Lecture 9

Saturday, February 7, 2015 3:32 PM

For $H \leq G$ a subgroup of G, recall that

$$G/H = \{gH \mid g \in G\}$$

is the set of left cosets of H in G. We know that the gH partition G, and that G/H has a gp structure given by $gH \cdot g'H = (gg')H$ iff $H \trianglelefteq G$: $gHg^{-1} = H$ $\forall g \in G$.

How big is G/H ?

Lagrange's Theorem If G is a finite group and $H \leq G$, then

$$|G/H| = \frac{|G|}{|H|}.$$ In particular, $|H|$ divides $|G|$.

Note This is one reason why when $H \trianglelefteq G$, G/H is called a quotient group.

Pf Let $|H| = n$, $|G/H| = k$. We claim that $H \longrightarrow gH$, $h \longmapsto gh$ is a bijection.
Indeed, it is surjective by def'n of gH.
Injectivity follows from cancellation.
Thus $|H| = |gH| = n$ $\forall g \in G$. Since G/H partitions G into k cosets each of size n, we learn that $|G| = kn = |G/H| \cdot |H|$, as desired. $\square$

Def'n If G is a group & $H \leq G$, then $|G/H|$ is called the index of H in G and is denoted $[G:H]$.

Note Book writes $|G:H|$. Other texts use $(G:H)$.

Cor If G is finite and $x \in G$, then $|x|$ divides $|G|$. In particular, $x^{|G|} = 1$.

Pf $|x| = |\langle x \rangle|$. $\square$

cyclic gp of order p written multiplicatively

Cor If $|G| = p$ is prime, then G is cyclic, isomorphic to Z_p.

Pf Let $x \in G \setminus \{1\}$ so that $|x|$ is a positive divisor of p. Since p is prime, $|x| = p \Rightarrow \langle x \rangle = G$ is cyclic of order p. $\square$

Saturday, February 7, 2015 3:50 PM

For G finite, Lagrange's theorem gives us an assignment

$$\{H \leq G\} \longrightarrow \{\text{divisors of } |G|\}$$
$$H \longmapsto |H|$$

For each divisor of $|G|$, is there a subgroup $H \leq G$ of that order?

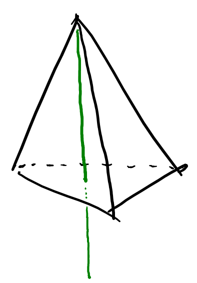
In general, <u>NO</u>. Let T be the group of symmetries of the tetrahedron, so $|T| = 12$. Suppose $\exists H \leq T$ with $|H| = 6$.

Then $|T/H| = 2$. General fact (we'll come back to this): every subgp of index 2 is a normal subgp, i.e. $H \trianglelefteq T$ and $T/H \cong \mathbb{Z}_2$.

$\forall g \in T$. $(gH)^2 = H \Rightarrow g^2 \in H$. If $|g| = 3$, then

$g = g^4 = (g^2)^2 \in H$, i.e. H must contain all elts of T of order 3.

But observe: there are 8 rotations of a tetrahedron of order 3:



rotation by $\pi/3$ & by $-\pi/3$ around each such axis (of which there are 4)

Since $|H| = 6$, we have reached a contradiction and learn that no such H exists!

Here is a partial converse to Lagrange's theorem.

<u>Cauchy's</u> <u>Theorem</u> If G is finite and p is a prime dividing $|G|$, then G has an element of order p.

<u>Pf</u> Later.

Strongest gen'l converse:

<u>Sylow's</u> <u>Theorem</u> If G is finite of order $p^\alpha m$, p a prime not dividing m, then G has a subgp of order p^α.

<u>Pf</u> Later later.

Und jetzt . . . a coset/subgroup grab bag!

Prop If $[G:H]=2$, then $H \trianglelefteq G$.

Pf Let $g \in G \setminus H$ so $G/H = \{H, gH\} = \{H, Hg\} = \{H, G\setminus H\}$.
Clearly $gH = G \setminus H = Hg$, so $gHg^{-1} = H$. $\square$

Defn Let $H, K \leq G$ and define $HK = \{hk \mid h \in H, k \in K\}$.

Prop If $|H|, |K| < \infty$, then $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

Pf $HK = \bigcup_{h \in H} \underbrace{hK}_{\substack{\text{all of size } |K| \text{ and} \\ \text{either equal or disjoint}}}$. Suffices to find the number of distinct hK.

$$h_1K = h_2K \iff \underbrace{h_1h_2^{-1}}_{\text{automatically in } H} \in K \iff h_1h_2^{-1} \in H \cap K \iff h_1(H\cap K) = h_2(H \cap K)$$

Thus # distinct hK, $h \in H$ = # distinct $h(H\cap K)$, $h \in H$.

By Lagrange, the latter # is $\dfrac{|H|}{|H \cap K|}$.

Since each hK has size $|K|$, we learn

$$|HK| = \frac{|H||K|}{|H \cap K|}. \quad \square$$

Prop If $H, K \leq G$, then $HK \leq G \iff HK = KH$.

Pf Reading (indices and inverses!) $\square$

⚠ $HK = KH$ does not mean elts of H commute w/ elts of K.

<u>Cor</u> $H, K \leq G$ & $H \leq N_G(K) \Rightarrow HK \leq G$.

In particular, if $K \trianglelefteq G$ then $HK \leq G \;\; \forall H \leq G$.

<u>Pf</u> Show that $HK = KH$. Let $h \in H$, $k \in K$. Since $H \leq N_G(K)$,

$hkh^{-1} \in K \Rightarrow hk = hk(h^{-1}h) = \underbrace{(hkh^{-1})}_{\in K} h \in KH$.

Thus $HK \subseteq KH$.

Similarly, $kh = h(h^{-1}kh) \in HK$, giving the opposite inclusion.

We now get the cor from the prop. $\square$

<u>Final note</u> $G/H = \{gH \mid g \in G\}$ = left cosets

$H \backslash G = \{Hg \mid g \in G\}$ = right cosets

$$gH = Hg \;\; \forall g \in G$$
$$\Updownarrow$$
$$H \trianglelefteq G \iff G/H = H\backslash G \text{ forms a group}$$
$$\Updownarrow$$
$$H = \ker(\varphi : G \to G') \text{ for some } \varphi$$

G/H & $H\backslash G$ are still <u>sets</u> when $H \leq G$ is <u>not</u> normal.

In fact, $G \circlearrowright G/H$ and this sort of action is super important.

$$g_0 \cdot (g_1 H) = (g_0 g_1) H$$