

EE2302 Foundations of Information and Data Engineering

Assignment 9 (Solution)

1.

a) It is not a group, since it violates the closure property. For example, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, whose determinant is not equal to 1.

b) It is a group. It is not Abelian, since for matrices, $AB \neq BA$ in general.

2. Totally, there are **four** possible Cayley's tables, as shown below:

*	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>e</i>

*	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>	<i>e</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>e</i>	<i>a</i>

*	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>e</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>e</i>	<i>a</i>	<i>b</i>

*	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>e</i>	<i>e</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>c</i>	<i>e</i>	<i>b</i>
<i>b</i>	<i>b</i>	<i>e</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>b</i>	<i>a</i>	<i>e</i>

There are **two** distinct groups, since the last three tables are the same.

In the third table, if we swap the roles of *a* and *b*, then we obtain the second table.

In the fourth table, if we swap the roles of *a* and *c*, then we obtain the second table.

3. Applying extended Euclidean algorithm, we find that $3(1) + 2(-1) = 1$. Hence, define $f(x, y) = 3x - 2y \pmod{6}$, or equivalently, $f(x, y) = 3x + 4y \pmod{6}$. According to the Chinese Remainder Theorem, f is a bijection, which can also be seen by listing all possible values:

$(0, 0)$	$(0, 1)$	$(0, 2)$	$(1, 0)$	$(1, 1)$	$(1, 2)$
0	4	2	3	1	5

It remains to show that f is a homomorphism. There are two methods.

Method 1: To show that f is a homomorphism (or equivalently, isomorphism since f is a bijection), the simplest way is to compare the Cayley tables of the two groups. The Cayley table for $\langle G, * \rangle$ is shown below:

+	$(0, 0)$	$(0, 1)$	$(0, 2)$	$(1, 0)$	$(1, 1)$	$(1, 2)$
$(0, 0)$	$(0, 0)$	$(0, 1)$	$(0, 2)$	$(1, 0)$	$(1, 1)$	$(1, 2)$
$(0, 1)$	$(0, 1)$	$(0, 2)$	$(0, 0)$	$(1, 1)$	$(1, 2)$	$(1, 0)$
$(0, 2)$	$(0, 2)$	$(0, 0)$	$(0, 1)$	$(1, 2)$	$(1, 0)$	$(1, 1)$
$(1, 0)$	$(1, 0)$	$(1, 1)$	$(1, 2)$	$(0, 0)$	$(0, 1)$	$(0, 2)$
$(1, 1)$	$(1, 1)$	$(1, 2)$	$(1, 0)$	$(0, 1)$	$(0, 2)$	$(0, 0)$
$(1, 2)$	$(1, 2)$	$(1, 0)$	$(1, 1)$	$(0, 2)$	$(0, 0)$	$(0, 1)$

For easy comparison, to draw the Cayley table for $\mathbb{Z}_6$, we order the elements of $\mathbb{Z}_6$, which matches with the above table. In other words, the header row is 0, 4, 2, 3, 1, 5, as shown below. Then we fill in the table using addition modulo 6.

+	0	4	2	3	1	5
0	0	4	2	3	1	5
4	4	2	0	1	5	3
2	2	0	4	5	3	1
3	3	1	5	0	4	2
1	1	5	3	4	2	0
5	5	3	1	2	0	4

By direct comparison, we can see that f is an isomorphism.

Method 2: Consider two arbitrary elements in G , namely, (x_1, y_1) and (x_2, y_2) . Then,

$$f((x_1, y_1) + (x_2, y_2)) = 3(x_1 + x_2 \pmod{2}) + 4(y_1 + y_2 \pmod{3}) \pmod{6}$$

Note that $x_1 + x_2 \pmod{2}$ is equal to $x_1 + x_2 + 2h$ for some integer h , and $y_1 + y_2 \pmod{3}$ is equal to $y_1 + y_2 + 3k$ for some integer k . Then,

$$\begin{aligned}
f((x_1, y_1) + (x_2, y_2)) &= 3(x_1 + x_2 + 2h) + 4(y_1 + y_2 + 3k) \pmod{6} \\
&= 3x_1 + 4y_1 + 3x_2 + 4y_2 + 6h + 12k \pmod{6} \\
&= 3x_1 + 4y_1 + 3x_2 + 4y_2 \pmod{6} \\
&= f(x_1, y_1) + f(x_2, y_2)
\end{aligned}$$

Hence, f is a homomorphism.

4. We can test whether an element a is a generator or not by listing out

$$a, \quad a + a, \quad a + a + a, \quad \dots$$

to check if all elements are included in the list.

1 is a generator because the corresponding list is 1, 2, 3, 4, 5, 6, 7, 8, 9, 0.

3 is a generator because the corresponding list is 3, 6, 9, 2, 5, 8, 1, 4, 7, 0.

7 is a generator because the corresponding list is 7, 4, 1, 8, 5, 2, 9, 6, 3, 0.

9 is a generator because the corresponding list is 9, 8, 7, 6, 5, 4, 3, 2, 1, 0.

Remark: 2 is *not* a generator because the corresponding list is 2, 4, 6, 8, 0, which does not include all elements. It can be verified that 0, 4, 5, 6, 8 are not generators by the same method.

5. There are four subgroups, namely, $\langle\{0\}, +\rangle$, $\langle\{0,3\}, +\rangle$, $\langle\{0,2,4\}, +\rangle$, $\mathbb{Z}_6$, where the operation $+$ is addition modulo 6.

Remark: $\langle\{0,1\}, +\rangle$ is *not* a subgroup because $0 + 1 = 2$, which does not belong to $\{0, 1\}$, violating the closure property. Intuitively, a group (or subgroup) must have some kind of symmetry. You should be able to see that $\{0, 3\}$ is somewhat symmetric in

$$\{\mathbf{0}, 1, 2, \mathbf{3}, 4, 5\}.$$

The elements 0 and 3 are marked in bold to highlight the “symmetry”. The same applies to $\{0, 2, 4\}$ as follows:

$$\{\mathbf{0}, 1, \mathbf{2}, 3, \mathbf{4}, 5\}.$$

6. Simply following the definition of cosets, we obtain

$$0 + H = 3 + H = 6 + H = \{0, 3, 6\}$$

$$1 + H = 4 + H = 7 + H = \{1, 4, 7\}$$

$$2 + H = 5 + H = 8 + H = \{2, 5, 8\}$$