

## MATH 30A: CHAPTER 24

### 24. SYLOW THEOREMS

This chapter proves the Sylow Theorems and gives many applications. The chapter also discusses conjugacy classes and the class equation.

**24.1. Class formula.** On the first day we talked about the relationship between the conjugacy class of an element and the centralizer of the element. After a long discussion I got you guys to give me the formula.

24.1.1. *conjugacy classes.*

**Definition 24.1.** *The conjugacy class  $cl(x)$  of an element  $x \in G$  is the set of all conjugates of  $x$ :*

$$cl(x) = \{gxg^{-1} \mid g \in G\}$$

Recall that the *centralizer* of  $x$  is the set of all elements of  $G$  which commute with  $x$ :

$$C(x) = \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}$$

The formula relating these is

**Lemma 24.2** (Lemma 9.8). *There is a 1-1 correspondence between the set of conjugates of  $x$  in  $G$  and the left cosets of the centralizer:*

$$\phi : G/C(x) \xrightarrow{\sim} cl(x)$$

*given by  $\phi(gC(x)) = gxg^{-1}$ .*

This is not hard to prove. The main point is to show that the function  $\phi$  is *well defined*: If a left coset can be written in two different ways then the formula should give the same value:

$$gC(x) = hC(x) \iff gxg^{-1} = h x h^{-1}$$

A consequence of this is that the number of conjugates of  $x$  is equal to the index of its centralizer:

$$|cl(x)| = |G : C(x)|$$

I gave two examples to show what happens.

---

*Date:* November 9, 2006.

24.1.2. *symmetric group*. First take the symmetric group  $S_3$ . This has  $m = 3$  conjugacy classes:

$$\begin{aligned} cl(x_1) &= \{e\} & x_1 &= e \\ cl(x_2) &= \{(12), (23), (13)\} & x_2 &= (12) \\ cl(x_3) &= \{(123), (132)\} & x_3 &= (123) \end{aligned}$$

The elements  $x_1 = e, x_2 = (12), x_3 = (123)$  are *representatives* of the conjugacy classes. You choose one from each set. I made this chart:

$x_i$	$e$	$(12)$	$(123)$
$ cl(x_i) $	1	3	2
$ C(x_i) $	6	2	3

The lemma says that the product of the numbers in each column is  $|S_3| = 6$ . I pointed out that the first row of numbers add up the the order of the group:

$$1 + 3 + 2 = 6 = |S_3|$$

This is because the group is a disjoint union of conjugacy classes:

$$G = \coprod_{i=1}^m cl(x_i)$$

The second row of numbers have the property that their inverses add up to 1:

$$\frac{1}{6} + \frac{1}{2} + \frac{1}{3} = 1$$

24.1.3. *dihedral group*. Next I did the dihedral group

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

This has  $m = 5$  conjugacy classes

$$\begin{aligned} cl(x_1) &= \{e\} & x_1 &= e \\ cl(x_2) &= \{r^2\} & x_2 &= r^2 \\ cl(x_3) &= \{r, r^3\} & x_3 &= r \\ cl(x_4) &= \{s, sr^2\} & x_4 &= s \\ cl(x_5) &= \{sr, sr^3\} & x_5 &= sr \end{aligned}$$

Here is the chart:

$x_i$	$e$	$r^2$	$r$	$s$	$sr$
$ cl(x_i) $	1	1	2	2	2
$ C(x_i) $	8	8	4	4	4

Again the first row adds up to the order of the group

$$1 + 1 + 2 + 2 + 2 = |D_4| = 8$$

and the sum of inverses of the second row adds up to 1:

$$\frac{1}{8} + \frac{1}{8} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$$

Why is that?

24.1.4. *class equation.*

**Theorem 24.3** (class equation, 1st form). *The order of a finite group  $G$  is the sum of the indices of the centralizers of the representatives  $x_i$  of the conjugacy classes of  $G$ :*

$$|G| = \sum_{i=1}^m |G : C(x_i)|$$

*Proof.* This just follows from the lemma:

$$|G| = \sum |cl(x_i)| = \sum |G : C(x_i)|$$

□

On the second day I refined this equation by asking: When is this number equal to 1?

$$|cl(x)| = |G : C(x)| = 1 \iff x \in Z(G)$$

This happens only when  $x$  is central. Each element in the center of  $G$  is its own conjugacy class and each element contributes 1 to the class equation. The other conjugacy classes are bigger and contribute numbers bigger than 1:

$$|G| = |Z(G)| + \sum_{i=r+1}^m \underbrace{|G : C(x_i)|}_{>1}$$

This is the second form of the class equation.

24.2. **p-groups.** I used the class equation to prove that the center of any p-group is nontrivial.

**Definition 24.4.** *A finite group  $G$  is called a p-group if its order is a power of a prime  $p$ :*

$$|G| = p^k$$

*An infinite group is called a p-group if the order of each element is a power of  $p$ .*

**Theorem 24.5.** *A finite nontrivial p-group has a nontrivial center.*

*Proof.* The equation:

$$|G| = p^k = |C(x_i)| \cdot |G : C(x_i)|$$

implies that the index  $|G : C(x_i)|$  must be a power of  $p$ . In the equation:

$$|G| = |Z(G)| + \sum |G : C(x_i)|$$

the terms in the sum are all at least 2. So they are divisible by  $p$ . Since  $|G|$  is also divisible by  $p$  this implies that  $|Z(G)|$  is divisible by  $p$ . But  $|Z(G)| \geq 1$  since  $e \in Z(G)$ . So,  $|Z(G)| \geq p$  and the center  $Z(G)$  must be nontrivial.  $\square$

**24.3. First Sylow theorem.** I explained the first Sylow theorem and proved half of it. But here is the whole proof. The theorem says that every finite group has a Sylow  $p$  subgroup.

24.3.1. *the theorem.*

**Theorem 24.6** (1st Sylow Theorem). *Suppose that  $|G| = p^k s$  where  $p$  does not divide  $s$ . Then  $G$  has a subgroup of order  $p^k$ . Any such subgroup is called a  $p$ -Sylow subgroup of  $G$ .*

*Proof.* By induction of  $|G|$  we assume that the theorem holds for all smaller groups. (It holds when  $|G| = 1$ .) We look at the class equation:

$$|G| = p^k s = |Z(G)| + \sum |G : C(x_i)|$$

There are two cases. Either  $p$  divides every index  $|G : C(x_i)|$  or there is at least one index  $|G : C(x_i)|$  which is not divisible by  $p$ . (I gave two examples to illustrate. See below.)

Case 2 If one of numbers  $|G : C(x_i)|$  is not divisible by  $p$  then, since

$$|G| = p^k s = |G : C(x_i)| \cdot |C(x_i)|$$

it follows that  $p^k$  divides  $|C(x_i)|$ . But,  $C(x_i)$  has index  $\geq 2$  in  $G$  and is therefore smaller than  $G$ . So, by induction,  $C(x_i)$  has a  $p$ -Sylow subgroup  $P$  with  $|P| = p^k$ . But

$$P \leq C(x_i) \leq G$$

So,  $P$  is also a  $p$ -Sylow subgroup of  $G$ .

Case 1 If all of the numbers  $|C(x_i)|$  are divisible by  $p$  then so is  $|Z(G)|$ . This means that  $Z(G)$  has an element  $z$  of order  $p$ . Let  $N = \langle z \rangle$ . Then,  $N$  is normal in  $G$  (any central subgroup is normal). The factor group  $G/N$  has order  $|G|/|N| = p^{k-1}s$ . So, by induction on  $G$

it contains a subgroup of order  $p^{k-1}$ . This subgroup has the form  $H/N$  where  $H$  is a subgroup of  $G$  containing  $N$ . But then

$$|H| = |N| \frac{|H|}{|N|} = p \cdot p^{k-1} = p^k$$

So,  $H$  is a  $p$ -Sylow subgroup of  $G$ . □

24.3.2. *examples.* First, I took the group  $S_4$  which also has  $24 = 2^3 \cdot 3$  elements and I took  $p = 2$ . This has 5 conjugacy classes only one of which is central:

$$|S_4| = 24 = 1 + (6 + 8 + 6 + \mathbf{3})$$

Here one of the numbers  $|G : C(x_i)|$  is not divisible by  $p = 2$ . This is an example of Case 2. The element  $x_5 = (12)(34)$  has exactly 3 conjugates (including itself). So, the order of its centralizer is

$$|C(x_5)| = \frac{|G|}{|cl(x_5)|} = \frac{24}{3} = 8$$

So,  $C(x_5)$  is a 2-Sylow subgroup of  $S_4$ .

Then I took the dihedral group  $D_4$  which has 5 conjugacy classes. The class equation gives:

$$\begin{aligned} |D_4| &= |Z(G)| + \sum |G : C(x_i)| \\ 8 &= 2 + (2 + 2 + 2) \end{aligned}$$

This is an example of Case 1 where all the numbers on the right are divisible by  $p = 2$ .

24.4. **Group actions.** In order to prove the other two Sylow theorems I need the orbit-stabilizer formula. So, I discussed group actions on sets and the signed permutation group (which has nothing to do with Sylow).

24.4.1. *signed permutations.* I pointed out that the rotation group of the cube is given by a set of  $3 \times 3$  matrices. For example rotation by 90 degrees about the  $z$ -axis is given by the matrix

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

This is called a *signed permutation matrix*

**Definition 24.7.** A permutation matrix is an  $n \times n$  matrix having  $n$  1's and all the rest 0's where there is exactly one 1 in every row and every column. (If you play chess think of these as 8 rooks which cannot take each other.)

There are exactly  $n!$  permutation matrices and the group of  $n \times n$  permutation matrices is isomorphic to the symmetric group  $S_n$ . The isomorphism is given by

$$\phi(\sigma) = (e_{\sigma(1)}, e_{\sigma(2)}, \dots, e_{\sigma(n)})$$

**Definition 24.8.** A signed permutation matrix is an  $n \times n$  matrix having  $n$   $\pm 1$ 's and all the rest 0's where there is exactly one  $\pm 1$  in every row and every column.

The signed permutation group can be written:  $\mathbb{Z}_2 \int S_n$  (wreath product of  $\mathbb{Z}_2$  and  $S_n$ ). This notation just means that we take  $n \times n$  permutation matrices and substitute elements of  $\mathbb{Z}_2$  for the 1's. Since I am putting  $\pm 1$  it might be more correct to write  $\{1, -1\} \int S_n$  but people usually write  $\mathbb{Z}_2$  instead of  $\{1, -1\}$ . Anyway,

$$|\mathbb{Z}_2 \int S_n| = 2^n n!$$

In particular,

$$|\mathbb{Z}_2 \int S_3| = 2^3 3! = 48$$

The rotation group of the cube (isomorphic to  $A_4$  with 12 elements) is a subgroup of this group with index 4.

#### 24.4.2. orbit-stabilizer.

**Definition 24.9.** A group  $G$  acts on a set  $X$  if for every  $g \in G$  and  $x \in X$  there is an element

$$gx \in X$$

so that

- (1)  $ex = x$
- (2)  $g(hx) = (gh)x$

Sometime I write  $g \cdot x$  to emphasize that this is an *action* of  $g$  on  $x$ .

**Definition 24.10.** The stabilizer  $H_{x_0}$  of  $x_0 \in X$  is the set of all elements of the group which fix  $x_0$

$$H_{x_0} := \{g \in G \mid gx_0 = x_0\}$$

**Definition 24.11.** The orbit  $orb(x_0)$  of  $x_0$  is the set

$$orb(x_0) := \{gx_0 \mid g \in G\}$$

**Theorem 24.12** (orbit-stabilizer). The size of the orbit is the index of the stabilizer:

$$|orb(x)| = |G : H_x|$$

*Proof.* There is a 1-1 correspondence between the set of left cosets of  $H_x$  and the orbit of  $x$ :

$$\phi : G/H_x \xrightarrow{\cong} orb(x)$$

this bijection is given by  $\phi(gH_x) = gx$ . You can check simultaneously that it is well-defined and 1-1:

$$gH_x = hH_x \iff g^{-1}h \in H_x \iff g^{-1}hx = x \iff hx = gx$$

the map is onto since the elements of the orbit are  $gx = \phi(gH_x)$ .  $\square$

24.4.3. *examples.* The first example I gave was the group  $S_4$  acting on the regular tetrahedron with vertices labeled 1, 2, 3, 4. I took one point  $x_0$  which was one the edge connecting vertices 1 and 2 but closer to 1 than to 2. I took another point  $x_1$  in the center of the edge connecting vertices 1 and 2. The group  $S_4$  moved the point  $x_0$  to 12 points three around each of the four vertices. These 12 points form the orbit of  $x_0$ . Since  $S_4$  has 24 elements, the orbit stabilizer equation predicts that the stabilizer of  $x_0$  will have exactly  $24/12 = 2$  elements. Looking closely at the tetrahedron we see that the stabilizer of  $x_0$  is

$$H_{x_0} = \{e, (34)\}$$

The point  $x_1$  has 6 elements in its orbit. These are the midpoints of the 6 edges. So, the stabilizer of  $x_1$  should have  $24/6 = 4$  elements. And it does:

$$H_{x_1} = \{e, (34), (12), (12)(34)\}$$

Now take a vertex  $v$ . What is the orbit of  $v$  and what is its stabilizer?

Another example: take the group  $S_n$  which acts on the set  $X = \{1, 2, \dots, n\}$ . What is the orbit of  $n$ ? What is the stabilizer of  $n$ ?

24.4.4. *permuting subgroups.* Let  $X$  be the set of all subgroups of  $G$ . Then  $G$  acts on the set  $X$  by conjugation:

$$g \cdot H := gHg^{-1}$$

This is an action:

- (1)  $e \cdot H = eHe^{-1} = H$
- (2)  $g \cdot (h \cdot H) = ghHh^{-1}g^{-1} = (gh)H(gh)^{-1} = (gh) \cdot H$

Take an element  $H \in X$ . This is a subgroup of  $G$ . What is the stabilizer of this element? By definition it is

$$stab(H) = \{g \in G \mid g \cdot H = H\}$$

but  $g \cdot H = gHg^{-1}$ . This is equal to the subgroup  $H$  iff  $g \in N(H)$ . So, the stabilizer of  $H$  considered as one point in  $X$  is equal to the

normalizer of  $H$  considered as a subgroup of  $G$ . What is the orbit of the point  $H$ ? This is just the set of subgroups

$$\text{orb}(H) = \{gHg^{-1} \mid g \in G\} \subset X$$

Notice that, in the orbit, these subgroups  $gHg^{-1}$  are considered as points.

The orbit of  $H$  has one element if and only if  $H$  is normal:

$$|\text{orb}(H)| = 1 \iff H \triangleleft G$$

Why is that?

**24.5. Sylow's other theorems.** We need to know when a  $p$ -Sylow subgroup  $P$  is normal in  $G$ .

24.5.1. *normal Sylow subgroups.*

**Lemma 24.13.** *If  $H$  is a  $p$ -group and  $\phi : H \rightarrow K$  is a homomorphism from  $H$  to some other group  $K$  then both the kernel of  $\phi$  and the image of  $\phi$  are  $p$ -subgroups.*

*Proof.*

$$|H| = p^j = |\ker \phi| \cdot |\phi(H)|$$

So, both  $|\ker \phi|$  and  $|\phi(H)|$  must be powers of  $p$ .  $\square$

**Theorem 24.14.** *Suppose that  $P$  is a normal  $p$ -Sylow subgroup of a finite group  $G$ . (So,  $|G| = p^k s$  and  $|P| = p^k$ .) Then*

- (a)  $P$  contains every  $p$ -subgroup of  $G$ .
- (b)  $P$  is the only  $p$ -Sylow subgroup of  $G$ .

*Proof.* If  $P \triangleleft G$  then the quotient group  $G/P$  is a group with  $s$  elements and we have a homomorphism

$$\phi : G \rightarrow G/P$$

with kernel  $P$ . If  $H$  is any  $p$ -subgroup of  $G$  then  $\phi(H)$  is a  $p$ -subgroup of  $G/P$ . But  $|G/P|$  is not divisible by  $p$ . So, the only  $p$ -subgroup of  $G/P$  is the trivial group  $\{eP\}$ . So,  $H$  is contained in the kernel of  $\phi$  which is  $P$ . This proves (a). If  $H$  is a  $p$ -Sylow subgroup then  $H \leq P$  by (a) and  $H = P$  since they have the same size. This shows (b).  $\square$

Conversely, if  $P$  is the only  $p$ -Sylow subgroup then it must be normal. Why is that?

In general, when  $P$  is not normal in  $G$ , we at least know that  $P$  is normal in its normalizer:  $P \triangleleft N(P)$ . So, the theorem can be applied to  $N(P)$  instead of  $G$ :

**Corollary 24.15.** *Suppose that  $P$  is any  $p$ -Sylow subgroup of a finite group  $G$ . Then*

- (a)  $P$  contains every  $p$ -subgroup of  $N(P)$ .
- (b)  $P$  is the only  $p$ -Sylow subgroup of  $N(P)$ .

Now we are ready to prove the other two Sylow theorems.

24.5.2. *Sylow's third thm.*

**Lemma 24.16.** *Every conjugate  $gPg^{-1}$  of a  $p$ -Sylow subgroup is also a  $p$ -Sylow subgroup of  $G$ .*

*Proof.*  $gPg^{-1} \cong P$ . So, it has  $p^k$  elements. So, it is a Sylow subgroup. □

**Theorem 24.17** (Sylow's 3rd). (1) *The number of  $p$ -Sylow subgroups of a finite group is congruent to 1 modulo  $p$ .*  
 (2) *Any two  $p$ -Sylow subgroups of  $G$  are conjugate.*

*Proof.* Let  $X$  be the set of all  $p$ -Sylow subgroups of  $G$ . If  $P$  is a  $p$ -Sylow subgroup. Then  $P$  is one point in  $X$  and  $P$  is also a group which acts on  $X$  by conjugation. Let  $Q \in X$  be another point. Then the  $P$ -orbit of  $Q$  and the  $P$ -stabilizer of  $Q$  are

$$orb_P(Q) := \{gQg^{-1} \mid g \in P\}$$

$$stab_P(Q) := \{g \in P \mid gQg^{-1} = Q\}$$

The orbit-stablizer formula says

$$|orb_P(Q)| \cdot |stab_P(Q)| = |P| = p^k$$

So, both  $|orb_P(Q)|$  and  $|stab_P(Q)|$  are powers of  $p$ .

When is  $|orb_P(Q)| = 1$ ?

$$\begin{aligned} |orb_P(Q)| = 1 &\iff |stab_P(Q)| = p^k \\ &\iff gQg^{-1} = Q \forall g \in P \\ &\iff P \leq N(Q) \\ &\iff P = Q \quad (Q \text{ is the only } p\text{-Sylow subgrp of } N(Q).) \end{aligned}$$

Thus there is only one orbit of size 1 (when  $Q = P$ ). All other orbits have  $p^j, j \geq 1$  elements. So,

$$|X| = \sum |orb_P(Q_i)| \equiv 1 \pmod{p}$$

This proves (1).

The same argument proves (2)! Suppose that not all  $p$ -Sylow subgroups are conjugate. Then

$$X = X_0 \amalg X_1$$

where  $X_0$  is the set of all  $p$ -Sylow subgroups conjugate to  $P$  and  $X_1$  are the other  $p$ -Sylow subgroups. The above argument with  $X$  replaced by  $X_0$  shows

$$|X_0| \equiv 1 \pmod{p}$$

Similarly,

$$|X_1| \equiv 1 \pmod{p}$$

So,

$$|X| = |X_0| + |X_1| \equiv 2 \pmod{p}$$

This is a contradiction. So, all  $p$ -Sylow subgroups must be conjugate.  $\square$

### 24.5.3. Sylow's second thm.

**Theorem 24.18** (Sylow's 2nd). *Suppose that  $|G| = p^k s$  where  $p$  does not divide  $s$ . Then any  $p$ -subgroup  $H$  of  $G$  is contained in a  $p$ -Sylow subgroup.*

*Proof.* Again let  $X$  be the set of  $p$ -Sylow subgroups of  $G$ . The group  $H$  with  $|H| = p^j$  acts on  $X$  by conjugation. For each  $Q \in X$ ,

$$|\text{orb}_H(Q)| \cdot |\text{stab}_H(Q)| = |H| = p^j$$

So,  $|\text{orb}_H(Q)|$  is a power of  $p$ . Since

$$\sum |\text{orb}_H(Q_i)| = |X| \equiv 1 \pmod{p}$$

there must be at least one point  $Q_0 \in X$  whose orbit has size  $|\text{orb}_H(Q_0)| = 1$ . But, as in the proof of the 3rd thm,

$$|\text{orb}_H(Q_0)| = 1 \iff H \leq N(Q_0)$$

By Corollary 24.15 (b),  $H$  is a subgroup of  $Q_0$  which is a  $p$ -Sylow subgroup of  $G$ .  $\square$

**24.6. Applications.** We need several lemmas before we do the examples in the book.

24.6.1. *normal Sylow subgroups.* What we already know from Theorem 24.14(b) is

**Theorem 24.19.** *Suppose that  $P$  is a  $p$ -Sylow subgroup of a finite group  $G$ . Then  $P$  is normal in  $G$  if and only if  $P$  is the only  $p$ -Sylow subgroup of  $G$ .*

Another fact that we need is:

**Lemma 24.20.** *If the Sylow subgroups  $P_{p_i}$  of  $G$  are all normal then  $G$  is the internal direct product of its Sylow subgroups*

$$G = \bigoplus P_{p_i}$$

*Proof.* I gave the proof in the case where there are only two primes dividing the order of  $G$ . So,  $G = p^a q^b$ . Suppose  $P, Q$  are the Sylow subgroups corresponding to  $p, q$ . Then  $P \triangleleft G, Q \triangleleft G, P \cap Q = \{e\}$  and  $PQ = G$ . So  $G = P \oplus Q$  proving the lemma.

The reason that  $PQ = G$  is by counting the number of elements:

$$|PQ| = \frac{|P| \cdot |Q|}{|P \cap Q|} = \frac{p^a q^b}{1} = |G|$$

□

#### 24.6.2. counting Sylow subgroups.

**Lemma 24.21.** *Suppose that  $H$  is any subgroup of  $G$ . Then the number of conjugates of  $H$  is equal to the index of its normalizer.*

*Proof.* This is an example of the orbit-stabilizer formula. Think of  $H$  as one point in the set  $X$  of all subgroups of  $G$ . Then

$$|\text{orb}(H)| = \text{number of conjugates of } H$$

$$\text{stab}(H) = N(H)$$

The orbit-stabilizer equation says

$$|\text{orb}(H)| \cdot |\text{stab}(H)| = |G|$$

or:

$$|\text{orb}(H)| = \frac{|G|}{|\text{stab}(H)|} = \frac{|G|}{|N(H)|} = |G : N(H)|$$

□

**Lemma 24.22.** *The number of  $p$ -Sylow subgroups of  $G$  is equal to the index of the normalizer of a  $p$ -Sylow subgroup.*

*Proof.* This follows from the previous lemma and the 3rd Sylow theorem which says that all  $p$ -Sylow subgroups are normal. □

#### 24.6.3. groups of order $pq$ .

**Lemma 24.23.** *If  $p < q$  are distinct primes, then any group of order  $pq$  has a normal  $q$ -Sylow subgroup.*

*Proof.* Let  $Q$  be a  $q$ -Sylow subgroup of  $G$ . Look at the Hasse diagram where the numbers on the edges indicate the indices  $a = |G : N(Q)|, b = |N(Q) : Q|$

$$\begin{array}{c} G \\ \backslash a \\ N(Q) \\ / b \\ Q \end{array}$$

Since  $ab = |G : Q| = p$ , either  $a = 1$  or  $a = p$ . But, Sylow's 3rd thm says that

$$a = |N(Q) : Q| \equiv 1 \pmod{q}$$

And  $p \not\equiv 1$ . So,  $a = 1$  which means that  $G = N(Q)$  which implies that  $Q \triangleleft G$  as claimed.  $\square$

**Theorem 24.24.** *Suppose that  $p < q$  are prime numbers so that  $q \not\equiv 1 \pmod{p}$ . Then any group of order  $pq$  is cyclic.*

*Proof.* We have  $|G| = pq$  with Sylow subgroups  $P, Q$  of order  $p, q$  respectively. The lemmas says that  $Q \triangleleft G$ . What about  $P$ ? Look at the diagram

$$\begin{array}{c} G \\ \backslash a \\ N(P) \\ / b \\ P \end{array}$$

Since  $ab = |G : P| = q$ , either  $a = 1$  or  $a = q$ . But, Sylow's 3rd thm says that  $a \equiv 1 \pmod{p}$ . So,  $a = 1$  and  $P \triangleleft G$ . Since both Sylow subgroups are normal we have

$$G = P \oplus Q \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

$\square$

**Example 24.25.** *Groups of order  $3 \cdot 5 = 15$  and  $3 \cdot 11 = 33$  are cyclic.*

24.6.4. *groups of order  $p^2q$ .*

**Theorem 24.26.** *Suppose that  $p, q$  are distinct primes,  $p \not\equiv \pm 1 \pmod{q}$  and  $q \not\equiv 1 \pmod{p}$ . Then any group of order  $p^2q$  is abelian.*

*Proof.* We have a group  $G$  of order  $p^2q$  and Sylow subgroups  $P, Q$  of orders  $|P| = p^2, |Q| = q$ . Since groups of order  $4p^2$  are abelian, both  $P$  and  $Q$  are abelian. As before,  $P$  must be normal since  $q \not\equiv 1 \pmod{p}$ . What about  $Q$ ? The index of the normalizer of  $Q$  must divide  $|G : Q| = p^2$ . So,  $|G : N(Q)| = a = 1, p$  or  $p^2$ . But  $p \not\equiv 1$  and  $p^2 \not\equiv 1$

mod  $q$  because of the assumption that  $p \not\equiv \pm 1 \pmod q$ . Therefore,  $Q$  is also normal. So,

$$G = P \oplus Q$$

is abelian. □

**Example 24.27.** *Groups of order  $3^2 \cdot 5 = 45$  and  $3^2 \cdot 11 = 99$  are abelian.*

We discussed the idea of generalizing this to  $p^3q$ . But the condition we would need is  $p^3 \not\equiv 1 \pmod q$ . It often happens that there are three solutions to the equation  $x^3 \equiv 1 \pmod q$ . For example the numbers 1, 2, 4 are cube roots of 1 modulo 7. ( $U(7)$  is a group of order 6 and therefore has an element of order 3.)

24.6.5. *groups of order 66.*

**Theorem 24.28.** *There are exactly 4 groups of order 66 (up to isomorphism). Namely:*

$$\mathbb{Z}_{66}, \quad D_{33}, \quad S_3 \oplus \mathbb{Z}_{11}, \quad D_{11} \oplus \mathbb{Z}_3$$

*Proof.* Since  $66 = 11 \cdot 3 \cdot 2$ , we have Sylow subgroups  $P, Q, R$  of order 11, 3, 2 respectively. The index of the normalizer of  $P$  divides 6. So it is 6, 3, 2 or 1. Since this number must be congruent to 1 modulo 11, it must be 1 and we conclude that  $P \triangleleft G$ .

Now take  $H = PQ$ . (The product of a normal subgroup and a subgroup is a subgroup.) This has order 33 and is therefore normal since subgroups of index 2 are normal:  $PQ \triangleleft G$ . We know that groups of order 33 are cyclic. Therefore,  $PQ \cong \mathbb{Z}_{33}$ . Pick a generator  $r$ . Then

$$PQ = \{e, r, r^2, \dots, r^{32}\}$$

Let  $R = \{e, s\}$ . Then the left coset  $sG$  has elements  $s, sr, sr^2$ , etc. So,

$$G = \{e, r, r^2, \dots, r^{32}, s, sr, sr^2, \dots, sr^{32}\}$$

This does not mean that  $G$  is dihedral. We need to know how  $s$  acts on  $r$  by conjugation. Since  $PQ = \langle r \rangle$  is normal,  $sr s^{-1} = sr s \in \langle r \rangle$ . In other words,  $sr s = r^n$  for some  $1 \leq n \leq 32$ . But  $n^2 \equiv 1 \pmod{33}$ .

At this point it looks like something is wrong since we get only two possibilities  $n = \pm 1$  and there are supposed to be 4 different groups. But wait! There are 4 solutions to this equation:  $n = 1, 10, 23, 32$ . These give:

$$\begin{array}{cccc} n = & 1 & 10 & 23 & 32 \\ G = & \mathbb{Z}_{66} & D_{11} \oplus \mathbb{Z}_3 & S_3 \oplus \mathbb{Z}_{11} & D_{33} \end{array}$$

When  $n = 1$  we have  $sr s = r$ , i.e.,  $G$  is abelian. So  $G = \mathbb{Z}_{66}$  in that case.  $sr s = r^{32} = r^{-1}$  is the dihedral group  $D_{33}$ . In the case  $sr s = r^{10}$ , the element  $r^3$  which has order 11 is sent to its inverse:  $sr^3 s = r^{30} =$

$r^{-3}$ . So,  $s$  and  $r^3$  generate the dihedral group  $D_{11}$ . Also, the element  $r^{11}$ , which has order 3, commutes with  $s$  since  $sr^{11}s = r^{110} = r^{11}$  ( $110 = 99 + 11$ ). So, this is  $D_{11} \oplus \mathbb{Z}_3$ .

In the case  $sr^3s = r^{23}$ , the element of order 11 (namely  $r^3$ ) commutes with  $s$  since  $sr^3s = r^{69} = r^3$ . Also, the element of order 3 (namely  $r^{11}$ ) is sent to its inverse:  $sr^{11}s = r^{243} = r^{22} = r^{-11}$ . So,  $G \cong D_3 \oplus \mathbb{Z}_{11}$ .  $\square$

24.6.6. *groups of order 12*. Finally, I talked about the groups of order 12. There are five of them:

$$\mathbb{Z}_{12} \quad \mathbb{Z}_6 \oplus \mathbb{Z}_2 \quad D_6 \quad A_4 \quad \widetilde{S}_3$$

The group  $\widetilde{S}_n$  is a “covering group” (or “central extension”) of  $S_n$ . It is a groups whose center is  $\mathbb{Z}_2$  with quotient  $S_n$ . The idea is that when you rotate  $360^\circ$  you are not quite the same as you were before. Your “spin” changes. When you rotate  $720^\circ$  you are back to normal.

Let’s do the dihedral group first. You need to think of  $\widetilde{D}_n$  as a rotation of a regular  $n$ -gon in 3-dimensional space. Then  $\widetilde{D}_n$  is the spinor group of the regular  $n$ -gon in 3-space. In this interpretation, the reflection  $s$  is a rotation by  $180^\circ$ . When you do it twice, you get to the central element  $-e$ . Similarly, the rotation  $r$  when done  $n$  times gives  $-e$ . So,  $\widetilde{D}_n$  has  $4n$  elements and they are:

$$\pm e, \pm r, \pm r^2, \dots, \pm r^{n-1}, \pm s, \pm sr, \dots, \pm sr^{n-1}$$

Since  $-e = s^2$  and  $-s = s^3$  this can be written as

$$\widetilde{D}_n = \{s^i r^j \mid i = 0, 1, 2, 3 \text{ and } j = 0, 1, 2, \dots, n-1\}$$

and multiplication rule given by

$$sr s^{-1} = r^{-1} = s^2 r^{n-1}, \quad r^n = s^2$$

The covering group (universal central extension) of  $A_5$  is called the *binary icosahedral group*. We will discuss it later (maybe).