Name => Shubham choudhary
Roll No => 21 bca 087
Notes => ~~2nd~~ Sem

Unit – I

Accessive differentiation

Q⇒ if $f(x) = \tan x$ show that $f^{iv}(0) = 16$

$f(x) = \tan x$ — (I)

$f'(x) = \sec^2 x = 1 + \tan^2 x$

$f''(x) = 2\tan x \sec^2 x$
$= 2\tan x (1 + \tan^2 x)$
$= 2\tan x + 2\tan^3 x$

$f'''(x) = 2f(x) + 2(f(x))^3$ — (III)

$f^{iii}(x) = 2f'(x) + 6(f(x))^2 f''(x)$ — (IV)

$f^{iv}(x) = 2f''(x) + 6(f(x))^2 f''(x) + 12 f(x)(f'(x))^2$

$f^{v}(x) = 2f'''(x) + 12(f'(x))^3 + 12 \times 2 f(x) f'(x) f''(x)$
$+ 12 f(x) f'(x) f''(x) + 6(f(x))^2 f'''(x)$ — (VI)

Put $x = 0$ in (I) to (VI)

$f(0) = \tan 0 = 0$

$f'(0) = 1 + \tan^2 0 = 1 + 0 = 1$

$f''(0) = 2f(0) + 2(f(0))^3 = 2 \times 0 + 2 \times 0 = 0$

$f'''(0) = 2f'(0) + 6(f(0))^2 f'(0) = 2 \times 1 + 6 \times 0 \times 1 = 2$

$f^{iv}(0) = 2f''(0) + 12 f(0)(f'(0))^2 + 6(f(0))^2 f''(0)$
$= 2 \times 0 + 12 \times 0 \times 1 + 6 \times 0 \times 0 = 0$

$f^{v}(0) = 2f'''(0) + 12(f'(0))^3 + 24 f(0) f'(0) f''(0)$
$+ 12 f(0) f'(0) f''(0) + 6(f(0))^2 f'''(0)$

$= 2 \times 2 + 12 \times (1)^3 + 0 + 0 + 0 = 4 + 12 = 16$

Q⇒ $y = \cosh(\log x) + \sinh(\log x)$. Prove that $y_n = 0$ for $n > 1$

Ans diff both sides w.r.t. x, we get

$y_1 = \sinh(\log x) \cdot \frac{1}{x} + \cosh(\log x) \cdot \frac{1}{x} \cdot (\log x)$

$x y_1 = \sinh(\log x) + \cosh(\log x)$

$x y_1 = y$

Again diff w.r.t. x, we get

$x y_2 + y_1 = y_1$

$x y_2 = 0$

$y_2 = 0$

$y_n = 0$ for $n > 1$

Ques⇒ $y = ae^{mx} + be^{-mx}$ then prove that $y_2 - m^2 y = 0$

⇒ $y = ae^{mx} + be^{-mx}$

$y_1 = ame^{mx} - bme^{-mx}$

$y_2 = am^2 e^{mx} + bm^2 e^{-mx}$

$y_2 = m^2 (ae^{mx} + be^{-mx})$

$y_2 = m^2 y$

$y_2 - m^2 y = 0$

Ques ⇒ $y = \tan^{-1} x$ show that $(1+x^2)\frac{d^2y}{dx^2} + (2x)\frac{dy}{dx} = 0$

$$\frac{dy}{dx} = \frac{1}{1+x^2}$$

$$(1+x^2)\frac{dy}{dx} = 1$$

$$(1+x^2)\frac{d^2y}{dx^2} + 2x\frac{dy}{dx} = 0$$

Derivative of n^{th} order of some standard function

(i) $y = (ax+b)^m$ then $y_n = m(m-1)(m-2)\ldots(m-n+1)(ax+b)^{m-n}a^n$

(ii) if $y = \frac{1}{ax+b}$ then $y_n = \frac{(-1)^n \lfloor n \, a^n}{(ax+b)^{n+1}}$, $x \neq -\frac{b}{a}$

(iii) if $y = \log(ax+b)$ then $y_n = \frac{(-1)^{n-1}\lfloor n-1}{(ax+b)^n} \cdot a^n$, $x > -\frac{b}{a}$

(iv) if $y = a^{mx}$ then $y_n = a^{mx}(\log a)^n m^n$

(v) if $y = \sin(ax+b)$, then $y_n = a^n \sin\left(ax+b+\frac{n\pi}{2}\right)$

(vi) if $y = \cos(ax+b)$, then $y_n = a^n \cos\left(ax+b+\frac{n\pi}{2}\right)$

(vii) if $y = e^{ax}\sin(bx+c)$, then $y_n = (a^2+b^2)^{\frac{n}{2}} e^{ax} \sin\left(bx+c+n\tan^{-1}\frac{b}{a}\right)$

(viii) if $y = e^{ax}\cos(bx+c)$, then $y_n = (a^2+b^2)^{\frac{n}{2}} e^{ax} \cos\left(bx+c+n\tan^{-1}\frac{b}{a}\right)$

Ques ⇒ find the n^{th} derivative $\sqrt{ax+b}$

⇒ $y = \sqrt{ax+b} = (ax+b)^{\frac{1}{2}}$

$$y_1 = \frac{1}{2}(ax+b)^{-\frac{1}{2}} \times a$$

$$y_2 = \frac{1}{2}\left(-\frac{1}{2}\right)(ax+b)^{-\frac{3}{2}} \times a^2$$

$$y_3 = \frac{1}{2}\left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)(ax+b)^{-\frac{5}{2}} \times a^3$$

$$y_n = \frac{(-1)^{n-1} \, 1.3.5\ldots(2n-1) \, a^n}{2^n (ax+b)^{2n-\frac{1}{2}}}$$

Q. Find the n^{th} derivative

$$y = \log(x^2-a^2) = \log[(x-a)(x+a)]$$

$$= \log(x-a) + \log(x+a)$$

$$y_n = \frac{(-1)^{n-1}\lfloor n-1}{(x-a)^n} + \frac{(-1)^{n-1}\lfloor n-1}{(x+a)^n}$$

Ques ⇒ find the n^{th} derivative of

$$y = \frac{1}{(x+2)(x+3)}$$

$$= \frac{1}{(x+2)(2+3)} + \frac{1}{(-3+2)(x+3)}$$

$$= \frac{1}{x+2} - \frac{1}{x+3}$$

$$y_n = \frac{(-1)^n \lfloor n}{(x+2)^{n+1}} - \frac{(-1)^n \lfloor n}{(x+3)^{n+1}}$$

Qu a ⇒ find n^{th} derivative $e^x \cos^3 x$

$$\cos^3 x = \frac{1}{4}\cos 3x + \frac{3}{4}\cos x \quad [\cos 3x = 3\cos x - 4\cos^3 x]$$

$$y = e^x\left[\frac{1}{4}\cos 3x + \frac{3}{4}\cos x\right]$$

$$y = \frac{1}{4}e^x \cos 3x + \frac{3}{4}e^x \cos x$$

$$y_n = \frac{1}{4}(1^2+3^2)^{\frac{n}{2}} e^x \cos(3x + n\tan^{-1}3/1) + \frac{3}{4}(1^2+1^2)^{\frac{n}{2}} e^x \cos(x + n\tan^{-1}\frac{1}{1})$$

Qus ⇒ let $y = \frac{x}{1+3x+2x^2}$

$$= \frac{x}{(x+1)(2x+1)}$$

$$= \frac{-1}{(x+1)(-2+1)} + \frac{-1/2}{(-\frac{1}{2}+1)(2x+1)}$$

$$= \frac{1}{(x+1)} - \frac{1}{2x+1}$$

$$y_n = \frac{(-1)^n \lfloor n}{(x+1)^{n+1}} - \frac{(-1)^n \lfloor n 2^n}{(2x+1)^{n+1}}$$

$$= (-1)^n \lfloor n \left[\frac{1}{(x+1)^{n+1}} - \frac{2^n}{(2x+1)^{n+1}}\right]$$

⇒ Leibnitz's Theorem

⇒ If u and v are functions of x possessing n^{th} order derivatives, then

$$(uv)_n = {}^nC_0\, u_n v + {}^nC_1\, u_{n-1} v_1 + {}^nC_2\, u_{n-2} v_2 + \ldots + {}^nC_r\, u_{n-r} v_r + \ldots + {}^nC_n\, u v_n$$

where u_r denotes the rth order derivative of u and ${}^nC_r$ denotes the number of combinations out of n different things taken r at a time.

Proof we have

$$(uv)_1 = u_1 v + u v_1 = {}^1C_0\, u_1 v + {}^1C_1\, u v_1$$

∴ theorem is true for $n=1$

Assume that the theorem is true for $n=m$, where m is a positive integer.

$$\therefore (uv)_m = {}^mC_0\, u_m v + {}^mC_1\, u_{m-1} v_1 + {}^mC_2\, u_{m-2} v_2 + \ldots + {}^mC_{r-1}\, u_{m-r+1} v_{r-1} + {}^mC_r\, u_{m-r} v_r + \ldots + {}^mC_m\, u v_m$$

Differentiating both sides w.r.t. x, we get,

$$(uv)_{m+1} = {}^mC_0\, u_{m+1} v + {}^mC_0\, u_m v_1 + {}^mC_1\, u_m v_1 + {}^mC_1\, u_{m-1} v_2 + {}^mC_2\, u_{m-1} v_2 + {}^mC_2\, u_{m-2} v_3 + \ldots + {}^mC_{r-1}\, u_{m-r+2} v_{r-1} + {}^mC_{r-1}\, u_{m-r+1} v_r + {}^mC_r\, u_{m-r+1} v_r + {}^mC_r\, u_{m-r} v_{r+1} + \ldots + {}^mC_m\, u_1 v_m + {}^mC_m\, u v_{m+1}$$

$\therefore (uv)_{m+1} = {}^mC_0\, u_{m+1}v + ({}^mC_0 + {}^mC_1)u_m v_1 + ({}^mC_1 + {}^mC_2)u_{m-1}v_2 + \ldots + ({}^mC_{r-1} + {}^mC_r)u_{m-r+1}v_r + \ldots + {}^mC_m u v_{m+1}$

But ${}^mC_0 = 1 = {}^{m+1}C_0$

${}^mC_0 + {}^mC_1 = {}^{m+1}C_1$

${}^mC_1 + {}^mC_2 = {}^{m+1}C_2$

${}^mC_{r-1} + {}^mC_r = {}^{m+1}C_r$

${}^mC_m = 1 = {}^{m+1}C_{m+1}$

$\therefore$ We have

$(uv)_{m+1} = {}^{m+1}C_0\, u_{m+1}v + {}^{m+1}C_1 u_m v_1 + {}^{m+1}C_2 u_{m-1}v_2 + \ldots + {}^{m+1}C_r u_{m-r+1}v_r + \ldots + {}^{m+1}C_{m+1}\, u v_{m+1}$

$\therefore$ theorem is true for $n = m+1$

$\therefore$ if the theorem is true for $n = m$, then it is also true for $n = m+1$

But the theorem is true for $n = 1$

$\therefore$ by the method of induction, theorem is true for all positive integers n.

1) Find the n^{th} derivative of $e^x \sin x$

Sol (i) $y = e^x \sin x$

Let $u = e^x$ $\quad v = \sin x$

$u_1 = e^x$ $\quad v_1 = \sin\left(x + \frac{\pi}{2}\right)$

$u_2 = e^x$ $\quad v_2 = \sin\left(x + 2\cdot\frac{\pi}{2}\right)$

$u_n = e^x$ $\quad v_n = \sin\left(x + n\frac{\pi}{2}\right)$

By Leibnitz's rule

$y_n = (uv)_n = {}^nC_0 u_n v + {}^nC_1 u_{n-1} v_1 + {}^nC_2 u_{n-2} v_2 + \ldots + {}^nC_n u v_n$

$= \left[1 \cdot e^x \sin x + n \cdot e^x \sin\left(x + \frac{\pi}{2}\right) + \frac{n(n-1)}{2\cdot 1} e^x \sin\left(x + 2\cdot\frac{\pi}{2}\right) + \ldots + 1 \cdot e^x \sin\left(x + \frac{n\pi}{2}\right)\right]$

$= e^x\left[1 \cdot \sin x + n \sin\left(x + \frac{\pi}{2}\right) + \frac{n(n-1)}{2\cdot 1}\sin\left(x + 2\cdot\frac{\pi}{2}\right) + \ldots + 1 \sin\left(x + \frac{n\pi}{2}\right)\right]$

(ii) If $y^{\frac{1}{m}} + y^{-\frac{1}{m}} = 2x$, prove that $(x^2-1)y_{n+2} + (2n+1)x y_{n+1} + (n^2 - m^2)y_n = 0$.

Sol $y^{\frac{1}{m}} + y^{-\frac{1}{m}} = 2x \Rightarrow y^{\frac{1}{m}} + \frac{1}{y^{\frac{1}{m}}} = 2x$

$\Rightarrow y^{\frac{2}{m}} + 1 = 2x y^{\frac{1}{m}} \Rightarrow y^{\frac{2}{m}} - 2x y^{\frac{1}{m}} + 1 = 0$

$\Rightarrow y^{\frac{1}{m}} = \frac{2x \pm \sqrt{4x^2 - 4}}{2} = x \pm \sqrt{x^2 - 1}$

$\Rightarrow y = (x+\sqrt{x^2-1})^m + (x-\sqrt{x^2-1})^m$

let us take $y = (x+\sqrt{x^2-1})^m$

$\therefore y_1 = m(x+\sqrt{x^2-1})^{m-1} \times \left[1+\frac{2x}{2\sqrt{x^2-1}}\right]$

$= m(x+\sqrt{x^2-1})^{m-1} \times \frac{\sqrt{x^2-1}+x}{\sqrt{x^2-1}} = \frac{m(x+\sqrt{x^2-1})^m}{\sqrt{x^2-1}}$

$\therefore y_1 = \frac{my}{\sqrt{x^2-1}} \Rightarrow y_1^2 = \frac{m^2y^2}{x^2-1} \quad -(1)$

Again when $y = (x-\sqrt{x^2-1})^m$

$y_1 = m(x-\sqrt{x^2-1})^{m-1} \times \left[1-\frac{2x}{2\sqrt{x^2-1}}\right]$

$= m(x-\sqrt{x^2-1})^{m-1} \times \left(\frac{\sqrt{x^2-1}-x}{\sqrt{x^2-1}}\right]$

$= \frac{-m(x-\sqrt{x^2-1})^m}{\sqrt{x^2-1}} = \frac{-my}{\sqrt{x^2-1}}$

$\Rightarrow y_1^2 = \frac{m^2y^2}{x^2-1} \quad -(2)$

from (1) and (2), we get

$y_1^2 = \frac{m^2y^2}{x^2-1} \Rightarrow (x^2-1)y_1^2 = m^2y^2$

Differentiating both side w.r.t x we get

$(x^2-1).2y_1y_2 + y_1^2(2x) = m^2.2yy_1$

Dividing both sides by $2y_1$, we get, $(x^2-1)y_2 + xy_1 = m^2y$

Differential both sides n times, we get,

$[{}^nC_0 y_{n+2}(x^2-1) + {}^nC_1 y_{n+1}(2x) + {}^nC_2 y_n.(2)]$
$+ [{}^nC_0 y_{n+1}.x + {}^nC_1 y_n.1] = m^2 y_n$

$= (x^2-1)y_{n+2} + 2nxy_{n+1} + n(n-1)y_n + xy_{n+1} + ny_n - m^2y_n$

$= (x^2-1)y_{n+2} + (2n+1)xy_{n+1} + (n^2-m^2)y_n = 0$ ($y_n = 0$)

Unit - 2

1) Rolle's Theorem

If a function f is

i) Continuous in the closed interval $[a, b]$

ii) derivable in the open interval (a, b)

iii) $f(a) = f(b)$

then there exists at least one real number $c \in (a, b)$ such that $f'(c) = 0$.

Proof. Case I $\Rightarrow$ if f is a constant function in $[a, b]$ then $f'(x) = 0 \ \forall x \in [a, b] \Rightarrow f'(c) = 0 \ \forall c \in (a, b)$
$\therefore$ the result is true in this case.

Case II if f is not a constant function throughout $[a, b]$, then as f is continuous in $[a, b]$, it is bounded and attains its l.u.b. and g.l.b. in $[a, b]$,
$\therefore$ f is not a constant function.

$\therefore$ at least one of the these bounds (l.ub. and g.l.b) must be different from the equal values $f(a)$, $f(b)$ and let this bound be attained at $x = c$ (say) where c is different from a and b i.e, $c \in (a, b)$.

Without any loss of generality, we assume that l.u.b. of f is attained at $x = c$.

$\therefore f(c+h) \leq f(c)$, where $c+h$ is any point in the nbd. of c, h may be positive or negative.

if $h > 0$, then $\frac{f(c+h) - f(c)}{h} \leq 0$

$\Rightarrow \lim_{h \to 0+} \frac{f(c+h) - f(c)}{h} \leq 0$

$\Rightarrow Rf'(c) \leq 0$

Again if $h < 0$, then $\frac{f(c+h) - f(c)}{h} \geq 0$

$\Rightarrow \lim_{h \to 0-} \frac{f(c+h) - f(c)}{h} \geq 0$

$\Rightarrow Lf'(c) \geq 0$

$\because f(x)$ is derivable in (a, b)

$\therefore f'(x)$ exists $\forall x \in (a, b) \Rightarrow f'(c)$ exists

$\Rightarrow Rf'(c) = Lf'(c) = f'(c)$

$\Rightarrow f'(c) = 0$ [$\because 0$ is the common value of $Lf'(c)$ and $Rf'(c)$]

$\Rightarrow f'(c) = 0$ for some $c \in (a, b)$

$\therefore$ the theorem is proved.

2) Lagrange's Mean Value Theorem

Statement. If a function f is
i) Continuous in $[a, b]$
ii) differentiable in (a, b),
then there exists at least one real number $c \in (a, b)$ such that

$$\frac{f(b)-f(a)}{b-a} = f'(c)$$

Proof. Consider a function

$$\phi(x) = f(x) + Ax \quad \ldots\ldots (1)$$

where A is a constant to be determined such that $\phi(a) = \phi(b)$

i.e., $f(a) + A \cdot a = f(b) + A \cdot b$

i.e., $A(a-b) = f(b) - f(a)$

i.e., $-A = \frac{f(b)-f(a)}{b-a} \quad \ldots\ldots (2)$

(i) Now $f(x)$ is continuous in $[a, b]$

Also Ax, being polynomial in x, is continuous in $[a, b]$

$\therefore$ $\phi(x)$, being the sum of two continuous functions in $[a, b]$, is continuous in $[a, b]$

(ii) $\phi(x)$, being the sum of two derivable functions $f(x)$ and Ax in (a, b), is derivable in (a, b)

(iii) Also $\phi(a) = \phi(b)$

$\therefore$ $\phi(x)$ satisfies all the conditions of Rolle's Theorem

$\therefore$ $\phi'(c) = 0$ where $a < c < b$

Now $\phi'(x) = f'(x) + A \Rightarrow \phi'(c) = f'(c) + A$

$\therefore$ $\phi'(c) = 0$ gives us $f'(c) + A = 0$

$\therefore$ $-A = f'(c) \quad \ldots\ldots (3)$

from (2) and (3), we get

$$\frac{f(b)-f(a)}{b-a} = f'(c)$$

Cor. Another form:
Put $b = a + h \; (h > 0)$

$\therefore$ $\frac{f(a+h)-f(a)}{a+h-a} = f'(c)$ where $a < c < a+h$

$\therefore$ $\frac{f(a+h)-f(a)}{h} = f'(a+\theta h), \; 0 < \theta < 1$

$[\because$ for $0 < \theta < 1$, $a < a+\theta h < a+h]$

$\therefore$ $f(a+h) - f(a) = h f'(a+\theta h)$

or $f(a+h) = f(a) + h f'(a+\theta h)$, where $0 < \theta < 1$

3) Cauchy's Mean Value Theorem

If f and g are two functions such that
(i) both are continuous in the closed interval $[a,b]$
(ii) both are derivable in the open interval (a,b)
and (iii) $g'(x) \neq 0$ for any x in (a,b)

then there exists at least one real number $c \in (a,b)$ such that

$$\frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(c)}{g'(c)}$$

Proof. First of all, we show that $g(a) \neq g(b)$

If possible, suppose $g(a) = g(b)$. Now function g is continuous in $[a,b]$, derivable in (a,b) and $g(a) = g(b)$. Therefore satisfies all the conditions of Rolle's Theorem. Therefore, there exists at least one real number $c \in (a,b)$ such that $g'(c) = 0$, which contradicts the result that $g'(x) \neq 0$ for any x in (a,b).

$\therefore$ our supposition is wrong
$\therefore g(a) \neq g(b) \Rightarrow \dfrac{f(b)-f(a)}{g(b)-g(a)}$ is meaningful.

Consider the function $\phi(x) = f(x) + Ag(x)$ ..... (1)
where A is a constant so chosen that $\phi(a) = \phi(b)$ ..... (2)
i.e. $f(a) + Ag(a) = f(b) + Ag(b)$

i.e., $f(b) - f(a) = -A\{g(b) - g(a)\}$

$$-A = \frac{f(b)-f(a)}{g(b)-g(a)} \quad \text{..... (3)}$$

Now the real valued function $\phi(x)$ is such that
(i) It is continuous in $[a,b]$ {$\because$ Algebraic sum of continuous functions}
(ii) It is derivable in (a,b) {$\because$ Algebraic sum of derivable functions}
(iii) $\phi(a) = \phi(b)$ [$\because$ of (2)]

$\therefore \phi(x)$ satisfies all the conditions of Rolle's Theorem in $[a,b]$
$\therefore$ there exists at least one real number $c \in (a,b)$ such that
$\phi'(c) = 0$ ..... (4)
Differentiating both sides of (1) w.r.t. x, we get,

$$\phi'(x) = f'(x) + Ag'(x) \Rightarrow \phi'(c) = f'(c) + Ag'(c)$$

$\Rightarrow$ Now $\phi'(c) = 0$ [$\because$ of (4)]
$\Rightarrow f'(c) + Ag'(c) = 0$

$$-A = \frac{f'(c)}{g'(c)} \quad \text{..... (5)}$$

From (3) and (5), we get,

$$-\frac{f(b)-f(a)}{g(b)-g(a)} = -\frac{f'(c)}{g'(c)}$$

$$\Rightarrow \frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(c)}{g'(c)}, \text{ where } c \in (a,b)$$

Hence the result.

II) Another form of Cauchy's Mean Value Theorem

If two functions f and g are such that
(i) both are continuous in $[a, a+h]$
(ii) both are derivable in $(a, a+h)$ and
(iii) $g'(x) \neq 0$ for any x in $(a, a+h)$,

then there exists at least one real number θ, $0<\theta<1$, such that

$$\frac{f(a+h)-f(a)}{g(a+h)-g(a)} = \frac{f'(a+\theta h)}{g'(a+\theta h)}$$

Proof. Let $b = a+h$, $c = a+\theta h$

$\therefore a < c < b \Rightarrow a < a+\theta h < a+h \Rightarrow 0 < \theta h < h \Rightarrow 0 < \theta < 1$

$$\therefore \frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(c)}{g'(c)} \Rightarrow \frac{f(a+h)-f(a)}{g(a+h)-g(a)} = \frac{f'(a+\theta h)}{g'(a+\theta h)}$$

For II Deduction of lagrange's Mean Value Theorem.

Take $g(x) = x$, $g'(x) = 1$ Exists for each x

$g(a) = a$, $g(b) = b$, $g'(c) = 1$

$$\therefore \frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(c)}{g'(c)} \Rightarrow \frac{f(b)-f(a)}{b-a} = \frac{f'(c)}{1}$$

$c \in (a, b)$

This result is the same as that of lagrange's mean value theorem.

Note 1. Cauchy's Mean Value theorem is a slightly more general form of the lagrange's Mean Value Theorem. Hence Cauchy's Mean Value theorem is also called Generalized Mean Value theorem or the second Mean Value theorem

Unit – 2

Division Algorithm

statement. For any two integers a and b, with $a>0$, there exist unique integers q and r such that

$$b = aq + r, \quad 0 \le r < |a|$$

Proof. when $b = 0$

Taking $q = 0, r = 0$, we have
$0 = a(0) + 0, \; 0 = r < |a|$
or $b = aq + r, \; 0 \le r < |a|$

Hence the result

when $b \neq 0$

Consider the infinite sequence of multiples of a
i.e $\ldots, -2a, -a, 0, a, 2a, \ldots$

Let aq be the greatest multiple of a such that

$b \ge aq$ and $b < (q+1)a$
$\therefore aq \le b < a(q+1)$ (combine)
$\Rightarrow 0 \le b - aq < a$ $\quad -aq$ every side
Put $b - aq = r$
$\therefore 0 \le r < a$
$\therefore b = aq + r, \; 0 \le r < |a| \quad \ldots (1)$

Uniqueness

If possible, let there exist another set of integers q_1 and r_1 such that

$$b = aq_1 + r_1, \; 0 \le r_1 < |a| \quad \ldots (2)$$

From (1) and (2), we get
$aq + r = aq_1 + r_1$
$\therefore r - r_1 = a(q_1 - q) \quad \ldots (3)$
$\Rightarrow$ a divides $r - r_1$

But $|r - r_1| < a \quad [\because 0 \le r < a, 0 \le r_1 < a]$

$\therefore r - r_1 = 0 \Rightarrow r_1 = r$
$\therefore$ from (3), $a(q_1 - q) = 0 \Rightarrow q_1 - q = 0$ as $a \neq 0$
$\therefore q_1 = q$

$\therefore$ for any two integers a and b, with $a>0$, there exist unique integers q and r such that
$b = aq + r, \; 0 \le r < |a|$.

Cor I. If a and b are any integers, with $a \neq 0$, then there exist unique integers q and r such that

$$b = aq + r, \; 0 \le r < |a|$$

Proof. We have proved the result for $a>0$
if $a<0$, then $|a| > 0$
$\therefore$ there exists unique integers q_2 and r such that

$b = q_2|a| + r, \; 0 \le r < |a|$
$= q_2(-a) + r, \; 0 \le r < |a|$
$= (-q_2)a + r, \; 0 \le r < |a|$
$= qa + r, \; 0 \le r < |a|$ where $q = -q_2 \in Z$

$\therefore b = aq + r, \; 0 \le r < |a|$
Hence the result.

Cor 2. If a and b are integers with $a \neq 0$, then there exists unique integers q and r such that

$$b = aq + r, \quad -\frac{|a|}{2} \leq r < \frac{|a|}{2}$$

Proof: By Division algorithm, for any integers $a \neq 0$ and b, $\exists$ unique integers q_1, r_1 such that

$$b = aq_1 + r_1, \quad 0 \leq r_1 < |a| \quad \ldots (1)$$

Now $0 \leq r_1 < |a| \Rightarrow 0 \leq r_1 < \frac{|a|}{2}$ or $\frac{|a|}{2} \leq r_1 < |a|$

if $0 \leq r_1 < \frac{|a|}{2}$, on taking $q_1 = q$, $r_1 = r$ in (1) we have

$$b = aq + r, \quad 0 \leq r < \frac{|a|}{2} \quad \ldots (2)$$

if $\frac{|a|}{2} \leq r_1 < |a|$, then

$$\frac{|a|}{2} - |a| \leq r_1 - |a| < |a| - |a|$$

$$-\frac{|a|}{2} \leq r_1 - |a| < 0$$

$$-\frac{|a|}{2} \leq r < 0 \quad \text{where } r = r_1 - |a| \text{ or } r_1 = r + |a|$$

$\therefore$ from (1), $b = aq_1 + r + |a|, \quad -\frac{|a|}{2} \leq r < 0$

$$= aq_1 + |a| + r$$

$$= a(q_1 \pm 1) + r \quad [\because |a| = \pm a]$$

$$= aq + r \text{ (say)}, \quad -\frac{|a|}{2} \leq r < 0 \quad \ldots (3)$$

Combining (2) and (3), we have

$$b = aq + r, \quad -\frac{|a|}{2} \leq r < \frac{|a|}{2}$$

As q_1, r_1 are unique so q, r are also unique. Hence the result.

Q1) Show that $2^{2n} + 1$ is divisible by 5, for +ve integer n.

Sol $2^{2n} + 1$

$(2^2)^n + (1)^n$

$(4)^n + (1)^n$

$[x^n + y^n = (x+y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 \ldots)]$

$= (4+1)(4^{n-1} + 4^{n-2} + 4^{n-3})$

$2^{2n} + 1 = 5(4^{n-1} + 4^{n-2} + 4^{n-3} \ldots)$

$\therefore 2^{2n} + 1 = 5k$

where k is an integer

$\therefore 2^{2n} + 1$ is divisible by 5

Q2) Prove that $8^n - 3^n$ is divisible by 5.

$8^n - 3^n = (8-3)(8^{n-1} + 8^{n-2} \cdot 3 + 8^{n-3} \cdot 3^2 + \ldots)$

$= 5(8^{n-1} + 3 \cdot 8^{n-2} + 9 \cdot 8^{n-3} \ldots)$

$= 5k$

$\therefore 8^n - 3^n$ is divisible by 5

Q3) Prove that 4 doesn't divide m^2+2 where m is an integer

Sol m is an integer
∴ m is either even or odd.

Case I Assume that m is even
∴ $m = 2K$
∴ m^2+2
$\Rightarrow (2K)^2+2$
$\Rightarrow 4K^2+2$
$\Rightarrow 2(2K^2+1)$
$\Rightarrow 2 \times$ (odd integer)

Case II Assume m is odd
$m = 2K+1$
$m^2+2 \Rightarrow (2K+1)^2+2$
$\Rightarrow 4K^2+1+4K+2$
$\Rightarrow 2(2K^2+2K+1)+1$
$\Rightarrow 2l+1$
where $l = 2K^2+2K+1$
∴ it is an odd no.
∴ it is not divisible by 4.

Q4) Prove that Sum and Product of two even integer is an even integer

Sol let a, b are two even integers.
$a = 2K$
$b = 2K_2$

$(a+b) = 2K+2K_2$
$= 2(K+K_2)$
$= 2l$
where $l = K_1+K_2$ and
∴ $(a+b)$ is an even integer

$a \cdot b = 2K_1 \cdot 2K_2$
$= 4K_1K_2$
where h. $h_1 h_2$ and
∴ (a, b) is an even integer.

Q5) The Sum of two odd integer is always an even integer

Sol let a, b be two odd integer
$a = 2K_1+1$, $b = 2K_2+1$ where K_1, K_2 are integer.

∴ $a+b = 2K_1+1+2K_2+1$
$= 2(K_1+1+K_2)$
$= 2(K)$
where $K = K_1+K_2+1$ is an integer

where ∴ $a+b$ is an even integer

Use of Principle of Mathematical induction.

Ques Prove that $n(n+1)(2n+1)$ is divisible by 6

Sol $n(n+1)(2n+1) = n(n+1)[(n+2)+(n-1)]$
$= n(n+1)(n+2)+(n-1)(n)(n+1)$

Now
$n(n+1)(n+2)$ being the product of three consecutive integer, is divisible by 3 factorial i.e 6
$\therefore (n-1)(n)(n+1)$ is also divided by 6
$\therefore n(n+1)(2n+1)$ is divisible by 6

Ques Prove that the Product $n(n^2-1)$ is a multiple of 6

Sol $n(n^2-1) = n(n-1)(n+1)$
$[\because a^2-b^2 = (a-b)(a+b)]$
$= (n-1)(n)(n+1)$

Now $(n-1)(n)(n+1)$ being the product of 3 Consecutive integers is divisible 3 factorial $=6$
$\therefore n(n^2-1)$ is a multiple of 6

Ques If n is even, prove that $n(n+1)(n+2)$ is divisible by 24

Sol since n is even
$\therefore n = 2K$, where K is an integer
$n(n+1)(n+2) = (2K)(2K+1)(2K+2)$
$= 4K(K+1)(2K+1)$
$= 4K(K+1)(2K+1) + 6K(K+1) - 6K(K+1)$
$= 4[K(K+1)(K+2) + (K-1)(K)(K+1)]$

Now each of $K(K+1)(K+2)$ & $(K-1)(K)(K+1)$ is the product of three Consecutive integers & Hence each of them is divisible by 3 i.e. 6

Ques Prove that $9^n - 8^n - 1$ is divisible by 8

Sol let $P(n) = 9^n - 8^n - 1$
$\therefore P(1) = 9 - 8 - 1 = 0$ which is divisible by 8
$\therefore$ result is true for $n=1$
Assume that result is true for $n=K$
$\therefore P(K) = 9^K - 8^K - 1$
let $9^K - 8^K - 1 = 8\ell$
$\therefore 9^K = 8\ell + 8^K + 1$

Now $P(K+1) = 9^{K+1} - 8^{K+1} - 1$
$= 9 \cdot 9^K - 8^{K+1} - 1$
$= 9(8\ell + 8^K + 1) - 8^{K+1} - 1$
$= 72\ell + 9 \cdot 8^K + 9 - 8 \cdot 8^K - 1$
$= 72\ell + 8^K + 8$
$= 8(9\ell + 8^{(K-1)} + 1)$ which is divisible by 8

$\therefore$ result is true for $n = K+1$
$\therefore$ by mathematical Induction, the result is true for all n.

Ques Show that $4^{2n+1} + 3^{n+2}$ is a multiple of 13

Sol let $P(n) = 4^{2n+1} + 3^{n+2}$
$\therefore P(1) = 4^3 + 3^3 = 64 + 27 = 91$
which is multiple of 13
$\therefore$ result is true for $n=1$
Assume that result is true for $n=K$

$\therefore P(K) = 4^{2K+1} + 3^{K+2} = 13\ell$
$4^{2K+1} = 13\ell - 3^{K+2}$

Now,
$P(K+1) = 4^{2(K+1)+1} + 3^{(K+1)+2}$
$= 4^2 \cdot 4^{2K+1} + 3 \cdot 3^{K+2}$
$= 16(13\ell - 3^{K+2}) + 3 \cdot 3^{K+2}$

$= 13 \times 16\ell - 13 \cdot 3^{k+2}$

$= 13(16\ell - 3^{k+2})$, which is a multiple of 13

∴ result is true for $n = k+1$

∴ if is also true for $n = k+1$

But the result is true for $n = 1$

∴ by mathematical induction, result is true for all n.

Ques Use the principle of mathematical induction to prove that

(i) $2^{3n} - 1$ is divisible by 7

Sol $P(n) = 2^{3n} - 1$

$P(1) = 2^3 - 1 = 8 - 1 = 7$

which is divisible by 7

∴ Result is true for $n = 1$

Assume that result is true for $n = k$

∴ $P(k) = 2^{3k} - 1$ is divisible by 7

Let $2^{3k} - 1 = 7\ell$ where ℓ is integer

∴ $2^{3k} = 7\ell + 1$

Now, $P(k+1) = 2^{3(k+1)} - 1$

$= 2^{3k} \cdot 2^3 - 1$

$= (7\ell + 1) \cdot 8 - 1$

$= 56 + 7$

$= 7(8\ell + 1)$, which is divisible by 7

∴ result is true for $n = k+1$

∴ if the result is true for $n = k$, then it is also true for $n = k+1$, But the result true for $n = 1$

∴ By mathematical induction, the result is true for all n

Ques (ii) $10^{2n-1} + 1$ is divisible by 11

Sol Let $P(n) = 10^{2n-1} + 1$

Let $n = 1$

$P(1) = 10^{2-1} + 1 = 10 + 1 = 11$

which is divisible by 11

∴ Result is true for $n = 1$

Assume that result is true for $n = k$

$P(k) = 10^{2k-1} + 1 = 11\ell$ (where ℓ is inserted)

∴ $10^{2k-1} = 11\ell - 1$ ——— (1)

∴ $P(k+1) = 10^{2(k+1)-1} + 1$

$= 10^{2k+2-1} + 1 = 10^{2k+1} + 1$

$= 10(11\ell - 1) \cdot 10 + 1$

$= 1100\ell - 100 + 1$

$= 1100\ell - 99$

$= 11(100\ell - 9)$ which is divisible by 11

∴ Result is true for $n = k+1$

By mathematical induction the result is true for all n.

(iii) $3^{2n} - 1$ is divisible by 8

Sol Let $P(n) = 3^{2n} - 1$

$n = 1$; $P(1) = 3^2 - 1 = 9 - 1 = 8$

which is divisible by 8

∴ Result is true for $n = 1$

Assume that Result is true for $n = k$

$P(k) = 3^{2k} - 1$ is divisible by 8

Let $3^{2k} - 1 = 8\ell$, where ℓ is a integer

$3^{2k} = 8\ell + 1$ ——— (1)

$P(k+1) = 3^{2(k+1)} - 1 = 3^{2k+2} - 1$

$= 3^{2k} \cdot (3)^2 - 1$

$(2\ell+1)q - 1 = 72\ell + 8$

$8(q\ell+1)$ which is divisible by 8

∴ Result is true for $n = k+1$

By mathematical induction Result is true for all n.

Q) Use Principle of Mathematical Induction Prove that $x + 4x + 7x + 1 \ldots + (3x-2)x = \frac{1}{2} x(3x-1)x$

Sol $x + 4x + 7x + \ldots + (3x-2)x = \frac{1}{2} x(3x-1)x$ —(1)

for $x = 1$

L.H.S $= x$

R.H.S $= \frac{1}{2} \times 1 \times (3-1)x = \frac{1}{2} \times 1 \times 2(x) = x$

∴ L.H.S = R.H.S

Result is true for $n = 1$

Assume that Result is true for $n = k$

~~By mathematical Induction Result is true for all~~

$x + 4x + 7x \ldots + (3k-2).x = \frac{1}{2} k(3k-1)x$

for $n = k+1$

$x + 4x + 7x + \ldots + (3k-2).x + (3k+1)$

$= \frac{1}{2}(k+1)(3k+3-1)x$

$\frac{1}{2} k(3k-1)x + (3k+1) = \frac{1}{2}(k+1)(3k+2)x$

L.H.S $= \frac{1}{2} k(3k-1)x + (3k+1)$

$= \frac{1}{2}(3k^2 - k)x + (3k+1)x$

$= \left[\frac{1}{2}(3k^2 - k) + (3k+1)\right] x$

$= \left(\frac{3k^2 - k + 6k + 2}{2}\right) x = \left(\frac{3k^2 + 5k + 2}{2}\right) x$

$= \frac{1}{2}(k+1)(3k+2)x$ = R.H.S

Q) By mathematical Induction. Prove that $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$

Sol $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ —(1)

for $n = 1$

L.H.S = 1

R.H.S $= \frac{1(2)(3)}{6} = 1$

∴ L.H.S = R.H.S

∴ Result is true for $n = 1$

Assume that Result is true for $n = k$

$1^2 + 2^2 + 3^2 + \ldots + k^2 = \frac{(k)(k+1)(2k+1)}{6}$ —(2)

Adding $(k+1)^2$ to both sides of eq (2)

$1^2 + 2^2 + 3^2 + \ldots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1) + (k+1)^2}{6}$

$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6}$

$= (k+1)\left[\frac{k(2k+1) + 6(k+1)}{6}\right]$

$= \frac{(k+1)}{6}\left[k(2k+1) + 6(k+1)\right]$

$= \frac{k+1}{6}\left[2k^2 + k + 6k + 6\right]$

$= \frac{k+1}{6}\left[2k^2 + 7k + 6\right]$

$$= \frac{k+1}{6}\left[k(2k+3) + 2(2k+3)\right]$$

$$= \frac{k+1}{6}\left[(k+2)(2k+3)\right]$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}$$

Ch-5

Greatest Common Divisor (GCD) And Equation Algorithm

\# Common divisor :- If c/a and c/b then c is called common divisor of a & b

\# Greatest common divisor: let a & b with 1 integer such that atleast one of them is non-zero then positive integer a is the greatest common divisor to the a & b

i) If d/a, d/b then d is common divisor of a & b

ii) if c/a, c/b then c is common divisor of a and b but $c \leq d$

Note: If $d = (a, b)$ where a & b not both zero then prove that there exist x & y such that $a = ax + by$

other definition of GCD

\# Relatively prime Number: Two integer a and b are said to relatively prime or co-prime or a is prime to b. If $(a, b) = 1$ i.e GCD of a & b is 1.

If a/bc and $(a, b) = 1$

then a/c

Proof

Given $(a,b)=1$ there exist x, y belongs to $\mathbb{Z}$

$\exists\ x, y \in \mathbb{Z}$

such that

$ax+by=1$

Multiply both side by c

$axc+byc=c$

we have given that a/bc also a/ac

$\therefore\ a/acx+bcy$ i.e. a/c

Hence, Proved.

$(a,n)=1$ $\quad a/b$ $\quad b/a$

integer x, y

$ax+ny=1$

with integer m, n.

$a/b \Rightarrow b=am$

$c/b \Rightarrow b=cn$

$bd = ac(mm+ny)$

$\Rightarrow dc/bd \Rightarrow bd=ac(mm+ny)$

$(a,4)=2 \Rightarrow 2/a \quad 2/4$

$\downarrow \quad \downarrow$

$a=2m \quad u=2h$

Q) If $(a, mn)=1$ iff $(am=1, (an)=1)$

Sol $(a,m)=1$

then there exits and integer x, y, such that

$ax+my=1$ — (1)

$(a,n)=1$

Then there exist integer z, t such that

$az+nt=1$

$az+nt(1)=1$

from (1)

$az+nt(ax+my)=1$

$az+nxta+nmty=1$

$a(z+ntx)+nm(ty)=1$

$as+mn.s=1$

where $s=(z+ntx)$, $s=ty$

$(a,mn)=1$

$(a, mn)=1$

Q) If $(a,c)=d$, a/b, c/b then show that ac/bd

Sol since a/b and c/b

then there exists integer m, n such that

a/b, c/b

$b=am$, $b=cn$

$(a,c)=d$

then there exist integer (x, y) such that

$ax+cy=d$

multiplie both side by b.

$abx+bcy=bd$

$cnax+amcy=bd$

$ac(nx+my)=bd$

$\Rightarrow$ $b \mid ac$ or $1 \mid b$

$\Rightarrow$ $bd = ac(nm+my)$ $\quad b = a \times$ Integer

$\Rightarrow$ $ac \mid bd$

Q) If $(a,4)=2$ and $(b,4)=2$ then Prove that $(a+b,4)=4$

Sol $(a,4)=2$

$\therefore 2 \mid a$ and $2 \mid 4$

$\therefore a = 2p$

$(b,4)=2$

$\therefore 2 \mid b$, $2 \mid 4$

$b = 2q$

$(a+b) = 2p+2q$

$(a+b) = 2(p+q)$

As both p, q are add so that $(p+q)$ is even

$\therefore (p+q) = 2k$

$(a+b) = 2 \times 2k$

$(a+b) = 4k$

$\therefore (a+b, 4) = 4$

Hence Proved

Q) Prove that integer n $30 \mid m^5 - m$

Sol let $m^5 - m = m(m^4-1)$

$= m((m^2)^2-1)$

$= m((m^2-1)(m^2+1))$

$= m((m-1)(m+1)(m^2+1))$

$= (m-1)m(m+1)(m^2+1)$

$\Rightarrow (m^3-m)(m^2+1)$

As 6 divides m^5-m $\therefore m^5-m = (m^2-1)m(m^2+1)$

3 Consecutive integer also divides by $3! = 6$

$6 \mid (m^3-m)(m^2+1)$

$\therefore 6 \mid m^5-m$ $\quad -(1)$

Also $m^5-m = (m^3-m)(m^2+1)$

$= (m^3-m)(m^2+5-4)$

$= (m^3-m)((m^2-4)+5)$

$= (m^2-4)(m^3-m) + 5(m^3-m)$

$= m(m^2-1)(m^2-4) + 5(m^3-m)$

$= m(m-1)(m+1)(m-2)(m+2) + 5(m^3-m)$

$= (m-1)(m-2)m(m+1)(m+2) + 5(m^3-m)$

$(m-2)(m-2)m(m+1)(m+2)$ $\quad -(2)$

$\therefore$ there are 5 Consecutive integers. So that

$5 \mid (m-2)(m-1)m(m+1)(m+2)$

$\therefore 5 \mid m^5-m$ $\quad -(3)$

$\therefore$ ~~obe~~ (2)

$\therefore$ because of (3) and (1) we get

$30 \mid m^5-m$

Q) If $(a,b)=1$ then Prove that $(a+b, a-b) = 1$ or 2

Sol let $(a+b), (a-b) = d$

$d \mid a+b$ and $d \mid a-b$

$d \mid (a+b)+(a-b)$ and $d \mid (a+b)-(a-b)$

$d \mid 2a$ and $d \mid 2b$

$d \mid (2a, 2b)$

$d \mid 2(a,b) \Rightarrow d \mid 2(1) \Rightarrow d \mid 2$ [$\because$ given $(a,b)=1$]

$d = 1$ or $2 \Rightarrow (a+b)(a-b) = 2$ or 1

Q) If $(a,b)=d$ then a/d , $b/d = 1$

Sol

$(a,b)=d$

$\therefore d \mid a$ and $d \mid b$ $\therefore$ there exist a and b integer

$a = a/b$, $b = b/d$

$\therefore$ There exist integer x and y such that

$ax + by = d$

$a_1 dx + b_1 dy = d$

$a_1 x + b_1 y = 1$

$(a_1, b_1) = 1$

$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ [$\because$ of 2]

Euclidean Algorithm

For any two positive integers a and b, on applying the division algorithm repeatedly to obtain a set of remainders $r_1, r_2, \ldots r_n$ defined successively by the following relations.

$$\left.\begin{aligned} b &= aq_1 + r_1, & a \le r_1 < a \\ a &= r_1 q_2 + r_2 & 0 \le r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, & 0 \le r_3 < r_2 \\ &\cdots\cdots & \\ r_{n-2} &= r_{n-1} q_n + r_n, & 0 \le r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} & \end{aligned}\right\} - (1)$$

Then show r_n, the last non zero remainder in the above process of g.c.d of a and b

Proof:- we have for any integer (x, y)

$(a,b) = (a, b + ax) = (a+by, b)$

using equation (I)

$$\begin{aligned} (a,b) &= (a, b - aq_1) \\ &= (a, r_1) \\ &= (a - r_1 q_2, r_1) \\ &= (r_2, r_1) \\ &= (r_1, r_1 - r_2 q_3) \\ &= (r_2, r_3) \end{aligned}$$

Continuing like this, we get

$$\begin{aligned} (a,b) &= (r_2, r_1) \\ &= (r_1, r_2) \\ &= (r_2, r_3) \cdots \\ &= (r_{n-1}, r_n) \\ &= (r_n, 0) = r_n \end{aligned}$$

$\therefore$ r_n last non-zero remainder is g.c.d of (a,b)

Cor-1:- Express G.C.D of a and b as a linear combination of a and b.

Proof:- From Eudidean Algorithm, we have

$$\begin{aligned} b &= aq_1 + r_1 & 0 \le r_1 < a \\ a &= r_1 q_2 + r_2 & 0 \le r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 & 0 \le r_3 < r_2 \\ &\cdots\cdots & \\ r_{n-4} &= r_{n-3} q_{n-3} + r_{n-2} & 0 \le r_{n-2} < r_{n-3} \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} & 0 \le r_{n-1} < r_{n-2} \end{aligned}$$

$r_{n-2} = r_{n-1} q_n + r_n \quad 0 \le r_n < r_{n-1}$

$r_{n-1} = r_n q_{n+1}$

Rewrite above equation as

$r_n = r_{n-2} - r_{n-1} q_n$

$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}$

$r_{n-2} = r_{n-4} - r_{n-3} q_{n-2}$

- - - - -

$r_3 = r_1 - r_2 q_3$

$r_2 = a - r_1 q_2$

$r_1 = b - a q_1$

$(a,b) = r_n = r_{n-2} - r_{n-1} q_n$

$= r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n$

$= (1 + q_{n-1} q_n) r_{n-2} + (-q_n) r_{n-3}$ — ①

$= (1 + q_{n-1} q_n)(r_{n-n} - r_{n-3} q_{n-2}) + (-q_n) r_{n-3}$

$= (1 + q_{n-1} q_n) r_{n-n} + (-q_n - q_{n-2} - q_{n-2} q_{n-1} q_n) r_{n-3}$ — ②

∴ eq ① gives r_n as linear combination r_{n-2} and r_{n-3}

∴ eq ② given r_n as linear combination of r_{n-3} and r_{n-4}

07/03/22

Q) find the GCD of 726 and 275 and express it in the form $726x + 275y$.

Sol on dividing 726 by 275

$726 = 275 \times 2 + 176$ — ①

$275 = 176 \times 1 + 99$ — ②

$176 = 99 \times 1 + 77$ — ③

$99 = 77 \times 1 + 22$ — ④

$77 = 22 \times 3 + 11$ — ⑤

$22 = 11 \times 2 + 0$

GCD of $(726, 275) = 11 \Rightarrow d = 11$

from eq 5

$11 = 77 - 3 \times 22$

$= 77 - 3(99 - 77 \times 1)$

from ③

$= 77 - 3 \times 99 + 3 \times 77$

$= 4 \times 77 - 3 \times 99$

$= 4(176 - 99 \times 1) - 3 \times 99$

$= 4 \times 176 - 4 \times 99 - 3 \times 99$

$= 4 \times 176 - 7 \times 99$

$= 4 \times 176 - 7 \times (275 - 176 \times 1)$ from ②

$= 4 \times 176 - 7 \times 275 + 7 \times 176$

$= 11 \times 176 - 7 \times 275$

$= 11 \times (726 - 275 \times 2) - 7 \times 275$ from eq ①

$= 11 \times 726 - 22 \times 275 - 7 \times 275$

$= 11 \times 726 - 29 \times 275$

$d = 726x + 275y$ where $x = 11, y = -29$

275 | 726 | 2
550
176 | 275 | 1
176
99 | 176 | 1
99
77 | 99 | 1
77
22 | 77 | 3
66
11
11 | 22 | 2
22
0

Q) find the GCD of 275 and 200, and express it in the form $275x + 200y$

Sol on dividing 275 by 200

$275 = 200 \times 1 + 75$ — (1)

$200 = 75 \times 2 + 50$ — (2)

$75 = 50 \times 1 + 25$ — (3)

$50 = 25 \times 2 + 0$

GCD(275, 200) = 25

$d = 25$

from eqn 3:

$d = 25 = 75 - 50 \times 1$

$= 75 - (200 - 75 \times 2) \times 1$ from (2)

$= (275 - 200) - 200 + 2 \times 75$

$= 275 + 2 \times (200) + 2x$

$= 75 - 200 + 2 \times 75$

$= -200 + 3 \times 75$

$= -200 + 3 \times (275 - 200)$

$= 3 \times 275 - 3 \times 200 - 200$

$= 3 \times 275 - 4 \times 200$

$275x + 200y = d$

$x = 3 \quad y = -4$

Q) find the GCD of 7200 by 3132 and exp it in the form $7200x + 3132y$

Sol on dividing 7200 by 3132, we have

$7200 = 3132 \times 2 + 936$ — (1)

$3132 = 936 \times 3 + 324$ — (2)

$936 = 324 \times 2 + 288$ — (3)

$324 = 288 \times 1 + 36$ — (4)

$288 = 36 \times 8 + 0$

GCD(7200, 3132) = 36

$d = 36$

from eqn 5

$d = 36 = 324 - 288 \times 1$

$= 324 - (936 - 324 \times 2)$ from (3)

$= 324 - 936 + 324 \times 2$

$= 3 \times 324 - 936$

$= 3 \times (3132 - 936 \times 3) - 936$ from (2)

$= 3 \times 3132 - 9 \times 936 - 936$

$= 3 \times 3132 - 10 \times 936$

$= 3 \times 3132 - 10 \times (7200 - 3132 \times 2)$ from (1)

$= 3 \times 3132 - 10 \times 7200 + 20 \times 3132$

$= 23 \times 3132 - 10 \times 7200$

$d = 7200x + 3132y$

$\therefore x = -10, y = 32$

Ques) find the GCD of 24 and 138 and exp it in the linear combination

Sol Dividing 138 by 24

$138 = 24 \times 5 + 18$

$24 = 18 \times 1 + 6$

$18 = 6 \times 3 + 0$

GCD (24, 138) = 6

$6 = 24 - 18$

$6 = 24 - (138 - 24 \times 5)$

$= 24 - 138 + 24 \times 5 = 6 \times 24 - 138$

$6 = 24 - (138 - 24 \times 5)$

$= 24 - 136 + 24 \times 5$

$= 6 \times 24 - 136$

$d = 136x + 24y$

$x = -1 \quad y = 6$

NOTE

$(a, b)[a, b] = ab$

Q) evaluate L.C.M [306, 657]

Sol firstly find G.C.d [657, 306]

by Euclidean algorithm

$657 = 306 \times 2 + 45$

$306 = 45 \times 6 + 36$

$45 = 36 \times 1 + 9$

$36 = 9 \times 4 + 0$

$\therefore$ G.C.D [657, 306) $= 9$

Now using $(a, b)[a, b] = ab$

we have $[a, b] = \frac{ab}{(a, b)}$

$[306, 657] = \frac{306 \times 657}{9} = 34 \times 657$

$= 22338$

Q) find LCM [1819, 3587]

Sol find GCD of [1819, 3587]

by Euclidean algorithm

$3587 = 1819(1) + 1768$

$1819 = 1768(1) + 51$

$1768 = 51 \times 34 + 17$

$51 = 17(3) + 0$

$\therefore$ GCD (1819, 3587) $= 17$

Now using $(a, b)[a, b] = ab$

we have $[a, b] = \frac{ab}{(a, b)}$

$[1819, 3587] = \frac{1819 \times 3587}{17}$

$= 107 \times 3587$

$= 383809$

Q) find LCM [714, 2030, 2205)

Sol we have

$[714, 2030, 2205] = [[714, 2030], 2205]$

finding first G.C.D (714, 2030)

$2030 = 714 \times 2 + 602$

$714 = 602 \times 1 + 112$

$602 = 112 \times 5 + 42$

$112 = 42 \times 2 + 28$

$42 = 28 \times 1 + 14$

$28 = 14 \times 2 + 0$

$d = 14$

$[714, 2030] = \frac{714 \times 2030}{14}$

$= 51 \times 2030 \Rightarrow 103530$

$\therefore [714, 2030, 2205] = [103530, 2205]$

Now finding G.C.D of (103530, 2205) by euclidean algo

$103530 = 2205 \times 46 + 2100$

$2205 = 2100 \times 1 + 105$

$2100 = 105 \times 20 + 0$

G.C.D $= 105$

$(103530, 2205) = \frac{103530 \times 2205}{105}$

$= 103530 \times 21$

$= 2174130$

Ch-6 CONGRUENCES

Congruence :- If a and b are integers such that $m \mid b-a$, then we call that "a is congruent to b modulo m"

$a \equiv b \pmod m$ [$m \nmid a-b$ not congruent]

Properties

(i) Reflexive

To show. $a \equiv a \pmod m \ \forall a \in \mathbb{Z}$

$a-a = 0$ and $m \mid 0$

$m \mid a-a$

$a \equiv a \pmod m$

(ii) Symmetric

$-a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$

$a \equiv b \pmod m \Rightarrow m \mid a-b$

$\Rightarrow (a-b) = mp$ for $p \in \mathbb{Z}$

$\Rightarrow b-a = -mp = m(-p)$

$\Rightarrow b-a = mq$ where $q = -p \in \mathbb{Z}$

$\Rightarrow b \equiv a \pmod m$

(iii) Transitive $\dfrac{a \equiv b \pmod m \text{ and } b \equiv c \pmod m}{a \equiv c \pmod m}$

$a \equiv b \pmod m$ and $b \equiv c \pmod m$

$m \mid a-b$ and $m \mid b-c$

$m \mid (a-b)+(b-c) \Rightarrow m \mid a-c$

$a \equiv c \pmod m$

Q) Write a single congruence which is equivalent to the pair of congruences

$x \equiv 1 \pmod 4$ and $x \equiv 2 \pmod 3$

Sol Given $x \equiv 1 \pmod 4$ and $x \equiv 2 \pmod 3$

$\therefore 4 \mid x-1$ and $3 \mid x-2$

$4 \mid (x-5)+4$, $3 \mid (x-5)+3$

$\Rightarrow 3 \mid x-5$

$12 \mid x-5$ as $(4,3) = 1$

$x \equiv 5 \pmod{12}$

Q) Show that $2^{20}-1$ is divisible by 41

$5^{20} = (25)^4 = (32)^4$ | $41 \mid 32+9$

$\equiv (-9 \pmod{41})^4$

$\equiv (-9)^4 \pmod{41}$

$\equiv (-9)^2 (-9)^2 \pmod{41}$

$\equiv (81)(81) \pmod{41}$

$\equiv (-1)(-1) \pmod{41}$ [$\because 81 \equiv -1 \pmod{41}$]

$2^{20} \equiv 1 \pmod{41}$

$41 \mid 2^{20}-1$

$\therefore 2^{20}-1$ is divisible by 41

Q) Show that $5^{48}-1$ is divisible by 24

$5^{48} = (5^2)^{24} = (25)^{24}$ | $25 \mid 24+1$

$\equiv (1 \pmod{24})^{24}$

$\equiv 1 \pmod 4$

$(25)^{24} \equiv 1 \pmod 4$

$24 \mid 5^{48}-1$

$\therefore 5^{48}-1$ is divisible by 24

Q) Find the remainder when 2^{50} is divided by 7

$(2)^{50} = 2^{48} \times 2^2$

$= (2^3)^{16} \times 4 = 8^{16} \times 4$

$8 \equiv 1 \pmod 7$

$8^{16} = (1)^{16} \pmod 7$

$8^{16} \times 4 = 1 \times 4 \pmod 7$

$2^{50} \equiv 4 \pmod 7$

$7 \mid 2^{50}-4$

$\therefore 2^{50}$ when divided by 4 leaves the rem 4

Q) find the rem when $(16)^{53}$ is divided by 7

$(16)^{53} \equiv 2 \pmod 7$

$\Rightarrow (16)^{53} \equiv 2^{53} \pmod 7$

$\equiv 2^{51} \times 2^2 \pmod 7$

$\equiv (2^3)^{17} (4) \pmod 7$

$\equiv 8^{17} (4) \pmod 7$

$(16)^{53} \equiv 4 \pmod 7$

$[\because 2 \equiv 1 \pmod 7 \Rightarrow 8^{17} \equiv 1^{17} \pmod 7]$

$\Rightarrow 8^{17} \times 4 \equiv 1 \times 4 \pmod 7$

16^{53} when divided by 7 leaves the remender 4

Q) show that $53^{103} + 103^{53}$ is divisible by 39.

we have $53 \equiv 14 \pmod{39}$ and $103 \equiv (-14) \pmod{39}$

$\therefore 53^{103} + (103)^{53} \equiv 14^{103} \pmod{39} + (-14)^{53} \pmod{39}$

$\equiv 14^{53} (14^{50} - 1) \pmod{39}$

$\equiv 14^{53} ((14^2)^{25} - 1) \pmod{39}$

$\equiv 14^{53} (196)^{25} - 1) \pmod{39}$

$\equiv 14^{53} (1 - 1) \pmod{39} \equiv 0 \pmod{39}$

$[\because 196 \equiv 1 \pmod{39} \Rightarrow (196)^{25} \equiv 1 \pmod{39}]$

$\Rightarrow 53^{103} + 103^{53}$ is divisible by 39.

Q) find rem when 4444^{4444} is divisible by 9.

$4444 = (9 \times 493 + 7)$

$\equiv 7 \pmod 9 \equiv (-2) \pmod 9$

$4444^{4444} \equiv (-2)^{4444} \pmod 9$

$\equiv (-2)^{3 \times 1481 + 1} \pmod 9$

$\equiv (-2)^{3 \times 1481} (-2) \pmod 9$

$\equiv (-8)^{1481} (-2) \pmod 9$

$\equiv (1)^{1481} (-2) \pmod 9$ $[\because -8 \equiv 1 \pmod 9]$

$\equiv -2 \pmod 9$

$\equiv 7 \pmod 9$

$\therefore 4444^{4444}$ when divided by 9 leaves the rem 7

Q) show that 2345718948 is divisible by 4.

$= 2 \times 10^9 + 3 \times 10^8 + 4 \times 10^7 + 5 \times 10^6 + 7 \times 10^5 + 1 \times 10^4 + 8 \times 10^3 + 9 \times 10^2 + 4 \times 10^1 + 8$

$\therefore a_0 + 2a_1$ ← last last

↑

last term

$= 8 + 2 \times 4 = 8 + 8 = 16$

which is divisible by 4

$4 / a_0 + 2a_1$ So that $4 / 2345718948$

Q) Show that 5876432145248 is divisible by 8

$= 5 \times 10^{12} + 8 \times 10^{11} + 7 \times 10^{10} + 6 \times 10^9 + 4 \times 10^8 + 3 \times 10^7 + 2 \times 10^6 + 1 \times 10^5 + 4 \times 10^4 + 5 \times 10^3 + 2 \times 10^2 + 4 \times 10 + 8$

$\Rightarrow \therefore a_0 + 2a_1 + 4a_2$

$= 8 + 2 \times 4 + 4 \times 2$

$= 8 + 8 + 8 = 24$

$8 / a_0 + 2a_1 + 4a_2 \Rightarrow 8 / 5876432145248$

Ch-7

Linear Congruences

Linear Congruence :-

A Congruence of the form $ax \equiv b \pmod m$ where $a \not\equiv 0 \pmod m$ and $a, b, m > 0$ are fixed integers is called linear Congruence.

Congruent and Incongruent Sol :-

The int which satisfy a given linear Congruence mod m and belong to the same residue class are called Congruent Sol. otherwise if they belong to diff. residue classes) called incongruent sol.

for eg :

$$4x \equiv 7 \pmod 5 \quad -(1)$$

$$5 \mid 4x - 7$$

Here out of 0, 1, 2, 3, 4 only $x = 3$ satisfies (1)

$\therefore x = 3$ is the only incongruent Sol of eqn (1)

where as $\ldots -7, -2, 3, 8, 13 \ldots$ all are Congruent solutions of (1)

Note : $\boxed{x = x_1 + \frac{m}{2} \times 8}$

Q.) How many sol this ≡ ;

$15x \equiv 25 \pmod{35}$

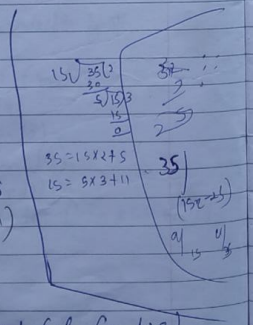
$a = 15, \; b = 25, \; m = 35$

$\therefore d = (15, 35) = (a, m)$

$d = 5$

$d \mid b \Rightarrow 5 \mid 25$

$\therefore$ there are 5 incongruent Sol. $(\mod 35)$



(ii) $15x \equiv 24 \pmod{35}$

$a = 15, \; b = 24, \; m = 35$

$(a, m) = d = (15, 24) = 5$

$d \mid b \Rightarrow 5 \mid 24$; 5×24

$\therefore$ there is no incongruent Sol of $(\mod 35)$

(iii) Solve $18x \equiv 30 \pmod{42} \quad -(1)$

$a = 18, \; b = 30, \; m = 42$

$d = (a, m) \Rightarrow (18, 42)$

$d = 6$

$6 \mid 30$

$\therefore$ Congruence (1) has six incongruent Sol's

Now from (1) $\frac{18x}{6} \equiv \frac{30}{6} \left(\mod \frac{42}{6}\right)$

$\Rightarrow 3x \equiv 5 \pmod 7 \quad -(2)$

Clearly $x = 4$ is a Sol. of (2) and hence of (1)

$\therefore$ six Sol. are given by

$x \equiv 4 + \frac{42}{6} p \pmod{42}$

$\equiv 4 + 7p \pmod{42}$

$x = 4, 11, 18, 25, 32, 39 \pmod{42}$

(iv) Solve $2x + 7y \equiv 5 \pmod{12}$

Sol

$2x + 7y \equiv 5 \pmod{12} \quad -(1)$

$\gcd(2, 7, 12) = 1 \mid 5$

Now eqn (1)

$2x \equiv 5 - 7y \pmod{12} \quad -(2)$

As $\gcd(2, 12) = 2$

$2 \mid 5 - 7y$

$7y \equiv 5 \pmod{12}$

Here $(7,12) = 1$ & $1 \mid 5$

∴ there is 1 incongruent soln

$y \equiv 1 \pmod{12}$

$y = 1 + 12k,\ k \in \mathbb{Z}$

∴ from eqn (2)

$2x \equiv 5 - 7(1 + 12k) \pmod{12}$

$2x \equiv -2 - 14k \pmod{12}$

$x \equiv -1 - 7k \pmod{6}$

$x = -1 - 7k + 6\ell$

∴ required Soln are

$y = 1 + 12k,\ x \equiv -1 - 7k + 6\ell \pmod{12}$

where $0 \le k \le 5,\ \ell = 0, 1,\ k \in \mathbb{Z}$

$y=1$	$y=3$	$y=5$	$y=7$	$y=9$	$y=11$
$x=11$	$x=4$	$x=9$	$x=2$	$x=7$	$x=0$

$(\ell = 0)$

$y=1$	$y=3$	$y=5$	$y=7$	$y=9$	$y=11$
$x=5$	$x=10$	$x=3$	$x=8$	$x=1$	$x=6$

Ques

$91x \equiv 1053 \pmod{221}$

$91x \equiv 1053 \pmod{221}$

$(91, 221) = 13$ & $13 \mid 1053$

∴ Congruence has 13 incongruent sol

$91x + 221y = 1053$

$221 = 2 \times 91 + 39$

$91 = 2 \times 39 + 13$

$39 = 3 \times 13$

∴ $13 = 91 - 2 \times 39 = 91 - 2(221 - 2 \times 91)$

$\Rightarrow 5 \times 91 - 2 \times 221$

$\Rightarrow 91 \times 5 + 221 \times (-2) = 13$

Multiply by 81

$91 \times 405 + 221 \times (-162) = 1053$

$x = 405$ & $y = -162$

$x = 405 + \frac{221}{13} \times p\ ;\ 0 \le p \le 12$

$\equiv 405 \times 17p$

$x \equiv 405 + 17p \pmod{221}$

$x \equiv -37 + 17p \pmod{221}$ ∵ $405 \equiv -37 \pmod{221}$

$x \equiv -37, -20, -3 \pmod{221}$

$x \equiv -37 + 17p \pmod{221}$ $3 \le p \le 12$

$x \equiv 184, 201, 218 \pmod{221}$

$x \equiv -37 + 17p \pmod{221}$ $3 \le p \le 12$

which is given in Sol

Q5 Sol

$9x \equiv 21 \pmod{30}$

$9x \equiv 21 \pmod{30}$

Here $(9, 30) = 3$

$9x + 3y = 21$ — (2)

g.c.d $(9, 30) = 3$ as linear combination

$3 = 9(-3) + 3(1)$

Multiply by 7

$21 = 9(-21) + 30(7)$

$x = -21,\ y = 7$

$x = -21 + \frac{30}{3} \times p$

$= -21 + 10p$

$p = 0, 1, 2$

$x \equiv -21 \pmod{30}$, $\equiv -11 \pmod{30}$, $x \equiv -1 \pmod{30}$

$\equiv -21 + 30 \pmod{30} \equiv -11 + 30 \pmod{30}$, $\equiv -1 + 30 \pmod{30}$

$a \pmod{30} \equiv 19 \pmod{30}, \equiv 29 \pmod{30}$

$x = 9, 19, 29 \pmod{30}$ are required Sol.

Ans Sol

$140x \equiv 133 \pmod{301}$

$(301, 140) = 7$

$\therefore$ 7 incongruent Soln

$\frac{140}{7} x \equiv \frac{133}{7} \pmod{\frac{301}{7}}$

$20x \equiv 19 \pmod{43}$

$40x \equiv 38 \pmod{43}$

$-3x \equiv 38 \pmod{43}$

$-45x \equiv 570 \pmod{43}$

$-2x \equiv 11 \pmod{43}$

$-42x \equiv 231 \pmod{43}$

$x \equiv 16 \pmod{43}$

$x \equiv 16 + \frac{301}{7} \times p$

$p = 0, 1, 2, 3, 4, 5, 6$

$x = 16 \pmod{301}$

$x = 59 \pmod{301}$

$x = 102 \pmod{301}$

$x = 145 \pmod{301}$

$x = 188 \pmod{301}$

$x = 231 \pmod{301}$

$x = 274 \pmod{301}$ Ans

Chapter – 8 Fermat (OR Fermat's little Theorem)

Fermat's Theorem

Statement : If a be any integer, then $a^p \equiv a \pmod{p}$

If $(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$

Proof We Prove that

$(A+B)^p = A^p + {}^pC_1 A^{p-1}B + {}^pC_2 A^{p-2}B^2 + \dots + {}^pC_{p-1} AB^{p-1} + B^p$

$\therefore (A+B)^p \equiv (A^p + B^p) \pmod{p}$

[$\because {}^pC_1, {}^pC_2, \dots {}^pC_{p-1}$ are all multiples of p]

Again $(A+B+C)^p \equiv [(A+B)^p + C^p] \pmod{p}$

$\Rightarrow (A+B+C)^p \equiv (A^p + B^p + C^p) \pmod{p}$

and S.O.M

ultimately,

$(A+B+C+ \dots \text{upto } a \text{ terms})^p \equiv A^p + B^p + C^p + \text{upto } a \text{ terms} \pmod{p}$

Put $A = B = C = \dots = 1$

$\therefore (1+1+1 \dots \text{upto } a \text{ terms})^p \equiv 1+1+1 \dots \text{upto } a \text{ terms} \pmod{p}$

$\therefore a^p \equiv a \pmod{p}$

$\Rightarrow a^{p-1} \cdot a \equiv a \pmod{p}$

By restricted cancellation law,

$a^{p-1} \equiv 1 \pmod{p}$

Ques Show that $5^{38} \equiv 4 \pmod{11}$

Sol By Fermat's little theorem

$5^{10} \equiv 1 \pmod{11}$ as $(5, 11) = 1$ — (1)

Now $5^{38} = 5^{30} \times 5^8 = (5^{10})^3 \times (5^2)^4$

$\equiv 1^3 \times 3^4 \pmod{11}$ [$\because 5^2 = 25 \equiv 3 \pmod{11}$ and using (1)]

$\equiv 81 \pmod{11}$

$\equiv 4 \pmod{11}$

$5^{38} \equiv 4 \pmod{11}$

Examples Find the least non negative residue of $11^{470} \pmod{37}$

sol By Fermat's little theorem,

$11^{36} \equiv 1 \pmod{37}$ as g.c.d $(11, 37) = 1$ and 37 is a Prime

$\Rightarrow (11^{36})^{13} \equiv 1^{13} \pmod{37}$ [$\because 470 = 36 \times 13 + 2$]

$\Rightarrow 11^{468} \equiv 1 \pmod{37}$

$\Rightarrow 11^{470} = 11^{468} \times 11^2 \equiv (1 \times 121) \pmod{37} \equiv 10 \pmod{37}$

$\therefore$ $11^{470} \equiv 10 \pmod{37}$

$\therefore$ 10 is the least non-negative residue of 11^{470} modulo 37.

Ques Show that $a^7 \equiv a \pmod{42}$ for all $a \in Z$.

Sol By fermat's little theorem

$a^7 \equiv a \pmod{7}$ as 7 is prime

$\Rightarrow 7 \mid a^7 - a$

Now $a^7 - a = a(a^6 - 1) = a(a^3 - 1)(a^3 + 1)$

$= a(a-1)(a^2 + a + 1)(a+1)(a^2 - a + 1)$

$= (a-1)a(a+1)(a^2 - a + 1)(a^2 + a + 1)$

Now know product of three consecutive integers is divisible by $\lfloor 3$

$\therefore (a-1)\,a(a+1)$ is divisible by $\lfloor 3 = 6$

$\Rightarrow (a-1)\,a(a+1)(a^2 - a + 1)(a^2 + a + 1)$ is also divisible by 6

$\Rightarrow a^7 - a$ is divisible by 6

$\Rightarrow 6 \mid a^7 - a$ ...(2)

From (1) & (2) $7 \times 6 \mid a^7 - a$ [$\because$ g.c.d $(6, 7) = 1$]

$\Rightarrow 42 \mid a^7 - a$

$\Rightarrow a^7 \equiv a \pmod{42}$ for all integers a.

Ques Prove $a^5 \equiv a \pmod{30}$ for all integers a.

Sol By fermat's little theorem,

$a^5 \equiv a \pmod{5}$ as 5 is Prime

$5 \mid a^5 - a$ ...(1)

Now $a^5 - a = a(a^4 - 1) = a(a^2 - 1)(a^2 + 1)$

$= (a-1)\,a(a+1)(a^2 + 1)$

we know, product of three consecutive integers is divisible by $\lfloor 3 = 6 = 3!$

$\therefore (a-1)\,a(a+1)$ is divisible by 6

$\Rightarrow 6 \mid (a-1)\,a(a+1)$

$\Rightarrow 6 \mid (a-1)\,a(a+1)(a^2 + 1)$

$6 \mid a^5 - a$

from (1) & (2), $5 \times 6 \mid a^5 - a$ as g.c.d $(5, 6) = 1$

$\Rightarrow 30 \mid a^5 - a$

$\therefore a^5 \equiv a \pmod{30}$ for all integers a.

Unit - 3

Groups

Definition Let G be a non-empty set together with binary operation star defined on a then algebric structure $\langle G, * \rangle$ is called a group. If it satisfies following properties.

1) $a * b \in G \quad \forall a, b \in G$ (Closer property)
2) $(a * b) * c = a * (b * c) \quad \forall a, b \in G$ (Associative property)
3) $\exists$ an element $e \in G$ such that $e * a = a = a * e \quad \forall a \in G$ then e is called identity element of G w.r.t the operation $*$ (Existence of identity)
4) $\forall a \in G$, $b \in G$ such that $a * b = e = b * a$ (Existence of inverse)

Note: $*$ is a operation is denoted by + or .

Finite and Infinite Group.

If the set G in the group $\langle G, * \rangle$ is finite set then it is called finite group otherwise it is called infinite group.

Order of Group.

The order of group $\langle G, * \rangle$ is defined as number of distinct element in G and it is denoted by $o(G)$

- If is Group G has n element then $o(G) = n$

Abilian and Non-abilian Group

A group $\langle G, * \rangle$ is called Abilian or Communated group iff $a * b = b * a$ for $\forall a, b \in G$.

If $a * b \neq b * a \quad \forall a, b \in G$ then it is non-Abilian group

Groupoid, Semi-group and M

1) Groupoid. In all empty set G together with binary operation $*$ defined on it if it satisfied following exams or properties
   - $\Rightarrow a * b \in G \quad \forall a, b \in G$ (closer)
2) Semigroup. In all empty set G together with binary operation $*$ defined on it if it satisfied
   - $\Rightarrow a * b \in G \quad \forall a, b \in G$ (closer)
   - $\Rightarrow (a * b) * c = a * (b * c) \quad \forall a, b \in G$ (associated)
3) M In all empty set a together with
   - $\rightarrow a * b \in G \quad \forall a, b \in G$ (closer)
   - $\Rightarrow (a * b) * c = a * (b * c) \quad \forall a, b \in G$ (Associative)
   - $\Rightarrow e * a = a = a * e \quad \forall a \in G$ (identity)

Q.2) Show that the set C of all complex numbers forms an infinite abelian group under the operation of addition of complex numbers.

Sol (i) let $z_1 = a + ib$ and $z_2 = c + id$ be any complex numbers.

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

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

$z_1 + z_2 \in C$ [$\because a, b, c, d \in R \Rightarrow a+c, b+d \in R$]

$\therefore$ C is closed under addition.

(ii) let $z_1 = a+ib$, $z_2 = c+id$, $z_3 = e+if$ be any three complex numbers.

Then

$(z_1+z_2)+z_3 = [(a+ib)+(c+id)] + (e+if)$

$= [(a+c)+i(b+d)] + (e+if)$

$= [(a+c)+e] + i[(b+d)+f]$

$= [a+(c+e)] + i[b+(d+f)]$

$= [a+if] + [(c+e)+i(d+f)]$

$= [a+ib] + [(c+id)+(e+if)]$

$= z_1 + (z_2+z_3)$

$\therefore$ addition is associative in C.

(iii) $\forall z = a+ib \in C$ there exists $0 = 0+i0 \in C$ such that $z+0 = (a+ib)+(0+i0) = (a+0)+i(b+0) = (a+ib) = z$

and

$0+z = (0+i0)+(a+ib) = (0+a)+i(0+b) = a+ib = z$

i.e $z+0 = z = 0+z$

$\therefore$ C possesses identity element $0 \in C$

(iv) $\forall z = a+ib \in C$ there is $-z = -a-ib \in C$ such that $z+(-z) = (a+ib)+(-a-ib) = (a+(-a))+i(b+(-b))$

$= 0+i0 = 0$

and $(-z)+z = 0$

i.e $z+(-z) = 0 = (-z)+z$

$\therefore$ C possesses inverse element $z \in C$

Thus $\langle C, + \rangle$ is a group.

(v) $\forall z_1 = a+ib$ and $z_2 = c+id \in C$

$z_1+z_2 = (a+ib)+(c+id) = (a+c)+i(b+d)$

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

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

$\therefore$ addition is commutative in C.

(vi) The number of elements in C is infinite

Thus, $\langle C, + \rangle$ is an infinite abelian group.

Ques $\Rightarrow$ Show that the set of rational numbers does not form a group under multiplication.

Ans Let Q be the set of all rational numbers

(i) Closure property. let $a, b \in Q$

$a = \frac{p_1}{q_1}$ and $b = \frac{p_2}{q_2}$ for some $p_1, q_1, p_2, q_2 \in Z$ and $q_1 \neq 0, q_2 \neq 0$

Then $a \cdot b = \frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2} \in Q$ since Z is closed under and

$q_1 \neq 0$, $q_2 \neq 0$ implies that $q_1 q_2 \neq 0$

Associativity => let $a, b, c \in Q$ so that

$$a = \frac{p_1}{q_1}, \quad b = \frac{p_2}{q_2}, \quad c = \frac{p_3}{q_3}$$ for some p's $\in Z$ and q's $\in Z$ and q's $\neq 0$

Then $(a, b) \cdot c = \left(\frac{p_1}{q_1} \cdot \frac{p_2}{q_2}\right) \cdot \frac{p_3}{q_3} = \frac{p_1 p_2}{q_1 q_2} \cdot \frac{p_3}{q_3}$

$$= \frac{(p_1 p_2) p_3}{(q_1 q_2) q_3} = \frac{p_1 (p_2 p_3)}{q_1 (q_2 q_3)}$$ since

Z is associative under multiplication

$$= \frac{p_1}{q_1} \cdot \frac{p_2 p_3}{q_2 q_3} = \frac{p_1}{q_1} \cdot \left(\frac{p_2}{q_2} \cdot \frac{p_3}{q_3}\right)$$

$$= a \cdot (b \cdot c)$$

(II) The number $1 \in Q$

let $a \in Q$ arbitrarily

Then $a = \frac{p}{q}$ for some p and $q \neq 0$ and $q \in Z$

Then $1.a = \frac{1}{1} \cdot \frac{p}{q} = \frac{1 \cdot p}{1 \cdot q} = \frac{p}{q} = a$

Similarly $a.1 = a$

$a.1 = a.1.a$

$\therefore$ 1 is identity element

(III) **Existence of inverse** => The number $0 \in Q$ But there does not exist any $a \in Q$ such that $0.a = 1$

$\therefore$ 0 has no multiplicative inverse in Q

$\therefore (Q, \cdot)$ is not a group

Ques => check whether all set E of all even integers forms a group under the binary operation $a * b = 2a + 2b$

Sol => E = set of all even integers

(I) let $a, b \in E$

$\therefore a, b$ are even integers

$\Rightarrow 2a + 2b$ is an even integer

$\Rightarrow a * b = 2a + 2b$ is an even integer

$\Rightarrow a * b \in E \ \forall \ a, b \in E$

$\Rightarrow$ closure property holds in E

(II) let $a, b, c \in E$

$\therefore (a * b) * c = (2a + 2b) * c$

$= 2(2a + 2b) + 2c = 4a + 4b + 2c$ — (I)

and $a * (b * c) = a * (2b + 2c) = 2a + (4b + 4c)$ — (II)

(I) and (II) $\Rightarrow (a * b) * c \neq a * (b * c)$ always

for example take

$a = 2, \ b = 4, \ c = 6$

Then $(a * b) * c = (2 * 4) * 6 = (2(2) + 2(4)) * 6$

$= 12 * 6 = 2(12) + 2(6) = 36$

$a * (b * c) = 2 * (4 * 6) = 2 * (2(4) + 2(6))$

$= 2 * 20 = 2(2) + 2(20) = 44$

$(a * b) * c \neq a * (b * c)$ in this case

Hence E is not associative under $*$

E does not form group under $*$

Ans => Let $\mathbb{Q}^*$ denotes the set of all rational numbers except 1, the show that $\mathbb{Q}^*$ forms an infinite abelian group under the operation o defined by $a \circ b = a+b-ab$ for all $a, b \in \mathbb{Q}^*$

Ans Let $\mathbb{Q}^*$ be the set of all rational numbers except 1 the binary Composition $\circ$ on $\mathbb{Q}^*$ is defined as

$$a \circ b = a+b-ab \quad \forall a, b \in \mathbb{Q}^*$$

To show that $\langle \mathbb{Q}^*, \circ \rangle$ forms an infinite abelian group

Closure property. Let $a, b \in \mathbb{Q}^*$ be any elements.

If possible, let

$$a+b-ab = 1$$
$$a+b-ab-1 = 0$$
$$a(1-b)-(1-b) = 0$$
$$(a-1)(1-b) = 0$$
$$a-1 = 0 \quad | \quad 1-b = 0$$
$$\boxed{a = 1} \quad | \quad \boxed{b = 1}$$

which is not possible as $(a, b) \in \mathbb{Q}^*$

$\therefore a+b-ab \neq 1$, also $a+b-ab \in \mathbb{Q}$ and so $a+b-ab \in \mathbb{Q}$

$\therefore a \circ b \in \mathbb{Q}^* \ \forall a, b \in \mathbb{Q}^*$

Thus closure property holds in $\mathbb{Q}^*$

Associativity => Let $a, b, c \in \mathbb{Q}^*$ be any element

$$(a \circ b) \circ c = (a+b-ab) \circ c$$
$$= a+b-ab+c-(a+b)c-ab)$$
$$= a+b+c-ab-bc-ac+abc$$
$$a \circ (b \circ c) = a \circ (b+c-bc)$$
$$= a+b+c-bc-a(b+c-bc)$$
$$= a+b+c-bc-ab-ac+abc$$

$\therefore (a \circ b) \circ c = a \circ (b \circ c)$

Thus, associative property holds in $\mathbb{Q}^*$

Existence of identity => let $\exists\ e \in \mathbb{Q}^*$ such that

$$e \circ a = a = a \circ e, \ \forall a \in \mathbb{Q}^*$$

i.e. $e+a-ea = a = a+e-ae$

$$e+a-ea = a \Rightarrow e-ea = 0$$
$$e(1-a) = 0$$
$$e = 0 \text{ for } a \neq 1$$

$e = 0 \in \mathbb{Q}^*$ works for an identity element in $\mathbb{Q}^*$

Existence of Inverse

Let $a \in \mathbb{Q}^*$ be any element, let $\exists\ b \in \mathbb{Q}^*$ s.t

$$a \circ b = e = b \circ a$$
$$a+b-ab = 0 = b+a-ba$$
$$a+b(1-a) = 0 \Rightarrow b(1-a) = -a$$

$$b = \frac{-a}{1-a} = \frac{a}{a-1}$$

Clearly, $b = \frac{a}{a-1} \in \mathbb{Q}^*$ is the inverse of element a in $\mathbb{Q}^*$

Commutativity : let $a, b \in Q^*$ be any elements
$a * b = a + b - ab = b + a - ba = b * a$

Ques> Let $G = \{a + b\sqrt{2} \quad : a, b \in Q\}$
Show that G is infinite terminal group w.r.t addition (composition defined by $a+b\sqrt{a}, c+d\sqrt{2} \in G$) and also $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + \sqrt{2}(b+d)$.

Sol

Let $G = \{a + b\sqrt{2} \quad : a, b \in Q\}$

① closure property:

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

$x + y = a + b\sqrt{2} + c + d\sqrt{2}$
$= (a+c) + \sqrt{2}(b+d) \quad \in G$
$\therefore$ there closure property

Since the set of all real numbers is associative under addition and $G \in R$ then G is associative under addition

② Existence of identity => $0 = 0 + 0\sqrt{2}$

$x + 0 = (a + b\sqrt{2}) + (0 + 0\sqrt{2})$
$= a + b\sqrt{2} = x$
$0 + x = (0 + 0\sqrt{2}) + (a + b\sqrt{2})$
$= a + b\sqrt{2} = x$
$x + 0 = x = 0 + x$

③ Existence of Inverse

$x = a + b\sqrt{2}$
$-x = -a - b\sqrt{2}$

$x + (-x) = (a + b\sqrt{2}) + (-a - b\sqrt{2})$
$= (a-a) + (b\sqrt{2} - b\sqrt{2})$
$= 0$
$-x + x = (-a - b\sqrt{2}) + (a + b\sqrt{2})$
$= (-a + a) + (-b\sqrt{2} + b\sqrt{2})$
$= 0$

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

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

Ques> Show that the set $\{1, 2, 3, 4, 5, 6\}$ form an infinite abelian group under multiplication mod 7

Sol Let $G = \{1, 2, 3, 4, 5, 6\}$
$\therefore$ Under operation multiplication mod 7
$a * b = r$

0	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

1 is the identity element of G
$1 \times_7 1 = 1 = 1 \times_7 1$
$2 \times_7 4 = 1 = 4 \times_7 2$

$3 \times_7 5 = 1 \quad = 5 \times_7 3$

$4 \times_7 2 = 1 \quad = 2 \times_7 4$

$5 \times_7 3 = 1 \quad = 3 \times_7 5$

$6 \times_7 6 = 1 \quad = 6 \times_7 6$

Note: $i = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$

$j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

$K = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

$\therefore \quad i^2 = j^2 = K^2 = -1$

$i \times j = K \quad , \quad j \times K = i$

$K * i = j$

$j \times i = -K \quad , \quad K * j = -i \quad , \quad i \times K = -j$

Ques Let $G = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}$

Prove that G forms a finite non-abelian group of order 8 under composition of matrix multiplication

Sol $G = \{ \pm I, \pm i, \pm j, \pm k \}$

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

$ij = K = -ji, \quad jk = i = -kj, \quad ki = j = -ik$

$a - b \in a$

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

The element $1 \in G$ works as identity elements

$a \cdot 1 = a = 1 \cdot a$

Thus a is finite non-abelian group.

Ques Show that set of all matrices is in the form.

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

where α is real number forms an abelian group under the operation of matrix multiplication.

$\Rightarrow$ let $G = A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$

closure $\Rightarrow$ $A_\beta = \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$

$$A_\alpha \times A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \times \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos\alpha\cos\beta - \sin\beta \times \sin\alpha & \sin\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta - \cos\alpha \times \sin\beta & -\cos\alpha\sin\beta - \cos\alpha\cos\beta \end{bmatrix}$$

$$A_{\alpha+\beta} = \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin\alpha+\beta & \cos\alpha+\beta \end{bmatrix}$$

Associative $\Rightarrow$ $A_\alpha, A_\beta, A_\gamma \in G$.

L.H.S

$$(A_\alpha \cdot A_\beta) \cdot A_\gamma = A_{\alpha+\beta} \cdot A_\gamma$$

$$= A_{(\alpha+\beta)+\gamma}$$

$$= A_{\alpha} \cdot A_{\beta+\gamma}$$

$$= A_\alpha A_\beta \cdot A_\gamma$$

(3) Existence of Identity: $A_0 = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} =$

4) Existence of Inverse: $A_{-\alpha} = \begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(\alpha) \end{bmatrix}$

$= \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}$

Commutative:

$A_\alpha \cdot A_\beta = A_{\alpha+\beta} = A_{\beta+\alpha} = A_\beta \cdot A_\alpha$

Elementary property of Group:

1) Uniqueness of identity element ⇒ The identity element of group is Unique

Proof: If possible, suppose e_1, e_2 are the identity element of groups even $e_1 * e_2 = e_2$ (since e_1 is identity element)

$e_1 * e_2 = e_1$ (since, e_2 is identity element) — (I)

from (I) & (II)

$e_1 = e_2$

∴ identity element is Unique.

2) Cancellation laws hold in a group.

$a, b \in G$

$a * b = a * c \Rightarrow b = c$ [left Cancellation law]

$b * a = c * a \Rightarrow b = c$ [Right Cancellation law]

Proof: Let $a, b, c \in G$

since, $a \in G$ so that $a^{-1} \in G$

Such that, $a^{-1} * a = e = a * a^{-1}$ — (I)

Now suppose, $a * b = a * c$

Pre

$a^{-1} * a * b = a^{-1} * a * c$

$(a^{-1} * a) * b = (a^{-1} * a) * c$

Acc to (I), $e * b = e * c$

$b = c$

3) Left identity and Right identity are same in the group.

let e and e' be the left and right identity in the group

$e * e' = e'$ — (I) [∵ e is the left identity]

$e * e' = e$ — (II) [∵ e is right identity]

$e' = e$

Thm: let G be a group such that $a^2 = e$ for all $a \in G$ show that a is abelian

Proof: let $a \in G$

then $a^2 = e$

$a * a = e$

Pre multiply by a^{-1}

$a^{-1} * a * a = a^{-1} * e$

$(a^{-1} * a) * a = a^{-1} * e$

$e \cdot a = a^{-1} e$

$a = a^{-1}$

∴ Every element has its own inverse

let $a, b \in G$ then $ab \in G$

$a^{-1} = a$

$b^{-1} = b$

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

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

$ab = ba$

∴ The G is abelian group

Ques: If $(ab)^n = a^n b^n$ holds for all $a, b \in G$ then G must be abelian

$\Rightarrow$ $(ab)^n = a^n b^n$

let put $n = 2$

$(ab)^2 = a^2 b^2$

$(ab)(ab) = (aa)(bb)$

$a(ba)b = a(ab)b$

$\therefore \quad ba = ab$

Property is commutative

$\therefore$ G is abelian

Ques: If $(ab)^n = a^n b^n$ holds for all $a, b \in G$ then G must be abelian

$\Rightarrow$ $(ab)^n = a^n b^n$

let put $n = 2$

$(ab)^2 = a^2 b^2$

$(ab)(ab) = (aa)(bb)$

$a(ba)b = a(ab)b$

$\therefore \quad ba = ab$

Property is commutative

$\therefore$ G is abelian.

Ques: Show that the equation $y^2 ay = a^{-1}$ is solvable for y in G iff a is the abe some element in G

$\Rightarrow$ let $y^2 ay = a^{-1}$ is solvable in G

$\exists \quad b \in G$ such that

$b^2 ab = a^{-1}$

$b \cdot baba = a^{-1}a = e$

$\therefore baba = b^{-1}e = b^{-1}$

$ba\,ba\,b = e$

$ba\,ba\,ba = ea = a$

$(ba)^3 = a$ where e is identity element of a

$\therefore a$ is cube of some element of G

Conversely: let $a = m^3$ for some element $m \in G$

$y^2 ay = (m^{-2})^2 a\, m^{-2}$ for $y = m^{-2}$

$= m^{-4} m^3 m^{-2}$

$= m^{-3} = a^{-1}$

$y^2 ay = a^{-1}$ is satisfied for $y = m^{-2} \in G$

equation $y^2 ay = a^{-1}$ is solvable for y in a group G.

a) let G be a group and $a, b \in G$ such that $b = pap^{-1}$ then prove that $b^n = pa^n p^{-1}$

$\Rightarrow$

Case 1: n is a positive integer then we shall prove that by principle of mathematical induction

let $n = 1$

$b^1 = pa^1 p^{-1}$

$\therefore$ Result is true for $n = 1$

So, Assume result is true for $n = k$

$b^k = pa^k p^{-1}$

Verify the result $n = k+1$

$\therefore b^{k+1} = b^k \cdot b$

$= pa^k p^{-1} \cdot pap^{-1}$

$= pa^k (p^{-1} \cdot p) ap^{-1}$

$= pa^k e ap^{-1}$

$= Pa^k a\ P^{-1}$

$b^{k+1} = Pa^{k+1} P^{-1}$

$\therefore$ Result is true for $n = k+1$

Que① definition of Group based on left Axiom

③ Def of Group based on Right Axiom

⇒① Let G be a non-empty set together with a binary operation $*$ defined on it, then the algebraic structure $\langle G, * \rangle$ is a group if it satisfies the following axioms

(i) $a*b \in G \quad \forall a, b \in G$ (closure prop.)

(ii) $(a*b)*c = a*(b*c) \quad \forall a, b, c \in G$ (Associative prop)

(iii) $\exists$ an element $e \in G$ such that
$e*a = a \quad \forall a \in G$ (Existence of left identity)

(iv) for all $a \in G$, $\exists$ an element $b \in G$ such that
$b*a = e$ [Existence of left inverse]

⇒② Let G be non-empty set together with a binary operation $*$ defined on it, then the algebraic structure $\langle G, * \rangle$ is a group if it satisfies the following axioms

(i) $a*b \in G, \forall a, b \in G$ (Closure prop)

(ii) $(a*b)*c = a*(b*c) \quad \forall a, b, c \in G$ (Associative p)

(iii) $\exists$ an element $e \in G$ such that
$a*e = a \quad \forall a \in G$ [Existence of right identity]

(iv) for all $a \in G$, $\exists$ an element $b \in G$ such that
$a*b = e$ [Existence of right inverse]

Elementary properties of a Group:

1) Uniqueness of Identity element ⇒ Suppose e_1 and e_2 are two identity elements of a group

$\therefore e_1 * e_2 = e_2$ (since e_1 is identity element) ... (i)

$e_1 * e_2 = e_1$ (since e_2 is identity element) ... (ii)

Thus from (i) and (ii)

$e_1 = e_2$

$\therefore$ The identity element of a group is Unique.

2) Cancellation law holds in a group:

For $a, b, c \in G$

$a*b = a*c \Rightarrow b = c$ (left Cancel law)

$b*a = c*a \Rightarrow b = c$ (right Cancel law)

Proof: let $a, b, c \in G$

since $a \in G$ so $a^{-1} \in G$

such that $a^{-1}*a = e = a*a^{-1}$

suppose $a*b = a*c$

$a^{-1} * (a*b) = a^{-1} * (a*c)$

$(a^{-1}*a) * b = (a^{-1}*a) * c$

$e * b = e * c$

$b = c$

$a*b = a*c$

$b = c$

Similarly we can prove that

$b*a = c*a \Rightarrow b = c$

3) for every $a \in G \ (a^{-1})^{-1} = a$

$\forall a \in G \Rightarrow a^{-1} \in G$

$a a^{-1} = e = a^{-1} a$

$a^{-1} a = e = a a^{-1}$

inverse of a^{-1} is a $\therefore (a^{-1})^{-1} = a$

(4) left identity and right identity are same in a group

let e and e^{-1} be left and right identity in a group $\langle G, * \rangle$ then

$e * e = e'$
$e * e' = e$
$e' = e$

Hence, left and right group are same

Cyclic Group $\Rightarrow$ a group G is called cyclic group if there exist $a \in G$ such that each element of G can be return as integral power of a

if $a \in G$ the there exist $a \in G$ such that $b = a^n$

$\therefore$ a is then called generator of G.

Q1) Find the order of each element of the group of four 4th roots of unity

Sol) let $G = \{1, -1, i, -i\}$ be the four fourth roots of unity under multiplication

Clearly, 1 is the identity of G

$o(1) = 1$
$o(-1) = 2$ $[\because (-1)(-1) = 1]$
$o(i) = 4$ $[\because i^4 = 1]$
$o(-i) = 4$ $[\because (-i)^4 = 1]$

2) Show that $G = \{1, 2, 3, 4\}$ forms a cyclic group under multiplication modulo 5.

Sol) let $G = \{1, 2, 3, 4\}$

The composition defined on G is multiplication modulo 5 i.e, $a \times_5 b = r$, where r is the remainder obtained when a b is divided by 5

Now $2^2 = 2 \times_5 2 = 4$
$2^3 = 2 \times_5 2 \times_5 2 = 3$
$2^4 = 2 \times_5 2 \times_5 2 \times_5 2 = 1$
$2^5 = 2 \times_5 2 \times_5 2 \times_5 2 \times_5 2 = 2$

Since every element of G can be written as some power of 2.

$\therefore G = \langle 2 \rangle$ is cyclic group of order 4 generated by 2.

Q3) If an abelian group of order 6 contains an element of order 3, then show that it must be cyclic group.

Sol) let $a \in G$ be an element such that $o(a) = 3$

Since G is of even order $\therefore$ G must contain atleast one element of order 2.

let $b \in G$ be such that $o(b) = 2$

Now $(o(a), o(b)) = 1 \Rightarrow o(a, b) = o(a) \cdot o(b) = 3 \times 2 = 6$

since $a, b \in G \Rightarrow ab \in G$ such that $o(a, b) = 6 = o(G)$

Hence G must be cyclic Group.

Unit → IV

1. Definition of Ring

A non-empty set R together with two binary operations denoted additively (+) and multiplicatively (.), is called a ring if for all $a, b, c \in R$, the following axioms are satisfied.

(i) $a+b \in R$ [closed under addition]
(ii) $(a+b)+c = a+(b+c)$ [addition is associative]
(iii) $\exists$ an element $0 \in R$ such that $0+a = a = a+0$ [existence of additive identity]
(iv) for every $a \in R$, $\exists$ an element $-a \in R$ such that $(-a)+a = 0 = a+(-a)$ [Existence of additive inverse]
(v) $a+b = b+a$ [addition is commutative]
(vi) $a.b \in R$ [closed under multiplication]
(vii) $(a.b).c = a.(b.c)$ [multiplication is associative]
(viii) $a.(b+c) = a.b + c.a$ and $(a+b).c = a.c + b.c$ [distributive laws hold]

A ring R under the binary operations (+) and (.) is denoted by the algebraic system $\langle R, +, \cdot \rangle$

Remark: The algebraic system $\langle R, +, \cdot \rangle$ is called a ring if R forms an abelian group under addition and semi-group under multiplication along with distributive property.

Q) A Gaussian integer is a complex number $a+ib$ where a and b are integers. Show that the set S of all gaussian integers is a ring with usual addition and multiplication of complex number.

Sol. Properties of Addition

1. closure
$x = a+ib$
$y = c+id$
$x+y = a+ib+c+id$
$= (a+c)+i(b+d) \in R$
$\therefore$ closure holds

2. Associative
$x = a+ib$
$y = c+id$
$z = e+if$
$(x+y)+z = ((a+ib)+(c+id))+e+if$
$= (a+c)+i(b+d)+e+if$
$= (a+c+e)+i(b+d+f)$
$= a+(c+e)+i(d+f)+ib$
$= a+ib+((c+id)+(e+if))$

3. Identity
$x = a+ib \quad e*x = x = x*e$
$\Rightarrow$
$e*(a+ib) = (a+ib)$
$e+(a+ib) = (a+ib)$
$e = a+ib-a-ib = 0$

4. Inverse
$z = a+ib$
$-z = -a-ib$
$z*(-z) = a+ib-a-ib$
$= (a-a)+(-ib-ib) = 0$

$-z+z = -a-ib+a+ib$

$= (-a+a)+(-ib+ib)$

$= 0$

$z+-z = 0 = -z+z$

(ii) Multiplication

Closure.

$(a.b) \in R$

$x = a+ib$

$y = c+id$

$(a+ib)(c+id) \in R$

$\therefore ac+iad+ibc+i^2bd$

$\therefore ac+iad+ibc-bd$

$\Rightarrow (ac-bd)+i(ad+bc) \in R$: Closure

(i) Associative

$(a.b).c = a.(b.c)$

$x = a+ib$

$y = c+id$

$z = e+if$

$(x.y).z = ((a+ib)(c+id)).(e+if)$

$= (ac+iad+ibc+i^2bd).(e+if)$

~~$= ace+iacf+ide$~~

$= (ace+iade+ibce+i^2bde+ifac + i^2adf+i^2bcf+i^3bdf)$

$x.(y.z) = (a+ib)((c+id).(e+if))$

$= (a+ib)[ce+icf+ied+i^2df]$

$= (ace+icfa+ieda+i^2dfa+ibce+i^2cf + i^2bed+i^3bdf)$

Ques Prove that Set $G = a+\sqrt{2}b$ where $a, b \in Q$ where Q is the set of rational is a ring.

Sol Addition properties

(i) Closure properties

$x = a+\sqrt{2}b$

$y = c+\sqrt{2}b$

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

$= a+c+\sqrt{2}(b+d) \in G$

$\therefore$ there closer properly

(ii) Associative

$x = a+b\sqrt{2}$, $y = c+d\sqrt{2}$, $z = e+f\sqrt{2}$

$(a+b)+c = a+(b+c)$

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

$(a+\sqrt{2}b+c+\sqrt{2}d)+e+\sqrt{2}f = a+\sqrt{2}b+(c+\sqrt{2}d + e+f\sqrt{2})$

$(a+c+\sqrt{2}(b+d))+e+\sqrt{2}f = a+\sqrt{2}b+(c+\sqrt{2}(d+f)+e]$

$a+c+e+\sqrt{2}(b+d+f) = a+\sqrt{2}b+(c+e+\sqrt{2}(d+f))$

$= a+c+e+\sqrt{2}(a+f+b)$

R.H.S = L.H.S

(iii) Existence of Identity

$x+e = e+x = x$

$a+\sqrt{2}b+e = a+\sqrt{2}b$

$e = a+\sqrt{2}b-a-\sqrt{2}b$

$e = (a-a)+\sqrt{2}b-\sqrt{2}b$

$e = 0$

(iv) Existence of inverse

$x - x = -x + x = e$

~~$x + e = a + \sqrt{2}b +$~~

$x - x = a + \sqrt{2}b - a - \sqrt{2}b$

$= 0$

$-x + x = -a - \sqrt{2}b + a + \sqrt{2}b$

$= 0$

$x - x = -x + x = 0$

then inverse is exist

(v) (vi) Multiplication

$x \cdot y \in \mathbb{Q}$ $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$

$xy = (a + b\sqrt{2}) \times (c + d\sqrt{2})$

$= a(c + d\sqrt{2}) + b\sqrt{2}(c + d\sqrt{2})$

$= ac + ad\sqrt{2} + bc\sqrt{2} + bd2 \in \mathbb{Q}$

(vii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \cdot (e + f\sqrt{2})$

$= [a(c + d\sqrt{2}) + b\sqrt{2}(c + d\sqrt{2})] \cdot (e + f\sqrt{2})$

$= (ac + ad\sqrt{2}) + b(\sqrt{2} + bd(\sqrt{2})^2 \cdot (e + f\sqrt{2}))$

$= (ac + ad\sqrt{2} + bc\sqrt{2} + bd2) \cdot e + f\sqrt{2}(ac + ad\sqrt{2} + bc\sqrt{2} + bd2)$

$= eac + ead\sqrt{2} + fce + fed2 + fac\sqrt{2} + fad(\sqrt{2})^2 + f^2c2 + f^2d\sqrt{2}$

$\Rightarrow x \cdot (y \cdot z)$

$= (a + b\sqrt{2})[(c + d\sqrt{2}) \cdot (e + f\sqrt{2})]$

$= (a + b\sqrt{2})[ce + cf\sqrt{2} + de\sqrt{2} + fd2]$

$= ace + acf\sqrt{2} + ade\sqrt{2} + af d2 + bce\sqrt{2} + bcf2 + bde2 + bf\sqrt{2}$

Prove $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(viii) Distributive

$x \cdot (y + z) = (a + b\sqrt{2}) \cdot (c + d\sqrt{2} + e + f\sqrt{2})$

$= ac + ad\sqrt{2} + ae + af\sqrt{2} + bc\sqrt{2} + bd2 + be\sqrt{2} + bf2$

$(x + y) z = (a + b\sqrt{2} + c + d\sqrt{2})(e + f\sqrt{2})$

$= ae + be\sqrt{2} + ce + de\sqrt{2} + af\sqrt{2} + bf2 + cf\sqrt{2} + df2$

(ix) Prove that set $R = \{(a, b) \mid a, b \in R\}$ is commutative ring under addition and multiplication.

$(a, b) + (c, d) = (a + c, b + a)$

$(a, b)(c, d) = (ac, bd)$

Sol (i) Closure property

$x + y \in R$

$(a, b) + (c, d) = [a + c, b + d] \in R$

closure holds

(ii) Addition is associative

$[(a, b) + (c, d)] + (e, f) = (a, b) + [(c, d) + (e, f)]$

$[a + c, b + d] + (e, f) = (a, b) + [c + e, d + f]$

$[a+c+e, b+d+f] = [a+c+e, b+d+f]$

L.H.S = R.H.S

(iii) Existence of additive identity

$e + x = x = x + e$

$e + (a, b) = (a, b)$

$e = (a, b) - (a, b)$

$e = (a-a, b-b) = 0$

(iv) Existence of inverse

$x - x = -x + x = e$

$x - x = (a, b) - (a, b) = [a-a, b-b] = 0$

$-x + x = -(a, b) + (a, b) = 0$

So the inverse is exist

(v) Closed under multiplication.

$x \cdot y \in R$

$x \cdot y = (a, b) \cdot (c, d)$

$= [ac, bd] \in R$

(vi) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$[(a, b) \cdot (c, d)] \cdot (e, f) = (a, b)[(c, d)(e, f)]$

$[ac, bd] \cdot (e, f) = (a, b)[ce, df]$

$[a(e), bd f] = [a(e), bd f]$

L.H.S = R.H.S

(viii) $x \cdot (y+z) = x \cdot y + z \cdot x$

$(a, b)[(c, a) + (e, f)] = (a, b) \cdot (c, d) + (e, f) \cdot (a, b)$

$(a, b)(c, d) + (a, b)(e, f) = [ac, bd] + [ea, fb]$

$[ac, bd] + (ae, bf) = (ac + ea, bd + fb]$

$[ac + ae, bd + bf] = [ac + ae, bd + bf]$

R.H.S = L.H.S

Q) Prove that Set $R = \{(a, b) \mid a, b \in R\}$ is commutative ring under addition and multiplication.

$(a, b) + (c, a) = (a + c, b + a)$

$(a, b)(c, d) = (ac, bd)$

Sol

(i) Closure

$a + b \in R$

$(f + g)x = f(x) + g(x) \in R$

(ii) $(a + b) + c = a + (b + c)$ [associative]

$[(f + g) + h]x = [f + (g + h)]x$

$[f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)]$

$f(x) + g(x) + h(x) = f(x) + g(x) + h(x)$

R.H.S = L.H.S

(iii) Existence of additive identity

$e+a = a = a+e$

$e + f(x) = f(x)$

$e = f(x) - f(x) = 0$

(iv) Existence of additive inverse

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

$-a+a = -f(x)+f(x) = 0$

$a+(-a) = f(x) - f(x) = 0$

(v) $a+b = b+a$ [Addition is ~~also~~ Commutative]

$(f+g)x = (g+f)x$

$f(x)+g(x) = g(x)+f(x)$

L.H.S = R.H.S

(vi) Properties of Multiplication

$(fg)(x) = f(x)g(x)$

$fg \in g$

g is closed under multiplication

2) Associative

$[(fg)h](x) = (fg)(x)\,[h(x)]$

$= [f(x)\,g(x)]\,[h(x)]$

$= f(x)\,(gh(x))$

$= f(gh)x$

$(fg)h = fg(h)$

$\forall f, g, h \in G$

3) Distributive law:

$f, g, h \in g$

then $[f(g+h)](x) = [f(x)]\,[(g+h)(x)]$

$= [f(x)]\,[g(x)+h(x)]$

$= f(x)\,g(x) + f(x)\,h(x)$

$= fg(x) + fh(x)$

$= [fg+fh](x)$

$f(g+h) = fg + fh$

by $(g+h)f = gf + fh$

$\therefore$ by $f, \to$ is a ring.

also $fg \in g$

$(fg)(x) = f(x)\,g(x) = g(x)\,f(x)$

$= gf(x)$

$fg = gf$

Commutative property of for multiplication is true in g.

Now $\forall f \in g$, there is $e \in g$

$e(x) = \forall x \in [0,1]$

such that $(ef)(x) = e(x)\,f(x)$

$= f(x)$

$\therefore f(x)\ \forall x \in [0,1]$

by $fe = f$

$ef = f = fe$

Polynomial

An infinite sequence $(a_0, a_1, a_2, \ldots a_n, a_{n+1})$ of the elements of a ring R is said to be a polynomial over R if all except a finite no. number of its terms a_i are equal to zero.

Sum and Product of two polinomial

$$f = \{a_0, a_1, a_2 \ldots\}$$

$$g = \{b_0, b_1, b_2 \ldots\}$$

$$f + g = \{a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots\}$$

$$f \times g = \{a_0 b_0, a_1 b_1, \ldots\}$$

2) Elementary properties of Ring

I a) $a.0 = 0.a = 0$ d) $a(b-c) = ab - ac$

b) $a(-b) = (-a)b = -ab$ e) $(b-c)a = ba - ca$

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

II a) $(a+b)(c+d) = ac + bc + ad + bd$

b) $(a-b)(c-d) = ac - bc - ad + bd$

c) $(a+b)^2 = a^2 + b^2 + ab + ba$

d) $(a-b)^2 = a^2 + b^2 - ab - ba$

e) $(a+b)(a-b) = a^2 - b^2 - ab + ba$

III $(na)(nb) = (n^2)(ab)$

Q> Prove that the given ring $x+y = y+x$ also hold in R and R is a ring.

Sol

W.K.T. 1 is the elements of R

$$x+y\,(1+1) = x(1+1) + y(1+1)$$
$$= x + x + y + y$$
$$= x(x+y) + y$$

OR

$$(x+y)(1+1)$$
$$(x+y)(1+1) = (x+y)1 + (x+y)$$
$$= x + y + x + y$$
$$= x + (y+x) + y$$

$\therefore (x+y) = (y+x)$

Hence R is a ring

Qus> If R is a ring with Identity element such that $(xy)^2 = x^2y^2$ Then show that R is Commutative

Sol Give an example to show that result may be false if R doesn't have a any identity

Let R be a ring such that

$$(xy)^2 = x^2y^2$$
$$(x(y+1))^2 = x^2(y+1)^2$$
$$(xy+x)^2 = x^2(y^2+1+2y)$$
$$= x^2y^2 + x^2 + 2x^2y$$
$$x^2y^2 + x^2 + 2x^2y = x^2y^2 + 2x^2y + y^2$$
$$xyx = x^2y$$

Replace x by $(x+1)$ in (1) we get

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

$(xy+y)(x+1) = (x^2+1+2x)y$

$xyx + xy + xy + y = x^2y + y + 2xy$

$\Rightarrow xyx = x^2y$

$\Rightarrow xy = yx$

$\therefore R$ is Commutative

Field

(A) Properties of addition

(i) $\forall a, b \in F \Rightarrow a+b \in F$ [closure Pro]

(ii) $\forall a, b, c \in F \Rightarrow (a+b)+c = a+(b+c)$ [Associative]

(iii) $\forall a \in F, \exists\, 0 \in F$ such that [Existence of Identity]
$a+0 = a = 0+a$

(iv) $\forall a \in F, \exists\, -a \in F$ such that [Existence of additive Inverse]
$a+(-a) = 0 = (-a)+a$

(v) $\forall a, b, \in F \Rightarrow a+b = b+a$ [Commutative Property]

(B) Properties of multiplication

(i) $\forall a, b \in F \Rightarrow ab \in F$

(ii) $\forall a, b, c \in F \Rightarrow a(bc) = (ab)c$

(iii) $\forall a \in F$, there exists $1 \in F$ such that
$1 \cdot a = a = a \cdot 1$
Here 1 is called unity of F

(iv) $\forall a\ (\neq 0) \in F$, $\exists\, b \in F$ such that
$a \cdot b = b \cdot a = 1$
Here b is called inverse of a

(v) $\forall a \cdot b \in F \Rightarrow a \cdot b = b \cdot a$

(C) Distributive laws
$\forall a, b, c \in F$
$a \cdot (b+c) = a \cdot b + a \cdot c$
$(b+c) \cdot a = b \cdot a + c \cdot a$

Ques Prove that the set $Q[\sqrt{2}] = \{a+\sqrt{2}b \mid a, b \in Q\}$ where Q is set of rationals, is a field under usual addition and multiplication of reals.

Sol(i) Properties of Addition

(i) $a+b \in Q$ [closure Propertie]

$x = a+\sqrt{2}b$

$y = c+\sqrt{2}d$

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

$= a+c+\sqrt{2}(b+d) \in Q$

$\therefore$ there closer property.

(ii) Associative Properties

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

$(a+\sqrt{2}b+c+\sqrt{2}d)+e+\sqrt{2}f = a+\sqrt{2}b+(c+\sqrt{2}d+e+\sqrt{2}f)$

$[a+c+\sqrt{2}(b+d)]+e+\sqrt{2}f = a+\sqrt{2}b+(c+\sqrt{2}(d+f)+e)$

$a+c+e+\sqrt{2}(b+d+f) = a+\sqrt{2}b+(c+e+\sqrt{2}(d+f))$

$= a+e+c+\sqrt{2}(b+d+f)$

R.H.S = L.H.S

(iii) Existence of Identity

$x+e = e+x = x$

$a+\sqrt{2}b+e = a+\sqrt{2}b$

$e = a+\sqrt{2}b-a-\sqrt{2}b$

$e = 0$

(iv) Existence of inverse

$x - x = e = -x + x$

$x + x = a + \sqrt{2}b + (-a - \sqrt{2}b) = 0$

$-x + x = -a - \sqrt{2}b + a + \sqrt{2}b = 0$

B) Properties of Multiplication.

(i) $\forall a, b \in F \Rightarrow ab \in F$

$x \cdot y = (a + b\sqrt{2}) \times (c + d\sqrt{2})$

$= a(c + d\sqrt{2}) + b\sqrt{2}(c + d\sqrt{2})$

$= ac + ad\sqrt{2} + cb\sqrt{2} + db(\sqrt{2})^2$

$= (ac + 2bd) + \sqrt{2}(ad + bc) \in F$

(ii) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$(a + b\sqrt{2}) \cdot (c + d\sqrt{2})(e + f\sqrt{2})$

$= a(c + d\sqrt{2}) + b\sqrt{2}(c + d\sqrt{2}) \cdot (e + f\sqrt{2})$

$= (ac + ad\sqrt{2}) + b(\sqrt{2} + bd(\sqrt{2})^2) \cdot (e + f\sqrt{2})$

$= (ac + ad\sqrt{2} + bc\sqrt{2} + bd2) \cdot e + f\sqrt{2}(ac + ad\sqrt{2} + bc\sqrt{2} + bd2)$

$= eac + ead\sqrt{2} + bce + bed2 + fac\sqrt{2} + fad(\sqrt{2})^2 + f^2c2 + f^2d2\sqrt{2}$

$\Rightarrow x \cdot (y \cdot z)$

$= (a + b\sqrt{2})((c + d\sqrt{2}) \cdot (e + f\sqrt{2}))$

$= (a + b\sqrt{2})(c + (a + b\sqrt{2})b\sqrt{2} \cdot (e + f\sqrt{2})$

$\Rightarrow (ac + bc\sqrt{2} + ab\sqrt{2} + b^2 2) \cdot (e + f\sqrt{2})$

$= aec + be2\sqrt{2} + ae b\sqrt{2} + b^2 e2 + fac\sqrt{2} + fbc2 + abf2 + b^2 f2\sqrt{2}$

Prove $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(iii) $x = l + \sqrt{2}m \in \mathbb{Q}[\sqrt{2}]$ $l, m \in \mathbb{Q}$

$1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ such that

$x \cdot 1 = (l + \sqrt{2}m)(1 + 0\sqrt{2}) = l + \sqrt{2}m = x$

and $1 \cdot x = (1 + 0\sqrt{2})(l + \sqrt{2}m) = l + \sqrt{2}m = x$

$\therefore x \cdot 1 = x = 1 \cdot x \; \forall x \in \mathbb{Q}[\sqrt{2}]$

$\therefore 1 + 0\sqrt{2}$ is multiplicative identity

(iv) let $x = l + \sqrt{2}m \neq 0$ $l, m \in \mathbb{Q}$

l and m is non-zero

Now $\frac{1}{x} = \frac{1}{l + \sqrt{2}m} = \frac{l - \sqrt{2}m}{(l + \sqrt{2}m)(l - \sqrt{2}m)} = \frac{l - \sqrt{2}m}{l^2 - 2m^2}$

$= \left(\frac{l}{l^2 - 2m^2}\right) + \sqrt{2}\left(\frac{-m}{l^2 - 2m^2}\right)$

we claim $l^2 - 2m^2 \neq 0$

since if $l^2 - 2m^2 = 0$

$\Rightarrow l^2 = 2m^2$

$\Rightarrow 2 = \frac{l^2}{m^2} = \left(\frac{l}{m}\right)^2$ [$\because$ at least one of l and m is non-zero and $l^2 = 2m^2$ implies that if l not m is zero $\Rightarrow m \neq 0$]

$\Rightarrow 2 = \left(\frac{l}{m}\right)^2$

which is impossible, since 2 cannot be square of any rational number

$\therefore \frac{l}{l^2-2m^2}$ and $\frac{-m}{l^2-2m^2}$ are non zero rational

$\Rightarrow \frac{1}{x} \in \mathbb{Q}[\sqrt{2}]$

Also $x \cdot \frac{1}{x} = (l+\sqrt{2}m)\left[\frac{l}{l^2-2m^2} + \sqrt{2}\left(\frac{-m}{l^2-2m^2}\right)\right]$

$= 1+0\sqrt{2}$

and $\frac{1}{x} \cdot x = \left[\frac{l}{l^2-2m^2} + \sqrt{2}\left(\frac{-m}{l^2-2m^2}\right)\right](l+\sqrt{2}m)$

$= 1+0\sqrt{2}$

$\therefore x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$

$\Rightarrow \frac{1}{x} = \left(\frac{l}{l^2-2m^2}\right) + \sqrt{2}\left(\frac{-m}{l^2-2m^2}\right)$ is the multiplicative inverse of each non zero element $l+\sqrt{2}m$ of $\mathbb{Q}[\sqrt{2}]$

(iv) $\forall\, x, y \in \mathbb{Q}[\sqrt{2}]$, $xy = yx$, where $x = l+\sqrt{2}m$ and $y = n+\sqrt{2}p$

(c) Distributive laws.

(i) $a \cdot (b+c) = a \cdot b + a \cdot c$

$x \cdot (y+z) = (a+b\sqrt{2})(c+d\sqrt{2} + e+f\sqrt{2})$

$= ac + ad\sqrt{2} + ae + af\sqrt{2} + bc\sqrt{2} + bd2 + be\sqrt{2} + bf2$

$x \cdot y + x \cdot z = (a+b\sqrt{2})(c+d\sqrt{2}) + (a+b\sqrt{2})(e+f\sqrt{2})$

$= ac + ad\sqrt{2} + bc\sqrt{2} + bd2 + ae + af\sqrt{2} + be\sqrt{2} + bf2$

L.H.S = R.H.S

So it is hold distributive laws

(ii) $(y+z) \cdot x = y \cdot x + z \cdot x$

$(y+z) \cdot x = \left((c+d\sqrt{2}) + (e+f\sqrt{2})\right) \cdot (a+b\sqrt{2})$

$= (c+d\sqrt{2}+e+f\sqrt{2})(a+b\sqrt{2})$

$= ac + ad\sqrt{2} + ae + af\sqrt{2} + bc\sqrt{2} + bd2 + be\sqrt{2} + bf2$

$y \cdot x + z \cdot x = (c+d\sqrt{2})(a+b\sqrt{2}) + (e+f\sqrt{2})(a+b\sqrt{2})$

$= ca + cb\sqrt{2} + ad\sqrt{2} + bd2 + ea + be\sqrt{2} + af\sqrt{2} + bf2$

R.H.S = L.H.S

So it is hold distributive laws.