OCTOBER 3 NOTES

1. 3.2: More on cosets and Lagrange's Theorem

Reminders from last time:

Theorem 1.1. *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.*

Corollary 1.2. If G is a finite group, then for any $x \in G$, $\operatorname{ord}(x)$ divides $|G|$. In other words, $x^{|G|} = 1$ for all $x \in G$.

Proposition 1.3. *If $|G| = p$ is a prime number, then G is cyclic and hence $G \cong \mathbb{Z}_p$.*

Proposition 1.4. *If H and K are finite subgroups of a group G, then*

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

Proposition 1.5. *For H and K subgroups of a group G, HK is a subgroup of G if and only if $HK = KH$.*

Corollary 1.6. 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 $H \leq G$.

2. 3.3: The Isomorphism Theorems

We will derive several facts about quotient groups from their definition, properties, and from Lagrange's theorem. These turn out to be so important that they go by the *First, Second, and Third Isomorphism Theorems.*

Theorem 2.1 (The First Isomorphism Theorem)**.** *If $\phi : G \to H$ is a homomorphism with kernel K, then $G/K \cong \phi(G)$.*

Proof. We saw in the first definition of quotient that G/K is the set of nonempty fibers X_a of ϕ. So, we can define a map $\psi : G/K \to \phi(G)$ by $X_a \mapsto a$. This is a homomorphism: $\psi(X_a \star X_b) = \psi(X_{ab}) = ab = \psi(X_a)\psi(X_b)$. It is also injective: if $\psi(X_a) = \psi(X_b)$, then $a = b$ so $X_a = X_b$. Finally, it is surjective: for any $a \in \phi(G)$, by definition $X_a \neq \emptyset$, so X_a is a nonempty fiber of ϕ mapping to a. Therefore, it is an isomorphism. □

When we talk about *modules*, we will talk about how this is really a special case of studying exact sequences.

As a special instance, we have the following theorem:

Theorem 2.2 (The First Isomorphism Theorem, Special Case)**.** *If $\phi : G \to H$ is a surjective homomorphism with kernel K, then $G/K \cong H$.*

This is very useful for understanding quotient groups!

Example 2.3. Prove that $\mathbb{R}/\mathbb{Z} \cong S^1$ where $S^1 = \{a + bi \in \mathbb{C} \mid a^2 + b^2 = 1\}$.

To prove this, all we need to do is use the First Isomorphism Theorem to construct a homomorphism $\mathbb{R} \to S^1$ with kernel $\mathbb{Z}$. This takes practice. Thinking geometrically, S^1 is the *unit circle*, which we know has something to do with sines and cosines. So, it turns out that the right thing to do is the following. Let $\phi : \mathbb{R} \to S^1$ be the map

$$\phi(r) = \cos(2\pi r) + \sin(2\pi r)i.$$

This is surjective because every point on the unit circle can be written as $(\cos(2\pi r), \sin(2\pi r))$. To prove this is a homomorphism requires some trigonometric identities (a good exercise!). Finally, $\ker \phi = \{r \in \mathbb{R} \mid \cos(2\pi r) + \sin(2\pi r)i = 1 + 0i\} = \mathbb{Z}$, since sine and cosine are only simultaneously 0 and 1 at integer multiples of 2π.

Theorem 2.4 (The Second Isomorphism Theorem)**.** *Let G be a group and $A, B \leq G$. Suppose $A \leq N_G(B)$. Then, AB is a subgroup of G such that $B \lhd AB$ and $A \cap B \lhd A$ and $AB/B \cong A/A \cap B$.*

Proof. We already proved, if $A \leq N_G(B)$, then AB is a subgroup of G. Because $A \leq N_G(B)$ by assumption and $B \leq N_G(B)$ be definition, $AB \leq N_G(B)$. This implies that $B \lhd AB$

Because B is normal in AB, the quotient group AB/B is well-defined, and let $\phi : A \to AB/B$ be the map $\phi(a) = aB$. By definition of the binary operation in AB/B, ϕ is a homomorphism.

It is also surjective: if abB is any coset of B in AB, because $bB = B$, $abB = aB$ so any element of AB/B can be written as aB.

Finally, we consider the kernel. In AB/B, the kernel is $1B$, so $\ker \phi = \{a \in A \mid aB = 1B\}$, but $aB = 1B$ if and only if $1^{-1}a = a \in B$, so $\ker \phi = \{a \in A \mid a \in B\} = A \cap B$. Therefore, $A \cap B$ is normal in A (because it is the kernel of a homomorphism) and $A/A \cap B \cong AB/B$. □

Theorem 2.5 (The Third Isomorphism Theorem)**.** *Let G be a group with $H, K \lhd G$ and $H \leq K$. Then, $K/H \lhd G/H$ and $(G/H)/(K/H) \cong G/K$.*

Proof. Now, let $\phi : G/H \to G/K$ be the map $\phi(gH) = gK$. First, we need to check that this is a function, i.e. if $g_1H = g_2H$, then $\phi(g_1H) = \phi(g_2H)$. Suppose $g_1H = g_2H$, which implies $g_1g_2^{-1} \in H$. Because $H \leq K$, $g_1g_2^{-1} \in K$ so $g_1K = g_2K$ and therefore $\phi(g_1H) = \phi(g_2H)$.

Because $g \in G$ can be any element, this function is surjective. It is also a homomorphism by definition of the binary operation in the quotient group. So, we just need to compute the kernel:

$$\ker \phi = \{gH \in G/H \mid \phi(gH) = 1K\} = \{gH \mid gK = 1K\} = \{gH \mid g \in K\} = K/H.$$

Because K/H is the kernel of a homomorphism, it is a normal subgroup of G/H.

Therefore, by the First Isomorphism Theorem, $(G/H)/(K/H) \cong G/K$. □

Finally, Dummit and Foote includes a 'fourth isomorphism theorem' but this terminology is not standard.

Theorem 2.6 (The Fourth Isomorphism Theorem)**.** *Let G be a group and let $N \lhd G$. There is a bijection between the subgroups of G containing N and the subgroups of G/N given by $A \leq G \leftrightarrow \overline{A} = A/N$. In particular, every subgroup of $\overline{G} = G/N$ is of the form A/N for some $A \leq G$ containing N.*

Proof. Homework! □

3. 3.4: Composition Series and the Holder Program

As we start to *classify* groups, we will see that normal subgroups are a very important tool to understanding groups as a whole. This section mentions some results in this direction.

Proposition 3.1. *Suppose G is a finite abelian group and p is a prime dividing $|G|$. Then, G contains an element of order p.*

Proof. We proceed by induction on $|G|$. This clearly holds for $|G| = 1$ as no primes divide 1. Now, assume the result is true for all groups of order less than n, and let $|G| = n > 1$. Let p be a prime dividing $|G|$. Since $|G| > 1$, there is an element $x \in G$ with $x \neq 1$. If $n = p$, then $\text{ord}(x) = p$ by Lagrange's Theorem so the result holds. Now suppose $n > p$. If p divides $\text{ord}(x)$, then $\text{ord}(x) = pk$ for some k, so $\text{ord}(x^k) = p$ and the result holds. If p does not divide $\text{ord}(x)$, let $N = \langle x \rangle$. Since G is abelian, $N \lhd G$, and $|G/N| = |G|/|N| < |G|$. Furthermore, since $p \mid |G|$ but $p \nmid \text{ord}(x)$ (and hence $p \nmid |N|$) we must have $p \mid |G/N|$. By the inductive hypothesis, $|G/N| < n$ so G/N contains an element yN of order p. Since yN has order p, it cannot be the identity, so $y \notin N$. But, $(yN)^p = y^pN$

is the identity, so $y^p \in N$. Therefore, $\langle y^p \rangle \neq \langle y \rangle$, so $\mathrm{ord}(y^p) = \mathrm{ord}(y)/(p, \mathrm{ord}(y)) < \mathrm{ord}(y)$, which implies $p \mid \mathrm{ord}(y)$. Therefore, $\mathrm{ord}(y) = pk$ for some k so $\mathrm{ord}(y^k) = p$, as desired. □

This is an example of a result where we use information about a normal subgroup N and the quotient G/N to obtain results about G. We will do this several times in the future! But, *not every group has normal subgroups, so we cannot always do this.*

Definition 3.2. A group G is called **simple** if $|G| > 1$ and the only normal subgroups of G are 1 and G.

Example 3.3. We proved, if $G = \mathbb{Z}_p$, then every subgroup $\langle x \rangle = G$ for $x \neq 1$, so $\mathbb{Z}_p$ is simple.

It turns out that these are the *only* finite simple groups of odd order, but this proof is incredibly difficult!

Theorem 3.4 (Feit-Thompson)**.** *If G is a simple group of odd order, then $G \cong \mathbb{Z}_p$ for some prime p.*

We can attempt to understand normal subgroups in general.

Definition 3.5. Let G be a group. A sequence of subgroups

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is called a **composition series** if $N_i \lhd N_{i+1}$ and N_{i+1}/N_i is a simple group for each i. The groups N_{i+1}/N_i are called the **composition factors** of G.

Example 3.6. The series $1 \lhd \langle r^2 \rangle \lhd \langle r \rangle \lhd D_8$ is a composition series for D_8: each subgroup is normal in the next as it has index 2, and for each quotient, N_{i+1}/N_i has two elements so is $\cong \mathbb{Z}_2$ which is simple.

Theorem 3.7 (Jordan-Holder)**.** *If G is a finite group with $|G| > 1$, then:*

(1) G has a composition series, and

(2) The composition factors are unique: given two series

$$1 = N_0 \leq N_1 \leq \cdots \leq N_{j-1} \leq N_j = G$$

and

$$1 = M_0 \leq M_1 \leq \cdots \leq M_{k-1} \leq M_k = G,$$

then $j = k$ and $N_{i+1}/N_i \cong M_{h+1}/M_h$ for some i, h.

We use these composition series to understand groups. We actually often use a weakening of this idea:

Definition 3.8. A group G is solvable if there is a chain of subgroups

$$1 = G_0 \leq G_1 \leq \cdots \leq G_{k-1} \leq G_k = G$$

such that G_{i+1}/G_i is abelian for each i.

Not every group is solvable:

Theorem 3.9. *A finite group G is solvable if and only if for every divisor n of G such that $(n, |G|/n) = 1$, then G has a subgroup of order n.*

Some of your homework will be to come up with examples of solvable groups!