Previously in Math 103a

G group of permutations of a set S, $i \in S$.

$\text{stab}_G(i) = \{\varphi \in G : \varphi(i) = i\} \subset G$ stabilizer of i

$\text{orb}_G(i) = \{\varphi(i) : \varphi \in G\} \subset S$ orbit of i

$\text{stab}_G(i)$ is a subgroup of G.

Orbit-Stabilizer Thm: $|G| = |\text{stab}_G(i)|\,|\text{orb}_G(i)|$

for any $i \in S$

Ex: Find $|G|$, the order of the group of rotations of a cube. (See previous notes.)

Mini-review: True or false questions. If true, give a reason. If false, give a counter-example.

(1) If $35 \mid ab$, where a and b are integers, then $7 \mid a$ or $7 \mid b$.

(2) If $a \in G$, a group, and $|a| = 2n+1$, n positive integer, then $\langle a^2 \rangle = \langle a \rangle$.

(3) If $\varphi \in S_5$, then $|\varphi| \leq 5$.

(4) If H is a proper subgroup of a group G, then $H \neq G$.

(5) If $H \leq G$, and H is nonabelian, then G is nonabelian.

Answers at end.

Putting groups together –

Direct (external) product

Suppose G_1, G_2 groups. Is there an "obvious" way to put a group multiplication on the set $G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$?

Ex 1. $G_1 = \mathbb{Z}_3$, $G_2 = \mathbb{Z}_5$ $\quad |G_1 \times G_2| = 15$

Try to add components separately:

e.g. put $(1,3) + (2,4) = ((1+2) \bmod 3, (3+4) \bmod 5)$

$= (0,2) \in \mathbb{Z}_3 \times \mathbb{Z}_5$

Identity $= (0,0)$ ✓

Inverses $(j,k)^{-1} = ((-j) \bmod 3, (-k) \bmod 5)$

e.g. $(2,4)^{-1} = ((-2) \bmod 3, (-4) \bmod 5)$

$= (1,1)$

check: $(2,4) + (1,1) = (0,0)$ in $\mathbb{Z}_3 \times \mathbb{Z}_5$

Call this group $\mathbb{Z}_3 \oplus \mathbb{Z}_5$

direct (external) product of $\mathbb{Z}_3$ & $\mathbb{Z}_5$.

Note that $\mathbb{Z}_3$ is isomorphic to a subgroup of $\mathbb{Z}_3 \oplus \mathbb{Z}_5$ by $\Phi(i) = (i,0)$

$\Phi(0) = (0,0)$
$\Phi(1) = (1,0)$
$\Phi(2) = (2,0)$

Same is true for $\mathbb{Z}_5$

$\mathbb{Z}_3 \oplus \mathbb{Z}_5$ is abelian.

Ex 2. $G_1 = S_2$, $G_2 = S_3$

$$G_1 \times G_2 = \{(\alpha, \beta) : \alpha \in S_2, \beta \in S_3\}$$

How to multiply? $(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = ?$

Can think of (α_i, β_i) acting on $\{1,2\}$ & $\{3,4,5\}$ separately

since α_i permutes 2 things &
β_i permutes 3 things

Then $(\alpha_1, \beta_1)\cdot(\alpha_2, \beta_2)\,(i,j)$ $\quad 1 \le i \le 2$, $3 \le j \le 5$

$= (\alpha_1, \beta_1)\,(\alpha_2(i), \beta_2(j))$

$= (\alpha_1(\alpha_2(i)), \beta_1(\beta_2(j))) = ((\alpha_1 \circ \alpha_2)(i), \beta_1 \circ \beta_2(i))$

(mult in S_2; mult in S_3)

So we should put $(\alpha_1, \beta_1)\cdot(\alpha_2, \beta_2) = (\alpha_1 \cdot \alpha_2, \beta_1 \cdot \beta_2)$

(mult in S_2; mult in S_3)

that is, multiplication in $S_2 \oplus S_3$ is component wise. $S_2 \oplus S_3$ is nonabelian. Why?

Formal definition: Let $G_1, G_2, \ldots, G_n$ groups. The (external) direct product of $G_1, \ldots, G_n$, written $G_1 \oplus G_2 \oplus \cdots \oplus G_n$

is the set $G_1 \times G_2 \times \cdots \times G_n$ with group mult. defined componentwise, i.e.,

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

Ex. If $|G|=4$, then either $G \approx \mathbb{Z}_4$ or $G \approx \mathbb{Z}_2 \times \mathbb{Z}_2$.

Reason: If $a \in G$, then by Lagrange's Thm, $|a|$ divides $|G|=4$. If $a \neq e$, then $|a|=4$ or $|a|=2$.

If $\exists\ a \in G$ with $|a|=4$, then $\langle a \rangle = G$ (why?)

& $G \approx \mathbb{Z}_4$, since both are cyclic of order 4.

An isomorphism is given by $\Phi(a)=1$, since 1 is a generator of $\mathbb{Z}_4$. Suppose $\nexists\ a \in G$ of order 4. Then all elements in G are of order 2, except e. Let $a, b \in G$, $a \neq b$, $a \neq e$, $b \neq e$. Then $ab \neq e$ & $ab \neq b$, $ab \neq a$

check this! $\therefore G = \{e, a, b, ab\}$, and $|ab|=2$.

Since $(ab)^2 = e = a^2 b^2$, we have

$$abab = a^2 b^2 \Longrightarrow ab = ba.$$

Define $\Phi : G \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$\begin{aligned} \Phi(e) &= (0,0) \\ \Phi(a) &= (1,0) \\ \Phi(b) &= (0,1) \\ \Phi(ab) &= (1,1) \end{aligned}$$

(Note that $\Phi(ab) = (1,1) = (1,0)+(0,1) = \Phi(a)+\Phi(b)$

Easy to check Φ preserves mult (which is addition mod 2 in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$).

Orders of elements in $G_1 \oplus G_2 \oplus \cdots \oplus G_n$:

Thm. $|(g_1, g_2, \ldots, g_n)| = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_n|)$

Does this remind you of something?

Recall: if σ, τ are disjoint cycles in S_n, then $|\sigma\tau| = \operatorname{lcm}(|\sigma|, |\tau|)$ (*)

(this is still true for a product of any finite number of disjoint cycles.)

In fact (*) follows from the Theorem above for direct products, by identifying the product $\sigma\tau$ as an element of $S_n \oplus S_n$

$\sigma\tau \longleftrightarrow (\sigma, \tau)$

Here's an example.

Ex. $n = 5$ $\sigma = (1,2)$, $\tau = (3,4,5)$ disjoint cycles.

Then $(\sigma, \tau) \in S_5 \oplus S_5$ since they act on separate sets of numbers:

$\sigma\tau(1) = 2$	$(\sigma,\tau)(1,1) = (2,1)$
$\sigma\tau(2) = 1$	$(\sigma,\tau)(2,1) = (1,1)$
$\sigma\tau(3) = 4$	$(\sigma,\tau)(3,3) = (3,4)$
$\sigma\tau(4) = 5$	$(\sigma,\tau)(3,4) = (3,5)$
$\sigma\tau(5) = 3$	$(\sigma,\tau)(3,5) = (3,3)$

Can check $(\sigma,\tau)^k = e \iff \sigma^k = e,\ \tau^k = e$

$\iff (\sigma\tau)^k = e$.

Answers to T-F questions

① True. $35 = 5 \times 7$, $35 \mid ab \Rightarrow 7 \mid ab$

$\Rightarrow 7 \mid a$ or $7 \mid b$

since 7 is prime. (Euclid's Lemma)

② True. Thm says $\langle a^j \rangle = \langle a \rangle \Leftrightarrow \gcd(j, n) = 1$, where $n = |a|$.

$\gcd(2, 2n+1) = 1 \Rightarrow \langle a^2 \rangle = \langle a \rangle$.

③ False. Take $\varphi = (1,2)(3,4,5)$

Then $|\varphi| = \operatorname{lcm}(|(1,2)|, |(3,4,5)|) = 6$

(It is true that $\varphi \in S_5 \Rightarrow |\varphi| \leq 6$.)

④ False. Take $G = \mathbb{Z}$, $H = 2\mathbb{Z} \subset G$

Then $\Phi : \mathbb{Z} \to 2\mathbb{Z}$ given by

$\Phi(n) = 2n$ is an isomorph.

$\Phi(n+m) = 2(n+m) = 2n+2m = \Phi(n) + \Phi(m)$

Φ is 1-1 & onto.

(It is true if $|G| < \infty$.)

⑤ True. If $\exists\ a, b \in H$ s.t. $ab \neq ba$

then take same $a, b \in G$.