MATH 306 – SOLUTIONS OF HOMEWORK ASSIGNMENT I

1. Since $\langle G, * \rangle$ is a group, $a*x = b$ has unique solution for any element $a, b \in G$. Therefore, each element appears only one times in each row and column. By this fact and the property **a.**, we can see that 0 is the identity element of the binary operation $*$. Let a_{ij} represent the ith row and jth column in the multiplication table. Again using the above fact, $a_{12} = a_{21} = 3$. Since the binary operation $*$ is associative in G and by the property **b.**, $1 * 3 = 1 * (1 * 2) = (1 * 1) * 2 = 0 * 2 = 2$; it means that $a_{13} = 2$. Similarly, we can obtain other entries in the multiplication table:

$1 * 4 = 5$ by property **a.**
$1 * 5 = 1 * (1 * 4) = (1 * 1) * 4 = 4$
$1 * 6 = 7$ by property **a.**
$2 * 1 = 3$ by property **a.**
$2 * 3 = 2 * (2 * 1) = (2 * 2) * 1 = 0 * 1 = 1$
$2 * 6 = 2 * (2 * 4) = (2 * 2) * 4 = 0 * 4 = 4$
$3 * 1 = (2 * 1) * 1 = 2 * (1 * 1) = 2 * 0 = 2$
$3 * 2 = (1 * 2) * 2 = 1 * (2 * 2) = 1 * 0 = 1$
$4 * 5 = (1 * 5) * 5 = 1 * (5 * 5) = 1 * 0 = 1$
$4 * 6 = 4 * (4 * 2) = (4 * 4) * 2 = 0 * 2 = 2$
$5 * 1 = (4 * 1) * 1 = 4 * (1 * 1) = 4 * 0 = 4$
$5 * 4 = (1 * 4) * 4 = 1 * (4 * 4) = 1 * 0 = 1$
$5 * 6 = (3 * 6) * 6 = 3 * (6 * 6) = 3 * 0 = 3$
$6 * 2 = (4 * 2) * 2 = 4 * (2 * 2) = 4 * 0 = 4$
$6 * 4 = 6 * (6 * 2) = (6 * 6) * 2 = 0 * 2 = 2$

The remainders are as below because they are only possibilities.

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

Note that the multiplication table of a binary operation $*$ on G satisfying the properties **a.**, **b.**, **c.** is obtained by a unique way. Hence, there is one and only one binary operation on G satisfying these properties.

2. Remember that a subset H of a group G is a subgroup if and only if $H \neq \emptyset$ and for all $x, y \in H$, $xy^{-1} \in H$.

Let $HK := \{hk \mid h \in H \text{ and } k \in K\}$. Note that $HK \subseteq G$ and $HK \neq \emptyset$ because $H, K \leq G$ implies that the identity element e of G is also the identity element of H and K; so $e = ee \in HK$. Let $h_1k_1, h_2k_2 \in HK$. Then

$$\begin{aligned} h_1k_1(h_2k_2)^{-1} &= h_1k_1(k_2^{-1}h_2^{-1}) \\ &= h_1(k_1k_2^{-1})h_2^{-1} \\ &= h_1h_2^{-1}(k_1k_2^{-1}) \text{ since } G \text{ is an abelian group.} \end{aligned}$$

Since H and K are subgroups of G, $h_1h_2^{-1} \in H$ and $k_1k_2^{-1} \in K$. Thus, $h_1k_1(h_2k_2)^{-1} \in HK$. Hence, HK is a subgroup of G.

3. Suppose that G has a finite number of subgroups. If G had an element g of infinite order, then G would have infinitely cyclic subgroups $\langle g\rangle, \langle g^2\rangle, \ldots$. But this would contradict with the assumption. Thus, every element of G has finite order. By assumption, G has a finite number of cyclic subgroups. Let k be the total number of distinct cyclic subgroups. The order of each cyclic group is equal to the order of its generators. Since every element of G has finite order, all cyclic subgroups have finite order. Let n be the largest order. Since $G = \bigcup_{g\in G}\langle g\rangle$, $|G| = |\bigcup_{g\in G}\langle g\rangle| \leq kn < \infty$. Hence, G is a finite group.

4. Note that $\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \end{bmatrix}$. Thus the matrix transforms $\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}$ into $\begin{bmatrix} 1 & 2 & 3 \end{bmatrix}$. So we can represent $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ by $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1$.

Similarly, $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ is represented by $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$,

$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ is represented by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$,

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ is represented by $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$,

$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ is represented by $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$,

$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ is represented by $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$.

These are elements of S_3. Since S_3 is a group under permutation multiplication, these six matrices form a group under matrix multiplication.

5. **a.** Let $\sigma := (1457)$. Then $\sigma^2 = (15)(47)$, $\sigma^3 = (1754)$, and $\sigma^4 = 1$. Therefore, the order of σ is 4.

b. A cyclic of length n has order n.

c. $\sigma^2 = (273)$, $\sigma^3 = (45)$, $\sigma^4 = (237)$, $\sigma^5 = (273)(45)$, $\sigma^6 = 1$. So, the order of σ is 6. Now, consider τ. $\tau^2 = (37)(58)$, $\tau^3 = (14)(3875)$, $\tau^4 = 1$. Then the order of τ is 4.

d. Call the permutations given in the exercises σ, τ and γ, respectively. Then their cycle decompositions are $\sigma = (18)(364)(57)$, $\tau = (134)(26)(587)$, and $\gamma = (13478652)$. By calculations, $\sigma^6 = 1$, $\tau^6 = 1$ and $\gamma^8 = 1$.

e. The order of a permutation is the least common multiple of the length of the cycles in its cycle decomposition.