Lecture 9

External Direct Product

- allow us to construct bigger groups out of smaller groups
- essential language for classification problems (e.g. classification of the group $U(n)$, finite abelian groups)

Def: Let $G_1, G_2, \cdots, G_n$ be a collection of groups. We define the **external direct product** of $G_1, \cdots, G_n$ written

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, \cdots, g_n) \mid g_i \in G_i\} = \{n \text{ tuples of elements where the } i\text{th element is in } G_i\}$$

multiplication rule:

$$(g_1, \cdots, g_n) \cdot (g_1', \cdots, g_n') = (g_1 g_1', g_2 g_2', \cdots, g_n g_n')$$

Facts:
- The identity element of $G_1 \oplus \cdots \oplus G_n$ is $(e, \cdots, e)$
- If $(g_1, \cdots, g_n) \in G_1 \oplus \cdots \oplus G_n$, then $(g_1, \cdots, g_n)^{-1} = (g_1^{-1}, \cdots, g_n^{-1})$

Example:

① $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$

② $\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$

③ $\mathbb{Z} \oplus S_6 = \{(n, \sigma) \mid n \in \mathbb{Z}, \sigma \in S_6\}$

$(n, \sigma) \cdot (m, \alpha) = (n+m, \sigma\alpha)$

④ $U(8) \oplus U(10) = \{(1,1), (1,3), (1,7), (1,9), (3,1), (3,3), (3,7), (3,9), (5,1), (5,3), (5,7), (5,9), (7,1), (7,3), (7,7), (7,9)\}$

⑤ $(3,7), (7,7) \in U(8) \oplus U(10)$

$(3,7) \cdot (7,7) = (5,9)$

Now consider $(3,7), (7,7) \in U(8) \oplus U(8)$

$(3,7) \cdot (7,7) = (5,1)$

Facts: if $G_1, \cdots, G_n$ are all finite groups, then

$$|G_1 \oplus \cdots \oplus G_n| = |G_1| \cdots |G_n|$$

Proposition: **groups of order 1**: They're all isomorphic to a set $\{e\}$ s.t. e is the identity cyclic.

groups of order 2: let $G = \{e, x\}$ Then $x^2 \neq x$ So $x^2 = e$. Therefore $|x| = 2$. All groups of order 2 are cyclic.

groups of order 3: cyclic

groups of order 4: not all groups of order 4 are cyclic. i.e. $U(8) = \{1, 3, 5, 7\}$ but $U(8)$ is not cyclic.
later we'll see $U(8) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Proposition: Suppose G is a group of order 4. Then either $G \approx \mathbb{Z}_4$ or $G \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Proof: If $\exists\, g \in G$ s.t. $|g|=4$, then G is cyclic
So $G \approx \mathbb{Z}_4$
So let's assume G doesn't have any elements of order 4.

Recall: If G is a finite group, $|g| \mid |G|$ for all $g \in G$
This is b/c $|g| = |\langle g \rangle|$. And Lagrange thm says $|\langle g \rangle| \mid |G|$
So g must have order 1 or 2.
write $G = \{e, a, b, ab\}$
$ab = ba$, G is Abelian
Define $\phi : G \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by
$\phi(e) = (0,0)$,
$\phi(a) = (1,0)$
$\phi(b) = (0,1)$
$\phi(ab) = (1,1)$
Exercise: verify ϕ is an isomorphism

groups of order 5: cyclic

general fact: If $|G| = p$, a prime, G is cyclic

groups of order 6: all groups of order 6 are either { isomorphic to $\mathbb{Z}_6$ / isomorphic to D_3

Last time, we proved that if $|G| = 2p$ where p is an odd prime. Then either $G \approx \mathbb{Z}_{2p}$ or $G \approx D_p$.

$D_3 \approx S_3$

Fact: Up to isomorphism, S_3 is the smallest non-abelian group.

Example: consider $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. What is the order of $(1,1)$?
The order is 6.

$(1,1)^n = (n,n) = (0,0)$
Q: What's the smallest positive integer s.t. $n \equiv 0 \mod 2$ and $n \equiv 0 \mod 3$
$n = 6$
So $|(1,1)| = 6$

Conclusion: $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic
In general, $\mathbb{Z}_n \oplus \mathbb{Z}_m$ need not be cyclic i.e. $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

every element has order 2
Theorem: Sps $G_1, \cdots, G_n$ are finite groups. then $|(g_1, \cdots, g_n)| = \operatorname{lcm}(|g_1|, \cdots, |g_n|)$

proof: consider all positive integers s s.t.
$(g_1, \cdots, g_n)^s = (e, \cdots, e)$
i.e. $g_1^s = e$, $g_2^s = e$, $\cdots$, $g_n^s = e$
So s must be a multiple of $|g_1|, \cdots, |g_n|$
So it is clear that the least such s is given by $\operatorname{lcm}(|g_1|, \cdots, |g_n|)$

Example: What are the possible orders of elements in $\mathbb{Z}_2 \oplus \mathbb{Z}_4$?

$\mathbb{Z}_2$: possible orders: 1, 2

$\mathbb{Z}_4$: possible orders: 1, 2, 4

Answers: $\text{lcm}(1,1), \text{lcm}(1,2), \text{lcm}(1,4)$

$\text{lcm}(2,1), \text{lcm}(2,2), \text{lcm}(2,4)$

In particular, we see $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ is not cyclic

Example: How many elements of $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ have order 5?

		elements of order	
$\mathbb{Z}_{25}$ has	1		1
	4		5
	20		25
$\mathbb{Z}_5$	1		5
	4		5

If $(x,y) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t. $|(x,y)|=5$, then $\text{lcm}(|x|,|y|)=5$

possibilities:

$|x|=1$, $|y|=5$: 4 such pairs

$|x|=5$, $|y|=5$: 16 such pairs

$|x|=5$, $|y|=1$: 4 such pairs

$\Rightarrow$ 24 elements of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$

since 5 elements of order 25. $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ is not cyclic

Thm: Let G, H be finite cyclic groups. Then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime

Proof:

($\Leftarrow$) Suppose $|G|, |H|$ are relatively prime. Let $g \in G$, $h \in H$ be generators. Then

$$|(g,h)| = \text{lcm}(|g|,|h|) = \text{lcm}(|G|,|H|) = \frac{|G| \cdot |H|}{\gcd(|G|,|H|)} = |G| \cdot |H|$$

($\Rightarrow$) Suppose $G \oplus H$ is cyclic

Suppose $(g,h) \subseteq G \oplus H$ is a generator. Then

$|(g,h)| = \text{lcm}(|g|,|h|) = |G| \cdot |H| = \text{lcm}\left(\frac{|G|}{m}, \frac{|H|}{k}\right)$ for some positive integers, m, k

$$\leq \text{lcm}(|G|,|H|) = \frac{|G| \cdot |H|}{\gcd(|G|,|H|)}$$

The only way this true is if $\gcd(|G|,|H|)=1$.

Corollary: Sps $G_1, \cdots G_n$ are finite cyclic groups. Then $G_1 \oplus \cdots \oplus G_n$ is cyclic iff $|G_1|, \cdots, |G_n|$ are pairwise relatively prime.

i.e. $\forall\, i \neq j$, $\gcd(|G_i|,|G_j|)=1$

Corollary: Let $n_1, \cdots, n_k$ be positive integers and $m = n_1 \cdots n_k$

Then $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k} \approx \mathbb{Z}_m$ iff $n_1, \cdots, n_k$ all pairwise relatively prime.

Def: let $n \geq 1$ be an int., let k be a divisor of n.
Then we define $U_k(n) = \{x \in U(n) \mid x \equiv 1 \bmod k\}$

Exercise: prove that $U_k(n)$ is a subgroup

Thm: let $s, t > 1$ be integers. Sps $\gcd(s,t) = 1$
Then $U(st) \approx U(s) \oplus U(t)$
Moreover, $U_s(st) \approx U(t)$
$U_t(st) \approx U(s)$

Proof: Define $\varphi: U(st) \to U(s) \oplus U(t)$ by
$\varphi(x) = (x \bmod s, x \bmod t)$

Exercise: verify that φ is an isomorphism.

Corollary: if $m = n_1 \cdot n_2 \cdots n_k$ s.t. $n_1, \dots, n_k$ are pairwise relatively prime,
then $U(m) \approx U(n_1) \oplus \cdots \oplus U(n_k)$
Let n be a positive integer, want to understand $U(n)$ factor n into primes

$n = p_1^{k_1} \cdots p_m^{k_m}$ where $p_1, \dots, p_m$ are distinct primes.
Then $U(n) \approx U(p_1^{k_1}) \oplus \cdots \oplus U(p_m^{k_m})$

Gauss Thm
$U(2) = \mathbb{Z}_1$ $U(4) = \mathbb{Z}_2 \oplus \mathbb{Z}_2$
$U(2^n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-1}}$ $n \geq 3$
If p is an odd prime
$U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}$

Example: $U(10) \approx U(2) \oplus U(5)$
$\approx \mathbb{Z}_1 \oplus \mathbb{Z}_4$
$\approx \mathbb{Z}_4$
$U(8) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$
$U(12) \approx U(3) \oplus U(4) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$
$U(105) \approx U(3) \oplus U(5) \oplus U(7) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$