a] Prove that every group of order 4 is abelian. (8)

Let G be a group and

$o(G) = 4$

we know that order of every element divides order of G.

$\therefore$ let a be orbitry element other than identity.

$\therefore$ possible $o(a) = 2, 4$

if $\exists$ an element a of order 4

$\Rightarrow \quad G = \langle a \rangle$

hence G is cyclic

$\Rightarrow G$ is abelian

now, let assume $\nexists$ an element $a \ni o(a) = 4$

$\Rightarrow \cancel{\forall}$ non identity element a $o(a) = 2$

$\therefore \cancel{\forall a \in G}$

$$a^2 = e$$

$\Rightarrow a = a^{-1} \; \cancel{\forall} a \in G$

consider, $a, b \neq e$

$$(ab)^2 = e$$

$$\Rightarrow ab = (ab)^{-1}$$

$$\Rightarrow ab = b^{-1} a^{-1}$$

$$\Rightarrow ab = b \cdot a$$

hence G is abelian

hence proved.

1a] let G be the set of all real numbers except -1 and define $a*b = a+b+ab$ $\forall a,b \in G$. Examine if G is an abelian Group under $*$. (16)

ans: 1) closure property

let $a \neq -1$, $b \neq -1$

$\therefore a*b = a+b+ab$

$\because a, b$ are Real no.

$a+b+ab \in \mathbb{R}$ and it can not equal to -1

because

if $a+b+ab = -1$

$\Rightarrow a+b+ab+1 = 0$

$\Rightarrow (a+1)(1+b) = 0$

$\Rightarrow$ either $a+1=0$ or $1+b=0$

$\Rightarrow a=-1$ or $b=-1$

it's contradiction

hence closure property holds.

2] Associativity:-

$(a*b)*c = (a+b+ab)*c$

$= a+b+ab+c+ca+cb+cab$

$= a+b+c+ab+bc+ac+abc$

$a*(b*c) = a*(b+c+bc)$

$= a+b+c+bc+ab+ac+abc$

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

3] Identity:-

let $e \in G$ $\ni$ $e \neq -1$

$a*e = a$

$a * e = a + e + ae = a$

$\therefore a + e + ae = a$

$\Leftrightarrow e + ae = 0$

$\Leftrightarrow e(1+a) = 0$

$\Rightarrow e = 0$ or $1 + a = 0$

but $1 + a = 0 \Rightarrow a = -1$

which is not possible

$\therefore e = 0$ is identity

<u>Inverse</u>: let $a \neq -1 \in G$

then b is inverse of a

$\Leftrightarrow a * b = 0$

$\Rightarrow a + b + ab = 0$

$\Rightarrow b + ab = -a$

$\Rightarrow b(1+a) = -a$

$\Rightarrow b = \dfrac{-a}{1+a}$

$\because a \neq -1 \Rightarrow 1 + a \neq 0$

$\therefore b$ is inverse element of G.

2(b) Let H and K are two finite normal subgroup of co-prime order of a Group G. Prove that $hk = kh \ \forall \ h \in H$ and $k \in K$. (10)

Sol:- $\because$ H and K are normal in G

$(o(H), o(K)) = 1$

we claim, $H \cap K = \{e\}$

~~let~~ let $o(H \cap K) \neq 1$

$\because$ H and K are subgroup of G

$\Rightarrow$ $H \cap K$ is also subgroup of H & K.

$\Rightarrow$ $o(H \cap K)$ divides $o(H)$

also $o(H \cap K)$ divides $o(K)$

$\Rightarrow$ $o(H \cap K) \mid$ g.c.d of $(o(H), o(K))$

but $(o(H), o(K)) = 1$

$\Rightarrow$ $H \cap K = \{e\}$

Let $h \in H$ and $k \in K$ be any elements,

then $h \in H$ and $k \in K \subseteq G$

H is normal in G

gives $k^{-1}hk \in H$ and we know $h^{-1} \in H$

$\Rightarrow$ $k^{-1}hkh^{-1} \in H$ --{closure property

again ~~$h^{-1} \in H$ and~~

$h^{-1} \in H \subseteq G$ and K is normal in G

then $(h^{-1})^{-1} k h^{-1} \in K$

$\Rightarrow$ $hkh^{-1} \in K$

also $k^{-1} \in K$

$\therefore$ $k^{-1}hkh^{-1} \in K$

$\therefore$ $k^{-1}hkh^{-1} \in H \cap K$

but $H \cap K = \{e\}$

$\therefore$ $k^{-1}hkh^{-1} = e$

$\Rightarrow$ $hk = kh$

Q.7(C) Let A be an ideal of a commutative Ring R and $B = \{x \in R : x^n \in A \text{ for } n \in \mathbb{N}\}$ is B an Ideal of R? justify your ans:- (10)

Soln:- $B = \{x \in R : x^n \in A \text{ for } n \in \mathbb{N}\}$

$\because$ A is ideal of R

$\therefore$ $\forall\ r \in R,\ a \in A$

$ra \in A$

let $x, y \in B$

$\Rightarrow \exists\ m, n \in \mathbb{N} \ni$

$x^m \in A,\ y^n \in A$

consider, $\cancel{(x+y)^{m+n}}$

$(x-y)^{m+n} = \cancel{(x + (-y))^{m+n}}$

$$= \sum_{r=0}^{m+n} (-1)^r\ {}^{n+m}C_r\ x^{n+m-r}\, y^r$$

($\because$ Binomial theorem is valid in commutative ring)

case-1] if $r \geq n$

$\Rightarrow y^r = y^n \cdot y^{-n+r}$

but $y^n \in A$ and A is ideal

and $y^{-n+r} \in R$

$\Rightarrow y^r \in A$

$\therefore (x-y)^{m+n} \in A$

case-2] if $r < n$

$\Rightarrow n - r > 0$

$\Rightarrow m + n - r > m$

$\therefore$ in both cases $(x-y)^{m+n} \in A$ — (1)

$\Rightarrow (x-y) \in B$

(ii) let $x \in B$ be arbitrary element

$\Rightarrow x^n \in A$ for some $n \in \mathbb{N}$

consider $r \in R$ arbitrary

$(rx)^n = (rx).(rx) \cdots (rx)$ n times

$= r^n . x^n$ — commutative

but $x^n \in A$ and A is ideal

$\therefore r^n . x^n \in A$

$\Rightarrow (rx)^n \in A$

$\Rightarrow rx \in B$

$\therefore$ B is ideal.

Prove that the ring
$\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}, i = \sqrt{-1}\}$
of Gaussian integers is Euclidean domain.

Def^n :- Euclidean domain :-
An Integral domain D is called a Euclidean domain if there is a function d from nonzeros elements of D to the non negative integers $\ni$

1) $d(a) \leq d(ab)$ for all non zero a, b in D
and
2] if $a, b \in D$, $b \neq 0$, then $\exists$ elements q and r in D $\ni$ $a = bq + r$ where $r = 0$ or $d(r) < d(b)$

Sol^n let $(G, +, \cdot)$ be the ring of Gaussian integers where $G = \{x+iy : x, y \in I\}$.
let $d : G - \{0\} \to N \cup \{0\}$
$d(x+iy) = x^2 + y^2 \quad \forall \; 0 + i0 \neq x+iy \in G$

now if $x+iy$ is a non-zero element of G then (x^2+y^2) is a non-negative integer.
Thus we have assigned an non-negative integer to every non-zero element of G.

If $x+iy$ and $m+in$ are two non-zero elements of G. then
$d[(x+iy)(m+in)]$
$= d[(xm - ny) + i(my + xn)]$

$= (xm-ny)^2 + (my+xn)^2$
$= x^2m^2 + n^2y^2 + m^2y^2 + x^2n^2$
$= (x^2+y^2)(m^2+n^2)$
$\geq x^2+y^2 \quad \therefore [\because m^2+n^2 \geq 1]$

Thus $d[(x+iy)(m+in)] \geq d(x+iy)$.

Now to show the existance of division algorithm in G.

Let $\alpha \in G$ and let β be a nonzero element of G. Let $\alpha = x+iy$, $\beta = m+in$. Define a complex number λ by eq^n

$$\lambda = \frac{\alpha}{\beta} = \frac{x+iy}{m+in}$$

$$= \frac{(x+iy)(m-in)}{m^2+n^2}$$

$$= p+iq$$

where p, q are rational numbers; here λ is not necessarily a guassian integers.

Also division by β is possible $\because \beta \neq 0$. Let p' and q' be the nearest integers to p and q respectively. Then obiviously

$$|p-p'| \leq 1/2, \quad |q-q'| \leq 1/2$$

Let $\lambda' = p'+iq'$. Then λ' is Guassian integer.

now $d = \frac{\alpha}{\beta}$

$\Rightarrow \alpha = d\beta$

$\Rightarrow \alpha = d'\beta + d\beta - d'\beta$

Thus $\alpha = d'\beta + (d-d')\beta$ --- (1)

~~Thus~~ $\because$ α, β, d' are Guassian integers

$\therefore$ from (1)

$(d-d')\beta$ is also guassian integer.

now if p and q are integers

then $p = p'$, $q = q'$

so $d - d' = (p-p') + i(q-q')$

$= 0 + i0$

thus $(d-d')\beta = 0 + i0$

if p and q are not both integers then $(d-d')\beta$ is a non-zero Gaussian integer and we have

$d[(d-d')\beta]$

$= d[\{(p-p') + i(q-q')\}(m+in)]$

$= [(p-p')^2 + (q-q')^2](m^2+n^2)$

$= [(p-p')^2 + (q-q')^2]\, d(\beta)$

$\leq \left[\frac{1}{4} + \frac{1}{4}\right] d(\beta)$

$= \frac{1}{2} d(\beta) < d(\beta)$

thus $\alpha = d'\beta + (d-d')\beta$ where d' and $(d-d')\beta$ are gaussian integers and

either $(d-d')\beta = 0$

or $d[(d-d')\beta] < d(\beta)$

$\therefore$ $Z[i]$ is euclidean ring.