	e	a	b
e			
a			
b			

0	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\simeq \mathbb{Z}_3$

·	e	a
e	e	a
a	a	e

$\simeq \mathbb{Z}_2$

How to compose elts?

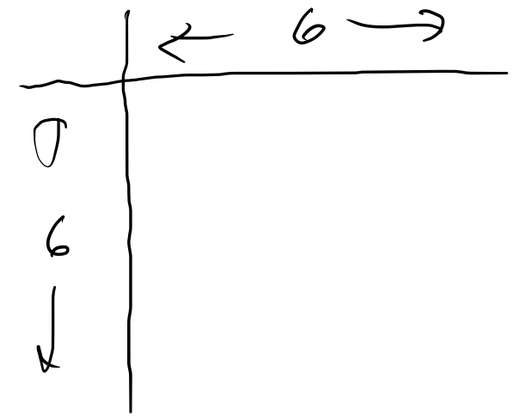
$G_2 \times \mathbb{Z}_3$

$(a,0) \circ (a,2) = ?$

$\|$

$(a \circ a, 0 \circ 2) = (e,2)$

op of G_2 op of $\mathbb{Z}_3$



Direct Product of Groups

$A = \{2,3,4\}$ $B = \{x,y\}$

$A \times B = \{(a,b) : a \in A, b \in B\}$ of sets.

$A \times B = \{(2,x)\ (2,y)\ (3,x)\ (3,y)\ (4,x)\ (4,y)\}$

- order matters $\Rightarrow$ $A \times B \neq B \times A$

$A \not\subset A \times B$ · elt of A of 2.

· elt of $A \times B$ $(3,y)$

For Groups:

$G_6 = G_2 \times \mathbb{Z}_3 = \{(e,0)\ (e,1)\ (e,2),\ (a,0), (a,1)\ (a,2)\}$

$(e,0)$: G_2, $\mathbb{Z}_3$; $(a,0)$: g_4; $(a,2)$: g_6

Claim: Let G & H be two groups, then the set $G \times H$ with the defined operation $(g_1, h_1) \circ (g_2, h_2) = (g_1 \circ g_2, h_1 \circ h_2)$, is a group.

Proof: ① Closure ✓

Given $(g_1 h_1)$ & $(g_2 h_2) \in G \times H$

We know: $\cdot\ g_1 \circ g_2 \in G$

$\cdot\ h_1 \circ h_2 \in H$

$\therefore (g_1 h_1) \circ (g_2, h_2) = (g_1 \circ g_2, h_1 \circ h_2) \in G \times H$

② Associativity: ✓

$$[(g_1, h_1) \circ (g_2, h_2)] \circ (g_3, h_3) = (g_1 g_2, h_1 h_2) \circ (g_3, h_3) = (g_1 (g_2 g_3), h_1 (h_2 h_3))$$

$$\rightarrow (g_1, h_1) \circ (g_2 \circ g_3, h_2 h_3) = (g_1 h_1) \circ [(g_2 h_2) \circ (g_3 h_3)]$$ ✓

③ Identity: Define identity $(e_G, e_H) = e_{G\times H}$ ⟶ check. ✓

i) $(e_G, e_H) \circ (g,h) = (e_G \circ g, e_H \circ h) = (g,h)$

$e_{G\times H} \circ X_{G\times H} = X_{G\times H}$ ✓

ii) $(g,h) \circ (e_G, e_H) = (g,h)$

$X_{G\times H} \circ e_{G\times H} = X_{G\times H}$ ✓

④ Existence of Inverse. ✓

- given an $(g,h) \longrightarrow$ define $(g,h)^{-1} = (g^{-1}, h^{-1})$

Check: $(g,h)\circ(g,h)^{-1} = (g,h)\circ(g^{-1},h^{-1})$

$= (g\circ g^{-1}, h\circ h^{-1})$

$= (e_G, e_H)$

$= e_{G\times H}$

What about a group of order 7?

$|G| = 7$

- holds for any prime order group

∴ $G\times H$ is a group under the defined product composition.

Eg, - four groups

G_2 of order 2.

G_4 of order 4

G_5 of order 5

elts in $G_2\times G_4$? $= 2\times 4 = 8$

$G_2\times G_4\times G_5 \Rightarrow$ order 40.

Suppose given a group of order 12.

Could $G_5 \times G_7 = 35$

12, 1

6, 2 → 322

4, 3 → 223

- How do properties of component group carry into the product

① Commutivity (Abelian)

Claim: If G & H are Abelian the G×H is Abelian.

Proof: Choose elts (g_1, h_1) & $(g_2 h_2)$ from G×H.

Then $(g_1, h_1) \circ (g_2 h_2) = (g_1 g_2, h_1 h_2)$

$= (g_2 g_1, h_2 h_1)$ - by commty of G & H

$\therefore (g_1, h_1) \circ (g_2, h_2) = (g_2, h_2) \circ (g_1, h_1)$ ∴ commute.

Abelian:

$a \cdot b = b \cdot a$

G & H Abelian → G×H Abelian

?

Claim

② Suppose every elt of G & H is its own inverse, ie, $g = g^{-1}$ & $h = h^{-1}$.

Then every elt of G×H is also its own inverse.

Proof: Choose $(g,h) \in G \times H$

Then $(g,h)^{-1} = (g^{-1}, h^{-1})$ by inverse in G×H

$(g,h)^{-1} = (g,h)$ by given property of inverse in G & H

H.) Powers of Elements of a Group.

Three Principles:

① Well Ordering Principle.

- suppose that A is a non-empty set of positive integers.
→ The A has a least element. ←

→ Equivalent to induction.

e.g. $A = \{2, 1, 4, 7\}$ $le(A) = 1$

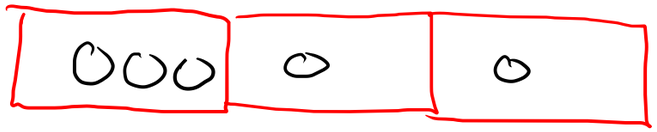
$A = \{2, 4, 6, 8, \ldots\}$ $le(A) = 2$

✗ $A = \{\ldots, -10, -8, -3, \ldots\}$

✗ $A = \{1, 1/2, 1/4, 1/8, 1/16, 1/32, \ldots\}$ $le(A) =$ doesn't exist.

② Pigeon Hole Principle.

5 pigeons
3 holes



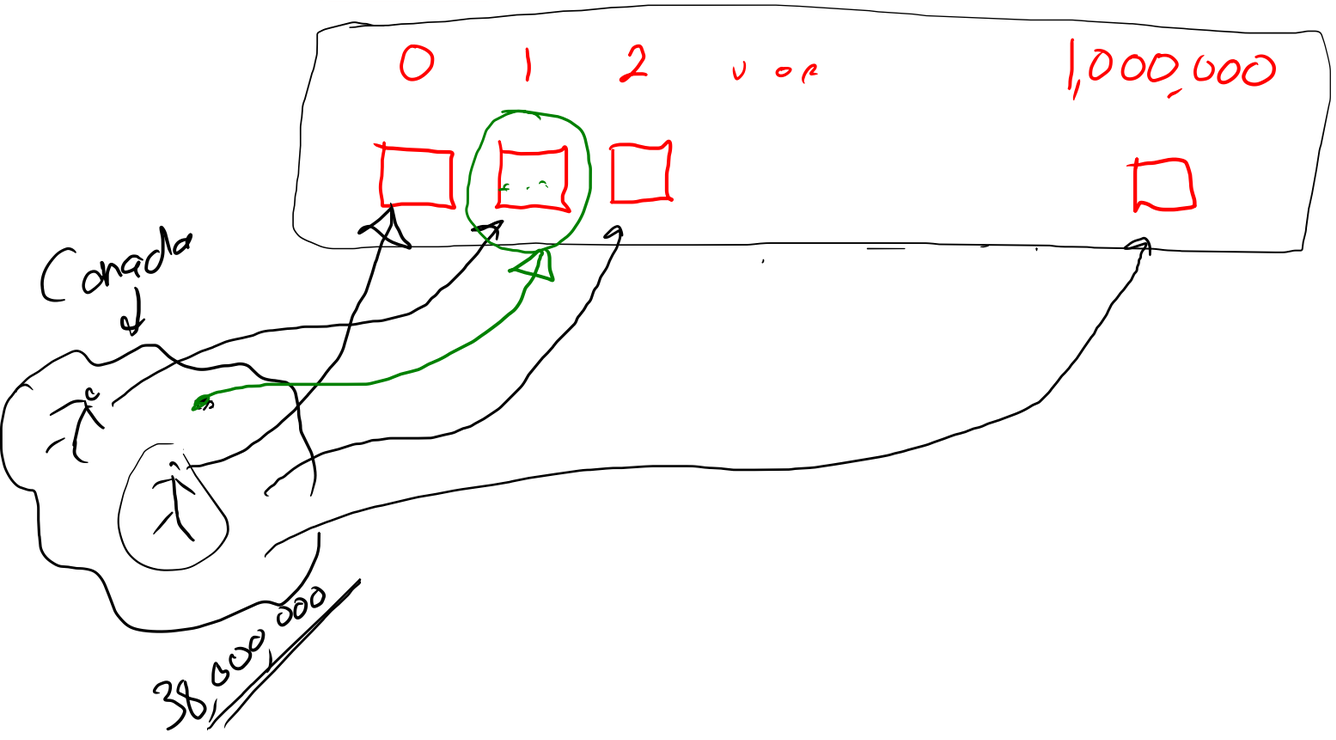
- if you have more pigeons than pigeon holes, then at least one pigeon hole has more than one pigeon.

---

eg. Canada has 38,000,000 people in it
→ there exist at least two ☆ the same number of hairs on their head.

Reason: typical has ≤ 1,000,000 hairs (typ 90,000 – 150,000)

Number hairs:



Existence Proof
→ not constructive.

② $[10] = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

- look at number pairs that differ by 5:

$(1,6)$ $(2,7)$ $(3,8)$ $(4,9)$ $(5,10)$. ← Pigeon holes.

- to guarantee two number differ by 5 need to pick.

③ Division Lemma - quotient & remainder lemma.

- if $m \& n \in \mathbb{Z}$ & $n > 0$

then $\exists$ unique q & $r \in \mathbb{Z}$

s.t. $m = nq + r$ ⟶ and $0 \leq r < n$.

$m = 5$
$n = 2$

$5 = 2 \cdot q + r$
$= 2 \cdot 2 + 1$