DANMARKS TEKNINSKE UNIVERSITET

DISCRETE MATHEMATICS 2: ALGEBRA

Course number: 01018

Assignment 2

Author:

Mads Esben Hansen, s174434

November 16, 2020

Question 1.

a) As usual, let $(Z_n, +_n, \cdot_n)$ denote the ring of integers modulo n. Prove that the map $\psi : Z_{12} \rightarrow Z_4$ given by $\psi(i) = i \; mod \; 4$, for $i \in Z_{12}$ is a ring homomorphism.

We can use definition 154 to check if ψ is in fact a ring homomorphism.

$$\begin{aligned} 0_{12} &= (\mathbb{Z} \cdot 12) \; mod \; 12 = 0 \\ 0_4 &= (\mathbb{Z} \cdot 4) \; mod \; 4 = 0 \\ \psi(0_{12}) &= 0 \; mod \; 4 = 0 \quad \Leftrightarrow \\ \psi(0_{12}) &= 0_4 \end{aligned}$$

Let $r_1, r_2 \in \mathbb{Z}$.

$$\begin{aligned} \psi(r_1 +_{12} r_2) &= \psi((r_1 + r_2) \; mod \; 12) = ((r_1 + r_2) \; mod \; 12) \; mod \; 4 = r_1 + r_2 \; mod \; 4 \\ \psi(r_1) +_4 \psi(r_2) &= ((r_1 \; mod \; 4) + (r_2 \; mod \; 4)) \; mod \; 4 = r_1 + r_2 \; mod \; 4 \quad \Rightarrow \\ \psi(r_1 +_{12} r_2) &= \psi(r_1) +_4 \psi(r_2) \end{aligned}$$

Since we chose $r_1, r_2 \in \mathbb{Z}$ freely, it holds for all combination of r_1, r_2. So criteria 1 of definition 154 is fulfilled. Now let us look at the second criteria.

$$\begin{aligned} 1_{12} &= 1 \\ 1_4 &= 1 \\ \psi(1_{12}) &= \psi(1) = 1 \; mod \; 4 = 1 = 1_4 \end{aligned}$$

The second criteria is also fulfilled. Let us now look at the third and final. Let r_1, r_2 be as before.

$$\begin{aligned} \psi(r_1 \cdot_{12} r_2) &= ((r_1 \cdot r_2) \; mod \; 12) \; mod \; 4 = (r_1 \cdot r_2) \; mod \; 4 \\ \psi(r_1) \cdot_4 \psi(r_2) &= (r_1 \cdot r_2) \; mod \; 4 \quad \Leftrightarrow \\ \psi(r_1 \cdot_{12} r_2) &= \psi(r_1) \cdot_4 \psi(r_2) \end{aligned}$$

So the third and final criteria is also fulfilled. We can now conclude that ψ is in fact a ring homomorphism.

b) Compute the image and the kernel of ψ.

The image is found directly as:

$$\begin{aligned} Im(\psi) &= \{\psi(r) \mid r \in \mathbb{Z}_{12}\} = \{r \; mod \; 4 \; \mid r \in \mathbb{Z}_{12}\} \\ Im(\psi) &= \{0, 1, 2, 3\} \end{aligned}$$

Following definition 155 we find the kernel as:

$$\begin{aligned} ker(\psi) &= \{r \in \mathbb{Z} | \psi(r) = 0_4\} = \{r \in \mathbb{Z} | \psi(r) = 0\} = \{r \in \mathbb{Z} | r \equiv 0 \; (mod \; 4)\} \\ ker(\psi) &= \mathbb{Z} \cdot 4 = \{..., -4, 0, 4, ...\} \end{aligned}$$

c) Is the map $\phi : Z_{14} \rightarrow Z_4$ given by $\phi(i) = i \; mod \; 4$, for $i \in Z_{14}$ a ring homomorphism?

It is if is satisfies all 3 criteria mentioned in definition 154. Let us check:

$$\begin{aligned} 0_{14} &= \mathbb{Z} \cdot 14 = \{..., -14, 0, 14, ..\} \\ \phi(0_{14}) &= (\mathbb{Z} \cdot 14) \; mod \; 4 = \{0, 2\} \neq 0_4 \end{aligned}$$

So it is not even a group homomorphism and there is therefore no way it can be a ring homomorphism.

Question 2.

Let $(D_4, \circ)$ be the dihedral group consisting of the symmetries of a square. As usual we write $D_4 = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\}$. The symmetries r and s satisfy $r^{-1} = r^3, s^{-1} = s$ and $sr = r^{-1}s$. For a group homomorphism $\phi : D_4 \longrightarrow S_8$ it is given that $\phi(r) = (1357)(2468)$ and $\phi(s) = (18)(27)(36)(45)$.

a) Compute $\phi(a)$ for all $a \in D_4$.

They are directly computed by:

$$
\begin{aligned}
\phi(e) &= id \\
\phi(r) &= (1357)(2468) \\
\phi(r^2) &= \phi(r) \cdot \phi(r) = (1357)(2468)(1357)(2468) = (15)(26)(37)(48) \\
\phi(r^3) &= \phi(r^2) \cdot \phi(r) = (15)(26)(37)(48)(1357)(2468) = (1753)(2864) \\
\phi(s) &= (18)(27)(36)(45) \\
\phi(rs) &= \phi(r) \cdot \phi(s) = (1357)(18)(27)(36)(45) = (16)(25)(34)(78) \\
\phi(r^2s) &= \phi(r^2) \cdot \phi(s) = (15)(26)(37)(48)(18)(27)(36)(45) = (14)(23)(58)(67) \\
\phi(r^3s) &= \phi(r^3) \cdot \phi(s) = (1753)(2864)(18)(27)(36)(45) = (12)(38)(47)(56)
\end{aligned}
$$

b) Determine a subgroup $H \subset S_8$ of $(S_8, \circ)$ such that $(D_4, \circ)$ is isomorphic to $(H, \circ)$.

In the previous exercise, we computed the image of ϕ. We further saw that $ker(\phi) = e$. According to theorem 118 in the book, we can now directly use the isomorphism given by:

$$\phi : \ (D_4, \circ) \longrightarrow im(\phi)$$

We can in turn define H to be the image of ϕ:

$$
\begin{aligned}
H = im(\phi) =& \{id, (1357)(2468), (15)(26)(37)(48), (18)(27)(36)(45), \ldots \\
& (16)(25)(34)(78), (14)(23)(58)(67), (12)(38)(47)(56)\}
\end{aligned}
$$

We do not even need to check that this is in fact a group, since this is guaranteed by theorem 118.

c) What is the smallest integer n such that $(D_4, \circ)$ is isomorphic to a subgroup of $(S_n, \circ)$?

We know that $(S_3, \circ)$ contains $3! = 6$ different cycles. It is therefore not possible to find a map from $(S_3, \circ)$ with a image that is larger than 6. Since D_4 contains 8 elements, finding a isomorphic subgroup with $n \leq 3$ is not possible.
Now we look at $(S_4, \circ)$, which contains $4! = 24$ different cycles. If we now define a map $\psi : \ D_4 \longrightarrow S_4$, where $\psi(e) = id$, $\psi(r) = (1234)$, and $\psi(s) = (14)(23)$, we have a group homomorphism. We further have that $ker(\psi) = e$ (this will not be proved formally). We can now do the same trick as in b) to find a subgroup $H \subset S_4$, s.t. $(H, \circ)$ is isomorphic to $(D_4, \circ)$. So for $n = 4$ $(D_4, \circ)$ is isomorphic to subgroup of $(S_n, \circ)$.
Finally we get $3 < n \leq 4 \implies n = 4$.