OCTOBER 17 NOTES

1. 4.4: Automorphisms

.

Definition 1.1. Let G be an group. An isomorphism $\phi : G \to G$ is called an **automorphism** of G. The set of all automorphisms of G forms a group under composition and is denoted $\text{Aut}(G)$.

Proposition 1.2. *If $H \lhd G$, then G acts by conjugation on H as automorphisms of H. Specifically, $g \in G$ acts on H by $h \mapsto ghg^{-1}$, and this is an automorphism of H because H is normal.*

Corollary 1.3. The permutation representation of this action gives a homomorphism $\phi : G \to \text{Aut}(H)$. The kernel is, by definition, $C_G(H)$, so by the First Isomorphism Theorem, $G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Corollary 1.4. For any $H \le G$, $H \lhd N_G(H)$, so $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, for any group G, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.

Definition 1.5. If G is a group and $g \in G$, conjugation by g is called an **inner automorphism** of G. The subgroup of all inner automorphisms in $\text{Aut}(G)$ is denoted by $\text{Inn}(G)$.

By the previous corollary, $\text{Inn}(G) \cong G/Z(G)$.

Let us use these abstract ideas to classify groups.

Proposition 1.6. *The automorphism group of $\mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_n^\times$, an abelian group of order $\phi(n)$. If n is prime, this is an abelian group of order $n-1$.*

Proof. Recall that $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$ and the binary operation is multiplication mod n.

Exercise: if $\phi \in \text{Aut}(\mathbb{Z}_n)$, then $\phi(x) = ax \mod n$ for some $a \in \mathbb{Z}_n$. (This is in fact true for any *homomorphism* $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$!)

If ϕ is an automorphism, then x and ax must have the same order, so we must have that $\text{ord}(x) = \text{ord}(ax) = \text{ord}(x)/(a, n)$, so we must have $(a, n) = 1$, i.e. $a \in \mathbb{Z}_n^\times$.

This gives a homomorphism $\text{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^\times$ by $a \mapsto a$ which one can check is an isomorphism. □

Now, a result on arbitrary groups!

Proposition 1.7. *If $|G| = pq$ where p, q are primes with $p \le q$ such that $p \nmid q - 1$, then G is abelian.*

Proof. First, suppose $Z(G) \ne \{1\}$. Then, $G/Z(G)$ has order $1, p$, or q, so must be cyclic which implies that G is abelian.

Now suppose $Z(G) = \{1\}$. If every non-identity element has order p, then the centralizer of each non-identity element has index q, so by the class equation, $pq = 1 + kq$ for some $k \in \mathbb{Z}$, but this is impossible since $q \nmid 1$. So, G contains an element x of order q. Let $H = \langle x \rangle$. Because $[G : H] = pq/q = p$ and p is the smallest prime dividing $|G|$, H is a normal subgroup of G. Since $H \le C_G(H) \le G$, we must have $|C_G(H)| = q$ or pq. It cannot be pq because then $C_G(H) = G$ so every element of H would commute with every element of G, which would imply $H \le Z(G) = \{1\}$, impossible. Therefore, $|C_G(H)| = q$ so $C_G(H) = H$. And, $N_G(H) = G$ because H is normal, so $N_G(H)/C_G(H) = G/H$ is a group of order p isomorphic to a subgroup of $\text{Aut}(H)$. But, H is cyclic of order q, so $\text{Aut}(H)$ has order $q - 1$! Because p does not divide $q - 1$, which is a contradiction. So, $Z(G) \ne \{1\}$. □

On your homework, you will prove that G in the previous proposition must actually be cyclic.

2. 4.5: The Sylow Theorems

Now, we will generalize the previous result to groups of small order!

Definition 2.1. 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 2.2. *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 $n_p \mid m$.

Note the following observation:

Corollary 2.3. If P is a Sylow p-subgroup of a group G, then $n_p = 1$ if and only if P is normal in G.

We will primarily use this result to classify groups in the next chapter. We will primarily use it to produce *normal* subgroups of groups; we'll see an example first.

Example 2.4. If $|G| = pq$ with $p < q$ (p, q prime), then the Sylow-q-subgroup is normal.

By the Sylow Theorem, because $|G| = q^1(p)$, $n_q = 1 \mod q$ and n_q divides p, but $p < q$ so we must have $n_q = 1$. Therefore, there is only one subgroup Q of order q. Because $|gQg^{-1}| = |Q|$ for any g, we must have that $gQg^{-1} = Q$ so Q is normal.

Knowing this, we could try to classify G by starting with $Q \cong \mathbb{Z}_p$ and classifying G/Q (in this case, G/Q has order p, so $G/Q \cong \mathbb{Z}_p$). We then could try to 'combine' Q and G/Q to get G.

Let us consider n_p. Since n_p must divide q, then we must have $n_p = 1$ or q. Also, $n_p = 1 \mod p$, so if $q \neq 1 \pmod p$ (or $p \nmid q-1$), we must have $n_p = 1$. In this case, $P \lhd G$. Let $P = \langle x \rangle$ and $Q = \langle y \rangle$. In the case $P \lhd G$, then $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P) = \mathrm{Aut}(\mathbb{Z}_p)$, and $|\mathrm{Aut}(\mathbb{Z}_p)| = p-1$, so $pq/|C_G(P)|$ divides $p-1$. This is possible if and only if $|C_G(P)| = pq$ or $C_G(P) = G$. Therefore, every element of G commutes with x, so $x \in Z(G)$ and x and y commute. Therefore, $\mathrm{ord}(xy) = pq$ (exercise!) so we must have $G = \langle xy \rangle \cong \mathbb{Z}_{pq}$ and in fact we will see later that $P \times Q \cong G$ by the isomorphism $(x^n y^n) \mapsto (x^{n \pmod p}, y^{n \pmod q})$.

What if $P \not\lhd G$? We will still be able to use the Sylow Theorems to show that $G \cong P \rtimes Q$ where $\rtimes$ will denote a semidirect product.

Now the proof! We only proved part (1) in class.

Proof. For (1), We use induction on $|G|$, with the result clear if $|G| = 1$. Assume now that Sylow p-subgroups exist for all groups of order less than $|G|$.

If $p \mid |Z(G)|$, then because $Z(G)$ is abelian, it has a subgroup N of order p. Then, $|G/N| = p^{k-1}m$ and G/N has a subgroup P/N of order p^{k-1}. By the fourth isomorphism theorem, P is a subgroup of G of order $|P| = |P/N||N| = p^k$, so a Sylow p-subgroup exists.

Now, suppose $p \nmid |Z(G)|$. From the class equation, we must have $p \nmid [G : C_G(g_i)]$ for some g_i. Let $H = C_G(g_i)$, so $|H| = p^k l$ where $p \nmid l$ and $g_i \notin Z(G)$ so $H < G$. By induction, H has a Sylow p-subgroup P, which is also a subgroup of G, so G has a Sylow p-subgroup.

Now we have shown that a p-subgroup exists. Let $\mathcal{S} = \{P_1, P_2, \ldots, P_r\}$ be the set of all conjugates of P, so $\mathcal{S} = \{gPg^{-1} \mid g \in G\}$. Let Q be any p-subgroup. By definition, Q acts on $\mathcal{S}$ by conjugation.

Write $\mathcal{S} = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_s$ as a union of orbits of this action. Note that $r = \sum |\mathcal{O}_i|$. We may assume, by renumbering, that $P_i \in \mathcal{O}_i$, for $1 \leq i \leq s$. From a previous proposition, $|\mathcal{O}_i| = [Q : N_Q(P_i)]$ and by definition, $N_Q(P_i) = N_G(P_i) \cap Q = P_i \cap Q$ by the following lemma. Therefore, $|\mathcal{O}_i| = [Q : P_i \cap Q]$.

This previous paragraph holds for any subgroup Q, so let $Q = P_1$. Then, $|\mathcal{O}_1| = 1$, and $P_i \neq P_1$ for $i > 1$, so $P_1 \cap P_i < P_1$, and $|\mathcal{O}_i| = [P_1 : P_1 \cap P_i] > 1$, but P_1 is a p-group, so $p \mid |\mathcal{O}_i|$ for each $2 \leq i \leq s$. Therefore, $r = \sum |\mathcal{O}_i| = 1 + kp = 1 \pmod p$.

Finally, we prove parts (2) and (3) of the theorem. Let Q be any p-subgroup. If Q is not contained in any P_i (i.e. $Q \not\leq gPg^{-1}$), then $Q \cap P_i < Q$ for all i, so considering the action of Q, we have $|\mathcal{O}_i| = [Q : P_i \cap Q] > 1$ so must have $p \mid |\mathcal{O}_i|$ for each i, a contradiction to $r = 1 \pmod p$. This proves (2).

For (3), let Q be any Sylow p-subgroup. We know $Q \leq gPg^{-1}$ for some g by (2), but these groups must have the same size, so we must have $Q = gPg^{-1}$ is conjugate to P. and therefore every Sylow p-subgroup is one of the P_i, so the number of such subgroups is $n_p = r = 1 \pmod p$. □

In the proof, we needed to use the following Lemma.

Lemma 2.5. *If $P \in Syl_p(G)$ and Q is any p-subgroup, then $Q \cap N_G(P) = Q \cap P$.*

Proof. Since $P \leq N_G(P)$, it is clear that $Q \cap P \leq Q \cap N_G(P)$, so we just need to show the reverse inclusion.

Let $H = N_G(P) \cap Q$. Since $H \leq Q$ by definition, we just need to show $H \leq P$. We will show this by proving that PH is a p-subgroup of G. Then, $P \leq PH$ by definition, by P was a p-subgroup of largest possible order, so $P = PH$. And, $H \leq PH$ by definition, so $H \leq P$, as desired.

Now we show that PH is a p-subgroup. Because $H \leq N_G(P)$, PH is a subgroup. We also know its order: $|PH| = |P||H|/|P \cap H|$, and all of these numbers are powers of p, so $|PH|$ is a p-group. □