RINGS.

A non-empty set R is said to be a ring (or an associative ring) if in R, there are two operations namely '+' and '.' respectively such that for all $a, b \in R$.

* $a+b \in R$ [additive closure]
* $a+b = b+a$ [commutative under +]
* $(a+b)+c = a+(b+c)$ [associative under +]
* $\exists$ an element $0 \in R$ such that $a+0 = 0+a = a \ \forall \ a \in R$. [additive identity]
* $\exists \ -a \in R$ such that $a+(-a) = (-a)+a = 0$ [additive inverse]
* $a.b \in R$ [multiplicative closure]
* $(ab)c = a(bc)$ [associative under .]
* $a(b+c) = ab + ac$ (left distributive)
  $(a+b)c = ac + bc$ (right distributive)

A ring R is denoted by $(R, +, \cdot)$

(1) - (5) : $(R, +)$ - abelian group.

$\cdot$ - closure, associative, distributive over +.

Eg 1. $(Z, +, \cdot)$ is a ring.

Eg 2. $(Z, +, -)$ is not a ring (Associative law is not true)

Eg 3. $(Z_n, \oplus_n, \odot_n)$ is a ring

Eg 4. $(M_2(R), +, \cdot)$ is a ring.

Eg 5. $Z[x]$ - set of all integer polynomials.

$(Z[x], +, \cdot)$ is a ring.

Eg 6. $Z[i] = \{a+ib \mid a, b \in Z\}$

$(Z[i], +, \cdot)$ is a ring - Ring of Gaussian integers

Eg 7. Ring of Real Qubernions is a division ring.

$R = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \text{ are reals}\}$

Consider, $x = a_0 + a_1 i + a_2 j + a_3 k$

$y = b_0 + b_1 i + b_2 j + b_3 k$.

$i^2 = j^2 = k^2 = -1$

Argand plane

i, j, k is not vector.

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

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

$= a_0b_0 + a_0b_1 i + a_0b_2 j + a_0b_3 k + a_1b_1 + a_1b_0 i + a_1b_2 j + a_1b_3 k + a_2b_0 j$

$xy \leftarrow R$ Multiplicative closure

$0+0i+0j+0k$ Additive identity.

SPECIAL TYPES OF RING

A ring with multiplicative identity is called ring with unity or ring with unit element.

Eg. $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$, $(C, +, \cdot)$, $(Z_n, \oplus_n, \odot_n)$, $(M_2(R), +, \cdot)$, $Z[x]$, $Z[i]$, Ring of real Quternions.

$(2Z, +, \cdot)$ - not a ring with unity as identity element 1 is not there.

Let R be a ring with unity. If every non-zero element in R has multiplicative inverse. Then R is a division ring or skew field.

Eg. $(Z, +, \cdot)$ is a ring with unity but not a division ring.

$(Q, +, \cdot)$ - Division ring $(GL_2(R), +, \cdot)$ - Division ring

$(R, +, \cdot)$ - Division ring $(Q[i], +, \cdot)$ - Division ring

$(M_2(R), +, \cdot)$ - not a division ring as if $|M| = 0$ inverse doesn't exists

$(Z[i], +, \cdot)$ - division ring.

A ring R such that $a.b = b.a \ \forall\ a, b \in R$, R is a commutative ring.

Eg. $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$

$(M_2(R), +, \cdot)$ - not a commutative ring as matrix multiplication is not commutative.

A division ring R is said to be a field if it is a commutative ring.

Field $(R, +, \cdot)$ - $(R, +)$ - abelian group.

$(R - \{0\}, \cdot)$ - abelian group.

distributivity ~~divisibility~~ over +.

Eg. $(Q, +, \cdot)$ field.

6M. Prove that the ring of real quaternions is a division ring.

1) Every commutative ring is not a field but every field is a commutative ring $(Z, +, \cdot)$

2) Every division ring is a ring with unity - true. But Every ring with unity is not a division ring.

3) Every ring is not a field but every field is not a ring.
$(Z_n, \oplus_n, \odot_n)$ is a ring but
$(Z_p, \oplus_p, \odot_p)$ is a field
↳ finite field.

Zero divisor:

Let R be a commutative ring. An element $a \neq 0$ in R is said to be a zero divisor, if there exist $b \neq 0$ in R such that $a \cdot b = 0$.

A non-zero element a in R is said to be a zero divisor if there exist b in R where $a *_2 b = 0$.

① $(Z, +, \cdot)$ no zero divisor.

② $(Z_4, \oplus_4, \odot_4)$ has zero divisor.

$1 \odot_4 4 = 0 \rightarrow 4$ is not a zero divisor $\because 4 \notin Z_4$

$2 \odot_4 2 = 0 \rightarrow 2$ is a zero divisor

Multiplicative identity - unity (unit element) $1 \in R$.

Multiplicative inverse - unit.

Properties of a ring:

If R is a ring $\forall a, b \in R$

* $a \cdot 0 = 0 \cdot a = 0$
* $a(-b) = (-a)b = -(ab)$
* $(-a)(-b) = ab$.

Commutative Ring which has no zero divisor - integral domain. (ID)

ID:

A commutative ring without zero divisor is called ~~zero divisor~~. Eg. $(Z, +, \cdot)$, $(Q, +, \cdot)$

Unit → zero divisor ✗

Zero divisor → unit ✗

Proof:

* $a \cdot 0 = a \cdot (0+0)$ left

$a \cdot 0 = a \cdot 0 + a \cdot 0$ ($\because$ distributive law)

By left cancellation law in $(R, +)$ $\because$ $(R, +)$ is a group.

$a \cdot 0 = 0$.

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

$0 \cdot a = 0 \cdot a + 0 \cdot a$.

$0 \cdot a = 0$.

$\therefore a \cdot 0 = 0 \cdot a = 0$.

* $a(-b) = (-a)b = -(ab)$

First we prove $a(-b) = -(ab)$

It is enough to prove $a(-b) + ab = 0$.

By left distributive law,

$a(-b) + ab = a(-b+b)$

$= a \cdot 0$ [By (i)]

$= 0$.

$\therefore a(-b) = -(ab)$

$(-a)b = -(ab)$

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

By right distributive law,

$(-a)b + ab = (-a+a) \cdot b$

$= 0 \cdot b$ [By (i)]

$= 0$

$\therefore (-a)b = -(ab)$

$\Rightarrow a(-b) = (-a)b = -(ab)$

* $(-a)(-b) = ab$.

$(-a)(-b) = -(a(-b))$ [$\because$ multiplicative associative]

$= -(-(ab))$ [By ii)]

$= ab$

In addition if R is a ring with unit element then

(i) $(-1)(-1) = 1$ (ii) $1 \cdot 0 = 0 \cdot 1 = 0$ (iii) $1(-1) = (-1)1 = -1$

Result:

In $(Z_4, \oplus_4, \odot_4)$,

$3 \odot_4 \frac{3}{4} = 1$

here 3 is not a zero divisor but it is a unit.

* Let R be a commutative ring with unity, then

$a \neq 0$ if a zero divisor $\Leftrightarrow$ a is not a unit. (or)

$a \neq 0$ if not a zero divisor $\Leftrightarrow$ a is a unit.

Proof: Let R be a commutative ring with unity and $a \neq 0 \in R$ be a zero divisor. Then there exists $b \neq 0 \in R$ such that $a \cdot b = 0$. (1)

We have to prove a if not a unit.

Suppose a is a unit. Then $a^{-1} \in R$.

From (1), $a^{-1}(a \cdot b) = a^{-1} \cdot 0$.

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

$1 \cdot b = 0$

$b = 0$ which is a contradiction.

$\therefore$ a is not a unit.

Theorem: A finite integral domain is a field.

Proof: Let $R = \{x_1, x_2, x_3 \ldots x_n\}$ be a finite integral domain. We have to prove that,

(i) There exists $1 \in a$ such that $a \cdot 1 = 1 \cdot a = a \ \forall\ a \in R$

(ii) For every $a \neq 0$, there exists $b \in R$ such that $a \cdot b = b \cdot a = 1$.

Let $a \neq 0 \in R$ Then consider $S_a = \{x_1 a, x_2 a, \ldots x_n a\}$

First we prove that all elements in Sa are distinct.

Suppose $x_i a = x_j a$ for some i, j

$x_i a - x_j a = 0$.

$(x_i - x_j)\, a = 0$ $\because a \neq 0$,

Suppose since R has no zero divisor

$x_i - x_j = 0$.

$x_i = x_j$ which is contradiction to R.

$\therefore$ All element in Sa are distinct. $\Rightarrow$ Sa = R.

$S_a = \{x_1 a, x_2 a, x_3 a, \ldots x_n a\} = R$.

$\because a \in R$, $a = x_{i_0} a = a x_{i_0}$ for some i_0 (commutative)

Let $y \in R$, then $y = x_j a$ for some j

$$y x_{i_0} = (x_j a) x_{i_0}$$
$$= x_j (a x_{i_0})$$
$$= x_j a$$
$$= y$$

By commutative, $x_{i_0} y = y$.

$\therefore y x_{i_0} = x_{i_0} y = y \quad \forall y \in R$.

$\Rightarrow x_{i_0} = 1 \in R$.

By construction of S_a and $1 \in R$, $1 = x_m a$ for some m.

$\because a$ is arbitrary every non-zero element has a inverse. $\therefore R$ is a field.

$(Z \times Z, *_1, *_2)$ - ring but not field & integral domain.

Definition of subring:

Let $(R, +, \cdot)$ be a ring. A non-empty subset S of R is said to be a subring if $(S, +, \cdot)$ is a ring.

* $(Z, +, \cdot)$ is a ring & $(nZ, +, \cdot)$ is a subring.
* $(R, +, \cdot)$ - ring & $(Z, +, \cdot)$ - subring.

Ideal: Let $(R, +, \cdot)$ be a ring. A non-empty subset I of R is said to be an ideal if

* $(I, +)$ is a subgroup of $(R, +)$
* $ra \in I$ (left) and $ar \in I$ (right) $\forall a \in I$ and $r \in R$.

Every subring is not an ideal

Eg: $(Z, +, \cdot)$

* $(2Z, +)$ is a subgroup.
* Let $r \in Z$ & $a \in 2Z$.

  $ar = ra =$ even.

  $\therefore (2Z, +, \cdot)$ is an ideal.

$(R, +, \cdot)$

* $(Z, +)$ is a subgroup
* $ar = ra \in R$.

  but it should $\in Z$.

  $\therefore (Z, +, \cdot)$ is not an ideal.

→ A subring need not be an ideal. Eg. $(R, +, \cdot)$ is a ring and $(Z, +, \cdot)$ is a subring but it is not an ideal.

→ Every ideal is a subring.

Problems:

1) $(M_2(R), +, \cdot)$ is a ring. Verify that the subset $I = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in R \right\}$

$(I, +)$ is a subgroup.

Let $A \in I$ & $B \in M_2(R)$

$A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ $B = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$

$AB \neq BA$.

$\therefore$ I is not an ideal but it is a subring.

2) Consider a ring $(Z_6, \oplus_6, \odot_6)$. subset: $\{0, 2, 4\}$ is an ideal or subring.

$R = (Z_6, \oplus_6, \odot_6)$

$I = \{0, 2, 4\}$

$(I, \oplus_6)$ is a subgroup.

Let $a \in I$ & $r \in R$

$ar = ra \in I$.

$\therefore \{0, 2, 4\}$ is an ideal and subring.

Theorem: Let R be a ring with unity and I be an ideal. If $1 \in I$, then prove that $I = R$.

To prove that $I = R$ we have to prove $I \subseteq R$ & $R \subseteq I$

By ideal definition, $I \subseteq R$. $\therefore$ We have to prove $R \subseteq I$.

Let $r \in R$. Then $1 \cdot r = r \in I$ [$\because ar \in I$, $a = 1$, By (ii)]

$\therefore R \subseteq I$.

$\Rightarrow I = R$.

Let R be a commutative ring with unity, Suppose $\{0\}$ and R are the only ideal of R. Then prove that R is a field

Proof: It is enough to prove that every non-zero element has a multiplicative inverse. Let $a \neq 0 \in R$.

Consider $Ra = \{ra : r \in R\}$ $\because 1 \in R$, $1 \cdot a = a \in Ra$.

$\therefore$ It is non-empty

Claim: Ra is an ideal of R. First we have to prove $(Ra, +)$ is a subgroup.

* closure: Let $u = r_1 a$ and $v = r_2 a$ for some $r_1, r_2 \in R$.
  Then $u + v = r_1 a + r_2 a = (r_1 + r_2) a \in Ra$.
* associative: It is obviously true.
* identity: $0 + a = a \in Ra$ $\therefore$ additive identity exist.
  $\because 0.a = 0 \in Ra$.
* inverse: If $u \in Ra$ i.e $u = ra$ then $-u = -ra \in Ra$.

$\therefore (Ra, +)$ is a subgroup.

Secondly, we have to prove $(Ra, +)$ is an ideal.

$ru \in Ra$ for all $r \in R$ and $u \in Ra$.

$\because u \in Ra$, $u = r_1 a$ for some $r_1 \in R$.

$ra \rightarrow ru = r(r_1 a) = (rr_1) a \in Ra$.

$\therefore Ra$ is an ideal.

$\because$ it is a commutative ring, ra & $ar \in Ra$.

$\because a \in Ra$, $Ra = R$.

$\because 1 \in R$, $1 \in Ra$ then $1 = r_1 a$ for some $r_1 \in R$.

$\therefore R$ is a field.

Let R be a field then prove that R has only two ideals $\{0\}$ and R.

Proof: Suppose I is an ideal and $I \neq \{0\}$ then there exists $a \neq 0 \in R$ such that $a \in I$. $\because R$ is a field, $a^{-1} \in R$ exists. Then $a^{-1}a = 1 \in I$ $[\because a^{-1} \in R, a \in I]$

$\therefore I = R$. [By 1st 2 mark].

Quotient ring:

Let R be a ring and I be an ideal. Then quotient ring is $\frac{R}{I} = \{r + I \mid r \in R\}$ under

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

(1st element, 2nd element)

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

Example. $R = (Z, +, \cdot)$ $I = (2Z, +, \cdot)$

$$\frac{R}{I} = \frac{Z}{2Z} = \{r + 2Z \mid r \in Z\}$$

$$= \{0 + 2Z,\ 1 + 2Z,\ -1 + 2Z,\ 2 + 2Z, \ldots\}$$

$$= \{2Z, \text{ set of all odd integers}\}$$

$0 + 2Z = 2Z.$
$1 + 2Z =$ set of odd integers
$-1 + 2Z =$ set of odd integers
$2 + 2Z = 2Z.$

Ring Homomorphism:

Let $(R, +, \cdot)$ and $(R', +', \cdot')$ be two rings. A function $f : R \to R'$ is said to be a homomorphism if

$$f(a + b) = f(a) +' f(b)$$
$$f(a \cdot b) = f(a) \cdot' f(b)$$

Kernel of $f = \{x \in R : f(x) = 0\} \subseteq R$

Range of $f = \{f(x) \in R' : x \in R\} \subseteq R'$

Eg1. Define $f : (Z, +, \cdot) \to (Z, +, \cdot)$ by $f(x) = 0$. (zero homomorphism)

$f(a + b) = f(a) +' f(b)$

LHS: $f(a + b) = 0.$

RHS: $f(a) = f(b) = 0.$

$f(a) + f(b) = 0$

$\therefore f(a + b) = f(a) +' f(b)$

$f(a \cdot b) = f(a) \cdot' f(b)$

LHS: $f(a \cdot b) = 0.$

RHS: $f(a) = f(b) = 0.$

$\therefore f(a \cdot b) = f(a) \cdot f(b)$

$\therefore f$ is a ring homomorphism.

Kernel $= Z.$

Range $= \{0\}$

Eg 2. $f : (Z, +, \cdot) \to (Z, +, \cdot)$ by $f(x) = x$. (Identity homomorphism)

It is a ring homomorphism.

Kernel $= \{0\}$ Range $= Z$.

Eg 3. $f : (Z, +, \cdot) \to (Z, +, \cdot)$ by $f(x) = 2x$.

Not a ring homomorphism.

Eg 4. Define $f : (Z, +, \cdot) \to (Z_n, \oplus_n, \odot_n)$ by $f(x) = x \% n$.

$f(a+b) = f(a) +' f(b)$

$f(a+b) = (a+b) \% n$

$f(a) = a \% n$

$f(b) = b \% n$

$f(a) \oplus_n f(b) = (a \% n) \oplus_n (b \% n)$

$\therefore f$ is a ring homomorphism.

$f(ab) = f(a) \cdot' f(b)$

$f(ab) = (ab) \% n$

$f(a) = a \% n$

$f(b) = b \% n$

$f(a) \odot_n f(b) = (a \% n) \odot_n (b \% n)$

Kernel $= nZ$ multiples of n. Range $= Z_n$.

Eg 5. Define $f : (C, +, \cdot) \to (C, +, \cdot)$ by $f(z) = \bar{z}$ where

$z = a + bi$, $\bar{z} = a - bi$

$f(z_1 + z_2) = f(a + bi + c + di)$

$= f((a+c) + i(b+d))$

$= (a+c) - i(b+d)$

$f(z_1) = a - bi$

$f(z_2) = c - di$

$f(z_1) + f(z_2) = a - bi + c - di$

$= (a+c) - i(b+d)$

$f(z_1 z_2) = f((a+ib)(c+id))$

$= f((ac - bd) + i(bc + ad))$

$= (ac - bd) - i(bc + ad)$

$\therefore$ ring homomorphism. Kernel $= \{0\}$, range $= C$.

$f(z_1) = a - bi$

$f(z_2) = c - di$

$f(z_1) f(z_2) = (a - ib)(c - di)$

$= (ac - bd) - i(bc + ad)$

Theorem: Let $f : R \to R'$ be a ring homomorphism then prove that kernel of f is an ideal of R.

Proof: Let kernel of $f = \{r \in R : f(r) = 0\} = I$

Since $f(0) = 0$, $0 \in I$ $\therefore I$ is non-empty.

To prove: $(I, +)$ is a subgroup.

* Closure: Let $r_1, r_2 \in I = \ker f$ Then $f(r_1) = f(r_2) = 0$.

To prove $r_1 + r_2 \in I$.

$f(r_1 + r_2) = f(r_1) + f(r_2)$ ($\because$ ring homomorphism)

$= 0$.

$\therefore r_1 + r_2 \in I$.

* associative obviously true.
* Identity : $\because f(0) = 0, \quad 0 \in I.$
* Inverse : Let $r \in I = \ker f$ Then $f(r) = 0.$

To prove $-r \in I = \ker f$ i.e $f(-r) = 0.$

$$f(-r) = -f(r)$$
$$= 0.$$

$\therefore -r \in I.$

$\therefore (I, +)$ is a subgroup.

We have to prove $a \in I, r \in R \Rightarrow ar \in I$ & $ra \in I.$

$\because a \in I, \quad f(a) = 0.$

To prove $f(ar) = 0.$

$$f(ar) = f(a) f(r) \quad (\because \text{ring homomorphism})$$
$$= 0 \cdot f(r)$$
$$= 0.$$

$\therefore ar \in I.$

$$f(ra) = f(r) f(a)$$
$$= f(r) \cdot 0$$
$$= 0$$

$\therefore ra \in I.$

Fundamental theorem of ring homomorphism:

Let $f : R \to R'$ be an onto isomorphism where R & R' are rings. Then $\frac{R}{\ker f} \cong R'.$

Result : $\frac{\mathbb{Z}}{n\mathbb{Z}} \cong Z_n$

Polynomial Rings: (integral domain but not field).

Let R be a ring. The set of all polynomials whose co-efficients are in R is denoted by $R[x]$ i.e

$$R[x] = \{ a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in R, \; 0 \le i \le n \}$$

* $2x^3 + 5x - \frac{7}{2}$ - polynomial over $Q, R, C, Q(\sqrt{2})$
* $x^2 + x + 1$ - polynomial over $Z, Z_2, R, Q, Z_n.$
* $x^3 + i$ - polynomial over C, $Z[i] = \{a + bi \mid a, b \in Z\}$

Irreducable polynomial : Let F be a field and $f(x) \in F[x]$. $f(x)$ is irreducable if whenever $f(x) = g(x)h(x)$, either $g(x)$ or $h(x)$ is of degree 0. $g(x)$ & $h(x) \in F[x]$

A polynomial which is not irreducable is called reducable.

Eg. $f(x) = x^2+1$ is irreducable over R.

$f(x) = x^2+1$ is reducable over C.

$f(x) = (x+i)(x-i)$

$f(x) = x^2+x+1$ over Z_2

$f(0) = 1 \,\%\, 2 = 1$.

$f(1) = 3 \,\%\, 2 = 1$

$\therefore$ Irreducable.

$f(x) = x^2+x+1$ over Z_3

$f(0) = 1$

$f(1) = 3 \,\%\, 3 = 0$.

$\therefore$ Reducable.

$x(x+1)+1$

Z_3 Reduce

$f(x) = 5x^3+4x+3$

$f(x) = \frac{5}{3}x^3 + \frac{4}{3}x + \frac{3}{3}$

$= 2x^3 + x + 0$.

Reducability test of degree 2 or 3 for polynomial :

Statement : Let F be a field, If $f(x) \in F[x]$ & degree of $f(x)$ is 2 or 3 then $f(x)$ is reducable over F if & only if $f(x)$ has a root in F.

Remark : Reducability test of degree 2 or 3 fails if the polynomial have degree strictly greater than 3.

Eg. Consider the polynomial $x^4 + 2x^2 + 1$ over Q.

$P(x) = x^4 + 2x^2 + 1$

$P(x) = (x^2+1)^2$

This polynomial has 4 roots $i, i, -i, -i$ which $\notin Q$.

$\therefore$ Reducability test fails. But the given polynomial is reducable.

Content of a Polynomial : Content of a non-zero polynomial $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ where $a_0, a_1, \dots a_n$ are integers is a greatest common divisor of $a_0, a_1, a_2 \dots a_n$.

Ex 1. $2x^3 + 4x^2 + 6x + 2$ has content 2.

Ex 2. $x^2 + x + 1$ has content 1. (primitive polynomial)

Primitive polynomial is a polynomial having content 1.

Remark : Any polynomial can be written as product of primitive polynomial

i.e. $p(x) = c \cdot q(x)$ ↗

① Gauss Lemma: Product of two primitive polynomial is again a primitive polynomial. also

Proof: Suppose $f(x)$ & $g(x)$ be 2 primitive polynomials.

claim: $f(x)\,g(x)$ is primitive.

Suppose $f(x)\,g(x)$ is not primitive. Then content of $f(x)\,g(x)$ is greater than 1 and $\exists$ p which divides content of $f(x)\,g(x)$.

Let $\overline{f(x)}$, $\overline{g(x)}$ & $\overline{f(x)g(x)}$ be polynomials in $Z_p[x]$ by reducing the co-efficients of $f(x)$, $g(x)$ & $f(x)\,g(x)$ modulo p.

$\because \overline{f(x)}\;\overline{g(x)} = \overline{f(x)\,g(x)}$ & $f(x)\,g(x) = c\,h(x)$

$\therefore \overline{f(x)}\cdot\overline{g(x)} = 0$. $\because Z_p[x]$ is an integral domain.

Either $\overline{f(x)}$ & $\overline{g(x)}$ should be 0. $\therefore$ every co-efficient of $f(x)$ & $g(x)$ divided by p. But $f(x)$ & $g(x)$ are primitive polynomials, which is contradiction. $\therefore$ $f(x)\,g(x)$ is primitive.

Reducible in $\mathbb{Q} \Rightarrow$ Reducible in Z.

② Suppose $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducable over $\mathbb{Q}$, then $f(x)$ is reducable in Z.

Proof: Let $f(x) \in Z[x]$ & $f(x)$ is primitive $\because f(x)$ is reducable over $\mathbb{Q}$,

$f(x) = g(x)\,h(x)$ where $g(x)$ & $h(x) \in \mathbb{Q}[x]$

T.P: $f(x) = g_1(x)\,h_1(x)$ where $g_1(x)$ & $h_1(x) \in Z[x]$

Let a = lcm of denominators of co-efficients of $g(x)$ and

b = lcm of denominators of co-efficients of $h(x)$

Now $ab\,f(x) = ab\,g(x)\,h(x)$

$ab\,f(x) = a\,g(x)\;b\,h(x)$.

Then $a\cdot g(x) \in Z[x]$ & $b\cdot h(x) \in Z[x]$

$\therefore a\cdot g(x) = c_1\,g_1(x)$ & $b\cdot h(x) = c_2\,h_1(x)$

where c_1, c_2 content of $a\cdot g(x)$ & $b\cdot h(x)$

$g_1(x)$ & $h_1(x)$ are primitive polynomials.

$ab\,f(x) = c_1\,g_1(x)\;c_2\,h_1(x)$

$ab\,f(x) = c_1 c_2\,g_1(x)\,h_1(x)$

$\therefore$ content of $f(x) = ab$ content of $g_1(x)\cdot h_1(x) = c_1c_2$.

content of LHS = RHS $\Rightarrow ab = c_1c_2$.

$ab\,f(x) = ab\,g_1(x)\,h_1(x)$ $\therefore f(x) = g_1(x)\,h_1(x)$ where

$g_1(x) \in Z[x]$ & $h_1(x) \in Z[x]$

$\therefore f(x)$ is reducable over Z.

If $g(x) = \frac{5}{3}x^2 + \frac{7}{2}$

$a = 6$.

$a\cdot g(x) = 10x^2 + 21$

$\Rightarrow g(x) \in Z[x]$

mod p Test (for degree more than 3): Let p be a prime number and suppose that $f(x) \in Z[x]$ with degree ≥ 1. Let $\overline{f(x)}$ be a polynomial in $Z_p[x]$ obtain from $f(x)$ by reducing the co-efficients of $f(x)$ modulo p. If $\overline{f(x)}$ is irreducible over Z_p then $f(x)$ is irreducible over Q.

$f(x) \in Z[x] \Rightarrow \overline{f(x)} \in Z_p[x]$ $\exists$ p-prime

$\overline{f(x)}$ is irreducible in $Z_p \Rightarrow f(x)$ is irreducible in Q.

Here degree of $f(x)$ = degree of $\overline{f(x)}$

Problems: 1) Prove that $f(x) = 21x^3 - 3x^2 + 2x + 9$ is irreducible over Q.

$f(x) \in Z[x]$. Take $p = 2$. $\because -1 \notin Z_2$

$\overline{f(x)} = x^3 + x^2 + 0x + 1$. $\because -1$ = additive inverse of 1 $= 1$.

$= x^3 + x^2 + 1 \in Z_2[x]$ Check 0 and 1 are zeros.

$\overline{f(0)} = 1$ and $\overline{f(1)} = 3 \% 2 = 1. \neq 0$.

$\therefore \overline{f(x)}$ is irreducible over $Z_2 \Rightarrow f(x)$ is irreducible over Q. (By mod p test).

2) $f(x) = \frac{3}{7}x^4 - \frac{2}{7}x^3 + \frac{9}{35}x + \frac{3}{5}$. Is it irreducible over Q?

$f(x) = \frac{15x^4 - 10x^2 + 9x + 21}{35}$

$35 f(x) = 15x^4 - 10x^2 + 9x + 21$

$h(x) = 15x^4 - 10x^2 + 9x + 21$

Take $p = 2$,

$\overline{h(x)} = x^4 + x + 1 \in Z_p[x]$

$\overline{h(0)} = 1$ $\overline{h(1)} = 3 \% 2 = 1$.

$\therefore \overline{h(x)}$ has no root in Z_2. We can't reduce it by a linear & cubic

$$x^4 + x + 1 = (a_1x^2 + b_1x + c_1)(a_2x^2 + b_2x + c_2)$$

Here $a_1a_2 = 1 \Rightarrow a_1 = a_2 = 1$.

$c_1c_2 = 1 \Rightarrow c_1 = c_2 = 1$.

$$x^4 + x + 1 = (x^2 + b_1x + 1)(x^2 + b_2x + 1)$$

$$= x^4 + b_2x^3 + x^2 + b_1x^3 + b_1b_2x^2 + b_1x + x^2 + b_2x + 1$$

$$= x^4 + (b_1 + b_2)x^3 + b_1b_2x^2 + (b_1 + b_2)x + 1$$

Equating, $b_1 + b_2 = 0$, $b_1b_2 = 0$, $b_1 + b_2 = 1$. which is not possible.

$\therefore \overline{h(x)}$ is irreducible over $Z_2 \Rightarrow f(x)$ is irreducible over $\mathbb{Q}$.

Eisenstein Criterian: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in Z[x]$. If $\exists$ a prime p such that $p \nmid a_n$ (does not divides), $p \mid a_{n-1}, \dots, p \mid a_1, p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Eg. $f(x) = 3x^5 + 15x^4 - 20x^3 + 10x + 20$.

Take $p = 5$. p divides 15, 20, 10, 20 but does not divides 3 & 25

$\therefore$ By Eisenstein criterian, $f(x)$ is irreducible over $\mathbb{Q}$.

Proof: $(b_0 + b_1 x + b_2 x^2)(c_0 + c_1 x + c_2 x^2 + c_3 x^3)$

$= b_0 c_0 + b_0 c_1 x + b_0 c_2 x^2 + b_0 c_3 x^3 + b_1 c_0 x + b_1 c_1 x^2 + b_1 c_2 x^3 + b_1 c_3 x^4 + b_2 c_0 x^2 + b_2 c_1 x^3 + b_2 c_2 x^4 + b_2 c_3 x^5.$

$= b_0 c_0 + (b_0 c_1 + b_1 c_0) x + (b_0 c_2 + b_1 c_1 + b_2 c_0) x^2 + (b_0 c_3 + b_1 c_2 + b_2 c_1) x^3 + (b_1 c_3 + b_2 c_2) x^4 + b_2 c_3 x^5.$

Constant $= b_0 c_0$, Co-eff of $x = b_0 c_1 + b_1 c_0$, Co-eff of $x^2 = b_0 c_2 + b_1 c_1 + b_2 c_0$

Co-eff of $x^3 = b_0 c_3 + b_1 c_2 + b_2 c_1$, Co-eff of $x^4 = b_1 c_3 + b_2 c_2$, Co-eff of $x^5 = b_2 c_3$

General: $(b_0 + b_1 x + b_2 x^2 + \dots b_r x^r)(c_0 + c_1 x + c_2 x^2 + \dots c_s x^s)$

Co-eff of $x^t = b_t c_0 + b_{t-1} c_1 + b_{t-2} c_2 + \dots + b_0 c_t$

Proof: Suppose $f(x)$ is reducible over $\mathbb{Q}$. By Gauss lemma (ii), $f(x)$ is reducible over Z. Then $f(x) = g(x) h(x)$ where $g(x), h(x) \in Z[x]$ & $1 \le$ degree $g(x) \le r$, $1 \le$ degree $h(x) \le s$. and $r + s = n$. Let $g(x) = (b_0 + b_1 x + b_2 x^2 + \dots + b_r x^r)$ & $h(x) = (c_0 + c_1 x + c_2 x^2 + \dots + c_s x^s)$ where $b_0, b_1, \dots b_r, c_0, c_1, \dots c_s \in Z$.

Now, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

$f(x) = (b_0 + b_1 x + \dots + b_r x^r)(c_0 + c_1 x + \dots c_s x^s)$ $\quad p \mid a_0 \Rightarrow p \mid b_0 c_0$

$\Rightarrow a_0 = b_0 c_0$ and $a_n = b_r c_s$, From given statement, ~~$p \mid a_0$ & $p \nmid b_r c_s$~~

$\Rightarrow p \mid b_0$ or $p \mid c_0$, $p \nmid a_n \Rightarrow p \nmid b_r c_s \Rightarrow p \nmid b_r$ & $p \nmid c_s$

Let b_t be the first term which does not divided by p.

i.e $p \mid b_0, p \mid b_1, \dots p \mid b_{t-1}$ & $p \nmid b_t$

Coeff of x^t = $a_t = b_t c_0 + b_{t-1} c_1 + \dots + b_0 c_t$

$a_t - b_{t-1} c_1 - b_{t-2} c_2 - \dots - b_0 c_t = b_t c_0$

LHS is divided by t but RHS is not divided by t which is contradiction.

$\because p^2 \nmid a_0 \Rightarrow p^2 \nmid b_0 c_0$

$p^2 \nmid c_0$ & $p^2 \nmid b_0$

$\Rightarrow p \nmid c_0$

$p \nmid b_t c_0$ $\because p \mid a_t, p \mid b_0, p \mid b_1, \dots p \mid b_{t-1}$

$\Rightarrow p \mid a_t - b_{t-1} c_1 - b_{t-2} c_2 - \dots - b_0 c_t$

now $p \mid$ LHS but $p \nmid$ RHS. which is $\Rightarrow\Leftarrow$

$\therefore f(x)$ is irreducible over $\mathbb{Q}$.