MATH 436 Notes: Sylow Theory.

Jonathan Pakianathan

October 7, 2003

1 Sylow Theory

We are now ready to apply the theory of group actions we studied in the last section to study the general structure of finite groups. A key role is played by the p-subgroups of a group. We will see that the Sylow theory will give us a way to study a group "a prime at a time".

First we record a very important special case of group actions:

Theorem 1.1 (p-group Actions). *Let p be a prime. If P is a p-group acting on a finite set X then $|X| \equiv |X^P|$ mod p.*

Proof. By the orbit decomposition formula we have:

$$|X| = |X^P| + \sum_{x_j \in J} |P : P_{x_j}|$$

where J is a set of orbit representatives of orbits of size > 1.

Since $|P : P_{x_j}|$ must divide $|P|$ and is > 1 we see that $p||P : P_{x_j}|$ for all $j \in J$. Thus modulo p, the equation becomes $|X| \equiv |X^P|$ as desired. □

Our first application of Theorem 1.1 is to prove a theorem of Cauchy:

Theorem 1.2 (Cauchy's Theorem on elements of order p). *Let p be a prime, G a finite group with $p||G|$, then there is $x \in G$ with $o(x) = p$.*

Proof. Consider $X = G \times \cdots \times G = \{(a_{\bar{1}}, \ldots, a_{\bar{p}}) | a_{\bar{i}} \in G\}$ the p-fold cartesian product of G. Here we will index the p-tuples with indices from $\mathbb{Z}/p\mathbb{Z}$. $P = (\mathbb{Z}/p\mathbb{Z}, +)$ acts on X by cyclic shifts, i.e.,

$$\bar{k} \cdot (a_{\bar{1}}, \ldots, a_{\bar{p}}) = (a_{1\bar{+}k}, \ldots, a_{p\bar{+}k})$$

It is easy to check that this is indeed an action of P on X.

Now let $Y = \{(a_{\bar{1}}, \ldots, a_{\bar{p}}) \in X | a_{\bar{1}} \ldots a_{\bar{p}} = e\}$. Note that $|Y| = |G|^{p-1}$ as once we have chosen the first $p-1$ elements in the p-tuple, the last one is determined via $a_{\bar{p}} = (a_{\bar{1}} \ldots a_{\bar{p-1}})^{-1}$.

Notice $a_{\bar{1}} \ldots a_{\bar{p}} = e$ gives $a_{\bar{2}} \ldots a_{\bar{p}} a_{\bar{1}} = e$ upon conjugation by $a_{\bar{1}}^{-1}$. (That is left multiplication by $a_{\bar{1}}^{-1}$ and right multiplication by $a_{\bar{1}}$. This holds even in a non-Abelian group! Thus we see that cyclic shifting takes one solution of $a_{\bar{1}} \ldots a_{\bar{p}} = e$ to another and so P acts on Y also.

By Theorem 1.1, we have $|Y^P| \equiv |Y| \equiv 0 \bmod p$. The final congruence follows as $|Y| = |G|^{p-1}$ which is a multiple of p by our assumptions on $|G|$.

On the other hand we see directly that $Y^P = \{(x, x, \ldots, x) | x \in G, x^p = e\}$ and so $(e, \ldots, e) \in Y^P$. Since $|Y^P| \equiv 0 \bmod p$ and Y^P is not empty we conclude that $Y^P = sp$ for $s \geq 1$. Thus in particular, $Y^P > 1$ and so there exists nontrivial $x \in G$ such that $x^p = e$ and so this x has $o(x) = p$.

□

Example 1.3 (Cauchy's Theorem holds only for primes). *Let $G = \Sigma_3$. Then $|G| = 6$. Since $2||G|$ and $3||G|$, Cauchy's theorem guarantees elements of that order, indeed $o((12)) = 2, o((123)) = 3$. However notice that all elements of G have order $1, 2$ or 3. Thus there is no element of order 6 even though $6||G|$ and so we see that Cauchy's theorem does not hold for composite numbers in general.*

In fact in general a group G has an element of order $|G|$ only if it is cyclic so there are many examples of this phenomenon.

Definition 1.4. *Let p be a fixed prime and $n \in \mathbb{N}$. By unique factorization we may write $n = p^k m$ for unique $k \geq 0, m \in \mathbb{N}, gcd(p, m) = 1$. We write $n_p = p^k$ in this case and $n_{p'} = m$. Thus any natural number may be written uniquely as $n = n_p n_{p'}$ where n_p is a power of p and $n_{p'}$ is relatively prime to p.*

We are now ready to consider an important type of p-subgroup of a given finite group.

Definition 1.5 (Sylow subgroups). *Let G be a finite group. A subgroup $P \leq G$ with $|P| = |G|_p$ is called a Sylow-p subgroup of G. The set of all Sylow-p subgroups of G is denoted $\mathcal{S}yl_p(G)$.*

Thus if $|G| = 24 = 2^3 \cdot 3$ then any subgroup of order 8 is a Sylow-2 subgroup and any subgroup of order 3 is a Sylow-3 subgroup. The unique

Sylow-p subgroup for $p \neq 2, 3$ is the identity subgroup. In general, it is not apriori clear that a finite group has a Sylow-p subgroup for any prime p. That is the content of the next proposition:

Proposition 1.6 (Sylow-p subgroups exist). *Let p be a prime and G be a finite group, then $\mathcal{S}yl_p(G) \neq \emptyset$.*

Proof. We prove this by induction on $n = |G|$. If $n = 1$, the trivial subgroup is the Sylow-p subgroup for all primes p so assume $n > 1$ and that the proposition is proved for all integers $1 \leq k < n$. Without loss of generality assume $p||G|$ as if not the trivial subgroup is the Sylow-p subgroup.

Case 1: Suppose G has a proper subgroup H such that $gcd(p, |G : H|) = 1$. Then $|G| = |H||G : H|$ gives $|G|_p = |H|_p$. Since $|H| < |G|$, by induction, H has a Sylow-p subgroup $P \leq H$. Thus $|P| = |H|_p = |G|_p$ but then it is clear that P is a Sylow-p subgroup for G also so we are done in this case. This leaves us with the following case:

Case 2: All proper subgroups H of G have $p||G : H|$. Now consider the action of G on itself by conjugation. The class formula gives:

$$|G| = |Z(G)| + \sum_{x_j \in J} |G : C_G(x_j)|$$

where J is a set of representatives of the noncentral conjugacy classes.

By our assumption in this case, $p||G : C_G(x_j)|$ for all $j \in J$ so the class equation becomes $0 \equiv |G| \equiv |Z(G)| \bmod p$. Since $e \in Z(G)$, this shows $|Z(G)| = sp$ for some integer $s \geq 1$. By Cauchy's Theorem, we may find $x \in Z(G)$ with $o(x) = p$. Let $H =< x >$ then $|H| = p$ and $H \trianglelefteq G$ as x is central.

Consider the canonical quotient $\phi : G \to G/H$, then $|G/H| = \frac{|G|}{|H|}$ gives $|G/H|_p = \frac{|G|_p}{p}$. Since $|G/H| < |G|$, by induction there exists $\hat{P} \leq G/H$ with $|\hat{P}| = |G/H|_p$. Now $P = \phi^{-1}(\hat{P}) \leq G$ and ϕ induces an isomorphism of P/H and $\hat{P}$ so $|P|/|H| = |G/H|_p$ and so $|P| = p|G/H|_p = |G|_p$ and so P is a Sylow-p subgroup of G and we are done in this case also.

Thus by induction, the proposition is proven.

□

Once again, the reader is warned that the previous theorem does not hold for composite numbers in general. For example later we will see that the alternating group A_4 on 4 letters is a group of order 12 with no subgroup

of order 6. Of course the previous theorem guarantees subgroups of order 4 and 3 exist.

Now that we know that Sylow-p subgroups always exist for any finite subgroup G, we will proceed to figure out how many there are in a given group. We will show in fact that all Sylow-p subgroups are conjugate and hence the isomorphism type of the Sylow-p subgroups of G is unique!

Theorem 1.7 (Sylow Theorems). *Let G be a finite group and p be a prime. Then:*
(a) For any p-subgroup H of G, if H acts on $\mathcal{S}yl_p(G)$ by conjugation then $\mathcal{S}yl_p(G)^H = \{P \in \mathcal{S}yl_p(G) | H \leq P\}$.
(b) $|\mathcal{S}yl_p(G)| \equiv 1$ mod p.
(c) For any p-subgroup H of G, $H \leq P$ for some $P \in \mathcal{S}yl_p(G)$.
(d) If $P, P' \in \mathcal{S}yl_p(G)$ then there exists $g \in G$ such that $P' = gPg^{-1}$. Thus any two Sylow p-subgroups are conjugate.
(e) If $P \in \mathcal{S}yl_p(G)$, then $|\mathcal{S}yl_p(G)| = \frac{|G|}{|N_G(P)|}$ is a divisor of $|G|$ which is relatively prime to p.

Proof. Let $X = \mathcal{S}yl_p(G)$ throughout this proof.
Proof of (a): First note if H is a p-subgroup of G then for any $h \in H, P \in X$, we have $h \cdot P = hPh^{-1} \in X$ as conjugation by h is an automorphism of G and hence $|hPh^{-1}| = |P| = |G|_p$. Thus H indeed does act on X by conjugation.

Now if $P \in X$ has $H \leq P$ then $h \cdot P = hPh^{-1} = P$ and so $P \in X^H$. On the other hand if $P \in X^H$ then $hPh^{-1} = P$ for all $h \in H$ and so $HP = PH$ is a subgroup of G. $|HP| = \frac{|H||P|}{|H \cap P|}$ is a power of p and $P = eP \leq HP$. Thus $P = HP$ as $|P| = |G|_p$. This means $H = He \leq HP = P$ as desired.
Proof of (b): Apply (a) to $H = \hat{P} \in \mathcal{S}yl_p(G)$. (We know $\hat{P}$ exists by the previous theorem.) Thus $X^{\hat{P}} = \{P \in X | \hat{P} \leq P\} = \{\hat{P}\}$. The final equality holds as all Sylow-p subgroups of G have the same order. Thus Theorem 1.1 shows that $|X| \equiv |X^{\hat{P}}| = 1 \bmod p$ as desired.
Proof of (c): Let H be a p-subgroup of G, by Theorem 1.1 and (b) we have $|X^H| \equiv |X| \equiv 1 \bmod p$. Thus in particular $X^H \neq \emptyset$. So by (a), we see that there is $P \in X$ such that $H \leq P$ as desired.
Proof of (d): Let P, P' be two Sylow-p subgroups of G. Let Y be the orbit of P under the G conjugation action, i.e., $Y \subseteq X$ is given by

$$Y = \{gPg^{-1} | g \in G\}.$$

By our basic orbit counting formulas we have $|Y| = |G : N_G(P)|$. Note that $|G : P| = |G : N_G(P)||N_G(P) : P|$ is a number relatively prime to p and so

$|Y| \not\equiv 0 \bmod p$. It is easy to check that P' acts on Y by conjugation and so Theorem 1.1 shows that $|Y^{P'}| \equiv |Y| \not\equiv 0 \bmod p$ and so $Y^{P'} \subseteq X^{P'}$ is not empty. Thus by (a), we see that $P' \leq gPg^{-1}$ for some $g \in G$. Since the two groups have the same order then $P' = gPg^{-1}$ for some $g \in G$ and so we have shown that all Sylow-p subgroups are conjugate and hence of the same isomorphism type.

Proof of (e): From (d) it follows that G acts transitively on X via conjugation. Thus if $P \in X$, then $\mathcal{O}_P = X$ and our basic orbit counting formula gives $|X| = \frac{|G|}{|N_G(P)|}$. We have seen in the proof of (d) that this number is relatively prime to p and it is a divisor of G by Lagrange's Theorem since $N_G(P) \leq G$.

□

Before we can profitably apply the Sylow Theory to study the structure of finite groups, we need to discuss a fundamental construction of group theory:

Definition 1.8 (Semidirect Products). *Let H and K be groups and $\phi : H \to Aut(K)$ be a "gluing" homomorphism. Then the semidirect product of K and H via ϕ is denoted $K \rtimes_\phi H$. As a set it is just the Cartesian product $K \times H = \{(k, h) | k \in K, h \in H\}$. The group binary operation $\star$ is given by:*

$$(k_1, h_1) \star (k_2, h_2) = (k_1 k_2^{\phi(h_1)}, h_1 h_2)$$

where $k_2^{\phi(h_1)} = \phi(h_1)(k_2) \in K$.

It is easy to check that a two-sided identity for $\star$ is given by $e = (e_K, e_H)$ where e_K and e_H are the identity elements of K and H respectively. It is a Homework exercise to show that $\star$ is associative and that $((k^{-1})^{\phi(h^{-1})}, h^{-1})$ is a two sided inverse for (k, h). Thus $\star$ does indeed define a group structure on $K \rtimes_\phi H$.

Let $G = K \rtimes_\phi H$. It is simple to check that $\lambda : K \to G$ given by $\lambda(k) = (k, e_H)$ is a monomorphism. Thus we may identify $Im(\lambda)$ with K and regard $K \leq G$. You will show in a homework exercise that in fact $K \trianglelefteq G$. Similarly it is simple to check that $\mu : H \to G$ given by $\mu(h) = (e_K, h)$ is a monomorphism and so we may identify $Im(\mu)$ with H and regard $H \leq G$.

Since $(k, h) = (k, e_H) \star (e_K, h)$ we have that $G = KH$ and it is clear that $K \cap H = \{e\}$.

The special case when $\phi : H \to Aut(K)$ is the trivial homomorphism, i.e., $\phi(h) = 1_K$ for all $h \in H$ is called the direct product of K and H. In this case it is just denoted $K \times H$ and the group multiplication is just $(k_1, h_1) \star (k_2, h_2) = (k_1 k_2, h_1 h_2)$.

Besides being a useful tool in constructing new groups out of old ones, the semidirect product is a useful tool in analyzing a group in terms of smaller subgroups. This is illustrated in the following fundamental theorem:

Theorem 1.9 (Characterization of semidirect products). *Let G be a group and $H \leq G$, $K \trianglelefteq G$ with $KH = G$ and $K \cap H = \{e\}$. Then $\phi : H \to Aut(K)$ defined by $\phi(h)(k) = hkh^{-1}$ is a homomorphism and the map*

$$\Theta : K \rtimes_\phi H \to G$$

given by $\Theta((k,h)) = kh$ is an isomorphism of groups.

If $H \trianglelefteq G$ also, then ϕ is the trivial homomorphism and $G \cong K \times H$.

Proof. Since K is normal, $\phi(h)(k) = hkh^{-1}$ does indeed define $\phi(h) \in Aut(K)$. It is then easy to check that the assignment $\phi : H \to Aut(K)$ is a homomorphism.

Thus we may define the semidirect product group $K \rtimes_\phi H$ and map Θ as in the statement of the theorem. We now show Θ is an isomorphism:
Surjective: Follows immediately as $G = KH$ by assumption.
Injective: Suppose $\Theta((k_1,h_1)) = \Theta((k_2,h_2))$ then $k_1h_1 = k_2h_2$ and so $k_2^{-1}k_1 = h_2h_1^{-1} \in K \cap H$. Since $K \cap H = \{e\}$ by assumption we have $k_2^{-1}k_1 = h_2h_1^{-1} = e$ which gives $(k_1,h_1) = (k_2,h_2)$. Thus Θ is injective.
Homomorphism: $\Theta((k_1,h_1))\Theta((k_2,h_2)) = k_1h_1k_2h_2 = k_1(h_1k_2h_1^{-1})h_1h_2 = k_1(k_2)^{\phi(h_1)}h_1h_2 = \Theta((k_1,h_1)\star(k_2,h_2))$. Thus Θ is a homomorphism and hence is an isomorphism as we desired to show.

Now suppose $H \trianglelefteq G$ also. Then for $h \in H, k \in K$ consider the commutator $[h,k] = hkh^{-1}k^{-1}$. On one hand since $K \trianglelefteq G$ we have $hkh^{-1} \in K$ and so $[h,k] \in K$ but on the other hand since $H \trianglelefteq G$ we also have $kh^{-1}k^{-1} \in H$ and so $[h,k] \in H$. Thus $[h,k] \in K \cap H = \{e\}$ and $hk = kh$ for all $h \in H, k \in K$. Hence the gluing map $\phi(h)(k) = hkh^{-1} = k$ and so $\phi(h) = 1_K$ for all $h \in H$ and $K \rtimes_\phi H$ is just the direct product $K \times H$. Hence the proof is complete. □

We are now ready to look at some examples of Sylow analysis. One final comment about semidirect products before we do so: If $H \cong \hat{H}$ and $K \cong \hat{K}$ then given a semidirect product $K \rtimes_\phi H$ there is a suitable gluing map $\hat{\phi} : \hat{H} \to Aut(\hat{K})$ such that $K \rtimes_\phi H \cong \hat{K} \rtimes_{\hat{\phi}} \hat{H}$ and so we will typically not worry about replacing the groups H and K in a semidirect product with isomorphic groups.

The following is a typical numerical example of Sylow analysis:

Example 1.10 (Classifying groups of order 6.). *Let G be a group with $|G| = 6 = 2 \cdot 3$. Let P be a Sylow-2 subgroup and Q be a Sylow-3 subgroup. Thus $|P| = 2, |Q| = 3$ so $P \cong \mathbb{Z}/2\mathbb{Z}$ and $Q \cong \mathbb{Z}/3\mathbb{Z}$. Now by Theorem 1.7 we have $|\mathcal{S}yl_3(G)| = 1$ or 2 as these are the only divisors of $|G|$ relatively prime to 3. However as $2 \not\equiv 1 \mod 3$, we see that this case is impossible again by Theorem 1.7. Thus there is a unique Sylow-3 subgroup P which is therefore normal in G. (Since any conjugate of a Sylow-p subgroup is a Sylow-p subgroup.)*

Note that $P \cap Q = \{e\}$ since any element in $P \cap Q$ must have order dividing both 2 and 3 and hence must have order 1.

Since $P \trianglelefteq G$, PQ is a subgroup of G and $|PQ| = \frac{|P||Q|}{|P \cap Q|} = \frac{2 \cdot 3}{1} = 6 = |G|$ and so $G = PQ$.

Thus by Theorem 1.9, $G \cong P \rtimes_\phi Q \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$ for some gluing homomorphism $\psi : \mathbb{Z}/2\mathbb{Z} \to Aut(\mathbb{Z}/3\mathbb{Z})$. We have seen in homework that $|Aut(\mathbb{Z}/3\mathbb{Z})| = 2$ and so there are only two possibilities for ψ:

Case (A): *ψ is the trivial homomorphism. In this case $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. The final isomorphism follows as $(1, 1)$ has order 6 in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and so must generate this group which is therefore cyclic.*

Case (B): *ψ is an isomorphism. This provides the only other possible isomorphism type of a group of order 6. It must therefore be Σ_3 and so $\Sigma_3 \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$.*

Thus we conclude that the only two groups of order 6 up to isomorphism are $\mathbb{Z}/6\mathbb{Z}$ and Σ_3. These two are clearly not isomorphic as one is Abelian and the other isn't.

One thing should be mentioned about the analysis above. Apriori there are $6^{36} \sim 10^{28}$ different binary operations on a set of size 6. (This is because for each of the 36 ordered pairs from the set we have to assign a product for which there are 6 choices.) Fixing an identity element, there are still $6^{25} \sim 3 \times 10^{19}$ possibilities roughly. A naive analysis would have to figure out which of these possibilities was associative with inverses and then determine which remaining things on the list are isomorphic and which are not. Notice how much less daunting the analysis was with a little bit of theory!!

We now do some more general analysis:

Proposition 1.11 (Groups of order pq). *Let $p < q$ be primes and let G be a group with $|G| = pq$. If $q \not\equiv 1 \mod p$ then $G \cong \mathbb{Z}/pq\mathbb{Z}$. If $q \equiv 1 \mod p$ then $G \cong (\mathbb{Z}/q\mathbb{Z}) \rtimes_\phi (\mathbb{Z}/p\mathbb{Z})$ for some gluing homomorphism $\phi : \mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$.*

Proof. By Theorem 1.7, $|\mathcal{S}yl_q(G)| = 1$ or p. However as $1 < p < q$ we see that $p \not\equiv 1 \bmod q$ and so there must be a unique normal Sylow-q subgroup Q. Let P be a Sylow p-subgroup. Then $P \cap Q = \{e\}$ as anything in the intersection must have order dividing both p and q and hence must have order 1. A simple count then shows $|PQ| = \frac{|P||Q|}{|P \cap Q|} = |G|$ and so

$$G \cong Q \rtimes_{\hat{\phi}} P \cong \mathbb{Z}/q\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/p\mathbb{Z}$$

by Theorem 1.9.

Similarly $|\mathcal{S}yl_p(G)| = 1$ or q. If $q \not\equiv 1 \bmod p$ then there must be a unique normal Sylow p subgroup P also and so $G \cong Q \times P \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by Theorem 1.9. Note that $(1, 1)$ has order pq in $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and so this group is cyclic of order pq. Thus $\mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$ and we are done. □

We will see in the future that in the case $q \equiv 1 \bmod p$, there are exactly two distinct semidirect products $\mathbb{Z}/q\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/p\mathbb{Z}$ up to isomorphism. One is the direct product where ϕ is the trivial homomorphism and the other one is a non-Abelian group corresponding to a monomorphism $\mathbb{Z}/p\mathbb{Z} \to Aut(\mathbb{Z}/q\mathbb{Z})$. (We will see that there is a unique cyclic subgroup of order p in $Aut(\mathbb{Z}/q\mathbb{Z})$ which gives us essentially only one nontrivial gluing map possibility.)

We will conduct one more example of Sylow analysis that illustrates a typical counting argument to eliminate one case:

Proposition 1.12 (Groups of order p^2q). *Let p, q be distinct primes and G be a group of order p^2q. Let P be a Sylow p subgroup and Q be a Sylow q subgroup then P is Abelian and Q is cyclic.*

If $q \not\equiv 1 \bmod p$ (For example when $q < p$) then $G \cong P \rtimes_{\phi} Q$.

If $q \equiv 1 \bmod p$ then either $G \cong P \rtimes_{\phi} Q$ or $G \cong Q \rtimes_{\phi} P$.

Thus in all cases, at least one of the Sylow subgroups is normal and G is the semidirect product of two Abelian groups.

Proof. Let P,Q be as in the statement of the proposition. Then P is Abelian as any group of order p^2 is Abelian. Note that in general $P \cap Q = \{e\}$ by considering the order of elements in the intersection. If one of P, Q is normal, then $|PQ| = |G|$ by the usual count and so G is the semidirect product of P and Q. (The type depending on which one is normal.)

So basically all we have to do is show that in all cases we have a normal Sylow subgroup.

Now $|\mathcal{S}yl_p(G)| = 1$ or q. If $q \not\equiv 1 \bmod p$ then Theorem 1.7 shows that we have a unique normal Sylow p subgroup. Thus $G \cong P \rtimes_\phi Q$ as discussed above.

If $q \equiv 1 \bmod p$ then in particular $q > p$ and both possibilities for $|\mathcal{S}yl_p(G)|$ can occur. Now $|\mathcal{S}yl_q(G)| = 1, p$ or p^2. Since $q > p$ in this case, $p \not\equiv 1 \bmod q$ and so that possibility is impossible. If there were a unique Sylow q subgroup then $G \cong Q \rtimes_\phi P$ and we would be done so assume then that there are p^2 Sylow q subgroups.

Counting elements of order q we see that each Sylow q subgroup has $q-1$ such elements. However distinct Sylow q subgroups cannot share any elements of order q and so we see that we have $p^2(q-1) = |G| - p^2$ elements of order q in G. Now any Sylow p subgroup has order p^2 and consists of elements relatively prime to q and so we see that there are only enough elements left in G to make one Sylow p subgroup.

Thus in the case where there is not a unique Sylow q subgroup, there is a unique normal Sylow p subgroup and G is hence a semidirect product $G \cong P \rtimes_\phi Q$.

Thus we are done in all cases.

□

2 Simple Groups

Sylow theory provides us a method to find nontrivial proper normal subgroups N of a given group G. Once we have a normal subgroup, we can understand G through the smaller groups N and G/N. Thus for most groups we can break down the study of the group into that of smaller associated groups.

However eventually this process stops and we reach pieces which cannot be decomposed any further. These are the fundamental "building blocks" for groups and are defined next:

Definition 2.1 (Simple Groups). *A group G with $|G| > 1$ is called simple if there do not exist any normal subgroups N of G besides $N = \{e\}$ and $N = G$. (We say there do not exist any proper nontrivial normal subgroups.)*

Example 2.2 (Abelian simple groups are $\mathbb{Z}/p\mathbb{Z}$ for p a prime). *Let A be an Abelian simple group with $|A| > 1$. Let x be a nonidentity element in A then $< x >$ is a nontrivial subgroup of A which is automatically normal as*

A is Abelian. Thus since A is simple, $A =< x >$ is cyclic. If A were infinite cyclic then $< x^2 >$ is a proper nontrivial normal subgroup so A has to be a finite cyclic group. Let p be a prime such that $p||A|$.

Now Cauchy's Theorem shows that A has an element y of order p and again by simplicity, $A =< y >$. Thus $A \cong \mathbb{Z}/p\mathbb{Z}$.

We have thus seen that the only Abelian simple groups are the cyclic groups of prime order.

Example 2.3 (There are no nonAbelian simple groups of order p^k, pq, p^2q for primes p,q and integer $k \geq 1$). *If G is a nonAbelian p-group with $|G| > 1$, then $\{e\} \neq Z(G) \neq G$ as centers of nontrivial p-groups are never trivial. Since $Z(G) \trianglelefteq G$, this shows that G is never simple.*

If $G = pq$ or p^2q then we have seen in the previous propositions that G contains a proper nontrivial Sylow subgroup which is normal. Thus G is never simple in this case either.

Indeed the smallest example of a nonAbelian simple group is a group of order $60 = 2^2 \cdot 3 \cdot 5$ called A_5, the alternating group on 5 letters. We will study this group in the next section. You will show in future homework that there are no nonAbelian simple groups of order less than 60.