

⑤ The direct product of $H \times K$ is the group:
 $\langle H \times K; \triangleright \rangle$ with $(h_1, k_1) \triangleright (h_2, k_2) = (h_1 * h_2, k_1 * k_2)$ per def. 5.8. / lemma 5.4.

To prove that it is isomorphic to G , we need to find an isomorphism from G to $\langle H \times K; \triangleright \rangle$.

Let's look at the map ψ :

$$\psi: G \rightarrow \langle H \times K; \triangleright \rangle \quad \text{with } \psi(g) = (h, k) \text{ where } h \in H \text{ and } k \in K \text{ such that } h * k = g.$$

ψ is a function since per (i) we know that such h, k exist for all $g \in G$ and we quickly prove that it is well-defined:

We know that the only representation of $e \in G$ is $e * e$, since if $h_e * k_e = e$ with $h_e \in H$, then h_e is the inverse of k_e and therefore $k_e \in H$. The only $k_e \in K$ which fulfills this is e per (ii).

Now assume $\psi(g) = (h_1, g_1) = (h_2, g_2)$.
 Then the unique inverse of g is $\hat{g} = h_2 * g_2$ since:

$$\begin{aligned} g * \hat{g} &= h_2 * g_2 * h_2 * g_2 \\ &= (h_2 * h_2) * (g_2 * g_2) \\ &= e * e = e \end{aligned} \quad \left| \begin{array}{l} g = h_2 * g_2 \text{ since } \psi(g) = (h_2, g_2) \\ G \text{ is commutative group} \\ G \text{ and } e \text{ is neutral element} \end{array} \right.$$

Then however:

$$\begin{aligned} g * \hat{g} &= e \\ \Rightarrow h_1 * k_1 * h_2 * g_2 &= e \\ \Rightarrow (h_1 * h_2) * (k_1 * k_2) &= e \\ \Rightarrow h_1 * h_2 &= e \text{ and } k_1 * k_2 = e \\ \Rightarrow h_1 &= \hat{h}_2 \text{ and } k_1 = \hat{k}_2 \\ \Rightarrow h_1 &= h_2 \text{ and } k_1 = k_2 \end{aligned} \quad \left| \begin{array}{l} g = h_1 * k_1 \text{ cause } \psi(g) = (h_1, k_1) \\ G \text{ is commutative group} \\ \text{since } (h_1 * h_2) \in H \text{ and } (k_1 * k_2) \in K \\ \text{def. of inverse we know from} \\ \hat{a} = a \text{ above they} \\ \text{have to be} \\ e. \end{array} \right.$$

Which shows that ψ is well-defined.

We now need to prove that ψ is a homomorphism; so that it satisfies $\psi(g * g') = \psi(g) \vee \psi(g')$ for all $g, g' \in G$.

So let g, g' be arbitrary (\in of G), then:

$$\begin{aligned}
 & \psi(g * g') \\
 &= \psi(h * k * h' * k') \quad \text{with } h * k = g, h' * k' = g' \text{ which exist per (i)} \\
 &= \psi((h * h') * (k * k')) \quad | * \text{ is commutative / associative} \\
 &= (h * h', k * k') \quad | \text{ def. of } \psi \\
 &= (h, h') \vee (h', k') \quad | \text{ def. of } \vee \\
 &= \psi(h * k) \vee \psi(h' * k') \quad | \text{ def. of } \psi \\
 &= \psi(g) \vee \psi(g') \quad | \text{ def. of } g, g' \text{ from above}
 \end{aligned}$$

Which is exactly the homomorphism-property.

It is left to show that ψ is a bijection, so injective, surjective:

• injective: for arbitrary $g, g' \in G$ with $g = h * k, g' = h' * k'$:

$$\begin{aligned}
 & g \neq g' \quad (\text{assume}) \\
 \Rightarrow & h * k \neq h' * k' \quad | \text{ def } g, g' \\
 \Rightarrow & h \neq h' \vee k \neq k' \quad | \text{ otherwise } h = h' \wedge k = k' \Rightarrow h * k = h' * k' \quad | \text{ de Morgan} \\
 \Rightarrow & (h, k) \neq (h', k') \quad | \text{ def. of tuple equality} \\
 \Rightarrow & \psi(g) \neq \psi(g') \quad | \text{ def. of } \psi \\
 & \text{which is the definition of injective}
 \end{aligned}$$

• surjective: For arbitrary $(h, k) \in \langle H \times K, \vee \rangle$ there must exist $g \in G$ such that $h * k = g$ per (i). Consequently $\psi(g) = (h, k)$ per def. of ψ .

Since we showed that ψ is a homomorphism and bijective, it is an isomorphism and therefore G is isomorphic to $H \times K$.

$$b) \langle \mathbb{Z}_{15}^*, \odot \rangle = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

• $A = \{1, 2, 4, 8\}$ is a subgroup of it, since $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 1$, meaning it is generated by 2 and therefore a group per def. 5.14.

• $B = \{1, 11\}$ is another subgroup since $11 \odot_{15} 11 = 1$ meaning it is closed.

• We calculate all products between elements of A and B:

\odot_{15}	1	2	4	8
1	1	2	4	8
11	11	7	14	3

and see that those are exactly $\langle \mathbb{Z}_{15}^*, \odot \rangle$. And since the groups only share 1 (the neutral element), they fulfill (i) and (ii) and so $A \times B \cong \langle \mathbb{Z}_{15}^*, \odot \rangle$.

• And since both groups are cyclic, they are also isomorphic to \mathbb{Z}_4 and \mathbb{Z}_2 per theorem 5.7.

• Now we can construct an isomorphism γ from $A \times B$ to $\mathbb{Z}_4 \times \mathbb{Z}_2$ with $\gamma((x, y)) = (a, b)$ s.t. $f(x) = a$ and $g(y) = b$ if f is the isomorphism from $A \rightarrow \mathbb{Z}_4$ and g from $B \rightarrow \mathbb{Z}_2$.

Since g, f are isomorphisms, γ is well defined and bijective and since the operations on $A \times B$ are defined component wise it is also a homomorphism.

• This shows that $\mathbb{Z}_4 \times \mathbb{Z}_2 \cong A \times B \cong \langle \mathbb{Z}_{15}^*, \odot \rangle$

meaning $\mathbb{Z}_4 \times \mathbb{Z}_2 \cong \langle \mathbb{Z}_{15}^*, \odot \rangle$