MA1214

Introduction to group theory

Prof. Zaitsev

Solutions to Sheet 7

leitner@stp.dias.ie

1. (a) As a set, $\mathbb{Z}_3 = \{[0], [1], [2]\}$ which forms a group under addition.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

(b) $\mathbb{Z}_6^*$ has been introduced in class: The set $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$ forms a group under addition. Define

$$\mathbb{Z}_6^* := \{[m] \in \mathbb{Z}_6 \setminus \{[0]\} | \gcd(m, 6) = 1\} = \{[1], [5]\} .$$

$\mathbb{Z}_6^*$ is the set of units in $\mathbb{Z}_6$. It is a multiplicative group:

·	[1]	[5]
[1]	[1]	[5]
[5]	[5]	[1]

(c) As a set, $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{([0], [0]), ([0], [1]), ([1], [0]), ([1], [1])\}$, where each copy $\mathbb{Z}_2$ forms a group under addition. This yields the following Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_2$:

+	([0],[0])	([0],[1])	([1],[0])	([1],[1])
([0],[0])	([0],[0])	([0],[1])	([1],[0])	([1],[1])
([0],[1])	([0],[1])	([0],[0])	([1],[1])	([1],[0])
([1],[0])	([1],[0])	([1],[1])	([0],[0])	([0],[1])
([1],[1])	([1],[1])	([1],[0])	([0],[1])	([0],[0])

(d)
- $\mathbb{Z}_3$ is cyclic, generated additively by 1: We have [1], and $[1] + [1] = [1 + 1] = [2]$ and $[1] + [1] + [1] = [1 + 1 + 1] = [0] = e$, so all elements are captured.
- $\mathbb{Z}_6^*$ is cyclic, generated multiplicatively by [5]: We have [5], and $[5]^2 = [1] = e$.
- $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic: There is no generator. (All diagonal elements of the Cayley table for $\mathbb{Z}_2 \times \mathbb{Z}_2$ are equal to ([0], [0]). It follows that for any element different from ([0], [0]) in this group, the repeated addition yields only two out of the four group elements.)

2. Let G be a group. Since G has *finite* order (=number of elements),

$$\forall\, a \in G \quad \exists\, m \in \mathbb{N}^+ \quad \text{s.t.} \quad a^m = e .$$

(Otherwise by successively increasing the power we obtain infinitely many different elements that all lie in G, contradiction to the order being finite.)
Let m be the smallest positive integer with this property. Then

$$\langle a \rangle \underset{\text{subgroup}}{\subseteq} G\,, \quad \operatorname{ord}\langle a \rangle = m\,.$$

For every subgroup $H \subseteq G$, we know that $\operatorname{ord} H | \operatorname{ord} G$, so we must have

$$m | \operatorname{ord} G\,.$$

Since $\operatorname{ord} G = p$ is *prime*, it follows that $m = 1$, or $m = p$:

- $m = 1 \;\Rightarrow\; a = e$, and
$$\langle a \rangle = \langle e \rangle$$
is the trivial proper subgroup. (Since $p \neq 1$, $\exists\, b \in G \setminus \{e\}$, so repeat the argument for b.)
- $m = p \;\Rightarrow\; a^p = 1$, and
$$\langle a \rangle = \{e, a, a^2, \dots, a^{p-1}\} \cong G$$
(same number of elements). Since also $\langle a \rangle \subseteq G$, we conclude $\langle a \rangle = G$.

We have shown that G is generated by one element $a \neq e$, so G is cyclic.

3. Subgroups:
   (a) $\operatorname{ord} \mathbb{Z}_3 = 3$ is prime, so the only subgroups of $\mathbb{Z}_3$ are $\langle e \rangle$ and $\mathbb{Z}_3$ itself.
   (b) $\operatorname{ord} \mathbb{Z}_6^* = 2$ is prime, so the only subgroups of $\mathbb{Z}_6^*$ are $\langle e \rangle$ and $\mathbb{Z}_6^*$ itself.
   (c) We have $\operatorname{ord} \mathbb{Z}_2 \times \mathbb{Z}_2 = 4$, and
$$1, 2, 4 | 4$$
so apart from the two trivial subgroups $\langle ([0],[0]) \rangle$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ of order 1 and 4, respectively, there is a subgroup of order 2. Actually there are 3 of them, which are all cyclic and given by
$$H_1 := \langle ([1],[1]) \rangle, \quad H_2 := \langle ([0],[1]) \rangle, \quad H_3 := \langle ([1],[0]) \rangle\,.$$
(Note that we have already remarked in problem 1d) that either of them contains $e = \langle ([0],[0]) \rangle$ and has order 2.)