Math 4550

9/22/25

(Topic 3 continued...)

Ex: $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ ← group under $+$

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{ \underbrace{(\bar{0},\bar{0})}_{\text{identity element}}, (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1}) \}$$

Because both groups $G_1 = \mathbb{Z}_2$ and $G_2 = \mathbb{Z}_2$ are using addition instead of writing

$$(\bar{0},\bar{1})(\bar{1},\bar{1}) = (\bar{0}+\bar{1}, \bar{1}+\bar{1}) \underset{\bar{2}=\bar{0} \text{ in } \mathbb{Z}_2}{=} (\bar{1},\bar{0})$$

we write

$$(\bar{0},\bar{1}) \underset{\text{put + here}}{+} (\bar{1},\bar{1}) = (\bar{0}+\bar{1}, \bar{1}+\bar{1}) = (\bar{1},\bar{0})$$

Group table:

$\mathbb{Z}_2 \times \mathbb{Z}_2$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{0},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$
$(\bar{1},\bar{0})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$
$(\bar{0},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{0})$
$(\bar{1},\bar{1})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$	$(\bar{0},\bar{0})$

Sample calculations

$$(\bar{1},\bar{0})+(\bar{1},\bar{0})=(\bar{1}+\bar{1},\bar{0})=(\bar{0},\bar{0})$$

$$(\bar{1},\bar{1})+(\bar{1},\bar{1})=(\bar{1}+\bar{1},\bar{1}+\bar{1})=(\bar{0},\bar{0})$$

Two facts from table:

① $\mathbb{Z}_2 \times \mathbb{Z}_2$ is an abelian group

$$(\bar{a},\bar{b})+(\bar{c},\bar{d})=(\bar{c},\bar{d})+(\bar{a},\bar{b})$$

② Every element is its own inverse because

$$(\bar{a},\bar{b})+(\bar{a},\bar{b})=(\bar{0},\bar{0})$$

for all $(\bar{a},\bar{b})\in\mathbb{Z}_2\times\mathbb{Z}_2$.

Q: Is $\mathbb{Z}_2\times\mathbb{Z}_2$ cyclic?

Answer #1:

We would need an element of order 4, but all the elements are order 2. So its not cyclic.

Answer #2:

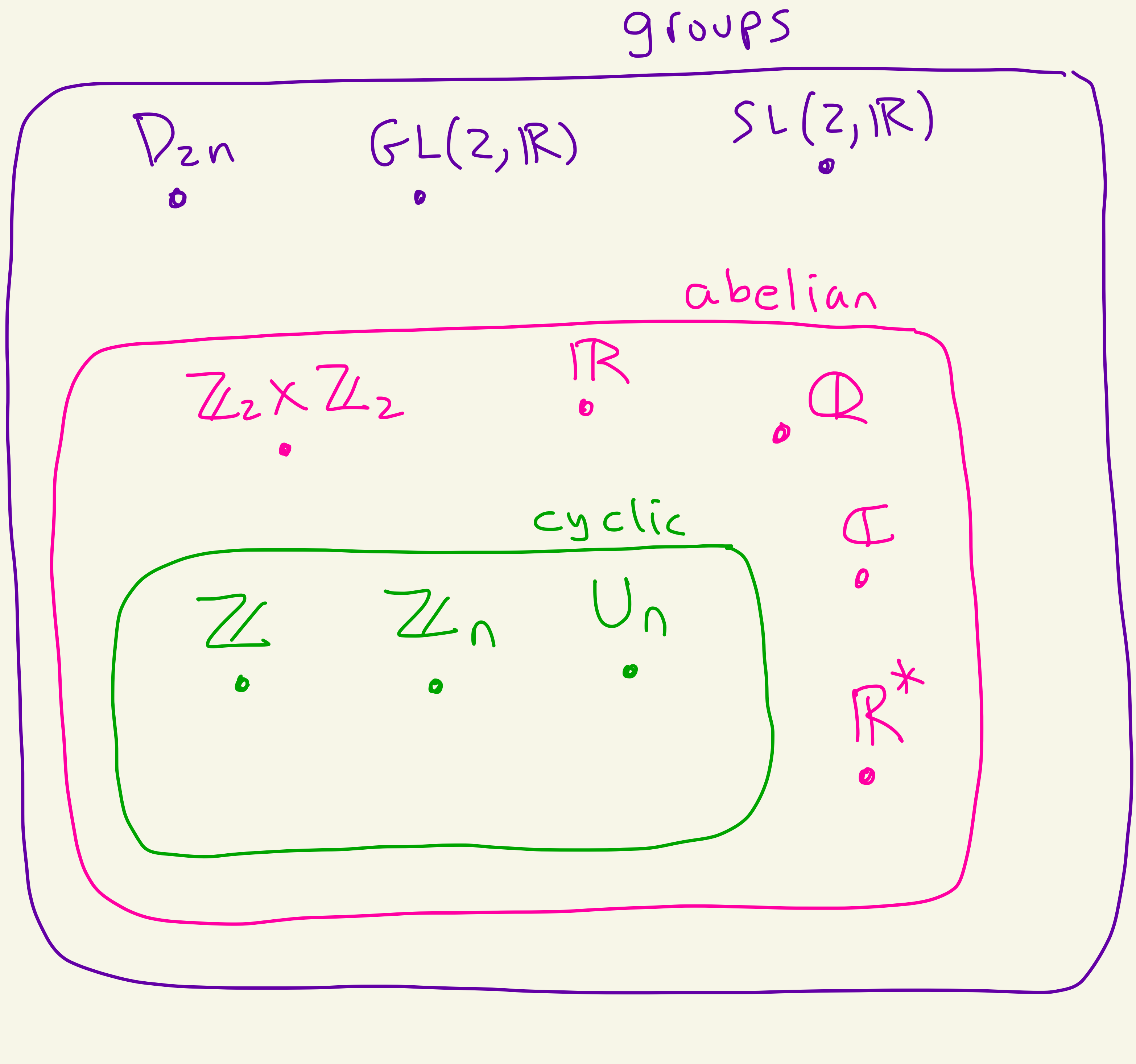
Let's see what each element generates.

$$\left.\begin{aligned}
\langle(\bar{0},\bar{0})\rangle &= \{(\bar{0},\bar{0})\}\\
\langle(\bar{1},\bar{0})\rangle &= \{(\bar{0},\bar{0}),(\bar{1},\bar{0})\}\\
\langle(\bar{0},\bar{1})\rangle &= \{(\bar{0},\bar{0}),(\bar{0},\bar{1})\}\\
\langle(\bar{1},\bar{1})\rangle &= \{(\bar{0},\bar{0}),(\bar{1},\bar{1})\}
\end{aligned}\right]$$

none of these are $\mathbb{Z}_2\times\mathbb{Z}_2$

So, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic

$\boxed{\text{PICTURE OF WORLD OF GROUPS}}$



Theorem: If G_1 and G_2 are both abelian groups, then $G_1 \times G_2$ is abelian.

Proof:

Let $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ where $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$

Then,

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$$

$$= (b_1 a_1, b_2 a_2)$$

Since G_1 is abelian and G_2 is abelian

$$= (b_1, b_2)(a_1, a_2).$$

So, $G_1 \times G_2$ is abelian ■

Theorem: $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m,n)=1$.

proof:

($\Leftarrow$) Suppose $\gcd(m,n)=1$.

We will show that $(\bar{1},\bar{1})$ generates all of $\mathbb{Z}_m \times \mathbb{Z}_n$.

Suppose that

$$\underbrace{(\bar{1},\bar{1})+(\bar{1},\bar{1})+\cdots+(\bar{1},\bar{1})}_{d \text{ times}} = \underbrace{(\bar{0},\bar{0})}_{\text{identity}}$$

where $d>0$.

Then,

$$(\bar{d},\bar{d})=(\bar{0},\bar{0})$$

So, $\bar{d} = \bar{0}$ in $\mathbb{Z}_m$ and

$\bar{d} = \bar{0}$ in $\mathbb{Z}_n$.

Thus, $d \equiv 0 \pmod{m}$ and $d \equiv 0 \pmod{n}$.

So, $m \mid (d-0)$ and $n \mid (d-0)$

So, $m \mid d$ and $n \mid d$,

So, d is a common multiple of m and n.

The least common multiple of m and n is $\dfrac{mn}{\gcd(m,n)}$ which in this case is mn.

gcd is 1

Thus, $d \geq mn$.

Also,

$$\underbrace{(\bar{1},\bar{1}) + (\bar{1},\bar{1}) + \cdots + (\bar{1},\bar{1})}_{mn \text{ times}} = (\overline{mn}, \overline{mn})$$

$$= (\bar{m}\cdot\bar{n}, \bar{m}\cdot\bar{n}) = (\bar{0}\cdot\bar{n}, \bar{m}\cdot\bar{0})$$

$\bar{m}=\bar{0}$ in $\mathbb{Z}_m$
$\bar{n}=\bar{0}$ in $\mathbb{Z}_n$

$$= (\bar{0}, \bar{0}).$$

Thus, $(\bar{1},\bar{1})$ has order mn.

So, $\underbrace{\mathbb{Z}_m \times \mathbb{Z}_n}_{\text{has } mn \text{ elements}} = \langle (\bar{1},\bar{1}) \rangle$

Thus, $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic with generator $(\bar{1},\bar{1})$.

$(\Rightarrow)$ "If $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, then $\gcd(m,n)=1$"

Contrapositive: "If $\gcd(m,n) \neq 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic"

Suppose $d = \gcd(m,n) > 1$.

Let $(\bar{r}, \bar{s}) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

We will show $(\bar{r}, \bar{s})$ cannot generate $\mathbb{Z}_m \times \mathbb{Z}_n$.

Then

$$\underbrace{(\bar{r}, \bar{s}) + (\bar{r}, \bar{s}) + \cdots + (\bar{r}, \bar{s})}_{\frac{mn}{d} \text{ times}} =$$

$\frac{mn}{d} \in \mathbb{Z}$ since d divides m and d divides n

$$= \left(\overline{\frac{mn}{d} r}, \overline{\frac{mn}{d} s} \right)$$

$$= \left(\overline{m} \cdot \overline{\frac{n}{d}} \cdot \overline{r}, \overline{n} \cdot \overline{\frac{m}{d}} \cdot \overline{s} \right)$$

$d | n$ so $\frac{n}{d} \in \mathbb{Z}$

$\boxed{d \mid m \text{ so } \frac{m}{d} \in \mathbb{Z}}$

$$= \left(\bar{0} \cdot \frac{n}{d} \cdot \bar{r}, \bar{0} \cdot \frac{m}{d} \cdot \bar{s}\right)$$

$\boxed{\begin{array}{l} \bar{m} = \bar{0} \text{ in } \mathbb{Z}_m \\ \bar{n} = \bar{0} \text{ in } \mathbb{Z}_n \end{array}}$

$$= (\bar{0}, \bar{0})$$

Thus, any element $(\bar{r}, \bar{s})$ of $\mathbb{Z}_m \times \mathbb{Z}_n$ has order at most $\frac{mn}{d} < mn$.

$\boxed{d > 1}$

Since $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements we know $(\bar{r}, \bar{s})$ cannot generate $\mathbb{Z}_m \times \mathbb{Z}_n$.

So, $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic $\blacksquare$