OCTOBER 19 NOTES

1. 4.5: The Sylow Theorems

A reminder of the Sylow theorems:

Definition 1.1. Let G be a group and let p be a prime.

(1) A group of order p^k for some $k \geq 1$ is called a **p-group**. Subgroups which are p-groups are called **p-subgroups.**
(2) If G has order $p^k m$ where $p \nmid m$, then a subgroup of order p^k is called a **Sylow-p-subgroup.**
(3) The set of Sylow p-subgroups is denoted by $Syl_p(G)$ and the number of Sylow p-subgroups in a particular group is denoted by n_p.

Theorem 1.2. *Let G be a group of order $p^k m$, where p is a prime not dividing m. Then:*

(1) Sylow p-subgroups exist, i.e. $n_p \neq 0$.
(2) If P is a Sylow-p-subgroup and Q is any p-subgroup, then for some $g \in G$, $Q \leq gPg^{-1}$. In particular, any two Sylow p-subgroups are conjugate.
(3) The number of Sylow p-subgroups is of the form $1+ap$ for some $a \geq 0$, i.e. $n_p \equiv 1 \pmod{p}$. Furthermore, $n_p = [G : N_G(P)]$, so $n_p \mid m$.

We proved (1) last time. We will prove the remaining parts on Tuesday. Today, we will focus on *using* the Sylow Theorems.

2. 5.1: Direct Products

We begin with reminders on direct products.

Definition 2.1. If $G_1, G_2, \dots$ are groups, then their **direct product** is

$$G_1 \times G_2 \times \cdots = \{(g_1, g_2, \dots) \mid g_i \in G_i\}$$

with binary operation

$$(g_1, g_2, \dots) \star (h_1, h_2, \dots) = (g_1 h_1, g_2 h_2, \dots).$$

Remark 2.2. By definition of the set $G_1 \times G_2 \times \dots$, we have $|G_1 \times G_2 \times \dots| = |G_1||G_2| \dots$.
The identity in the direct product is the element $(1, 1, \dots)$.
The inverse is the element $(g_1, g_2, \dots)^{-1} = (g_1^{-1}, g_2^{-1}, \dots)$.

We have the following proposition, whose proof is left as an exercise.

Proposition 2.3. *Let $G = G_1 \times G_2 \times \cdots \times G_n$.*

(1) For each i, G_i is isomorphic to a subgroup of G given by $G_i \cong \{(1, 1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}$ (the g_i appears in the ith spot.
(2) If we identify G_i with this subgroup, then $G_i \triangleleft G$ and $G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$.
*(3) For each i, there is a surjective **projection** homomorphism $\pi_i : G \to G_i$ given by $\pi_i(g_1, \dots, g_n) = g_i$. The kernel is*

$$\ker \pi_i = \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n) \mid g_j \in G_j\} \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

Example 2.4. We already saw the group $\mathbb{Z}_p \times \mathbb{Z}_p$ as one of the two groups of order p^2 in the previous section.

3. 5.2: Fundamental Theorem of Finitely Generated Abelian Groups

We use direct products to classify all finitely generated abelian groups. We will actually prove this theorem at the end of the semester by the classification of finitely generated modules over PIDs.

Definition 3.1. A group G is **finitely generated** if there is a finite subset $A \subset G$ such that $G = \langle A \rangle$.

Example 3.2. For each $r \in \mathbb{Z}$, the group $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ (r copies of $\mathbb{Z}$) is finitely generated. It is called the **free abelian group of rank** r.

Theorem 3.3. *Let G be a finitely generated abelian group. Then:*

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_s}$$

where $r \geq 0$ and each q_i is a power of a (not necessarily distinct) prime number.

If G is finite with $|G| = n$, then

$$G \cong \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_s}$$

where $n = q_1 \times q_s$ and each q_i is a power of a (not necessarily distinct) prime.

Example 3.4. Suppose $|G| = 20$. Then $20 = 2^2 \cdot 5$, so the possible abelian groups of order 20 are $\mathbb{Z}_4 \times \mathbb{Z}_5$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$.

Proposition 3.5. *If $G = \mathbb{Z}_n \times \mathbb{Z}_m$ and $\gcd(n, m) = 1$, then $G \cong \mathbb{Z}_{nm}$.*

Proof. Exercise: verify that the map $\mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ given by $a \mapsto (a \pmod n, a \pmod m)$ is an isomorphism, or verify that $\text{ord}(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$ is nm, so that $\mathbb{Z}_n \times \mathbb{Z}_m$ must be cyclic. □

Using the proposition, we could write the groups in the previous example alternatively as: $\mathbb{Z}_{20}$ or $\mathbb{Z}_2 \times \mathbb{Z}_{10}$.

We will attempt to classify groups of small order using direct products (but will shortly generalize to semidirect products).

4. 5.4: Recognizing Direct Products

If we can find two normal subgroups of G such that $H \cap K = \{1\}$ (which occurs, for example, if $|H|$ and $|K|$ are relatively prime) and $|G| = |H||K|$ and, then G must be the direct product of H and K.

Theorem 4.1. *Suppose G is a group with normal subgroups H and K with $H \cap K = 1$ such that $HK = G$. Then, $G \cong H \times K$.*

Proof. Because $G = HK$, every element $g \in G$ can be written as $g = hk$ for $h \in H$, $k \in K$. Because $H \cap K = 1$, this is actually unique. Indeed, suppose $g = hk = h'k'$. Then, $h^{-1}h' = k(k')^{-1}$, so $h^{-1}h' \in K$ and hence $h^{-1}h' \in H \cap K$ so $h^{-1}h' = 1$, so $h = h'$, and similarly $k = k'$.

Therefore, we have a function $\phi : G = HK \to H \times K$ given by $\phi(hk) = (h, k)$. This is a well-defined bijection by the uniqueness statement above, so we just need to show that it is a homomorphism.

To show this, it suffices to show that $h_1k_1h_2k_2 = h_1h_2k_1k_2$ for any $h_i \in H, k_i \in K$, which is equivalent to $k_1h_2 = h_2k_1$, which is equivalent to $k_1h_2k_1^{-1}h_2^{-1} = 1$. Because H is normal, we know $k_1h_2k_1^{-1} \in H$, so $k_1h_2k_1^{-1}h_2^{-1} \in H$. Similarly, $k_1h_2k_1^{-1}h_2^{-1} \in K$, so $k_1h_2k_1^{-1}h_2^{-1} \in H \cap K = 1$, and therefore $k_1h_2k_1^{-1}h_2^{-1} = 1$. □

Example 4.2. Let G be a group of order 15. Then, by the Sylow Theorems, both the Sylow 3-subgroup H (with $H \cong \mathbb{Z}_3$) and the Sylow 7-subgroup K (with $K \cong \mathbb{Z}_5$) are normal, and $(3, 5) = 1$, so $|H \cap K| = 1$ and $|H||K| = |G|$. Therefore, the previous theorem implies that $G \cong H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. So, there is only one group of order 15.

5. 5.5: Semidirect Products

Finally, we conclude group theory with semidirect products. We wish to generalize the previous section to classify groups G with subgroups H and K such that $H \cap K = 1$, H is normal in G (but K is not necessarily!) and $|H||K| = |G|$. It turns out we have an analogue of the direct product that we can use to classify these!

In the previous proof, we needed to compute $(h_1k_1)(h_2k_2)$. If only H is normal, we can write this as

$$h_1k_1h_2k_2 = h_1k_1h_2k_1^{-1}k_1k_2 = h_1h_3k_1k_2$$

where $h_3 = k_1h_2k_1^{-1}$ is the conjugation of h_2 by k_1. This is an *automorphism of H*. So we will construct a group that 'looks like' a product but instead of $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$, we will have the binary operation given by $(h_1, k_1)(h_2, k_2) = (h_1\phi_{k_1}(h_2), k_1k_2)$ where ϕ_{k_1} is some automorphism of H induced by $k_1 \in K$.

We state the general construction.

Definition 5.1. Let H and K be groups and let $\phi : K \to \mathrm{Aut}(H)$ be a homomorphism. Given $k \in K$, let ϕ_k denote the automorphism of H given by $\phi(k)$. Then, the set $G = \{(h, k) \mid h \in H, k \in K\}$ is a group with binary operation $(h_1, k_1) \cdot (h_2, k_2) = (h_1\phi_{k_1}(h_2), k_1k_2)$.

This is called the **semi-direct product** of H and K, denoted $H \rtimes_\phi K$.

By definition of semidirect product, we have the following:

Theorem 5.2. *Suppose G is a group with a normal subgroup H and another subgroup K with $H \cap K = 1$ such that $HK = G$. Let $\phi : K \to \mathrm{Aut}(H)$ be the homomorphism sending k to conjugation by k. Then, $G \cong H \rtimes_\phi K$.*

Note that semidirect products are *rarely* abelian, even if H and K are themselves abelian: $(h_1, k_1)\cdot(h_2, k_2) = (h_1\phi_{k_1}(h_2), k_1k_2)$ is typically not the same as $(h_2, k_2)\cdot(h_1, k_1) = (h_2\phi_{k_2}(h_1), k_2k_1)$ because there is no reason that $\phi_{k_1}(h_2) = \phi_{k_2}(h_1)$.

Let us do some examples!

Example 5.3. Suppose $|G| = 10$. What are the possible groups of order 10?

By the Sylow Theorems, because $10 = 5 \cdot 2$, and $5 > 2$, the Sylow 5-subgroup $H \cong \mathbb{Z}_5$ is normal. There exists a 2-Sylow subgroup $K \cong \mathbb{Z}_2$ which is not necessarily normal.

To classify all possible groups of order 10, we just need to understand the possible homomorphisms $\phi : K \cong \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_5) = \mathbb{Z}_5^\times \cong \mathbb{Z}_4$. By properties of cyclic groups, there are only two possible ϕ: $1 \in K$ has order 2, so must map to an element of order dividing 2, so $\phi(1) = 0$, which is the identity, or $\phi(1) = 2$.

*Note: in certain cases, like this one, we actually **know** the automorphisms given by ϕ. If the automorphism is the identity, then it is the function that **does nothing**, so the semidirect product is just the usual direct production. But in this case, we actually even know what the other automorphism is. For instance, H is abelian, and for any abelian group, there is an automorphism of order 2 given by $g \mapsto g^{-1}$. Because $\mathrm{Aut}(\mathbb{Z}_5)$ only has one element of order 2, it must actually be this inversion automorphism. We will discuss this on Monday!*

There are only two possible homomorphisms to $\mathrm{Aut}(H)$, so only two possible groups. The first is the identity, so the first semidirect product is $H \times K \cong \mathbb{Z}_5 \times \mathbb{Z}_2 \cong \mathbb{Z}_{10}$.

The second is this inversion automorphism (call it ϕ) so it says the second possible semidirect product is $G = \mathbb{Z}_5 \rtimes_\phi \mathbb{Z}_2$. W

On Monday, we will show that we have seeen this group before! As a preview: write $r = (1, 0) \in G$ and write $s = (0, 1) \in G$. Then, we certainly have the elements $1, r, r^2, r^3, r^4$ and s, rs, r^2s, r^3s, r^4s in G, but we can say more! We know $r^5 = 1$ and $s^2 = 1$, and let us compute sr:

$$sr = (0, 1) \cdot (1, 0) = (0 + \phi_1(1), 1 + 0) = (4, 1)$$

(remember, $\phi_1(1)$ is the inverse of 1, which is 4 in $\mathbb{Z}_5$). Because

$$r^4 s = (4,0)\cdot(0,1) = (4+\phi_1(0), 0+1) = (4,1)$$

We see that $sr = r^4 s$, so this is exactly the dihedral group D_{10}! In fact, this is true in much more generality that $D_{2n} \cong \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2$ where $\phi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ is the function assigning 1 to inversion!

The punchline: there are only two groups of order 10, either $\mathbb{Z}_{10}$ or D_{10}.

We will do more examples next time, but in summary: combining our knowledge of the Sylow theorems, group actions, and automorphisms with this new tool of semidirect products, we can effectively classify finite groups (at least of small order).