Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

September 12, 2006

0.1 TALK SLOWLY AND WRITE NEATLY!!

0.2 Introduction

Before Class

(1) Write my name, office and office hours on the board.

(2) Write name of teaching assistant.

(3) Write the course web address

I hope you all had a great weekend. Introduce myself and the TA again (incase someone wasn't there last time). Also give the course website address again and tell them that the first homework is posted and will be due one week from today

0.3 Sylow's Theorems

Now if you remember Lagrange's theorem from last time, it told us something about the order of subgroups of a finite group. Today we are going to look at Sylow's theorems which will give us significantly more information about the subgroups of a finite group

0.4 First Sylow Theorem

0.4.1 Theorem

1st Sylow Theorem

Theorem 0.4.1.1 (First Sylow Theorem)**.** *Let G be a finite group of order n ($|G| = n$) and let p be a prime such that that*

$$n = p^e \cdot m$$

p does not divide m.

then there is an element of G of order p^e.

Proof. Let $S = \{X \subseteq G : |X| = p^e\}$. The way we are going to prove this theorem is to show that one of the elements of S has a stabilizer (under left multiplication) of order p^e and this stabilizer will be the desired subgroup.

Number of subsets of size p^e

Lemma 0.4.1.2. *The size of S is*

$$N = \left(\begin{array}{c} n \\ p^e \end{array} \right) = \frac{n(n-1)(n-2)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots 1}$$

And further p doesn't divide N.

Proof. It is a standard result that N is the number of subsets of n of size p^e. To see that N is not divisible by p observe that the above product can be written as

$$\Pi_{0 \leq k < p^e}(n-k)/(p^e-k)$$

But if we let $k = p^i l$ we know that $i \leq e$ and so

$$(n-k)/(p^e-k) = \frac{p^i(p^{e-i}m - l)}{p^i(p^{e-i} - l)} = \frac{(p^{e-i}m - l)}{(p^{e-i} - l)}.$$

And because p doesn't divide l we know that p doesn't divide $p^{e-i} - l$ or $p^{e-i}m - l$.

So N can be expressed as a/b where p doesn't divide a or b. Hence p doesn't divide N. □

$|Stab(U)|$ **divides** $|U|$

Lemma 0.4.1.3. *If* $U \subseteq G$ *then* $|Stab(U)|$ *divides* $|U|$.

Proof. First note that if H is a group which operates on S and $T \subseteq S$ then H stabilizes T if and only if T is a union of H orbits.

This is just the definition of orbit.

But, if $Stab(U) \subseteq G$ then we can restrict the group action of left multiplication to be a group action of $Stab(U)$ on G.

So in particular, we know that U is the union of $Stab(U)$ orbits. But an orbit of $Stab(U)$ under left multiplication is just a right coset of $Stab(U)$.

Hence every orbit is the size $|Stab(U)|$ and so $|Stab(U)|$ divides $|U|$. $\square$

Now we can break S into orbits under left multiplication

$$n = |S| = \Sigma_{\text{Orbits O}}|O|$$

And, as p does not divide N there must be a set U of size p^e such that $|Orbit(U)|$ isn't divisible by p.

We know that $|Stab(U)|$ must divide $|U| = p^e$. So in particular $|Stab(U)| = p^f$.

But then we also know

$$|Stab(U)| \cdot |Orbit(U)| = |G| = p^e m$$

. Hence, because $|Orbit(U)|$ is not divisible by p and $|Stab(U)|$ is a power of p, we must have $|Stab(U)| = p^e$. $\square$

0.4.2 Consequences

Sylow group definition

Definition 0.4.2.1. If $|G| = p^e m$ where p is prime and $e \geq 1$ then a subgroup of order p^e is called a Sylow p-subgroup or just a Sylow subgroup

We then have the following corollary of the first Sylow theorem.

1st Sylow Theorem Example

Corollary 0.4.2.2. *If p divides $|G|$ then G contains an element of order p.*

Proof. Let $|G| = p^e m$ and let H be a Sylow subgroup of G.

Now let $x \in H - 1$.

Then the order of x must divide p^e and so the order must be p^r for some $0 < r \leq e$.

Now let $y = x^{p^{r-1}}$. Then $y^p = x^{p^r} = 1$ and so the order

of y is p □

0.5 Second Sylow Theorem

0.5.1 Theorem

2nd Sylow Theorem

Theorem 0.5.1.1. *Let K be a subgroup of G with order divisible by p. Let H be a p-Sylow subgroup of G. Then there is a conjugacy subgroup of $H = gHg^{-1} = H'$ such that $K \cap H'$ is a Sylow p-subgroup of K.*

Proof. First we need a lemma.

Conjugation stabilizer

Lemma 0.5.1.2. *Let $(S, \circ)$ be a G-Set and let $s \in S$. Let s' be in the orbit of s, say $s' = a \circ s$. Then*

$$G_{s'} = aG_s a^{-1}$$

where $G_s, G_{s'}$ are the stabilizers of s, s' respectively.

Proof. This is homework. □

Now, let $S = G/H$ the set of left co-sets of H in G.

Now observe that S has a single orbit under the action of left multiplication by G.

Further, H is the stabilizer of $1H = s$.

So by the homework we have that the stabilizer of $a \circ s$ is aHa^{-1}

Now we can restrict the action of G on S to K and look at the K orbits of S.

Since H is a Sylow subgroup and we know that $|H| \cdot |S| = |G|$ we know that $|S|$ is not divisible by p.

But then there must be some K-orbit O such that p does not divide $|O|$. Lets say O is the orbit of as (where $s = 1H$).

Now let H' be the stabilizer of as which is aHa^{-1}.

Hence, it is obvious that the stabilizer of as in the restriction of the action to K is just

$$\{k \in K : kas = as\} = \{g \in G : gas = as\} \cap K = H' \cap K$$

Hence, $[K : K \cap H']$ is $|O|$ by previous theorems.

But, we know that $|K \cap H'| \cdot |O| = |K|$ and further p doesn't divide $|O|$ and $|K \cap H'| = p^i$ because it is a subgroup of H' which is a p-group.

Hence if $|K| = p^n m$ we must have $|K \cap H'| = p^n$ and

$|O| = m$. □

0.5.2 Examples

Sylow Group Conjugation

Corollary 0.5.2.1. *The Sylow p-subgroups of a group G are all conjugate. Further the conjugate of a Sylow p-subgroup is a Sylow p-subgroup.*

Proof. The second part is trivial.

Let H, K be Sylow p-subgroups of G.

Notice that $|K| = p^e$ and so the Sylow p-subgroup of K is K.

But then we know by the Second Sylow theorem that there is a conjugate H' of H such that $H' \cap K = K$. Hence $H' = K$ as they have the same size. □

0.6 Third Sylow Theorem

0.6.1 Theorem

3rd Sylow Theorem

Theorem 0.6.1.1 (Third Sylow Theorem)**.** *Let* $|G| = n = p^e m$ *where* p *does not divide* m*. Let* s *be the number of* p*-Sylow subgroups of* G*. Then* s *divides* m *and* $s = ap + 1$ *for some integer* a*.*

Proof. **Definition Normalizer**

Definition 0.6.1.2. Let H be a subgroup of G. We call the stabilizer of H under conjugation the Normalizer of H. It is the set

$$N(H) = \{g \in G : gHg^{-1} = H\}$$

Specifically $N(H)$ is the largest subgroup of G such that H is a normal subgroup of $N(H)$.

By the previous theorem, we know that s is the size of

the orbit of H under conjugation and hence is equal to $[G : N(H)]$.

But, since $H \subseteq N(H)$ we know that $[G : N(H)]$ divides $[G : H] = m$.

Now let $S = \langle H_1, \cdots, H_s \rangle$ be the collection of all Sylow subgroups with $H = H_1$. We now want to look at the orbits of S under conjugation by elements of H.

Specifically we know that the orbit of H_i consists of a single Sylow subgroup if and only if $H \subseteq N(H_i)$. I.e. H is in the normalizer of H_i.

But we know

(1) H_i is normal in $N(H_i)$ by the definition of normalizer

(2) $H \subseteq N(H_i)$

(3) H, H_i are Sylow p-subgroups of $N(H_i)$ and hence conjugate.

So we can conclude that $H = H_i$ and there is only one element of order 1.

But we know that the order of any orbit under conjugation by H must divide H.

And, as H is a p-subgroup this means that the order of every other orbit must be a multiple of p.

Hence $s = 1 + ap$ for some integer a. $\square$