MTH 101 - Symmetry
Assignment 5

Group Theory

1. For a positive interger n, let $I_n = \{0, 1, 2, \cdots, n-1\}$. Define a binary operation, $\oplus_n$ = *addition modulo n* on I_n as follows:
$$x \oplus_n y = \begin{cases} x + y & \text{if } 0 \leq x + y < n, \\ x + y - n & \text{if } x + y \geq n, \end{cases}$$
   (a) Prove that $(I_n, \oplus_n)$ is a group. Denote this group by $\mathbb{Z}_n$. Show that $\mathbb{Z}_n$ is a cyclic group.
   (b) If m divides n, show that $\mathbb{Z}_n$ contains a subgroup of order m. Does $\mathbb{Z}_n$ contain more than one subgroup of order m.
   (c) Find all the subgroups of each of the groups $\mathbb{Z}_4, \mathbb{Z}_7, \mathbb{Z}_{12}$.
   (d) Let H be the subgroup of $\mathbb{Z}_{12}$ generated by the element 8. Determine the sets xH for $x \in Z_{12}$.
   (e) Make a list of those elements of $\mathbb{Z}_{12}$ which generate $\mathbb{Z}_{12}$. Answer the same question for $\mathbb{Z}_5$ and for $\mathbb{Z}_9$.
2. Let D_4 be the group of bijections of the set of vertices of a square to itself. Let H be a proper subgroup of D_4 of order 2. Determine the sets $(1234)H$ and $H(1234)$.
3. Let G be a group of prime order. Prove that G is cyclic.
4. Let x and g be two elements of a group G. Show that the elements x and gxg^{-1} have the same order. Now prove that for all $x, y \in G$, order of xy is equal to order of yx.
5. Define an operation $\circ_n$ = *multiplication modulo n* on the set $I_n^{\times} = \{1, 2, \cdots, n-1\}$ by:
$$x \circ_n y = \begin{cases} xy & \text{if } 0 \leq xy < n, \\ xy - n & \text{if } xy \geq n, \end{cases}$$
   Can $(I_n^{\times}, \circ_n)$ be a group ?
   (a) Which of the following sets form a group under *multiplication modulo 14*
$$\begin{array}{ll} \{1, 3, 5\}, & \{1, 3, 5, 7\} \\ \{1, 7, 13\}, & \{1, 9, 11, 13\}. \end{array}$$
   (b) Verify that each of the sets
$$\{1, 3, 7, 9, 13, 17, 19\},$$
$$\{1, 3, 7, 9\},$$
$$\{1, 9, 13, 17\}$$
   forms a group under *multiplication modulo 20.*
   (c) Let $U_n = \{x \in I_n^{\times} : g.c.d(x, n) = 1\}$. Prove that $(U_n, \circ_n)$ is a group. Work out the multiplication table for $(U_{15}, \circ_{15})$ and find the order of each element in $(U_{15}, \circ_{15})$.

<u>Matrices</u>

1. Let $M_n(\mathbb{R})$ be the set of all $n \times n$ matrices with entries from $\mathbb{R}$. Let $C^{\mathbf{r}}_{c\mathbf{r}} : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ be a function that scales the $\mathbf{r}^{th}$ column vector of the matrix by c and maps the other column vectors to themselves. Then given a matrix $A \in M_n(\mathbb{R})$, determine the matrix $C^{\mathbf{r}}_{c\mathbf{r}}(A)$. Check that $C^{\mathbf{r}}_{c\mathbf{r}}(A) = AC^{\mathbf{r}}_{c\mathbf{r}}(I_n)$.

2. Let $C^{\mathbf{k}}_{\mathbf{k}+c\mathbf{r}} : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ be the function that replaces the $\mathbf{k}^{th}$ column vector of the matrix with the $\mathbf{k}^{th}$ column vector of the matrix plus c times the $\mathbf{r}^{th}$ column vector of the matrix and maps the other column vectors to themselves. Then given a matrix $A \in M_n(\mathbb{R})$, determine the matrix $C^{\mathbf{k}}_{\mathbf{k}+c\mathbf{r}}(A)$ and show that $C^{\mathbf{k}}_{\mathbf{k}+c\mathbf{r}}(A) = AC^{\mathbf{k}}_{\mathbf{k}+c\mathbf{r}}(I_n)$.

3. Let $C^{\mathbf{r}}_{\mathbf{s}} : M_n(\mathbb{R}) \to M_n(\mathbb{R})$ be the function that interchanges the $\mathbf{r}^{th}$ column vector of the matrix with the $\mathbf{s}^{th}$ column vector of the matrix and maps the other columns vectors to themselves. Then given a matrix $A \in M_n(\mathbb{R})$, determine the matrix $C^{\mathbf{r}}_{\mathbf{s}}(A)$ and show that $C^{\mathbf{r}}_{\mathbf{s}}(A) = AC^{\mathbf{r}}_{\mathbf{s}}(I_n)$.

4. Let $D = (d_{ij})$ be an $n \times n$ diagonal matrix. Let A be a $n \times m$ matrix. Compute AD. Show that D can be written as the product of the matrices $C^{\mathbf{r}}_{c\mathbf{r}}(I_n)$ with $c \in \mathbb{R}$ and $1 \leq r \leq n$.

5. Let $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 5 \\ 3 & 5 & 8 \end{pmatrix}$ Using the operations $C^{\mathbf{r}}_{c\mathbf{r}}$, $C^{\mathbf{r}}_{\mathbf{s}}$ and $C^{\mathbf{k}}_{\mathbf{k}+c\mathbf{r}}$, prove that A is not invertible.

Note: To determine an $m \times n$ matrix $A = (a_{ij})$, one has to explicitly determine the entries a_{ij}.