Group Theory

$$\begin{array}{c} \mathbb{F}_q \\ n \Big| \\ \mathbb{F}_p \end{array} \qquad q = p^n$$

$[\mathbb{F}_q : \mathbb{F}_p] = n$

$S = \{ \sigma \mid \sigma : \mathbb{F}_q \to \mathbb{F}_q \text{ ring homomorphism} \}$

$$\begin{aligned} \circ :\ & S \times S \longrightarrow S \\ & \sigma \quad \tau \longrightarrow \sigma \circ \tau \end{aligned}$$

$$\begin{tikzcd} \mathbb{F}_q \arrow[r, "\tau"] \arrow[rr, bend right, "\sigma\circ\tau"'] & \mathbb{F}_q \arrow[r, "\sigma"] & \mathbb{F}_q \end{tikzcd}$$

Thm. $(S, \circ)$ is a group.

pf: 1) identity map $id : \mathbb{F}_q \to \mathbb{F}_q$

$\sigma \circ id = id \circ \sigma = \sigma$

2) $\sigma, \tau \in S$, then $\sigma \circ \tau \in S$.

$\sigma \circ \tau (a \underset{\substack{\uparrow \\ \times}}{+} b) = \sigma(\tau(a) \underset{\substack{\uparrow \\ \times}}{+} \tau(b)) = \sigma(\tau(a)) \underset{\substack{\uparrow \\ \times}}{+} \sigma(\tau(b))$.

$\sigma \circ \tau(1) = \sigma(1) = 1$

3) $\exists\, \delta \in S$ s.t. $\delta \circ \sigma = \sigma \circ \delta = id$.

4) Associative Law: $\sigma \circ (\tau \circ \delta) = (\sigma \circ \tau) \circ \delta$ natural follows. composition of maps.

Side Question: $\sigma \in S$, $\ker(\sigma) = ?$

Ans: $\ker(\sigma) = 0$ since $\ker(\sigma)$ is an ideal in $\mathbb{F}_q$. But $\mathbb{F}_q$ is a field, so its ideal is either (0) or $\mathbb{F}_q$. So $\ker(\sigma) = (0)$ because $\sigma(1) \neq 0$. So σ is actually a ring isomorphism

---

$\mathbb{F}_q \xrightarrow{\sigma} \mathbb{F}_q$ is both injective & surjective following from $\ker(\sigma) = (0)$.

$\forall a \in \mathbb{F}_q.\ \exists! x \in \mathbb{F}_q$ s.t. $\sigma(x) = a$ call x $\sigma^{-1}(a)$

So we define $\delta : \mathbb{F}_q \longrightarrow \mathbb{F}_q$.

$a \longrightarrow \sigma^{-1}(a)$

We need to show that $\delta \in S$

$$\delta(a+b) = \delta(\sigma(\alpha) + \sigma(\beta))$$

Say $\sigma(\alpha) = a$, $\sigma(\beta) = b$

$$= \delta(\sigma(\alpha+\beta))$$

$$= \alpha + \beta = \delta(a) + \delta(b)$$

same thing holds for $\times$. $\square$.

Rmk: since $\mathbb{F}_q$ contains finitely many elements.

$S \subseteq \{\text{maps between } \mathbb{F}_q \text{ and } \mathbb{F}_q\}$ must be finite.

Examples for finite grps?

eg. 1) $\mathbb{F}_p^\times = (\mathbb{F}_p \setminus \{0\}, \times)$, $\mathbb{F}_q^\times$ p prime $q = p^n$

$(F^\times, \times)$ F is a field.

2) $\mathbb{Z}_m = (\{0, 1, \cdots, m-1\}, +)$

$(R, +)$ R is a ring. although might not be finite

All previous example we encountered are abelian grps.

Example for non-abelian finite grps:

$$S_n := (\{\text{permutations of } n \text{ letters}\}, \overset{\text{composition}}{\circ})$$

$$= (\{\sigma : \{1,2,\cdots,n\} \to \{1,2,\cdots,n\} \mid \sigma \text{ is bijection}\}, \circ)$$

$n=3$

σ		τ	
$1 \to 2$		$1 \to 2$	
$2 \to 3$		$2 \to 1$	
$3 \to 1$		$3 \to 3$	

Q: How many elements in S_3? 6

$3 \times 2 \times 1 = 3!$

Q: $\sigma \circ \tau$ $\qquad$ $\tau \circ \sigma$

$\sigma \circ \tau$	$\tau \circ \sigma$
$1 \to 3$	$1 \to 1$
$2 \to 2$	$2 \to 3$
$3 \to 1$	$3 \to 2$

$$\sigma \circ \tau(1) = \sigma(\tau(1)) = \sigma(2) = 3$$

$$\sigma \circ \tau \neq \tau \circ \sigma$$

Def (grp homomorphism) Given $f: G_1 \to G_2$ a map between grps, f is a grp homomorphism if $f(a \cdot_1 b) = f(a) \cdot_2 f(b)$.

(*) Notice by def, $f(e) = e$.

Def (subgrp) Given a grp G, a subset $H \subseteq G$ is called a subgrp if H is closed under grp operation and taking inverse.

Suppose G is a finite grp. and $H \subseteq G$ a subgrp.

We can define a relation on G, "$\sim$".

$$g_1 \sim g_2 \iff g_1^{-1} \cdot g_2 \in H.$$

← Recall similar definitions in a ring with respect to an ideal. $r_1 \sim r_2 \iff r_1 - r_2 \in I$.

Lemma. "$\sim$" is an equivalence relation.

Pf: 1) $g \sim g$ because $\underset{\overset{\parallel}{e}}{g^{-1} \cdot g} \in H$

2) $g_1 \sim g_2$ then $g_2 \sim g_1$ because

$$g_1^{-1} \cdot g_2 \in H \xRightarrow{\text{inverse}} g_2^{-1} \cdot g_1 \in H$$

3) $g_1 \sim g_2$, $g_2 \sim g_3$ then $g_1 \sim g_3$ because

$$g_1^{-1} \cdot g_2 \in H,\ g_2^{-1} \cdot g_3 \in H \xRightarrow{\text{product}} g_1^{-1} \cdot g_3 \in H.$$

□.

Therefore "$\sim$" gives a partition on G into equivalence classes.

Fix $g \in G$, what is $[g] = \{ x \in G \mid g \sim x \}$?

$$g \sim x \iff g^{-1} \cdot x \in H \iff x \in g \cdot H$$

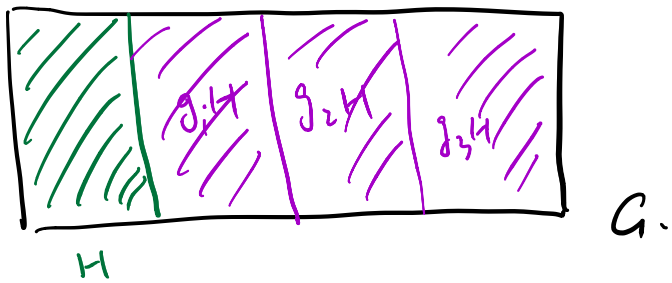
$$g \cdot H \overset{\triangle}{=} \{ g \cdot h \mid h \in H \}$$

So $[g] = g \cdot H$

Q: How many elements in $[g]$?

$\#[g] = \#H$

[since elements in $g\cdot H$ are all different.
$g\cdot h_1 = g\cdot h_2$ then $h_1 = h_2$ by cancellation law.]



Def (index) The index of H in G is the number of equivalence classes of "$\sim$". Denote index by $[G:H]$.

(Lagrange)
Thm. $|G|/|H| = [G:H]$.

pf: $G = \bigcup gH$. is a disjoint union of equivalence classes.

Def (coset). We call $g\cdot H$ a coset of H.

Recall Lemma from last time:

(Δ) Thm. $|G| = n$. Then $\forall g \in G$. $g^n = e$.

Def (cyclic grp) A finit grp G is cyclic grp if $\exists g \in G$ s.t. for every element $x \in G$ $\exists k \in \mathbb{Z}$ s.t $x = g^k = \underbrace{g\cdot g\cdots g}_{k \text{ times}}$

g is called a generator for the cyclic grp.

eg. $(\mathbb{Z}_m, +)$ because 1, is the generator.

$n = \underbrace{1+1+\cdots+1}_{n \text{ times}}$

Claim: A finite cyclic grp has to be isomorphic to $(\mathbb{Z}_m, +)$ for some m.

Pf: Let g be the generator. Then the grp contains

$$\{g, g^2, g^3, \cdots, g^k, \cdots, g^{n-1}, g^n = e\} \Leftarrow$$

where n is the smallest positive integer s.t. $g^n = e$.

Then $G \simeq (\mathbb{Z}_m, +)$ as a grp. (A grp isomorphism is a grp homomorphism that is injective and surjective).

by mapping $g \longrightarrow 1$

Def. (order) Given $g \in G$, the order of g is the smallest positive integer $n > 0$ s.t $g^n = e \in G$.

We will denote subgrp generated by g to be $\langle g \rangle \subseteq G$.

Proof of thm Δ:

Given $g \in G$, define $H = \langle g \rangle$ to be a subgrp and H is cyclic. $|H|$ is equal to the order of g

By the theorem of Lagrange. $|G| = |H| \cdot [G:H]$

$$g^{|G|} = g^{|H| \cdot [G:H]} = e^{[G:H]} = e \qquad \square.$$

Application: Fermat's Little Theorem.

$\forall\, p \nmid n \in \mathbb{Z} \qquad n^{p-1} \equiv 1 \pmod p$.

Pf: Apply Thm Δ with $\mathbb{F}_p^\times$. where $|\mathbb{F}_p^\times| = p-1$. $\square$.

Warning: $\mathbb{F}_{25}$ is not $\mathbb{Z}_{25}$. although $\mathbb{F}_5 = \mathbb{Z}_5$

$\mathbb{Z}_m$ is a field $\Leftrightarrow$ m is prime

$(\mathbb{F}_{25}, +)$ $(\mathbb{Z}_{25}, +)$ are not the same as grps.

since $5 \cdot 1 = 0$ in $\mathbb{F}_{25}$ but

$5 \cdot 1 \neq 0$ in $\mathbb{Z}_{25}$

Q: Why is $|\langle g \rangle| = \mathrm{ord}(g)$?

$\langle g \rangle = \{e, g, \cdots, g^{n-1}\}$ suppose $\mathrm{ord}(g) = n$

$g^k = g^r$, $0 \le r < n$.

suppose $g^{r_1} = g^{r_2}$ then $g^{r_1 - r_2} = e$ (WTLG, $r_1 > r_2$)

contradicts with n being $\mathrm{ord}(g)$.