13.1

Last time: • X finite set. $\sigma \in Syn(X)$ can be written uniquely (up to order) as a product of disjoint cycles.

• Lagrange's Theorem: G finite group, $H < G$ subgroup. Then

$$|G| = |H|\,|G/H| = |H|\,|H\backslash G|$$

where $G/H = \{gH\}_{g\in G}$, $H\backslash G = \{Hg\}_{g\in G}$.

Remark In general $\{gH\}_{g\in G}$ and $\{Hg\}_{g\in G}$ are different partitions of the set G.

Ex $G = S_3 = \{id, (12), (13), (23), (123), (132)\}$

Let $H = \langle 12 \rangle = \{id, (12)\}$

Then $H\backslash G$, G/H consist of $\frac{|S_3|}{|H|} = \frac{3!}{2} = 3$ sets each.

What are they? Note

$$(12)(13) = \begin{pmatrix} 1\mapsto 3 \mapsto 3 \\ 3 \mapsto 1 \mapsto 2 \\ 2 \mapsto 2 \mapsto 1 \end{pmatrix} = (132) \qquad (13)(12) = \begin{pmatrix} 1\mapsto 2 \mapsto 2 \\ 2 \mapsto 1 \mapsto 3 \\ 3 \mapsto 3 \mapsto 1 \end{pmatrix} = (123).$$

Hence $H\cdot(13) = \{(13), (12)(13)\} = \{(13), (132)\}$ $\quad S_3 \setminus (H \cup H(13))$

$\Rightarrow H\backslash S_3 = \{H = \{id, (12)\}, \underbrace{\{(13), (12)(13)\}}_{H(13)} = \{(13), (132)\}, \underbrace{\{(23), (123)\}}_{H(23)}\}$

$S_3/H = \{H, (13)H = \{(13), (123)\}, \{(23), (132)\}\}.$

Corollary (of Lagrange's theorem) Let G be a finite group, $g \in G$. Then $|\langle g\rangle| \mid |G|$.

Proof For any subgroup H of G, $|H| \mid |G|$ since $|G| = |H|\,|G/H|$. In particular $|\langle g \rangle| \mid |G|$.

Remark 13.1 Recall that $\langle g \rangle \simeq \mathbb{Z}_n$ where $n = |\langle g \rangle|$ and that $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$ with $g^n = e$.

So, in particular $\boxed{g^{|\langle g\rangle|} = e.}$

Note: Since $|\langle g \rangle| \mid |G|$, $\boxed{g^{|G|} = e}$ as well.

Fermat's little theorem. For any prime p, $k^p \equiv k \mod p$.

Proof: If $k \equiv 0 \mod p$, not much to prove: $k^p \equiv 0^p \equiv 0 \equiv k \mod p$.

Suppose $k \not\equiv 0 \mod p$ ie $p \nmid k$. Then $\gcd(k,p) = 1$

$\Rightarrow \exists x, y \in \mathbb{Z}$ s.t $kx + py = 1$. $\Rightarrow \exists x \in \mathbb{Z}$ st $kx \equiv 1 \mod p$,

$\Rightarrow$ If $[k] \in \mathbb{Z}_p$ and $[k] \neq [0]$, $\exists [x] \in \mathbb{Z}_p$ s.t $[k][x] = [1]$

$\Rightarrow \mathbb{Z}_p^\times := \{[k] \in \mathbb{Z}_p \mid [k] \neq [0]\}$ is a group under multiplication.

By remark 13.1, $\forall [k] \in \mathbb{Z}_p^\times$

$$[k]^{|\mathbb{Z}_p^\times|} = [1]$$

Since $\mathbb{Z}_p^\times = p-1$,

$$[k^{p-1}] = [1] \quad (\text{in } \mathbb{Z}_p)$$

ie. $k^{p-1} \equiv 1 \mod p$

$\Rightarrow k^p = k \mod p$ $\square$

Corollary 13.2 Suppose G is a finite group and $p = |G|$ is prime. Then

1) The only subgroups of G are G and $\{e\}$.

2) $\forall g \in G, g \neq e, \langle g \rangle = G$, hence $G \simeq \mathbb{Z}_p$

3) For any group H and any homomorphism $f: G \to H$ either f is 1-1 or $f(g) = e_H$ $\forall g \in G$.

Proof (1) If $H < G$ is a subgroup, then $|H| \mid |G| = p$. $\Rightarrow |H| = p$ or 1

$\Rightarrow H = G$ or $\{e\}$

(2) If $g \neq e$, then $\langle g \rangle \neq \{e\}$. But $\langle g \rangle$ is a subgroup. By (1), $\langle g \rangle = G$.

(3) $\ker f$ is a subgroup of G. Hence by (1) either $\ker f = \{e\}$ and then f is 1-1 or $\ker f = G$ and then $f(g) = e_H$ $\forall g \in G$. $\square$

Definition A subgroup N of a group G is normal iff

$\forall n \in N$ $\forall g \in G$, $\boxed{gng^{-1} \in N}$

Notation $N \lhd G$ if N is normal in G.

"Ex" If G is abelian (ie, commutative) then any subgroup N is normal. <u>Reason:</u> $\forall g \in G$, $\forall n \in N$, $gng^{-1} = gg^{-1}n = n$.

"Ex" G, $\{e\}$ are always normal in G.

"Ex" Let $f: G \to H$ be a homomorphism. Then $N = \ker f$ is normal in G.

<u>Check</u> $\forall n \in \ker f$, $\forall g \in G$ $\quad f(gng^{-1}) = f(g)f(n)(f(g))^{-1} = f(g)e_H(f(g))^{-1}$
$= e_H$.

$\Rightarrow \quad gng^{-1} \in \ker f$.

Hence $SO(2) \lhd O(2)$ since $SO(2) = \ker(\det : O(2) \to \mathbb{R}^\times)$
$SL(n,\mathbb{R}) \lhd GL(n,\mathbb{R})$ since $SL(n,\mathbb{R}) = \ker(\det : GL(n,\mathbb{R}) \to \mathbb{R}^\times)$.

<u>Proposition 13.3</u> Let N be a subgroup of G.
N is normal in G $\iff$ $gH = Hg \quad \forall g \in G$.

<u>Proof</u> ($\Rightarrow$) Suppose $N \lhd G$. Then $\forall n \in N$, $g \in G$
$gn = (gng^{-1})g \in Ng$. $\Rightarrow gN \subseteq Ng$
Similarly $ng = gg^{-1}ng = g \cdot \underbrace{g^{-1}n(g^{-1})^{-1}}_{\in N} \in gN$. $\Rightarrow Ng \subseteq gN$.

$\therefore$

Thus $N \lhd G \Rightarrow gN = Ng$.

($\Leftarrow$) Suppose $gN = Ng$ $\forall g \in G$. Then $\forall g \in G$ $\forall n \in N$
$gn \in gN = Ng \Rightarrow \exists n' \in N$ s.t. $gn = n'g \Rightarrow gng^{-1} = n' \in N$.
$\therefore \quad N \lhd G$. $\square$

<u>Note</u> If $N \lhd G$ $\quad N\backslash G = G/N$.

Corollary 13.4 Suppose N is a subgroup of G and $|G/N| = 2$. (G and N need not be finite). Then N is normal in G.

Proof By homework the map $G/N \to N\backslash G$, $gN \mapsto Ng^{-1}$ is a bijection. Hence since $|G/N| = 2$, $|N\backslash G| = 2$ as well.
Since cosets partition G, since N is a coset and since there only two cosets all together, $G/N = \{N, G \setminus N\}$
Similarly $N\backslash G = \{N, G\setminus N\}$
Therefore, if $g \notin N$, $gN = G \setminus N = Ng$.
(and if $g \in N$, $gN = N = Ng$).
$\therefore \forall g \in G \quad gN = Ng$.
By 13.3, $N \trianglelefteq G$. $\square$

Ex $G = S_3$ $N = \langle (123) \rangle$. Since (123) is a 3-cycle $|N| = 3$. $\Rightarrow |S_3/N| = |S_3|/|N| = 3!/3 = 2$
$\Rightarrow N \trianglelefteq S_3$.

Nonexample $\langle (12) \rangle$ is not normal in S_3 since $S_3/\langle (12) \rangle \neq \langle (12) \rangle \backslash S_3$.

Next time (cf Thm 1 p 132 of Nicholson) Let N be a normal subgroup of a group G. Then the set $G/N = \{gN\}_{g \in G}$ has a unique multiplication $*$ that makes G/N into a group and
$\pi : G \to G/N$, $\pi(g) = gN$ into a (group) homomorphism.