Cosets and the orders of subgroups

Even though we can't define the quotient group G/H for every subgroup $H \leq G$, we showed that the left cosets still form a parition of G. For $|G|$ finite, this gives an easy proof of Lagrange's Theorem:

Thm: (Lagrange's theorem) If G is a finite group and $H \leq G$, $|H|$ divides $|G|$, and $\frac{|G|}{|H|}$ is the number of left cosets of H in G.

Pf: Let $g \in G$, and consider the coset gH.

Define the function $f: H \to gH$ by $h \mapsto gh$.

f is surjective by definition of gH, and if $gh = gh'$, then $h = h'$, so f is also injective. Thus, $|H| = |gH|$, so all cosets have the same # of elements.

Since they partition G, $|G| = |H| \cdot \alpha$, where α = # of cosets. $\square$

In the case of infinite groups, it's possible for a subgroup to have a finite # of cosets:

e.g. $n\mathbb{Z} \leq \mathbb{Z}$ has n left cosets.

Def: If G is any group (possibly infinite) and $H \leq G$, the number of left cosets of H in G is called the index of H in G and is denoted $|G:H|$.

Ex: $H = \{(a,0) \mid a \in \mathbb{Z}\} \leq \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = G$

The cosets are $\underset{(0,0)+H}{\mathbb{Z} \times \{0\}}$, $\underset{(0,1)+H}{\mathbb{Z} \times \{1\}}$, $\underset{(0,2)+H}{\mathbb{Z} \times \{2\}}$, so $|G:H| = 3$.

$G/H \cong \mathbb{Z}/3\mathbb{Z}$.

Ex: Let $H \leq G$ be a subgroup of index 2.

Then for any $g \notin H$, $\{gH, 1H\}$ are the left cosets of H.

Similarly, the right cosets are Hg and $H1$.

Thus, $\forall \; g \in G - H$, $gH = Hg$. If $g \in H$, $gH = 1H = H = H1 = Hg$.

$\Rightarrow gH = Hg \; \forall \; g \in G \Rightarrow H \trianglelefteq G$. That is, every subgroup of index 2 is normal.

Note: The index is also equal to the # of right cosets. So while every subgroup has the same # of left and right cosets (HW) they are only equal if the subgroup is normal.

The converse to Lagrange's Thm is not true. i.e. it's not always true that G will have a subgroup of every order that divides $|G|$, but we can give a partial converse now (we'll see another in the next chapter).

Cauchy's Theorem: If G is a finite abelian group and p is a prime dividing $|G|$, then G contains an element of order p (and thus a subgroup of order p).

Pf: We will prove this by induction on the order of G. Assume it's true for every group whose order is less than $|G|$.

Since $|G|>1$, $\exists\ x\in G$ s.t. $x\neq 1$. If $|G|=p$ then $|x|=p$ by Lagrange's Theorem, and we're done. Thus, assume $|G|>p$.

Suppose p divides $|x|$ and write $|x|=pn$. Then $|x^n|=\frac{pn}{(pn,n)}=p$, and we're done.

Thus, assume p doesn't divide $|x|$. Let $N=\langle x\rangle$. G is abelian, so $N\trianglelefteq G$. By Lagrange's Thm $|G/N|=\frac{|G|}{|N|}$.

Since $N\neq 1$, $|G/N|<|G|$. p doesn't divide $|N|$, so p divides $|G/N|$. By induction, G/N contains an element yN of order p.

$yN\neq 1N$, so $y\notin N$, but $y^p\in N$. Thus $\langle y^p\rangle\neq\langle y\rangle$.

$\Rightarrow |y^p|<|y| \Rightarrow |y^p|=\frac{|y|}{(|y|,p)}$ But $(|y|,p)\neq 1$, so $p\,\big|\,|y|$. Thus, we are done by an argument above. $\square$

The idea here is that we could use the fact that G has a normal subgp to deduce something about G from G/N. This is a common approach in algebra. An obvious obstruction to this is if G has no normal subgps other than 1 and G. This is called a <u>simple group</u>.

Products of subgroups

Def: Let H and K be subgroups of G. Define

$$HK = \{hk \mid h \in H, k \in K\}.$$

Note that $H \subseteq HK$ and $K \subseteq HK$, but HK is not necessarily a subgroup of G — e.g. $\langle(1\,2)\rangle\langle(2\,3)\rangle = \{1, (1\,2), (2\,3), (1\,2\,3)\}$, which has order 4 and is thus not a subgroup of S_3.

If G is abelian, then $(hk)(h'k')^{-1} = (hh'^{-1})(kk'^{-1}) \in HK$, so $HK \leq G$. In fact, it is a subgroup in a more general setting:

Thm: $HK \leq G \iff HK = KH$.

Pf: If $HK \leq G$, then $\forall\ h \in H, k \in K$, we know $h \cdot 1 = h \in HK$ and $1 \cdot k = k \in HK$, so $kh \in HK$. Thus

$KH \subseteq HK$.

For the reverse containment, if $hk \in HK$, then $(hk)^{-1} \in HK$, so $(hk)^{-1} = h_1 k_1$, some $h_1 \in H$, $k_1 \in K$

Thus $hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$. So $HK = KH$.

For the converse, assume $HK = KH$.

Let $a, b \in HK$. We want to show $ab^{-1} \in HK$

Let $a = h_1 k_1$, $b = h_2 k_2$. Then $ab^{-1} = h_1 \underbrace{k_1 k_2^{-1} h_2^{-1}}_{\in\, KH = HK} = h_1 h_3 k_3 \in HK$.

$\Rightarrow HK \leq G$. $\square$

(Note that $HK = KH$ does <u>not</u> mean elements of H commute w/ elements of K. It just means we can write hk as $hk = k'h'$, for some $k' \in K$, $h' \in H$.)

<u>Cor</u>: If $K \trianglelefteq G$, then $HK \leq G$ for any $H \leq G$.

<u>Pf</u>: Assume $K \trianglelefteq G$. $HK = \bigcup_{h \in H} hK \overset{\uparrow}{=} \bigcup_{h \in H} Kh = KH$. $\Rightarrow HK \leq G$. $\square$

normality!

If G is finite, how many elements does HK have?

HK is the union of cosets, but some of those cosets may be equal.

$$h_1K = h_2K \iff h_1 = h_2k, \text{ some } k \in K$$
$$\iff h_2^{-1}h_1 \in K.$$
$$\iff h_2^{-1}h_1 \in H \cap K \iff h_1(H\cap K) = h_2(H \cap K).$$

So the number of distinct cosets in the union is

$\dfrac{|H|}{|H\cap K|}$ by Lagrange's theorem. Since each coset

has $|K|$ elements,

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