Homework 8

Due Friday, April 10th

Theorem 1 (Cauchy's Theorem)**.** *Let G be a group of order n, and p a prime number dividing n. Then G has an element of order p.*

Remark. *In the next exercise deduce Cauchy's theorem from Sylow's theorem. One may worry that we used Cauchy's theorem to prove Sylow's theorem, and that therefore our logic here is circular. But notice that we used Cauchy's theorem on the center $Z(G)$ in the proof of Sylow's theorem, which is an abelian subgroup of G. Since we have already proved Cauchy's theorem for abelian groups, there is no issue.*

1. Let G be a group of order n, and let p be a prime dividing n.

   (a) Use Sylow's theorem to show that there is some $x \in G$ with $|x| = p^i$ for some i.

   Proof. Let $n = p^\alpha m$ with p^α the maximal p divisorm and note that since p divides n we know $\alpha \geq 1$. Then by Sylow's theorem there is a nontrivial Sylow p-subgroup $P \leq G$ with $|P| = p^\alpha$. Fix any $x \in P$ not equal to 1. Then by Lagrange's theorem $|x|$ divides p^α, so that $|x|$ must be a power p. Since x is also in G, we are done. □

   (b) Raise x from part (a) to an appropriate power to produce $y \in G$ with $|y| = p$.

   Proof. From part (a) we have $x \in G$ of order p^i. Let $y = x^{p^{i-1}}$. Then we claim $|y| = p$. Indeed:

   $$y^p = (x^{p^{i-1}})^p = x^{p^i} = 1,$$

   and for $j < p$,

   $$y^j = (x^{p^{i-1}})^j = x^{jp^{i-1}} \neq 1,$$

   because $jp^{i-1} < p^i$. □

2. Show that a group G of order 200 has a normal Sylow 5-subgroup. Conclude that G is not simple.

   Proof. $200 = 25 * 8 = 5^2 * 8$. By Sylow's theorem, the number of Sylow 5 subgroups is one more than a multiple of 5:

   $$n_5 = 1 + 5 * k \in \{1, 6, 11, 16, \cdots\}.$$

   But we also by Sylow's theorem, n_5 must divide 8. The only number in that list dividing 8 is 1, so $n_5 = 1$. Thus there is a unique Sylow 5-subgroup P. Since any conjugate of P is also a Sylow 5-subgroup, we conclude that $gPg^{-1} = P$ for all $g \in G$, so that $P \trianglelefteq G$. Since $|P| = 25$, we have produced a nontrivial normal sbgroup, so that G cannot be simple. □

3. Show that for $n \geq 3$ we have $Z(S_n) = 1$. (Hint: what is the conjugacy class of an element in the center of a group? What is the conjugacy class of an element in S_n?).

Proof. First note that for any group G, if $g \in Z(G)$, then $hgh^{-1} = g$ for all $h \in G$ (since the h and g commute). Therefore the conjugacy class of g is just the set $\{g\}$.

Recall that two permutations are conjugate in S_n if and only if they have the same cycle type−or what we called *shape* in class (this is Dummit and Foote Proposition 4.11). Now suppose $\sigma \in S_n$ for some $n \geq 2$, and $\sigma \neq 1$. We will show that σ. Write the cycle decomposition of σ as

$$\sigma = (a_1 \;\; a_2 \;\; \cdots \;\; a_t)(b_1 \;\; b_2 \;\; \cdots)\cdots$$

First suppose that some $i \in \{1, \cdots, n\}$ does not appear in the cycle decomposition of σ. Then let

$$\sigma' = (i \;\; a_2 \;\; \cdots \;\; a_t)(b_1 \;\; b_2 \;\; \cdots)\cdots$$

Then certainly $\sigma \neq \sigma'$ (indeed, the former fixes i while the latter does not), but they are conjugate since they have the same shape. Although it isn't necessary to the proof, we can in fact explicitely show that σ' is a conjugate of σ. Indeed if τ is the transposition $(a_1 \;\; i)$ then $\sigma' = \tau\sigma\tau^{-1}$.

We may now assume every integer from 1 to n appears in the cycle decomposition. First assume that σ is not a n-cycle. Then let

$$\sigma'' = (b_1 \;\; a_2 \;\; \cdots \;\; a_t)(a_1 \;\; b_2 \;\; \cdots)\cdots$$

is a different permutation with the same shape, and therefore a conjugate of σ. As above we can explicitely show this as well, noting that if $\tilde{\tau} = (a_1 \;\; b_1)$ then $\sigma'' = \tilde{\tau}\sigma\tilde{\tau}^{-1}$.

Finally we must settle the case where $\sigma = (a_1, \;\; \cdots \;\; a_n)$ is an n cycle. Then $|\sigma| = n$ so that $\sigma^2 \neq \sigma$ is another n-cycle. Again noticing that all n-cycles have the same shape, we see that σ^2 is a conjugate of σ.

In each case we see that the conjugacy class of σ is nontrivial, so that σ cannot be in $Z(S_n)$, so that $Z(S_n) = 1$ □

4. (a) Let $x, y \in G$ be two elements of finite order and suppose that $xy = yx$. Conclude that $|xy|$ divides the least common multiple of $|x|$ and $|y|$.

   Proof. Let l be the least common multiple of $|x|$ and $|y|$. Then $x^l = y^l = 1$, so that $(xy)^l = x^l y^l = 1$ Therefore $|xy|$ divides l. □

   (b) Let G be an abelian group of order pq for primes $p < q$. Use Cauchy's theorem and part (a) to conclude that G is cyclic. (This completes the argument from class about groups of order pq).

   Proof. By Cauchy's theorem, we can find $x, y \in G$ with $|x| = p$ and $|y| = q$. Since x and y commute, then applying part (a) we know that $|xy|$ divides pq, so it is one of $1, p, q, pq$. If it is 1 then $y = x^{-1}$ contradiction that their orders are not the same. If it is p then $(xy)^p = y^p = 1$ so that q divides p, which it does not. We can similarly rule out q. Thus $|xy| = pq$ so that $G = \langle xy \rangle$. □

5. Recall that an abelian group V of order p^n is called an *elementary abelian group of order* p^n if every $x \in V$ has order $\leq p$. Show by induction on n that

$$V \cong \underbrace{Z_p \times Z_p \times \cdots \times Z_p}_{n \text{ times}}$$

Proof. We proceed by induction on n. The base case where $n = 1$ then V has prime order so it must be cyclic of order p. For the general case, $1 \neq x \in V$. Then $|x| = p$ and $\langle x \rangle \leq V$ is normal since V is abelian. Then $V' = V/\langle x \rangle$ is an elementary abelian group of order p^{n-1}. Therefore by induction:

$$V' \cong \underbrace{Z_p \times Z_p \times \cdots \times Z_p}_{n-1 \text{ times}}$$

Let $e_i = (1, \cdots, 1, g, 1, \cdots, 1)$ be the generator of the ith factor of V' (that is $g \in Z_p$ is a generator placed in the ith position of the tuple). Notice that the e_i form a set of generators for V'. Let $\pi : V \to V'$ be the natural projection, and for each $i = 1, \cdots, n-1$ fix some element of the fiber $y_i \in \pi^{-1}(e_i)$. We now define an isomorphism:

$$\varphi : \underbrace{Z_p \times Z_p \times \cdots \times Z_p}_{n \text{ times}} \to V$$

according to the rule: $\varphi(e_i) = y_i$ for $i \leq n-1$, and $\varphi(e_n) = x$ (since the e_i generate the left hand side, this defines a homomorphism). We now show φ is injective and surjective.

To observe surjectivity, fix some $v \in V$. Then

$$\pi(v) = (g^{r_1}, \cdots, g^{r_{n-1}}).$$

Thus $v \cdot y_1^{-r_1} \ldots y_{n-1}^{-r_{n-1}} \in \ker \pi$, so it is equal to a power of x, say x^{r_n}. In particular:

$$v = y_1^{r_1} \cdots y_{n-1}^{r_{n-1}} \cdot x^{r_n} = \varphi(g^{r_1}, \cdots, g^{r_n}).$$

Since the two groups have the same order, injectivity follows immediatley and we are done. □

6. Write all the conjugacy classes for Q_8, and use this to verify that the class equation holds for Q_8.

Proof. Since $1, -1 \in Z(Q_8)$, their conjugacy classes are $\{1\}$ and $\{-1\}$ respectively. Next we compute the conjugacy class of i. We can do this directy by conjugating it with every other element, but it is more efficient to use the orbit stabilizer theorem to notice that:

$$|Q_8 * i| = |Q_8 : (Q_8)_i| = |Q_8 : C_{Q_8}(i)|$$

We certainly have that $\langle i \rangle \leq C_{Q_8}(i) \leq Q_8$, so that the centrailzer is either $\langle i \rangle$ or all of Q_8. But since $i \notin Z(Q_8)$ then the centralizer of i can't be everything, so that $C_{Q_8}(i) = \langle i \rangle$ and therefore

$$|Q_8 * i| = |Q_8|/|\langle i \rangle| = 8/4 = 2.$$

We know i is in its own conjugacy class, so we must find the one remaining member. We check that

$$jij^{-1} = ji(-j) = (-k)(-j) = kj = -i.$$

Thus the conjugacy class of i is $\{\pm i\}$. Similar reasoning says the remaining conjugacy classes are $\{\pm j\}$ and $\{\pm k\}$. Therefore the class equation becomes:

$$8 = |Q_8| = |Z(Q_8)| + |Q_8 : C_{Q_8}(i)| + |Q_8 : C_{Q_8}(j)| + |Q_8 : C_{Q_8}(k)| = 2 + 2 + 2 + 2 = 8.$$

□

7. Let G a group of order 203, and suppose that it has a normal subgroup H of order 7. Show that $H \leq Z(G)$, and conclude that G is abelian. (Hint: This should essentially follow the same argument for groups of order 45 with a normal subgroup of order 9).

Proof. We begin by facoring $203 = 7 \cdot 29$. Since 7 divides 28 it is not immediate from previous calculations that G is abelian. Nevertheless, H is a Sylow 7 subgroup of G, and is normal. We did show in class that if $|G| = pq$ with $p < q$ and there is a normal Sylow p-subgroup, then G is abelian. Nevertheless, the goal was to go through the proof directly in this example, so let's do it.

Since $H \trianglelefteq G$, we know that G acts on H via conjugation. The permutation representation induces a homomorphism $G \to \mathrm{Aut}(H)$ whose kernel is $C_G(H)$. In particular, applying the first isomorphism theorem $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. But H is isomorphic to the cyclic group of order 7, and so its automorphism group is isomorphic to the multiplicative group of $\mathbb{Z}/7\mathbb{Z}$. We summarize in the following diagram.

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & \mathrm{Aut}(H) \arrow[r, "\sim"] & (\mathbb{Z}/7\mathbb{Z})^{\times} \\
G/C_G(H) \arrow[ur, hook] & & .
\end{tikzcd}$$

By Lagrange's theorem, $|G/C_G(H)|$ must divide $|G| = 203$, and also must divide $|Aut(H)| = 6$. The only factor these two numbers share is 1, so that $G/C_G(H)$ is the trivial group, or equivalently $G = C_G(H)$. This is precisely that $H \leq Z(G)$. This implies that $|G/Z(G)|$ must divide 29, which is prime. In particular $G/Z(G)$ is cyclic, so that by HW 6 problem 5(b), we conclude that G is abelian. □