NOTES ON SYLOW'S THEOREMS

MATH 113, SECTION 1

1. Notes on Sylow's theorems, some consequences, and examples of how to use the theorems.

Here are some notes on Sylow's theorems, which we covered in class on October 10th and 12th.

Textbook reference: Section 4.5.

1.1. **Sylow's theorems and their proofs.**

Definitions. Let G be a group, and let p be a prime number.

- A group of order p^k for some $k \geq 1$ is called a ***p*-*group***. A subgroup of order p^k for some $k \geq 1$ is called a ***p*-subgroup**.
- If $|G| = p^\alpha\ m$ where p does not divide m, then a subgroup of order p^α is called a **Sylow *p*-subgroup** of G.

Notation.

$$Syl_p(G) = \text{the set of Sylow } p\text{-subgroups of } G$$
$$n_p(G) = \text{the \# of Sylow } p\text{-subgroups of } G\ = |Syl_p(G)|$$

Sylow's Theorems. *Let G be a group of order $p^\alpha\ m$, where p is a prime, $m \geq 1$, and p does not divide m. Then:*

1. *$Syl_p(G) \neq \emptyset$, i.e. Sylow p-subgroups exist!*
2. *All Sylow p-subgroups are conjugate in G, i.e., if P_1 and P_2 are both Sylow p-subgroups, then there is some $g \in G$ such that $P_1 = g\ P_1 g^{-1}$. In particular, $n_p(G) = (G : N_G(P))$.*
3. *Any p-subgroup of G is contained in a Sylow p-subgroup.*
4. *$n_p(G) \equiv 1 \mod p$.*

We'll prove each of the statements (1) through (4).

Proof of (1). By induction on $|G|$.

Base step: $|G| = 1$: in this case there are no prime factors in the first place, so the statement of (1) is trivially true.

Date: Fall 2011.

Inductive hypothesis: Suppose (1) holds for all groups of order $< n$.

Inductive step: Let G be a group of order n. Let p be a prime that divides n, and suppose $n = p^{\alpha}\, m$, where p does not divide m. We want to show that there is a Sylow p-subgroup, i.e, a subgroup of G of order p^{α}.

Two separate cases: p divides $|Z(G)|$, and p does not divide $|Z(G)|$.

Case (i): p divides $|Z(G)|$.

Then Cauchy's Theorem $\implies Z(G)$ has an element of order p, hence a subgroup of order p, call it N. Note: $N \lhd G$, since $\forall n \in N, \forall g \in G, gng^{-1} = n \in N$ since n is in the center of G so it commutes with g.

G/N is a group of order $n/p = p^{\alpha}m/p = p^{\alpha-1}m$. Now $p^{\alpha-1}m < n$ so the inductive hypothesis $\implies G/N$ has a Sylow p-subgroup, call it $\overline{P}$. That is, $\overline{P} \leq G/N$ has order $p^{\alpha-1}$.

Now define $P = \{g \in G | gN \in \overline{P}\}$.

$P \leq G$: Check with the subgroup criterion: $1N$ is the identity in G/N so $1N \in \overline{P}$. Therefore $1 \in P$, so $P \neq \emptyset$. Now suppose $g_1, g_2 \in P$, i.e. $g_1N, g_2N \in \overline{P}$. Then $(g_1g_2^{-1})N = (g_1N)(g_2N)^{-1} \in \overline{P}$ since $\overline{P}$ is closed under inverses and multiplication. Hence $g_1g_2^{-1} \in P$.

Also, $N \leq P$, since for all $n \in N$, $nN = N \in \overline{P}$. Therefore the homomorphism

$$\begin{aligned} \varphi : P &\to \overline{P} \\ g &\mapsto gN \end{aligned}$$

is surjective (by construction), and $\ker\varphi = P \cap N = N$. First Isomorphism Theorem $\implies P/N \cong \overline{P}$. Hence $|\overline{P}| = (P : N) = |P|/|N| \implies |P| = |\overline{P}||N| = p^{\alpha-1}\, p = p^{\alpha}$.

Therefore P is a Sylow p subgroup of G.

Case (ii): p does not divide $|Z(G)|$.

Class Equation: $|G| = |Z(G)| + \sum_{i=1}^{r}(G : C_G(g_i))$, where $g_1, \dots, g_r \in G$ are representatives of the distinct conjugacy classes of size > 1 (so the

g_i's are NOT elements of $Z(G)$).

p can't divide all of the terms $(G : C_G(g_i))$ since then it would divide their sum, and since p also divides $|G|$ it would force p to divide $|Z(G)|$, which we're assuming it doesn't.

So let g_i be a representative of a conjugacy class of size > 1 such that p does not divide $(G : C_G(g_i))$. By Lagrange's theorem $(G : C_G(g_i)) = |G|/|C_G(g_i)|$ so if p doesn't divide it, then all the factors of p in $|G|$ must be factors of $|C_G(g_i)|$, i.e., $|C_G(g_i)| = p^\alpha k$ for some k.

Note: k has to be less than m, because the only way it can be m is if $|C_G(g_i)| = |G|$, which would mean $G = C_G(g_i)$, so every element of G would have to commute with g_i, which would mean $g_i \in Z(G)$, and this is NOT the case.

So the inductive hypothesis applies to $C_G(g_i)$, and it has a Sylow p-subgroup of order p^α. It's also a subgroup of G, which makes it a Sylow p-subgroup of G.

□

Proof of (2). From (1) we know that there's *some* Sylow p-subgroup. So let P_1 be a Sylow p-subgroup of G.

Now let $S = \{P_1, \dots, P_k\}$ be the set of all distinct conjugates of P_1. In other words, for every $g \in G$, the subgroup gP_1g^{-1} is one of these conjugates, and each P_i is equal to gP_1g^{-1} for some $g \in G$.

First we'll show that p can't divide $k = |S|$.

Let G act on S by conjugation, i.e., $g \cdot P_i = gP_ig^{-1}$. The stabilizer of P_i is the subgroup $\{g \in G | gP_ig^{-1} = P_i\}$ which by definition is the normalizer $N_G(P_i)$.

Since each of the P_i's is conjugate to P_1, everything is in the orbit of P_1, there's only one orbit, which is all of S. So $|S| = |\text{orbit of } P_1| = (G : N_G(P_1))$ by the formula for orbit size.

Lagrange's theorem says $|G| = (G : N_G(P_1))|N_G(P_1)|$ which implies that $(G : N_G(P_1)) = |G|/|N_G(P_1)|$. Now $N_G(P_1)$ contains P_1 as a subgroup, so by Lagrange's theorem, $|N_G(P_1)|$ contains p^α as a factor, which is the maximum power of p that it can have. So the ratio

$|G|/|N_G(P_1)|$ contains no factor of p. Therefore $|S|$ contains no factor of p, so p does not divide $|S|$.

Now we'll argue that *any* Sylow p-subgroup has to be in S, so any Sylow p-subgroup has to be conjugate to P_1.

Let Q be any Sylow p-subgroup. Let Q act on S by conjugation.

Even without knowing what the orbits look like, we know that the orbits of Q's action partition S into disjoint orbits. So suppose the distinct orbits are the orbits of $P_{i_1}, P_{i_2}, \ldots, P_{i_j}$.

Then $|S| = |\text{orbit of } \ P_{i_1}| + |\text{orbit of } \ P_{i_2}| + \ldots + |\text{orbit of } \ P_{i_j}|$.

By the formula for orbits, $|\text{orbit of } \ P_i| = (Q : \text{stabilizer of } P_i)$, so by Lagrange's theorem this number has to divide $|Q| = p^\alpha$. So the size of each orbit can only be 1 or some power of p.

But we just showed that p doesn't divide $|S|$, which means that we can't have p dividing the size of *all* of the orbits (since then p would divide the sum of all the orbits, which is $|S|$).

Which means that there must be *some* orbit of size 1. Let's say it's the orbit of P_m. So $1 = |\text{orbit of } \ P_m| = (Q : \text{stabilizer of } P_m)$, and the stabilizer of P_m is $\{g \in Q | gP_mg^{-1} = P_m\} = \{g \in Q | g \in N_G(P_m)\} = Q \cap N_G(P_m)$.

So $|Q|/|Q \cap N_G(P_m)| = 1$, which forces $Q = Q \cap N_G(P_m)$. This says every element of Q is also in $N_G(P_m)$, so $Q \leq N_G(P_m)$.

Finally, P_m is a normal subgroup of its normalizer, and the order of the quotient group $N_G(P_m)/P_m$ has no factors of p in it (since by Lagrange's theorem $|N_G(P_m)/P_m| = |N_G(P_m)|/|P_m| = |N_G(P_m)|/p^\alpha$ and p^α is the maximum power of p possible for subgroups of G).

Since Q is a subgroup of $N_G(P_m)$, we can restrict the canonical homomorphism $\pi : N_G(P_m) \to N_G(P_m)/P_m$ to Q to get a homomorphism $\pi : Q \to N_G(P_m)/P_m$, given by $\pi(x) = xP_m$. Every non-identity element of Q has order equal to some power of p. But the quotient group contains no elements of order equal to a power of p, since it has no factors of p at all. Therefore every element of Q that has order equal to a power of p has to map to the identity element of the quotient group. This means every element of Q maps to the identity element of $N_G(P_m)/P_m$.

In other words, for all $x \in Q, \quad xP_m = P_m$, which is equivalent to $x \in P_m$. Therefore, $Q \leq P_m$. But these are both Sylow p-subgroups so they're both of order p^α, so Q is equal to P_m.

This shows that after all, Q is in S.

□

Before we go on to proving (3) and (4), we prove a Lemma that we'll use.

Lemma. *Let P be a Sylow p-subgroup of G, and let Q be any p-subgroup. Then $Q \cap P = Q \cap N_G(P)$.*

Proof. $P \leq N_G(P)$ so automatically $Q \cap P \leq Q \cap N_G(P)$.

We need to show $Q \cap P \geq Q \cap N_G(P)$.

Instead of always writing out $Q \cap N_G(P)$, let's call it H.

Since it's the intersection, $H \leq Q$ and $H \leq N_G(P)$. Since Q is a p-subgroup, H is either trivial or it's a p-subgroup as well (by Lagrange's theorem).

Now we do the same thing we did towards the end of proving (2):

We know that P is a normal subgroup of $N_G(P)$ and the order of the quotient group $N_G(P)/P$ has no factors of p left in it. Since H is a subgroup of $N_G(P)$, we can restrict the canonical homomorphism $\pi : N_G(P) \to N_G(P)/P$ to H and consider the homomorphism $\pi : H \to N_G(P)/P$. That is, $\pi(x) = xP$.

Every element in H whose order is a power of p must map to the identity element in $N_G(P)/P$, since $N_G(P)/P$ has no elements whose orders are powers of p.

Therefore, $xP = P$ for all $x \in H$, i.e., for all $x \in H$, $x \in P$.

So $H \leq P$. And since we already have $H \leq Q$, we get $H \leq Q \cap P$.

Therefore (returning to what H is), $Q \cap N_G(P) \leq Q \cap P$. □

Proof of (3). Let H be any p-subgroup of G. We want to show that $H \leq P_i$ for some P_i in S.

So we let H act on $S = \{P_1, \ldots, P_k\}$, by conjugation.

We know that the orbits of this action will partition S. Suppose the distinct orbits are the orbits of $P_{i_1}, \ldots, P_{i_m}$, so

$$|S| = |\text{orbit of } \ P_{i_1}| + |\text{orbit of } \ P_{i_2}| + \ldots + |\text{orbit of } \ P_{i_m}|.$$

Then the orbit formula says that for any P_i in S, $|\text{orbit of } \ P_i| = (H : H \cap N_G(P_i))$, since $H \cap N_G(P_i)$ is the stabilizer of P_i under the action of H.

So the size of each orbit has to divide $|H|$, which is a power of p.

Remember though that p doesn't divide $|S|$, so we can't have p dividing all of the terms $|\text{orbit of } \ P_{i_1}|, \ldots, |\text{orbit of } \ P_{i_m}|$ (or else p would divide their sum, and therefore $|S|$).

So one of these orbits, say the orbit of P_{i_j}, has $|\text{orbit of } \ P_{i_j}| = 1$.

By the orbit formula, $1 = |\text{orbit of } \ P_{i_j}| = (H : H \cap N_G(P_{i_j}))$. This means $H = H \cap N_G(P_{i_j})$, and since H is a p-subgroup the Lemma says $H \cap N_G(P_{i_j}) = H \cap P_{i_j}$. Therefore $H = H \cap P_{i_j}$, so every element of H is also in P_{i_j}, so $H \leq P_{i_j}$, so our p-subgroup H is a subgroup of the Sylow p-subgroup P_{i_j}.

So we have proved that any p-subgroup of G must be contained in one of the Sylow p-subgroups of G.

□

Proof of (4). We need to show that $|S| \equiv 1 \ mod \ p$.

Write $S = \{P_1, \ldots, P_k\}$ for the distinct Sylow p-subgroups of G.

Now let P_1 act on S by conjugation.

So S becomes a disjoint union of orbits.

The orbit of P_1 has size 1, since it consists only of P_1 itself (since for all $x \in P_1$, $xP_1x^{-1} = P_1$ as P_1 is closed under multiplication by its own elements!)

If $P_i \neq P_1$, then by the orbit formula, $|\text{orbit of } P_i| = (P_1 : P_1 \cap N_G(P_i))$.

And since P_1 is a p-subgroup of G, the Lemma says $P_1 \cap N_G(P_i) = P_1 \cap P_i$. So in fact $|\text{orbit of } P_i| = (P_1 : P_1 \cap P_i)$.

By assumption P_1 and P_i are *different* subgroups of G of the same size, so $|P_1 \cap P_i|$ has to be strictly smaller than $|P_1|$. Therefore, $|P_1|/|P_1 \cap P_i| = (P_1 : P_1 \cap P_i)$ can't be 1. Since it also has to divide $|P_1| = p^\alpha$, it must be a power of p. Therefore, $|\text{orbit of } P_i|$ is a power of p, so in particular p divides every orbit that's not the orbit of P_1.

So now, going back to our equation for $|S|$, we see that $|S| = |\text{orbit of } P_1| + \sum |\text{the other orbits}| = 1 + px$ (since p divides every term in the sum $\sum |\text{the other orbits}|$, it also divides the whole sum).

$|S| = 1 + px$ implies $|S| \equiv 1 \ mod \ p$.

□

1.2. Consequences that you need to know.

- n_p has to divide $|G|/p^\alpha$. Combining this with the condition that $n_p \equiv 1 \ mod \ p$ cuts down the number of candidates for n_p.
  Reason: We know that if we take any Sylow p-subgroup P, then $n_p = (G : N_G(P)) = |G|/|N_G(P)|$. Since $N_G(P)$ contains P, its order contains p^α as a factor. So $|G|/|N_G(P)|$ has no factor of p left in it.
- If a Sylow p-subgroup is a normal subgroup of G, it must be the only one, i.e. $n_p = 1$. And vice versa, if $n_p = 1$, then the one Sylow p-subgroup is a normal subgroup of G.
  Reason: Sylow's theorem says that we get all the Sylow p-subgroups by picking one of them, call it P, and looking at all the possible conjugates gPg^{-1}. So $n_p = 1 \iff gPg^{-1} = P$ for all $g \in G \iff P$ is a normal subgroup of G.
- In particular, if G is abelian, any subgroup is normal. So abelian groups have exactly one Sylow p-subgroup for each p. We'll have a lot more to say about finite abelian groups in a couple more lectures.
- Sylow p-subgroups for different primes can only have trivial intersection.
  Reason: If p_1, p_2 are distinct primes, and $P_1 \in Syl_{p_1}(G), P_2 \in Syl_{p_2}(G)$, then $P_1 \cap P_2$ is a subgroup of both P_1 and P_2. So

by Lagrange's theorem its order has to divide $|P_1|$ and it also has to divide $|P_2|$, but of course with different primes the only common factor they have is 1, so $P_1 \cap P_2 = 1$, the identity element of G.

1.3. **Examples.**

(1) Let G be a group of order pq where p, q are both prime, and $p < q$. Then G has exactly one subgroup of order q, which is therefore a normal subgroup of G.

Reason: Let's work out n_q using Sylow's theorem. On the one hand we know it has to divide $pq/q = p$. So it can only be 1 or p. On the other hand it has to be congruent to 1 mod q. Since p is greater than one and less than q it's definitely less than $q + 1$, so the only possibility for n_q is 1. Therefore the Sylow q-subgroup (which has order q) is the only one, so it's a normal subgroup of G.

(2) Let G be a group of order 12. Then either G has a normal Sylow 3-subgroup, or else it's isomorphic to A_4.
Reason: $12 = 2^2 \cdot 3$. We know n_3 has to divide $2^2 = 4$, and it also has to be congruent to 1 mod 3. So it can be either 1 or 4. If $n_3 = 1$, then G has a normal Sylow 3-subgroup.

If $n_3 = 4$, then we know that the four Sylow 3-subgroups are acted on by G, by conjugation. Let's call the set $S = \{P_1, \ldots, P_4\}$. The action of G gives us a homomorphism $\varphi : G \to S_4$.

We'll first show that φ is injective, then we'll show that the image of φ is A_4. This will show that $G \cong \text{im}\varphi = A_4$.

To show φ is injective, we need to show that $\ker \varphi = 1$.

$$\begin{aligned}\ker \varphi &= \{g \in G | gP_ig^{-1} = P_i \text{for all } \ P_i \in S\} \\ &= \cap_{i=1}^4 N_G(P_i).\end{aligned}$$

We know that for each i, $n_3 = (G : N_G(P_i)) = |G|/|N_G(P_i)|$, so we have here that $|N_G(P_i)| = 12/4 = 3$. Since $P_i \leq N_G(P_i)$ and $|P_i|$ is also 3, it means $P_i = N_G(P_i)$. So in our case,

$$\ker \varphi = \cap_{i=1}^4 P_i.$$

The P_i's happen, in this case, to be distinct groups of prime order (their order is 3). A general and useful fact about distinct groups of the same prime order is that they can only intersect each other trivially. (Take for example two subgroups P_1 and P_2 of order p, then the subgroup $P_1 \cap P_2$ has to have order 1 or p. If it has order p then $P_1 = P_2$, so if P_1 and P_2 are not the same subgroup, $P_1 \cap P_2$ has to have order 1, i.e., it's the trivial subgroup.)

Applying this to our case we get $\ker\varphi = 1$. Therefore φ is injective, and $G \cong \mathrm{im}\varphi$.

Now G has 4 subgroups, $P_1, \ldots, P_4$, of order 3. Each of these subgroups has two elements of order 3 and the identity element. The two elements of order three have to be different for each P_i (since different P_i's have only the identity element in common). Therefore G contains 8 different elements of order 3.

Since G is isomorphic to $\mathrm{im}\varphi$, these 8 different elements of order 3 have to map to 8 different elements of order 3 in S_4. The only elements of order three in S_4 are 3-cycles. And 3-cycles are even permutations, so are elements in A_4.

So $A_4 \cap \mathrm{im}\varphi$ is a subgroup of both A_4 and $\mathrm{im}\varphi$ with at least 8 elements. But since both A_4 and $\mathrm{im}\varphi$ have 12 elements, this intersection subgroup has to also divide 12. The only factor of 12 that's greater than or equal to 8 is 12. So $A_4 \cap \mathrm{im}\varphi$ is a subgroup of both A_4 and $\mathrm{im}\varphi$ of size 12, and since A_4 and $\mathrm{im}\varphi$ only have 12 elements anyway, it means $A_4 \cap \mathrm{im}\varphi = A_4 = \mathrm{im}\varphi$.

(3) Let G be a group of order 351. Then G has a normal Sylow p-subgroup for some prime p dividing 351.

Reasoning: $351 = 3^3 \cdot 13$. So a Sylow 3-subgroup would have order $3^3 = 27$, and a Sylow 13-subgroup would have order 13.

Let's start out with what n_{13} can be. n_{13} divides 27, and $n_{13} \equiv 1 \bmod 13$. Only two possibilities: $n_{13} = 1$ or 27.

If $n_{13} = 1$, then the Sylow 13-subgroup is a normal subgroup of G, and we're done.

If $n_{13} = 27$, then we're going to show that there can only be room for one Sylow 3-subgroup, and therefore the Sylow 3-subgroup is normal in G.

We'll use the fact that *distinct* subgroups of order p for some prime p can only have the identity element in their intersection. (Suppose P_1 and P_2 are subgroups of order p. Then $P_1 \cap P_2 \leq P_1$ and $P_1 \cap P_2 \leq P_2$. So $|P_1 \cap P_2|$ must be either 1 or p, and the only way it can be p is if $P_1 \cap P_2 = P_1$ and $P_1 \cap P_2 = P_2$, making $P_1 = P_2$. Therefore if P_1 and P_2 are *not* the same subgroup, their intersection has order 1, so contains only the identity element.) Do be warned, though, that this is only true about subgroups of *prime* order, so this argument wouldn't work if, say, the Sylow 13-subgroups had order 13^2.

Since the Sylow 13-subgroups are subgroups of order 13, they can only intersect each other at the identity element. Also, every element of order 13 forms a subgroup of order 13, which has to be one of the Sylow 13-subgroups.

Each Sylow 13 subgroup contains 12 elements of order 13 (every element except for the identity). There are 27 Sylow 13 subgroups, so there are a total of $27 \times 12 = 324$ elements of order 13 in G.

This leaves $351 - 324 = 27$ elements of G that do not have order 13. Since a Sylow 3-subgroup would have to have exactly 27 elements in it, this means that all these 27 elements form a Sylow 3-subgroup, and it must be the only one (since there aren't any extra elements of G to use). So $n_3 = 1$, and this Sylow 3-subgroup must be normal in G.