Takehome Assignment 2 Solutions

In this assignment, we complete the proof of Sylow's Theorems. Let's recall the relevant definitions and statements.

Definition 1. *Let p be a prime number. A group H is called a **p-group** if $|H| = p^r$ for some r. If G is a group and $H \leq G$ is a subgroup which is a p-group, we call it a **p-subgroup** of G.*

Definition 2. *Let G be a finite group of order $|G| = p^\alpha m$ for p a prime not dividing m. A subgroup $P \leq G$ of order p^α is called a **Sylow p-subgroup** of G. The collection of all Sylow p-subgroups of G is denoted $Syl_p(G)$ and the number of Sylow p-subgroups is often denoted $n_p = \#Syl_p(G)$.*

Theorem 3 (Sylow's Theorems)**.** *Adopt the notation from Definition 2.*

- ***(Sylow 1)*** *There exists a Sylow p-subgroup of G.*
- ***(Sylow 2)*** *Let $P \in Syl_p(G)$ and let $Q \leq G$ any p-subgroup of G. Then there exists some $g \in G$ with $gQg^{-1} \leq P$.*
- ***(Sylow 3)*** *Let $P \in Syl_p(G)$.*
  (a) $n_p \equiv 1 \mod p$.
  (b) $n_p = [G : N_G(P)]$. *In particular $n_p | m$.*

We already proved **(Sylow 1)** in class, **(Sylow 2)** and **(Sylow 3)** remain. As is often the case, group actions will be a useful tool! To help us along the way, we introduce one more definition.

Definition 4. *Let G be a group acting on a set A. The fixed points of the action are:*

$$A^G = \{a \in A : g \cdot a = a \text{ for all } g \in G\}.$$

1. Let's establish a few facts about the fixed points.

   (a) Let G be a group. Compute the fixed points of the following actions.

   i. G acting on G by left multiplication.

   Proof. There are two cases to consider here. First if $G = \{1\}$ is the trivial group. Then for any $g, a \in G$ we have $g * a = 1 * 1 = 1 = a$, so that a is fixed by g. Since everything fixes everything, $G^G = G$.

   If G is nontrivial, then we can find an element $g \neq 1$. Then for any $a \in G$, we have $g * a \neq a$ (else we could solve for $g = 1$), so that a is not fixed by g. In particular, nothing is fixed by g, and therefore nothing is fixed by all of G, so that we can conclude that $G^G = \emptyset$. □

   ii. G acting on G by conjugation.

   Proof. . The action is $g * a = gag^{-1}$, so that unwinding the definitions we see:

   $$G^G = \{a \in G : gag^{-1} = a \text{ for all } g \in G\} = Z(G).$$

   □

(b) Let G be a p-group acting on a finite set A. Show that $|A^G| \equiv |A| \mod p$. (*Hint:* One could model this off of the proof of the class equation. Use the orbit-stabilizer theorem to see what happens when reducing mod p).

Proof. We begin by collecting the orbits of the action of G on A. Call them

$$\mathcal{O}_1, \cdots, \mathcal{O}_t, \hat{\mathcal{O}}_1, \cdots, \hat{\mathcal{O}}_s,$$

where the $\mathcal{O}_i$ are the singleton orbits and the $\hat{\mathcal{O}}_j$ are the orbits with more than one element. Since the orbits partition A (TH1 Problem 1(c)), we see that

$$|A| = |\mathcal{O}_1| + \cdots + |\mathcal{O}_t| + |\hat{\mathcal{O}}_1| + \cdots + |\hat{\mathcal{O}}_s|. \tag{1}$$

Notice that $a \in A^G$ if and only if its orbit is a singleton: $G * a = \{a\}$. In particular,

$$A^G = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_t,$$

which, since orbits are disjoint, implies that:

$$|A^G| = |\mathcal{O}_1| + |\mathcal{O}_2| + \cdots + |\mathcal{O}_t| = t.$$

We can therefore substitute this into Equation (1) to obtain:

$$|A| = |A^G| + \sum_{i=1}^{s} |\hat{\mathcal{O}}_s|. \tag{2}$$

Let's consider the non-singleton orbits. If we fix some $a \in \hat{\mathcal{O}}_i$, then the orbit stabilizer theorem says that $|\hat{\mathcal{O}}_i| = |G/G_a| = n$, and by Lagrange's theorem, $n|p^r$. Since $\hat{\mathcal{O}}_i$ is not a singleton set, $n > 1$, so it must be a positive power of p, implying that $p|n$. In particular, $|\hat{\mathcal{O}}_i| \equiv 0 \mod p$, so that reducing Equation (2) mod p gives the result:

$$|A| \equiv |A^G| \mod p.$$

□

(c) Let G be a p-group acting on a nonempty set A, and suppose that p does not divide $|A|$. Show that the action of G on A has at least one fixed point.

Proof. Applying part (b) and the fact that $p \not| |A|$, we immediately see that

$$|A^G| \equiv |A| \not\equiv 0 \mod p,$$

so that in particular $|A^G| \neq 0$. □

(Sylow 2) now follows from a clever application of 1(c). All we have to do is look at the right group action!

2. Let G be as in Definition 2, and P a Sylow p-subgroup of G. Let $Q \leq G$ be a p-subgroup.

(a) Use 1(c) to deduce that the action of Q on G/P by left multiplication has a fixed point. (There are 2 cardinality conditions to apply 1(c), explain why they both hold.)

Proof. We first record that Q is a p-group by assumption. Then we notice that $|G/P| = \frac{p^\alpha m}{p^\alpha} = m$. Since $p \not| m$, we may apply 1(c) to observe that $(G/P)^Q \neq \emptyset$. □

(b) Use the fixed point of this action to show that a conjugate of Q is contained in P, thereby proving **(Sylow 2)**.

Proof. By part (a) we know that there is a fixed point of the action of Q on G/P by left multiplication, call it the coset xP. Being a fixed point implies that for every $q \in Q$, we have:

$$qxP = xP.$$

Multiplying on the left by x^{-1} gives:

$$x^{-1}qxP = P,$$

which in turn implies that $x^{-1}qx \in P$. Since $q \in Q$ we arbitrary, we may conclude that $x^{-1}Qx \subseteq P$, as desired. □

(c) Deduce that all Sylow p-subgroups of G are conjugate and isomorphic.

Proof. We start with the following general observation: if A, B are groups, $K \leq A$ a subgroup, and $\varphi : A \to B$ is an isomorphism, then $K \cong \varphi(K)$. Indeed, restricting φ to K gives a homomorphism $\varphi|_K : K \to \varphi(K)$, which is injective since it is the restriction of an injective map, and is surjective by definition. As a special case, notice that if $P \leq G$ is any subgroup and $x \in G$, then xPx^{-1} is the image of P under the 'conjugate by x' isomorphism from G to itself, so that $P \cong xPx^{-1}$.

Now let $P, Q \in Syl_p(G)$. By part (b) above, there is some $x \in G$ such that $xQx^{-1} \subseteq P$. But we also know that $Q \cong xQx^{-1}$ so that $|xQx^{-1}| = |Q| = |P|$, and therefore $xQx^{-1} = P$, and so P and Q are conjugate, and therefore also isomorphic by the previous paragraph. □

The two parts of **(Sylow 3)** follow from the orbit-stabilizer theorem and clever application of 1(b), keeping careful track of the numerics!

3. Let G be as in Definition 2, and P a Sylow p-subgroup of G.

(a) Show that G acts on the set $Syl_p(G)$ by conjugation. What is the stabilizer of P?

Proof. For any $g \in G$ and $P \in Syl_p(G)$ we know by 2(c) that $g * P = gPg^{-1} \in Syl_p(G)$, so that acting by conjugation gives a well defined function $G \times Syl_p(G) \to Syl_p(G)$. Furthermore, one can check that:

$$1 * P = 1P1^{-1} = P,$$

and

$$g * (h * P) = g * (hPh^{-1}) = ghPh^{-1}g^{-1} = (gh)P(gh)^{-1} = (gh) * P,$$

so that it is in fact a group action. To compute the stabilizer of $P \in Syl_p(G)$ we observe that by definition

$$G_P = \{g \in G : gPg^{-1} = P\} = N_G(P).$$

□

(b) Use the orbit-stabilizer theorem of the action from part (a) to prove **(Sylow 3)(b)**. (You can use 2(c) to compute the orbit $G * P$).

Proof. By 2(c), the Sylow p-subgroups of G are precisely the conjugates of P, that is $G * P = Syl_p(G)$. Therefore, applying the orbit stabilizer theorem and part (a), we compute:

$$n_p = |Syl_p(G)| = |G * P| = [G : G_P] = [G : N_G(P)].$$

□

(c) Restrict the action from part (a) to an action of P on $Syl_p(G)$. Show that the action of P on $Syl_p(G)$ has a single fixed point: P itself!

Proof. Notice that (by HW6 Problem 1(a)), $P \leq N_G(P)$. Therefore for any $p \in P$, we have $pPp^{-1} = P$, so that $P \in (Syl_P(G))^P$. Fix any other $Q \in (Syl_p(G))^P$. We'd like to show that $Q = P$. Since $pQp^{-1} = Q$ for every $p \in P$, we have that $P \leq N_G(Q)$. And we also have (as above) that $Q \leq N_G(Q)$. In particular, P and Q are both Sylow p subgroups of $N_G(Q)$, and are therefore (by 2(c)) conjugate in $N_G(Q)$. That is, there is some $x \in N_G(Q)$ such that:

$$P = xQx^{-1} = Q,$$

where the last equality comes from the fact that $x \in N_G(Q)$. □

(d) Deduce **(Sylow 3)(a)** from 1(b) and 3(c).

Proof. Since P is a p-group, we may apply 1(b) to compute:

$$n_p = |Syl_p(G)| \equiv |\,(Syl_p(G))^P\,| \mod p.$$

But by 3(c) we know that $|\,(Syl_p(G))^P\,| = 1$, completing the proof. □

Good job! You did it! We will explore many consequences of these results in the coming week!