Sylow theorems

Mendel Keller

November 17, 2017

All the groups we'll be working with will be finite.

1 Lagrange's theorem

The first tool for studying groups using their orders, is that the order of a subgroup divides the order of a group. Consequentially, we have that the number of cosets of a subgroup also must divide the order of the group. First we show that cosets *partition* a group. That means that each group element is in exactly one coset. First, we certainly have, by the fact that $1 \in H$ that $a \in aH$, next we show that $a \in bH \Rightarrow b \in aH$, we have this because $a \in bH \Rightarrow a = bh$ for some $h \in H \Rightarrow b = ah^{-1} \Rightarrow b \in aH$. Lastly, we show that $aH = bH$ by showing that $a \in bH$ and $b \in cH \Rightarrow a \in cH$, we have this because we have $a = bh$ and $b = ch'$ so $a = (ch')h = c(h'h) = ch''$. Now we show that $|aH| = |H|$ we have $|H|$ many products ah, one for each $h \in H$, so we need only show that $ah = ah' \Rightarrow h = h'$ but we have that by multiplying on the left by a^{-1}.

We state this result as $|G| = |H|[G : H]$

Some examples are given by the permutation group S_n, for example take S_3, this has four subgroups, one of order 3 $\{1, \sigma, \sigma^2\}$, and 3 of order 2, each given by a transposition. This satisfies the above since 2 and 3 both divide 6.

2 Orbit stabilizer

The second thing to know is somewhat more subtle. If we have a group G and a set S, a group operation $G \circlearrowright S$ on a set is a way of assigning for a pair $g \in G$ and $s \in S$ an element $gs \in S$, so that g takes every element in S to another element of S. It must satisfy the two conditions that $1s = s$ and $g(hs) = (gh)s$ i.e. the identity acts as an identity, and applying one group element and then another is the same as applying their product. This lets the group operation be compatible with the group structure. Now, every set element has some corresponding subset $O_s \subset S$ which is all the elements that it gets mapped to under the operation of G, we also have that $s = gs' \Rightarrow O_s = O_{s'}$, since we can act by g^{-1}, so that S is partitioned into orbits. Similarly, there is an associated subgroup Z_s that fixes any element s. This is a subgroup because $1 \in Z_s$, we also have that if $gs = s$ then $g^{-1}s = g^{-1}(gs) = (g^{-1}g)s = 1s = s$ so that $g^{-1} \in Z_s$ as well, lastly if $gs = s$ and $hs = s$ then $(gh)s = g(hs) = gs = s$.

The orbit-stabilizer theorem says that $|G| = |O_s||Z_s|$.

Look at the group of triangle, which is S_3. We can view the group as acting on the set of 3 vertices, the stabilizer of a vertex has order 2, so this works out. We could also consider the group as acting on the set of 2 faces, where each face has stabilizer of size 3. Notice that both faces have the same stabilizer, so it is **not** in general true that the stabilizers of elements yield everything in the group (in fact this is impossible, since the identity stabilizes everything, and will therefore appear many times). If we consider in general S_n as acting on a set of n elements, we find that the stabilizer of an element is exactly equivalent to S_{n-1}, so that $|S_n| = n|S_{n-1}|$ this by induction gives that $|S_n| = n!$ as we well know to be the case.

3 Conjugation

One important group operation, is a group acting on itself by conjugation. Given two elements $g, h \in G$ we have g act on h by sending it to ghg^{-1}, clearly the identity fixes anything, and we observe that $g(hk) =$

$g(h*k*h^{-1}) = g*h*k*h^{-1}*g^{-1} = (g*h)k$ (we use $*$ here to denote multiplication, and juxtaposition to denote the operation, to remove ambiguity). There's a lot we can say about conjugation, but we'll just keep moving on in order to get to the Sylow theorems. We will see conjugation again before the lecture is over however.

4 Prime squares

Before presenting the Sylow theorems, we characterize groups of size p^2. The first thing to notice is that the elements that commute with an element g are a subgroup, in fact it's the stabilizer Z_g of the element under conjugation. Now, by having the group act on itself by conjugation, an element that commutes with everything is stabilized by everything, we call this subgroup Z. If we have a group with $|G| = p^2$, an element must have orbit of $1, p$ or p^2 under conjugation, since the orbit must divide p^2. But it cannot have p^2, since nothing is in the conjugacy class of the identity ($g1g^{-1} = gg^{-1} = 1$). Now if everything besides the identity had conjugacy class of order p (and so $Z = \{1\}$), the class equation would look like $np + 1$, which is impossible, because it needs to be p^2. So we must have at least one other element in Z. Now since Z is a subgroup with order greater than 1, it must have order p or p^2. But it must in fact have order p^2, because if $|Z| = p$, then given an element g of G that wasn't in that subgroup Z, we clearly have $g \in Z_g$, and also $Z \subset Z_g$, this gives that $|Z_g| > p \Rightarrow |Z_g| = p^2 \Rightarrow g \in Z \Rightarrow |Z| > p \Rightarrow |Z| = p^2$ (essentially this is actually just a proof by contradiction). So we know the group is commutative. Now if the group has an element of order p^2, it is cyclic, generated by such an element. If it does not, then every element has order p, choose two elements $x, y \in G$ with $< x > \cap < y > = \{1\}$, then we have $< x > \times < y > \cong G$.

5 Stating the theorems

There are three theorems, and we will now state them.

Theorem. *Given a group G and prime p with $|G| = p^n k$ where $p \not| k$:*

1. *There exists a subgroup H of G with $|H| = p^n$, we call such a subgroup a sylow-p subgroup.*
2. *Given a subgroup K of G with $|K| = p^m$ we have that K is contained in some gHg^{-1}, a conjugate subgroup of H. In particular, all sylow-p subgroups are conjugate.*
3. *The number of sylow-p subgroups divides k and is equal to 1 mod p.*

6 An application or two

Consider the group S_4, it has order 24, so it has a subgroup of order $8 = 2^3$. It has either 1 or 3 of these. We know that there is a subgroup of order 4 generated by any cyclic element of order 4. We also have a subgroup of order 4 given by $\{1, (12), (34), (12)(34)\}$. Trying to combine these into a subgroup of order 8 we find that the subgroup is $\{1, (12), (34), (1324), (1423), (12)(34), (13)(24), (14)(23)\}$ and there are three such conjugate subgroups, one for each pair of transpositions.

As you may notice, the thing we have shown about groups of order p^2 isn't helped out by the Sylow theorems, and is essentially completely unrelated to them. Essentially, the Sylow theorems deal only with cases with a more complicated prime factorization, and use more convoluted arguments. Whereas the arguments that can be made about groups of size a prime power are more straightforward.

A more direct and mechanical application is in showing that there is only one group of order 15. Here, we have $15 = 5 \times 3$, so that there is one Sylow subgroup of each size. These are cyclic, since any group of prime order is (an element must have order dividing that of the group). So we have the subgroups are $1, x, x^2$ and a, y, y^2, y^3, y^4. It turns out by some other theorems, that this gives that the group is the "product" of these two subgroups, which turns out to be the product of everything in the one subgroup by everything in the other. So the group is $\{x^i y^j : 0 \leq i \leq 2, 0 \leq j \leq 4\}$. It turns out then that xy has order 15, and this is a cyclic group of order 15 (I think this application requires some more group theory to appreciate, but the general point is that facts can be deduced just from knowing a group's order, and this will limit the types of things the group could possibly be, I personally prefer applications of the first type, where the second theorem is used to find a sylow-p subgroup, and knowing this along with the 3rd theorem helps one figure out what the other sylow-p subgroups are).

7 Proving the theorems

We start with the first theorem.

Proof. Consider the set S, of all subsets (not necessarily subgroups) of order p^n. There are $\binom{p^n k}{p^n}$ such subsets. Writing this binomial expansion out, we find that $p \not| |S|$. Operating by multiplication by group elements, by the fact that a group action partitions S into orbits, we get that $|S| = \sum |O_s| = \sum |G|/|Z_s|$. Now we have that the stabilizer of a subset of order p^n is at most p^n, because picking a single element g of a subset and multiplying by any two different elements yields a different result, because we could cancel using g^{-1}. But conversely, if every stabilizer had order less than p^n, then p would divide the size of every orbit, so it would divide the sum of sizes of orbits, so it would divide $|S|$, which it does not. Therefore at least one element of S has stabilizer of size p^n, and the stabilizer is a subgroup, so teh theorem is proved. ■

The proof used is here is somewhat of a clever trick, and doesn't actually tell us much about the sylow-p subgroup. But it does the job. all the proofs of sylow theorems use similar slight of hand, as we will see. We now prove the second theorem. Before proving it, we point out a fact about stabilizers. If $gs = s'$ then $Z'_s = gZ_sg^{-1}$ this is true because $gs = s' \Rightarrow s = g^{-1}s'$ so that given an element $h \in Z_s$ we multiply $ghg^{-1}s'$ to obtain $ghs = gs = s'$ (this gives us containment, to get equality we do the same process in the opposite direction to get the other containment, which gives equality). We are now ready to prove the second Sylow theorem.

Proof. We choose the set S of cosets of our Sylow-p subgroup H. This set has size k, by Lagrange's theorem. In particular, $p \not| k$. Now, we have the operation of $G \circlearrowleft S$. We consider the restriction of this action to K (this could be denoted $G \circlearrowleft |_K S$, but that's just fancy notation). Now we have that $|K| = p^m$, so the order of the orbit of s is $p^m/|Z_s|$. By the fact that $k = |S| = \sum |O_s|$ we have that at least one stabilizer must have order p^m i.e. is the whole of K, denote the element stabilized by K by L. We have that $L = gH$ for some $g \in G$, by definition of a coset. Now the stabilizer of H in G is exactly H, so that the stabilizer of L in G is exactly gHg^{-1}, and thus we have shown that $K \subset gHg^{-1}$, as we have set out to. ■

Again, as you can see, this isn't very direct. It's basically just finding the correct way to fiddle with the right set, and use some divisibility argument. The proof of the third theorem is somewhat more satisfying, as it validates our intuition about it. Without further ado, we prove the third and final Sylow theorem.

Proof. We take the set S of Sylow-p subgroups, and operate on them by G using conjugation. Using the second theorem, we have that these form a single orbit (we call such an operation transitive, for example the operation by G in the previous proof was transitive). The stabilizer of a Sylow subgroup Z_H is a subgroup, since every stabilizer is, and it contains all of H, so that $H \subset Z_H$ and so this gives that $|S|\,|k$, proving the first half of the theorem.

Now, restricting the above operation to the action of H, clearly H stabilizes itself, so that its orbit is 1. If we could show that H doesn't fix any H', we will have that every other orbit has order divisible by p (since every subgroup of H has order p^m for $m \leq n$). But if H fixed some H', then $H \subset Z_{H'}$ but we also have $H' \subset Z_{H'}$. So that these are both Sylow-p subgroups of $Z_{H'}$, which means that something in $Z_{H'}$ conjugates H' into H, but this is impossible, because by definition $Z_{H'}$ conjugates H' into itself. ■

Here the argument is more natural, and reflects what's actually going on, to a much greater extent than the other two theorems.

8 Group of semiprime order

Given a group of order pq, where p and q are distinct primes, we must have one greater than the other, say that $p > q$. We then must have only one subgroup of order p. Since, letting n_p denote the number of Sylow-p subgroups, we need $q|n_p$ so that $n_p = 1$ or $n_p = q$. But we also need $n_p = 1 + pk$ and so we cannot have $n_p = q$ because $p > q$. If it is that case that $q \not| (p-1)$ we also have only one subgroup of order q. This is true because $n_q|p \Rightarrow n_q = 1$ or $n_q = p$. But if it is equal to p we would need $p = 1 + qk \Rightarrow p - 1 = qk \Rightarrow q|(p-1)$ which we said was not the case. So that, there are $p - 1$ elements of order p and $q - 1$ of order q, there are some remaining elements, and these must have order pq, so that the group is cyclic. Even if this is not the case, the Sylow theorems tell us quite a bit about the group, and these are some of the simplest cases for applying the Sylow theorems.