ETH zürich

Discrete Mathematics **2024**

Student: Jeferson Morales Mariciano <jmorale@ethz.ch>

Assignment 8 **Due date:** Thursday, 14 November 2024, 23:59

Exercise 8.5, Inner Direct Products ($\star$) (8 Points)

a) Let $\langle G; *, \widehat{\ }, e\rangle$ 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 proved it. **Do not** prove the isomorphism directly.

a)

By the exercise statement, all the elements of G can be written as $h*k$ for some $h \in H$ and $k \in K$ by the first condition (i), thus all the elements of H and K are in G as well because $\forall\, h \in H,\ h * e \in G$ and $\forall\, k \in K,\ e * k \in G$. The group G is stated to be abelian, so H and K are abelian as well and recall $*$ is associative by Definition 5.7 of Group.

For the subgroups $\langle H; *, \widehat{\ }, e\rangle$ and $\langle K; *, \widehat{\ }, e\rangle$ of G, their direct product $H \times K$ is defined as algebra $\langle H \times K; \star, \widehat{\ }, e\rangle$. where the component wise operation $\star$ is defined as

$$(a_1, b_1) \star (a_2, b_2) = (a_1 * a_2,\ b_1 * b_2) \quad a_1, a_2 \in H,\ b_1, b_2 \in K \qquad \text{(Definition 5.9)}$$
$$\implies (h_1, k_1) \star (h_2, k_2) = (h_1 * h_2,\ k_1 * k_2) \quad (h_1, k_1), (h_2, k_2) \in H \times K$$

.

From Lemma 5.4 $\langle G_1 \times \cdots \times G_n; *\rangle$ is a group where the neutral element and the inversion operation are component wise in the respective groups, but by Definition 5.11 of Subgroups, H, K and group G share the same neutral element e, inverse operation $\widehat{\ }$, and are closed under the operation $*$.

Let's define the mapping function ψ.

$$\psi : G \to H \times K \qquad h * k \mapsto (h, k) \quad \forall\, h * k \in G$$

The group homomorphism property of ψ is check as follows

$$\psi(a * b) = \psi(a) \star \psi(b) \quad \forall\, a, b \in G \qquad \text{(CHECK Definition 5.10)}$$
$$\psi((h_1 * k_1) * (h_2 * k_2)) = \psi(h_1 * k_1) \star \psi(h_2 * k_2) = ((h_1, h_2), (k_1, k_2)) \qquad \text{(group elems notation)}$$
$$\psi((h_1 * k_1) * (h_2 * k_2)) \implies \psi(h_1 * (k_1 * h_2) * k_2) \qquad \text{(associativity)}$$
$$\implies \psi(h_1 * (h_2 * k_1) * k_2) \qquad \text{(commutativity)}$$
$$\implies \psi((h_1 * h_2) * (k_1 * k_2)) \qquad \text{(associativity)}$$
$$\implies \psi(h * k) \qquad h = h_1 * h_2,\ k = k_1 * k_2$$
$$\implies (h, k) \implies ((h_1 * h_2), (k_1 * k_2)) \implies ((h_1, k_1) \star (h_2, k_2))$$
$$\implies \psi(h_1 * k_1) \star \psi(h_2 * k_2) \implies \psi(a) \star \psi(b) \qquad \square$$

From G to direct product of 2 subgroups of G.

Injectivity: let $\psi(a) = \psi(b)$ for some $a, b \in G$, then

$$\begin{aligned}\psi(a) = \psi(b) \implies (h_a, k_a) = (h_b, k_b) \implies h_a = h_b,\, k_a = k_b \\ \implies a = b \implies \psi(a) = \psi(b) \implies \psi \text{ is injective}\end{aligned}$$

For any $(h, k) \in H \times K$, it exists an element a in G by definition (i) such that $a = h * k$ and $\psi(a) = (h, k)$. Thus, ψ is surjective. Finally, *psi* is bijective, then the homomorphism ψ is an isomorphism and $G \simeq H \times K$, where G is the inner direct product of H and K.

b)

The group $\mathbb{Z}_{15}^*$ is the set of all integers a such that $a \in Z_{15} \wedge \gcd(a, 15) = 1$ by Definition 5.16. Hence, the group $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and $|\mathbb{Z}_{15}^*| = 8$ which is the order of $\mathbb{Z}_{15}^*$ due to Definition 5.13. By Definition 5.15, such group is not cyclic.

Then, the group $\mathbb{Z}_2 \times \mathbb{Z}_4$ is closed under modular addition $\oplus$ because for modular multiplication $\odot$ in general the group $\mathbb{Z}_n$ may have elements without the multiplication inverse, as $\mathbb{Z}_{12}$ with the element 8 which has no inverse. Such group $\mathbb{Z}_2 \times \mathbb{Z}_4$ can be seen as the direct product of the groups $\mathbb{Z}_2$ and $\mathbb{Z}_4$ from the previous subtask. From Theorem 5.7, $\langle \mathbb{Z}_n; \oplus \rangle$ is the standard notation for the cyclic group of order n. The definition is $\mathbb{Z}_2 \times \mathbb{Z}_4 = \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3)\}$. So we know that $\mathbb{Z}_2, \mathbb{Z}_4$ are cyclic groups.

Notice $|\mathbb{Z}_2 \times \mathbb{Z}_4| = 8 = |\mathbb{Z}_{15}^*|$ so a totally well defined mapping ψ could be defined as in the previous subtask, and it can be shown that it is both injective and surjective, hence bijective and an isomorphism.

The order of elements from $\mathbb{Z}_{15}^*$ are as follows: $ord = 2$ for $4, 11, 14$, $ord = 4$ for $2, 7, 8, 13$, and $ord = 1$ for 1 as it is the multiplicative inverse and also self inverse.

The cyclic subgroups of $\mathbb{Z}_{15}^*$ generated by generator elements $2, 4$ are $\langle 2 \rangle = \{1, 2, 4, 8\}$ with $ord(\langle 2 \rangle) = 4$ and $\langle 4 \rangle = \{1, 4\}$ with $ord(\langle 4 \rangle) = 2$ respectively using Definition 5.14.

By Theorem 5.7, a cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n; \oplus \rangle$ and abelian. So $\langle 2 \rangle, \langle 4 \rangle$ are isomorphic to $\mathbb{Z}_4, \mathbb{Z}_2$ w.r.t. their order, i.e. $\langle 2 \rangle \simeq \langle \mathbb{Z}_4; \oplus \rangle$, $\langle 4 \rangle \simeq \langle \mathbb{Z}_2; \oplus \rangle$.

Hence, from the previous subtask **a)**, the group G can be seen as $\mathbb{Z}_{15}^*$ and the direct product of $H \times K$ would be the direct product of the cyclic subgroups $\langle 2 \rangle, \langle 4 \rangle$, which are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$, i.e. $\mathbb{Z}_{15}^* \simeq \langle 2 \rangle \times \langle 4 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$. The proof is complete and a direct isomorphism is not needed from the exercise statement.