Previously in Math 103a (before 2nd midterm!)

Direct (external) product of groups:

G_1, G_2 groups (any flavor!)

$$G_1 \oplus G_2 = \{(g_1, g_2) : g_1 \in G_1,\ g_2 \in G_2\}$$

with group multiplication

$$\boxed{(g_1, g_2)\cdot(g_1', g_2') = (g_1 g_1',\ g_2 g_2')}$$

identity $= (e_1, e_2)$ $\quad e_1 =$ id in G_1, $e_2 =$ id in G_2

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$$

Thm Order of $(g_1, g_2, \dots g_n)$

$$= \operatorname{lcm}(|g_1|, |g_2|, \dots, |g_n|)$$

Ex. $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$

$(1,0) + (0,1) = (1,1)$ $\quad (0,1) + (1,1) = (1,0)$

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

Abstractly: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \{e, a, b, c\}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Ex 1. How many elements of order 4 are in $\mathbb{Z}_{16} \oplus \mathbb{Z}_4$?

Ans Use Theorem!

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

$$\therefore \quad |(a,b)| = 4 \iff 4 = \text{lcm}(|a|,|b|)$$

$|a| = 1, 2, 4, 8, \text{ or } 16$ since $|a| \mid 16$

$|b| = 1, 2, \text{ or } 4$

# of elts of order k in $\mathbb{Z}_n$ is $\varphi(k)$ if $k \mid n$

φ = phi function

$\lvert a\rvert$	$\lvert b\rvert$
1	4
2	4
4	1
4	2
4	4

$1 \times \varphi(4) = 2$ such elts

$1 \times \varphi(4) = 2$

$\varphi(4) \times 1 = 2$

$\varphi(4) \times 1 = 2$

$\varphi(4) \times \varphi(4) = 4$

12 elts order 4

Ex 2 How many cyclic subgroups of order 10 in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$?

Ans Not so easy! First find all elts of order 10

$|a| = 1, 2, 5, 10, \cancel{20}, \cancel{25}, \cancel{50}$

$|b| = 1, 5$

$\lvert a\rvert$	$\lvert b\rvert$
2	5
10	1
10	5

4
4
$4 \times 4 = 16$

24 elts order 10

If a group has 24 elements of order 10, how many cyclic subgroups of order 10?

Observation: If $|a| = 10$, and $a \in H_1 \cap H_2$, where H_1 & H_2 are subgroups with $|H_1| = |H_2| = 10$ then $H_1 = H_2$. Reason: $\langle a \rangle \subset H_1$, $\langle a \rangle \subset H_2$ $|\langle a \rangle| = |H_1| = |H_2| \Rightarrow \langle a \rangle = H_1 = H_2$.

Each cyclic subgroup of order 10 contains $\varphi(10) = 4$ elements of order 10. Since each element of order 10 belongs to just one subgroup,

$$24 = \#(a \in G : |a| = 10) = \#(H : \text{cyclic}, |H| = 10) \times 4$$

$\therefore$ there are 6 cyclic subgps of order 10

Q: When is $\mathbb{Z}_n \oplus \mathbb{Z}_2$ cyclic?

Thm If G_1, G_2 cyclic groups, then

$$G_1 \oplus G_2 \text{ cyclic} \iff \gcd(|G_1|, |G_2|) = 1$$

Pf This is pretty easy.

$\Leftarrow$ Suppose $\gcd(|G_1|, |G_2|) = 1$. Choose $a \in G_1$ with $|a| = |G_1|$ & $b \in G_2$ with $|b| = |G_2|$

Then Thm says $|(a,b)| = \text{lcm}(|G_1|, |G_2|) = \dfrac{|G_1| \cdot |G_2|}{\gcd(|G_1|, |G_2|)}$

$= |G_1| \cdot |G_2|$

$= |G_1 \oplus G_2|$

Similarly, if $\gcd(|G_1|, |G_2|) > 1$, there is no (a,b) with $|(a,b)| = |G_1 \oplus G_2|$, so $G_1 \oplus G_2$ is not cyclic.

True for any number of factors:

$G_1 \oplus G_2 \oplus \cdots \oplus G_m$ cyclic $\iff$ $\operatorname{lcm}(|G_1|, |G_2|, \ldots |G_m|)$
$= |G_1| \times |G_2| \times \cdots \times |G_m|$
$\iff \gcd(|G_1|, |G_2|, \ldots, |G_m|) = 1$.

Ex $\quad \mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_6$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ not cyclic

$\mathbb{Z}_7 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \approx \mathbb{Z}_{84}$.

Thm If $\gcd(s,t) = 1$, then

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

This is harder to prove. The isomorphism Φ is given by

$$\Phi: U(st) \to x \longmapsto (x \bmod s, x \bmod t)$$

First: $|U(st)| = |U(s)| \times |U(t)|$ since

$|U(st)| = \varphi(st) = \varphi(s)\varphi(t)$ if $\gcd(s,t) = 1$

φ function $\qquad\qquad$ $= |U(s)| \times |U(t)|$

So if Φ is 1-1, then it's onto.

Also have to check Φ preserves multiplication.

Instead of proving these, let's look at an example.

Ex $U(12) \approx U(4) \oplus U(3)$

$$x \longmapsto (x \bmod 4,\ x \bmod 3)$$

$x \bmod 4$ & $x \bmod 3$ determines $x \bmod 12$

since

$$\left.\begin{aligned} x &= 4q_1 + r_1 \\ x &= 3q_2 + r_2 \end{aligned}\right\} \Rightarrow \begin{aligned} 3x &= 12q_1 + 3r_1 \\ 4x &= 12q_2 + 4r_2 \end{aligned}$$

$$\Rightarrow x = 12(q_2 - q_1) + 4r_2 - 3r_1$$

$$\therefore x = (4r_2 - 3r_1) \bmod 12$$

$\therefore$ 1-1

Preserving multiplication is trickier

Note that $(n \bmod 12) \bmod 4 = n \bmod 4$

check it!

Let's try $\Phi(5)\Phi(7)$

$$\Phi(5) = (5 \bmod 4,\ 5 \bmod 3) = (1, 2)$$
$$\Phi(7) = (7 \bmod 4,\ 7 \bmod 3) = (3, 1)$$

$$\Phi(5) \cdot \Phi(7) = (3 \bmod 4,\ 2 \bmod 3) = (3, 2)$$

$$\Phi(5 \times 7) = ((5 \bmod 4)(7 \bmod 4),\ (5 \bmod 3)(7 \bmod 3))$$
$$= (3, 2)$$

see how the terms match up!