from scratch series...........

SYLOW'S FIRST THEOREM

Let G be a group. If p is a prime and p^k is the highest power of p that divides $|G|$, then G has a subgroup of order p^k.

BACKGROUND:

A very important question about a group is "What are its subgroups?". A converse to Lagrange's Theorem would be very useful in this regard. Unfortunately, the converse of Lagrange's Theorem, which would say that if n divides the order of a group G, then G has a subgroup of order n, is famously not true. For example, the alternating group A_4 has order 12, but has no subgroup of order 6. Cauchy proved a weak converse: If a prime p divides the order of a group, then the group contains an element of order p, hence a cyclic subgroup of order p. Gallian proves an even weaker result early in his book, where the Cauchy-type theorem applies only to abelian groups. He needs to have this established before he proves Sylow's First Theorem, then he recovers Cauchy's Theorem (full power, no abelian restriction) as a corollary of Sylow. In all of these theorems, whenever the condition is asserted that a prime p divides the order of the group, it is redundant to specify that the group is finite. Keep in the back of your mind the notion that it is possible to extend Sylow's results to groups of infinite order. I'll mention how to do that below.

Ludvik Sylow was a high school teacher in present day Oslo, Norway, from about 1858 to 1898. He was an adjunct at Christiania University (now Oslo Universitet) until they finally hired him as a professor in 1898. He lived until 1918. The theorem proved below was first enunciated and proved by him in 1872. It is widely regarded as the most profound theorem in the theory of finite groups. Lagrange's Theorem is more important, but not as deep. It is an existence theorem, obviously, but there is no companion uniqueness assertion. The subgroups that Sylow's First Theorem identifies may or may not be unique, but that possibility is addressed in Sylow's Third Theorem.

KEY DEFINITIONS:

1) A *p-group* or subgroup is a group or subgroup with order equal to some power of the prime p.

2) A *p-Sylow subgroup* is a maximal p-subgroup, i.e. it is not contained in any larger p-subgroup. So if a group has a subgroup of order p^k, but not p^{k+1}, then such a subgroup would be a p-Sylow subgroup. You may see p-Sylow subgroup written as "Sylow p-subgroup", as Gallian does. They mean the same thing. Notice that only the maximality and not a particular value of k is crucial in defining the notion of p-Sylow subgroup.

3) The *centralizer* of an element $g \in G$ is the collection of all elements that commute with g, and it is a subgroup of G. We write it as $C(g)$, and note that $C(g) \leq G$.

4) The *center* of a group is the collection of all elements that commute with every element of G. We write it as $Z(G)$, and note that $Z(G) \leq G$.

5) The *conjugacy class* of an element $g \in G$ is the collection of all elements expressible as hgh^{-1} as h runs thru the elements of G. Conjugacy classes are not subgroups themselves unless the particular class is generated by the identity, in which case it collapses to the trivial subgroup.

KEY FACTS:

1) Lagrange's Theorem : If $H \leq G$, then $|G| = |G : H||H|$

2) The Class Equation: $|G| = |Z(G)| + \sum_{g \in \Lambda} |G : C(g)|$, where the summation is over a set of representatives of the non-trivial conjugacy classes.

3) The Weak Cauchy Theorem: if G is an abelian group and p divides the order of G, then G has an element of order p

4 The Correspondence Theorem: If $N \triangleleft G$, and $N \leq H \leq G$, then the mapping $H \mapsto H/N$ is injective. Translation: there is a one to one correspondence between subgroups sandwiched between a group and a normal subgroup and the factor groups created by taking each such sandwiched subgroup modulo the normal subgroup. This is an exercise in Gallian, but often proved in other texts (see for example Walker, *Introduction to Abstract Algebra*, p.51 ,§2.3.9)

PROOF STRATEGY:

This proof follows the original due to Georg Frobenius (a German mathematician contemporary with Sylow and, coincidentally, a first cousin, mathematically speaking, of mine) and is the one in our book. A combinatorial proof by H. Wielandt is presented in Wikipedia. A powerful method of proving things in group theory involves induction on the order of a group. If the base case for some property can be established and a factor group created by finding some non-trivial normal subgroup, then the order of the factor group is less than the order of the original group, and the assertion of the induction hypothesis applies immediately to the factor group. The trick is to then show that if the factor group has the property, it must be the case that the original group has that property. In many cases, this can be done.

Divisibility criteria play an important role in this proof, but that would be expected, since the Sylow Theorem is predicated on divisibility by primes.

PROOF:

First we establish the base case for induction. Suppose the order of G is 2, then the theorem is true for $p = 2$ and $k = 1$, since the group itself $G = \mathbb{Z}_2$ is the subgroup we are looking for. Gallian starts by establishing the theorem for $|G| = 1$. However, since 1 is not regarded as a prime, there is no prime which divides "the order of the group", moreover there is no subgroup with prime power order for the same reason. In this situation, the statement of the theorem is one of those false implies false material implications from logic which is defined as true from the truth table. While logically impeccable, this seems not as straightforward to me as showing that the claim of the theorem really does work for some base case. Hence my choice of $p = 2$. OK... so we have the base case.

Now assume the theorem is true for all groups with order less than $|G|$. At this point, either G contains a proper subgroup H which itself satisfies the premise of the theorem (i.e. p^k divides the order of H) or it does not. If it does, then we get our conclusion immediately by the induction hypothesis. If it does not, then no proper subgroup of G has order divisible by p^k . Think about why this is a very productive statement. Either the theorem is proved at once, or we can assume no subgroup can have its order divisible by p^k. We are now entering the realm of proof by contradiction, even though Gallian never mentions that explicitly. Logically, the argument is of the form (i) either statement A or statement not-A is true, (ii) not-A implies A, contradiction (iii) therefore A is true.

There are generally lots of subgroups running around in any group, at least formally. Consider the center or the centralizer of any element, for example. If none of these groups can have order divisible by p^k, and yet $|G|$ is divisible by p^k, then Lagrange's Theorem forces us to conclude that the index of every subgroup in G must be divisible by at least one factor of p. Stated more succinctly, if $H \leq G$, then $|G| = |G : H||H|$, and there must be k factors of p on the right, not all of which are contained in $|H|$. So at least one factor of p is contained in $|G : H|$.

Consider what the class equation says now that we know every index $|G : C(g)|$ must be divisible by p. Rewriting it as $|G| - \sum_{g \in \Lambda} |G : C(g)| = |Z(G)|$, we note that p divides the left, since it divides both $|G|$ and every index, hence it divides the right. We conclude that the prime p divides the order of the abelian (sub)group $Z(G)$. Turning the crank on the weak version of Cauchy's Theorem, we are assured of the existence of an element $g \in Z(G)$ with order p. We construct the cyclic subgroup $\langle g \rangle$ with order p, and note that since $\langle g \rangle \leq Z(G)$, in fact $\langle g \rangle \triangleleft G$. Recall the center of any group is always normal and any subgroup inside the center is as well. Now we are on the verge of being able to realize the point of our induction strategy.

Since $\langle g \rangle$ is normal in G, it makes sense to form the factor group $G/\langle g \rangle$. We know $|G/\langle g \rangle| = \dfrac{|G|}{|\langle g \rangle|}$, so $|G/\langle g \rangle| = \dfrac{|G|}{p} \leq |G|$. The induction hypothesis therefore applies to the factor group, and since p^{k-1} must divide $|G/\langle g \rangle|$, we conclude that $G/\langle g \rangle$ contains a subgroup of order p^{k-1}. It wouldn't hurt to remind ourselves that the induction hypothesis applies to groups with order less than $|G|$ and any prime power divisor of that order, so long as that is the maximal power of the prime divisor. This is implicit in Gallian's argument. We have deliberately created the situation where p^{k-1} is the maximal power of p that divides the order of $G/\langle g \rangle$.

So $G/\langle g \rangle$ has a subgroup of order p^{k-1}, which we may represent as $H/\langle g \rangle$, where $\langle g \rangle \leq H \leq G$. What permits us to say this? The Correspondence Theorem. Now the order of H must satisfy the equation $\dfrac{|H|}{|\langle g \rangle|} = |H/\langle g \rangle|$, and it is immediate that $|H| = |H/\langle g \rangle| \cdot |\langle g \rangle| = p^{k-1} \cdot p = p^k$. And we see that the subgroup H is the one guaranteed by the theorem and we are done.

The indirect nature of this proof (the method of proof by contradiction) got buried in the fact that the contradictory conclusion was actually the statement we were looking for. Usually, proofs by contradiction hinge on some sublety and not the main assertion.

If we allow $|G| = \infty$, then we are at a loss to develop conditions based on divisibility by primes, but we can still retain some of the flavor of the theorem by defining a *p-Sylow subgroup* to be a p-subgroup of G which is maximal in the sense that it is not properly included in any other p-subgroup of G. The relation "being a sub-group of" is a partial order on the family of p-subgroups of a given group, and partially ordered sets are subject to Zorn's Lemma: If a partially ordered set S has the property that every chain (linearly ordered subset) has an upper bound in S, then S has at least one maximal element. Every chain of p-subgroups has an upper bound in G (prove that by taking the appropriate union). So a maximal p-subgroup exists. That would be a p-Sylow subgroup, and we have an extension of Sylow's First Theorem to the case where the group G has infinite order.