ABSTRACT ALGEBRA

(Assignments & Solutions - MM Mam)

Name : Surojit Dhara.

Course : 2 Year. M.Sc (Mathematics)

Mob. No : 8240500362.

1. GROUPS, SUBGROUPS.

Pr(1) Let $G = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \mid a \neq 0, a \in \mathbb{R} \right\}$. Is it a group under multiplication?

Soln: Let, $A = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$, $B = \begin{pmatrix} b & b \\ b & b \end{pmatrix} \in G$, $a, b \neq 0$, $a, b \in \mathbb{R}$.

then, $AB = \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix}$

$= \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} \in G$.

As usual the associativity holds for matrix multiplication.

Now, the matrix $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = J$ (say) serves the purpose of identity as,

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}\begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

for every matrix $\begin{pmatrix} a & a \\ a & a \end{pmatrix} \in G$

Also, for matrix $\begin{pmatrix} a & a \\ a & a \end{pmatrix} \in G$, its inverse is of the form $\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix} \in G$ as

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix} = \begin{pmatrix} \frac{1}{4a} & \frac{1}{4a} \\ \frac{1}{4a} & \frac{1}{4a} \end{pmatrix}\begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

So, G forms a group under matrix multiplication

Pr(2) Let $G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid |a| + |b| \neq 0, a, b \in \mathbb{R} \right\}$. Is it a group under multiplication?

Soln: Let, $M = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $N = \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \in G$, $|a|+|b| \neq 0$, $|c|+|d| \neq 0$, $a, b, c, d \in \mathbb{R}$

then, $MN = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix} \in G$.

As usual associativity holds for matrix multiplication

As, for any matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

& $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$, we take the identity • to be the matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Also, for any matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$, we have,

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

So, $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in G.$

Hence, G forms a group under matrix-multiplication.

Pr(3). Let $G = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Show that the non-zero elements in G form a group denoted by G^* under multiplication.

Soln: For $a+b\sqrt{2}, c+d\sqrt{2} \in G$, $a, b, c, d \in \mathbb{Q}$, we have $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in G$. So G is closed under multiplication.

As $G \subseteq \mathbb{R}$, associativity holds as well.

$1+0\sqrt{2} = 1$ is the identity element,

i.e, $(a+b\sqrt{2}).1 = 1.(a+b\sqrt{2}) = a+b\sqrt{2}$.

Also, for $a+b\sqrt{2} \in G$ s.t $a+b\sqrt{2} \neq 0$, $(a+b\sqrt{2})^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in G$. So $(G^*, \times)$ is a group.

Pr(4). Show that the set of all transformations of the type $z \longmapsto \frac{az+b}{cz+d}$, $ad-bc \neq 0$ of the complex no's in itself, is a group for the operation of composite transformations.

(This group is called Mobius transformation group)

Soln: Let us denote,

$$M = \left\{ f : \mathbb{C} \longrightarrow \mathbb{C} \mid f(z) = \frac{az+b}{cz+d},\ ad-bc \neq 0 \right\}$$

Let, $f, g \in M$ s.t

$$f(z) = \frac{az+b}{cz+d}, \quad ad-bc \neq 0.$$

$$g(z) = \frac{pz+q}{rz+s}, \quad ps-qr \neq 0,$$

Now, $(fog)(z) = f\left(\frac{pz+q}{rz+s}\right) = \frac{(ap+br)z + (aq+bs)}{(cp+dr)z + (cq+ds)}$

& $(ap+br)(cq+ds) - (aq+bs)(cp+dr)$

$= (ad-bc)(ps-qr) \neq 0$.

$\therefore fog \in M$.

Hence, M is closed under composition operation.

As usual function composition holds its associativity

As identity element, we take the identity transformation, i.e, I s.t

$$I(z) = z = \frac{1.z+0}{0.z+1} \quad \& \quad foI = Iof = f \ \forall f \in M$$

Also for $f \in M$ s.t $f(z) = \frac{az+b}{cz+d}$, $ad-bc \neq 0$,

$$f^{-1}(z) = \frac{\left(\frac{d}{ad-bc}\right)z + \left(-\frac{b}{ad-bc}\right)}{\left(-\frac{c}{ad-bc}\right)z + \left(\frac{a}{ad-bc}\right)} = \frac{dz-b}{-cz+a} \quad \text{s.t } fof^{-1} = f^{-1}of = I$$

so, $f^{-1} \in M$.

Thus, M forms a group under the composition operation.

Pr(5). Find the order of the group $GL_n(\mathbb{F}_p)$ where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of integers modulo a prime number p.

Soln: With $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$,

$$GL_n(\mathbb{F}_p) = \left\{ A \in M_{n\times n}(\mathbb{F}_p) \mid \det A \neq 0 \right\}$$

We write each matrix $A \in M_{n\times n}(\mathbb{F}_p)$ as,

$$A = (u_1, u_2, \ldots, u_n)$$

where $u_i = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{pmatrix}$ are the column vectors of $A = (a_{ij})_{n\times n}$.

Now, each $u_i \in \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n \text{ times}}$.

For $\det A \neq 0$, $u_1 \in \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \setminus (0,0,\ldots,0)$ So, elements of u_1 can be chosen in $(p^n - 1)$ no of different ways. In other words there may be $(p^n - 1)$ no of different u_1's.

Again for $\det A \neq 0$, u_2 should be linearly independent with u_1, i.e, $u_2 \neq au_1$ where $a \in \mathbb{Z}_p$. Hence no of different choices for u_2 is $(p^n - p)$.

Next, for $\det A \neq 0$, u_3 should be linearly independent with u_1 & u_2, i.e, $u_3 \neq au_1 + bu_2$ where $a, b \in \mathbb{Z}_p$. So, no of different choices for u_3 is $(p^n - p^2)$.

Continuing in this way, we find that, no of different choices of u_n so that $\det A \neq 0$, is $(p^n - p^{n-1})$.

Hence,

$$|GL_n(\mathbb{F}_p)| = |GL_n(\mathbb{Z}_p)|$$
$$= (p^n - p^{n-1})(p^n - p^{n-2}) \cdots (p^n - p)(p^n - 1).$$

Pr(6). Show that every $\sigma \in S_n$ can be expressed as a product of disjoint cycles.

Soln: $\sigma \in S_n \Rightarrow \sigma$ is a map from the set $\{1,2,\ldots,n\}$ to itself. Not only that, σ is also a bijection, i.e, σ is 1:1 and onto.

Now, let $a_1 = 1$ & $a_{i+1} = \sigma(a_i)$, $i = 1,2,\ldots,n-1$

As no of elements in $\{1,2,\ldots,n\}$ is finite, the chain $a_1 \to a_2 \to a_3 \to \ldots$ can't go infinitely and thus there exists integer $j \in \{1,2,\ldots,n\}$ such that $a_j \to a_1$, i.e, $a_1 = \sigma(a_j) = a_{j+1}$

Lets say, $\tau_1 = (a_1\ a_2 \ldots\ldots\ a_{j+1})$

If $\sigma = \tau_1$, then we are done.

If not, say, $a_k \notin \tau_1$. Then by above argument, we form $\tau_2 = (a_k\ a_{k+1} \ldots\ldots\ a_m)$ and obviously τ_1 & τ_2 are disjoint, otherwise if for some i, $a_{k+i} \in \tau_1 \cap \tau_2$, then we find $\sigma^{m-k-i}(a_{k+i}) = a_m \in \tau_1$ and hence $\sigma(a_m) = a_k \in \tau_1$, a contradiction.

Again if $\sigma = \tau_1 \circ \tau_2$, then we are done.

If not, inductively we find $\tau_3, \tau_4, \ldots, \tau_r$ s.t $\sigma = \tau_1 \circ \tau_2 \circ \tau_3 \circ \ldots \circ \tau_r$ and all τ_i's are disjoint cycles.

This completes the proof.

Pr(7). Every $\sigma \in S_n$ can be expressed as a product of transpositions.

Soln: We have earlier proved every permutation $\sigma \in S_n$ can be expressed as a product of disjoint cycles, say, $\tau_1, \tau_2, \ldots, \tau_r$.

i.e, $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r$.

Now to prove the required we only need to show that every cycle in S_n can be written as product of transpositions.

Now every cycle $\sigma = (a_1\ a_2\ a_3 \dots a_k) \in S_n$ can be expressed as,

$$\sigma = (a_1\ a_k)(a_1\ a_{k-1}) \dots (a_1\ a_3)(a_1\ a_2)$$

[product of transpositions]

Therefore this follows that every $\sigma \in S_n$ can be expressed as product of transpositions.

Pr.(8). The set A_n of all even permutations forms a subgroup of S_n of order $n!/2$.

(This group is called Alternating group)

Soln: As composition of two even permutations is again an even permutation, A_n is closed under composition rule.

(1) acts as the identity since it is an even permutation and

$$\sigma(1) = (1)\sigma = \sigma \quad \forall \sigma \in A_n.$$

Again inverse of an even permutation is again an even permutation, so must belong to A_n.

Hence A_n is a subgroup of S_n.

Now, let S denote the set of all odd permutations in S_n.

Define $f: A_n \longrightarrow S$ by $\sigma \longmapsto (1\ 2)\sigma \quad \forall \sigma \in A_n$.

Then f is 1-1 and onto, Hence $|A_n| = |S|$, i.e no of even permutations is equal to the no of odd permutations in S_n.

Also, $A_n \cap S = \phi$ as no permutation can be even and odd simultaneously.

$\therefore$ As $|S_n| = n!$, this implies,

$$|A_n| = n!/2.$$

Pr(9). List all the elements of order 2 in S_4.
How many elements of S_n have order 2?

Soln: The elements of order 2 in S_4 are listed below:

2-cycles: $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3,4)$

product of 2-cycles: $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$

Second Part:

An element of S_n has order two iff this element is a product of k-disjoint transpositions where $1 \leq k \leq [n/2]$

Fix an integer k s.t $1 \leq k \leq [n/2]$. The product of k disjoint transpositions has the form

$$\delta = (i_1\ j_1)(i_2\ j_2) \cdots\cdots (i_k\ j_k)$$

where the numbers $i_1, j_1, i_2, j_2, \ldots, i_k, j_k$ are distinct elements of the set $\{1, \ldots, n\}$.

Now since $(i\ j) = (j\ i)$, we can choose the 1st transposition in $\binom{n}{2}$ different ways. For each of these choices, we may choose the 2nd transposition in $\binom{n-2}{2}$ different ways. For each of these choices, the 3rd transposition can be chosen in $\binom{n-4}{2}$ different ways and so on.

Again as disjoint cycles commute, resuffling of these k-transpositions results in same permutation in S_n. So, no of distinct elements of S_n that are products of k distinct transpositions is

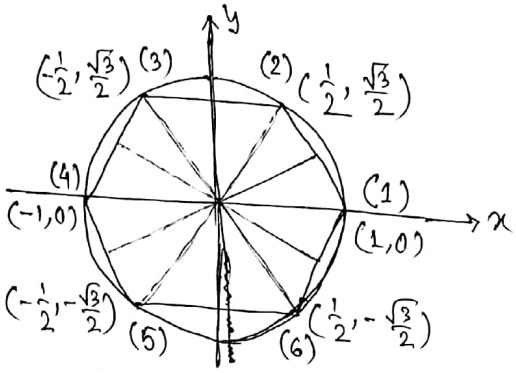
$$\frac{1}{k!} \prod_{s=0}^{2(k-1)} \binom{n-2s}{2}$$

So, total no of elements of S_n having order 2 is

$$\sum_{k=1}^{[n/2]} \frac{1}{k!} \prod_{s=0}^{(k-1)} \binom{n-2s}{2}$$

Pr(10). Write elements as permutation in S_6 of the dihedral group of symmetries of a regular hexagon inscribed in a unit circle with one vertex on the x-axis.

Soln:



The elements are,

$\{(1), (1\ 2\ 3\ 4\ 5\ 6), (1\ 3\ 5)(2\ 4\ 6), (1\ 4)(2\ 5)(3\ 6), (1\ 5\ 3)(2\ 6\ 4), (1\ 6\ 5\ 4\ 3\ 2), (2\ 6)(3\ 5), (1\ 3)(4\ 6), (1\ 5)(2\ 4), (1\ 4)(2\ 3)(5\ 6), (1\ 6)(2\ 5)(3\ 4), (1\ 2)(3\ 6)(4\ 5)\}$

Pr(11). Let $|x|$ denote the order of an element x in a group G. Show that $|x| = |x^{-1}| = |gxg^{-1}|$ for any $g \in G$. Deduce that $|ab| = |ba|$ for any $a, b \in G$.

Soln: Let $|x| = m$, i.e., $x^m = 1$ & $x^r \neq 1$ for any $0 < r < m$.

Now, $(x^{-1})^m = (x^m)^{-1} = (1)^{-1} = 1 \Rightarrow |x^{-1}| \leq m$.

but if $|x^{-1}| = n$ (say) s.t. $0 < n < m$, then

$(x^{-1})^n = 1 \Rightarrow (x^n)^{-1} = 1 \Rightarrow x^n = 1$ with $0 < n < m$, which is a contradiction to the minimality of m.

$\Rightarrow |x^{-1}| \not< m$

$\Rightarrow |x^{-1}| = m = |x|$.

Again, $(gxg^{-1})^m = gx^m g^{-1} = g.1.g^{-1} = g.g^{-1} = 1$

$\Rightarrow |gxg^{-1}| \leq m$.

but if $|gxg^{-1}| = q$ (say) s.t. $0 < q < m$, then $(gxg^{-1})^q = 1 \Rightarrow gx^q g^{-1} = 1 \Rightarrow x^q = g^{-1}g = 1$ with $0 < q < m$, again a contradiction.

$\therefore |gxg^{-1}| = m = |x| = |x^{-1}|$.

Now for any $a, b \in G$,

$$|ab| = |(ab)^{-1}| = |b^{-1}a^{-1}| = |b(b^{-1}a^{-1})b^{-1}| = |bb^{-1}a^{-1}b^{-1}|$$
$$= |a^{-1}b^{-1}| = |(ba)^{-1}| = |ba|. \quad [|ab| = |babb^{-1}| = |ba|]$$

Pr(12). Prove that if $x^2 = 1 \ \forall x \in G$, then G is abelian.

Soln: $\forall x \in G$, we have $x^2 = 1$

$$\Rightarrow x = x^{-1} \ \forall x \in G.$$

Now, $\forall a, b \in G$, $ab = a^{-1}b^{-1}$ $[\because a = a^{-1}, b = b^{-1}]$

$$= (ba)^{-1}$$
$$= ba \quad [\because ba \in G \Rightarrow (ba)^{-1} = ba]$$

So, G is abelian.

Pr(13). Show that G is abelian group iff $(ab)^n = a^2b^2$.

Soln: G is abelian $\Leftrightarrow ab = ba \ \forall a, b \in G$.

$\Leftrightarrow a(ab)b = a(ba)b \ \forall a, b \in G$.

$\Leftrightarrow a^2b^2 = abab \ \forall a, b \in G$

$\Leftrightarrow (ab)^n = a^nb^n \ \forall a, b \in G$.

Pr(14). Prove that any finite group of even order contains an element of order 2.

Soln: Let G be a finite group of even order, i.e., $|G| = 2m$ (say).

If possible, let $x^2 \neq 1 \ \forall x \in G$ s.t $x \neq 1$

i.e, $x \neq x^{-1} \ \forall x \in G$, s.t $x \neq 1$.

Then we collect all pairs (x, x^{-1}) by means of which we cover all the non-identity elements of G.

Now as $1^{-1} = 1$ or $1^2 = 1$, we add 1 to the collection to cover whole of G. But that makes $|G|$ to be odd, which is a contradiction.

Hence, $\exists x (\neq 1) \in G$ s.t

$$x^2 = 1$$

i.e, $\exists x \in G$ s.t $o(x) = |x| = 2$.

Pr.(15). Let $\mathbb{F}$ be a field. The Heisenberg group $H(\mathbb{F})$ is defined to be the multiplicative group:

$$H(\mathbb{F}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F} \right\}$$

(a) Find formulas for products and inverses of elements in $H(\mathbb{F})$.

(b) Show that $H(\mathbb{F})$ is non-abelian group.

(c) Prove that every non-identity element of $H(\mathbb{R})$ has infinite order.

(d) Let $\mathbb{F}$ be a field (finite) with q elements. Show that $|H(\mathbb{F})| = q^3$.

(e) Find orders of elements of $H(\mathbb{F}_2)$.

Soln:

(a)
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+e & b+f+ag \\ 0 & 1 & c+g \\ 0 & 0 & 1 \end{pmatrix}$$

A B — product of two elements.

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

— inverse of an element.

(b)
$$\begin{pmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+e & b+f+ce \\ 0 & 1 & c+g \\ 0 & 0 & 1 \end{pmatrix}$$

B A

So, $AB \neq BA$ for $A, B \in H(\mathbb{F})$,

Hence, $H(\mathbb{F})$ is non-abelian.

(c) For non-identity $A \in H(\mathbb{R})$,

$$A^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \neq I_{3\times 3} \text{ for any } n < 2$$

So, every non-identity element of $H(\mathbb{R})$ has infinite order.

(d) If $|\mathbb{F}| = q$, then we choose each of the unknown parameters a, b, c in q many different ways in order to form an element of $H(\mathbb{F})$.

So, $|H(\mathbb{F})| = q^3$.

(e) $H(\mathbb{F}_2)$

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ → order 1 (Identity element)

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ → order 2, $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ → order 2

$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ → order 2, $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ → order 2

$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ → order 4, $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ → order 2

$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ → order 4.

Pr(16) Let G be an abelian group. Prove that the set $t(G) = \{g \in G : |g| < \infty\}$ is a subgroup of G, (called the TORSION SUBGROUP of G). Give an example to show that $t(G)$ is not a subgroup when G is not abelian.

Soln: Clearly $1 \in t(G)$, hence $t(G) \neq \emptyset$.

If $g_1, g_2 \in t(G)$, then $|g_1| < \infty$, $|g_2| < \infty$.

$|g_1| = m$, $|g_2| = n$ (say)

Now, as G is abelian,

$$|g_1 g_2^{-1}| = \text{lcm}(|g_1|, |g_2^{-1}|)$$
$$= \text{lcm}(|g_1|, |g_2|) \quad [\because |g_2^{-1}| = |g_2|]$$
$$= \text{lcm}(m, n) < \infty.$$

hence, $g_1 g_2^{-1} \in t(G)$.

Thus, if G is abelian, $t(G)$ forms a subgroup of G.

Examples where $t(G)$ is not a subgroup:

(1) In $GL_2(\mathbb{Q})$, consider,

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

then $|A| = 4$, $|B| = 3$

thus $A, B \in t(G)$ where $G = GL_2(\mathbb{Q})$.

But $AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is of infinite order

as $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

$\therefore AB \notin t(G)$.

Hence $t(G)$ is not a subgroup of $G = GL_2(\mathbb{Q})$.

(2) Consider the infinite dihedral group of a plane. $= \{x, y \mid x^2 = y^2 = 1\}$,

$x \equiv$ Reflection about $x = 0$

$y \equiv$ " " $x = 1$.

then $|x| = |y| = 2 \quad \therefore x, y \in t(G)$

but $xy \equiv$ translation of a point of 2 unit towards $(-)$ ve x-axis

thus, xy is of infinite order.

$\Rightarrow xy \notin t(G)$

$\therefore t(G)$ is not a subgroup of G.

Pr(17). Let H & K be subgroups of a group G.

Then $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G iff $HK = KH$. – Prove.

Soln: First, lets assume $HK = KH$.

Clearly HK is non-empty as $1 = 1.1 \in HK$.

Now, let, $h_1k_1, h_2k_2 \in HK$ where $h_1, h_2 \in H$

$k_1, k_2 \in K$,

Then $(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$

$= h_1k_3h_2^{-1}$ [$\because k_1, k_2 \in K$, $k_1k_2^{-1} \in K \Rightarrow k_1k_2^{-1} = k_3$ (say)]

$= h_1h_3k_4$ [$\because k_3h_2^{-1} \in KH = HK$, $\exists\ h_3 \in H$ & $k_4 \in K$, s.t $k_3h_2^{-1} = h_3k_4$]

$= h_4k_4$ [$\because h_1, h_3 \in H$, $h_1h_3 \in H \Rightarrow h_1h_3 = h_4$ (say)]

$\in HK$.

Therefore, HK is a subgroup of G.

Conversely, lets assume HK is a subgroup of G.

R.T.P: $HK = KH$.

Let $x \in HK \Rightarrow \exists\ h_1 \in H$ & $k_1 \in K$ s.t $x = h_1k_1$

since HK is a subgroup $x^{-1} \in HK \Rightarrow (h_1k_1)^{-1} \in HK$

$\Rightarrow k_1^{-1}h_1^{-1} \in HK$. $\Rightarrow \exists\ h_2 \in H$ & $k_2 \in K$ s.t

$k_1^{-1}h_1^{-1} = h_2k_2$

$\Rightarrow (k_1^{-1}h_1^{-1})^{-1} = (h_2k_2)^{-1}$

$\Rightarrow h_1k_1 = k_2^{-1}h_2^{-1} \in KH$. $\Rightarrow x \in KH$.

$\therefore HK \subseteq KH$.

Similarly, we can show $KH \subseteq HK$.

Consequently, $HK = KH$.

Pr(18). Give example of a group G and two subgroups H & K s.t HK is not a subgroup.

Soln: Let us consider, $G = S_3$, $H = \{(1), (1\ 2)\}$ & $K = \{(1), (1\ 3)\}$ then H & K are subgroups of $G = S_3$.

But $HK = \{(1), (1\ 2), (1\ 3), (1\ 3\ 2)\}$ is not a subgroup of G as $(1\ 3\ 2)^{-1} = (1\ 2\ 3) \notin HK$.

Pr(19). Show that a group can not be the union of two proper subgroups.

Soln: Let G be group & H_1, H_2 be its two proper subgroup s.t $G = H_1 \cup H_2$ (if possible).

Now, $H_1 \neq H_2$, otherwise $G = H_1$ or $G = H_2$ contradicting the fact that H_1 & H_2 are proper subgroups of G.

So, let; $x \in H_1 \setminus H_2 \subset G$
$y \in H_2 \setminus H_1 \subset G$.

As G is a group, $x, y \in G$, thus, $xy \in G = H_1 \cup H_2$

i.e., $xy \in H_1$ or $xy \in H_2$

If $xy \in H_1$, then as $x \in H_1 \Rightarrow x^{-1} \in H_1$ [$\because H_1$ is a subgroup]

$\Rightarrow x^{-1}.xy = y \in H_1$, contradiction.

Again if $xy \in H_2$, then as $y \in H_2 \Rightarrow y^{-1} \in H_2$ [$\because H_2$ is a subgroup]

$\Rightarrow xy.y^{-1} = x \in H_2$, contradiction,

Therefore, there doesn't exist two proper subgroups H_1 & H_2 of G s.t $G = H_1 \cup H_2$. ['in fact $H_1 \cup H_2$ is not a subgroup even if $H_1 \not\subset H_2$ and $H_2 \not\subset H_1$]

Pr(20). Find all subgroups of S_3 & D_4.

Soln: All subgroups of S_3 are:

order 1: $\{(1)\}$

order 2: $\{(1), (1\,2)\}, \{(1), (1\,3)\}, \{(1), (2\,3)\}$

order 3: $\{(1), (1\,2\,3), (1\,3\,2)\}$

All subgroups of D_4 are:

Order 1: $\{R_{0^\circ}\}$

order 2: $\{R_{0^\circ}, R_{180^\circ}\}, \{R_{0^\circ}, H\}, \{R_{0^\circ}, V\}$,
$\{R_{0^\circ}, D_1\}, \{R_{0^\circ}, D_2\}$

order 4: $\{R_{0^\circ}, R_{90^\circ}, R_{180^\circ}, R_{270^\circ}\}$,
$\{R_{0^\circ}, H, V, R_{180^\circ}\}, \{R_{0^\circ}, R_{180^\circ}, D_1, D_2\}$

Pr(21). Let H be a subgroup of G and $a \in G$. Show that $a \in H$ iff $aH = H$.

Soln: Let $a \in H$.

$$aH = \{ah \mid h \in H\}$$
$$= \{h' \mid h' \in H\} \quad [\because a \in H, h \in H \Rightarrow ah = h' \in H]$$
$$= H.$$

Conversely let $aH = H$.

then $ah \in aH = H$ where $h \in H$

$\Rightarrow ah = h'$ for some $h' \in H$

$\Rightarrow a = h'h^{-1} \in H$ as H is a subgroup of G

$\Rightarrow a \in H$.

Pr(24). Let G be a group and $x, y \in G$ have finite orders m and n resp. Prove that $|xy|$ divides $\text{lcm}(m,n)$ if $xy = yx$.

Give an example of x and y so that $|xy| < \text{lcm}(m,n)$. What can you say if $xy \neq yx$.

Soln: Let $\text{lcm}(m,n) = q$ (say)

$\Rightarrow q = mk_1$ & $q = nk_2$ for some k_1 & $k_2 \in \mathbb{Z}$.

Now, as $xy = yx$,

$$(xy)^q = \underbrace{xy \cdot xy \cdot \cdots \cdots \cdot xy}_{q \text{ times}}$$
$$= x^q y^q = (x^m)^{k_1} (y^n)^{k_2} = (1)^{k_1}(1)^{k_2} = 1$$

Hence, $|xy|$ divides q.

i.e., $|xy|$ divides $\text{lcm}(m,n)$ if $xy = yx$.

Consider $G = S_3$ & $x = (1\ 2)$, $y = (1\ 2\ 3)$

then $|x| = 2$ & $|y| = 3$.

but, $|xy| = |(1\ 2)(1\ 2\ 3)| = |(2\ 3)| = 2 < 6 = \text{lcm}(|x|,|y|)$

If $xy \neq yx$, then $|xy|$ may be infinite if G is infinite and if G is finite, no conclusion can be drawn about $|xy|$.

Pr(25). Give an example of a group G which is not cyclic group but every proper subgroup of which is cyclic.

Soln: Let us consider the group S_3. (S_3 is not cyclic)

The proper subgroups of S_3 are listed below:

$$\{(1)\} = \langle(1)\rangle$$
$$\{(1),(1\,2)\} = \langle(1\,2)\rangle$$
$$\{(1),(1\,3)\} = \langle(1\,3)\rangle$$
$$\{(1),(2\,3)\} = \langle(2\,3)\rangle$$
$$\{(1),(1\,2\,3),(1\,3\,2)\} = \langle(1\,2\,3)\rangle$$

– all are cyclic.

Pr(26). Show that a cyclic group with just one generator has at most two elements.

Soln: Let $G = \langle x\rangle$ where x is the only generator of G.

Now, let $|x| > 2$, i.e., $|G| > 2$

then, $x^2 \neq 1 \Rightarrow x \neq x^{-1}$

$\Rightarrow x^{-1}$ is another generator of G distinct from x, which is a contradiction.

$\therefore |x| \leq 2$, consequently $|G| \leq 2$.

Pr(27). Prove that an infinite cyclic group has exactly two generators.

Soln: Let G be an infinite cyclic group s.t $G = \langle x\rangle$.

Then, also, $G = \langle x^{-1}\rangle$ and $|x| \neq 2$.

$\therefore x$ & x^{-1} are two generators of G.

Now if possible, let there exist another generator of G, say x^m, $m \in \mathbb{Z}^+$.

i.e, $G = \langle x^m\rangle$ for some $1 < m \in \mathbb{Z}^+$

Then, $x \in G = \langle x^m\rangle \Rightarrow \exists\, k \in \mathbb{Z}$ s.t $x = (x^m)^k$

$\Rightarrow x^{mk-1} = 1$ & $(mk-1)$ is finite, which contradicts the fact that x is of infinite order.

Hence, G has only two generators.

2. HOMOMORPHISM, ISOMORPHISM

Pr(1). Let $(a_1, a_2, \dots, a_k)$, $\sigma \in S_n$.
Then show that $\sigma(a_1 a_2 \cdots a_k)\sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_k))$

Soln: Let $\pi = (a_1, a_2, \dots, a_k)$

Since $\sigma \in S_n$, σ is a one-one mapping from I_n onto I_n. Thus the elements $\sigma(1), \sigma(2), \dots, \sigma(n)$ are all distinct and so, $I_n = \{\sigma(1), \sigma(2), \dots, \sigma(n)\}$.

Let r be any integer s.t $1 \le r < k$.
then, $\sigma\pi\sigma^{-1}(\sigma(a_r)) = \sigma\pi(\sigma^{-1}(\sigma(a_r)))$
$= \sigma(\pi(a_r))$
$= \sigma(a_{r+1})$

Also, $\sigma\pi\sigma^{-1}(\sigma(a_k)) = \sigma(\pi(a_k)) = \sigma(a_1)$

Now, let $a \in I_n$ be s.t $a \neq \sigma(a_r)$ for all r, $1 \le r \le k$.
Then, $\sigma^{-1}(a) \in I_n$ and $\sigma^{-1}(a) \neq a_r$ for all r, $1 \le r \le k$.

$\Rightarrow \pi(\sigma^{-1}(a)) = \sigma^{-1}(a)$

$\Rightarrow \sigma\pi\sigma^{-1}(a) = \sigma(\pi(\sigma^{-1}(a)))$
$= \sigma(\sigma^{-1}(a)) = a$.

Hence, it follows that;

$$\sigma(a_1, a_2, \dots, a_k)\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k))$$

Pr(2). Let $\phi : G \to H$ be an isomorphism. Prove that $\phi^{-1} : H \to G$ is an isomorphism.

Soln: $\phi : G \to H$ is an isomorphism
$\Rightarrow \phi$ is a bijection from G onto H
$\Rightarrow \phi^{-1}$ is a bijection from H onto G.

Now, let, $h_1, h_2 \in H \Rightarrow \exists\, g_1, g_2$ s.t $\phi(g_1) = h_1$ & $\phi(g_2) = h_2$
then, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$
$= h_1 h_2$

$\Rightarrow \phi^{-1}(h_1 h_2) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$
$\Rightarrow \phi^{-1}$ is a group-homomorphism from H onto G.
$\Rightarrow \phi^{-1} : H \to G$ is an isomorphism. (Proved)

Pr(3). Let $a \in G$ and $i_a : G \to G$ be the map

$$i_a(g) = aga^{-1} \quad \forall g \in G.$$

Show that i_a is an automorphism of G.

Let $B(G)$ denote the group of bijections of G.

Define $\psi : G \to B(G)$ by $\psi(a) = i_a$.

Show that ψ is a group-homomorphism and $\ker \psi = Z(G)$. Show that the image $I(G)$ of G under ψ is a normal subgroup of $Aut(G)$.

Soln: Clearly, the map $i_a : G \to G$ is well-defined.

i_a is a group-homomorphism:

Let $g_1, g_2 \in G$.

then $i_a(g_1 g_2) = a(g_1 g_2)a^{-1}$

$= (a g_1 a^{-1})(a g_2 a^{-1})$

$= i_a(g_1) . i_a(g_2)$

i_a is onto:

If $g \in G$, then $a^{-1}ga \in G$ s.t

$$i_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = g.$$

$$\ker(i_a) = \{ g \in G \mid i_a(g) = 1 \}$$
$$= \{ g \in G \mid aga^{-1} = 1 \}$$
$$= \{ g \in G \mid g = a^{-1}a = 1 \}$$
$$= \{1\}.$$

Hence i_a is 1-1 and consequently i_a is an isomorphism from G to G,

i.e, i_a is an automorphism of G. (Proved)

$\psi : G \to B(G)$ defined by,

$$\psi(a) = i_a .$$

ψ is a group-homomorphism:

Let $a, b \in G$, then,

$$\psi(ab)(g) = i_{ab}(g)$$
$$= (ab)g(ab)^{-1} = abgb^{-1}a^{-1} = i_a(i_b(g))$$
$$= i_a i_b(g) = \psi(a)\psi(b)(g) \quad \forall g \in G$$

$\therefore \psi(ab) = \psi(a)\psi(b) \quad \forall a,b \in G$.

$\therefore \psi$ is a group-homomorphism. (Proved)

$\ker\psi = \{ g \in G \mid \psi(g) = I \}$, I is the identity mapping

$= \{ g \in G \mid i_g = I \}$

$= \{ g \in G \mid i_g(x) = x \ \forall x \in G \}$

$= \{ g \in G \mid gxg^{-1} = x \ \forall x \in G \}$

$= \{ g \in G \mid gx = xg \ \forall x \in G \}$

$= Z(G)$.

$\therefore \ker\psi = Z(G)$. (Proved)

Now, $I(G) = \{ i_g \in B(G) \mid g \in G \} \subset Aut(G)$.

<u>$I(G)$ is a subgroup</u>

First we see that, $i_g(gxg) = gxg \quad \forall x \in G$.

$\Rightarrow (i_g)^{-1}(x) = g^{-1}xg$.

$= i_{g^{-1}}(x) \quad \forall x \in G$

$\Rightarrow (i_g)^{-1} = i_{g^{-1}} \quad \forall g \in G$.

Now if $i_g, i_h \in I(G)$, then,

$(i_g)(i_h)^{-1} = i_g i_{h^{-1}} = i_{gh^{-1}} \in I(G)$, as $gh^{-1} \in G$.

$\therefore I(G)$ is a subgroup of $Aut(G)$.

<u>$I(G)$ is normal in $Aut(G)$</u>

For $i_g \in I(G)$ & $k \in Aut(G)$, we have,

$k i_g k^{-1}(x) = k i_g(x')$ where $k(x') = x$.

$= k(gx'g^{-1})$

$= k(g)k(x')k(g)^{-1}$

$= k(g)\,x\,k(g)^{-1}$

$= i_{k(g)} \in I(G)$ as $k(g) \in G \ \forall g \in G$.

$\therefore k i_g k^{-1} \in I(G) \quad \forall i_g \in I(G)$.

$\therefore I(G) \triangleleft Aut(G)$.

Pr(4). Show that the map $\varphi : GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$ defined by $\varphi(A) = (A^t)^{-1}$ is an automorphism.

Soln: Clearly the map $\varphi : GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$ is well-defined.

Now, let $A, B \in GL_n(\mathbb{R})$

then, $\varphi(AB) = ((AB)^t)^{-1}$

$= (B^t A^t)^{-1}$

$= (A^t)^{-1}(B^t)^{-1}$

$= \varphi(A)\varphi(B)$

$\therefore \varphi$ is a group homomorphism.

If $A \in GL_n(\mathbb{R})$, then $(A^t)^{-1} \in GL_n(\mathbb{R})$ s.t

$\varphi((A^t)^{-1}) = \left(((A^t)^{-1})^t\right)^{-1} = (A^{-1})^{-1} = A.$

$\therefore \varphi$ is surjective.

$\ker \varphi = \{A \in GL_n(\mathbb{R}) \mid \varphi(A) = I_{n\times n}\}$

$= \{A \mid (A^t)^{-1} = I_{n\times n}\}$

$= \{A \mid A^t = I_{n\times n}\}$

$= \{A \mid A = I_{n\times n}\} = \{I_{n\times n}\}$

$\therefore \varphi$ is 1-1.

Consequently, φ is an automorphism of $GL_n(\mathbb{R})$.

Pr(5). Show that the map $\varphi : G \to G$ defined by $\varphi(x) = x^{-1}$ is an automorphism iff G is abelian.

Soln: Suppose $\varphi(x) = x^{-1}$ is automorphism.

then $\varphi(xy) = \varphi(x)\varphi(y) \quad \forall\, x, y \in G$

$\Rightarrow (xy)^{-1} = x^{-1}y^{-1} \quad \forall\, x, y \in G$

$\Rightarrow xy = (x^{-1}y^{-1})^{-1} \quad \forall\, x, y \in G$

$\Rightarrow xy = yx \quad \forall\, x, y \in G.$

$\Rightarrow G$ is abelian.

Conversely if G is abelian, then, $\varphi(xy) = (xy)^{-1} = x^{-1}y^{-1}$

$= \varphi(x)\varphi(y) \quad \forall\, x, y \in G$

$\therefore \varphi$ is a group homomorphism.

Clearly φ is 1-1 & onto. So, φ is an automorphism.

Pr.(6). Show that upto isomorphism the only cyclic groups are $\mathbb{Z}/n\mathbb{Z}$, $n=0,1,2,\ldots$.

Soln: Let us consider a cyclic group G.

Case 1: $|G|$ is finite, say, $|G|=n$.

We show that, $G \cong \mathbb{Z}/n\mathbb{Z}$

Since G is cyclic, $\exists\, x \in G$ s.t $|x|=n$ and $G=\langle x\rangle$

$$G = \{1, x, x^2, \ldots, x^{n-1}\}$$

Define $\phi : \mathbb{Z} \longrightarrow G$ by $\phi(m) = x^m$.

Clearly ϕ is well-defined.

$$\phi(m+n) = x^{m+n} = x^m \cdot x^n = \phi(m)\,\phi(n)$$

$\therefore \phi$ is a group homomorphism.

Clearly ϕ is surjective.

$$\begin{aligned}\ker\phi &= \{m \in \mathbb{Z} \mid \phi(m) = 1\}\\ &= \{m \in \mathbb{Z} \mid x^m = 1\}\\ &= \{m \in \mathbb{Z} \mid n \text{ divides } m\}\\ &= \{m \in \mathbb{Z} \mid m = nk,\ k \in \mathbb{Z}\}\\ &= n\mathbb{Z}.\end{aligned}$$

Hence by 1st isomorphism theorem,

$$\mathbb{Z}/n\mathbb{Z} \cong G$$

Case 2: $|G|$ is infinite.

We show that $G \cong \mathbb{Z}$.

Then we see the above mapping is a onto group homomorphism and has a kernel

$$\begin{aligned}\ker\phi &= \{m \in \mathbb{Z} \mid \phi(m) = 1\}\\ &= \{m \in \mathbb{Z} \mid x^m = 1\}\\ &= \{0\} = 0\mathbb{Z}.\end{aligned}$$

Hence by 1st isomorphism theorem,

$$\mathbb{Z}/0\mathbb{Z} = \mathbb{Z} \cong G.$$

Hence, upto isomorphism, the only cyclic groups are $\mathbb{Z}/n\mathbb{Z}$, $n=0,1,2,\ldots$.

Pr(7). Determine the group of automorphisms of $\mathbb{Z}$, S_3 and $\mathbb{Z}/n\mathbb{Z}$.

Soln: **Aut($\mathbb{Z}$):**

Let φ be an automorphism of $\mathbb{Z}$.

i.e, $\varphi : \mathbb{Z} \to \mathbb{Z}$ is an isomorphism.

Now, as $\varphi(n) = \varphi(\underbrace{1+1+\cdots+1}_{n \text{ times}})$

$$= \underbrace{\varphi(1)+\varphi(1)+\cdots+\varphi(1)}_{n \text{ times}}$$

$$= n\varphi(1),$$

hence the function φ is completely determined by where it maps 1 to.

Again as φ is an isomorphism and 1 is a generator of $(\mathbb{Z}, +)$, φ must map 1 to a generator.

$\therefore \varphi(1) = 1$ or $\varphi(1) = -1$.

Corr. to $\varphi(1) = 1$, the map φ is defined by $\varphi(n) = n$ and corr. to $\varphi(1) = -1$, the map φ is defined by $\varphi(n) = -n$. These are the only possible automorphisms of $\mathbb{Z}$.

$\therefore$ Aut($\mathbb{Z}$) is a group of order 2, hence cyclic. Hence,

$$\text{Aut}(\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2.$$

Aut(S_3):

$$S_3 = \{1, x, x^2, y, xy, x^2y \mid x^3 = 1, y^2 = 1\}.$$

Since an isomorphism preserves the order of an element, we have, if φ is an automorphism of S_3, then

$$|\varphi(x)| = 3 \;\&\; |\varphi(y)| = 2$$

$\therefore \varphi(x)$ has 2 different choices in the group S_3 and for each of those, $\varphi(y)$ has 3 different choices. If $\varphi(x)$ and $\varphi(y)$ is fixed, then the mapping is determined completely.

Hence, $|\text{Aut}(S_3)| = 2 \times 3 = 6$.

Also, as S_3 is non-abelian, $Aut(S_3)$ is non-cyclic.

So, $Aut(S_3) \simeq S_3$.

[If $Aut(S_3)$ be cyclic $\Rightarrow$ $Inn(S_3)$ is cyclic $\Rightarrow$ $S_3/Z(S_3)$ is cyclic $\Rightarrow$ S_3 is abelian]

$Aut(\mathbb{Z}/n\mathbb{Z})$:

First define $U(n) = \{\bar{m} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(m,n) = 1\}$. This is called the GROUP of UNITS IN $\mathbb{Z}_n$.

Now, if ϕ be an automorphism of $\mathbb{Z}/n\mathbb{Z}$, then $\phi(\bar{n}) = n\phi(\bar{1})$. So ϕ is totally determined by the choice $\phi(\bar{1})$. Since $\bar{1}$ is a generator of $\mathbb{Z}/n\mathbb{Z}$, we must have $\phi(\bar{1})$ as a generator in $\mathbb{Z}/n\mathbb{Z}$.

$\therefore |Aut(\mathbb{Z}_n)| = \phi(n)$. [Euler-$\phi$ function]

Now, define $T: Aut(\mathbb{Z}_n) \longrightarrow U_n$ by

$$\phi \longmapsto \phi(\bar{1}). \quad \text{as } \phi(\bar{1}) \in U_n.$$

Let $\phi_1, \phi_2 \in Aut(\mathbb{Z}_n)$ s.t. $T(\phi_1) = T(\phi_2)$

$$\Rightarrow \phi_1(\bar{1}) = \phi_2(\bar{1})$$
$$\Rightarrow k\phi_1(\bar{1}) = k\phi_2(\bar{1}) \quad \forall k \in \mathbb{Z}$$
$$\Rightarrow \phi_1(\bar{k}) = \phi_2(\bar{k})$$
$$\Rightarrow \phi_1 = \phi_2$$

$\therefore$ T is 1-1.

If $r \in U_n$, then $\gcd(r,n) = 1$, so, $\bar{r}$ can be a generator in $\mathbb{Z}_n$, so, $\exists$ an automorphism defined by

$$\phi(\bar{1}) = \bar{r}$$

i.e., $T(\phi) = \bar{r}$.

So, T is surjective.

Finally, let $\phi_1, \phi_2 \in Aut(\mathbb{Z}_n)$, then

$$T(\phi_1\phi_2) = \phi_1\phi_2(\bar{1})$$
$$= \phi_1(\phi_2(\bar{1}))$$
$$= \phi_1(\bar{s}) \quad [\text{if } \phi_2(\bar{1}) = \bar{s}]$$
$$= s\phi_1(\bar{1})$$
$$= \phi_1(\bar{1})\phi_2(\bar{1})$$
$$= T(\phi_1)T(\phi_2)$$

$\therefore$ T is a group-homomorphism. $\therefore$ $Aut(\mathbb{Z}/n\mathbb{Z}) \simeq U_n$.

Pr(8). Give an example of a subgroup of index 3 which is not normal.

Soln: Let us consider the group $G = S_3$ and $H = \{(1), (1\ 2)\} \subseteq G$.

Then H is a subgroup of G of index

$$[G : H] = \frac{|G|}{|H|} = \frac{6}{2} = 3.$$

Now, $(1\ 3) \in S_3$ but

$$(1\ 3)(1\ 2)(1\ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3)$$
$$= (2\ 3) \notin H.$$

so, H is not normal in G.

Pr(9). Show that the functions $f(x) = 1/x$ and $g(x) = (x-1)/x$ generate, under composition of functions, a group isomorphic to S_3.

Soln: The group generated by f and g is

$$\langle f, g \rangle = \{I, f, g, g^2, fg, fg^2\}$$

$f^2(x) = f\left(\frac{1}{x}\right) = x$. $\therefore f^2 = I$ $\quad \therefore |f| = 2$

$g^2(x) = g\left(\frac{x-1}{x}\right) = -\frac{1}{x-1}$ $\quad \therefore |g^2| = 3$

$g^3(x) = g\left(-\frac{1}{x-1}\right) = x$. $\therefore g^3 = I$. $\therefore |g| = 3$

$fg(x) = f\left(\frac{x-1}{x}\right) = \frac{x}{x-1}$ $\quad \therefore |fg| = 2$

$fg^2(x) = f\left(-\frac{1}{x-1}\right) = 1-x$. $\quad \therefore |fg^2| = 2$

$gf(x) = g\left(\frac{1}{x}\right) = 1-x$.

$g^2f(x) = g^2\left(\frac{1}{x}\right) = \frac{x}{x-1}$

Hence, $\langle f, g \rangle$ is a group of order 6 but it doesn't have any element of order 6. So it is not cyclic. as $fg \neq gf$, the group is non-abelian.

$\therefore \langle f, g \rangle \cong S_3$.

Pr(11). Prove that the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to the dihedral group of order 8.

Soln: $D_4 = \langle 1, x, y \mid x^2 = 1, y^4 = 1, xy = y^3x \rangle$

$= \{1, x, y, y^2, y^3, yx, y^2x, y^3x\}$

Group of upper triangular matrices in $GL_3(\mathbb{F}_2)$,

$$U = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{F}_2 \right\}$$

Now we define an isomorphism from D_4 onto U as,

$f : D_4 \longrightarrow U$

$$1 \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad y^3 \longmapsto \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$x \longmapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad yx \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$y \longmapsto \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad y^2x \longmapsto \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$y^2 \longmapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad y^3x \longmapsto \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Thus, $U \simeq D_4$.

Pr(12). Let G be an abelian group of odd order. Prove that the map $\phi : G \longrightarrow G$ defined by $\phi(g) = g^2 \ \forall g \in G$ is an automorphism.

Soln: Clearly $\phi : G \to G$ is well defined.

$\phi(g_1g_2) = (g_1g_2)^2 = g_1^2g_2^2$ [$\because G$ is abelian]

$= \phi(g_1)\phi(g_2) \ \forall g_1, g_2 \in G$.

$\therefore \phi$ is a group-homomorphism.

If $g \in G$ then, $|g|$ is odd, say $2m+1$, then $g^{m+1} \in G$

s.t $\phi(g^{m+1}) = (g^{m+1})^2 = g^{2m+1+1} = g$.

so, ϕ is surjective.

Again if $\phi(g_1) = \phi(g_2) \Rightarrow g_1^2 = g_2^2$ for some $g_1, g_2 \in G$

$\Rightarrow (g_1g_2^{-1})^2 = 1$

but $2 \nmid |G| \Rightarrow g_1g_2^{-1} = 1 \Rightarrow g_1 = g_2$.

$\therefore \phi$ is 1-1. So, ϕ is an automorphism of G.

Pr(13). Show that $GL_2(\mathbb{R})$ is not a normal subgroup of $GL_2(\mathbb{C})$.

Soln: As $GL_2(\mathbb{R}) \subseteq GL_2(\mathbb{C})$ and $GL_2(\mathbb{R})$ is itself a group, it is a subgroup of $GL_2(\mathbb{C})$.

Now, $\begin{pmatrix} 1 & 1 \\ 0 & i \end{pmatrix} \in GL_2(\mathbb{C})$ & $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$.

$$\begin{pmatrix} 1 & 1 \\ 0 & i \end{pmatrix}^{-1} = \begin{pmatrix} 1 & i \\ 0 & -i \end{pmatrix}$$

Now, $$\begin{pmatrix} 1 & 1 \\ 0 & i \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & i \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix} \notin GL_2(\mathbb{R})$$

So, $GL_2(\mathbb{R})$ is not normal in $GL_2(\mathbb{C})$.

Pr(14). Give examples of three groups $G \triangleleft H \triangleleft K$ so that G is not normal in K.

Soln: Let $K = D_4$,

$H = \{R_{0^\circ}, R_{180^\circ}, H, V\}$

$G = \{R_{0^\circ}, H\}$

Here, $[H:G] = 2$, so, $G \triangleleft H$

& $[K:H] = 2$, so $H \triangleleft K$.

but, $DHD^{-1} = V \notin G$, so, G is not normal in K.

Pr(15). Suppose H and K are subgroups of finite index in the group G with $[G:H] = m$ and $[G:K] = n$. Prove that $\text{lcm}(m,n) \leq [G : H \cap K] \leq mn$.

Deduce that if m and n are relatively prime, then $[G:H \cap K] = [G:H][G:K]$.

Soln: $\exists\ a, b \in \mathbb{Z}$ s.t $am + bn = \gcd(m,n)$.

Now as, $H \cap K \leq H$ and $H \cap K \leq K$,

we have, $|H \cap K| \mid b|H| + a|K| = b\frac{|G|}{m} + a\frac{|G|}{n}$

$$= \frac{am+bn}{mn}|G| = \frac{\gcd(m,n)}{mn}|G|$$

$$= \frac{1}{\text{lcm}(m,n)}|G|$$

$\therefore |H \cap K| \leq \frac{|G|}{\text{lcm}(m,n)}$

$\Rightarrow \text{lcm}(m,n) \leq [G : H \cap K]$ ——(1)

Again, $|G| \geq |HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{\frac{|G|}{m} \cdot \frac{|G|}{n}}{|H \cap K|}$

$\Rightarrow \frac{|G|}{|H \cap K|} \leq mn \Rightarrow [G : H \cap K] \leq mn$ — (2)

So, from (1) & (2), we have,

$$\text{lcm}(m,n) \leq [G : H \cap K] \leq mn \text{ . (Proved)}$$

Hence, if m, n are relatively prime, then from above relation,

$$\text{lcm}(m,n) = mn \leq [G : H \cap K] \leq mn .$$

$\therefore [G : H \cap K] = mn$

$= [G : H][G : K]$. (Proved)

Pr(16). Let $K < H < G$ be subgroups of a finite group G. Show that $[G : K] = [G : H][H : K]$.

Soln: Since cosets form a partition of a group, we have

$$G = \bigcup_{i \in I} g_i H \quad \& \quad H = \bigcup_{j \in J} h_j K$$

where I & J are sets of indexes s.t $|I| = [G : H]$ & $|J| = [H : K]$.

$$\Rightarrow G = \bigcup_{i \in I} \bigcup_{j \in J} h_j K = \bigcup_{(i,j) \in I \times J} g_i h_j K$$

Now we prove that this union is disjoint.

On the contrary, suppose, $g_i h_j K \cap g_{i'} h_{j'} K \neq \phi$

then $\exists\ k, k' \in K$ s.t

$$x = g_i h_j k = g_{i'} h_{j'} k'$$

Since $h_j k, h_{j'} k' \in H$, thus we have, $x \in g_i H \cap g_{i'} H \Rightarrow i = i'$ by contradiction.

$\therefore g_i h_j K = g_i h_{j'} k' \Rightarrow h_j k = h_{j'} k'$

$\Rightarrow g_i^{-1} x \in h_j K \cap h_{j'} K \neq \phi \Rightarrow j = j'$ by contradiction.

Hence, the union is disjoint.

Then $[G : K] = |I \times J| = |I| \cdot |J| = [G : H][H : K]$.

Pr(17). Prove that if H and K are finite subgroups of G whose order are relatively prime, then $H \cap K = \{1\}$.

Soln: Let $x \in H \cap K$, then $x^{|H|} = 1$ & $x^{|K|} = 1$

$\Rightarrow$ if $|x| = n$, then $n \mid |H|$ & $n \mid |K|$

$\Rightarrow n = 1$ as $|H|$ & $|K|$ are relatively prime

$\Rightarrow x = 1$.

$\Rightarrow H \cap K = \{1\}$.

Pr(18). Let $H < G$. Prove that the map $x \longmapsto x^{-1}$ sends each left coset of H in G onto a right coset of H and gives bijection between the set of left cosets and the set of right cosets of H in G.

Soln: Let, L = set of left cosets of H in G

R = set of right cosets of H in G.

We see if $H = \{h_1, h_2, h_3, \ldots\}$

then $xH = \{xh_1, xh_2, xh_3, \ldots\}$

if $\phi(x) = x^{-1}$, then,

$$\phi(xH) = \{h_1^{-1}x^{-1}, h_2^{-1}x^{-1}, h_3^{-1}x^{-1}\}$$
$$= Hx^{-1}$$

Hence, ϕ sends each left coset xH of H in G onto a right coset Hx^{-1} of H in G.

Define, $\phi : L \to R$ by $\phi(xH) = Hx^{-1}$

Let $\phi(xH) = \phi(yH)$

$\Rightarrow Hx^{-1} = Hy^{-1} \Rightarrow y^{-1}x \in H$

$\Rightarrow xH = yH$.

$\therefore \phi$ is 1-1.

given $Ha \in R$, $\exists\ a^{-1}H \in L$ s.t. $\phi(a^{-1}H) = Ha$.

$\therefore \phi$ is onto.

Hence ϕ is a bijection.

Pr(19). For $n \in \mathbb{N}$, $\phi(n) := \{j \in \mathbb{N} \mid 1 \leq j \leq n \text{ and } (j,n)=1\}$ (31) is called the Euler's phi function. Use Lagrange's theorem in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to prove Fermat's little Theorem:

if p is a prime, then $a^p \equiv a \pmod p$ $\forall\, a \in \mathbb{Z}$.

Soln: By division algorithm in $\mathbb{Z}$, $\exists\, q, r \in \mathbb{Z}$ s.t.

$$a = pq + r, \quad 0 \leq r \leq p-1.$$

Hence to prove the theorem it suffices to prove $r^p \equiv r \pmod p$.

if $r = 0$, then it holds obvious.

If $r \neq 0$, then $r \in (\mathbb{Z}/p\mathbb{Z})^\times = \{1, 2, \ldots, p-1\}$

Then by Lagrange's th.,

$$r^{p-1} \equiv 1 \pmod p$$
$$\Rightarrow r^p \equiv r \pmod p$$
$$\Rightarrow a^p \equiv a \pmod p \quad \forall\, a \in \mathbb{Z}.$$

Pr(20). Let p be a prime and n be a (+)ve integer. Find the order of $\bar{p}$ in $(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times$ and deduce that $n \mid \phi(p^n-1)$.

Soln: Let $|\bar{p}| = m$, then, $p^m \equiv 1 \pmod{p^n-1}$

$$\Rightarrow p^m - 1 \equiv 0 \pmod{p^n-1}$$
$$\Rightarrow p^n - 1 \mid p^m - 1$$
$$\Rightarrow m \geq n. \Rightarrow |\bar{p}| \geq n.$$

as, $p^n - 1 \mid p^n - 1$

$$\Rightarrow |\bar{p}| = n.$$

Also this implies, n divides $|(\mathbb{Z}/(p^n-1)\mathbb{Z})^\times|$

i.e., $n \mid \phi(p^n-1)$.

Pr(21). Use Lagrange's theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove Euler's theorem: $a^{\phi(n)} \equiv 1 \pmod n$ $\forall\, a \in \mathbb{Z}$ s.t. a is relatively prime to n.

Soln: Similar proof as (19).

3. Product and Quotient Groups

Pr(1). Let $G = H \times K$. Show that G is abelian iff both H and K are abelian.

Soln: Let $(h,k), (h',k') \in G = H \times K$ where $h, h' \in H$ & $k, k' \in K$.

Now, G is abelian

$\Leftrightarrow (h,k)(h',k') = (h',k')(h,k)$

$\Leftrightarrow (hh', kk') = (h'h, k'k)$

$\Leftrightarrow hh' = h'h$ & $kk' = k'k$

$\Leftrightarrow$ H & K are abelian.

Pr(2). Is the symmetric group S_3 a direct product of its proper subgroups?

Soln: NO.

S_3 has two proper subgroups: one of order 2, thus isomorphic to $\mathbb{Z}_2$ and another of order 3, hence isomorphic to $\mathbb{Z}_3$.

Now if S_3 were direct product of these two subgroups then,

$S_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \simeq \mathbb{Z}_6$, a contradiction to the fact that S_3 is non-abelian.

Pr(3). Prove that the direct product of two infinite cyclic groups is not cyclic.

Soln: Any infinite cyclic group is isomorphic to the group $(\mathbb{Z}, +)$.

Hence we need to show $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

If possible, let $\mathbb{Z} \times \mathbb{Z}$ be cyclic.

Then $\exists\ (a,b) \in \mathbb{Z} \times \mathbb{Z}$ s.t $\mathbb{Z} \times \mathbb{Z} = \langle (a,b) \rangle$

But $(na+1, nb) \notin \langle (a,b) \rangle = \mathbb{Z} \times \mathbb{Z}$, which is a contradiction.

Thus, $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

Pr(4). Prove that if $G/Z(G)$ is cyclic, then G is abelian.

Soln: Let $G/Z(G)$ be cyclic.

Then, $\exists\ gZ(G) \in G/Z(G)$ s.t $G/Z(G) = \langle gZ(G) \rangle$

Let $a, b \in G$

then, $aZ(G) = (gZ(G))^i = g^iZ(G)$

and $bZ(G) = (gZ(G))^j = g^jZ(G)$ for some $i, j \in \mathbb{Z}$

Then for some $x, y \in Z(G)$,

$$a = g^i x \text{ and } b = g^j y.$$

$$\Rightarrow ab = g^i x g^j y = g^j g^i x y \quad (\because xy \in Z(G))$$

$$= ba$$

Hence $ab = ba\ \forall\ a, b \in G \Rightarrow G$ is abelian.

Pr(5). Let a group G contain normal subgroups of order 3 and 5. Show that G has an element of order 15.

Soln: Let H and K be two normal subgroups of G of order 3 and 5 respectively.

Let $x \in H \cap K \Rightarrow |x| \mid 3$ and $|x| \mid 5 \Rightarrow |x| = 1 \Rightarrow x = 1$.

$\therefore H \cap K = \{1\}$.

Let $a \in H$ & $b \in K$, then,

$aba^{-1}b^{-1} \in H$ [as $H \trianglelefteq G$, $ba^{-1}b^{-1}, a \in H$]

$aba^{-1}b^{-1} \in K$ [as $K \trianglelefteq G$, $aba^{-1}, b^{-1} \in K$]

$\Rightarrow aba^{-1}b^{-1} \in H \cap K = \{1\} \Rightarrow ab = ba\ \forall a \in H$ & $\forall b \in K$.

Now as 3 and 5 are prime divisors of $|H|$ & $|K|$ respectively, H and K have elements of order 3 and 5 resp.

Let $x \in H$ s.t $|x| = 3$ & $y \in K$ s.t $|y| = 5$.

Then $xy = yx$ and hence $|xy| = \text{lcm}(3, 5)$

$= 15$.

$\therefore xy \in G$ s.t $|xy| = 15$.

Pr(6). Let G be a group of order ab where G has two subgroups H and K of order a and b resp. Show that if $H \cap K = \{1\}$, then $G = HK$. Is G isomorphic to $H \times K$?

Soln: As H and K are subgroups of G, we have,

$$HK \subseteq G.$$

Again, $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{a.b}{1} = ab = |G|$.

Hence, $G = HK$.

But G need not be equal to $H \times K$.

For example consider $G = S_3$, $H = \{(1), (1\,2)\}$, $K = \{(1), (1\,2\,3), (1\,3\,2)\}$.

then H and K have all the above properties but $G \neq H \times K$.

Pr(7). Show that $H = \{A \in GL_n(\mathbb{R}) \mid \det A > 0\}$ is a normal subgroup of $GL_n(\mathbb{R})$. Describe the quotient group.

Soln: Clearly H is nonempty as $I_{n \times n} \in H$.

If $A, B \in H$, then $\det(A), \det(B) > 0$.

so, $\det(AB^{-1}) = \frac{\det A}{\det B} > 0$.

$\Rightarrow AB^{-1} \in H$

Hence, H is a subgroup of $GL_n(\mathbb{R})$.

If $M \in GL_n(\mathbb{R})$, $A \in H$, then,

$$\det(MAM^{-1}) = \det(M).\det(A).\frac{1}{\det(M)}$$

$$= \det(A) > 0.$$

$\Rightarrow MAM^{-1} \in H$.

Hence, H is a normal subgroup of $GL_n(\mathbb{R})$.

The quotient group $GL_n(\mathbb{R})/H$ contains two elements, say H and K, where,

$$K = \{A \in GL_n(\mathbb{R}) \mid \det A < 0\}$$

Thus, $GL_n(\mathbb{R})/H \cong \mathbb{Z}_2$.

Pr. (8) Let G be group.

Prove that $N = \{x^{-1}y^{-1}xy \mid x, y \in G\}$ is a normal subgroup of G and G/N is abelian.

(N is called the COMMUTATOR SUBGROUP of G)

Soln: Clearly N is non-empty as $1 = 1^{-1}1^{-1}1.1 \in N$.

denote $x_1^{-1}y_1^{-1}x_1y_1$ by s_1

then if $h_1, h_2 \in N$, then

$h_1 = s_1 s_2 \cdots s_m$
$h_2 = s_i s_{i+1} \cdots s_k$ for some, $m, i, k \in \mathbb{N}$.

Then, $h_1 h_2^{-1} = (s_1 s_2 \cdots s_m)(s_i s_{i+1} \cdots s_k)^{-1}$

$= s_1 s_2 \cdots s_m s_k^{-1} \cdots s_i^{-1}$

$\in N$ as, $s_i^{-1} = (x_i^{-1}y_i^{-1}x_iy_i)^{-1}$

$= y_i^{-1}x_i^{-1}y_ix_i \in N$.

Hence, N is a subgroup of G.

Now if $g \in G$, $h \in N$, then, $[h = s_1 s_2 \cdots s_m]$

$ghg^{-1} = g(s_1 \cdots s_m)g^{-1}$

$= (gs_1g^{-1})(gs_2g^{-1}) \cdots (gs_mg^{-1})$

Now, $gs_ig^{-1} = gx_i^{-1}y_i^{-1}x_iy_ig^{-1}$

$= (gx_i^{-1}g^{-1})(gy_i^{-1}g^{-1})(gx_ig^{-1})(gy_ig^{-1})$

$= (gx_ig^{-1})^{-1}(gy_ig^{-1})^{-1}(gx_ig^{-1})(gy_ig^{-1}) \in N$.

$\Rightarrow ghg^{-1} \in N$. $\forall h \in N$ & $\forall g \in G$.

$\Rightarrow N$ is a normal subgroup of G.

So, G/N is well-defined.

Now, given $a, b \in G$,

$aba^{-1}b^{-1} \in N$

$\Rightarrow (ab)(ba)^{-1} \in N$

$\Rightarrow (ab)N = (ba)N$

$\Rightarrow aN.bN = bN.aN$

Hence, G/N is abelian.

Pr(9). Let M and N be normal subgroups of a group G such that $G = MN$. Prove that;

$$G/(M \cap N) \cong G/M \times G/N.$$

Soln: Define $\phi : G \longrightarrow G/M \times G/N$

by $g \longmapsto (gM, gN)$ $[\because G = MN]$

Clearly, ϕ is well-defined.

ϕ is homomorphism

$$\phi(g_1g_2) = (g_1g_2M, g_1g_2N)$$
$$= (g_1M, g_1N)(g_2M, g_2N)$$
$$= \phi(g_1)\phi(g_2) \quad \forall\, g_1, g_2 \in G.$$

ϕ is surjective.

Let $(xM, yN) \in G/M \times G/N$.

as $G = MN$, $x \in G$, so, $x = mn$ for some $m \in M$, $n \in N$.

$\therefore xM = mnM = n(n^{-1}mn)M$

$= nM$ [as $n^{-1}mn \in M$ as $M \trianglelefteq G$]

Similarly $y \in G$, so $y = m'n'$ for some $m' \in M$, $n' \in N$.

$\therefore yN = m'n'N = m'N$.

Consider, $\phi(m'n') = (m'nM, m'nN)$

$= (n(n^{-1}m'n)M, m'N)$

$= (nM, m'N) = (xM, yN)$

$$\ker \varphi = \{ g \in G \mid (gM, gN) = (M, N) \}$$
$$= \{ g \in G \mid gM = M,\ gN = N \}$$
$$= \{ g \in G \mid g \in M,\ g \in N \}$$
$$= M \cap N.$$

Therefore $(M \cap N) \triangle G$ and, by 1st Isomorphism th,

$$G/(M \cap N) \cong G/M \times G/N.$$

Pr(10). Show that, $Z(G \times H) = Z(G) \times Z(H)$.

Soln: $(m, n) \in Z(G \times H)$

$\Leftrightarrow (m, n)(g, h) = (g, h)(m, n) \quad \forall (g, h) \in G \times H.$

$\Leftrightarrow (mg, nh) = (gm, hn) \quad \forall g \in G \ \& \ h \in H.$

$\Leftrightarrow mg = gm \ \& \ nh = hn \quad \forall g \in G \ \& \ h \in H$

$\Leftrightarrow m \in Z(G) \ \& \ n \in Z(H)$

$\Leftrightarrow (m, n) \in Z(G) \times Z(H)$

$\therefore Z(G \times H) = Z(G) \times Z(H).$

Pr(11). Show that any normal subgroup of G of order 2 is contained in the centre of G.

Soln: Let $H = \{1, x\}$ be any normal subgroup of G of order 2.

Then, $|x| = 2$, i.e., $x = x^{-1} \neq 1$.

Now, as $H \triangle G$, $\forall g \in G$, $gxg^{-1} \in H$.

if $gxg^{-1} = 1$, then $x = 1$, a contradiction.

So, $gxg^{-1} = x \Rightarrow gx = xg \ \forall g \in G \Rightarrow x \in Z(G)$.

also, $1 \in Z(G)$ trivially.

Hence, $H \subseteq Z(G)$.

Pr(12). Show that the multiplicative group of non-zero complex numbers is isomorphic to the direct product of $(\mathbb{R}^{\times}_{>0}, \cdot)$ and $(\mathbb{R}/\mathbb{Z}, +)$.

Soln: Consider $\varphi : \mathbb{C}^{\times}_{\neq 0} \longrightarrow (\mathbb{R}^{\times}_{>0}, \cdot) \times (\mathbb{R}/\mathbb{Z}, +)$ defined by

$$z = re^{2\pi\theta i} \longmapsto (r, \theta + \mathbb{Z})$$

Clearly φ is well-defined and surjective.

$$\ker \varphi = \{ z = re^{i2\pi\theta} \in \mathbb{C}\setminus\{0\} \mid (r, \theta+\mathbb{Z}) = (1, \mathbb{Z}) \}$$

$$= \{ z = re^{i2\pi\theta} \in \mathbb{C}\setminus\{0\} \mid r = 1, \theta \in \mathbb{Z} \}$$

$$= \{ z = 1 \} = \{1\}.$$

Hence φ is 1-1.

Now, $\varphi(z_1 \cdot z_2) = \varphi(r_1 e^{i2\pi\theta_1} \cdot r_2 e^{i2\pi\theta_2})$

$$= \varphi(r_1 r_2 e^{i2\pi(\theta_1+\theta_2)})$$

$$= (r_1 r_2, \theta_1 + \theta_2 + \mathbb{Z})$$

$$= (r_1, \theta_1 + \mathbb{Z}) \times (r_2, \theta_2 + \mathbb{Z})$$

$$= \varphi(z_1)\varphi(z_2)$$

$\therefore$ φ is a group-homomorphism.

Hence, $\mathbb{C}\setminus\{0\} \simeq (\mathbb{R}^+_{>0}, \cdot) \times (\mathbb{R}/\mathbb{Z}, +)$.

Pr(1). Prove or disprove: An abelian group is simple, if it has prime order.

Soln: A group that has prime order, is cyclic and hence abelian. Now it has only subgroups $\{1\}$ and itself the group, say G [as 1 & p are the only divisors of a prime p]. Now both the subgroups are normal as G is abelian but both are ~~improper~~ trivial.

Hence, G has no non-trivial proper subgroup. Consequently, G is ~~not~~ simple.

Pr(2). Prove that a group of prime power order is not simple.

Soln: We know, for any group of prime power order, i.e. if $|G| = p^n$ for some prime p and some $n \in \mathbb{Z}^+$, then $Z(G)$, centre of the group G, is a normal subgroup of G s.t

$$|Z(G)| \geq p.$$

Now if G is non-abelian, then $Z(G)$ is a normal proper subgroup of G, hence G is not simple.

On the other hand, if G is abelian, then since $p \mid |G|$, G has a subgroup H of order p, which again is normal in G as G is abelian. So, then also, G is not simple.

Pr(3). Determine the class eqⁿ for each of the following groups:

(a) Q_8 (b) The Klein 4-group (K_4)

(c) the dihedral group D_4 (d) The group of upper triangular matrices in $GL_2(\mathbb{F}_2)$

(e) S_5.

Soln: (a) Quaternion Group:

We have $Z(Q_8) = \{1, -1\}$, thus, $O(1) = \{1\}$ & $O(-1) = \{-1\}$.

Also as $(-x)y(-x)^{-1} = xyx^{-1}$ $\forall x, y \in Q_8$, we find $O(i) = \{i, -i\}$, $O(j) = \{j, -j\}$ & $O(k) = \{k, -k\}$.

Hence, class eqn is,

$|Q_8| = 1+1+2+2+2$

i.e., $8 = 1+1+2+2+2$.

(b) The Klein's 4-group:

Since, K_4 is abelian, hence, $|K_4| = |Z(K_4)| = 4$

Hence, class eqn is,

$4 = 1+1+1+1$.

(c) The dihedral group D_4:

$D_4 = \langle x, y \mid |x| = 4, |y| = 2, xy = yx^3 \rangle$

$= \{1, x, x^2, x^3, y, yx, yx^2, yx^3\}$

We see, $Z(D_4) = \{1, x^2\}$, so $O(1) = \{1\}$ & $O(x^2) = \{x^2\}$

$O(x) = \{x, x^3\} = O(x^3)$, $O(y) = \{y, yx^2\} = O(yx^2)$,

$O(yx) = \{yx, yx^3\} = O(yx^3)$.

Hence, the class eqn is,

$8 = 1+1+2+2+2$.

(d) The group of upper triangular matrices in $GL_2(\mathbb{F}_3)$:

(e) Symmetric group S_5:

Cycle type	An elt of that type	Conjugate elements	$\lvert C(\sigma)\rvert$
$1+1+1+1+1$	(1)	(1)	1
$1+1+1+2$	$(1\,2)$	10 elements	10
$1+1+3$	$(1\,2\,3)$	20 3-cycles	20

Cycle type	An elt of that type	Conjugate elts	$\lvert Z(\sigma)\rvert$
1+4	(1 2 3 4)	30 4-cycles	30
1+2+2	(1 2)(3 4)	15 elements	15
2+3	(1 2)(3 4 5)	20 elements	20
5	(1 2 3 4 5)	24 5-cycles	24.

$\therefore$ Class eqn of S_5,

$$120 = |S_5| = 1 + 10 + 20 + 30 + 15 + 20 + 24$$
$$= |Z(S_5)| + 10 + 15 + 20 + 20 + 24 + 30$$
$$\text{as } Z(S_5) = \{(1)\}.$$

Prob(4). Determine all groups having atmost three conjugacy classes.

Soln: Case-1: Let, G has only one conjugacy class, then $G = \{1\}$.

Case-2: Let, G has two conjugacy classes, $\therefore |G| = 1 + x$,

Also $x \mid |G| = 1 + x \Rightarrow x \mid 1 \Rightarrow x = 1$.

$\therefore |G| = 2 \Rightarrow G \cong \mathbb{Z}/2\mathbb{Z}$.

Case-3: Let, G has three conjugacy classes, $\therefore |G| = 1 + x + y$

Now, $x \mid |G|$ & $x \mid |G| - x = 1 + y$

Similarly $y \mid 1 + x$.

$\therefore x \leq 1 + y \leq 2 + x$

$\therefore y = x$ or $y = 1 + x$.

Subcase-3a: $y = x \Rightarrow x \mid 1 + x \Rightarrow x = 1 = y$

$\therefore |G| = 3 \therefore G \cong \mathbb{Z}/3\mathbb{Z}$

Subcase-3b: $y = 1 + x \Rightarrow x \mid 2 + x \Rightarrow x \mid 2 \Rightarrow x = 1$ or 2.

If $x = 1$, then $y = 2$, $\therefore |G| = 1 + 1 + 2 = 4 \Rightarrow G \cong \mathbb{Z}/4\mathbb{Z}$ or V_4, i.e G is abelian, then $y = 2$ is not possible.

So $x = 2$ $\therefore y = 1 + 2 = 3$.

$\therefore |G| = 1 + 2 + 3 = 6$

The only non-abelian group of order 6, having three conjugacy classes in S_3. $\therefore G \cong S_3$.

Pr(5). Let N be a normal subgroup of a group G. Suppose $|N| = 5$ and $|G|$ is odd. Prove that

$$N \subseteq Z(G).$$

Soln: Since $N \triangleleft G$, $gng^{-1} \in N$, i.e G acts on N by conjugation. $\therefore \delta_g \in Aut(N)$ where $\delta_g(n) = gng^{-1}$

Define automorphism, $f: G \longrightarrow Aut(N)$

by $g \longmapsto \delta_g$

$U_5 \cong \mathbb{Z}_4$

Now $Aut(N) \cong Aut(\mathbb{Z}_5) \cong$ & image (f) is a subgroup of $Aut(N)$ s.t $|image(f)| = |G|$ is odd.

$\Rightarrow |image(f)| = 1 \Rightarrow image(f) =$ Identity map.

$\Rightarrow \delta_g = Id \ \forall \ g \in G$

$\Rightarrow \delta_g(n) = n \ \forall \ g \in G$

$\Rightarrow gng^{-1} = n \ \forall \ g \in G \Rightarrow gn = ng \ \forall \ g \in G$

$\Rightarrow n \in Z(G)$.

Hence, $N \subseteq Z(G)$.

Pr(6). Let G be a finite group with a proper subgroup H whose index is the smallest prime number p dividing $|G|$. Show that $H \triangleleft G$.

Soln: Here G acts on the set of left cosets of H, $\{gH \mid g \in G\}$ by left multiplication,

$$x \cdot (gH) = xgH$$

This action induces a homomorphism from $G \to S_p$ whose kernel in contained in H.

[$x \in K \Rightarrow xaH = aH \ \forall \ aH$ in the set of left cosets of H. in particular $xH = H$, so $x \in H$. $\Rightarrow$ $K \subset H$]

Then G/K is isomorphic to a subgroup of S_p, so has order dividing $p!$. But it must also have order dividing $|G|$, and since p is the smallest prime divisor of $|G|$, thus $|G/K| = p$

Now, $|G/K| = [G:K] = [G:H][H:K] = p[H:K]$

$\Rightarrow p = p[H:K] \Rightarrow [H:K] = 1$

$\Rightarrow H = K.$

Since, K is normal in G, H is normal in G.

Pr.(7). Let G be a group of order $2m$ where m is odd. Show that G has a normal subgroup of index 2.

Soln:

Pr(8). Find the no of sylow-p-subgroups of S_p where p is a prime number. Hence deduce Wilson's theorem in number theory:

p divides $(p-1)! + 1$.

Soln: Since $p \mid |S_p| = p!$ but $p^2 \nmid p!$,

any sylow p-subgroup of S_p has order p, hence it is cyclic and has $(p-1)$ elements of order p.

Now in S_p, any element of order p is p-cycle, thus no of such elements is $\frac{p!}{p \cdot 0!} = (p-1)!$

Since any two cyclic subgroups of order p intersect trivially, we have, no of p-sylow p-subgroups

$$= \frac{(p-1)!}{(p-1)}$$

$$= (p-2)!$$

Hence, according to sylow's theorem,

$$n_p \equiv 1 \pmod p \quad \& \quad n_p = (p-2)!$$

$$\therefore (p-2)! \equiv 1 \pmod p$$

$$\Rightarrow (p-1)! + 1 \equiv (p-1) \cdot 1 + 1 \pmod p$$

$$\equiv p \pmod p$$

$$\equiv 0 \pmod p$$

$\therefore$ p divides $(p-1)! + 1$.

Pr(9). Let G be a group of order $p^\alpha m$ s.t $p \nmid m$. Then G has a unique sylow p-subgroup P if and only if P is normal in G.

Soln: Let $g \in G$, then gPg^{-1} is also a subgroup of order p^α, same as $|P|$.

but if P is unique, we have $gPg^{-1} = P \quad \forall g \in G$.

hence, $P \trianglelefteq G$.

Conversely, Let P be normal in G.

Let Q be another sylow p-subgroup in G.

Then, $gQg^{-1} \subseteq P = gPg^{-1} \quad \forall g \in G$

$\Rightarrow Q \subseteq P$ and $|Q| = |P|$

$\Rightarrow Q = P$.

Hence, P is unique.

Pr(10). How many elements of order 5 are there in a group of order 20?

Soln: By Sylow's theorem,

n_5 = no of 5-order subgroups (5-sylow subgroup)

$\equiv 1 \pmod 5$ & $n_5 \mid 4$

$\Rightarrow n_5 = 1$.

Hence, no of elements of order 5 in a group of order 20 is $\phi(5) = 4$.

Pr(11). Show that a group of order 30 is not simple.

Soln: $30 = 2 \cdot 3 \cdot 5$

By sylow's theorem,

no of sylow 5-subgroups (order 5) $= n_5 \equiv 1 \pmod 5$

& $n_5 \mid 6$

$\therefore n_5 = 1$ or 6.

Similarly $n_3 \equiv 1 \pmod 3$ & $n_3 \mid 10 \Rightarrow n_3 = 1$ or 10.

& $n_2 \equiv 1 \pmod 2$ & $n_2 \mid 15 \Rightarrow n_2 = 1, 3, 5$ or 15.

Now, if any one of n_5, n_3 or n_2 is 1, then that sylow subgroup is unique & hence normal, so G becomes non-simple.

Now, let $n_5 = 6$ & $n_3 = 10$.

Then as any cyclic subgroup of order 5 & 3 intersect trivially, G would have 24 elements of order 5 & 20 elements of order 3 but $24 + 20 > 30$.

hence, any one of n_5 or n_3 is 1,

consequently, G becomes non-simple.

Hence, any group of order 30 is not simple.

Ex(12). Classify group of order 8.

Soln: Let G be a group of order 8.

Case 1: Let G have an element of order 8, then G is cyclic, so,

$$G \cong \mathbb{Z}/8\mathbb{Z}$$

Case 2: Suppose G has no element of order 8, hence by Lagrange's theorem, every non-identity element of G has order 2 or 4.

Suppose G has no element of order 4, i.e., every non-identity element in G is of order 2.

$\therefore$ if $x \in G$ then $x^2 = 1 \Rightarrow x = x^{-1}$

$\therefore F: G \to G$ defined by $F(x) = x^{-1}$ is actually the identity map, hence an isomorphism. This implies G is abelian.

Choose $a, b \in G$ and choose $c \in G$ distinct from $1, a, b$ & ab.

Then, $G = \langle a, b, c \mid a^2 = b^2 = c^2 = 1, ab = ba, ac = ca, bc = cb \rangle$

Then, $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 3: Suppose $a \in G$ has order 4.

Define $H = \langle a \rangle = \{1, a, a^2, a^3\}$

Choose $b \in G \setminus H$, then $H \neq Hb$

$\therefore$, $G = H \cup Hb = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$

This is true for any choice of $b \in G \setminus H$.

Furthermore, $ab \neq ba$ and $ab \notin \langle a \rangle$ as $b \notin \langle a \rangle$.

Subcase-3a: Let $|b| = 2$.

Then $ba \neq a^2b$, otherwise

$ba^2b = baab = a^2bab = a^2a^2bb = 1$

& $a = 1 \cdot a = b^2a = b \cdot ba = ba^2b = 1$, contradiction

so either $ba = ab$ or $ba = a^3b$.

Subsubcase 3ai:

If $ba = ab$, then G is abelian.

Then $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Subsubcase 3aii:

If $ba = a^3b$, then $G = \langle a, b \mid a^4 = 1, b^2 = 1, ba = a^3b \rangle$
$\cong D_4$

Subcase-3b:

Suppose every element of $G \setminus H$ has order 4.

Then $|b| = 4$ & $|b^2| = 2$

$\therefore b^2 \in \langle a \rangle = H \Rightarrow b^2 = a^2$, as a^2 is the only element in $\langle a \rangle$ of order 2.

$ba \neq ab$, otherwise,

$(a^3b)^2 = a^3ba^3b = a^6b^2 = a^2b^2 = a^4 = 1$,
contradicts the fact that $|a^3b| = 4$

$ba \neq a^2b$, otherwise,

$ba = a^2b = b^2.b = b^3 \Rightarrow a = b^2$,
contradiction as $|a| = 4$ & $|b^2| = 2$

$\therefore G = \langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, ba = a^3b \rangle$
$\cong Q_8$.

Hence there are five isomorphic classes of group of order 8,

$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,
D_4, Q_8.

Pr(13) Show that the subgroup of strictly upper triangular matrices in $GL_n(\mathbb{F}_p)$ is a sylow p-subgroup.

Soln: $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$
$= p.p^2.p^3 \cdots p^{n-1}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$
$= p^{n(n-1)/2} . m$

Where $m = (p^n - 1)(p^{n-1} - 1) \cdots (p - 1)$

as $p \nmid (p^n - 1), p \nmid (p^{n-1} - 1), \ldots, p \nmid (p - 1)$, $\Rightarrow p \nmid m$.

Now if H be the mentioned subgroup, then $|H| = p^{\frac{n(n-1)}{2}}$

$\therefore H$ is a sylow p-subgroup.

Pr(14). Show that the number of sylow p-subgroups of $GL_2(\mathbb{F}_p)$ is $p+1$.

Soln: $|GL_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$

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

$\therefore$ Any p-sylow subgroup of G has order p.

Now, $n_p \equiv 1 \pmod p$ & $n_p \mid (p-1)^2(p+1)$

$\therefore n_p = 1,\ p+1,\ (p-1)^2$ or $(p+1)(p-1)^2$

~~Now let $n_p = 1$, then G has a unique (hence normal) sylow p-subgroup, say H.~~

~~Let $b \in G \setminus H$.~~

~~So there are $\{p(p-1)(p^2-1) - p\} = p(p^3-p^2-p)$ distinct choices of such b but~~

~~$bhb^{-1} \in H\ \forall h \in H$.~~

~~& $|bHb^{-1}| \le p$~~

~~Now if $b, b' \in G \setminus H$ & [illegible], then~~

Now, consider the element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ which is of order p and generates a sylow p-subgroup P. Its transpose is also of order p, so $n_p \neq 1$.

$H = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$

Now if $a, d \neq 0$, then,

$$\frac{1}{ad}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & ad^{-1} \\ 0 & 1 \end{pmatrix}$$

whence every such $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is in the normalizer $N_p(H)$. There are $p(p-1)^2$ such elements.

So, $n_p = [G : N_p(H)]$

$= \dfrac{p(p-1)^2(p+1)}{p(p-1)^2}$

$= p+1$.

$\therefore$ no of sylow p-subgroups of $GL_2(\mathbb{F}_p)$ is $(p+1)$.

Pr (15). Prove that group of order pq are not simple where p, q are prime numbers.

Soln: as $p \mid pq$ & $q \mid pq$,

if G be the group of order pq, then G has elements of order p & q, consequently subgroups of order p & q.

Now, $n_p \equiv 1 \pmod{p}$ & $n_p \mid q$.
$n_q \equiv 1 \pmod{q}$ & $n_q \mid p$.

Now if $p < q$, then, $n_q = 1$, hence G has a unique subgroup of order q, hence it is normal in G, hence G is not simple.

else if, $p = q$, then $|G| = p^2$, so G is abelian & hence G is not simple,

else, $p > q$, then $n_p = 1$, hence G has a unique subgroup of order p, hence it is normal in G, hence G is not simple.

Pr (16). Classify group of order 55.

Soln: Let G be a group of order $55 = 5 \cdot 11$.

as 5 and 11 are prime divisors of $|G|$, G has subgroups of order 5 & 11.

Say $H \leq G$ & $K \leq G$ s.t $|H| = 5$, $|K| = 11$.

By sylow's theorem,

$n_5 \equiv 1 \pmod{5}$ & $n_5 \mid 11$ $\quad \therefore n_5 = 1$ or 11
$n_{11} \equiv 1 \pmod{11}$ & $n_{11} \mid 5$ $\quad \therefore n_{11} = 1$.

$\therefore K \triangleleft G$.

Case-1: $n_5 = 1 \Rightarrow H$ is the unique 5-order subgroup of G.
$\Rightarrow H \triangleleft G$.

Also $H \cap K = \{1\}$. and also $G = HK$ as $|HK| = 55 = |G|$.

that implies $G \cong H \times K$.
$\cong \mathbb{Z}_5 \times \mathbb{Z}_{11}$
$\therefore G \cong \mathbb{Z}_{55}$.

Case-2: $n_5 = 11$.

Now if $y \in H$ & $x \in K$, then

$yxy^{-1} = x^r$, $r < 11$, $r \neq 0$, otherwise $x = 1$, contradiction

Now, $y^5xy^{-5} = x^{r^5} \Rightarrow x^{r^5-1} = 1$

$\Rightarrow 11 \mid r^5 - 1$

$\Rightarrow r = 1, 3, 4, 5$ or 9.

but if $r = 1$, then $yxy^{-1}x^{-1} = 1$

then G becomes abelian, so H becomes normal, a contradiction.

Now if $r = 3$, then $yxy^{-1} = x^3$

then $G = \langle x, y \mid x^{11} = 1, y^5 = 1, yx = x^3y \rangle$

if $r = 4$, then $yxy^{-1} = x^4$

$\Rightarrow y^3xy^{-3} = x^{64} = x^9$

also $yxy^{-1} = x^3 \Rightarrow y^2xy^{-2} = x^9$ and $\langle y^2 \rangle = \langle y^3 \rangle$ so they are same groups.

if $r = 5$, then $yxy^{-1} = x^5$

$\Rightarrow y^2xy^{-2} = x^{25} = x^3$

again $\langle y^4 \rangle = \langle y^2 \rangle$

so they are same group.

Again if $r = 9$, then $yxy^{-1} = x^9$

also $\langle y \rangle = \langle y^2 \rangle$

so they are also same group.

Hence, upto isomorphism, there are only two groups of order 55 —

(i) $\mathbb{Z}/55\mathbb{Z}$

(ii) $G = \langle x, y \mid x^{11} = 1, y^5 = 1, yx = x^3y \rangle$.

5. Structure Theorem For Finitely Generated Abelian Groups

Pr (1) How many number of non-isomorphic abelian groups are there of order 320? Write down the invariant decomposition and also the elementary decomposition for each of the groups.

Soln: $320 = 2^6 . 5$.

So, number of non-isomorphic abelian groups of order

$320 = P(6) . P(1)$

$= 11 . 1$

$= 11$.

$G = \{1+1+1+1+1+1, 1+1+1+1+2, 1+1+2+2, 1+3+2, 2+2+2, 1+1+1+3, 3+3, 1+1+4, 2+4, 1+5, 6\}$

Hence the non-isomorphic abelian groups of order 320 are,

Elementary decomp.		Invariant decomp.
(i) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{10} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
(ii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{20} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
(iii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{20} \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
(iv) $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{20} \times \mathbb{Z}_4 \times \mathbb{Z}_4$
(v) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{40} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
(vi) $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{40} \times \mathbb{Z}_4 \times \mathbb{Z}_2$
(vii) $\mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{40} \times \mathbb{Z}_8$
(viii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{16} \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{80} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
(ix) $\mathbb{Z}_4 \times \mathbb{Z}_{16} \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{80} \times \mathbb{Z}_4$
(x) $\mathbb{Z}_2 \times \mathbb{Z}_{32} \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{160} \times \mathbb{Z}_2$
(xi) $\mathbb{Z}_{64} \times \mathbb{Z}_5$	$\cong$	$\mathbb{Z}_{320}$

Pr(2). Let G and H be finite groups. Let $|g| = m$ for $g \in G$ and $|h| = n$ for $h \in H$. Then prove that $|(g,h)| = \text{lcm}(m,n)$ for $(g,h) \in G \times H$.

Soln: Let, $|(g,h)| = d$

$\Rightarrow (g,h)^d = (1_G, 1_H)$

$\Rightarrow (g^d, h^d) = (1_G, 1_H)$

$\Rightarrow g^d = 1_G$ & $h^d = 1_H$.

$\Rightarrow |g| = m \mid d$ & $|h| = n \mid d$.

Then d is a common multiple of m & n.

$\therefore |(g,h)| = \min\{d \mid m \& n \text{ both divides } d\}$

$= \text{lcm}(m,n)$.

Pr(3). Which pair of abelian groups are isomorphic from the list below:

$\{4, 18\}, \{12, 6\}, \{72\}, \{36, 2\}$.

Soln: $\{4,18\} = \mathbb{Z}_4 \times \mathbb{Z}_{18} \cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_2 \cong \mathbb{Z}_{36} \times \mathbb{Z}_2$

$\{12,6\} = \mathbb{Z}_{12} \times \mathbb{Z}_6 = \{36,2\}$.

$\{72\} = \mathbb{Z}_{72}$, $\{36,2\} = \mathbb{Z}_{36} \times \mathbb{Z}_2$

$\therefore \{4,18\}$ & $\{36,2\}$ are isomorphic.

Pr(4). Let G be a finite abelian group with invariant factor type $(n_1, n_2, \ldots, n_t)$. Prove that G contains an element of order m if $m \mid n_1$.

Soln: $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t}$

Since $\mathbb{Z}_{n_1}$ is cyclic group of order n_1 & $m \mid n_1$, $\exists$ an element $x \in \mathbb{Z}_{n_1}$ s.t $|x| = m$.

Then, $(x, 0, 0, \ldots, 0) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_t} = G$

s.t $|(x,0,0,\ldots,0)| = \text{lcm}(m, 1, 1, \ldots, 1) = m$.

Pr(5). Suppose that G is a finite abelian group that has exactly one subgroup for each divisor of $|G|$. Show that G is cyclic.

Soln: On the contrary, let G is not cyclic.

Then G has invariant-factor decomposition

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}, \text{ for some } s \in \mathbb{N}.$$

Now, let $p \mid n_2 \Rightarrow p \mid n_1$, p is prime.

$\Rightarrow \mathbb{Z}_{n_1}$ & $\mathbb{Z}_{n_2}$ have elements of order p, say x & y respectively,

i.e, $x \in \mathbb{Z}_{n_1}$ s.t $|x| = p$
& $y \in \mathbb{Z}_{n_2}$ s.t $|y| = p$.

Then $(x,0,0,\ldots,0) \in G$ & $(0,y,0,\ldots,0) \in G$ s.t $|(x,0,0,\ldots,0)| = p$
& $|(0,y,0,\ldots,0)| = p$.

Then $\langle (x,0,0,\ldots,0) \rangle$ & $\langle (0,y,0,\ldots,0) \rangle$ are subgroups of order p of G with

$$\langle (x,0,0,\ldots,0) \rangle \neq \langle (0,y,0,\ldots,0) \rangle$$

— which is a contradiction.

Hence, G is cyclic.

6. RING, IDEAL

Pr(1) Describe the group of units in $\mathbb{R}[x]$, $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}[i]$.

Soln: Let $f(x) \in \mathbb{R}[x]$ be unit.

Then $\exists\ g(x) \in \mathbb{R}[x]$ s.t $f(x)g(x) = 1$

but degree (fg) = degree (f) + degree (g)

So, $fg = 1 \Rightarrow \deg(f) + \deg(g) = \deg(1)$

$= 0$

$\Rightarrow \deg(f) = 0$ & $f \neq 0$.

So, units are constant non-zero polynomials in $\mathbb{R}[x]$ which form the group, $(\mathbb{R}^\times, \cdot)$

Units in $\mathbb{Z}/n\mathbb{Z}$ are $\bar{m}$ s.t $\gcd(m,n) = 1$ $\therefore$ group $= U_n$.

Let $a+bi \in \mathbb{Z}[i]$, (i.e, $a, b \in \mathbb{Z}$) is a unit.

$\Rightarrow \exists\ c+di \in \mathbb{Z}[i]$ s.t

$$(a+bi)(c+di) = 1$$

$$\Rightarrow (ac - bd) + i(ad + bc) = 1$$

$\therefore$ $ac - bd = 1$, $a, b, c, d \in \mathbb{Z}$.
$ad + bc = 0$

Now, $(ac-bd)^2 + (ad+bc)^2 = 1$

$\Rightarrow a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = 1$

$\Rightarrow (a^2+b^2)(c^2+d^2) = 1$

$\Rightarrow a^2 + b^2 = 1$ & $c^2 + d^2 = 1$

$\therefore$ $a = \pm 1$, $b = 0$ or $a = 0$, $b = \pm 1$,

$\therefore$ the units are $\pm 1, \pm i$. $\therefore$ Group $\cong \mathbb{Z}_4$.

Pr(2). An element a of a ring R is called nilponent if $a^n = 0$ for some $n \in \mathbb{N}$. Show that if u is a unit and a is nilpotent in R then $u+a$ is a unit.

Soln: u is a unit $\Rightarrow \exists\ v \in R$ s.t $uv = 1$

a is a nilpotent $\Rightarrow \exists\ m \in \mathbb{N}$ s.t $a^m = 0$

$\Rightarrow a^n = 0\ \forall\ n \geq m$.

Now as $a \in R, v \in R$, $v(1 - av + a^2v^2 - a^3v^3 + \cdots + (-1)^{m-1} a^{m-1} v^{m-1}$

Also, $(u+a).v(1-av+a^2v^2-a^3v^3+\cdots\cdots-(-1)^m a^{m-1}v^{m-1})$

$= (u+a).v(1-av+a^2v^2-a^3v^3+\cdots\cdots-(-1)^m a^{m-1}v^{m-1}+\cdots$
$+(-1)^n a^n v^n-\cdots\cdots\cdots)$

$= (u+a).v(1+av)^{-1}$

$= (uv+av)(1+av)^{-1} = (1+av)(1+av)^{-1} = 1$,

hence, $(u+a)$ is a unit in R.

Pr(3). Let E be the set of all integer sequences $a=(a_1, a_2, a_3, \cdots\cdots)$. We add sequences componentwise. Let R be the set of all mappings $f: E \to E$ s.t $f(a+b) = f(a)+f(b)$ $\forall a,b \in E$. Let $T: E \to E$ be the shift operator $T(a_1, a_2, a_3, \cdots\cdots) = (0, a_1, a_2, a_3, \cdots\cdots)$. Show that T has a left inverse but not a right inverse.

Soln: Let S be the shift operator s.t

$$S(a_1, a_2, a_3, \cdots\cdots) = (a_2, a_3, a_4, \cdots\cdots)$$

Then $S: E \to E$ s.t

$$S(a+b) = S(a_1+b_1, a_2+b_2, \cdots\cdots)$$
$$= (a_2+b_2, a_3+b_3, \cdots\cdots)$$
$$= (a_2, a_3, \cdots\cdots)+(b_2, b_3, \cdots\cdots)$$
$$= S(a)+S(b)$$

$\Rightarrow S \in R$.

Now, $ST(a) = ST(a_1, a_2, a_3, \cdots\cdots)$

$= S(0, a_1, a_2, \cdots\cdots)$

$= (a_1, a_2, a_3, \cdots\cdots)$

$= a \quad \forall a \in E$.

$\Rightarrow ST = I$, identity mapping.

$\Rightarrow S$ is the left inverse of T.

Now on the contrary, if possible, let $\exists$ a right inverse of T in R as well.

Let that be $T' : E \to E$

Then, for a sequence $(a_1, a_2, a_3, \ldots)$ with $a_1 \neq 0$,

$TT'(a_1, a_2, \ldots) = (a_1, a_2, a_3, \ldots)$

$\Rightarrow (0, T'(a_1), T'(a_2), \ldots) = (a_1, a_2, a_3, \ldots)$

$\Rightarrow a_1 = 0$, contradiction.

Hence $\exists$ no right inverse of T in R.

Pr(4). Let R be a ring and $R[[t]]$ denote the set of all formal power series in an indeterminate t. A formal power series is a formal expression of the form $f(t) = \sum_{i=0}^{\infty} a_i t^i$ where $a_i \in R \ \forall i$. We add and multiply formal power series as we add and multiply polynomials. Under these operations $R[[t]]$ is a ring. Show that $f(t)$ is a unit iff a_0 is a unit; Show that if $f(t)$ is nilpotent, then a_i are so. Is the converse true?

Soln: ☒ $f(t)$ is a unit in $R[[t]]$

$\Leftrightarrow \exists\ g(t) \in R[[t]]$ s.t $f(t).g(t) = 1$,

$\Leftrightarrow \sum_{i=0}^{\infty} a_i t^i . \sum_{j=0}^{\infty} b_j t^j = 1$ where $g(t) = \sum_{j=0}^{\infty} b_j t^j$

Comparing coefficients,

$$a_0 b_0 = 1 \ \& \ a_n b_n = 0 \ \forall\ n \geq 1.$$

$\Leftrightarrow$ for $a_0 \in R$, $\exists\ b_0 \in R$ s.t $a_0 b_0 = 1$

$\Leftrightarrow a_0$ is a unit in R. (Converse part done later)

☒ If $f(t)$ is nilpotent, then $\exists\ n \in \mathbb{N}$ s.t $\{f(t)\}^n = 0$

$\Rightarrow \left(\sum_{i=0}^{\infty} a_i t^i\right)^n = 0$

~~$\Rightarrow \sum_{i=0}^{\infty} a_i t^i = 0$~~

~~Comparing coefficients for each t^i, $i \geq 0$~~

$\Rightarrow a_0^n = 0$, comparing coefficient $\Rightarrow a_0$ is nilpotent.

Now let a_i is nilpotent $\forall i < r$,

Then the coefficient of x^{rn} is $a_r^n + T$, where every term of T contains elements a_i for $i < r$.

So, $a_r^n + T = 0$

$\Rightarrow a_r^n$ is nilpotent

$\Rightarrow a_r$ is nilpotent.

[We use the result: sum & product of nilpotent elements is again nilpotent]

Hence, by induction, a_i is nilpotent $\forall i$.

The converse is not true.

For an example, take

$$R = \mathbb{F}_2[t, t^{1/2}, t^{1/3}, \ldots]/(t)$$

Form the power series $p(x) = \sum_{n \geq 1} a_n x^n$ where $a_n = t^{1/n}$ $\forall n \in \mathbb{N}$.

Clearly each a_n is nilpotent in the ring R.

But for each positive integer k,

$$p(x)^{2^k} = \sum_{n \geq 1} t^{2^k/n} x^{2^k n}$$, which is not zero because the coeff of $x^{2^k n} \neq 0$ when $n > 2^k$.

Hence, $p(x)$ is not nilpotent.

Pr(5). Let $\mathbb{Q}[\alpha, \beta]$ denote the smallest subring of $\mathbb{C}$ containing $\alpha = \sqrt{2}$ & $\beta = \sqrt{3}$. Show that

$$\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma] \text{ where } \gamma = \alpha + \beta.$$

Soln: Since $\sqrt{2} \in \mathbb{Q}[\alpha, \beta]$ & $\sqrt{3} \in \mathbb{Q}[\alpha, \beta]$

$\sqrt{2} + \sqrt{3} \in \mathbb{Q}[\alpha, \beta]$, since it is a subring.

But $\mathbb{Q}[\gamma]$ is the smallest subring containing $\sqrt{2} + \sqrt{3}$, thus,

$$\mathbb{Q}[\gamma] \subset \mathbb{Q}[\alpha, \beta]. \quad \text{——(1)}$$

Again, $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\gamma]$

$\Rightarrow (\sqrt{2}+\sqrt{3})^2 \in \mathbb{Q}[\gamma]$

$\Rightarrow 5+2\sqrt{6} \in \mathbb{Q}[\gamma]$

$\Rightarrow \frac{1}{2}(5+2\sqrt{6}-5) \in \mathbb{Q}[\gamma]$

$\Rightarrow \sqrt{6}(\sqrt{2}+\sqrt{3}) \in \mathbb{Q}[\gamma]$

$\Rightarrow 2\sqrt{3}+3\sqrt{2} \in \mathbb{Q}[\gamma]$

$\therefore (2\sqrt{3}+3\sqrt{2})-2(\sqrt{2}+\sqrt{3}) = \sqrt{2} \in \mathbb{Q}[\gamma]$.

$3(2\sqrt{3}+\sqrt{2})-(2\sqrt{3}+3\sqrt{2}) = \sqrt{3} \in \mathbb{Q}[\gamma]$.

but $\mathbb{Q}[\alpha,\beta]$ is the smallest subring containing $\sqrt{2}$ & $\sqrt{3}$.

$\therefore \mathbb{Q}[\alpha,\beta] \subseteq \mathbb{Q}[\gamma]$ ——— (2)

From (1) & (2), we have,

$$\mathbb{Q}[\alpha,\beta] = \mathbb{Q}[\gamma].$$

Pr(6). Prove that every non-zero ideal in $\mathbb{Z}[i]$ contains a non-zero integer.

Sol: Let I be a non-zero ideal in $\mathbb{Z}[i]$,

Then $a+bi \in I$ for some $a, b \in \mathbb{Z}$, not all zero.

Now if $b=0$, then the result is obvious.

So, let $b \neq 0$.

~~Since, $(a+bi) \in I \Rightarrow (a+bi)^2 = a^2-b^2+2ib \in I$~~

~~also, as I is an ideal,~~

$(a-bi)(a+ib) \in I \Rightarrow a^2+b^2 \in I$, which is a non-zero int as $b \neq 0$.

~~Hence, $(a^2+b^2)-(a^2-b^2+2ib) = 2b^2-2ib \in I$~~

~~i.e., $2b(b-i) \in I$~~

~~$\Rightarrow 2b(b-i) \in I$~~

~~$\Rightarrow 2b(b+1) \in I$~~ ~~$2b(b+1)$ is a non-zero integer as $b \neq 0$.~~

~~Hence, every non-zero ideal in $\mathbb{Z}[i]$ contains a non-zero integer.~~

Pr(7). Describe the kernels of the homomorphisms:

(a) $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ given by $\varphi(f(x)) = f(2+i)$.

Soln: $\ker \varphi = \{ f(x) \in \mathbb{R}[x] \text{ s.t. } \varphi(f(x)) = 0 \}$

$= \{ f(x) \in \mathbb{R}[x] \mid f(2+i) = 0 \}$

Now we see that;

$p(x) = x^2 - 4x + 5 \in \ker \varphi$ & no polynomial with degree < 2 belongs to $\ker \varphi$.

$p(2+i) = (2+i)^2 - 4(2+i) + 5$

$= 3 + 4i - 8 - 4i + 5 = 0$.

Now if $g(x) \in \ker \varphi$, then, by division algorithm, we can write,

$g(x) = p(x)q(x) + r(x)$ for some $q(x), r(x) \in \mathbb{R}[x]$

where $r(x) = 0$ or $\deg(r(x)) < 2$.

$\therefore \; g(x) - p(x)q(x) = r(x) \in \ker \varphi$

$\Rightarrow r(x) = 0$.

$\therefore \; g(x) = p(x)q(x)$

Hence, kernel $\varphi = (x^2 - 4x + 5)$.

~~(b) $\varphi : \mathbb{R}[x,y,z] \to \mathbb{R}[t]$ defined by $\varphi(x) = t$, $\varphi(y) = t^2$ and $\varphi(z) = t^3$.~~

~~Soln: Here $\varphi(f(x,y,z)) = f(t)$ where f is a polynomial~~

~~Then, $\ker \varphi = \{ f(x,y,z) \in \mathbb{R}[x,y,z] \mid \varphi(f(x,y,z)) = 0 \}$~~

~~Now the function φ doesn't change the coefficient of a complex polynomial in x,y,z.~~

~~$\Rightarrow \varphi(f(x,y,z)) = 0 \Rightarrow$ every coefficient of the polynomial is zero.~~

~~i.e. $f(x,y,z) = 0$.~~

~~$\therefore \ker \varphi = \{0\}$.~~

(c) $\varphi : \mathbb{R}[x,y] \to \mathbb{C}[t]$ defined by $\varphi(x) = t^3$ and $\varphi(y) = t^5$ and $\varphi(a) = a$ $\forall a \in \mathbb{R}$.

Soln: [illegible].

Pr.(8). Show that nilpotent elements of a ring R form an ideal. This ideal, denoted by $\text{nil}(R)$, is called the nilradical of R.

Determine the nilradical of $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ & $\mathbb{R}[x]$.

Soln: Let $I = \{a \in R \mid a \text{ is nilpotent}\}$, clearly I is a subgroup of $(R,+)$

if $x \in I$, $\exists\, n \in \mathbb{N}$ s.t $x^n = 0$.

if $r \in R$, then, $(rx)^n = r^n x^n = 0 \Rightarrow rx \in I$.

That shows, $rI \subset I$.

Since R is commutative, this implies that I is an ideal of R.

nilradical of $\mathbb{Z}/12\mathbb{Z}$ is $\{\bar{0}, \bar{6}\}$.

Let $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{R}[x]$

Then $f(x)$ is nilpotent $\Leftrightarrow$ $a_k \in R$ are nilpotent $\forall\, 0 \le k \le n$.

$\Leftrightarrow a_k = 0 \quad \forall\, 0 \le k \le n$.

$\Leftrightarrow f(x) = 0$

$\therefore$ nilradical of $\mathbb{R}[x]$ is the zero ideal, i.e., (0).

$\mathbb{Z}/n\mathbb{Z}$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, Let $m = p_1 p_2 \cdots p_n$.

Claim: $\langle m \rangle = \text{nil}(\mathbb{Z}/n\mathbb{Z})$

$m^{\max(\alpha_i)} = \bar{0} \Rightarrow \langle m \rangle \subseteq \text{nil}(\mathbb{Z}/n\mathbb{Z})$

Let $x \in \text{nil}(\mathbb{Z}/n\mathbb{Z})$

$\Rightarrow x^a = \bar{0}$ for some a

$\Rightarrow x^a = nq$ for some $q \in \mathbb{Z} \Rightarrow x \in \langle m \rangle$

hence, $\text{nil}(\mathbb{Z}/n\mathbb{Z}) = \langle m \rangle$.

Pr(9). Show that all ideals of the power series ring $R[[x]]$ are principal.

Soln: Let $f(x) = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$

Then if l be the minimum natural no s.t $a_l \neq 0$, then,

$$f(x) = x^l \sum_{j=0}^{\infty} a_{j+l} x^j$$

$$\in (x^l) \text{ as } \sum_{j=0}^{\infty} a_{j+l} x^j \in R[[x]].$$

Now, let us consider the ideal in $R[[x]]$ to be $\left(\sum_{i=0}^{\infty} a_i x^i, \sum_{j=0}^{\infty} b_j x^j\right)$, where the minimum natural no's s.t $a_i \neq 0$ & $b_j \neq 0$ are $i = l$ & $j = m$ where $l < m$.

Then, $\sum_{i=0}^{\infty} a_i x^i \in (x^l)$

$\sum_{j=0}^{\infty} b_j x^j \in (x^m) \subset (x^l)$

Hence, we have $\left(\sum a_i x^i, \sum b_j x^j\right) \subset (x^l)$

Also, converse part that $(x^l) \subset \left(\sum_i a_i x^i, \sum_j b_j x^j\right)$ is obvious.

Thus, $\left(\sum_{i=0}^{\infty} a_i x^i, \sum_{j=0}^{\infty} b_j x^j\right) = (x^l)$ where $l = \min\{i, j \mid a_i \neq 0 \wedge b_j \neq 0\}$

Similarly, we can show every ideal which is generated by more than one power series is ultimately of the form (x^l), where l is defined as before.

Thus, all ideals of the power series ring $R[[x]]$ are principal.

Pr(10). Let I & J be ideals of a ring R.

$I + J = \{x + y \mid x \in I, y \in J\}$. Show that $I + J$ is an ideal of R.

Soln: clearly $I+J$ is a subgroup of $(R,+)$

Now let $a \in I+J$

$\Rightarrow \exists\, x \in I$ & $y \in J$ s.t $a = x+y$.

then $\forall\, r \in R$, $ra = r(x+y)$

$= rx + ry \in I+J$.

[$\because I$ is ideal, $x \in I, r \in R \Rightarrow rx \in I$
$\because J$ is ideal, $y \in J, r \in R \Rightarrow ry \in J$]

hence, $I+J$ is an ideal of R.

Pr(11). I & J be ideals of a ring R.

$IJ = \{\sum x_i y_i \mid x_i \in I, y_i \in J\ \forall i\}$

Show that IJ is an ideal and $I \cap J \supseteq IJ$. Show by example, IJ need not be equal to $I \cap J$.

Soln: Clearly, IJ is a subgroup of $(R,+)$

Now, let $a \in IJ$

$\Rightarrow a = \sum_i x_i y_i$, $x_i \in I$, $y_i \in J$.

then $\forall\, r \in R$, $ra = r\left(\sum_i x_i y_i\right)$

$= \sum_i (rx_i) y_i \in IJ$ ($\because I$ is an ideal, $x_i \in I, r \in R \Rightarrow rx_i \in I\ \forall i$)

hence, IJ is an ideal.

~~Now let $x \in IJ$~~

~~$x \in I$ and $x \in J$.~~

~~$\Rightarrow$~~

Now, let $x \in IJ$

$\Rightarrow x = \sum_i x_i y_i$ for some $x_i \in I$ & $y_i \in J$

Since $x_i \in I\ \forall i$ & $y_i \in R \Rightarrow x_i y_i \in I\ \forall i$

$\Rightarrow \sum_i x_i y_i \in I$

$\Rightarrow x \in I$.

Again since, $x_i \in R$ & $y_i \in J\ \forall i \Rightarrow x_i y_i \in J\ \forall i$

$\Rightarrow \sum_i x_i y_i \in J$

$\Rightarrow x \in J$.

$\Rightarrow x \in I \cap J$

therefore, $IJ \subseteq I \cap J$.

To show IJ need not be equal to $I \cap J$, Consider the example,

Consider the ring $(\mathbb{Z}, +, \cdot)$ and ideals $I = 2\mathbb{Z}$ & $J = 4\mathbb{Z}$.

Then $IJ = 8\mathbb{Z}$ & $I \cap J = 4\mathbb{Z}$.

So, $IJ \subseteq I \cap J$ but $IJ \neq I \cap J$.

i.e, $IJ \subsetneq I \cap J$.

Pr(12). An isomorphism of a ring R is called an automorphism of R. Determine all automorphisms of $\mathbb{Z}[x]$ & R.

Soln: Automorphism of $\mathbb{Z}[x]$:

First, we see that $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ is an automorphism $\Rightarrow \varphi(1) = 1 \Rightarrow \varphi(c) = c$ $\forall$ constant terms c.

Hence, φ is completely determined by $\varphi(x)$.

Let $\deg(\varphi(x)) = d$

Then given $f(x) \in \mathbb{Z}[x]$,

$$\deg(\varphi(f(x))) \geq d.$$

Also as φ is surjective, given $x \in \mathbb{Z}[x]$, $\exists$ a fn $f(x) \in \mathbb{Z}[x]$ s.t

$$\varphi(f(x)) = x$$

Therefore, d must be 1.

i.e, $\varphi(x) = \alpha x$

Suppose, $\alpha = pq$ for $p, q \in \mathbb{Z}$ and $\varphi(g(x)) = qx$,

Then $\varphi(x) = \alpha x = pq(x) = \varphi(p)\varphi(g(x))$

$$= \varphi(p\, g(x))$$

$\Rightarrow p = \pm 1$ & $g(x) = \pm x$.

$\therefore$ There are only two automorphisms of $\mathbb{Z}[x]$, namely the fns φ_1, φ_2 s.t $\varphi_1(x) = x$ & $\varphi_2(x) = -x$

& $\varphi_i(a) = a$ $\forall a \in \mathbb{Z}$, $i = 1, 2$.

Automorphism of $\mathbb{R}$:

Let f be an automorphism of $\mathbb{R}$.

$\Rightarrow f(x) = x \quad \forall\, x \in \mathbb{N}$ as $x = \underbrace{1+1+1+\cdots+1}_{x \text{ times}}$.

$\Rightarrow f(x) = f(1)+f(1)+\cdots+f(1)$

$= 1+1+\cdots+1 = x$,

Since a rational number r can be written in the form, $r = (x-y)z^{-1}$ where $x, y, z \in \mathbb{N}$

Thus, $f(r) = \{f(x)-f(y)\}f(z)^{-1}$

$= (x-y)z^{-1} = r$

Hence, f fixes all rational numbers,

Now, let f be a non-identity map, then $f(x) \neq x$ for some $x \in \mathbb{R}$

Without loss of generality, assume,

$f(x) > x$.

Then $\exists$ a rational number q s.t.

$x < q < f(x)$.

but f preserves ordering,

[if x is +ive, then $\exists\, y \in \mathbb{R}$ s.t. $x = y^2$

$\Rightarrow f(x) = f(y)^2 > 0$

So if $x > y \Rightarrow x-y > 0 \Rightarrow f(x-y) > 0$

$\Rightarrow f(x)-f(y) > 0 \Rightarrow f(x) > f(y)$]

hence, $x < q \Rightarrow f(x) < f(q)$

i.e, $f(x) < q$, contradicts that $q < f(x)$

Hence f must be the identity map.

Therefore there are only one automorphism of $\mathbb{R}$ which is the identity map I.

Pr(4).

(Converse part)

Suppose a_0 is a unit.

We want to form a formal power series $\sum_{n\geq 0} b_n x^n$ s.t $\left(\sum_{n\geq 0} a_n x^n\right)\left(\sum_{n\geq 0} b_n x^n\right) = 1$.

as a_0 is unit, $\exists\ b_0 \in R$ s.t $a_0 b_0 = 1$.

For $n>0$, we want,

$$\sum_{k=0}^{n} a_k b_{n-k} = 0$$

$$\Rightarrow a_0 b_n = -\sum_{k=1}^{n} a_k b_{n-k}$$

$$\Rightarrow b_n = -b_0\left(\sum_{k=1}^{n} a_k b_{n-k}\right)$$

Thus, b_n is determined by known coeffs a_i & $b_0, b_1, \ldots, b_{n-1}$. These can be found recursively, obtaining the inverse of a given power series.

$\therefore \sum_{i\geq 0} a_i x^i$ is a unit.

Pr(7). Describe the kernels of the homomorphisms:

(b) $\varphi : \mathbb{C}[x,y,z] \longrightarrow \mathbb{C}[t]$ defined by $\varphi(x) = t$, $\varphi(y) = t^n$, $\varphi(z) = t^3$ and $\varphi(a) = a$ $\forall\ a \in \mathbb{C}$

Soln: Since, $\varphi\{f_1(x,y,z)(x^2-y) + f_2(x,y,z)(xy-z) + f_3(x,y,z)(zx-y^2)\}$

$= \varphi(f_1(x,y,z)).0 + \varphi(f_2(x,y,z)).0 + \varphi(f_3(x,y,z)).0$

$= 0$,

$(x^2-y, xy-z, zx-y^2) \subseteq \ker\varphi$.

(c) $\varphi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}[t]$ defined by $\varphi(x) = t^3$ and $\varphi(y) = t^5$, and $\varphi(a) = a$ $\forall\ a \in \mathbb{C}$

Soln: Since, $\varphi(f(x,y)(x^5-y^3)) = \varphi(f(x,y))\{\varphi(x^5) - \varphi(y^3)\}$

$= \varphi(f(x,y)).\{t^{15} - t^{15}\}$

$= 0$.

$(x^5-y^3) \subseteq \ker\varphi$.

7. Integral Domain, Prime Ideal and Maximal Ideal

Pr(1). Let R be an Integral Domain. Prove that units in the polynomial ring R[x] are units of R.

Soln: Let $p(x) \in R[x]$ be a unit in $R[x]$

$\Rightarrow \exists\ q(x) \in R[x]$ s.t.

$$p(x)q(x) = 1$$

$\Rightarrow \deg(p(x)q(x)) = \deg(1) = 0$

$\Rightarrow \deg p(x) = 0$ & $\deg q(x) = 0$. [$\because$ R is an ID]

$\therefore p(x) = a_0 \in R$ & $q(x) = b_0 \in R$.

$\therefore a_0 b_0 = 1$

$\Rightarrow a_0$ & b_0 are units of R $\Rightarrow p(x)$ is a unit of R.

Hence, units in R[x] are units in R.

Pr(2). Is there an integral domain containing exactly 10 elements.

Soln: Let R be a ring with 10 elements.

Since $(R,+)$ is abelian, $(R,+) \cong (\mathbb{Z}_{10},+)$

$\therefore R \cong (\mathbb{Z}_{10},+,\cdot)$

Now, $(\mathbb{Z}_{10},+,.)$ is not an integral domain since $\bar{2}, \bar{5} \in \mathbb{Z}_{10}$ & $\bar{2}.\bar{5} = \bar{0}$, $\bar{2} \neq \bar{0}$, $\bar{5} \neq \bar{0}$.

$\therefore$ R is not an integral domain.

So there cannot be an ID with exactly 10 elements.

Pr(3). Find the quotient field of the power series ring R[[x]].

Soln: Quotient field $= \left\{ \frac{f(x)}{g(x)} \mid f,g \in R[[x]] \text{ and } g(x) \neq 0 \right\}$

Pr(4). Find integral domains among the rings $R = \mathbb{F}_5[x]/(x^2+x+1)$ and $S = \mathbb{F}_3[x]/(x^2+x+1)$.

Soln: $x^2+x+1 = 0$ has no root in $\mathbb{F}_5$, so (x^2+x+1) is irreducible over $\mathbb{F}_5$.

Since $\mathbb{F}_5[x]$ is a PID, (x^2+x+1) is a prime ideal in $\mathbb{F}_5[x]$.

Hence, $R = \mathbb{F}_5[x]/(x^2+x+1)$ is an integral domain.

On the other hand, $x^2+x+1 = 0$ has a root in $\mathbb{F}_3$ ($\because \bar{1}^2+\bar{1}+\bar{1} = \bar{3} = \bar{0}$)

$\Rightarrow x^2+x+1$ is reducible over $\mathbb{F}_3$.

so, (x^2+x+1) is not a prime ideal.

Hence, $S = \mathbb{F}_3[x]/(x^2+x+1)$ is not an integral domain.

Pr(5). Determine maximal ideals of $\mathbb{Z}[x]$ and $\mathbb{F}[[x]]$, where $\mathbb{F}$ is a field.

Soln: Maximal ideals in $\mathbb{Z}[x]$ are of the form $(p, f(x))$ where p is prime & $f(x)$ is irreducible over $\mathbb{Z}_p$.

In general, $\dfrac{\mathbb{Z}[x]}{(p, f(x))} \cong \dfrac{\mathbb{Z}/p\mathbb{Z}[x]}{(\overline{f(x)})}$

$(f(x)) \subset (f(x), p)$, $p \nmid$ leading coeff of $f(x)$

Thus, if $(\overline{f(x)})$ is irreducible, then, $(\overline{f(x)})$ is maximal in $\mathbb{Z}/p\mathbb{Z}[x]$, consequently $\mathbb{Z}_p[x]/(\overline{f(x)})$ is a field, then, $\mathbb{Z}[x]/(p, f(x))$ is field, so, $(p, f(x))$ becomes maximal.

Consider, $\varphi : \mathbb{F}[[x]] \longrightarrow \mathbb{F}$ defined by

$$\varphi(f(x)) = f(0)$$

Then φ is a surjective ring homomorphism & $\ker \varphi = \{ f(x) \in \mathbb{F}[[x]] \mid f(0) = 0 \}$

$= \{ xg(x) \mid g(x) \in \mathbb{F}[[x]] \} = (x)$. $\because \dfrac{\mathbb{F}[[x]]}{(x)} \cong \mathbb{F}$, field.

$\therefore (x)$ is maximal ideal.

Pr(6). Prove that $m = (x+y^2, y+x^2+2xy^2+y^4) \subset \mathbb{C}[x,y]$ is a maximal ideal.

Soln: $m = (x+y^2, y+x^2+2xy^2+y^4)$

$= (x+y^2, y+(x+y^2)^2)$

$= (x+y^2, y) = (x,y)$, which is maximal in $\mathbb{C}[x,y]$ since, $\frac{\mathbb{C}[x,y]}{(x,y)} \cong \mathbb{C}$.

Hence m is maximal in $\mathbb{C}[x,y]$.

Pr(7). Consider the ideal $I = (y^2+x^3-17)$ of $R = \mathbb{C}[x,y]$. Find generators of all maximal ideals in the quotient ring R/I.

Soln: Maximal ideals of R/I are maximal ideals of $R = \mathbb{C}[x,y]$ which contains I.

Maximal ideals of $\mathbb{C}[x,y]$ are of the form $(x-a, y-b)$, for some $a, b \in \mathbb{C}$.

Here $I = (y^2+x^3-17)$

We want $(y^2+x^3-17) \subseteq (x-a, y-b)$

$\Rightarrow$ a and b also satisfies $y^2+x^3-17 = 0$.

Hence if a and b belongs to $\mathbb{C}$ s.t $y^2+x^3-17=0$ is satisfied by a and b, then the required maximal ideals are $(x-a, y-b)$.

Pr(8). Show that $\mathbb{Z}_3[x]/(x^2+x+1)$ is not a field.

Soln: Since $\bar{1} \in \mathbb{Z}_3$ s.t $\bar{1}^2+\bar{1}+\bar{1} = \bar{3} = \bar{0}$ in $\mathbb{Z}_3$, thus, x^2+x+1 is reducible in $\mathbb{Z}_3[x]$.

Since $\mathbb{Z}_3[x]$ is a PID, x^2+x+1 is not maximal ideal in $\mathbb{Z}_3[x]$.

Consequently, $\frac{\mathbb{Z}_3[x]}{(x^2+x+1)}$ is not a field.

Pr(9). How many elements are in $\mathbb{Z}[i]/(3+i)$? Give reason.

Soln: Let $S = \mathbb{Z}[i]/(3+i)$

Then $3+i = 0$ in $S \Rightarrow i = -3$ in $S \Rightarrow i^2 = 9$ in S

$\Rightarrow 10 = 0$ in S.

Now, define,

$$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/10\mathbb{Z} \text{ by}$$
$$\varphi(a+ib) = (a-3b) \pmod{10}$$

Then φ is a ring homomorphism (Verify!!!). Also, φ is surjective.

Since $\varphi(3+i) = 3-3 \pmod{10}$
$= 0$

thus, $(3+i) \subseteq \ker \varphi$.

Also if $a+ib \in \ker \varphi$

$\Rightarrow a-3b = 0 \Rightarrow a = 3b$.

$\therefore a+ib = 3b+ib = b(3+i) \subseteq (3+i)$.

$\Rightarrow \ker \varphi \subseteq (3+i)$.

So, $\ker \varphi = (3+i)$

Hence, by 1st isomorphism theorem,

$$\frac{\mathbb{Z}[i]}{(3+i)} \cong \mathbb{Z}/10\mathbb{Z}.$$

So $\mathbb{Z}[i]/(3+i)$ has 10 elements.

Pr(10) Let $R = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is a continuous function}\}$ Show that $I = \{f \in R \mid f(0) = 0\}$ is a maximal ideal of R.

Soln: Define $\varphi : R = \{f : \mathbb{R} \xrightarrow{\text{cont}} \mathbb{R}\} \longrightarrow \mathbb{R}$.

by $\varphi(f) = f(0)$

Then, φ is a ring homomorphism which is surjective.

$$\ker \varphi = I = \{f \in R \mid f(0) = 0\}$$

Then by 1st isomorphism theorem,

$R/I \cong \mathbb{R}$, a field

$\Rightarrow I$ is maximal ideal of R.

Pr(11). Show that $\mathbb{Z}[i]/(1-i)$ is a field. How many elements does this field have?

Soln: Define, $\varphi: \mathbb{Z}[i] \to \mathbb{Z}/2\mathbb{Z}$

by $\varphi(a+bi) = a+b \pmod 2$

Then φ is a surjective ring homomorphism with $\ker \varphi = (1-i)$.

$\therefore \mathbb{Z}[i]/(1-i) \cong \mathbb{Z}/2\mathbb{Z}$, field

Thus, $\mathbb{Z}[i]/(1-i)$ is a field.

It has 2 elements.

Pr(12). In $\mathbb{Z}_5[x]$, Let $I = (x^2+x+2)$. Find multiplicative inverse of $2x+3+I$ in $\mathbb{Z}_5[x]/I$.

Soln: Any element $f(x)+I$ in $\mathbb{Z}_5[x]/I$ is such that degree $f(x) \leq 1$.

Let $f(x) = ax+b$ be s.t $f(x)+I$ is the multiplicative inverse of $2x+3+I$.

Then, $(ax+b+I)(2x+3+I) = 1+I$

$\Rightarrow 2a(x^2+x+2) + (ax+b)I + (2x+3)I + ax + 2bx + 3b - 4a = 1+I$

$\Rightarrow (a+2b)x + (3b-4a) = 1$.

Comparing coeff's, we get,

$$\begin{aligned} a+2b &= 0 \\ 3b-4a &= 1 \end{aligned} \quad \Rightarrow 11b = 1 \pmod 5$$

$\Rightarrow b = 1$, $\therefore a = 3$

$\therefore$ The multiplicative inverse is $3x+1+I$.

Pr(13). In $\mathbb{Z}[x]$, Let $I = \{f(x) \in \mathbb{Z}[x] \mid f(0)$ is an even integer$\}$. Prove that $I = (2,x)$. Is I a prime ideal of $\mathbb{Z}[x]$? Is I a maximal ideal? How many elements does $\mathbb{Z}[x]/I$ have?

Soln: Let $f(x) \in (2,x)$

$\Rightarrow f(x) = 2m + xg(x)$ where $m \in \mathbb{Z}$, $g(x) \in \mathbb{Z}[x]$

$\therefore f(0) = 2m$, even integer.

$\therefore (2,x) \subseteq I$.

Now let, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

$\in I$

$\Rightarrow f(0) = a_0$ is even number. ($a_0 = 2r$, say)

Then, $f(x) = x(a_n x^{n-1} + a_{n-1} x^{n-2} + \cdots + a_1) + 2r$

$\in (2,x)$.

$\therefore I \subseteq (2,x)$

Hence, $I = (2,x)$.

Now, $\frac{\mathbb{Z}[x]}{(2,x)} \cong \frac{\mathbb{Z}[x]/(2)}{(2,x)/(2)} \cong \frac{\mathbb{Z}_2[x]}{(x)} \cong \mathbb{Z}_2$, a field.

Thus, I is a prime ideal as well as a maximal ideal.

$\therefore \mathbb{Z}[x]/I$ has 2 elements.

Pr(14). Prove that $(2+2i)$ is not a prime ideal in $\mathbb{Z}[i]$.

Soln: First, we see that neither 2 nor $1+i$ belongs to $(2+2i)$.

Let, $2 \in (2+2i)$

$\Rightarrow \exists\ (a+bi) \in \mathbb{Z}[i]$ s.t $2 = (a+bi)(2+2i)$

$\therefore \begin{matrix} 2a-2b = 2 \\ 2a+2b = 0 \end{matrix} \Rightarrow a = \frac{1}{2}, b = -\frac{1}{2}$ but $a, b \notin \mathbb{Z}$

So, $2 \notin (2+2i)$

Let $(1+i) \in (2+2i)$

$\Rightarrow \exists\ (c+di) \in \mathbb{Z}[i]$ s.t $1+i = (c+id)(2+2i)$

$\therefore \begin{matrix} 2c-2d = 1 \\ 2c+2d = 1 \end{matrix} \Rightarrow c = \frac{1}{2}, d = 0$ but $c \notin \mathbb{Z}$

$\therefore 1+i \notin (2+2i)$.

Thus, we see, $2(1+i) = 2+2i \in (2+2i)$ but neither 2 nor $1+i$ belongs to $(2+2i)$.

Hence, $(2+2i)$ is not a prime ideal in $\mathbb{Z}[i]$.

Pr(15). Prove that (3) is a maximal ideal in $\mathbb{Z}[i]$.

Soln: We know, $\mathbb{Z}[i] \cong \frac{\mathbb{Z}[x]}{(1+x^2)}$

Now, $\frac{\mathbb{Z}[i]}{(3)} \cong \frac{\mathbb{Z}[x]/(1+x^2)}{(3, 1+x^2)/(1+x^2)}$

$\cong \frac{\mathbb{Z}[x]}{(3, 1+x^2)} \cong \frac{\mathbb{Z}[x]/(3)}{(3, 1+x^2)/(3)} \cong \frac{\mathbb{Z}_3[x]}{(1+x^2)}$

Since $1+x^2$ is irreducible over $\mathbb{Z}_3$, thus $\mathbb{Z}_3[x]/(1+x^2)$ is a field.

Consequently, $\mathbb{Z}[i]/(3)$ is a field

$\Rightarrow$ (3) is a maximal ideal in $\mathbb{Z}[i]$.

6. UFD, PID, ED AND IRREDUCIBILITY OF POLYNOMIALS

Pr(1). Show that $\mathbb{R}[x,y]$ and $\mathbb{Z}[x]$ are not PIDs.

Soln: For any ring R, we first show that, $R[x]$ is a PID iff R is a field.

Consider, $f: R[x] \longrightarrow R$ defined by

$$f(p(x)) = p(0).$$

Then, $\ker f = (x)$.

$$\therefore \frac{R[x]}{(x)} \cong R.$$

Since $R \subset R[x]$ & $R[x]$ is an ID, R is also an ID.

$\Rightarrow \frac{R[x]}{(x)}$ is an ID $\Leftrightarrow (x)$ is prime ideal.

$\Leftrightarrow (x)$ is maximal ideal, ($\because R[x]$ is PID)

$\Leftrightarrow \frac{R[x]}{(x)}$ is a field $\Leftrightarrow R$ is a field.

Now, $\mathbb{R}[x,y] = \mathbb{R}[x][y]$, so if $\mathbb{R}[x,y]$ is a PID, then $\mathbb{R}[x]$ must be a field but this is not true as $x \neq 0 \in \mathbb{R}[x]$ but x is not a unit.

$\therefore \mathbb{R}[x,y]$ is not a PID.

Similarly, if $\mathbb{Z}[x]$ is a PID, then $\mathbb{Z}$ must be a field, but this is not true as any $a \in \mathbb{Z}$ s.t $a \neq \{1,-1\}$ is non-unit.

$\therefore \mathbb{Z}[x]$ is not a PID.

Pr(2). Prove that $2, 3, 1 \pm \sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.

Soln: Let $2 = (a+b\sqrt{-5})(c+d\sqrt{-5})$, $a,b,c,d \in \mathbb{Z}$.

Then, $2.\overline{2} = (a^2+5b^2)(c^2+5d^2)$

$\Rightarrow 4 = (a^2+5b^2)(c^2+5d^2)$

but for $a,b,c,d \in \mathbb{Z}$, $a^2+5b^2 \neq 2$, $c^2+5d^2 \neq 2$.

Thus, any one of a^2+5b^2 or c^2+5d^2 is 1 and other is 4.

say $a^2+5b^2 = 1 \Rightarrow a = \pm 1, b = 0. \Rightarrow a+b\sqrt{-5} = \pm 1$, unit.

hence, 2 is irreducible.

Similarly if $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$\Rightarrow 9 = 3.3 = (a^2+5b^2)(c^2+5d^2)$

but $a^2+5b^2 \neq 3$

$c^2+5d^2 \neq 3$.

then any one of the two factors must be a unit, consequently 3 is irreducible.

$1 \pm \sqrt{-5} = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$\Rightarrow 6 = (1\pm\sqrt{5})(1\pm\sqrt{-5}) = (a^2+5b^2)(c^2+5d^2)$

but $a^2+5b^2 \neq 2, 3$

$c^2+5d^2 \neq 2, 3$.

then any one of the two factors must be a unit, consequently $1\pm\sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.

Pr2(3). Show that $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[w]$ are EDs, where $w = \exp(2\pi i/3)$.

Soln: We define a size function N on $\mathbb{Z}[\sqrt{-2}]$ by

$N(a+b\sqrt{-2}) = a^2+2b^2$.

We show that, $\mathbb{Z}[\sqrt{-2}]$ is an ED with this size fn N;

Let $\alpha = a+b\sqrt{-2}$, $\beta = c+d\sqrt{-2} \neq 0$.

then, $\frac{\alpha}{\beta} = \frac{a+b\sqrt{-2}}{c+d\sqrt{-2}}$

$= \frac{(a+b\sqrt{-2})(c-d\sqrt{-2})}{c^2+2d^2}$

$= \frac{ac+2bd}{c^2+2d^2} + \frac{bc-ad}{c^2+2d^2}\sqrt{-2}$

$= r+s\sqrt{-2} \in \mathbb{Q}[\sqrt{-2}]$

Now, we choose nearest integers p & q to r & s, i.e., $|p-r| < \frac{1}{2}$, $|q-s| < \frac{1}{2}$.

then set

$\theta = (r-p)+(s-q)\sqrt{-2}$

$$\therefore \gamma = \beta\theta = \beta\left[(r+p) + (s+q)\sqrt{-2}\right]$$

$$= \beta(r + s\sqrt{-2}) - \beta(p+q\sqrt{-2})$$

$$= \alpha - \beta(p+q\sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$$

$$\therefore \alpha = \beta(p+q\sqrt{-2}) + \gamma$$

$$N(\gamma) = N(\beta\theta) = N(\beta)N(\theta)$$

$$\leq N(\beta)\left(\frac{1}{4} + \frac{2}{4}\right) = \frac{3}{4}N(\beta) < N(\beta).$$

Hence, $\mathbb{Z}[\sqrt{-2}]$ is an ED.

▨ We define a size function N on $\mathbb{Z}[w]$ by

$$N(a+bw) = a^2 - ab + b^2.$$

We show that $\mathbb{Z}[w]$ is an ED with the size fn N.

Let $\alpha = a+bw$, $\beta = c+dw \neq 0$.

Then, $\frac{\alpha}{\beta} = \frac{a+bw}{c+dw}$

$$= \frac{(a+bw)(c+dw^2)}{c^2 - cd + d^2}$$

$$= \frac{ac+bd-ad}{c^2-cd+d^2} + \frac{bc-ad}{c^2-cd+d^2}\,w.$$

$$= r + sw \in \mathbb{Q}[w]$$

We choose p & q, nearest to r & s, i.e., $|r-p| < \frac{1}{2}$, $|s-q| < \frac{1}{2}$, $p, q \in \mathbb{Z}$.

Set, $\theta = (r-p) + (s-q)w$.

$$\therefore \gamma = \beta\theta = \beta\left[(r-p) + (s-q)w\right]$$

$$= \beta(r+sw) - \beta(p+qw)$$

$$= \alpha - \beta(p+qw) \in \mathbb{Z}[w]$$

$$\therefore \alpha = \beta(p+qw) + \gamma$$

$$N(\gamma) = N(\beta\theta) = N(\beta)N(\theta)$$

$$\leq N(\beta)\left(\frac{1}{4} + \frac{1}{4} - \frac{1}{2}\cdot\frac{1}{2}\right) < N(\beta).$$

Hence, $\mathbb{Z}[w]$ is an ED.

Pr(6). Factor 30, 10, $1-3i$ into product of Gaussian primes.

Soln: $30 = 3.(1+i)(1-i)(1+2i)(1-2i)$

$10 = (1+i)(1-i)(1+2i)(1-2i)$

$1-3i = [illegible](1-i)(2-i)$.

Pr(7). Prove that every Gaussian prime divides exactly one prime integer.

Soln: Let $\alpha = a+bi$ be a Gaussian prime.

Then, $\alpha = a+bi \mid a^2+b^2 = p$ or p^2, where p is an integer prime.

Then in either case $\alpha \mid p$.

Now, let $\alpha \mid q$, where q is any prime integer.

$\Rightarrow q = (a+bi)(c+di)$ for some $c+di \in \mathbb{Z}[i]$

$\Rightarrow q\cdot\bar{q} = (a^2+b^2)(c^2+d^2)$

$\because a^2+b^2 \mid q\cdot\bar{q} = q^2$

$\Rightarrow$ either p or p^2 divides q^2.

$\Rightarrow p$ divides q, but q is prime.

$\Rightarrow p = 1$ or q

But p is a prime., so $p \neq 1$. $\Rightarrow p = q$.

Hence, every Gaussian prime divides exactly one prime integer.

Pr(9). Prove that the polynomials $f(x) = x^2+26x+213$, $g(x) = 8x^3-6x+1$ are irreducible over $\mathbb{Q}[x]$.

Soln: $f(x-2) = (x-2)^2+26(x-2)+213$

$= x^2+22x+165$.

now for prime $p = 11$, in the above polynomial, $a_2 = 1 \notin (p)$, $a_1 = 22 \in (p)$, $a_0 = 165 \in (p)$ but $a_0 = 165 \notin (p^2)$.

Thus, by Eisenstein's criterion,

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

$g(x+1) = 8(x+1)^3 - 6(x+1) + 1$

$= 8x^3 + 24x^2 + 18x + 3$

Now, for prime $p = 3$, $8 \notin (p)$, $24 \in (p)$, $18 \in (p)$, $3 \in (p)$, but $3 \notin (p^2)$.

Hence by Eisenstein's criterion,

$g(x)$ is irreducible over $\mathbb{Q}[x]$.

Ex (10). Factor $x^5 + 5x + 5$ into irreducible factors in $\mathbb{Q}[x]$ and $\mathbb{F}_2[x]$.

Soln: Since $x^5 + 5x + 5$ is monic polynomial and integers dividing $a_0 = 5$ are 1, −1, 5, −5 but none of them is root of $x^5 + 5x + 5 = 0$, thus $x^5 + 5x + 5$ is irreducible over $\mathbb{Q}[x]$.

Also, $x^5 + 5x + 5 = 0$ has no root in $\mathbb{F}_2$, thus it is irreducible over $\mathbb{F}_2[x]$ also.

Ex (11). Factor $x^3 + x + 1$ in $\mathbb{F}_p[x]$ where $p = 2, 3, 5$.

Soln: $x^3 + x + 1$ is irreducible over $\mathbb{F}_2[x]$.

Over $\mathbb{F}_3[x]$, $x^3 + x + 1 = (x-1)(x^2 + x + 2)$

$x^3 + x + 1$ is irreducible over $\mathbb{F}_5[x]$.

Ex (12). Let $f(x)$ be a monic integer polynomial of $+$ve degree having a rational root r. Show that r is an integer.

Soln: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

where $a_i \in \mathbb{Z}$ $\forall$ $i = 0, 1, 2, \ldots, n-1$

Now, let $r = \frac{p}{q}$ where $p, q \in \mathbb{Z}$, $\gcd(p, q) = 1$.

then $f(r) = 0 \Rightarrow f\left(\frac{p}{q}\right) = 0$

$\Rightarrow p^n + a_{n-1}p^{n-1}q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$

$\Rightarrow p^n = q\left(-a_{n-1}p^{n-1} - \cdots - a_0 q^{n-1}\right)$

$\Rightarrow q \mid p^n$

then by assumption $\gcd(p, q) = 1$, we must have $q = 1$.

Hence, $r = p$ is an integer.

Pr(4). Let F be a subfield of $\mathbb{C}$. Show that an irreducible polynomial in $F[x]$ has no multiple roots.

Soln: Since $f(x)$ is irreducible polynomial in $F[x]$, then $\gcd(f(x), f'(x)) = 1$.

Now if possible, let $\alpha \in \mathbb{C}$ be a multiple (n-order) root of $f(x)$ in $\mathbb{C}$. $(n>1)$

Then $f(x) = (x-\alpha)^n g(x)$

$\Rightarrow f'(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n g'(x)$

This imply $\gcd(f(x), f'(x)) = (x-\alpha)^{n-1} \neq 1$,

so a contradiction.

Hence, $f(x)$ has no multiple root in $\mathbb{C}$.

Pr(5). Show that an integer prime p is a prime element of $\mathbb{Z}[\sqrt{3}]$ iff x^2-3 is irreducible in $\mathbb{Z}_p[x]$.

Soln: Let us consider the function,

$$f: \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\sqrt{3}]$$
$$\text{defined by } x \longmapsto \sqrt{3}$$

Then f is a surjective ring homomorphism & $\ker f = (x^2-3)$

$$\Rightarrow \frac{\mathbb{Z}[x]}{(x^2-3)} \cong \mathbb{Z}[\sqrt{3}]$$

Now,
$$\frac{\mathbb{Z}[\sqrt{3}]}{(p)} \cong \frac{\mathbb{Z}[x]/(x^2-3)}{(p, x^2-3)/(x^2-3)}$$
$$\cong \frac{\mathbb{Z}[x]}{(p, x^2-3)} \cong \frac{\mathbb{Z}[x]/(p)}{(p, x^2-3)/(p)}$$
$$\cong \frac{\mathbb{Z}_p[x]}{(x^2-3)}$$

Thus, if p is prime in $\mathbb{Z}[\sqrt{3}]$, $\Leftrightarrow$ $\mathbb{Z}[\sqrt{3}]/(p)$ is an ID, $\Leftrightarrow$ $\mathbb{Z}_p[x]/(x^2-3)$ is an ID $\Leftrightarrow$ (x^2-3) is prime ideal in $\mathbb{Z}_p[x]$, i.e., x^2-3 is irreducible in $\mathbb{Z}_p[x]$.

Pr(8). Prove that $f, g \in \mathbb{Z}[x]$ are relatively prime in $\mathbb{Q}[x]$ iff $(f,g)\mathbb{Z}[x] \cap \mathbb{Z} \neq (0)$.

Soln: Let $(f,g)\mathbb{Z}[x] \cap \mathbb{Z} \neq (0)$

Let $c \in (f,g)\mathbb{Z}[x] \cap \mathbb{Z}$

$\Rightarrow c \in (f,g)$

$\Rightarrow c = rf + sg$ where $r, s \in \mathbb{Z}[x]$

$\Rightarrow 1 = \frac{r}{c} f + \frac{s}{c} g$

$= r'f + s'g$ where $r' = \frac{r}{c} \in \mathbb{Q}[x]$, $s' = \frac{s}{c} \in \mathbb{Q}[x]$.

hence $\gcd(f,g) = 1$ in $\mathbb{Q}[x]$.

i.e, f, g are relatively prime in $\mathbb{Q}[x]$.

Conversely, suppose f, g are relatively prime in $\mathbb{Q}[x]$.

$\Rightarrow \exists\ r, s \in \mathbb{Q}[x]$ s.t

$$rf + sg = 1$$

then by clearing the denominators from r & s, we get that

$$r'f + s'g = c \quad [c \text{ is the lcm of denominators of all coeffs of } r \text{ \& } s]$$

$\Rightarrow c \in (f,g)\mathbb{Z}[x] \cap \mathbb{Z}$

$\Rightarrow (f,g)\mathbb{Z}[x] \cap \mathbb{Z} \neq (0)$.