AMP-Algebra Day 7

Cosets & Normal Subgroups

A new day, a new definition: Suppose you have a subgroup $H < G$. Take some $x \in G$. The <u>left</u> <u>coset</u> <u>of</u> <u>H</u> <u>containing</u> <u>x</u> is the set

$$xH = \{xh : h \in H\}$$

You can think of this as taking the subgroup H and "translating" it by x. Some orienting facts: $eH = H$. But also if $x \in H$ already, then $xH = H$ (why?). Let's go over one easy example and one hard example:

Consider the group $\mathbb{Z}_6 = \{0\ 1\ 2\ 3\ 4\ 5\}$ and its subgroup $H = \{0, 3\} < \mathbb{Z}_6$. The coset $1H$ (often denoted $1+H$ since our operation is "+") will be $1H = \{1+0, 1+3\} = \{1, 4\}$. See, we just took H and translated it over by 1.

Similarly $2H = \{2+0, 2+3\} = \{2, 5\}$. Notice something here: since the identity is in any subgroup, $\underline{x \in xH}$ always. What if we translated by a different number though? Well, notice that $4H = \{4+0, 4+3\} = \{4, 1\}$ again, and $5H = \{5+0, 5+3\} = \{5, 2\}$.

This suggests something that we should formalize as a theorem. ... But first I said I'd do another example.

Consider the group G I gave you in an exercise once that, as a set, could be written as $\{e\ a\ b\ ab\ ba\ aba\}$ and the group operation satisfied $aa=e$, $bb=ee$, and $aba=bab$. This group is actually isomorphic to S_3 via the bijection $G \longleftrightarrow S_3$

$$e \longleftrightarrow e \qquad a \longleftrightarrow (1\ 2) \qquad b \longleftrightarrow (2\ 3)$$

$$ab \longleftrightarrow (1\ 2\ 3) \quad ba \longleftrightarrow (1\ 3\ 2) \quad aba \longleftrightarrow (1\ 3).$$

But that isomorphism is incidental. Look at the subgroup $\{e,a\}=H < G$. If we translate by b on the left we get the coset $bH=\{be,ba\}=\{b,ba\}$, and if we translate by ab on the left we get $(ab)H=\{abe,aba\}=\{ab,aba\}$. But notice too

$$(ba)H=\{bae,baa\}=\{ba,b\}=bH$$

$$(aba)H=\{abae,abaa\}=\{aba,ab\}=(ab)H$$

Now we're gotta write that theorem! ... nah, not yet

Do some exercises first, then right-cosets.

Everything we've done so far deals with left cosets, but now what about right cosets? Let's define

$$~~\text{}~~\; Hx = \{hx : h \in H\}$$

for some $H < G$ and $x \in G$. How do these compare to the left cosets from before?

Do exercises #2 and #3

Notice that for $\{0,3\} < \mathbb{Z}_6$, the left and right cosets coincide whereas for $\{e,a\} < S_3$ they don't. This property is important, and will be key to what we discuss tomorrow, so let's name ~~it~~ it. We'll say a subgroup $N < G$ is normal in G if the left cosets and right cosets of N coincide. In equations, this means that $xN = Nx$ for all $x \in G$. Sometimes you'll see this condition written as $xNx^{-1} = N$. And its customary to write $N \triangleleft G$ for a normal subgroup.

THEOREM – If $y \in xH$, then $x \in yH$, and furthermore we get that $yH = xH$.

Proof If $y \in xH$, this means there exists an $h \in H$ such that $y = xh$. Multiplying by h^{-1} on the right we get $yh^{-1} = x$, so $yH \ni x$ since we can write x as y times $h^{-1} \in H$. Then for any h' in H we have that $y = xh \Rightarrow yh' = xhh' \in xH$. Since $yh' \in xH$ for ANY $h' \in H$, $yH \subset xH$.

Now in this entire previous paragraph, x and y were both general elements of G, so the previous proof is still valid if we swap x and y. Therefore $xH \subset yH$ too, and so $xH = yH$. $\square$

This theorem strongly suggests another theorem, but I don't want to prove this one so we'll call it a proposition instead.

PROPOSITION — For any $H < G$, and any $x, y \in G$ we have $xH = yH$ or we have $xH \cap yH = \emptyset$. I.e. the cosets of a subgroup H partition G into disjoint cosets.

Nah, this is easy to prove, so let's do it. All we must show is that $xH \cap yH \neq \emptyset$, then $xH = yH$.

Proof Take $z \in xH \cap yH$. By the previous theorem $zH = xH$ and $zH = yH$, so $xH = yH$. $\square$

And from this we get tons of lovely facts, including Lagrange's theorem (see the exercises). One more tidbit of knowledge: If you have $H < G$ the index of H in G is the number of cosets of H in G. The index is usually denoted $[G:H]$, or some slight variation of that.