The Sylow Theorems

Daniel Rostovtsev
Date: 5 November, 2017

Subset-Stabilizer Lemma

Let U be a subset of G, and G act on $S = \{U \subseteq G\}$ by left multiplication. Then $|\text{stab}(U)|$ divides both $|U|$ and $|G|$. (from Algebra by Michael Artin)

Proof. Consider the subset $U \in S$ and its stabilizer under the group action of $G * S$, $\text{stab}(U)$. The orbit of each $g \in U$ under $\text{stab}(U)$ is equal to the right coset $\text{stab}(U)g$. Therefore:

$$|U| = \bigcup_{g \in \text{stab}(U)} \text{stab}(U)g = n|\text{stab}(U)| \text{ for some } n \in \mathbb{Z}^+ \implies |\text{stab}(U)| \text{ divides } |U|$$

Since $|G| = |\text{stab}(U)||\text{orb}(U)|$, $|\text{stab}(U)|$ divides the order of G as well. □

p^e-Subset Lemma

Let G be a group, and $|G| = n = p^e m$ such that p does not divide m. Let the set, S, be defined as the following: $S = \{U \subseteq G : |U| = p^e\}$. Then $|S|$ is not divisible by p. (from Algebra by Michael Artin)

Proof. Direct calculation of $|S|$ shows that the order of S cannot be divisible by p.

$$|S| = \binom{n}{p^e} = \frac{(n)(n-1)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots(1)}$$

For $|S|$ not to be divisible by p, all $(n-k)$ in the numerator divisible by some p^i must have a corresponding term, $(p^e - k)$, in the denominator for which p^i is also a multiple. This way, all p in the numerator cancel, proving $|S|$ cannot be divisible by p. Take a term $(n-k)$ in the numerator of N divisible by some p^i. Since $(n-k)$ is divisible by p^i, it follows that $(n-k) \mod p^i \equiv 0$. Since $n = p^e m$, it follows that $(p^e m - k) \mod p^i \equiv 0$. Thus, for $p^e m - k$ to be divisible by p^i, k must be divisible by p^i. So k can be written as $k = p^i l$. Thus $(n-k) = (p^e m + p^i l) = p^i(p^{e-i}m - l)$. There is a unique term in the denominator which also has a factor of p^i. For some $(p^e - k')$, it must follow that $(p^e - k') = (p^e - p^i l') = p^i(p^{e-i} - l')$. This concludes the proof. □

The First Sylow Theorem

Every group G (of order $n = p^e m$) has a Sylow p-subgroup (of order p^e). (from Algebra by Michael Artin)

Proof. Let S be all the subsets of G of order p^e. If a Sylow p-subgroup exists, then some element of S will be a subgroup of G. It will be shown that there always exists a stabilizer of some $U \in S$ that has order p^e, and that stabilizer is, in turn, a p-subgroup.

$$\binom{n}{p^e} = |S| = \sum_{\text{orbits } O} |O|$$

By the p^e-subset lemma, p doesn't divide S, so at least one orbit, $O = \text{orb}(U)$, must not have an order divisible by p. By the orbit stabilizer theorem, $|G| = |\text{stab}(U)||\text{orb}(U)|$. Since $|\text{orb}(U)|$ is not divisible by p, $|\text{stab}(U)| = p^e n$ where n divides m. However, $|\text{stab}(U)|$ must divide $|U| = p^e$, so $|\text{stab}(U)| = p^e$, and the existence of a Sylow p-subgroup has been proven. □

The Second Sylow Theorem

(a) Let H and K be Sylow p-groups in G,

then H and K are conjugate.

(b) Let K be a p-subgroup and H be a Sylow p-subgroup,

then $K \leq H'$ where H' is a conjugation of H.

Proof. Consider the set G/H where H is a Sylow p-subgroup. Take the group action $G * G/H$. Under this action, G/H is transitive. Since for any two cosets aH and bH in G/H, the element $ba^{-1} \in G$ takes aH to bH. There is also at least one coset whose stabilizer is equal to H, namely the identity coset eH - since $\text{stab}(eH) = H$. Since the stabilizers in the same orbit are conjugate, and there is only one orbit in G/H, all the possible stabilizers are conjugate. All stabilizers have order p^e, so some Sylow p-subgroups are conjugate to other Sylow p-subgroups, but it hasn't been shown that all Sylow p-subgroups are conjugate to all other Sylow p-subgroups.

Since H is a Sylow p-subgroup, and, by Lagrange's theorem, $(G : H) = |G|/|H| = p^e m/p^e = m$, it follows that the order of H in G must not divide p. Let K be a p-subgroup of G. Define an action of K on G/H. Since K is a p-subgroup of G and the order of H in G does not divide p, there exists an element $gH \in G/H$ such that $\text{stab}(gH) = K$ by the fixed point theorem. It then must follow that K must be a subgroup of a larger stabilizer of gH in $G * G/H$ - that $K \leq H'$ where H' is some conjugate of H. Thus, since all p-subgroups are contained in conjugates of H, all Sylow p-subgroups are conjugates of eachother. $\square$

The Third Sylow Theorem

Let s be the number of Sylow p-subgroups in G. Then s divides m, and $s \equiv 1 \mod p$.

Proof. Applying the normalizer and the orbit-stabilizer theorem will prove that s divides m and that $s \equiv 1 \mod p$.

First, to show that s divides m, consider the group action with conjugation, $G * S$ where S is the set of Sylow p-subgroups of G. By second Sylow theorem, $G * S$ must be transitive, since all Sylow p-subgroups are conjugate. Also, the stabilizer of a Sylow P subgroup is $\{g \in G : gHg^{-1} = H\}$, which, by definition, is also the normalizer of H. By the orbit stabilizer theorem:

$$
\begin{aligned}
|S| &= |\text{orb}(H)||\text{stab}(H)| \equiv \\
m &= s|N(H)| \\
&\therefore s|m
\end{aligned}
$$

Next, to show that $s \equiv 1 \mod p$, consider the group action with conjugation of $H * S$, where H is a Sylow p-subgroup. The orbit of H is equal to H, since H is closed under multiplication. Thus $|\text{orb}(H)| = 1$. To show that H is the only Sylow p-subgroup with an orbit of order of 1 in $H * S$, take the arbitrary Sylow p-subgroup H'. H' has an orbit of order 1 if and only if $\text{stab}(H') = H$, which, by definition, only happens if and only if $H \leq N(H')$. Since $H \leq N(H') \leq G$ and $H' \leq N(H') \leq G$, and $|H| = |H'| = p^e$, both H and H' are Sylow p-subgroups of $N(H')$. But all H' are normal in $N(H')$, so H must equal H', and thus H is the only Sylow p-subgroup with an orbit of order 1 in $H * S$. Since the orbits under $H * S$ partition S, $|S| = s = |\text{orb}(H)| + \sum |\text{orb}(H_i)| = 1 + \sum($ multiples of $p)$, because H is the only element to have an orbit of 1. So $s \mod p = 1$. $\square$