

2/12

- Quiz (Jupiter ~~can~~ take a

- S_n cycle decomposition

Cyclic subgroup $\exists o(g) < \infty$ say $o(g) = n$ least pos.
natural
s.t. $g^n = e$

$o(e) = 1$ $\langle g \rangle = \{g, g^2, \dots, g^{n-1}, g^n = e\}$. $|\langle g \rangle| = n$.

Question what is $o(g^j)$? $j \in \mathbb{N}$ (fixed)

so what is least k s.t. $(g^j)^k = e$.
pos.

$\mathbb{Z}_{10}$ $= \langle 1 \rangle = \{1, 2, \dots, 9, 0\} = \langle 9 \rangle$ $o(g) = o(g^{-1})$
 $o(9) = 10$

$\langle 2 \rangle = \{2, 4, 6, 8, 0\}$ $o(2) = 5 = o(8)$

$\langle 4 \rangle = \{4, 8, 2, 6, 0\}$ $o(4) = 5 = o(6) = 5$

$\langle 8 \rangle = \{8, 6, 4, 2, 0\}$ $o(5) = 2$

$\langle 5 \rangle = \{5, 0\}$

$\langle 3 \rangle = \{3, 6, 9, 2, 5, 8, 1, 4, 7, 0\}$ $o(3) = 10 = o(7)$

~~$\langle 6 \rangle =$~~

~~$\langle 7 \rangle =$~~

② $\phi(g) = n$ $j \in \mathbb{Z}$

$$\phi(g^j) = \frac{n}{\gcd(n, j)}$$

prime in $\mathbb{Z}$
 $|p| > 1$
 & its only divisors are $\{\pm 1, \pm p\}$

$\phi(5) = 12$ $\phi(5^3) = 4$

$\phi(5^9) = 4$

$\frac{\gcd(9, 12) = 3}{12/3}$

$\phi(g) = 49$ $\phi(g^{35}) = \frac{49}{\gcd(49, 35)} = 7$ $\gcd(49, 35) = 7$

When is $\phi(g^i) = n$ iff $\gcd(i, n) = 1$
 iff so n, i are relatively prime.
 (equiv co-prime)

R ring I $\neq$ P. if $ab \in I$, then $a \in I$ or $b \in I$
 $\leq$ ideal

$\mathbb{Z}$ p is prime $|p| > 1$
 if $plab$, then $pl a$ or $pl b$

②

$$o(g)=n$$

$$\langle g \rangle$$

$$g^j \in \langle g \rangle$$

$$\langle g^j \rangle \leq \langle g \rangle$$

if $H \leq G$

~~$K \in H$~~

~~$\langle K \rangle \leq H$~~

Question when are they equal.

$|\langle g \rangle| = n$ we would need $|\langle g^j \rangle| = n$.

iff $o(g^j) = n$ iff j, n rel. prime.

— So how many generators are there for

$$\langle g \rangle \quad o(g) = n.$$

equivalent

— how many numbers between $1+n$ are rel. prime to n .

Ex. if n is prime, then $\langle g^j \rangle = \langle g \rangle \quad \forall j$
 $j=1, \dots, n-1$

This produces a function on ~~$\mathbb{N}$~~ $\mathbb{N} \setminus \{1\}$.

$\phi(n)$ = the number of $j \quad 1 \leq j < n$ s.t.
 $\gcd(j, n) = 1$.

$$\phi(27) = 18$$

1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26,

④ ϕ is called the Euler phi-function
aka Euler totient function

p prime $\phi(p) = p - 1$

p prime $\phi(p^a) = p^a - p^{a-1}$

$$\begin{aligned}\phi(27) &= \phi(3^3) = 27 - 3^2 \\ &= 27 - 9 \\ &= 18\end{aligned}$$

m, n rel. prime

$$\phi(mn) = \phi(m) \phi(n)$$

$$\phi(2^3 \cdot 3^5 \cdot 7^{10})$$

$$= \phi(2^3) \cdot \phi(3^5) \cdot \phi(7^{10})$$

$$= (2^3 - 2^2) (3^5 - 3^4) (7^{10} - 7^9)$$

$$\begin{aligned}100 \\ 2 \cdot 5 \\ 5 \cdot 10 \\ 5 \cdot 5 \cdot 2 \\ 2^2 \cdot 5^2\end{aligned}$$

How many gen. does $\langle g \rangle$ have $o(g) = n$.

$$\underline{\phi(n)}$$

⑤ a subgroup of a cyclic group
is cyclic.

$$G = \langle g \rangle$$

$$H = \{ g^k \mid k \text{ pos.} \}$$

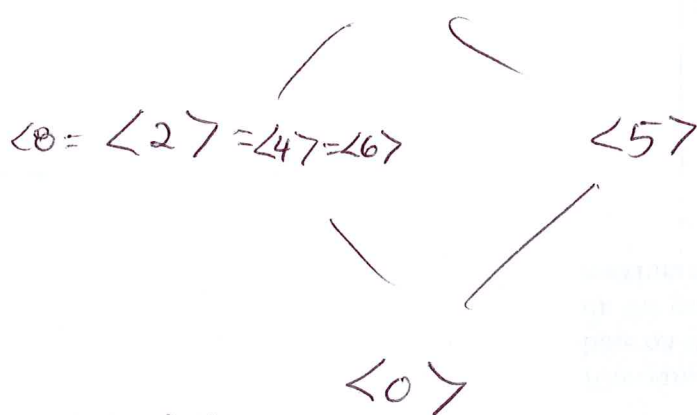
$$g^k \in H$$

$$\langle g^k \rangle = H$$

$$\mathbb{Z}_{10}$$

$$\mathbb{Z}_{10}$$

$$1, 3, 7, 9$$



$$\mathbb{Z}_n$$

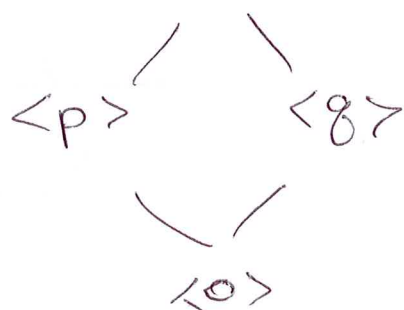
$$\langle \frac{n}{k} \rangle$$

$$H$$

$$\text{smallest } k \in \mathbb{N}$$

p, q distinct primes

$$\mathbb{Z}_{pq}$$



$$\mathbb{Z}_p$$

$$\langle 0 \rangle$$

$$\mathbb{S}_n$$

$$\langle e \rangle$$

$$\mathbb{Z}_{p^2}$$

$$\langle p \rangle$$

$$\langle 0 \rangle$$

$$\mathbb{Z}_{p^3}$$

$$\langle p \rangle$$

$$\langle p^2 \rangle$$

$$\langle 0 \rangle$$

⑥

$$1 \leq a, b < n \text{ in } \mathbb{Z}_n$$

$$\frac{a|b}{\langle a \rangle \mid \langle b \rangle}$$

$$a \cdot k = b$$

$$a \in \langle b \rangle \text{ or } \langle a \rangle$$

$$\langle b \in \langle a \rangle \rangle$$

<

$$\mathbb{Z}_n \mid \langle p_1 \rangle \mid \langle p_2 \rangle \dots \mid \langle p_k \rangle$$

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \text{ distn.}$$

$$[\mathbb{Z}_n : \langle p_1 \rangle] = 2$$

$$\begin{aligned} \phi(p_1) &= \frac{n}{\gcd(p_1, n)} \\ &= \frac{n}{p_1} \\ &= p_1^{\alpha_1-1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \end{aligned}$$

if $H \leq G$ +

$$[G:H] = p \text{ prime}$$

then H is maximal

$$n = 2^2 \cdot 5^2$$

$$\phi(2) = 50$$

$$\begin{array}{c} G \\ \nearrow \\ H \end{array}$$

Gonna give another quiz on

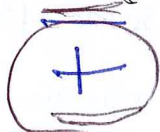
S_n + computing

can make up

9. In which theorems have we used the Division Algorithm?

every subgroup of a cyclic group.

10. When you think of $\mathbb{Z}$ or $\mathbb{Q}$ has a group, you should automatically assume which operation?



(not mult.)

11. If you are dealing with a subset of $\mathbb{R}$ and you want to think of multiplication as a group operation, which element should you remove and why?



$\mathbb{R}^$ is a group under multiplication*

12. If you are dealing with a field F and you want to think of multiplication as a group operation, which element should you remove and why?



F^ is a group under multiplication*

13. If you are dealing with a ring R and you want to think of multiplication as a group operation, which set should you restrict your attention to?

$U(R)$

R a field

14. Name as many different "types" of groups as you can.

$U(R) = R^$*

$$(ab)(ab) = e$$

MAS 4301 - Cosets
 $= \{e, (12)\}$

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

Let $G = S_3$ be the symmetric group and let $H = \langle (12) \rangle$ and $K = \langle (123) \rangle$.

1. How many left cosets of H are there?

3

$$gH = \{gh \mid (13)(12)\}$$

2. I want you to find all of the left cosets of H and list their elements. Here is the algorithm.

- (a) Write out the elements in H (as a set).

$$H = \{e, (12)\}$$

- (b) Pick an element in $g \in G \setminus H$. Operate all of your elements in H by g to form a new coset gH . List the elements in gH (as a set).

$$(13)(12) = (123) \quad (12) \quad g = (13) \quad gH = \{(13), (123)\} = (123)H$$

- (c) Pick an element that doesn't belong in either of these cosets, say $g_2 \in G$ and operate H by g_2 and list the elements in g_2H (as a set).

$$g_2 = (23) \quad (23)H = \{(23), (132)\}$$

- (d) Continue until you have exhausted all of the elements of G . List the left cosets of H and their elements.

$$H, (13)H, (23)H$$

$$H(13) = \{(13), (132)\}$$

$$(12)(13) = (132)$$

3. List the right cosets of H .

$$H, H(13), H(23)$$

$$\text{index} \quad [G:H] = \frac{|G|}{|H|}$$

4. List the left and right cosets of K .

$$(13)H \neq H(13)?$$

partition

$$x \in gH$$

$$x = gh$$

$$xH = gH$$

$$xh_1 = gh_1$$