OCTOBER 24 NOTES

1. Some review and other examples

Today, we did several examples of problems related to the Sylow theorems and semi-direct products.

Here is a review of the relevant definitions/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 $n_p \mid m$.

Definition 1.3. 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 $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \phi_{k_1}(h_2), k_1 k_2)$.

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

Notation. As in the definition, we will use the following notation: for $\phi : K \to \mathrm{Aut}(H)$ and $k \in K$, each $\phi(k)$ is an automorphism of H, i.e. $\phi(k)$ is a function $\phi(k) : H \to H$. So, we can plug in values of h to $\phi(k)$: $\phi(k)(h)$ is the function $\phi(k)$ evaluated at $h \in H$. Instead of writing $\phi(k)(h)$, we will write $\phi_k(h)$.

We use semidirect products as follows:

Theorem 1.4. *Suppose G is a group with a normal subgroup H and another subgroup K with $H \cap K = 1$ such that $HK = G$. Then, $G \cong H \rtimes_\phi K$ for some homomorphism $\phi : K \to \mathrm{Aut}(H)$.*

A few remarks before we use this:

- If $\phi : K \to \mathrm{Aut}(H)$ is the trivial homomorphism, meaning $\phi(k)$ is the identity in $\mathrm{Aut}(H)$ for all $k \in K$, then $\phi_k(h)$ is the identity function. In other words, $\phi_k(h) = h$. So, the semidirect product has binary operation $(h_1, k_1)(h_2, k_2) = (h_1 \phi_{k_1}(h_2), k_1 k_2) = (h_1 h_2, k_1 k_2)$. **This is just the usual direct product**. In other words, if $\phi : K \to \mathrm{Aut}(H)$ is trivial, then $H \rtimes_\phi K = H \times K$.
- We will need to know something about $\mathrm{Aut}(H)$ for various groups H. Often, these will be Sylow p-subgroups of the form $H = \mathbb{Z}_p$. On your homework, you computed $\mathrm{Aut}(\mathbb{Z}_n)$, which we recall here: every $f \in \mathrm{Aut}(\mathbb{Z}_n)$ is of the form $f(x) = ax \pmod{n}$ for some $a \in \mathbb{Z}_n^\times$, where $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid (a,n) = 1\}$ (which is a group under multiplication). In fact, you showed that $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$.
- If $\phi : K \to \mathrm{Aut}(H)$ is a homomorphism, then $\mathrm{ord}(\phi(k))$ must divide $\mathrm{ord}(k)$. This helps us to understand exactly what possiblities we have for ϕ.

- We can often use the explicit understanding of automorphism groups to write down generators and relations for semidirect products. Let's seem some examples!

Example 1.5. 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 $\phi : K \cong \mathbb{Z}_2 \to \text{Aut}(\mathbb{Z}_5) = \mathbb{Z}_5^\times = \{1, 2, 3, 4\}$. We have two elements in $\mathbb{Z}_2$, 0 and 1. Because ϕ is a homomorphism $\phi(0)$ must be the identity in $\text{Aut}(\mathbb{Z}_5)$, i.e. $\phi_0(x) = x$. We have a few choices for $\phi(1)$: because, in $\mathbb{Z}_2$, $\text{ord}(1) = 2$, we know $\phi(1)$ has order dividing 2, so $\text{ord}(\phi(1))$ is either 1 or 2. Using the description of $\text{Aut}(\mathbb{Z}_5) = \mathbb{Z}_5^\times = \{1, 2, 3, 4\}$, the orders of these elements (remember: binary operation is multiplication mod 5) are $1, 4, 4$, and 2. So, $\phi(1)$ can either be the automorphism corresponding to 1, the identity, $\phi_1(x) = x$, or the automorphism corresponding to 4, so $\phi_1(x) = 4x$.

There are only two possible homomorphisms to $\text{Aut}(H)$, so only two possible groups. The first is the trivial homomorphism, sending everything to 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 the homomorphism where $\phi_0(x) = x$ and $\phi_1(x) = 4x$. We have actually seen this group before! 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, $\phi_1(1) = 4(1) = 4$ 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 $\phi : \mathbb{Z}_2 \to \text{Aut}(\mathbb{Z}_n)$ is the function assigning 1 to $\phi_1(x) = (n - 1)x$!

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

A few other things from class:

Example 1.6. Classify groups of order 15. (We already know this, but let's see what the Sylow theorems in this way say.)

As above, the Sylow 5-subgroup $H \cong \mathbb{Z}_5$ must be normal. Let $K \cong \mathbb{Z}_3$ be the Sylow 3-subgroup.

We know $G \cong H \rtimes_\phi K$ where ϕ is some homomorphism $\phi : K \to \text{Aut}(H)$. So, $\phi : \mathbb{Z}_3 \to \text{Aut}(\mathbb{Z}_5) = \mathbb{Z}_5^\times$. As above, $\phi(1)$ must be an element of order dividing 3, so $\text{ord}(\phi(1))$ is 1 or 3. BUT, no elements of $\text{Aut}(\mathbb{Z}_5)$ have order 3, so we must have $\phi(1)$ is the identity (the only element of order 1). Similarly, $\phi(2)$ is the identity. So, ϕ must in fact be the trivial homomorphism, and hence $G \cong H \times K = \mathbb{Z}_5 \times \mathbb{Z}_3$.

Example 1.7. (Old qualifying problem.) Show that there are at least two non-isomorphic, non-abelian groups of order $147 = 3 \cdot 7^3$.

(Possibly useful facts: $18^3 = 1 \pmod{49}$ and $2^3 = 1 \pmod 7$.)

We construct these using semidirect products and the Sylow Theorems. Suppose $|G| = 147$. By the Sylow theorems, the Sylow 7-subgroup is normal: $n_7 = 1 \pmod 7$ and $n_7 \mid 3$, so $n_7 = 1$. The Sylow 3-subgroup may or may not be normal: $n_3 = 1 \pmod 3$ and $n_3 \pmod 4 9$, so n_3 could be $1, 7$, or 49.

The Sylow 7-subgroup H has 49 elements, so by the classification of groups of order p^2, $H = \mathbb{Z}_{49}$ or $H = \mathbb{Z}_7 \times \mathbb{Z}_7$. In each case, we will write $G = H \rtimes K$ so will find two non-isomorphic groups (because their Sylow subgroups are not the same).

In both cases, let K be a Sylow 3-subgroup. Because $|K| = 3$, $K = \mathbb{Z}_3$. If $H = \mathbb{Z}_{49}$, we can construct a semidirect product $H \rtimes_\phi K$. Let $\phi : K = \mathbb{Z}_3 \to \mathrm{Aut}(H) = \mathbb{Z}_{49}^\times$ be the map sending 1 to the automorphism $\phi_1(x) = 18x \pmod{49}$. This is a non-trivial homomorphism (we are using that the order of 18 in $\mathbb{Z}_{49}$ is 3 by the possibly useful fact). Then, $G_1 = H \rtimes_\phi K$ is a group of order 147 with a Sylow 7-subgroup isomorphic to $\mathbb{Z}_{49}$. It is also non-abelian: $(1,0) \cdot (0,1) = (1,1)$ but $(0,1) \cdot (1,0) = (0 + \phi_1(1), 1 + 0)$, but ϕ_1 is the automorphism corresponding to 18 in $\mathrm{Aut}(H)$, i.e. $\phi_1 : \mathbb{Z}_{49} \to \mathbb{Z}_{49}$ is the map $\phi_1(x) = 18x$. So, $(0,1) \cdot (1,0) = (0 + \phi_1(1), 1 + 0) = (18, 1)$.

Similarly, if $H = \mathbb{Z}_7 \times \mathbb{Z}_7$, there is an automorphism of order 3 given by $(a, b) \mapsto (2a, b)$. Let $\phi : K \to \mathrm{Aut}(H)$ be the map sending $1 \in \mathbb{Z}_3 = K$ to this automorphism. Then, $G_2 = H \rtimes_\phi K$ is a group of order 147 with a Sylow 7-subgroup isomorphic to $\mathbb{Z}_7 \times \mathbb{Z}_7$, so $G_2 \ncong G_1$, and G_2 is non-abelian by similar reasoning as that above.

(There are several other non-abelian groups one could list here.)