Challenge 1

Monday, 11 November 2024 20:41

Let G, H, K be groups, and $G \times K \cong H \times K$. Prove or disprove that $G \cong H$.

Let $G = \langle \mathbb{Z}_2, \otimes_1 \rangle$ $H = \langle \mathbb{Z}_2 \times \mathbb{Z}_2, \otimes_2 \rangle$ and $K = \langle \mathbb{Z}_2^\infty, \otimes_\infty \rangle$

(the groups of 1-bit, 2-bit and semi-infinite bitstrings, with the XOR operator)

and let $\star_G$ and $\star_H$ be the binary operators of the inner products $G \times K$ and $H \times K$.

G is obviously a group (example 5.27) $\Rightarrow H = G \times G$ is also a group (Lemma 5.4)

Let a_n denote the n-th bit of a, for all $a \in \mathbb{Z}_2^\infty$.

For all $x, y \in \mathbb{Z}_2^\infty$:

$x \otimes_\infty y$ is another semi-infinite bitstring (closure)

$1 \otimes 0 = 1$ and $0 \otimes 0 = 0$

$\Rightarrow$ For all $x \in \mathbb{Z}_2^\infty$, for all $n \in \mathbb{N}$: $x_n \otimes 0 = x_n \Rightarrow x \otimes_\infty 0_\infty = x$, where 0_∞ is the infinite bitstring of 0,

$\Rightarrow \langle \mathbb{Z}_2^\infty, \otimes_\infty \rangle$ has an identity element $e = 0_\infty$ s.t. $\forall x \in \mathbb{Z}_2^\infty: x \otimes_\infty e = x$ (G2')

For all $w, x, y \in \mathbb{Z}_2^\infty$:

For all $n \in \mathbb{N}^*$:

$$\begin{aligned}((w \otimes_\infty x) \otimes_\infty y)_n &= (w_n \otimes_1 x_n) \otimes_1 y_n \quad (\otimes_\infty \text{ is a bitwise operation})\\ &= w_n \otimes_1 (x_n \otimes_1 y_n) \quad (\langle \mathbb{Z}_2, \otimes_1 \rangle \text{ is a group + G1})\\ &= (w \otimes_\infty (x \otimes_\infty y))_n \quad (\otimes_\infty \text{ is a bitwise operation})\end{aligned}$$

$\Rightarrow (w \otimes_\infty x) \otimes_\infty y = w \otimes_\infty (x \otimes_\infty y)$ (since all their bits are equal ($\otimes_\infty$ is a bitwise operation)

$\Rightarrow \otimes_\infty$ is associative (G1)

For all $x \in \mathbb{Z}_2^\infty$:

For all $n \in \mathbb{N}^*$:

$$\begin{aligned}(x \otimes_\infty x)_n &= x_n \otimes_1 x_n \quad (\otimes_\infty \text{ is a bitwise operator})\\ &= 0 \quad (1 \otimes_1 1 = 0 \otimes_1 0 = 0)\end{aligned}$$

$\Rightarrow x \otimes_\infty x = 0_\infty = e$

$\Rightarrow$ each element x has an inverse $\hat{x} \in \mathbb{Z}_2^\infty$ s.t.:

$x \otimes_\infty \hat{x} = x \otimes_\infty x = \hat{x} \otimes_\infty x = 0_\infty$

$\Rightarrow$ G3

Thus, $\langle \mathbb{Z}_2^\infty, \otimes_\infty \rangle$ is also a group.

Let $\psi: G \times K \to K$ and $\varphi: H \times K \to K$ be functions defined as:

$\psi(g, k) = g \| k$ for all $(g, k) \in G \times K$,

$\varphi(h, k) = h \| k$ for all $(h, k) \in H \times K$, where $\|$ is the concatenation operator.

Since the $\|$ operator simply concatenates 2 bitstrings, and the XOR operator is bitwise:

$a \| b = c \| d$ and $l(a) = l(c) \Rightarrow a = c \wedge b = d$, (1)

$l(a) = l(c)$ and $l(b) = l(d) \Rightarrow a \| b \otimes c \| d = a \otimes c \| b \otimes d$ (2) where $l(x)$ is the length of the bitstring x

$a \| b = c \| d$ and $l(a) = l(c) \Rightarrow a = c \wedge b = d$, (1)

$l(a) = l(c)$ and $l(b) = l(d) \Rightarrow a \| b \otimes c \| d = a \otimes c \| b \otimes d$ (2) where $l(x)$ is the length of the bitstring x

For all $(g,k),(g',k') \in G \times K$:
$\Psi(g,k) = \Psi(g',k')$
$\Leftrightarrow g \| k = g' \| k'$ (def of Ψ)
$\Leftrightarrow g = g'$ and $k = k'$ ($l(g) = l(g')$, (1))
$\Leftrightarrow (g,k) = (g',k')$
$\Rightarrow \Psi$ is injective

For all $(h,k),(h',k') \in H \times K$:
$\varphi(h,k) = \varphi(h',k')$
$\Leftrightarrow h \| k = h' \| k'$ (def of φ)
$\Leftrightarrow h = h'$ and $k = k'$ ($l(h) = l(h')$, (1))
$\Leftrightarrow (h,k) = (h',k')$
$\Rightarrow \varphi$ is injective

For all $x \in K$:
Let g be the first bit of x and k be the rest of x.
By definition: $x = g \| k = \Psi(g,k)$
g is one bit, so $g \in G$ and k is also a semi-infinite bitstring: $k \in K$
$\Rightarrow \Psi$ is surjective

For all $x \in K$:
Let h be the first 2 bits of x and k be the rest of x
By definition: $x = h \| k = \varphi(h,k)$
h has 2 bits, so $h \in H$ and k is also a semi-infinite bitstring: $k \in K$
$\Rightarrow \varphi$ is surjective

Hence, Ψ and φ are bijective.

For all $(g,k),(g',k') \in G \times K$:

$$\begin{aligned}\Psi(g,k) \otimes_\infty \Psi(g',k') &= g \| k \otimes_\infty g' \| k' \quad \text{(def of } \Psi) \\ &= g \otimes_1 g' \| k \otimes_\infty k' \quad (2) \\ &= \Psi(g \otimes_1 g', k \otimes_\infty k') \quad \text{(def of } \Psi) \\ &= \Psi((g,k) \star_G (g',k')) \quad \text{(def of } \star_G)\end{aligned}$$

For all $(h,k),(h',k') \in H \times K$:

$$\begin{aligned}\varphi(h,k) \otimes_\infty \varphi(h',k') &= h \| k \otimes_\infty h' \| k' \quad \text{(def of } \varphi) \\ &= h \otimes_2 h' \| k \otimes_\infty k' \quad (2) \\ &= \varphi(h \otimes_2 h', k \otimes_\infty k') \quad \text{(def of } \varphi) \\ &= \varphi((h,k) \star_H (h',k')) \quad \text{(def of } \star_H)\end{aligned}$$

$\Rightarrow \Psi$ and φ are homomorphisms
$\Rightarrow \Psi$ and φ group isomorphisms
$\Rightarrow G \times K \cong K$ and $H \times K \cong K$

$\Rightarrow \Psi$ and φ group isomorphisms

$\Rightarrow G \times K \cong K$ and $H \times K \cong K$

Consider the function $f : H \times K \to G \times K$, $f = \Psi^{-1} \circ \varphi$

Ψ and φ are bijective $\Rightarrow \varphi$ and Ψ^{-1} are bijective $\Rightarrow f$ is bijective

$\forall (h, k), (h', k') \in H \times K$:

$$
\begin{aligned}
f(h,k) \star_G f(h',k') &= \Psi^{-1}(\varphi(h,k)) \star_G \Psi^{-1}(\varphi(h',k')) && (\text{def of } f) \\
&= \Psi^{-1}(h \| k) \star_G \Psi^{-1}(h' \| k') && (\text{def of } \varphi) \\
&= (h_1, (h_2 \| k)) \star_G (h'_1, h'_2 \| k') && (\text{def of } \Psi^{-1} + h = h_1 \| h_2) \\
&= (h_1 \otimes_1 h'_1, (h_2 \| k) \otimes_\infty (h'_2 \| k')) && (\text{def of } \star_G) \\
&= (h_1 \otimes_1 h'_1, h_2 \otimes_1 h'_2 \| k \otimes_\infty k') && (2) \\
&= \Psi^{-1}(h_1 \otimes_1 h_1 \| (h_2 \otimes_1 h_2 \| k \otimes_\infty k')) && (\text{def of } \Psi^{-1}) \\
&= \Psi^{-1}((h_1 \| h_2) \otimes_2 (h'_1 \| h_2) \| k \otimes_\infty k') && (\text{associativity of } \| + (2)) \\
&= \Psi^{-1}(h \otimes_2 h' \| k \otimes_\infty k') && (h = h_1 \| h_2) \\
&= \Psi^{-1}(\varphi((h,k) \star_H (h',k'))) && (\text{def of } \varphi) \\
&= f((h,k) \star_H (h',k')) && (\text{def of } f)
\end{aligned}
$$

$\Rightarrow f$ homomorphic

$\Rightarrow f$ isomorphic (f bijective)

$\Rightarrow G \times K \cong H \times K$

However:

$2 \neq 4$

$\Leftrightarrow |\mathbb{Z}_2| \neq |\mathbb{Z}_2 \times \mathbb{Z}_2|$

$\Rightarrow$ There is no bijection from G to H

$\Rightarrow G \ncong H$

Hence, the statement is false.