

$$1. (a). A \times C = \{(a, c) \mid a \in A \vee c \in C\}.$$

$$\begin{aligned} & a \in A \subset B \\ & c \in C \subset D \end{aligned}$$

$$\therefore (a, c) \in B \times D.$$

$$\therefore A \times C \subseteq B \times D$$

$$(b). \bigcap_{i=1}^k A_i \subseteq \bigcap_{i=1}^k B_i$$

$$A_1 \subseteq B_1 \quad \checkmark$$

$$\text{Assume } \bigcap_{i=1}^k A_i \subseteq \bigcap_{i=1}^k B_i$$

$$\text{WTS } \bigcap_{i=1}^{k+1} A_i \subseteq \bigcap_{i=1}^{k+1} B_i$$

$$\therefore \bigcap_{i=1}^{k+1} A_i = \bigcap_{i=1}^k A_i \cap A_{k+1} \quad \bigcap_{i=1}^{k+1} B_i = \bigcap_{i=1}^k B_i \cap B_{k+1}$$

$$\bigcap_{i=1}^k A_i \subseteq \bigcap_{i=1}^k B_i \quad A_{k+1} \subseteq B_{k+1}.$$

$$\therefore \bigcap_{i=1}^{k+1} A_i \subseteq \bigcap_{i=1}^{k+1} B_i \quad \therefore \bigcap_{i=1}^n A_i \subseteq \bigcap_{i=1}^n B_i \quad n \in \mathbb{Z}^+$$

$$(c). (i). \bigcup_{k=1}^{\infty} A_k = \{0, 1, 2, \dots, \infty\} \\ = \{0\} \cup \mathbb{N} = \mathbb{W}.$$

$$\bigcap_{k=1}^{\infty} A_k = \{0, 1, 2, 3, 4, 5, 6, 7\}.$$

$$(ii). \bigcup_{k=1}^{\infty} A_k = \{0, 1, 2, \dots, \infty\} \\ = \mathbb{W}.$$

$$\bigcap_{k=1}^{\infty} A_k = \emptyset$$

$$(iii). k \rightarrow \infty$$

$$\frac{3}{k} \rightarrow 0 \quad 5k+2 \rightarrow \infty$$

$$\bigcup_{k=1}^{\infty} A_k = (0, \infty).$$

$$\bigcap_{k=1}^{\infty} A_k = [3, 7] \cup [10].$$

$$(d). f(n) = \begin{cases} 1/2 & 2|n \\ 3n+1 & 2 \nmid n \end{cases}$$

$$2(a) (G, *)$$

Group:

- Closure

$$\forall x, y \in G, \\ x * y \in G.$$

- Associativity

$$\forall x, y, z \in G,$$

$$(x * y) * z = x * (y * z)$$

- Neutral.

$$\exists e \in G,$$

$$x * e = e * x = x.$$

- Invertibility

$$\forall x \in G, \exists y \in G, \\ x * y = e.$$

(i) injection fixing at most one solution

$$f(n)=4 \quad n=8 \text{ or } n=1$$

Not injective.

(ii). Surjection. fixing at least one solution.

$$\forall y \in N \exists z \in G$$

$$\therefore f(xz) = y \quad \text{Surjective.}$$

3. (a) congruent modulo. :

two numbers have a same modulo when divided by a certain number

class of residues

all integers that have a same modulo when divided by a certain number

$$(b). 27, 27-83, 27+83 \rightarrow 1^{10}$$

(c) gcd input two positive integers

$\text{gcd}(a, b)$

by calculating modulo with one another

and stops when modulo = 0
the divisor is $\text{gcd}(a, b)$.

$$1680 \equiv 140 \pmod{540}$$

$$1540 \equiv 0 \pmod{140}$$

$$\therefore \text{gcd}(1680, 1540) = 140$$

$$(d). 5bx \equiv 23 \pmod{93}$$

$$\phi(93) = 2 \times 30 = 60$$

$$5b^{60} \equiv 1 \pmod{93}$$

$$5b^{-1} \equiv 5b^{59} \equiv x \pmod{93}$$

subgroup: $H \subseteq G$

$(H, *)$ satisfies a group.

H is a subgroup of G .
left coset.

Let $g \in G$.

$(H, *)$ a subgroup of $(G, *)$

gH is a left coset

$$gH = \{g * h \mid h \in H\}$$

(b).

$g \in G$.

$$g * g' = \epsilon$$

$$g * g'' = \epsilon$$

g 's inverse g', g''

$$(g * g') * g'' = \epsilon * g'' = g''$$

$$g * g' * g'' = (g * g') * g = g.$$

$\therefore g'' = g'$ \therefore Only one inverse for g .

(c)

$$H = H_1 \cap H_2.$$

$$x, y \in H.$$

$$x, y \in H_1 \vee x, y \in H_2.$$

Closure.

$$x * y \in H_1 \vee x * y \in H_2 \vee \dots$$

Associativity

$$\rightarrow *$$

Neutral

$$\rightarrow \epsilon \in H_1 \vee \epsilon \in H_2$$

$$\epsilon \in H.$$

Invertibility

$$x \in H_1, x^{-1} \in H_1,$$

$$x \in H_2, x^{-1} \in H_2$$

$$\therefore x^{-1} \in H.$$

$$\leftarrow y^{-1} \in H.$$

$\therefore H$ is a group

$$H \subseteq H_1 \subseteq G.$$

\downarrow
Subgroup of G .

$\text{gcd}(56, 93)$

p_i	q_i	s_i	t_i
93	1	0	0
56	1	0	1
37	1	1	-1
19	1	-1	2
18	1	2	-3
1	18	-3	5
0			

$$\begin{aligned} l &= 56 \times 5 - 93 \times 3 \\ &= 280 - 279 \\ &\equiv 1. \end{aligned}$$

$$56^{-1} \equiv 56^{19} \pmod{93}$$

$$5 \times 23 \equiv 115 \equiv 22 \pmod{93}$$

$$\therefore x \equiv 22 + 93k, \quad k \in \mathbb{Z}.$$

$$(e) 7^{62} \pmod{120} \quad 120 = 2^3 \times 3 \times 5$$

$$\begin{aligned} \phi(120) &= (120 \times (1 - \frac{1}{2})) \times (1 - \frac{1}{3}) \times (1 - \frac{1}{5}) \\ &= (120 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5}) = 32. \end{aligned}$$

$$7^{32} \equiv 1 \pmod{120}$$

$$7^{64} \equiv 1 \pmod{120}$$

$$7^{63} = 7^{-1} \equiv ? \pmod{120}$$

p_i	q_i	s_i	t_i
120	1	0	0
7	17	0	1
1	7	1	-1
0			

$$l = 120 - 17 \times 7$$

$$7^{-1} \equiv -17 \pmod{120}$$

$$\equiv 103 \pmod{120}$$

$$7^{-2} \equiv 103^2 \pmod{120}$$

$$\equiv 10609 \pmod{120}$$

$$\equiv 49 \pmod{120}$$

$$\therefore 7^{62} \equiv 49 \pmod{120}$$

(d). Closure: for $\forall q_i \in R, q_i \neq -1$.

if $g_1 + g_2 = g_1 + g_2 + g_1 g_2 = -1$.

$$g_1 g_2 + g_1 + g_2 + 1 = 0$$

$$(g_1 + 1)(g_2 + 1) = 0$$

$$g_1 = -1 \text{ or } g_2 = -1$$

Contrary to $g_i \neq -1$.

$\therefore g_1 + g_2 \neq -1$.

$g_1 + g_2 + g_1 g_2$ is a real number.
not equal to -1 . \checkmark

Associativity

$$g_1 * (g_2 * g_3)$$

$$= g_1 * (g_2 + g_3 + g_2 g_3)$$

$$= g_1 + g_2 + g_3 + g_2 g_3 + g_1(g_2 + g_3 + g_2 g_3)$$

$$= g_1 g_2 + g_1 g_3 + g_2 g_3 + g_1 g_2 g_3$$

$$+ g_1 + g_2 + g_3$$

$$= (g_1 + g_2 + g_1 g_2) * g_3$$

$$= (g_1 * g_2) * g_3 \quad \checkmark$$

Neutral. $g_i + 0 = g_i + 0 + 0 \times g_i = g_i$
 $0 * g_i = 0 + g_i + 0 \times g_i = g_i$
 \therefore neutral element.

Invertibility.

$$g_i + g_i' + g_i g_i' = 0$$

$$g_i + g_i'(g_i + 1) = 0$$

$$g_i'(g_i + 1) = -g_i$$

$$g_i' = \frac{-g_i}{g_i + 1}$$

$\therefore g_i \neq -1$.

$$\therefore \boxed{\frac{-g_i}{g_i + 1}} \text{ GR.}$$

\checkmark

(ii) $g = 5, \Sigma = 0$

$$5 + g_2 + 5g_2 = 0 \quad 6g_2 = -5$$

$$g_2 = -\frac{5}{6}$$

$$(f) x^7 \equiv 2 \pmod{21}$$

$$\phi(21) = 21 \times \frac{2}{3} \times \frac{4}{7} = 12$$

$$x = \sqrt[7]{2} \equiv 2^{7^{-1}} \pmod{21}$$

$$y \equiv 7^{-1} \pmod{\phi(21)} \equiv 7^{-1} \pmod{12}$$

$$\gcd(7, 12) - 1 = 7 \times 1 - 12 \times 4$$

$$7^{-1} \pmod{12} \equiv 7 \pmod{12}$$

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

$$x \equiv 2^7 \pmod{21} \equiv 128 \pmod{21}$$

$$\equiv 2 \pmod{21}$$

$$x = 2 + 21k \pmod{k \in \mathbb{Z}}$$

4. (a). Partition: divide Set $\underset{\sim}{S}$

Set of subsets S' such that each element appears only once in S' 's element sets

Relation

a collection of ordered pairs from two sets, with one element from each one of them.

Equivalence relation

Reflexivity $\forall x E(x, x)$

Symmetry $\forall x, y \quad E(x, y) \rightarrow E(y, x)$

Transitivity $\forall x, y, z \quad E(x, y) \vee E(y, z) \rightarrow E(x, z)$

Equivalence class

a subset of form $\{x \in X : E(x, a)\}$

where E is a equivalence relation.
a is an element of X

5.

$$(a). S = \begin{pmatrix} 1 & 3 \\ 2 & 1 \\ 3 & 2 \\ 4 & 6 \\ 5 & 7 \\ 6 & 4 \\ 7 & 8 \\ 8 & 5 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 8 \\ 2 & 4 \\ 3 & 6 \\ 4 & 2 \\ 5 & 5 \\ 6 & 7 \\ 7 & 3 \\ 8 & 1 \end{pmatrix}$$

$$ST = \begin{pmatrix} 1 & 5 \\ 2 & 6 \\ 3 & 4 \\ 4 & 1 \\ 5 & 7 \\ 6 & 8 \\ 7 & 2 \\ 8 & 3 \end{pmatrix}$$

$$TS = \begin{pmatrix} 1 & 6 \\ 2 & 3 \\ 3 & 4 \\ 4 & 7 \\ 5 & 3 \\ 6 & 2 \\ 7 & 1 \\ 8 & 5 \end{pmatrix}$$

$$T^{-1} = \begin{pmatrix} 1 & 8 \\ 2 & 4 \\ 3 & 7 \\ 4 & 2 \\ 5 & 5 \\ 6 & 3 \\ 7 & 6 \\ 8 & 1 \end{pmatrix}$$

$$(g)$$

$$j^{30} \equiv 1 \pmod{31}$$

$$\phi(31) = 30$$

(b). Assume not form a partition.

Then $\exists a \in E_1 \quad a \in E_2$. (not same class)

$$E(a, e_1) \vee E(a, e_2)$$

$$\rightarrow E(e_1, e_2)$$

$$\rightarrow E_1 = E_2 \text{ not true.}$$

Contradiction

(c). Reflexivity

$$(i) xRx \rightarrow x - x = 0 \in \mathbb{Z}$$

Symmetry

$$xRy \rightarrow x - y = k \in \mathbb{Z}$$

$$yRx \rightarrow y - x = -k \in \mathbb{Z}$$

Transitivity

$$xRy \rightarrow x - y = k_1 \in \mathbb{Z}$$

$$yRz \rightarrow y - z = k_2 \in \mathbb{Z}$$

$$xRz = x - z = x - y + y - z = k_1 + k_2 \in \mathbb{Z}$$

(ii)

$$\{x | x = \sqrt{2} + k \pmod{k \in \mathbb{Z}}\}$$

(d). Prove : $a \equiv b \pmod{n}$.

$$a = kn + m$$

$$b = kn + m$$

$$a^2 = kn^2 + 2knm + m^2$$

$$b^2 = kn^2 + 2knm + m^2$$

\equiv modulo

$$(b) \sigma = (132)(46)(578)$$

$$\tau = (18)(24)(367) = (5).$$

$$(c) \text{order}(\sigma) = 6$$

$$\text{order}(\tau) = 6$$

$$(d) \sigma = (13)(32)(46)(57)(78)$$

$$\tau = (18)(24)(367)$$

$$(e) \sigma^{2240} = \sigma^{6 \times 373 + 2} = \sigma^2 = (123)(587)$$

$$\tau^{10395} = \tau^{6 \times 1732 + 3} = \tau^3 = (18)(24)$$

(f) σ, τ both even.

(g) - - -

7. (a). eigenvalue λ

eigenvector v .

$$\lambda v = Av. \quad v \neq 0$$

$$(b). \quad Av - \lambda v = 0$$

$$|A - \lambda E|_F = 0$$

$$\begin{vmatrix} a-\lambda & b \\ b & -a-\lambda \end{vmatrix} = 0$$

$$(a-\lambda)(-a-\lambda) - b^2 = \lambda^2 - a^2 - b^2 = \lambda^2 - 1 = 0.$$

$$\lambda = 1 \quad \text{or} \quad \lambda = -1.$$

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

$$(a-1)x + by = 0$$

$$bx - (a+1)y = 0$$

$$(a-1)bx + b^2y = 0$$

$$b(a-1)x - (a^2-1)y = 0$$

$$(c). \quad 121 \equiv 81 \pmod{4}$$

$$11 \not\equiv 9 \pmod{4}$$

$$6. (a) \quad \begin{cases} x-w=2 \\ y-z+w=3 \\ az=1 \\ y+bw=0 \end{cases}$$

$$w=x-2$$

$$x+y-z=5.$$

$$az=1$$

$$y+bz=2b.$$

$$\{(b-1)x+z=2b-5.$$

$$az=1.$$

$$a=0 \quad \text{or} \quad b=1 \quad a+\frac{1}{3}$$

$$(b) \quad a \neq 0 \quad \text{and} \quad b \neq 1$$

$$z = \frac{1}{a} \quad (b-1)x = 2b-5-\frac{1}{a}$$

$$x = \frac{2b-5-\frac{1}{a}}{b-1}$$

$$w = \frac{2b-5-\frac{1}{a}}{b-1} - \frac{2b-2}{b-1}$$

$$= \frac{-3-\frac{1}{a}}{b-1} = -\frac{3+\frac{1}{a}}{b-1}$$

$$y = 2b - \frac{2b^2-5b-b}{b-1}$$

$$= \frac{2b^2-2b-2b^2+5b+b}{b-1}$$

$$= \frac{3b+b}{b-1}$$

$$(c). \quad b=1 \quad a=-\frac{1}{3}$$

$$x \in \mathbb{R}.$$

$$z = -3$$

$$y = -x+2$$

$$w = x-2$$

$$(d)$$

$$\begin{cases} x-w=2. \\ y-z+w=3 \end{cases} \quad (1)$$

$$\begin{cases} z=1. \\ y+5w=0 \end{cases} \quad (2)$$

$$\begin{cases} z=1. \\ y+5w=0 \end{cases} \quad (3)$$

$$\begin{cases} z=1. \\ y+5w=0 \end{cases} \quad (4)$$

$$(1) \times 5 + (4) \quad 5x - 5w = 10$$

$$(b^2 + a^2 - 1)y = 0 \quad y \in \mathbb{R}.$$

$$x = \frac{(a+1)y}{b}$$

$$\text{let } y=1 \quad x = \frac{a+1}{b}$$

$$v = \begin{pmatrix} \frac{a+1}{b} \\ 1 \end{pmatrix}$$

$$\lambda = -1.$$

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

$$(a+1)x + by = 0$$

$$bx + (-a+1)y = 0$$

$$(a+1)bx + b^2y = 0$$

$$b(a+1)x + (-a+1)(a+1) = 0$$

$$b^2y - (1-a^2)y = 0$$

$$(b^2 - 1 + a^2)y = 0$$

$$x = \frac{(a-1)}{b}y$$

$$\text{let } y=1 \quad v = \begin{pmatrix} \frac{a-1}{b} \\ 1 \end{pmatrix}$$

$$\textcircled{1} + \textcircled{2}$$

$$\begin{aligned} 5x+y &= 10 & \textcircled{5} \\ x+y-z &= 5 & \textcircled{6} \end{aligned}$$

$$\textcircled{3} \quad z = \frac{1}{2}$$

$$x+y = \frac{11}{2} \quad \textcircled{7}$$

$$\textcircled{5} - \textcircled{6} \quad 4x = \frac{9}{2}$$

$$x = \frac{9}{8}$$

$$y = \frac{44}{8} - \frac{9}{8} = \frac{35}{8}$$

$$w = \frac{9}{8} - 2 = -\frac{7}{8}$$

$$(c). A^2 = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$$

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

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

identity matrix

$$A^3 = A$$