External Products

"Put together two groups to get a single group out of them"

↳ any finite number!

also denoted $G \times H$

If G & H are groups, the external direct product $G \oplus H$ is the group where

$$G \oplus H = \{(g,h) \mid g \in G, h \in H\}$$

and the group operation is "componentwise"

$$(g,h) \cdot (g',h') = (gg', hh')$$

Thm. $|(g,h)| = \text{lcm}(|g|, |h|)$.

$D_3 = \{R_0, R_{120}, R_{240}, F_1, F_2, F_3\}$

Ex. Consider $D_3 \oplus \mathbb{Z}_2$

- Elements are $(R_0, 0)$, $(F_1, 0)$, $(R_{120}, 1)$, $(R_0, 1)$, ...
- $(R_0, 1)(R_{120}, 1) = (R_0 R_{120}, \underbrace{1+1}_{\text{mod } 2}) = (R_{120}, 0)$
- $(R_0, 1)$ has order 2
  - $(R_0,1)(R_0,1) = (R_0^2, 1+1) = (R_0, 0)$ is the identity elt (b/c identity in both coords)
  - $|(R_0,1)| = \text{lcm}(|R_0|, |1|) = \text{lcm}(1, 2) = 2.$
- $(R_{120}, 0)$ has order 3.
  - $|(R_{120},0)| = \text{lcm}(|R_{120}|, |0|) = \text{lcm}(3,1) = 3.$
- $(R_{120}, 1)$ has order 6.
  - $\text{lcm}(|R_{120}|, |1|) = \text{lcm}(3,2) = 6.$
- How many elements of order 2?

  $(R_0, 1)$

  $(F_1, 1)$ $(F_2, 1)$, $(F_3, 1)$.

  $(F_1, 0)$ $(F_2, 0)$, $(F_3, 0)$.

  Can't have anything of the form $(R_{120}, *)$ or $(R_{240}, *)$ because R_{120} & R_{240} have order 3, so these pairs will have order ≥ 3.
  $(R_0, 0)$ is not of order 2 b/c it's the identity (has order 1).

$U(n)$ as a product: next time!

1. $\mathbb{Z}_8 \oplus \mathbb{Z}_2$

How many elts of order 2 ?

$2 = |(a,b)| = \text{lcm}(|a|, |b|)$

we must have $|a| = 1$ or 2, $|b| = 1$ or 2, but we can't have $|a| = |b| = 1$.

Elements of order 1 or 2 in $\mathbb{Z}_8$: 0, 4.

Elements of order 1 or 2 in $\mathbb{Z}_2$: 0, 1.

$(0,1)$, $(4,0)$, $(4,1)$

3 elements of order 2.

How many elements of order 4 ?

$(2,0)$, $(2,1)$

2 has order 4 in $\mathbb{Z}_8$, so $|(2,\overset{1}{0})| = \text{lcm}(|2|, \overset{|1|}{|0|}) = \text{lcm}(4,\overset{2}{1}) = 4.$

$(6,0)$, $(6,1)$

6 also has order 4 in $\mathbb{Z}_8$. $|(6,1)| = \text{lcm}(|6|, |1|) = \text{lcm}(4,2) = 4.$

b/c

$6 = 6 \cdot 1$

order of $6 \cdot 1$ is $\dfrac{|1|}{\gcd(6,|1|)} = \dfrac{8}{\gcd(6,8)} = \dfrac{8}{4} = 2.$

using thm that says $|a^k| = \dfrac{|a|}{\gcd(|a|,k)}$

That's all of the elements:

$4 = |(a,b)| = \text{lcm}(\underbrace{|a|}_{\text{so this must be } 4}, \underbrace{|b|}_{1 \text{ or } 2})$

so this boils down to finding elements of order 4 in $\mathbb{Z}_8$.

By results on cyclic groups, we know 2 & 6 are the only such elts.

So a must be 2 or 6, and b can be either 0 or 1. so 4 elements total.

2. $D_3 \oplus D_3$

How many elts of order 3 ?

- $(R_{120}, \underbrace{*}_{\text{any rotation}})$ $\quad$ $(R_{240}, \underbrace{*}_{\text{any rotation}})$

$(R_{120}, R_{240})^2 = (R_{120}, R_{240}) \cdot (R_{120}, R_{240}) = (R_{240}, R_{120})$

$(R_{120}, R_{240})^3 = (R_{240}, R_{120}) \cdot (R_{120}, R_{240}) = (R_0, R_0).$

$|(R_{120}, R_{240})| = \text{lcm}(|R_{120}|, |R_{240}|) = \text{lcm}(3,3) = 3.$

- (R_0, R_{120}) & (R_0, R_{240}) also have order 3.

  $\mathrm{lcm}(1,3) = 3$.

- I have 8 elements.

- That's all of them because..

  if $3 = |(a,b)| = \mathrm{lcm}(|a|, |b|)$

  we must have $|a| = 1$ or 3, $|b| = 1$ or 3, & $|a|$ & $|b|$ are not both 1.

  In D_3, 3 elements have order 1 or 3 — namely, the rotations.

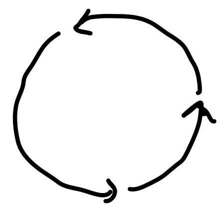
  So I have 9 elements in $D_3 \oplus D_3$ where both entries have order 1 or 3, but then we throw out the elt when both entries have order 1 (ie, the identity elt (R_0, R_0)).

Is this isomorphic to D_{18}?

In D_{18}, we only have 2 elements of order 3: R_{120}, R_{240}.

So the groups cannot be isomorphic!

use geometry, or note that rotations form a cyclic group of order 18, so can use results about cyclic groups



$\langle R_{360/18} \rangle$ the elts of order 3 are $R^k_{360/18}$ where k has property that $\gcd(k, 18) = 6$, b/c

$$|R^k_{360/18}| = \frac{18}{\gcd(k,18)} = 3.$$

$\iff \gcd(k,18) = 6.$

$\iff k = 6, 12.$

$R^6_{360/18} = R_{120}$ $\qquad$ $R^{12}_{360/18} = R_{240}.$

10. G finite grp, $|a|=2$, $|b|=3$. Must $|ab|$ divide 6?

- Obs: if a & b commute,

$$(ab)^6 = a^6 b^6 = (a^2)^3 (b^3)^2 = e^3 e^2 = e.$$

and so the order of ab must divide 6.

So, to find a counterexample, must consider G non-abelian.

- Obs: Might want to use dihedral group (it's familiar), but we can't.

in D_n, if $|b|=3$, then b is a rotation.

If a is a rotation, then a & b commute, and we're back in case 1.

If a is a reflection, ab is a reflection, and it has order 2, which divides 6.

- Try symmetric group!

Cayley's Thm says that any finite grp is isomorphic to a subgroup of S_n for some n. So, if there exists a counterexample at all, there must exist a counterexample in S_n!

Any elt of S_n of order 2 must be a 2-cycle.

Any elt of S_n of order 3 must be a 3-cycle.

If a & b are disjoint, then they'll commute & case 1 says order will divide 6 (in fact, then the order of ab is $\operatorname{lcm}(|a|,|b|) = \operatorname{lcm}(2,3) = 6$).

So we're looking for non-disjoint a & b.

$a = (1\,2)$ $\quad$ $b = (2\,3\,4)$

$$ab = (1\,2)(2\,3\,4) = (1\,2\,3\,4)$$

$|ab| = 4$ which does not divide 6.

Say G has order 12, or 24.
$|G|$ is div by 6
but $|ab|$ is not, eg in example we produced!
←
$(1\,2)(1\,2\,3)$
$= (1)(2\,3) = (2\,3)$
has order 2
$(1\,2)(1\,3\,2)$
$= (1\,3)$ has order 2

5. $\langle 2 \rangle$ in $U(7)$ operation is mult.

$H = \langle 2 \rangle = \{\ldots, 2^{-1}, 1, 2, 2^2, 2^3, \ldots\} = \{1,2,4\}$

$2^{-1} \to 4$, $1 \to 1$, $2 \to 2$, $2^2 \to 4$, $2^3 \to 1$

# of cosets is $\dfrac{|U(7)|}{3} = \dfrac{6}{3} = 2$

$\{1,2,4\} = H = 1H = 2H = 4H$

$\{3,5,6\} = 3H = 5H = 6H$

cosets partition group into disjoint pieces of equal sizes.

Ex. $H = \langle 6 \rangle = \{1, 6\}$ 3 cosets.

$2H = \{2,5\} = 5H$
$3H = \{3, 4\} = 4H.$ } the other 2

6. $\varphi: \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ aut with property that $\varphi(2) = 4$

Thm says $Aut(\mathbb{Z}_{10}) \approx U(10)$
$[\varphi(x) = cx] \longleftarrow c$

$U(10) = \{1,3,7,9\}$ so $\mathbb{Z}_{10}$ has 4 automorphisms

$c \in U(10)$	$\varphi(2)$
1	2
3	6
7	4 ←
9	8

only 1 aut. has $\varphi(2)=4$ and it's the one given by $\varphi(x) = 7x$.

8. H is a subgrp of D_{11}, contains at least 2 distinct reflections. F_1, F_2.
Then H also contains F_1F_2 which is a nontrivial rotation.
Let $R = F_1F_2$. This is a nontrivial elt of the cyclic subgroup of rotations, and there are 11 rotations, and 11 is prime, so R must have order 11, by Lagrange. So $R^0, R^1, \dots, R^{10}$ is all of the rotations in D_{11}.
But $R \in H$, so $R^0, \dots, R^{10} \in H$.
So I know that $\{\underbrace{R^0, \dots, R^{10}}_{11 \text{ elts}}, \underbrace{F_1, F_2}_{+2}\} \subseteq H$. So $|H| \geq 13$. But by Lagrange,
$|H|$ divides $|D_{11}| = 22$, so $|H| = 22$, ie, $H = D_{22}$.

10 (contd). Say G is a finite grp, $a, b \in G$, $|a| = 2$, $|b| = 3$. By Cayley, there exists a subgrp $H \leq S_n$ for some n such that $G \approx H$. Let $\varphi: G \to H$ be the isomorphism.
$|\varphi(a)| = 2$, $|\varphi(b)| = 3$. $|ab| = |\varphi(ab)|$.
The order of any element of H is the same even if I think of it as an element of S_n.

9. By Cayley, we know that $D_{12} \cong H$ for some subgroup $H \subseteq S_n$ for some n.

on Fri, we counted elts of D_{12} of order 2 & showed that its not the same as # of elts of order 2 in S_4. It will be true that D_{12} has same # of elts of order 2 as does H, but S_n might have more elements of order 2 than H...!

7.