(Difficulty) Exercises Week 8 (Solutions at the end)

+++

① Prove Lemma 5.5 from the script. So prove that:

A group homomorphism ψ from $\langle G; *, \hat{}, e\rangle$ to $\langle H; \triangle, \sim, e'\rangle$ satisfies

1) $\psi(e) = e'$
2) $\psi(\hat{a}) = \widetilde{\psi(a)}$ for all a

+++

② Bonus from last year

8.5 Inner Direct Products (⋆) **(8 Points)**

a) Let $\langle G; *, \hat{}, e\rangle$ be a commutative group. Let H and K be subgroups of G such that

i. $G = \{h * k \mid h \in H, k \in K\}$,

ii. $H \cap K = \{e\}$.

Prove that G is isomorphic to the direct product $H \times K$. In this case, G is called the *inner* direct product of H and K.

b) Use the previous subtask to prove that $\langle \mathbb{Z}_{15}^*, \odot_{15}\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$. You can use the subtask even if you have not proven it. **Do not** prove the isomorphism directly.

++

③ Take the Algebra $\langle B; \circ\rangle$ where B is the set of all bijective functions from $\mathbb{Z}$ to $\mathbb{Z}$ and $\circ$ is the function composition we know.
Find a suitable neutral and inverse elements and prove that it is a group.

+

④ Take the algebra $\langle \{0,1\}^*; \text{concat}\rangle$ where $\{0,1\}^*$ is the set of finite bitstrings and $\text{concat}(b_1, b_2) = b_1 b_2$.

a) Is concat associative? (Is it a semigroup)
b) Is there a neutral element?
c) If yes, is there an inverse?

Solutions

(1)

1) $\varphi(e) = \varphi(e)$ (φ well defined)

$= \varphi(e * e)$ (e neutral element)

$= \varphi(e) \vartriangle \varphi(e)$ (φ homomorphism)

So we have $\varphi(e) = \varphi(e) \vartriangle \varphi(e)$.

$\Rightarrow \varphi(e) \vartriangle e' = \varphi(e) \vartriangle \varphi(e)$ (e' neutral element)

$\Rightarrow e' = \varphi(e)$ (left cancellation law)

2) Take any $a \in G$.

$\varphi(e) = \varphi(e)$ (φ well defined)

$= \varphi(a * \hat{a})$ ($\hat{a}$ inverse of a exists)

$= \varphi(a) \vartriangle \varphi(\hat{a})$ (φ homomorphism)

So we have $\varphi(a) \vartriangle \varphi(\hat{a}) = \varphi(e)$

$= e'$ (per 1))

This shows that $\varphi(\hat{a})$ is a right inverse of $\varphi(a)$, the proof for the left inverse is analogous.

(2)

Solution on emils.site → session 8

(3)

We can take $id_{\mathbb{Z}}$ as the neutral element. Since $id_{\mathbb{Z}}$ is bijective, it is in B.
We can take the inverse function $\hat{f}$ for the inverse element of f. Since every bijective function has an inverse, which is also bijective, this works.

We know from the script that $\circ$ is associative, therefore it is a group.
For a graded exercise you would need to argue a bit more formally here.

④

- It is associative. This is an informal exercise, just imagine you have any bitstrings a, b, c. It does not matter if you stich a to b and then c to them to get abc or if you first make bc and then stich a to the left of it.
- The empty bitstring λ is a neutral element.
- There is no inverse since we cannot delete bits.