1 Sylows Theorem

1.1 Group Axioms

Definition 1.1.1: Group axioms

Let $G = (G, *)$ be a group where G is a set and $*$ the group operation. Then, the following are true:

1. There exists an identity element $1_G \in G$ such that $g * 1_G = 1_G * g = g$ for all $g \in G$.
2. Every element $g \in G$ has an inverse $g^{-1} \in G$ such that $g * g^{-1} = 1_G$
3. The product elements in G is associative such that for $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
4. The product of two elements in G is commutative if and only if the group is abelian. (Ie. if a group G is abelian then $g * q = q * g$ for all $g, q \in G$)

1.2 Group Actions, Orbits, and Stabilizers

Definition 1.2.1: Group Actions

Let G be a group. A set S is a G-set if there is a function from $G \times S \to S$ (which we write as $g \cdot s$ for $g \in G$ and $s \in S$) satisfying:

1. $(gh) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$ and $s \in$, and
2. $1 \cdot s = s$ for all $s \in S$

Definition 1.2.2: Orbits

Let G be a group and S be a set such that there exists a group action $\sigma : G \times S \to S$. The **orbit** of an element $s \in S$ is the set of all points s can be moved to:

$$\text{Orb}(s) = \{g \cdot x \mid g \in G\}$$

Definition 1.2.3: Stabilizers

Let G be a gruop and S be a set such that there exists a group action $\sigma : G \times S \to S$. The **stabilizer** of an element $s \in S$ is the *subgroup* that s fixed:

$$\text{Stab}(g) = \{g \in G \mid g \cdot s = s\}$$

Now with these two established we have

Theorem 1.1 (Orbit-Stabilizer)**.** *Let G be a finite group, S be any set that G acts on. Then for any $s \in S$,*

$$|G| = |Orb(s)| \cdot |Stab(s)|$$

The proof of this theorem is omitted for sake of the project.

1.3 Proof of Sylows Theorem

Lemma 1.2 (Lucas's Lemma)**.** *Let p and m be integers such that p is prime and* $\gcd(p, m) = 1$. *Then*

$$\binom{p^k m}{p^k} \equiv m \pmod{p}$$

Once again, the proof is omitted for the sake of the project.

Theorem 1.3 (Sylows First[1] Theorem)**.** *Given a group G of size $p^k m$ where p is a prime and* $\gcd(p, m) = 1$ *we have that G has a subgroup of size p^k.*

Proof. We start by defining a set of sub*sets* $\Omega = \{X \subseteq G \mid |X| = p^k\}$. Next, we will define a group action such that G acts on Ω by $g \cdot X = \{gx \mid x \in X\}$, noting that the map $x \mapsto gx$ is bijective and thus the size is preserved between X and $g \cdot X$.

If we take a look at the size of the set we just created, Ω, notice that by definition of Ω we are choosing subsets of size p^k from G which has size $p^k m$. So,

$$|\Omega| = \binom{p^k m}{p^k} \equiv m \pmod{p}$$

with the congruence coming from Lemma (1.2).

Now since, we can split Ω into a disjoint union of orbits, the size of Ω must be the sum of the sizes of each set in the disjoint union. Since $|\Omega| \equiv m \pmod{p}$ we know that one orbit of the action of G has a size that is **not** a multiple of p since $\gcd(p, m) = 1$. We will call this orbit O.

Now choose a set inside O, say $\alpha \in O$. Then, the orbit of α must be O itself, $G \cdot \alpha = O$ because the orbit of an element in an orbit is the orbit itself. Applying the Orbit-Stabilizer Theorem (1.1) we can see that if G_α is the stabilizer of α then,

$$|G_\alpha| \cdot |G \cdot \alpha| = p^k m.$$

However, since $p^k \nmid |G \cdot \alpha|$, we know that $p^k \mid |G_\alpha|$. We must now show that $|G_\alpha| = p^k$.

We start by considering some $a \in \alpha$ and the map $G \to G$ given by $g \mapsto ga$ for $g \in G$. This map is clearly a bijection since we are able to multiply by a^{-1}. Now if $g \in G_\alpha$ then $ga \in \alpha$ by definition of a stabilizer. However, because this map was a bijection we know that $|G_\alpha| \leq |\alpha|$ (since ga is in some subset of α). But $|\alpha| = p^k$ so $|G_\alpha| \leq p^k$ and since $p^k \mid |G_\alpha|$ we have $p^k \leq |G_\alpha|$. Therfore $|G_\alpha| = p^k$ and the stabilizer G_α is the desired group. ☐

[1] There are actually three theorems attributed to Sylow, and they're all related!