SEPTEMBER 28 NOTES

1. 3.1: Quotient groups and homomorphisms

Last time, we introduced quotient groups as the group of all fibers of a homomorphism. Before my computer gave up, we were in-progress of relating that definition to cosets, which we will continue today.

Definition 1.1. Let $H \leq G$ be any subgroup and $g \in G$. The **left coset** of H with respect to g is

$$gH = \{gh \mid h \in H\}.$$

The **right coset** is

$$Hg = \{hg \mid h \in H\}.$$

With this definition, we showed last time that:

Theorem 1.2. *Let G be a group and let K be the kernel of some homomorphism from G to another group, $\phi : G \to H$. Then, the fibers $X = \phi^{-1}(a)$ are equal to cosets of K: precisely, for any $u \in X$, $X = uK$. And, the set of left cosets of K forms a group G/K with binary operation $uKvK = (uv)K$.*

And ended with:

Proposition 1.3. *Let H be any subgroup of G. The set of left cosets form a partition of G, meaning for every $g \in G$, g appears in some coset of H, and for two different elements $u, v \in G$, either $uH = vH$ or $uH \cap vH = \emptyset$. Furthermore, $uH = vH$ if and only if $v^{-1}u \in H$.*

Now, we want to talk about quotients by general subgroups (not necessarily kernels).

Definition 1.4. A subgroup N of G is normal if and only if it satisfies any of the following equivalent conditions:

1. For all $g \in G, n \in N$, $gng^{-1} \in N$.
2. For all $g \in G$, $gNg^{-1} = N$.
3. For all $g \in G$, $gN = Ng$.
4. $N_G(N) = G$

If N is normal in G, we denote this by $N \lhd G$.

Some terminology: for $n \in N$, $g \in G$, the element gng^{-1} is called the **conjugate** of n by g. We say g **normalizes** N if $gNg^{-1} = N$.

Proposition 1.5. *Let G be a group and let N be a subgroup of G. Then:*

(1) N is normal if and only if the operation $uNvN = (uv)N$ is well-defined.
(2) If the operation is well-defined, then the set of cosets of N forms a group called G/N.

Proof. We prove (1) and leave (2) as an exercise. The key points for (2) are that $1N$ is the identity in G/H and $(uN)^{-1} = u^{-1}N$.

To prove (1), assume first that N is normal, i.e. $gng^{-1} \in N$ for all $g \in G, n \in N$. To show the operation is well defined, we need to show that if $u, u_1 \in uN$ and $v, v_1 \in vN$, then $uvN = u_1v_1N$. Because $u_1 \in uN$, write $u_1 = un$ and similarly $v_1 = vm$ for some $n, m \in N$. To see that $u_1v_1 \in uvN$, we write:

$$u_1v_1 = (un)(vm) = u(vv^{-1})n(vm) = uv(v^{-1}nv)m.$$

Because N is normal, $v^{-1}nv = n_1 \in N$, so we have

$$u_1v_1 = (un)(vm) = u(vv^{-1})n(vm) = uv(v^{-1}nv)m = uvn_1m = (uv)n_1m \in uvN.$$

Therefore, we have shown that $u_1v_1 \in uvN$, so $uvN \cap u_1v_1N \neq \emptyset$, so we have $uvN = u_1v_1N$ as desired.

For the converse, assume that the operation is well-defined as above. Let $g \in G$ and $n \in N$. If $u = 1$, $u_1 = n$, $v = v_1 = g^{-1}$, then we see that $1g^{-1}N = ng^{-1}N$, so $g^{-1}N = ng^{-1}N$. Therefore, $ng^{-1} \in g^{-1}N$ so $ng^{-1} = g^{-1}n_1$ for some $n_1 \in N$, so $gng^{-1} \in N$, as desired. □

This says exactly that we can define the quotient group G/N for *any* normal subgroup of G. It turns out that this is not actually different than the first definition, and normal subgroups are precisely the subgroups that arise as kernels of homomorphisms.

Proposition 1.6. *A subgroup N of a group G is normal if and only if it is the kernel of some homomorphism.*

Proof. If $N = \ker \phi$ for a homomorphism ϕ, we leave it as an exercise to show that N is normal.

Now, suppose N is normal. Then, let $H = G/N$ and consider $\pi : G \to H$ defined by $\pi(g) = gN$. This is called the **projection homomorphism**. It is indeed a homomorphism by definition of the binary operation in G/N:

$$\pi(g_1g_2) = (g_1g_2)N = g_1Ng_2N = \pi(g_1)\pi(g_2).$$

To compute the kernel, we use the definition:

$$\ker \pi = \{g \in G \mid \pi(g) = 1N\} = \{g \in G \mid gN = 1N\} = \{g \in G \mid g \in N\} = N.$$

Therefore, N arises as the kernel of a homomorphism. □

There are many other interesting quotient groups!

Example 1.7. Let $G = \mathbb{R}^2$ with $H = \mathbb{R}$ and $\phi : G \to H$ given by $\phi(a, b) = a$. The kernel of this map is just $K = \{(0, b) \mid b \in \mathbb{R}\}$, and the fibers of the map are just $\phi^{-1}(a) = \{(a, b) \mid b \in \mathbb{R}\}$. Schematically, the fibers are just the points in the xy-plane on the line $x = a$. The quotient group G/K is then just the set of fibers, which is just the set of vertical lines in the plane, with binary operation given by adding the lines $x = a$ and $x = a_1$ to get the line $x = (a + a_1)$.

2. 3.2: More on cosets and Lagrange's Theorem

Now, we move to discussing cosets in general (not just in the normal case).

Note that if G is abelian, then *every* subgroup is normal, but typically most subgroups are not normal. For example, an exercise: show that $\langle (12) \rangle$ is not a normal subgroup of S_3 (or S_n for any $n \geq 3$).

We start with an essential theorem:

Theorem 2.1. *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

Proof. Let $|H| = n$ and let the number of left cosets in H equal k. We have a bijection between H and gH given by $h \mapsto gh$ (injective by the cancellation law, and surjective by definition of gH). Since the left cosets partition G and they all have the same size, we have $|G| = nk$, so $|H| = n$ divides $|G|$. □

Definition 2.2. The number of left cosets of H is called the **index** of H in G, denoted $[G : H]$.

Lagrange's theorem has many important corollaries!

Corollary 2.3. If G is a finite group, then for any $x \in G$, $\mathrm{ord}(x)$ divides $|G|$. In other words, $x^{|G|} = 1$ for all $x \in G$.

Proof. Because $\text{ord}(x) = |H|$ where $H = \langle x \rangle$, this follows directly from Lagrange's theorem. The second sentence follows because, if $\text{ord}(x)$ divides $|G|$, then $|G| = \text{ord}(x)k$ for some k, so $x^{|G|} = (x^{\text{ord}(x)})^k = 1$. □

Proposition 2.4. *If $|G| = p$ is a prime number, then G is cyclic and hence $G \cong \mathbb{Z}_p$.*

Proof. Let $x \in G$, $x \neq 1$. Let $H = \langle x \rangle$. By Lagrange's theorem, $|H|$ divides $|G| = p$ but $|H| > 1$ by construction so we must have $|H| = p$ and hence $H = G$. Therefore, $G = \langle x \rangle$. □

In the coming chapters, we will prove several related results to Lagrange's theorem. For now, we conclude this section with some other useful corollaries of Lagrange's theorem.

Definition 2.5. Let H and K be subgroups of G and let $HK = \{hk \mid h \in H, k \in K\}$.

Proposition 2.6. *If H and K are finite subgroups of a group G, then*

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

Proof. To try to apply Lagrange's theorem, we count cosets! Note that $HK = \cup_{h \in H} hK$ is a union of cosets of K, and each coset of K has $|K|$ elements. So, we just need to know how many distinct cosets there are. By what we already proved, $h_1K = h_2K$ is and only if $h_2^{-1}h_1 \in K$, so $h_1K = h_2K$ if and only if $h_2^{-1}h_1 \in H \cap K$, if and only if $h_1(H \cap K) = h_2(H \cap K)$. Therefore, the number of cosets of K of the form hK is the number of cosets $h(H \cap K)$, which is $|H|/|H \cap K|$ by Lagrange's Theorem. So, HK is the union of $|H|/|H \cap K|$ cosets of size $|K|$, so we have $|HK| = \frac{|H||K|}{|H \cap K|}$. □

Note that we did not need HK to be a subgroup to prove the previous proposition. It is typically not!

Proposition 2.7. *For H and K subgroups of a group G, HK is a subgroup of G if and only if $HK = KH$.*

Proof. Assume $HK = KH$. Let $a, b \in HK$. We must show that $ab^{-1} \in HK$. Write $a = h_1k_1$ and $b = h_2k_2$ so $b^{-1} = k_2^{-1}h_2^{-1}$, so $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1k_3h_3$ by writing $k_3 = k_1k_2^{-1}$ and $h_3 = h_2^{-1}$. Since $HK = KH$, then $k_3h_3 = h_4k_4$ for some $h_4, k_4 \in H, K$, so $ab^{-1} = h_1h_4k_4 \in HK$, as desired.

Now, suppose HK is a subgroup. Then $K \leq HK$ and $H \leq HK$ (because $1 \in H$ and $1 \in K$), so $KH \leq HK$ (because HK must be closed under the binary operation). Now, let $hk \in HK$ be any element. Because HK is closed under inverses, $(hk)^{-1} = k^{-1}h^{-1} = h_1k_1$ for some $h_1, k_1 \in H, K$, so $hk = k_1^{-1}h_1^{-1} \in KH$, so $HK \subset KH$ and hence $HK = KH$. □

Corollary 2.8. If H and K are subgroups such that $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \lhd G$, then $N_G(K) = G$ so $HK \leq G$ for any $H \leq G$.

Proof. If $H \leq N_G(K)$, then for $h \in H, k \in K$, $hkh^{-1} \in K$ so $hk = (hkh^{-1})h \in KH$. Therefore, $HK \subset KH$. Similarly, $KH \subset HK$ so $HK = KH$ and the statement follows from the previous proposition. □