

EE2302 Foundations of Information and Data Engineering

Assignment 10 (Solution)

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

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

| <i>*</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>*</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>*</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.

2. 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 $1 + 1 = 2$, 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

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

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

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

3. a) Multiplication table:

| \circ | <i>e</i> | <i>r</i> | <i>r</i>² | <i>f</i> | <i>rf</i> | <i>r</i>²<i>f</i> |
|-------------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|-------------------------------------|
| <i>e</i> | <i>e</i> | <i>r</i> | <i>r</i> ² | <i>f</i> | <i>rf</i> | <i>r</i> ² <i>f</i> |
| <i>r</i> | <i>r</i> | <i>r</i> ² | <i>e</i> | <i>rf</i> | <i>r</i> ² <i>f</i> | <i>f</i> |
| <i>r</i>² | <i>r</i> ² | <i>e</i> | <i>r</i> | <i>r</i> ² <i>f</i> | <i>f</i> | <i>rf</i> |
| <i>f</i> | <i>f</i> | <i>r</i> ² <i>f</i> | <i>rf</i> | <i>e</i> | <i>r</i> ² | <i>r</i> |
| <i>rf</i> | <i>rf</i> | <i>f</i> | <i>r</i> ² <i>f</i> | <i>r</i> | <i>e</i> | <i>r</i> ² |
| <i>r</i>²<i>f</i> | <i>r</i> ² <i>f</i> | <i>rf</i> | <i>f</i> | <i>r</i> ² | <i>r</i> | <i>e</i> |

b) No, it is not an Abelian group. It is because the multiplication table is not symmetric across the diagonal, i.e., the operation is not commutative. For example, $r \circ f = rf$ but $f \circ r = r^2f$, which are not equal.