SC421: Introduction to Modern Algebra **Assignment 1** **Jan 15, 2025**
DA-IICT, B.Tech, winter 2024

1. In the following determine whether the systems described are groups. If they are not, point out which of the Group axioms fail to hold.

   (a) G = set of all integers, $a * b = a - b$.
   soln:
   This is not a group. The given operation is not associative.
   $a-(b-c) = (a-b)+c \neq (a-b)-c$. Also there is no identity element in $\mathbb{Z}$ w.r.t the given operation.
   $a - e = a \Rightarrow e = 0,$ and $e - a = a \Rightarrow e = 2a$.

   (b) G = set of all positive integers, $a * b = ab$ the usual product of integers.
   soln:
   This is not a group because the multiplicative inverse of every positive integers doesn't exist.

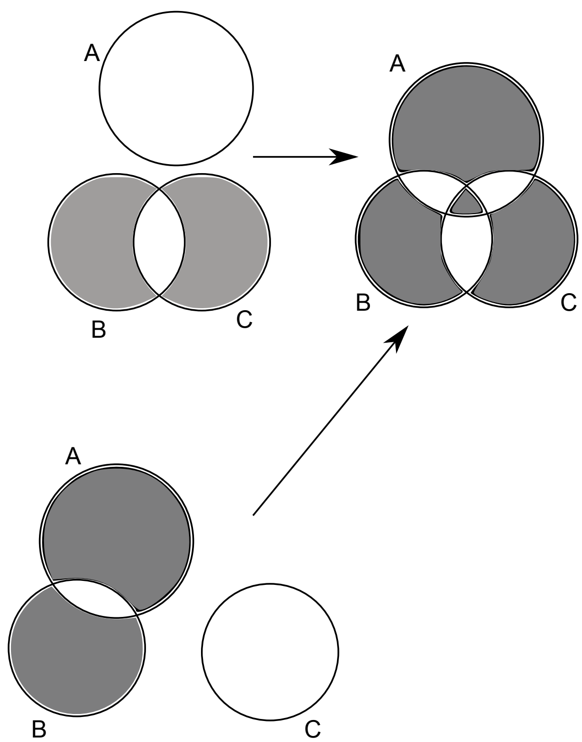
   (c) G = set of all rational numbers with odd denominators, $a * b = a + b$ the usual addition.
   soln:
   This is a group. The non-trivial property to verify is closure. Others are trivial. let $a = \frac{p}{q}, b = \frac{r}{s} \in G$. Then $a + b = \frac{ps+qr}{qs}$. qs is odd since q and s are odd and it cannot have an even factor.

   (d) Let S be a set. Which of the following is a group?
   (i) $\langle \mathcal{P}(S), \cup \rangle$, (ii) $\langle \mathcal{P}(S), \cap \rangle$, (iii) $\langle \mathcal{P}(S), \Delta \rangle$, where $A\Delta B = A \cup B \backslash A \cap B$
   soln:
   (i) For $A, B \in \mathcal{P}(S)$, $A \cup B \in \mathcal{P}(S)$. Hence $\mathcal{P}(S)$ is closed under $\cup$.
   Set union is an associative operation.
   $\phi \cup A = A \cup \phi = A, \forall A \in \mathcal{P}(S)$. So ϕ acts as the identity element with respect to $\cup$ in $\mathcal{P}(S)$.
   However for any $A \in \mathcal{P}(S)$ we can't find a subset of S whose union with A will give the empty set.
   Hence $\langle \mathcal{P}(S), \cup \rangle$ is not a group.

   (ii) $\mathcal{P}(S)$ is closed under $\cap$.
   $\cap$ is associative.
   The set S acts as the identity with respect to $\cap$ in $\mathcal{P}(S)$.
   However for any $A \in \mathcal{P}(S)$ we can't find a $B \in \mathcal{P}(S)$ such that $A \cap B = S$.
   Hence $\langle \mathcal{P}(S), \cap \rangle$ is not a group.

   (iii) $A\Delta B$ is some subset of S. By definition $\mathcal{P}(S)$ is a collection of all possible subsets of S. So $A\Delta B \in \mathcal{P}(S)$, $\forall$ A, $B \in \mathcal{P}(S)$. So $\mathcal{P}(S)$ is closed under Δ.
   The operation Δ is associative. This is easily seen using a venn diagram for three subsets A, B and C. $B\Delta C$ is represented by the shaded region of set B and set

C. Finally $A\Delta(B\Delta C)$ is shown as the shaded region of the three sets. It is clear that only those elements remain which occur exactly in one of the three sets or in all the three sets.
It is clear from the figure we arrive at the same final set if we construct $(A\Delta B)\Delta C$.



The empty set ϕ acts as the identity element with respect to Δ.

$$A\Delta\phi = A \cup \phi \backslash A \cap \phi = A\backslash\phi = A$$

Every subset is the inverse of itself with respect to Δ.

$$A\Delta A = A \cup A\backslash A \cap A = A\backslash A = \phi$$

which as mentioned above acts as the identity. So the set $\mathcal{P}(S)$ satisfies all the group axioms under Δ. Hence it is a group under Δ.

2. Let $G = \{\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} | x, y \in \mathbb{R}\}$. Let the binary operation on G be the matrix multiplication.

   (a) Is G closed under multiplcation ?
   soln:
   Consider $\begin{pmatrix} x_1 & 0 \\ y_1 & 0 \end{pmatrix}$ and $\begin{pmatrix} x_2 & 0 \\ y_2 & 0 \end{pmatrix}$ in G.

   $$\begin{pmatrix} x_1 & 0 \\ y_1 & 0 \end{pmatrix}\begin{pmatrix} x_2 & 0 \\ y_2 & 0 \end{pmatrix} = \begin{pmatrix} x_1x_2 & 0 \\ y_1y_2 & 0 \end{pmatrix} \in G$$

   So G is closed under multiplication.

(b) Find a matrix $E \in G$ such that $AE = A, \forall A \in G\}$.
The matrix $\begin{pmatrix} 1 & 0 \\ b & 0 \end{pmatrix}$ is a possibility for E. We may take $b = 0$.

(c) Is $EA = A, \forall A \in G$?
soln:
$EA = \begin{pmatrix} 1 & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} x & 0 \\ bx & 0 \end{pmatrix}$
$\therefore \quad EA \neq A, \forall\ A \in G$

(d) Is G a group?
soln:
G is not a group since no element in G acts as the identity according to the Group Axioms.

(e) Show that in a group G, $a * e = a, \forall a \in G \quad \implies \quad e * a = a$
soln:
Here we will assume all the group axioms to be valid except the axiom for the identity element.
$a * e = a \ \ \forall \ \ a \in G$
$\therefore \quad a^{-1} * e = a^{-1}$
$\therefore \quad a^{-1} * e * a = a^{-1} * a = e$
$\therefore \quad a * a^{-1} * e * a = a * e = a$
$\therefore \quad e * e * a = e * a = a$
So $a * e = a \implies \ e * a = a$ when G is a group.

3. (a) A permutation is a one-one mapping of a set of n natural numbers onto itself. Justify that the set of all permutations on n objects denoted as S_n forms a group under the operation of composition of permutations.
soln:
Consider the set of integers $N = \{1, 2, 3, ..., n\}$.
Let f and g be two permutations on N. Then f and g are one one and onto on N.
So $h = f \circ g$ is also one one and onto. Hence S_n is closed under composition of permutations.
The composition of functions is associative since
$h \circ (f \circ g)(a) = h(f(g(a)))$ and $(h \circ f) \circ g(a) = h(f(g(a)))$ for any $a \in N$.
The identity permutation given by the function $e(a) = a \ \forall a \in N$ is the identity element w.r.t composition. If f is any permutation then $f(e(a)) = f(a)$ and $e(f(a)) = f(a)$. So

$$f \circ e = e \circ f = f$$

Every one-one and onto function has an inverse function. The inverse function acts as the inverse permutation of a given permutation. Hence the collection of all permutations S_n forms a group under the operation of composition.

(b) Consider the set $\{1, 2, 3\}$. Consider the two permutations $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ of S_3 the permutation group on three elements. Write down all the elements of this group using composites of σ and τ. Work out the group table .

soln

$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

$\sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e = \tau^2$, $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Therefore the six elements of S_3 are $\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$.

Verify that $\sigma\tau = \tau\sigma^2$ and $\sigma^2\tau = \tau\sigma$. The group table is

	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

4. (a) Prove that a group of order 4 have to be abelian.

   soln:

   Let $G = \{e, a, b, c\}$ where e is the identity. The only non-trivial product where we have to check commutativity is $ab = c$ or permutations of the symbols a, b, c in this equation.

   (Note: If any of a, b, c is replaced by e in the above eqn. then the product has to be commutative by the def of identity and inverse elements.)

   If $ba = a, \quad \text{or}, \quad b$ then either $b = e$ or $a = e$ which is not true.

   If $ba = e$ then $ab = e$ which contradicts the above eqn.

   Therefore the only possibility is $ba = c \Rightarrow G$ is abellian.

   (b) Write down all possible group table of order 4.

   soln:

   To make the group table we observe that if a and c pair up as inverses then b is its own inverse.

   The other possibility is that every element is its own inverse. Now based on the discussion in part (a) and using the fact that each row and each column of a group table contains an element exactly once, we can fill up the group table for the two cases uniquely.

$*$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

5. Let $G = \{(a, b) | a, b \in \mathbb{Q}\}$ and $G^* = G - \{(0, 0)\}$.

(a) Let the binary operation in G^* be defined as $(a_1, b_1) \times (a_2, b_2) = (a_1a_2, b_1b_2)$. Is G^* along with this binary operation a group?
soln:
G^* is not closed under the given group operation. Elements like $(a, 0); a \neq 0$ and $(0, b); b \neq 0$ belongs to G^* but $(a, 0) \times (0, b) = (0, 0) \notin G^*$. Hence G^* is not a group under the given operation.

(b) Now let the binary operation be defined as $(a_1, b_1) \times (a_2, b_2) = (a_1a_2 + 2b_1b_2, a_1b_2 + b_1a_2)$. Is G^* along with this binary operation a group?
soln:
We have to first verify whether G^* is closed under the given operation. Let (a_1, b_1) and $(a_2, b_2) \in G^*$ To ensure that $(a_1, b_1) \times (a_2, b_2) \in G^*$ we must ensure that $(a_1, b_1) \times (a_2, b_2) = (a_1a_2 + 2b_1b_2, a_1b_2 + b_1a_2) \neq (0, 0)$.
Let if possible the product be $(0, 0)$.
Then $a_1a_2 + 2b_1b_2 = 0$ and $a_1b_2 + b_1a_2 = 0$.
Suppose we know (a_1, b_1). Then we can treat the above equations as a system of two linear equations to evaluate (a_2, b_2) as follows:

$$\begin{pmatrix} a_1 & 2b_1 \\ b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

This system will have a non-zero solution only if the determinant of the coeficient matrix is 0, i.e , $a_1^2 - 2b_1^2 = 0$.
This will happen only if $a_1/b_1 = \sqrt{2}$ or $a_1 = b_1 = 0$.
G^* doesn't contain $(0, 0)$ and $a_1/b_1 \neq \sqrt{2}$ since $a_1, b_1 \in \mathbb{Q}$. So the only possible solution for (a_2, b_2) is $(0, 0)$. So the product of elements of G^* is not (0, 0).
$\therefore$ G^* is closed under the given operation.
The product is associative (check).
$(1, 0)$ is the identity element (verify).
Let us find inverse of $(a, b) \in G^*$. Let the inverse be (x, y).
Then $ax + 2by = 1$ and $ay + bx = 0$.

$$\therefore \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

The unique solution to these system of equations is $\left(x = \frac{a}{a^2-2b^2}, y = \frac{-b}{a^2-2b^2}\right)$ since $a^2 - 2b^2 \neq 0$.
Hence G^* is a group with this operation.

(c) Redefine G^* so that G^* along with the binary operation in part **(a)** forms a group.
soln:
If we modify the set G^* as $G^* = \{(a, b) | a, b \in \mathbb{Q}^*\}$ then G^* forms a group under the multiplication as defined in part (a).

6. If G is a group of even order , prove that it has an element $a \neq e$ such that $a^2 = e$.
soln:
Every element in a group has an inverse. An element and its inverse pairup to make inverses of each other.

If we collect elements which are not its own inverse we get an even number of group elements.
The identity in a group is its own inverse. So we have collected an odd number of elements. So the number of elements left in the group which are its own inverse is odd.

7. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo 2 and the determinant is non zero. Prove that G is a group of order 6 under the operation of matrix multiplication.
soln:
The only matrices with $ad - bc \neq 0$ in G are
$a_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$
$a_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad a_4 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad a_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$
a_0 is the identity and matrix multiplication is associative.
We have to check for closure.
Determinant of a product of matrices is equal to the product of the determinants. Since the determinant of any matrix in G is 1 or $-1 \equiv 1 (\text{mod } 2)$ determinant of any of products will also be 1. So the product will be one of the above six matrices.
Now we perform the Group multiplication and verify that each element has an inverse.
$a_1^2 = a_2^2 = a_3^2 = a_0 = \mathbb{1}$
$a_4 a_5 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\text{mod} 2) = a_0,$
$a_5 a_4 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\text{mod} 2) = a_0$
The Group table is

$*$	a_0	a_1	a_2	a_3	a_4	a_5
a_0	a_0	a_1	a_2	a_3	a_4	a_5
a_1	a_1	a_0	a_4	a_5	a_2	a_3
a_2	a_2	a_5	a_0	a_4	a_3	a_1
a_3	a_3	a_4	a_5	a_0	a_1	a_2
a_4	a_4	a_3	a_1	a_2	a_5	a_0
a_5	a_5	a_2	a_3	a_1	a_0	a_4