2025-26
SRIMAAN

SRIMAAN

PG-TRB

MATHEMATICS

NEW SYLLABUS 2025-2026

POST GRADUATE ASSISTANTS (P.G ASST.)

UNIT-1- ALGEBRA

POST GRADUATE ASSISTANTS

PG-TRB

MATHEMATICS

UNIT-1: ALGEBRA

NEW SYLLABUS 2025-2026

Groups – Examples – Cyclic Groups – Permutation Groups – Lagrange's theorem – Normal subgroups – Homomorphism – Cayley's theorem – Cauchy's theorem –Sylow's theorems – Finite Abelian Groups

Groups

1. Definition and Basic Properties

Definition: Let G be a set.

A binary operation on G is a function $f : G \times G \to G$

A group is a set G, together with a binary operation $f : G \times G \to G$ such that the following axioms hold:

(i) Associativity: For any $a, b, c \in G$,

$$f(f(a,b),c) = f(a, f(b,c))$$

(ii) Identity: $\exists e \in G$ such that

$$f(a,e) = f(e,a) = a \quad \forall a \in G$$

(iii) Inverse: For any $a \in G, \exists a' \in G$ such that

$$f(a,a') = f(a',a) = e$$

Notation: Given a group (G, f) as above, we write

$$ab := f(a,b)$$

Hence the first axiom reads: $(ab)c = a(bc)$ for all $a, b, c \in G$. Note that the operation may not be multiplication in the usual sense.

Example:. $(\mathbb{Z}, +)$ is a group. $(\mathbb{Z}, -)$ is not a group. $(\mathbb{N}, +)$ is not a group.

$(\mathbb{Q}, \cdot)$ is not a group, but $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \cdot)$ is. Similarly, $\mathbb{R}^*$ and $\mathbb{C}^*$ are groups.

$(\mathbb{R}^n, +), (\mathbb{C}^n, +)$ are groups. More generally, any vector space is a group under addition. The Dihedral groups D_n = the group of symmetries of a regular n-gon

Proposition. *Let $(G, *)$ be a group*

Uniqueness of Identity: *Suppose $e_1, e_2 \in G$ are such that $ae_1 = ae_2 = a = e_1a = e_2a$, then $e_1 = e_2$*

Cancellation laws: Suppose $a, b, c \in G$ such that $ab = ac$, then $b = c$. Similarly, if $ba = ca$, then $b = c$

Uniqueness of inverses: Given $a \in G$, suppose $b_1, b_2 \in G$ such that $ab_1 = ab_2 = e = b_1a = b_2a$, then $b_1 = b_2$

Proof. By hypothesis, $e_1 = e_1e_2 = e_2$.

If $ab = ac$, then choose $a' \in G$ such that $aa' = a'a = e$, so $a'(ab) = a'(ac)$

By associativity, $$(a'a)b = (a'a)c$$

But $a'a = e$ and $eb = b$. Similarly on the RHS, so $b = c$. The right cancellation law is similar.

Suppose $ab_1 = ab_2$, then by left cancellation, $b_1 = b_2$.

Definition . Let G be a group, $a \in G$

For $n \in \mathbb{Z}$, define
$$a^n := \underbrace{a \cdot a \cdot a \ldots a}_{n \text{ times}}$$

Note that by associativity, we may write this expression without any parentheses. Furthermore,

$$a^n a^m = a^{n+m}, \text{ and } (a^n)^m = a^{nm}$$

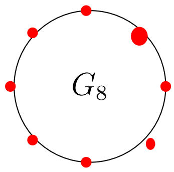
A group G is said to be cyclic if $\exists a \in G$ such that, for any $b \in G$, $\exists n \in \mathbb{Z}$ with $b = a^n$. Such an element a is called a **generator of G** (note that it may not be unique).

Example 1.1. $(\mathbb{Z}, +)$ is cyclic with generators 1 or -1

$(\mathbb{Z} \times \mathbb{Z}, +)$ is not cyclic

Proof. Suppose $a = (a_1, a_2)$ generated $\mathbb{Z} \times \mathbb{Z}$. Then $\exists n, m \in \mathbb{Z}$ such that $(1, 0) = n(a_1, a_2)$ and $(0, 1) = m(a_1, a_2)$

But $n(a_1, a_2) = (na_1, na_2)$, so this would imply that $na_2 = 0$, whence $n = 0$ or $a_2 = 0$. But if $n = 0$ this equation cannot hold, so $a_2 = 0$. Similarly, from the other equation $a_1 = 0$, so $(a_1, a_2) = (0, 0)$. But this contradicts the first equation.



For $k \in \mathbb{N}$, define $G_k = \{\xi \in \mathbb{C} : \xi^k = 1\}$. G_k is cyclic with generator $\xi_0 = e^{2\pi i/k}$

Note: Every cyclic group is either the same as $\mathbb{Z}$ or the same as G_k for some k. Can represent G_k as a *cycle* in $\mathbb{C}$. Hence the term cyclic.

Definition . A group G is said to be abelian if $a * b = b * a$ for all $a, b \in G$

Example : $(\mathbb{Z}, +)$ is abelian. In general, any cyclic group is abelian.

$(\mathbb{Z} \times \mathbb{Z}, +)$ is abelian, but not cyclic.

Consider the water molecule: It has one rotational symmetry R_{180}, and two reflection symmetries V about the XZ-plane and H about the XY-plane. We write

$$V_4 := \{e, R_{180}, V, H\}$$

for the symmetries of this molecule. Note that

$$R_{180}^2 = V^2 = H^2 = e$$

Thus, this group is not cyclic. **It is abelian.**

D_4 is non-abelian (and hence not cyclic)

Proof. $HR_{90} = D$ but $R_{90}H = D'$

so it is **non-abelian.**

For $n \in \mathbb{N}$, the general linear group is defined as

$$GL_n(\mathbb{R}) := \{A = (a_{i,j})_{n \times n} : \det(A) \neq 0\}$$

This is the collection of all invertible matrices, which is a group under multiplication. It is nonabelian and infinite.

Definition. The order of a group G is $|G|$, the cardinality of the underlying set. Table of groups discussed thus far (Note that *Cyclic* $\Rightarrow$ *Abelian*)

Group	Finite	Cyclic	Abelian
G_k	Y	Y	Y
V_4	Y	N	Y
D_n	Y	N	N
$\mathbb{Z}$	N	Y	Y
$\mathbb{Z} \times \mathbb{Z}$	N	N	Y
$GL_n(\mathbb{R})$	N	N	N

2. The Integers

Axiom **(Well-Ordering Principle)***:* Every non-empty subset of positive integers contains a smallest member.

Definition : For $a, b \in \mathbb{Z}, b \neq 0$, we say that b divides a (In symbols $b \mid a$) if $\exists q \in \mathbb{Z}$ such that $a = bq$.

Note: If $a \mid b$ and $b \mid a$, then $a = \pm b$.

A number $p \in \mathbb{Z}$ is said to be prime if, whenever $a \mid p$, then either $a = \pm 1$ or $a = \pm p$.

Theorem (Euclidean Algorithm). *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then $\exists$ unique $q, r \in \mathbb{Z}$ with the property that*

$$\boldsymbol{a = bq + r \text{ and } 0 \leq r < b}$$

Proof. We prove existence and uniqueness separately.

- **Existence: Define** $S := \{a - bk : k \in \mathbb{Z}, \text{ and } a - bk \geq 0\}$ Note that S is non-empty because:
  - If $a \geq 0$, then $a - b \cdot 0 \in S$
  - If $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$ because $b > 0$ If $0 \in S$, then $b \mid a$, so we may take $q = a/b$ and $r = 0$.

  Suppose $0 \notin S$, then S has a smallest member, say $\boldsymbol{r = a - bq}$

  Then $a = bq + r$, so it remains to show that $0 \leq r < b$. We know that $r \geq 0$ by construction, so suppose $r \geq b$, then

$$\boldsymbol{r - b = a - b(q + 1) \in S}$$

- Uniqueness: Suppose r', q' are such that

$$a = bq' + r' \text{ and } 0 \leq r' < b$$

Then suppose $r' \geq r$ without loss of generality, so $r' - r + b(q' - q) = 0$

Hence, $b \mid (r' - r)$, but $r' - r \leq r' < b$, so this is impossible unless $r' - r = 0$. Hence, $\boldsymbol{q' - q = 0}$ because $b \neq 0$.

Theorem: *Given two non-zero integers $a, b \in \mathbb{Z}$, there exists $d \in \mathbb{Z}_+$ such that*

1. $d \mid a$ *and* $d \mid b$
2. *If* $c \mid a$ *and* $c \mid b$, *then* $c \mid d$

Furthermore, $\exists s, t \in \mathbb{Z}$ *such that*

$$d = sa + tb$$

***Note that** this number if unique and is called the greatest common divisor (GCD) of a and b, denoted by*

$$gcd(a, b) = (a, b)$$

Definition . Given $a, b \in \mathbb{Z}$, we say that they are relatively prime if $gcd(a, b) = 1$

Lemma (Euclid's Lemma). *If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$. In particular, if p prime and $p \mid bc$, then either $p \mid b$ or $p \mid c$*

Proof. By the previous theorem, $\exists s, t \in \mathbb{Z}$ such that $sa + tb = 1$

Hence,

$$sac + tbc = c$$

Since $a \mid sac$ and $a \mid tbc$, it follows that $a \mid c$.

Theorem (Unique Factorization theorem). *Given $a \in \mathbb{Z}$ with $a > 1$, then $\exists$ prime numbers $p_1, p_2, \ldots,$*

$p_k \in \mathbb{Z}$ such that

$$a = p_1 p_2 \ldots p_k$$

Furthermore, these primes are unique upto re-arrangement. ie. If $q_1, q_2, \ldots, q_m \in \mathbb{Z}$ are primes such that

$$a = q_1 q_2 \ldots q_m$$

Then $m = k$ and, after rearrangement, $q_i = p_i$ for all $1 \leq i \leq m$.

Proof.
- **Existence:** Let $a \in \mathbb{Z}_+$ with $a > 1$. If $a = 2$, then there is nothing to prove, so suppose $a > 2$. By induction, assume that the theorem is true for all numbers $d < a$.

  Now fix a and note that if a is prime, there is nothing to prove. Suppose a is not prime, then $\exists b \in \mathbb{Z}_+$ such that $b \mid a$, but $b \neq \pm a$ and $b \neq \pm 1$. Hence, $a = bc$ where we may assume that $1 < b, c < a$. So by induction hypothesis, both b and c can be expressed as products of primes. Hence, a can be too.

- Uniqueness: Suppose a can be expressed in two ways as above. Then $p_1 \mid a = q_1 q_2 \ldots q_m$

By Euclid's lemma, $\exists 1 \leq j \leq m$ such that $p \mid q_j$. Assume without loss of generality that $p \mid q_1$. Since p is prime, $p \neq \pm 1$. Since q_1 is prime, it follows that $p = \pm q_1$.

Hence,

$$q_1 p_2 p_3 \ldots p_k = q_1 q_2 \ldots q_m$$

Cancellation implies that

$$p_2 p_3 \ldots p_k = q_2 q_3 \ldots q_m$$

Now induction completes the proof (How?)

3. Subgroups and Cyclic Groups

Definition: Let $(G, *)$ be a group and $H \subset G$. H is called a subgroup of G if, $(H, *)$ is itself a group. If this happens, we write $H < G$.

Lemma: let G be a group and $H \subset G$. Then $H < G$ if and only if, for each $a, b \in H$, $ab^{-1} \in H$.

Proof. Suppose H is a subgroup, then for any $a, b \in H, b^{-1} \in H$, so $ab^{-1} \in H$.

Conversely, suppose this condition holds, then we wish to show that H is a subgroup.

- Identity: If $a \in H$, then $aa^{-1} = e \in H$
- Inverse: If $a \in H$, then $ea^{-1} = a^{-1} \in H$
- Closure: If $a, b \in H$, then $b^{-1} \in H$, so $b = (b^{-1})^{-1} \in H$. Hence, $ab = a(b^{-1})^{-1} \in H$.
- Associativity: holds trivially because it holds in G.

Examples :

(i) For fixed $n \in \mathbb{N}$, consider $n\mathbb{Z} := \{0, \pm n, \pm 2n, \ldots\}$

(ii) $\{R_0, R_{90}, R_{180}, R_{270}\} < D_4$

(iii) (See Example 1.5(iii)) $G_k < S^1$ where $S^1 := \{z \in \mathbb{C} : |z| = 1\}$.

(iv) $(\mathbb{Q}, +) < (\mathbb{R}, +)$

(v) $SL_n(\mathbb{R}) < GL_n(\mathbb{R})$ where $SL_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$

Theorem: Every subgroup $H < \mathbb{Z}$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$

Proof. If $H < \mathbb{Z}$, then consider $S := \{h \in H : h > 0\}$, then S has a smallest member n by the well-ordering principle. We claim $H = n\mathbb{Z}$

Since $n \in H$, so $n\mathbb{Z} \subset H$. So suppose $h \in H$, we WTS: $h \in n\mathbb{Z}$. Assume WLOG that $h > 0$, and use Division Algorithm to write

$h = nq + r,$ where $0 \leq r < n$

Now, $nq \in H$ and $h \in H$, so $r \in H$. But then $r \in S$, and $0 \leq r < n$. If $r > 0$, then this would contradict the minimality of n, so $r = 0$. Hence, $\boldsymbol{h = nq \in n\mathbb{Z}}$

Proof. Let $a, b \in \mathbb{Z}$. WTS: $\exists d \in \mathbb{Z}$ with the required properties. Consider

$$H := \{sa + tb : s, t \in \mathbb{Z}\}$$

Then $H < \mathbb{Z}$. Hence, $\exists d \in \mathbb{Z}_+$ such that $H = d\mathbb{Z}$. Now observe:

- $a = 1 \cdot a + 0 \cdot b \in H$, so $d \mid a$. Similarly, $d \mid b$
- $\exists s, t \in \mathbb{Z}$ such that $d = sa + tb$.
- If $c \mid a$ and $c \mid b$, then $c \mid sa + tb = d$. Hence, $d = gcd(a, b)$.

Remark : G a group, $a \in G$ fixed.

(i) Cyclic subgroup generated by a is the set

$$\{a^n : n \in \mathbb{Z}\}$$

and is denoted by

(ii) Order of a, denoted by $O(a)$, is $|\langle a \rangle|$. If $n = O(a) < \infty$, then

(a) $a^m = e \Leftrightarrow n \mid m$

(b) $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

Example :

(i) $G = \mathbb{Z}$, $a = n$, then a has infinite order

(ii) $G = D_4$, $a = R_{90}$, then $O(a) = 4$

(iii) $G = S^1, a = e^{2\pi i/k}$, then $O(a) = k$

Theorem: Every subgroup of a cyclic group is cyclic.

Proof. Suppose $G = \langle a \rangle$ is cyclic, and $H < G$, then consider

$$S := \{n \in \mathbb{Z} : a^n \in H\} \subset \mathbb{Z}$$

Since $e \in H, 0 \in S$. If $n, m \in S$, then $a^n, a^m \in H$, so

$$a^{n-m} = a^n(a^m)^{-1} \in H \Rightarrow n - m \in S$$

Hence, $S < \mathbb{Z}$ By Theorem $\exists k \in \mathbb{Z}$ such that $S = k\mathbb{Z}$. Hence, $a^n \in H \Leftrightarrow k \mid n$

In other words, $H = \langle a^k \rangle$.

4. Orthogonal Matrices and Rotations

Definition :

(i) Real Orthogonal matrix is a matrix A such that $A^t A = AA^t = I$

(ii) $O_n(\mathbb{R})$ is the set of all orthogonal matrices.

$$SO_n(\mathbb{R}) := \{A \in O_n(\mathbb{R}) : \det(A) = 1\}$$

Note that $O_n(\mathbb{R})$ and $SO_n(\mathbb{R})$ are subgroups of $GL_n(\mathbb{R})$

Theorem : Let A be an $n \times n$ real matrix. Then TFAE :

(i) $A$is an orthogonal matrix

(ii) $\langle Ax, Ay \rangle = \langle x, y \rangle$ for all $x, y \in \mathbb{R}^n$

(iii) The columns of A form an orthonormal basis of $\mathbb{R}^n$

Proof. We prove each implication (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i)$\Rightarrow$ (ii): If $AA^t = A^tA = I$, then fix $x, y \in \mathbb{R}^n$, then

$$\langle Ax, Ay\rangle = (Ay)^t(Ax) = (y^tA^t)(Ax) = y^t(A^tA)x = y^tx = \langle x, y\rangle$$

(ii)$\Rightarrow$ (iii): If $\langle Ax, Ay\rangle = \langle x, y\rangle$, then consider the standard basis $\{e_1, e_2, \ldots, e_n\}$ of $\mathbb{R}^n$. Then

$$\langle Ae_i, Ae_j\rangle = \langle e_i, e_j\rangle = \delta_{i,j}$$

But the columns of A are precisely the vectors $\{Ae_i : 1 \leq i \leq n\}$

(iii)$\Rightarrow$ (i): Suppose the columns of A form an orthonormal basis of $\mathbb{R}^n$. Then, for any $1 \leq i \leq n$,

$$\langle e_i, e_j\rangle = \delta_{i,j} = \langle Ae_i, Ae_j\rangle = \langle A^tAe_i, e_j\rangle$$

This is true for all $1 \leq j \leq n$, so (Why?)

$$A^tAe_i = e_i$$

Hence, $A^tA = I$ because the $\{e_i\}$ form a basis. Similarly, $AA^t = I$ as well.

Example :

(i) For $\theta \in \mathbb{R}$, $\rho_\theta = \left(\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \right) \in SO_2(\mathbb{R})$

(ii) $r = \begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix}\Big) \in O_2(\mathbb{R}) \setminus SO_2(\mathbb{R})$

Lemma: $SO_2(\mathbb{R}) = \{\rho_\theta : \theta \in \mathbb{R}\}$. Hence, $SO_2(\mathbb{R})$ is called the 2×2 rotation group.

Proof. If

$$A = \begin{pmatrix} c & a \\ s & b \end{pmatrix}$$

is an orthogonal matrix, then $(c, s) \in \mathbb{R}^2$ is a unit vector. Hence, $\exists\theta \in \mathbb{R}$ such that $c = \cos(\theta)$ and $s = \sin(\theta)$. Now let

$$R := \begin{pmatrix} c & -s \\ s & c \end{pmatrix} = \rho_\theta$$

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

$$P := R^tA = \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in SO_2(\mathbb{R})$$

By the previous lemma, the second column of P is a unit vector perpendicular to $(0, 1)$. Hence,

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$$

Since $\det(P) = 1$, $P = I$, so $A = R = \rho_\theta$.

Definition: A rotation of $\mathbb{R}^3$ about the origin is a linear operator ρ with the following properties:

(i) ρ fixes a unit vector $u \in \mathbb{R}^3$

(ii) ρ rotates the two dimensional subspace W orthogonal to u.

The matrix associated to a rotation is called a rotation matrix, and the axis of rotation is the line spanned by u.

(i) The identity matrix is a rotation, although its axis is indeterminate.

(ii) The matrix
$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$$
is a rotation matrix with axis $\operatorname{span}(e_1)$.

(iii) If ρ is a rotation that is not the identity, then let u be a unit vector in its axis of rotation. Let $W := \{u\}^{\perp}$ denote the subspace orthogonal to u. Then $W \cong \mathbb{R}^2$, and
$$\rho|_W : W \to W$$
is a rotation. Hence, we may think of $\rho|_W \in SO_2(\mathbb{R})$. The angle of rotation (computed by the Right Hand Rule) is denoted by θ, and we write $\rho = \rho_{(u,\theta)}$.

The pair (u, θ) is called the spin of the rotation ρ.

Lemma: If $A \in SO_3(\mathbb{R}), \exists v \in \mathbb{R}^3$ such that $Av = v$.

Proof. We show that 1 is an eigen-value of A. To see this, note that

$\det(A - I) = (-1)\det(I - A)$ and $\det(A - I) = \det((A - I)^t)$ by the properties of the determinant. Since $\det(A) = 1$, we have

$\det(A - I) = det((A - I)^t) = \det(A)\det(A^t - I) = \det(AA^t - A) = det(I - A)$ Hence, $\det(A - I) = 0$ as required.

Euler's Theorem: The elements of $SO_3(\mathbb{R})$ are precisely all the rotation matrices. ie.
$$SO_3(\mathbb{R}) = \{\rho_{u,\theta} : u \in \mathbb{R}^3 \text{ unit vector}, \theta \in \mathbb{R}\}$$

Proof. (i) Let $\rho = \rho_{u,\theta}$. Since u is a unit vector, there is an orthonormal basis $\mathcal{B}$ of $\mathbb{R}^3$ containing u. Let P denote the change of basis matrix associated to $\mathcal{B}$. Then $P \in SO_3(\mathbb{R})$ because its columns are orthogonal

Furthermore,
$$B := PAP^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Hence, $B \in SO_3(\mathbb{R})$. Since $P \in SO_3(\mathbb{R})$, it follows that $\rho \in SO_3(\mathbb{R})$.

(ii) Conversely, suppose $A \in SO_3(\mathbb{R})$, then choose a unit vector $v \in \mathbb{R}^3$ such that $Av = v$. Consider an orthonormal basis $\mathcal{B}$ of $\mathbb{R}^3$ containing v, then with P as above,
$$B := PAP^{-1} \in SO_3(\mathbb{R})$$
Let $W := \{e_1\}^{\perp}$, then $B(e_1) = e_1$ and $B(W) \subset W$. Hence, B has the form
$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}$$
Let $C := \begin{pmatrix} a & b \\ c & b \end{pmatrix}$, then $\det(C) = \det(B) = 1$, and the columns of C are orthogonal vectors. Hence by Lemma 4.2, $C \in SO_2(\mathbb{R})$. Hence, $\exists \theta \in \mathbb{R}$ such that
$$C = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$
Hence, $B = \rho_{e_1,\theta}$, so $A = \rho_{v,\theta}$.

Corollary: Composition of rotations about any two axes is a rotation about some other axis.

5. Homomorphisms

Definition: Let $(G, *)$ and $(G', \cdot)$ be two groups. A function $\varphi : G \to G'$ is called a group homomorphism if

$$\varphi(g_1 * g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

for all $g_1, g_2 \in G$.

Examples :

(i) $n \mapsto 2n$ from $\mathbb{Z}$ to $\mathbb{Z}$

(ii) $x \mapsto e^x$ from $(\mathbb{R}, +)$ to $(\mathbb{R}^*, \times)$

(iii) $det : GL_n(\mathbb{R}) \to \mathbb{R}^*$

(iv) $\theta \mapsto \rho_\theta$ from $(\mathbb{R}, +)$ to $SO_2(\mathbb{R})$

Lemma : Let $\varphi : G \to G'$ be a group homomorphism, then

(i) $\varphi(e) = e'$ where e, e' are the identity elements of G and G' respectively

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$ *Proof.* (i) Note that

$$e' \cdot \varphi(e) = \varphi(e) = \varphi(e * e) = \varphi(e) * \varphi(e)$$

By cancellation, $\varphi(e) = e'$

(ii) For $g \in G$,

$$\varphi(g) \cdot \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e) = e' = \varphi(g) \cdot \varphi(g)^{-1}$$ By cancellation $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Definition : $\varphi : G \to G'$ a homomorphism

(i) $\ker(\varphi) := \{g \in G : \varphi(g) = e'\}$. Note that $\ker(\varphi) < G$

(ii) $\text{Image}(\varphi) := \{\varphi(g) : g \in G\}$. Note that $\text{Image}(\varphi) < G'$.

Examples :

(i) φ: $\mathbb{Z} \to \mathbb{Z}$ is $\varphi(n) = 2n$, then $\ker(\varphi) = \{0\}$, $\text{Image}(\varphi) = 2\mathbb{Z}$

(ii) φ: $GL_n(\mathbb{R}) \to \mathbb{R}^*$ is $\varphi(A) = det(A)$, then $\ker(\varphi) = SL_n(\mathbb{R})$, $\text{Image}(\varphi) = \mathbb{R}^*$

(iii) φ: $\mathbb{R} \to SO_2(\mathbb{R})$ is $\varphi(\theta) = \rho_\theta$, then $\ker(\varphi) = 2\pi\mathbb{Z}$, $\text{Image}(\varphi) = SO_2(\mathbb{R})$ by Lemma 4.4

(iv) φ: $\mathbb{C}^* \to \mathbb{R}^*$ is $\varphi(z) = |z|$, then $\ker(\varphi) = S^1$, $\text{Image}(\varphi) = \mathbb{R}^*$

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

(i) $\varphi$is said to be injective (or one-to-one) if, for any $g_1, g_2 \in G$, $\varphi(g_1) = \varphi(g_2) \Rightarrow g_1 = g_2$

(ii) $\varphi$is said to be surjective (or onto) if, for any $g' \in G', \exists g \in G$ such that $\varphi(g) = g'$.

(iii) φ is said to be bijective if it is both injective and surjective. Note, if φ is bijective, then

$$\varphi^{-1} : G' \to G$$

is also a group homomorphism. If such a homomorphism exists, then we say that φ is an isomorphism, and we write

$$G \cong G'$$

Theorem : $\varphi : G \to G'$ is injective iff $\ker(\varphi) = \{e\}$. In that case, $\varphi : G \xrightarrow{\sim} \text{Image}(G)$.

Proof. (i) If φ is injective, and $g \in \ker(\varphi)$, then $\varphi(g) = e' = \varphi(e)$. Hence, $g = e$, whence $\ker(\varphi) = \{e\}$.

(ii) Conversely, if $\ker(\varphi) = \{e\}$, and suppose $g_1, g_2 \in G$ such that $\varphi(g_1) = \varphi(g_2)$, then

$$\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e'$$

Hence, $g_1 g_2^{-1} \in \ker(\varphi)$, so $g_1 g_2^{-1} = e$, whence $g_1 = g_2$. Thus, φ is injective. The second half of the argument follows from the fact that $\varphi : G \to$ **Image(φ) is surjective.**

Examples :

(i) φ: $\mathbb{Z} \to \mathbb{Z}$ is $\varphi(n) = 2n$, then φ is injective, but **not surjective**

(ii) φ: $(\mathbb{R}, +) \to SO_2(\mathbb{R})$ is $\varphi(\theta) = \rho_\theta$, then f is surjective, but not injective, because $\rho_0 = \rho_{2\pi}$.

(iii) If G is a finite cyclic group with $|G| = k$, then $G \cong G_k$

Proof. Let $G = \langle a \rangle$ with $|a| = k$. Define a map $\varphi : G \to G^k$ by $a^n \mapsto \zeta^n$

where $\zeta = e^{2\pi i/k}$. φ is an isomorphism.

(iv) $G_4 \not\cong V_4$

Proof. Suppose there were an isomorphism $\varphi : G_4 \to V_4$, then consider $b := \varphi(\zeta)$, **where** $\zeta = e^{2\pi i/\ 4}$. Since $|\zeta| = 4$, it follows that $|b| = 4$ .. But V_4 has no elements of order 4, so this is impossible.

6. The Symmetric Group

Definition : Let X be a set

(i) Apermutation of X is a bijective function $\sigma : X \to X$

(ii) Let S_X denote the set of all permutations of X. Given two elements $\sigma, \tau \in S_X$, the product $\sigma \circ \tau \in S_X$ is given by composition. Since composition of functions is associative, this operation makes S_X a group, called the symmetric group on X.

Lemma : If $|X| = |Y|$, then $S_X \cong S_Y$

Proof. If $|X| = |Y|$, there is a bijective function $f : X \to Y$. Define $\Theta : S_X \to S_Y$ by

$$\Theta(\sigma) := f \circ \sigma \circ f^{-1}$$

Then

(i) Θ is a group homomorphism:

$$\Theta(\sigma \circ \tau) = f \circ \sigma \circ \tau \circ f^{-1} = f \circ \sigma \circ f^{-1} \circ f \circ \tau \circ f^{-} = \Theta(\sigma) \circ \Theta(\tau)$$

(ii) Θ is injective: If $\sigma \in \ker(\Theta)$, then $f \circ \sigma \circ f^{-1} = \text{id}_Y$. For each $y \in Y$,

$$f(\sigma(f^{-1}(y)) = y \Rightarrow \sigma(f^{-1}(y)) = f^{-1}(y) \quad \forall y \in Y$$

Since f^{-1} is surjective, this implies $\sigma(x) = x \quad \forall x \in X$

So $\sigma = \text{id}_X$.

(iii) Θ is surjective: Given $\tau \in S_Y$, define $\sigma := f^{-1} \circ \tau \circ f$, then $\boldsymbol{\sigma \in S_X}$ **and** $\boldsymbol{\Theta(\sigma) = \tau}$.

Definition : If $X = \{1, 2, \ldots, n\}$, then S_X is denoted by S_n, and is called the symmetric group on n letters. By the previous lemma, if Y is any set such that $|Y| = n$, then $S_Y \cong S_n$

Remark :

(i) $O(S_n) = n!$

Proof. Let $\sigma \in S_n$, then $\sigma(1) \in \{1, 2, \ldots, n\}$ has n choices. Now $\sigma(2)$ has $(n-1)$ choices, and so on. The total number of possible such σ's is $n \times (n-1) \times \ldots \times 1 = n!$.

(ii) If $\sigma \in S_n$, we represent σ by $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$

(iii) For $\sigma \in S_n$, define $P_\sigma \in GL_n(\mathbb{R})$ by $P_\sigma(e_i) = e_{\sigma(i)}$. Since the columns of P_σ are orthogonal, $P_\sigma \in O_n(\mathbb{R})$

Theorem : The function $\varphi : S_n \to O_n(\mathbb{R})$ by $\sigma \mapsto P_\sigma$ is a homomorphism. *Proof.* Given $\sigma, \tau \in S_n$, consider

$$P_{\sigma\circ\tau}(e_i) = e_{\sigma\circ\tau(i)} = e_{\sigma(\tau(i))} = P_\sigma(e_{\tau(i)}) = P_\sigma P_\tau(e_i)$$

This is true for each i, so $P_{\sigma\circ\tau} = P_\sigma P_\tau$.

Definition :

(i) Note that $\det : O_n(\mathbb{R}) \to \{\pm 1\}$ is a group homomorphism. Define the sign function

$sgn : S_n \to$ as the composition $\sigma \mapsto P_\sigma \mapsto \det(P_\sigma)$

(ii) The alternating group on n letters is

$$A_n := \{\sigma \in S_n : sgn(\sigma) = 1\}$$

Example :

(i) In S_3, consider $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto -1$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \mapsto 1$$

Hence,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in A_3 \text{ but } \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \notin A_3$$

(ii) $S_n = A_n \sqcup B_n$ where $B_n = \{\sigma \in S_n : sgn(\sigma) = -1\}$ [Not a subgroup of S_n]

(iii) Let $\sigma_0 \in S_n$ denote the permutation

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 2 & 1 & 3 & \ldots & n \end{pmatrix}$$

For any $\sigma \in A_n, \sigma_0\sigma \in B_n$ and conversely. Hence the map $f : A_n \to B_n$ given by $\sigma \mapsto \sigma_0\sigma$ is a bijection (not a group homomorphism though). Hence, $\boldsymbol{S_n = A_n \sqcup B_n}$ and

$$\boldsymbol{|A_n| = |B_n| = \frac{n!}{2}}$$

Quotient Groups

1. Modular Arithmetic

Definition : Let X be a set. An equivalence relation on a set X is a subset $R \subset X \times X$ such that

(i) $(x, x) \in R$ for all $x \in X$ [Reflexivity]

(ii) If $(x, y) \in R$, then $(y, x) \in R$ [Symmetry]

(iii) If $(x, y), (y, z) \in R$, then $(x, z) \in R$ [Transitivity]

We write $x \sim y$ if $(x, y) \in R$.

Examples :

(i) X any set, $x \sim y \Leftrightarrow x = y$

(ii) $X = \mathbb{R}^2$, $(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow y_1 - y_2 = x_1 - x_2$

(iii) $X = \mathbb{C}$, $z \sim w \Leftrightarrow |z| = |w|$

(iv) $X = \mathbb{Z}$, $a \sim b \Leftrightarrow n \mid (b - a)$. Denote this by $a \equiv b \pmod{n}$

Proof. (a) Reflexivity: Obvious

(b) Symmetry: If $a \sim b$, then $b - a = nk$ for some $k \in \mathbb{Z}$, so $a - b = n(-k)$, whence $n \mid (a - b)$, so $b \sim a$.

(c) Transitivity: If $a \sim b$ and $b \sim c$, then $\exists k, \ell \in \mathbb{Z}$ such that $b - a = nk$ and $c - b = n\ell$

Hence

$$c - a = c - b + b - a = n(\ell + k) \Rightarrow n \mid (c - a) \Rightarrow a \sim c$$

Definition: Let X be a set, and $\sim$ an equivalence relation on X. For $x \in X$, the equivalence class of x is the set

$$[x] := \{y \in X : y \sim x\}$$

Note that $x \in [x]$, so it is a non-empty set.

Theorem : Equivalence classes partition the set

Proof. Since $x \in [x]$ for all $x \in X$, we have that

$$X = \bigcup_{x \in X} [x]$$

WTS: Any two equivalence classes are either disjoint or equal. So fix two classes $[x], [y]$ and suppose

$$z \in [x] \cap [y]$$

WTS: $[x] = [y]$ So choose $w \in [x]$, then

$w \sim x \sim z \sim y \Rightarrow w \in [y]$. Hence, $[x] \subset [y]$. Similarly, $[y] \subset [x]$

Examples :

(i) $[x] = \{x\}$

(ii) $[(x_1, y_1)] =$ the line parallel to the line $y = x$ passing through (x_1, y_1)

(iii) $[z] =$ the circle of radius $|z|$

(iv) $[a] = \{b \in Z : \exists q \in \mathbb{Z}$ such that $b = a + nq\}$

Lemma : Consider $\mathbb{Z}$ with $\equiv \pmod{n}$

(i) There are exactly n equivalence classes $\{[0], [1], \ldots, [n-1]\}$

(ii) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $a + b \equiv (a' + b') \pmod{n}$

Proof.

(i) Firstly note that if $0 \leq i, j \leq n-1$, then $i \nsim j$. Hence, there are at least $n-1$ equivalence classes as listed above. To see that there are exactly n equivalence classes, note that if $a \in \mathbb{Z}$, then by the Division Algorithm, $\exists q, r \in \mathbb{Z}$ such that

$$a = nq + r, \text{ and } 0 \leq r < n$$

Hence, $[a] = [r]$ as required.

(ii) If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then $\exists k, \ell \in \mathbb{Z}$ such that

$$a = a' + kn \text{ and } b = b' + \ell n$$

Hence, $$\boldsymbol{a + b = a' + b' + n(k + \ell)}$$

so $\boldsymbol{(a + b) = (a' + b')} \pmod{n}$ as required.

Definition: Consider the set of all equivalence classes

$$\mathbb{Z}_n := \{[0], [1], [2], \ldots, [n-1]\}$$

We define the sum of two classes as

$$[a] + [b] := [a + b]$$

This is well-defined by the previous lemma.

Theorem: $\mathbb{Z}_n = \{[0], \ldots, [n-1]\}$ is a cyclic group of order n with generator

Proof. (i) Associativity: Because $+$ on $\mathbb{Z}$ is associative.

(ii) Identity: $[0]$ is the identity element.

(iii) Inverse: Given $[a] \in \mathbb{Z}_n$, assume without loss of generality that $0 \leq a < n$, then $b := n - a$ has the property that

$$[a] + [b] = [a + b] = [n] = [0]$$

(iv) Cyclic: For any $a \in \mathbb{Z}$ $\quad [a] = a[1]$

so $\mathbb{Z}_n$ is cyclic with generator.

Permutation Groups:

A permutation is a one-one mapping of a set onto itself.

The set S(E) is the set of all permutations of the set E is a group. S(E) is contains n! elements,

S(E) is denoted by s_n is called same times as **symmetric group** of degree n.

Let S_3 be the symmetric grou on 3symbols.Then $O(S_3)$ is 3! = 6 **(TRB-2012)**

Let $x_1,x_2,x_3\ldots x_n$ be distinct elements of the set E, the symbol ($x_1,x_2,x_3,\ldots$ x_r)) be denote the permutation that sent $x_1 \rightarrow x_2, x_2 \rightarrow x_3$ $x_r \rightarrow x_1$ ther element of E fixed.This permutation called a **cycle** of length r

$(x_1,x_2,x_3,\ldots x_n)$, $(x_2,x_3,x_4,\ldots x_n,x_1)$, ….. $(x_r,x_1,x_2,x_3\ldots x_{n-1})$ ……… all are same permutations

Example:

E = {1,2,3,4,5}

$(2,4,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 5 & 2 \end{pmatrix}$

Inverse of a cycle

Inverse of a cycle is obtained by writing its elements in the reverse order.

Example:

The inverse of (1,3,5) is (5,3,1)

In S_n there are $\frac{1}{r}\frac{n!}{(n-r)!}$ distinct r cycles **(TRB 2017)**

If p is prime number, than there are (p-1)!+1 element in s_p satisfies $x^p = e$ **(TRB-2004)**

Disjoint cycle

Two cycles are said to be disjoint if they have no element in common.

Example:

(1,2,5) and (3,4) are disjoint cycle.

(1,3,5) and (2,3,4) are not disjoint cycle.

- Every permutation can be expressed as product of disjoint cycles.

Transposition

A cycle of lengh 2 is called a transposition. **(TRB-2004,2006)**

Any permutation of a finite set can be expressed as a product of transpositions.

Example:

1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$ = (1,6,2,5)(3,4) = (1,6)(1,2)(1,5)(3,4)
2. If b = (1 2 3 4 5 6 7) , then c^3 is

   (a) (1 3) (2 4) (b) (1 3) (c) (2 4) (c) (2 3)(3 1)
3. order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$ is

   (a) 3 (b) 4 (c) 5 (d) 6
4. Given permutation a = (1 2 3 4 5 6 7), then a^3 is

   (a) (1 3 5 7 2 4) (b) (1 4 7 3 6 2 5) (c) (1 7 6 5 4 3 2) (d) (1 2 3 4 5 6 7)
5. The inverse of a cycle of cycle (4 6 2 7 3)

   (a) (4 2 7 3 6) (b) (3 7 2 6 4) (c) (2 6 4 3 7) (d) (6 7 3 2 4)
6. order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$ in S_7 **(TRB-2005)**

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 6 & 4 & 1 & 2 & 3 \end{pmatrix}$$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = e$. Order = 4

Express the permutation of disjoint cycles

(a) (1,2,3)(4,5)(1,6,7,8,9)(1,5) = (1,2)(1,3)(4,5)(1,6)(1,7)(1,8)(1,9)(1,5)

(b) .(1,2)(1,2,3)(1,2) = (1,2)(1,2)(1,3)(1,2) = (1,2)(1,3)

Odd and Even permutation

- A permutation of a finite set is even or odd If can be expressed as the product of an even or odd numbers of transposition.
- A cycle ($x_1,x_2,x_3,\ldots$ x_m) of length m can be expressed as the product of (m-1) transposition.
- cycle is even if m is odd.
- cycle is odd if m is even.

- The identity permutation is an even
- The product of two even permutations is an even.
- The product of two odd permutations is an even.
- The product of an even and odd permutations is odd.
- Inverse of even permutation is even.
- Inverse of odd permutation is odd.
- The set of all even permutations A_n is a subgroup of S_n

$O(A_n) = \frac{n!}{2}$

An is called the **alternating group**

Example:

product of (1,2)(2,4)(3,6) is $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$

Example:

Determine which of the following an even permutation

(a). $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 5 & 1 & 6 & 7 & 9 & 8 \end{pmatrix}$ is odd

(b). (1,2,3,4,5)(1,2,3) is even

copute $a^{-1}ba$ of the following

(c).If a = (1,3,5)(1,2) , b = (1,5,7,9)

a = (1,3,5,2)

$a^{-1}ba$= (2,5,3,1)(1,5,7,9)(1,3,5,2) = (2,7,9,3)

(d).If a = (5,7,9) , b = (1,2,3) copute $a^{-1}ba$

$a^{-1}ba$ = (9,7,5)(1,2,3)(5,7,9) = (1,2,3)

(e). The solution of the equation ax = b in s_3 where a =$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$,b = $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, **(TRB-2005)**

$x = a^{-1}b$ = $\begin{pmatrix} 3 & 2 & 1 \\ 1 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

Lagrange Theorem

If G is a finite group and H is subgroup of G, than O(H) is a divisor of O(G)
That is, O(H) \O(G)

Example:

A group of order 8 can not have subgroup of order 3,5,6 or 7

Group must be of order 2 or 4

Example:

G = {1,-1,i,-i}, H ={1,-1,i} or {i,-i,1} are not a subgroup of G [O(H)\O(G)]
Converse of Lagrange theorem need not true. H ={i ,-i }is not a subgroup of G but O(H)\O(G)

Coset

If H is a subgroup of G,a$\in A, than\ Ha = \{ha \backslash h \in H\}. Ha\ is\ called\ a\ right\ coset\ of\ H\ in\ G.$
$aH = \{ah \backslash h \in H\}. aH\ is\ called\ a\ left\ coset\ of\ H\ in\ G.$

Example:

Z ={ … -2,-1,0,1,2,… } is a group under addition

Let H be a multiples of 5. H ={ …-10,-5,0,5,10,… } is a sub set of Z Than, 0+H ={ …-10,-5,0,5,10,… }

1+H ={ …-9,-4,1,6,11… }

2+H ={ …-8,-3,2,7,12… }

3+H ={ …-7,-2,3,8,13… }

4+H ={ …-6,-1,4,9,14… } are distinct left coset of H in Z and their union is Z

- H is a right and left coset of H

  eH =H =He

- If H is an abelian ,than aH =Ha
- Any two left cosets (right cosets) of H in G are either Identical or have no element in common.
- There is one-one correspondence between any two right cosets of H in G

Index of H in G

The number of distinct left coset of H in G is called the Index of H in G

It is denoted by [G:H] or $I_G(H)$

[G:H] = $I_G(H) = \frac{O(G)}{O(H)}$

If G is a finite group and a$\in G, than\ O(a) divides\ O(G)$ **(TRB-2006)**

that is, O(a)\O(G)

If G is afinite group of order n and a$\in G$,than $a^n = e$ { $a^{O(G)} = e$ }

Euler function

$\varphi(n)$ is called Eular function which is number of element and relatively prime to n lessthan n

If n is prime number,Than $\varphi(n)$ = n-1

If n is positive integer and a is relative prime to n, than $a^{\varphi(n)} \equiv 1 \pmod n$

Fermat theorem

If p is a prime number and 'a' is any integer, than $a^p \equiv a \pmod p$ or $a^{p-1} \equiv 1 \pmod p$

Wilson's theorem

If p is a prime number, than 1+(p-1)! is divisible by p

If G is group of order pq, where p and q are prime numbers,than there is atmost one cyclic subgroup of order p.

Example:

If O(G) = 30,Than it has atleast **8** number of subgroup.

Number of divisor of 30 is 8 which are 1,2,3,5,6,10,15,30 Divisor formula $N = p^a q^b r^c$

$\Rightarrow d(N) = (a+1)(b+1)(c+1)$

Example:

A cyclic group have a generator of order 15 ,than the cyclic group may have **8** number of generators.

O(G) = 15. Number of relatively prime to 15 is 8 { 1,2,4,7,8,11,13,14 }

$\varphi(n) = n(1-\frac{1}{p})\left(1-\frac{1}{q}\right)(1-\frac{1}{r})$ { 15 =3× 5 , since $n = p^x q^y r^z$

$= 15(1-\frac{1}{3})\left(1-\frac{1}{5}\right) = 8$

Example:

1. Find the remainder when 2^{16} is divisible by 17

   $2^{17-1} \equiv 1 \pmod{17}$

   $2^{16} \equiv 1 \pmod{17}$

2. Find the remainder when 2^{50} is divisible by 17

   $2^{40} \equiv 5 \pmod{17}$

3. Find the remainder when 3^{100} is divisible by 13 $a^{p-1} \equiv 1 \pmod p$ $\Rightarrow 3^{13-1} \equiv 1 \pmod{13}$

   $3^{12} \equiv 1 \pmod{13}$ $\Rightarrow (3^{12})^8 \equiv 1 (mod 13)$ $3^{96} \equiv 1(mod 13)$ $\Rightarrow 3^{96} \times 3^4 \equiv 3^4 (mod 13)$

   $3^{100} \equiv 81(mod 13)$ $\Rightarrow 3^{100} \equiv 3(mod 13)$

4. Find the remainder when 2^{103} is divisible by 5

   $2^{103} \equiv 3 (\text{mod } 5)$

5. Find the remainder when 5^{50} is divisible by 12

   $a^{\varphi(n)} \equiv 1(\text{mod } n)$ $\{ \quad \varphi(n) = n(1-\frac{1}{p})\left(1-\frac{1}{q}\right)(1-\frac{1}{r}) \quad =12(1-\frac{1}{2})\left(1-\frac{1}{3}\right)$

   $= 4$ $5^{4} \equiv 1(\text{mod } 12)$

   $(5^4)^{12} \equiv 1(\text{mod } 12) \Rightarrow 5^{48} \equiv 1(\text{mod } 12)$

   $5^{48} \times 5^2 \equiv 25(\text{mod } 12) \Rightarrow 5^{50} \equiv 1(\text{mod } 12)$

Example:

1. Find the remainder when 2^{16} is divisible by 17

   $2^{17-1} \equiv 1(\text{mod } 17)$

   $2^{16} \equiv 1(\text{mod } 17)$

2. Find the remainder when 2^{50} is divisible by 17

   $2^{40} \equiv 5(\text{mod } 17)$

3. Find the remainder when 3^{100} is divisible by 13 $a^{p-1} \equiv 1(\text{mod } p) \Rightarrow 3^{13-1} \equiv 1(\text{mod } 13)$

   $3^{12} \equiv 1(\text{mod } 13) \Rightarrow (3^{12})^8 \equiv 1(mod 13)$ $3^{96} \equiv 1(mod 13) \Rightarrow 3^{96} \times 3^4 \equiv 3^4(mod 13)$

   $3^{100} \equiv 81(mod 13) \Rightarrow 3^{100} \equiv 3(mod 13)$

4. Find the remainder when 2^{103} is divisible by 5

   $2^{103} \equiv 3(\text{mod } 5)$

TO BE CONTINUED.....

TN-MAWS-MUNICIPAL ADMINISTRATION & WATER SUPPLY DEPARTMENT-(DEGREE & DIPLOMA) STUDY MATERIALS AVAILABLE.

TRB-ASSISTANT PROFESSORS IN GOVERNMENT ARTS AND SCIENCE COLLEGES & COLLEGES OF EDUCATION STUDY MATERIALS AVAILABLE.

UG-TRB MATERIALS

GRADUATE TEACHERS / BLOCK RESOURCE TEACHER EDUCATORS (BRTE) & SGT

- UG TRB: TAMIL MATERIAL WITH QUESTION BANK.
- UG TRB: ENGLISH STUDY MATERIAL +Q. BANK.
- UG-TRB: MATHEMATICS MATERIAL WITH Q. BANK (E/M)
- UG TRB: PHYSICS MATERIAL WITH QUESTION BANK (E/M)
- UG TRB: CHEMISTRY MATERIAL + QUESTION BANK (E/M)
- UG TRB: HISTORY MATERIAL + Q.BANK (E/M)
- UG TRB: ZOOLOGY MATERIAL + QUESTION BANK (E/M)
- UG TRB: BOTANY MATERIAL +QUESTION BANK (T/M& E/M)
- UG TRB: GEOGRAPHY STUDY MATERIAL (E/M)

SCERT/DIET/GTTI (LECTURER) STUDY MATERIAL AVAILABLE.
TNPSC-(CESE)-JSO STUDY MATERIAL AVAILABLE.

TANGEDCO (TNEB)-(T/M & E/M)
ASSESSOR/ASSISTANT ENGINEER (A.E)/JUNIOR ASSISTANT (ACCOUNTS)