Normal subgroups (D+F 3.1)

We've now shown how to define G/K if K is the kernel of some homomorphism. However, we showed that you can define the multiplication in the group w/out using the homomorphism at all. i.e. $(aK)(bK) = abK$. This raises a natural question:

Question: If $H \leq G$, can we define the quotient group G/H?

Answer: In general, no!! We will see why soon. In fact, we'll show that the group operation on G/H is well-defined if and only if H is the kernel of a homomorphism. We'll soon give a criterion to determine when H is a kernel.

First, we'll show that for *any* subgroup, the following holds:

Prop: Let $N \leq G$. The set of left cosets of N in G form a partition of G.

Pf: For any $g \in G$, $g \in gN$, since $1 \in N$. Thus, the union of cosets is all of G.

Suppose $uN \neq vN$. WLOG, let $un \in uN$ but not in vN.

We want to show $uN \cap vN = \emptyset$. For the sake of contradiction, assume $g \in uN \cap vN$, then $g = ua = vb$

$\Rightarrow \quad un = uaa^{-1}n = vba^{-1}n \in vN$, a contradiction. Thus, the cosets form a partition. $\square$

Note: This means that u and v are in the same coset $\Longleftrightarrow uN = vN \Longleftrightarrow u = vn$, some $n \in N \Longleftrightarrow v^{-1}u \in N$.

Prop: Let G be a group and $N \leq G$.

1.) The operation on left cosets $uN \cdot vN = uvN$ is well-defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

2.) If the above operation is well-defined, then the cosets form a group, G/N, w/ identity $1N = 1$, and $(gN)^{-1} = g^{-1}N$.

Pf: 1.) First assume it's well-defined. i.e. if $uN = u'N$ and $vN = v'N$ then $uvN = u'v'N$.

$$(1N)(g^{-1}N) \qquad (nN)(g^{-1}N)$$

Let $g \in G$, $n \in N$. Then $1N = nN$, so $1g^{-1}N = ng^{-1}N$

$\Rightarrow gg^{-1}N = gng^{-1}N$

$\Rightarrow N = gng^{-1}N \Rightarrow gng^{-1} \in N$.

Now we prove the converse. Assume $gng^{-1} \in N \ \forall n \in N, g \in G$.

Suppose $u, u' \in uN$ (i.e. $uN = u'N$) and $v, v' \in vN$.

We need to show $u'v' \in uvN$. For some $n, m \in N$, we have

$u'v' = (um)(vn) = uvv^{-1}mvn = uv(v^{-1}mv)n$.

$v^{-1}mv \in N$, $n \in N$, so $uv(v^{-1}mv)n \in uvN$, as desired.

2.) If the operation is well-defined, we just need to check the group axioms:

For $g \in G$, $1N\, gN = 1gN = gN = gN\,1N$, so $1N$ is the identity.

$gN\, g^{-1}N = gg^{-1}N = 1N = g^{-1}gN = g^{-1}N\, gN$, so gN has inverse $g^{-1}N$.

If $a, b, c \in G$, associativity follows from associativity on G. $\square$

So now we have a condition for when G/N is a group. More formally:

Def: gng^{-1} is the <u>conjugate</u> of $n \in N$ by g.

The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the <u>conjugate</u> of N by g.

g <u>normalizes</u> N if $gNg^{-1} = N$.

A subgroup $N \leq G$ is <u>normal</u> if every element of G normalizes N, and we write $N \trianglelefteq G$ to denote that N is a normal subgroup of G.

Sometimes it's hard to check $gNg^{-1} = N$, so we can use the following:

Thm: The following are equivalent:

1.) $N \trianglelefteq G$

2.) $gN = Ng \quad \forall\, g \in G$.

3.) $gNg^{-1} \subseteq N \quad \forall\, g \in G$.

Pf: Clearly 1.) $\Rightarrow$ 3.). For the rest, see HW.

Now we show that normal subgroups are exactly possible kernels of homomorphisms.

Theorem: $N \leq G$ is normal $\Leftrightarrow$ it is the kernel of a homomorphism.

Pf: If N is the kernel of a homomorphism, then we showed left cosets are the same as right cosets. Thus, the above shows $N \trianglelefteq G$.

Now assume $N \trianglelefteq G$. Then let $H = G/N$, and define

$$\varphi : G \to G/N \text{ by } \varphi(g) = gN$$

By the definition of the operation on G/N, if $g, h \in G$,

$$\varphi(gh) = ghN = gN\,hN = \varphi(g)\varphi(h),$$

so this is a homomorphism, and

$$\varphi(g) = 1N \iff gN = 1N \iff g \in N, \quad \text{so} \quad \ker\varphi = N. \ \square$$

Ex:

1.) Any subgroup of an abelian group is normal since $gng^{-1} = n \ \forall \ g, n \in G$.

In fact, if $N \leq Z(G)$, then N is normal in G since every element of N commutes w/ every element of G.

2.) $Z(D_8) = \{1, r^2\}$, so $\langle r^2 \rangle \trianglelefteq D_8$.

The cosets in $D_8/\langle r^2 \rangle$ are the two element sets $\{g, gr^2\}$, so there are 4 of them. i.e. $|D_8/\langle r^2 \rangle| = 4$.

Which group of order 4 is it isomorphic to?

$r^2 \in \langle r^2 \rangle$, so $|r\langle r^2 \rangle| = 2$. $\quad s^2 = 1 \in \langle r^2 \rangle$, so $|s\langle r^2 \rangle| = 2$.

i.e. 2 distinct elements have order 2, so $D_8/\langle r^2 \rangle \not\cong \mathbb{Z}_4$.

Thus $D_8/\langle r^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

3.) Let $H = \langle (1\,2\,3) \rangle \leq S_3$. Is $H \trianglelefteq S_3$? On HW: $H \trianglelefteq S_3 \iff N_{S_3}(H) = S_3$.

$$\underset{\substack{\shortparallel \\ (1\,2)^{-1}}}{(1\,2)}(1\,2\,3)(1\,2) = (1\,3\,2) \in H. \quad \text{Thus} \quad (1\,2) \in N_G(H).$$

We know $\underset{\substack{\uparrow \\ \text{order } 3}}{H} \leq \underset{\substack{\uparrow \\ \text{order} > 3}}{N_{S_3}(H)} \leq \underset{\substack{\uparrow \\ \text{order } 6}}{S_3}$ so $N_{S_3}(H) = S_3 \implies H \trianglelefteq S_3$.

$|S_3/H| = 2$, so $S_3/H \cong \mathbb{Z}_2$

Ex: (non-normal subgroup) Let $H = \langle (1\,2) \rangle \leq S_3$.

$(1\,3)(1\,2)(1\,3) = (2\,3) \notin H$. Thus $N_{S_3}(H) \neq S_3$ (In fact it is just H), so $H \ntrianglelefteq S_3$.