**Group Theory**

\[ \overline{F}_q \quad q = p^n \quad S = \{ \sigma \mid \sigma : \overline{F}_q \rightarrow \overline{F}_q \text{ ring homomorphism} \} \]

\[ \mathbb{n} \quad \begin{array}{c}
\overline{F}_p \\
\mathbb{F}_p \\
\end{array} \]

\[ [\overline{F}_q : \overline{F}_p] = n \quad \begin{array}{c}
\overline{F}_q \\
\overline{F}_q \\
\mathbb{F}_q \\
\mathbb{F}_q \\
\end{array} \]

\[ \begin{array}{c}
\xrightarrow{\tau} \\
\xrightarrow{\sigma} \\
\end{array} \]

\[ 6 \circ \tau \rightarrow 6 \circ \tau \]

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

**pf:** 1) identity map \(\text{id} : \overline{F}_q \rightarrow \overline{F}_q\)

\[ 6 \circ \text{id} = \text{id} \circ 6 = 6 \]

2) \(6, \tau \in S\), then \(6 \circ \tau \in S\).

\[ 6 \circ \tau (a + b) = 6 \left( \tau(a) + \tau(b) \right) = 6(\tau(a)) + 6(\tau(b)) \]

\[ 6 \circ \tau (1) = 6(1) = 1 \]

3) \(\exists \delta \in S\) s.t. \(\delta \circ 6 = 6 \circ \delta = \text{id}\).

4) Associative Law: \(6 \circ (\tau \circ \delta) = (6 \circ \tau) \circ \delta\) natural follows.

composition of maps.

---

**Side Question:** Ans: \(\text{Ker}(\delta) = 0\) since \(\text{Ker}(\delta)\) is an ideal in \(\overline{F}_q\). But \(\overline{F}_q\) is a field, so its ideal is either \((0)\) or \(\overline{F}_q\). So \(\text{Ker}(\delta) = (0)\) because \(\delta(1) \neq 0\). So \(\delta\) is actually a ring isomorphism.
\[ \overline{F_q} \rightarrow \overline{F_q} \] is both injective & surjective, following from \( \ker(s) = \{0\} \).

\[ \forall a \in \overline{F_q}, \exists! x \in \overline{F_q} \text{ s.t. } s(x) = a \Rightarrow a = s^{-1}(a) \]

So we define \( s : \overline{F_q} \rightarrow \overline{F_q} \)

\[ a \mapsto s^{-1}(a) \]

We need to show that \( s \in S \)

\[ s(a+b) = s(s(a)+s(b)) \]

So \( s(a) = a = s(a+b) \)

\[ s(b) = b = a + b = s(a) + s(b) \]

same thing holds for \( x \).

\[ \square. \]

Rmk: since \( \overline{F_2} \) contains finitely many elements.

\( S \subseteq \{\text{maps between } \overline{F_q} \text{ and } \overline{F_q}\} \) must be finite.

Examples for finite grps?

1) \( \overline{F_p}^x = (\overline{F_p} \setminus \{0\},\times) \), \( \overline{F_p}^x \) \( p \) prime \( q=p^n \)

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

\( (\mathbb{F},+) \) \( \mathbb{F} \) is a field.

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

All previous example we encountered are abelian grps.
Example for non-abelian finite 
grps: composition

\[ S_n = \{ \text{permutations of } n \text{ letters} \}, \circ \]

\[ = \{ 6 : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} | 6 \text{ is bijection} \} \]

- \( n = 3 \)
  - \( 1 \to 2 \)
  - \( 2 \to 3 \)
  - \( 3 \to 1 \)

Q: How many elements in \( S_3 \)? \( 6 \)

\[ 3 \times 2 \times 1 = 3! \]

- \( G \circ T \)
  - \( 1 \to 3 \)
  - \( 2 \to 2 \)
  - \( 3 \to 1 \)

- \( T \circ 6 \)
  - \( 1 \to 1 \)
  - \( 2 \to 3 \)
  - \( 3 \to 2 \)

\[ G \circ T(1) = G(T(1)) = G(2) = 3 \]

\[ G \circ T \neq T \circ 6 \]

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

(*) 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 group and $H \subseteq G$ a subgroup. We can define a relation on $G$, $\sim$:

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

Lemma. $\sim$ is an equivalence relation.

pf: 1) $g \sim g$ because $g^{-1}g \in H$.

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

$$g_1^{-1}g_2 \in H \implies g_2^{-1}g_1 \in H.$$ 

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

$$g_1^{-1}g_2 \in H, \ g_2^{-1}g_3 \in H \implies g_1^{-1}g_3 \in H.$$ 

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

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

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

So $[g] = g \cdot H$. 

<Read similar definitions in a ring with respect to an ideal.>

$$r_1 \sim r_2 \iff r_1 - r_2 \in I.$$
Q: How many elements in \( [g] \)?

\[
\#_[g] = \#_H
\]

since elements in \( g \cdot H \) are all different.

\[
g \cdot h_1 = g \cdot h_2 \text{ then } h_1 = h_2 \text{ by cancellation law.}
\]

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:

(\( \Delta \))Thm. \( |G| = n \). Then \( \forall g \in G \), \( g^n = e \).

Def (cyclic grp) \( \forall x \in G \), \( \exists \ k \in \mathbb{Z} \) s.t. \( x = g^k = g \cdot g \cdot \ldots \cdot g \).

A finite grp \( G \) is cyclic grp if \( \exists g \in G \) s.t. \( g \) is called a generator for the cyclic grp. \( k \) times

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

\[
\begin{align*}
n = 1 + 1 + \ldots + 1 \\
\text{\( n \) times}
\end{align*}
\]
Claim: A finite cyclic grp has to be isomorphic to (Zm, +) for some m.

pf: Let g be the generator. Then the grp contains
\{ g, g^2, g^3, \ldots, g^k, \ldots, g^{n-1}, g^n = e \} 
where n is the smallest positive integer s.t. g^n = e.

Then G = (Zm, +) as a grp. (A grp isomorphism is a grp homomorphism that is injective and surjective).

Def. (order) Given g \in G, the order of g is the smallest positive integer n \geq 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 \triangle:

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\| = \|H\| \cdot [G:H]

\rightarrow e \equiv e \pmod{[G:H]}

Application: Fermat's Little Theorem.

\forall p \mid n \in \mathbb{Z}, \quad n^{p-1} \equiv 1 \pmod{p}.

If: Apply Thm \triangle with \mathbb{F}_p^x, where \|\mathbb{F}_p^x\| = p-1.

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

Z_m is a field \iff m is prime
$(\mathbb{F}_{25}, +)$ and $(\mathbb{Z}_{25}, +)$ are not the same as groups.

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

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

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

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

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

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