Group Theory

Krish Ramkumar

2022-2023 Trimester 3

Contents

1 Introduction and Acknowledgements

This file serves as my lecture notes and notes for Trimester 3 Group Theory Elective for the 2022-2023 School year. These notes should not serve as a standalone learning instrument for Group Theory (as there are hundreds out there on the internet) but rather a supplement to taking the Group Theory elective at Bergen Academies. I included additional exercises to supplement your understanding of certain sections and also a section highlighting the most humorous aspects of each class to add a personal touch to the curriculum. This text is best consumed on a PDF reader to take advantage of the hyperlinks and table of contents.

I taught four classes in total: investigating the symmetries of regular polygons (Class 1), going over selected exercises on abelian groups and subgroups (class 5), the dihedral group and its conjugacy classes (class 11), proof of burnside's lemma and standard problems with burnsides lemma (class 19). I also gave a few sections like all groups of order 4 (class 7) homomorphism and isomorphism (class 9).

Thank you to the class for being wonderful listeners and participants. Thank you to Ms. Pinke for giving me the motivation to grow and care for this project. Most importantly, thank you to Dr. Abramson for trusting me with teaching his class. Without him, none of this would have been possible. I have only him to thank for my improved typesetting and my improvement in giving lectures.

2 Monday, March 20th (Class 2)

§2.1 Class One Recap

The first day of class was investigating the symmetries of regular polygons. We showed that for a regular n-gon, there would be $2n$ symmetries: n rotations by $\frac{2\pi}{n}$ and n reflections about each line of symmetry in the polygon. Rather than writing a day of notes on this investigation, we can classify this more formally with terminology learned in the second class.

§2.2 Definitions

Definition 2.2.1. A set G with a binary operation $\cdot$ is called a *group* if the following holds:

1. G is *closed* under $\cdot$, i.e, $\forall g, h \in G \; g \cdot h \in G$
2. G is *associative* under $\cdot$, i.e, $\forall g, h, j \in G \; (gh)j = g(hj)$
3. G has an *identity* (often denoted as e or e_G but referred to by Jeremy as 1) which menas $\forall g \; eg = ge = g$
4. Every element of G has an *inverse*, i.e $\forall g \in G \; \exists g^{-1} \in G \quad gg^{-1} = g^{-1}g = e$

Furthermore, a group is *abelian* if its elements commute, i.e. $\forall g, h \in G \; gh = hg.$. If elements do not commute, then the group is *nonabelian*

> **Remark 2.2.2.** It is absolutely vital to get familiar with the quantifier definitions for the conditions to be a group. A lot of proofs that we do in class will call upon them.

§2.3 Examples

There are lots of examples of groups that we are already familiar with. If we think about the binary operation of addition, we can say that the following are groups:

- $(\mathbb{Z}, +)$
- $(\mathbb{R}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{C}, +)$

Notably missing from this list is $(\mathbb{N}, +)$. This is not a group as it does not have an identity element, 0, nor does it have inverses, negative numbers.

If we consider multiplication, we must remember to take zero out of our set (which will be denoted by putting an x at the top right corner) as zero does not have an inverse.

- $(\mathbb{R}^x, \times)$

- $(\mathbb{C}^x, \times)$
- $(\mathbb{Q}^x, \times)$

If we consider using modular arithmetic, then $(\mathbb{Z}_n, +)$ for $n \in \mathbb{N}$ is a group (notably, our first group with finitely many elements). Similarly, for p prime, $(\mathbb{Z}_p^x, \times)$ is also a group. The rationales for why inverses exist largely rely on number theory.

If we recall our work from day one, we can claim that given a regular n-gon, the set of all symmetries under composition is a group. We can split this into two options: just rotating, or both rotating and reflecting. We did not delve into this group but these groups will recieve special attention on a later date.

Furthermore, we can also use a set of matricies with the operation of matrix multiplication. While these groups have specific names, right now we are putting the qualification that these matricies are n by n and invertible, or more specifically having nonzero determinant (do not worry if you do not know how to multiply matricies or what a determinant is, this will be covered later in the course). Notably, this group is nonabelian.

§2.4 Symmetric Group

Let $n \geq 2$ be a natural number. Let

$$S_n = \{\text{all permutations of } (1, 2, ..., n)\}$$

where the group operation is composition. What might the elements of S_3 look like? Well, we need to track where individual elements track after they are permuted. Thus, the notation of the 6 elements of S_3 look like

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Composition of these elements means doing these permutations from right to left. What this usally involves is tracking one element's journey. Consider

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Let's track the journey of 1. We read from the top right and see what is vertically below 1. This means that starting at one, this permutation will bring one to 3. Then we must do the next permutation. We see that three goes to three. This means our journey of one is $1 \to 3 \to 3$. Similarly, our journey for 2 is $2 \to 1 \to 2$ and our journey for 3 is $3 \to 2 \to 1$. Thus,

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \cdot \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

Remark 2.4.1. Often times the operation that we have with a group is composition. Function composition is essentially associative by definition, so we often times leave that to the side while proving something is a group.

What are the inverses of elements and what is the identity of the group? Evidently, $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ will be the identity as it is telling us to not permute any elements. If we

wanted to find the inverse of an element, say for example $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1}$, how would we go about that? Daniel had the visualization to imagine flipping the rows and rearranging them back into order. This makes sense intuitively, as we want all of the right arrows of where we are permuted to be flipped, so now $2 \to 1, 3 \to 2$, and $1 \to 3$. Thus, the inverse of that element is

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1} = \begin{pmatrix}2&3&1\\1&2&3\end{pmatrix} \to \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Remark 2.4.2. To find how many elements are in S_n just remember that this is a group of permutations, meaning there are $n!$ elements.

§2.5 Group Lingo

Definition 2.5.1. The *order* of a group is the number of elements in a group, referred to as $|G|$. If the group does not have finitely many elements, it has *infinite order*.

Definition 2.5.2. H is a *subgroup* of G (denoted as $H \leq G$) if

1. The elements of H are a subset of the elements of G
2. H itself is a group under the same operation as G

An example of a subgroup would be the even integers being a subgroup of the integers under addition, or that $(2\mathbb{Z}, +) \leq (\mathbb{Z}, +)$

§2.5.1 Subgroups of $(\mathbb{Z}, +)$

Theorem 2.5.3

Except for $\{0\}$, the groups $(n\mathbb{Z}, +)$ for $n \in \mathbb{N}$ represent the complete list of subgroups of $(\mathbb{Z}, +)$.

Proof. We must have 0 (as we need an identity element). If we are to have any nonzero elements, we must have both positive and negative elements. By the well-ordering principle (do not worry if you do not know what this is, it is unnecessarily fancy mathematical machinery) we must have a least positive element, which we can call k. Our claim is that having this element must force the set to be $k\mathbb{Z}$. If we said have some n for which $k \nmid n$, then we must have an element less than k as $n \pmod k$ must be in the set and it is less than k but positive. □

§2.6 Kinda Sorta

We will delve much more into the topic of groups being *isomorphic*, but to describe similar groups we will call them "kinda sorta similar". The main idea is that we can create a one-to-one correspondence. If we imagine a clock (which Dr. Abramson conveniently had on the ground), we could consider two actions of symmetries: rotational symmetries of a 12-gon, or adding hours together, which is $(\mathbb{Z}_{12}, +)$.

Furthermore, the two groups which we previously called subgroups are kinda sort of similar. As Tony and Daniel said, if you imagine scaling or dilating everything by two you can go from the integers to the even integers.

After a wordle, we decribed the group of addition mod n and rotations of an $n-gon$ to be something known as *cyclic*, which will be expanded upon later.

§2.7 Exercises

Exercise 2.7.1. Prove (semirigorously) that $(\mathbb{C}^x, \times)$ is a group. Try not to look at your notes when looking for the conditions of a group!

Exercise 2.7.2. Find $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 6 & 4 & 7 \end{pmatrix}^{17}$.

Exercise 2.7.3. Provide a rationale why $(\{cis\theta \mid \theta \in \mathbb{R}\}, \times) \leq (\mathbb{C}^x, \times)$ (remember, you must show why both are groups!)

3 Thursday, March 23rd (Class 3)

§3.1 Group Properties

Rather than looking at specific groups we will look at group properties in general.

Theorem 3.1.1

Let G be a group with identity e.

1. The identity element is unique
2. Inverses are unique and demonstrate why a left inverse must be a right inverse
3. Why do we need associativity to define x^3 for $x \in G$
   a) How can we talk about x^n in general? Do exponent rules work?

Proof. 1. Assume for the sake of contradiction that in addition to e we have an element $\tilde{e}$ which is distinct from e but also an identity. Because $e = e$, we know that $\tilde{e}e = e$, because $\tilde{e}$ is an identity. However because e is also an identity, we have that $\tilde{e} = e$, meaning that they are not distinct. This contradicts our initial assumption that we had atleast two distinct identities, meaning that the identity element is unique.

2. Assume for the sake of contradiction that in addition to g^{-1}, we have another element g'^{-1} (tildes sadly did not render well) that is also the inverse of an element g. Since $e = e$, we can rewrite e as both $g'^{-1}g$ and $g^{-1}g$ on the left and right sides of the equal sign. But if we multiply on the right side by g^{-1}, we can simplify:

$$e = e$$
$$g'^{-1}g = g^{-1}g$$
$$(g'^{-1}g)g^{-1} = (g^{-1}g)g^{-1}$$
$$g'^{-1}(gg^{-1}) = g^{-1}(gg^{-1})$$
$$g'^{-1}(e) = g^{-1}(e)$$
$$g'^{-1} = g^{-1}$$

This contradicts our inital assumption that there were atleast two distinct inverses, meaning inverses are unique.

3. We mainly 'talked through this' in class, but if we want $x^3 = x \cdot x \cdot x$, we want $(x \cdot x) \cdot x = x \cdot (x \cdot x)$. Because of associativity, we can sort of 'recursively/inductively' define x^n as $x * x^{n-1}$. Because we are associative, x^n will be legal with this definition, and then prove exponential laws. We can similarly define $x^{-n} = (x^{-1})^n$

Problem 3.1.2. Suppose G is a group whose elements are a, b, c, and e. and suppose

$$a^2 = b^2 = c^2 = e.$$

Write a multiplication table for G

Solution.

	e	a	b	c
e	e	a	b	c
a	a	e	?	?
b	b	?	e	?
c	c	?	?	e

Here is the multiplication table. The goal of this exercise was to figure out constraints on ?'s must be. We claim that every row and every column in this group must have each element (i.e, e, a, b, and c in some order). For notation, the column is what we multiply on the right and the row is what we multiply on the left. Thus, we can rewrite the table:

	e	a	b	c
e	e	a	b	c
a	a	e	ab	ac
b	b	ba	e	bc
c	c	ca	cb	e

We have the underlying assumption that $e \neq a \neq b \neq c$. Lets take a look at what the element ab could be.

- If $ab = e$, then $b = a^{-1} = a$, which contradicts our assumption
- If $ab = a$ then $b = e$, which contradicts our assumption
- If $ab = b$ then $a = e$, which contradicts our assumption
- Since the group is closed, $ab = c$. By multiplying by a on the left on both sides, $b = ca$. By multipling by c on the left on both sides, $cb = a$. We can continue this process to see that multiplying two nonidentity elements always yields the third. We can now complete the table.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Remark 3.1.3. Notice that the group is abelian as we are symmetric across the diagonal. Could we have proved this from the get go? This will be left as an exercise.

□

The next three exercises did not recieve much discussion in class. They often follow from multiplying on both sides by what seems obvious.

Exercise 3.1.4. Prove $(gh)^{-1} = h^{-1}g^{-1}$

Exercise 3.1.5. Show if g and h commute (i.e. gh = hg), then $(gh)^n = g^n h^n$

Exercise 3.1.6. Simplify $(g^{-1}hg)^n$

Remark 3.1.7. This act of sandwiching h between g^{-1} and g appears so often it gets a special name: $g^{-1}hg$ is reffered to as conjugating h by g. We will talk about this in much greater detail later in the course.

Problem 3.1.8. If G is finite, for any g in G, prove $\exists n \in \mathbb{N}$ such that $g^n = e$

Solution. Let the order of G be k., i.e $|G| = k$. Consider the set of the first $k+1$ powers of an arbitrary element g. The group G is closed, meaning all powers of g must be in the group. However, there must be a repeat as G has only k elements. Suppose that for $n < m \leq k+1$, $g^n = g^m$. Thus,

$$g^n = g^m$$
$$g^{-n}g^n = g^{-n}g^m$$
$$e = g^{m-n}$$

Since $m, n \in \mathbb{N}$ and $n < m$, $m - n$ is a natural number power of g that is equal to the identity. □

Remark 3.1.9. The style used in this proof is most commonly referred to as the **Pidgeonhole Principle**. You have k holes and $k+1$ pigeons, so there must be a hole with two pigeons.

Remark 3.1.10. Dr. Abramson labeled this as the most important problem for today's class. This will appear more in detail when we discuss the *order* of elements.

§3.2 Exercises

The first three exercises were taken from the 'Section 2.2 Exercises' of David Nash's Group Theory textbook.

Exercise 3.2.1. Let G be a group. Prove that if $(ab)^2 = a^2b^2$ for all $a, b \in G$ then G is a Abelian.

Exercise 3.2.2. Prove that if G is a group with $|G| \leq 4$, then G is an Abelian.

Exercise 3.2.3 (*)**.** Show that if G is a finite group with $|G|$ even, then there exists some $g \neq e \in G$ such that $g^2 = e_g$

The last exercise arises from my own brain after playing around with the multiplication table.

Exercise 3.2.4. Prove that a (not necessarily finite) group where every element has *order* 2 (i.e $\forall g \in G, g^2 = e$) must be necssarily be abelian. (Hint: Use Exercise 2.1.4.)

§3.3 Funny Stuff

Remark 3.3.1. The T.A. test is that if you find food you must offer it to the teacher before you eat it yourself. I miserably failed the TA test.

Remark 3.3.2. If you are caught with cake in the hallway you will be met with a hearty "HA!"

□

4 Monday, March 27th (Class 4)

§4.1 Order (of elements)

Recall if G is finite then $\forall g \in G\ \exists n \in \mathbb{N}, g^n = e$.

Definition 4.1.1. Call the smallest such natural number n such that $g^n = e$ the *order of* g and write $o(g) = n$

We proved last class (from our pigeonhole argument) that $o(g) \leq |G|$

Theorem 4.1.2
If $g^k = \text{e}$, then $o(g) \mid k$

Proof. As gabe said, if $o(g) = k$, then we're done. Otherwise, we use the division algorithm on k which says that $k = (o(g))q + r$ for some natural numbers q and $r < o(g)$. Thus,

$$g^{((o(g))q+r)} = g^{(o(g))q} * g^r = g^r$$
$$r < n \implies r = 0$$

□

Problem 4.1.3. If $o(g) = n$, what can we say about

1. g^{-1}
2. $o(g^k)$?

Solution. 1. $g^{-1} = e * g^{-1} = g^n * g{-}1 = g^{n-1}$

2. Suppose $\gcd(n, k) = r$. Necessarily, for some x and y, $k = rx$ and $n = ry$. We have g^{rx} and we know $g^{ry} = e$, because $\gcd(x, y) = 1$, the smallest power we can raise g^{rx} to is y, meaning $o(g^k) = \frac{n}{\gcd(n,k)}$

□

Exercise 4.1.4. What are the orders of the elements of

- $(\mathbb{Z}_5, +)$
- $(\mathbb{Z}_6, +)$
- $(\mathbb{Z}_8^\times, \times)$ (all of the elements relatively prime to 8, or having a multiplicative inverse)
- The symmetries of a square?

Remark 4.1.5. All of the orders we have encountered divide the size of the group... we can conjecture for now that $o(g) \mid |G|$ with G a finite group. We will prove this in 1-2 classes.

Recall the definition of a subgroup (found in 2.5.2).

Definition 4.1.6. If $g \in G$, let

$$\langle g \rangle = \{g^n = n \in \mathbb{Z}\}$$

Theorem 4.1.7

$\langle g \rangle$ is a subgroup of G, which we refered to as *generated* by g

Proof. We are closed as we are multiplying g with itself. We have inverses as any g^n has g^{-n}. We have $g^0 = e$. Associativity follows from the fact that G is already a group, meaning its operation must be associative □

Exercise 4.1.8. Classify the subgroups generated by each of the elements in

1. $(\mathbb{Z}_5, +)$
2. $(\mathbb{Z}_6, +)$
3. $(\mathbb{Z}_8^\times, \times)$
4. The symmetries of a square

Exercise 4.1.9.
1. In $(\mathbb{Z}, +)$, what is $\langle 11 \rangle$?
2. In $(\mathbb{C}^\times, \times)$, what is $\langle \operatorname{cis} 60° \rangle$?

Remark 4.1.10. $\langle \operatorname{cis} 60° \rangle$ is very very similar to the rotations of the hexagon!

Definition 4.1.11. A group is *cyclic* if it can be generated by a single element.

What groups are cyclic? Well, $\mathbb{Z}_n = \langle 1 \rangle$ and $\mathbb{Z} = \langle 1 \rangle$, but definetly not $\mathbb{C}$ or the symmetries of the square.

Theorem 4.1.12

The only subgroups of cyclic groups are themselves cyclic.

Proof. Assume G is a cyclic group where $|G| = n$, which can be written as $\{e, g, g^2, g^3, ...g^{n-1}\}$ for a generator g. Suppose $H \leq G$. H must necessarily consist of power of g. If $H = e$, we have what we want (as $e = \langle e \rangle$). Similarly, if $g \in H, H = G$, which means H is cyclic (as G is cyclic). Otherwise, let $k > 1$ be the smallest k such that $g^k \in H$. It remains to show $\langle g^k \rangle = H$.

Let g^t be an arbitary element in H. Because of the divison algorithm, $t = mk + r$ for $0 \leq r < k$. but since $g^t \in H, g^{mk} \in H \implies g^{-mk} \in H \implies g^r \in H$. But since k is the least element, $r = 0$. Thus, any power of an element must be divisible by k. This shows that $\langle g^k \rangle = H$.

□

§4.2 Exercises

Exercise 4.2.1. (Exercise 2.5.96 in the Textbook) Let G be a group and let $H \leq G$

1. If $g \in G$, show that the set $g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$ is a subgroup of G (the subgroup $g^{-1}Hg$ is known as a *conjugate* of H by g)
2. Show that the subset $N(H) = \{g \in G \mid g^{-1}Hg = H\}$ is a subgroup of G
3. Show that $H \leq N(H)$

Exercise 4.2.2. (Exercise 2.5.101 in the Textbook) Let G be a group and let $H \leq G$. True or false, and why (TorF & y)?

If G is abelian, then H is also abelian. If H is abelian, then G is also abelian

If something false, identify a counterexample.

The next exercise is important to our discussion of *cosets* (which will be defined in a few classes).

Definition 4.2.3. A binary relation $\sim$on a set A is a predicate with two arguments (for example for $x, y, z, a \in A$, $x \sim y = T$ or $z \sim a = F$ are examples of statements with a binary relation). An *equivalence relation* is a relation that is *symmetric, reflexive,* and *transitive*.

- Symmetric: $\forall a, b \in A, a \sim b \implies b \sim a$.
- Reflexive: $\forall a \in A, a \sim a$.
- Transitive: $\forall a, b, c \in A, ((a \sim b)(b \sim c)) \implies a \sim c$.

While $<$ is a relation on $\mathbb{R}$, it is not reflexive. $=$ is an equivalence relation on $\mathbb{R}$.

Exercise 4.2.4. (Exercise 2.5.105 in the Textbook) Let G be a group and let H be a subgroup. Consider the relation $\sim$ defined on G by declaring that $x \sim y$ if there exists some $h \in H$ such that $y = hx$. Prove that $\sim$ is an equivalence relationship.

5 Thursday, March 30th (Class 5)

Today, I'll be lecturing! We will first go over a few of the exercises I have selected over the last few classes.

§5.1 Problem Review

Problem 5.1.1. Let G be a group. Prove that if $(ab)^2 = a^2b^2$ for all $a, b \in G$ then G is a Abelian.

Solution. This problem serves as an example of what to do when you encounter any group theory fact which may not seem immediately obvious. It's important to remember what the definitions of the objects you are working with are. Furthermore, if you are trying to prove something that involves proving it for all elements over a set, take an arbitrary element of the set and show that it works.

We have $\forall a, b \in G\ (ab)^2 = a^2b^2$

We expand everything and use inverses:

$$abab = aabb$$

$$bab = abb$$

$$ba = ab$$

This is the condition for being abelian, so we are done. □

Problem 5.1.2. Prove that a (not necessarily finite) group where every element has *order* 2 (i.e $\forall g \in G, g^2 = e$) must be necssarily be abelian.

Solution. Let $a, b \in G$. To prove a group is abelian, we want to show that $\forall a, b, \in G,\ ab = ba$. We know that since $ab \in G$, $(ab)^2 = e$, meaning that

$$(ab) = (ab)^{-1} = b^{-1}a^{-1}.$$

But since a and b have order two, $b = b^{-1}$ and $a = a^{-1}$. Thus, $ab = ba$ □

Problem 5.1.3. Show that if G is a finite group with $|G|$ even, then there exists some $g \neq e \in G$ such that $g^2 = e_g$

Solution. The solution to this problem largely involves a trick. Consider grouping every element with it's inverse. So instead of writing the set as

$$G = \{e, g_1, g_2, g_3, g_4...\}$$

Write the set as

$$G = \{e, g_1, g_1^{-1}, g_2^{-1}, g_3, g_3^{-1}, ...\}$$

If we consider this pattern, e has nothing to pair up with as it is technically its own inverse. Thus, this exaplins the missing element in the list– we know there must be an element which does not pair up with another as it is its own inverse. Since it is not the identity, it must have order two. □

§5.2 Categorizing Subgroups

Theorem 5.2.1

Let G be a group and let $H \subseteq G$ be a non-empty subset. Then, the following are equivalent:

1. $H \leq G$
2. For all $x, y \in H$ we have both $xy \in H$ and $x^{-1} \in H$
3. For all $x, y \in H$ we have $xy^{-1} \in H$
4. For all $x, y \in H$ we have $x^{-1}y \in H$

Remark 5.2.2. Let's first think of clever ways to use our knowledge of logic to reduce the amount of work we need to do, as if we showed both directions of each statement to eachothe it would be $\frac{4*3}{2} * 2 = 12$ proofs.

The first clever option is to show that $1 \implies 2 \implies 3 \implies 4 \implies 1$. This uses hypothetical syllogism to allow us to jump around to any forward and backward implication. The second option is to show $1 \iff 2, 1 \iff 3, 1 \iff 4$ and use hypothetical syllogism to jump around and show that $2 \iff 4$. This helps us if one of our equivalent conditions is especially strong or easy to work with.

§5.3 Intersecting Subgroups

Theorem 5.3.1

Let H and K be subgroups of G. Then, $H \cap K$ is a subgroup of G

Proof. The intersection has e is nonempty. Everything else follows by assuming that something is in the set. The inverses must necessarily exist and the products must necssarily exist. □

§5.4 Exercises

No exercises for this class (as thats what the entire class was for!) Next class we will develop more theory with subgroups with the idea of *cosets*.

6 Monday, April 3rd (Class 6)

Definition 6.0.1. Let G be a group and $A \subseteq G$. A *left coset* of A is (for some $g \in G$)

$$gA = \{ga \mid a \in A\}$$

Similarly, a *right coset* of A is

$$Ag = \{ag \mid a \in A\}$$

For example in $(\mathbb{Z}_6, +)$ where $A = \{1, 3\}$. Then $1 + A = \{2, 4\}$.

Theorem 6.0.2

Lagrange's Theorem Suppose G is finite and $H \leq G$. Then $|H| \mid |G|$

Given H, consider all possible left cosets, i.e $\{gH \mid g \in G\}$. Lets first do an example with $6\mathbb{Z} \leq \mathbb{Z}$. Our left cosets will look like

$$\begin{aligned} 6\mathbb{Z} \\ 1 + 6\mathbb{Z} \\ 2 + 6\mathbb{Z} \\ 3 + 6\mathbb{Z} \\ 4 + 6\mathbb{Z} \\ 5 + 6\mathbb{Z} \\ \vdots \end{aligned}$$

It turns out that our 'horizontal dots' could just be a period, as thats where we stop. Furthemore, if we take the intersection of any two left cosets, they will be the empty set.

Lemma 6.0.3

Given two left cosets g_1H and g_2H either

- $g_1H = g_2H$
- $g_1H \cap g_2H = \emptyset$, referred to as being disjoint.

In english, if two left cosets are not disjoint, they are the same.

Exercise 6.0.4.

- When is $gH = H$?
- When is $g_1H = g_2H$?
- Suppose $k \in g_1H \cap g_2H$

Proof. If their intersection is empty, then we are done. Otherwise, theres an element they have in common. suppose $\exists h_1, h_2$ such that $k = g_1h_1 = g_2h_2$. So far, we have a single element in common. Let g_2h_i be an arbitrary element of g_2H. Necessarily, $g_2h_i =$

$g_2h_2h_2^{-1}h_i = g_1(h_1h_2^{-1}h_i)$ and because $(h_1h_2^{-1}h_i) \in H$ (because of closure), $g_2h_i \in g_1H$. Similarly, let g_1h_j be an arbitrary element of g_1H. $g_1h_j = g_1h_1h_1^{-1}h_j = g_2(h_2h_1^{-1}h_j)$, and since $(h_2h_1^{-1}h_j) \in H$, $g_1h_j \in g_2H$. Thus, both sets are subsets of eachother and thus they are the same set. □

Its also easy to see that $|gH| = |H|$ (theres a one to one correspondance, as Joy has mentioned). We can find every g in some left coset (take gH for example). So, different cosets are disjoint. G is a union of disjoint cosets, which are all the same size. Since we are adding an integer number of cosets to get G, it has been shown $|H| \mid |G|$.

Corollary 6.0.5

Suppose G is finite and $g \in G$. Then,

$$o(g) \mid |G|$$

where $o(g)$ was the order of that element.

Proof. Consider $\langle g \rangle = \{e, g, g^2, ..., g^{o(g)-1}\}$. We proved that this is a subgroup, and since g has order n, $|\langle g \rangle| = o(g)$. We have a subgroup the size of $o(g)$, so by Lagrange's Theorem $o(g) \mid |G|$ □

§6.1 Isomorphic

Right now, we only have a qualitative definition of being 'isomorphic'. It is essentially when two groups for all intents and purposes are the same. Our example was $\mathbb{Z}_12$ and the rotations of a dodecagon.

Theorem 6.1.1

There is a "unique" (up to isomorphisms) group of order p for each prime p and it is cyclic.

Proof. We need a group with only e and the group itself as subgroups. If we were to take a non-identity element and try to 'make' a subgroup from it, it would necessarily generate the whole group. A group that is generated by a single element is cyclic! Furthermore,

Any element necessarily has order 1 or p. If order 1, youre the identity, if order p youre a generator. The only subsets of these groups are the identity element and the group itself. □

Problem 6.1.2. In $\mathbb{Z}_{2023}$, find all possible orders of elements & one element of that order. Then add them, take it mod 1000, and bubble in your answer.

Solution. $(1 + 17 + 289)(1 + 7) = 2,456$ which is congruent to 456 mod 1000. □

§6.2 Exercises

Exercise 6.2.1. What are the subgroups of the rotations of the dodecagon?

Exercise 6.2.2. What are the subgroups of the symmetries of squares? (We will classify this group better later)

§6.3 Funny Stuff

Remark 6.3.1. If you introduced two isomorphic groups to their mom, their mother wouldn't be able to tell them apart.

Remark 6.3.2. $\mathbb{Z}_p$ passed the '50% of its letters are the same' test which cyclic also passes.

7 Thursday, April 6th (Class 7)

§7.1 All groups of order 4

Exercise 7.1.1. Identify as many groups of order 4 that you know.

A few examples would include $\mathbb{Z}_4, \mathbb{Z}_5^\times, \mathbb{Z}_8^\times, \mathbb{Z}_{12}^\times$, and the rotations of a square.

Let G be a group of order four. From our corrolary of Lagrange's Theorem, we know that all elements must have order 1, 2, or 4. If an element has order 4, we must necessarily be the cyclic group of order 4 as a single element generates all elements. If not, every nonidentity element has order 2. This set would look like $\{e, a, b, c\}$ where $a^2 = e,\ b^2 = e,\ c^2 = e$. We have identified a group like this and have already created a multiplication table.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Furthermore, if we took a square with rotation by 180, reflection over the y - axis, and reflection over the x - axis, this is what it's multiplication table would look like.

§7.2 Direct Product

Definition 7.2.1. Given groups G and H, the direct product $\times$ is defined as follows:

- The underlying set is the Cartesian product, $G \times H$. That is, the ordered pairs (g, h), where $g \in G$ and $h \in H$
- The binary operation is defined componentwise.

I.e, $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$ with their respective operations

Theorem 7.2.2

$G \times H$ is a group under their prescribed operation. Furthermore, if G and H are abelian, then $G \times H$ is abelian.

Proof. We will show closure, identity, inverses, and associativity. $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$, since G and H are closed $G \times H$. Furthermore, since the operations in G and H are associative $G \times H$ is associtative. We can find the identity by taking the identities e_G and e_H, and inverses can be shown in the same way. □

Exercise 7.2.3. Make a multiplication table for $\mathbb{Z}_2 \times \mathbb{Z}_2$ (also known as the Klein 4-group, the same Klein with the same bottle)

Theorem 7.2.4
$G \times H \cong H \times G$

We cannot prove this yet as we don't have a definition, but since these are essentially the same we can guess this for now.

Exercise 7.2.5. Make a multiplication table for $\mathbb{Z}_3 \times \mathbb{Z}_2$.

As Michael said, this is a cyclic group generated by $(1, 1)$. If its cyclic, its isomorphic to $\mathbb{Z}_6$. Remember, cyclic times cyclic is not ALWAYS cyclic (consider $\mathbb{Z}_2 \times \mathbb{Z}_2$). We eventually want to make a conjecture about something that is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$. We can guess that when m and n are relatively prime, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

Theorem 7.2.6
Let $g \in G$ and $h \in H$. Given that $o(g) = m$ and $o(h) = n$, show that $o(g, h) = \text{lcm}(m, n)$.

Proof. We have shown for $g \in G$, $g^k = e$ if and only if $o(g) \mid n$. Thus, $(g, h)^k = e \implies (g^k, h^k) = (e, e)$. We can start looking at the elements individually, meaning $m \mid k$ and $n \mid k$. This means that if an element were to be the order of our elements, it must be a multiple of both m and n. From number theorey, $m, n \mid k \implies \text{lcm}(m, n) \mid k$. It thus follows that since the order is the least, our order is the least common multiple. □

§7.3 All groups of order 6

We proceed in a similar fashion analyzing the order of elements. We have already proved that if a group has even order it must have an element of order 2.

If we are abelian, we could be cyclic (thats one type of group done!), but what if every element was order 2 (we have proved that this is necessarily abelian)? Well consider elements e, x, y. Since G is abelian, $xy = yx$. This means that

$$\{e, x, y, xy\} \leq G$$

But that isn't possible as a subgroup of order 4 cannot live in groups of order 6 (this violates lagrange)!

We also know the intersection of two subgroups is a subgroup. We know we have a subgroup of order 2. What if we had a subgroup of order 3 (i.e, there are no elements of order 6)? Intersect, you must get a subgroup, meaning their intersection is order 1 (as intersection is GCD) meaning its $\{e\}$. Thus. we have cyclic subgroup or order 2, cyclic subgroup of order 3. None of the elements nonidentity elements can be eachother. Thus, we have elements e, a, b, b^2 and because of closure, ab, ab^2, b. Somethings must be equal here (or else we aren't order 6). If $ab = ba$, every element must commute (as the a's commute with themselves and b's commute with themselves, and they commute with eachother). Since b is of order 3 and a is order 2, if ab is not the identity and we are in a commutative group, $(ab)^k = a^k b^k \implies 3, 2 \mid k \implies o(ab) = 6$. Since we have an element of order 6, this is the cyclic group!

What if $ba = ab^2$? If we multiply by a on the left and b on the right, we have that

$$abab = a^2 b^3 = e$$

This means $o(ab) = 2$. We also know that $(ba)(ab^2) = beb^2 = b^3 = e$. Since we supposed they are equal, this means $o(ba) = 2$. Thus, we are in a group where we have three elements of order 2, and two elements of order 3 (as $o(b^2)$ can't be anything else). Is everything legal? Have we classified another group? It turns out that we have! This is what we have previously referred to as the symmetries of a triangle, which has three reflections and three rotations. Whats especially interesting to note is that this group is nonabelian. Since we have classified everything up to this, we just found **the smallest finite nonabelian group!**

§7.4 Fun Stuff

Remark 7.4.1. Group theorists cannot find every single group ever so they settle for classifying all groups up to isomorphism for a certain order

8 Monday, April 17th (Class 8)

We spent some time cleaning up our proof of all groups of order 6. Our conclusion was that the two groups up to isomorphism are the **dihedral** group of order 6 (i.e the symmetries of a triangle and $\mathbb{Z}_6$, referred to as the cyclic group of order 6.

§8.1 Symmetric Group (Revamped!)

Recall our definition of a cyclic group that for a natural number $n \geq 2$

$$S_n = \{\text{all permutations of } (1, 2, ..., n)\}$$

where the group operation is composition. We have already proved that this is closed, has an associative operation, has an identity, and that each element has an inverse. We eventually want to look into the order of elements. Before we do this, we will develop alternate notation, often referred to as *cycle* notation.

§8.1.1 Cycle Notation

Consider the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}.$$

If we do this permutation upon itself, we can trace the path of a single elemet. 1 goes to 2, which goes to 3, which goes back to 1. Similarly, 4 goes to 5, which goes back to 4. These are two cycles, meaning we can refer to the entire permutation as $(123)(45)$. This explicitly states that this permutation has a cycle of the elements $1, 2$ and 3 and a cycle of 4 and 5. Furthermore, you can follow the path of a single element by reading the number immediately to the right of the number you want to track. For example, 2 must go to 3. Additionally, the notation says that the the parenthesis are like a portal– once you go through a right parenthesis, you are at the left side parenthesis. This means that if we track 5 and read one to the right, 5 goes to 4.

> **Remark 8.1.1.** If an element a does not change positions, rather than writing (a) in the cycle notation, we simply leave it out. This means that you cannot tell which orde symmetric group you are in simply through the cycle notation.

Notice this is the exact same as $(231)(54)$ as we chose to follow the path of 1 arbitrarily. Furthermore, this is also the same as $(45)(123)$

Multiplication in cycle notation follows in the same way that multiplication of two 'permutation matricies':

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$$

which we learned to compute by following the path of each element. Similarly, if we write both in cycle notation, this would yield

$$(123)(45) \cdot (24)(15) = (143)(25)$$

This takes a while getting used to, but remember that you are following the path of a single element. Begin with 1. 1 goes to 5, and then 5 goes to 4. Continue this process with 4 (as we are trying to figure out the entire cycle 1 is in). 4 goes to 2, which goes to 3. Then, 3 goes to 3, which goes to 1. Thus, we have finished a cycle, as we are back at 1. Repeat this process with 2 (because it has not been identified by our previous cycle 'exploration', it must be in a completely different cycle)

Exercise 8.1.2. Compute (123456)(143562)

§8.1.2 The symmetric group of order 6

We have already classified all groups of order 6. Thus, S_3 (which has $3! = 6$ elements) must be isomorphic to either the dihedral group of order 6 (the triangle) or Z_6. These six elements are:

$$S_3 = e, (123), (12), (13), (23), (132)$$

We can guess that because $(123)(12) = (13)$ and $(12)(123) = (23)$, we aren't commutative, meaning we must be isomorphic to the symmetries of a triangle.

To show why, we need to have the structure of an identity, 2 element of order 3, and 3 elements of order 2. Note that a cycle $(123...n)$ has order n and is referred to as an n-cycle (as each time you do the cycle, you move one more element down, so you have to do it n times to get back to where you started). From what we wrote above, we have exactly that structure! e has order 1. (123) and (132) are order 3 (as they're 3-cycles), and we have $(12), (13)$ and (23) as our elements of order 2.

Exercise 8.1.3. Verify $(123)^2 = (132)$ and $(23) = (12)(132)(132) = (132)(12)$. The second was our property of the arbitrary 'second' group of order 6 before we identified it as a triangle (i.e $ba = ab^2$).

§8.2 Fun Stuff

> **Remark 8.2.1.** "$n!$" is pronounced as n (loudly). Joy should have picked up on that earlier before she had to leave the room in shame.

9 Thursday, April 20th (Class 9)

§9.1 More Cycle Notation

Problem 9.1.1. Compute $(12)(1234...n)$

Solution. Track the trajectory of 1 first. 1 goes to 2, 2 goes to 1, so 1 goes to itself. N goes to 1, 1 goes to 2, so N goes to 2. The rest won't be messed with due to the multiplication, so we can get $(234...n)$ □

Notice that $(1234...n) = (12)(12)(1234...n) = (12)(234...n)$. We decomposed an n cycle into a $n-1$ and 2 cycle. Similarly, $(12)(234...n) = (12)(23)(34.....n)$.

Theorem 9.1.2

Any element in S_n can be written as a (nonunique) product of *transpositions* (i.e, 2-cycles). Furthermore, given an element of S_n, the number of transpositions in any decomposition is always the same parity.

To see the extreme of why this is not unique, e can be written as a product of any even number of transpositions (Such as $(12)(12)$, $(98)(98) = (12)(13)(13)(12)$).

Proof. To prove this, we will show that every element in S_n can be written as a product of cycles, and every cycle can be written as a product of transpositions. Because permutations are 1 to 1 maps, when we follow the path of a single element we always end up with a cycle. Thus any permutation is thus the product of cycles (and because cycles are disjoint, they can commute with eachother).

The proof of the parity is within our reach but is quite complicated. We will return to this at a later date. □

Definition 9.1.3. An element of S_n is called even if it requires an even number of transpositions and odd if odd. Define A_n to be

$$A_n = \{\text{even permutations in } S_n\}$$

Parity for these elements is known as 'well defined', a term that mathematicians through around a lot to mean 'makes sense'. Something can't have both an even and odd number of transpositions (due to the theorem we have not yet proved).

§9.2 Alternating Group

Theorem 9.2.1

A_n is a subgroup of S_n, and A_n is called the alternating group on n things. Furthermore, $|A_n| = \frac{n!}{2}$

Proof. e is in the group. Furthermore if multiple two numbers with an even number of transpositions, their product has an even number of transpositions. Finally,

$$((ab)(cd)(ef)...(yz))^{-1} = (yz)...(ef)(cd)(ab)$$

We can show that $|A_n| = n!$ by using a coset. Take an arbitrary transposition (ab). It is not immedietly evident that $A_n \cup (ab)A_n = S_n$. $(ab)A_n$ clearly has odd elements, but is it all odd elements? Take an arbitrary element $Z \in S_n$ which is odd. $(ab)Z$ is even, meaning it is in A_n. $(ab)(ab)Z$ is in our coset, but that's the same as writing Z, so every odd element must be in this set. Thus they are the cosets are the same size and partition the group, so they must each be half of $n!$. □

What parity is an $n-cycle$? It is the parity of $(n-1)$ (this can be observed from (123)=(12)(13)).

Theorem 9.2.2

A_n can be generated by its three-cycles. This means that every element of A_n can be written as a product of its three-cycles.

Proof. Consider (ab)(cd) where they aren't the same transposition. For the first case, assume these are all different. Then,

$$(ab)(bc) = (ab)(bc)(bc)(cd) = (abc)(bcd).$$

If any of them are the same, combine them in the way that we are used to. □

Remark 9.2.3. We may eventually use this fact the show that A_n is simple (if we last that long)

§9.3 Vital Definitions

At this point, we arrive at a very important junction in our group theory career. We will move into another level of abstraction by talking about conjugacy and normal subgroups, which have *lots* of results about them. I would strongly reccomend to take some time with these definitions and process them by doing exercises. **These won't go away**.

§9.3.1 Homomorphism, Isomorhism, Isomorphic

Definition 9.3.1. A map φ from groups G to H (i.e $\varphi : G \to H$) is a *homomorphism* if $\forall g_1, g_2 \in G, \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$

Some examples of homomorphisms include

$$\varphi : \mathbb{Z}_4 \to \mathbb{Z}_4 \text{ s.t. } \varphi(g) = 2 * g$$

$$\varphi : \mathbb{Z} \to 17\mathbb{Z} \text{ s.t. } \varphi(g) = 289 * g$$

$$\varphi : \mathbb{R}^\times \to \{-1, 1\} \text{ s.t. } \varphi(g) = \text{sign}(g)$$

Exercise 9.3.2. Verify that these are homomorphisms

Definition 9.3.3. An *isomorphism* is a bijective homomorphism. For a homomorphism φ, it is a bijective map if it is is one-to-one, or injective, meaning that $\varphi(g_1) = \varphi(g_2) \iff g_1 = g_2$ and a bijection is onto, or surjective, meaning that $\forall h \in H\ \exists g \in G$ s.t. $\varphi(g) = h$. Two groups are *isomorphic* if you can construct an isomorphism between them.

Remark 9.3.4. Understanding bijections is foundational for any math that involves sets. Injectivity means that two items in the same domain cannot map to the same element. For functions, this means the horizontal line test. Surjectivity means that every element in our codomain is covered. Thus, $y = x^3$ is a bijection while $y = x^2$ is not. Furthermore, remember that a wonderful property of bijections is that they have inverses.

Remark 9.3.5. When two groups are isomorphic, we have essentially the same structure. The map that we create is a 'structure-preserving' map from the properties it must satisfy, giving a formal reflection of two groups being 'the same in disguise'. This gives us the ability to precicely determine when two groups have no differences.

§9.3.2 Index, Conjugate, Normal

Definition 9.3.6. Let G be a group and H be a subgroup. Define $[G : H]$ to be the index of H in G which is the number of distinct left cosets. Specifically for finite G,

$$|G| = |G : H||H|$$

Example 9.3.7

What is $[\mathbb{Z} : 17\mathbb{Z}]$?

Solution. As Michael mentioned, all of these cosets are the residue classes mod 17, of which there are 17. □

Theorem 9.3.8

Let $H \leq G$, let $g \in G$. Define $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$. Prove that $gHg^{-1} \leq G$

Proof. We showed this a long time ago! We are associative as the operation in H is associative. The identity is in there as the identity must be in H, meaning $geg^{-1} = e \in gHg^{-1}$. We are closed as $gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1}$ (and since H is a subgroup, $h_1h_2 \in H$). By the same logic we have inverses since $ghg^{-1}gh^{-1}g^{-1} = e$. Thus, we are a subgroup. □

Definition 9.3.9. Let G be a group, $H_1, H_2 \leq G$, and $g \in G$, $h \in H$. An element b is *conjugate* to an element a if there exists a $g \in G$ such that $b = gag^{-1}$. The conjugate of h by g is the element ghg^{-1}. The conjugate of H by g is the set

$$gH_1g^{-1} = \{ghg^{-1} \mid h \in H\},$$

which we have shown to be a subgroup. Two subgroups are said to be *conjugate subgroups* if $\exists g \in G$ where $gH_1g^{-1} = H_2$

Remark 9.3.10. Conjugate, conjugacy, and conjugation are hard and they take a lot of getting used to. These will become even more important when we learn about conjugacy classes and group actions.

Definition 9.3.11. We call H *normal* in G ($H \trianglelefteq G$) if for all $g \in G$, $gHg^{-1} = H$. H is referred to as a *normal subgroup*.

Remark 9.3.12. In abelian groups all subgroups are normal. In nonablian groups it may seem difficult to identify which groups are normal. We will go much more in depth to normal groups. Understanding normal groups is vital as it helps us define quotient groups later down the line.

All of these remarks aren't here to scare you but to remind you the importance of these abstract concepts. To command good understanding of these concepts you should practice and get your hands dirty with them.

§9.4 Exercises

There are not many exercises we can do just yet without spending more time on these things during class, but please familiarize yourself with the definitions.

Exercise 9.4.1. (Exercise 2.5.95 in the Book) Let G be a group and let $H \leq G$.

1. Show that the subset $N(H) = \{g \in G \mid g^{-1}Hg = H\}$is a subgroup of G (Remember, this is not the same thing as $g^{-1}Hg$!)
2. Show that $H \leq N(H)$. (HINT: Remember being a subgroup means that you are a subset which is also a group. We already know that H is a group, so we only need to show that H is a subset of $N(H)$)).

Exercise 9.4.2. Prove for a homomorphism $\varphi : G \to H$ that

1. $\varphi(e_G) = e_H$
2. $\varphi(g^{-1}) = (\varphi(g))^{-1}$

§9.5 Funny Stuff

Remark 9.5.1. If you wrote an unreasonably long acronym in your notes, it stood for "that we will not prove today but at a later date"

Remark 9.5.2. The pronunciation of words like homogenous and homomorphism all use the same long O sound (like g**o**), NOT the short O sound (like **o**n or t**o**p)

10 Monday, May 1st (Class 10)

§10.1 Relations

Definition 10.1.1. A relation $\sim$ on a set X is a subset of $\psi \subseteq X \times X$ (where elements are in the form (a, b)) We say $a \sim b$ (or a is related to b) if $(a, b) \in \psi$

Definition 10.1.2. A relation is *reflexive* if $\forall a \in X, a \sim a$. A relation is *symmetric* if $\forall a, b \in X \ a \sim b \implies b \sim a$. A relation is *transitive* if $\forall a, b, c \in X, a \sim b \& b \sim c \implies a \sim c$. If a relation is reflexive, symmetric, and transitive, we call it an *equivalence relation.*

Example 10.1.3 1. Let our set be $\mathbb{Z}$. Define the relation $a \sim b \implies 7 \mid (a - b)$. Is this an equivalence relation?

2. Let our set be the people in the world. $x \sim y$ if x an y are siblings.

3. Let our set be $\mathbb{R}^\times$, and $x \sim y$ if $\frac{x}{y} > 0$.

Solution. 1. Yes, in fact this is our being equivalent mod 7.

2. This is not an equivalence relation, as you aren't your own sibling and stepsiblings exists, meaning we are not reflexive, we are symmetric, but we are not transitive.

3. Yes. This can be more simply stated as having the same sign.

□

Problem 10.1.4. Let $a, b \in G$. We say a is conjugate to b (written $a \sim b$) if $\exists\ g \in G$ such that $b = gag^{-1}$

Prove:

1. Conjugacy is an equivalence relation

2. Any two transpositions in S_n are conjugate.

Solution. Let $b = gag^{-1} = g_1 c g_1^{-1}$. Conjugacy is reflexive (let g be the identity), symmetric (let just multiply on the left by g^{-1} and on the right by g) and transitive $(a = g^{-1}g_1 c g_1^{-1} g = (g^{-1}g_1)c(g^{-1}g_1)^{-1}.)$

To solve the second part of the problem, we will return after developing a bit more theory about the symmetric group. □

§10.2 Symmetric Group

Let $h \in S_n$ and $a \in \{1, 2, ...n\}$. Treat this permutation like a function where we look at where a is taken by h, i.e $h(a) = b$. Let $\sigma \in S_n$. By inspection,

$$\sigma \circ h \circ \sigma^{-1}(\sigma(a)) = \sigma(b)$$

More generally if $h = (a_1 a_2 ... a_k)$ and we repeat this process many times, we can see that conjugating h by σ leads to the cycle $(\sigma(a_1)\sigma(a_2)...\sigma(a_k))$.

What this tells us is that conjugating preserves cycle structure, meaning conjugating transpositions gives us transpositions. So for two disjoint transpositions, i.e (ab) and (cd).

$$(ac)(bd)(ab)(ac)(bd) = (cd)$$

Furthermore, if we want to show (123) is conjugate to (456), our element would be $(14)(25)(36)$. We simply construct the permutation which takes each element where we want it to go.

§10.3 Conjugacy Classes

Definition 10.3.1. Given $g \in G$, the *conjugacy class* in g is the set of everything conjugate to g, which is denoted by $[g]$. Because conjugacy is an equivalence relation, these sets are either disjoint or equal.

In abelian groups, the conjugacy classes of an individual element would be themselves. We can conjecture that everything with the same cycle structure is in the same conjugacy class.

Let $H_1, H_2 \subseteq G$. H_1 is conjugate to H_2 (written $H_1 \sim H_2$) if

$$\exists\ g \in G \text{ such that } gH_1g^{-1} = H_2$$

we previously showed that if H_1 is a group, so is H_2.

note that

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

Take for example S_4. We have the subgroup $\{e, (12), (34)(12)(34)\}$. If we conjugate this by (13), then

$$(13)\{e, (12), (34)(12)(34)\}(13) = \{e, (23), (14), (14)(23)\}$$

which we can verify is another subgroup.

Exercise 10.3.2. Verify that the multiplication I did above is correct (it takes a long time to get familiar with S_n and D_n so don't get worried to just get your hands dirty and work with them a lot).

Definition 10.3.3. A subgroup H is *normal* in G (written as $H \trianglelefteq G$) if $gHg^{-1} = H \forall g \in G$.

§10.4 Exercises

We are going to do a dive into conjugacy classes and normal groups regarding the **dihedral group** next class, so exercises to get familiar with these concepts will be found in next section.

§10.5 Funny Stuff

> **Remark 10.5.1.** The *entire* class mistakenly called $\{e, (12), (34)(1234)\}$ a group. However, it was all corrected when Dr. Abramson told us that "That [(12)(34) instead of (1234)] is in my head what I had wrote"

11 Thursday, May 4th (Class 11)

Today, I'm lecturing! We will talk about the dihedral group and its conjugacy classes.

Exercise 11.0.1. Let G be a group and $g, a \in G$. What is $(gag^{-1})^n$

Recall that for a group G and $H \leq G$, the *index* of H in G is the number of left cosets of H and is referred to as $[G : H]$. We also have that if G is finite, $|G| = |G : H||H|$. There is absolutely nothing special about cosets being on the left, and all of the stuff that we proved earlier about cosets (that they partition a group, they are the same or disjoint, etc.) can also be applied to right cosets. Thus, it follows that $[G : H]$ is also the number of right cosets

> **Remark 11.0.2.** There is nothing forcing these left and right cosets to be the *exact same in general*, but we will soon analyze a special case in which they are.

Theorem 11.0.3
If $[G : H] = 2$ then $H \trianglelefteq G$ (i.e, $gHg^{-1} = H$ for all $g \in G$).

Proof. We know that we have two left cosets and two right cosets. For some $g \notin H$ we have the two left cosets H and gH and two right cosets H and Hg. Since these sets partition the group, $gH = Hg$. Because multiplication is associative,

$$gH = Hg \implies gHg^{-1} = (Hg)g^{-1} = H$$

which is the definition of being a normal subgroup. □

§11.1 Dihedral Group

Definition 11.1.1. Define D_{2n} to be the group of symmetries of a regular n-gon. We have the subgroup $R_{2n} = \{e, r, r^2, ...r^{n-1}\}$ where r is the rotation of $2\pi/n$. Similarly, we have the element s which is any old reflection.

Theorem 11.1.2
$R_{2n} \trianglelefteq D_{2n}$

Proof. It is sufficient to show that the index of R is two. As we know, if we reflect over and then rotate we get all of the symmetries on the 'other side' of the polygon (the two sets R and sR). Thus, we have index two and are consequently normal. □

Problem 11.1.3. Where's rs?

Solution. We know that rs is a reflection, so it must be sr^k for some $k \in \{1, 2, ...n-1\}$. We will find which k specifically in the next problem □

Problem 11.1.4. Since we are assuming that $rs = sr^k$, we can multiply by s on the left, yielding $srs = r^k$. Find the k for which $(srs) = r^k$.

Solution. $(srs)^a = sr^a s = r^{ak}$, from our do now. If we let $a = k$, then $sr^k s = r^{k^2}$. Notice that we could have multiplied by s on the right to $rs = sr^k$, giving us that $r = sr^k s$. Consolidating, we have

$$r = sr^k s = r^{k^2}$$

Thus $r^{k^2-1} = e \implies n \mid k^2 - 1$. We know that both $k = 1$ or $k = -1$ satisfy this constraint.

if $k = 1$ we want to find the order of sr. The order can't be odd, as $(sr)^m = sr^m$ but the identity cannot invert r^m. Thus, m must be even and the smallest m which satisfies this is $2n$ (n is an odd prime). However, this is the order of our group, meaning this is a cyclic group!

If $k = -1$, we have $sr^k s = r^- k \implies r^{-k} s = sr^k$. This turns out to be one of our constraints for being a dihedral group, which is being generated by the elements s and r and having $sr = r^{-1} s$. □

Problem 11.1.5. Find all of the conjugacy classes of D_{2n}

Solution. What can be conjugate to a reflection? Since reflections commute with eachother it would be meaningless to conjugate a reflection with another reflection. Instead, let's try conjugating a reflection with a rotation, namely sr^a.

$$(sr^a)r^b(sr^a)^{-1} = (sr^a)r^b(r^{-a}s) = sr^a s = r^{-a}$$

What this tells us is that by conjugating a rotation by any reflection we get its inverse. Thus, every rotation is in a conjugacy class with it's inverse. For the special case of r_{180} when we are in polygons with an even number of sides, it is alone instead of paired up in its conjugacy class.

What can be conjugate to a reflection? If we conjugated a reflection sr^a by r^b we get

$$r^b sr^a r^{-b} = sr^{-b} r^a r^{-b} = sr^{a-2b}$$

Similarly, if we conjugate a reflection sr^a by sr^b, we get

$$sr^b sr^a (sr^b)^{-1} = r^{-b} r^a r^{-b} s = sr^{2b-a}$$

.

What does this make of our conjugacy class? Well, we know that $sr^a \sim sr^b$ if a and b are the same parity (as we are changing by multiples of 2). For polygons with an even number of sides, this will give us two seperate conjugacy classes of reflections while in a polygon with an odd number of sides we have all reflections being conjugate to one another.

Visually, we can think about which points are fixed by each reflection.

> **Remark 11.1.6.** Geometrically, in an odd polygon every axis of symmetry passes through a vertex and a side (fixing one point– the vertex), while in an even polygon there are two types of axes for reflection, each corresponding to their own conjugacy class: those that pass through two vertices (or fix two verticies upon reflection) and those that pass through two sides (which fix no verticies upon reflection)

This exploration of conjugacy classes has shown us that they have deep insights about the structure of a group and its elements. As many authors on algebra textbooks say (and wikipedia), "The study of conjugacy classes of non-abelian groups is fundamental for the study of their structure" □

12 Monday, May 8th (Class 12)

§12.1 Cauchy's Theorem

Theorem 12.1.1

Suppose p is a prime and G is a group whose order is divisble by p. Then G has elements of order p

In order to prove this, we will have to 'count some stuff'.

§12.1.1 Thing 1

Consider all p-tuples $(g_1, g_2, ..., g_p)$in G^p (meaning $G \times G \times G ... \times G)p$ times) where

$$g_1 g_2 g_3 ... g_p = e$$

. For example, if we were in $\mathbb{Z}_{12}$, since $3 \mid 12$, we have p-tuples like (g^4, g^6, g^2) and (g^5, g^7, e).

Problem 12.1.2. How many p-tuples *(which are ordered lists) are there which satisfy this?

Solution. Remember that groups are closed and every element has inverses. Thus, the first $p-1$ elements you have complete freedom for, and just fix the last element to be the inverse of the product of all of the previous elements, i.e $g_p = g_{p-1}^{-1} \dots g_2^{-1} g_1^{-1}$. Thus, there are $|G|^{p-1}$ p-tuples which multiply to the identity. □

§12.1.2 Thing 2

Suppose (g, h, i, j, k) is one such 5- tuple which works.

Problem 12.1.3. Find me another.

Solution. We know that since this is the identity, if we invert it its *still* the identity. So we have $(k^{-1}, j^{-1}, i^{-1}, h^{-1}, g^{-1})$. But, we can also conjugate our product by g^{-1}.. Since the right side is still the identity, (h, i, j, k, g) is another tuple. □

Problem 12.1.4. Given a p-tuple, how many p tuples are potentially spawned in this fashion.

Solution. If all is well, we can cycle through p times. On a bad day, if we had all (e, e, e, e, e), theres only 1 we can make in this fashion. The p-tuples all go back to the beginning after cycling p times. This also means that our extreme situations cycle back in 1 time. Can they cycle back to the beginning in $1 < n < p$ times? □

Problem 12.1.5. Can they cycle back to the beginning in $1 < n < p$ times?

Solution. According to Joy, if it takes less than p times to cycle fully, that means that n needs to be a divisor of p. If you cycle back every n turns, you cycle back every an times (for an integer a), and similarly you cycle back every bp times for b an integer. Since our factors or p are just 1 and p, this is not possible. □

§12.1.3 Putting our things together

1. We have $|G|^{p-1}$ p-tuples
2. $p \mid |G|$
3. $(e, e, ...e)$ is one of our p-tuples
4. p-tuples tend to spawn in bunches of p

With this, we can prove $\exists$ elements of order p.

Proof. From our good-day tuples, we have kp tuples where k is an integer. From our bad-day, we get 1 p tuple. If we didn't have elements of order p, then we are claiming that $p \mid n^{p-1} = kp + 1$. Obviously this isn't possible, so we have to add our number of elements which are our bad day case (i.e, the elements of order p, yay!). Remember, this relies on the fact that they come in bunches of 1 or bunches of p. □

With this, we have proved that when p divides the order of the group, we must have elements of order p.

§12.2 Classifying Groups

Theorem 12.2.1

If p is prime, the only groups of order $2p$ are $\mathbb{Z}_{2p}$ and D_{2p}.

Proof. Due to Cauchy, we must have both elements r and s where $r^p = e$ and $s^2 = e$. We have the list of elements $e, r, r^2, ..., r^{p-1}, s, sr, sr^2, ..., sr^{p-1}$. Where is rs? We showed that since p is prime, $rs = sr$ or $rs = sr^{-1}$, which represents the cyclic group of order $2p$ and the dihedral group of $2p$. □

Group theorists want to find all groups of a certain order, and so far we haven't done only a couple in the first 20.

§12.3 Groups of Order 15

We don't have enough to prove this just yet, but we can create our starting ground now that we have our theorem. Claim: The only group of order 15 is Z_{15}.

We know that from cauchy, we must have an elements of order 3 and order 5 and that the elements must have order $1, 3, 5, 15$. If we are in a non cyclic group of order 15, then we can only have elements of order 3 or 5.

Let $g^3 = h^5 = e$. Our list of elements is thus

$$e, h, h^2, h^3, h^4$$

$$g, gh, gh^2, gh^3, gh^4$$

$$g^2, g^2hg^2h^2, g^2h^3, g^2h^4$$

§12.4 Funny Stuff

Remark 12.4.1. Why was the duck a such good detective. Because he always quacked the case!

Remark 12.4.2. Why was the duck such a good comedian. He made everyone quack up!

Remark 12.4.3. You are so $\sqrt{1+\tan^2 c}$.

13 Thursday, May 11th (Class 13)

$H \leq G$ is a normal subgroup (written $H \trianglelefteq G$) if $\forall g \in G, gHg^{-1} = H$ or $gH = Hg$

Recall that in an abelian group all subgroups are normal and that $[G : H] = 2 \implies H \trianglelefteq G$.

Theorem 13.0.1

Let $H \trianglelefteq G$ and $K \leq G$. Define

$$HK = \{hk \mid h \in H, k \in K\}.$$

Prove that $HK \leq G$.

Proof. The identity is easy.

$H \trianglelefteq G \implies \forall k \in GkH = Hk \implies \exists h'$ such that $kh = h'k$. Thus

$$h_1k_1h_2k_2 = h_1h_2'k_1k_2 = (h_1h_2')(k_1k_2) \in HK.$$

We are closed, we have our identity, we are associative (because the operation is associative). To show that we have inverses, $(hk)^{-1} = k^{-1}h^{-1} = h'^{-1}k^{-1} \in HK$.

□

Definition 13.0.2. Let $H \trianglelefteq G$. Denote G/H (called "G mod H") $= \{gH \mid g \in G\}$.

Theorem 13.0.3

G/H forms a group under the multiplication in G.

§13.1 Quotient Group

Example 13.1.1

$4\mathbb{Z} \trianglelefteq \mathbb{Z}$, and our operation is additions. Our cosets are $4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$. Everything in $\mathbb{Z}$ are in these cosets. $(2 + 4\mathbb{Z} + 3 + 4\mathbb{Z} = 1 + 4\mathbb{Z})$. $(2 + 4\mathbb{Z})^{-1}$

Definition 13.1.2. $\mathbb{Z}/n\mathbb{Z}$ is the correct name for $\mathbb{Z}_n$.

Proof. To show G/H is a group, we make use of the fact that $gH = Hg$. Firstly, the identity is H. For a sanity check.

$$(gH)H = g(HH) = gH$$

$$H(gH) = (Hg)H = (gH)H = gH$$

For closure,

$$g_1(Hg_2)H = g_1(g_2H)H = g_1g_2H.$$

For inverses,

$$(gH)^{-1} = H^{-1}g^{-1} = Hg^{-1} = g^{-1}H$$

.

Thus, these are subgroups (associativity is given). □

Example 13.1.3

$(\mathbb{Z}/8\mathbb{Z})/\{0,4\} = \{\{0,4\},\{1,5\},\{2,6\},\{3,7\}\}$. What does this look like? It looks like $\mathbb{Z}/4\mathbb{Z}$. These are in fact isomorphic.

Example 13.1.4

$D_{20}/R \cong \mathbb{Z}/2\mathbb{Z}$. Our cosets are the rotations and the reflection. (Recall that D_{20} is the dihedral group of order 20 and R is our rotations).

Example 13.1.5

$S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$ where S_n is the symmetric group and A_n was the alternating group (of just even permutations). The cosets are all even permutations.

§13.2 Dihedral group of order 4

The 180 degree rotation commutes with everything. Thus, $\{e, r_{180}\} \trianglelefteq D_8$. We know that $8/2 = 4$, meaning the quotient group could be one of two groups: $Z_2 \times Z_2$ or $\mathbb{Z}_4$. Our four cosets are $\{e, r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\}$. Also remember that everything in $Z_2 \times Z_2$ has order 2, so we can just check the order of every element. After checking, we see that everything has order 2, meaning they're isomorphic. We can generalize saying that $D_{4n}/\{e, r_{180}\} \cong \mathbb{Z}_n \times \mathbb{Z}_2$

Remark 13.2.1. Remember that elements of the quotient groups are the cosets. When you multiply the cosets, you multiply the element which translate them. So if you have $H \trianglelefteq G$, then $(aH)(bH) = (ab)H$. Alternatively, just multiple every element in the cosets. If you do that, you will end up with another coset, which in turn can help you determine what you have translating it by.

§13.3 Funny Stuff

Remark 13.3.1. Remember, Joy, that the index of the normal subgroup is the number of elements in the quotient group.

14 Monday, May 15th (Class 14)

Problem 14.0.1. Recall that in an abelian group, all subgroups are normal.

1. Describe $\mathbb{R}/\mathbb{Z}$
2. Prove or disprove: All elements of $\mathbb{Q}/\mathbb{Z}$ have finite order
3. Let $\tilde{\mathbb{Q}} = \{q^2 \mid q \in \mathbb{Q}\}$. What is
$$\tilde{\mathbb{Q}^\times}/\mathbb{Q}^\times$$

The answer to the first is $[0, 1)$ where when you add the number you take just the fractional part of their sum. For the second, you will have elements of $\frac{n}{m}$ where $0 \leq n < m$. This element will become 0 after a finite number of additions (m), so it must have finite order.

For the third one, notice that every non-identity element must have order 2. Every single coset has a representative that is square free (all of its prime factors only have an exponent of 1). It turns out that the cosets we can use is $n\tilde{\mathbb{Q}^\times}$ where n is squarefree. We know that $1/n$ and n are in the same coset, as $n * 1/n^2 = 1/n$. This means that we don't need to worry about any of the denominator. As an example,

$$15\tilde{\mathbb{Q}^\times} \times 35\tilde{\mathbb{Q}^\times} = 21\tilde{\mathbb{Q}^\times}$$

Definition 14.0.2. Circle group: $\{e^{i\theta} \mid \theta \in \mathbb{R}\}$ under multiplication

§14.1 Centralizer

Let G be a group and $g \in G$. The centralizer of g in G, written as Z_g, is

$$\{h \in G \mid gh = hg\},$$

or the set of all elements which commute with g. Moreover, the center of g, written $Z(G) = \{h \in G \mid hg = gh \ \forall g \in G\}$. You can think of the center as the intersection of all centralizers. For abelian groups, both the center and the centralizers are boring (the entire group).

Example 14.1.1
Prove $Z_g \leq G$

Rewrite our condition as $ghg^{-1} = h$. If we multiply two elements in the group, h_1, h_2, then because of the properties of conjugation, $h_1h_2 = gh_1h_2g^{-1}$, meaning that we are closed. Similarly, h^{-1} is in the group, as we can multiple on both sides of $gh = hg$ by h^{-1}, which is our condition for being in the group. Finally, our identity commutes with everything, meaning it must be in the centralizer of g.

Example 14.1.2
In S_5, find $Z_{(12)}$

We are trying to find all h for which $h(12)h^{-1} = h$. When you conjugate a cycle by a permutation, we have a permutation $\sigma \in S_5$, our cycle will go from (12) to $(\sigma(1)\sigma(2))$. There are 6 such permutation which leave one and two alone, and the other 6 can be found because $(12) = (21)$

15 Thursday, May 18th (Class 15)

§15.1 Do Now

Example 15.1.1
Let G be a group. If $G/Z(G)$ is cyclic, prove G is abelian.

Solution. This is a cyclic group, so call the coset which generates this $gZ(g)$. Suppose the order is n, meaning $g^n Z(g) = Z(g)$. Since cosets partition the group, every element in G can be written as $g^k z$. If we multiply this by an arbitrary element $g^l z'$,

$$(g^k z)(g^l z') = g^{k+l} zz' = (g^l z')(g^k z).$$

Thus, every element commutes with eachother, meaning G is abelian. □

Remark 15.1.2. If G is abelian, $Z(G) = G$ and $G/Z(G) \cong \{e\}$.

§15.2 Group Actions

Groups can 'act' on other objects.

Definition 15.2.1. Let G be a group and X a set. An *action* of G on X is a set of permutations ϕ_g of X (one for each g in the group) such that

1. If x is in X, $\phi_e(x) = x$
2. If x is in X. for all $g, h \in G$, $\phi_{gh}(x) = \phi_g(\phi_h(x))$

Example 15.2.2
Let $G = S_5$, and $X = \{1, 2, 3, 4, 5\}$. $\phi_{(123)}$ takes 1 to 2, 2 to 3, 3 to 1, 4 to 4, and 5 to 5.

Remark 15.2.3. Due to the way that we defined the symmetric group, we would expect this to work.

Example 15.2.4
Let $G = \mathbb{Z}_3$ and $X = \{a, b\}$ ϕ_0 has to leave everything the same. ϕ_1 could take a to b and b to a. According to our second rule, $\phi 0(x) = \phi_2(\phi_1(x))$, meaning ϕ_2 has to bring a to b and b to a. But, since $\phi_1(\phi_1(x)) = \phi_2$, ϕ_2 must bring a to a and b to b, so this action is no good. However if we defined every permutation to be the identity, the rules of an action still hold. This is called the *trivial action.*

§15.3 Orbits

Definition 15.3.1. Let $x \in X$. The orbit of x is everything that you can get to with one of these maps, namely

$$\text{orb}(x) = \{\phi_g(x) \mid g \in G\}.$$

For our first example, $\text{orb}(1) = \{1, 2, 3\} = \text{orb}(2) = \text{orb}(3)$

Example 15.3.2

Say we have our set X being the edges of a cube and $\mathbb{Z}_4$ acts on this set where we have 90 degree rotations. Then, our top edges, side edges, and bottom edges are in orbits together.

Problem 15.3.3. Can you find a nontrivial action of Z_3 on $\{a, b, c, d, e\}$?

Solution. Let $1(a) = b, 1(b) = c, 1(c) = a$ and $2(a) = c, 2(b) = a, 2(c) = b$. This gives us 1 orbit of size 3, and two orbits of size 1. □

Problem 15.3.4. Let $G \leq S_8$ where G is generated by $(123)(45)$ and (78). Our orbits would be $\{1, 2, 3\}, \{4, 5\}, \{7, 8\}, \{6\}$. This will be referred to as 'the previous problem'

Theorem 15.3.5

Orbits partition the set, meaning $\text{orb}(x) = \text{orb}(y)$ if and only if they are in eachother orbit.

Proof. There has to be some $g \in G$ such that $\phi_g(y) = x$, which implies $\phi_{g^{-1}}(y) = x$. Take an arbitrary $z \in \text{orb}(x)$. This is only true if $z = \phi_h(x)$ for some $h \in G$. Thus, $\phi_g(\phi_h(z)) = y$, meaning $z \in \text{orb}(y)$. □

§15.4 Stabilizers

Definition 15.4.1. GIven $x \in X$, the stabilizer of x is $\text{stab}(x) = \{g \in G \mid \phi_g(x) = x\}$, i.e all of the elements which do nothing to an element.

Example 15.4.2

In 'the previous problem', $\text{Stab}(1) = \{e, (45), (78), (45)(78)\}$.

Theorem 15.4.3

$\text{stab(x)} \leq G$.

Proof. We have the identity, and if $g, h \in \text{Stab(x)}$, $\phi_{gh}(x) = \phi_g(\phi_h(x)) = \phi_g(x) = x$, meaning that we have closure. By the same reasoning if $g \in \text{Stab(x)}$, $x = \phi_e(x) = \phi_{g^{-1}}\phi_g(x) = \phi_{g^{-1}}(x)$, meaning that we have an closure, an identity, inverses, and we are associative.

□

§15.5 Theorem with a name (Orbit-Stabilizer Theorem)

Theorem 15.5.1

For any $x \in X, |G| = |\text{Stab}(x)||\text{orb}(x)|$

Remark 15.5.2. The reason we failed with $\mathbb{Z}_3$ acting on $\{a, b\}$ is that any orbit of size 2 would need to divide 3.

Theorem 15.5.3

If orb(x)=orb(y). Then Stab(x) and Stab(y) are conjugate subgroups.

§15.6 Funny Stuff

Remark 15.6.1. Cameron guessed the name of the theorem with a name! (Who would have thought that after learning orbits and stabilizers our theorem would be named the orbit stabilizer theorem).

Remark 15.6.2. If a prisoner escapes from prison, drinks apple cider from a jug, and consumes an apple, its a Con-Jug-Ate!

16 Monday, May 22nd (Class 16)

Before we address proving the Orbit-Stabilizer theorem, we first return to parity in the symmetric group.

§16.1 Parity in the Symmetric Group

Theorem 16.1.1

Recall that an element of S_n is even if when it is decomposed into transpositions it has an even number of transpositions and odd otherwise. Prove that being even or odd is a well-defined notion (i.e that you cannot split an element into an even number of transpositions and an odd number of transpositions by decomposing it in different ways)

Proof. Let S_n act on the *Vandermonde polynomial* of an ordered set of n variables $x_1, x_2, ..., x_n$, which is

$$P(x_1, x_2, ..., x_n) = \prod_{1 \le i < j \le n} (x_j - x_i)$$

where are action simply permutes the indices of the variables. For instance, when $n = 3$ our polynomial is $(x_1 - x_2)(x_2 - x_3)(x_1 - x_3)$, and if we permuted the indices by (12) the polynomial would become $(x_2 - x_1)(x_1 - x_3)(x_1 - x_3) = -P(x_1, x_2, x_3)$, meaning that transposing it brough the polynomial to the negative of itself. We claim that acting on this polynomial by a transposition *always* brings it to the negative of itself.

Lemma 16.1.2

If (ab) is a transposition, $(ab)P = -P$ (where P is our polynomial in question)

Proof. WLOG $a < b$. We want to analyze what happens to $(ab)(x_i - x_j)$ with $i < j$. If neither of i, j are a, b, nothing happens. Then, we have to split into three cases: $j < a$, $a < j < b$, and $b < j$

1. Case 1 ($j < a$): The elements $(x_j - x_a)$ and $(x_j - x_b)$ will both be negated, leaving the polynomial unchanged.

2. Case 2 ($a < j < b$): We will have (ab) acting on $(x_a - x_j)(x_j - x_b)$, which becomes $(x_b - x_j)(x_j - x_a)$, which is still a double negation leaving the polynomial the same.

3. Case 3 ($b < j$): $(ab)[(x_a - x_j)(x_b - x_j)]$ is a double negation just like the first case, which levae the polynomial the same.

The only case we havent analyzed is $(ab)[x_a - x_b]$, which negates itself and causes the entire polynomial to become negative.

■

Since any element of the symmetric group can be decomposed and can act on the polynomial, the polynomial can only be positive, corresponding to an even number of transpositions, or odd, corresponding to an odd number of transpositions. Thus parity is well defined. □

§16.2 Proving the Orbit-Stabilizer Theorem

In class, you all went through the definitions of orbits and stabilizers again and then went through an example of a permutation subgroup acting on a set of elements, classifying the size of both the orbit and stabilizer and verifying it works. I will cut to the chase (as if you need definitions again, you can click here for orbits and click here for stabilizer.

Theorem 16.2.1

Let $x \in X$ be acted on by a group G. Then $|\text{orb}(x)||\text{stab}(x)| = |G|$

Proof. Suppose that if $X = \{x_1, x_2, x_3, ...x_n\}$, $\text{orb}(x_1) = \{x_1, x_a, x_b, ..., x_m\}$. For every element $g \in G$, $\phi_g(x_1) \in \text{orb}(x_1)$, so suppose two elements map to the same place, meaning $\phi_{g_1}(x_1) = \phi_{g_2}(x_1)$. This means that $x_1 = (\phi_{g_2^{-1}}(\phi_{g_1})(x_1))$, implying that $g_2^{-1}g_1 \in \text{stab}(x_1)$.

Now, if we loook at the left cosets of $\text{stab}(x_1)$, from what we just showed, $g_2^{-1}g_2 \in \text{stab}(x_1) \implies g_1 \in g_2\text{stab}(x_1)$. But we also know that $g_1 \in g_1\text{stab}(x_1)$ (since stabilizers are subgroups), and since left cosets are the same or disjoint, $g_1\text{stab}(x_1) = g_2\text{stab}(x_1)$.

Since every element in the orbit must have an element of g which maps x_1 to it, suppose g_a maps x_1 to x_a, g_b maps x_1 to x_b, and so on. When $\text{stab}(x)$ is multiplyed on the left by any of these elements, since they map x_1 to different places they must be different cosets (as we showed that when they map to the same element the must be the same coset). Furthermore, every element g must fall into one of these cosets (as the orbit accounts for every possible place x_1 could map with every element of G). Thus, every element of G falls into one of these cosets and there are $|\text{orb}(x_1)|$ of them. This means that $|\text{orb}(x_1)||\text{stab}(x_1)| = |G|$, proving the theorem. □

§16.3 Groups acting on themselves

An important aspect of group actions are when groups act on themselves. The usually do so through left/right multiplication, or conjugation. For the former, for some $g, h \in G$, $\phi_g(h) = gh$ is the action of left multiplication. On the other hand, $\phi_g(h) = ghg^{-1}$ is the action of conjugation.

17 Thursday, May 25th (Class 17)

§17.1 Groups acting on themselves by conjugation

Definition 17.1.1. For p prime, a $p-group$ is a group whose order is a power of p.

Theorem 17.1.2
If G is a $p-group$, then $Z(G)$ is nontrivial (meaning not just the identity).

Proof. We are going to let G act on itself by conjugation, i.e. if $g \in G$ and $h \in G$, $\phi_g(h) = ghg^{-1}$. We are going to look at orbits of ϕ_g. We also know from the orbit stabilizer theorem that the size of the orbit necessarily divides the size of the group. This means that the size of any orbit is a power of p and if we add the sum of sizes of distinct oribts, we get the size of the group (i.e if $|G| = p^n$, the sum of the sizes of distinct orbits is p^n).

If $h \in Z(G)$, then $\phi_g(h) = ghg^{-1} = hgg^{-1} = h$, meaning that if $h \in Z(G)$ the size of its orbit is 1. e is in the center, but if this was the only orbit of size 1 then the number of elements in the group would be 1 mod p but we need it to be divisible by p. Thus, there must be others. □

Remark 17.1.3. It is both necessary and sufficient that for this action $|\text{orb}(h)| = 1 \iff h \in Z(G)$

Theorem 17.1.4
For p prime, all groups of order p^2 are abelian and the only ones are $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof. We know that from our previous theorems we must have an element of order p and and we must have more than just the identity which commutes with everything. This means that if we aren't abliean, the center is neither the center of the group, and it can't be one, so the order of the center must be EXACTLY p (as the center is a subgroup and must divide the order of the group). Suppose $|G| = p^2, |Z(G)| = p$, and because it is of order p it must be a cyclic subgroup.

$$Z(G) = \langle h \rangle \text{ where } \mathrm{O}(h) = p$$

.

Let $g \in G$, $g \notin Z(G)$. $G/Z(G)$ will consist of cosets gZ. The cosets wil be able to form $g^k Z(G)$ where $k \in \{0, 1, 2, ..., p-1\}$. This is the set of all left cosets of $Z(G)$, meaning anything in G is of the form $g^r z$ where $z \in Z(G)$. If we multiply two arbitrary elements $g^r z_1$ and $g^s z_2$. If we multiply them and play around with the commutativity of elements in the center and powers of g, it can be shown that $g^r z_1 g^s z_2 = g^s z_2 g^r z_1$. This means that EVERY pair of elements commutes (because we started with arbitrary elements and they commuted). The group is therefore abelian, but why is it one of those two? If we

have an element of order p^2, we are cyclic. Otherwise, everything that isnt the identity has order p.

If every element has order p, we can look at the cyclic subgroups each element generates. If every element generates the same cyclic subgrop, we would be order p, meaning that we can take two of the elements and see that their intersection is solely the identity. Suppose our elements are, g and h, meaning that $\langle g\rangle \cup \langle h\rangle = \{e\}$. This also means that any product of two elements must be different, as if $g^a h^b = g^c h^d$, some power of g is another power of h, meaning their intersection is nonempty. This means that there are p options for each of the exponents and each element is different, meaning we have classified every element of the group.

§17.2 Remarks

No funny stuff for today as class was a half day and thus went by very quickly. Over the remainder of the year, we will likely get through items like The Lemma that is not Burnsides and the first sylow theorem. Have a great memorial day weekend everyone! □

18 Thursday, June 1 (Class 18)

§18.1 Burnside's Lemma

Lemma 18.1.1

Let G be a finite group which acts on the set X. Let X/G be the set of orbits of X (i.e each element of X/G is a distinct orbit, which taken together form the entire set). For any element $g \in G$, let X^g be the set of points that are fixed by g, i.e $\{x \in X \mid \phi_g(x) = x\}$. The lemma that is not burnsides states that

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

In english, this means that the number of orbits of a set X is the sum of the number of fixed points for each element g divided by the number of elements in the group.

Proof. This lemma directly follows from the orbit stabilizer theorem, stating that for an element $x \in X$,

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

where $\text{orb}(x) = \{\phi_g(x) \mid g \in G\}$ and $\text{stab}(x) = \{g \in G \mid \phi_g(x) = x\}$. The orbit is all of the places that x can go while the stabilizer is all of the members of the group which leave x fixed. We now want to use this to describe the number of orbits of a set, the sum of the number of fixed points for each elements, and the total size of the group.

Lets take a few steps back to what X^g and $\text{stab}(x)$ mean. The first is which elements g fixes, so X^g could be $\{x_1, x_2, ..., x_n\}$. $\text{stab}(x_1)$, on the other hand, are all $g \in G$ which fix x_1. meaning $\text{stab}(x_1)$ could look like $\{g_1, g_2, ..., g_n\}$. Each element is fixed by some amount of g's (i.e the size of its stabilizer) and each g fixes some amount of x's (i.e the size of X^g). Since we are adding up over all g,

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |\text{stab}(x)|. \tag{18.1}$$

This is the first important step in our proof. We want to get things as close as possible to orbits and stabilizers, so we used a nice counting argument to convert from X^g to $\text{stab}(x)$, namely that counting the number of elements which fix an element can be done in two ways: counting how many elements of the set are fixed by the elements of the group, and how many elements of the group fix an element of the set.

Now we are working with the statement

$$|X/G| = \frac{1}{|G|} \sum_{x \in X} |\text{stab}(x)|.$$

Now, we can utilize the orbit-stabilizer theorem.

$$\sum_{x \in X} |\text{stab}(x)|. = \sum_{x \in X} \frac{|G|}{|\text{orb}(x)|}.$$

We can factor $|G|$, making our new expression

$$|X/G| = \sum_{x \in X} \frac{1}{|\text{orb}(x)|}.$$

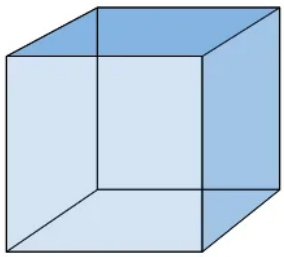
At this point, our equation may look more complicated than before. Is the right side even an integer? Well, consider if $|\text{orb}(x_1)| = n$. This means that the element x_1 wil contribute $\frac{1}{n}$. However, the orbit being size n means that there will be n elements for which we will have to contribute $\frac{1}{n}$, meaning that in this distinct orbit all n elements have contributed $\dfrac{1}{n}$, meaning this distinct orbit was counted once on the right side. This is the end of the proof, as now we can see that the expression on the right counts each distinct orbit exactly once, which is the definition of the left side. □

Example 18.1.2

How many *distinct* ways are there to color a cube with 3 colors up to rotations?

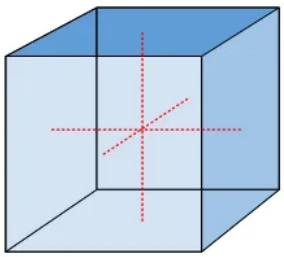
Solution. Let G be the rotations of a cube act on X, the set of all colorings. We want to count the number of orbits, as if you can rotate from one coloring to another that means they are in the same orbit. We make use of burnside's lemma and realize that we just need to sum up the number of elements fixed by each type of rotation and then divide by the total number of rotations.

First, what are the rotations of a cube?



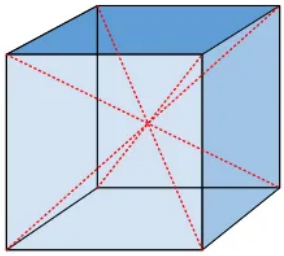
The identity rotation, or do nothing to the cube:

- 1 rotation



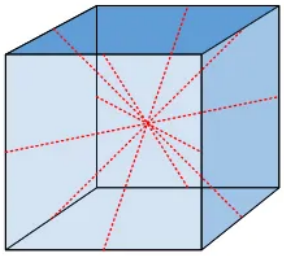
Rotate around lines through centres of opposing faces:

- 3 axes of rotation
- 3 rotations (90°, 180°, 270°)
- 3 × 3 = 9 rotations



Rotate around lines between diagonally opposing vertices:

- 4 axes of rotation
- 2 rotations (120°, 240°)
- 4 × 2 = 8 rotations



Rotate around lines between the mid-points of diagonally opposing edges:

- 6 axes of rotation
- 1 rotation (180°)
- 6 × 1 = 6 rotations

Total number of symmetrical rotations of a cube:

- 1 + 9 + 8 + 6 = 24

Remark 18.1.3. It is very, *very*, helpful to have a cube of some sort on hand. Otherwise many of these rotations (and finding which faces are fixed) are very difficult to visualize.

Now, we need to find how many elements are fixed by each rotation.

- The identity fixes every coloring, so it contributes 3^6
- The 90 and 270 degree rotations each leave their top and bottom faces fixed, meaning only the lateral edges all have to be the same color. This means 3^3 such elements are fixed and there are 6 such rotations.
- For 180 degree rotations through the center, we have freedom in two of the lateral edges and the top and bottom, meaning there are 3^4 elements fixed and 3 such rotations.
- The 120 and 240 degree fix the three faces touching each vertex on the line of rotation. That means we have 3^2 elements fixed and 8 such rotations.
- The 180 degree rotation brings each face to another face, meaning we have 3 pairs of faces and thus 3^3 elements fixed and 6 such rotations.

. Thus,

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g| = \frac{1}{24}(3^6 + 3^3 * 6 + 3^4 * 3 + 3^2 * 8 + 3^3 * 6) = \frac{1368}{24} = \boxed{57}$$

. □

19 Monday, June 5th (Class 19)

Example 19.0.1

You start a new Business - Baniel's Bracelets! You sell bracelets with 6 beads, each of which can be any of n colors.

1. How many bracelets if you can rotate the bracelet around your arm?
2. The same as 1 but you can also take it off and flip it?

Solution. From burnsides lemma, we want for the first one the number of elements fixed by each element of our group action divided by the size of the group. For the first, we have the rotations of a hexagon and the second D_{12}.

$$\frac{1}{6}(n^6 + n + n^2 + n^3 + n^2 + n) = \frac{n^6 + n^3 + 2n^2 + 2n}{6}$$

.

For the second, its the same but with rotations. We have two types of reflections, one which connects two midpoints and one which connects two edges.

$$\frac{1}{12}((n^6 + n^3 + 2n^2 + 2n) + 3n^3 + 3n^4) = \frac{n^6 + 3n^4 + 4n^3 + 2n^2 + 2n}{12}$$

□

§19.1 Sylow's First Theorem

Definition 19.1.1. A p-group is a group where its size is a power of p.

Theorem 19.1.2

Suppose $|G| = p^n k$ where p is prime and $p \nmid k$. Then G has a subgroup of order p^n

Lemma 19.1.3

$$p \nmid \binom{p^n k}{p^n}$$

Proof. Proof. Lets take care of all of the elements which have a factor of p

$$\frac{(p^n k)(p^n k - p)(p^n k - 2p)...(p^n k - p^n + p)}{(p^n)(p^n - p)(p^n - 2p)...(p)}.$$

Upon inspection each of the top and bottoms have the same amount of $p's$ as after factoring out the largest power of p the top and bottom cancel. I.e,

$$\frac{p^n k - ap}{p^n - ap} = \frac{p(p^{n-1}k - a)}{p(p^{n-1} - a)} = \frac{(p^{n-1}k - a)}{(p^{n-1} - a)},$$

where if a is not divisible by p, neither the top nor the denominator contribute factors of p. ■

We continue with group actions. Our set is

$$X = \{A \subseteq G \mid |A| = p^n\},$$

Meaning that X is all subsets of G such that the size of the subset is p^n. Consider $x_0 \in X$. Our group is $g \in G, \phi_g(X_0) = \{gx \mid x \in X_0\}$

> **Remark 19.1.4.** It is very important to track the exact meanings of the set and how the group acts on the set. The set is all subsets of the group of size $p^n k$ which have size p^n. The group acts on subsets of itself by left multiplication.

As Middelzong stated,

$$|X| = \binom{p^n k}{p^n}.$$

Can we say anything about $|\text{orb}(x_0)|$? Well clearly because of orbit-stabilizer,

$$|\text{orb}(x_0)| \mid p^n k.$$

Lets suppose we have $X_0 \in X$, where we know $|X_0| = p^n$. If we look at where this set maps to after being acted upon by g, we know that its size is $|\phi_g(x_0)| = p^n$. These two sets can intersect nontrivially, meaning their union is at most size $2p^n$. The way we defined our action means that we can acess every element in the group as each element is represented in atleast one element of the orbit. To elaborate, if we wanted to find the element h and we had the element g in our set X_0, we would just use the map $\phi_{hg^{-1}}(X_0)$ and we would be able to find a set in the orbit of X_0 which contains any element in the group.

If we wanted to fill the group, we could take the union of all the sets in the orbit, meaning we would need atleast k elements as if we take the union all of these sets with size p^n to get $p^n k$ elements. So a crude lower bound is

$$k \leq |\text{orb}(x_0)| \mid p^n k$$

§19.1.1 Lower Bound

Lets suppose we are working with $2^2 5$. $X = \{\{g_1, g_2, g_3, g_4\} \mid g_i \in G\}$. Our orbit will have elements $\{g_1, g_2, g_3, g_4\}$ and $\{gg_1, gg_2, gg_3, gg_4\}$. We aren't guarenteed that their intersections are nonempty, but every element of the group is in atleast one of the elements of this. When we take the union of all of the orbits, we get the whole group. So, there is no way we can do this with fewer than 5 elements in the orbit.

Since when we take the union of all the orbits we get the set X, which itself is not a multiple of p. The orbits are all disjoint, so when we add the sizes of each of these orbits we must have atleast one thing which is not a multiple of p. Therefore, the size of some orbit is not a multiple of p.

Lets called the orbit whose size is not a multiple of p as X_1. Putting our facts together, $|\text{orb}(X_1)| = k$. The largest thing which is not a multiple of p that divides $p^n k$ is k itself, and we know this thing is atleast k. Thus, the stabilizer is size p^n and the stabilizer is also a subgroup. We found our subgroup of size p^n.

□

Theorem 19.1.5

Suppose $p < q$ are both prime. Then

1. The group of size q is normal in any group of size pq.
2. If $q \not\equiv 1 \pmod{p}$ The only group of order pq is cyclic.

We will tackle these two theorems next class.

§19.2 Funny Stuff

Remark 19.2.1. Brennan could have owned a lucrative bead business had he been here.

Remark 19.2.2. Cam was forced to make his duck joke again. I wasnt going to include it until Sean reminded me that I could just say "Recall Cam's Duck joke." (Thanks Sean!)

20 Thursday, June 8th (Class 20)

§20.1 Theorems from Last Class

The whole class was dedicated to proving this one theorem.

Theorem 20.1.1

Let $q < p$ be primes. The only groups of order pq are cyclic unless $p \equiv 1 \pmod{q}$

Proof. Let G be a group of order pq. We know by Cauchy's theorem that there exist elements of order p and order q. Let $g^q = h^p = e$. We claim that $\langle h \rangle \trianglelefteq G$.

Lemma 20.1.2

$\langle h \rangle \trianglelefteq G$.

Proof. Suppose k is an element of order p with $k \notin \langle h \rangle$. Then $\langle k \rangle \cap \langle h \rangle = \{e\}$. Since these are both subgroups, the size of their intersection (which is a subgroup) must divide the order of both of the subgroups we are intersecting. Since they are both primes, the only element they share is the identity.

Consider the elements $k^a h^b, k^c h^d$ where $a, b, c, d \in \{0, 1, 2, ..., p-1\}$.. If $k^a h^b = k^c h^d$ then from what we proved in the last paragraph, $a = c$, $b = d$. This gives us p^2 different elements, but because $q < p \implies pq < p^2$, we have more elements than we did originally. Oops! This means that there cannot be another subgroup of order p.

Since there is only one subgroup of order p, if we conjugated $\langle h \rangle$ we get another subgroup which is order p, meaning $\forall a \in G \;\; a\langle h \rangle a^{-1} = \langle h \rangle$. This means $\langle h \rangle \trianglelefteq G$. ■

$\langle h \rangle \trianglelefteq G$, which means $ghg^{-1} = h^a$ for some $a \in \{1, 2, ..., p-1\}$. If $a = 1$ then $gh = hg$, meaning $g^r h^s$ commutes. Furthermore, $g^r h^s = g^t h^u$ only when $r = t$ and $s = u$. This gives us pq elements and the group is size pq, so every element is in this form. That means $(gh)^n = e \iff p \mid n \;\&\; q \mid n \implies o(gh) = pq$. This means that the group is cyclic.

However, that is when we suppose $a = 1$. Now suppose not, meaning $ghg^{-1} = h^a, a \neq 1$. In our discussion of conjugation and conjugacy classes a while ago, we showed that given $ghg^{-1} = h^a$ and that $(ghg^{-1})^a = gh^a g^{-1}$, we now have that $g^2 hg^{-2} = gh^a g^{-1} = h^{a^2}$, and since g^q is the identity, $h = g^q h g^{-q} = h^{a^q}$. This means $h^{a^q - 1} = e$.

We also know that the order of h is p. This means that $p \mid a^q - 1$. From Fermat's Little Theorem, we also know that $a^{p-1} \equiv 1 \pmod{p}$ and from the previous sentance, $a^q \equiv 1 \pmod{p}$.

Assume $q \not| (p-1)$. Then because q is prime, $\gcd((p-1), q) = 1$, meaning by Bezout's Lemma,

$$\exists r, s \in \mathbb{Z} \; r(p-1) + sq = 1,$$

meaning that

$$a^1 \equiv a^{r(p-1)+sq} \equiv (a^{p-1})^r * (a^q)^s \equiv 1 \pmod{p}.$$

But we assumed $a \not\equiv 1$! Uh oh! This makes sense as the dihedral group of order $2p$ for p some odd prime is not abelian nor cyclic (and p is always 1 mod 2). The next best item is 21, which we will discuss next time (as 7 is 1 mod 3). □

§20.2 Funny Stuff

Remark 20.2.1. Brennan was quite displeased of the repeated use of variable names. This isn't VSCode, Brennan! We aren't being 'overly restrictive'. Thankfully, Dr. Abramson became cautious and started creating many names for many variables.

21 Monday, June 12th (Class 20.5)

§21.1 The Futurama Theorem

Thank you to Brennan for preparing this lecture. Much of this primer was taken directly from the Futurama Wiki. Futurama is an American animated science fiction sitcom created by Matt Groening for the Fox Broadcasting Company and later revived by Comedy Central. The Futurama theorem is a real-life mathematical theorem invented by writer Ken Keeler (who holds a PhD in applied mathematics from Harvard), purely for use in the Season 6 episode "The Prisoner of Benda".

In the episode "The Prisoner of Benda", Professor Farnsworth and Amy create a mind-switching machine, only to afterwards realise that when two people have switched minds, they can never switch back with each other. Throughout the episode, the Professor and a few mathematicians try to find a way to solve the problem using two or more additional bodies, and, in the end, the solution is shown both in action and on the board. The theorem proves that, regardless of how many mind switches between two bodies have been made, they can still all be restored to their original bodies using only two extra people, provided these two people have not had any mind switches prior (assuming two people cannot switch minds back with each other after their original switch).

First, lets label the people who are present

1. Michael
2. Shawn
3. Daniel
4. Cam
5. Devon
6. Joy
7. Krish
8. Gabe
9. Handy
10. Kimberly

Now, we begin to swap them. (Terri and Sam will be special people who are left alone now)

Michael and Gabe Swap
Shawn and Daniel Swap
'Daniel' swaps with Cam
'Cam' swaps with Devon
'Devon' swaps with Krish
'Krish' swaps with Joy
'Gabe' swaps with Shawn
Handy swaps with Daniel

Kimberly swaps with Cam
This can be represented by

$$(4\ 10)(3\ 9)(2\ 8)(6\ 7)(6\ 10)(5\ 7)(4\ 5)(3\ 4)(2\ 3)(1\ 8)$$

$$(1264938)(5\ 10\ 7)$$

The two bodies cannot be in the same machine but the two minds can be. How many extra bodies do we need to make everything back to normal?

Let m be the number of extra bodies

1. If $m = 0$, then if (12) we can't do anything.
2. If $m = 1$, then if we started with (12), the only options we can use are $(2X)$ or $(1X)$, which we can't do anything

Now we are in the case that $m = 2$. If we have two additional people X and Y. It turns out that $(xy)(2x)(1y)(2y)(1x) = (12)$. So this works out so far.

What if we had a k-cycle?

WLOG we are trying to invert $\theta = (12...k)$. Fix some variable i such that $1 < 1 < k$. Let $\alpha = (1x)(2x)...(ix)$ and $\beta = ((i+1)y)((i+2)y)...(ky)$.

$$\alpha = (i(i-1)...21x)$$

$$\beta = (k(k-1)...(i+1)iy)$$

Consider $\pi = \alpha\beta(i+1\ x)(1\ y)$

Lets look at where an element t is taken by one of these permutations.

If $t \in \{2, 3..., i\}$, then $\pi(t) = \alpha\beta(t) = \alpha(t) = t - 1 = \theta^{-1}(t)$

If $t \in \{i+2, ...k\}$ then $\pi(t) = \alpha\beta(t) = \alpha(t-1) = t - 1 = \theta^{-1}(t)$

If $t = 1$ then $\pi(1) = \alpha\beta(y) = \alpha(k) = k = \theta^{-1}(t)$ If $t = i + 1$ then $\pi(i+1) = \alpha\beta(x) = \alpha(x) = i = \theta^{-1}(t)$ If $t = x$ then $\pi(x) = y$ and by pidgeonhole and $\pi(y) = x$ Thus, $\theta^{-1} = (xy)\pi$.

What if we have more cycles in our permutation? If the number of cycles is even, $\sigma^{-1} = \pi_r...\pi_2\pi_1$, and if the number of cycles is odd then its $\sigma^{-1} = (xy)\pi_r...\pi_2\pi_1$

In class we actually untangled this mess, but you as the reader could try it for yourself.

22 Thursday, June 15th (Class 21)

Definition 22.0.1. A free group over a given set consists of all 'words' that can be built from members of the set, considering two words to be different unless their equality follows from the group axioms. The members of the set are called generators of the free group, and the number of generators is the rank of the free group.

Example 22.0.2

Suppose we have the free group of the letters in the english alphabet (a through z) such that every generator has order two. Furthermore, suppose that all fifty states (which are words) are the identity of the group. What is this group isomorphic to?

For example, a nice starting point could be *mississippi*. Using our conditions, $e = mississippi = m$, meaning that we can erase the m from every word as it is the identity.

Solution. It turns out that after a lot of simplification this group is $\mathbb{Z}_2$. The only thing which remains is q, which does not appear in any of the states. Everything else is equal to the identity. □