2/19

- review today

Def. Let S be a set. A partition of S is a collection of subsets of S, $\{A_i\}_{i\in I}$ such that

1) if $i \neq j$, then $A_i \cap A_j = \emptyset$
2) $\bigcup A_i = S$.

Ex $S = \{1,2,3,4,5\}$

$\{\{1,2\},\{3,5\},\{4\}\}$ ✓

$\{\underset{A_1}{\{2,3\}},\underset{A_2}{\{4,5\}}\}$ 1 isn't in any of the sets.

$A_1 \cup A_2 = \{2,3,4,5\} \subsetneq S$.

Ex ~~The co~~ G, $H \leq G$.

$\{g_i H\}_{i\in I}$ the cosets partition G.

~~gach~~ $x \sim y$ iff $y^{-1}x \in H$.

g_i are representatives of the coset

②

$G = \underline{S_3}$ $\quad H = \langle (13) \rangle = \{e, (13)\}$.

I. $(23)H = \{(23)\cdot e, (23)(13)\}$.
$= \{(23), (123)\}$.

$H = eH$

II $(12)H = \{(12)\cdot e, (12)(13)\}$
$= \{(12), (132)\}$

$K = \langle (123) \rangle = \{e, (123), (132)\}$ $\quad \frac{|G|}{|H|} = [G:H]$ Index

\# of cosets

$(12)K = \{(12), (13), (23)\}$.

$K = eK = (123)K = (132)H$.

$\mathbb{Z} \leq \mathbb{R}$ $\quad |\mathbb{R}/\mathbb{Z}| = |[0,1)|$ $\quad \frac{|\mathbb{R}|}{|\mathbb{Z}|}$

$|G| = \infty$ $\quad \frac{|G|}{|H|} = \infty$

$|H| = \infty$

or $\frac{|G|}{|H|} < \infty$

~~$\mathbb{C}/\mathbb{R}$~~

$[\mathbb{C} : \mathbb{R}]$

(3) $\sigma = (1\,3\,5)(2\,4)$ $\quad$ 2,3 $\qquad \tau = (2\,6)$

i. $o(\sigma) = \text{lcm}(2,3) = 6$

ii $\tau \circ \sigma$

iii cycle decom of σ^{-1}

$\sigma^{-1} = (1\,5\,3)(2\,4)$

$\boxed{(2\,4)(1\,5\,3)}$

cycle decom

prod of disj. cycles

$\tau \circ \sigma = (2\,6)(1\,3\,5)(2\,4)$

$(S_n, \circ)$

$\varphi_1 : \{1, \dots, n\} \to \{1, \dots, n\}$ $\quad$ 1-1, onto

φ_2

$(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$

iff they commute.

$(\varphi_2 \circ \varphi_1)(x) = \varphi_2(\varphi_1(x))$

$\boxed{(2\,6)(1\,3\,5)(2\,4)}(1) = (2\,6)(1\,3\,5) \text{ of } \big((2\,4)(1)\big)$

$= (2\,6)(1\,3\,5) \text{ of } (1)$

$= (2\,6)\big[(1\,3\,5)(1)\big]$

$= (2\,6)(3) = 3$

$(2\,6)(1\,3\,5)(2\,4)$

$\tau \circ \sigma \; (1\,3\,5)(2\,4\,6)$

$\sigma \circ \tau = (1\,3\,5)(2\,4)(2\,6)$

$(1\,3\,5)(2\,6\,4)$

$\text{lcm}(3,3) = 3$

not cycle dec

$2 \to 1$

4. $\sigma = (1234)(245)$

$(ab)^{-1} = b^{-1}a^{-1}$

$\sigma^{-1} = (254)(1432)$

$\sigma^{-1}\,(542)(4321)$

ab $\cancel{\sigma^{-1}(4321)}$

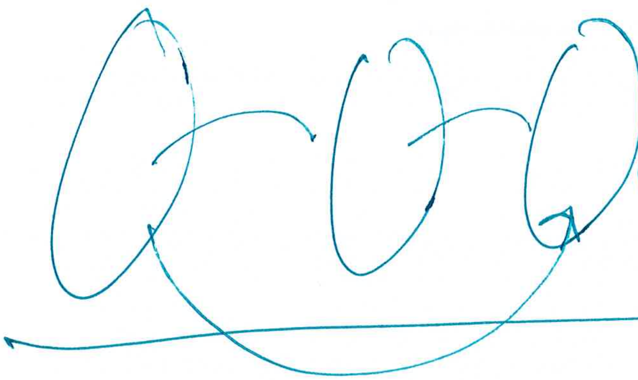
(4321)

(1432)

$1 \to 1 \to 2$

$(245)(1234)$

$2 \to 3$



$(123)(132)$

$\sigma = (25)(143)$

$\sigma \circ \tau$

$\tau = (23)(54)$

$(25)(143)(23)(54)$

$(142)(35)$

~~[illegible]~~

(1)

$(23)(54)(25)(143)$

$(153)(24)$

$(42)(531)$

5 common themes

Definitions

Problems mult σ, τ.

$U(n)$

$U(10)=\{1,3,7,9\}$

$\langle 3 \rangle = \{3,9,7,1\}$ $o(3)=4$. cyclic

$\langle 9 \rangle = \{9,1\}$ 3, 7 are generators

$a \equiv b \bmod n$

if $n \mid b-a$

$\mathbb{Z}_n$ - how many generators? $\phi(n)$

$\phi(42)=\phi(2\cdot 3\cdot 7)=\phi(2)\cdot\phi(3)\cdot\phi(7)$

$= (2-1)(3-1)(7-1) = 1\cdot 2\cdot 6 = 12$

$\phi(p^\alpha)=p^\alpha - p^{\alpha-1}$ $\phi(mn)=\phi(m)\cdot\phi(n)$

p prime m,n rel. prime

42

$2\cdot 21$

$3\cdot 7$

ϕ

84

$2\cdot 42$

$2\cdot 3\cdot 7$

$2^2\cdot 3\cdot 7$

$\phi(84)$

$=(2^2-2)(3-1)(7-1)$

$= 24$

6 $\phi(\underbrace{2\cdot 2\cdot 2}\cdot\underbrace{3\cdot 3}\cdot\underbrace{5\cdot 5})$

$\phi(8)\cdot\phi(9)\cdot\phi(25)$

$(2^3-2^2)(3^2-3)(5^2-5)$

$4\cdot 6\cdot 20$

480

$\phi(n) = |\{\text{gen. for } \mathbb{Z}_n\}| = |U(n)|$

~~ϕ(number of~~ if $U(n)$ is cyclic,

then how many generators does it have

$\phi(\phi(n))$

$n = 25$ $\quad \mathbb{Z}_{25}$ $\quad U(n) = \{$

$25 = 5^2$

$\phi(5^2) = 5^2 - 5$
$= 20$

$|U(25)| = 20$

$U(25) = \{1, 2, 3, 4, 6, 7, 8, 9, 11, \ldots$

$\langle 2\rangle = \{2, 4, 8, 16, 7, 14, 3, 6, 12, -1, 23$

2 is a generator

7

$U(8) = \{1, 3, 5, 7\}.$

$\langle 3 \rangle = \{3, 1\}$ $\quad \langle 7 \rangle = \{7, 1\}$ $\quad \langle 1 \rangle = \{1\}$

$\langle 5 \rangle = \{5, 1\}$

<u>$U(8)$ not cyclic</u>

$$
\begin{tikzcd}[column sep=small]
 & U(8) \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\langle 3 \rangle \arrow[dr, no head] & \langle 5 \rangle \arrow[d, no head] & \langle 7 \rangle \arrow[dl, no head] \\
 & \langle 1 \rangle &
\end{tikzcd}
$$

$\underline{\mathbb{Z}_2 \times \mathbb{Z}_2} = \{(0,0), (0,1), (1,0), (1,1)\}$

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

$G = \langle g \rangle$ $\qquad o(g^k) = \dfrac{n}{\gcd(n,k)}.$

$\underline{|G| = n}$

$3 \overline{)111}$ $\quad 37$ $\quad 9$

$G = \mathbb{Z}_{111}$ $\qquad o(3) = \dfrac{111}{\gcd(3,111)} = \dfrac{111}{3} = 37$

$\mathbb{Z}_{111} = \langle 1 \rangle$

$3 = 3 \cdot 1$

~~$G = \langle g \rangle$ $(G, +, 0)$ $|G| = 4$~~

$o(k \cdot g) = \dfrac{n}{\gcd(n,k)}$

8

$m = (a_n a_{n-1} a_{n-2} \dots a_0)$

2173

$= \underline{2 \cdot 10^3 + 1 \cdot 10^2 + 7 \cdot 10^1 + 3 \cdot 10^0}$

mod 3

$10 \equiv 1 \mod 3$

$10^2 \equiv 1 \mod 3$

$10^k \equiv 1 \mod$

$\underline{2+1+7+3} \to 0$

$3 \mid a_n + a_{n-1} + \dots + a_0$ iff.

$3 \mid a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 \cdot 10 + a_0 \cdot 10^0$

$|U(p)| \overset{\text{prim}}{=} p - 1$