Lecture 3 - Subgroups, Quotients & Homomorphisms

Note Title 1/25/2008

Last time, finished with subgroups. Today we pick-up that thread and its dual: quotient spaces.

Def Let S be a subset of G. Then the subgroup generated by S is defined by
$$\langle S \rangle = \bigcap_{S \subset H} H$$

Prop 6 $\langle S \rangle = \{ \underbrace{a_1 \cdots a_n}_{\text{arbitrary length}} \mid a_i \in S \text{ or } a_i^{-1} \in S \}$

Let's say that $S^{-1} = \{ a \mid a^{-1} \in S \}$. Then the strings are those with $a_i \in S \cup S^{-1}$

Pf Call the RHS R. We have to show that $R \subseteq \langle S \rangle = \bigcap_{S \subseteq H} H$ & $\langle S \rangle \subseteq R$.

$\langle S \rangle \subseteq R$: If R is a subgroup, then this follows, since
$$\langle S \rangle = \bigcap_{S \subset H} H = \Big(\bigcap_{\substack{S \subset H \\ H \neq R}} H \Big) \cap R \subseteq R$$

By Lemma 4, R is a subgroup iff $g, h \in R \Rightarrow g^{-1} h \in R$. So let

$g = a_1 \cdots a_n$, $h = b_1 \cdots b_m$, $a_i, b_j \in (S \cup S^{-1}) \Rightarrow$

$g^{-1} h = a_n^{-1} \cdots a_1^{-1} b_1 \cdots b_m$ is also a string with entries in S or S^{-1}.

$\Rightarrow g^{-1} h \in R$.

$R \subseteq \langle S \rangle$: Since $\langle S \rangle = \bigcap_{S \subset H} H$, we have to show that $R \subseteq H$ for all $H \supseteq S$.

This is easy. Since $S \subseteq H$ & H is a subgroup, $S^{-1} \subseteq H$. Again, since H is a subgroup, we can form arbitrary products of elements in H and stay in $H \Rightarrow$ any string with elements in S or S^{-1} is again in $H \Rightarrow R \subseteq H$. ∎

Def A group G is finitely generated if $G = \langle S \rangle$ for some finite set S.

A group is cyclic if it is generated by one element.

Lemma 3 shows us that cyclic groups are especially nice. We do more on this later.

Def The order of a group G is the number of elements in the underlying set: $|G|$

If $g \in G$, the order of g, $o(g)$, is the number of elements in $\langle g \rangle$.

Lemma 6: Let G be a group, $g \in G$, then

a) $o(g) = \infty \leftrightarrow g^n \neq e \quad \forall n$

b) $o(g) = n \Leftrightarrow g^n = e, \; g^{<n} \neq e$

c) $g^k = e \Leftrightarrow k$ is divisible by $o(g)$ $\left(o(g) \mid k \right)$

Pf: $o(g)$ is finite iff $g^r = g^s$ for some $r \neq s$ (in fact, for ∞ly many r's). Can assume $r > s$, and multiply both sides by g^{-s}, getting $g^{r-s} = e$. This shows

$$o(g) < \infty \leftrightarrow g^r = g^s, \; r \neq s \leftrightarrow g^{r-s} = e$$

This shows a).

Let $n = o(g) < \infty$, $\Rightarrow g^m = e$ some minimal m. $\Rightarrow$ (by above argument about r's) $\{e, g, \dots, g^{m-1}\}$ are all distinct elements of $\langle g \rangle$. If $k \in \mathbb{Z}$, we can write $k = qm + r$, where $0 \le r < m$, and Lemma 3 $\Rightarrow g^k = g^{qm} g^r = e^q g^r = g^r$.

So the m elements $\{e = g^0, g^1, \dots, g^{m-1}\}$ are all of the elements of $\langle g \rangle$, and $n = m$. $\Rightarrow$ b). We also see that if $g^k = e$, then $k = qm$ for some $q \Rightarrow$ c) ☒

We'll soon see that all cyclic groups are either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ = ints modulo n.

Quotient Spaces:

Let $H \subset G$ be a subgroup. We can define two equivalence relations on G as follows:

$$a \sim_L b \leftrightarrow a^{-1} b \in H$$
$$a \sim_R b \leftrightarrow a b^{-1} \in H$$

basically the same form, so all results about each hold for the other.

Why is this an equivalence relation?

$$a \overset{?}{\sim_L} a \leftrightarrow a^{-1} a = e \in H \quad \checkmark$$
$$(a \sim_L b \overset{?}{\Rightarrow} b \sim_L a) \leftrightarrow a^{-1} b \in H \Rightarrow b^{-1} a = (a^{-1} b)^{-1} \in H \quad \checkmark$$
$$(a \sim_L b, \; b \sim_L c \overset{?}{\Rightarrow} a \sim_L c) \leftrightarrow a^{-1} b, \; b^{-1} c \in H \Rightarrow a^{-1} c = (a^{-1} b)(b^{-1} c) \in H \quad \checkmark$$

So "$\sim$ is an equiv relation" is basically the same as "H is a s.group"

Def The quotient of G by H is the set of equivalence classes:

$$G/H = G/\sim_L$$
$$H \backslash G = G/\sim_R$$

The elements of $G/\sim_?$ are called cosets. Why?

Prop 7 $[a] = aH = \{ah \mid h \in H\}$

Pf: If $b \in [a]$, then $a \sim_L b \leftrightarrow a^{-1}b = h \in H \leftrightarrow b = ah$. ☒

Remark if $\sim$ were $\sim_R$, $[a] = Ha = \{ha \mid h \in H\}$.

We saw in lecture 1 that equivalence classes are either equal or disjoint

$\Rightarrow$ G/H forms a partition of G (each element is in exactly one of the subsets)

Def The number of elements of G/H is the index of H in G:

$$|G/H| = [G:H]$$

Thm 8: a) $|H| = |aH|$ for all a

b) $|G| = [G:H] \cdot |H|$

Pf Part b) follows from a) as follows: G/H is a partition of G into $[G:H]$ sets of the form aH. Part a) says these are all the same size, namely $|H|$. $\Rightarrow$ $\underset{\substack{\uparrow \\ \text{number} \\ \text{of elem.}}}{|G|} = \underset{\substack{\uparrow \\ \text{number of} \\ \text{subsets}}}{[G:H]} \cdot \underset{\substack{\uparrow \\ \text{size of} \\ \text{each subset}}}{|H|}$

For part a), we define mutually inverse functions $H \xrightarrow{\phi} aH$ and $aH \xrightarrow{\psi} H$

$\phi(h) = ah$, $\psi(ah) = h$. ☒

Remark ϕ and ψ are defined on all of G: $\phi(g) = ag$, $\psi(g) = a^{-1}g$. They are

They are bijections of G with itself and they swap H and aH.

Cor 9: 1) If $|G|$ is finite, then $|H| \mid |G|$ for all subgroups H

2) If $g \in G$, then $o(g) \mid |G|$

3) If $|G| = p$ is prime, then the only subgroups of G are $\{e\}$ and G

4) If $|G| = n$, then $g^n = e$ $\forall g \in G$.

Pf: Theorem 8b gives 1) since $[G:H]$ is an integer.

1) gives 2), since $o(g) = |\langle g \rangle|$.

For 3), If H is a subgroup of G, then $|H| \mid |G|$ by 1) $\Rightarrow$ $|H| = 1$ or p

If $|H| = 1$, $H = \{e\}$, if $|H| = |G|$, then $H = G$.

For 4) 2) $\Rightarrow$ $o(g) \mid n$, and Lemma 6c $\Rightarrow$ $g^n = e$. ☒

Now we will build the morphisms in our category.

Def A function $f: G \to H$ is a homomorphism if

$$f(a \cdot b) = f(a) \cdot f(b)$$

• in G • in H

So a homomorphism translates the product in G into the product in H.

The Hom sets in groups are $\mathrm{Hom}(G,H) = \{f: G \to H \mid f \text{ is a homomorphism}\}$

Same!

Big Question: When does G/H have the structure of a group so that the projection $\pi_H: G \longrightarrow G/H$ is a homomorphism?

Recall: $\pi_H(g) = [g]$, so for this to be a hom, we must have

$$[a \cdot b] = \pi_H(a \cdot b) = \pi_H(a) \cdot \pi_H(b) = [a] \cdot [b]$$

Need to check that this is well-defined. Ie we need to know that if $a \sim a'$, $b \sim b'$, then $ab \sim a'b'$ (since $[a] = [a']$, etc).

So we must check that $ab \sim (ah_1)(bh_2) \longleftrightarrow (ab)^{-1}(ah_1)(bh_2) \in H$

$\longleftrightarrow b^{-1}h_1 b h_2 \in H$. Since $h_2 \in H$, $\longleftrightarrow b^{-1}h_1 b \in H$ for all h_1 & b.

$\longleftrightarrow b^{-1}Hb = H \quad \forall b.$

Def A subgroup N is normal if $b^{-1}Nb \subseteq N \quad \forall b.$

Thm 10 If N is normal, then $[a] \cdot [b] = [ab]$ endows G/N with the structure of a group & the natural projection $G \to G/N$ is a homomorphism.

Pf The second half we have seen. We have also seen that if N is normal, then the mult on G/N is well defined. Associativity of this follows from that of G.

- $[e]$ is the identity: $[e] \cdot [g] = [e \cdot g] = [g] = [g] \cdot [e]$
- $[g^{-1}]$ is the inverse of $[g]$: $[g^{-1}] \cdot [g] = [g^{-1}g] = [e]$.