Math 322, lecture 9, 5/10/2017

Last time: $G/H \overset{\text{def}}{=} G/\cdot \equiv_L \cdot (H)$ = space of left cosets

$[G:H] \overset{\text{def}}{=} |G/H|$

Thm (Lagrange) $|G| = [G:H] \cdot |H|$

Cor (G finite) (1) $\#H \mid \#G$, (2) if $g \in G$ then $\operatorname{order}(g) \mid \#G$,

(3) $g^{\#G} = e$.

Eg: (Fermat little thm) $\forall a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $a^{p-1} = [1]_p$

equiv: $a^p \equiv a \ (p)$ for all $a \in \mathbb{Z}$

Cor: If $\#G = p$ then $G \simeq C_p$

Pf: Let $g \in G \setminus \{e\}$. Then $\operatorname{order}(g) = p$ so $\underset{\overset{\wr\wr}{C_p}}{\langle g \rangle} = G$

Today: Normal subgps & Quotient groups

We will answer question "which $H < G$ are of the form $\operatorname{Ker}(f)$?"

Lemma: Let $f \in \operatorname{Hom}(G, H)$, let $g \in G$. Then $\underbrace{g \operatorname{Ker}(f) g^{-1}}_{= \{gng^{-1} \mid n \in \operatorname{Ker}(f)\}} = \operatorname{Ker}(f)$

Pf: Suppose $g \in G$, $n \in \operatorname{Ker}(f)$.

Then $f(gng^{-1}) \underset{f \text{ is a hom}}{=} f(g) f(n) f(g^{-1}) \overset{n \in \operatorname{Ker} f}{\underset{f \text{ is a hom}}{=}} f(g) \cdot e_H f(g)^{-1} = f(g) f(g)^{-1} = e_H$.

So $gng^{-1} \in \operatorname{Ker}(f)$

~~got~~ $g \operatorname{Ker}(f) g^{-1} \subset \operatorname{Ker}(f)$ For reverse see PS 5.

Def: Call $N < G$ <u>normal</u> if $gN = Ng$ for all $g \in G$

equivalently if $gNg^{-1} = N$ for all $g \in G$

In that case write $N \triangleleft G$

(HW: enough to check $gNg^{-1} \subset N$ for all $g \in G$)

<u>Examples</u>: (0) $\{e\}$, G allways normal in G.

(1) Every subgp of an abelian gp

(2) $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ (Kernel of det)

(if det $x = 1$ then $\det(gxg^{-1}) = 1$ as well)

(3) $A_n \triangleleft S_n$ (Kernel of $\operatorname{sgn} \in \operatorname{Hom}(S_n, \{\pm 1\})$)

(4) $\{\text{Translations}\} \triangleleft \left\{\begin{matrix}\text{Rigid maps} \\ \text{of } \mathbb{E}^n\end{matrix}\right\} = \operatorname{Isom}(\mathbb{E}^n)$

(5) In D_{2n}, "rotations" $= \langle r \rangle \triangleleft D_{2n}$

<u>Lemma</u>: The intersection of any (non empty) family of normal subgps is normal

<u>Pf</u>: Say $N = \bigcap \mathcal{N}$ $g \in G$, $n \in N$ then for all $H \in \mathcal{N}$,

$n \in H$, so $gng^{-1} \in H$ (H is normal) so $gng^{-1} \in N$.

Def: The <u>normal closure of</u> $S \subset G$ is the normal subgp

$$\langle S \rangle^N = \bigcap \{N \triangleleft G \mid S \subset N\}.$$

<u>non example</u>: $G = S_3$, $H = \{(12), id\}$

let $\sigma = (123) \in G$. Check: $\sigma H \sigma^{-1} = \{\sigma (12) \sigma^{-1}, id\} \neq H$.

Quotient groups

Let G be a gp, $N \trianglelefteq G$. We want to understand how G is put together from N & "something more".

Lemma: The subgp $N < G$ is normal iff the relation $\equiv_L (N)$ respects products & inverses

Pf: Suppose $N \trianglelefteq G$, $g \equiv g' \ (N)$, $h \equiv h' \ (N)$.

if N is normal, $\equiv_L (N)$, $\equiv_R (N)$ are same

Then $(gh)^{-1} \cdot (g'h') = h^{-1} g^{-1} g' h' =$

$$= h^{-1}(g^{-1}g') h \, (h^{-1}h')$$

now $g^{-1}g' \in N$ $\quad (g \equiv g' \ (N))$

$h^{-1}(g^{-1}g') h \in N$ $\quad$ (N is normal)

$h^{-1}h' \in N$ $\quad (h \equiv h' (N))$

$\Rightarrow h^{-1}(g^{-1}g') h (h^{-1}h') \in N$ $\quad$ (N is closed under pdts)

so $gh \equiv g'h' (N)$

Similarly, $g^{-1} \equiv (g')^{-1} \ (N)$ because $g(g')^{-1} g = g(g')^{-1} g g^{-1} =$

$$= g\left((g')^{-1} g\right) g^{-1} = g\left((g^{-1}g')^{-1}\right) g^{-1} \in N$$

because $g^{-1}g' \in N$ and N is a normal subgp

(Converse is in PS 5)

Cor: Defining group operations via representatives in G/N is well-defined when N is normal.

Def: $(gN)\cdot(hN) \overset{\text{def}}{=} gh\cdot N$

Now have: (1) Set G/N (2) operation $\cdot : G/N \times G/N \to G/N$

(3) $q : G \to G/N$ $(q(g) = gN)$ s.t. $q(gh) = q(g)\,q(h)$

"quotient map" "quotient group" $[g]_{\equiv(N)}$

Lemma: $(G/N, \cdot)$ is a group.

Pf: Map q is surjective by ~~construct~~ definition so can view all elements of G/N as images by q of elements of G.

Next: (1) $(q(a)\,q(b))\,q(c) = q(ab)\cdot q(c) = q((ab)c)$ $\big\}$ by assoc law in G.

$q(a)\,(q(b)\,q(c)) = q(a)\,q(bc) = q(a(bc))$

(2) $q(e_G)\cdot q(a) = q(e_G \cdot a) = q(a)$ (e_G identity of G)

(3) $q(a^{-1})\cdot q(a) = q(a^{-1}a) = q(e_G)$

So G/N has an identity & left inverses.

Def: Call G/N the quotient (group) of G by N.

Lemma: $q : G \to G/N$ is a surjective gp hom with kernel N

Pf: Only thing remaining to check is $\mathrm{Ker}(q)$:

$g \in \mathrm{Ker}(q)$ iff $q(g) = q(e) \Leftrightarrow gN = eN \Leftrightarrow e \equiv g\ (N)$

$\Leftrightarrow g \in N$

Digression; Why care?

(1) Construction: from G, N make new group G/N.

(2) G/N hopefully simpler than G (N got killed off)

(3) G is "assembled" from N, G/N.

(4) If G is finite, $N \neq \{e\}, G$ then N, G/N are smaller

(5) If $f \in \mathrm{Hom}(G, H)$, and $N \subset \mathrm{Ker}(f)$, N normal
Can interpret f as a function on G/N.

PS 5: Given groups N, H, "extra data"
Can make gp $N \rtimes H$ ("semidirect product")
s.t. N is normal there, quotient is H, and more...

Def: Call G simple if G has no normal subgps other than $\{e\}$, G.

Ex: C_p is simple (Lagrange: every subgp has order 1 or p)

Fact: A commutative finite simple group is isom to some C_p

Problem: List all non-commutative finite simple groups

Eg: $\{A_n\}_{n \geq 5}$ are simple.