The Sylow Theorems

Daniel Rostovtsev
Date: January 27, 2017
*edited May 1, 2017

The First Sylow Theorem

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

Proof. Applying the orbit-stabilizer theorem:

If it is possible to show that there is an element, U, of some set, S, which G operates on, and that the orbit of U does not divide p, then, by the orbit stabilizer theorem:

$|G| = p^e m = |\text{stab}(U)||\text{orb}(U)|$ where $|\text{stab}(U)| = p^e l$ since $|\text{orb}(U)|$ is not divisible by p.

By the subset-stabilizer lemma, $|\text{stab}(U)|$ divides $|U|$ and $|G|$. So, in the above case $|\text{stab}(U)|$ divides p^e and $p^e m$. Thus $|\text{stab}(U)| = p^e$. Also, since $\text{stab}(U) \leq G$, it follows that G must have a Sylow p-subgroup of order p^e.

One set that has an orbit which does not divide p is the set of all subsets of G with order p^e. Explicitly, $S = \{U \subseteq G : |U| = p^e\}$. Note that $|S| = \binom{n}{p^e}$. By the p^e-subset lemma, the order of S is not divisible by p. Since the orders of the orbits of S divide the order of S, no orbit is divisible by p. This proves the first Sylow theorem.

□

p^e-Subset Lemma

Let G be a group, and $|G| = n = p^e m$. Let the set, S, be defined as the following: $S = \{U \subseteq G : |U| = p^e\}$. Then $|S|$ is not divisible by p.

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, then 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 the $(n-k)$ 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.

□

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 $|G|$.

Proof. Clearly $|\text{stab}(U)|$ divides $|G|$, since $\text{stab}(U) \leq G$. All that is left to show is that $|\text{stab}(U)|$ divides $|U|$.

Consider the group action of $\text{stab}(U) * U$, where elements in $\text{stab}(U)$ act on elements of U by left multiplication. Each H-orbit is equal to some set $\{hu : h \in \text{stab}(U), u \in U\}$, which is the same as the coset $[\text{stab}(U)]$. Since the elements of U are also elements of G, each hu must be unique, so each H-orbit has an order of H. But, the H-orbits also partition U, so $|U|$ must divide $|G|$. This proves the subset-stabilizer lemma.

□

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. Considering the set, C, of cosets of a Sylow p-subgroups, H, $C = \{gH : g \in G\}$. This proof will argue that, since all stabilizers of $c \in C$ under $G * C$ are conjugate to H, and the conjugate orbit of H contains all p-subgroups, all Sylow p-subgroups are conjugate, and all p subgroups will be contained in some conjugate of a Sylow p-subgroup.

Take the group action $G * C$. Under this action, C is transitive. Since for any two cosets aH and bH in C, the element $ba^{-1} \in G$ takes aH to bH:

$$g(aH) = (ba^{-1})(aH) = (bH)$$

There is also at least one element, gH, in C where the stabilizer of c is equal to H. In the trivial case, $\text{stab}(eH) = H$. Since the stabilizers in the same orbit are conjugate, and there is only one orbit in C, all the possible stabilizers are conjugate. And since all stabilizers are subgroups of G, with order p^e, they are all Sylow p-subgroups, too. Therefore Sylow p-subgroups are conjugate to other Sylow p-subgroups, but it hasn't yet been shown that all Sylow p-subgroups are conjugate to all Sylow p-subgroups.

Since H is a Sylow p-subgroup, and, by Lagrange's theorem, $[G : H] = \frac{|G|}{|H|} = \frac{p^e m}{p^e} = m$, 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 C: $K * C$. Since K is a p-subgroup of $|G|$ and the order of H in G does not divide p, it follows from the Fixed Point Theorem that there exists an element $c \in C$ such that $\text{stab}(c) = K$. It follows, then, that K must be a subgroup of a larger stabilizer of c in $G * C$–that $K \leq H'$ where H' is some conjugate of H.

Since all p-Subgroups are contained in conjugates of H, all Sylow p-subgroups are contained in conjugates of H, so all Sylow p-subgroups are conjugates of each other. This concludes the proof.

□

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 is is the set of Sylow p-subgroups of G. By the Second Sylow Theorem, $G * S$ must be transitive, since all Sylow p-subgroups are conjugate. Also, the stabilizer of a Sylow p-subgroup is, the set $\{g \in G : gHg^{-1} = H\}$, which, by definition is the normalizer of H, $N(H)$. By the Orbit Stabilizer Theorem:

$$|\text{orb}(H)||\text{stab}(H)| = |S| = [G : H] \equiv (s)|N(H)| = (m) \equiv |N(H)| = \frac{m}{s}$$

So s must divide m.

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' is 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 $p)$. So $s \mod p = 1$. □