MA1214

# Introduction to group theory

Prof. Zaitsev

## Solutions to Sheet 9

leitner@stp.dias.ie

1. (a) Let $G_1$, $G_2$ be two groups. We have to show that $G_1 \times \{e_2\}$ is a *normal subgroup* in $G_1 \times G_2$, i.e.

$$\forall\,(g_1, g_2) \in G_1 \times G_2, \quad (g_1, g_2)^{-1}\, G_1 \times \{e_2\}\,(g_1, g_2) = G_1 \times \{e_2\}\,.$$

We have $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$ and

$$\begin{aligned}(g_1, g_2)^{-1}\, G_1 \times \{e_2\}\,(g_1, g_2) &= (g_1^{-1} G_1 g_1) \times g_2^{-1}\{e_2\} g_2 \\ &= G_1 \times \{e_2\}.\end{aligned}$$

Let us consider the first factor: $G_1$ is closed under inversion and under multiplication from either side, so $\forall\, g_1 \in G_1$, we have

$$g_1^{-1} \in G_1 \;\Rightarrow\; g_1^{-1} G_1 \subseteq G_1\,, \quad \text{and} \quad G_1 g_1 \subseteq G_1\,.$$

We also have

$$g_1^{-1} G_1 \supseteq G_1\,, \quad G_1 g_1 \supseteq G_1$$

(For the first relation, for instance, we observe that any $h \in G_1$ is reached by applying $g_1^{-1}$ from the left to $g_1 h \in G_1$.) We conclude that $g_1^{-1} G_1 = G_1$, $G_1 g_1 = G_1$, and altogether $g_1^{-1} G_1 g_1 = G_1$.

(b) From part 1a) we know that both $G$ itself and $\{e\}$ are normal subgroups of $G$. These are the largest and the smallest normal subgroup in $G$, respectively. Indeed, every subgroup of $G$ must contain at least its identity. Thus the intersection of all normal subgroups is $\{e\}$, which is normal.

2. Recall from problem sheet 8 that for a homomorphism $f : G_1 \to G_2$ of groups, where $G_1$ is cyclic, is determined by specifying its value on the generating element of $G_1$. Moreover, a group homomorphism maps the identity to the identity. (Indeed, if $G_1, G_2$ are multiplicative, then for any $a \in G_1$, $f(e_1) = f(a^0) = f(a)^0 = e_2$. If $G_1, G_2$ are additive, then $f(e_1) = f(0 \cdot a) = 0 \cdot f(a) = e_2$. For a map between a multiplicative and an additive group cf. problem sheet 8, problem 2.)

(a) $f : \mathbb{Z}_2 \to \mathbb{Z}_4$ homomorphic:

- The generationg element of $\mathbb{Z}_2$ is [1]. Define $f$ on [1] by $f([1]) = 0$. Since by assumption $f$ is a homomorphism, it follows that

$$f([0]) = f([1 + 1]) = f([1]) + f([1]) = [0] + [0] = [0]\,.$$

So $f$ is well-defined, since it maps the identity of $\mathbb{Z}_2$ to the identity of $\mathbb{Z}_4$.

- Define $f$ by $f([1]) = 1$. We have $f([0]) = f([1+1]) = f([1])+f([1]) = [1] + [1] = [2] \neq [0]$ in $\mathbb{Z}_4$. So $f$ is **not** well-defined.
- Define $f$ by $f([1]) = 2$. We have $f([0]) = f([1+1]) = f([1])+f([1]) = [2] + [2] = [4] = [0]$ in $\mathbb{Z}_4$. So $f$ is well-defined.

- Define $f$ by $f([1]) = [3]$. We have $f([0]) = f([1+1]) = f([1]) + f([1]) = [3] + [3] = [6] = [2] \neq 0$ in $\mathbb{Z}_4$. So $f$ is **not** well-defined.

The map $f([1]) = [m]$ for any $[m] \in \mathbb{Z}_4$ with

$$m + m = 2m \equiv 0 \mod 4$$

is well-defined.

(b) $f : \mathbb{Z}_2 \to \mathbb{Z}_5$ homomorphic:

- Define $f$ by $f([1]) = 0$. We have $f([0]) = f([1+1]) = f([1]) + f([1]) = [0] + [0] = [0]$. So $f$ is well-defined.
- Define $f$ by $f([1]) = 1$. We have $f([0]) = f([1+1]) = f([1]) + f([1]) = [1] + [1] = [2] \neq [0]$ in $\mathbb{Z}_5$. So $f$ is **not** well-defined.
- Define $f$ by $f([1]) = 2$. We have $f([0]) = f([1+1]) = f([1]) + f([1]) = [2] + [2] = [4] \neq [0]$ in $\mathbb{Z}_5$. So $f$ is **not** well-defined.
- Define $f$ by $f([1]) = [3]$. We have $f([0]) = f([1+1]) = f([1]) + f([1]) = [3] + [3] = [6] = [1] \neq [0]$ in $\mathbb{Z}_4$. So $f$ is **not** well-defined.
- Define $f$ by $f([1]) = [4]$. We have $f([0]) = f([1+1]) = f([1]) + f([1]) = [4] + [4] = [8] = [3] \neq [0]$ in $\mathbb{Z}_4$. So $f$ is **not** well-defined.

5 is not divisible by 2, so

$$m + m = 2m \equiv 0 \mod 5$$

is solved by $[m] = [0]$ only. The only homomorphism is the trivial map.

3. Recall that the order of a group is the number of its elements. $\mathbb{Z}_8 = \{[0], \ldots, [7]\}$ has order 8.

(a) Denote by [4] be the equivalence class mod 8. $\langle [4] \rangle = \{[0], [4]\}$ defines a subgroup of $\mathbb{Z}_8$ of order two. So

$$\mathbb{Z}_8 / \langle [4] \rangle = \{[0], [1], [2], [3]\}$$

has order $8 : 2 = 4$ and is cyclic, generated by [1].

(b) We have

$$\begin{aligned}
3 = 3 &\equiv 3 \mod 8 \\
3+3 = 6 &\equiv 6 \mod 8 \\
3+3+3 = 9 &\equiv 1 \mod 8 \\
3+3+3+3 = 12 &\equiv 4 \mod 8 \\
3+3+3+3+3 = 15 &\equiv 7 \mod 8 \\
3+3+3+3+3+3 = 18 &\equiv 2 \mod 8 \\
3+3+3+3+3+3+3 = 21 &\equiv 5 \mod 8 \\
3+3+3+3+3+3+3+3 = 24 &\equiv 0 \mod 8 \,.
\end{aligned}$$

By adding another copy of 3, we restart from above. We observe that all numers between 0 and 7 occur, so that the subgroup $\langle [3] \rangle$ actually equals $\mathbb{Z}_8$:

$$\mathbb{Z}_8 / \langle [3] \rangle = \{[0]\} \,,$$

whose order is $8 : 8 = 1$. It is trivially cyclic.

More generally, when $gcd(m, n) = 1$ and $[m]$ denotes the equivalence class mod $n$, then $\langle [m] \rangle = \mathbb{Z}_n$.