(1) Let S be a set having exactly one element. How many different binary operations can be defined on S? Answer the question if S has exactly 2 elements, 3 elements, n elements

Ans: Number of distinct binary operations on a set = number of unique configurations of the composition table for the set

For $S_1 = \{a\}$

	a
a	a

∴ distinct binary operations = 1

For $S_2 = \{a, b\}$

	a	b
a	1	2
b	3	4

A unique configuration exists depending on whether each cell from 1-4 has an 'a' or 'b'
∴ distinct binary operations = 2^4

Similarly, for S_3 distinct binary operations = 3^9 ← size of table, 3 ← possible values
Thus, for a set with n elements, number of distinct binary operations
= $\boxed{n^{(n^2)}}$

(2) How many different commutative binary operations can be defined on a set of 2 elements? on a set of 3 elements? on a set of n elements.

Ans: Number of distinct binary operations (commutative) on a set
= number of unique configurations of the composition table that is symmetric about the main diagonal

For $S_2 = \{a, b\}$

	a	b
a	1	2
b		3

Since the bottom left cell must contain the same value as cell #2 [ab = ba],
distinct commutative binary operations = 2^3

Similarly for $S_3 = \{a, b, c\}$

	a	b	c
a	1	2	3
b		4	5
c			6

number of distinct commutative binary operations
= 3^6 ← area of upper triangle (units), 3 ← possible values

□□□....□ → n
□□....□ → n-1
□....□ → n-2
⋮
□ → 1

Area = $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ units

Thus, for a set with n elements, number of distinct commutative binary operations

= $\boxed{n^{\frac{n(n+1)}{2}}}$

① Determine whether * defined as follows gives a binary operation on the set or not. If not, justify; else check for associativity, commutativity and identity element

Axioms for binary operation on set S.

i) operation must be defined for all elements in S.

ii) result must be single valued and must lie in S.

Commutative : $a * b = b * a \quad \forall a, b \in S.$

Associative : $(a * b) * c = a * (b * c) \quad \forall a, b, c \in S.$

Identity : $\exists e \in S$ such that $a * e = e * a = a \quad \forall a \in S$

i) On $\mathbb{Z}^+$, $a * b = a - b$

Binary operation – not defined as $a - b \notin \mathbb{Z}^+$ for $b > a$

ii) On $\mathbb{Z}^+$, $a * b = a^b$

- Binary operation is defined
- Commutative → no, $a^b \neq b^a \quad \forall a, b \in \mathbb{Z}^+$
- Associative → no, $a^{(b^c)} \neq (a^b)^c \quad \forall a, b, c \in \mathbb{Z}^+$
- Identity → none, $a^e = e^a = a$ cannot exist $\forall a \in \mathbb{Z}$

iii) On $\mathbb{R}$, $a * b = a - b$.

- Binary operation is defined
- Commutative → no, $a - b \neq b - a \quad \forall a, b \in \mathbb{R}$
- Associative → no, $(a - b) - c \neq a - (b - c) \quad \forall a, b, c \in \mathbb{R}$
- Identity → none, $a - e = e - a = a$ cannot exist $\forall a \in \mathbb{R}$

iv) On $\mathbb{R}$, $a * b = |a| + |b|$.

- Binary operation is defined
- Commutative → yes.
- Associative → yes, $||a| + |b|| + |c| = |a| + |b| + |c| = |a| + ||b| + |c|| \quad \forall a, b, c \in \mathbb{R}$
- Identity → none, $|a| + 0 = 0 + |a| = |a| \neq a \quad \forall a \in \mathbb{R}$.

v) On $\mathbb{Z}$, $a * b = |a|b$

- Binary operation is defined
- Commutative → no, $|a|b \neq |b|a \quad \forall a,b \in \mathbb{Z}$
- Associative → yes, $||a|b|c = |a||b|c = |a|(|b|c) \quad \forall a,b,c \in \mathbb{Z}$
- Identity → none, $|a|e = |e|a = a$ cannot exist $\forall a \in \mathbb{Z}$

vi) On $\mathbb{Q}$, $a * b = ab + 3$

Binary operation is defined

Commutative → yes

Associative → no, $abc + 3c + 3 \neq abc + 3a + 3 \quad \forall a,b,c \in \mathbb{Q}$

Identity → none, $ae + 3 = ea + 3 = a \Rightarrow e = \frac{a-3}{a} \Rightarrow e$ not ...

④ Either prove the following statement or give a counter-example

a) Every binary operation on a set consisting of a single element is both commutative and associative

Let the set be $S = \{a\}$ and the binary operation be $*$

Commutative → yes, $a * a = a * a. = a.$

Associative → yes, $a * (a * a) = (a * a) * a. = a * a = a.$

b) Every commutative binary operation on a set with just two elements is associative

Consider $*$ defined as follows on a set, $S = \{a, b\}$

*	a	b
a	b	b
b		a.

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

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

Thus, associativity is not valid

⑤ Determine whether the binary operation $*$ defined as follows gives a group structure or not. If not, justify

Group axioms for a set G

i) binary operation, $*$ is defined

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

iii) (identity) $\exists e \in G$ such that $a*e = e*a = a \quad \forall a \in G.$

iv) (invertibility) $\forall a \; \exists a' \in G$ such that $a * a' = a' * a = e$

i) $\langle \mathbb{Z}, * \rangle : a * b = ab$

Not a group, as inverse does not exist for $0 \in \mathbb{Z}$

ii) $\langle 2\mathbb{Z}, * \rangle : a * b = a + b$

- Binary operation is defined as $a+b$ is single valued and $\in 2\mathbb{Z}$ $\forall a, b \in 2\mathbb{Z}$
- (Associativity) $(a+b)+c = a+(b+c)$ $\forall a, b, c \in 2\mathbb{Z}$ $\therefore$ true
- (Identity) $a+0 = 0+a = a$ $\forall a \in 2\mathbb{Z}$ and $0 \in \mathbb{Z}$ $\therefore$ true
- (Invertibility) $\forall a \; \exists (-a) \in 2\mathbb{Z} : a+(-a) = -a+a = 0$ $\therefore$ true

Thus, it is a group.

iii) $\langle \mathbb{R}^+, * \rangle : a * b = \sqrt{ab}$

(Associativity) $a*(b*c) = \sqrt{a\sqrt{bc}}$, $(a*b)*c = \sqrt{\sqrt{ab}\,c}$ $\Rightarrow$ not associative $\forall a, b, c \in \mathbb{R}^+$

$\therefore$ not a group

iv) $\langle \mathbb{R}^*, * \rangle : a * b = a/b$

(Associativity) $a*(b*c) = a/bc$, $(a*b)*c = ac/b$ $\Rightarrow$ not same $\forall a, b, c \in \mathbb{R}^*$

$\therefore$ not a group

v) $\langle \mathbb{C}, * \rangle : a * b = |ab|$

Not a group, as identity, e : $|ae| = |ea| = a$ cannot exist $\forall a \in \mathbb{C}$

vi) $\langle \mathbb{Q}[\sqrt{2}], + \rangle : \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

- Binary operation is defined as $p+q$ is single valued and $\in \mathbb{Q}[\sqrt{2}]$ $\forall p, q \in \mathbb{Q}[\sqrt{2}]$
- (Associativity) Addition is associative
- (Identity) $p+0 = 0+p = p$ $\forall p \in \mathbb{Q}[\sqrt{2}]$ and $0 = 0+0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$
- (Invertibility) $\forall p \; \exists (-p) \in \mathbb{Q}[\sqrt{2}] : p+(-p) = -p+p = 0$

Thus, it is a group

vii) $\langle \mathcal{P}(X), \Delta \rangle$ where $\mathcal{P}(X)$ = power set of X, Δ = Symmetric difference

- Binary operation is defined as $R \Delta S$ is single valued and $\in \mathcal{P}(X)$ $\forall R, S \in \mathcal{P}(X)$
- (Associativity) Symmetric difference is associative
- (Identity) $R \Delta \emptyset = \emptyset \Delta R = R$ $\forall R \in \mathcal{P}(X)$ and null set, $\emptyset \in \mathcal{P}(X)$
- (Invertibility) $\forall R \in \mathcal{P}(X)$ $R \Delta R = \emptyset$

Thus, it is a group.

viii) $\langle \mathbb{Q}^*[\sqrt{2}], \cdot \rangle$ where $\mathbb{Q}^*[\sqrt{2}] = \mathbb{Q}[\sqrt{2}] - \{0\}$

- Binary operation is defined as $p.q$ is single valued and $\in \mathbb{Q}[\sqrt{2}]$ $\forall p, q \in \mathbb{Q}[\sqrt{2}]$
  Let $p = a_1 + b_1\sqrt{2}$; $q = a_2 + b_2\sqrt{2}$ $\Rightarrow p * q = pq = (a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$ $\in \mathbb{Q}[\sqrt{2}]$
- (Associativity) Multiplication is associative
- (Identity) $p1 = 1p = p$ $\forall p \in \mathbb{Q}[\sqrt{2}]$ and $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$
- (Invertibility) $\forall p (= a + b\sqrt{2}) \exists q \left(= \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}\right) \in \mathbb{Q}[\sqrt{2}]$

  such that $pq = qp = 1$

Thus, it is a group.

ix) $\langle G, * \rangle$ where $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} : a \in \mathbb{R}^* \right\}$ and $*$ = matrix multiplication

- Binary operation is defined as $p * q$ is single valued and $\in G$ $\forall p, q \in G$
  Let $p = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $q = \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \in G$, $p * q = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in G$ $\forall a, b \in \mathbb{R}^*$
- (Associativity) Multiplication is associative
- (Identity) $p \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} p = p$ $\forall p \in G$ and $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in G$
- (Invertibility) $\forall p = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}; a \in \mathbb{R}^*$ $\exists q = \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} \in G : pq = qp = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

⑥ Give an example of an abelian group with exactly 1000 elements

$\langle \mathbb{Z}_{1000}, +_{1000} \rangle$ i.e. group of $\mathbb{Z}$ mod 1000 under addition mod 1000

⑦ done after Q10

(8) Suppose that a group G has an element x such that $ax = x \quad \forall a \in G$. Show that G contains only the identity element

Given $ax = x \quad \forall a \in G, \; x \in G$.

$\Rightarrow axx^{-1} = xx^{-1}$ [x^{-1} exists by group axiom]

$\Rightarrow a = e$

Thus $\forall a \in G, \; a = e \Rightarrow G$ contains only the identity element

(9) Let G be a group and $a, b \in G$. Show that $(aba^{-1})^n = aba^{-1}$ iff $b^n = b$

$$(aba^{-1})^n = \underbrace{(aba^{-1})(aba^{-1})(aba^{-1}) \ldots (aba^{-1})}_{n\text{-times}}$$

$$= ab(a^{-1}a)b(a^{-1}a)b(a^{-1}a) \ldots ba^{-1} \quad \text{[associativity]}$$

$$= abebeb \ldots eba^{-1}$$

$$= ab^n a^{-1} \quad -(1)$$

- Given $(aba^{-1})^n = aba^{-1} \Rightarrow ab^n a^{-1} = aba^{-1}$ [using (1)]

$$\Rightarrow a^{-1}(ab^n a^{-1})a = a^{-1}(aba^{-1})a$$

$$\Rightarrow (a^{-1}a)b^n(a^{-1}a) = (a^{-1}a)b(a^{-1}a)$$

$$\Rightarrow b^n = b$$

- Given $b^n = b \Rightarrow (aba^{-1})^n = ab^n a^{-1} = aba^{-1}$ [using (1)]

QED

(10) An element $a \in G$ is called idempotent if $a^2 = a$. Show that the only idempotent element in G is the unit element

Given $a^2 = a. \quad a \in G.$

$a^2a^{-1} = aa^{-1}$ [$a^{-1} \in G$ by group axiom]

$a = e.$

Let $b \in G$ such that $b^2 = b$ and $b \neq a$. [b^{-1} exists by group axiom]

$\Rightarrow b^2b^{-1} = bb^{-1} \Rightarrow b = e = a$ which is a contradiction

Thus, the only idempotent element in G is the unit element.

⑦ Let G be a group with finite number of elements. Show that for any $a \in G$, there exists $n \in \mathbb{N}$ such that $a^n = e$

Case 1 (trivial): $a = e \Rightarrow a^n = e^n = e$ (proved)

Case 2: $a \neq e$.

Since G has a finite number of elements, $\exists\, m_1, m_2 \in \mathbb{N} \cdot a^{m_1} = a^{m_2}$

Let $m_1 > m_2$ $\quad a^{m_1} = a^{m_2}$

$\Rightarrow a^{m_1} \cdot a^{-m_2} = a^{m_2} \cdot a^{-m_2}$ $\quad [a^{-m_2}$ exists by group axiom$]$

$\Rightarrow a^{m_1 - m_2} = e$

$\Rightarrow a^n = e$ for $n = m_1 - m_2 \in \mathbb{N}$

QED

⑪ Find a solution of the equation $ax = b$ in S_3 where

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

Let $x = \begin{pmatrix} 1 & 2 & 3 \\ x_1 & x_2 & x_3 \end{pmatrix} \in S_3$ for $x_1, x_2, x_3 \in \mathbb{N}^{\leq 3}$ and $x_1 \neq x_2 \neq x_3$

Computing ax using R→L convention and comparing with b

$1 \xrightarrow{x} x_1 \xrightarrow{a} 1 \Rightarrow x_1 = 3$

$2 \xrightarrow{x} x_2 \xrightarrow{a} 3 \Rightarrow x_2 = 1$

$3 \xrightarrow{x} x_3 \xrightarrow{a} 2 \Rightarrow x_3 = 2$

$\Rightarrow x = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

⑫ If G is a group such that $a^2 = e$, $\forall a \in G$. Show that G is abelian

Is it true for $a^3 = e$, $\forall a \in G$

i) Given: $a^2 = e \quad \forall a \in G$.

$a^2 a^{-1} = e a^{-1}$ $\quad [a^{-1} \in G$ by group axiom$]$

$a = a^{-1}$ $\quad -①$

To prove: G is abelian i.e. $ab = ba \quad \forall a, b \in G$.

Let $ab = k$

$a^{-1}ab = a^{-1}k$

$b = a^{-1}k$

$b^{-1}b = b^{-1}a^{-1}k$

$e = b^{-1}a^{-1}k$

$k^{-1} = b^{-1}a^{-1}kk^{-1}$

$k^{-1} = b^{-1}a^{-1}$

Using ① $k = ba$ } $ab = ba \Rightarrow G$ is abelian
But, $k = ab$ }

QED

ii) Given: $a^3 = e$

$a^3 a^{-1} = e a^{-1}$

$a^2 = a^{-1}$ —②

Let $ab = k$. $\Rightarrow k^{-1} = b^{-1}a^{-1}$ (as shown before)

Using ② $k^2 = b^2a^2$ } $(ab)^2 = b^2a^2 \neq ab = ba \quad \forall a, b \in G$.
But $k = ab$ }

Thus., G is not abelian

(13) Show that G is abelian iff $(ab)^2 = a^2b^2 \quad \forall a, b \in G$

- Given $(ab)^2 = a^2b^2 \quad \forall a, b \in G$.
  $\Rightarrow abab = aabb$.
  $\Rightarrow a^{-1}(abab)b^{-1} = a^{-1}(aabb)b^{-1}$ [$a^{-1}, b^{-1} \in G$ by group axiom]
  $\Rightarrow ba = ab \quad \forall a, b \in G$.
  $\Rightarrow G$ is abelian
- Given G is abelian
  $\Rightarrow ab = ba \quad \forall a, b \in G$.
  $\Rightarrow a(ab)b = a(ba)b$ [operating with a on the left, b on the right]
  $\Rightarrow aabb = abab$
  $\Rightarrow a^2b^2 = (ab)^2 \quad \forall a, b \in G$.

QED

(14) Let G be a finite group with even number of elements. Show that there exists atleast one element, $a \in G$ such that $a^2 = e$ and $a \neq e$

For all elements in $G - \{e\}$, we make pairs of an element and its inverse [Note: the inverse of an element is unique and two elements cannot have the same inverse]. Since $o(G)$ is even, $G - \{e\}$ has an odd number elements. ie. atleast one element, $a \in G - \{e\}$ has been paired with itself
$\Rightarrow aa = a^2 = e$ and $a \neq e$

QED

(15) Give an example to show that the union of two subgroups may not be a subgroup

Let $G_1 = \langle \mathbb{R}^*, \cdot \rangle$. Consider subgroups $H_1 = \{2^k : k \in \mathbb{Z}\}$, $H_2 = \{5^k : k \in \mathbb{Z}\}$

But $H_1 \cup H_2$ is not a subgroup of G_1

Example: $2 \in H_1$ and $5 \in H_2$ but $2 \cdot 5 = 10 \notin H_1 \cup H_2$

i.e. closure property is violated

(16) If K is a subgroup of H and H is a subgroup of G_1, show that K is a subgroup of G_1.

Given: $H \leq G_1$ and $K \leq H$

To prove: $K \leq G_1$.

- $K \leq H \Rightarrow \forall a \in K, a \in H.$
  $H \leq G_1 \Rightarrow \forall a \in H, a \in G_1.$
  $\Rightarrow K \subseteq G_1.$ — (1)
- Let $*_{G_1}, *_H, *_K$ be the (associative) binary operation of G_1, H, K resp.
  $K \leq H \Rightarrow *_K \equiv *_H$
  $H \leq G_1 \Rightarrow *_H \equiv *_{G_1}$
  $\Rightarrow *_K \equiv *_{G_1}.$ — (2)
- Let e_{G_1}, e_H, e_K be the identity elements of G_1, H, K resp
  $K \leq H \Rightarrow e_K = e_H$
  $H \leq G_1 \Rightarrow e_H = e_{G_1}$
  $e_K = e_{G_1}.$ — (3)
- Let $a \in G_1 \Rightarrow a^{-1} \in G_1$ [by group axiom]
  If $a \in H \Rightarrow a^{-1} \in H$ [$H \leq G_1$]
  If $a \in K \Rightarrow a^{-1} \in K$ [$K \leq H$]
  Thus, $\forall a \; \exists a^{-1} \in \underbrace{K \subseteq G_1}_{\text{from (1)}}$ — (4)

K inherits the binary operation of G_1 (2), is a subset of G_1 (1) and satisfies the group axioms for the elements and the operation (3, 4)

Thus, K is a subgroup of G_1

(17) If G is an abelian group, show that $H = \{a : a \in G, a^2 = e\}$ is a subgroup of G.

Clearly, $H \subseteq G$ as $\forall a \in H, a \in G$. by definition

To prove $H \leq G$, we must prove H inherits commutativity from G under the binary operation of G. — ①

Given $ab = ba \quad \forall a, b \in G$.

$$c^2 = e \Rightarrow c = c^{-1} \quad \forall c \in H \quad — ②$$

Let $cd = k \quad c, d, k \in H$

$\Rightarrow (cd)^{-1} = k^{-1}$

$\Rightarrow d^{-1}c^{-1} = k^{-1}$

$\Rightarrow dc = k \quad$ [using ②]

$\Rightarrow dc = cd \quad \forall c, d \in H$

$\Rightarrow H$ is abelian under the binary operation of G

Thus, using ① $H \leq G$.

(18) Show that a group cannot be expressed as a union of two proper subgroups.

Let $H < G$ and $K < G$ where G is the group.

Since H, K are proper subgroups of G $\exists h \in H \setminus K$ and $\exists k \in K \setminus H$

Now, $hk \in G$ but $hk \notin H \cup K$ as closure property is violated

Thus, G cannot be expressed as a union of two proper subgroups.

(19) Give an example of a group which is not cyclic, but every proper subgroup of it is cyclic.

The group $\langle \mathbb{R}^*, \cdot \rangle$ is not cyclic.

However, each subgroup of it is of the form $\langle \{a^k : k \in \mathbb{Z}\}, \cdot \rangle$, $a \in \mathbb{R}^*$ which is cyclic with generator a

(20) Let $a, b \in G$ such that $b = xax^{-1}$ for some $x \in G$. Show $o(a) = o(b)$

Let $o(a) = n \Rightarrow a^n = e$ — ①

$o(b) = m \Rightarrow b^m = e$ — ②

To prove: $n = m$

Given: $b = xax^{-1}$

$\Rightarrow b^m = (xax^{-1})^m$

$\Rightarrow e = (xax^{-1})^m = (xax^{-1})(xax^{-1})\ldots\ldots(xax^{-1})$ (m-times) [using ②]

$\Rightarrow e = xa(x^{-1}x)a(x^{-1}x)\ldots(x^{-1}x)ax^{-1}$ [associativity]

$\Rightarrow e = xa^m x^{-1}$

$\Rightarrow x^{-1}x = e = x^{-1}xa^m x^{-1}x = a^m$

$\Rightarrow a^m = e$ — ③

But $a^n = e$ [from ①]

Let $m = nq_1 + r_1$

$a^m = e$ [from ③]

$a^{nq_1} \cdot a^{r_1} = e$

$a^{r_1} = e$

$r_1 = 0$

$m \mid n$

Let $n = mq_2 + r_2$

$a^n = e$ [from ①]

$a^{mq_2} \cdot a^{r_2} = e$

$a^{r_2} = e$

$r_2 = 0$

$n \mid m$

$m = n$.

$[n_1, r_2, q_1, q_2 \in \mathbb{Z}, \ 0 \le r_1 < n, \ 0 \le r_2 < m]$

$[\text{as } o(a) = n \le m \text{ and } a^n = e \Rightarrow r \not< n]$

QED

(21) Let $a, b \in G$. Show that $o(ab) = o(ba)$

Let $o(ab) = n \Rightarrow (ab)^n = e$ — ①

$o(ba) = m \Rightarrow (ba)^m = e$ — ②

To prove: $n = m$

From ① $(ab)^n = e$

$(ab)(ab)(ab)(ab)\ldots(ab) = e$ (n-times)

$a(ba)(ba)\ldots(ba)b = e$

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

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

$(ba)^n = e$ — ③

But $(ba)^m = e$

Let $m = nq_1 + r_1$

$(ba)^m = e$ [from ②]

$(ba)^{nq_1}.(ba)^{r_1} = e$

$(ba)^{r_1} = e$

$r_1 = 0$

$m \mid n$

Let $n = mq_2 + r_2$

$(ba)^n = e$ [from ③]

$(ba)^{mq_2}.(ba)^{r_2} = e$

$(ba)^{r_2} = e$

$r_2 = 0$

$n \mid m$.

$\left[r_1, r_2, q_1, q_2 \in \mathbb{Z} \quad 0 \le r_1 \in n \quad 0 \le r_2 < m \right]$

$\left[\text{as } o(ba) = m \le n \text{ and } (ba)^x = e \Rightarrow x \nmid n \right]$

$\Rightarrow n = m$.

QED

(12) Write all the complex roots of $x^6 = 1$. Show that they form a group under the usual complex multiplication.

Roots of unity are of the form $\exp\left(\frac{2k\pi i}{n}\right)$; $k \in \mathbb{Z} : 0 \le k < n$.

Thus, the group, U_6 consisting of the complex roots of $x^6 = 1$ are

$$U_6 = \left\{1, \exp\left(\frac{\pi i}{3}\right), \exp\left(\frac{2\pi i}{3}\right), \exp(\pi i), \exp\left(\frac{4\pi i}{3}\right), \exp\left(\frac{5\pi i}{3}\right)\right\}$$

with the binary operation = complex multiplication.

- Binary operation is defined as $a*b$ is single valued and $\in U_6$ $\forall a, b \in U_6$
- (Associativity) multiplication is associative
- (Identity) $1a = a1 = a$ $\forall a \in U_6$ and $1 \in U_6$
- (Invertibility) $\forall a \; \exists a^{-1} \in U_6 : aa^{-1} = a^{-1}a = 1$

Thus, $\langle U_6, \cdot \rangle$ is a group

(13) Let $G_1 = \{a \in \mathbb{R} : -1 < a < 1\}$. Define a binary operation $*$ on G_1 by $a * b = \frac{(a+b)}{1+ab}$ $\forall a, b \in G_1$. Show that $\langle G_1, * \rangle$ is a group.

- Binary operation is well-defined (given in Q)
- (Associativity) Let $a, b, c \in G_1$.

$a*(b*c)$

$= a * \left(\frac{b+c}{1+bc}\right)$

$= \frac{a + \left(\frac{b+c}{1+bc}\right)}{1 + \frac{a(b+c)}{1+bc}}$

$= \frac{a+b+c+ab}{1+ab+bc+ca}$.

$(a*b)*c$.

$= \left(\frac{a+b}{1+ab}\right) * c$.

$= \frac{\left(\frac{a+b}{1+ab}\right) + c}{1 + \frac{(a+b)c}{1+ab}}$

$= \frac{a+b+c+abc}{1+ab+bc+ca}$.

- (Identity) $0 * a = a * 0 = a \quad \forall a \in G$ and $0 \in G$.
- (Invertibility) $\forall a \; \exists (-a) \in G : a * (-a) = (-a) * a = 0$

Thus, $\langle G, * \rangle$ is a group.

(24) Let $\langle G, * \rangle$ be a group and $a, b \in G$. Suppose that $a^2 = e$ and $aba = b^7$. Prove that $b^{48} = e$

Given: $a^2 = e$

$aba = b^7$

To prove: $b^{48} = e$

$b^{49} \cdot b^{-1}$

$= (aba)^7 b^{-1}$

$= (aba)(aba) \ldots (aba) b^{-1}$ (7 times)

$= ab(aa)b(aa) \ldots bab^{-1}$

$= abebe \ldots bab^{-1}$

$= ab^7ab^{-1}$

$= a(aba)ab^{-1}$

$= (aa)b(aa)b^{-1}$

$= ebeb^{-1}$

$= bb^{-1}$

$= e$

QED

(25) Let $\langle G, * \rangle$ be a group such that $(ab)^{-1} = a^{-1}b^{-1} \quad \forall a, b \in G$.

Show that G is a commutative group.

Given: $(ab)^{-1} = a^{-1}b^{-1} \quad \forall a, b \in G$.

To prove: G is abelian

Let $(ab)^{-1} = k$. $\quad k \in G$.

$\Rightarrow (ab)(ab)^{-1} = (ab)k$.

$\Rightarrow e = (ab)k$

$\Rightarrow k^{-1} = ab \quad -①$

$\Rightarrow a^{-1}b^{-1} = k$.

$\Rightarrow a(a^{-1}b^{-1}) = ak$

$\Rightarrow bb^{-1} = bak$.

$\Rightarrow k^{-1} = ba. \quad -②$

[Inverse of an element is unique]

From ① and ② $ab = ba$

$\therefore G$ is abelian

(26) Prove that a group $\langle G, * \rangle$ is a commutative if $(ab)^n = a^n b^n$ for any three consecutive integer n and for all $a, b \in G$

Let the integers be $k, k+1, k+2 : k \in \mathbb{Z}^+$ i.e. $(ab)^k = a^k b^k$ $\forall a, b \in G$

To prove : $ab = ba$ $\forall a, b \in G$.

$(ab)^{k+1} = a^{k+1} b^{k+1}$

$(ab)^{k+2} = a^{k+2} b^{k+2}$.

$(ab)^{k+1} = (ab)^k ab$

$a^{k+1} b^{k+1} = a^k b^k ab$

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

$ab^k = b^k a$ — (1)

$(ab)^{k+2} = (ab)^{k+1}(ab)$

$a^{k+2} b^{k+2} = a^{k+1} b^{k+1} ab$

$a^{-(k+1)}(a^{k+2} b^{k+2}) b^{-1} = a^{-(k+1)}(a^{k+1} b^{k+1}) abb^{-1}$

$ab^k b = b^k ba$

$ab^k = b^k bab^{-1}$ — (2)

Comparing (1) and (2)

$b^k a = b^k bab^{-1}$

$b^{-k}(b^k a) b = b^{-k}(b^k bab^{-1}) b$

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

QED

① Prove that the order of a permutation on a finite set is the least common multiple of the lengths of its disjoint cycles

If σ is a permutation on a finite set, the σ can be written as a finite product of k disjoint cycles, say $\sigma = t_1 \circ t_2 \circ \dots \circ t_k$

Let the order of $\sigma = m$ and the order of $t_i = m_i$ $\forall$ cycles t_i

$\Rightarrow \sigma^m = (t_1 \circ t_2 \circ \dots \circ t_k)^m = \epsilon$ where ϵ = identity

$\Rightarrow t_1^m \circ t_2^m \circ \dots \circ t_k^m = \epsilon$ [as $t_1, t_2, \dots, t_k$ are disjoint]

$\Rightarrow t_i^m = \epsilon$ $\forall$ cycles t_i

$\Rightarrow m_i \mid m$ $\forall\, m_i$ = order of cycle t_i

$\Rightarrow m$ is the smallest term that divides m_i $\forall\, m_i$

$\Rightarrow m = \text{lcm}(m_1, m_2, \dots, m_k)$

QED

② Prove that the number of even permutations on a finite set with atleast two elements is equal to number of odd permutations on it

Let S_n be the set of permutations on a set S of cardinality $n > 1$

A_n be the set of even permutations in S_n

B_n be the set of odd permutations in S_n.

To prove: $|A_n| = |B_n|$

If there exists a bijective function, $f(x) : A_n \to B_n$, then $|A_n| = |B_n|$

Define $f(x) = tx$ $\forall x \in A_n$ where transposition, $t = (1,2) = t^{-1}$

[note: 1, 2 represent the first two elements of S]

- Checking $f(x) : A_n \to B_n$

  Since x is an even permutation $\forall x \in A_n$,

  then tx is an odd permutation and $tx \in B_n$

- Checking $f(x)$ is one-to-one $A_n \to B_n$

  Let $x_1, x_2 \in A_n$ and $f(x_1) = f(x_2) \Rightarrow tx_1 = tx_2$

  Since S_n is a group, by left-hand cancellation law, $x_1 = x_2$

- Checking $f(x)$ is onto B_n

  Let $y \in B_n$. Then $t^{-1}y \in A_n$ and $f(t^{-1}y) = t(t^{-1}y) = y$

Thus, $f(x) : A_n \to B_n$ is bijective and there exists a one-to-one correspondance between A_n and B_n $\Rightarrow |A_n| = |B_n|$

QED

(3) Let $\alpha = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 6&4&7&5&2&3&1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1&2&3&4&5&6&7 \\ 1&4&6&7&3&5&2 \end{pmatrix}$ be the elements of S_7

i) Write α as a product of disjoint cycles.

$\alpha = (1,6,3,7)(2,4,5)$

ii) Write β as a product of odd cycles

$\beta = (2,4,7)(3,6,5) = (2,4)(2,7)(3,6)(3,5)$

iii) Is β an even permutation

β can be written as a product of 4 transpositions $\Rightarrow \beta$ is an even permutation

iv) Is α^{-1} an even permutation

From (i), $\alpha^{-1} = (5,4,2)(7,3,6,1) = (5,4)(5,2)(7,3)(7,6)(7,1)$

α^{-1} can be written as a product of 5 transpositions $\Rightarrow \alpha^{-1}$ is not an even permutation

(4) Let H, K be subgroups of a group G. Prove HK is a subgroup of G iff $HK = KH$

Given: $H, K \leq G$.

To prove: $HK \leq G \Leftrightarrow HK = KH$

- Proving $HK \leq G \Rightarrow HK = KH$.

Let $h \in H$, $k \in K$. By group axiom, $h^{-1} \in H$, $k^{-1} \in K$

$h = he \in HK$; $h^{-1} = eh^{-1} \in KH$ [$e \in K \leq G$]

$k = ek \in HK$; $k^{-1} = k^{-1}e \in KH$ [$e \in H \leq G$]

$kh \in HK$; $h^{-1}k^{-1} \in KH$ [closure property]

$\Rightarrow KH \subseteq HK$ $-①$; $\Rightarrow HK \subseteq KH$. $-②$

From ① and ②, $HK = KH$

- Proving $HK = KH \Rightarrow HK \leq G$.

1) $H \leq G$, $K \leq G \Rightarrow HK \subseteq G$

2) $e \in H$, $e \in K$ $\Rightarrow e \in HK \subseteq G \Rightarrow$ identity of G = identity of $HK = e$

3) (Closure) Let $x, y \in HK$

$\exists\, h_x, h_y \in H$ and $k_x, k_y \in K$: $h_x k_x = x$ and $h_y k_y = y$

Since $HK = KH$, $\exists\, h' \in H$, $k' \in K$: $k_x h_y = h'k'$

$\Rightarrow xy = (h_x k_x)(h_y k_y) = h_x (k_x h_y) k_y = h_x h' k' k_y \in HK$

4) (Invertibility) Let $x = hk \in HK$.

$x^{-1} = k^{-1}h^{-1} \in KH = HK \Rightarrow x^{-1} \in HK$.

Thus, $HK \subseteq G$ and HK satisfies all the group axioms under the (associative) binary operation of $G \Rightarrow HK \leq G$.

QED

⑤ Show that $Z(G) = \{x \in G : xg = gx \ \forall g \in G\}$ is a subgroup of G

1) $Z(G) \subseteq G$, by definition of G

2) (Identity) $xe = ex \Rightarrow e \in Z(G)$ where e = identity in G.

3) (Closure) Let $a, b \in Z(G) \Rightarrow ax = xa$ and $bx = xb$

$\Rightarrow (ab)x = a(bx) = a(xb) = (ax)b = x(ab) \Rightarrow ab \in Z(G)$

4) (Invertibility) Let $a \in Z(G) \Rightarrow ax = xa$

$\Rightarrow a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1} \Rightarrow xa^{-1} = a^{-1}x \Rightarrow a^{-1} \in Z(G)$

Thus, $Z(G)$ is a subset of G and satisfies all the group axioms under the (associative) binary operation of $G \Rightarrow Z(G)$ is a subgroup of G.

⑥ Let G be a group. Prove $C(a) = \{x \in G : xa = ax\}$ is a subgroup of G

1) $C(a) \subseteq G$, by definition of $C(a)$

2) (Identity) $ea = ae \Rightarrow e \in C(a)$ where e = identity in G.

3) (Closure) Let $x, y \in C(a) \Rightarrow xa = ax$ and $ya = ay$

$\Rightarrow (xy)a = x(ya) = x(ay) = (xa)y = a(xy) \Rightarrow xy \in C(a)$

4) (Invertibility) Let $x \in C(a) \Rightarrow xa = ax$

$\Rightarrow x^{-1}(xa)x^{-1} = x^{-1}(ax)x^{-1} \Rightarrow ax^{-1} = x^{-1}a \Rightarrow x^{-1} \in C(a)$

Thus, $C(a)$ is a subset of G and satisfies all the group axioms under the (associative) binary operation of $G \Rightarrow C(a)$ is a subgroup of G.

⑦ See Q10(ii)

⑧ Prove that $\langle \mathbb{Q}, + \rangle$ is a non-cyclic group.

Proof by contradiction: Let $\langle \mathbb{Q}, + \rangle$ be a cyclic group with generator q

Since $q \in \mathbb{Q}$, q can be expressed as $\frac{a}{b}$ for $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$

Thus, all elements in $\langle \mathbb{Q}, + \rangle$ can be expressed as $nq = \frac{na}{b}$ for $n \in \mathbb{Z}$

Now, $\frac{q}{k} \in \mathbb{Q}$ for $k \in \mathbb{Z}^*$, but for $k \neq 1, n$, $\frac{q}{k}$ cannot be expressed as $\frac{na}{b}$.

which is a contradiction

Thus $\langle \mathbb{Q}, + \rangle$ is not a cyclic group.

(9) Prove that the intersection of any collection of subgroups of a group G is a subgroup of G.

Let $\{H_i : i \in \mathbb{Z}^+ \text{ and } H_i \leq G\}$ be any collection of subgroups of G.

Define H to be the intersection of these subgroups.

To prove: $H \leq G$.

1) $H_i \leq G$ $\forall$ subgroups $\Rightarrow H \subseteq G$.

2) (Identity) $e \in H_i \leq G$ $\forall$ subgroups $\Rightarrow e \in H$.

3) (Closure) Let $a, b \in H \Rightarrow a, b \in H_i$ $\forall$ subgroups.
$\Rightarrow ab \in H_i$ $\forall$ subgroups $\Rightarrow ab \in H$

4) (Invertibility) Let $a \in H \Rightarrow a \in H_i$ $\forall$ subgroups
$\Rightarrow a^{-1} \in H_i$ $\forall$ subgroups. $\Rightarrow a^{-1} \in H$

Thus, H is a subset of G and satisfies all the group axioms under the (associative) binary operation of $G \Rightarrow H$ is a subgroup of G

(10) Let $G = \langle a \rangle$ be a cyclic group of order n

i) Prove if H is a subgroup of G, then $|H|$ divides $|G|$

Given: $G = \langle a \rangle$ and $|a| = n$

Since subgroups of cyclic groups are cyclic, let $H = \langle a^k \rangle : k \in \mathbb{Z}^+$

Let $|H| = m \Rightarrow (a^k)^m = e \Rightarrow n \mid km$. —① [$\because |a| = n$].

Let $d = \gcd(n, k) \in \mathbb{Z}^+$

From ① $\frac{n}{d} \mid \frac{km}{d} \Rightarrow \frac{n}{d} \mid m$ —② [$\because \frac{n}{d} \nmid \frac{k}{d}$]

Also, $(a^k)^m = e$.
and $(a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$
} $km \mid \frac{nk}{d} \Rightarrow m \mid \frac{n}{d}$ — ③

From ② and ③, $m = \frac{n}{d} \Rightarrow md = n \Rightarrow m \mid n \Rightarrow |H| \mid |G|$

ii) If m is a positive integer such that $m \mid n$, then there exists a unique subgroup of G of order m

Given: $G = \langle a \rangle$ and $|a| = n$

Let $n = mk : k \in \mathbb{Z}^{\geq 0}$ [$\because m \mid n$ given]

Since subgroups of cyclic groups are cyclic, consider $H = \langle a^k \rangle$

- $|a| = n \Rightarrow a^n = e \Rightarrow a^{mk} = e \Rightarrow (a^k)^m = e \Rightarrow |H| \mid m$
- $(a^k)^{|H|} = e \Rightarrow n \mid k|H| \Rightarrow mk \mid k|H| \Rightarrow m \mid |H|$

} $|H| = m$.

Thus, there exists a subgroup of G with order $m \in \mathbb{Z}^+ : m \mid n$.

Proving uniqueness: Consider another subgroup, $X = \langle a^x \rangle$ of G_1 with order m
To prove: $H = X$ i.e. $k = x$ where k is the smallest +ve integer, s.t. $a^{km} = e$
Let $x = kq + r$ by division algorithm $[0 \leq r < k]$
$e = (a^x)^m = (a^{kq+r})^m = a^{kmq} \cdot a^{rm} = ea^{rm} = a^{rm} \Rightarrow r = 0$
Thus, $k \mid x \Rightarrow a^x \in \langle a^k \rangle = H$
If $|\langle a^x \rangle| = |\langle a^k \rangle|$, then x must $= k$ i.e. $H = X$

(11) Let G_1 be a group of order 28. Show that G_1 has a non-trivial subgroup
Using result of Q14, Assignment #1, [28 is even]
$\exists a \in G_1 : a^2 = e$. Thus a non-trivial subgroup of G_1 is $\{e, a\}$
$(\Rightarrow a = a^{-1})$

(12) Let G_1 be a group and H be a subgroup of G_1. Let $a, b \in G_1$.
Prove that $aH = bH$ if and only if $a^{-1}b \in H$

1) Proving $aH = bH \Rightarrow a^{-1}b \in H$ $[a, b \in G_1, H \leq G_1]$
$b \in bH = aH \Rightarrow \exists h \in H : b = ah \Rightarrow a^{-1}b = h \in H \Rightarrow a^{-1}b \in H$

2) Proving $a^{-1}b \in H \Rightarrow aH = bH$
Let $a^{-1}b = h \in H$
- For some $k_1 \in H$, $ak_1 \in aH \Rightarrow b(h^{-1}k_1) \in aH \Rightarrow bH \subseteq aH$
- For some $k_2 \in H$, $bk_2 \in bH \Rightarrow a(hk_2) \in bH \Rightarrow aH \subseteq bH$

$\Big\}\ aH = bH$

(13) Prove that any two left cosets of H in a group G_1 have the same cardinality
Consider two left cosets, aH and bH, of subgroup, H in a group, G_1 $[a, b \in G_1]$
Define a mapping, $\phi : H \to aH$. i.e. $\phi(h) = ah \quad \forall h \in H$
(Injective) Let $\phi(h_1) = \phi(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$.
(Surjective) By definition of aH, $\exists h \in H : \phi(h) = ah$
Thus, ϕ is a bijective mapping $H \to aH$. Similarly for bH
$\Rightarrow |H| = |aH| = |bH|$ for $a, b \in G_1$ and $H \leq G_1$

(14) Prove that the order of each element in a finite group G_1 is a divisor of $O(G_1)$
Let $a \in G_1$, order of a = order of cyclic group, $\langle a \rangle$, generated by a
Let $H = \langle a \rangle$. Since $a \in G_1$, $H \leq G_1$.
Using Lagrange theorem, order of H divides order of finite group G_1. $H \leq G_1$
$\Rightarrow$ order of a divides order of G_1 $\forall a \in G_1$

(15) Let G be a finite group and $a \in G$. Prove that $a^{o(G)} = e$.
Hence prove Fermat's Little Theorem

Let the order of $G = n$ and order of $a \in G$ = order of $\langle a \rangle = m$ i.e. $a^m = e$
From the result of the previous question, $m | n$. Let $n = mq$ for $q \in \mathbb{Z}^+$

$a^{o(G)} = a^n = a^{mq} = (a^m)^q = e^q = e$. Hence proved. — ①

Fermat's Little Theorem (proof):

Let $G = \langle \mathbb{Z}_p^*, \cdot_p \rangle$ i.e group of $\mathbb{Z}^*$ mod p under multiplication mod p
where p is a prime number. $\Rightarrow G = \{1, 2, 3, \ldots, p-1\}$

Order of $G = p-1$ and identity of G, $= 1 \pmod p$

From ① $\forall a \in G$, $a^{p-1} = 1 \pmod p$

QED

(16) Prove that every group of order less than 6 is commutative

1) Every group of prime order is cyclic and hence abelian
Thus groups with order 2, 3, 5 are commutative
2) Group of order one is trivially abelian as it contains only the identity
3) Let G be a group of order 4 and $\exists x, y \in G$ such that $x \neq y \neq e$
Let G be non-abelian
- $xy \neq e$ and $yx \neq e$ (x and y don't commute and $y \neq x^{-1}$)
- $xy \neq x$ and $yx \neq x$ ($\because y \neq e$)
- $xy \neq y$ and $yx \neq y$ ($\because x \neq e$)

$\Rightarrow G$ has 5 distinct elements $\{e, x, y, xy, yx\}$ which is a contradiction
$\Rightarrow xy$ must $= yx$ in G.

Thus, every group of order less than 6 is commutative

(17) Prove that $Z(G)$ is a normal subgroup of G

$Z(G) = \{x \in G : xg = gx \ \forall g \in G\}$.

1) $Z(G)$ is a subgroup of G (proved in Q5)
2) To prove $Z(G)$ is a normal subgroup i.e $aZ(G) = Z(G)a$ for $a \in G$.

Let $p \in aZ(G) \Rightarrow p = ax = xa \in Z(G)a$ for $x \in Z(G)$ and $a \in G$
$\therefore aZ(G) \subseteq Z(G)a$ — ①

Let $p \in Z(G)a \Rightarrow p = xa = ax \in aZ(G)$ for $x \in Z(G)$ and $a \in G$.
$\therefore Z(G)a \subseteq aZ(G)$ — ②

From ① and ② $aZ(G) = Z(G)a$.

Thus $Z(G)$ is a normal subgroup

(18) Let H and K be finite subgroups of a group G. Prove $|HK| = \frac{|H||K|}{|H \cap K|}$

$HK = \{hk \mid h \in H, k \in K\}$

HK can have atmost $|H||K|$ elements if $H \cap K = \emptyset$

For $H \cap K \neq \emptyset$, there may be distinct $h_1, h_2 \in H$, $k_1, k_2 \in K$ and $h_1 k_1 = h_2 k_2$.

$\forall t \in H \cap K$, $hk = (ht)(t^{-1}k) \in HK$.

Thus, every group element in HK is represented by atleast $|H \cap K|$ products

For $h_1 k_1 = h_2 k_2 = t \in HK$, $t = h_1^{-1} h_2 \in H$ and $t = k_2 k_1^{-1} \in K$. $\Rightarrow t \in H \cap K$

Thus, each element in HK is represented by exactly $|H \cap K|$ products

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

(19) Let H be a subgroup of a group G such that $[G : H] = 2$.
Prove that H is a normal subgroup of G.

Since $[G : H] = 2$, the two distinct cosets are $H = eH$ and $G - H$

Let $a \in G$.

Case 1: $a \in H \Rightarrow aH = H = Ha$.

Case 2: $a \in (G - H) \Rightarrow aH = G - H = Ha$ (since there are only two cosets)

Thus, $aH = Ha$ $\forall a \in G$. $\Rightarrow H$ is a normal subgroup of G.

(20) Find all subgroups of S_3. Show that the union of any two non-trivial distinct subgroups of S_3 is not a subgroup of S_3

$S_3 = \{\underset{\sigma_0}{(1)}, \underset{\sigma_1}{(1,2)}, \underset{\sigma_2}{(1,3)}, \underset{\sigma_3}{(2,3)}, \underset{\sigma_4}{(1,2,3)}, \underset{\sigma_5}{(1,3,2)}\}$

Subgroups of S_3 (Non-trivial, distinct) $= \{\sigma_0, \sigma_1\}, \{\sigma_0, \sigma_2\}, \{\sigma_0, \sigma_3\}, \{\sigma_0, \sigma_4, \sigma_5\}$

Order of $S_3 = 6$; Order of any two non-trivial distinct subgroup's union $\neq$

By Lagrange Theorem, order of a subgroup divides the order of a finite group.

Since $4 \nmid 6$ and $5 \nmid 6$, the union of any 2 non-trivial distinct subgroups of S_3 is not a subgroup of S_3