**Prof. Alexandru Suciu**

**MATH 3175** **Group Theory** **Spring 2024**

# Solutions for Homework 1

---

**1.** Write down all the possible multiplication tables on the set $S = \{0, 1\}$. In each case, determine whether the resulting magma $(S, *)$ has (one or more or none) of the following properties:

(i) The operation $*$ is associative (so that $(S, *)$ is a *semigroup*).

(ii) The operation $*$ has a (two-sided) identity element (so that $(S, *)$ is a *unital magma*).

(iii) The operation $*$ has the cancellation property (so that the multiplication table is a *Latin square*).

(iv) $(S, *)$ is a *group*.

| | |
|---|---|
| $\begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix}$ | The operation is associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 0 & 0 \\ 1 & 0 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 0 & 0 \\ 0 & 1 \end{matrix}$ | The operation is associative, has identity 1, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 1 \\ 0 & 0 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 0 \\ 1 & 0 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 0 \\ 0 & 1 \end{matrix}$ | The operation is associative, has identity 1, it is a Latin square, $S$ is a group. |
| $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$ | The operation is associative, has identity 0, it is a Latin square, $S$ is a group. |
| $\begin{matrix} 0 & 1 \\ 0 & 1 \end{matrix}$ | The operation is associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 0 & 0 \\ 1 & 1 \end{matrix}$ | The operation is associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 1 \\ 0 & 1 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}$ | The operation is not associative, has no identity, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}$ | The operation is associative, has identity 0, not a Latin square, $S$ is not a group. |
| $\begin{matrix} 1 & 1 \\ 1 & 1 \end{matrix}$ | The operation is associative, has no identity, not a Latin square, $S$ is not a group. |

**2.** Consider the two binary operations on the set $S = \{1, \dots, 6\}$ given by the following multiplication tables (which are, in fact, reduced Latin squares):

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 3 | 4 | 5 | 6 | 1 |
| 3 | 6 | 1 | 2 | 4 | 5 |
| 4 | 1 | 5 | 6 | 2 | 3 |
| 5 | 4 | 6 | 3 | 1 | 2 |
| 6 | 5 | 2 | 1 | 3 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 3 | 1 | 5 | 6 | 4 |
| 3 | 1 | 2 | 6 | 4 | 5 |
| 4 | 5 | 6 | 1 | 2 | 3 |
| 5 | 6 | 4 | 2 | 3 | 1 |
| 6 | 4 | 5 | 3 | 1 | 2 |

Which (if any) of these binary operations gives $S$ the structure of a group? Prove your answer.

The first table is a (self-indexing) Latin square that does not correspond to any group, since the corresponding operation $*$ on $S$ is not associative. For instance, $(3 * 2) * 5 = 6 * 5 = 3$, whereas $3 * (2 * 5) = 3 * 6 = 5$.

For the second table, one may verify directly that the corresponding operation $*$ on $S$ is associative (for instance, $(3 * 2) * 5 = 1 * 5 = 5$ and $3 * (2 * 5) = 3 * 6 = 5$, etc), has identity equal to 1, and each element has an inverse ($1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$, $5^{-1} = 6$, and $6^{-1} = 5$), and therefore $(S, *, 1)$ is a group (in fact, an abelian group).

Alternatively, one may note that the second table corresponds to the Cayley table of the (additive) cyclic group $(\mathbb{Z}_6, +, [0]_6)$, under the bijection $\{1, 2, 3, 4, 5, 6\} \leftrightarrow \{[0]_6, [2]_6, [4]_6, [3]_6, [5]_6, [1]_6\}$.

**3.** Let $G$ be the set of all $2 \times 2$ matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

with $a, b \in \mathbb{R}$ and $a \neq 0$.

(i) Show that $G$ forms a group under matrix multiplication.

Totality: Let $a \neq 0$ and $c \neq 0$; then

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} ac & ad + b \\ 0 & 1 \end{pmatrix}.$$

Since $ac \neq 0$, this matrix belongs to $G$.

Associativity: Matrix multiplication is associative.

Identity: Taking $a = 1$ and $b = 0$, we see that the $2 \times 2$ identity matrix belongs to $G$

Inverses:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{pmatrix}.$$

Since $a^{-1} \neq 0$, this matrix belongs to $G$.

Thus, $G$ is a group.

(ii) Find all elements of $G$ that commute with $\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$.

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \text{ if and only if } \begin{pmatrix} 3a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3a & 3b \\ 0 & 1 \end{pmatrix},$$

which only happens if $b = 3b$, that is, $b = 0$.

**4.** Let $G = \{x \in \mathbb{R} \mid x > 0 \text{ and } x \neq 1\}$. Define an operation $*$ on $G$ by $x * y = x^{\ln y}$ for all $x, y \in G$. Show that $(G, *)$ is an abelian group.

Totality: Since $x > 0$, we also have $x^{\ln y} > 0$. Moreover, since $y \neq 1$, we have that $\ln y \neq 0$, and hence $x^{\ln y} \neq 1$. This shows that $x * y \in G$.

Associativity: $x * (y * z) = x^{\ln(y*z)} = x^{\ln(y^{\ln z})} = x^{(\ln z)(\ln y)} = (x^{\ln y})^{\ln z} = (x * y) * z$.

Identity is $e$ (the base of natural logarithms): $e * x = e^{\ln x} = x$ and $x * e = x^{\ln e} = x^1 = x$.

Inverses: $x^{-1} = e^{1/\ln(x)}$. Indeed, $x * (e^{1/\ln(x)}) = x^{\ln(e^{1/\ln(x)})} = x^{1/\ln(x)} = e$, since $\ln(x^{1/\ln(x)}) = (1/\ln(x)) \cdot \ln(x) = 1 = \ln(e)$.

Commutativity: $\ln(x * y) = \ln(x^{\ln y}) = \ln(y)\ln(x) = \ln(x)\ln(y) = \ln(y^{\ln x}) = \ln(y * x)$, and thus $x * y = y * x$.

**5.** Let $G$ be a finite group with an even number of elements and with identity $e$. Show that there must exist an element $a \in G$ such that $a \neq e$ and yet $a^2 = e$.

Since $|G|$ is even, $G \neq \{e\}$, and so there must be an element $a_1 \in G$ such that $a_1 \neq e$. If $a_1^{-1} = a_1$, then $a_1^2 = e$ and $a = a_1$ is the desired element. Otherwise, again since $|G|$ is even, there must be an element $a_2 \in G$ such that $a_2 \notin \{e, a_1, a_1^{-1}\}$. If $a_2^{-1} = a_2$, then $a_2^2 = e$ and $a = a_2$ is the desired element. Otherwise, we keep going, and at some point, since $|G|$ is finite, we reach an index $n$ such that either $a_n^{-1} = a_n$, that is $a_n^2 = e$, and so $a = a_n$ is the desired element, or $G = \{e, a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$—which cannot happen, since $|G|$ is even. This proves the claim.