in I$

$$\begin{aligned} &\Rightarrow \quad g - nq \in I \quad \because I \text{ is ideal} \\ &\Rightarrow \quad r \in I \end{aligned}$$

$\because (r < n)$ and n is least positive in I So, $r = 0$ OR $g = nq$ Since, g was arbitary so every element of I can be written in product of n OR $I = nR$ OR
Since, I was arbitary so each ideal of Z can be shown as principal ideal and Hence,Z is principal ideal ring.

Quotient Ring :

If I be ideal of R then $\left(\frac{R}{I}\right)$

$$\frac{R}{I} = \{r + I., r \in R\}$$

is set of cosets of I in R and is known as quotient ring

Addition of Quotient ring ;

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2)\, I. r_1 r_2 \in R$$

Multiplication of Qutient ring;

$$(r_1 + I)\,(r_2 + I) = (r_1 r_2) + I$$

Note :

$\Rightarrow$ Multiplication identity of $\frac{R}{I}$ is $1 + I$ and additive identity of $\frac{R}{I}$ is $0 + I$
$\Rightarrow$ If R is commutative ring with unity then $\frac{R}{I}$ is also commuatative ring with unity

Question#

Show that a quotient ring is a ring.

Solution :

we prove that if R is a ring and I is an ideal of R then the set $\frac{R}{I}$ with defined operations

satisfy the ring axioms

Closure :

for any $a + I, b + I \in \frac{R}{I}$

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I \\ (a + I) \cdot (b + I) &= (ab) + I \end{aligned}$$

So, that $\frac{R}{I}$ is closed under both operations

Associative :

$$\begin{aligned}((a+I)(b+I))+(c+I) &= (a+b+c)+I \\ ((a+I)(b+I)(c+I)) &= (abc)+I\end{aligned}$$

So, associatvie holds in $\frac{R}{I}$

Additive identity :

The element $0+I=I$ act as addative identity because

$$(a+I)+(0+I)=(a+0)+I=a+I$$

Additive Inverse :

For $a+I$

$$-(a+I)=(-a)+I$$

Since

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

Distributive Laws:

$$\begin{aligned}(a+I)((b+I)+(c+I) &= (a+I)(b+c+I) \\ &= (a(b+c))+I \\ &= (ab+ac)+I \\ &= (ab+I)+(ac+I)\end{aligned}$$

Distributive law hold .

*A*ll axiom hold so that $\frac{R}{I}$ is a ring.

Theorem :

Let I be a ideal of ring R then the mapping

$\Phi : R \to \frac{R}{I}$forms epimorphism with $\ker \Phi = I$

Pr**oof**

Consider mapping $\Phi : R \to \frac{R}{I}$ s.t $\Phi(r) = r+I$

For Homomorphism:

for $r_1, r_2 \in R$

(i)

$$\begin{aligned}\Phi(r_1+r_2) &= (r_1+r_2)+I \\ &= (r_1+I)+(r_2+I) \\ &= \Phi(r_1)+\Phi(r_2)\end{aligned}$$

(ii)

$$\begin{aligned}\Phi(r_1 r_2) &= r_1 r_2 + I \\ &= (r_1+I)+(r_2+I) \\ &= \Phi(r_1)\Phi(r_2)\end{aligned}$$

Hence, Φ is homomorphism .

For onto;

Since $\Phi(r) = r + I$ for each $r + I \in \frac{R}{I}$ there is an $r \in R$ such that $\Phi(r) = r + I$

Hence, Φ is onto

Since, Φ is both homomorphism and onto So, it is epimorphism

Next to show $\ker \Phi = I$

Let $r \in \ker \Phi$ then

$$\Phi(r) = 0 + I$$

but generally

$$\begin{aligned} \Phi(r) &= r + I \\ &\Rightarrow r + I = 0 + I = I \\ &\Rightarrow r \in I \\ &\Rightarrow \ker \Phi \subseteq I ... (i) \end{aligned}$$

For any $r \in I$

$$\begin{aligned} \Phi(r) &= r + I = o + I \\ &\Rightarrow r \in \ker \Phi \\ &\Rightarrow I \subseteq \ker \Phi .... (2) \end{aligned}$$

combing(1) and (2)

$$\Rightarrow I = \ker \Phi \qquad \blacksquare$$

First Fundamental Theorem of Homomorphism:

Let I be ideal of ring R and $\Psi : R \to R^{'}$ is an epimorphism with $\ker \Psi = I$ then $R^{'} \cong \frac{R}{I}$

Pr **oof**

Define a mapping $\Phi : \frac{R}{I} \to R^{'}$ s.t $\Phi(r + I) = r^{'}$

Well -defined :

For $r_1 + I, r_2 + I \in \frac{R}{I}$ Let

$$\begin{aligned} r_1 + I &= r_2 + I \\ (r_1 - r_2) + I &= (r_2 - r_2) + I \\ &= 0 + I = I \\ &\Rightarrow (r_1 - r_2) \in I \\ &\Rightarrow (r_1 - r_2) \in \ker \Psi \\ &\Rightarrow \Psi(r_1 - r_2) = 0 \in R^{'} \\ \Psi(r_1) &= \Psi(r_2) \\ r_1^{'} &= r_2^{'} \\ \Phi(r_1 + I) &= \Phi(r_2 + I) \end{aligned}$$

$\Rightarrow \Phi$ is well define

Φ is Homomorphism :

For $r_1 + I, r_2 + I \in \frac{R}{I}$

(i)

$$\begin{aligned}
\Phi\left((r_1+r_2)+I\right) &= \left(r_1+r_2\right)^{'} \\
&= \Psi\left(r_1+r_2\right) \\
&= \Psi\left(r_1\right)+\Psi\left(r_2\right) \\
&= r_1^{'}+r_2^{'} \\
\Phi\left((r_1+r_2)+I\right) &= \Phi\left(r_1+I\right)+\Phi\left(r_2+I\right)
\end{aligned}$$

(ii)

$$\begin{aligned}
\Phi\left((r_1r_2)+I\right) &= \left(r_1r_2\right)^{'} \\
&= \Psi\left(r_1r_2\right) \\
&= \Psi\left(r_1\right)\Psi\left(r_2\right) \\
&= r_1^{'}r_2^{'} \\
&= \Phi\left(r_1+I\right)\Phi\left(r_2+I\right)
\end{aligned}$$

$\Rightarrow \Phi$ is Homomorphism

One-to-One :

Assume that

$$\Phi\left(r_1+I\right)=\Phi\left(r_2+I\right)$$

using defination of Ψ

$$\begin{aligned}
\Psi\left(r_1\right) &= \Psi\left(r_2\right) \\
\Psi\left(r_1\right)-\Psi\left(r_2\right) &= 0 \\
\Psi\left(r_1-r_2\right) &= 0 \\
&\Rightarrow \quad r_1-r_2\in\ker\Psi \qquad\qquad \because \ker\Psi = I \\
&\Rightarrow \quad r_1-r_2\in I \\
&\Rightarrow \quad r_1+I=r_2+I \\
&\Rightarrow \quad \Psi \text{ is one -to-one}
\end{aligned}$$

Onto:

Every $r^{'}\in R^{'}$ there exists some $r\in R$ such that $\Psi\left(r\right)=r^{'}$ But $\Phi\left(r+I\right)=\Psi\left(r\right)=r^{'}$ Therefore every elements of $R^{'}$ has a preimage in $\frac{R}{I}$. Hence, it is onto.

Norm on a ring :

Let R be a ring a mapping $R\to\mathbb{Z}^{+}\cup\{0\}$ is called Norm of a ring R .if $N\left(a\right)>0\ \forall a\in R$ then N is called positive Norm.$N\left(0\right)=0$

Euclidean Domain :

Let R be an integral domain and a norm $R\to\mathbb{Z}^{+}\cup\{0\}$ is defined on it R is called Euclidean domain if for $a,b\in R$ there exist $q,r\in R$ s.t $a=bq+r$ with $r=0$ OR$N\left(r\right)<N\left(b\right)$

Example# Every field is trivialy Euclidean domain .

$*$ $\mathbb{Z}$(set of integers) is Euclidean domain with Norm $N\left(x\right)=|x|$

Principal Ideal Domain :

An integral domain in which every ideal is principal ideal is called PID .

Note :

Every PID is Euclidean Domain .

Example# Every Field is trivially PID.

$*$ $\mathbb{Z}$ is PID because every ideal of $\mathbb{Z}$ is Principal.

Irredeucible Element :

A non zero element r of R which is non-unit is irreducible if we can write $r = ab$ for some $a, b \in R$, either a is unit oR b is unit

Prime Element :

An element $p \in R$ is prime if (p) ideal generated by p is prime ideal of R

Associative Element :

For $a, b \in R$ if there exist a unit element $u \in R$ s.t $a = ub$ then a and b are associates of each other

Unique Factorization Domain (**UFD**) :

For an integral domain R if $r \in R$ is a non-unit element with these two properties

(i) r can be written as finite product of irreducible $p_i s \in R$ i.e $r = p_1 p_2 p_3 ... p_n$

(ii) This product is unique upto associates

Example# Eveery foeld is UFD because there is no non-unit element in field so we do not need to satisfy any of the condition

$*$ $\mathbb{Z}$ is UFD (being PID $\mathbb{Z}$ is UFD)

Note: In a PID an element is prime iff it is irrducible

Theorem : Every PID is UFD .In particular Every Eulidean domain is UFD.

Proof

Let R be PID which is not a field and consider $r \in R$ be a non-zero unit element of R .To show R is UFD we have to prove

(i) r can be represented as product of irreducible elements.

(ii) Representation of r is unique upto associates

(i) $\because$ for any non-unit element of PID ,there must exist irreducib an element in PID which divides that element .So, for $r \in R$ assume $p_i \in R$ is irreducible in R s.t $\frac{p_1}{r}$ OR $r = p_1 r_1 \, (r_1 \in R)$

$\Rightarrow (r) \subseteq (r_1)$ (Ideal generated by r is contained in ideal generated by r_1)

We claim $(r) = (r_1)$

$$\begin{aligned} \Rightarrow \quad & r_1 \in (r) \, OR \\ = \quad & r_1 = rp = p_1 r_1 p \\ \Rightarrow \quad & 1 = p_1 p \\ \Rightarrow \quad & p_1 \text{ is unit} \end{aligned}$$

Which is contraduction as p_1 is irreducible

$$\begin{aligned} \Rightarrow \quad & (r) \neq (r_1) \\ (r) \quad \subset \quad & (r_1) \end{aligned}$$

Now, for $r = p_1 r_1$ If r_1 is unit then by defination r is irreducible element and we are done .

Now, if r_1 is not unit .

Then there must exist an irreducible element $p_2 \in R$ s.t

$$\begin{aligned} & \frac{p_2}{r_1} OR \\ r_1 &= p_2 r_2 \, (r_2 \in R) \\ &\Rightarrow (r_1) \subseteq (r_2) \\ &\Rightarrow (r) \subset (r_1) \subset (r_2) \end{aligned}$$

if r_2 is unit then r_1 becomes irreducible element and from (i)

$$r = p_1 r_1 \, (\text{both } p_1 \text{and are irreducible elements,so we are done })$$

If r_2 is not unit element then the process repeats for some irreducible element p_3 and so on .We obtain an asscending chain of ideals in R which must ends(finite)because being PID R satisfies Asscending chain of ideal i.e $(r_1) \subset (r_2) \subset (r_3) \ldots (r_n) \in R \;\; for \; n \in \mathbb{N}$.So, that $r = p_1 p_2 p_3 \ldots p_n$ r is product of finite number of irreducible elements .
$Hence, proved$
(ii) Let $r = p_1 p_2 p_3 .. p_n = q_1 q_2 q_3 \ldots q_m$ where $m, n \in \mathbb{N}$ and all $p_i s$ and $q_i s$ are irreducible elements ($\because$ In PID an element is prime iff it is irreducible)
$\Rightarrow$ *All* $p_i s$ and $q_i s$ are prime
Case-1 Let $m > n$ $\because p_1 | r = q_1 q_2 q_{3 \ldots\ldots} q_m$
P_1 divedes one of the q_1Let $p_1 | q_1$that is $q_{1=} p_1 x_1$ Associate
$r = P_1 P_2 P_3 \ldots\ldots\ldots P_n = P_1 x_1 q_2 q_{3 \ldots\ldots} q_m$
$P_2 \ldots\ldots\ldots P_n = x_1 q_2 \ldots\ldots q_m$
Repeating the process's for $\frac{p_2}{q_2} \Rightarrow q_2 = p_2 x_2$

$$\begin{aligned} & p_2 \cdots p_n x_1 p_2 x_2 q_3 \cdots q_m \\ p_3 \cdots p_n &= x_1 x_2 q_3 \cdots q_m \end{aligned}$$

Repeating the process $n-$times we obtain

$$\begin{aligned} 1 &= (x_1 x_2 \cdots x_n q_{n+1} \cdots q_{m-1} q_m) \\ 1 &= (x_1 \cdots q_{m-1}) \, q_m \end{aligned}$$

$\Rightarrow q_m$ is unit which is contraduction because all $q_i s$ are irreducible .
$Hence, m \not> n$
Theorem:

Every Eulidean domain is PID.

Proof

Let R be a euclidean domain
To show R is PID we have to show every ideal of R is principal ideal for thus let $A \in R$ be any ideal of R if $A = \{0\}$ then A can be write as $A = 0 \quad OR \; (zero * Ring) = (0)$ (ideal generated by 0)And Hencem A is principal
If A is contain non-zero element too then for any $a \neq 0, a \in A \; N(a) > 0$ Here N is norm defined on Euclidean domain R) i.e $N : R \to \mathbb{Z}^+ \cup \{0\}$
$N(0) = 0$
Consider the set

$$S = \{N(0) \, ; a \in A, a \neq 0\}$$

this set is al positive because $N(0) \in \mathbb{Z}^+ \; \forall a \in A$.

By well odering property S must contain a least element that is for some $c \in A, N(c)$ is least element in S .
Now, for $a, c \in A$ there must exist $q, r \in R$ s.t

$$a = qc + r \quad \text{where } r = 0 \text{ OR } N(r) < N(c) \text{ (because } R \text{ is Euclidean domain)}$$

If $r = 0$ then $a = qc$
$if\ r \neq 0 \Rightarrow N(r) < N(c)$ But

$$\begin{aligned} a &= qc + r \\ a - qc &= r \qquad \because a \in A, c \in A, q \in R \\ &\Rightarrow qc \in A \qquad \because A \text{ is ideal} \\ &\Rightarrow (a - qc) = r \in A \\ &\Rightarrow N(r) \subset S \text{ and } N(r) * N(c) \end{aligned}$$

because $N(c)$ was the least element of S.So,

$$\begin{aligned} r &= 0 \\ &\Rightarrow a = qc \\ &\Rightarrow A \subset A \text{ was arbitary so, every element of } A \text{ can be written as} \\ a &= rc \text{ for some } r \in R \text{ so, that} \\ A &= (c) \text{ ideal generated by } c \end{aligned}$$

Hence, A is principal ideal using the same argument we can show each ideal of ED is principal ideal and hence ,R is PID.
Note :
Since, every PID is UFD and every ED is PID so, we can say every ED is also UFD.
Modules :
Let R be ring and M be a non-empty set M is said to be $R-$Modules over R if
(i) M is abelian group under addition
(ii) An action form $R \times M \to M$ is defined that is $r \in R, m \in M \Rightarrow rm \in M$ with following properties
$(i)\,(s + r)\, m = sm + rm$ s,r,m $\in R$,
$(ii)\, r\,(m + n) = rm + rn \quad m \in M; r, s \in R$
$(iii)\, r\,(sm) = (rs)\, m \qquad m \in M; r, s \in R$
(iv) If $1 \in R$ then $1.m = m$ where $m \in M$ for $r \in R, m \in M, rm \in M$ then M is called left modules and for $r \in R, m \in M, mr \in M$ then M is called right modules
For a field F if M is module over F then M is a vector space .
$\Rightarrow E$very Ring R is module over itself
Example : **Any abelian group under addition M is Z − module**.
Solution:Given that $(M, +)$ is abelian group .
For any $m \in M, r \in \mathbb{Z}$

$$rm = (m + m + m + \cdots + m)_{r-times} \in M$$

(i)

$$\begin{aligned} (s + r)\, m &= (m + m + m + m + \cdots + m)_{(r+s)times} \text{ where } r, s \in \mathbb{Z} \\ &= (m + m + m + \cdots + m)_{r-times} + (m + m + m + \cdots + m)_{s-times} \\ &= rm + sm \end{aligned}$$

(ii)

$$\begin{aligned} r(m+n) &= [(m+n)+(m+n)+\cdots+(m+n)]_{r-times} \\ &= (m+m+m+\cdots+m)_{r-times}+(n+n+n+\cdots+n)_{r-times} \\ &= rm+rn \end{aligned}$$

(iii)

$$\begin{aligned} r(sm) &= r(m+m+m+\cdots+m)_{s-times} \\ &\quad r(1+1+1+\cdots+1)m \\ &= (rs)m \end{aligned}$$

(4) As $1 \in \mathbb{Z}$ So, for any $m \in M \Rightarrow m.1 = m$
$Hence, M$ is $R-$Module over $\mathbb{Z}$.
R − Submodule :

A subset N of M is called $R-Submodule$ if
(i) for $a, b \in N \Rightarrow a-b \in N$
(ii) for $a \in N, r \in R \Rightarrow ar \in N$
Every submodule of M is also a module over R.
Note :

If N is a $R-$module over a filed then N is vector subspace
Example :

Let M be left -module over R and N be any left ideal of R s.t $N \subset M$ then N is $R-$Submodule of M .
Solution :

(i) For $a, b \in N, a-b \in N$ Since, N is ideal .
(ii) For $a \in N, r \in R$,$ra \in N$ Since, N is ideal .
$Hence$, N is $R-$Submodule.
Module Homomorphism :

Let M and N are R-module over ring R .The mapping $\Phi : M \to N$ is called Module -Homomorphism if
$(i)\ \Phi(x+y) = \Phi(x)+\Phi(y) \quad x, y \in M$
$(ii)\ \Phi(rx) = r\Phi(x) \quad r \in R$
Note:

A Module -Homomorphism need not to be Ring -Homomorphism
Example Let $F : R \to R \quad f(x) = 2x$
f is module -Homomorphism as
$(i)\ f(x+y) = 2(x+y) = 2x+2y = f(x)+f(y)$
$(ii)\ f(rx) = 2(rx) = r(2x) = rf(x)$
But f is not Ring-Homomorphism because
$(ii)\ f(xy) = 2xy = (2x)(y) \neq f(x)f(y)$
If M is $R-$module where R is field then its module-Homorphism is linear transformation .
Theorem :

Both $Ker\Phi$ and imgΦ of a module-Homomorphism are Submodule.
Pr **oof**

Let $\Phi : M \to N$ be module-Homomorphism
$(1)\ \ker\Phi = \{x | \Phi(x) = 0\}$ where $x \in \mathbf{M}, \mathbf{0} \in \mathbf{N}$ .Let $x, y \in \ker\Phi$
$\Phi(x) = 0, \Phi(y) = 0$

$(i)\, 0 = \Phi(x) - \Phi(y) = \Phi(x-y)$ Since, Φ is homomorphism,
$\Rightarrow x - y \in \ker \Phi$
$(ii)\, \Phi(rx) = r\Phi(x) = r(0) = 0$
$\Rightarrow rx \in \ker \Phi$ Since,Φ is homomorphism
$Hence$, $\ker \Phi$ is $R-$ Submodule
(2) $\text{Img}\Phi = \{\Phi(x) | x \in M\}$
Let $\Phi(x), \Phi(y) \in \text{img}\Phi$ for some $x, y \in M$

$$\begin{aligned} \Phi(x) - \Phi(y) &= \Phi(x-y) \quad \text{Since,}\Phi \text{ is homomorphism} \\ &\Rightarrow \Phi(x-y) \in img\Phi \end{aligned}$$

$\Phi(rx) = r\Phi(x)$ Since, Φ is homomorphism
$\Rightarrow r\Phi(x) \in \text{Im}\, g\Phi$ because $\text{img}\Phi = N$ and N is $R-$module for any $r \in R, \Phi(x) \in N, r\Phi(x) \in N$ $\text{img}\Phi$ is $R-$submodule .

Quotient Module :

Let M be $R-$ module and N be $R-$ submodule then quotient group $\frac{M}{N}$ can be made $R-$module khown as quotient module ,Moreover, the mapping $\Phi : M \to \frac{M}{N}$ i.e $\Phi(x) = x + N$ $x \in M$ is module Homomorphism .

Field :

A Ring F is called a field if it is
$[F_1]$ Commutative
$[F_2]$ With unity
$[F_3]$ Its every non-Zero element is invertible i.e has multriplicative inverse.

Remark:

It may be observed that in a field $(F, +, \times)$ each equation of the form $a + x = b; x + a = b; ax = b; xa = b;$ has unique solution in F $\forall$ $a, b \in F$ $a \neq 0$

Example#1

The following rings of numbers $(\mathbb{Q}, +, \times)$ $(\mathbb{R}, +, \times)$ $(\mathbb{C}, +, \times)$ because each is a commutavie ring with unity and multiplicative inverse $\frac{1}{a}$ of every non-zero element of ring exists

Example#2

Module ring($Z_3 = \{0, 1, 2\}$ $, +_3, \times_3)$ is a field from composition table of Z_3 it is clear that Z_3 is a commutative ring with unity 1 and 2 is its own inverse.

Remark

In a field every element is unit element except the zero element .

Example#

In the ring $[\{0, 1, 2, 3, 4\}, +_5, \times_5]$ is unit because $1 \times_5 1 = 1; 2 \times_5 3 = 1; 4 \times_5 4 = 1$

Example#

Show that the set of real number of the forms $m + n\sqrt{2}$ $m, n \in \mathbb{Z}$ with ordinary addition and multiplication of numbers forms a ring is it a field.

Solution:

Let $\left\{m + n\sqrt{2}; m, n \in \mathbb{Z}\right\}$Clearly, G is subset of $\mathbb{R}$
Let $x, y \in G$

$$\begin{aligned} x &= m_1 + n_1\sqrt{2}; y = m_2 + n_2\sqrt{2} \quad \text{where } m_1, m_2, n_1, n_2 \in \mathbb{Z} \\ x + y &= \left(m_1 + n_1\sqrt{2}\right) + \left(m_2 + n_2\sqrt{2}\right) \\ &= (m_1 + m_2) + (n_1 + n_2)\sqrt{2} \qquad \because m_1, m_2, n_1 n_2 \in \mathbb{Z} \\ &\Rightarrow x + y \in Z \end{aligned}$$

Now,

$$\begin{aligned} x \times y &= \left(m_1 + n_1\sqrt{2}\right) + \left(m_2 + n_2\sqrt{2}\right) \\ &= (m_1 m_2 + 2n_1 n_2) + (m_1 n_2 + n_1 m_2)\sqrt{2} \\ &\Rightarrow x \times y \in \mathbb{Z} \end{aligned}$$

$\Rightarrow G$ is closed under addition and multiplication

$$\begin{aligned} x - y &= \left(m_1 + n_1\sqrt{2}\right) - \left(m_2 + n_2\sqrt{2}\right) \\ &= (m_1 - m_2) + (n_1 - n_2)\sqrt{2} \in G \\ &\Rightarrow x - y \in G \end{aligned}$$

$\Rightarrow (G, +, \times)$ is a subgroup of abelian group $(R, +)$
$\Rightarrow$ $(G, +)$ is it self is a abelian group .Also multiplication of real number is associative commutative and distributive over addition .Hence,$(G, +, \times)$ is a commutative ring.
Now,we see that the multiplicative inverse of any non-zero number $m + n\sqrt{2} \in G$ in R

$$\begin{aligned} & \frac{1}{m + n\sqrt{2}} \times \frac{m - n\sqrt{2}}{m - n\sqrt{2}} \\ = & \frac{m - n\sqrt{2}}{(m^2 - 2n^2)} \\ = & \frac{m}{m^2 - 2n^2} - \frac{n}{m^2 - 2n^2}\sqrt{2} \end{aligned}$$

which is need not to be in G because $\frac{m}{m^2-2n^2} \& -\frac{n}{m^2-2n^2}$ will not always integer
So, is is not a field .

Remark

It can be easily seen that $(G, +, \times)$ is an integral domain because $1 = 1 + 0\sqrt{2}$ and G has no zero divisor.

Subfield :

A non void subset F' of a field F is called a subfield if F' is closed for the composition in F and F' itself is a field for the induceed composition .

Example#

The field $(\mathbb{Q}, +, \times)$ of rational numbers is a subfield $(\mathbb{R}, +, \times)$ of real numbers which itself is a subfield of the field $(\mathbb{C}, +, \times)$ of complex number.

Theorem :

The necessary and sufficient conditions for a non void subset S of a field F to be a subfiled of F are
(i) $a \in S, b \in S \Rightarrow a - b \in S$
(ii) $a \in S, b \in S \Rightarrow ab^{-1} \in S$

Proof

Necessary condition:

Suppose that S is a subfiled of F and let $a \in S, b \in S$.Now, S is a subfiled
$\Rightarrow S$ is subring of F

$$a \in S, b \in S \Rightarrow a - b \in S$$

Again S is subfield

$\Rightarrow S - \{0\}$ is a multiplicative abelian group

$$\begin{aligned} 0 &\neq b \in S \Rightarrow b^{-1} \in S \\ &\Rightarrow a \in S \;\; 0 \neq b \in S \\ &\Rightarrow ab^{-1} \in S \end{aligned}$$

The condition is necessary

Sufficient Condition:

Suppose that S is non empty subset of field F then (i) and (ii) holds

Then by (i) $(S,+)$ is an abelian group by (ii) $[S-\{0\}]$ is commuattive group lastly distributive over addition holds in F therefore also holds in S .

$\Rightarrow (S,+,\times)$ is a field and So, the given condition is sufficient.

Example#

Prove that the set $S = \left\{a + b\sqrt{2} | a, b \in \mathbb{Q}\right\}$ is a subfield $(\mathbb{R},+,\times)$ of real numbers.

Solution:

For every$a, b \in \mathbb{Q}$ $\left(a + b\sqrt{2}\right) \in \mathbb{R}$

$\Rightarrow S$ is non-empty subset of $\mathbb{R}$

Let

$$\begin{aligned} xy &\in S \quad x = a_1 + b_1\sqrt{2} \quad y = a_2 + b_2\sqrt{2} \\ x - y &= \left(a_1 + b_1\sqrt{2}\;\right) - \left(a_2 + b_2\sqrt{2}\right) \\ &= (a_1 - a_2) + (b_1 - b_2)\sqrt{2} \in S \end{aligned}$$

Again if $y \neq 0\,(i.e\ a_2 \neq 0, b_2 \neq 0)$

$$\begin{aligned} xy^{-1} &= \left(a_1 + b_1\sqrt{2}\right)\left(\frac{1}{a_2 + b_2\sqrt{2}}\right) \\ &= \frac{(a_2 + b_2\sqrt{2})(a_2 + b_2\sqrt{2})}{a_2^2 - 2b_2^2} \\ &= \frac{(a_1a_2 - 2b_1b_2) + (a_2b_1 - a_1b_2)\sqrt{2}}{a_2^2 - 2b_2^2} \\ &= \frac{(a_1a_2 - 2b_1b_2)}{a_2^2 - 2b_2^2} + \frac{(a_2b_1 - a_1b_2)\sqrt{2}}{a_2^2 - 2b_2^2} \end{aligned}$$

$\Rightarrow xy^{-1} \in S$

$\Rightarrow S$ is the subfiled of the filed $(\mathbb{R},+,\times)$.

Prime Field :

A field F which has no proper subfield i.e A field F is a prime field if the only subfield of F is F itself.

Example :

The field $(Z_p, +_p, \times_p)$ where p is a prime number is a prime field.

|Solution:

To show that $(Z_p, +_p, \times_p)$ is a prime field i.e to show that it does not have a proper subfield .Let k be a subfield of Z_p.Then $1 \in k, 0 \in k$ and $k \subset Z$.Now, $1 \in k \Rightarrow 1+1 \in k \Rightarrow 2 \in k \Rightarrow 3 \in k \cdots (p-2)+1 = p-1 \in k$

Hence, $Z \subset k$

$\Rightarrow k = Z_p$
$\Rightarrow Z_p$ is prme field .

Example#

The field $(\mathbb{Q}, +, \times)$ is a prime field .

Solution:

To show $(\mathbb{Q}, +, \times)$ is a prime field i.e to show that there is no proper subfield of $\mathbb{Q}$.Let k be a subfield of $\mathbb{Q}$.We will show that $k = \mathbb{Q}$
Now,$k \subset \mathbb{Q}$ and $1 \in k \Rightarrow 1 + 1 = 2 \in k$
$1 + 1 + 1 + \cdots m-\text{times} = m \in k$
$m \in k \Rightarrow -m \in k \;\; m \in Z$ (Since, k is field) $Z \subset k$
Now,$m \in Z \;\; 0 \neq n \in Z$
$\Rightarrow m \in k \;\; n^{-1} \in k$
$\Rightarrow mn^{-1} \in k$
$\Rightarrow \left\{\frac{m}{n} | n \neq 0 \;\; m, n \in Z\right\} \subset k$
$\Rightarrow \mathbb{Q} \subset k$
$\Rightarrow \mathbb{Q} = k$
Hence, $\mathbb{Q}$ is a prime filed.

Extension of field :

Let F be any field then the field extension of F is a pair (k, F) where k is another field and F is monomorphism of F into k Then k is said to be a field extension of F if
(i) F is subfiled of k
(ii) k forms a vector space over F
(iii) k must have a basis and dimension over F

Degree of filed extension :

The dimension of k as a vector space over F is called the degree of k and is denoted by $[k; F]$

Finite Extension :

If $[k; F]$ is finite then k is called finite extension

Infinite Extension :

If $[k; F]$ is infinite then k is said to be infinite extension .

Example#

$Q(\sqrt{2}) = \left\{a + b\sqrt{2}; a, b \in Q\right\}$ is finite field extension .The subset $\left\{1, \sqrt{2}\right\}$ forms a basis for Q($\sqrt{2}$) over Q i.e $\left[Q(\sqrt{2}), Q\right] = 2$

Theorem (Transitive of finite Extension) :

If k is a finite field extension of F and L is a finite field extension of k then L is a finite field extension of F and $[L; F] = [L : k]\,[k : F]$

Proof

Let $[L : K] = m, [K : F] = n$ .Let $\{a_1, a_2, \cdots a_m\}$ be basis of L over K and $\{b_1, b_2, \cdots b_n\}$ be basis of K over F We show that $\{a_i b_j | 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of L over F s.t $a_i \in L, b_i \in K \Rightarrow b_j \in L$
$\Rightarrow a_i b_j \in L$ for all i, j
Let

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} a_i b_j = 0 \text{ where } \alpha_{ij} \in F$$

Then

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\left(\alpha_{ij}b_j\right)a_i = 0, \sum_{j=1}^{n}\alpha_{ij}b_j \in K$$

Since $\{a_1, a_2, \cdot\, a_m\}$ are linearly independent over K,

$$\sum_{j=1}^{n}\alpha_{ij}b_j = 0 \text{ for all } i = 1\cdot\cdots\cdot m$$

Also $\{b_1, b_2, \cdot\cdots b_n\}$are linearly independent over F

$$\begin{aligned}\alpha_{ij} &= 0 \text{ for all } i = 1\cdot\cdots\cdot m, j = 1\cdot\cdots\cdot n\\ &\Rightarrow \{a_ib_j | 1 \le i \le m, 1 \le j \le n\}\end{aligned}$$

is linearly independent subset of L over F.Let $a \in L$.Since $\{a_1, a_2, \cdot\, a_m\}$ is a basis of L over K $a = \alpha_1a_1 + \alpha_2a_2 + \cdot\, \cdot + \alpha_ma_m \in K$ and $\{b_1 \cdots b_n\}$ is basis of K over F

$$\begin{aligned}&\Rightarrow \alpha_i = \beta_{i1}b_1 + \cdots + \beta_{in}b_n, \beta_{ij} \in F\\ &\Rightarrow a = \sum_{i=1}^{m}\alpha_ia_i = \sum_{i=1}^{m}\left(\beta_{i1}b_1 + \cdots + \beta_{in}b_n\right)a_i\end{aligned}$$

Also $b_1, b_2, \cdots b_n$ are linearly independent over F,

$$\begin{aligned}\alpha_{ij} &= 0 \text{ for all } i = 1\cdot\cdots\cdot m, j = 1\cdots n\\ &\Rightarrow \{a_ib_j | 1 \le i \le m, 1 \le j \le n\}\end{aligned}$$

is linearly independent subset of L over F .Let $a \in L$Since $\{a_1, a_2, \cdot\, a_m\}$ is a basis of L over K $a = \alpha_1a_1 + \alpha_2a_2 + \cdot\, \cdot + \alpha_ma_m \in K$ and $\{b_1 \cdots b_n\}$ is basis of K over F

$$\begin{aligned}&\Rightarrow \alpha_i = \beta_{i1}b_1 + \cdots + \beta_{in}b_n, \beta_{ij} \in F\\ &\Rightarrow a = \sum_{i=1}^{m}\alpha_ia_i = \sum_{i=1}^{m}\left(\beta_{i1}b_1 + \cdots + \beta_{in}b_n\right)a_i\\ &= \sum_{i=1}^{m}\sum_{j=1}^{n}\beta_{ij}a_ib_j, \beta_{ij} \in F\end{aligned}$$

$\{a_ib_j | 1 \le i \le m, 1 \le j \le n\}$ spans Lover F and so forms a basis of L over F.
$\Rightarrow [L : F] = mn = [L : K]\,[K : F]$
Corrolary : If L is finite extension of F and K is subfield of L which contains F Then $[K : F]$ divides $[L : F]$
Corrolary : If K is an extension of F,Then $K = F$ iff $[K : F] = 1$

Corrolary : If L is an extension of F and $[L : F]$ is a prime number p,then there is no field K s.t $F \subset K \subset L$
Simple Extension :

Let K be an extension of a field F.If K is generated by α single element over F then K is called simple extension of F i.e $K = F(\alpha)$ for some $\alpha \in K$

Example:
(1) $Q\sqrt{2}$ is simple extension of Q.
(2) $\mathbb{C}$ is simple extension of $\mathbb{R}$as $\mathbb{C} = \mathbb{R}(i)$

Algebraic Element :

Let K be an extension of field F then an element α of K is said to be algebraic element over F if α is root of non-zero polynomial $f(x) \in F[x]$

Algebraic Extension :

An extension K of a field F is said to be algebraic extension of F if every element of K is algebraic over F.

Example :

$\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.

Solution:

Let $z = a + ib$ be any complex number Then for all $a, b \in \mathbb{R}$,Let $f(x) = x^2 - 2ax + (a^2 + b^2)$ Then $f(x) \in R[x]$ and $f(x) = (a + ib)^2 - 2a(a + ib) + (a^2 + b^2)$

$$\begin{aligned} f(x) &= a^2 - b^2 + 2abi - 2a^2 - 2abi + ah2 + b^2 \\ f(x) &= 0 \end{aligned}$$

$\Rightarrow Z$ is algebraic over $\mathbb{R}$.Since Z is abrbitary ,so every member of $\mathbb{C}$ is algebraic over $\mathbb{R}$.
$\Rightarrow \mathbb{C}$ is algebraic extension of $\mathbb{R}$.

Transcedental Extension :

Let K be extension of field F .If there exists an at least one element "a" $\in K$ such that "a" is not is not algebraic over F then it is called Trancedental Extension.

Example :

The field $\mathbb{R}$ of set of real numbers is not algebraic extension over $\mathbb{Q}$
So, $\mathbb{R}$ over $\mathbb{Q}$ is Transcedental Extension.

Theorem :

Every finite extension of field is an algebraic extension

Proof:

Let K be finite extension of field F .Let $[K : F] = n$ .Let $a \in K$,Since K is a field and $a \in K$ So, $1, a, a^2, \cdots a^n$ are all in K.Now, dimension of vector space K over F is n, So, these $(n + 1)$ elelment of K are linearly independent over F .Thus, $\exists\ \alpha_\circ, \alpha_1, \alpha_2, \cdots \alpha_n \in F$ not all zero such that

$$\alpha_\circ 1 + \alpha_1 a + \alpha_2 a^2 + \cdots \alpha_n a^n = 0$$

Consider $f(x) = \alpha_\circ + \alpha_1 x + \alpha_2 x^2 + \cdots \alpha_n x^n$ Then $f(x) \in F[x]$ such that $f(a) = 0$ So,"a" is algebraic over F.Thus, every element of K is algebraic over F and so K is an algebraic extension of F.
So, every finite extension of field is an algebraic extension.

Chinese Remainder theorem :

Let $m_1, m_2, \cdots \cdots m_r$ be positive integers that are realatively prime in pairs i.e $(m_i, m_j) = 1$ for all $i \neq j$.Then for any integers $a_1, a_2, \cdots \cdots a_r$ the $r-$congruences $x \equiv a_i \pmod{m_i}$ where $i = 1, 2, 3 \cdot r$
Hence, a common solution morever any two solutions are congruent madulo $m_1, m_2, \cdots m_r$.

Proof:
Here,

$$\begin{aligned} x &\equiv a_1 \,(\mathrm{mod}\, m_1) \\ x &\equiv a_2 \,(\mathrm{mod}\, m_2) \\ x &\equiv a_2 \,(\mathrm{mod}\, m_2) \\ &\vdots \qquad\qquad \vdots \\ x &\equiv a_r \,(\mathrm{mod}\, m_r) \end{aligned}$$

where $(m_i, m_j) = 1$ for all $i \neq j$. Let $M = m_1, m_2, m_3, \cdots m_r$
Consider $M = \frac{M}{m_i}\,(i = 1, 2, 3, \cdots r)$,$M_i = m_1, m_2, m_3, \cdots m_{i-1}, m_{i+1}, m_{i+2} \cdots m_r$
Now, $(m_i, m_j) = 1$ for all $i \neq j$
$\Rightarrow (m_i, m_1) = 1\,(m_i, m_2) = 1 \cdot\cdot (m_i, m_{i-1}) = 1\,(m_i, m_{i+1}) = 1 \cdots (m_i, m_r) = 1$
$\Rightarrow (m_1, m_2, m_3, \cdots m_{i-1}, m_{i+1} \cdots m_r) = 1$
$\Rightarrow (m_i, M_i) = 1$ for all $i = 1, 2, 3, 4, \cdots r$
$\Rightarrow$Each linear congruence $M_i x \equiv 1\,(\mathrm{mod}\, m_i)$ (say b_i) for all $i = 1, 2, 3, 4, \cdots r$ i.e $M_i b_i \equiv 1\,(\mathrm{mod}\, m_i)\, i = 1, 2, 3, 4, \cdots r$
Let

$$\begin{aligned} x^* &= M_1 a_1 b_1 + M_2 a_2 b_2 + \cdots + M_r a_r b_r \\ \Rightarrow\; x^* &= \sum_{i=1}^{r} M_i a_i b_i \end{aligned}$$

Claim :
x^* is a common solution of $r-$congruent equations $x \equiv a_i \,(\mathrm{mod}\, m_i)$ .Let $j = 1, 2, 3, \cdots r$ be a particular number then $\frac{m_j}{M_i}$ whenever $i \neq j$
Now, $x^* = M_1 a_1 b_1 + M_2 a_2 b_2 + \cdots + M_r a_r b_r$
$x^* = M_1 a_1 b_1 + M_2 a_2 b_2 + \cdots + M_i a_{i-1} b_{i+1} + M_i a_i b_i + M_{i+1} a_{i+1} b_{i+1} + \cdot\cdot$
$\cdot\cdot + M_r a_r b_r$
$x^* = M_i a_i b_i \,(\mathrm{mod}\, m_i)$
$x^* = (M_i b_i)\, a_i \,(\mathrm{mod}\, m_i)$
$x^* = 1 a_i \,(\mathrm{mod}\, m_i) \quad \because M_i b_i \equiv 1 \,(\mathrm{mod}\, m_i)$ for all $1, 2, 3, \cdot r$
Now, let $x^* y^*$ be any two common solution
$x^* \equiv a_i \,(\mathrm{mod}\, m_i)$ and $y^* \equiv a_i \,(\mathrm{mod}\, m_i)$
$\Rightarrow x^* = y^* \,(\mathrm{mod}\, m_i)$ for all $i = 1, 2, 3 \cdots r$
$\Rightarrow \frac{m_i}{x^* - y^*}$for all $i = 1, 2, 3 \cdots r$

$$\begin{aligned} \Rightarrow\; & \frac{[m_1, m_2, \cdots m_r]}{x^* - y^*} \\ \Rightarrow\; & \frac{M}{x^* - y^*} \\ \Rightarrow\; & x^* - y^* \equiv 0 \,(\mathrm{mod}\, M) \\ x^* &= y^* \,(\mathrm{mod}\, M) \end{aligned}$$

where

$$M = m_1, m_2, \cdots m_r \;.\blacksquare$$