

## Question 1

### Problem a

There are  $n$  inputs to  $n$  outputs  
 $\Rightarrow$ Number of combinations :  $n^2$   
 $\Rightarrow$ Number of binary operation :  $n^{n^2}$

### Problem b

There are  $n$  inputs to  $n - 1$  outputs  
 $\Rightarrow$ Number of combinations :  $\frac{n(n-1)}{2}$   
 $\Rightarrow$ Also add the ordered pairs  $x = y : \frac{n(n-1)}{2} + n = \frac{n(n+1)}{2}$   
 $\Rightarrow$ Number of binary operation :  $n^{\frac{n(n+1)}{2}}$

## Question 2

$$(b * d) * a = b * (d * a)$$

$$c * a = b * d$$

$$c * a = c$$

$$(b * d) * b = b * (d * b)$$

$$c * b = b * b$$

$$c * b = b$$

$$(b * d) * c = b * (d * c)$$

$$c * c = b * c$$

$$c * c = c$$

$$(b * d) * d = b * (d * d)$$

$$c * d = b * a$$

$$c * d = b$$

$$\Rightarrow \begin{array}{c|cccc} * & a & b & c & d \\ \hline a & a & b & c & d \\ b & b & b & c & c \\ c & c & b & c & b \\ d & d & b & c & a \end{array}$$

### Question 3

#### Problem a

$$\begin{aligned} & a * b \\ &= 5ab \\ &= 5ba \\ &= b * a \leftarrow \text{commutative} \\ & a * (b * c) \\ &= a * (5bc) \\ &= 5a(5bc) \\ &= 25abc \\ & (a * b) * c \\ &= (5ab) * c \\ &= 5 \times 5abc \\ &= 25abc \\ &= a * (b * c) \leftarrow \text{associative} \end{aligned}$$

#### Problem b

$$\begin{aligned} & a * b \\ &= 5ab - 1 \\ &= 5ba - 1 \\ &= b * a \leftarrow \text{commutative} \\ & a * (b * c) \\ &= a * (5bc - 1) \\ &= 5a(5bc - 1) - 1 \\ &= 25abc - 5a - 1 \\ & (a * b) * c \\ &= (5ab - 1) * c \\ &= 5 \times (5ab - 1)c - 1 \\ &= 25abc - 5c - 1 \\ &\neq a * (b * c) \leftarrow \text{not associative} \end{aligned}$$

### Problem c

$$\begin{aligned}a * b &= a - b + 1 \\b * a &= b - a + 1 \\ \Rightarrow a * b &\neq b * a \\ \Rightarrow &\text{not commutative} \\ a * (b * c) &= a * (b - c + 1) = a - (b - c + 1) + 1 = a - b + c \\ (a * b) * c &= (a - b + 1) * c = a - b + 1 - c + 1 = a - b - c + 2 \\ \Rightarrow a * (b * c) &\neq (a * b) * c \\ \Rightarrow &\text{not associative}\end{aligned}$$

### Problem d

$$\begin{aligned}a * b &= 3^{a+b} \\b * a &= 3^{b+a} \\ \Rightarrow a * b &= b * a \\ \Rightarrow &\text{commutative} \\ a * (b * c) &= a * (3^{b+c}) = 3^{a+3^{b+c}} \\ (a * b) * c &= (3^{a+b}) * c = 3^{3^{a+b}+c} \\ \Rightarrow a * (b * c) &\neq (a * b) * c \\ \Rightarrow &\text{not associative}\end{aligned} \tag{1}$$

## Question 4

$$\langle A, * \rangle := \begin{array}{c|cc} & * & a & b \\ \hline a & & b & a \\ b & & a & a \end{array}$$

The operation is commutative since it is symmetric along the diagonal

$$a * (a * b) = a * a = b$$

$$(a * a) * b = b * b = a$$

$$\Rightarrow a * (a * b) \neq (a * a) * b$$

$$\Rightarrow \langle A, * \rangle \text{ is not associative}$$

## Question 5

### Problem 1

$$\langle G, * \rangle := \begin{array}{c|cc} * & a & b \\ \hline a & a & b \\ b & b & a \end{array}$$

$$\Rightarrow a^2 \neq b \wedge b^2 \neq b$$

$$\Rightarrow \nexists x \in G : x^2 = b$$

### Problem 2

Suppose :  $x \in G$  appears twice in one row

$$u * v := x \wedge u * w := x, v \neq w \in G$$

$$\Rightarrow u * v = u * w$$

$$u^{-1} * (u * v) = u^{-1} * (u * w)$$

$$(u^{-1} * u) * v = (u^{-1} * u) * w$$

$$e * v = e * w$$

$$v = w \nleftrightarrow v \neq w$$

$$\Rightarrow \forall x \in G \text{ appears at most once in one row}$$

Since each row has  $|G|$  different outputs for  $|G|$  different inputs

$$\Rightarrow \text{There must exactly one element in each row}$$

The logic is the same for the proposition in column.

## Question 6

### Problem 1

identity value :

$$a * e = a = e * a$$

$$a * e = a + e$$

$$\Rightarrow a + e = a$$

$$\Rightarrow e = 0$$

inverse :

$$a * a^{-1} = e$$

$$\Rightarrow a + a^{-1} = 0$$

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

associative :

$$a * (b * c)$$

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

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

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

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

closure :

$$\exists a, b \in G$$

$$\Rightarrow a := 3m, b := 3n$$

$$a * b$$

$$= a + b$$

$$= 3m + 3n$$

$$= 3(m + n) \in G$$

$$\Rightarrow \langle G, * \rangle \text{ is a group}$$

### Problem 2

identity value :

$$\begin{aligned} & a * e \\ &= a + 2e \\ &= a \\ \Rightarrow e &= 0 \end{aligned}$$

$$\begin{aligned} & e * a \\ &= e + 2a \\ &= a \\ \Rightarrow e &= -a \end{aligned}$$

$e = 0 \nleftrightarrow e = -a$   
 $\Rightarrow$  There is no identity value for  $*$   
 $\Rightarrow \langle G, * \rangle$  is not a group

### Problem 3

identity value :

$$\begin{aligned} & a * e \\ &= |ae| \\ &|ae| = a \\ &LHS \geq 0 \end{aligned}$$

$\Rightarrow a < 0 \implies |ae| = a$  has no solution for  $e$   
 $\Rightarrow \langle G, * \rangle$  is not a group

### Problem 4



identity value :

$$a * e$$

$$=ae$$

$$=a$$

$$\Rightarrow e = 1 = 1 + 0 \times \sqrt{2} \in G$$

$$e * a = ea = a$$

inverse :

$$a * a^{-1} = e$$

$$\Rightarrow a \cdot a^{-1} = 1$$

$$\Rightarrow a^{-1} = \frac{1}{a}$$

associative :

$$a * (b * c)$$

$$=a * (bc)$$

$$=abc$$

$$=(ab)c$$

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

closure :

$$a := a_1 + a_2\sqrt{2}, b := b_1 + b_2\sqrt{2}$$

$$a * b$$

$$=ab$$

$$=(a_1 + a_2\sqrt{2})(b_1 + b_2\sqrt{2})$$

$$=(a_1b_1 + 2a_2b_2) + (a_1b_2 + b_1a_2)\sqrt{2} \in G$$

$$\Rightarrow \langle G, * \rangle \text{ is a group}$$

## Problem 5

identity value :

$$a * e$$

$$=\sqrt{ae}$$

$$\sqrt{ae} = a$$

$$\Rightarrow e = a$$

$\Rightarrow$  there cannot be an identity

$\Rightarrow \langle G, * \rangle$  is not a group

### Problem 6

identity value :

$$A * E$$

$$=AE$$

$$=A$$

$$\Rightarrow E = I_2$$

inverse :

$$A * A^{-1} = E$$

$$\Rightarrow A \cdot A^{-1} = I_2$$

$$A^{-1} \cdot A \cdot A^{-1} = A^{-1} \cdot I_2$$

$$A^{-1} = A^{-1}$$

associative :

$$A * (B * C)$$

$$=A * (BC)$$

$$=ABC$$

$$=(AB)C$$

$$=(A * B) * C$$

closure :

$$C := A * B$$

$$\Rightarrow C = AB$$

$$M_{a \times b} \times M_{b \times c} = M_{a \times c}$$

$$\Rightarrow C \in M_{2 \times 2}(\mathbb{R})$$

$$\Rightarrow \langle G, * \rangle \text{ is a group}$$

### Problem 7

identity value :

$$A * E$$

$$=AE$$

$$=A$$

$$\Rightarrow E = I_2 \in G$$

inverse :

$$A * A^{-1} = E$$

$$\Rightarrow A \cdot A^{-1} = I_2$$

$$A^{-1} \cdot A \cdot A^{-1} = A^{-1} \cdot I_2$$

$$A^{-1} = A^{-1}$$

associative :

$$A * (B * C)$$

$$=A * (BC)$$

$$=ABC$$

$$=(AB)C$$

$$=(A * B) * C$$

closure :

$$C := A * B$$

$$\Rightarrow C = AB$$

$$\det(C) = \det(A) \det(B)$$

$$\Rightarrow \det(C) = 1 \times 1 = 1$$

$$\Rightarrow C \in G$$

$$\Rightarrow \langle G, * \rangle \text{ is a group}$$

## Problem 8

identity value :

$$\begin{aligned} & A * E \\ = & AE \\ = & A \end{aligned}$$

$$\Rightarrow E = I_2 \in G$$

inverse :

$$\begin{aligned} & A * A^{-1} = E \\ \Rightarrow & A \cdot A^{-1} = I_2 \\ & A^{-1} \cdot A \cdot A^{-1} = A^{-1} \cdot I_2 \\ & A^{-1} = A^{-1} \end{aligned}$$

associative :

$$\begin{aligned} & A * (B * C) \\ = & A * (BC) \\ = & ABC \\ = & (AB)C \\ = & (A * B) * C \end{aligned}$$

closure :

$$A := \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}, B := \begin{bmatrix} 2 & 1 \\ -3 & -2 \end{bmatrix}$$

$$A^2 = B^2 = I_2$$

$$C := A * B$$

$$C = AB = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \neq I_2$$

$$\Rightarrow \langle G, * \rangle \text{ is not closed}$$

$$\Rightarrow \langle G, * \rangle \text{ is not a group}$$

## Question 7

### Problem 1

$$\begin{aligned} & \exists a, b \in G \\ & a = a^{-1} \\ \Rightarrow & a^2 = e \\ & c := a * b \\ \text{Consider : } & a * b * b * a \\ & a * b * b * a \\ = & a * (b * b) * a \\ = & a * e * a \\ = & a * a \\ = & e \\ \Rightarrow & c * (b * a) = e \\ & c \text{ has only one inverse } a * b \\ \Rightarrow & a * b = b * a \\ \Rightarrow & \langle G, * \rangle \text{ is commutative} \end{aligned}$$

### Problem 2

$$\begin{aligned} & \text{Suppose : } \forall a \neq e \in G, |G| = 2n, n \in \mathbb{Z}^+ : a \neq a^{-1} \\ & \forall a \neq b \in G : a, a^{-1}, b, b^{-1} \text{ are all distinct} \leftarrow \text{properties of group} \\ \Rightarrow & \text{Every } a \text{ and } a^{-1} \text{ can form a pair without repetition} \\ \Rightarrow & |G| = 2n + 1, n \in \mathbb{Z}^+ \leftarrow e^{-1} = e \\ & |G| = 2n + 1 \nleftrightarrow |G| = 2n \\ \Rightarrow & \exists a \neq e \in G : a^{-1} = a \end{aligned}$$

## Reference

Jeffery Shu