Math 4550

Topic 3 - Direct Products

<u>Def:</u> Let $G_1, G_2$ be groups.

The <u>direct product</u> of $G_1$ and $G_2$ is

$$G_1 \times G_2 = \{ (x_1, x_2) \mid x_1 \in G_1 \text{ and } x_2 \in G_2 \}$$

---

<u>Ex:</u>

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{ (\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2}) \}$$

---

<u>Ex:</u>

$$D_6 \times \mathbb{Z}_2 = \{ (1,\bar{0}), (r,\bar{0}), (r^2,\bar{0}), (s,\bar{0}), (sr,\bar{0}), (sr^2,\bar{0}), (1,\bar{1}), (r,\bar{1}), (r^2,\bar{1}), (s,\bar{1}), (sr,\bar{1}), (sr^2,\bar{1}) \}$$

---

Theorem: Let $G_1$ and $G_2$ be groups with identity elements $e_1$ and $e_2$, respectively. The direct product $G_1 \times G_2$ is a group under the operation

$$(a,b)(c,d) = (\underbrace{ac}_{\text{operation in } G_1}, \underbrace{bd}_{\text{operation in } G_2})$$

The identity element is $(e_1, e_2)$.
The inverse of $(a,b)$ is $(a^{-1}, b^{-1})$.

---

proof:

① (closure) Let $(a,b), (c,d) \in G_1 \times G_2$.
Then $a, c \in G_1$ and $b, d \in G_2$.
Since $G_1$ is a group we get $ac \in G_1$.
Since $G_2$ is a group we get $bd \in G_2$.
Thus, $(a,b)(c,d) = (ac, bd) \in G_1 \times G_2$.

② Let $(a,b), (c,d), (f,g) \in G_1 \times G_2$.

Then,
$$(a,b)\big[(c,d)(f,g)\big] = (a,b)\big[(cf, dg)\big]$$

$$= (a(cf), b(dg))$$

$$\overset{\text{Since } G_1 \text{ and } G_2 \text{ are groups and are associative}}{=} ((ac)f, (bd)g)$$

$$= [(ac, bd)](f,g)$$

$$= [(a,b)(c,d)](f,g)$$

Thus, $G_1 \times G_2$ is associative.

③ (identity)

Let $(a,b) \in G_1 \times G_2$.

Then,

$$(e_1, e_2)(a,b) = (e_1 a, e_2 b) = (a,b)$$

$$(a,b)(e_1,e_2) = (ae_1, be_2) = (a,b)$$

since $e_1$ is the identity of $G_1$ and $e_2$ is the identity of $G_2$

Thus, $(e_1, e_2)$ is an identity for $G_1 \times G_2$.

④ Let $(a,b) \in G_1 \times G_2$.

Then $a \in G_1$ and $b \in G_2$.

Since $G_1$ is a group we get that $a^{-1} \in G_1$

Since $G_2$ is a group we get that $b^{-1} \in G_2$.

Thus, $(a^{-1}, b^{-1}) \in G_1 \times G_2$ and we have:

$$(a,b)(a^{-1},b^{-1}) = (aa^{-1}, bb^{-1}) = (e_1, e_2)$$
$$(a^{-1},b^{-1})(a,b) = (a^{-1}a, b^{-1}b) = (e_1, e_2)$$

So, $(a^{-1}, b^{-1})$ is the inverse of $(a,b)$.

By ①, ②, ③, ④ we get that $G_1 \times G_2$ is a group. $\blacksquare$

---

**Ex:** Consider

$$D_6 \times \mathbb{Z}_2 = \{(1,\bar{0}), (r,\bar{0}), (r^2,\bar{0}), (s,\bar{0}), (sr,\bar{0}), (sr^2,\bar{0}), (1,\bar{1}), (r,\bar{1}), (r^2,\bar{1}), (s,\bar{1}), (sr,\bar{1}), (sr^2,\bar{1})\}$$

The identity is $(\underset{\text{identity of } D_6}{1}, \underset{\text{identity of } \mathbb{Z}_2}{\bar{0}})$

Some computations:

$$(r,\bar{1})(r^2,\bar{1}) = (rr^2, \bar{1}+\bar{1}) = (r^3, \bar{2}) = \underbrace{(1,\bar{0})}_{\text{identity}}$$

$\boxed{r^3 = 1}$

Thus,

$$(r,\bar{1})^{-1} = (r^2, \bar{1})$$

Here's another:

$$(sr, \bar{1})(r^2, \bar{0}) = (srr^2, \bar{1}+\bar{0}) = (sr^3, \bar{1}) \underset{r^3=1}{=} (s, \bar{1})$$

---

<u>Ex:</u> $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1})\}$

The identity element is $(\underbrace{\bar{0}}_{\text{identity of } \mathbb{Z}_2}, \underbrace{\bar{0}}_{\text{identity of } \mathbb{Z}_2})$

Since both groups use addition instead of writing $(\bar{0},\bar{1})(\bar{1},\bar{0}) = (\bar{0}+\bar{1}, \bar{1}+\bar{0}) = (\bar{1},\bar{1})$ we write $(\bar{0},\bar{1})+(\bar{1},\bar{0}) = (\bar{0}+\bar{1}, \bar{1}+\bar{0}) = (\bar{1},\bar{1})$.

Here's the group table:

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

You can see from the table that the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian.

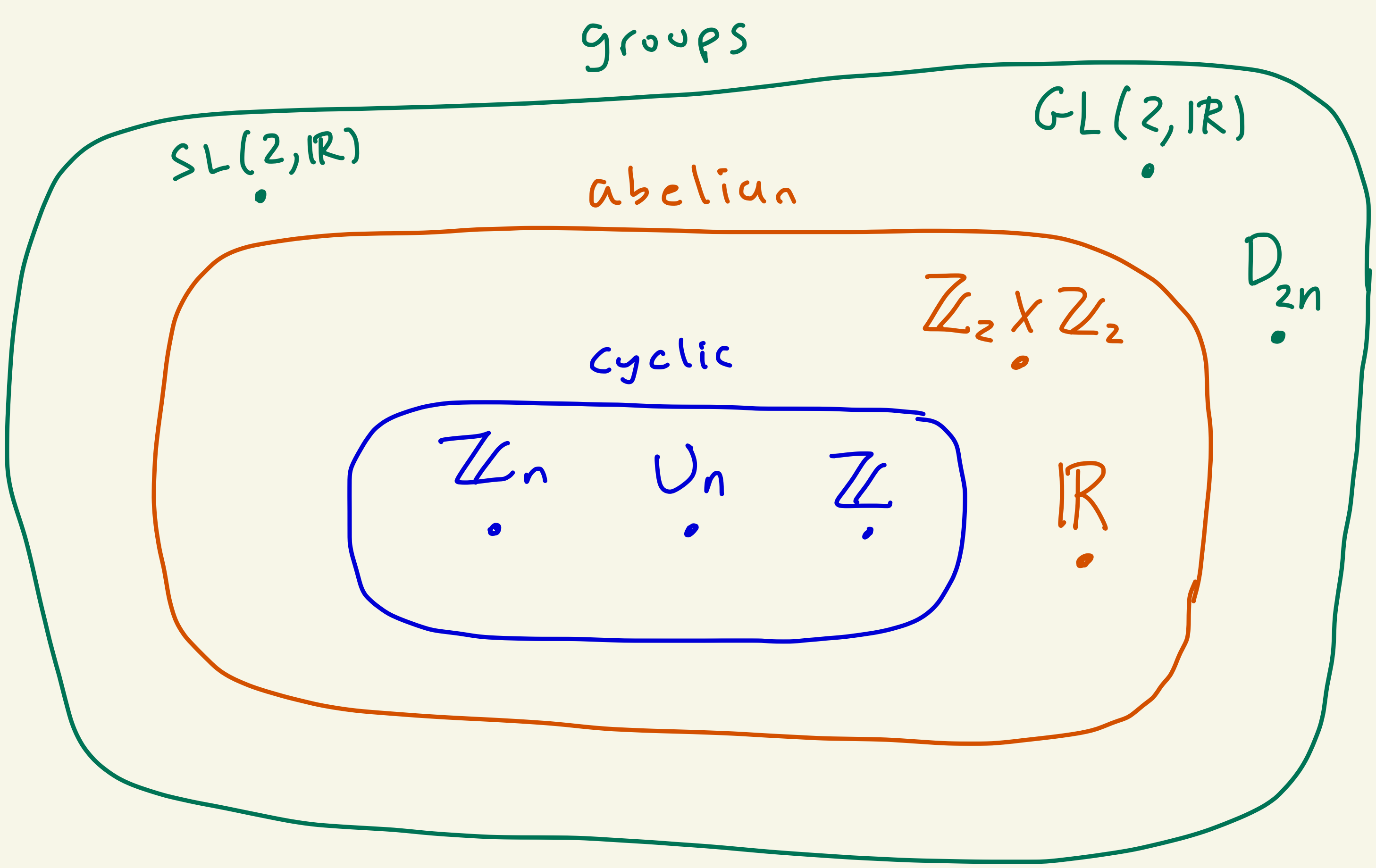
However it is not cyclic.

$$\langle(\bar{0},\bar{0})\rangle = \{(\bar{0},\bar{0})\}$$
$$\langle(\bar{1},\bar{0})\rangle = \{(\bar{1},\bar{0}),(\bar{0},\bar{0})\}$$
$$\langle(\bar{0},\bar{1})\rangle = \{(\bar{0},\bar{1}),(\bar{0},\bar{0})\}$$
$$\langle(\bar{1},\bar{1})\rangle = \{(\bar{1},\bar{1}),(\bar{0},\bar{0})\}$$

no element generates all of $\mathbb{Z}_2 \times \mathbb{Z}_2$ so $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Thus, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is abelian but not cyclic.

---



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

**proof:** HW $\square$

---

**Ex:** $\mathbb{Z}_n \times \mathbb{Z}_m$ is abelian

---

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

**proof:** (Don't do in class, point out in notes)

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

We will show that $\mathbb{Z}_m \times \mathbb{Z}_n = \langle(\bar{1},\bar{1})\rangle$.

Suppose that

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

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, $m$ divides $d$ and $n$ divides $d$.

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

From number theory, the least common multiple of $m$ and $n$ is $\frac{mn}{\gcd(m,n)}$ which in this case is $mn$.

Thus, $mn \le d$.

So the order of $(\bar{1},\bar{1})$ is at least $mn$.

Also,

$$\underbrace{(\bar{1},\bar{1})+(\bar{1},\bar{1})+\dots+(\bar{1},\bar{1})}_{mn \text{ times}} = (\underbrace{\overline{mn}}_{\bar{0} \text{ in } \mathbb{Z}_m}, \underbrace{\overline{mn}}_{\bar{0} \text{ in } \mathbb{Z}_n}) = (\bar{0},\bar{0})$$

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

So, $\mathbb{Z}_m \times \mathbb{Z}_n = \langle(\bar{1},\bar{1})\rangle$ since $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$.

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

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

Then,

$$\underbrace{(\bar{r},\bar{s})+(\bar{r},\bar{s})+\dots+(\bar{r},\bar{s})}_{\frac{mn}{d} \text{ times}} = \left(\overline{\tfrac{mn}{d} r}, \overline{\tfrac{mn}{d} s}\right)$$

(note: $d|m$ & $d|n$ so $\frac{mn}{d} \in \mathbb{Z}$)

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

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

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

($\frac{n}{d}, \frac{m}{d} \in \mathbb{Z}$ since $d|m$, $d|n$)

So, every element of $\mathbb{Z}_m \times \mathbb{Z}_n$ has order at most $\frac{mn}{d} < mn$ since $d > 1$. So, $\mathbb{Z}_m \times \mathbb{Z}_n$ is not cyclic if $\gcd(m,n) > 1$. $\square$