Week 3.

Group homomorphism:

Def: Let $(G, *)$, $(H, *)$ be groups. A function $f: G \to H$ is a group homomorphism iff

$$\forall\, g_1, g_2 \in G, \quad f(g_1) \times f(g_2) = f(g_1 * g_2).$$

Isomorphisms are bijective group homomorphisms.

E.g. There exists an isomorphism $S_3 \cong D_6$.

All groups of order 2 are isomorphic.

E.g. of homomorphisms. Let G, H be groups.

1) trivial homomorphism

$f: G \to H$ by $f(g) = e_H$.

2) $\mathbb{1}_G: G \to G$ identity homomorphism.

$f_2: \mathbb{Z} \xrightarrow{x} 2\mathbb{Z}$ (multiplication by 2)

$\iota: \mathbb{Z} \to \mathbb{Q}$ (inclusion).

$f_2: \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}$

3) $\exp: (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, \times)$

4) $f: GL_2(\mathbb{R}) \to \mathbb{R}^*$ by $f(A) = \det(A)$.

Group homomorphism preserves identities, inverses.

$\ker f = f^{-1}(e_H)$ $\quad$ $\operatorname{im} f = f(G) = \{f(g) : g \in G\}$.

Q: What's the ker, im of previous examples?

Let $f: G \to H$ be a ~~homo~~ homomorphism. Then f is surjective iff $\operatorname{im}(f) = H$, injective iff $\ker(f) = \{e_G\}$.

Coset

Let $H \leq G$ be a subgroup. Denote $aH = \{ah : h \in H\}$ the left coset, and Ha is defined similarly.

Eg. 1) $2\mathbb{Z} \leq \mathbb{Z}$, $6 + 2\mathbb{Z} = 0 + 2\mathbb{Z}$. (even numbers)

$1 + 2\mathbb{Z} = 5 + 2\mathbb{Z}$ (odd numbers).

2) Let $H = \langle s \rangle \leq D^6$, i.e $H = \{e, s\}$. then

$rH = \{r, rs = sr^{-1}\}$. but $Hr = \{r, sr\}$.

Prop: $aH = bH \Rightarrow b^{-1}a \in H$.

Pf: $\Rightarrow$ $aH = bH \Rightarrow a \in bH$, so $a = bh$ for some $h \in H$.

$\Rightarrow b^{-1}a = h \in H$,

$\Leftarrow$) $b^{-1}a \in H$ Let. $b^{-1}a = h_0 \Rightarrow a = bh_0$. Consider any $ah \in aH$, $ah = bh_0h = b(h_0h) \in bH \Rightarrow aH \subseteq bH$.

The other direction is similar.

Left coset of a subgroup $H \leq G$ gives a partition of equal size.

Index: $|G:H|$ is the number of left cosets of H in G.

THM (Lagrange). Let G be a finite group and $H \leq G$ is a subgroup. Then $|H|$ divides $|G|$. Moreover,

$$|H| \cdot |G:H| = |G|.$$

Note: Only true for finite groups!

Cor. Groups of prime order are cyclic, and every non-identity elements are generators.

~~$\mathbb{Z}_+ \neq$~~ $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group. How about multiplication?

Let $U_n = \{ [a] \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1 \}$.

Euler totient function $\phi_n = |U_n|$.

Note: $\phi(p) = p-1$ for p prime.

Note: $\sum_{d|n} \varphi(d) = n$.

Proposition U_n is a group under multiplication mod n.

D). Closure: if a, b are coprime to n, then $a \cdot b$ is also coprime to n. So $[a][b] \in U_n \Rightarrow [a][b] = [a \cdot b] \in U_n$.

1) Identity: 1. 2) Let $[a] \in U_n$, the map $U_n \to U_n$ by $[c] \mapsto [ac]$ is 1-1. In fact, if $[ac_1] = [ac_2]$ $\Rightarrow$ n divides $(c_1 - c_2)$ since a is coprime to n.
Since U_n is finite, this also a surjection, so $\exists\, c'$ s.t. $[ac'] = [a][c'] = 1$. $\Rightarrow [c'] = [a]^{-1}$. $\square$

THM (Fermat-Euler) $n \in \mathbb{N}$, $a \in \mathbb{Z}$ coprime to $\mathbb{N}$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Pf: $[a] \in U_n \Rightarrow [a]^{|U_n|} = [1] \Rightarrow a^{\phi(n)} \equiv 1 \bmod n$.

Cor. (Fermat's little theorem) $n = p$ is a prime,

$$a^{p-1} \equiv 1 \bmod p.$$

Another example on D_{2n}.

Recall $D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, \quad sr = r^{-1}s \rangle$.

If H is a group containing a and b with $a^n = b^2 = 1$, $ba = a^{-1}b$, then clearly there exist a homomorphism from D_{2n} to H by sending $r \mapsto a$, $s \mapsto b$.

For instance, suppose $k \mid n$, $k \geq 3$. then $\exists$

$$\varphi : D_{2n} \longrightarrow D_{2k}$$

Note φ is not an isomorphism for $k < n$.

$D_6 \cong S_3$.

Let $H = S_3$ with $a = (123)$ $b = (12)$, we can easily check that $ba = a^{-1}b$. Also S_3 is generated by these two elements, so $s \mapsto b$, $r \mapsto a$ gives an isomorphism $D_6 \cong S_3$.