Definition: A law of composition on a set S is a function $f : S \times S \to S$. we denote $f(a,b) = ab$ or $a * b$

Definition: A law of composition is called associative if $(ab)c = a(bc)$ $\forall\ a,b,c \in S$ and it is called commutative if $ab = ba$ $\forall\ a, b \in S$

Definition: An identity for a law of composition on a set S is an element e such that $ae = ea = a$ $\forall a \in S$

conventionally, if the law of composition is written multiplicatively, we denote the identity by '1' and in case of additive definition, we use '0'

Definition: Suppose e is the identity for a law of composition on a set S, an element $a \in S$ is called invertible if $\exists\ b \in S$ s.t. $ab = ba = 1$

THEOREM 1

If identity exists, it is unique. further, every element has a unique inverse (provided, an inverse exists)

THEOREM 2

If a, b are invertible elements of a set S equipped with a law of composition, then ab is invertible as $(ab)^{-1} = b^{-1}a^{-1}$

Definition: A group is a set G equipped with a law of composition that has the following properties:

> The law is associative and admits an identity
> Every element is invertible in the group.

Definition : An **Abelian group** is a group in which the law of composition is commutative

Definition : The **order of a group** is the number of elements in it. **Finite groups** have finite order and **infinite groups** don't have a finite order.

THEOREM 3

If a, b, c belong to a group and $ab = ac$ or if $ba = ca$, we have $b = c$

Definition: we define some common groups as follows:

$\mathbb{Z}^+$: integers with addition

$\mathbb{R}^+$: reals with addition

$\mathbb{R}^\times$: $\mathbb{R} \setminus \{0\}$ with multiplication

$\mathbb{C}^+$: $\mathbb{C}$ with addition

$\mathbb{C}^\times$: $\mathbb{C} \setminus \{0\}$ with multiplication

$\mathbb{Z}_n$: set of integers modulo n with addition

GL_n : set of $n \times n$ invertible matrices with matrix mult

THEOREM 4

If $a \in \mathbb{Z}_n$ is invertible, then $\gcd(a, n) = 1$ and vice versa. Further $U(n) = \{ [m] \in \mathbb{Z}_n \mid \gcd(m, n) = 1 \}$ is called the **group of units** and is an abelian group under multiplication. Specifically, $\mathbb{Z}_p \setminus \{[0]\}$ is abelian where p is prime.

THEOREM 5

The circle group $\Gamma_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$ is of order n

Definition: The special linear group SL_n is a subset of GL_n, having only those matrices of unit determinant and the orthogonal group is the set of all $n \times n$ orthogonal matrices with matrix multiplication

THEOREM 6

The transformation $T_A : \mathbb{R}^n \to \mathbb{R}^m$ corresponding to an $m \times n$ orthogonal matrix preserves dot product (i.e. $\vec{Au} \cdot \vec{Av} = \vec{u} \cdot \vec{v}$) and hence length of vectors, further, it also preserves angles between vectors (converse is also true)

THEOREM 7

Any 2×2 orthogonal matrix is of the form

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \quad \text{or} \quad S_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}.$$

Further, R_θ induces rotation by θ in anti-clockwise direction and S_θ induces reflection wrt. line $y = x \tan(\frac{\theta}{2})$

we refer to the group of R_θ matrices as SO_n for $n = 2$ or the special orthogonal group (matrices which are orthogonal with $+1$ determinat)

Definition: A symmetry σ of a subset X of $\mathbb{R}^n$ is a bijection, $\sigma : X \to X$ so that $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ is a distance preserving map. The set of symmetries of X form a group under composition

COREM 8

For a regular n-gon with vertices located on the roots of unity in $\mathbb{C}$, we define the dihedral group as

$$D_{2n} = \{1, T, T^2, \ldots, T^{n-1}, S, ST, ST^2, \ldots, ST^{n-1}\}$$

where T denotes rotation by $\frac{2\pi}{n}$ in ACW direction and S denotes reflection with respect to the x axis. This is a group and further is the group of all symmetries of a regular polygon inscribed in a unit circle about the origin

THEOREM 9

Every distance preserving map (symmetry) is of the form $f(u) = Au + b$ for some $A \in O_n$, $b \in \mathbb{R}^n$ (vectors)

Definition: We define the boolean group $B(X)$ as the set of all subsets of X and the law of composition used is $+$ defined as $A + B = (A \setminus B) \cup (B \setminus A)$. This is abelian group

Definition: We define the unitary group (U_n) and the special unitary group (SU_n) as complex counterparts of O_n and SO_n respectively

THEOREM 10

Upgrading theorem 6, if $B \in GL(n, \mathbb{C})$ and B preserves Hermitian inner product, then $B \in U_n$ and vice versa holds.

Definition: For $(a,b,c,d) \in \mathbb{R}^4$, and $z = a + ib$, $w = c + id$, we associate the matrix $q = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}$, we call q a quaternion associated to (a,b,c,d)

THEOREM 11

The set of all q as described as above forms a group under regular matrix multiplication. Further, quaternions are an extension of complex numbers and $q = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \to I$, $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \to i$, $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \to j$, $\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \to k$

Thus, $\{I, i, j, k\}$ are the coordinate vector components and any $q = aI + bi + cj + dk$.

THEOREM 12

$i^2 = j^2 = k^2 = -I$, $ij = k$, $jk = i$, $ki = j$ and $ji = -k$, $kj = -i$, $ik = -j$

q is realized as a formal sum $a + bi + cj + dk$, then $\bar{q} := a - bi - cj - dk \Rightarrow q\bar{q} = a^2 + b^2 + c^2 + d^2 = \det(q)$

$\Rightarrow q^{-1} = \frac{\bar{q}}{a^2+b^2+c^2+d^2}$ $\left[\because a^2 + b^2 + c^2 + d^2 \neq 0 \right)$

THEOREM 13

In accordance with the above, $\det(pq) = \det(p)\det(q)$ and $(a+bi+cj+dk)(e+fi+gj+hk) = (ae - bf - cg - dh) + (af + be + ch - dg)i + (ag + ce + df - hb)j + (ah + de + bg - cf)k$. Further, in vector form, if $q_1 = w_1 + \underbrace{x_1 i + y_1 j + z_1 k}_{\vec{v}_1}$, then,

$q_1 q_2 = (w_1 w_2 - \vec{v}_1 \cdot \vec{v}_2) + (w_1 \vec{v}_2 + w_2 \vec{v}_1 + \vec{v}_1 \times \vec{v}_2)$

THEOREM 14

Consider $\{q \in H(\mathbb{R}) \mid |q| = 1\}$. Clearly q^{-1} also belongs to this set making it a group. This group is the same as SU_2 and also $S^3 = \{(a,b,c,d) \mid a^2+b^2+c^2+d^2 = 1\}$ which is the 4-sphere

Note: Any element of SU_2 is $\begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}$ s.t. $|\alpha|^2 + |\beta|^2 = 1$

(This is the modern motivation for teaching quaternions)

Note: S^3 law of composition is kind obtained through the group of unit modulus quaternions

THEOREM 15

The only unit spheres S^n with a group structure compatible with the topology on S^n (or $\mathbb{R}^n$) are S^1 and S^3

Definition: Let F be any field. The **Heisenberg group** over F is $H(F) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \mid a, b, c \in F \right\}$ under matrix multiplication

Definition: A map $m : \mathbb{R}^n \to \mathbb{R}^n$ is an **isometry** of $\mathbb{R}^n$ if $\forall\, u, v \in \mathbb{R}^n$, $\|m(u) - m(v)\| = \|u - v\|$

THEOREM 16

Isometries are one-one. Further, they are bijections of $\mathbb{R}^n$ and hence they form a group under composition.

THEOREM 17

Similar (or exactly) as theorem 9, every isometry is composed of an orthogonal transformation and a translation. As a lemma used to prove this, every isometry that fixes the origin is an orthogonal transformation

THEOREM 18

The following are equivalent for $m : \mathbb{R}^n \to \mathbb{R}^n$

(i) $m : \mathbb{R}^n \to \mathbb{R}^n$ is an origin fixing isometry

(ii) m preserves dot product

(iii) $\exists$ an $n \times n$ orthogonal matrix A so that $M(u) = Au$

Definition: For H & K subsets of a group G we define $HK := \{ hk \mid h \in H, k \in K \}$

Definition: Let $H \subset G$ such that $H \neq \emptyset$. If H is a group under the binary operation induced from G, we say that H is a subgroup of G

THEOREM 19

A non-empty subset H of a group G is a subgroup iff (i) $a, b \in H \Rightarrow ab \in H$, (ii) $a \in H \Rightarrow a^{-1} \in H$, Further, if H is a finite subgroup of G, if H is closed under multiplication (a^{-1} is dropped since it is redundant for finite subgroups)

THEOREM 20

Any subgroup of $\mathbb{Z}^+$ is of the form $n\mathbb{Z}$

THEOREM 21

If $\mathfrak{r}$ denotes reflection wrt x-axis, ρ_θ denotes rotation by θ in ACW direction and t_v denotes translation by $\vec{v}$,

(i) $\rho_\theta t_v = t_{\rho_\theta(v)} \rho_\theta$

(ii) $\mathfrak{r} t_v = t_{\mathfrak{r}(v)} \mathfrak{r}$

(iii) $\mathfrak{r} \rho_\theta = \rho_{-\theta} \mathfrak{r}$

(iv) $t_v t_w = t_{v+w}$

(v) $\rho_\alpha \rho_\beta = \rho_{\alpha+\beta}$

(vi) $\mathfrak{r} \cdot \mathfrak{r} = id$

THEOREM 22

A finite subgroup of O_2 is one of the following

(i) The cyclic group C_n generated by $\rho_{\frac{2\pi}{n}}$ for some positive integer n

(ii) The dihedral group D_{2n} generated by $\rho_{\frac{2\pi}{n}}$ and the reflection $\mathfrak{r}'$ about a line through the origin

THEOREM 23

Every isometry of $\mathbb{R}^2$ is one of the following

(i) translation

(ii) rotation about angle θ followed by translation

(iii) reflection about a line

(iv) glide reflection - reflection followed by translation by vector parallel to reflection line

~~Also note: rotation by θ followed by translation = translation by $\rho_\theta(v)$ followed by~~

ndr: M_n = isometries of $\mathbb{R}^n$

THEOREM 24

Let G be a finite subgroup of M_n. Then there is a common fixed point of all isometries in G

THEOREM 25

Let G be a finite subgroup of M_n and let s be a fixed point of all $m \in M$. Then $t_{-s} G t_s$ is a finite subgroup of O_n

Definition: A subspace V of $\mathbb{R}^n$ is called a hyperplane if $\dim V = n-1$. A linear transform $T : \mathbb{R}^n \to \mathbb{R}^n$ is called a reflection wrt a hyperplane H if $Tu = -u$ where $u \perp H$ and $Tu = u$ for all $u \in H$

Definition: The householder matrix of a unit vector $\hat{u}$ is $H_u = I - 2uu^t$

THEOREM 26

H is symmetric and orthogonal. Further, $H^2 = I$ and moreover, $L_H : \mathbb{R}^n \to \mathbb{R}^n$ is a reflection wrt to the hyperplane $W = \{ v \in \mathbb{R}^n \mid \langle v, u \rangle = 0 \}$

Definition: A rotation of $\mathbb{R}^3$ is $f : \mathbb{R}^3 \to \mathbb{R}^3$ s.t. $f(u) = u$ for some unit vector u (called a pole of f) and $f : u^\perp \to u^\perp$ is a rotation of the 2D subspace $u^\perp$ of $\mathbb{R}^3$.

THEOREM 27

Every matrix corresponding to a rotation of $\mathbb{R}^3$ belongs to SO_3 and further every SO_3 matrix has an e.val = 1

THEOREM 28 (Euler's rotation theorem)

The set of 3×3 rotation matrices is SO_3

As a corollary : composition of rotations is a rotation

(This corollary was actually what Euler found out :P)

THEOREM 29

Let M be the matrix corresponding to the $\mathbb{R}^3$ rotation $f_{(u,\alpha)}$. Then,

(i) $tr(M) = 1 + 2\cos\alpha$

(ii) If $B \in SO_3$ then matrix of $f_{(Bu,\alpha)}$ is BMB^t

Definition: Let G be a group and $x \in G$. Then $H = \{x^n \mid n \in \mathbb{Z}\}$ is the smallest subgroup of G containing x. We write $H = \langle x \rangle$ and call H the cyclic group generated by x

Definition: We define permutation of $[n]$ as σ, where $\sigma(i) = i$ if $i \notin \{a_1, a_2, \cdots a_k\}$ and $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3 \cdots$, $\sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$. We then write $\sigma = (a_1 \cdots a_k)$ and call it a k-cycle

THEOREM 30

We define the symmetric group $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. Letting $\sigma = (123)$, $\tau = (12)$, we have $\sigma^3 = (1)$ and $\tau^2 = (1) \Rightarrow S_3 = \{1, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\} = \langle \sigma, \tau \rangle$

Thus, S_3 has one cyclic subgroup $\langle \sigma \rangle$ of order 3 and 3 cyclic subgroups $\langle \tau \rangle$, $\langle \sigma\tau \rangle$, $\langle \sigma^2\tau \rangle$ of order 2 each.

THEOREM 31

Let G be a cyclic group generated by $x \in G$:

(i) If $x^n \neq x^m$ for all $m \neq n$, then H is infinite

(ii) If $x^n = x^m$ for some $n > m$, then H is of finite order r with $r = \min\{ i > 0 \mid x^i = 1 \}$

Definition: we define the order of an element x in a cyclic group G as $\min\{ i > 0 \mid x^i = 1 \}$

THEOREM 32

If $x^m = x^n = 1$ for $m, n \in \mathbb{Z} \setminus \{0\}$, $x^{\gcd(m,n)} = 1$ and in particular, $o(x) \mid m$ and $o(x) \mid n$ and $o(x) \mid \gcd(m,n)$

THEOREM 33

Let $H = \langle x \rangle$ and 'a' be a non zero integer.

If $o(x) = \infty$, then $o(x^a) = \infty$

If $o(x) = n$, then $o(x^a) = \dfrac{n}{\gcd(a,n)}$

THEOREM 34

Let $H = \langle x \rangle$. If H is infinite, the only generators are x and $-x$. If H is finite, $H = \langle x^a \rangle$ $\forall$ a such that $\gcd(a,n) = 1$

Definition: $q = bi + cj + dk$ is called an imaginary quaternion

THEOREM 35

Purely imaginary quaternions for a 3D subspace of $\mathbb{H}$ and are $\perp$ to the real quaternions

THEOREM 36

(i) If u, v are purely imaginary quaternions and realised as vectors in $\mathbb{R}^3$,

$$uv = -\langle \vec{u}, \vec{v} \rangle + \vec{u} \times \vec{v}$$

(ii) purely imaginary unit quaternions are in one-one correspondence with the 2 sphere in $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$

(iii) Any unit vector in $\mathbb{H}$ can be written as $\cos\theta + u \sin\theta$ where u is a purely imaginary unit quaternion

THEOREM 37

If t is a unit quaternion, $\phi_t, \mu_t : \mathbb{H} \to \mathbb{H}$ as $\mu_t(q) = qt$ and $\phi_t(q) = t^{-1}q$ are orthogonal linear maps.

THEOREM 38

Let $t = \cos\theta + u \sin\theta$ be a unit quaternion where u is a purely imaginary unit quaternion. Let $V \subset \mathbb{H}$ be the 3 dim. subspace of imaginary quaternions. Then $\gamma_t : V \to V$ as $\gamma_t(q) = t^{-1} q t$ is a rotation of V with $\mathbb{R}u$ as the axis and 2θ as the angle

Definition: Let G be a group. We define the center of the group G as $Z(G) = \{ g \in G \mid gh = hg \ \forall h \in G \}$

THEOREM 39

$$Z(SU_2) = \{I, -I\}$$

Definition: We define the n-dimensional sphere $S^n \subset \mathbb{R}^{n+1}$ as $S^n = \{ x = (x_0, x_1, \dots, x_n) \in \mathbb{R}^{n+1} \;/\; \|x\| = 1 \}$.

THEOREM 40 (stereographic proj of S^2)

If $p = (1,0,0)$ is taken to be the pole and $\mathbb{R}p$ is taken to be the vertical axis of S^2, $f : S^2 \setminus p \to \mathbb{R}^2$ given by $f(x_0, x_1, x_2) = \left(\frac{x_1}{1-x_0}, \frac{x_2}{1-x_0} \right)$ is the stereographic projection of $S^2 \setminus p$ on $\mathbb{R}^2$.

Note: To include p, we define $f(p) = \infty$ and $\mathbb{R}^2$ has this one single ∞ in all directions

THEOREM 41

If $p = (1,0,0,\dots 0)$ is the pole of S^n, then, $f \to S^n \to \mathbb{R}^n$ given by $f(x_0, x_1, \dots, x_n) = \left(\frac{x_1}{1-x_0}, \frac{x_2}{1-x_0}, \dots, \frac{x_n}{1-x_0} \right)$ is the general stereographic projection for $x_0 \neq 1$ and $f(p) = \infty$

Definition: The latitudes of S^3 are the intersections of the planes $x_0 = c$, $-1 < c < 1$ with S^3

THEOREM 42

The eigenvalues of $P \in SU_2 \setminus \{ I, -I \}$ are $z, \bar{z} \in \mathbb{T}$ so that $|z| = 1$

THEOREM 43

$P, Q \in SU_2$ are conjugate in SU_2 iff $tr(P) = tr(Q)$

THEOREM 44

There is a bijection between points of the equator E of S^3 and the conjugacy class of all trace zero matrices in SU_2.

In general, there is a bijection between points on any lattitude $L(c)$ of S^3 and the conjugacy class of matrices in SU_2 with trace $2c$

THEOREM 45

Let $H = \langle x \rangle$. Every subgroup K of H is either $\{1\}$ or $\langle x^d \rangle$ where $d = \min \{ n \mid x^n \in K \}$. Further, if H is of a finite order n, then the map $d \to \langle x^{n/d} \rangle$ is a bijection between divisors of n and set of all subgroups of H

THEOREM 46

Let $G = \langle x \rangle$ be of order n and $d \mid n$. The no. of elements of order d in G is $\phi(d)$ and as a corollary we have $\sum_{d \mid n} \phi(d) = n$

Definition: For a non empty set X, the symmetric group on X is $S_X := \{ f : X \to X \mid f \text{ is a bijection} \}$. The permutation group is $[n]$ denoted S_n for convenience.

If $\sigma \in S_n$, $\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{bmatrix}$. Clearly $|S_n| = n!$

THEOREM 47

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} y \\ z \\ x \end{bmatrix} \longleftrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$ and hence permutations can be realised as matrices obtained by exchanging rows of I.

In particular, if $P = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$, $Q = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$,

$S_3 = \{I, P, P^2, Q, PQ, P^2Q\}$ with $P^3 = I$, $Q^2 = I$ and $QPQP = I$

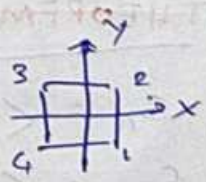
THEOREM 48

The elements of D_8 (symmetries of square) have a direct correspondence to permutations as follows.

$D_8 = \{I, \rho, \rho^2, \rho^3, \phi, \phi\rho, \phi\rho^2, \phi\rho^3\}$ where ρ is rotation by 90° and hence $\rho = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}$.

and ϕ is reflection wrt x axis and hence $\phi = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$

Note: This is when I corresponds to



Definition: $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$ in cycle notation is given by $(12)(346)(5)$ where (i) denotes fixed element and $(a_1 \cdots a_k)$ means $\begin{bmatrix} a_1 & a_2 & \cdots & a_k \\ a_2 & a_3 & \cdots & a_1 \end{bmatrix}$

Definition: $(a_1 \cdots a_r)$ & $(b_1 \cdots b_s)$ are disjoint if $\{a_1 \cdots a_r\} \cap \{b_1 \cdots b_s\} = \emptyset$

THEOREM 49

Every permutation in S_n can be written as a product of disjoint cycles

THEOREM 50

If α, β are disjoint cycles, $\alpha\beta = \beta\alpha$

THEOREM 51

If $\sigma \in S_n$ is a product of disjoint cycles of lengths $m_1, m_2, \dots, m_r$, then $o(\sigma) = \text{lcm}(m_1, m_2, \dots m_r)$

THEOREM 52

Every permutation can be expressed as a product of 2-cycles

Definition: we say that a subset S of a group G generates G if every element of G is a product of finitely many elements of S. we denote $G = \langle S \rangle$

THEOREM 53

$S_n = \langle (12), (13), \dots, (1n) \rangle$

$S_n = \langle (12), (23), \dots (n-1\ n) \rangle$

$S_n = \langle (12), (123\dots n) \rangle$

Definition: In accordance with theorem 52, if a permutation is a product of even number of transpositions, it is called even permutation else it is called an odd permutation

THEOREM 54

For each $\tau \in S_n$, it is possible to assign a sign 1 or -1 to it satisfying:

(i) if τ is a 2-cycle, $\operatorname{sgn}(\tau) = -1$.

(ii) if $\sigma, \tau \in S_n$, $\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)$

THEOREM 55

A permutation $\tau \in S_n$ is a product of even no. of transpositions iff $\tau\Delta = \Delta$ where Δ is any function; ie. $\operatorname{sgn}(\tau) = 1$

Note: if $\Delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$, then,

$\tau = (12) \Rightarrow \tau\Delta = (x_2 - x_1)(x_1 - x_3)(x_3 - x_2)$

THEOREM 56

The set of even permutations in S_n is denoted A_n and is a subgroup of S_n of order $\frac{n!}{2}$. We call it the alternating group

THEOREM 57

A_3 is the group of rotational symmetries of an equilateral triangle while A_4 is the group of rotational symmetries of a regular tetrahedron

Definition: Let G and G' be groups. A homomorphism $f: G \to G'$ is a map so that $f(ab) = f(a)f(b)$ $\forall a, b \in G$.

If f is injective and surjective, we say f is an isomorphism between G & G'. If G and G' are isomorphic, we write $G \cong G'$

THEOREM 58

All cyclic groups of order n are isomorphic to $\mathbb{Z}_n$

Definition: A map $\gamma_a : G \to G$ defined as $\gamma_a(g) = aga^{-1}$ where $a \in G$, is called a conjugation map by a. In particular bab^{-1} is the conjugate of a by b. Further, two elements $x, y \in G$ are called conjugates if $\exists\ b \in G$ so that $x = byb^{-1}$.

THEOREM 59

Let $\phi : G \to G'$ be a group homomorphism. Then $\phi(G)$ is a subgroup of G'

Definition: Let G be a group and $a \in G$. The map $T_a : G \to G$ defined by $T_a(g) = ag\ \forall\ g \in G$ is called the left translation by a

THEOREM 60 (Cayley's Theorem)

Every group is isomorphic to a group of permutations. In particular, if G has order n, then G is isomorphic to some subgroup of S_n.

In particular, the proof involves showing that $G \cong \{T_g \mid g \in G\}$ and that $\{T_g \mid g \in G\} = S_G$ or the set of permutations on G

THEOREM 61

Let $\varphi : G \to G'$ be a group homomorphism. Then $\varphi(id) = id$ and $\varphi(a^{-1}) = (\varphi(a))^{-1}\ \forall\ a \in G$

THEOREM 62

Let $\varphi : G \to G'$ be a group homomorphism.

(i) $\ker \varphi := \{ g \in G \mid \varphi(g) = id \}$ is a subgroup of G

(ii) φ is injective iff $\ker \varphi = \{ id \}$

(iii) $\forall\, g \in G \quad ghg^{-1} \in \ker \varphi \;\forall\; h \in \ker \varphi$

Definition: A subgroup $H \subset G$ is called a normal subgroup of G if $gHg^{-1} = H$ for all $g \in G$. ($H \lhd G$)

Definition: The center of a group G is a subgroup of G and further if G is abelian. $Z(G) = G$.

Moreover,

THEOREM 63

(i) $Z(G) = G$ iff G is abelian

(ii) center of a group is a normal subgroup of G

(iii) Any subgroup of an abelian group is normal

Definition: Let G be a group and $a \in G$. The centralizer of a denoted as $C(a)$ is the set

$$C(a) = \{ g \in G \mid ga = ag \}$$

THEOREM 64

$C(a)$ is a subgroup of G $\forall\, a \in G$

THEOREM 65

If $f : G_1 \to G'$ is an isomorphism, so is $f^{-1} : G' \to G$

THEOREM 66

Any infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$ and any finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +)$

Definition: An isomorphism $f: G \to G$ is called an automorphism. The group of Automorphisms of G is $Aut(G)$

Definition: Any automorphism of the form $f: G \to G$ where $f(g) = aga^{-1}$ for some $a \in G$ is called an inner automorphism. Outer automorphism is an automorphism which is not inner.

THEOREM 67

$Aut(\mathbb{Z}_n) \cong U_n$.

THEOREM 68

Every automorphism of S_3 is an inner automorphism and hence $Aut(S_3) \cong S_3$

Complicated proof but $Aut(S_n) \cong S_n \quad \forall \; n \neq 2, 6$

Definition: Let $f: S \to T$. The fibres of f are the sets $f^{-1}(t) = \{a \in S \mid f(a) = t\}$ where $t \in Im(f)$

Definition: Define a relation on S by the rule $a \sim b$ if $f(a) = f(b)$. Clearly if $a \sim b$, $a \in f^{-1}(f(b))$. Hence, the fibres of f are equivalence classes

Definition: Let $H < G$ (subgroup). Define an equivalence relation on G as $a \sim b$ if $a^{-1}b \in H$. The equivalence classes are $C_a = \{x \in G \mid a \sim x\} = \{x \in G \mid a^{-1}x \in H\}$

for some $a \in G$, $C_a = \{x \in G \mid x = ah \text{ for some } h \in H\} = aH$

we call aH as the left coset of H. Analogously Ha is the right coset of H (arise from $a \sim b$ if $b = ha$ for some $h \in H$)

THEOREM 69

Two left cosets are either equal or disjoint. Further, if $a, b \in G$, then $aH = bH \iff a \sim b \iff a^{-1}b \in H$

THEOREM 70

If $\varphi : G \to G'$ is a homomorphism, $|G| = |\ker \varphi| \cdot |\text{Im } \varphi|$

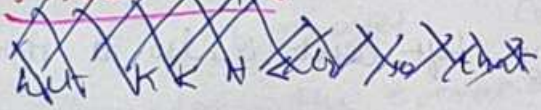
THEOREM 71

If $\mathbb{F}_q$ is a finite q element field, the map $f : GL_n(\mathbb{F}_q) \to \mathbb{F}_q^{\times}$ given by $f(A) = \det(A)$ is a surjective homomorphism and $\ker f = SL_n(\mathbb{F}_q)$.

Thus, $o(GL_n(\mathbb{F}_q)) = (q-1) \cdot o(SL_n(\mathbb{F}_q))$. But

$$o(GL_n(\mathbb{F}_q)) = \prod_{i=0}^{n-1} q^n - q^i \Rightarrow o(SL_n(\mathbb{F}_q)) = \frac{1}{q-1} \prod_{i=1}^{n-1} q^n - q^i$$

THEOREM 72



Definition: Let $H < G$. The number of left cosets of H in G is called the index of H in G and is denoted by $[G : H]$

THEOREM 72 (Lagrange's theorem)

If $H < G$, $|G| = |H|[G : H]$. In particular, the order of any subgroup divides the order of the group. Also, as a corollary, $o(a) \mid G \ \forall a \in G$.

As another corollary, if $o(G) = |G|$ is prime, then, G is cyclic.

THEOREM 73

A_4 has no subgroup of order 6 (counter for converse of Lagrange not being true in general)

THEOREM 74

Let $K < H < G$ so that $[G:H]$, $[H:K]$ are finite. Then $[G:K]$ is finite with $[G:K] = [G:H][H:K]$

THEOREM 75 (Euler, Fermat, Wilson theorems)

1) $a^{\phi(n)} \equiv 1 \pmod{n}$ if $(a,n) = 1$
($\phi(n)$ is the Euler totient function)

2) $a^p \equiv a \pmod{p}$ for prime p and any a

3) $(p-1)! \equiv -1 \pmod{p}$ iff p is prime

THEOREM 76

A subgroup is normal iff every left coset is also a right coset.

THEOREM 77

- If H is a subgroup of G and $g \in G$, $gHg^{-1} < G$
- If a group has only one subgroup of finite order, it is normal
- If $H < G$ with $[G:H] = 2$, $H \triangleleft G$

THEOREM 78 (Correspondence Theorem)

Let $f: G_1 \to G'$ be a homomorphism. Let $H' < G'$ and $f^{-1}(H') = \{g \in G \mid f(g) \in H'\}$. Let K denote $\ker(f)$. Then -

(i) $1 < C f^{-1}(H') < G$

(ii) $H < G \Rightarrow f(H) < G'$

(iii) $H' \triangleleft G' \Rightarrow f^{-1}(H') \triangleleft G$

(iv) If f is onto, $f^{-1}(H') \triangleleft G \Rightarrow H' \triangleleft G'$

(v) If f is onto, there is a one to one correspondence between $\{H \mid H < G, K \subset H\} \longleftrightarrow \{H' \mid H' < G'\}$ given by $H \longmapsto f(H)$, $H' \longmapsto f^{-1}(H')$.

Further, $H \triangleleft G \Leftrightarrow f(H) \triangleleft G'$ and

$|f^{-1}(H')| = |K||H'|$

Definition: Let N be a normal subgroup of G. The set of left cosets $G/N = \{gN \mid g \in G\}$ forms a group under the operation $gN \times hN = ghN$. This is called as the quotient group

Definition: $AB = \{ab \mid a \in A, b \in B\}$

THEOREM 79

Let $N \triangleleft G$, $aN, bN \in G/N$. Then $aNbN = abN$

THEOREM 80

The map $f: G \to G/N$ as $f(g) = gN$ is a group homomorphism. Further, $\ker f = N$

THEOREM 81 (first isomorphism theorem)

Let $f: G \to G'$ be a homomorphism and let $N = \ker f$. Then the map $\bar{f}: G/N \to \text{Im}(f)$ given by $\bar{f}(gN) = f(g)$ $\forall g \in G$ is an isomorphism

THEOREM 82

Let G be finite and abelian. Let $d \mid n = |G|$. Then, G has a subgroup of order d (converse of Lagrange is applicable for abelian groups)

THEOREM 83 (second isomorphism theorem)

If $H, N < G$, $N \triangleleft G$, $H \cap N \triangleleft H$ and further, $\frac{H}{H \cap N} \simeq \frac{HN}{N}$

THEOREM 84

If H, N are subgroups of G, HN is a subgroup of G iff $HN = NH$

THEOREM 85 (Third isomorphism theorem)

If $N \subset H$ are normal subgroups of a group G then $H/N \triangleleft G/N$ and $\frac{G/N}{H/N} \simeq \frac{G}{H}$

THEOREM 86

For any group G, $\frac{G}{Z(G)} \simeq \text{Inn}(G)$ = collection of all inner automorphisms of G

THEOREM 87

If $G/Z(G)$ is cyclic then G is abelian.

Definition: we define the product of the groups $G_1, G_2, \cdots, G_n$ as $\{(g_1, g_2, \cdots, g_n \mid g_i \in G_i \ \forall i\}$

THEOREM 88

The product of groups is a group under the binary operation $(g_1, \cdots, g_n) * (h_1, \cdots, h_n)$

$= (g_1 h_1, \cdots, g_n h_n)$

The order of this group is $\prod_{i=1}^{n} |G_i|$

THEOREM 89

Let $(g_1, \cdots, g_n) \in \prod_{i=1}^{n} G_i$. Then the order of $(g_1, \cdots, g_n) = o(g_1, \cdots g_n) = \text{lcm}(o(g_1), \cdots, o(g_n))$

★ THEOREM 90

$C_m \times C_n$ is cyclic iff $\gcd(m,n) = 1$

★ THEOREM 91 (product formula)

Let $H, K < G$ with G being finite. Then,

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

THEOREM 92

Let $H, K \neq < G$. Define $f: H \times K \to G$ by

$f(h,k) = hk$. $\text{Im}(f) = HK$.

(i) f is injective iff $H \cap K = \{1\}$

(ii) f is a homomorphism iff $hk = kh \quad \forall h \in H, k \in K$

(iii) If $H \triangleleft G$, $HK < G$

(iv) f is isomorphism iff $H, K \triangleleft G$ and $H \cap K = \{1\}$ and $HK = G$.

Definition: Let G be a group and X be any set. We say that G acts on X if there is a map $G \times X \to X$ defined as $(g, x) \mapsto x$ satisfying,

$1 \cdot x = x \quad \forall x \in X$ (unitality axiom)

$g(hx) = (gh)x \quad \forall x \in X$ (associativity axiom)

THEOREM 93

There is a one-one correspondence between set of actions of G on X and homomorphisms from G to S_X.

Further, $G \simeq \varphi(G)$

Definition: Let G operate on X. We define the orbit of $x \in X$ as a set $O(x) = \{ gx \mid g \in G \}$. The stabilizer of ~~this group~~ $x \in X$ is $G_x = \{ g \in G \mid gx = x \}$

Definition: If G acts on G by conjugation as $\alpha(g, h) := ghg^{-1}$, then the orbit of $a \in G$ is $\{ gag^{-1} \mid g \in G \}$ which is called the conjugacy class of a and the stabilizer of $a \in G$ is $\{ g \in G \mid gag^{-1} = a \}$ which is the centralizer of a, $Z(a)$

THEOREM 94

$$Z(a) = G \iff a \in Z(G)$$

Definition: Defining the group action $G \times X \to X$ where X is the set of all subgroups of G, as $(g, H) \mapsto gHg^{-1}$, the stabilizer of H is $\{g \in G \mid gHg^{-1} = H\}$. This is called the normalizer of H, $N(H)$ and it is clear that $H \triangleleft N(H)$

THEOREM 95 (Fundamental theorem of group actions) (orbit-stabilizer theorem)

Let G act on a set X

(i) Let $x \in X$. $f : G/G_x \to O(x)$ defined as $f(gG_x) = gx$ is a bijection and hence $|O(x)| = [G : G_x]$

(ii) X is a disjoint union of ~~orbits~~ distinct orbits

(iii) Let $O(x_i)$ be distinct orbits of X for $i = 1, 2, \cdots, r$

$$|X| = [G : G_{x_1}] + [G : G_{x_2}] + \cdots + [G : G_{x_r}]$$

(iv) if $g \in G$, $x \in X$ then $G_{gx} = g G_x g^{-1}$

THEOREM 96

Let p be the smallest prime dividing $|G|$ for a finite group G. If $H < G$ has index p, $H \triangleleft G$
i.e. $[G : H] = p$

THEOREM 97 (The class equation)

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : Z(x_i)]$$

Definition: A group is simple if it has no proper non-trivial subgroup (the only normal subgroups are $\{e\}$ and itself)

THEOREM 98 (Jordan's simple grp theorem)

A_5 is simple and A_n is simple for $n \geq 5$.

Consequently, the only normal subgroups of S_n $(n \geq 5)$ are A_n and $\{(1)\}$

THEOREM 99

If G has order p^n for some $n > 0$, prime p, G is called a p-group.

If G is a p-group, $Z(G) \neq \{1\}$

THEOREM 100

If $|G| = p^2$. Then G is abelian.

Lemmas used: (i) $|G| = p \Rightarrow G$ is cyclic

(ii) $G/Z(G)$ is cyclic $\Rightarrow G$ is abelian and $G = Z(G)$

THEOREM 101 (Cauchy)

if G is finite and $p \mid |G|$, G admits an element of order p

THEOREM 102 (First Sylow theorem)

Let $|G| = p^r m$ with $(p, m) = 1$. Then G has subgroups of order $p, p^2, \ldots, p^r$

Definition: Let G be some group. Subgroups of G of order p^α are called p-subgroups. Let G now have order $p^r m$. Subgroups of G of order p^r are called sylow p-subgroups

THEOREM 103 (Second sylow theorem)

Any p-subgroup of G (with $|G| = p^r m$, $(p, m) = 1$) is contained in a sylow p-subgroup ie. $P \leq gQg^{-1}$ for some g where P is a p-subgroup and Q is a sylow-p subgroup. Moreover, any two sylow-p subgroups are conjugates.

THEOREM 104 (Third sylow theorem)

$|G| = p^r m$ with $(p, m) = 1$. Let N_p denote no. of sylow p subgroups. Then $N_p \equiv 1 \pmod p$ and $N_p \mid m$

THEOREM 105

Groups of order 21 have only 2 isomorphism classes C_{21} and $\langle x, y \mid x^7 = 1 = y^3, yx = x^2 y \rangle$

THEOREM 106

Groups of order 12 have the following 5 isomorphism classes C_{12}, D_6, A_4, $C_2 \times C_2 \times C_3$, $\langle x, y \mid x^4 = y^3 = 1, yxy = x \rangle$ as the only isomorphism classes.

Definition: $B_1, B_2, \ldots, B_r < G$. We define their sum as $B_1 + \cdots + B_r := \{ x_1 + \cdots + x_r \mid x_i \in B_i \}$

(The + is just the operation in the group)

THEOREM 107

Let $H, K < G$ such that $G = H + K$ and every $g \in G$ can be uniquely written as $g = h + k$ where $h \in H$, $k \in K$.

Define $f : H \times K \to H \oplus K$ by $f(h,k) = h + k$. Then f is an isomorphism

Definition and Clarifications:

If $G = B_1 + \cdots + B_r$ and every g in G can be uniquely written as $g = b_1 + b_2 + \cdots + b_r$, then G is a direct sum of $\{B_i\}_{i=1}^{r}$ and G is said to be indecomposable if it cannot be written as a direct sum of proper subgroups.

clarifications:

$H \times K$ (cartesian product) is same as HK iff $H \cap K = \{e\}$.

$H \times K$ is same as $H \oplus K$ iff $H \oplus K = G$

HK and $H+K$ are essentially the same

THEOREM 108

Any cyclic group of order p^n is indecomposable.

THEOREM 109 (Fundamental thm for Abelian groups).

Every finite group which is abelian, is a direct sum of cyclic groups $C_{p_j^{r_j}}$ where $p_j | |G|$ are prime numbers. Moreover, r_j's are uniquely determined

THEOREM 110

Let G be a finite abelian grp of order mn where $(m,n)=1$.

Let $G(m) = \{g \in G \mid mg = 0\}$, $G(n) = \{g \in G \mid ng = 0\}$

Then $G = G(m) \oplus G(n)$

(in the sum notation $mg = g^m$ $ng = g^n$ $0 = e = 1$)

THEOREM 111

An indecomposable finite abelian group is a p-group

THEOREM 112

A non-trivial abelian p-group having a unique cyclic group of order p, is cyclic. Converse also holds.

THEOREM 113

Let G be finite abelian p-group and g be an element of maximal order. Then $G = \langle g \rangle \oplus H$ for a subgroup H

As a corollary, an indecomposable finite abelian p-group is cyclic.

THEOREM 109 (Re)

A finite abelian group is a direct sum of cyclic subgroups of prime power orders. (restating theorem 109 because it requires knowledge of theorems 110 to 113 beforehand)

Definition: A finite p-group G is said to be of the type $(p^{a_1}, p^{a_2}, \cdots, p^{a_s})$ if G is isomorphic to a product of cyclic groups as $C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_s}}$

THEOREM 114

Every finite abelian p-group is isomorphic to a product of cyclic p-groups and the $(a_1, \cdots, a_s)$ are uniquely determined

Definition: A non empty set R is called a ring if it has two binary operations denoted $+, *$ satisfying

(i) $(R, +)$ is an abelian grp

i.e. $a + b = b + a \quad \forall\, a, b \in R$

$(a+b)+c = a+(b+c) \quad \forall\, a, b, c \in R$

$\exists\, e \in R, \ \forall\, a \in R \ (a+e = e+a = a)$

$\forall\, a \in R, \ \exists\, b \in R \ (a+b = b+a = e)$

(ii) $a*(b*c) = (a*b)*c \quad \forall\, a, b, c \in R$

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

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

Note: If we allow three more rules which are that - multiplication is commutative, admits identity and every element other than zero has a multiplicative inverse, we get a field.

Definitions:

- Commutative ring : multiplication is commutative
- ring having identity : There is a multiplicative identity
- $U(R)$ or $R^\times$ is the set of all invertible elements (or called units). (This forms a group under $*$)
- division ring/skew field : $1 \neq 0$ in R, all non zero elements of R are invertible (only $a*b = b*a$ stops it from being a field)
- Zero divisor : element a of R such that $\exists\ b \neq 0$ so that $a*b = 0$ or $b*a = 0$
- integral domain : a commutative ring with id all non-zero elements of R are non zero divisors (not "non-zero divisors") (not zero divisors)

THEOREM 115

Let R be a ring. Let $-a$ denote the additive inverse of $a \in R$. Then

(i) $0*a = a*0 = 0 \quad \forall\ a \in R$

(ii) $(-a)*b = a*(-b) = -(a*b) \quad \forall\ a, b \in R$

(iii) if R has multiplicative identity, it is unique and denoted by 1. Further $-a = (-1)*a$ $\forall\ a \in R$

(iv) If a has left inverse b & right inverse c then $b = c$

Definition: A division ring which is also a finite dim real vector space is called as finite dim division algebra

THEOREM 116 (Frobenius theorem)

Any finite dimensional division algebra over the real field is isomorphic to $\mathbb{R}$ or $\mathbb{C}$

THEOREM 117 (Wedderburn's little theorem)

Every finite division ring is commutative and is hence a field.

Definition: Let R be a commutative ring with identity. We define $R[x]$ to be the set of polynomials with coefficients taken from R

THEOREM 118

If R is an integral domain (ie. $\forall a \neq 0, ab = 0 \Rightarrow b = 0$) then so is $R[x]$

(Note: $R[x]$ is a ring with usual addition and multiplication of polynomials)

Definition: For a commutative ring R with identity, we define $R[[x]]$ to be the set of formal sums $\sum_{n=0}^{\infty} a_n x^n$ where $a_n \in R \ \forall n$. This forms a ring (called the formal power series ring) with addn and multiplication defined as

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) * \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} \left(\sum_{j+k=n} a_j b_k\right) x^n$$

Definition: Let d be a square free integer. The set $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is called as the quadratic field generated by $\sqrt{d}$.

we define the field norm $N: \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ as

$$N(a+b\sqrt{d}) = (a+b\sqrt{d})(\overline{a+b\sqrt{d}}) = (a+b\sqrt{d})(a-b\sqrt{d})$$
$$= a^2 - b^2 d$$

THEOREM 119

The group of units in $\mathbb{Z}[\omega]$ is $U(\mathbb{Z}[\omega])$
$= \{\alpha \in \mathbb{Z}[\omega] \mid |N(\alpha)| = 1\}$

Definition: $\mathbb{Z}[i]$ is the ring of Gaussian integers and the units group is $\{\pm 1, \pm i\}$

Definition: A subset I of a commutative ring R having identity is called an ideal if it is an additive subgroup of R and $\forall\ r \in R$, $\forall\ a \in I$, $a \times r \in I$

Definition: An ~~ideal~~ ideal I of a ring R is called a principal ideal if $\exists\ a \in I$ s.t. $I = aR$. we say a generates I and write $I = (a)$

THEOREM 120

Every ideal of $\mathbb{Z}$ or $k[x]$ (polynomial ring) over a field k is principal

Definition: We define operations on ideals along with their significance.

(i) **Intersection**: $I_1 \cap I_2$ is the usual set intersection. The significance is that the intersection of any family of ideals is an ideal

(ii) **Sum**: $I + J := \{a+b \mid a \in I, b \in J\}$
The significance is that it is the smallest ideal of R containing I, J

(iii) **product**: $IJ := \{a_1b_1 + \cdots + a_nb_n \mid a_i \in I, b_i \in J\}$
significance is that this is also an ideal

(iv) **radical**: The radical of an ideal is $\sqrt{I}$ and it is the set $\{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}$. This is also an ideal

Definition: Let k be a field and let $R = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables. Let $m_1, \ldots, m_g$ be the monomials in R and $I = (m_1, \ldots, m_g)$ be the generated ideal. This ideal is called the **monomial ideal**

Definition: Let R, S be rings. A map $f: R \to S$ is called a **ring homomorphism** if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)\,f(b)$ and $f(1) = 1$. If further, f is a bijection, we call it a **ring isomorphism**

THEOREM 121

If $f: R \to S$ is a ring homomorphism,

(i) $f(0) = 0$

(ii) $f(a) = f^{-1}(a)$ $\forall$ $a \in R$

Definition: Let $f: R \to S$ be a ring hom. Then $f^{-1}(s)$ is the fiber of f as s varies over S

THEOREM 122

$\ker(f) = f^{-1}(0)$ is an ideal

Definition: Let R be a ring. Fix some ideal I of the ring. Let $x, y \in R$. $x \sim y$ if $x - y \in I$. This equivalence relation partitions R into disjoint subsets $x + I$ we define R/I to be the set of the equivalence classes. i.e. $\bar{x} = x + I \in R/I$, $x \in R$ Defining $\bar{x} + \bar{y} = \overline{x+y}$, $\bar{x}\bar{y} = \overline{xy}$ turns R/I into a ring. It can be shown that this addition & multiplication is well defined. Further, the map $f: R \to R/I$ defined as $f(a) = \bar{a}$ has $\ker(f) = I$.

This way we define quotient rings.

THEOREM 123 (Ring isomorphism theorems)

Let $f: R \to S$ be a surjective ring homomorphism with $\ker(f)$ denoted by K

1) $\bar{f}: R/K \to S$ defined as $\bar{f}(x+K) = f(x)$ is an isomorphism

2) There is a one-one correspondence between

$\{I \mid I \text{ is an ideal of } R, K \subset I\} \overset{\phi}{\underset{\psi}{\rightleftarrows}} \{\text{ideals of } S\}$

given by $J \xmapsto{\psi} f^{-1}(J)$, $I \xmapsto{\phi} f(I)$

3) Let J be an ideal of S. Then,

$$\frac{R}{f^{-1}(J)} \simeq \frac{S}{J}$$

Definition: An ideal I of ring R with $\neq R$ is called prime if $ab \in I$ for some some $a, b \in R$ implies either $a \in I$, $b \in I$

THEOREM 124

I is a prime ideal of a ring R iff R/I is an integral domain

THEOREM 125

Every finite integral domain is a field

THEOREM 126

Every ideal of $R = k[[x]]$ is principal and (0), (x) are the only prime ideals.

Definition : (Construction of quotient field)

Let R be an integral domain.

Define $P = \{ (a,b) \mid a \in R, b \neq 0, b \in R \}$

Define $(a,b) \sim (c,d)$ if $ad = bc$. This is an equiv relation and the equivalence class of (a,b) is denoted $\frac{a}{b}$

Put $K = \{ \frac{a}{b} \mid (a,b) \in P \}$

Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

This turns K into a field (quotient field)

THEOREM 127

Let R be an integral domain with quotient field K. Let $f : R \to L$ be an injective homomorphism or embedding of R into a field L. There is, then, a unique embedding $f^* : K \to L$ whose restriction to R is f (K is the quotient field)

Definition: An ideal $I \neq R$ is called a maximal ideal if whenever $I \subset J \subset R$ and J is another ideal of R, then $J = I$ or $J = R$

THEOREM 127

Let R be a non zero commutative ring with identity

(i) maximal ideals exist

(ii) m is a maximal ideal iff R/m is a field

~~(iii) [illegible]~~

THEOREM 128

A ring has only two ideals (i.e. (0) and R) iff it is a field

Definition:

An integral domain R is called principal ideal domain (PID) if every ideal of R is principal

Definition:

Let R be an integral domain. For $a, b \in R^\times$ and if $a = bc$ for some $c \in R$, we say b divides a. If c is a unit, we say $a \& b$ are associates and write $a \sim b$. If b, c are not units, they are called as proper divisors of a. A non zero $a \in R$ is called irreducible if it is not a unit and whenever $a = bc$ then either b or c is a unit. We say a is prime if (a) is a prime ideal

THEOREM 129

Let R be an integral domain. Let $a, b \in R$. Let $\alpha \in R$

(i) α is a unit in R iff $(\alpha) = R$

(ii) a, b are associates iff $(a) = (b)$

(iii) $a \mid b$ iff $(b) \subset (a)$

(iv) a is a proper divisor of b iff $(b) < (a) < R$

(v) a is irreducible iff (a) is maximal among proper principle ideals

(vi) $a \in \mathbb{Z}$ is prime iff (a) is a prime ideal

THEOREM 130

Let R be an integral domain, $0 \neq a \in R$, If a is a prime element, it is irreducible

Definition:

A non-zero element a of an integral domain R is said to have a unique factorisation into irreducibles if $a = up_1p_2 \cdots p_n$ for a unit $u \in R$ and irreducibles $p_1 \cdots p_n$ of R: and this is unique upto permutation of the p_i's

We say R is a unique factorisation domain (UFD) if every non-zero element has a unique factorisation

THEOREM 131

Irreducibles in a UFD are prime

Definition:

An integral domain is a factorisation domain (FD) if every non zero element can be expressed as a product of irreducibles

THEOREM 132

An FD is a UFD iff every irreducible is a prime element

Definition:

Let R be a ring. It satisfies the ascending chain condition on principal ideals if for any chain $(a_1) \subset (a_2) \subset \cdots$ of principal ideals of R, $\exists\, n$ s.t. $(a_n) = (a_{n+i})$ for $i = 1, 2, 3 \cdots$

THEOREM 133

Let R be a PID. Then ascending chain condition holds on principal ideals

THEOREM 134

If the integral domain satisfies the acc on principal ideals then it is a FD

THEOREM 135

Let R be an integral domain. If $g: R^{\times} \to N \cup \{0\}$ such that if a is a proper divisor of b, then $g(a) < g(b)$, then R satisfies the acc on principal ideals and hence is a FD

As a corollary : $\mathbb{Z}$, $\mathbb{Z}[i]$, $F[x]$, $F[[x]]$ are all FD's

THEOREM 136 (Fundamental theorem of ideal domains)

Every PID is a UFD but the converse is not true as seen by choosing $\mathbb{Z}[x]$

Definition: An integral domain R is called a Euclidean domain if $\exists$ a map $\delta: R^{\times} \to N \cup \{0\}$ s.t. $\forall a, b \in R$, $b \neq 0$, we have $a = bq + r$ where $q, r \in R$, and $r = 0$ or $\delta(r) < \delta(b)$

THEOREM 137

Every Euclidean domain is a PID and hence UFD but $R = \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is PID but not Euclidean domain (I swear, JKV has the best example set)

Definition: Let R be a UFD. Then we define the content of $f \in R[x]$ as $c(f) := \gcd\{a_i \mid a_i \text{ is a coeff of } f\}$

If $c(f) = 1$, we say $f(x)$ is primitive

THEOREM 138

If $f(x), g(x) \in R[x]$ are primitive, so is $f(x)g(x)$

As a corollary $c(f)\,c(g) = c(fg)$

THEOREM 139

Let R be a UFD with quotient field K. If $f(x), g(x)$ in $R[x]$ are primitive and associates in $K[x]$, then they are associates in $R[x]$

THEOREM 140

For a UFD R and its quotient field K, let $f(x) \in R[x]$ be irreducible. Then $f(x)$ is irreducible in $K[x]$

THEOREM 141 [Gauss theorem]

R is a UFD $\Rightarrow$ $R[x]$ is a UFD

THEOREM 142 (Eisenstein Criterion)

Let R be any integral domain, P be a prime ideal of R. Let $f(x) = a_0 + \cdots + a_n x^n \in R[x]$, $n \geq 1$. Suppose $a_0, \ldots, a_{n-1} \in P$, $a_0 \in P \setminus P^2$, $a_n \notin P$. Then $f(x)$ has no divisors of degree d s.t. $1 \leq d \leq n-1$

Definition: A prime will be called a rational prime and prime elements of $\mathbb{Z}[i]$ will be called Gaussian primes

THEOREM 143

(i) $N(a+ib) = p$ is a rational prime $\Rightarrow a+ib$ is a Gaussian prime

(ii) If π is a Gaussian prime, then $N(\pi)$ is either a rational prime or a square of a rational prime

THEOREM 144

For a rational prime p, TFAE

(i) $p = \pi\bar{\pi}$ where π is a Gaussian prime

(ii) $p = a^2+b^2$ for some $a, b \in \mathbb{N}$

(iii) $x^2 \equiv -1 \pmod{p}$ has an integer solution

(iv) $p = 2$ or $p \equiv 1 \pmod{4}$

THEOREM 145

The irreducible Gaussian integers are

(i) $1+i$ and its associates

(ii) odd rational primes

(iii) Any irreducible $a+bi$ and its associates where $a^2+b^2 = p$ where p is an odd prime

Definition: solutions (a, b, c) to $x^2+y^2 = z^2$ are called pythagorean triples

THEOREM 146

upto interchange between x & y, the pythagorean triples are precisely $(a^2-b^2, 2ab, a^2+b^2)$

TUTORIAL 1

1) Prove that $GL_n(\mathbb{R})$ is not abelian

Ans Let $A, B \in GL_n(\mathbb{R})$ be defined as

$$A_{ij} = \begin{cases} 1 & \text{if } i=1,\ j=n \\ 1 & \text{if } i=j \\ 0 & \text{otherwise} \end{cases}$$

ie. $A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}$ $\det(A) = 1$

$$B_{ij} = \begin{cases} 1 & \text{if } i+j = n+1 \\ 0 & \text{otherwise} \end{cases}$$

ie. $B = \begin{bmatrix} 0 & \cdots & 1 & 1 \\ \vdots & \iddots & 1 & \\ 1 & 1 & \iddots & \vdots \\ 1 & & \cdots & 0 \end{bmatrix}$ $\det(B) = \pm 1$

$(AB)_{11} = 1$, $(BA)_{11} = 0$

$\therefore AB \neq BA$

$\therefore GL_n(\mathbb{R})$ is not abelian

2) Show that $\mathbb{Z}_n \setminus \{\bar{0}\}$ is a group under multiplication iff n is prime

Ans Let $\bar{a}, \bar{b} \in \mathbb{Z}_n \setminus \{\bar{0}\}$

$\bar{a}\,\bar{b} = \overline{ab}$

To be a group, $\bar{a}$ must be invertible

Suppose it is a group, then $\exists\ \bar{1}$ s.t.

- $\bar{a} \cdot \bar{b} = \overline{ab} = \bar{1}$

$\therefore ab = 1 \pmod n$

$\therefore n \mid ab - 1$

$\therefore nq = ab - 1$ (for some $q \in \mathbb{Z}$)

$\therefore 1 = ab - nq$

$\therefore 1 = ab + nq'$ ($q' = -q \in \mathbb{Z}$)

$\therefore \gcd(a, n) = 1$ (from number theory)

This is true $\forall\ a \in \mathbb{Z}_n \setminus \{0\}$

$\therefore \gcd(a, n) = 1 \quad \forall\ a = 1, 2, \cdots, n-1$

$\therefore n$ is prime by definition

Conversely if n is prime,

$\forall\ a \in \{1, 2, \cdots, n-1\}$,

$\gcd(a, n) = 1$

$\therefore \exists\ r, s$ s.t.

$ar + ns = 1$

$\therefore ns = 1 - ar$

$\therefore n \mid 1 - ar$

$\therefore ar \equiv 1 \pmod n$

$\therefore \overline{a}\overline{r} = \overline{1}$

$\therefore \bar{a}\,\bar{r} = \bar{1}$

$\therefore \bar{r}$ is the inverse of $\bar{a}$ and $\bar{a}$ is invertible

$\therefore \mathbb{Z}_n \setminus \{\bar{0}\}$ is a group under multiplication

3) Show that for any $M \in SO_2(\mathbb{R})$,

$$M = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \text{ for some } \theta \in [0, 2\pi)$$

Ans $M \in SO_2(\mathbb{R})$

$\therefore M$ is an orthogonal matrix with unit det.

ie. $\det(M) = 1$

M is orthogonal $\Rightarrow$ column vectors are mutually $\perp$ unit vectors

$$\therefore M = \begin{pmatrix} \cos\theta & \sin\theta \\ \cos\phi & \sin\phi \end{pmatrix}$$

(M is orthogonal $\Rightarrow$ M^T is orthogonal)

Also, $(\cos\theta\,\hat{i} + \sin\theta\,\hat{j}) \cdot (\cos\phi\,\hat{i} + \sin\phi\,\hat{j}) = 0$

$\therefore \cos(\theta - \phi) = 0$

$\therefore \theta - \phi = 2n\pi \pm \frac{\pi}{2}$

$\therefore \phi = \theta + 2n\pi \pm \frac{\pi}{2}$

$$\therefore M = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \text{ or } \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

$\det M = 1$ forces it to be the former choice and we are done.

4) Show that any matrix in $O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$ is of the form

$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

Ans Let $M \in O_2(\mathbb{R})$

By prev problem,

$$M = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \quad \text{or} \quad M = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

$M \neq \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ since $\det M$ would be $+1$

and hence $M \in SO_2(\mathbb{R})$

$$\therefore M = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$$

5) Show that the above matrix represents reflection about the line $y = x \tan(\theta/2)$

Ans
$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x\cos\theta + y\sin\theta \\ x\sin\theta - y\cos\theta \end{bmatrix}$$

Any vector along the given line is

$(a, a\tan\frac{\theta}{2})$ and any vector

perpendicular to the given line is

$(b, -b\cot\frac{\theta}{2})$

Let $\{(1, \tan\frac{\theta}{2}) - (1, -\cot\frac{\theta}{2})\}$ be the

basis of $\mathbb{R}^2$.

Represent $\begin{bmatrix} x \\ y \end{bmatrix}$ in this basis. as

$$a \times \begin{bmatrix} 1 \\ \tan\frac{\theta}{2} \end{bmatrix} + b \times \begin{bmatrix} 1 \\ -\cot\frac{\theta}{2} \end{bmatrix}$$

$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} 1 \\ \tan\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} \cos\theta + \sin\theta \tan\frac{\theta}{2} \\ \sin\theta - \cos\theta \tan\frac{\theta}{2} \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ \tan\frac{\theta}{2} \end{bmatrix}$$

$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} 1 \\ -\cot\frac{\theta}{2} \end{bmatrix} = \begin{bmatrix} -1 \\ \cot\frac{\theta}{2} \end{bmatrix}$$

$$\therefore \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = M_\theta \begin{bmatrix} x \\ y \end{bmatrix}$$

and $M_\theta \begin{bmatrix} x \\ y \end{bmatrix} = M_\theta \cdot \left(a \begin{bmatrix} 1 \\ \tan\frac{\theta}{2} \end{bmatrix} + b \begin{bmatrix} 1 \\ -\cot\frac{\theta}{2} \end{bmatrix} \right)$

$$= a \cdot \begin{bmatrix} 1 \\ \tan\frac{\theta}{2} \end{bmatrix} - b \begin{bmatrix} 1 \\ -\cot\frac{\theta}{2} \end{bmatrix}$$

$\therefore$ component along line did not change while component $\perp$ to the line changed

$\therefore$ It is indeed a reflection about the given line $y = x \tan(\theta/2)$

6) Show that $M_\theta M_\delta$ is a rotation. Find the angle also.

Ans $M_\theta M_\delta = \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \cos\delta & \sin\delta \\ \sin\delta & -\cos\delta \end{bmatrix}$

$$= \begin{bmatrix} \cos(\delta-\theta) & -\sin(\theta-\delta) \\ \sin(\theta-\delta) & \cos(\delta-\theta) \end{bmatrix}$$

$$= R_{\theta-\delta}$$

$\therefore$ angle of rotation is $\theta - \delta$

7) Find eigenvalues and eigenvectors of R_θ, M_θ as complex matrices

Ans (i) R_θ :

$$\det(R_\theta - tI) = 0$$

$$\Rightarrow \begin{vmatrix} \cos\theta - t & -\sin\theta \\ \sin\theta & \cos\theta - t \end{vmatrix} = 0$$

$$\therefore (t-\cos\theta)^2 + \sin^2\theta = 0$$

$$\therefore t^2 - 2t\cos\theta + 1 = 0$$

$$\therefore t = \frac{2\cos\theta \pm \sqrt{4\cos^2\theta - 4}}{2}$$

$$\therefore t = \cos\theta \pm i\sin\theta = e^{\pm i\theta}$$

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = e^{\pm i\theta} \begin{bmatrix} x \\ y \end{bmatrix}$$

$$\therefore \quad x\cos\theta - y\sin\theta = e^{i\theta}x$$
$$x\sin\theta + y\cos\theta = e^{i\theta}y$$
$\Rightarrow$ soln is $y = -i^{\circ}x$
$\therefore$ e.vec is $\begin{pmatrix} 1 \\ -i \end{pmatrix}$

$$x\cos\theta - y\sin\theta = e^{-i\theta}x$$
$$x\sin\theta + y\cos\theta = e^{-i\theta}y$$
soln is $y = ix$
$\therefore$ e.vec is $\begin{pmatrix} 1 \\ i \end{pmatrix}$

(ii) S_θ :

$$\det(S_\theta - tI) = 0$$
$$\Rightarrow \begin{vmatrix} \cos\theta - t & \sin\theta \\ \sin\theta & -\cos\theta - t \end{vmatrix} = 0$$
$$\Rightarrow t^2 - \cos^2\theta - \sin^2\theta = 1$$
$$\Rightarrow t^2 = 1$$
$$\Rightarrow t = \pm 1$$
$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \pm\begin{bmatrix} x \\ y \end{bmatrix}$$

$$x\cos\theta + y\sin\theta = x$$
$$x\sin\theta - y\cos\theta = y$$
soln is $\frac{y}{x} = \frac{1-\cos\theta}{\sin\theta}$
$\therefore$ e.vec is $\begin{pmatrix} 1 \\ \frac{1-\cos\theta}{\sin\theta} \end{pmatrix}$
$= \begin{pmatrix} 1 \\ \tan\theta/2 \end{pmatrix}$

$$x\cos\theta + y\sin\theta = -x$$
$$x\sin\theta - y\cos\theta = -y$$
soln is $\frac{y}{x} = -\frac{(1+\cos\theta)}{\sin\theta}$
$\therefore$ e.vec is $\begin{pmatrix} 1 \\ -\frac{(1+\cos\theta)}{\sin\theta} \end{pmatrix}$
$= \begin{pmatrix} 1 \\ -\cot\frac{\theta}{2} \end{pmatrix}$

8) Find the order of the group $GL_2(\mathbb{Z}_3)$

Ans Any matrix in $GL_2(\mathbb{Z}_3)$ has 2 columns.

The first column can be any vector except $(0,0)$ to preserve invertibility

$\therefore$ choices $= 3 \times 3 - 1 = 8$

The second column can be any vector except any scalar multiple of the first column.

Given a first column, there are 3 scalar multiples (multiplying by 0 or 1 or 2)

$\therefore$ choices $= 3 \times 3 - 3 = 6$

$\therefore |GL_2(\mathbb{Z}_3)| = 8 \times 6 = 48.$

9) Find the order of $GL_n(\mathbb{F}_p)$

Ans Proceeding exactly as above:

choices for $C_1 = p^n - 1$

choices for $C_2 = p^n - p$

choices for $C_3 = p^n - p^2$

$\vdots$

choices for $C_n = p^n - p^{n-1}$

$\therefore$ Total choices $= |GL_n(\mathbb{F}_p)| = \prod_{i=1}^{n-1} (p^n - p^i)$

10) Find orders of all elements in $\mathbb{Z}_{12}$ (additive)

Ans we brute force our way through

$o(\bar{0}) = 1$

$\bar{1} + \bar{1} + \cdots + \bar{1}$ (12 times) $= \bar{0} \Rightarrow o(\bar{1}) = 12$

$\bar{2} + \bar{2} + \cdots + \bar{2}$ (6 times) $= \bar{0} \Rightarrow o(\bar{2}) = 6$

$\bar{3} + \bar{3} + \cdots + \bar{3}$ (4 times) $= \bar{0} \Rightarrow o(\bar{3}) = 4$

$\bar{4} + \bar{4} + \cdots + \bar{4}$ (3 times) $= \bar{0} \Rightarrow o(\bar{4}) = 3$

$\bar{5} + \bar{5} + \cdots + \bar{5}$ (12 times) $= \bar{0} \Rightarrow o(\bar{5}) = 12$

Similarly others

ex: for $\bar{5}$, $n \times \bar{5} = \bar{0}$

$\therefore 12 \mid 5n$

least such non zero $n = 12$

11) Find orders of all elements in $\mathbb{Z}_{12} \setminus \{\bar{0}\}$ (multiplicative)

Ans $\mathbb{Z}_{12} \setminus \{\bar{0}\} = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

(as proved in Q2, only those a are present s.t $\gcd(a, 12) = 1$)

$o(\bar{1}) = 1$

$o(\bar{5}) = 2$ ($\because 25 \equiv 1$)

$o(\bar{7}) = 2$ ($\because 49 \equiv 1$)

$o(\bar{11}) = 2$ ($\because 121 \equiv 1$)

12) let $G = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Show that all non zero elements form a group under multiplication

Ans (i) multiplication is a binary operation:

$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2} \in G$

(ii) multiplication is associative

$\big((a+b\sqrt{2})(c+d\sqrt{2})\big)(e+f\sqrt{2}) = \big((ac+2bd)+(ad+bc)\sqrt{2}\big)(e+f\sqrt{2})$

$= (ace + 2bde + 2acf + 2bdf) + \sqrt{2}(acf + 2bdf + ace + bde)$

$= (a + b\sqrt{2})\left((ce + 2df) + \sqrt{2}(cf + de)\right)$

$= (a + b\sqrt{2})(\quad\quad (c + d\sqrt{2})(e + f\sqrt{2}))$

(iii) multiplication admits identity

Claim that $1 + 0\sqrt{2} = 1$ is the identity

$(a + b\sqrt{2}) \cdot (1 + 0\sqrt{2}) = a + b\sqrt{2} \quad \forall\ a, b \in \mathbb{Q}$

(iv) multiplication has inverse

$(a + b\sqrt{2})\left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right) = 1$

13) Show that $|x| = |x^{-1}| = |g^{-1}xg| \quad \forall g \in G$ where x is some element of G. Deduce $|ab| = |ba|$

Ans Let $o(x) = |x| = n$

$\therefore x^n = 1$

$(g^{-1}xg)^n = g^{-1}x^n g$

$= g^{-1}g$

$= 1$

$\therefore |g^{-1}xg| \leq n$ and $|g^{-1}xg| \mid n$.

Let $m = |g^{-1}xg|$

$\therefore (g^{-1}xg)^m = g^{-1}x^m g = 1$

$\Rightarrow x^m g = g$

$\Rightarrow x^m = 1$

$\Rightarrow n \mid m$

we have $m \mid n$, $n \mid m$

$\therefore m = n$

$\therefore |x| = |g^{-1} x g| \quad \forall\ g \in G$

~~[illegible]~~

~~[illegible]~~

~~[illegible]~~

but $|x^{-1}| = m$, $|x| = n$

$\therefore (x^{-1})^n = 1$

$\therefore x^{-n} = 1 \Rightarrow x^n = 1$

$\therefore n \mid m$

$(x^{-1})^n = x^{-n} = 1 \quad (\because x^n = 1)$

$\therefore m \mid n$

$\therefore m = n$

$\therefore |x| = |x^{-1}|$

$ab = b^{-1} b a b = b^{-1} (ba) b$

$\therefore |ab| = |ba|$

14) If $x^2 = 1 \ \forall\ x \in G$ prove G is abelian

Ans $x^2 = 1 \ \forall\ x \in G$

In particular, for any $a \in G$, $b \in G$,

we have $ab \in G$

and $(ab)^2 = 1$

$\therefore abab = 1$

$\therefore a(ba)b = 1$

$\therefore a \cdot a(ba)bb = ab$

$\therefore a^2 ba b^2 = ab$

$\therefore ba = ab$

This holds for all $a, b \in G$

$\therefore$ By definition, G is abelian

15) Prove that any finite grp of even order contains an element of order 2 (other than Id)

Ans (Dead easy using Lagrange theorem/Cauchy theorem)

Let $t(G) = \{ g \in G \mid g^2 \neq 1 \}$

If $g \in t(G)$, then $g \neq g^{-1}$ and vice versa

Also $g \in t(G) \iff g^{-1} \in t(G)$

$\therefore t(G)$ has an even no. of elements

$1 \notin t(G)$

$\therefore 1 + |t(G)|$ is odd

But $|G|$ is even

If no element of G has order 2, all elements of G are either 1 or are in $t(G)$

$\therefore G = \{1\} \cup t(G)$

$\therefore |G| = 1 + |t(G)|$

But LHS is even while RHS is odd

$\lightning$ contradiction

$\lightning$ $\exists\ g \in G$ s.t. $g \notin t(G)$ ie.

$g^2 = 1$

16) $H(F)$ denotes heisenberg group which has matrix of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ s.t. $a, b, c \in F$ and the operation is multiplication.

(i) Find formulae for products & inverses

(ii) Show that $(HF, \times)$ is non-abelian

(iii) Show that all elements other than id have 6 order

(iv) Show that $|H(\mathbb{F}_p)| = p^3$ for a prime p.

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

Ans (i) $\begin{bmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{bmatrix}$

$= \begin{bmatrix} 1 & a_1+a_2 & b_1+b_2+a_1c_2 \\ 0 & 1 & c_1+c_2 \\ 0 & 0 & 0 \end{bmatrix}$

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

(ii)
$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & y+b+az \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & y+b+xc \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{bmatrix}$$

They will commute iff $az = cx$

Choose $a=0, c=1, x=1, z=1$

(any field always has 0, 1)

$\therefore$ non abelian

(iii)
$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & na & \gamma_n \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{bmatrix} = I \text{ (set)}$$

$\therefore na = 0 = nc = \gamma_n$

$\therefore a = c = 0$

$\therefore \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^n = I$

$\therefore \begin{bmatrix} 1 & 0 & nb \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I \Rightarrow b = 0$

$\therefore$ we did not get a non-identity matrix

$\therefore$ Contradiction

Since $M^1 = I$ holds iff $M = I$

(iv) Choices for $a, b, c = p^3$

(v) $\mathbb{F}_2 = \{0, 1\}$

$a = b = c = 0 \Rightarrow$ order $= 1$

otherwise,

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2a & 2b + ac \\ 0 & 1 & 2c \\ 0 & 1 & 1 \end{bmatrix}$$

if $a = 0$ or 1, $2a = 0$

if $c = 0$ or 1, $2c = 0$

if $b = 0$ or 1, $2b = 0$

$\therefore$ It is reduced to $\begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$\therefore$ if a or $c = 0$, order is 2

if not,

then in the case of $a = 1, c = 1$,

$$\begin{bmatrix} 1 & 1 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$\therefore$ order is infinite for $a=1, c=1, b=0$ or 1 (two cases)

17) Let G be a finite group. Prove $\exists\ n \geq 0$ so that $a^n = 1\ \forall a \in G$

Ans Let $S = \{1, g, g^2, \ldots\}$

Since G is finite, S is finite

$\therefore g^i = g^j$ for some $i > j$

$\therefore g^{i-j} = 1 \Rightarrow n_g = i - j$

Doing this process for every $g \in G$, we can show existence of n

(If we want one common n for all $g \in G$, choose it to be the lcm of the individual n_g's)

16) Let $\forall a, b \in G$, $(ab)^2 = a^2b^2$. Prove G is abelian

Ans $(ab)^2 = a^2b^2$

$abab = aabb$

$\therefore ba = ab$

18) Find $a, b \in S_3 = \langle a, b, c \mid a^2 = b^2 = c^3 = abc = 1 \rangle$ s.t. $(ab)^2 \neq a^2b^2$

Ans $(ab)^2 = (c^{-1})^2 = (c^2)^2 = c^4 = c^3 \cdot c = c$

$a^2b^2 = 1 \cdot 1 = 1$

$\therefore (ab)^2 \neq a^2b^2 \quad \forall a, b \in S_3$

20) Give a group where a, b have finite order, but ab has infinite order

Ans $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}$

in $GL_2(\mathbb{Q})$

$A^4 = B^6 = I \Rightarrow o(A) = 4,\ o(B) = 6$

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

$$\therefore (AB)^n = \begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}$$

$\therefore o(AB)$ is infinite.

TUTORIAL 2

1) Let s be rotation of plane with angle $\pi/2$ about $[1,1]$. write a formula for s as a product $t_a f_\theta$

Ans

$$s = t_{(1,1)}\, f_{\frac{\pi}{2}}\, t_{(-1,-1)}$$

$$= t_{(1,1)}\, t_{f_{\pi/2}(-1,-1)}\, f_{\pi/2} \quad \text{(thm 2.1)}$$

$$= t_{(1,1)}\, t_{(1,-1)}\, f_{\pi/2}$$

$$= t_{(2,0)}\, f_{\pi/2} \quad \text{(thm 2.1)}$$

2) Let s be reflection about $x = 1$. Find an isometry g such that $gtg^{-1} = s$, write s as $t_a f_\theta$ & (note: t_a is reflection wrt x-axis)

Ans

Claim: $g = t_{(1,0)} \cdot \rho_{\pi/2}$ works.

$$
\begin{aligned}
g s g^{-1} &= t_{(1,0)}\, \rho_{\pi/2}\, s\, \rho_{-\pi/2}\, t_{(-1,0)} \\
&= t_{(1,0)}\, \rho_{\pi/2}\, \rho_{\pi/2}\, s\, t_{(-1,0)} \\
&= t_{(1,0)}\, \rho_{\pi}\, t_{s(-1,0)}\, s \\
&= t_{(1,0)}\, \rho_{\pi}\, t_{(1,0)}\, s \\
&= t_{(1,0)}\, t_{\rho_\pi(-1,0)}\, \rho_{\pi}\, s \\
&= t_{(1,0)}\, t_{(1,0)}\, \rho_{\pi}\, s \\
&= t_{(2,0)}\, \rho_{\pi}\, s \\
&= s
\end{aligned}
$$

All using theorem 21

The last step is because

$$
\begin{aligned}
&(t_{(2,0)} \circ \rho_\pi \circ s)\,(a,b) \\
&= t_{(2,0)}\, \rho_\pi\, (a,-b) \\
&= t_{(2,0)}\, (-a,b) \\
&= (2-a,\, b) \\
&= s\,(a,b)
\end{aligned}
$$

3) Let l_1, l_2 be lines through $(0,0)$ intersecting at π/n. Let s_i be the reflection about l_i. Prove that s_1, s_2 generate the dihedral group D_{2n}

Ans WLOG,

y_1 is $y = 0$ line

y_2 is $y = \tan\left(\frac{\pi}{n}\right) x$ line

r_1 is reflection about y_1 $\Rightarrow$ r_1 is given by $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

r_2 is reflection about y_2 $\Rightarrow$ r_2 is given by $B = \begin{bmatrix} \cos\left(\frac{2\pi}{n}\right) & \sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & -\cos\left(\frac{2\pi}{n}\right) \end{bmatrix}$

(reflection about $y = x \tan\frac{\theta}{2}$ is $\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}$)

notice that $BA = \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix} = \rho_{\frac{2\pi}{n}}$

Claim: $\langle A, B \rangle = \langle A, BA \rangle$

since $BA = BA$

and $(BA) \cdot A = B$

BA is represented by $\rho_{\frac{2\pi}{n}}$

A is represented by s

$\therefore \langle BA, A \rangle$ is the dihedral group D_{2n}

4) Let f, g be rotations about distinct points with non zero angles of rotation θ, ϕ. Prove that $\langle f, g \rangle$ contains a translation

Ans WLOG $f = f_\theta$

$$g = t_a f_\phi t_{-a}$$
$$= t_a t_{\phi f_\phi(-a)} f_\phi$$
$$= t_{a + f_\phi(-a)} f_\phi$$
$$= t_{a+a'} f_\phi$$

$$f \cdot g = f_\theta t_{a+a'} f_\phi$$
$$= t_{f_\theta(a+a')} f_{\theta+\phi}$$

$$g \cdot f = t_{a+a'} f_{\theta+\phi}$$

$$(fg)(gf)^{-1} = t_{f_\theta(a+a')} f_{\theta+\phi} f_{(-\theta-\phi)} t_{-(a+a')}$$

$$= t_{f_\theta(a+a')-a-a'}$$

This is a translation provided it is not identity

ie. $f_\theta(a+a') \neq a+a'$

This will happen only if $a+a' = (0,0)$

ie. if $a + f_\theta(-a) = (0,0)$

$\theta \neq 0$ and hence this never happens

5) Prove that a linear operator on $\mathbb{R}^2$ is a reflection iff its eigen values are ± 1 and the e.vecs corresponding to $+1, -1$ are orthogonal

Ans ($\Rightarrow$) already proven in Q7 of tut 1

($\Leftarrow$) let f be linear with e-vecs v and u s.t.

$v \cdot u = 0$, $f(v) = v$, $f(u) = -u$

$v \perp u \Rightarrow \{v, u\}$ is a basis of $\mathbb{R}^2$

matrix of f wrt $\{v,u\}$ basis is $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ which

is orthogonal

$\therefore \vec{v} \cdot \vec{u} = v^T u = (f(v))^T (f(u))$

(orthogonal operator preserves dot product)

$= -v^T u$

$\therefore v^T u = 0$

Moreover, f is a reflection about the line joining $\vec{0}$ and $\vec{v}$ since all vectors $\parallel$ to $\vec{v}$ are unchanged & vectors $\parallel$ to $\vec{u}$ flip sign. and

u & v are $\perp$

6) let G be an abelian group. Prove that $t(G) := \{g \in G \mid |g| < \infty\}$ is a subgroup of G ('torsion subgroup'). Give example to show that $t(G)$ is not a subgroup when G is non-abelian

Ans $t(G) = \{ g \in G \mid |g| < \infty \}$

Clearly $1 \in t(G)$

let $a, b \in t(G)$

Then $(ab)^{\text{lcm}(|a|,|b|)} = a^{\text{lcm}|a|,|b|} \times b^{\text{lcm}|a|,|b|}$

$= 1$

$\therefore ab \in t(G)$

Let $a \in t(G)$ with $a^n = 1$

then $(a^{-1})^n = 1$

$\therefore a^{-1} \in t(G)$

$\therefore t(G) < G$

For nonabelian G, take ex of Q20 of tut 1

in which $A \in t(G)$, $B \in t(G)$ but $AB \notin t(G)$

7) Show that $\{g \in D_{2n} \mid g^2 = 1\}$ is not a subgroup of D_{2n} for $n \geq 3$

Ans We know $\langle r, f_{\frac{2\pi}{n}} \rangle = D_{2n}$

and hence $\langle r, f_{\frac{2\pi}{n}} r \rangle = D_{2n}$

(since $f_{\frac{2\pi}{n}} = \left(f_{\frac{2\pi}{n}} r\right) \cdot r$)

order of $r = 2$

order of $f_{\frac{2\pi}{n}} r = 2$ ($\because f_{\frac{2\pi}{n}} r f_{\frac{2\pi}{n}} r$

but order of $= f_{\frac{2\pi}{n}} f_{-\frac{2\pi}{n}} r r$

$\left(f_{\frac{2\pi}{n}} \cdot r\right) \cdot r = f_{\frac{2\pi}{n}}$ $= 1$)

is n

$\therefore r \in \{g \in D_{2n} \mid g^2 = 1\}$, $f_{\frac{2\pi}{n}} \cdot r \in \{g \in D_{2n} \mid g^2 = 1\}$

But $(\rho_{\frac{2\pi}{n}} \circ \mu_x)(x) \notin \{ g \in D_{2n} \mid g^2 = 1 \}$

8) Let G be a group and $x, y \in G$ have finite orders m, n respectively. Prove that $|xy|$ divides $\text{lcm}(m,n)$. Give an example of x, y so that $|xy| < \text{lcm}(m,n)$. What can you say about $|xy|$ if $xy \neq yx$

Ans If $xy = yx$,

$(xy)^k = x^k y^k$ (proved using induction)

$\therefore (xy)^{\text{lcm}(m,n)} = x^{\text{lcm}(m,n)} \, y^{\text{lcm}(m,n)}$

$= 1 \times 1$

(since $\text{lcm}(a,b) = t \times a$ for some $t \in \mathbb{Z}$)

$\therefore |xy| \mid \text{lcm}(m,n)$

Let x be such that $|x| = n > 1$

Then choosing $y = x^{-1}$, $|y| = |x^{-1}| = n$

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

and $|xy| = |x x^{-1}| = |e| = 1$

If $xy \neq yx$, we restate ex from tut 1 Q20

i.e. $|xy|$ may be infinite

9) Fix a prime p and define $Z = \{ z \in \mathbb{C} \mid z^{p^n} = 1 \text{ for some } n \}$

Prove that:

(i) $H_k := \{ z \in \mathbb{C} \mid z^{p^k} = 1 \}$. Prove that H_k is cyclic

(ii) Any proper subgroup of Z is of the form of H_k

(iii) Z is not finitely generated

Ans (i) $H_k = \{ z \in \mathbb{C} \mid z^{p^k} = 1 \}$

H_k is the set of the p^k-th roots of unity.

$\therefore H_k = \{ e^{\frac{2\pi i}{p^k}} \mid i = 0, 1, \ldots, p^k - 1 \}$

Clearly H_k is cyclic with $H_k = \langle e^{\frac{2\pi}{p^k}} \rangle$

(ii) $\{1\}$ is clearly a subgroup of $\mathbb{Z}$ and

Clearly $H_0 = \{ z \in \mathbb{C} \mid z = 1 \} = \{1\}$

Let M be a proper subgroup of $\mathbb{Z}$ other than $\{1\}$

Let $z_0 \in M$

Note that $z_0^{p^k} = 1 \Rightarrow z_0^{p^{k+i}} = (z_0^{p^k})^{p^i} = 1$

$\forall\ i > 0$

$\therefore$ Let $z_0 \in H_\alpha$ where α is the least possible value i.e. $z_0 \notin H_\beta\ \forall\ \beta < \alpha$

Then $(z_0^2)^{p^k} = (z_0^{p^k})^2 = 1$

$\therefore z_0^2 \in M$

Similarly all powers of $z_0 \in M$

$\therefore H_\alpha \subseteq M$

Let $z_1 \in M$ s.t. $z_1 \notin H_\alpha$

Let $z_1^{p^\beta} = 1$ i.e. $z_1 \in H_\beta$

Note that $H_0 \subseteq H_1 \subseteq \cdots \subseteq H_\alpha \cdots \subseteq H_\beta$

further let β be lowest possible index

$\therefore$ $z_1 \in H_\alpha$, $z_2 \in H_\beta$ (both minimally)

since M is a subgroup of Z,

$z_1 z_2 \in M \subseteq Z$

$\therefore \exists\ n \in \mathbb{N}$ s.t.

$(z_1 z_2)^{p^n} = 1$

choosing $n \geq \beta$ does the job

$\therefore$ $H_\beta \subseteq M$

In fact, if we keep doing this, we end up with the following idea.

let $z_1 \in M < Z$

let $z_1 \in H_\alpha$ and $z_1 \notin H_m$ $\forall\ m < \alpha$

$\therefore$ $H_\alpha \subseteq M$

let $z_2 \in M \setminus H_\alpha$

let $z_2 \in H_\beta$ (minimally)

Then $H_\beta \subseteq M$ Also $\beta > \alpha \Rightarrow H_\alpha \subsetneq H_\beta \subseteq M$

Since M is finite, the process ends with $H_\delta = M$ for some index δ and we are done

(iii) let Z be finitely generated.

Then $Z = \langle z_1, z_2, \cdots, z_n \rangle$

where $z_i \in H_{k_i} \quad \forall i = 1, 2, \cdots n$

(Because if $z_1, z_2 \in H_{k_t}$ for some t, H_{k_t} being cyclic, we can delete either z_1 or z_2)

WLOG $k_1 < k_2 < \cdots < k_n$

But $H_{k_1} \subseteq H_{k_2} \subseteq \cdots \subseteq H_{k_n}$

$\therefore Z = \langle z_n \rangle = H_{k_n}$

This is a contradiction since Z is infinite while A_{k_n} is finite

1a) Describe all groups with no proper subgroups

Ans $\{e\}$ is a group with no proper subgroups

if $G \neq \{e\}$ $\exists\ g \in G$ s.t. $g \neq id$

$H = \{1, g, g^2, \cdots\}$ is a subgroup

$\therefore G = H$ (no proper subgroups)

If $|G| = \infty$,

then $F = \{1, g^2, g^4 \cdots\}$ is a subgroup

$\therefore G = \{1, g, g^2, \cdots, g^{n-1}\}$

but if n is not prime, then $n = mn'$

then $\{1, g^m, g^{2m}, \cdots, g^{mn'}\}$ is a proper subgroup

$\therefore n$ is prime $\Rightarrow G = \langle g \rangle$ finite

TUTORIAL 3

1) Give a geometric argument to find a formula to find a formula for reflection in $\mathbb{R}^n$ wrt the hyperplane $u^\perp \subset \mathbb{R}^2$ where $\|u\| = 1$

Ans We know that u is a unit vector and $u^\perp$ denotes the vector space generated by the hyperplane perpendicular to u

Let v be a vector in $\mathbb{R}^n$ to be reflected.

If $v \in u^\perp$, $\text{reflec}(v) = \text{ref}(v) = v$

Let $v \notin u^\perp$

If $v = \lambda u$ for some λ,

$\text{ref}(v) = -\lambda u$

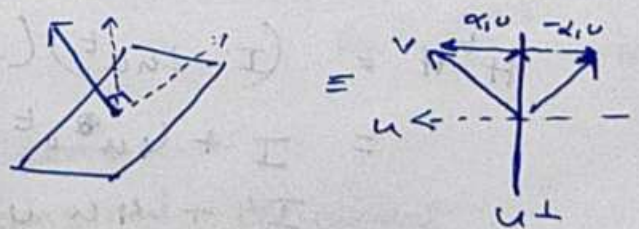
Let $\{u, v_1, v_2, \cdots, v_{n-1}\}$ be a basis for $\mathbb{R}^n$.

Clearly, $v_1, v_2, \cdots, v_{n-1} \in u^\perp$

Let $v = \alpha_1 u + \alpha_2 v_1 + \cdots + \alpha_n v_{n-1}$

Then $\text{ref}(v) = -\alpha_1 u + \alpha_2 v_1 + \cdots + \alpha_n v_{n-1}$

We flipped component $\parallel$ to u and kept those components same which were $\perp$ to u.



2) Let $u, v \in \mathbb{R}^3$. Let $H_u = I - 2uu^t$, $H_v = I - 2vv^t$ be the reflection matrices w.r.t the hyperplanes of u^t, v^t. Verify that they are indeed reflection matrices. Also verify that $H_u H_v$ is a rotation. Find its axis and the angle.

Ans $H_u(u) = (I - 2uu^t)u$

$= u - 2uu^t u$

$= u - 2u \quad (\because u^t u = 1)$

$= -u$

$H_u(v) = (I - 2uu^t)v \quad (\text{where } v \perp u)$

$= v - 2u u^t v$

$= v - 0 \quad (\because u^t v = \vec{u} \cdot \vec{v} = 0)$

$= v$

$\therefore H_u$ is indeed a reflection in $u^\perp$

$H_u H_v = (I - 2uu^t)(I - 2vv^t)$

$= I + 4uu^t vv^t - 2uu^t - 2vv^t$

Cant proceed from here :c

Claim: H_u is orthogonal

$H^t = (I - 2uu^t)^t$

$= I - 2uu^t$

$H^t H = (I - 2uu^t)(I - 2uu^t)$

$= I + 4u v^t u v^t - 2uu^t - 2uu^t$

$= I + 4u v^t - 4uv^t = I$

$\therefore H^t H = I \Rightarrow H$ is orthogonal

$\therefore \det(H) = \pm 1$

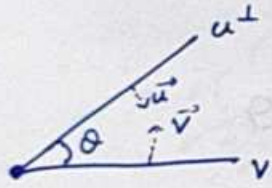
$\therefore \det(H_u H_v) = (\pm 1)(\pm 1) = 1$

($\because H_u, H_v$ are reflection matrices)

product of orthogonal matrices is orthogonal

$\therefore H_u H_v$ is orthogonal with det 1 $\Rightarrow H_u H_v$ is indeed a rotation in $\mathbb{R}^3$

Claim: $H_u H_v$ is a rotation about the line of intersection of the planes $u^\perp, v^\perp$ by 2θ where θ is the angle between $\vec{u}, \vec{v}$



$\odot \vec{m}$

Any point on the this, say $\vec{\omega}$ is perpendicular to both $\vec{u}, \vec{v}$ and hence

$H_u H_v(\omega) = H_u(H_v(\omega)) = H_u(\omega) = \omega$

Consider $\vec{\omega} \perp \vec{m}$ (where m is perp to both u, v)

Then $\vec{\omega} = \lambda_1 \vec{u} + \lambda_2 \vec{v}$

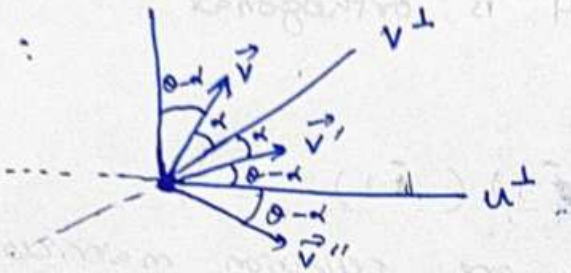
$H_u H_v(\lambda_1 \vec{u} + \lambda_2 \vec{v}) = H_u(\lambda_1 H_v(\omega) - \lambda_2 \vec{v})$

$= \lambda_1 H_u H_v(\vec{u}) - \lambda_2 H_u(\vec{v})$

$\theta = \vec{u} \cdot \vec{v}$

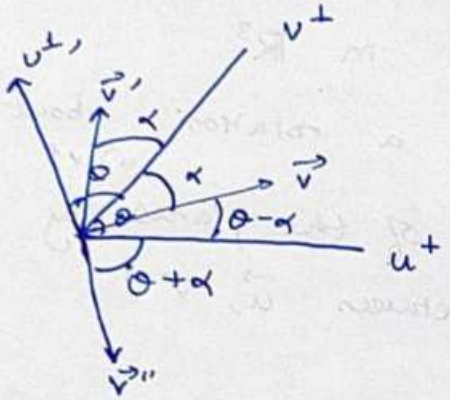
We give a geometrical argument

Case 1 :



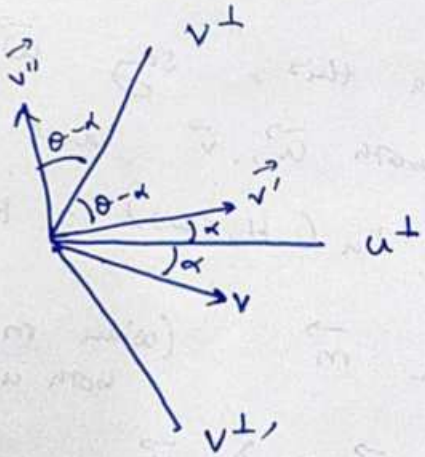
angle between $\vec{v}$, $\vec{v}''$ $= 2\theta$

Case 2 :



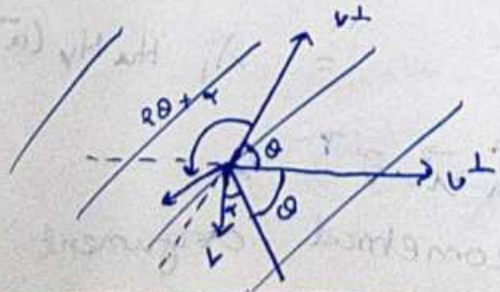
angle between $\vec{v}$, $\vec{v}''$ $= 2\theta$

Case 3 :

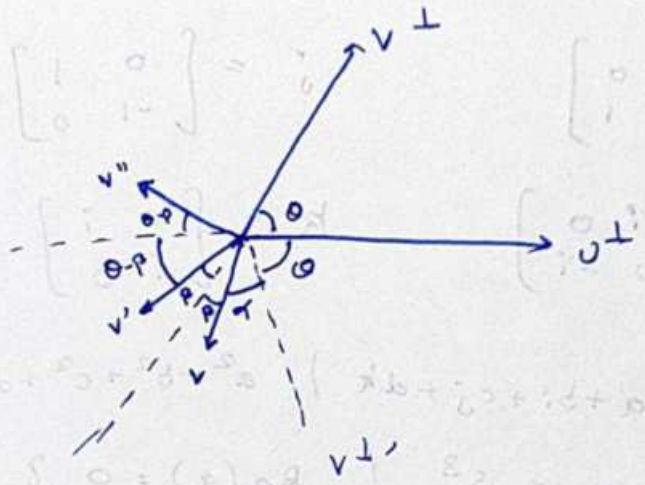


angle between $\vec{v}$, $\vec{v}''$ $= 2\theta$

Case 4 :

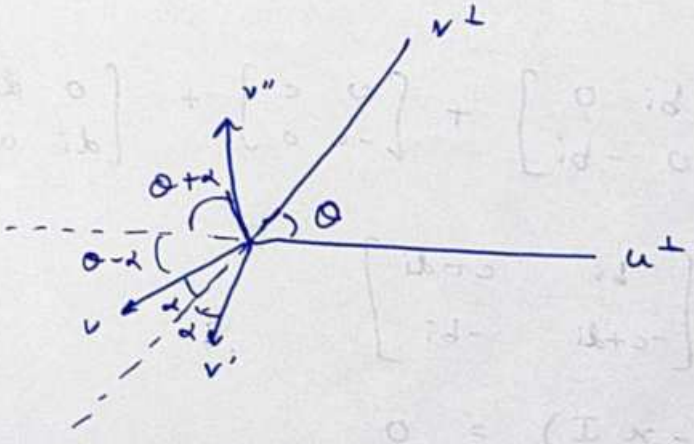


Case 4



angle between $v, v'' = 2\theta$

Case 5



angle between $v, v'' = 2\theta$

3) The algebra $\mathbb{H}$ of quaternions is a 4D real vector space with basis as the 4 matrices I, i, j, k. Let S^3 be quaternions of length 1. The equator of S^3 is the set of matrices $\mathbb{E} = \{ bi + cj + dk \mid b^2 + c^2 + d^2 = 1 \}$. Show that TFAE

(i) $A \in \mathbb{E}$

(ii) eigen values of A are $i, -i$

(iii) $A^2 + I = 0$

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

$i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ $k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$

$S^3 = \{ a + bi + cj + dk \mid a^2 + b^2 + c^2 + d^2 = 1 \}$

$E = \{ q \in S^3 \mid Re(q) = 0 \}$

(i) → (ii)

$A \in E$

$\therefore A = \begin{bmatrix} bi & 0 \\ 0 & -bi \end{bmatrix} + \begin{bmatrix} 0 & c \\ -c & 0 \end{bmatrix} + \begin{bmatrix} 0 & di \\ di & 0 \end{bmatrix}$

$= \begin{bmatrix} bi & c+di \\ -c+di & -bi \end{bmatrix}$

$\det(A - xI) = 0$

$\therefore \begin{vmatrix} bi - x & c+di \\ -c+di & -bi - x \end{vmatrix} = 0$

$\therefore x^2 + b^2 + c^2 + d^2 = 0$

$\therefore x^2 + 1 = 0$

$\therefore x = \pm i$

(ii) → (iii)

eigen values are $\pm i$

Matrix is a 2×2 matrix

$tr(A) = \lambda_1 + \lambda_2 = 0$

$\det(A) = \lambda_1 \lambda_2 = i(-i) = 1$

$\therefore A^2 + I = 0$ (2x2 characteristic eqn)

(iii) $\rightarrow$ (i)

$A^2 + I = 0$

$\therefore (\det(A))^2 = \det(-I) = 1$

$\therefore \det(A) = \pm 1$

Let $A = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$

$\alpha\delta - \beta\gamma = \pm 1$

and $\alpha^2 + \beta\gamma + 1 = 0$

$\delta^2 + \beta\gamma + 1 = 0$

$\alpha\beta + \delta\beta = 0$

$\alpha\gamma + \gamma\delta = 0$

Case 1: $\beta = 0$

$\alpha^2 + 1 = 0 \Rightarrow \alpha = \pm i$

$\delta^2 + 1 = 0 \Rightarrow \delta = \pm i$

$\alpha\delta = \pm 1$ (anyways satisfied)

$(\alpha + \delta)\gamma = 0$

Case 1.1: $\gamma = 0$

$\therefore A = \begin{bmatrix} \pm i & 0 \\ 0 & \pm i \end{bmatrix}$

Choosing $A = \begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}$, we see that

$A^2 + I = 0$ is indeed true but $A \notin E$

Thus the question is wrong ! LOL !

4) Show that the 3D subspace V of $\mathbb{H}$ generated by purely imaginary quaternions is orthogonal to the line of real quaternions

Ans Let $q \in V$

Then $q = bi + cj + dk$

Let $q' \in V^{\perp}$ = line of real quaternions

$\therefore q' = a$

note : $a, b, c, d \in \mathbb{R}$.

$$q \cdot q' = a \cdot (bi + cj + dk)$$

$$= 0$$

5) (i) Let $u = ai + bj + ck$, $v = xi + yj + ck$.

Show that $uv = -\langle u, v \rangle + u \times v$

(ii) Show that product of purely imaginary quaternions is purely imaginary iff $u \perp v$. Moreover if u is a purely imaginary unit quaternion, then $u^2 = -1$. Show that such quaternions are in 1-1 correspondence with the 2-sphere in $\mathbb{R}i + \mathbb{R}j + \mathbb{R}k$

(iii) Prove that any unit vector in $\mathbb{H}$ is $q = \cos\theta + u\sin\theta$ where u is a purely imaginary quaternion of unit length

Ans (i) $uv = (ai + bj + ck)(xi + yj + ck)$

$= -(ax+by+cz) + i(bz-cy) + j(cx-az) + k(ay-bx)$

Now $-\langle u, v\rangle = -(ax+by+cz)$

$$u \times v = \begin{vmatrix} i & j & k \\ a & b & c \\ x & y & z \end{vmatrix}$$

$$= (bz-cy)\,i - (az-cx)\,j + (ay-bx)\,k$$

(ii) $uv = -\langle u, v\rangle + u \times v$

$= -(ax+by+cz) + i(bz-cy) + j(cx-az) + k(ay-bx)$

$\therefore uv$ is purely imaginary iff $-\langle u, v\rangle = 0$

i.e. $u \perp v$

u is a purely imaginary unit quaternion

$\therefore uu = u^2 = -\langle u, u\rangle + u \times u$

$= -1 + 0$

$= -1$

V = set of purely imaginary unit quaternions

$= \{ bi + cj + dk \mid b^2 + c^2 + d^2 = 1 \}$

$S^2 = \{ (a, b, c) \in \mathbb{R}^3 \mid a^2 + b^2 + c^2 = 1 \}$

The map $f : V \to S^2$ which maps $bi + cj + dk$ to (b, c, d)

is clearly a bijection and hence we have established the one-one correspondence.

(iii) $q = a + bi + cj + dk$

$|q| = 1$

$\therefore a^2 + b^2 + c^2 + d^2 = 1$

let $a = \cos\theta$

$\therefore \sqrt{b^2+c^2+d^2} = \sin\theta$

$bi + cj + dk$

$= \sqrt{b^2+c^2+d^2} \; \dfrac{bi+cj+dk}{\sqrt{b^2+c^2+d^2}}$

$= \sin\theta \; u$

where $|u| = 1$

$\therefore q = \cos\theta + u \sin\theta$

6) Let G be a group. Let $g, h \in G$. g, h are said to be conjugates if $\exists\, a \in G$ s.t. $aga^{-1} = h$. Let $P, Q \in SU_2$. Show that P, Q are conjugates iff $tr(P) = tr(Q)$

Ans ($\Rightarrow$) Let P, Q be conjugates

$\therefore \exists\, M \in SU_2$ such that

$MPM^{-1} = Q$

$\therefore P$ and Q are similar

$\therefore tr(P) = tr(Q)$ (similar matrices have same trace)

($\Leftarrow$) $\operatorname{tr}(P) = \operatorname{tr}(Q)$

$P, Q \in SU_2$

$\therefore P = \begin{bmatrix} a & -b^* \\ b & a^* \end{bmatrix}$, $|a|^2 + |b|^2 = 1$

$Q = \begin{bmatrix} c & -d^* \\ d & c^* \end{bmatrix}$, $|c|^2 + |d|^2 = 1$

$\operatorname{tr}(P) = \operatorname{tr}(Q)$

$\Rightarrow a + a^* = c + c^*$

$\Rightarrow \operatorname{Re}(a) = \operatorname{Re}(c)$

$\operatorname{tr}(P) = \operatorname{tr}(Q)$ in SU_2 implies same e.vals since trace is $z + \frac{1}{z} \in [-2, 2]$.

Same evals for matrices $\Rightarrow$ they are similar matrices

$\therefore P \sim Q$ have the same eigenvalues and are hence similar.

7) Show that there is a bijection between points of the equator E of S^3 and the conjugacy class of all trace zero matrices in SU_2

Ans $E = \{ (a, b, c) \mid a^2 + b^2 + c^2 = 1 \}$

Let $M \in SU_2$

$\therefore M = \begin{bmatrix} a+bi & -c+di \\ c+di & a-bi \end{bmatrix}$

Also, $tr(M) = 0$

$det(M) = 1$

$\therefore a^2 + b^2 + c^2 + d^2 = 1$

and $2a = 0$

$\therefore a = 0$

$\therefore M = \begin{bmatrix} bi & -c+di \\ c+di & -bi \end{bmatrix}$ and $b^2 + c^2 + d^2 = 1$

There is a clear bijection

$$\begin{bmatrix} bi & -c+di \\ c+di & -bi \end{bmatrix} \longleftrightarrow (b, c, d)$$

8) Let u be a unit imaginary quaternion and $t = \cos\theta + u\sin\theta$ with $V \subset \mathbb{H}$ be the subspace of imaginary quaternions. Show that $\gamma_t : V \to V$ as $\gamma_t(q) = t^{-1} q t$ is a rotation of V with $\mathbb{R}u$ as the axis and 2θ as the angle

Ans $\gamma_t(\lambda u) = t^{-1}(\lambda u)\, t$

$= (\cos\theta - u\sin\theta)(\lambda u)(\cos\theta + u\sin\theta)$

$= \lambda(\cos\theta - u\sin\theta)(u\cos\theta - \sin\theta)$

$= \lambda(u\cos^2\theta + u\sin^2\theta - u^2\sin\theta\cos\theta - \sin\theta\cos\theta)$

$= \lambda u$

$\therefore \mathbb{R}u$ is indeed the axis.

We just need to verify that the angle is 2θ

Construct $\phi_t, \mu_t : \mathbb{H} \to \mathbb{H}$ given by $\mu_t(q) = qt$ and $\phi_t(q) = t^{-1}q$

Both are linear maps and for any $q \in \mathbb{H}$,

$|qt| = |q||t|$ (matrix representation)

$= |q|$

Also $|t^{-1}q| = |t^{-1}||q| = |q|$

$\therefore$ length of vectors is preserved $\Rightarrow$ orthogonal

$\therefore \phi_t \circ \mu_t$ is an orthogonal linear map

Let $v \in V$ be a unit vector and $v \perp u$.

Then $\{u, v, u \times v\}$ is an orthonormal basis of V

$$uv = -\langle u, v \rangle + u \times v = u \times v$$

$$v(u \times v) = -\langle v, u \times v \rangle + v \times (u \times v)$$

$$= -v\langle u, v \rangle + u\langle v, v \rangle$$

$$= u$$

$$(u \times v)u = v \quad \text{(similar to above)}$$

$$t^{-1}vt = (\cos\theta - u\sin\theta)\, v\, (\cos\theta + u\sin\theta)$$

$$= (v\cos\theta - uv\sin\theta)(\cos\theta + u\sin\theta)$$

$$= v(\cos^2\theta - \sin^2\theta) - 2\cos\theta\sin\theta\,(u \times v)$$

$$(\because uv = u \times v = -v \times u = -vu)$$

$$= v\cos 2\theta - (u \times v)\sin 2\theta$$

Similarly $t^{-1}(u \times v)t = v \sin 2\theta + (u \times v)\cos 2\theta$

$\therefore \gamma_t$ wrt $\{v, w\}$ basis is a rotation of $u^\perp$ by an angle of 2θ

TUTORIAL 4

1) Find orders of elements in $U(12)$

Ans $U(12) = \{1, 5, 7, 11\}$

$5^2 = 25 = 1 \pmod{12}$

$7^2 = 49 = 1 \pmod{12}$

$11^2 = 121 = 1 \pmod{12}$

$\therefore |5| = |7| = |11| = 2$, $|1| = 1$

2) Show $U(49)$ is cyclic of order 42. How many elements in $U(49)$ can generate it

Ans $\phi(49) = \phi(7^2) = 49 \times (1 - \frac{1}{7}) = 42$

$\therefore U(49) = \{1, g, g^2, \ldots, g^{41}\}$

no. of generators = no of a s.t. $\gcd(a, 42) = 1$

$= \phi(42) = 12$

(assuming it is cyclic).

Now we prove it is cyclic.

$\langle 3 \rangle = U(49)$ and we are done.

(Why 3? Hit and trial lol. No other way)

3) Prove that $U(2^n)$ is not cyclic for $n \geq 3$ but is cyclic for $n = 1, 2$

$U(2^1) = U(2) = \{1\}$ cyclic ✓

$U(2^2) = U(4) = \{1, 3\}$ cyclic ✓

$\gcd(1 + 2^{n-1}, 2^n) = 1 \quad \forall\, n \geq 3$

$\therefore 1 + 2^{n-1} \in U(2^n)$

$(1+2^{n-1})^2 = 1 + 2^n + 2^{2n-2} = 1 \pmod{2^n}$

$\therefore o(1+2^{n-1}) = 2$

Also $o(-1 + 2^{n-1}) = 2$

$1^2 = 1$

$-1^2 = 1$

$\therefore x^2 = 1$ has at least 4 solutions

A cyclic group of order 2^{n-1} $(\because \phi(2^n) = 2^{n-1})$

can only have 1 subgroup of order 2

$\therefore x^2 = 1$ should only have 2 solutions

$\therefore U(2^n)$ is not cyclic

4) List all cyclic subgroups of $U(30)$

Ans $\phi(30) = \phi(2 \cdot 3 \cdot 5) = \phi(2)\,\phi(3)\,\phi(5)$

$= 1 \times 2 \times 4 = 8$

$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$

$o(7) = 4 = o(13) = o(17) = o(23)$

$o(11) = 2 = o(19) = o(29)$

Now,

$\langle 7 \rangle = \{1, 7, 19, 13\} = \langle 13 \rangle$

$\langle 11 \rangle = \{1, 11\}$

$\langle 17 \rangle = \{1, 17, 19, 23\} = \langle 23 \rangle$

$\langle 29 \rangle = \{1, 29\}$

$\langle 19 \rangle = \{1, 19\}$

Dont forget $\{1\}$

There are the cyclic subgroups of $U(30)$

5) Show existence of 4 cyclic subgroups in $U(12)$

Ans $U(12) = \{1, 5, 7, 11\}$

$o(5) = o(7) = o(11) = 2$

$\{1\}$

$\{1, 5\}$

$\{1, 7\}$

$\{1, 11\}$

6) Let p be an odd prime. Use binom theorem to show that $|1+p| = p^{n-1}$ in the multiplicative group $U(p^n)$

Ans $(1+n)^{n^k} \equiv 1 \pmod{n^{k+1}}$ (Claim)

Base case: $k=0$: $1+n \equiv 1 \pmod{n}$ is true

Assume true for $k \geq 0$

$(1+n)^{n^{k+1}} = ((1+n)^{n^k})^n$

$= (1 + t n^{k+1})^n$ (induc hypo)

$= 1 + n(t n^{k+1}) + \binom{n}{2}(t n^{k+1})^2 + \cdots + (t n^{k+1})$

$\therefore (1+n)^{n^{k+1}} \equiv 1 \pmod{n^{k+2}}$

$\therefore$ We are done by induction

Claim 2: $(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$

for an odd prime p

$k=0$ is true since $1+p \equiv 1+p \pmod{p^2}$

Assume true for $k \geq 0$

$$(1+p)^{p^{k+1}} = \left((1+p)^{p^k}\right)^p$$

$$= \left(1 + p^{k+1} + t p^{k+2}\right)^p$$

$$= \left(1 + p^{k+1}(1+tp)\right)^p$$

$$= 1 + p \cdot p^{k+1}(1+tp) + \binom{p}{2}\left(p^{k+1}(1+tp)\right)^2 + \cdots + \left(p^{k+1}(1+tp)\right)^p$$

$$\equiv 1 + p^{k+2} + t p^{k+3} + \binom{p}{2}\left(p^{k+1}(1+tp)\right)^2 + \cdots + \left(p^{k+1}(1+tp)\right)^p$$

Since p is an odd prime, $\frac{p(p-1)}{2}$ is divisible by p

$$1 + 2(k+1) = 2k+3 \geq k+3$$

$$3(k+1) = 3k+3 \geq k+3$$

$$\therefore (1+p)^{p^{k+1}} \equiv 1 + p^{k+2} \pmod{p^{k+3}}$$

Now we prove $|1+p| = p^{n-1}$.

$\gcd(1+p, p^n) = 1 \Rightarrow 1+p \in U(p^n)$

$(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ by claim]

$\therefore |1+p| \mid p^{n-1}$

if $n = 1$,

$|1+p| = p^{1-1} = 1 = p^{n-1}$

if $n \geq 2$,

$(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$

$\therefore (1+p) = p^{n-1}$ since

$|1+p| \nmid p^{n-2}$

but $|1+p| \mid p^{n-1}$

7) Exhibit a non-cyclic proper subgroup of ⑩

Ans Consider $\langle \frac{1}{2}, \frac{1}{3} \rangle$

It is a proper subgroup of ⑩ since

$\frac{1}{5} \notin \langle \frac{1}{2}, \frac{1}{3} \rangle$

$\frac{1}{3} \notin \langle \frac{1}{2} \rangle$ and $\frac{1}{2} \notin \langle \frac{1}{3} \rangle$ and

hence it is not cyclic

8) List all elements of order 2 in S_4. How many elements of S_n have order 2?

Ans order 2 elements are only transpositions and conjunction of disjoint transpositions.

Thus, in S_4, they are,

(12), (13), (14), (23), (24), (34),

$(12)(34)$, $(13)(24)$, $(14)(23)$

In S_n, we need of product of k disjoint cycles

If $n = 2m$,

we have $$\sum_{k=1}^{m} \frac{\binom{2m}{2}\binom{2m-2}{2} \cdots \binom{2m-2(k-1)}{2}}{k!}$$

(the $k!$ arises since $(12)(34)$, $(34)(12)$ are the same)

If $n = 2m+1$

we have $$\sum_{k=1}^{m} \frac{\binom{2m+1}{2}\binom{2m-1}{2} \cdots \binom{2m+1-2(k-1)}{2}}{k!}$$

(You can still only make a maximum of m 2-cycles which are disjoint)

9) Let $m, n \in \mathbb{Z}$. Find the generator of $\langle m \rangle \cap \langle n \rangle$

Ans Claim: $\langle m \rangle \cap \langle n \rangle = \langle d \rangle$

where $d = \text{lcm}(m, n)$ (If $m, n \neq 0$).

If m or $n = 0$, $\langle m \rangle \cap \langle n \rangle = \langle m \rangle$

(WLOG $n = 0$)

If $m, n \neq 0$,

• $d = \text{lcm}(m,n) \in \langle m \rangle \cap \langle n \rangle$

let $g \in \langle m \rangle \cap \langle n \rangle$

$\therefore m \mid g \,,\; n \mid g$

$\therefore d \mid g$

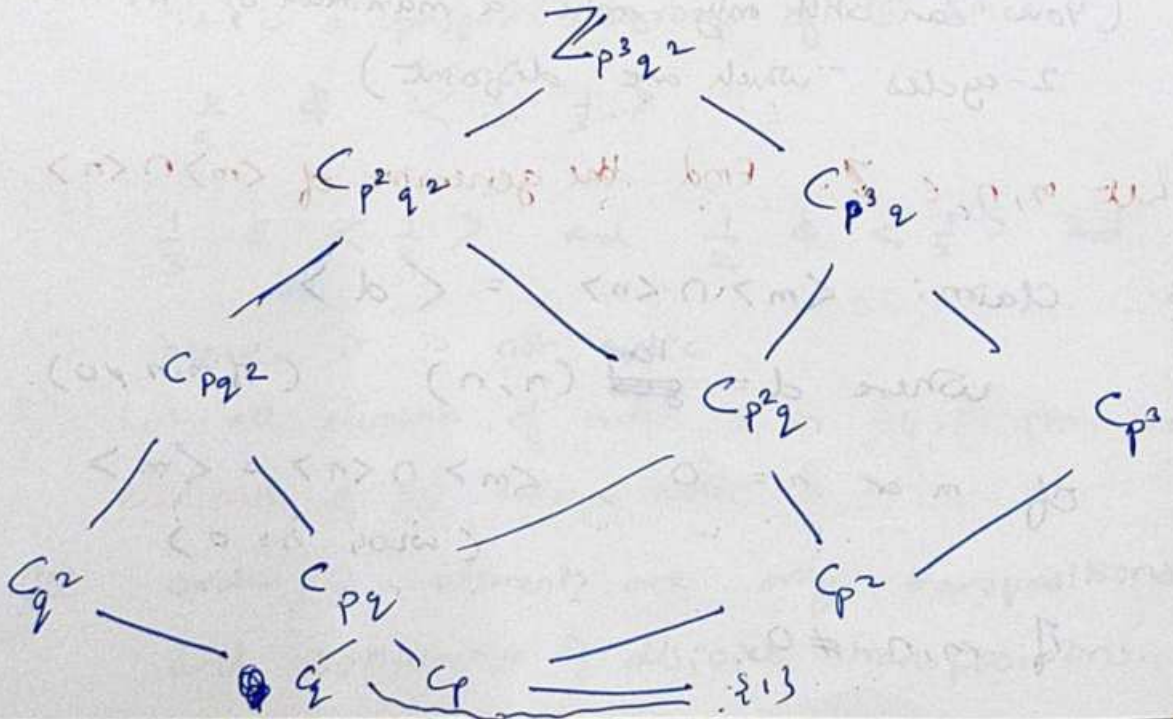
$\therefore \langle d \rangle = \langle m \rangle \cap \langle n \rangle$

10) Determine lattice of subgroups of $\mathbb{Z}_{p^3q^2}$ where p, q are prime

Ans: no of divisors $p^3q^2 = 12$

For each divisor of p^3q^2, there is a unique cyclic subgroup of order d. If $d \mid e \mid p^3q^2$, then $C_d \subseteq C_e$

$\therefore$ The lattice is



11) Show that the group of positive rational numbers under multiplication is not cyclic

Ans if G is cyclic, then $G = \langle \frac{a}{b} \rangle$ where

$\frac{a}{b} \in \mathbb{Q}$

$\therefore 2 = (\frac{a}{b})^n$, This is a contradiction

unless $\frac{a}{b}$ is 2

but if $\frac{a}{2} = 2$, then $G = \langle 2 \rangle$

and $\frac{3}{2} \notin G$. Hence a contradiction

12) Suppose G only has 1 proper subgroup of order 7, what is the order of G

Ans we use Lagrange's theorem to conclude that

$7 \mid |G|$

since G has exactly 3 subgroups, it can only have 3 divisors : 1, 7, $|G|$

hence $|G| = 49$ and $G = C_{49}$ works

so that $\{1\}$, C_7, C_{49} are the only subgroups of C_{49}

13) Let $G = \langle x \rangle$ be cyclic of order 40. Find all elements of order 10

Ans Let $H = \langle y \rangle$ be a subgroup of order 10.

$o(y) = 10$. $o(y^a) = 10 \iff \gcd(a, 10) = 1$

$\therefore a = 1, 3, 7, 9$

(note: $o(y^a) = \frac{10}{\gcd(a, 10)}$)

Take $H = \langle x^4 \rangle$ so that $x^4, x^{12}, x^{28}, x^{36}$ are all elements of order 10

(note: G is cyclic and hence there is a unique subgroup $H = \{ x^{4n} \mid 0 \le n \le 9 \}$ of order 10)

14) Find all cyclic subgroups of D_8

Ans $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$o(r) = 4$
$o(r^2) = 2$
$o(r^3) = 4$
$o(s) = 2$
$o(sr) = 2$
$o(sr^2) = 2$
$o(sr^3) = 2$

$r^4 = 1$
$s^2 = 1$
$srs = r^3$
$rsr \cdot s$

∴ Cyclic subgroups are

$\{1, r, r^2, r^3\} = \langle r \rangle = \langle r^3 \rangle$

$\{1, r^2\} = \langle r^2 \rangle$

$\{1, s\} = \langle s \rangle$

$\{1, sr\} = \langle sr \rangle$

$\{1, sr^2\} = \langle sr^2 \rangle$

$\{1, sr^3\} \quad \langle sr^3 \rangle$

15) Let $o(x) = n$. Prove $\langle x^r \rangle = \langle x^s \rangle \Leftrightarrow \gcd(r,n) = \gcd(s,n)$

Ans

$o(x) = n$

$\therefore o(x^r) = \frac{n}{\gcd(r,n)} = p$ (say)

$o(x^s) = \frac{n}{\gcd(s,n)} = q$ (say)

$\therefore \langle x^r \rangle = \langle x^s \rangle \Rightarrow$ both have same order / no. of elements

$\therefore \gcd(r,n) = \gcd(s,n)$

Conversely,

$\gcd(r,n) = \gcd(s,n) \Rightarrow o(x^r) = o(x^s)$

$\langle x^r \rangle = \{1, x^r, x^{2r}, \dots, x^{(p-1)r}\}$

$\langle x^s \rangle = \{1, x^s, x^{2s}, \dots, x^{(p-1)s}\}$

$(\because p = q)$

$\therefore \langle x^r \rangle = \langle x^s \rangle$

(Let $x^r = x^{ts} \Rightarrow x^{r-ts} = 1$

$\therefore n \mid r-ts$

$\therefore nk = r-ts$

$\therefore ts + nk = r$

$\therefore \gcd(ts, n) = 1$

$\therefore \langle x^0 \rangle = \langle x^{ts} \rangle$)

TUTORIAL 5

1) Prove that $(a_1 a_2 \cdots a_k)$ generates a cyclic group of order k

Ans $(a_1 a_2 \cdots a_k)^k = 1$

and $(a_1 a_2 \cdots a_k)^t$ sends a_1 to a_t for all $t \in \{1, 2, \ldots, k-1\}$

$\therefore o((a_1 a_2 \cdots a_k)) = k$

$\therefore \langle (a_1 a_2 \cdots a_k) \rangle$ is a cyclic group of order k

2) Show that a k-cycle is an even perm if k is odd and an odd perm if k is even

Ans $(a_1 a_2 \cdots a_k) = (a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)$

which is a product of $k-1$ 2-cycles

$\therefore$ If k is odd, we have a product of even number of transpositions making σ an even cycle

Similarly k is even $\Rightarrow$ σ is odd permutation

3) Find the orders of:

$$\sigma_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix}$$

$$\sigma_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix}$$

Ans We give 2 methods to solve this.

Method 1 : Cycle notation :

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix} \equiv (1\,2)(3\,5\,6)(4)$$

$\therefore$ order $= \text{lcm}(2, 3) = 6$

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} \equiv (1\,6)(2\,5)(3\,4)$$

$\therefore$ order $= \text{lcm}(2, 2, 2) = 2$

Method 2 : Matrix notation

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 4 & 6 & 3 \end{bmatrix} \equiv \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\left(\text{Since } \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 5 \\ 4 \\ 6 \\ 3 \end{bmatrix} \right)$$

and order of this matrix is 6

Similarly, $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} \equiv \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

order = 2

4) Show that A_8 has an element of order 15

Ans $(123)(4567) \in A_8$

(since odd length cycles are even permutations)

5) Show that (1234) is not a product of 3 cycles

Ans (1234) is an odd permutation

three cycles are even permutations

Note: This logic won't work for, lets say,

"show that (12345) is not a product of 4 cycles"

Because set of even perms forms a subgroup

but set of odd perms don't since odd perm multiplied by odd perm is an even perm

6) Write all order 5 elements in S_6.

Ans order 5 elements are 5 cycles

To form a 5 cycle we first choose the 5 elements in $\binom{6}{5}$ ways.

Further $(a_1\ a_2\ a_3\ a_4\ a_5)$ has 5! perms

now $(a_1\ a_2\ a_3\ a_4\ a_5) = (a_2\ a_3\ a_4\ a_5\ a_1)$

and similarly other 3 equivalences

$\therefore \frac{5!}{5} = 24$

Hence total no. of 5 cycles $= \binom{6}{5} \times 24$

$= 6 \times 24$

$= 144$

The question most probably asks this number. No one is wild enough to write down all 144 5 cycles in S_6

7) Find a cyclic & non-cyclic group of order 4 in S_4

Ans $o((1234)) = 4$

$\therefore \langle (1234) \rangle = \{ (1), (1234), (13)(24), (1432) \}$

is a cyclic subgroup of order 4

$\{ (1), (12)(34), (13)(24), (14)(23) \}$ is a non cyclic subgroup of order 4

8) Show that S_n is non abelian for $n \geq 3$

Ans $(12)(123) = (23)$

$(123)(12) = (13)$

$\therefore$ non abelian for $n \geq 3$

9) Let $\beta = (123)(145)$, Write β^{99} as a product of disjoint cycles and find its order

Ans $\beta = (123)(145)$

$= (13)(12)(15)(14)$

$= (1452\,3)$

$o(\beta) = 5$

$\therefore \beta^{100} = (1)$

$\therefore \beta^{99} = \beta^{-1} = (3\,2\,5\,4\,1)$

$\therefore o(\beta^{99}) = 5$

Also $o(\beta) = 5 \Rightarrow o(\beta^{99}) = \dfrac{5}{\gcd(99, 5)} = 5$

10) Show that A_5 has 24 elements of order 5, 20 elements of order 3, 15 elements of order 2

Ans elements of order 5 are 5-cycles and luckily 5 cycles belong in A_5

no of 5 cycles in $A_5 = \dfrac{5!}{5}$

since $a_1 a_2 \cdots a_5$ has 5 different representations which are all the same

$\therefore$ 24 elements of order 5

elements of order 3 are 3 cycles (we cant have 2 disjoint 3 cycles in A_5)

no of 3 cycles in $A_5 = \binom{5}{3} \times 2!$

$= 20$

elements of order 2 are 2 disjoint 2-cycles (1 2 cycle is not in A_5, 3 - 2-cycles are not possible)

total no $= \binom{5}{4} \times \dfrac{\binom{4}{2}}{2} = 15$

11) Let $\beta = (1\ 3\ 5\ 7\ 9\ 8\ 6)(2\ 4\ 10)$. Find smallest positive n s.t. $\beta^n = \beta^{-5}$

Ans • Clearly, $o(\beta) = \text{lcm}(7, 3) = 21$

$\therefore \beta^{21} = 1$

$\beta^{n+5} = 1$

$\therefore$ smallest $n = 16$

12) Let H be a subgroup of S_n. Show that either $H \subseteq A_n$ or half of the permutations in H are even

Ans Let $H \not\subseteq A_n$

$\therefore \exists\ \sigma \in H \cap (S_n \setminus A_n)$

Let $O = \{ \tau \in H \mid \tau \text{ is odd} \}$

$E = \{ \tau \in H \mid \tau \text{ is even} \}$

Define $\phi : E \to O \quad \tau \longmapsto \sigma\tau$

$\psi : O \to E \quad \tau \longmapsto \sigma\tau$

both are injective

$\therefore |E| = |O|$

13) Find the maximum order in A_{10} possible.

Ans The complete cycle elements are identity, 3 cycles, 5 cycles, 7 cycles, 9 cycles (orders are $1, 3, 5, 7, 9$)

If we have 2 disjoint cycles, and elements have a restriction on the length since odd + odd or

multiple cycles (disjoint) possibilities are :

9+1	6+4	5+2+2+1
8+2	6+2+1+1	5+1+1+1+1+1
7+3	5+5	4+3+2+1
7+1+1+1	5+3+1+1	

and other < 10 length elements

maximum order = 21

Note: we cant include $7+2+1$ since it has
(2-cycles + 1 2-cycle $\Rightarrow$ not in A_{10})

14) Show that a product of 2 transpositions can be written as a product of 3-cycles

Ans $(ab)(ab) = (1) = (abc)(abc)(abc)$

$(ab)(ac) = (acb)$

$(ab)(cd) = (acb)(acd)$

15) Find a shuffle of 13 cards that requires 42 repeats to return the cards to their original order

Ans we want element of order 42 in S_{13}

$42 = 6 \times 7$

$\therefore (123456)(78910\,11\,12\,13)$ does the job

16) Let p be prime. How many cyclic subgroups of order p are there in S_p

Ans cyclic group of order p in S_p is generated by a

p-cycle.

$\therefore$ no. of p-cycles in $S_p = \binom{p}{p} \times \frac{p!}{p} = (p-1)!$

17) Find no. of order 5 elements in S_7

Ans 5 cycles are order 5

no of 5 cycles $= \binom{7}{5} \times \frac{5!}{5} = 21 \times 24 = 504$

18) Show that there are 90 odd permutations of order 4 in S_6

Ans • order 4 can only be a 4 cycle since lcm(2,2) $\neq 4$

no of 4 cycles in $S_6 : \binom{6}{4} \times \frac{4!}{4}$

$= 15 \times 6$

$= 90$

19) Find order of each element of A_4

Ans $A_4 = \{$ (1), ~~(12), (123), (132), (14), (124), (142),~~ (12)(34), (14)(23), (13)(24), (123), (132), (124), (142), (134), (143), (234), (243) $\}$

Orders are 1, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3

20) Find sign of σ defined as $\sigma(j) = n - (j-1)$ $\forall j = 1, 2, \ldots n$

Ans $\sigma(n-j+1) = j$, $\sigma(n-j+1) = j$

$\therefore$ if n is even and $n = 2m$, we have 2 cycles

ie. $\sigma = \prod_{j=1}^{m} (j \;\; n-j+1)$

odd if n is odd

even if n is even.

if $n = 2m+1$,

$\sigma(j) = j$ $= 2m+1-j+1 \iff j = m+1$

$\therefore$ $m+1$ is the fixed element and we have m other 2 cycles

$\therefore$ n is odd $\Rightarrow$ σ is odd

n is even $\Rightarrow$ σ is even

TUTORIAL 6

1) Let $f: G \to G'$ be a group homomorphism. Let H' be a subgroup of G'. Show that $f^{-1}(H') < G$

Ans Let $h_1, h_2 \in f^{-1}(H')$

$\therefore f(h_1), f(h_2) \in H'$

Consider $f(h_1 h_2)$

$= f(h_1) f(h_2)$

since H' is a subgroup of G',

$f(h_1) f(h_2) \in H'$

$\therefore f(h_1 h_2) \in H'$

$\therefore h_1 h_2 \in f^{-1}(H')$

Hence, $f^{-1}(H') < G$

2) Find an isomorphism $\mathbb{Z} \to 2\mathbb{Z}$

Ans $f : \mathbb{Z} \to 2\mathbb{Z}$

$f(z) = 2z$

$f(ab) = 2(a+b)$ (note that $ab \equiv a+b$)

$f(a)f(b) \equiv f(a) + f(b)$

$= 2a + 2b$

$= 2(a+b)$

$\therefore f$ is a homomorphism

$\ker(f) = \{ a \in \mathbb{Z} \mid f(a) = 0 \}$

$= \{0\}$

$\therefore f$ is injective

f is clearly onto since

$f(a) = 2a \in 2\mathbb{Z}$

$\therefore f$ is an isomorphism

3) Show that $U(8) \neq U(10)$

Ans $U(8) = \{1, 3, 5, 7\}$

$U(10) = \{1, 3, 7, 9\}$

- orders in $U(8)$ are 1, 2, 2, 2

orders in $U(10)$ are 1, 4, 4, 2

$\therefore U(8) \not\cong U(10)$

Also note that $U(10)$ is cyclic. $\langle 3 \rangle = \langle 7 \rangle = U(10)$

but $U(8)$ isn't

4) Show that $U(8) \simeq U(12)$

Ans $U(8) = \{1, 3, 5, 7\}$

$U(12) = \{1, 5, 7, 11\}$

$\therefore f : U(8) \to U(12)$

$1 \mapsto 1$

$3 \mapsto 5$

$5 \mapsto 7$

$7 \mapsto 11$

is an isomorphism

It is clearly a bijection and f is a homomorphism since

$3 \cdot 5 = -1 = 7 \mapsto 5 \cdot 7 = -1$

$3 \cdot 7 = -3 = 5 \mapsto 5 \cdot 11 = 7$

$5 \cdot 7 = 3 \mapsto 7 \cdot 11 = 5$

$f(3 \times 5) = f(15) = f(7) = 11$

$f(3) \times f(5) = 5 \times 7 = 35 = 11$ ✓

$f(3 \times 7) = f(21) = f(5) = 7$

$f(3) \times f(7) = 5 \times 11 = 55 = 7$ ✓

$f(5 \times 7) = f(35) = f(3) = 5$

$f(5) \times f(7) = 7 \times 11 = 77 = 5$ ✓

5) Let $G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n\}$. Show that $f : G \to G$ as $f(z) = z^k$ is not an isom but is a surjective homomorphism

$f(z_1 z_2) = (z_1 z_2)^k = z_1^k z_2^k = f(z_1) f(z_2)$

$\therefore f$ is a homomorphism

Clearly f is not injective since all k-th roots of unity get mapped to 1

Let $z \in G$

and let $z^{n_0} = 1$

We want to find $y \in G$ so that

$f(y) = y^k = z$

$y^k = z$

$\therefore y = z^{1/k}$

we need to show that $z^{1/k} \in G$ and we are done

$z^{n_0} = 1 \rightarrow z = e^{\frac{2\pi i}{n_0}}$ for $i = 1, 2, \ldots n_0$

$z^{1/k} = e^{\frac{2\pi i}{n_0 k}}$ for $i = 1, 2, \ldots, n_0$

Clearly $z^{1/k} \in G$

since $(z^{1/k})^{n_0 k} = 1$

$\therefore f$ is onto

6) Let $k \in \mathbb{Q}^+$. Show that $f: \mathbb{Q} \rightarrow \mathbb{Q}$ given by $f(q) = kq$ is an automorphism of the additive group $\mathbb{Q}$

Ans $f(q_1 + q_2) = k(q_1 + q_2) = kq_1 + kq_2 = f(q_1) + f(q_2)$

$\therefore f$ is a homomorphism

$f(a) = f(b) \Rightarrow ka = kb$

$k \in \mathbb{Q}^* \Rightarrow a = b$

$\therefore f$ is injective

Given $q \in \mathbb{Q}$, $f\left(\frac{1}{k} q\right) = q$

$\therefore f$ is surjective

$\therefore f$ is an automorphism

7) Find all automorphisms of $\mathbb{Z}$

Ans $f : \mathbb{Z} \to \mathbb{Z}$ is an automorphism

$\langle 1 \rangle = \mathbb{Z}$

$\therefore \langle f(1) \rangle = \mathbb{Z}$

But only $1, -1$ generate $\mathbb{Z}$

$\therefore f(1) = 1$ or $f(1) = -1$

$\therefore f(a) = a \cdot f(1)$ or $f(a) = a \cdot f(1)$

$\therefore f(a) = a$ $\therefore f(a) = -a$

$\therefore$ only 2 automorphisms

8) Show that $S_4 \not\cong D_{24}$

Ans $D_{24} = \{1, r, r^2, \cdots, r^{11}, s, sr, sr^2, \cdots, sr^{11}\}$

$o(sr^i) = 2 \quad \forall\ i = 1, 2, \cdots 11$

since $sr^i sr^i = s \cdot s = 1$

$(\because srs = s \Rightarrow r^k s r^k = s)$

$$o(x^i) = \frac{12}{\gcd(i,12)} \quad \forall\ i = 1, 2, \ldots, 11$$

whereas S_4 does not have any element of order 12

since $4 = 1+1+1+1$

$= 2+1+1$

$= 3+1$

$= 2+2$

$= 4+0$

$\therefore$ elements of S_4 are only of orders 1, 2, 3, 4

5) show that $\phi : GL_n(\mathbb{R}) \to GL_n(\mathbb{R})$ defined as $\phi(A) = (A^t)^{-1}$ is an automorphism

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

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

$= ((AB)^t)^{-1}$

$= \phi(AB)$

$\therefore \phi$ is a homomorphism

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

$\Rightarrow A^t = I$

$\Rightarrow A = I$

$\therefore \ker \phi = I \Rightarrow \phi$ is injective

$\phi((A^{-1})^t) = A$

$\therefore \phi$ is surjective

$\therefore \phi$ is automorphism

10) Show that $\phi : G \to G$ defined as $\phi(x) = x^{-1}$ is an automorphism iff G is abelian

Ans ($\Leftarrow$) let G be abelian

$$\phi(xy) = (xy)^{-1}$$
$$= y^{-1}x^{-1}$$
$$= x^{-1}y^{-1}$$
$$= \phi(x)\,\phi(y)$$

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

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

$\Rightarrow a = b$

$\therefore \phi$ is injective

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

$\therefore \phi$ is surjective

$\therefore \phi$ is an automorphism

($\Rightarrow$) ϕ is an automorphism

$\therefore \phi(xy) = \phi(x)\,\phi(y)$

$\therefore (xy)^{-1} = x^{-1}y^{-1}$

$\therefore y^{-1}x^{-1} = x^{-1}y^{-1}$

$\therefore xy = yx$

$\therefore G$ is abelian

11) Find all automorphisms of S_3

Ans Refer theorem 68 which says $\text{Aut } S_3 \simeq S_3$

In fact $\text{Aut}(S_n) \simeq S_n \quad \forall\, n \neq 2, 6$

12) Show that $f: U(16) \to U(16)$ as $x \mapsto x^3$ is an automorphism. Are $x \mapsto x^5$, $x \mapsto x^7$ automorphisms

Ans $U(16) = \{1, 3, 5, 7, 9, 11, 13, 15\}$

$U(16)$ is abelian since multiplication in $\mathbb{Z}$ is commutative

$\therefore (xy)^3 = x^3 y^3$ and f is a homomorphism

$\ker(f) = \{x \mid x^3 = 1\}$

$x^3 = 1 \Rightarrow o(x) = 1$ or 3

but $U(16)$ doesn't have order 3 elements.

x	1	3	5	7	9	11	13	15
$o(x)$	1	4	4	2	2	4	4	2
x^3	1	11	13	7	9	3	5	15

$\therefore x \mapsto x^3$ is an automorphism

similarly one can check that the other two maps are also automorphisms

shorter way using lagrange's theorem:

$(xy)^5 = x^5 y^5$ f is hom $-$

$x^5 = 1 \Rightarrow o(x) \mid 5 \Rightarrow o(x) = 1$ or 5

but $o(x)$ divides order of group which is 8

$\therefore o(x) = 1 \Rightarrow f$ is injective.

$f: X \to X$ is injective $\Rightarrow f$ is surjective

$\therefore f$ is an automorphism

13) Show that $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic

Ans $\mathbb{Z}$ is cyclic with $\langle 1 \rangle = \mathbb{Z}$

$\mathbb{Q}$ is not cyclic. Suppose $\mathbb{Q}$ is cyclic, then $\langle \frac{a}{b} \rangle = \mathbb{Q}$ for some $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a,b) = 1$

$\therefore \mathbb{Q} = \{ \frac{na}{b} , n \in \mathbb{Z} \}$

$\frac{1}{2b} \in \mathbb{Q} \Rightarrow \frac{1}{2b} = n_0 \frac{a}{b}$ for some n_0

$\therefore n_0 a = \frac{1}{2}$

but $a, n_0 \in \mathbb{Z}$ and this is a contradiction.

14) Show that $f(x) = \frac{1}{x}$, $g(x) = \frac{x-1}{x}$ generate a group isomorphic to S_3 under composition.

Ans Let $G = \langle f, g \rangle$

$f^2 = fof(x) = x$

$g^2 = \dfrac{\frac{x-1}{x} - 1}{\frac{x-1}{x}} = \dfrac{\frac{-1}{x}}{\frac{x-1}{x}} = \frac{1}{1-x}$

$g^3 = \dfrac{\frac{1}{1-x} - 1}{\frac{1}{1-x}} = 1 - (1-x) = x$

$\therefore f^2 = g^3 = id$

$\therefore \quad G = \langle f, g \mid f^2 = g^2 = id, \; fgfg = id \rangle$

$\therefore G \simeq S_3 = \langle a, b \mid a^2 = b^3 = id, \; aba = b^{-1} \rangle$

(note; we take $a = (12)$, $b = (123)$ for S_3)

15) Let $\phi : G \to G'$ be a surjective hom. Show that for any $N \triangleleft G$, $\phi(N) \triangleleft G'$

Ans Let $g' \in G'$, $z' \in \phi(N)$

since f is surjective,

$\exists \; g$ s.t. $f(g) = g'$

Also, let $z' = f(z)$ for some $z \in N$

consider $g' z' (g')^{-1}$

$= f(g) f(z) (f(g))^{-1}$

$= f(g) f(z) f(g^{-1})$ ($\because f$ is a hom)

$= f(g z g^{-1})$ ($\because f$ is a hom)

since $N \triangleleft G$,

$g z g^{-1} = z_2 \in N$

$\therefore f(g z g^{-1}) = f(z_2)$

$\in \phi(N)$ ($\because z_2 \in N$)

$\therefore \forall \; g' \in G', \; \forall \; z' \in \phi(N)$,

$g' z' (g')^{-1} \in \phi(N)$

$\therefore \quad \therefore \phi(N) \triangleleft G'$

16) Show that $i_a : G \to G$ defined as $i_a(g) = aga^{-1}$ $\forall g \in G$ is an automorphism of G. Let $B(G)$ be the group of bijections of G. Define $\varphi : G \to B(G)$ as $\varphi(a) = i_a$. Show that φ is a group hom and $\ker(\varphi) = Z(G)$. Show that Image $I(G)$ under φ is a normal subgroup of $Aut(G)$

Ans $i_a(g) = aga^{-1}$

$aga^{-1} = id$

$\Rightarrow ag = a$

$\Rightarrow a^{-1}ag = id$

$\Rightarrow g = id$

$\therefore \ker(i_a) = id \Rightarrow i_a$ is injective

$i_a(gh) = agha^{-1}$

$i_a(g)\, i_a(h) = aga^{-1}aha^{-1} = agha^{-1}$

$\therefore i_a$ is a homomorphism

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

$\therefore i_a$ is surjective

$\therefore i_a$ is an automorphism

$\varphi(a) = i_a$

$\varphi(ab) = i_{ab}$

$\varphi(a)\,\varphi(b) = i_a \circ i_b$

$i_{ab}(g) = abg$

$i_a \circ i_b(g) = a(bg) = abg$

$\Rightarrow \varphi$ is a homomorphism

$\ker(\varphi) = \{ g \in G \mid i_g = id \}$

$\therefore i_g(h) = h \quad \forall h \in G$

$\therefore ghg^{-1} = h \quad \forall h \in G$

$\therefore gh = hg \quad \forall h \in G$

$\therefore g \in Z(G)$

$\therefore \ker(\varphi) \subseteq Z(G)$

Let $t \in Z(G)$

$\therefore th = ht \quad \forall h \in G$

$\therefore tht^{-1} = h \quad \forall h \in G$

$\therefore i_t(h) = h \quad \forall h \in G$

$\therefore i_t$ is the identity map

$\therefore t \in \ker \varphi$

$\therefore \ker(\varphi) \supseteq Z(G)$

$\therefore \ker(\varphi) = Z(G)$

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

Let $\phi : G \to G$ be an automorphism of G

$(\phi \circ i_g \circ \phi^{-1})(a) = \phi(i_g(\phi^{-1}(a)))$

$= \phi(g \phi^{-1}(a) g^{-1})$

$= \phi(g) \, a \, \phi(g^{-1})$

$= i_{\phi(g)} \in I(G)$

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

17) Prove that the subgroup of upper triangular matrices in $GL_3(\mathbb{F}_2)$ is isomorphic to D_8

trns

$$U = \left\{ \begin{bmatrix} a & d & e \\ 0 & b & f \\ 0 & 0 & c \end{bmatrix} \;\middle|\; a,b,c \neq 0,\ a,b,c \in \mathbb{F}_2 \right\}$$

$$= \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \;\middle|\; a,b,c \in \mathbb{F}_2 \right\}$$

Clearly, $|U| = 2^3 = 8 = |D_8|$

$D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$r^4 = 1 = s^2$

$rsrs = 1$

So we now wish to find elements of order 2 and 4 in U

$$A^2 = I \Rightarrow \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}^2 = I$$

$$\Rightarrow \begin{bmatrix} 1 & 2x & 2y+xz \\ 0 & 1 & 2z \\ 0 & 0 & 1 \end{bmatrix} = I$$

But $2x, 2y, 2z$ are always zero in $\mathbb{F}_2$

$$\therefore \begin{bmatrix} 1 & 0 & xz \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I$$

$\therefore xz = 0$

$\therefore x = 0$ or $z = 0$

$\therefore$ 5 elements of order 2:

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$ (note: we dont consider id)

These are precisely r^2, s, sr, sr^2, sr^3 (in some order)

let us find order 4 element

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^4 = \begin{bmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{bmatrix} = I$$

This is always identity so

but element of order 4 does not have

$A^2 = I$

$$\therefore \begin{bmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \neq I$$

$\therefore ac = 1 \Rightarrow a = 1, c = 1$

$\therefore \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$ are order 4

These correspond to r, r^3 is some order

Check that

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

$\therefore$ Map $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \longmapsto r$

Also check that

r^2 will be $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Now we need to identify s

We have matrices for s, sr, sr^2, sr^3

By hit and trial,

S corresponds to $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$

18) Show that $D_8 \neq Q_8$

Ans $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

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

$\therefore$ orders are 4 for $\pm i, \pm j, \pm k$

But in D_8 only 2 elements have order 4

19) Let G be finite abelian with no element of order 2. Show that $\varphi : G \to G$ with $\varphi(g) = g^2$ is auto-morphism. Show that if G is infinite, φ need not be an automorphism

Ans $\varphi(g_1 g_2) = (g_1 g_2)^2 = g_1^2 g_2^2$ ($\because$ abelian)

$\varphi(g_1)\,\varphi(g_2) = g_1^2 g_2^2$

$\varphi(g) = g^2 = 1 \Rightarrow o(g) = 1$ or 2 but $o(g) \neq 2$ since it is given. Hence $g = id$ $\therefore \varphi$ is injective

because $\ker(g) = \{ g \in G \mid \varphi(g) = g^2 = 1 \} = \{ id \}$

$\varphi : G \to G$ is injective and G is finite $\Rightarrow$ φ is onto $\Rightarrow$ φ is an automorphism

For $|G|$ = infinite, let $G = (\mathbb{Z}, +)$

$\varphi(x) = 2x$ is an injective hom but not onto and hence not an automorphism

20) Let G be a group and $g \in G$, $z \in Z(G)$. Show that i_g, i_{zg} are equal

Ans $i_g(h) = ghg^{-1}$

$i_{zg}(h) = zgh(zg)^{-1}$

$= gzhg^{-1}z^{-1}$

$= ghzg^{-1}z^{-1}$

$= ghg^{-1}zz^{-1}$

$= ghg^{-1}$

$= i_g(h)$

$z \in Z(G)$ and hence commutes with any given element.

TUTORIAL 7

1) Let $G = (\mathbb{C}^*, \times)$, $H = \{ z \in \mathbb{C}^* \mid |z| = 1 \}$.

Draw the cosets wH for $w \in G$

Ans $wH = \{ wz \in \mathbb{C}^* \mid |z| = 1 \}$

$\therefore |wz| = |w|$

let $w = re^{i\theta}$

$z = e^{i\alpha}$

$\Rightarrow wz = re^{i\theta + \alpha}$

$\therefore wH$ is a circle centered at $(0,0)$ and radius $= r$

2) Find $5^{15} \pmod 7$, $7^{13} \pmod{11}$

Ans $\gcd(5,7) = 1$

$\Rightarrow 5^{\phi(7)} \equiv 1 \pmod 7$

$\Rightarrow 5^6 = 1$

$\therefore 5^{15} = 5^3 = 25 \times 5 = 4 \times 5 = 20 = 6$

$\gcd(7,11) = 1$

$\therefore 7^{10} = 1$

$\therefore 7^{13} = 7^3 = 49 \times 7 = 5 \times 7 = 35 = 2$

3) Prove that a non-abelian group of order 10 has 5 elements of order 2

Ans $|G| = 10$

By lagrange theorem, $o(g) \mid 10 \quad \forall g \in G$

$\therefore o(g) = 1, 2, 5, 10$

if $o(g) = 10$ for some g,

$G = \langle g \rangle$ which is abelian but G is non abelian

if $o(g) = 2 \ \forall g \in G, \quad g = g^{-1} \ \forall g \in G$

$\therefore (gh)^{-1} = gh \Rightarrow h^{-1}g^{-1} = gh \Rightarrow hg = gh$

$\therefore G$ is abelian

but G is non abelian

$\therefore \exists \ g \in G$ s.t. $o(g) = 5$

let it be x

set $N = \langle x \rangle$

If there is no element of order 2, the only proper subgroups of G have order 5.

let there be n of these

Then $|G| = 4n + 1 = 10$.

This is a contradiction

(Why $4n$? Group of order 5 is cyclic since 5 is prime and since all elements have order 5, we can have $\{1, g, g^2, g^3, g^4\}$ for any g and hence other than 1 there are 4 other elements. Thus if there are n of these, $4n + 1 = 10$ (using all elements in G))

$\therefore \exists \ s \in G$ s.t. $o(s) = 2$.

Consider $\langle r, s \rangle$

$\langle r \rangle$ itself generates $1, r, r^2, r^3, r^4$

$\langle s \rangle$ itself generates $1, s$

$\therefore \langle r, s \rangle$ has at least 6 elements but

$|\langle r, s \rangle|$ divides 10 by lagrange's theorem

$\therefore \quad \langle r, s \rangle = 10 \Rightarrow \langle r, s \rangle = G$

Suppose s is the only element of order 2.

Then rsr^{-1} has order 2 and hence

$rsr^{-1} = s \Rightarrow rs = sr \Rightarrow G$ is abelian

(since $G : \langle r, s \rangle$)

$\therefore$ there are at least 2 elements of order 2.

If there is another subgroup of order 5, then

G has $1 + 8 + 2$ elements which is a contradiction

and hence G has 5 elements of order 2

(G has only 1 subgroup of ordr 5 $\Rightarrow$ other elements must have order 2)

4) Let $|G| = 22$. Suppose $x \neq 1$, $y \in G \setminus \langle x \rangle$, show that $G = \langle x, y \rangle$

Ans $G \neq \langle x \rangle$, $x \neq 1$

$\therefore o(x) \mid 22 \Rightarrow o(x) = 2, 11$

if $o(x) = 11$, $|\langle x, y \rangle| \geq 12 \Rightarrow |\langle x, y \rangle| = 22$

(since it must divide 22)

$\therefore \langle x, y \rangle = G$

if $o(x) = 2$, $|\langle x, y \rangle| = 11$ or 22 but $|\langle x, y \rangle| \neq 11$ as $|x| = 2$

$(2 \nmid 11)$

5) Let $S \subseteq G$ and $1 \in S$. Let $g \in G$ and gS be the set $\{gx : x \in S\}$. Suppose $\{gS \mid g \in G\}$ is a partition of G, show that $S < G$

Ans Let $x, y \in S$. Then $x \in xS \cap S$

But xS, S are in the partition set $\Rightarrow$

$xS = S$

$\Rightarrow xy \in xS \cap S = S$

$\therefore x \in S$, $y \in S$

$\Rightarrow xy \in xS = S$

$\therefore S < G$

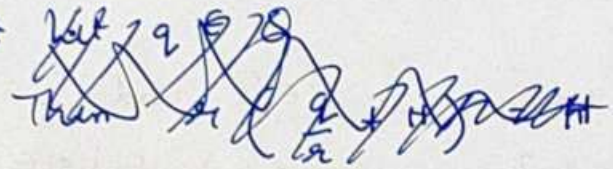
6) Let $|G| = 33$. Show that $\exists\ g \in G$ s.t. $o(g) = 3$

Ans If G is cyclic, g^{11} has order 3. If g has no element of order 3, then all elements of g have order 11. Let there be n subgrps of order 11. $\therefore 10n + 1 = 33 \Rightarrow$ no soln. for $n \Rightarrow \exists$ element of order 3

7) Show that $(\mathbb{Q}, +)$ has no proper subgroup of finite index

but $H < \mathbb{Q}$ and $[\mathbb{Q} : H] = r \geq 2$.

The cosets of S constitute a group of order r (since every subgroup is normal since $(\mathbb{Q}, +)$ is abelian)



but $q + H$ be an element of this group

By lagrange thrm, $o(q+H) \mid r$

$$\Rightarrow (q+H)^r = r(q+H)$$
$$= rq + H$$
$$= H$$

$\therefore rq \in H \quad \forall \; q \in \mathbb{Q}$

$\therefore r\mathbb{Q} \subseteq H$

but $r\mathbb{Q} = \mathbb{Q}$ for any integer r

$\therefore \mathbb{Q} \subseteq H$

$\therefore \mathbb{Q} = H$

8) Determine all subgroups of D_{10}

Any proper subgroup of D_{10} has order 2 or 5

Order 2 subgroups are $\langle sr^i \rangle$ for $i = 1, 2, 3, 4$

order 5 subgroups are $\langle r^i \rangle$ for $i = 1, 2, 3, 4$

9) Let $|G| = p^n$. Show that G has an element of order p

Ans $o(g) \mid p^n \Rightarrow o(g) = p^r$ for some $r \geq 1$

$$o(g^{p^{r-1}}) = \frac{p^r}{\gcd(p^r, p^{r-1})} = p$$

$\therefore g^{p^{r-1}}$ is the required element

10) In the additive group $\mathbb{R}^m$ of vectors, let $W = \{u \in \mathbb{R}^n \mid Au = 0\}$ where A is some $m \times n$ matrix. Let $b \in \mathbb{R}^m$. Show that $S = \{v \in \mathbb{R}^n \mid Av = b\}$ is either empty or a coset of W

Ans If $Au = b$ has no solutions it is empty.

If $Ac = b$ for some $c \in \mathbb{R}^n$, then, $c + W = S$

Since for any $v \in W$, $A(c+v) = Ac + Av = b$

If d is such that $d \in S$, then

$A(c-d) = Ac - Ad = b - b = 0 \Rightarrow c - d \in W$

$\therefore d \in c + W$

11) Let $H < G$, $[G:H] = 2$. Show that $H \triangleleft G$. Find an example to show that H may not be normal if $[G:H] = 3$ or 4.

Ans $[G:H] = 2$

$\therefore$ For some $a \in G \setminus H$,

$G = H \cup aH$

$H \neq Ha$ since $a \notin H$

$\therefore G = HU Ha = HU aH$

If $g \in aH$, then $g \notin H \Rightarrow g \in Ha$

$\Rightarrow aH \subseteq Ha$

similarly $Ha \subseteq aH$

$\therefore aH = Ha \quad \forall a \in G \setminus H$

$\Rightarrow H$ is normal in G

(note: if $a \in H$, $aH = Ha$ is anyway true)

For $G = S_3$, $H = \{(1), (12)\}$,

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

and H is not normal since $(123)H(123)^{-1}$.

$= \{(1), (23)\} \neq H$

For $G = D_8$, $H = \{1, s\}$,

$[G:H] = \frac{8}{2} = 4$

and H is not normal since $rHr^{-1} = \{1, sr^2\} \neq H$

12) Let G be a finite abelian group and let $n \in \mathbb{N}$ with n and $|G|$ coprime. Show that $a \mapsto a^n$ is automorphism

Ans $f(a) = a^n$

$f(ab) = (ab)^n = a^n b^n \quad (\because \text{abelian})$

$\therefore f(a) f(b) = a^n b^n = f(ab)$

Also if $a^n = 1$, then $o(a) \mid n$ but $o(a) \mid |G|$

$\therefore o(a) \mid \gcd(n, |G|) = 1 \Rightarrow o(a) = 1 \Rightarrow a = id$

$\therefore f$ is injective. G is finite $\Rightarrow f$ is surjective

13) Show that $x^2 \equiv 1 \pmod{p}$ (p odd prime) $\Rightarrow x = 1$ or -1 only

Ans $(x+1)(x-1) \equiv 0 \pmod{p}$

p is an odd prime

$\therefore$ p must divide only one of $x+1$ or $x-1$

(else $p \mid 2$)

$\therefore \quad p \mid x \pm 1$

$\therefore \quad x \equiv \pm 1 \pmod{p}$

14) Let $G = \{a_1 \cdots a_n\}$ be finite abelian and let $x = \prod_{i=1}^{n} a_i$.

Show that $x^2 = 1$

Ans There are two types of elements → self inverse elements (include identity) and elements whose inverse is some other element.

The former kind will give rise to id in the product of squares. The latter will also give id since for every a $\exists$ b s.t. $ab = id$

$\Rightarrow a^2 b^2 = (ab)^2 = id$

and these occur in pairs since $(g^{-1})^{-1} = g$

$\therefore$ Everything cancels and we get 1

15) Prove that p is prime iff $(p-1)! \equiv -1 \pmod{p}$

Ans As noted in prev problem,

$$x = \prod_{i=1}^{n} a_i = \prod_{g : g \text{ is of order } 2} g$$

(Only self inverse elements survive)

Elements of order 2 in $G = \mathbb{Z}_p^{\times}$ are the roots of $x^2 - 1 = 0$ which are only 1 & -1 as noted in an earlier problem

∴ with $G = \mathbb{Z}_p^{\times}$,

$$x = \prod_{i=1}^{n} a_i^{\circ} = 1 \times -1 = -1$$

but $\prod_{i=1}^{n} a_i^{\circ}$ in $\mathbb{Z}_p^{\times} = (p-1)!$

since $\mathbb{Z}_p^{\times} = \{1, 2, 3, \ldots, p-1\}$

$\therefore (p-1)! = -1 \pmod{p}$

Conversely suppose

$(n-1)! = -1 \pmod{n}$

and $n = ab$ with $1 < a \leq b < n$.

If $a < b$, $n = ab \mid (n-1)!$ ($\because a \times b$ occurs somewhere in $(n-1)!$)

$\therefore (n-1)! \equiv 0 \pmod{n}$ ⟶ ○

If $a = b$, then $n = a^2$

and $(a^2-1)! = -1 \pmod{a^2}$ is the statement

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

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

but $a \mid (a^2-1)!$

$\therefore a \mid \gcd((a^{k-1})! + 1, (a^{k-1})!) = 1$

$\therefore a = 1 \quad \longrightarrow \leftarrow$

16) Prove that $M, N \triangleleft G \Rightarrow M \cap N, MN \triangleleft G$

Ans Let $g \in G$

$g(M \cap N) g^{-1} \subseteq gMg^{-1} \cap gNg^{-1} = M \cap N$

$\therefore M \cap N \triangleleft G$

Firstly $MN < G$. *

This is because,

$mn = mnm^{-1}m = n'm \quad (\because N \triangleleft G)$

$\in NM$

$nm = nmn^{-1}n = m'n \in MN$

$\therefore MN = NM$

and $m_1 n_1 m_2 n_2 = m_1 (n_1 m_2) n_2$

$= m_1 (m_3 n_3) n_2$

$= m_4 n_4 \in MN$

and $m_1 n_1 n_1^{-1} m_1^{-1} = id$

and $(n_1^{-1} m_1^{-1}) \in NM = MN$

Let $g \in G$

$gmng^{-1} = gmg^{-1}gng^{-1} = m'n' \in MN$

$\therefore MN \triangleleft G$

17) $H \leq G$, $N \triangleleft G$. Show that $HN = NH$, $HN < G$

Ans $h_1 n_1 = h_1 n_1 h_1^{-1} h_1 = n_4 h_1 \in NH$

$n_2 h_2 = h_2^{-1} h_2 n_2 h_2 = h_2^{-1} n_3 \in HN$

$\Rightarrow HN = NH$

Now we show $HN = NH \leq G$

$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} \in NH \in HN$

(∵ inverse of elements in HN is in HN)

$h_1(n_1 h_2) n_2 = h_1 h_3 n_3 n_2 \in HN$

(∵ product of two elements in HN is in HN)

$\therefore HN \leq G$

18) $H \trianglelefteq G$, $|H| = 2 \Rightarrow H \subset Z(G)$

Ans Let $H = \{1, g\}$

$\forall h \in G, \quad hHh^{-1} = H$

For 1 it is trivial since $h \cdot 1 \cdot h^{-1} \in H$ (which is true)

But for g, we have,

$\forall h \in G, \quad hgh^{-1} \in H$

Suppose $hgh^{-1} = 1 \Rightarrow g = 1$ (contradiction)

$\therefore hgh^{-1} = g$

$\therefore \forall h \in G, \quad hg = gh$

$\therefore g \in Z(G)$

Also $1 \in Z(G)$

$\therefore H \subset Z(G)$

19) Prove that A_5 does not have normal subgroup of order 2

Ans order 2 elements are product of 2 disjoint 2-cycles ie. $\sigma = (ab)(cd)$

if $\langle \sigma \rangle \trianglelefteq A_5$, then $\sigma \in Z(A_5)$

Let e be the 5th element.

$(eac)(ab)(cd) = (eabcd)$

$(ab)(cd)(eac) = (ebaidc)$

$\therefore (ab)(cd) \in \langle c \rangle$ but

$(ab)(cd) \notin Z(A_5)$

$\longrightarrow \leftarrow$

Note: There is a much stronger result that

$Z(A_n) = \{1\} \quad \forall \quad n \geq 4$

20) $H = \{g^2 \mid g \in G\} < G$. Show that $H \triangleleft G$

Ans $x g^2 x^{-1} = x g x^{-1} x g x^{-1}$

$= (x g x^{-1})^2$

$\in H$

$\therefore H \triangleleft G$

21) Show that $GL_n(\mathbb{R}) \not\cong GL_n(\mathbb{C})$

Ans when $n = 2$

$$\begin{bmatrix} 1+i & i \\ i & 1-i \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 1+i & i \\ i & 1-i \end{bmatrix}^{-1}$$

$$= \begin{bmatrix} 3 & 2i \\ -2i & 1 \end{bmatrix} \notin GL_n(\mathbb{R})$$

Aim was to just find matrix in $GL_n(\mathbb{R})$ whose eigen values were not real

22) Give examples of 3 groups $G \triangleleft H \triangleleft K$ so that $G \not\triangleleft K$

Ans $V = \{ (1), (12)(34), (13)(24), (14)(23) \}$

$V \triangleleft S_4$ and $H = \langle (12)(34) \rangle$ has index 2 in $V \Rightarrow H \triangleleft V$ by Q11

$\therefore H \triangleleft V \triangleleft S_4$ but

$H \not\triangleleft S_4$ since

$(13)(12)(34)(13) = (32)(14) \notin H$

23) Let $G = GL_2(\mathbb{C})$, $H < G$ be subgrp of upper Δ matrices. Show that $G = \bigcup_{g \in G} g H g^{-1}$

Ans From linear algebra (I think Schurs lemma):

If A is an $n \times n$ matrix over a field F that contains all e-vals of A, then $\exists$ non singular matrix S such that $S^{-1} A S$ is upper triangular

Clearly $H < G$ (product & inv of upper Δ is upper Δ)

By the theorem, if $A \in GL_2(\mathbb{C})$, then $\exists S$ such that $S^{-1} A S \in H$ so $A \in S H S^{-1}$

Hence $G = \bigcup_{S \in G} S H S^{-1} = \bigcup_{g \in G} g H g^{-1}$

24) Let $H < G$ with $|H| = n$. Show that $\bigcap_{|H| = n} H \triangleleft G$

Let $g \in G$. $H < G \Rightarrow g H g^{-1} < G$ and $|g H g^{-1}| = |H|$ as $g H g^{-1} = i_g(H)$

where $i_g : G \to G$ is the automorphism $i_g(x) = gxg^{-1}$

let $y \in \bigcap_{|H|=n} H$

$\therefore \forall K < G$ s.t. $|K| = n$, $y \in K$

and in particular $|gKg^{-1}| = n$

$\Rightarrow y \in gKg^{-1}$

$\Rightarrow gyg^{-1} \in K \quad \forall y \in K$ (also $\forall K$)

~~$K \lhd G$~~ $\notin$

$\therefore \bigcap_{|K|=n} K \lhd G$

3) $H \lhd G$ with H cyclic, show that every subgroup $K \subset H$ is also normal in G.

Ans $H = \langle g \rangle$, $K = \langle g^n \rangle$ for some $n \geq 1$

$gag^{-1} = a^t$ for some t

$ga^n g^{-1} = a^{nt} \in K$

$\Rightarrow g(a^n)^s g^{-1} = a^{nst} = (a^{nt})^s \in K$

$\therefore K \lhd G$

TUTORIAL 8

1) Let $H, K < G$. Show that $xH \cap yK$ is either empty or is a left coset of $H \cap K$. Prove that $[G : H \cap K] < \infty$ if $[G:H]$ and $[G:K] < \infty$

Ans let $xH \cap yK$ not be empty

$\therefore a \in xH \cap yK$

but $a \in aH \cap aK = a(H \cap K)$ (with intersection)

two left cosets are either empty or equal

$\therefore a(H \cap K) = xH \cap yK$

Also, each left coset of $H \cap K$ is an intersection of a left coset of H and a left coset of K

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

2) Let $f : G \to G'$ be a surjective homomorphism. Let $H' < G'$ and $H = f^{-1}(H')$. Show that $[G : H] = [G' : H']$

Ans Define $\varphi : \frac{G}{H} \to \frac{G'}{H'}$

as $\varphi(gH) = f(g)H'$

f is surjective $\Rightarrow \varphi$ is surjective

Let $aH = bH$ i.e. $ab^{-1} \in H$

we need to make sure $f(a)H' = f(b)H'$

i.e. $f(ab^{-1}) \in H'$

$H = f^{-1}(H') \Rightarrow ab^{-1} \in f^{-1}(H')$

$\Rightarrow f(ab^{-1}) \in H'$

and hence f is well defined

Also $f(a)H' = f(b)H'$

$\Rightarrow f(ab^{-1}) \in H'$

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

$\Rightarrow aH = bH$ $\therefore f$ is one-one

Hence f is bijective and

$$[G:H] = [G':H']$$

3) Find all 6 subgroups of S_4 containing the Klein 4 group V

Ans) $V = \{(1), (12)(34), (13)(24), (14)(23)\}$

We know $\frac{S_4}{V} \simeq S_3$

Let $\varphi : S_4 \to \frac{S_4}{V}$ be the natural map

$\varphi(\sigma) = \sigma V$

There are 3 subgroups of order 2 in S_3, whose inverse images have order 8 in S_4. There is one subgroup of order 3 namely A_3. Its inverse image has order 12 and is normal in S_4. Hence it must be A_4

$(12)V = (34)V$

$(13)V = (24)V$

$(14)V = (23)V$

So the 3 subgroups of S_4 of order 8 that contain V are inverse images of $\langle (12), V \rangle$, $\langle (13), V \rangle$ and $\langle (14), V \rangle$

$\therefore$ 6 subgroups of S_4 containing V are

S_4, A_4, V, $\langle (12), V \rangle$, $\langle (13), V \rangle$, $\langle (14), V \rangle$

4) Let $G = \langle x \rangle_{12}$, $G' = \langle y \rangle_6$. Define $f : G \to G'$ as $f(x) = y$. Establish 1-1 correspondence b/w subgrps of G & G'

Ans $f : G \to G'$

$f(x) = y$

$\ker(f) = \{ x \in G \mid f(x) = 1 \}$

$= \{ x^i \mid f(x^i) = y^i = 1 \}$

$= \{ 1, x^6 \}$

Subgroups of G' have orders $1, 2, 3, 6$ and they are $\{1\}$, $\langle y^3 \rangle$, $\langle y^2 \rangle$, $\langle y \rangle$

The inv images have orders $2, 4, 6, 12$

These are uniquely determined since G is cyclic

Subgroups of $\{1, x, x^2, \cdots, x^{11}\}$ containing $\{1, x^6\}$ are

$\langle x \rangle$, $\langle x^2 \rangle$, $\langle x^3 \rangle$, $\langle x^6 \rangle$,

$o = 12$ $o = 6$ $o = 4$ $o = 2$

5) Is S_3 a direct product of its proper subgroups

Ans S_3 has 2 proper subgroups of order 2 & order 3 which are cyclic. Thus their direct product is cyclic but S_3 is not. Hence, no!

6) Prove that the product of ∞ cyclic groups is not cyclic

Ans We show $\mathbb{Z} \times \mathbb{Z}$ is not cyclic

Let $\mathbb{Z} \times \mathbb{Z} = \langle (1, b) \rangle$

if $a=0$, then $(1,0) \notin \langle (0,b) \rangle$

if $b=0$, then $(0,1) \notin \langle (a,0) \rangle$

if $a,b \neq 0,0$, then if $(1,0) \in \langle (a,b) \rangle$ then

$(1,0) = n(a,b)$

$b \neq 0 \Rightarrow n = 0 \Rightarrow 1 = 0 \longrightarrow \leftarrow$

7) $H < G$, $K < G$. Show that $HK < G \iff HK = KH$

$(\Rightarrow)$ But $hk \in HK$

$(hk)^{-1} = k^{-1}h^{-1} \in HK$

But $k^{-1}h^{-1} \in KH$

$\therefore HK \subseteq KH$

Conversely if $kh \in KH$,

then $kh = (h^{-1}k^{-1})^{-1} \in HK$

(since $h^{-1}k^{-1} \in HK$ and $HK < G$)

$\therefore KH \subseteq HK$

$\therefore HK = KH$

$(\Leftarrow)$ $h_1k_1h_2k_2$

$= h_1(k_1h_2)k_2$

$= h_1 h'k' k_2$

$= h''k'' \in HK$

and $k_1^{-1}h_1^{-1} \left(= (h_1k_1)^{-1}\right) \in KH = HK$

$\therefore HK < G$

8) Let G have normal subgroups of order 3, 5. Show that G has an element of order 15

Ans Prime groups are cyclic

$\Rightarrow$ WLOG, $H = \langle x \rangle_3$, $K = \langle y \rangle_5$

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} = x(yx^{-1}y^{-1})$$

$(xyx^{-1}) \in K$, $(yx^{-1}y^{-1}) \in H$

$$\in H \cap K = \{1\}$$

$\therefore xy = yx$

We claim $o(xy) = 15$

$(xy)^{15} = 1 \Rightarrow o(xy) \mid 15$

Let $o(xy) = t$

$\therefore x^t = y^{-t}$

$\therefore o(x^t) = \frac{3}{\gcd(t,3)}$

$o(y^{-t}) = \frac{5}{\gcd(t,5)}$

if $t \neq 15$, then $t = 3$ or 5 or 1

$t \neq 1$ else $xy = 1 \Rightarrow x^{-1} = y$

but $x^{-1} = x^2 \Rightarrow y = x^2$ $\rightarrow\leftarrow$ since $H \cap K = \{1\}$

if $t = 3$, $o(x^t) = 1$, $o(y^{-t}) = 5$

$\therefore (xy)^t = x^t y^t = x^3 y^3 = y^3 \neq 1 \quad \rightarrow \leftarrow$

If $t = 5$,

$(xy)^5 = x^5 y^5 = x^2 \neq 1 \quad \rightarrow \in$

$\therefore t = \underline{\underline{15}}$

9) $|G| = ab$, $H, K < G$, $|H| = a$, $|K| = b$. Show that if $H \cap K = (1)$, then $G = HK$. Is $G \simeq H \times K$?

Ans We know that $|HK| = \frac{|H||K|}{|H \cap K|}$ by the product formula (theorem 91)

$|H \cap K| = 1 \Rightarrow |HK| = |H||K| = |H \times K| = ab = |G|$

$\therefore G = HK$

$G \neq H \times K$ in general as seen when

$G = S_3$, $H = \langle (12) \rangle$, $K = \langle (123) \rangle$

(Although $H \cap K = \{1\}$)

10) Let G, G' be groups. Prove $G \times \{1\} \trianglelefteq G \times G'$ and

$\frac{G \times G'}{G \times \{1\}} \simeq G'$

Ans We $h \in G$, $(g, g') \in G \times G'$

$(g, g') \cdot (h, 1) \cdot (g^{-1}, g'^{-1}) = (ghg^{-1}, 1)$

$\in G \times \{1\}$

$f : G \times G' \to G'$ as $f(g, g') = g'$

$\ker(f) = G \times \{1\}$

f is a surjective hom

$\Rightarrow \dfrac{G \times G'}{G \times \{1\}} \cong G'$

11) Show that $H = \{ A \in GL_n(\mathbb{R}) : \det(A) > 0 \} \triangleleft GL_n(\mathbb{R})$.

Further, describe $GL_n(\mathbb{R}) / H$

Ans Let $B \in GL_n(\mathbb{R})$, $A \in H$.

$\det(BAB^{-1}) = \det(A) > 0$

$\therefore BAB^{-1} \in H$

$\therefore H \triangleleft GL_n(\mathbb{R})$

Define $f : GL_n(\mathbb{R}) \to \{\pm 1\}$ as

$f(A) = \dfrac{\det A}{|\det A|}$

Then $\ker f = H$

and f is a surjective hom

$\Rightarrow \dfrac{GL_n(\mathbb{R})}{H} \cong \{\pm 1\} \cong C_2$

12) Let G be set of real upper triangular invertible 2×2 matrices.

Determine if the following describe normal subgrp

(i) $a_{11} = 1$, (ii) $a_{12} = 0$, (iii) $a_{11} = a_{22}$ (iv) $a_{11} = a_{22} = 1$

Further, analyse G/H if $H \triangleleft G$

Ans (i) $a_{11} = 1$

$$\Rightarrow H = \left\{ \begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix} \mid y \neq 0 \right\}$$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & y \end{bmatrix} \begin{bmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix}$$

$$= \begin{bmatrix} a & ax+by \\ 0 & cy \end{bmatrix} \begin{bmatrix} \frac{1}{a} & \frac{-b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \text{doesn't care} \\ 0 & y \end{bmatrix} \in H$$

$\therefore H \triangleleft G$

$f: G \to \mathbb{R}^\times$ s.t. $f(A) = a_{11}$ is a surjective hom with ker H

$$\therefore \frac{G}{H} \simeq \mathbb{R}^\times$$

(ii) $a_{12} = 0$

$$\Rightarrow H = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid ab \neq 0 \right\}$$

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & -x \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} a & bx - ax \\ 0 & b \end{bmatrix}$$

if $a \neq b$, this $\notin H$

$\therefore H \not\triangleleft G$

(iii) $a_{11} = a_{22}$

$\therefore H = \left\{ \begin{bmatrix} a & x \\ 0 & a \end{bmatrix} \mid a \neq 0 \right\}$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} a' & x \\ 0 & a' \end{bmatrix} \begin{bmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix}$$

$$= \begin{bmatrix} a' & -\frac{a'x}{c} \\ 0 & a' \end{bmatrix} \in H$$

$\therefore H \lhd G$

Define $f : G \to \mathbb{R}^*$ as $f(A) = \frac{a_{11}}{a_{22}}$

f is a surjective hom with kernel H

$\therefore \frac{G}{H} \simeq \mathbb{R}^*$

(iv) $a_{11} = a_{22} = 1$

$$H = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{R} \right\}$$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix} = \begin{bmatrix} 1 & \frac{ax}{c} \\ 0 & 1 \end{bmatrix}$$

$\in H$

$\therefore H \lhd G$

Define $f : G \to GL_2(\mathbb{R})$ as $f(A) = \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix}$

f is a hom with ker H

$\therefore G/H \simeq$ Im (f) = diagonal matrices in $GL_2(\mathbb{R})$

13) Find all normal subgroups of Q_8

Ans $H = \{1, -1, i, -i, j, -j, k, -k\}$

-1: order 2; $i, -i, j, -j, k, -k$: order 4

$\langle -1 \rangle$ :: clearly normal since

$x(-1) = (-1)x \quad \forall x \in Q_8$

subgroups of H other than $\langle -1 \rangle$ are

$\langle i \rangle, \langle j \rangle, \langle k \rangle$ (any combination like $\langle i, j \rangle$ is equal to Q_8)

To check if $\langle i \rangle = \{1, i, -i, -1\}$ is normal, it suffices to check if $x i x^{-1} \in \langle i \rangle$ $\forall x \in Q_8$

$x i x^{-1} \in \{1, i, -i, -1\}$ is indeed true for $\forall x \in Q_8$ (check manually)

Hence $\langle j \rangle$, $\langle k \rangle$ are also normal

14) Let $M, N \trianglelefteq G$ with $G = MN$. Prove that

$$\frac{G}{M \cap N} \simeq \frac{G}{M} \times \frac{G}{N}$$

Ans

$f : G \to \frac{G}{M} \times \frac{G}{N}$ as

$f(g) = (gM, gN)$

f is clearly a homomorphism

Since $f(gh) = (ghM, ghN)$

$f(g)f(h) = (gM, gN) \cdot (hM \cdot hN)$

$= (gMhM, gNhN)$

$= (ghM, ghN) \quad (\because M, N \triangleleft G)$

Let $f = \{g \in G \mid gM = M, gN = N\}$

$= M \cap N$

let $y \in \frac{G}{M} \times \frac{G}{N}$

$\therefore y = (m_1 n_1 M, m_2 n_2 N)$

We want to prove that $\exists\, g$ s.t.

$f(g) = (gM, gN) = (m_1 n_1 M, m_2 n_2 N)$

Note that $m_1 n_1 M = m_1 M n_1$

$= M n_1$

$= n_1 M$ $\}(\because M \triangleleft G)$

Illy $m_2 n_2 N = m_2 N$

$\therefore y = (n_1 M, m_2 N)$

Pick $g = n_1 m_2$

$\therefore f(g) = (n_1 m_2 M, n_1 m_2 N)$

$= (n_1 M, n_1 N m_2)$

$= (n_1 M, N m_2)$

$= (n_1 M, m_2 N)$

$= y$

Thus f is a surjective hom

$$\therefore \frac{G}{M \cap N} \cong \frac{G}{M} \times \frac{G}{N} \quad \text{by I isom thm}$$

15) Let $G = \{ z \in \mathbb{C}^\times \mid z^{p^n} = 1 \text{ for some } n \}$ for a fixed p. Prove that $f : G \to G$ as $z \longmapsto z^p$ is onto. Show that $G \cong \frac{G}{\ker f}$

Ans We need to make sure f is a surjective hom and we are done

Let $z \in G$. Then $z^{p^n} = 1$ for some n. Let ω be such that $\omega^p = z$

We need to show that $\omega \in G$

$$z^{p^n} = 1 \Rightarrow (\omega^p)^{p^n} = 1 \Rightarrow \omega^{p^{n+1}} = 1$$

$\therefore \omega \in G$ hence we are done by 1st iso thm

(f is clearly a hom)

16) Consider the abelian grp $E_{p^n} = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ (n times)

Show that $\forall\, g \in E_{p^n} \setminus \{1\}$ $o(g) = p$. Also Show that E_{p^2} has exactly $p+1$ subgrps of order p

Ans $g = (a_1, a_2, \cdots, a_n)$

$|g| = \text{lcm}(|a_1|, \cdots, |a_n|) = p$

($\because$ all of them are not 1)

Let r be no. of subgroups of order p.

$|E_{p^n}| = p^n = (p-1)r + 1$

$\therefore r = \frac{p^n - 1}{p-1}$

for $n = 2$, $r = p + 1$

(Why is $|E_{p^n}| = (p-1)r + 1$? Because two subgroups of order p are cyclic & hence intersect only at $\{1\}$)

(similar logic used in Q3 part 7)

17) Show that $Z(G \times H) = Z(G) \times Z(H)$

Ans $(g, h) \in Z(G \times H)$

$\Leftrightarrow \forall x, y \in G \times H$, $(xg, yh) = (gx, hy)$

$\Leftrightarrow \forall x \in G$ $xg = gx$, $\forall y \in H$, $yh = hy$

$\Leftrightarrow g \in Z(G)$, $h \in Z(H)$

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

via the bijection $f((g, h)) = (g, h)$

18) Let G be a group and $T = G \times G$. Show that $D = \{(g, g) \mid g \in G\}$ is isomorphic to G. Show that $D \lhd T$ iff G is abelian.

Ans $f : G \to D$ as $f(g) = (g, g)$

f is clearly onto and one one

$f(gh) = (gh, gh) = (g, g) \cdot (h, h)$

$= f(g)\, f(h)$

$\therefore D \simeq G$

$D \triangleleft T$ $(\forall g \in G)$

$\Leftrightarrow \forall (x, y) \in G \times G,\ (xg, yg) \cdot (gx, gy)$

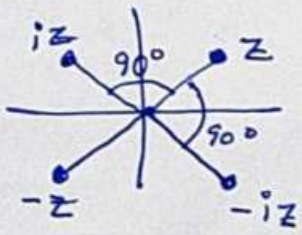
$\Leftrightarrow \forall x \in G,\ xg = gx, \quad \forall y \in G,\ gy = yg \ (\forall g \in G)$

$\Leftrightarrow \forall x \in G \quad xg = gx \quad (\forall g \in G)$

$\Leftrightarrow G$ is abelian

19) Let $H = \{\pm 1, \pm i\} < \mathbb{C}^*$. Find all left cosets of H and show that $\frac{G}{H} \simeq G$

Ans $zH = \{\pm z, \pm iz\}$



Let $f: G \to G$ as $f(z) = z^4$

Then f is a surjective hom with

kernel $= \{z \mid z^4 = 1\} = H$

$\therefore \frac{G}{H} \simeq G$

20) $K \triangleleft G$, $K' \triangleleft G'$. Show that $K \times K' \triangleleft G \times G'$ and $\frac{G \times G'}{K \times K'} \simeq \frac{G}{K} \times \frac{G'}{K'}$

Ans $f : G \times G' \to \frac{G}{K} \times \frac{G'}{K'}$

$f(g, g') = (gK, g'K')$

$\ker f = K \times K'$

f is a hom since $K \trianglelefteq G$, $K' \trianglelefteq G'$

We know ker of a hom is normal subgrp

$\therefore K \times K' \trianglelefteq G \times G'$

and f is a surjective hom

$$\Rightarrow \frac{G \times G'}{K \times K'} \simeq \frac{G}{K} \times \frac{G'}{K'}$$

TUTORIAL 9

1) Let $G = D_4$ be the group of symmetries of a square. Find the stabiliser group of vertices & edges

Ans $D_4 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

Let $V = \{1, 2, 3, 4\}$

• WLOG, we shall find G_v for $v \in V$ and $v = 1$

G acts on V and V is clearly an orbit because of rotations.

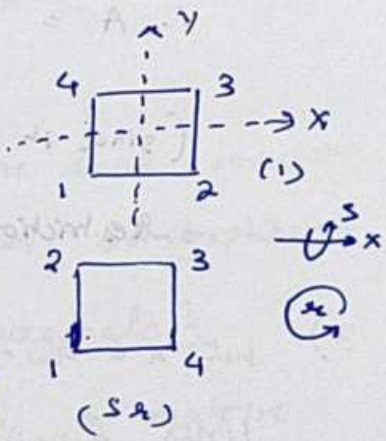
$\therefore |o(1)| \times |G_1| = |D_4| = 8$

$\therefore 4 \times |G_1| = 8$

$\therefore |G_1| = 8$

$1 \in G_1$ (by default)

$sr \in G_1$



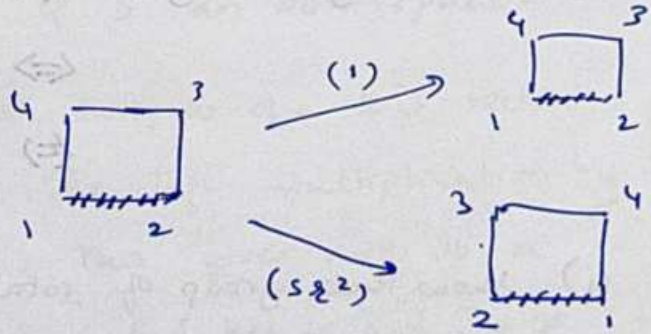
(note: under action of any group element, 1, 3 always remain opp)

By rotation, all 4 edges also form an orbit

$\therefore |G_{\overline{12}}| = 2$

$1 \in G_{\overline{12}}$

and $sr^2 \in G_{\overline{12}}$



2) $GL_n(\mathbb{C})$ acts on $\mathbb{R}^n$ by left multiplication. Describe decomposition of $\mathbb{R}^n$ into orbits. Find stab grp of e_1.

Ans The orbit of 0 is $\{0\}$

Any vector in $\mathbb{R}^n \setminus \{0\}$ can be transformed to any other vector in $\mathbb{R}^n \setminus \{0\}$ via some transformation $T \in GL_n(\mathbb{R})$.

This is justified because $\exists\ T \in GL_n(\mathbb{R})$ that changes the basis $\{v, v_1, v_2, \cdots, v_{n-1}\}$ to $\{v, v_2, v_3, \cdots, v_{n-1}\}$ and hence $T(v) = v$ (Additionally $T(v_i) = v_i$)

$\therefore \mathbb{R}^n \setminus \{0\}$ is an orbit.

If $A \in G_{e_1}$, then $Ae_1 = e_1$

$$\therefore A = \begin{bmatrix} e_1 & v_2 & v_3 & \cdots & v_n \end{bmatrix}_{n \times n} \in GL_n(\mathbb{R})$$

(since it is invertible, $\{v_2, \cdots, v_n\}$ have additional restriction that $\{e_1, v_2, \cdots, v_n\}$ must form a basis)

3) Let $x \in G$. Show that if the left multiplication by x fixes every coset of $H = \langle x \rangle$ in G, then $H \triangleleft G$

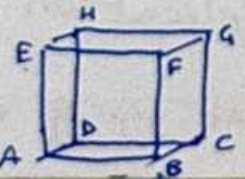
Ans $xgH = gH \iff g^{-1}xg \in H$

$\iff g^{-1}x^i g \in H$

$\iff H \triangleleft G$

4) Show that group of rotational symmetries of a cube is isomorphic to S_4 by considering action on body diagonals

Ans



$X = \{AG, BH, CE, DF\}$ = set of body diagonals

Considering the action on faces, the orbit has all 6 faces for any given face

$\therefore |O(x)|\,|G_x| = |G|$

and $|G_x| = 4$ for any given face x

4 rotations

$\therefore |G| = 6 \times 4 = 24$

Define $\varphi : G \to S_4$ where the homomorphism arises from the group action of G on the body diagonals set X. Note that $S_X = S_4$

Note that $|G| = |S_4| = 24$.

Thus if we show injectivity, we are done since it automatically is surjective and hence an isomorphism

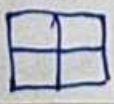
$\ker \varphi = \{g : \varphi(g)$ fixes all body diagonals$\}$

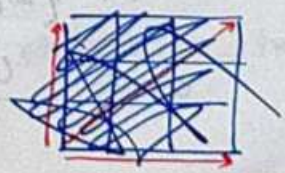
But any 3 diagonals are LI and if a matrix fixes them, it must be the identity matrix.

$\therefore \ker \varphi = \{id\} \Rightarrow \varphi$ is an isomorphism

5) Let $F = \mathbb{F}_3$. There are 4 1D subspaces of a 2D vector space F^2. Describe them. The left multiplication by $A \in GL_2(\mathbb{F}_3)$ permutes them. This gives rise to a homomorphism $\varphi : GL_2(F) \to S_4$. And $\ker \varphi$ and $\mathrm{Im}\,\varphi$

Ans $F^2 = \mathbb{F}_3 \times \mathbb{F}_3 = \{0,1,2\} \times \{0,1,2\}$





Any 1D subspace is generated by u and is hence $\{0, u, 2u\}$ for any of the 9 vectors a from $\mathbb{F}_3 \times \mathbb{F}_3$

Putting $u=0$ just gives $\{0\}$ which is 0-dimensional

For the other 8 options, u & $2u$ occur twice

ie. 2 options are the same

$u = (1,0) = e_1$ or $(2,0)$ gives $\{(0,0), (1,0), (2,0)\} = \langle e_1 \rangle$

$u = (0,1) = e_2$ or $(0,2)$ gives $\{(0,0), (0,1), (0,2)\} = \langle e_2 \rangle$

$u = (1,1)$ or $(2,2)$ gives $\{(0,0), (1,1), (2,2)\} = \langle e_1+e_2 \rangle$

$u = (1,2)$ or $(2,1)$ gives $\{(0,0), (1,2), (2,1)\} = \langle e_1-e_2 \rangle$

Thus we have 4 1D subspaces defined as above

$|GL_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 48$

Notice that e_1, e_2, e_1+e_2, e_1-e_2 are all LI. Thus they can be permuted by some $g \in GL_2(\mathbb{F}_3)$

$\therefore$ All 2-cycles are present in $\operatorname{Im}\varphi$ (why? even IDK :c)

But 2-cycles generate S_4 and hence φ is onto

$$\therefore \frac{G}{\ker\varphi} \simeq S_4 \quad \Rightarrow \quad \frac{48}{|\ker\varphi|} = 24$$

$$\therefore |\ker\varphi| = 2$$

$I \in \ker\varphi$

Also, $-I$ fixes each 1D subspace

$\therefore \{I, -I\} = \ker\varphi$

and $\dfrac{GL_2(\mathbb{F}_3)}{\ker\varphi} \simeq S_4$

6) Prove that G is a simple abelian grp $\Leftrightarrow$ $|G|$ is prime

Ans ($\Leftarrow$) $|G|$ is a prime number. Let $|G| = p$

let $x \in G$

$o(x) \mid p$

$\therefore o(x) = p \quad (x \neq e)$

$\therefore$ G is a cyclic group of order p

$\therefore G = \langle x \rangle_p$

$\therefore$ G is abelian

G is also simple since order of each non-identity element divides p and hence is p.

Thus every subgroup is the full group

($\Rightarrow$) Suppose $|G| = \infty$,

then since G is simple, for some $x_0 \in G$

$G = \langle x_0 \rangle$

But $\langle x_0^2 \rangle \triangleleft G$ which is a contradiction

$\therefore |G| < \infty$

let $|G| = n$. For any $d \mid n$, $\exists$ a subgrp of G of order d. Since G is abelian, every subgroup is normal.

$\therefore$ there should exist no such d $\Rightarrow d = 1$ or n

Hence, n is prime

7) Find $|C\left(\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\right)|$ in $GL_2(\mathbb{F}_5)$

Ans $|GL_2(\mathbb{F}_5)| = (5^2-1)(5^2-5) = 480$

$|C\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)| = [G : G_A]$ by the orbit stab theorem (where $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$)

let us find $|G_A|$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} a & 2b \\ c & 2d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ 2c & 2d \end{bmatrix}$$

$2b = b \Rightarrow b = 0$

$2c = c \Rightarrow c = 0$

$\therefore G_A = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in GL_2(\mathbb{F}_5) \;\middle|\; a, d \in \mathbb{F}_5, \det \neq 0 \right\}$

$\therefore |G_A| = 16$

$(\because a \neq 0, d \neq 0$ else $\det = 0)$

$\therefore [G : G_A] = \frac{480}{16} = 30$

8) Find class equations for

(i) Quaternion group

(ii) Group of upper triangular matrices in $GL_2(\mathbb{F}_3)$

(iii) $SL_2(\mathbb{F}_3)$

Ans (i) $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$

$Z(Q_8) = \{\pm 1\}$

$C(i) = \{\pm i\}$

$C(j) = \{\pm j\}$

$C(k) = \{\pm k\}$

$\therefore 8 = 2 + 2 + 2 + 2$

is the required class eqn.

(iii) we claim that U = grp of upper triangular matrices in $GL_2(\mathbb{F}_3)$, is isomorphic to D_{2n} with $n = 6$.

This is seen by choosing the isomorphism

$f: D_{12} \to U$ such that

$$f(r) = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$$

$$f(s) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$\therefore$ we just need to find the class eqn of D_{2n} with $n = 6$. we find the general class eqn of D_{2n}

$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$

let us find the conjugacy classes for n = odd

$\{1\}$ forms its own conjugacy class

$C(r^i) = \{r^i, r^{-i}\}$

since $(sr^t)^{-1} = sr^t$

and $sr^t \times r^i \times sr^t$

$= s r^i r^t s r^t$

$= s r^i s$

$= r^{-i}$

(conjugation with r^t gives r^i only)

$C(sr^i) = \{sr^k \mid k = 0, 1, \dots, n-1\}$

since $sr^t sr^i sr^t = sr^k$

$\Rightarrow n \mid 2t - i - k$

and hence we choose $t = \frac{i+k}{2}$ or $\frac{i+k+n}{2}$ (n odd)

Also, $x^t s x^i x^{-t} = s x^{i-2t}$

∴ The class equation is :

$$1 + \underbrace{2 + 2 + 2 + \cdots + 2}_{\frac{(n-1)}{2} \text{ 2's}} + \frac{n}{2}$$

For n even, we get

$$2 + \underbrace{2 + 2 + \cdots + 2}_{\left(\frac{n-2}{2}\right) \text{ 2's}} + \frac{n}{2} + \frac{n}{2}$$

$Z(G) = \{1, x^{n/2}\}$; same as before ; $\{sx^{2k+1} \; \forall k\}$; $\{sx^{2k} \; \forall k\}$

(note that $i+k$ will be forced to be even and hence we get 2 separate conjugacy classes for the sx^t type elements)

Here $n = 6 \Rightarrow 2 + 2 + 2 + 3 + 3$ is the required class equation

(iii) $$|SL_2(\mathbb{F}_3)| = \frac{1}{3-1} \prod_{i=0}^{2-1} (3^2 - 3^i)$$

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

$$= 24$$

$Z(G) = \{\pm I\}$

Pick

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \quad C = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix} \quad E = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \quad D = \begin{bmatrix} -1 & -1 \\ 0 & -1 \end{bmatrix}$$

A, B → order 3
C, D → order 6
E → order 4

} Clearly Conjugacy classes wont intersect due to different orders

Claim: $\nexists\ X \in SL_2(F_3)$ s.t. $XAX^{-1} = B$

and $\nexists\ X \in SL_2(F_3)$ s.t. $XCX^{-1} = D$

Suppose $XA = BX$,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$\Rightarrow c = 0,\ a + d = 0 \Rightarrow c = 0,\ a = -d$

But [redacted] $\cdot\ ad - bc = 1$

$\Rightarrow$ [redacted] $- a^2 = 1$

$\Rightarrow a^2 = -1$

but this has no solution in F_3

Similarly $XCX^{-1} = D$ cannot hold

∴ All these 5 matrices form 5 disjoint conjugacy classes

Find $|Z(M)|$ $\forall$ $M = A, B, C, D, E$.

and then we are done (very lengthy)

The class eqn is $\underbrace{1 + 1}_{|Z(G)|} + 4 + 4 + 4 + 4 + 6$

1) Let $N \trianglelefteq G$ with $|N| = 5$, $|G|$ odd. Consider the action of G on N via conjugation. Prove that $N \subseteq Z(G)$

Ans group action gives a homomorphism $\varphi : G \to Aut(N)$

[redacted] with $\varphi(g) = i_g$

and $i_g(n) = gng^{-1}$ $\forall n \in N$

$|G| = |\ker\varphi||\mathrm{Im}\,\varphi|$ (holds ∀ homomorphisms)

$\mathrm{Aut}\,N \cong U(5)$ ($\because |N|=5 \Rightarrow N \cong \mathbb{Z}_n$ & $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$)

$\Rightarrow |\mathrm{Aut}\,N| = 4$ ($\because \phi(5) = 5(1-\frac{1}{5}) = 4$)

$\therefore |\mathrm{Im}\,\varphi| = 1$ or 2 or 4 ($\because \mathrm{Im}(\varphi) <$ [redacted](φ))

G is odd $\Rightarrow |\mathrm{Im}\,\varphi| = 1$

$\therefore i_g(n) = gng^{-1} = n \quad \forall g \in G$

$\therefore N \subseteq Z(G)$

10) Let G be a finite grp, $H \leq G$ with index n so that $|G| \nmid n!$. Show that G is not simple.

Ans Let G act on G/H via left multiplication as

$G \times G/H \to G/H$ with $(a, gH) \mapsto agH$.

Let $\varphi : G \to S_n$ be the induced homomorphism.

If $\ker\varphi = \{1\}$ then bcoz $\varphi(G) < S_n \Rightarrow |\varphi(G)| \mid n!$

(since $\ker\varphi = \{1\}$, $|\varphi(G)| = |G| \mid n!$) Contradiction!

$\therefore \ker(\varphi) > \{1\}$ and kernel is a normal subgroup. Also, $\ker(\varphi) \neq G$ else

$\varphi(a) = id \quad \forall a \in G \Rightarrow agH = gH \quad \forall g, a \in G$

$\Rightarrow g^{-1}ag \in H \quad \forall g, \forall a \in G \Rightarrow G = H$ →←

$\therefore \ker(\varphi)$ is a normal proper subgrp

$\therefore G$ is not simple

11) Let $|G| < \infty$, $H \leq G$ with $[G:H]$ = smallest prime p which divides $|G|$. Prove that $H \trianglelefteq G$

Ans Let H act on G/H as

$(h, gH) \mapsto hgH$

By orbit stab theorem,

$|o(gH)| \mid |H|$

and $|H| \mid |G|$

$\therefore |o(gH)| \mid |G|$

Now, there are p left cosets of H in G

But p is the smallest prime dividing G

$\therefore |o(gH)|$ has to be $1 \ \forall \ gH$

or $|o(gH)| = p$ (ie. only one orbit)

Second option is impossible since orbit of H is just H

$\therefore$ All orbits are single element orbits

$\therefore \forall h \in H, \ hgH = gH$

$\therefore g^{-1}hg \in H \ \forall \ h \in H$

g was arbitrary in G

$\therefore H \triangleleft G$

12) Let $|G| = p^n$ with $p > n$. Prove that if $H < G$ with $|H| = p$, then $H \triangleleft G$

Ans Really easy with Sylow theorems at hand but without them also, we can prove it.

Claim: There is a unique subgroup of order p

Supposing our claim is true, then if H is a subgroup (of order p), we know that gHg^{-1} is always a subgroup $\forall g$ ($\forall H < G$)

$\therefore gHg^{-1} = H \Rightarrow H \lhd G$. Now we prove the claim

Suppose P & Q are subgroups of order p and $P \neq Q$. Then $P \cap Q = \{1\}$ by Lagranges theorem. (since P & Q are cyclic bcoz of prime order)

($\because |H \cap K|$ divides $|H| = p \Rightarrow |H \cap K| = 1$ or p)

$|G| = pn < p^2$, $P = \langle x \rangle_p$, $Q = \langle y \rangle_p$

elements of the form $x^i y^j \in G$ $\forall i, j \in \{1, 2, \ldots, p\}$

But $|G| < p^2$

$\therefore x^i y^j = x^k y^l$ for some indices i, j, k, l with $(i, j) \neq (k, l)$

$\therefore x^{i-k} = y^{l-j}$

Contradiction since $P \cap Q = \{1\}$

13) Let $|G| = 2m$ with m odd. Analyse action of G on G by left multiplication and show that G has a subgroup of index 2

Ans $G \times G \longrightarrow G$

$(g, h) \mapsto gh$

$\varphi : G \longrightarrow S_{2m}$ is the induced hom

$|G| = 2m \Rightarrow 2 \mid |G| \Rightarrow$ G has an element of order 2 (call it x)

Then $f(x) \in S_{2m}$

and $(f(x))(g) = xg$

$o(x) = 2 \Rightarrow f(x)$ has no fixed points

(else, $(f(x))(g) = g \Rightarrow xg = g \Rightarrow x = 1$)

f is one-one since $f(a) = f(b) \Rightarrow f(a) \& f(b)$ agree $\forall g \in G \Rightarrow (f(a))(g) = (f(b))(g)$

$\Rightarrow ag = bg$

$\Rightarrow a = b$

$\therefore o(f(x)) = 2$ (one one hom preserves order)

Now $f(x)$ is of ordr 2 & has no fixed points and $f(x) \in S_{2m}$

$\therefore f(x)$ is a product of m disjoint 2-cycles

$\therefore f(x)$ is an odd permutation

$\therefore f(G)$ has a subgrp H of index 2 consisting of even permutations (idk how :c)

14) Let G be finite of order p^n, $n \geq 2$. Show that any subgroup H of order p^{n-1} is normal in G

Ans G acts on G/H by left multiplication

$f : G \to S_{G/H}$ is the induced permutation rep

$\ker f = \{g \in G \mid gaH = aH \ \forall a \in G\}$

$gaH = aH \iff g \in aHa^{-1}$

$\therefore \ker f = \bigcap_{a \in G} aHa^{-1} \subseteq H$

(since $eHe^{-1} = H$)

Denote $\ker f = K$

$K < H \Rightarrow p^2 \mid \left|\frac{G}{K}\right| \mid p!$

But $p^2 \nmid p^2 \Rightarrow \ker f = H \lhd G$

$\because \left|\frac{G}{\ker f}\right| = |\mathrm{Im}\, f| \mid |S_{G/H}| = p!$

(Alternative path from here :

$\frac{|G|}{|K|} \mid p!$

$\Rightarrow \frac{p^n}{|K|} \mid p!$

$\Rightarrow |K| = p^n$ or p^{n-1}

$K \subseteq H$ and $|H| = p^{n-1}$

$\Rightarrow |K| = p^{n-1}$ and in particular $K = H$

15) Find the centraliser of $(12)(34)$ in S_n for $n \geq 4$ and prove that $|Z((12)(34))| = (n-4)! \times 8$

Ans $\sigma(12)(34)\sigma^{-1}$

$= (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$

$= (1\ 2)(3\ 4)$

∴ We need those perms σ which fix 1234 to 1234 (these are $(n-4)!$ of them) and further $\sigma(1)$ can be 1, 2, 3 or 4 after which $\sigma(2)$ is forced & $\sigma(3)$ has 2 choices left $\Rightarrow$ 8 choices to make.

$\therefore (n-4)! \times 8$

b) Prove for an odd n that the set of all n-cycles in A_n is a disjoint union of two conjugacy classes of equal size (by first computing centraliser of an n-cycle)

Any n = odd $\Rightarrow$ n-cycle $\in A_n$

There are $\frac{n!}{n} = (n-1)!$ no. of n-cycles

Let us find the centraliser. Let σ be in the centraliser. σ (n cycle) σ^{-1} = (n cycle)

$\therefore \sigma(a_1\ a_2 \cdots a_n)\sigma^{-1} = (a_1 \cdots a_n)$

$\Rightarrow (\sigma(a_1)\ \sigma(a_2) \cdots \sigma(a_n)) = (a_1 \cdots a_n)$

$\sigma(a_1)$ has n choices & after this is picked, we are forced to choose other $\sigma(a_i$'s)

$\therefore$ σ has $\leq n$ possibilities

BW- $\langle n\text{-cycle} \rangle \subset Z(n\text{-cycle})$

$\therefore |Z(n\text{cycles})| = n$

$\therefore |C(n\text{cycle})| = \frac{n!}{2n} = \frac{(n-1)!}{2}$

Thus there are two conjugacy classes of equal order
(conjugacy classes have all the elements of the same cycle type)

17) Let $\sigma \in S_n$ be a product of k_i cycles of length m_i for $i = 1, 2, \dots, s$ and $n = \sum_{i=1}^{s} k_i m_i$.

Show that $|C(\sigma)| = \frac{(n!)}{(m_1^{k_1} m_2^{k_2} \cdots m_s^{k_s})(k_1! \cdots k_s!)}$

Any There are k_1 no. of m_1-cycles [illegible] ...

$\therefore$ These can be written in $m_1^{k_1}$ ways which are all the same and further they can be swapped as $\sigma\tau = \tau\sigma$ (since they are all disjoint)

$\therefore |C(\sigma)| = \frac{n!}{\prod_{i=1}^{s} m_i^{k_i} k_i!}$

18) Find conjugacy classes of D_{2n}

Ans Already seen in Q8(ii) but anyways ... they are

$\{1\}$, $\{r^k\}$, $\{r^{\pm 1}\}$, $\{r^{\pm 2}\}, \dots, \{r^{\pm(k-1)}\}$

$\{sr^{2b} \mid b = 1, 2, \dots k\}$, $\{sr^{2b+1} \mid b = 1, \dots, k\}$

for $n = 2k$

and for $n = 2k+1$, they are

$\{1\}, \{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm k}\}$,

$\{sr^{2b} \mid b = 1, 2, \ldots k\}, \{sr^{2b-1} \mid b = 1, 2, \ldots, k\}$

19) Let $p < q$ be primes. Let $|G| = pq$. Show that G has a non-normal subgroup of order p and hence find an injective hom from G to S_q

Ans We have already seen in Q12 that there exists a normal subgroup of order q. (Call it H)

Suppose K is a subgroup of G of order p

(K exists by Cauchy's theorem).

H & K are prime groups and hence cyclic

Let $H = \langle x \rangle_q$, $K = \langle y \rangle_p$

Claim: $H \cap K = \{1\}$

$H \cap K < H$

$\Rightarrow |H \cap K| \mid q$

$\Rightarrow |H \cap K| = 1$ or q

But $|H \cap K| \neq q$ else $|H \cap K| < K$ is violated

Since $q \neq p$

$\therefore$ By the product formula, $|HK| = \frac{|H|\,|K|}{|H \cap K|}$

$\Rightarrow |HK| = pq$ but $HK \subseteq G \Rightarrow HK = G$

But $H \cap K = id \Rightarrow HK \cong H \times K$

$\therefore G \cong H \times K$

but H & K are prime cyclic with orders p, q

$\Rightarrow H \times K$ is cyclic

$\Rightarrow G$ is cyclic

$\Rightarrow G$ is abelian

$\longrightarrow \longleftarrow$

$\therefore K$ is non-normal of order p

Now let G act on G/K

$G \times G/K \longrightarrow G/K$

$(g, aK) \longmapsto gaK$

This gives rise to the homomorphism

$\varphi : G \to S_{G/K} \cong S_{\left|\frac{G}{K}\right|} = S_q$

i.e. $\varphi : G \to S_q$

We know, $\ker(\varphi)$

$= \{ g \in G \mid gaK = aK \ \forall a \in G \}$

$= \{ g \in G \mid a^{-1}ga \in K \ \forall a \in G \}$

$= \{ g \in G \mid g \in aKa^{-1} \ \forall a \in G \}$

$\subseteq K$

Also, $\ker(\varphi) \leq K$

since $\forall\ a, b \in \ker \varphi$,

$\varphi(ab) = \varphi(a)\varphi(b) = id \cdot id = id$

and $\forall\ a \in \ker \varphi$

$(\varphi(a))^{-1} = \varphi(a^{-1}) = id \Rightarrow a^{-1} \in \ker \varphi$

Also since $\varphi : G \to S_p$,

$\ker \varphi \triangleleft G$

$|\ker \varphi| \mid |K| = p$

$\Rightarrow |\ker \varphi| = 1$ or p

But order p subgroups are not normal in G

and $\ker \varphi \triangleleft G$

$\Rightarrow |\ker \varphi| = 1$

$\Rightarrow \varphi$ is injective

20) For $|G| = \text{odd}$, $x \in G$ s.t. $x \neq 1$, show that x and x^{-1} are not conjugates.

Ans Suppose they are conjugates.

Then $\exists\, g$ s.t.

$$g x g^{-1} = x^{-1}$$

i.e. $x g x = g \quad \Rightarrow xg = gx^{-1}$

$(xg)^1 = xg$

$(xg)^2 = g^2$

$(xg)^3 = g^2 xg = g^3 x^{-1}$

$(xg)^4 = g^4$

$(xg)^5 = g^5 x^{-1}$

$\vdots$

By induction,

$(xg)^{2k} = g^{2k}$

$(xg)^{2k+1} = g^{2k+1} x^{-1}$

let $|G| = n = \text{odd}$.

$\therefore (xg)^{n-1} = g^{n-1}$

and $(xg)^{n-1} g = g^n = id \quad (\because o(g) \mid n)$

$\therefore g^{-1} = (xg)^{n-1}$

$\therefore (xg)(g^{-1}) = (xg)^n$

$\therefore x = g^n x^{-1}$

$\therefore x = x^{-1}$

$\therefore x^2 = 1$

But $|G| = \text{odd} \Rightarrow G$ has no order 2 element

$\therefore x = 1$

$\rightarrow \leftarrow$

TUTORIAL 10

1) Show that there are two isomorphism classes of groups of order 6

Ans Claim: There are only 2 isomorphism classes of groups of order 6 which are precisely C_6 and S_3

proof of claim:

$6 = 2 \times 3$

Let N_2 be the no. of sylow 2 subgrps

N_3 be the no. of sylow 3 subgroups

Then $N_2 \mid 3$ and $2 \mid N_2 - 1$

$\therefore N_2 = 1$ or 3

Similarly $N_3 \mid 2$ and $3 \mid N_3 - 1$

$\therefore N_3 = 1$

By Sylow's 2nd theorem,

the Sylow 3 subgroup is normal

If $N_2 = 1$, the Sylow 2 subgroup is also normal

and $\{1, x\}$ and $\{1, y, y^2\}$ will be

groups such that $H \cap K = \{1\}$

$\Rightarrow G \simeq H \times K \simeq C_2 \times C_3 \simeq C_6$

If $N_2 = 3$, let the three groups be $P = \{1, y\}$

let Q be the normal sylow 3 subgroup $\{1, x, x^2\}$

$y^{-1} x y \in Q$

$y^{-1} x y \neq id$ else $x = id$ $\rightarrow\leftarrow$

$y^{-1} x y \neq x$ else $xy = yx$ and $o(xy) = 6$

$\Rightarrow G$ is abelian and we get back C_6

$\therefore y^{-1} x y = x^2 \Rightarrow xy = y x^2 = y x^{-1}$

$\Rightarrow xyxy = id$

$\therefore G = \langle x, y \mid x^3 = 1, y^2 = 1, xyxy = 1 \rangle$

$\simeq S_3$

2) Every group of order 15 is cyclic

Ans $n_5 \mid 3$ and $n_5 \equiv 1 \pmod 5$

$\Rightarrow n_5 = 1$

$\Rightarrow \exists ! \; P \lhd G$ with $|P| = 5$

$n_3 \mid 5$ and $n_3 \equiv 1 \pmod 3$

$\Rightarrow n_3 = 1$

$\Rightarrow \exists ! \; Q \lhd G$ with $|G| = 3$

but $P = \{1, a, a^2, a^3, a^4\}$

$Q = \{1, b, b^2\}$

$P \cap Q < P \Rightarrow |P \cap Q| \mid 5$

$P \cap Q < Q \Rightarrow |P \cap Q| \mid 3$

$\Rightarrow P \cap Q = \{1\}$

$\Rightarrow HK \cong H \times K \quad (H, K = P, Q)$

but $|HK| = 15 = |G|$

$\Rightarrow G \cong H \times K$

$\Rightarrow G \cong C_5 \times C_3$

$\Rightarrow G$ is cyclic

3) Classify Abelian groups of order 18

Ans $18 = 2 \times 3^2$

$n_2 \mid 9$, $n_2 \equiv 1 \pmod 2$

$\Rightarrow n_2 = 1$ or 9

$n_3 \mid 2$, $n_3 \equiv 1 \pmod 3$

$\therefore N_3 = 1$

$\therefore$ There is a sylow 3 subgroup

$\therefore \exists! \; P \text{ s.t. } |P| = 9, \quad P \trianglelefteq G$

There could be a unique sylow 2 subgrp of 9 different sylow-2 subgroups but we know for sure that order 2 subgroups are isomorphic to C_2

let $|H| = 2, \quad H = \{1, x\}$

Now we classify P (i.e. groups of order 9)

(note: index of P in G = 2 $\Rightarrow P \trianglelefteq G$ anyways)

$9 = 3^2$ and group of order p^2 is abelian

By classification of abelian groups,

$$P \cong C_9 \quad \text{or} \quad P \cong C_3 \times C_3$$

Alternately, $3 \mid 9$ and P is abelian (or also first sylow can be used) $\Rightarrow$ P has element of order 3. Consider it to be some $a \in P$

(Note that if $P \neq C_9$, then $\forall a \in P, \; o(a) = 3$ for $a \neq e$)

$\langle a \rangle < P$ but $b \in P \setminus \langle a \rangle$. Consider $\langle b \rangle$. This is also a subgroup of P.

$\langle a \rangle \cap \langle b \rangle = e \quad \Rightarrow |\langle a, b \rangle| > 3$

but $|\langle a, b \rangle| \mid 9 \quad \Rightarrow |\langle a, b \rangle| = 9$

$\Rightarrow G = \langle a, b \rangle$

$H \simeq C_2$ $\quad$ $H \simeq C_2$

$P \simeq C_9$ $\quad$ $P \simeq C_3 \times C_3$

$\Downarrow$ $\quad$ $\Downarrow$

$G \simeq H \times P$ $\quad$ $G \simeq H \times P$

(since $H \cap P = \{1\}$ (bcoz $|H|, |P|$ are coprime))

4) Find the no. of Sylow p subgroup of S_p

Ans $\quad |S_p| = p! = p(p-1)!$

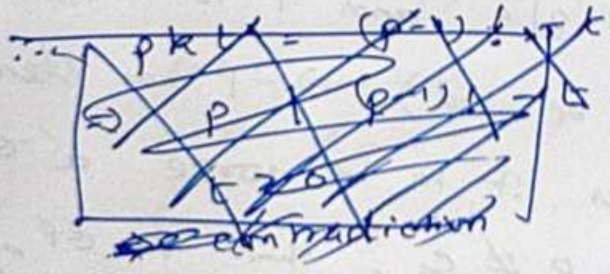
$n_p \mid (p-1)!$, $\quad n_p \equiv 1 \pmod p$

$n_p = pk + 1$ for some $k \in \mathbb{Z}$

$pk+1 \mid (p-1)!$

$k = 0$ Otherwise,

$(pk+1)t = (p-1)!$



$\Rightarrow t \mid (p-1)!$

Cant solve from here :'(

Any sylow p subgroup is cyclic of order p (in S_p)

Further, any 2 sylow p subgroups intersect at $\{1\}$.

no. of p cycles in $S_p = (p-1)!$

- If $\{p\text{-cycles}\} = \{1, x_1, x_2, \ldots, x_{(p-1)!}\}$,

then we form N_p no. of p-size groups, each grp has 1 along with $p-1$ other elements

$\therefore N_p \times (p-1) = (p-1)!$ (using all of the x_i)

$\therefore N_p = (p-2)!$

Also, $(p-2)! \mid (p-1)!$

and $p \mid (p-2)! - 1$

Alternate proof of Wilsons

(From here, $(p-2)! \equiv 1 \pmod p$

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

$= -1 \pmod p$)

5) G is a group of order 28 which is non-abelian. It has all Sylow 2-subgroups cyclic. Find N_2, N_7 and show that there is only one such G upto isomorphism. Find its class equation

Ans $|G| = 2^2 \times 7$

$N_2 \mid 7$, $N_2 \equiv 1 \pmod 2$ $\Rightarrow N_2 = 1$ or 7

$N_7 \mid 4$, $N_7 \equiv 1 \pmod 7$ $\Rightarrow N_7 = 1$

$\therefore$ Sylow 7 subgrp is a cyclic, unique, normal subgp of order 7

let $P = \langle x \rangle_7$

$N_2 \neq 1$ else

$\langle y \rangle_4$ is a unique normal subgrp of order 4

and $\langle x \rangle_7 \cap \langle y_4 \rangle = \{1\}$

$\Rightarrow G = \langle x \rangle_7 \times \langle y \rangle_4$

$\Rightarrow$ G is cyclic

$\Rightarrow$ G is abelian

contradiction

$\therefore N_2 = 7$

$P = \langle x \rangle_7$, $Q = \langle y \rangle_4$ (we know P is unique, Q is not unique (in fact there are 7 such subgrps))

Note: if Q is unique, then

$P \triangleleft G$

$Q \triangleleft G$

and $|PQ| = 28$

$PQ < G$

$\Rightarrow G \cong PQ \cong P \times Q$

But if $Q \not\triangleleft G$ then $PQ \ncong P \times Q$

$\therefore$ G will be isomorphic/equal to PQ

but not to $P \times Q$ and we will not be able to contradict wrong abelianness

$P \triangleleft G$

$\Rightarrow y x y^{-1} = x^i$

$y^2 x y^{-2} = y x^i y^{-1} = (x^i)^i = x^{i^2}$

$y^3 x y^{-3} = x^{i^3}$

$y^4 x y^{-4} = x^{i^4} = x$

$\therefore i^4 \equiv 1 \pmod 7$

$\therefore 7 \mid i^4 - 1$

$\therefore 7 \mid (i^2+1)(i+1)(i-1)$

Note : $i = 0, 1, 2, \ldots 6$

Manual solution is 1, 6 ie 1, −1

$i = 1 \Rightarrow y x y^{-1} = x$

$\Rightarrow yx = xy$

$\Rightarrow G$ is abelian $\longrightarrow\leftarrow$

$\therefore i = -1$

$\Rightarrow y x y^{-1} = x^{-1}$

$\Rightarrow xyx = y$

$\therefore$ one single group possible upto isomorphism

class eqn:

$G = \langle x, y \mid y^4 = id, x^7 = id, xyx = y \rangle$

claim: Every element of G can be written as $x^\alpha y^\beta$ because, $yx = x^{-1}y = x^6 y$

y^2 centralizes both x and y

Also, $\langle ab^2 \rangle$ has order 14 $\Rightarrow$ index 2 $\Rightarrow$ normal

We now list all conjugacy classes :

$\{1\}$ $\{a^i, a^{-i}\}$ → 3 classes $\{a^i b : i=0,1,\dots,6\}$

$\{b^2\}$ $\{a^i b^2, a^{-i}b^2\}$ → 3 classes $\{a^i b^3 : i=0,1,\dots 6\}$

[redacted]

$\therefore 28 = \underbrace{1+1}_{|Z(G)|} + (2+2+2) + (2+2+2) + (7) + (7)$

6) $|G| = 2p$ w odd prime p. show that $G \simeq D_{2p}$ or G is cyclic

Ans $N_2 \mid p$, $N_2 \equiv 1 \pmod 2 \Rightarrow N_2 = 1$ or p

$N_p \mid 2$, $N_p \equiv 1 \pmod p \Rightarrow N_p = 1$

$\therefore \exists!$ P s.t. $|P| = p$, $P \lhd G$

let $P = \langle x \rangle = \{1, x, x^2, \dots, x^p\}$

if $N_2 = 1$, we have seen so many times by now, $G \simeq PQ \simeq P \times Q \Rightarrow G$ is cyclic when $Q \lhd G$ and $|Q| = 2$

if $N_2 = p$,

we have $Q = \{1, y\}$ but $Q \not\lhd G$

$P \lhd Q$

$\Rightarrow$ [redacted] $yxy^{-1} = x^i$

[redacted]

$\Rightarrow$ $y\,yxy^{-1}\,y^{-1} = y^2xy^{-2} = (x^i)^i = x^{i^2}$

$\therefore \quad x = x^{i^2}$

$\Rightarrow \quad i^2 \equiv 1 \pmod{p}$

$\Rightarrow \quad i = \pm 1$

$i \neq 1$ else abelian $\Rightarrow$ cyclic

$\therefore i = -1$

$\therefore \quad y x y^{-1} = x^{-1}$

$\Rightarrow \quad xyx y^{-1} = id$

$\Rightarrow xy xy = id$

$yxyx = x^{-1} y y x = id$

$\therefore \quad G = \langle x, y \mid x^p = y^2 = 1, \; xy xy = yxyx = id \rangle$

$\cong D_{2p}$

7) classify groups of order 99

Ans $99 = 11 \times 3^2$

$n_{11} \mid 9$, $\quad n_{11} \equiv 1 \pmod{11} \Rightarrow n_1 = 1$

$n_3 \mid 11$, $\quad n_3 \equiv 1 \pmod{3} \Rightarrow n_3 = 1$

$\therefore$ Sylow 3 & Sylow 11 subgroups are both unique and normal

$\therefore \quad P \cap Q = id \Rightarrow G \cong PQ \cong P \times Q$

where $|P| = 11$, $\quad |Q| = 9$

$|Q| = 9 \Rightarrow Q \cong C_9$ or $Q \cong C_3 \times C_3$

$\therefore G \cong C_{11} \times C_3 \times C_3$ or $C_{11} \times C_9$

8) Let $|G| = 55$. Prove that $G = \langle x, y \rangle$ with $|x| = 11$, $|y| = 5$ with $yxy^{-1} = x^r$ for some $r \in \{1, 2, \ldots, 10\}$. Show that $r = 2, 6, 7, 8, 10$ are not possible but others are possible. Conclude that there are two isomorphism classes

Ans $|G| = 5 \times 11$

$n_{11} \mid 5$, $n_{11} \equiv 1 \pmod{11} \Rightarrow n_{11} = 1$

$n_5 \mid 11$, $n_5 \equiv 1 \pmod{5} \Rightarrow n_5 = 1$ or 11

Let the sylow 11 unique normal cyclic subgrp be $\langle x \rangle_{11}$

If $N_5 = 1$, then we have a unique normal cyclic subgrp of ordr 5 $\langle y \rangle_5$

and G is abelian with $G \cong \langle x \rangle_{11} \times \langle y \rangle_5$

and $yxy^{-1} = x^1$ ($\because G$ is abelian)

Let $N_5 = 11$ and $\langle y \rangle_5$ be the sylow 5 subgrp

Consider $\langle x, y \rangle$

$|\langle x, y \rangle| > 11 \Rightarrow |\langle x, y \rangle| = 55$

Also $\langle x \rangle_{11} \trianglelefteq G$

$\Rightarrow yxy^{-1} = x^r$ for some $r \in \{1, \ldots, 10\}$

($r \neq 0$ else $x = id$)

$\Rightarrow y^5 x y^{-5} = x^{r^5} = x$

$\Rightarrow x^{r^5} \equiv 1 \pmod{11}$

$\therefore r = 3, 4, 5, 9$

$yxy^{-1} = x^4 \Rightarrow y^2xy^{-1} = x^5 \Rightarrow y^3xy^{-3} = x^9$

$\Rightarrow y^4xy^{-4} = x^3 \Rightarrow r = 1, 4, 5, 9$ all correspond to a single group G

$\therefore G \simeq C_{55} \simeq C_{11} \times C_5$

or

$G \simeq \langle x, y \mid x^{11} = y^5 = id,\ yxy^{-1} = x^3 \rangle$

$\simeq \langle \quad " \quad " \quad x^4 \rangle$

$\simeq \langle \quad " \quad " \quad x^5 \rangle$

$\simeq \langle \quad " \quad " \quad x^9 \rangle$

9) Find no. of elements of order 5 in G s.t $|G| = 20$

Ans $|G| = 2^2 \times 5$

$n_5 \mid 4$, $n_5 \equiv 1 \pmod 5 \Rightarrow n_5 = 1$

$n_2 = 1$ or 5

$\therefore n_5 = 1 \Rightarrow$ 4 elements of order 5

(not more bcoz any element of order 5 will form the sylow 5-subgroup which is unique)

10) $G = \left\{ \begin{bmatrix} 1 & a \\ 0 & c \end{bmatrix} : a, c \in \mathbb{F}_7, c = 1, 2, 4 \right\}$. Show that any non abelian H s.t. $|H| = 21$ is isomorphic to G

Ans $|H| = 7 \times 3 = 21$

$N_7 = 1$

$N_3 = 1$ or 7

If $N_3 = 1$, H is abelian $\longrightarrow \leftarrow$

$\therefore N_3 = 7$

Let $\langle x \rangle_7$ be the unique normal sylow 7 subgrp

$\langle y \rangle_3$ be a sylow 3 subgrp

$y x y^{-1} = x^i$

$y^3 x y^{-3} = x^{i^3} = x$

$\Rightarrow i^3 \equiv 1 \pmod 7$

$\Rightarrow i = 1$ or 2 or 4

Notice that $y x y^{-1} = x$

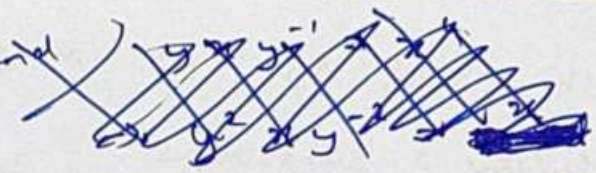
$\Rightarrow y^2 x y^{-2} = x^2$

$\Rightarrow y^4 x y^{-4} = x^4$

$\therefore H \cong \langle x, y \mid x^7 = 1, y^3 = 1, y x y^{-1} = x \rangle$

$i \neq 1$. else abelian

Suppose $i = 2$ or 4

$y x y^{-1} = x^2$ and 

$\Rightarrow y^2 x y^{-2} = x^4$

$\therefore$ $i = 2, 4$ corresponds to the same ~~set~~ grp

$\therefore H \cong \langle x, y \mid x^7 = y^3 = 1, \; y x y^{-1} = x^2 \rangle$

Now we show $H \cong G$

$\phi : H \to G$

$x \longmapsto \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $y \longmapsto \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$

$x^7 = 1$ ✓

$y^3 = 1$ ✓

$yx = x^4 y$ ✓

$\therefore H \cong G$

11) Show that the subgroup $U = \left\{ \begin{bmatrix} 1 & * & & \\ & 1 & \ddots & \\ & & \ddots & * \\ 0 & & & 1 \end{bmatrix}, * \in F_p \right\}$ is a Sylow p subgroup of $GL_n(F_p)$

Ans $|GL_n(F_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$

$|U| = p^{n-1+n-2+\cdots+1} = p^{\binom{n}{2}}$

we need to find the maximum power of p that divides $(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$

This is $p^{1+2+\cdots+n-1} \cdot p^{\binom{n}{2}}$

$\therefore$ we are done ✓

b) Show that $N_p = p+1$ in $GL_2(\mathbb{F}_p)$. Exhibit 2 distinct Sylow p subgroups

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

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

$N_p \mid (p-1)^2(p+1)$

$N_p \equiv 1 \pmod p$

$\therefore N_p = pk+1$ for some k

A sylow p subgroup has size p^1

$\therefore \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has order p & generates a sylow p subgp

By Sylow's II theorem, any two sylow p subgroups are conjugate and hence any matrix of order p is conjugate to some power of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

we compute $N_G(P)$ so that $N_p = \frac{|G|}{|N_G(P)|}$

If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in N_G(P)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ conjugates $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ to some power of $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} ad-bc-ac & a^2 \\ -c^2 & ad-bc-ac \end{pmatrix}$$

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

$\Rightarrow c = 0$, $ad \neq 0$

$\therefore |N_G(P)| = \underset{a}{(p-1)}\ \underset{d}{(p-1)} \times \underset{b}{p}$

$\therefore \quad N_p = p+1$

let $x \neq 0, \quad g = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 1-x & x \\ -x & x+1 \end{bmatrix} \notin N_G(P)$$

$\therefore g N_G(P) g^{-1}$ :: another subgrp (p sylow) of $GL_2(F_p)$

13) let $H = \left\langle \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \right\rangle < GL_2(F_7)$. Show that $H \simeq C_3 \times C_3$

Ans $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 8 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore o\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = o\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = 3$

$\therefore |H| = 9$

$\therefore H \simeq C_9 \text{ or } C_3 \times C_3$

Clearly $H \simeq C_3 \times C_3$

since $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^i \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \; \forall \; i = 1, 2, 3$

[redacted]

14) Basically sylow's first theorem skipped (look into the proofs section)

~~14) p is a prime, $|G| = p^n$. Prove that G has a normal~~

15) Let $G_1 < G_2$ be groups so that there is a prime p which divides $|G_1|$, $|G_2|$. Show that $\forall$ $H_1 \overset{\text{sylow p}}{\subset} G_1$, $\exists$ sylow p subgroup H_2 of G_2 so that $H_1 = H_2 \cap G_1$. use this to provide an alternate Sylow I theorem proof

Ans Let $|H_1| = p^t$

H_1 is sylow p subgroup of G_1 & a p-subgroup of G_2 (maybe sylow, maybe not)

H_2 is sylow p subgroup of G_2

$\therefore H_1 \leq g H_2 g^{-1}$ for some $g \in G_2$

(Sylow II theorem on G_2)

Here we have $H_1 \underset{\text{sylow p}}{\subset} G_1 < G_2$

H_2 is Sylow in G_2

$\therefore H_1 \leq H_2$

Since $H_1 \leq G_1$ we might as well write $H_1 \leq H_2 \cap G_1$

Now $G_1 \cap H_2 \leq H_2 \Rightarrow G_1 \cap H_2$ is also a p-subgroup of G_1.

But among all p subgroups of G_1, H_1 has highest order $\Rightarrow G_1 \cap H_2 \leq H_1$

$\therefore H_1 = G_1 \cap H_2$

Now let G be a group with $|G| = p^r m = n$ (say)

By Cayley's theorem, $\exists$ injective $\varphi : G \to S_G \cong S_n$.

let $\sigma \in S_G \cong S_n$

let $M(\sigma)$ = matrix obtained by permuting identity matrix according to σ (permute rows)

i.e. $M(\sigma) = \begin{bmatrix} e_{\sigma(1)} \\ \vdots \\ e_{\sigma(n)} \end{bmatrix} \in GL_n(\mathbb{F}_p)$

This allows a map ψ

$$\sigma \xmapsto{\psi} M(\sigma)$$

ψ is an injective group homomorphism

$\therefore G \cong$ subgroup of $GL_n(\mathbb{F}_p)$.

$GL_n(\mathbb{F}_p)$ has a subgroup of order p^{α}

$\therefore G$ also has one

16) Prove that for $n \geq 5$, $|H \leq A_n$, $[A_n : H] \geq n$

Ans $[A_n : H] = t$ (say)

Action: $A_n \times A_n/H \to A_n/H$

$(\sigma_1, \sigma_2 H) \mapsto \sigma_1 \sigma_2 H$

corresponding hom: $\varphi : A_n \to S_t$

$\sigma \mapsto \varphi(\sigma)$

where $\varphi(\sigma)(\tau H) = \sigma\tau H$

$$\ker\varphi = \{\sigma_1 \in A_n \mid \sigma_1\sigma_2 H = \sigma_2 H \ \forall\ \sigma_2 \in A_n\}$$

$$= \{\sigma_1 \in A_n \mid \sigma_2^{-1}\sigma_1\sigma_2 \in H \ \ \forall \sigma_2 \in A_n\}$$

If $\sigma_1 \in \ker\varphi$, then $\sigma_2^{-1}\sigma_1\sigma_2 \in H \ \ \forall \sigma_2 \in A_n$

i.e. $\sigma_1 \in H$, in particular

$\therefore \ker\varphi \subseteq H \lneq A_n$.

We know A_n is simple for $n \geq 5$ and, kernel is a normal subgroup $\Rightarrow \ker\varphi = (1)$ or A_n

but $\ker\varphi \subseteq H \lneq A_n \Rightarrow \ker\varphi = (1)$

$\therefore \varphi$ is injective

$\therefore \frac{n!}{2} \leq t!$

If $t \leq n-1$, then

$n! \leq 2 \cdot t! \leq 2 \times (n-1)!$

$\Rightarrow n \leq 2$ (contradiction)

$\therefore t > n-1$

$\Rightarrow t \geq n$

17) Show that a group of order p^2q is not simple

Ans Case I : $p = q$

$|G| = p^3$.

~~$\therefore G$ has normal subgroup of order p^2~~

If G is abelian, since $\exists$ subgroups of order p, p^2, we have that these are all normal and hence G is not simple

If G is non abelian, $Z(G) \neq G$ and $|Z(G)| \neq id$ (for any G with order p^k)

$Z(G) \trianglelefteq G \Rightarrow G$ is not simple.

Case 2: $p < q$

$n_q \mid p^2$, $n_q \equiv 1 \pmod q$

$\therefore 1 + nq = 1$ or p or p^2

$1 + nq = 1 \Rightarrow n = 0 \Rightarrow n_q = 1 \Rightarrow$ sylow q subgroup is normal $\Rightarrow G$ not simple

$1 + nq = p \Rightarrow q \mid p - 1$. But $p < q$ $\longrightarrow \leftarrow$

$1 + nq = p^2 \Rightarrow q \mid p^2 - 1 \Rightarrow q \mid p + 1$. But $p + 1 \leq q$

and hence $q = p + 1$. The only primes that differ by 1 are 2, 3 $\Rightarrow p = 2, q = 3$

$\therefore |G| = 4 \times 3 = 12 \longrightarrow$ not simple

($\because n_3 \equiv 1 \pmod 3$, $n_3 \mid 4 \Rightarrow n_3 = 1$ or 4) ← normal

For $N_3 = 4$,

$N_2 \mid 3$, $N_2 = 1 \pmod 2$

$\therefore N_2 = 3$

$N_2 \Rightarrow N_3 = 4$ will give normal subgroup N_2

Since $N_3 = 4 \Rightarrow$ Sylow 3 subgrp have 8 elements of order 3. Remaining 4 elements form subgrp of order 4 & hence normal (Sylow 2 subgrp $\Rightarrow$ normal)

(∵ 4 Sylow 3 subgrps $\Rightarrow$ 2+2+2+2 elements of order 3)

(also remaining 4 elements form subgrp of order 4 since by Sylow, grp of order 4 exists)

Case 3: $p > q$

$N_p = 1 + np \mid q$

$\therefore 1 + np = 1$ or q

$1 + np = q \Rightarrow p \mid q - 1$ but $q < p$

$\rightarrow \leftarrow$

$\Rightarrow 1 + np = 1 \Rightarrow N_p = 1 \Rightarrow G$ is not simple

18) Show that groups of order pq are not simple

Ans $p = q \Rightarrow |G| = p^2 \Rightarrow$ not simple (see prev Q)

$p < q$ (WLOG) $\Rightarrow N_q = 1 + nq \mid p$.

$p < q \Rightarrow n = 0 \Rightarrow N_q = 1$ $\Rightarrow$ normal $\Rightarrow$ not simple

19) Groups of order 30 all not simple. Prove it.

Ans $N_3 = 1 + 3t \mid 10 \Rightarrow N_3 = 1 \text{ or } 10$

$N_5 = 1 + 5t \mid 6 \Rightarrow N_5 = 1 \text{ or } 6$

If any of N_3 or $N_5 = 1$ we are done.

Suppose not. Then we have 10 cyclic groups of order 3, 6 cyclic groups of order 5

10 cyclic subgrps of order 3 $\Rightarrow$ at least 10×2 elements

6 cyclic subgrps of order 5 $\Rightarrow$ at least 6×4 elements

Contradiction since $30 < 44$

20) $|G| = pq$, $p < q$, $p \nmid q-1$. Show G is cyclic

Ans ~~$N_q = 1 + tq \mid p$~~ $N_p = 1 + np \mid q$

~~$1 + np = p$~~ ~~is not possible~~ else

$1 + np = 1$ or q

$1 + np = q \Rightarrow p \mid q-1 \rightarrow \leftarrow$

$\therefore N_p = 1 \Rightarrow$ Sylow p subgrp is normal & cyclic

$N_q = 1 + nq \mid p$

$\Rightarrow q \mid p-1$ but $q > p \Rightarrow \rightarrow \leftarrow$

$\therefore N_q = 1 \Leftrightarrow$ Sylow q subgrp is normal & cyclic

$P \cap Q = (1)$ & P & Q are cyclic of order p, q

$\therefore G \cong C_p \times C_q \cong C_{pq}$

TUTORIAL 11

1) Find the number of elements of order 2 and number of subgroups of index 2 in $Z_{60} \times Z_{45} \times Z_{12} \times Z_{36}$

Ans Let (a, b, c, d) have order 2

Then $\text{lcm}(o(a), o(b), o(c), o(d)) = 2$

$\therefore$ At least one of a, b, c, d has order 2

and rest may have order 1 or 2

Z_{45} doesnt have an element of order 2

$\therefore$ the total no. of choices is 8 but all cannot have order 1 and hence answer is 7

2) Let G be an abelian group of order n that has a unique subgroup of order d for every divisor d of n. Prove that G is cyclic

Ans Let $n = \prod_{i=1}^{R} p_i^{n_i}$

If H_i denotes the Sylow p_i subgroup, then

$G_n \simeq H_1 \times H_2 \times \cdots \times H_R$

we prove that each H_i is cyclic

Let M be a group of order p^m for some prime p

Let $g \in M$ have maximum order, say, k

Let h be any element of M. $o(h) = l$

$\langle g \rangle$ is cyclic $\Rightarrow$ it has a unique subgroup of order p^l since $p^l \mid p^k$

But $|\langle h \rangle| = p^l$

$\therefore \langle h \rangle \subseteq \langle g \rangle \Rightarrow h \in \langle g \rangle$

h is arbitrary $\Rightarrow G \in \langle g \rangle \subseteq G \Rightarrow G = \langle g \rangle$

and $k = m$

$\therefore H_i$ is cyclic and we are done

Note: we never cared about G being abelian !

3) Prove that an abelian group of order 2^n $(n \neq 1)$ must have an odd number of elements of order 2

Ans $|G| = 2^n$

$G \cong C_1 \times \cdots \times C_r$

where $|C_i| = 2^{n_i} \geq 2$

But each C_i has some element of order 2

$\therefore$ Total choices $= 2^r - 1$ (all cant be identity)

Lemma used : Group of even order has odd no. of order 2 elements

$g^2 = e \iff g = g^{-1}$

$G = \{id\} \cup \{g \in G \mid o(g) = 2\} \cup \{g \in G \mid o(g) > 2\}$

The last set has even no. of elements and G has even no of elements. Hence middle set has odd cardina

4) Let $G = \{1, 4, 11, 14, 16, 19, 26, 29, 31, 34, 41, 44\}$ be a multiplicative group under Modulo 45. Write G as a direct product of cyclic groups

Ans

	1	4	11	14	16	19	26	29	31	34	41	44
x	6	6	6	3	2	3	6	3	6	6	2	

G is not cyclic and hence is not $C_3 \times C_4$

and hence, G must be $C_3 \times C_2 \times C_2$

5) If a, b are relatively prime, then the AP $an+b$ has infinitely many primes. Using this, prove that every abelian group (finite) is isomorphic to a subgroup of $U(n)$ for some n

Ans We prove it by induction

If $G = Z_{p^m} \times Z_{q^n}$ for primes p & q,

then $p_1 = sp^m + 1$ for some s (p_1 = prime)

$p_2 = tq^n + 1$ for some t (p_2 = prime)

and $p_1 \neq p_2$ (there are ∞ primes)

$|U(p_1)| = sp^m$, $|U(p_2)| = tq^n$

$\therefore Z_{p^m} \simeq$ subgroup of $U(p_1)$

$Z_{q^n} \simeq$ subgroup of $U(p_2)$

$\therefore G \hookrightarrow U(p_1) \times U(p_2) \cong U(p_1 p_2)$

$(\because p_1 \neq p_2)$

The induction now follows.

6) Let G be an abelian group of order 16 and let it have an element of order 8 and 2 elements of order 2. Find the isomorphism class of G

Ans It could be C_{16}, $C_8 \times C_2$, $C_4 \times C_2 \times C_2$, $C_4 \times C_4$, $C_2 \times C_2 \times C_2 \times C_2$

Not C_{16} since 2 elements of order 2

Not $\begin{cases} C_2 \times C_2 \times C_2 \times C_2 \\ C_4 \times C_4 \\ C_4 \times C_2 \times C_2 \end{cases}$ since element of order 8

$\therefore$ It is $C_8 \times C_2$

7) Characterise n for which G_n (abelian) is cyclic

Ans Let $n = p_1 p_2 \cdots p_r$ (distinct primes). Then $G_n \cong C_{p_1} \times \cdots \times C_{p_r}$ which is cyclic

However if we have a factor of p^2, then the group may have $C_p \times C_p$ which is not cyclic

8) Show that there all 2 abelian groups of order 108 that have 4 subgroups of order 3

Ans $108 = 3^3 \times 2^2$

no. of elements of order 3 in $C_{27} = 2$ (18 and 9)

no of elements of order 3 in $C_3 \times C_3 \times C_3 = 3^3 - 1 = 26$

no of elements of order 3 in $C_9 \times C_3$

$= 1 \times 2 + 2 \times 1 + 2 \times 2 = 8$

(3 elements of order 3 in both C_9 & C_3 including id)

8 elements of order 3 $\Rightarrow$ 4 subgroups of order 3

(will pair up & occur)

(in general, n elements of order p $\Rightarrow$ $\frac{n}{p-1}$ subgroups of order p)

9) classify abelian groups of order 360

Ans $360 = 2^3 \cdot 3^2 \cdot 5$

$C_8 \times C_9 \times C_5$

$C_8 \times C_3 \times C_3 \times C_5$

$C_4 \times C_2 \times C_9 \times C_5$

$C_4 \times C_2 \times C_3 \times C_3 \times C_5$

$C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$

$C_2 \times C_2 \times C_2 \times C_9 \times C_5$

10) Prove that every finite abelian group is isomorphic to a direct product of cyclic groups of order $n_1, \cdots, n_t$ where $n_i \mid n_{i+1}$ $\forall\ i = 1, 2, \cdots, t-1$

Ans Let $G = \prod_{i=1}^{s} H_i$ where each H_i has order $p_i^{n_i}$

Let $H_i \cong C_{p_i^{n_{i1}}} \times C_{p_i^{n_{i2}}} \times \cdots \times C_{p_i^{n_{ir}}}$

where $n_{i1} + n_{i2} + \cdots + n_{ir} = n_i$

(r may be fixed for each i by letting n_{ik}'s to be 0) 1)

Assume WLOG $n_{11} \le n_{12} \le \cdots \le n_{1r}$

$n_{21} \le n_{22} \le \cdots \le n_{2r}$ 2)

$\vdots$

$n_{s1} \le n_{s2} \le \cdots \le n_{sr}$

Let $N_k = \prod_{j=1}^{s} p_j^{n_{jk}}$

Then $N_1 \mid N_2 \mid N_3 \mid N_4 \mid \cdots \mid N_r$ 2

and we are done since $G \cong C_{N_1} \times \cdots \times C_{N_r}$

11) Let $G \cong \langle x_1 \rangle \times \cdots \times \langle x_n \rangle$ be a finite abelian p-group. Consider $\varphi : G \to G$ as $\varphi(g) = g^p$

(a) Show that φ is a homomorphism

(b) Find $\text{Im}\,\varphi$ and $\ker \varphi$ in terms of $x_1, \ldots, x_n$

(c) Show $\ker \varphi$ and $G/\text{Im}\,\varphi$ are direct products of n cyclic groups of order p.

Ans (a) $\varphi(gh) = (gh)^p = g^p h^p = \varphi(g)\varphi(h)$ (abelian)

(b) $\text{Im}\,\varphi = \{ (x_1^{m_1 p}, x_2^{m_2 p}, \ldots, x_n^{m_n p}) \}$

$\ker \varphi = \{ x \in G \mid x^p = 1 \}$

Let $|x_i| = p^{t_i}$

$x \neq 1, x^p = 1 \iff x = (a_1, \ldots, a_n)$ where at least one a_i has order p.

$|a_i| = p \iff a_i = x_i^{p^{t_i - 1}}$

$\therefore \ker \varphi \cong C_p \times C_p \times \cdots \times C_p$ (n times)

Note: $o(x_i^p) = p^{t_i - 1}$

Also, $\text{Im}\,\varphi \cong C_{p^{t_1 - 1}} \times \cdots \times C_{p^{t_n - 1}}$

(c) $\therefore \dfrac{G}{\text{Im}\,\varphi} \cong \dfrac{C_{p^{t_1}}}{C_{p^{t_1 - 1}}} \times \cdots \times \dfrac{C_{p^{t_n}}}{C_{p^{t_n - 1}}} \cong C_p \times C_p \times \cdots \times C_p$

TUTORIAL 12

1) Show that the sum of a unit & a nilpotent element is also a unit in a ring R

Ans Let u be the unit in $R \Rightarrow ub = 1$

and a be nilpotent with $a^n = 0$

We assume rings to be comm unless stated otherwise

Then $(u+a)^{-1} = u^{-1}(1+u^{-1}a)^{-1}$

$= u^{-1}\left(1 - u^{-1}a + u^{-2}a^2 - u^{-3}a^3 + \cdots + (-1)^{n-1} a^{n-1} u^{-(n-1)}\right)$

(can check by multiplying out since we have a finite sum times finite sum)

$\therefore (u+a)^{-1} = u^{-1}(1 - au^{-1} + a^2u^{-2} - \cdots + (-1)^{n-1} a^{n-1} u^{1-n})$

2) Prove the following for a ring R

(i) $0 \cdot x = 0$

(ii) $(-x) \cdot y = -xy$

(iii) $(-x)(-y) = xy$

(iv) $1 = 0 \Rightarrow R = \{0\}$

(v) If 'a' has both left & right inv, they are equal

Ans (i) $0 + 0 = 0$

$x \cdot 0 + x \cdot 0 = x \cdot 0$

$\therefore x \cdot 0 = 0$

(ii) $xy + (-x) \cdot y$

$= (x + (-x)) \cdot y$

$= 0 \cdot y$

$= 0$

$\therefore -xy = (-x) \cdot y$

(iii) $(-x)(-y) = -x(-y)$

$x(-y) + xy = x \cdot (-y + y) = 0$

$\therefore xy = -x(-y) = (-x)(-y)$

(iv) $8 = 1 \cdot x = 0 \cdot x = 0 \Rightarrow R = \{0\}$

(v) $ba = ac = 1$

$b = b \cdot 1 = b \cdot (ac) = (ba) \cdot c = 1 \cdot c = c$

$\therefore b = c$

3) Show that commutativity of addition is redundant

Ans It can be derived from distributivity. If the multiplicative identity exists

$(-1)\cdot x = -x$ (since $x + (-1)\cdot x = 0$)

$\therefore (-1)(a+b)$

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

$= -a - b$

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

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

$= a + 0 - a$

$= a - a$

$= 0$

$\therefore a + b = b + a$

4) If $x^2 = x \quad \forall x \in R$ then show that R is comm

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

$\therefore x^2 + 2x + 1 = x + 1$

$\therefore x^2 + x = 0$

$\therefore 2x = 0$

$\therefore x = -x$

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

$= x^2 + xy + yx + y^2$

$= x + xy + yx + y$

$\therefore xy + yx = 0 \Rightarrow xy = -yx = yx$

5) Let E be the set of all integer sequences & let S be collection of all functions $f: E \to E$ such that $f(a+b) = f(a) + f(b)$. Prove that the element $T \in S$ defined as $T(a_1, a_2, \ldots) = (0, a_1, a_2, \ldots)$ has a left inverse but no right inverse wrt composition of functions

Ans The left inverse of T is $G \in S$ which is such that $G(a_1, a_2, \ldots) = (a_2, a_3, a_4, \ldots)$

So that $G \circ T (a_1, a_2, \ldots)$

$= G(0, a_1, a_2, \ldots)$

$= (a_1, a_2, \ldots)$

Suppose T has a right inverse H, Then

$T \circ H = Id$

But T is not surjective

$\therefore T \circ H (1, 0, 0, 0, 0, \ldots) = Id(1, 0, 0, \ldots)$

$= (1, 0, 0, \ldots)$

But $(1, 0, 0, \ldots) \notin$ Range (T)

6) Let R be ring of continuous real valued functions on $[0, 1]$. Find units of R. Prove that functions with only finite number of zeroes are not zero divisors

Ans Suppose f is a unit, Then $\exists\, g \in R$ s.t.

$fg = gf = id$

$\therefore g(x) = \frac{1}{f(x)}$ $\quad \forall\ x \in [0,1]$

$\therefore$ If $f(x) \neq 0 \ \forall\ x \in [0,1]$, f is a unit since such a $g \in R$ exists.

Suppose f is non zero at $x_1, x_2, \ldots, x_n$

Then suppose $f(x)g(x) = 0 \quad \forall\ x \in [0,1]$

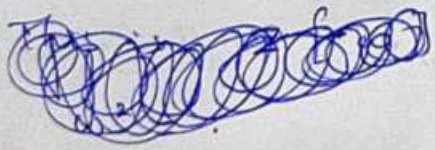
Thus, $g(x) = 0 \quad \forall\ x \in [0,1] \setminus \{x_1, x_2, \ldots, x_n\}$

$\therefore g(x) = 0$ a.e.

$\Rightarrow g(x) = 0 \quad \forall\ x \in [0,1]$ since g is continuous

$\therefore f$ is not a zero divisor

7) Find units of $\mathbb{Z}\left[\frac{(1+\sqrt{-3})}{2}\right]$

Ans 

Defining $N(a+b\omega) = a^2+b^2+ab$

we see that units correspond to unit modulus norm

$\therefore a^2+ab+b^2 = \pm 1 \Rightarrow$

$a=0,\ b=\pm 1$

$b=0,\ a=\pm 1$

$a=1,\ b=-1$

$a=-1,\ b=1$

$\left.\begin{matrix} \pm 1 \\ \pm \omega \\ \pm \omega^2 \end{matrix}\right\}$

8) Find infinitely many units in $\mathbb{Z}[\sqrt{2}]$

Ans Define $N(a+b\sqrt{2}) = a^2 - 2b^2$

We see that if $a+b\sqrt{2}$ is a unit,

$N(a+b\sqrt{2}) = \pm 1$ & vice versa

$a^2 - 2b^2 = \pm 1$ has infinitely many solutions

9) Show that for an integral domain R, $R[x] = R[g(x)]$ for some $g(x) \in R[x]$ iff $g(x) = ax+b$ for a unit $a \in R$

Ans

let $\deg(g(x)) = d$ and $R[g(x)] = R[x]$

let $x = a_0 + a_1 g(x) + a_2 g^2(x) + \dots$

$x - a_0 = g(x)(a_1 + a_2 g(x) + \dots)$

R is a domain $\Rightarrow \deg(m(x)\,n(x))$

$= \deg(m(x)) + \deg(n(x))$

$\therefore 1 = \deg(g(x)) + \deg(a_1 + a_2 g(x) + \dots)$

$1 - \deg(g(x)) = 0$ or 1

$\deg(g(x)) \neq 0$ else $x - a_0 = k$

$\Rightarrow d = 1$

$\Rightarrow g(x) = ax + b$

$x = a_0 + a_1(ax+b) + \cdots + a_n(ax+b)^n$

$a_n a^n = 0 \Rightarrow a_n = 0 \quad (\because a \neq 0 \Leftrightarrow a^n \neq 0)$

$\therefore a_n$ has to be 0 for $n \geq 2$

$\therefore x = a_0 + a_1(ax+b)$

$\therefore a_1 a = 1, \; a_0 + a_1 b = 0$

$\therefore a$ is a unit

$\therefore x \in R[g(x)]$

$\therefore R[x] \subset R[g(x)] \subset R[x] \Rightarrow R[x] = R[g(x)]$

10) Prove that $f(x) \in R[[x]]$ is a unit iff $f(0)$ is a unit in R

Ans $f(x) = \sum_{i=0}^{\infty} a_i x^i$ is a unit

$g(x) = \sum_{i=0}^{\infty} b_i x^i$ is its inverse

$f(x)g(x) = 1 \Rightarrow a_0 b_0 = 1 \Rightarrow a_0$ is a unit.

Conversely let a_0 be a unit.

$\therefore b_0 a_0 = 1 \Rightarrow b_0 = a^{-1}$

Inductively we can construct g and be done.

11) Show that for fixed non zero a, b in a ring, the equation $ax = b$ can have more than one solution

Ans Consider $3x = 6$ in $\mathbb{Z}_{12}$

$x = 2$ and $x = 6$ are both solutions

However if a is a unit, then there is a unique solution

12) Give example of non-comm ring with 16 elements

Ans Quaternions over $\mathbb{Z}_2$

(They are represented by matrices & clearly not commutative)

13) Find units in $M_2(\mathbb{Z})$

Ans $A^{-1} = \frac{1}{\det(A)} \operatorname{adj}(A)$

$A^{-1} \in M_2(\mathbb{Z})$ iff $\det(A) = \pm 1$

$\therefore A$ is a unit iff $\det(A) = \pm 1$

14) Find units in $\mathbb{Z}[x]$

Ans $f(x)g(x) = 1 \Rightarrow \deg f + \deg g = 0 \Rightarrow \deg f = \deg g = 0$

$\therefore \pm 1$ are the only units

15) Show that $U\left(\bigoplus_{i=1}^{n} R_i\right) = \bigoplus_{i=1}^{n} U(R_i)$ for rings $R_1, \ldots, R_n$ (comm with id)

Ans Let $(x_1, \ldots, x_n) \in U\left(\bigoplus_{i=1}^{n} R_i\right) = R$ (say)

$\therefore \exists (y_1, y_2, \ldots, y_n) \in R$ s.t.

$(x_1 y_1, \ldots, x_n y_n) = (1, 1, \ldots, 1)$

$\therefore x_i \in U(R_i) \quad \forall i$

$\therefore R \subseteq \bigoplus_{i=1}^{n} U(R_i)$

Conversely other direction (very easy)

$\therefore R = \bigoplus_{i=1}^{n} U(R_i)$

16) Find all idempotents ($a^2 = a$) in an integral domain

Ans $a^2 = a$

$\Rightarrow a(a-1) = 0$

$\Rightarrow a = 0$ or $a - 1 = 0$

$\Rightarrow 0$ or 1

17) Show that $\mathbb{Z}_3[i]$ is a field with 9 elements

Ans It clearly has 9 elements. It is already a ring.

$(a+bi)(c+di) = (c+di)(a+bi)$

$\Rightarrow$ commutative & identity also exists

$(a+bi)(c+di) = 1$

$\Rightarrow \quad ac - bd = 1$

$ad + bc = 0$

b, d exist and hence inverse exists

18) Find zero divisors and idempotent elements. Find group of units of R. $R = \mathbb{Z}_5[i]$

Ans $(a+bi)(c+di) = 0$ and $a+bi \neq 0$

$\therefore ac = bd, \quad bc = -ad$

If $b = 0$, $ac = 0 \Rightarrow c = 0, d = 0$

If $b \neq 0$, b^{-1} exists

$\therefore b^{-1}(a+bi)(c+di) = 0$

$\therefore$ WLOG assume $b = 1$

$c = -ad$

$ac = d \Rightarrow ac = -a^2 d = d$

Q16)(contd.) we wanted to find non zero zero divisors of $R = \mathbb{Z}_5[i]$ and also idempotent elements

$(a+bi)(c+di) = 0$ and $a+bi \neq 0$ is fixed.

we want to find values of non zero $c+di$

If $b=0$, then $c=d=0$

If $b \neq 0$, we can assume WLOG $b=1$

$\therefore c = -ad$, $ac = d$

$\therefore ac = -a^2d = d$

$d \neq 0 \rightarrow a^2 = -1 \Rightarrow a = 2, 3$

$\therefore (2+i)$, $(3+i)$ are zero divisors and hence any non zero multiple of these are also included

Now we find idempotents

$(a+bi)^2 = a+bi$

$\therefore a^2 - b^2 = a$, $2ab = b$

$b=0 \Rightarrow a^2 = a \Rightarrow a = 0$ or 1

$b \neq 0 \Rightarrow 2a = 1 \Rightarrow a = 3$

$\therefore 3^2 - b^2 = 3 \Rightarrow b^2 = 1 \Rightarrow b = \pm 1$

Now we find units in $\mathbb{Z}_5[i]$

Define norm $N(a+bi) = a^2 + b^2$

~~Units correspond one-one with $N(a+bi)=1$~~

$N(x)N(y) = N(xy) \quad \forall\, x, y \in R$

If $(a+bi)$ is a unit,

$N(a+bi)\,N(c+di) = 1$

$\Rightarrow a^2+b^2 \neq 0$

$\Rightarrow (a+ib)(a-ib) \neq 0$

$\Rightarrow (a+ib)\left((a^2+b^2)^{-1}(a-ib)\right) = 1$

$\therefore a+ib$ is invertible $\forall\, a, b$ except $a=0=b$

19) Let $R = \{ f : \mathbb{R} \to \mathbb{R} \mid f \text{ is a function} \}$ under addition and multiplication of functions. Find non zero zero divisors and nilpotents. Prove that every element is either a zero divisor or a unit

Ans $f^n = 0 \Rightarrow f(x)^n = 0 \ \forall x \Rightarrow f(x) = 0 \ \forall x$

$\therefore 0$ is the only nilpotent

Suppose f is not a unit. Then $\exists\, x_0 \in R$ such that $f(x_0) = 0$ (if there is no such x_0, then f is a unit since $g = \frac{1}{f}$ is its inverse)

Defining g as $g(x_0) = 1$ and $g(x) = 0$ everywhere else, we see that $fg = 0$

20) Find isomorphism class of abelian group of non zero elements of $\mathbb{Z}_3[i]$

Ans $G = \mathbb{Z}_3[i] \setminus \{0\}$

$|G| = 8$

Consider $1+i \in G$

$o((1+i)) = 8$ i.e. $(1+i)^8 = 1 \Rightarrow G \simeq C_8$

21) Characteristic p prime for which $\mathbb{Z}_p[i]$ is a field

Ans If $p = 2$,

$\mathbb{Z}_2[i]$ is not a field since

$(1+i)(1-i) = 1+1 = 2 = 0$

If $p = 4n+1$,

$p = a^2 + b^2$ for some $a, b < p$ (Fermat's theorem)

$\therefore (a+bi)(a-bi) = a^2+b^2 = p = 0$

$\therefore a+bi$ is a zero divisor $\Rightarrow$ no inverse $\Rightarrow$ not field

If $p = 4n+3$,

$x+iy$ is a unit iff $N(x+iy) = x^2+y^2 = \pm 1$

$y = 0 \Rightarrow x$ is a unit

$y \neq 0 \Rightarrow y$ is a unit in $\mathbb{Z}_p \Rightarrow y^{-1}(x+iy)$

$= y^{-1}x + i$ is a unit

$x=0 \Rightarrow iy$ is a unit

Suppose $x, y \neq 0$

Then WLOG we prove $x+i$ is a unit for all $x \neq 0$, $N(x+i) = \pm 1 \Rightarrow x^2+1 = \pm 1$

As $x \neq 0$, $x^2+1 = -1 \Rightarrow x^2 = -2 = p-2$

$\therefore$ If is a field iff $x^2 = -2 \pmod p$ has a solution

22) Show that any finite field has p^n elements where p is a prime, $n \geq 1$

Any Let $|F| = rs$ where $\gcd(r,s) = 1$

Then F is a finite abelian group under addition

$\Rightarrow F \cong F(r) \oplus F(s)$ where

$F(r) = \{x \in F \mid rx = 0\}$

Any Let 1 have order p wrt $+$ ie. characteristic of f is p. Then p divides $|F|$ since $(F, +)$ is an abelian group. Let q be any other prime dividing $|F|$. Then since F is abelian wrt addition, $\exists\ x \in (F, +)$ with order q $\Rightarrow q \cdot x = 0$. But $p \cdot x = 0$. Since $(p, q) = 1$,

$ap + bq = 1$ for some $a, b \in \mathbb{Z}$

$\therefore (ap + bq) \cdot x = x$

But $(ap + bq) \cdot x = 0$

$\therefore x = 0$

Contradiction since $o(x) \geq 2$ in $(F, +)$

$\therefore q$ doesn't exist

$\therefore |F| = p^n$

23) Show that $F_4 = \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in F_2 \right\}$ has 4 elements and is a field

Ans If clearly has 4 elements

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Clearly closed wrt addition.

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore F_4^{\times} = \{ I, A, A^2 \}$ & is hence an abelian group under multiplication

Thus, F_4 is a field which has 4 elements

over $\mathbb{C}$

24) Show that ring of quaternions isn't a division ring

Ans $R = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{C} \}$

and $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$

$(1 + \sqrt{-1}\, i)(1 - \sqrt{-1}\, i)$

$= 1 - (-1) i^2 = 0$

$\therefore 1 + \sqrt{-1}\, i$ is not invertible

$\therefore$ Not a division ring

25) Show that ring of quaternions over a field F is a division ring iff the only solutions of $x^2 + y^2 + z^2 + w^2 = 0$ are $x = y = z = w = 0$

Ans $a = x + iy + jz + kw$

$\bar{a} = x - iy - jz - kw$

$a\bar{a} = x^2 + y^2 + z^2 + w^2 = N(a)$

Suppose the only solution of $N(a) = 0$ is the trivial solution, then, if $a \neq 0$,

$N(a) \neq 0 \Rightarrow a^{-1} = \frac{\bar{a}}{N(a)}$ exists

Conversely if (4) is a division ring.

a^{-1} exists

$a\,a^{-1} = 1$

$\therefore N(a)\,N(a^{-1}) = 1$

$\because N(a) = 0$ iff $a = 0$

TUTORIAL 13

1) Prove that I is maximal iff R/I is a field

Ans Let R/I be a field.

Let $I \subsetneq J \subseteq R$. We prove $J = R$

Let $a \in J$ such that $a \notin I$

Then $\bar{a} = a + I$ is not zero element of R/I

$\therefore \exists\ \bar{b}$ s.t. $\bar{a}\bar{b} = \bar{1}$

i.e. $(a+I)(b+I) = 1+I \Rightarrow ab-1 \in I$

$\therefore ab - 1 \in J$

But $a \in J \Rightarrow ab \in J \Rightarrow 1 \in J$

$\therefore J = R$

Let I be maximal.

We want to show that $\forall\ a + I$ (non zero in R/I),

$\exists\ b + I$ s.t. $ab - 1 \in I$

but $a \notin I$

$\therefore$ Given $a \in R$, we want to show existence of $b \in R$ s.t. $ab - 1 \in I$

Let $M' = \{ ar + s \mid r \in R, s \in I \}$

Then $I \subseteq M'$

But $I \subsetneq M'$ since $a \in I$, $a \in M'$

$\therefore M' = R \Rightarrow 1 \in M'$

$\therefore ar_0 + s_0 = 1 \Rightarrow ar_0' - 1 \in I$ for some r_0' in R and this is our b

2) Let $R = \{ f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ is a function} \}$. Let I be those functions for which $f(0)$ is even. Prove that I is an ideal of R. Is it a subring

Ans Let $g \in R$, $h \in I$

Then $g \cdot h(0) = g(0)\, h(0)$ is even and hence I is indeed an ideal

$I \not\ni id_m$ (the multiplicative identity $f(n) = 1 \; \forall n$) and hence is not a subring

3) Prove that every non zero ideal in $\mathbb{Z}[i]$ contains a non zero integer.

Ans Let $a+bi \in I$ be a non zero element

$(a+bi)(a-bi) = a^2+b^2 \in I$ and is an integer

4) Describe the kernels of

(i) $\phi : \mathbb{R}[x] \to \mathbb{C}$ $\quad \phi(f(x)) = f(2+i)$

(ii) $\phi : \mathbb{C}[x,y,z] \to \mathbb{C}[t]$ $\quad \phi(x) = t$, $\phi(y) = t^2$, $\phi(z) = t^3$ and $\phi(a) = a \ \forall\, a \in \mathbb{C}$, ϕ is linear

(iii) $\phi : \mathbb{C}[x,y] \to \mathbb{C}[t]$ as $\phi(x) = t^3$, $\phi(y) = t^5$, $\phi(a) = a \quad \forall\, a \in \mathbb{C}$

Ans (i) $f(2+i) = 0$

$\Rightarrow f(x) = (x^2-4x+5)g(x)$ for $g(x) \in \mathbb{R}[x]$

since if $f(x) \in \ker \varphi$,

$f(x) = q(x)\cdot(x^2-4x+5) + r(x)$

where $\deg(r) \leq 1 \Rightarrow r(x) = ax+b$

$f(2+i) = 0 = 0 + r(2+i) = a(2+i)+b = 0$

$\therefore a = b = 0 \quad (a, b \in \mathbb{R})$

(ii) $\phi(f(x,y,z)) = f(t, t^2, t^3) = 0$

Claim: $\ker = (x^2-y, x^3-z)$

Divide f with x^2-y to get

$f(x,y,z) = q(x,y,z)(x^2-y) + g(x,z)$

further divide g by $x^3 - z$ to get

$g(x,z) = q'(x,z)(x^3-z) + h(x)$

$g(t,t^3) = 0 \Rightarrow h(t) = 0$

$\therefore h(x) = 0$

$\therefore f = q_{xyz}(x^2-y) + q'_{xz}(x^3-z)$

(iii) claim:

$\ker = (x^5 - y^3)$

Divide f by $y^3 - x^5$ in $(\mathbb{C}[x])[y]$

$\therefore f(x,y) = q(x,y)(y^3-x^5) + a(x)y^2 + b(x)y + c(x)$

$\therefore 0 = a(t^3)t^{10} + b(t^3)t^5 + c(t^3)$

This holds for all t and hence,

$a = b = c = 0$ throughout

$\Rightarrow \ker = (x^5 - y^3)$

5) Find automorphisms of $\mathbb{Z}[x]$

Ans Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ be an automorphism.

Then $\mathbb{Z}[\varphi(x)] = \mathbb{Z}[x]$

$\therefore \varphi(x) = ax + b$ for a unit a i.e. $a = \pm 1$

$\therefore \varphi\left(\sum_{n=1}^{k} a_n x^n\right) = \sum_{n=1}^{k} a_n (ax+b)^n$

Another way to reach here :

$\deg(\phi(x)) = d$ (say)

Then for non zero $f \in \mathbb{Z}[x]$,

$\deg(\phi(f(x))) \geq d$

But $\exists f$ s.t. $\phi(f) = x$ (surjective)

$\therefore d = 1$ or 0 ($d \neq 0$ clearly)

$\therefore \phi(x)$ is linear $ax + b$

6) Let $f(y) \in R[y]$. Define $\phi : R[x,y] \to R[x,y]$ as $\phi(x) = x + f(y)$, $\phi(y) = y$, $\phi(a) = a$ $\forall a \in R$. Prove that ϕ is an automorphism

Any ϕ is a substitution map and hence a homomorphism

If $\varphi : R[x,y] \to R[x,y]$ as $\varphi(x) = x - f(y)$, $\varphi(y) = y$, $\varphi(a) = a$ $\forall a \in R$, then φ and ϕ are inverses and hence both are automorphisms

7) Show that nilpotent elements form an ideal. This ideal is denoted $nil(R)$. Find $nil(R)$ for R being $\mathbb{Z}_{12}$, $R[x]$

Ans Let $a \in nil(R)$ be a nilpotent element of order α. Let $b \in R$

$(ab)^\alpha = a^\alpha b^\alpha = 0 \Rightarrow ab \in nil(R)$

Let $f \in R[x]$ / $f = a_0 + a_1 x + \cdots + a_n x^n$

f is nilpotent

$\Leftrightarrow f^m = 0$ for some m

$\Leftrightarrow a_0^m = 0$ for some m

$\Leftrightarrow f - a_0$ is nilpotent

$\Leftrightarrow a_1$ is nilpotent

$\Leftrightarrow a_i$ is nilpotent $\forall i = 0, 1, \ldots n$

$\therefore nil(R[x]) = (nil R)[x]$

Now we find $nil(\mathbb{Z}_{12}) = nil(\mathbb{Z}/12\mathbb{Z})$

We prove that:

$nil(R/I) \simeq \sqrt{I}/I$ where $\sqrt{I}$ denotes the radical ideal $\{x \in R \mid x^n \in I$ for some $n \in \mathbb{Z}^+\}$

$\bar{x} \in nil(R/I)$

$\Leftrightarrow \bar{x}^n = \bar{0}$ for some n (definition)

$\Leftrightarrow x^n \in I$ for some n ($\bar{x} = x + I$, $\bar{x}^n = x^n + I$)

$\Leftrightarrow x \in \sqrt{I}$

$\Leftrightarrow \bar{x} \in \sqrt{I}/I$

$\therefore nil(\mathbb{Z}/12\mathbb{Z}) = \sqrt{12\mathbb{Z}}/12\mathbb{Z} \cong 6\mathbb{Z}/12\mathbb{Z}$

Note:

$\sqrt{m\mathbb{Z}} = r\mathbb{Z}$ where r = product of all distinct primes in m

8) Prove that $nil(R/\sqrt{0}) = (0) = \{0\}$

Ans $nil(R/\sqrt{0}) = \sqrt{\sqrt{0}}/\sqrt{0} = \sqrt{0}/\sqrt{0} \cong \{0\}$

9) Prove that $R[[x]]$ is a PID

Ans Let I be a non zero proper ideal

Let $f(x) = \sum a_n x^n \in R[[x]]$ and min degree of f be d. call this order of f.

Let $m = \min\{ \text{ord } f \mid f \text{ is non zero}, f \in I \}$

We show $I = (x^m)$

Let $g(x) \in I$

$g(x) = a_n x^n + a_{n+1} x^{n+1} + \cdots$ where $n \geq m$

since m is minimum

$\therefore g(x) = x^m (a_n x^{n-m} + \ldots) = x^m h(x)$

$\therefore g(x) \in (x^m) \Rightarrow I \subseteq (x^m)$

But $x^m \in I \Rightarrow (x^m) \subseteq I$

$\therefore (x^m) = I$

10) Identify the following :

(i) $\frac{\mathbb{Z}[x]}{(x^2-3, 2x+4)}$ (ii) $\frac{\mathbb{Z}[i]}{(2+i)}$ (iii) $\frac{\mathbb{Z}[x]}{(6, 2x-1)}$

(iv) $\frac{\mathbb{Z}[x]}{(x^2+3, 5)}$ (v) $\frac{\mathbb{Z}[i]}{(2+3i)}$

Ans (i) $(x^2-3, 2x+4)$

$= (x^2-3, 2x+4, 4x+6)$

$= (x^2-3, 2, 2x+4)$

$= (x^2-1, 2)$

$\therefore \frac{\mathbb{Z}[x]}{(x^2-1, 2)} \simeq \frac{\mathbb{Z}_2[x]}{(x^2-1)}$.

(ii) $\frac{\mathbb{Z}[i]}{(2+i)} \simeq \frac{\mathbb{Z}[x]}{(x^2+1, 2+x)}$

$(x^2+1, 2+x) = (x^2+1, 2+x, 2x-1)$

$= (x^2+1, 5, 2+x)$

$\therefore \frac{\mathbb{Z}[x]}{(x^2+1, 2+x, 5)} \simeq \frac{\mathbb{Z}_5[x]}{(x^2+1, 2+x)}$

$(x^2+1, x+2) = \gcd(x+2, x^2+1) = (x+2)$

since in $\mathbb{Z}_5[x]$, $2^2+1 = 0$

$\therefore \dfrac{\mathbb{Z}_5[x]}{(x+2)} \cong \mathbb{Z}_5$

(iii) $\dfrac{\mathbb{Z}[x]}{(6, 2x-1)} \cong \dfrac{\mathbb{Z}[x]}{(6, 2x-1, 3)} \cong \dfrac{\mathbb{Z}_3[x]}{(2x-1)}$

(in $\mathbb{Z}_3$, $6 = 0$)

$\dfrac{\mathbb{Z}_3[x]}{(2x-1)} \cong \mathbb{Z}_3$ (evaluate with $x=2$)

(iv) $\dfrac{\mathbb{Z}[x]}{(x^2+3, 5)} \cong \dfrac{\mathbb{Z}_5[x]}{(x^2+3)} = F$ (say)

(x^2+3) is irreducible in $\mathbb{Z}_5[x]$ $\Rightarrow$ it is a maximal ideal $\Rightarrow$ F is a field

$f(x) \in \mathbb{Z}_5[x]$

$\Rightarrow f(x) = q(x)(x^2+3) + ax+b$ for some $q(x) \in \mathbb{Z}_5[x]$, $ax+b \in \mathbb{Z}_5[x]$

hence $\overline{f(x)} = 0 + a\bar{x} + b \cdot \bar{1}$

$\therefore$ F is a vector space with basis $\bar{x}, \bar{1}$

10) Identify the following :

(i) $\frac{\mathbb{Z}[x]}{(x^2-3, 2x+4)}$ (ii) $\frac{\mathbb{Z}[i]}{(2+i)}$ (iii) $\frac{\mathbb{Z}[x]}{(6, 2x-1)}$

(iv) $\frac{\mathbb{Z}[x]}{(x^2+3, 5)}$ (v) $\frac{\mathbb{Z}[i]}{(2+3i)}$

Ans (i) $(x^2-3, 2x+4)$

$= (x^2-3, 2x+4, 4x+6)$

$= (x^2-3, 2, 2x+4)$

$= (x^2-1, 2)$

$\therefore \frac{\mathbb{Z}[x]}{(x^2-1, 2)} \simeq \frac{\mathbb{Z}_2[x]}{(x^2-1)}$.

(ii) $\frac{\mathbb{Z}[i]}{(2+i)} \simeq \frac{\mathbb{Z}[x]}{(x^2+1, 2+x)}$

$(x^2+1, 2+x) = (x^2+1, 2+x, 2x-1)$

$= (x^2+1, 5, 2+x)$

$\therefore \frac{\mathbb{Z}[x]}{(x^2+1, 2+x, 5)} \simeq \frac{\mathbb{Z}_5[x]}{(x^2+1, 2+x)}$

$(x^2+1, x+2) = \gcd(x+2, x^2+1) = (x+2)$

since in $\mathbb{Z}_5[x]$, $2^2+1 = 0$

$\therefore \dfrac{\mathbb{Z}_5[x]}{(x+2)} \simeq \mathbb{Z}_5$

(iii) $\dfrac{\mathbb{Z}[x]}{(6, 2x-1)} \simeq \dfrac{\mathbb{Z}[x]}{(6, 2x-1, 3)} \simeq \dfrac{\mathbb{Z}_3[x]}{(2x-1)}$

(in $\mathbb{Z}_3$, $6 = 0$)

$\dfrac{\mathbb{Z}_3[x]}{(2x-1)} \simeq \mathbb{Z}_3$ (evaluate with $x=2$)

(iv) $\dfrac{\mathbb{Z}[x]}{(x^2+3, 5)} \simeq \dfrac{\mathbb{Z}_5[x]}{(x^2+3)} = F$ (say)

(x^2+3) is irreducible in $\mathbb{Z}_5[x]$ $\Rightarrow$ it is a maximal ideal $\Rightarrow$ F is a field

$f(x) \in \mathbb{Z}_5[x]$

$\Rightarrow f(x) = q(x)(x^2+3) + ax+b$ for some $q(x) \in \mathbb{Z}_5[x]$, $ax+b \in \mathbb{Z}_5[x]$

hence $f(x) = 0 + a\bar{x} + b\cdot\bar{1}$

$\therefore$ F is a vector space with basis $\bar{x}, \bar{1}$

$\therefore F \simeq \mathbb{Z}_5 \otimes \mathbb{Z}_5$ and has 25 elements

(v) $\dfrac{\mathbb{Z}[i]}{(2+3i)} = R$

Define $\phi : \mathbb{Z} \to R$ as

$$\phi(n) = \begin{cases} 1_R + 1_R + \cdots + 1_R \ (n \text{ times}) & n > 0 \\ -\phi(-n) & n < 0 \\ 0 & n = 0 \end{cases}$$

Then ϕ is a homomorphism since

$\phi(1) = \phi(id) = id = 1_R$

$\phi(m+n) = \phi(m) + \phi(n)$ $\quad \{ m, n > 0$

$\phi(m+n) = -\phi(-m-n)$ $\quad \{ m, n < 0$

$= -(\phi(-m) + \phi(-n))$

$= \phi(m) + \phi(n)$

$\phi(m+n) = \phi(m - n')$ $\quad \{ m > 0, n < 0$ (or $m < 0, n > 0$ similarly)

$= \phi(m) + \phi(-n')$

$= \phi(m) + \phi(n)$

Also, $\phi(mn) = \phi(m)\phi(n)$ $\quad \{ m, n > 0$

$\phi(mn) = -\phi(-mn)$ $\quad \{ m, n < 0$

$= -\phi(mn')$ $\quad \{ m > 0, n < 0$

$= -(\phi(m)\phi(n')) = \phi(m)\phi(n)$

∴ ϕ is a homomorphism -

We now show that $\ker \phi = 13\mathbb{Z}$

(ϕ is surjective (clearly))

$13 \in \ker \phi$ since

$\phi(13) = 13 \cdot 1_R$

$= 13 + (2+3i)$

But $13 \in (2+3i)$

∴ $\phi(13)$ is the 0 element of R

∴ $13\mathbb{Z} \subseteq \ker \phi$

Let $n \in \ker \phi$

Then $\phi(n)$ is 0 element of R

$\Rightarrow$

$\therefore n \in (2+3i)$

$\therefore n = (a+bi)(2+3i)$

$\therefore n = 2a - 3b + i(2b+3a)$

$\therefore 2b + 3a = 0 \Rightarrow 4b + 6a = 0$

$\Rightarrow 6a - 9b = -13b$

$\therefore 2n = -13b$

$\therefore 2n \in 13\mathbb{Z} \Rightarrow n \in 13\mathbb{Z}$

$\therefore \ker \phi \subseteq 13\mathbb{Z}$

11) Prove $\mathbb{Z}_2[x]/(x^2+x+1)$ is a field but $\mathbb{Z}_3[x]/(x^2+x+1)$ is not a field

Ans x^2+x+1 has no root in $\mathbb{Z}_2[x]$ but has one in $\mathbb{Z}_3[x]$

$\therefore (x^2+x+1)$ is maximal ideal of $\mathbb{Z}_2[x]$ and not of $\mathbb{Z}_3[x]$

12) Show $\mathbb{Q}[\sqrt{2}] \not\cong \mathbb{Q}[\sqrt{5}]$

Ans $\mathbb{Q}[\sqrt{2}] \simeq \frac{\mathbb{Q}[x]}{(x^2-2)}$, $\mathbb{Q}[\sqrt{5}] \simeq \frac{\mathbb{Q}[x]}{x^2-5}$

If $f: \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{5}]$ is an isomorphism, then,

$f((\sqrt{2})^2) = f(2) = 2$

(since $f(x) = x \ \forall\ x \in \mathbb{Q}$)

$\therefore (a+b\sqrt{5})^2 = 2$ not possible !

13) show $\mathbb{R} \not\cong \mathbb{C}$ (wrt ring isomorphism)

Ans $\varphi(i^2) = (\varphi(i))^2$ where $\varphi: \mathbb{C} \to \mathbb{R}$

$\therefore \varphi(-1) = (\varphi(i))^2$

$\therefore (\varphi(i))^2 = -1$ not possible for $\varphi(i) \in \mathbb{R}$

14) Find all ring homomorphisms from $\mathbb{R}$ to $\mathbb{R}$

Ans $\varphi(1) = 1$

$\therefore \varphi(n) = n \quad \forall\, n \in \mathbb{N}$

$\varphi\left(\frac{a}{b}\right) \cdot \varphi(a)\,\varphi(b^{-1}) = ab^{-1} \quad \forall\, \frac{a}{b} \in \mathbb{Q}$

$\therefore \varphi(x) = x \quad \forall \quad x \in \mathbb{Q}$

$\mathbb{Q}$ is dense in $\mathbb{R} \Rightarrow \varphi(x) = x \;\; \forall\, x \in \mathbb{R}$

Since : let $x \in \mathbb{R}$, $x < \varphi(x)$

let $q \in \mathbb{Q}$ with $x < q < \varphi(x)$

$\Rightarrow \varphi(x) \leq \varphi(q)$

$\Rightarrow \varphi(x) \leq q < \varphi(x)$

$\rightarrow \leftarrow$

(note: $\varphi(x) > 0$ for $x > 0$ was used since $\varphi(x) = \varphi(y^2) = (\varphi(y))^2$)

Hence only identity

15) Let $R = M_2(\mathbb{R})$. Show that the only ideals of R are (0), R but R is not a field

Ans clearly R is not a field due to commutativity being absent

Let $I \neq (0)$. be an ideal

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in I$ and WLOG $a \neq 0$

Then $\begin{bmatrix} a^{-1} & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & a^{-1}b \\ 0 & 0 \end{bmatrix} \in I$

$\Rightarrow \begin{bmatrix} 1 & a^{-1}b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I$

$\Rightarrow \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & a^{-1}b \end{bmatrix} \in I$

$\Rightarrow \begin{bmatrix} 0 & 0 \\ 1 & a^{-1}b \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a^{-1}b & 1 \end{bmatrix} \in I$

$\Rightarrow \begin{bmatrix} 0 & 0 \\ a^{-1}b & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \in I$

$\Rightarrow \begin{bmatrix} 1 & b \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ -+ & + \end{bmatrix} \in I \Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & + \end{bmatrix} \in I$

$\therefore I = R$

6) Prove $\dfrac{M_n(R)}{M_n(I)} \simeq M_n(R/I)$

for ring R with ideal I

Ans Define $\varphi : M_n(R) \to M_n(R/I)$ as

$$\varphi(a_{ij}) = \overline{a_{ij}} = a_{ij} + I$$

Clearly φ is surjective

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

$\varphi(AB) = \varphi(A)\varphi(B)$ (Check!)

$\varphi(I) = id$

$\therefore \varphi$ is a hom

$\ker \varphi = \{ [a_{ij}] \mid \overline{a_{ij}} = \overline{0} \} = M_n(I)$

$$\therefore \frac{M_n(R)}{M_n(I)} \cong M_n\left(\frac{R}{I}\right)$$

17) Let R be a commutative ring with id. Prove that any ideal of $M_2(R)$ is of the form $M_2(I)$ for an ideal I of R

Ans Let I be an ideal of $M_2(R)$. By prev question, all entries of some $A \in I$ are elements of an ideal J of R

$\therefore A \in M_2(J)$ and we are done

18) Show that $(3, x^3 - x^2 + 2x - 1)$ is not principal in $\mathbb{Z}[x]$

Ans $I = (3, f(x))$

Let $h(x)$ generate I

Then $3 = h(x)\, g(x)$

$\therefore h(x), g(x)$ are constants

$\therefore h(x) = \alpha \in \mathbb{Z}$ (say)

$\therefore x^3 - x^2 + 2x - 1 = \alpha\, f(x)$

$\therefore \alpha = \pm 1$ (comparing constants)

But $(1), (-1) = \mathbb{Z}[x]$ and

$(3, f(x)) \neq \mathbb{Z}[x]$ since if

$\mathbb{Z}[x] = (3, f(x))$

then $\mathbb{Z}_3[x] = (\overline{f(x)})$ which is false

since $1 \notin \overline{f(x)}$

9) Find infinitely many roots of $x^2 + 1$ in $H(\mathbb{R})$

Ans $x = a + bi + cj + dk$

$\therefore 1 + x^2 = (1 + a^2 - b^2 - c^2 - d^2)$

$+ 2ab\,i + 2ac\,j + 2ad\,k$

$\therefore 1 + a^2 = b^2 + c^2 + d^2$

$2ab = 2ac = 2ad = 0$

Let $a = 0$, we get ∞ solutions

classmate Date Page

mult wrt

20) Let F be a field & G be a finite subgroup of $F^\times$. Prove that G is cyclic

Ans G is a finite abelian group

$\therefore G \simeq C_{n_1} \times \cdots \times C_{n_r}$ where $n_1 | n_2 | \cdots | n_r$

$m = lcm(n_1, \ldots, n_r)$

$\therefore m \leq n_1 n_2 \cdots n_r$

If $a_i \in C_{n_i}$ then $a_i^{n_i} = 1$

$\therefore a_i^m = 1$

$\therefore$ Every element of G is a root of $x^m = 1$

But G has $n_1 n_2 \cdots n_r$ elements $\Rightarrow n_1 n_2 \cdots n_r \leq m$

$\therefore m = n_1 n_2 \cdots n_r$

$\therefore \gcd(n_1, \ldots, n_r) = 1$

$\Rightarrow G \simeq C_{n_1 n_2 \cdots n_r} \simeq C_m$

21) Let $F = \{0, a_1, \ldots, a_{q-1}\}$ be a field with $q = p^n$ elements for a prime p which is odd

(i) Prove that $a_1 \cdots a_{q-1} = -1$

(ii) Use the above part to prove wilsons theorem : $(p-1)! \equiv -1 \pmod p$

Ans (i) $F^\times = \{a_1, \cdots, a_{q-1}\}$ is cyclic (prev Q)

$\therefore F^\times = \langle x \rangle = \{1, x, \cdots, x^{q-2}\}$

$\prod_{i=1}^{\frac{q-1}{2}} a_i = x^{1+2+\cdots+q-2} = x^{\frac{(q-1)}{2}}$

$\therefore \left(\prod a_i\right)^2 = x^{q(q-1)} = (x^{q-1})^q = 1$

$\therefore \prod a_i = \pm 1$

$x^2 = 1$ has 2 solutions $1, -1$ (since F is field)

Here $1, -1$ are distinct since $2 \nmid q$

$\prod a_i = 1 \Rightarrow o(x) = q-1 \mid (q-1)\left(\frac{q}{2}\right)$

$\Rightarrow q$ is even $\longrightarrow\leftarrow$

$\therefore \prod a_i = -1$

(ii) Use $F = \mathbb{Z}_p$

So that $(p-1)! \equiv -1$ in $\mathbb{Z}_p$

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

TUTORIAL 14

1) Show that every finite integral domain is a field

Ans Let R be a finite integral domain.

Construct $\varphi : R \to R$ as $\varphi(x) = ax$

for some fixed non-zero $a \in R$

$\varphi(m) = \varphi(n)$

$\Leftrightarrow am = an$

$\Leftrightarrow a(m-n) = 0$

$\Leftrightarrow m-n = 0$ (R is integral domain, $a \neq 0$)

$\therefore \varphi$ is injective

R is finite $\Rightarrow$ R is surjective

$\therefore \varphi(b) = 1$ for some $b \in R$

$\therefore ab = 1$ for some $b \in R$

a is arbitrary $\Rightarrow$ every $a \in R \setminus \{0\}$ has an inverse

2) Prove that units in $R[x]$ are units of R for an integral domain R

Ans Clearly units of R are units of $R[x]$ by linearity but f be a unit in $R[x]$. $\therefore \exists g$ ... blah blah

Then $\deg f + \deg g = 0$

$\therefore \deg f = \deg g = 0 \Rightarrow f, g$ are constants & hence belong to R

$\therefore U(R[x]) = U(R)$

3) Is there an integral domain containing exactly 10 elements?

Ans $\varphi : \mathbb{Z} \to R$ s.t. $\varphi(1) = 1$

R is finite $\Rightarrow$ $\ker \varphi \neq (0)$

let $I = \ker \varphi$

Ans finite integral domain = field

field $\Rightarrow$ 10 = prime power

not possible

4) Find the quotient field of $F[[x]]$ for a field F

Ans let $f \in F[[x]]$

$$\therefore f(x) = \sum_{k=n}^{\infty} a_k x^k, \quad a_n \neq 0$$

$$= a_n x^n + a_{n+1} x^{n+1} + \cdots$$

$$= a_n x^n \left(1 + \frac{a_{n+1}}{a_n} x + \frac{a_{n+2}}{a_n} x^2 + \cdots\right)$$

units in $F[[x]]$ are those with non zero constant term

$\therefore \left(1 + \frac{a_{n+1}}{a_n} x + \cdots\right)$ is invertible in $F[[x]]$. let its inverse be $h(x)$

$$\therefore f(x) = a_n x^n (h(x))^{-1}$$

$$\therefore \frac{1}{f(x)} = \frac{h(x)}{a_n x^n}$$

$$\text{but } \frac{h(x)}{a_n} = \sum_{k=0}^{\infty} b_k x^k$$

$$\therefore \frac{1}{f(x)} = \sum_{k=0}^{\infty} b_k x^{k-n}$$

$$\therefore \frac{1}{f(x)} = = \sum_{k=-n}^{\infty} c_k x^k$$

$$\therefore K(F[[x]]) = F((x))$$

↓ ring of formal Laurent series

5) Are the rings $F_5[x]/(x^2+x+1)$, $F_3[x]/(x^3+x+1)$ integral domains

Yes we need to check if (x^2+x+1) is a prime ideal of $F_5[x]$. x^2+x+1 has no root in $F_5[x]$ and is hence irreducible and hence it is prime. but x^3+x+1 can be written as $(x-1)(x^2+x+2)$ and neither one belongs to (x^3+x+1) since both degrees are less than 3

6) $\varphi : R \to S$ is an integral domain isomorphism. Prove that $K(R) \simeq K(S)$ (K denotes quotient field)

Ans Define $f : K(R) \to K(S)$ as

$$f\left(\frac{a}{b}\right) = \frac{\varphi(a)}{\varphi(b)} \quad \forall \; b \neq 0$$

$$f\left(\frac{a}{b} + \frac{c}{d}\right) = f\left(\frac{ad+bc}{bd}\right) = \frac{\varphi(ad) + \varphi(bc)}{\varphi(bd)}$$

$$= \frac{\varphi(a)}{\varphi(b)} + \frac{\varphi(c)}{\varphi(d)} = f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right)$$

similarly $f\left(\frac{a}{b} \cdot \frac{c}{d}\right) = f\left(\frac{a}{b}\right) f\left(\frac{c}{d}\right)$

$$f\left(\frac{1}{1}\right) = \frac{\varphi(1)}{\varphi(1)} = \frac{1}{1} = 1$$

$\therefore f$ is a homomorphism

$$\ker f = \left\{ \frac{a}{b} \mid \frac{\varphi(a)}{\varphi(b)} = \frac{0}{1} \right\} = \left\{ \frac{a}{b} \mid \frac{a}{b} = \frac{0}{1} \right\}$$

$$\therefore \ker f = \left\{ \frac{0}{1} \right\} = \{ id \}$$

Also since φ is onto, f is onto

$\therefore f$ is an isomorphism

7) Find $K(R[x])$ pr R = integral domain

Ans Claim: $K(R[x]) = K((K(R))[x])$

~~for any $f, g \in R[x]$, $g \neq 0$, $\frac{f}{g} \in K(R[x])$~~

To simplify notation, let $K(R) = Q$

claim: fraction field of $R[x] \simeq$ fraction field of $\mathbb{Q}[x]$

Clearly fraction field for $R[x] \subseteq$ fraction field for $\mathbb{Q}[x]$ by direct inclusion of $R \subseteq \mathbb{Q}$

(technically not subset but maybe $\frac{R}{1} \subseteq \mathbb{Q}$)

let $f(x) = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i = \frac{1}{b} \sum_{i=0}^{n} a_i' x^i$

$g(x) = \sum_{i=0}^{n} \frac{c_i}{d_i} x^i = \frac{1}{d} \sum_{i=0}^{n} c_i' x^i$

(where $b = \text{lcm}(b_i)$, $d = \text{lcm}(d_i)$)

$\therefore \frac{f(x)}{g(x)} = \frac{\sum_{i=0}^{n} d\, a_i' x^i}{\sum_{i=0}^{n} b\, c_i' x^i} \in$ fraction field $R[x]$

$\therefore K(R[x]) \simeq K(\mathbb{Q}[x])$

8) Find all prime & maximal ideals separately for $\mathbb{R}[x]$

Ans. Any prime ideal is generated by irreducibles of $\mathbb{R}[x]$

These are also maximal (prime $\Leftrightarrow$ maximal)

The irreducibles in $\mathbb{R}[x]$ are linear, quadratic with imaginary roots

Note:

R is field $\Rightarrow$ $R[x]$ is PID

$\Rightarrow$ I is maximal iff prime iff generated by irreducible

9) Describe all prime & maximal ideals of $\mathbb{Z}_n$

Ans We know that ideals of $\mathbb{Z}_n$ are additive subgroups of $\mathbb{Z}_n$ i.e. (d) where $d \mid n$

(Note: $\mathbb{Z}_n$ has all ideals principal but it is not a PID since it is not an ID in general because maybe for $\mathbb{Z}_{12}$, $6 \times 2 = 0$ but $6, 2 \neq 0$ and hence not ID. $\mathbb{Z}_n$ is PID if n is prime)

∴ If an ideal is maximal, it must contain other ideals & no ideal should contain it

∴ If $(d_1) \subseteq (d_2)$, we know that $d_2 \mid d_1$ & conversely also true

∴ In order for (d) to be maximal, d must be prime

∴ maximal ideals of $\mathbb{Z}_n$ are (p) for prime numbers p dividing n

Any maximal ideal is ALWAYS prime anyways.

Prime elements are just prime factors of n

let $d = \gcd(q, n)$

(q is our prime element)

$d > 1$ (else it will be a unit)

$d \mid q$, $d \mid n$

claim: d is a prime number in $\mathbb{Z}$

Suppose there is some x s.t.

$$qx \equiv ab \pmod{n}$$

$\therefore d \mid ab \Rightarrow d \mid a$ or $d \mid b$

$\therefore q$ is a prime element in $\mathbb{Z}_n$

if $d = st$, then $d \mid st$ but $d \nmid s$, $d \nmid t$

(Suppose $d \mid s$, then $dx \equiv s \pmod{n} \Rightarrow d \mid 1$ in $\mathbb{Z}$ which is a contradiction)

10) Find maximal ideals of $\mathbb{R}[x]/(x^2)$, $\mathbb{R}[x]/(x^2+x+1)$

Ans $\mathbb{R}[x]/(x^2+x+1)$ is a field $\Rightarrow (0)$ is the only maximal ideal

For the first part, we invoke the 'fourth' ring isomorphism theorem:

Given a ring R, ideal I, $A (\supset I)$ is an ideal of R iff A/I is an ideal of R/I

∴ ideals in $\frac{R[x]}{(x^2)}$ correspond to ideals in $R[x]$ containing (x^2)

$R[x]$ is a PID

but $(x^2) \subseteq (f(x))$

since it is an integral domain, $f(x) \mid x^2$

$\therefore f(x) = 1, x, x^2$

But we are looking for maximal ideals

∴ maximal ideal of $R[x]$ containing (x^2) is (x) (we dont want the entire ring)

∴ $\frac{(x)}{(x^2)}$ is the only proper maximal ideal of the ring

11) Prove that $(x+y^2, y+x^2+2xy^2+y^4)$ is a maximal ideal in $\mathbb{C}[x,y]$

Ans $y+x^2+2xy^2+y^4 = y+x^2+xy^2+y^2(x+y^2)$

$\therefore y+x^2+xy^2 \in I$

$\therefore y+x(x+y^2) \in I$

$\therefore y \in I \Rightarrow x \in I \Rightarrow I = (x,y)$

(x,y) is a maximal ideal in $\mathbb{C}[x,y]$

not quotient!

12) Let M be an ideal of R s.t. R/M has only units. Show that M is the only maximal ideal of R.

Any Let $N \neq M$ be an ideal of R s.t. $N \neq R$

Then $\exists\, x \in N \setminus M \Rightarrow x \notin M \Rightarrow x$ is a unit $\Rightarrow N = R \longrightarrow\leftarrow$

13) Let R be a ring in which $a^n = a$ for some $n \geq 2$. Show that every prime ideal is maximal

Any $a(a^{n-1} - 1) = 0$

Let P be a prime ideal

For some $a \notin P$, consider $\bar{a} \in R/P$

$0 \in P \Rightarrow a \in P$ or $a^{n-1} - 1 \in P$

$\therefore a^{n-1} - 1 \in P$

$\therefore \overline{a^{n-1} - 1} = \bar{0} \Rightarrow \overline{a^{n-1}} = \bar{1}$

$\therefore \overline{a^{n-1}}$ is a unit

$\therefore \bar{a}$ is a unit

$\therefore R/P$ is a field

$\therefore P$ is a maximal ideal

14) Let $f(x)$ be a polynomial in $\mathbb{C}[x]$ with degree $d \geq 1$. Show that $\mathbb{C}[x]/(f(x))$ has at most d maximal ideals

Ans maximal ideals in $\mathbb{C}[x]/(f(x))$ correspond to maximal ideals in $\mathbb{C}[x]$ that contain $f(x)$.

$\mathbb{C}[x]$ is a PID

Thus, if $(g(x)) \supseteq (f(x))$,

we have $g(x) \mid f(x)$

$f(x)$ has d roots in $\mathbb{C}[x]$ and maximal ideals correspond to irreducibles

Thus if $f(x)$ has roots $d_1, d_2, \ldots$, $(x-d_1)$ $(x-d_2)$ --- form maximal ideals & hence there are d maximal ideals at most.

15) Let $x^2+x+1 = f(x) \in \mathbb{F}_2[x]$. Show that f is irreducible in $\mathbb{F}_2[x]$ & show that it has a root in $\mathbb{F}_4$

Ans f has no roots in $\mathbb{F}_2[x] \Rightarrow f$ is irreducible

$\mathbb{F}_4 \cong \left\{ \begin{bmatrix} a & b \\ b & a+b \end{bmatrix} : a, b \in \mathbb{F}_2 \right\}$

For $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $A^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\therefore A^2 + A + I = \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix} = 0$

$\therefore f(x)$ has a root in $\mathbb{F}_4$

TUTORIAL 15

1) For a subfield F of $\mathbb{C}$, show that an irreducible polynomial in $F[x]$ has no multiple roots

Ans Let $f(x) \in F[x]$ and $(x-r)^2 \mid f(x)$

$\therefore f(x) = (x-r)^2 g(x)$

$f'(x) = 2(x-r)g(x) + (x-r)^2 g'(x)$

$= (x-r)[g(x) + (x-r)g'(x)]$

$\therefore f'(r) = 0$

Suppose f, f' are relatively prime, then $\exists\, u, v$ in $F[x]$ s.t. $uf + vf' = 1$ (Bezout)

$\therefore f, f'$ cannot have a common root

Here f, f' have a common root

$\therefore \gcd(f, f') \neq 1 \Rightarrow \gcd(f, f')$ is some polynomial (call it g)

$\therefore g \mid f$ (contradicts irreducibility of f)

2) Show that $\mathbb{R}[x,y]$, $\mathbb{Z}[x]$ are not PID's

Ans (x, y) is not principal in $\mathbb{R}[x,y]$ because, if $(f(x,y)) = (x, y)$, then,

$x = fh$, $y = fg$

$\therefore \deg f = 1$ or 0

But $\deg f \neq 0$ since we don't f to be a unit

$\therefore \deg f = 1$, $\deg h = \deg g = 0$

$\therefore h, g \in R^\times$

$\therefore f = rx = sy$ for $r, s \in R^\times$

not possible since x, y are indeterminates

In $\mathbb{Z}[x]$, $(2, x)$ is not principal.

Suppose $(f(x)) = (2, x)$

$\therefore 2 = fg$, $x = fh$

$\therefore \deg f = \deg g = 0 \Rightarrow \deg h = 1$

$\therefore f, g \in \mathbb{Z}^\times$

$\therefore f = \pm 2$ or ± 1

$f \neq \pm 1$ else we get entire ring

but $(2, x) \neq \mathbb{Z}[x]$

since $1 \notin (2, x)$

$\therefore f = \pm 2$

WLOG $f = 2$

$\therefore (2, x) = (2)$

But $x \notin (2)$

$e^{\frac{2\pi i}{3}}$

3) Show that $\mathbb{Z}[w]$, $\mathbb{Z}[\sqrt{-2}]$ are Euclidean doms

Ans Define $N(a+b\sqrt{\omega}) = (a+bw)(a+b\bar{\omega})$

$= a^2 + b^2 - ab$

$(\because w+1+w^2=0 \Rightarrow \bar{w} = w^2)$

For $x, y \in \mathbb{Z}[w]$, $y \neq 0$,

write $\frac{x}{y} = a + bw$

for some $a, b \in \mathbb{Q}$

Find $c, d \in \mathbb{Z}$ s.t. $|a-c| \leq \frac{1}{2}$, $|b-d| \leq \frac{1}{2}$

$\therefore x = y(c+dw) + y((a-c)+(b-d)w)$

$N(y((a-c)+(b-d)w)) = N(y)\, N((a-c)+(b-d)w)$

$= N(y)\left((a-c)^2 + (b-d)^2 - (a-c)(b-d)\right)$

$\leq N(y)\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right)$

$< N(y)$

Define $N(a+b\sqrt{-2}) = a^2 + 2b^2$

For $x, y \in \mathbb{Z}[-\sqrt{2}]$, $y \neq 0$,

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

:

Same as above one

4) Prove that. $2, 3, 1 \pm \sqrt{-5}$ are irred in $\mathbb{Z}[\sqrt{-5}]$

Ans $N(a+b\sqrt{-5}) = a^2 + 5b^2 \in \mathbb{Z}$

Let $2 = \alpha\beta$

$\therefore 4 = N(\alpha) N(\beta)$

$\therefore N(\alpha) = 2$ (WLOG)

(∵ 2 is reducible, α, β not units and hence $N(\alpha), N(\beta) \neq 1$)

But $a^2 + 5b^2 = 2$ has no integer solutions

Let $3 = \alpha\beta$

$\therefore 9 = N(\alpha) N(\beta)$

$\therefore N(\alpha) = 3$

But $a^2 + 5b^2 = 3$ has no integer solutions

Let $1 \pm \sqrt{-5} = \alpha\beta$

$\therefore 6 = N(\alpha) N(\beta)$

$N(\alpha) = 2$ or $N(\alpha) = 3$ has no solutions

5) Show that $\mathbb{Z}[\sqrt{5}]$ is not a UFD

Ans $N(a + b\sqrt{5}) = a^2 - 5b^2$

units correspond to $N(a) = 1$

Suppose $2 = (a+b\sqrt{5})(c+d\sqrt{5})$ and $a+b\sqrt{5}$, $c+d\sqrt{5}$ are not units, then,

$N(2) = 4 = N(a+b\sqrt{5})\,N(c+d\sqrt{5})$

$\therefore N(a+b\sqrt{5}) = \pm 2$

$\therefore a^2 - 5b^2 = \pm 2$

Reducing in modulo 5, $a^2 \equiv \pm 2 \pmod 5$

This has no integer solution

$\therefore 2$ is irreducible

But (2) is not a prime ideal since $2 \mid (5+\sqrt{5})(5-\sqrt{5})$

but $2 \nmid 5+\sqrt{5}$, $2 \nmid 5-\sqrt{5}$

1) Show that $\mathbb{Z}[\sqrt{-5}]$ is not a PID by showing that $(3, 2+\sqrt{-5})$ is not principal

Ans $I = (3, 2+\sqrt{-5}) = (a+b\sqrt{-5})$ (say)

Then $3 = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$\therefore 9 = (a^2+5b^2)(c^2+5d^2)$

$(3, 2+\sqrt{-5}) \neq (1) = (-1)$

$\therefore \quad a^2 + 5b^2 = 3 \text{ or } 9$

$a^2 + 5b^2 = 3$ has no solution

$a^2 + 5b^2 = 9$

$\Rightarrow \quad a = 3, \; b = 0$

$a = 2, \; b = 1$

$\therefore I = (3) \text{ or } (2 + \sqrt{-5})$

Clearly $(3, 2+\sqrt{-5}) \neq (3)$ $\rightarrow 2+\sqrt{-5} \notin (3)$

and $\neq (2+\sqrt{-5})$ $\rightarrow 3 \notin (2+\sqrt{-5})$

7) Show that $1+3\sqrt{-5}$ is irred but not a prime in $\mathbb{Z}[\sqrt{-5}]$

Any $(1+3\sqrt{-5}) = (a+b\sqrt{-5})(c+d\sqrt{-5})$

$\Rightarrow 46 = (a^2+5b^2)(c^2+5d^2)$

$\therefore a^2+5b^2 = 2 \text{ or } 23$

Both no solutions

$\mathbb{Z}[\sqrt{-5}]$ is not a UFD $\Rightarrow 1+3\sqrt{-5}$ is not prime

Does this feel circular?

$$\frac{\mathbb{Z}[\sqrt{-5}]}{(1+3\sqrt{-5})} \simeq \frac{\mathbb{Z}[x]}{(x^2+5, 1+3x)} \simeq \frac{\mathbb{Z}[x]/(x-15)}{(x^2+5, 1+3x, x-15)/(x-15)}$$

$$\simeq \mathbb{Z}/46\mathbb{Z}$$

But $\mathbb{Z}_{46}$ is not an integral domain since 46 is not prime

$\therefore 1+3\sqrt{-5}$ is not prime

8) let $F = \mathbb{C}(x) = K(\mathbb{C}[x])$, F.

let $f, g \in \mathbb{C}[x,y]$. Show that f, g have a common factor in $F[y]$ iff they have a common factor in $\mathbb{C}[x,y]$

try let f, g have common factor in $F[y]$

let $f = d f_1$, $g = d g_1$ } $d \in F[y]$, $f_1, g_1 \in F[y]$

$\therefore \exists\ d_1, f_2 \in \mathbb{C}[x,y]$, $z \in \mathbb{C}^\times$ such that $f = z d_1 f_2$

Similarly $g = w d_1 g_2$

$\therefore$ They have a common factor d_1 in $\mathbb{C}[x,y]$

Now reverse the process.

9) Show that $f, g \in \mathbb{Z}[x]$ are coprime in $\mathbb{Q}[x]$ iff $(f,g) = I$ ($\subset \mathbb{Z}[x]$) is such that $I \cap \mathbb{Z} \neq (0)$

Ans Let $n \neq 0$ be such that $n \in (f,g)\mathbb{Z}[x] \cap \mathbb{Z}$

$\therefore n \in (f,g)\mathbb{Q}[x]$

But n is a unit in $\mathbb{Q}[x]$

$\therefore (f,g)\mathbb{Q}[x] = \mathbb{Q}[x]$

$\therefore f, g$ are relatively prime in $\mathbb{Q}[x]$

Conversely, if

$$(f,g) = \mathbb{Q}[x],$$

$$1 = hf + lg \qquad h, l \in \mathbb{Q}[x]$$

clearing denominators,

$$n = h_1 f + l_1 g \qquad h_1, l_1 \in \mathbb{Z}[x]$$

$\therefore n \in (f,g)\mathbb{Z}[x] \cap \mathbb{Z}$

10) Prove that $xy - zw$ is irred in $\mathbb{C}[x,y,z,w]$

Ans Let $xy - zw \in \mathbb{C}[x,z,w][y]$

This is a linear polynomial in y

$\therefore$ Suppose it is reducible,

$(xy - zw) = k \cdot f(y)$ where

$k \in \mathbb{C}[x,z,w]$, $f(y) \in \mathbb{C}[x,z,w][y]$

and $\deg f = 1$

$k \mid x$, $k \mid zw$

Bw x, zw are coprime in $\mathbb{C}[x,z,w]$

$\therefore k$ is a unit in $\mathbb{C}[x,z,w]$

$\therefore k$ is a unit in $\mathbb{C}[x,z,w][y]$

$\simeq \mathbb{C}[x,y,z,w]$

$\therefore$ irreducible

11) Show that $f = x^2 + 26x + 213$, $g = 8x^3 - 6x + 1$ are irreducible in $\mathbb{Q}[x]$

Ans $g(x+1) = 8x^3 + 24x^2 + 18x + 3$

Consider $P = (3)$ in $\mathbb{Z}[x]$.

It is a prime ideal

$8 \notin P$; $24, 18, 3 \in P$; $3 \notin P^2$

$\therefore g(x+1)$ is not a product of polynomials of degree d s.t $1 \le d \le 2$

$\therefore g(x+1)$ is irreducible

f doesn't have any roots in $\mathbb{Q}[x]$ and hence irreducible

12) Factor $x^5 + 5x + 5$ into irred factors in $\mathbb{Q}[x]$ and $\mathbb{F}_2[x]$

Ans Take $P = (5)$ a prime ideal in $\mathbb{Q}[x]$

Then f is irred in $\mathbb{Q}[x]$

No root of f in $\mathbb{F}_2$ $\Rightarrow$ no linear factors

The only irred quadratic in $\mathbb{F}_2[x]$ is $x^2 + ax + b$

But $x^2 + x$, x^2, $x^2 + 1$ are all reducible

$\therefore x^2 + x + 1$ is irred

$$x^2+x+1 \overline{)\, x^5 + x + 1 \,(\, x^3 + x^2 + 1}$$

$$0$$

$\therefore (x^5 + x + 1) = (x^2 + x + 1)(x^3 + x^2 + 1)$

irred in $\mathbb{F}_2[x]$

13) Factor $x^3 + x + 1$ in $\mathbb{F}_p[x]$ for $p = 2, 3, 5$

Ans $p = 2$: $x^3 + x + 1$ has no root in $\mathbb{F}_2$

$\therefore$ irreducible in $\mathbb{F}_2[x]$

$p = 3$: 1 is a root

$(x - 1)(x^2 + x + 2)$

irred in $\mathbb{F}_3[x]$

$\therefore$ done

$p = 5$: no root in $\mathbb{F}_5$ $\Rightarrow$ irred in $\mathbb{F}_5[x]$

14) For a prime number p, $A \in \mathbb{Z}^{n \times n}$, $A \neq I$, $A^p = I$, prove that $p - 1 \leq n$

Ans A satisfies $x^p - 1$ which has p distinct roots

$\therefore$ minimal polynomial of A has distinct roots

$\therefore A$ is diagonalizable

Now $A^p = I \Rightarrow A \in GL_n(\mathbb{Z})$ is invertible

with e.vals being p^{th} roots of unity

$A \neq I \Rightarrow \text{ord}(A) = p$

$m_A(x) \mid x^p - 1 = (x-1) f(x)$

$A \neq I \Rightarrow \deg(m_A(x)) = p - 1 \leq n$

15) Find no. of monic irreducible quadratics in $\mathbb{F}_p[x]$

Ans A monic quadratic is red if it has both roots in $\mathbb{F}_p[x]$ i.e.

$(x - r)(x - s)$ $r, s \in \mathbb{F}_p$

There are $\binom{p}{2} + p$ such polynomials

$(x-a)(x-b)$ $\quad$ $(x-a)^2$

∴ Total no. of monic mixed quadratics are

$$p^2 - \left(\left(\frac{p}{2}\right) + p\right) = \left(\frac{p}{2}\right)$$