# Math 128A, Mon Oct 12

- Use a laptop or desktop with a large screen so you can read these words clearly.
- In general, please turn off your camera and mute yourself.
- Exception: When we do groupwork, please turn both your camera and mic on. (Groupwork will not be recorded.)
- Please always have the chat window open to ask questions.
- Reading for today: Ch. 8. Reading for one week from today: Ch. 9.
- PS06 due today.
- **EXAM 2 Mon Oct 19.** (on PS04-06, i.e., Chs. 4-7)
- Exam review Fri Oct 16, 10:00–noon on Zoom.

Last 20-25 min of class today: Open time to answer questions.

# External direct products

## Definition

$G$, $H$ groups. **External direct product** $G \oplus H$ is: the group defined by:

- Set: Cartesian product $G \times H = \{(g, h) \mid g \in G,\ h \in H\}$.
- Operation is componentwise:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Identity is: $(e_G, e_H)$

Inverse of $(g, h)$ is: $(g^{-1}, h^{-1})$

# Why external direct products?

Among other applications, they provide a convenient way to describe non-cyclic abelian groups. For example:

**Theorem**

*If $|G| = 4$, then either $G$ is cyclic, or $G$ is isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.*

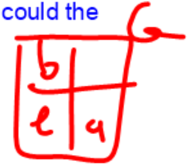
**Proof:**

Because |G| = 4, by Lagrange, any element of G has order 1, 2, or 4.
If G has an element a of order 4, then <a> has 4 elements, so G=<a> and G cyclic. So we may as well suppose that G has no elements of order 4, which means that it remains to show that if every element of G has order 2, then G is isomorphic to Z_2 x Z_2.

The only element of order 1 is the identity e, so every nonidentity element has order 2. Suppose a, b are distinct elements not equal to e. What could the order of ab be?

ord(ab)=1 $\Rightarrow$ ab=e

If ab=e, then



$aab = ae$ ← a on L

$a^2 = e$

when $a^2 = e$, $a^{-1} = a$

$b = a$; contra.

So $\text{ord}(ab) = 2$, and $(ab)^2 = e$

PS06 #6 G abelian

So we can construct Cayley of G

| | e | x | y | z |
|---|---|---|---|---|
| | e | | | |
| | | e | | |
| | | | e | |
| | | | | e |

| | e | a | b | ab |
|---|---|---|---|---|
| e | e | a | b | ab |
| a | a | e | ab | b |
| b | | | e | a |
| ab | | | | e |

$a^2 b$
$= eb$

Same Cayley as Z_2 x Z_2.
(Or if you go back to PS01, this is Cayley table of symmetries of painted cube.)

AKA Klein 4-group.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$

| $+$ | $\overset{e}{(0,0)}$ | $\overset{a}{(1,0)}$ | $\overset{b}{(0,1)}$ | $\overset{ab}{(1,1)}$ |
|---|---|---|---|---|
| $(0,0)$ | | | | |
| $(1,0)$ | $\overset{a}{(1,0)}$ | $\overset{e}{(0,0)}$ | $\overset{ab}{(1,1)}$ | $\overset{b}{(0,1)}$ |
| | | | | |

$$(1,0)+(1,0)=(2,0)=(0,0)$$

$(\text{mod } 2)$

## When is $G \oplus H$ cyclic?

We'll see that every finite abelian group is isomorphic to a group of the form $\mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_k}$, just like any positive integer is a product of primes.

Also, just as prime factorization is unique up to rearrangement, the form $\mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_k}$ is unique up to rearrangement and a particular kind of ambiguity.

$30 = 2 \cdot 3 \cdot 5$
$= 2 \cdot 5 \cdot 3$

To start:

### Theorem

*For $(g, h) \in G \oplus H$, if $\operatorname{ord}(g)$ and $\operatorname{ord}(h)$ are finite, then*

$$\operatorname{ord}((g, h)) = \operatorname{lcm}(\operatorname{ord}(g), \operatorname{ord}(h)).$$

**Proof:** $(g,h)^m = (g^m, h^m)$
That $= (e,e)$
when ord(g) div m

If ord(g) = k, then $g^m = e$ when k div m.

and ord(h) div m.

Smallest such pos m is, by defn,

LCM(ord(g), ord(h)).

## Counting orders of elements

ord 1, 3, 9

**Example:** Let $G = \mathbf{Z}_9 \oplus \mathbf{Z}_{27}$.

ord 1, 3, 9, 27

- A How many elements of order 9 are there in $G$?
- B How many cyclic subgroups of order 9 does $G$ have?

A: For ord(g, h) = 9, need

LCM(ord(g), ord(h)) = 9.

ord(g) = 9, ord(h) = 1

Order pairs

(9, 1) $6 \cdot 1$

(9, 3) $6 \cdot 2$

$\varphi(9) = 6$ (9, 9) $6 \cdot 6$

So there are 72 elements of order 9 in G.

$\varphi(3)=2$ $(1,9)$ $1\cdot 6$

$\varphi(1)=1$ $(3,9)$ $2\cdot 6$

Recall: $\mathbb{Z}_n$ has $\varphi(d)$ elts of order $d$ ($d$ div $n$)

(9,3): How many pairs (g,h) are there where ord(g) = 9 and ord(h) = 3? Well, Z_9 has phi(9) = 6 elements of order 9, and Z_27 has phi(3) = 2 elements of order 3, so there are 6*2 = 12 such pairs.

$\boxed{B}$

Every cyclic subgroup of order 9 has phi(9) = 6 generators, and each element of order 9 generates one cyclic subgroup. So there are 6 times as many elements as subgroups, so there are 72/6 = 12 subgroups of order 9.

# Back to "When is $G \oplus H$ cyclic?"

Ex $\mathbb{Z}_2 \oplus \mathbb{Z}_5 \simeq \mathbb{Z}_{10}$, but $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \not\simeq \mathbb{Z}_{12}$

**Theorem**

$G =$ $\mathbf{Z}_n \oplus \mathbf{Z}_k$ *is cyclic if and only if* $\gcd(n, k) = 1$.

**Proof:**

$$LCM(n,k) = \frac{nk}{\gcd(n,k)}$$

So $\max \operatorname{ord}(g,h)$

$= LCM(n,k) = nk$ iff $\gcd = 1$.

$G$ cyclic $\Leftrightarrow$ $G$ has elt ord $nk$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_6 \not\cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$$

$$\mathbb{Z}_3 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_{12}$$

# $U(n)$ as an external direct product

For $k$ dividing $n$, let U(n) = {all 1... n-1 that are r.p. to n}, operation *

$$U_k(n) = \{x \in U(n) \mid x \equiv 1 \pmod{k}\} . \leq U(n)$$

Theorem

*If* $\gcd(s,t) = 1$, *then* so: $\varphi(st) = \varphi(s)\varphi(t)$

$$U(st) \approx U(s) \oplus U(t).$$

*Also,* $U_s(st) \approx U(t)$ *and* $U_t(st) \approx U(s)$.

Proof delayed until Ch. 10.

**Facts:** We also have that $U(2)$ is trivial, and

$$U(4) \approx \mathbf{Z}_2$$

$$U(2^n) \approx \mathbf{Z}_{2^{n-2}} \oplus \mathbf{Z}_2 \qquad \text{for } n \geq 3$$

$$U(p^n) \approx \mathbf{Z}_{p^n - p^{n-1}} \qquad \text{for } n \geq 3,\ p \text{ an odd prime.}$$

I.e., U(p^n) is cyclic if p is an odd prime.

# Example of computing the isomorphism type of $U(n)$

Let $n = 63 = 3^2 \cdot 7$ .

Then $U(n)$ is:

$$U(63) \simeq U(9) \oplus U(7) \quad (\gcd(7,9) = 1)$$

$$U(63) \simeq \mathbb{Z}_6 \oplus \mathbb{Z}_6$$

elts $\equiv 1 \pmod 7$

$1 \pmod 9$

$\varphi(7) = 6$

$\varphi(9) = 6$

# Questions?

Ch 4

Sec 119 prob

Example: What can you say about a non-cyclic group of order 15?

Suppose |G|=15, G not cyclic.
By Lagrange, only possible orders of nontrivial elements of G are 3, 5, and 15.

Not cyclic = G has no elements of order 15, so only possible orders of elements are 3 and 5.

\# elts order 3 mult of $\varphi(3)=2$

" " " 5 mult of $\varphi(5)=4$

There are 14 elements of G not equal to e, so the possible numbers of nontrivial elements of different orders are:
* 12 elements order 5, 2 elements order 3
* 8 elements order 5, 6 order 3
* 4 order 5, 10 order 3
* 14 elements order 3.