MATH 403A: Introduction to Modern Algebra II

University of Washington

Andrew Chen

Winter 2026

Hello and welcome! This is my lecture notes on MATH 403A: Modern Algebra II. This course is the second of three courses on abstract algebra offered here at UW, covering Rings, **Groups**, and Galois Theory, respectively. Why is the second course 403 and not 402? Who knows. The professor is **Natalie Naehrig**, and we meet MWF at **10:30 am** for lectures. The textbook that we are using is **Thomas W. Hungerford's Abstract Algebra, an Introduction**. Also note that theorem names might not necessarily be accurate; it's probably just whatever my textbook / professor said it is.

The goal of these lecture notes is to write **understandable** math. As the great Albert Einstein put it, "If you can't explain it to a six year old, then you don't understand it yourself". The hope is that anyone coming across these notes (like you!) will be able to at least take away the gist of these concepts. Should you find any errors in my mathematics, please contact me at zchen66@uw.edu

Contents

List of Definitions

List of Theorems

1 Lecture 01: Jan. 5th

Today was the first lecture of the quarter! We went over basic course logistics, including the very in-depth syllabus lol. It is definitely a unique take on an upper-div mathematics course. Additionally, we've defined the main player of the course: groups.

1.1 Course logistics

A little more on the logistics of this course that I did not cover in the premable. This course is taught in a **flipped-classroom** setting, meaning that prior to each in-person lecture, students are responsible for watching an introductory "mini" lecture that briefly covers the contents of the lecture at a high-level, so that students may bring questions into lecture, and lecture times can be better alotted for more proof-based and in-depth discussions, as well as examples.

Students will be assessed by 4 bi-weekly quizzes throughout the quarter, and surprisingly, there will be no final exam. Rather, students are also responsible for creating "mindmaps" of concepts covered in lecture.

As for the nature of these lecture notes, I will take notes on both the pre-lecture materials, as well as the proofs and examples covered in lecture. Contents will be grouped together (pre and during lecture) by the specific lecture dates.

7.1 Groups

Without further ado, we dove straight into the course content and began discussing groups.

Definition (Groups)**.** A **group** is a *non-empty* set G equipped with a binary operation $* : (a, b) \mapsto a * b$, which satisfies the following axioms:

1. Closure: if $a, b \in G$, then $a * b \in G$
2. Associativity: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$
3. There exists an element $e \in G$ (called the **identity element** of G) such that $a * e = e * a = a$ for all $a \in G$
4. For each $a \in G$, there is an element $d \in G$ (called the **inverse** of a) such that $a * d = e$ and $d * a = e$

   Furthermore, a group G is called **abelian** if it additionally satisfies
5. Commutativity: $a * b = b * a$ for all $a, b \in G$

Moreover, a group is called *finite* or of *finite order* if it has only finitely many elements. Here, the number of elements of G is called the **order** of G. If G has infinitely many elements, it is said to be of *infinite order*.

Immediately, my mind went to thinking about the real numbers and how a group could be defined there. But instead, the professor began with quite an inteersting example.

Example 1.1. We discuss the **Symmetric Group** S_3, which is defined as follows:

Definition (Symmetric groups)**.** A symmetric group S_i is the collection of all bijective functions on i points. In other words, it is the collection of all permutations on $\{1, \ldots, i\}$.

For example, S_3 would contain all bijective functions defined from $\{1, 2, 3\} \to \{1, 2, 3\}$. We denote elements in S_3 using the following notation:

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \in S_3$$

$$f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Here, the top row of the "matrices" represents the original ordering of the elements $1, 2, 3$, and the bottom row represents the permutation $2, 1, 3$ that is the output of f_1. For example, $f_2(1) = 2$, $f_2(2) = 1$, $f_2(3) = 3$ in this case.

What we have failed to do thus far is define a proper binary operation on this group. How exactly can we say $f_i * f_j$? Well, recall that elements of S_3 are all functions, and we can "combine" functions using our good composition of functions: $f_i \circ f_j$.

Let's investigate this a bit using $f_2 \circ f_5$:

$$f_2 \circ f_5(1) = f_2(3) = 3 \qquad f_2 \circ f_5(2) = f_2(2) = 1 \qquad f_2 \circ f_5(3) = f_2(1) = 2$$

We see that

$$f_2 \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_6 \in S_3$$

Interesting, we can hypothesize that the functional composition operation seems to be closed in S_3. Is this always the case though?

Turns out, this is exactly the case since the composition of bijective functions must remain bijective, and since S_3 contains *all* bijective functions, the operation must be closed.

And with that, we can actually make some pretty important observations:

1. S_3 is obviously non-empty
2. We've shown that the operation $*$ is closed in S_3
3. Combining functions is associative by nature
4. f_1 is the identity element
5. Since all functions of S_3 are bijective, they must be invertible by nature.

Thus, S_3 is indeed a group. Is it abelian though? We can see that

$$f_5 * f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2 * f_5$$

And we conclude this example that the symmetric group S_3 is a non-abelian group of order 6.

Let's take a look at another example, but this time, we will omit the axioms and only look at the definition.

Example 1.2. This time, we discuss the **Dihedral Group** D_4, which is defined as follows:

Definition (Dihedral groups)**.** A dihedral group D_n is the collection of all operations on a regular, n-sided polygon.

For example, in D_4, the operations are the following:

- $r_0 :=$ rotation of $\deg 0$
- $r_1 :=$ rotation of $\deg 90$
- $r_2 :=$ rotation of $\deg 180$
- $r_3 :=$ rotation of $\deg 270$
- $d :=$ reflection across the x-axis
- $t :=$ reflection across the y-axis
- $h :=$ reflection across $y = x$
- $v :=$ reflection across $y = -x$

The combination of these operations form a group. Source: trust me bro.

2 Lecture 02: Jan. 7th

summary

7.1 Groups (cont'd)

This part of the notes is on the pre-lecture, which is in the form of textbook reading. Essentially, we explored many many more examples of groups to solidify our understanding. I will highlight below some of the important examples.

Example 2.1. The nonzero rational numbers $\mathbb{Q}^*$, the nonzero real numbers $\mathbb{R}^*$, and the nonzero complex numbers $\mathbb{C}^*$ are all ablean groups under multiplication.

This is because each system is closed under multiplication, and the existance of the identity 1 as well as the inverse for any element a being $1/a$. Most importantly, note that **0 is excluded in all of these**.

Remark. Rings are never groups under multiplication because the additive identity 0 will never be invertible.

Example 2.2. In general for some integer n, the nonzero elements of $\mathbb{Z}_n$ do not form a group under multiplication because (among many other things) closure fails. For instance, in $\mathbb{Z}_6$, we have $2 \cdot 3 = 0 \notin \mathbb{Z}_6 \setminus \{0\}$.

However, whence $n = p$ for prime p, then $\mathbb{Z}_p \setminus \{0\}$ forms a group. This is because all elements in $\mathbb{Z}_p$ are invertible since they are all co-prime with the modulus.

More generally, in $\mathbb{Z}_n$, all elements that are co-prime with n will form a group under multiplication as well. We denote this set of elements by U_n. In other words, U_n is the set of *units* of $\mathbb{Z}_n$.

Example 2.3. The set of matrices

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \text{where } a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}$$

is a group under multiplication. We call this the **general linear group** of degree 2 over $\mathbb{R}$ and denoted $GL(2, \mathbb{R})$ (and sometimes $GL_2(\mathbb{R})$). Since we have the condition $ad - bc \neq 0$, we know that these matrices must be invertible. Additionally, the identity matrix is apart of the set.

Closure is a bit tricky as we have to show that the product mustn't be the zero matrix. Suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ are in $GL(2, \mathbb{R})$. Upon multiplication, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}$$

Now, verify that

$$(aw + by)(cx + dz) - (ax + bz)(cw + dy) = (ad - bc)(wz - xy) \neq 0$$

since the product of two nonzero real numbers cannot be 0 ($\mathbb{R}$ is an integral domain!).

Remark. The same result holds for general linear groups formed with $\mathbb{Q}, \mathbb{C}, \mathbb{Z}_p$ with p prime. Note here that $\mathbb{Z}_p$ may contain the zero element, so long as $ad - bc$ is still satisfied in $GL(2, \mathbb{Z}_p)$.

*****

We began the in-person lecture with a few theorems.

Theorem 7.2.

The nonzero elements F^* of a field F form a group under multiplication. (Note: the definition of a field comes with $1 \neq 0$)

Proof. We show that F^* satisfies all criterias of a group:

1. Closure: for $a, b \in F^*$, we must have $ab \in F \setminus \{0\} = F^*$ since F is an integral domain
2. Associativity: implied since F is a ring
3. Identity: F, as a field, is defined to have an identity element $1 \neq 0$
4. Inverses: F^* has unit elements that, by definition all have inverses

□

Theorem 7.3.

Let R be a ring with identity e and let U be the set of all units in R. The U is a group under multiplication.

Having these ideas in mind, we visit some examples.

Example 2.4. Take $R = \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$. The units are all elements of the set which are coprime with 8. In other words, we have

$$U = \{1, 3, 5, 7\}$$

which form a group under multiplication.

Now that we've taken a look at all the ways in which groups can be formed from rings, what if we wanted to make our own groups from other groups?

This is a great segue into talking about cartesian products and how to construct groups.

Theorem 7.4.

Let G be a group with operation $*$ and let H be a group with operation $\diamond$. Define an operation $\cdot$ on $G \times H$ such that

$$(a, b) \cdot (c, d) = (a * c, b \diamond d)$$

Then $G \times H$ is a group too. If G and H are abelian then so is $G \times H$. If H and H are finite, then so is $G \times H$, and $|G \times H| = |G||H|$.

7.2 Properties of groups

Before we begin talking about some of the more non-trivial properties of groups, let's first clear up the notational mess that we've been stuck in for a bit.

In general, if we are dealing with abstract groups, then we agree on using the multiplication symbol, which is the standard notation. So from this point on, we write $ab = a * b$. There really isn't a difference between this "clash" of notation, but we're just lazy to write the $*$ I guess lol.

Note that if we are working with addition, such as in $\mathbb{Z}, \mathbb{Z}_n, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, we will continue using the $+$ sign for the group operation, just to not confuse ourselves.

To clear it up,

	Muliplicative notation	**Additive Notation**
Operation:	ab	$a + b$
Identity:	e	0
Inverse:	a^{-1}	$-a$

Additionnally, notice that for rings such as $\mathbb{Z}$, they only form a group with respect to the addition $+$ operation, since elements may not have multiplicative inverses and thus fails to form a group in that regard.

Thus, in the future when we refer to rings like $\mathbb{Z}$ as a "group", it is automatically implied that we mean as a group with respect to $+$.

Let's get back to our theorems.

Theorem 7.5.

Let G be a group and let $a, b, c \in G$. Then,

1. *G has a unique identity element*
2. *Cancelation holds: If $ab = ac$ then $b = c$ and if $ba = ca$ then $b = c$*
3. *Each element has a unique inverse*

Proof. (1) Assume e, e' are both identity elements. Then, we have

$$e = ee' = e'$$

since both elements are identities, they must be equal.

(2) If $ab = ac$, then

$$a^{-1}ab = a^{-1}ac \quad \Rightarrow \quad eb = ec \quad \Rightarrow \quad b = c$$

(3) Let $a \in G$ and let $a^{-1}, \tilde{a}^{-1}$ be inverses of a. Then,

$$a^{-1} = a^{-1}e = a^{-1}(a\tilde{a}^{-1}) = (a^{-1}a)\tilde{a}^{-1} = e\tilde{a}^{-1} = \tilde{a}^{-1}$$

□

3 Lecture 03: Jan. 9th

summary

7.2 Properties of groups (cont'd)

This part of the notes is on the pre-lecture. We begin with a conversation on group exponentiation.

Definition (Group exponentiation)**.** Let G be a group and $a \in G$ be arbitrary. Then, for some $n \in \mathbb{N}$, we define

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ times}}$$

Furthermore, we have tho following properties:

1. For identity e of G, we have $a^0 = e$
2. $a^n = a \cdot a^{n-1}$
3. $a^{-n} = a^{-1}a^{-n+1}$

Remark. Be very careful when working with abelian groups. In general,

$$(ab)^n \neq a^n b^n$$

With this definition now, we need to make an addition to our notation table from the previous lecture.

	Muliplicative notation	**Additive Notation**
Operation:	ab	$a + b$
Identity:	e	0
Inverse:	a^{-1}	$-a$
Exponents:	$a^n = aa \cdots a (n \text{ factors})$	$na = a + a + \cdots + a (n \text{ summands})$

Fantastic! We now moved onto another definition:

Definition (Element order)**.** Let G be a group and let $a \in G$.

1. a is said to be of **finite order** if there is a positive k such that $a^k = e$
2. In the above case, the *smallest* such integer n such that $a^n = e$ is called the **order** of a and denoted $|a|$.
3. If there is not such positive k, ie if $a^k \neq 0$ for all $k > 0$, we say that a has **infinite order**.

Example 3.1. Find the order of every element in S_3.

We see that

$$\left|\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right| = \left|\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right| = \left|\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right| = 2$$

and

$$\left|\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right| = \left|\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right| = 3$$

There are a couple key observations we can make after playing around with S_3 in this example.

The first is that since elements of S_3 represent permutations, if we shuffle the elements following the same rule again and again, we will always end up at our original position.

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

and through applying the same rule, we sometimes pass by some "intermediate" steps that are also elemenst of the same group, as seen with $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ in the above case.

Another observation, perhaps more nontrivial, is that all possible orders of elements (1, 2, and 3) all divides the total order of the group $|S_3| = 3! = 6$.

Let's explore if both of these observations always holds and can be generalized to other groups. Consider the following theorem:

Theorem 7.8.

Let G be a group and let $a \in G$.

1. *If $a^i = a^j$ with $i \neq j$, then a has finite order.*
2. *If a has infinite order then the elements a^k, where $k \in \mathbb{Z}$, are all distinct.*

Proof. Let $i \neq j > 0$ and WLOG assume $i > j$. Then, $a^i = a^j$ implies that $a^i \cdot a^{-j} = a^j \cdot a^{-j}$. With a bit more manipulation, we see that

$$a^{i-j} = a^0 = e$$

And since $i > j$, we have $i - j > 0$, so $|a| \leq i - j$, and we conclude that a has finite order.

(2) is the contrapositive of the statement we've just proved. □

Great! Essentially, the theorem we've just proved says that if an element is "cyclic" in anyway, as in applying the group operation to itself eventually leads back to itself, then the element *must* have finite order.

In fact, intuitively this tells us that *all* elements of a finite group must have finite order. But that fact, along with observation (2) we've made above, will be shown more clearly in the following theorem:

Theorem 7.9.

Lete G be a group and let $a \in G$ with order n.

1. *$a^k = e$ if and only if $n \mid k$.*
2. *$a^i = a^j$ if and only if $i \equiv j \mod k$.*
3. *If $n = td$, with $d \geq 1$, then a^t has order d.*

Proof. (1) ($\Rightarrow$) We begin with the division theorem and suppose that $k = nq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. From here,

$$e = a^k = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$$

As $|a| = n$, by definition, n must be the *smallest* positive integer with $a^n = e$. This implies that we must have $r = 0$ since $r < n$. Thus, $k = nq$ which means $n \mid k$.

($\Leftarrow$) If $nq = k$, then $a^k = (a^n)^q = e^q = e$.

(2) If $a^i = a^j$, when WLOG $i \geq j$...

(3) Let $n = td$. Then $(a^t)^d = a^{td} = e$. Additionally, let $k \in \mathbb{Z}$ such that $(a^t)^k = e$ as well. We wish to show $d \leq k$. If $(a^t)^k = e$, then $n \mid tk$ as proven above. Furthermore, by the hypothesis, $td \mid tk$, which means there exists some $m \in \mathbb{Z}$ such that $tdm = tk$, which implies $dm = k$ and $d \mid k$. Thus, $d \leq k$ by definition of divides. □

4 Lecture 04: Jan. 12th

summary

7.2 Properties of groups (cont'd)

Picking up from where we left off, we have the following corollary.

Corollary 4.0.1.
Element c with largest order, i.e. all a have $|a| < |c|$, then all orders divide $|c|$.

Then, ...

7.3 Subgroups

Today we began our discussion with subgroups. Let's begin with the definition.

Definition (Subgroups)**.** A subset H of a group G is a **subgroup of** G, and denoted $H \leq G$, if H is itself a group under the *same* operation in G.

Let's take a look at some examples!

Example 4.1. $\{e\}$ and G are subgroups of G. These are known as the **trivial subgroups** of G. In fact, all other subgroups are called **proper subgroups**.

Example 4.2. $\mathbb{Z} \subseteq \mathbb{Q}$ is a subgroup *only under addition '+'*. Because recall that integers do not have multiplicative inverses.

Example 4.3. $\{1, -1, i, -i\} \subseteq \mathbb{C}^*$ is a subgroup. This is interesting because it is a non-trivial finite subgroup in an infinite group.

Example 4.4. $H = \{1, 3\} \subseteq U_8 = \{1, 3, 5, 7\}$ is a subgroup. We can check because in $\mathbb{Z}_8$, we have $3^{-1} = 3$ and $1^{-1} = 1$. The other conditions then follow.

Example 4.5. $H = \{(0, 0), (3, 0), (0, 2), (3, 2)\} \subseteq \mathbb{Z}_6 \times \mathbb{Z}_4$ is a subgroup... but under which operation? Well, given that $\mathbb{Z}_6$ and $\mathbb{Z}_4$ are groups under addition, we say that H is a subgroup with respect to addition.

Through the explorations from the examples above, we may have picked up a few patterns, specifically regarding which of the original 4 conditions we need to check in order to conclude if something is a subgroup or not.

For example... why do we *not* need to prove associativity in H?

Well, since the same operation of G is inherited by subgroups H, and we know that the operation is associative in G, it then *must* be associative in H anyway.

What about closure? identity? inverse?

Theorem 7.11.

*A **nonempty** subset H of a group G is a subgroup of G provided that*

1. *If $a, b \in H$, then $ab \in H$.*
2. *If $a \in H$, then $a^{-1} \in H$.*

Proof. Closure and inverses are given by the conditions of the theorem. We've also shown that associativity does not need to be shown since the same operation is inherited. Finally, we have that if $a \in H$ and $a^{-1} \in H$, then $aa^{-1} = e \in H$. □

Let's practice!

Example 4.6. Show that $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$ is a subgroup of $GL(2, \mathbb{R})$.

To show this, we check the 3 conditions from the previous theorem.

1. Clearly $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}$, and thus H is nonempty.
2. Let $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, then

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

   And since $a + b \in \mathbb{R}$, we have $AB \in H$.

3. Define $A^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix}$. Then,

$$AA^{-1} = \begin{pmatrix} 1 & a + (-a) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

We thus conclude that H is a subgroup of $GL(2, \mathbb{R})$.

5 Lecture 05: Jan. 14th

summary

7.3 Subgroups (cont'd)

Recall our conversation last lecture about subgroups, and specifically, how to prove that something is a subgroup or not. To do this, we studied a theorem that stated that a subgroup must (1) be closed and (2) contain inverses. The existance of these two properties will imply the rest.

BUT! It can sometimes feel like a lot of work to check all the properties that make something a subgroup. Wouldn't it be nice if we had a shortcut whence some other properties are satisfied??

Well, we do.

Theorem 7.12.
Let H be a nonempty finite subset of G. If H is closed the operation in G, then H is a subgroup of G.

Proof. By **theorem 7.11**, we only need to prove that the inverse of a is in H. Since H is finite, we know that for some arbitrary $a \in H$, a must have finite order n. Further, since $n - 1 \equiv -1 \pmod{n}$, we have $a^{n-1} = a^{-1}$ by the cyclic nature of finite groups. There are two cases here:

(1) If $n > 1$, then $a^{n-1} = a^{-1} \in H$, since H is closed under the group operation.
(2) If $n = 1$, then $a^1 = e = a^{-1}$, so $a^{-1} \in H$ as well. □

Let's take a look at some examples where we can apply our newly learned trick.

Example 5.1. Let $H = \{f \in S_5 : f(1) = 1\}$. Note $|S_5|$ is finite, meaning H is also finite. Furthermore, we see that $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \in H$. By theorem proved sometime before, we need to prove that the group operation $\circ$ is closed in H.

Let $f, g \in H$ be some bijective functions, which means $f(1) = 1$ and $g(1) = 1$. Then,

$$f \circ g(1) = f(g(1)) = f(1) = 1$$

Clearly, $f \circ g \in H$ as well. Since $\circ$ is closed in H, we conclude that H is a finite subgroup of S_5.

Now that we know what a subgroup is, let's take a look at some special examples of subgroups. But first, we need to establish some definitions:

Definition (Center)**.** Let G be a group. The **center** of G is defined as

$$Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$$

Note that $e \in Z(G)$ always.

Why did we define this? Well, it turns out, we have the following theorem relating to *center subgroups*.

Theorem 7.13.
The center $Z(G)$ of a group G is a subgroup of G.

Proof. We show all the properties of a subgroup.

- $e \in Z(G)$ trivially, so $Z(G) \neq \emptyset$
- For some $a, b \in Z(G)$, we want to show $ab \in Z(G)$. To show this, notice for any $g \in G$, we have
$$abg = a(bg) = a(gb) = (ag)b = (ga)b = gab$$
- For some $a \in Z(G)$, we want to show $a^{-1} \in Z(G)$. Since a is a center, we see that $ag = ga$ for all $g \in G$. Then, multiplying on the left by a^{-1}, we have $g = a^{-1}ga$. Finally, multiplying on the right by a^{-1}, we end up with
$$ga^{-1} = a^{-1}g$$
as desired.

□

Another special example of a subgroup that we concern ourselves with is the *cyclic subgroup*.

But first again, let's go over some definitions. We are interested in the following interesting exponentiated set. We define

$$\langle a \rangle = \{..., a^{-2}, a^{-1}, a^0, a^1, a^2, ...\} = \{a^n \mid n \in \mathbb{Z}\}$$

This gives us lots to talk about.

Theorem 7.14.
*If G is a group and $a \in G$, then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G known as the **cyclic subgroup**.*

Proof. The product of any two elements of $\langle a \rangle$ is also in $\langle a \rangle$ because $a^i a^j = a^{i+j}$. The inverse of a^k is a^{-k}, which is also in $\langle a \rangle$. By the theorem above, this creates a subgroup of G. □

Let's talk more about these interesting cyclic subgroups. We have the following theorem:

Theorem 7.15.

Let G be a group and let $a \in G$. Then,

1. *If a has infinite order, then $\langle a \rangle$ is an infinite subgroup consisting of distinct elements a^k for $k \in \mathbb{Z}$*
2. *If a has finite order n, then $\langle a \rangle$ is a subgroup of order n and $\langle a \rangle = \{e = a^0, a^1, ..., a^{n-1}\}$*

Proof. (1) We proved in the previous lecture than if a has infinite order then a^k are all distinct.

(2) Let a^i be an element of $\langle a \rangle$. Then consider $j \equiv i \pmod{n}$ where now $j \in \{0, 1, ..., n-1\}$. Additionally, we proved in the previous lecture that $a^i = a^j$ iff $i \equiv j \pmod{n}$. Furthermore, no other integer $k \in \{0, 1, ..., n-1\}$ is congruent to i mod n. Thus, $a^i = a^j \in \{a^0, a^1, ..., a^{n-1}\}$, and $\langle a \rangle$ has finite order n. □

But what if, and this is entirely possible, that $\langle a \rangle = G$? Well, we actually have the following definition:

Definition (Cyclic group)**.** G is a **cyclic group** if for some $a \in G$, we have $\langle a \rangle = G$.

It's important to note that every cyclic group must be abelian, since $a^i a^j = a^{i+j} = a^j a^i$.

Exploring further, we may begin to notice that these cyclic groups occur much more frequently that we'd previous expected. In fact, take a look at these following theorems:

Theorem 7.16.

Every finite subgroup of F^* is cyclic

Proof. Let G be a finite subgroup of F^*, and let $c \in G$ be such that c has the greatest order among all eleents in G. We will show $G = \langle c \rangle$.

Let $a \in G$ be arbitrary. By corollary as proven previously, $|a| \mid |c|$. This means $a^{|c|} = 1$. Thus far, this means that every element in G satisfies $a^{|c|} = 1$.

In other words, every element in G is a root of the polynomial $x^{|c|} - 1 \in F[x]$. Notice that $x^{|c|} - 1$ has at most $|c|$ roots. This means $|G| \leq |c|$. But since $\langle c \rangle \subseteq G$, we must have that $G = \langle c \rangle$. This concludes the proof. □

Theorem 7.17.

Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ be a cyclic group, and let $H \leq G$ be a subgroup. If $H = \{e\}$ is the trivial group, we see that $H = \langle e \rangle$, which is a cyclic group.

Let's now consider the nontrivial case, i.e. $H \neq \{e\}$. Here, there must exist some $b \in H \subseteq G$, where $b \neq e$. Since G is cyclic, we know that there must be some $i \neq 0$ such that $b = a^i$. More specifically, since H is a subgroup, notice that if $b \in H$, then we must have $b^{-1} \in H$. This is the same thing as saying that if $a^i \in H$, then so must a^{-i}.

Now, we can consider only the cases for which $i > 0$, WLOG. Let $k \in \mathbb{Z}$ be the smallest positive integer such that $a^k \in H$. We aim to show that $H = \langle a^k \rangle$.

Let $h \in H \subseteq G$ be some arbitrary element. Again, since G is cyclic, we write $h = a^m$ for some m. We now express using the division theorem that $m = kq + r$. In other words, $a^r = a^m \cdot a^{-kq} = a^m \cdot (a^k)^{-q}$. Here, notice that since $a^m \in H$ and $a^k \in H$, we must have that $a^r \in H$, where by the division theorem, $0 \leq r < k$.

However, recall that k is the *smallest* positive integer for which $a^k \in H$. This forces $r = 0$. We now have $a^r = e = a^m \cdot (a^k)^{-q}$. Rebalancing our equation, we get $a^m = (a^k)^q$, thus showing that $a^m = h \in \langle a^k \rangle$.

Finally, since $h \in H$ was arbitrary, we conclude that $H = \langle a^k \rangle$ which shows that all subgroups of a cyclic group G must also be cyclic. □

Holy dense proof final boss bro wtf we pulled out well-ordering principle AND division theorem like *damn*.

But unfortunately, this is no time for a break as we are on the verge of another very dense theorem.

Theorem 7.18.

Let S be a nonempty subset of the group G. Let $\langle S \rangle$ be the set of all possible products, in every order, of elements of S and their inverses. Then,

1. *$\langle S \rangle$ is a subgroup that contains S*
2. *If H is a subgroup of G that contains S, then H contains the entire subgroup $\langle S \rangle$.*

This is one of those weird cases where the theorem leads us to a definition, and we'll worry about the proof after the fact (after we actually know what we're doing).

Definition (Subgroup generated by S)**.** The above theorem shows that $\langle S \rangle$ is the smallest subgroup of G that contains S. We say that $\langle S \rangle$ is the **subgroup generated by** S.

Furthermore, if $\langle S \rangle = G$, we say that S generates G, and that the elements of S are generators of the group.

In the special case that $S = \{a\}$, we have $\langle S \rangle = \langle a \rangle$, the cyclic subgroup.

6 Lecture 06: Jan. 16th

summary

7.4 Group homomorphisms

Today we began our discussion on what it means to be a homomorphism in the Group theory setting. But first, recall that in abstract algebra, whenever we encounter the concepts "——orphisms", we are going to be dealing with function sthat preserve and respect the algebraic structures at hand.

Let's take a trip down memory lane about ring homomorphisms, which are defined as functions f over a ring R such that

$$f(a+b) = f(a) + f(b) \text{ AND } f(ab) = f(a)f(b)$$

Furthermore, recall that a ring *isomorphism* essentially just represents a "renaming" of the domain to the co-domain, since both sets produce identically the same behaviors.

We'll see that this is very similar in groups.

Definition (Group homomorphisms)**.** Let G, H be groups. A function $f : G \to H$ is called a **group homomomorphism** if

$$f(ab) = f(a)f(b)$$

for $a, b \in G$.

- If f is additionally injective *and* surjective, we call f a **group isomorphism**. In this case, we say G is *isomorphic* to H and denote $G \cong H$
- If $f : G \to G$ is an isomorphism, we call it an **automorphism**

But there is one thing we should watch out for that's actually been haunting us thus far in the course, and that is the notation of things:

G multiplicative, H additive	$f(ab) = f(a) + f(b)$
G additive, H multiplicative	$f(a+b) = f(a)f(b)$
G additive, H additive	$f(a+b) = f(a) + f(b)$

Let's now take a look at a couple examples.

Example 6.1. Show that $U_8 = \{1, 3, 5, 7\}$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

First, note that the binary operation is multiplication in the domain and pairwise addition in the co-domain. Also, since we are seeking to establish an isomorphism, it should only make sense that the identity is mapped to the identity.

We can consider the following

$$f(1) = (0,0) \qquad f(3) = (1,0) \qquad f(5) = (0,1) \qquad f(7) = (1,1)$$

This is actually an isomorphism! For example, we have that

$$f(3 \cdot 5) = f(7) = (1,1) = (1,0) + (0,1) = f(3) + f(5)$$

But that wasn't very rigorous. Let's try something a bit more formal:

Example 6.2. Define $f : \mathbb{R} \to \mathbb{R}^{**}$ where $f(a) = 10^a$. Show that f is a group isomorphism.

First, let's check that f is a group homomorphism. Let $a, b \in \mathbb{R}$. Then,

$$f(a+b) = 10^{a+b} = 10^a \cdot 10^b = f(a)f(b)$$

This looks weird at first, but remember that $\mathbb{R}$ is an additive group (since it includes 0), whereas $\mathbb{R}^{**}$ is a multiplicative group.

We now show bijectivity:

1. Injective: let $f(a), f(b) \in \mathbb{R}^{**}$, and suppose $f(a) = f(b)$. Then,

$$f(a) = f(b) \Rightarrow 10^a = 10^b \Rightarrow a = b$$

2. Surjective: Let $y \in \mathbb{R}^{**}$. Then, we have

$$f(\log y) = 10^{\log y} = y$$

and since $\log y \in \mathbb{R}$, we have that f is surjective.

We thus conclude that f is a bijective group homomorphism, or in other words, a group isomorphism.

Example 6.3. Two finite groups with different numbers of elements cannot be isomorphic.

This is obviously true, since a bijection cannot be established.

Example 6.4. Are S_3 and $\mathbb{Z}_6$ isomorphic?

Well at first glance, they both look like they have the same number of elements. However, notice that $(\mathbb{Z}_6, +)$ is abelian, while $(S_3, \circ)$ is not. Thus, these groups cannot be isomorphic.

This gives us some good intuition actually. A natural question to wonder now is: do group homomorphisms *all* preserve commutativity?

Example 6.5. Let $f : G \to H$ be a *surjective* homomorphism of groups where G is abelian. Show that H is abelian.

Let $a, b \in H$ be arbitrary elements. Since f is a surjective homomorphism, we know there must exist $c, d \in G$ such that $f(c) = a$ and $f(d) = b$.

Since G is abelian, we know that $f(cd) = f(dc)$. Further expanding on that thought, we have

$$ab = f(c)f(d) = f(cd) = f(dc) = f(d)f(c) = ba$$

Since $ab = ba$ and they were arbitrary elements in H, we conclude that H is abelian. □

So yes, group homomorphisms does preserve commutativity. However, note that in this case we required f to be surjective. So actually, the commutativity is only preserved on the *image* of H.

Let's take a look at more examples and try to poke around to find all the properties of homomorphisms.

Example 6.6. Are $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ isomorphic?

Well, it looks like they both have the same order, and they both are abelian. So thus far by our investigation, it should be?

Hell no!!!!!!!! Here we establish another important property that's preserved.

Notice that $\mathbb{Z}_4$ is a cyclic group, where $\langle 1 \rangle = 1 \cdot n = \mathbb{Z}_4$. However, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is *not cyclic*, as no element...

Remark. If f is an isomorphism, then a and $f(a)$ have the same order.

Remark. Let G be a group and let $c \in G$ be one fixed element. Then $f : G \to G, f(a) = c^{-1}ac$ is a group automorphism. It is called the **inner automorphism** induced by c.

Proof. Let's check that inner automorphisms have all properties needed to be considered an isomorphism.

1. homo
2. injective
3. surjective

□

And now, we move onto the characterization of cyclic groups:

Theorem 7.19.

Let G be a cyclic group.

1. *If G is infinite, then G is isomorphic to the additive group $\mathbb{Z}$.*
2. *If G is finite of order n, then G is isomorphic to the additive group $\mathbb{Z}_n$.*

Proof. Let $G = \langle a \rangle$. Recall that if $|G| = \infty$, then each a^k is distinct for all $k \in \mathbb{Z}$. Now, consider $f : a^k \mapsto k$ for some $k \in \mathbb{Z}$. We verify that

$$f(a^i a^j) = f(a^{i+j}) = i + j = f(a^i) + f(a^j)$$

thus, f is a homomorphism. It is also trivial to show that f is bijective. Therefore, $G \cong \mathbb{Z}$ in this case.

Now suppose $G = \langle b \rangle$ with $|b| = n$. We define $g : G \to \mathbb{Z}_n$ where $g(b^k) = [k]$. Now,

$$g(b^i b^j) = g(b^{i+j}) = [i + j] = [i] + [j] = g(b^i) + g(b^j)$$

thus g is a homomorphism. The proof of bijectiveness is left as an exercise for the reader. □

7 Lecture 07: Jan. 21st

summary

7.4 Group homomorphisms (cont'd)

To begin lecture, we started with a few examples to jog our memory of group homomorphisms. Remember that isomorphisms simply represent the same set under a "renaming".

Example 7.1. The function $f : \mathbb{R}^* \to \mathbb{R}^*, f(r) = r^2$ is a homomorphism of multiplicative groups.

To show this, we check homomorphic properties:

$$f(rs) = (rs)^2 = r^2s^2 = f(r)f(s)$$

Do note that $f(1) = f(-1)$ so f is not injective.

Example 7.2. The function $f : \mathbb{Z} \to \mathbb{Z}_5, f(a) = [a]$ is a homomorphism.

Again, we first show homomorphic properties:

$$f(a + b) = [a + b] = [a] + [b] = f(a) + f(b)$$

Recall from ring theory that the sum of two elements is equal to the sum of two residue classes. Also do note that f is not surjective.

Let's now move to some new definitions.

Definition (Image)**.** Let $f : G \to H$ be a group homomorphism. The set $\text{Im}(f) = \{f(g) : g \in G\}$ is called the **image of** f. The image has the following properties:

1. $\text{Im}(f)$ is a subset of H
2. $F : G \to \text{Im}(f)$ is surjective

We explore some more properties given that we know the image now.

Theorem 7.20.
Let G, H be groups with identity elements e_G, e_H, respectively. If $f : G \to H$ is a group homomorphism, then

1. $f(e_G) = e_H$
2. $f(a^{-1}) = f(a)^{-1}$ *for all* $a \in G$
3. $\text{Im}(f)$ *is a subgroup of* H
4. *If f is injective, then* $G \cong \text{Im}(f)$

8 Lecture 08: Jan. 26th

summary

7.5 Alternating groups

The professor began the pre-lecture with a short blurb about how this certain section isn't very very relevant later down the line, meaning a lot of the section will be very intuition based, rather than strictly rigorous math.

With that said, let's begin with a new notation for permutatinos. Recall previously that for elements in symmetric groups S_n, we've always denoted them like

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

But, we wish to introduce something that's simpler and more effective in showing specific properties when talking about alternating groups or permutation groups.

Using the above as an example, our new notation involes collapsing that matrix into a single vector

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

To parse this new notation, notice that 1 maps to 2, 2 maps to 4, 4 maps to 3, and since 3 maps back to 1 completing a cycle, we close the vector. Then, we have a standalone vector of just 5, since it maps to itself (although most times 1-cycles are omitted from the notation).

Notice how this already reveals a lot more about the cyclic nature of the permutations. Let's now formally define this.

Definition (k-cycle)**.** If a permutation can be written as $(a_1 \quad a_2 \quad a_3 \dots a_k)$ for distinct elements $a_1, ..., a_k$ of the given group, we call that a cycle of length k, or a k**-cycle**.

Additionally, a 2-cycle is called a **transposition**, and two cycles are **disjoint** if they have no common elements.

Let's take a look at an example in translating our old S_3 notation to the new one.

Example 8.1. Translate the following notations:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \Longrightarrow (1) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \Longrightarrow (2 \quad 3) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \Longrightarrow (1 \quad 3)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \Longrightarrow (1 \quad 2) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \Longrightarrow (1 \quad 2 \quad 3) \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \Longrightarrow (1 \quad 3 \quad 2)$$

As a remark, the identity consists of three 1-cycles, and it is the only case for which we will write out a 1-cycle in our notation, to denote the identity as (1).

Example 8.2. We now go over another example on how composition of permutations look in cycle notation. Take the following as an example:

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

Recall that we read compositions from right to left: $1 \to 2 \to 4$, $2 \to 4 \to 3$, $3 \to 1 \to 1$, $4 \to 3 \to 2$.

Now converting everything to cycle notation, we have

$$(2 \quad 4 \quad 3) \circ (1 \quad 2 \quad 4 \quad 3) = (1 \quad 4 \quad 2 \quad 3)$$

Notice how everything is much more friendly to read? We simply take the next entry (if it exists) in our k-cycle vector as the input into the other cycle.

*****

We began the in-person portion of the lecture with a remark.

Remark. Every transposition is its own inverse. In other words, for some transposition (ab), we have

$$(ab) \circ (ab) = (1)$$

Let's look at a motivating example following this remark:

Example 8.3. We claim that the inverse of the product $(12)(34)(14)(13)$ is the transpositions but in reverse order $(13)(14)(34)(12)$.

To prove this claim, we simply compose the two products:

$$\begin{aligned}(12)(34)(14)(13) \circ (13)(14)(34)(12) &= (12)(34)(14) \circ (1) \circ (14)(34)(12)\\ &= (12)(34) \circ (1) \circ (34)(12)\\ &= (12) \circ (1) \circ (12)\\ &= (1)\end{aligned}$$

To extend on the previous remark, we have now

Remark. If $\sigma_1, \sigma_2, ..., \sigma_n$ are transpositions, then

$$(\sigma_1\sigma_2...\sigma_{n-1}\sigma_n)^{-1} = (\sigma_n\sigma_{n-1}...\sigma_2\sigma_1)$$

To dive deeper into the idea of transpositions, we have the following theorem:

Theorem 7.26.

Every permutation in S_n is a product of (not necessarily disjoint) transpositions.

Proof. Since every permutation in S_n can be written as a product of disjoint cycles, we simply need to prove that every cycle $(a_1a_2...a_k)$ can be written as a product of transpositions:

$$(a_1a_2...a_k) = (a_1a_2)(a_2a_3)\cdots(a_{k-1}a_k)$$

□

Definition (Parity of permutations)**.** A permutation in S_n is said to be **even** if it can be written as a product of an even number of transpositions, and **odd** if it can be written as a product of an odd number of transpositions.

As a direct result, we should first show that

Lemma 8.2.

The identity permutation in S_n is even but not odd.

> **Intuition.** *Pretty trivial that it's even, since we can write* $(1) = (12)(12)$*. Intuitively also,* (1) *cannot be odd because it would require an even number of swaps to return a permutation back to its original ordering. An odd number of swaps will always leave something inverted.*

Theorem 7.28.

No permutation in S_n is both even and odd

Proof. Suppose we have some permutation α that can be represented by $\sigma_1\cdots\sigma_j$ and $\tau_1\cdots\tau_k$, where σ_i and τ_i are transpositions, with j odd and k even.

Since every transposition is its own inverse, we can use the previous remark to write

$$\begin{aligned}(1) = \alpha\alpha^{-1} &= (\sigma_1\cdots\sigma_j)(\tau_1\cdots\tau_k)^{-1}\\ &= \sigma_1\cdots\sigma_j\tau_k\cdots\tau_1\end{aligned}$$

The above shows that (1) is a product of an odd number of transposition – a direct contradiction of the previous lemma. Thus, we conclude that α cannot be both even and odd. □

We end with a culminating definition and theorem.

Definition (Alternating groups)**.** The set of all *even* permutations in S_n, denoted A_n is called the **alternating group** of degree n.

Theorem 7.29.

A_n is a subgroup of S_n with order $|A_n| = \frac{n!}{2}$.

> **Intuition.** *There's always $n!$ permutations of n elements. Half of them are even.*

8.1 Congruence

Recall that in ring theory, we introduced the idea of congruence on the integers $\mathbb{Z}$, where

$$a \equiv b \bmod n \text{ if } n \mid a - b$$

And more generally outside of the integers, we said that two elements a, b in some ring R is congruent if

$$a \equiv b \bmod I \text{ if } a - b \in I$$

for some ideal I in R. Let's now define it in group theory!

Definition (Group congruence)**.** Let K be a subgroup of a group G and let $a, b \in G$. Then a is congruent to b modulo K (denoted $a \equiv b \pmod K$) if $ab^{-1} \in K$.

As a remark, remember that in the multiplicative notation, $a - b$ is denoted as ab^{-1}.

Theorem 8.1.

Let K be a subgroup of a group G. Then the relation 'congruence modulo K' is an equivalence relation, ie

1. *It is reflexive*
2. *It is symmetric*
3. *It is transitive*

Additionally, whenever we have an equivalence relation, we automatically have the following:

1.

9 Lecture 09: Jan. 28th

summary

8.1 Congruence (cont'd)

We began with a rewrite of the congruence class

$$\begin{aligned}[a] = \{b \in G : b \equiv a \bmod K\} &= \{b \in G : ba^{-1} = k \text{ for } k \in K\} \\ &= \{b \in G : b = ka, k \in K\} \\ &= Ka\end{aligned}$$

To sumarize: the conguence class of a modulo K is the **right coset** $Ka = \{ka : k \in K\}$. And as always, when we're concerned with an additive group, we have $K + a$ instead.

> **Intuition.** *Recall from ring theory that we opened with congruence on integers, then congruence on polynomials, and eventually congruence on ideals (which are sets).*
>
> *The definition of a coset in the rings sense is almost a one-to-one matching to the cosets we're defining here. It's just all elements in G that are "the same away" from some subgroup K*

Let's try some examples.

Example 9.1. List the distinct cosets of K in G:

(1) $K = \{(1), (23)\}, G = S_3$. We have,

$$\begin{aligned}K \cdot (1) &= \{(1), (23)\} \\ K \cdot (12) &= \{(12), (132)\} = K(132) \\ K \cdot (13) &= \{(13), (123)\} = K(123)\end{aligned}$$

Remark. Notice here that each coset has 2 elements, and there are 3 cosets in general. This gives us a total of $2 \cdot 3 = 6 = |S_3|$. This is a theorem we will prove in the future.

(2) $K = \langle 3 \rangle, G = \mathbb{Z}_{12}$. We have,

$$\begin{aligned}K + 0 &= \{0, 3, 6, 9\} = K + 3 = K + 6 = K + 9 \\ K + 1 &= \{1, 4, 7, 10\} = K + 4 = K + 7 = K + 10 \\ K + 2 &= \{2, 5, 8, 11\} = K + 5 = K + 8 = K + 11\end{aligned}$$

(3) K is the subgroup generated by 12 and 20 in $G = \mathbb{Z}_{40}$. We first argue that $K = \langle 4 \rangle \leq \mathbb{Z}_{40}$. Then, show like (2) such that $K + 0 = K + 4 = ...$

(4) $K = \langle 7 \rangle, G = \mathbb{Z}$.

These examples gives us a lot more intuition as to how cosets function within groups.

Theorem 8.4.

Let K be a subgroup of a group G. Then,

1. *G is the union of the right cosets of K : $G = \bigcup_{a \in G} Ka$.*
2. *For each $a \in G$, there is a bijection $f : K \to Ka$. Consequently, if K is finite, any two right cosets contain the same number of elements.*

Definition (Index)**.** Let K be a subgroup of G. Then the number of right cosets of K in G is called the **index of K in G**. It is denoted by $[G : K]$.

If G is a finite group then the index $[G : K]$ is finite. If G is an infinite gorup then the index may be finite or infinite.

Let's take a look at some examples.

Example 9.2. Let $G = \mathbb{Z}_7^*$ with $K = \{1, 2, 4\}$. Compute $[G : K]$.

Well, we see that

$$K1 = \{1, 2, 4\} = K2 = K4$$
$$K3 = \{3, 5, 6\} = K5 = K6$$

Notice now that since $K1 \dot{\cup} K3 = \mathbb{Z}_7^*$, we know that these two cosets are the only two distinct cosets of G. Thus giving us $[G : K] = 2$.

Let's take another example:

Example 9.3. $\mathbb{Z}$ is a subgroup of the additive group $\mathbb{Q}$. Then, we have that the cosets $\mathbb{Z} + a$ and $\mathbb{Z} + c$ are equal, if and only if $a - c \in \mathbb{Z}$.

As a consequence, for any $0 < c < a < 1, \mathbb{Z} + 1$ is distinct from $\mathbb{Z} + c$. And because of this, there are infinitely many such a, c, meaning $[\mathbb{Q} : \mathbb{Z}] = \infty$.

In other words, there are infinitely many different integer cosets in the set of rationals.

This is actual a motivation for our first named theorem in the course.

Theorem 8.5 (Lagrange's Theorem).

Let K be a subgroup of a finite *group G. Then the order of K divides the order of G.*

More specifically,

$$|G| = |K|[G : K]$$

Before we dive into the proof, here's a little intuition:

Intuition. *Remember that "cosets" are just a fancy name for congruence classes mod K. Congruence classes are disjoint and the union of all of them covers the entirety of G. Since G is made up of disjoint chunks of cosets (exactly $[G:K]$ of them), its order must be the sum of all the orders of the cosets*

Now, since cosets are with respect to some subgroup K, they must have exactly the same number of elements as K. This means that the number of elements in G must be a multiple of the number of elements in K.

Proof. First, begin by noting that if A, B disjoint, then $|A \cup B| = |A| + |B|$.

Now, let $[G:K] = n.$, so we have n distinct right cosets $Kc_1, Kc_2, ..., Kc_n$. Then, by the above, we have

$$G = \dot{\bigcup}_{1 \le i \le n} Kc_i$$

Which gives us

$$|G| = \sum_{i=1}^{n} |Kc_i| = \sum_{i=1}^{n} |K| = [G:K] \cdot |K|$$

This concludes our proof. □

So why is this the first name drop of the course? What makes this so special? Let's take a look at some of the uses.

Example 9.4. What are the possible orders of the subgroup of G when G is $\mathbb{Z}_{24}$ or S_{24}?

Well, since $|\mathbb{Z}_{24}| = 24$, we have that all subgroups $K \le |\mathbb{Z}_{24}|$ must have orders that divide 24. Thus, possible orders of subgroups are $1, 2, 3, 4, 6, 8, 12, 24$.

However, we need to be *very* careful with our wording in the previosu example. (something about POSSIBLE subgroups which may not exist because the condition doesnt go the other way)

Theorem 8.6.

Let G be a finite group.

1. *If $a \in G$, then $|a| \mid |G|$.*
2. *If $|G| = k$, then $a^k = e$ for all $a \in G$.*

Look at **Theorem 8.6.1**!!! This is the idea that was hinted back all the way when we first introduced what the order of an element was. We finally did it!!

...

Theorem 8.7.

Let p be a positive prime number. Every group of order p is cyclic and isomorphic to $\mathbb{Z}_p$.

Proof. Let G be a group with order p, and let $a \in G$ such that $a \neq e$. Then, $\langle a \rangle$ is a subgroup of order G with order greater than 1. However, since G has prime order, all subgroups of G must have order 1 or p. Thus, $\langle a \rangle$ has order p, meaning $\langle a \rangle = G$.

Since G is cyclic with order p, it must be isomorphic to $\mathbb{Z}_p$. This result has been shown in **Theorem 7.19**, but as an intuition, consider $f : G \to \mathbb{Z}_p$ with $f(a) = [a]$. □

10 Lecture 10: Jan. 30th

summary

8.1 Congruence (connt'd)

...

Theorem 8.8.

Every group of order 4 is isomorphic to either $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Theorem 8.9.

Every group G of order 6 is isomorphic to either $\mathbb{Z}_6$ or S_3.

Given these theorems (8.7 - 8.9), we can now build a simple classification table.

Order of G	Isomorphism type
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6$ or S_3
7	$\mathbb{Z}_7$

8.2 Normal subgroups

We began the pre-lecture portion with some motivation. Recall from ring theory that once we've established what it means to modulo by a set (in the context of ideals and cosets), we then established arithmetics on cosets.

The goal of the next couple of lectures in section 8.2 is to establish the same arithmetics on cosets in terms of groups. We'll soon realize that group cosets are a bit less nice, and not all of them will obey to regular arithmetics.

But first, a motivating example!

Example 10.1. Recall the definition of dihedral groups – groups relating to the rotation of polygons. Specifically, remember that

$$D_4 = \{r_0, r_1, r_2, r_3, d, h, t, v\}$$

Now, for $K = \{r_0, v\}$, find Kd and dK. We have

$$Kd = \{kd : k \in K\} = \{r_0 d, vd\} = \{d, r_3\}$$
$$dK = \{dk : k \in K\} = \{dr_0, dv\} = \{d, r_1\}$$

We notice that here, $Kd \neq dK$. This makes sense, because we've already known that D_4 is not abelian. In ring theory, this behavior would mirror that of a subring but not an ideal.

Now, for $N = \{r_0, r_1, r_2, r_3\}$, find Nv and vN. We have

$$Nv = \{r_0v, r_1v, r_2v, r_3v\} = \{v, d, h, t\}$$
$$vN = \{vr_0, vr_1, vr_2, vr_3\} = \{v, t, h, d\}$$

We quickly realize that $Nv = vN$! And as a fun fact, $Ng = gN$ for all $g \in D_4$.

There is obviously a difference between these two cosets. Let's now define exactly what that is.

Definition (Normal subgroups)**.** A subgroup N is called a **normal subgroup** of G, denoted $N \lhd G$, if $Na = aN$ for all $a \in G$.

Remark. Note that $Na = aN$ refers to the *set equality*, and NOT the abelian nature of the groups. For instance, it does NOT imply $an = na$ for all elements $n \in N$ and $a \in G$.

For example, N is a normal subgroup as shown in the example above. However, notice that $r_3 \circ v = t$ but $v \circ r_3 = d$, so clearly $r_3 \circ v \neq v \circ r_3$, even though $Nv = vN$.

Remark. With that said though, for an abelian group G, *every* subgroup $K \leq G$ is a normal subgroup.

Let's take a look at another example now.

Example 10.2. Let $M = \{r_0, r_2\}$ in D_4. Notice that $r_0a = ar_0$ and $r_2a = ar_2$ for all $a \in D_4$. In this case, to call back to a definition we've made a couple weeks ago, we have $M = Z(D_4)$.

To connect this to our current conversation regarding normal subgroups, since elements are commutative, we definitely have $Ma = aM$ in this case, making M a normal subgroup.

Let's generalize what just happened. Let G be a group. Because $az = za$ for all elements $a \in G$ and all $z \in Z(G)$, we immediately see that $Z(G)$ is (always) a normal subgroup of G.

Going back to our original conversation about doing arithmetics on cosets, we can now define the following.

Theorem 8.10.
Let N be a normal subgroup of G. If $a \equiv b \mod N$ and $c \equiv d \mod N$, then $ac \equiv bd \mod N$.

Proof. Let $ab^{-1} = n_1 \in N$ and $cd^{-1} = n_2 \in N$. This implies that $a = n_1b$ and $c = n_2d$, giving us $ac = n_1bn_2d$.

Now, since N is a normal subgroup, we know that $bN = Nb$, meaning that for bn_2, we know there must exist some other element $n_3 \in N$ such that $bn_2 = n_3 b$.

Applying this to our case, we have $ac = n_1 n_3 bd$, meaning $ac \in Nbd$, proving our desired claim. □

We are beginning to notice the power of normal subgroups. Let's take a look at some of the equivalent forms:

Theorem 8.11.

The following conditions on a subgroup N of G are equivalent:

1. *N is a normal subgroup of G*
2. *$a^{-1}Na \subseteq N$ for all $a \in G$*
3. *$aNa^{-1} \subseteq N$ for all $a \in G$*
4. *$a^{-1}Na = N$ for all $a \in G$*
5. *$aNa^{-1} = N$ for all $a \in G$*

This gives us a new way of finding and verifying normal subgroups! In the future, we simply need to check that $aNa^{-1} \subseteq N$ for all $a \in G$.

Let's do more examples!

Example 10.3. Prove that $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R}, ad \neq 0 \right\}$ is a group under matrix multiplication. Then, prove that $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R} \right\}$ is a normal subgroup of G.

First, we ensure closure.

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & dz \end{pmatrix}$$

Since $ad \neq 0$ and $xz \neq 0$, we must have $axdz \neq 0$ as well.

Associativity is implied by the operation.

Consider

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \frac{1}{ad} \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} ad/ad & 0 \\ 0 & da/ad \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus, both the identity as well as the inverse exist in G.

Let's now show N is a subgroup. We have for $A, B \in N$, we have ...

8.3 Quotient groups

Remember quotient rings? We got quotient groups too!

Definition (Quotient groups)**.** Let N be a normal subgroup G. Then,

$$G/N = \{Na : a \in G\}$$

the set of all cosets of N in G, is called the **quotient group** or **factor group** in G.

Within these quotient groups, the operation is defined

$$(Na) \cdot (Nb) = N(ab)$$

At first, it is entirely valid to be skeptical of this group and the well-defined nature of the operation. That's why we have

Theorem 8.12.
Let N be a normal subgroup of G. If $Na = Nc$ and $Nb = Nd$ in G/N, then $Nab = Ncd$.

Proof. By definition, $Na = Nc$ implies $a \equiv c \pmod N$. Similarly, $b \equiv d \pmod N$. Therefore, $ab = cd \pmod N$ by properties of coset arithmetics, which directly implies $Nab = Ncd$. □

11 Lecture 11: Feb. 2nd

summary

8.3 Quotient groups (cont'd)

Recall our conversation last lecture about quotient groups. We now discuss the order of G/N.

Theorem 8.13.

Let N be a normal subgroup of G. Then,

1. *G/N is a group under the opertaion defined by*

$$(Na) \cdot (Nb) = Nab$$

2. *If G is finite, then the order of G/N is $|G|/|N| = [G : N]$*

The coset N is a group element of G/N, it is the identity!!

Let's look at a couple concrete examples now:

Example 11.1. Let N be the cyclic subgroup $\langle (1,2) \rangle$ of $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. Since $(1,2)+(1,2) = (0,0)$, we see that $N = \{(0,0),(1,2)\}$. Consequently, G/N consists of the following cosets:

$$\begin{aligned} N + (0,0) &= \{(0,0),(1,2)\} = N + (1,2) \\ N + (1,0) &= \{(1,0),(0,2)\} = N + (0,2) \\ N + (0,1) &= \{(0,1),(1,3)\} = N + (1,3) \\ N + (1,1) &= \{(1,1),(2,3)\} = N + (2,3) \end{aligned}$$

This gives us the following addition table:

	$N+(0,0)$	$N+(1,0)$	$N+(0,1)$	$N+(1,1)$
$N+(0,0)$	$N+(0,0)$	$N+(1,0)$	$N+(0,1)$	$N+(1,1)$
$N+(1,0)$	$N+(1,0)$	$N+(0,0)$	$N+(1,1)$	$N+(0,1)$
$N+(0,1)$	$N+(0,1)$	$N+(1,1)$	$N+(1,0)$	$N+(0,0)$
$N+(1,1)$	$N+(1,1)$	$N+(0,1)$	$N+(0,0)$	$N+(1,0)$

Using the table, we can verify that G/N is actually a cyclic group generated by $N+(0,1)$. And by what we've discovered in the previous section, $G/N \cong \mathbb{Z}_4$.

Example 11.2. Let $K \leq \mathbb{Z}$ where $K = \langle 4 \rangle$.

Notice that here we have $a \equiv b \pmod 4$ implies $a - b \in K$. Hence $a \equiv b \pmod 4$ if and only if $a \equiv b \pmod K$.

In other words, the set of integers that are congruent to a moludo 4, the congruence classes $[a]$, is the exact same as the set of integers that are congruent to a modulo K, the cosets $K + a$. So we have $[a] = K + a$.

Therefore $\mathbb{Z}/K$ is the gorup of congruence classes modulo 4, that is, $\mathbb{Z}/K = \mathbb{Z}/\langle 4\rangle = \mathbb{Z}_4$. The same argument goes for any integer n, meaning

$$\mathbb{Z}/\langle n\rangle = \mathbb{Z}_n$$

Intuition. *This should be* very *remeniscent of the notation $\mathbb{Z}/n\mathbb{Z}$ in ring theory, because it's pretty much the same thing!*

Example 11.3. Let $G = \mathbb{Z}$, and $N = \{3k : k \in \mathbb{Z}\} = 3\mathbb{Z} = \langle 3\rangle$.

As a ring: $\mathbb{Z}/3\mathbb{Z}$ is a ring, so it is a group with $+$. To expand further, we have

$$\mathbb{Z}/3\mathbb{Z} = \{N, N+1, N+2\}$$

This gives us the table

$+$	N	$N+1$	$N+2$
N	N	$N+1$	$N+2$
$N+1$	$N+1$	$N+2$	N
$N+2$	$N+2$	N	$N+1$

Thus $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$. This is a result from ring theory proved using quotient group logic!

Example 11.4. Let N be $\langle 4\rangle \leq \mathbb{Z}_{20}$. Find the order of $13 + N$ in $\mathbb{Z}_{20}/N$.

Alongside this, it would be helpful if we can also identify the isomorphism type of $\mathbb{Z}_{20}/N$. Notice that $N = \langle 4\rangle = \{0, 4, 8, 12, 16\}$. This gives us that $|\mathbb{Z}_{20}/N| = 20/5 = 4$.

Since G/N has order 4, we know it must be isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$. Let's now identify the order $|13 + N|$.

$$\begin{aligned}(13 + N) &= 13 + N \neq N\\ 2(13 + N) &= 26 + N = 6 + N \neq N\\ 3(13 + N) &= 39 + N = 19 + N \neq N\\ 4(13 + N) &= 12 + N = N\end{aligned}$$

We have found that $|13 + N| = 4$, and thus, $\mathbb{Z}_{20}/\langle 4\rangle \cong \mathbb{Z}_4$.

Now let's take a look at an example where the result is not so trivial.

Example 11.5. Give an example of a nonabelian group G so that $G/Z(G)$ is abelian.

Let's consider D_4 where $Z(D_4) = \{e = r_0, r_2\}$. This gives us

$$|D_4/Z(D_4)| = 8/2 = 4 \quad \Longrightarrow \quad D_4/Z(D_4) \cong \mathbb{Z}_4 \text{ or } \mathbb{Z}_2 \times \mathbb{Z}_2$$

Since its congruent to either abelian groups, we know that $D_4/Z(D_4)$ must be abelian.

Notice how we did this without having to write out a multiplication table! How nice.

On the other side of the coin,

Example 11.6. Give an example of a group G so that $G/Z(G)$ is not abelian.

Let's consider now $S_3 = G$. We're aiming for $|G/Z(G)| = 6$ where it would be congruent to S_3, because as far as we've discovered, that's the only way to build a non-abelian group with a small order.

A question could be: which subgroups does S_3 have? Spoiler alert! The center of S_3 is that $Z(S_3) = \{e\}$. This solves the example, since $S_3/\{e\} = S_3$ is obviously not abelian.

The previous two "non-trivial" examples gives us some insight into the structure preservation properties of a quotient group.

Notice that if we start with a group G and sort its elements via the filter of a given normal subgroup N, then a lot of the structure of G is reflected in G/N, and vice versa - whereas some structures get lost. This will give us some great intuition as our discussion moves towards factor groups.

But first, a theorem specifically about the preservation of abelian properties.

Theorem 8.14.
Let N be a normal subgroup of a group G. Then G/N is abelian if and only if $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.

As a direct consequence of this theorem, **if G is abelian, then G/N must be abelian as well.** Well, what about the converse? When can we conclude that G is abelian?

Theorem 8.15.
If G is a group such that the quotient group $G/Z(G)$ is cyclic, then G is abelian.

Proof. We can take for granted that $Z(G)$ is a normal subgroup of G as shown previously. Now let

$$G/Z(G) = \{Z(G) \cdot c^i : c \in G, i \in \mathbb{Z}\}$$

We wish to show now that $ab = ba$ for all $a, b \in G$. By definition of cosets, we know

$$G = \bigcup_i Z(G) \cdot c^i$$

since a group is a disjoint union of all its cosets. This directly imply that there must exist $z_1, z_2 \in Z(G)$ such that $a = z_1 \cdot c^i$ and $b = z_2 \cdot c^j$. Then,

$$ab = (z_1 \cdot c^i)(z_2 \cdot c^j) = z_2 z_1 c^{i+j} = z_2 z_1 c^j c^i = (z_2 \cdot c^j)(z_1 \cdot c^i) = ba$$

This concludes the proof. □

12 Lecture 12: Feb. 4th

summary

8.4 Quotient groups and homomorphisms

To open the pre-lecture material, the professor contextualized the section as an investigation into which properties are preserved by homomorphisms.

It may seem as if we've already discussed this topic earlier in **section 7.4**, but as it turns out, much like in ring theory, homomorphisms are tightly knitted with quotient groups as well.

But before we get ahead of ourselves, let's start with some basic definitions.

Definition (Kernel)**.** Let $f : G \to H$ be a homomorphism of groups. Then the **kernel of** f is the set $K = \{a \in G : f(a) = e_H\} \subseteq G$.

Let's start with some examples.

Example 12.1. Let $\mathbb{R}^{**} \leq \mathbb{R}^*$ and consider the homomorphism $f : \mathbb{R}^* \to \mathbb{R}^{**}$ given by $f(a) = a^2$. We've previously shown that this is a homomorphism. What is the kernel?

In this case, since we know the identity of the codomain is 1, we can explicitly define the kernel by the definition to be

$$K = \{g \in \mathbb{R}^* : f(g) = 1\} = \{g \in \mathbb{R}^* : g^2 = 1\} = \{-1, 1\}$$

Example 12.2. Consider two groups G, H as the homomorphism $f : G \times H \to \mathbb{H}$, defined by $f((a, b)) = b$.

Here, the kernel of f by definition is $K = \{(a, 1) : a \in G\} = G \times \{1\}$. Interestingly enough, in this case, we have $\ker f \leq G \times H$.

Example 12.3. Previously, we've also seen the homomorphism $f : \mathbb{Z} \to \mathbb{Z}_5$, defined by $f(a) = [a]_5$. Here, the kernel is

$$K = \{a \in \mathbb{Z} : [a]_5 = [0]\} = \{a \in \mathbb{Z} : 5 \mid a\} = \langle 5 \rangle$$

There's actually quite a few interesting properties relating kernels of homomorphims to subgroups. Namely,

Theorem 8.16.

Let $f : G \to H$ be a homomorphism of groups with kernel K. Then K is a normal subgroup of G.

Proof. We are going to skip the subgroup proof as it is left as an exercise for the reader.

Instead, assuming $K \leq G$, we show that $K \lhd G$. Let $g \in G$ be arbitrary, our goal is to show that $g^{-1}Kg \subseteq K$.

Let $k \in K$ be arbitrary. We show $g^{-1}kg \in K$. Applying homomorphic properties, we see that

$$f(g^{-1}kg) = f(g^{-1})f(k)f(g) = f(g)^{-1}e_H f(g) = f(g)^{-1}f(g) = e_H$$

Since k, g were arbitrary elements of their respective groups, we conclude that K is a normal subgroup of G. □

Let's take a look at an example application of this theorem:

Example 12.4. Show that the alternating group A_n is a normal subgroup of S_n.

Consider the function $f : S_n \to \mathbb{Z}_2$, where $f(a) = 0$ if a is an even cycle, and $f(a) = 1$ otherwise. We can easily show that f is a homomorphism of groups, and its kernel is the alternating group A_n, since by definition, A_n is the set of all even cycles.

Then, by **Theorem 8.16** as proven above, A_n is a normal subgroup of S_n. □

Perhaps building off of the previous theorem, we also have that

Theorem 8.17.
Let $f : G \to H$ be a homomorphism of groups with kernel K. Then f is injective if and only if $K = \{e_G\}$.

The proof of this theorem is very similar to that in Ring theory.

Proof. ($\Rightarrow$) Let f be injective. Note that since f is a homomorpism of groups, we must have $f(e_G) = e_H$.

Now let $a \in K$ be arbitrary. By definition we must have $f(a) = e_H$. Since f is injective, we must have $f(e_H) = e_G = a$. Thus $a = e_G$.

($\Leftarrow$) Let $K = \{e_G\}$. Let $a, b \in G$ such that $f(a) = f(b)$. Then,

$$e_H = f(a)f(b)^{-1} = f(ab^{-1}) \quad \Longrightarrow \quad ab^{-1} \in K \quad \Longrightarrow \quad ab^{-1} = e_G \quad \Longrightarrow \quad a = b$$

Thus f is injective and this concludes the proof. □

As a bit of intuition, we can say that

> **Intuition.** *The kernel of a group homomorphism f measures how far f is from being injective.*

In case you haven't gotten the hint by now, this entire section very much mirrors (the most difficult part of) Ring Theory, specifically building up to the First Isomorphism Theorem.

Take a trip down memory lane – when we did this in ring theory, one key player that we spend much time discussing about was the idea of a *natural* homomorphism, which in laymans words, was basically a modulo ooperator in the world of ideals and cosets.

Well guess what, the same thing also exists in group theory. Let's get into it.

Theorem 8.18.

If N is a normal subgroup of G, then the map $\pi : G \to G/N$ defined by $\pi(a) = Na$ is a surjective homomorphism with kernel N, the so called ***natural homomorphism*** *with respect to N.*

> **Intuition.** *Connecting this to our current conversation of relating homomorphisms to quotient groups, this theorem lets us conclude that every normal subgroup N is a kernel and gives rise to a surjective homomorphism.*

This gives us one last definition for the day.

Definition (Homomorphic image)**.** Let $f : G \to S$ be a surjective homomorphism of groups. We say that S is the **homomorphic image** of G.

Let's finally do an example to lock in everything.

Example 12.5. Find all homomorphic images of D_4 and S_3 (up to isomorphism).

The entire gist of the lecture today was for us to discover the following relationship:

Homomorphic images $\leftrightarrow$ Surjective homomorphisms $\leftrightarrow$ kernels $\leftrightarrow$ normal subgroups

This essentially means if we can find all the kernels (normal subgroups), then we'll have found all the homomorphic images.

In D_4, we have

$$\{e = r_0\}, \{r_0, r_2\} = Z(G), \{r_0, r_1, r_2, r_3\} = \langle r_1 \rangle, D_4$$

which gives us

$$D_4/\{e\} \cong D_4 \qquad D_4/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad D_4/\langle r_1 \rangle \cong \mathbb{Z}_2 \qquad D_4/D_4 \cong \{e\}$$

Similarly, in S_3 we have

$$\{e = (1)\}, A_3, S_3$$

which gives us

$$S_3/\{e\} \cong S_3 \qquad S_3/A_3 \cong \mathbb{Z}_2 \qquad S_3/S_3 \cong \{e\}$$

And these are the only homomomorphic images up to isomorphism.

13 Lecture 13: Feb. 9th

summary

8.4 Quotient groups and homomorphisms (cont'd)

Recall our conversation regarding homomorphisms and how that relates to different quotient groups. Specifically, remember the relationship

Homomorphic images $\leftrightarrow$ Surjective homomorphisms $\leftrightarrow$ kernels $\leftrightarrow$ normal subgroups

We now dive head first into a very monumental, but very familiar theorem.

Theorem 8.20 (First Isomorphism Theorem).
Let $f : G \to H$ be a surjective homomorphism of groups with kernel K. Then,

$$G/K \cong H$$

Proof. Begin by considering the map $\varphi : G/k \to H$ defined by $\varphi(Ka) = f(a)$. We now show that φ is an isomorphism of groups.

1. Well-defined: Let $Ka, Kb \in G/K$ such that $Ka = Kb$. We want to show $\varphi(Ka) = \varphi(Kb)$, or in other words, $f(a) = f(b)$.

   Not going to show the entire proof, but the idea is that since K is the kernel of f, Ka and Kb are equally as far away from the kernel, meaning they must correspond to the same image.

2. Homomorphic properties:

$$\varphi(Ka \cdot Kb) = \varphi(K \cdot (ab)) = f(ab) = f(a)f(b) = \varphi(Ka)\varphi(Kb)$$

3. Injectivity: Assume $\varphi(Ka) = \varphi(Kb) \Leftrightarrow f(a) = f(b)$. Then, that implies $f(a)f(b)^{-1} = e_H$. Since f is a homomorphism of groups, we can rewrite $f(ab^{-1}) = e_H$, meaning $ab^{-1} \in K$. Finally, by definition of cosets, this implies $Ka = Kb$.

4. Surjectivity: Let $h \in H$ be arbitrary. Since f is surjective, there must exist some $c \in G$ such that $f(c) = h$. Then, we have $\varphi(Kc) = f(c) = h$. Thus, φ is surjective as well.

□

Now that we have this theorem in our hands, let's do a couple examples!

Example 13.1. Prove that $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 1)\rangle \cong \mathbb{Z}$.

To take advantage of the first homomorphism theorem that we just proved, we can aim to find some surjective homomorphism $f : G \to H$ such that $\ker f = K$.

In this case, we aim to find $f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ such that $\ker f = \langle(1,1)\rangle = \{(1,1),(0,0),(-1,-1)...\}$. A natural guess would be that $(a,b) \mapsto a-b$. Let's try that.

We first confirm homomorphic properties:

$$f(a,b) + f(c,d) = a - b + c - d = (a+c) - (b+d) = f(a+c, b+d)$$

We now confirm surjectivity. Let $r \in \mathbb{Z}$ be arbitrary. Then, $f(r,0) = r - 0 = r$.

Let's now more explicitly outline the kernel. We have that by definition of f,

$$\ker f = \{(a,b) : a-b=0\} = \{(a,b) : a=b\} = \{(a,a) : a \in \mathbb{Z}\} = \langle(1,1)\rangle$$

Finally, this allows us to conclude that, by the first isomorphism theorem, we have $\mathbb{Z} \times \mathbb{Z}/\langle(1,1)\rangle \cong \mathbb{Z}$, as desired. □

Example 13.2. Make a list of groups such that every homomorphic image of $\mathbb{Z}_{12}$ is isomorphic to exactly one group on the list.

Well first, recall the relationship we established last lecture, but now that we know FIT, let's update it a bit:

$$f : G \to H \text{ surjective} \leftrightarrow G/K \cong H \leftrightarrow \text{kernels} \leftrightarrow \text{normal subgroups}$$

Applying this relationship to our current problem, we know that by FIT, every homomorphic image is isomorphic to some quotient group formbed by the kernel of some surjective homomorphism.

Further, all surjective homomorphisms gives rise to kernels, which are also formed by normal subgroups! So our task now is to find all normal subgroups of $\mathbb{Z}_{12}$.

Since $\mathbb{Z}_{12} = \langle 1\rangle$ is cyclic, we know that all subgroups must be cyclic as well. Additionally, by Lagrange's theorem, we know that the order of all subgroups must divide the order of the original group. Then,

$$\begin{array}{lll} \langle 1\rangle = \mathbb{Z}_{12} & \langle 4\rangle \leq \mathbb{Z}_{12} & \langle 2\rangle \leq \mathbb{Z}_{12} \\ \langle 6\rangle \leq \mathbb{Z}_{12} & \langle 3\rangle \leq \mathbb{Z}_{12} & \{e\} \leq \mathbb{Z}_{12} \end{array}$$

Since these are all the possible normal subgroups of $\mathbb{Z}_{12}$, they are also all possible kernels of surjective homomorphisms on $\mathbb{Z}_{12}$. This gives rise to 6 different quotient groups:

$$\begin{array}{lll} \mathbb{Z}_{12}/\langle 1\rangle = \{e\} & \mathbb{Z}_{12}/\langle 4\rangle \cong \mathbb{Z}_4 & \mathbb{Z}_{12}/\langle 2\rangle \cong \mathbb{Z}_2 \\ \mathbb{Z}_{12}/\langle 6\rangle \cong \mathbb{Z}_6 & \mathbb{Z}_{12}/\langle 3\rangle \cong \mathbb{Z}_3 & \mathbb{Z}_{12}/\{e\} = \mathbb{Z}_{12} \end{array}$$

Thus, we can conclude that the only possible homomorphic images of $\mathbb{Z}_{12}$ are

$$\{e\}, \mathbb{Z}_4, \mathbb{Z}_2, \mathbb{Z}_6, \mathbb{Z}_3, \mathbb{Z}_{12}$$

To bring back our conversation of quotient groups preserving properties of their original group, we should think of the normal subgroups as "sieves" that preserve some specific structure of the original group.

When we go over from G to G/N, we lose some structure. If we take a different normal subgroup, we lose a different structure of G. So what remains in G/N heavily depends on N (structure and size).

This gives us some motivation of the following theorem:

Theorem 8.21.

Let N be a normal subgroup of a group G and let H be any subgroup of G that contains N. Then H/N is a subgroup of G/N.

Proof. We show subgroup properties:

1. If $N \lhd G$, then $N \lhd H$
2. H/N is meaningful and

$$\{Nh : h \in H\} = H/N \subseteq G/N = \{Ng : g \in G\}$$

As H/N is a group by (2), it implies $H/N \leq G/N$. □

Fun fact: if H is normal, we can strengthen the above statement even more.

Theorem 8.22 (Third Isomorphism Theorem).

Let H and N be normal subgroups of a group G with $N \subseteq H \subseteq G$. Then H/N is a normal subgroup of G/N, and the quotient group $(G/N)/(H/N)$ is isomorphic to G/H.

14 Lecture 14: Feb. 11th

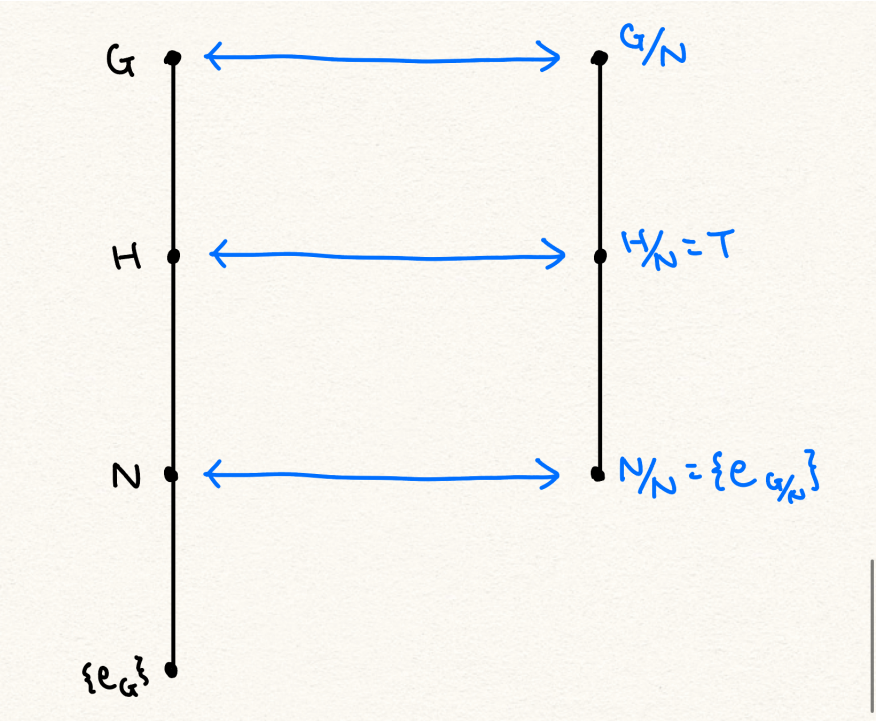
summary

8.4 Quotient groups and homomorphisms (cont'd)

Picking up from the previous lecture, we started with a theorem:

Theorem 8.24.

Let N be a normal subgroup of a group G and T be any subgroup of G/N. Then $T = H/N$ for some subgroup H of G that contains N.



A quick fact:

Proposition 14.2.

If $H \leq G$ with $[G : H] = 2$, then H is normal in G.

Proof. If $[G : H] = 2$, then H, Ha are the only cosets. We want to show that $Ha = aH$ for all $a \in G$. □

*****

To begin today's discussion, think back to **section 8.1**, where we made this very simple and quite naive list of groups with different orders (up to 7) and their corresponding isomorphism

types.

Classifying groups by their isomorphism types, it turns out, is quite the challenge. Let's discuss this a bit more.

But before we do that, let's first introduce a key player in our discussion.

Definition (Simple groups)**.** A group G is **simple** if its only *normal* subgroups are $\langle e \rangle$ and G.

Example 14.1. As we've discussed before, if a group G has prime order p, then by Lagrange's theorem, its subgroups must have order either 1 (trivial) or p. Thus, any prime ordered group is simple.

This example leads us to a theorem.

Theorem 8.25.

G is a simple abelian group if and only if G is isomorphic to the additive group $\mathbb{Z}_p$ for some p.

Essentially, the only simple abelian groups that exists must have prime order. In addition, nonabelian simple groups are pretty rare, with only 5 of order less than 1000, and 56 of order 1,000,000 (a large class of which are the alternating groups that we've previously discussed!).

So why exactly do we care about these simple groups, and what makes them "key players" in the classification problem? Let's conduct a thought experiment.

Let G be some finite group. Then logically it could only have finitely many normal subgroups other than itself (one of which is the trivial $\{e\}$). Let's let G_1 be the largest one of those subgroups. We claim that G/G_1 is simple.

Proof. Suppore for contradiction that G/G_1 had a proper mormal subgroup, then by the theorems we've covered previously, we know that its proper normal subgroup must come in the form M/G_1 for some $G_1 \subsetneq M \subsetneq G$. But that's clearly a contradiction to our hypothesis! □

Now if G_1 wasn't the trivial subgroup, we could actually induct on this logic and let G_2 be the largest proper normal subgropu of G_1. Then G_1/G_2 must be simple as well! If we keep going, we'll find

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_{n-1} \supsetneq G_n = \langle e \rangle$$

such that G_i/G_{i+1} is simple. These simple groups are called the **composition factors** of G, and they're *kinda* analogous to primes. It turns out, regardless of the choice of G_i, the simple quotient groups (composition factors) obtained would be isomorphic.

This gives us a way of classifying groups by their composition factors, akin to the unique factorization of an integer. **This is why simple groups are so crucial to the classification problem.**

If we could first classify all the simple groups, then show how the composition factors of an arbitrary group determine the structure of that group, it would be very doable to classify every group in existance.

(good news, the first part is done!)

8.5 The simplicity of A_n

To start the section, we began with a theorem.

Theorem 8.26.

For each $n \neq 4$, the alternating group A_n is simple.

Corollary 14.4.1.

If $n \geq 5$, then S_n has only 3 normal subgroups, $\{(1)\}, A_n, S_n$.

15 Lecture 15: Feb. 13th

summary

9.1 Direct products

Friday the 13th! Spooky. What's more spooky is that with the conclusion of section 8, we have completed most of the fundamentals of Group Theory. So from this point on, we are going to be diving a little deeper into some of the more involved (advanced?) topics.

Recall that we ended our conversation previously with a discussion on classifying groups. The goal of this section will be to classify all abelian groups. And to do this, we will need the help of one specific object.

Definition (Direct products)**.** Let $G_1, G_2, ..., G_n$ be groups. The set $G_1 \times G_2 \times \cdots \times G_n$ with coordinate-wise operation

$$(a_1, a_2, ..., a_n) \cdot (b_1, b_2, ..., b_n) = (a_1 b_1, a_2 b_2, ..., a_n b_n)$$

is a group called the **direct product** of $G_1, G_2, ..., G_n$.

Let's take a look at a couple examples:

Example 15.1. Consider $a = (1, 5, 0), b = (3, 5, 2) \in G = U_4 \times U_6 \times \mathbb{Z}_3$. Then,

$$a * b = (1, 5, 0) * (3, 5, 2) = (1 \cdot 3, 5 \cdot 5, \mathbf{0} + \mathbf{2}) = (3, 1, 2)$$

Note that because the third element is in $\mathbb{Z}_3$, we have that the group operation is addition rather than multiplication.

Example 15.2. Is it true for $5 \in U_6$ that $5 \in G$?

We can consider $(1, 5, 0) \in G$. Since $1, 0$ are the identities in their respective groups G_i, we have that $(1, 5, 0)$ behaves similarly in G as compared to $5 \in U_6$.

With these examples, we come to the following remarks:

Remark. It is important to note that G_i **is not** a subgorup of the direct product $G = G_1 \times G_2 \times \cdots \times G_n$. But G_i must be isormorphic to one such subgroup by definition.

Remark. If $G = G_1 \times G_2 \times \cdots \times G_n$ for finite groups G_i, then G is finite and $|G| = \prod_i |G_i|$.

Returning to our conversations of how direct products help classify abelian groups, there is one crucial insight that we will need to understand, and it's best illustrated in the following example:

Example 15.3. Consider the normal subgorups $M = \{0, 3\}$ and $N = \{0, 2, 4\} \in \mathbb{Z}_6$.

Observe that any element of $\mathbb{Z}_6$ can be written in one and *only one* way as the sum of an element of M and N.

$$0 = 0 + 0 \quad 1 = 3 + 4 \quad 2 = 0 + 2 \quad 3 = 3 + 0 \quad 4 = 0 + 4 \quad 5 = 3 + 2$$

Thus, the addition table of $\mathbb{Z}_6$ can be re-written as

	$0+0$	$3+4$	$0+2$	$3+0$	$0+4$	$3+2$
$0+0$	$0+0$	$3+4$	$0+2$	$3+0$	$0+4$	$3+2$
$3+4$	$3+4$	$0+2$	$3+0$	$0+4$	$3+2$	$0+0$
$0+2$	$0+2$	$3+0$	$0+4$	$3+2$	$0+0$	$3+4$
$3+0$	$3+0$	$0+4$	$3+2$	$0+0$	$3+4$	$0+2$
$0+4$	$0+4$	$3+2$	$0+0$	$3+4$	$0+2$	$3+0$
$3+2$	$3+2$	$0+0$	$3+4$	$0+2$	$3+0$	$0+4$

And recall the addition table of $M \times N$:

	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$
$(0,0)$	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$
$(3,4)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$	$(0,0)$
$(0,2)$	$(0,2)$	$(3,0)$	$(0,4)$	$(3,2)$	$(0,0)$	$(3,4)$
$(3,0)$	$(3,0)$	$(0,4)$	$(3,2)$	$(0,0)$	$(3,4)$	$(0,2)$
$(0,4)$	$(0,4)$	$(3,2)$	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$
$(3,2)$	$(3,2)$	$(0,0)$	$(3,4)$	$(0,2)$	$(3,0)$	$(0,4)$

We should realize that these tables are literally a one-for-one match. In other words, $M \times N$ is isormorphic to $\mathbb{Z}_6$ in this case.

Further, since $\mathbb{Z}_6$ is a direct product of M and N, representations from both addition tables are valid ways of showing this fact. It should depend on the context for which approach is more useful.

This example modivates the following theorem:

Theorem 9.1.

Let $N_1, N_2, ..., N_k$ be normal subgroups of G such that every element in G can be written uniquely in the from $a_1 a_2 \cdots a_k$ with $a_i \in N_i$. Then, G is isormorphic to the direct product $N_1 \times N_2 \times \cdots \times N_k$.

To build up to the proof of why this theorem makes sense, we first have to establish a helpful lemma:

Lemma 15.2.

Let M, N be normal subgroups of G such that $M \cap N = \{e\}$. If $a \in M$ and $b \in N$, then $ab = ba$.

Proof. To prove this lemm, consider $a^{-1}b^{-1}ab$. Since M is normal, we have that $b^{-1}ab \in M$. Then by closure, $a^{-1}b^{-1}ab \in M$. Similarly the normality of N implies that $a^{-1}b^{-1}a \in N$ implying $a^{-1}b^{-1}ab \in N$ by closure. Since $a^{-1}b^{-1}ab$ is in both sets, we concclude $a^{-1}b^{-1}ab = e$. Multiplying both sides gives us $ab = ba$. □

Let's now tune our previous definition a bit and add some details:

Definition (Direct products, direct factors)**.** If G is a grou and (normal) $N_1, N_2, ..., N_k$ are subgroups satisfying that every element in G can be written uniquely in the form $a_1a_2 \cdots a_k$ with $a_i \in N_i$, we say that G is the **direct product** of $N_1, N_2, ..., N_k$ and write

$$G = N_1 \times N_2 \times \cdots \times N_k$$

Each N_i is called a **direct factor** of G.

Furthermore, if G is additive, we write $G = N_1 \oplus N_2 \oplus \cdots \oplus N_k$ and call each N_i a **direct summands** of G.

And as established in the motivating example, depending on the context, we can see G as either

- The *inner direct product* (each element uniquely written as $a_1a_2 \cdots a_k$) or
- The *external direct product* (each element as a k-tuple $(a_1, a_2, ..., a_k)$)

Longest definition of all time. Let's all collectively take a breather.

Okay, continuing on. We're going to now talk about how to actually verify that G is the direct product of some subgroups M and N.

We do this by introducing the following notation. For $M, N \lhd G$, we have

$$MN = \{mn : m \in M, n \in N\}$$

The following theorem gives us a verification method.

Theorem 9.3.

If M, N are normal subgroups of a group G such that $G = MN$ and $M \cap N = \{e_g\}$, then $G = M \times N$.

Proof. Let $g \in G$ be arbitrary where $mn = g = \tilde{m}\tilde{n}$ for $m, \tilde{m} \in M$ and $n, \tilde{n} \in N$. Then,

$$mn = \tilde{m}\tilde{n} \quad \Longrightarrow \quad \tilde{m}^{-1}m = \tilde{n}n^{-1}$$

By closure, $\tilde{m}^{-1}m \in M$ and $\tilde{n}n^{-1} \in N$, and since they're equal, we must have that $\tilde{m}^{-1}m, \tilde{n}n^{-1} \in M \cap N = \{e\}$. In other words,

$$\tilde{m}^{-1}m = e = \tilde{n}n^{-1}$$

which implies $\tilde{m} = m$ and $\tilde{n} = n$. □

16 Lecture 16: Feb. 18th

summary

9.2 Finite Abelian Groups

Picking up from why we were even talking about direct products last time, in this section we will finally be classifying all finite abelian groups.

To do this, we shall prove that every finite ablian group G is some direct sum of cyclic subgroups and that orders of these subgroups are uniquely determined by G... almost like a "prime decomposition" but in terms of groups.

Remark. We are going to be primarily working over additive groups in this section, so to refresh, this means direct products are written

$$G \cong N_1 \oplus N_2 \oplus \cdots \oplus N_k$$

and all other additive notations apply to G as well.

Furthermore, we define a new notation. If G is an abeliankr group and p is a prime, then $G(p)$ denotes the set of elements in G whose order is some power of p; that is,

$$G(p) \coloneqq \{a \in G : |a| = p^n \text{ for some } n \geq 0\}$$

It is easly to show that $G(p)$ is a subgroup of G, which will be left as an exercise for the reader.

The idea today is to "sort G by prime orders". It'll be easy to show that G is the direct sum of cyclic subgroups if we can simply show that it is a direct sum of it's "prime factors" $G(p)$.

Lemma 16.1.

Let G be an abelian group and $a \in G$ an element of finite order. Then $a = a_1 + a_2 + \cdots + a_t$ where $a_i \in G(p_i)$ and p_i are the distinct prositive primes that divide the order of a.

Proof. We induct on the number of distinct primes that divide the order of a.

Let $n = 1$. Then $|a| = p^r$ meaning $a \in G(p)$ implying $a = a$.

Assume inductively that whenever $|a| = p_1^{r_1} \cdots p_t^{r_t}$ for $t < k$, then $a = a_1 + \cdots + a_t$ where $a_i \in G(p_i)$.

Now let $a \in G$ such that $|a| = p_1^{r_1} \cdots p_k^{r_k}$ and let $m = p_2^{r_2} \cdots p_k^{r_k}$ and $n = p_1^{r_1}$. Then $|a| = mn$.

From here, since $\gcd(m, n) = 1$, by bezout's identity, $1 = mu + nv$ for some $u, v \in \mathbb{Z}$. This implies

$$a = 1a = mua + nva$$

which gives us two conclusions:

1. $mua \in G(p_1)$. This is because since $|a| = mn$, we have $p_1^{r_1}(mua) = (n)(mua) = u(mna) = u(0) = 0$. Since $G(p_1)$ is a subgroup and thus closed, and $p_1^{r_1} \in G(p_1)$, we must have that $mua \in G(p_1)$.
2. Similarly, $m(nva) = v(mna) = v \cdot 0 = 0$, meaning $|nva| \mid m$. Since m is an integer with $k-1$ distinct prime factors, by our inductive hypothesis, we must have that $nva = a_2 + a_3 + \cdots + a_k$ with $a_i \in G(p_i)$.

Combining the two conclusions, we have $a = mua + nva = mua + a_2 + a_3 + \cdots + a_k$. Now simply let $mua = a_1$ and we have reached our desired conclusion. □

Theorem 9.5.

If G is a finite abelian group, then $G = G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_t)$, where $p_1, p_2, ..., p_t$ are the distinct positive primes that divide the order d of G.

So far on our quest to identify all finite abelian groups, we've discovered that we can write G as

$$G = G(p_1) \oplus \cdots \oplus G(p_t)$$

Now we need to analyze each $G(p)$. Recall an interesting example from our homework, where we proved that $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$. Given what we know now, we also have $\mathbb{Z}_{12} \cong G(3) \oplus G(2)$. So can we conclude $G(2) = \mathbb{Z}_4$?? Let's dig in.

Definition (p-group)**.** If p is a prime, then a group in which every element has order a power of p is called a **p-group**.

Further, an element a of a p-group B is called an element of **maximal order** if $|b| \leq |a|$ for every $b \in B$.

That is to say, if $|a| = p^n$ and $b \in B$, then b has order p^j with $j \leq n$. Since $p^n = p^{n-j}p^j$, we see that $p^n b = p^{n-j}(p^j b) = 0$. Hence, **if a is an element of maximal order p^n in a p-group B, then $p^n b = 0$ for all $b \in B$.**

Okay but what's the point of all this. Well, the next step in our journey of identifying finite abelian groups is to show that all p-groups are direct sums of cyclic groups.

To do this, we'll need another lemma.

Lemma 16.3.

Let G be a finite abelian p-group and a an element of maximal order in G. Then there is a subgroup K of G such that $G = \langle a \rangle \oplus K$.

Yeah after reading the proof I ain't writing that shit on here lol feel free to prove it yourself if you want!

This brings us to another massively important theorem.

Theorem 9.7 (The Fundamental Theorem of Finite Abelian Groups).
Every finite abelian group G is the direct sum of cyclic groups, each of prime power order.

Proof. We've previously shown that G is the direct sum of its subgroups $G(p)$, one for each prime p that divides $|G|$. Since each $G(p)$ is a finite abelian p-group, it remains to be shown that all finite abelian p-groups are a direct sum of cyclic groups.

We argue this by induction on the size of some p-group H. When $|H| = 2$, clearly it's a direct sum of the cyclic group, since itself is a cyclic.

We now assume inductively that the claim is true for all groups whose order $< |H|$.

Let a be the element of maximal order p^n in H. Then $H = \langle a \rangle \oplus K$ by the previous lemma. Since a is clearly not the identity as it has order p^n, we know that $\langle a \rangle$ has nontrivial order, meaning $|K| = |H|/|\langle a \rangle| < |H|$. Thus we apply inductive hypothesis and say K is a direct sum of cyclic groups, which when combined with $\langle a \rangle$, implies that H must also be a direct sum of cyclic groups. □

17 Lecture 17: Feb. 23rd

summary

9.2 Finite Abelian Groups (cont'd)

Picking up from the previous lecture, we dive straight into the fundamental theorem of finite abelian groups. This theorem is very powerful in that given any finite abelian group G with $|G| = n$, we will have a pool of "candidate direct products H_i" where each direct product H_i corresponds to a prime decomposition of n, and G must be isomorphic to some H_i in that pool.

Perhaps this is clearer with an example.

Example 17.1. Consider $n = 36$. We have $36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 3^2 = 2^2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2$.

Thus, by the fundamental theorem, we have that all finite abelian groups of order 36 is isomorphic to one of the 4 groups:

- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_9$

But now the problem is... which one? Consider $\mathbb{Z}_{36}$, how do we know which of the previous groups it's isomorphic to?

Lemma 17.1.
If $\gcd(m, k) = 1$, *then* $\mathbb{Z}_m \oplus \mathbb{Z}_k \cong \mathbb{Z}_{mk}$

Using this example, we know now that $\mathbb{Z}_{36} = \mathbb{Z}_4 \oplus \mathbb{Z}_9$. We won't be going over the entire proof, but here's a proof sketch:

Proof. (sketch)
We show that $(1, 1)$ is a generator of $\mathbb{Z}_m \oplus \mathbb{Z}_k$, since $\mathbb{Z}_{mk}$ is cyclic. In other words, we show $|(1, 1)| = mk$. □

This lemma actually brings us to

Theorem 9.9.
If $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, *where* $p_1, \ldots, p_t$ *are distinct primes, then* $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$

The proof of this theorem should follow directly from the previous lemma.

Using our newfound knowledege, we can actually represent finite abelian groups in a new way. Take a look at the following example:

Example 17.2. Consider the group $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{25}$

We now arrange the prime power orders of the cyclic factors by size, one row for each size

2	2	2^2	2^3
	3	3	3
		5	5^2

We now rearrange the cyclic factors of G by each column:

$$G = (\mathbb{Z}_2) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_3) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25})$$

Now, we can apply **Theorem 9.9** and see that

$$G = \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{600}$$

There are two observations to be made here for arguments as to why this new representation may be beneficial:

1. There are typically less summands when represented this way
2. The order of each summand divides the order of the next one

In fact, that second point brings us to the next theorem.

Theorem 9.10.

Every finite abelian group is the direct sum of cyclic groups of orders $m_1, m_2, \ldots, m_t$, where $m_1 \mid m_2, m_2 \mid m_3, \ldots, m_{t-1} \mid m_t$.

As a corollary,

Corollary 17.3.1.

If G is a finite subgroup of the multiplicative group of nonzero elements of a field, then G is cyclic.

Proof. Let F^* be the multiplicative group of nonzero elements of some field F, and let $G \leq F^*$ be a subgroup. Then G is finite and abelian, and we apply **theorem 9.10** to say that

$$G \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_t}$$

where each m_i divides m_t. Then, we know that for any element $b \in \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t}$, we must have that $m_t b = 0$. And since the two groups are isomorphic, this necessarily implies that $g^{m_t} = 1_F$ for all $g \in G$. In other words, for any $g \in G$, it must be the solution to the equation $g^{m_t} - 1_F = 0$.

The aforementioned polynomial can only have up to m_t distinct solutions, and since $|G| = m_1 m_2 \cdots m_t$, we know then that we must have $t = 1$ and therefore $G \cong \mathbb{Z}_{m_t}$. □

So these m_i's seem to be quite important, meaning we should probably give them a name.

Definition (Invariant factors)**.** Let G be a finite abelian group that is the direct sum of cyclic groups orders $m_1, m_2, \ldots, m_t$. Each m_i is an **invariant factor** of G.

In contrast to before, we have

Definition (Elementary divisors)**.** Let G be a finite abelian group that is the direct sum of cyclic groups of prime powers. Each prime power is an **elementary divisor** of G.

Essentially, these two definitions helps us classify the two ways we've learned to "factor" finite abelian groups in this section. Let's tie it all together with an example.

Example 17.3. All abelian groups of order 36 can be classified up to isomorphism in terms of their elementary divisors (**Example 17.1**) and their invariant factors.

We thus have the following table:

Group	Elementary Divisors	Invariant Factors	Isomorphic Group
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	2, 2, 3, 3	6, 6	$\mathbb{Z}_6 \oplus \mathbb{Z}_6$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$	2, 2, 3^2	2, 18	$\mathbb{Z}_2 \oplus \mathbb{Z}_{18}$
$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$	2^2, 3, 3	3, 12	$\mathbb{Z}_3 \oplus \mathbb{Z}_{12}$
$\mathbb{Z}_4 \oplus \mathbb{Z}_9$	$2^2, 3^2$	36	$\mathbb{Z}_{36}$

To wrap up our discussion of classifying finite abelian groups, we should patch up some holes in our logic. So far, the fundamental theorem gives us a way of identifying all possible abelian groups of a certain order.

However, to complete the classification, we should ensure that no two groups on the list are isomorphic to each other. This is akin to ensuring that the prime factorization of integers are unique.

Theorem 9.12.

Let G and H be finite abelian groups. Then G is isomorphic to H if and only if G and H have the same elementary divisors.

Proof. (sketch.)
($\Leftarrow$) If G and H share the same elementory divisors, then both G and H are isomorphic to the same direct sum of cyclic groups and, therefore, isomorphic to each other.

($\Rightarrow$) Let $f : G \to H$ be an isomorphism. Then $f(G(p)) = H(p)$, meaning $G(p) \cong H(p)$. The elementary divisiors of G that are powers of the prime p are exactly the elementary divisors of $G(p)$. Same for H.

Because of this fact, we simply need to show that isomorphic p-groups must have the same elementary divisors. We do this by induction and the rest is left as an exercise for the reader. □

18 Lecture 18: Feb. 25th

summary

9.3 The Sylow Theorems

Recall the overaching goal of this chapter: to classify finite groups. In the previous two sections, we've sucessfully classified all finite *abelian* groups.

The bad news: nonabelian groups are *much* harder to classify. But we will try anyway. Once again, a major theme of this chapter is the connection between the structure of a group G and the arithmetic properties of the integer $|G|$.

For the remainder of this section, all groups will be written multiplicatively, and G will automatically refer to a group.

Recall that when we were investigating abelian groups, we first defined a direct product, which was of great help to us. A similar thing will be done in this section with Sylow p-groups and the associated Sylow Theorems.

We already had the Lagrange theorem, which restricts the possible subgroups of G to those with sizes that divides $|G|$. The first Sylow Theorem gives us a (partial) converse to this statement.

Theorem 9.13 (First Sylow Theorem).
Let G be a finite group. If p is a prime and p^k divides $|G|$, then G has a subgroup of order p^k.

We're also not gonna do any proofs and leave them for the next section. Let's look at an example.

Example 18.1. $|S_6| = 6! = 720 = 2^4 \cdot 3^2 \cdot 5$, so by the first sylow theorem, S_6 has orders $2, 4, 8, 16, 3, 9, 5$.

It is important to note though, that we don't yet know how many such subgroups a group has (but at least one of each).

Then Cauchy comes along and steals everything.

Corollary 18.1.1 (Cauchy's Theorem).
If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

Proof. Let p be some prime that divides $|G|$. Then by the First Sylow Theorem, G must have a subgroup H of order p, implying $H = \langle a \rangle$ is cyclic and thus must have an element of order p. □

Definition (Sylow p-subgroup)**.** Let G be a finite group and p be a prime. If p^n is the largest power of p that divides $|G|$, then a subgroup of order p^n (which must exist by the First Sylow Theorem) is called the **Sylow p-subgroup of G**

Let's look at an example.

Example 18.2. Since S_4 has order $4! = 2^3 \cdot 3$, every subgroup of order 8 is Sylow 2-subgroup of S_4, since $8 = 2^3$ is the largest order of 2 that divides $4! = 24$.

One example (of which there are 3) is

$$\{(1), (1234), (13)(24), (1432), (24), (12)(34), (13), (14)(32)\}$$

Any subgroup of order 3 is a Sylow 3-subgroup. There are 4 such groups,

$$\langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle$$

Example 18.3. Let p be a prime and G be an abelian group with order $|G| = p^n m$ where $p \nmid m$. Then,

$$G(p) = \{a \in G : |a| = p^k, k \geq 0\}$$

has order p^n and is thus a Sylow p-subgroup of G.

As a direct result of this example, combined with **Theorem 9.5**, we say that G is the direct sum of all of its Sylow p-subgroups, where p are the various divisors of $|G|$.

Before proceeding, it may be worthwhile to to a quick review of some things covered previously.

Review. Let G be a gorup and $a \in G$ and $K \leq G$. Then,

1. $f_a : G \to G, f_a(g) = a^{-1}ga$ is an isomorphism.
2. $a^{-1}Ka = \{a^{-1}ka : k \in K\} \leq G$
3. $K \cong a^{-1}Ka$
4. In particular, order is preserved under f_a.

Thus,

Remark. If K is a Sylow p-subgroup of G, then $a^{-1}Ka$ is a Sylow p-subgroup of G.

But the real powerful part is that the converse is also true!

Theorem 9.15 (Second Sylow Theorem).
Let P and K be Sylow p-subgroups of a group G. Then there exists $a \in G$ such that $P = a^{-1}Ka$.

Corollary 18.2.1.

Any two Sylow p-subgroups are isomorphic.

Corollary 18.2.2.

Let G be a finite group and K a Sylow p-subgroup for some prime p. Then K is normal if and only if K is the only Sylow p-subgroup in G.

Proof. ($\Rightarrow$) Let $K \trianglelefteq G$ be a Sylow p-subgroup, and let $\tilde{K} \leq G$ be some other Sylow p-subgroup. By the Second Sylow Theorem, there exists $a \in G$ such that $K = a^{-1}\tilde{K}a$ which implies $K = \tilde{K}$.

($\Leftarrow$) Let K be the only Sylow p-subgroup of G. Let $a \in G$, and then $|a^{-1}Ka| = |K|$ since there exists an isomorphism. This implies $a^{-1}Ka$ is also a Sylow p-subgroup of G. But since K is the only Sylow p-subgroup, we know $a^{-1}Ka = K$ thus implying normality of K. □

So far, the First Sylow Theorem allowed us to formally define a Sylow p-subgroup. Then, the Second Sylow Theorem established the relationship between any two given Sylow p-subgroups.

The next and final theorem tells us a bit more about the number of such p-subgroups.

Theorem 9.17 (Third Sylow Theorem).

The number of Sylow p-subgroups of a group G divides $|G|$ and is of the form $1 + pk$, or $\equiv 1 \pmod{p}$, for some nonnegative integer k.

So how are the Sylow Theorems actually helpful in classifying finite nonabelian groups? Well, we will soon see that these theorems are vital in determining the normality of subgroups, and by extension, the simplicity of groups.

Consider the following example.

Example 18.4. Let G be a group with order $63 = 3^2 \cdot 7$.

We know based on the First Sylow Theorem that there exists Sylow 7-subgroups of G with order 7. Additionally, we know that the number of such subgroups must divide 63 and be in the form $1 + 7k$.

The divisors of 63 are 1, 3, 7, 9, 21, 63
The numbers in the form $1 + 7k$ are 1, 8, 15, 22, 29, 36, 43, 50, 57, 64, etc.

Since 1 is the only number present in both of the above lists, we know then by the Third Sylow Theorem that there exists only 1 Sylow 7-subgroup of G. From there, as a corollary of the Second Sylow Theorem, this subgroup must be normal, consequently implying that no group of order 63 is simple.

This is actually quite a powerful tool in determinining simplicity. Let's take a look at another example.

Example 18.5. Can there exist a simple group of order 56?

Let G be an arbitrary group of order 56. Begin by noticing that $56 = 2^3 \cdot 7$. We now investigate the Sylow 7-subgroups. The only divisors of 56 that are of the ford $1 + 7k$ are 1 and 8, meaning there is either 1 Sylow 7-subgroup, or 8 of them.

1. If there is only 1 Sylow 7-subgroup, then it must be normal by the Second Sylow Theorem, thus implying that G is not simple.
2. Suppose there are then 8 Sylow 7-subgroups. Recall that the intersection of any two subgroups is another subgroup. Since each Sylow 7-subgroup has order 7 in this case, it implies that the intersection of any of the 8 Sylow 7-subgroups must be trivially $\langle e \rangle$, as subgroups must have orders that divide 7.

   Further recall that elements of Sylow 7-subgroups must all have order 7, giving us then 48 distinct elements of G with order 7.

   Now, Sylow **2**-subgroups of G must have order 8, and each element must also have order that divides 8. Since there are already 48 elements with order 7, this leaves us with room for exactly *one* such Sylow 2-subgroup, implying then that this subgroup must be normal by the Second Sylow Theorem.

In either case G has a nontrivial normal subgroup, and therefore groups of order 56 cannot be simple.

In both of these previous examples, we've used the Sylow Theorms to show negative results (ie. a group G does *not* satisfy some property). However, it's worth mentioning that these theorems can be used for positive results as well!

One exapmle is that they allow us to classify certain finite groups.

Corollary 18.3.1.

Let G be a group of order pq, where p, q are primes such that $p > q$. If $q \nmid (p-1)$, then $G \cong \mathbb{Z}_{pq}$.

Proof. By the Third Sylow Theorem, the number of Sylow p-subgroups must divide pq, and thus must be either $1, p, q, pq$. Since $p > q$, we know that $q \neq 1 + pk$. Further, both $p = 1 + pk$ and $pq = 1 + pk$ would imply $p \mid 1$, which is impossible. We're thus left with only one Sylow p-subgroup of G, call it H, which then must be normal.

A similar argument can be made for Sylow q-subgroups of G using the fact that $q \nmid (p-1)$. Call this unique q-subgropu K.

Since $H \cap K$ is a subgroup of both H and K, its order must divide p and q, thus implying $H \cap K = \langle e \rangle$. Further, it can be shown that $G = HK$. These two facts imply that $G = H \times K$ is a direct product.

Since $H \cong \mathbb{Z}_p$ and $K \cong \mathbb{Z}_q$, this implies

$$G = H \times K \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$$

□

19 Lecture 19: Feb. 27th

summary

9.4 Conjugacy and Proof of the Sylow Theorems

To begin, we first define the concept of conjugacy.

Definition (Conjugates)**.** Let G be a group and $a, b \in G$. We say that a **is conjugate to** b, denoted $a \sim b$, if there exists $x \in G$ such that $b = x^{-1}ax$.

For example, (12) is conjugate to (13) is S_3 because

$$(123)^{-1}(12)(123) = (132)(12)(123) = (13)$$

There is a key fact about conjugacies that we will be relying on.

Theorem 9.19.
Conjugacy is an equivalent relation on G.

Proof. Reflexive: $a \sim a$ since $a = eae = e^{-1}ae$.

Symmetric: if $a \sim b$, then $b = x^{-1}ax$ for some $x \in G$. Multiplying both sides by x and x^{-1} gives us $a = xbx^{-1} = (x^{-1})^{-1}b(x^{-1})$.

Transitive: if $a \sim b$ and $b \sim c$, then for some $x, y \in G$, we have $b = x^{-1}ax$ and $c = y^{-1}by$. Then, $c = y^{-1}(x^{-1}ax)y = y^{-1}x^{-1}axy = (xy)^{-1}a(xy)$. □

Where else have we seen an equivalence relation between elements of a set in all of algebra? Well, we've been constantly working with it in terms of modular congruence!

The equivalence class idea from modular congruence also carries over to conjugacy. Specifically, we say that a conjugacy class of an element a consists of all elements in G that are conjugate to a.

Furthermore, conjugacy classes must be disjoint or identical, and the group G is the union of all its conjugacy classes. Let's take a look at an example:

Example 19.1. The conjugacy class of (12) in S_3 consists of all elements $x^{-1}(12)x$, with $x \in S_3$.

Straight forward calculation that will be omitted in the interest of space and my laziness shows that for any $x \in S_3$, $x^{-1}(12)x$ is one of $(12), (13), (23)$. Thus, the conjugacy class of (12) is the set $\{(12), (13), (23)\}$.

Furthermore, we can show that the three distinct conjugacy classes of S_3 are

$$\{(1)\} \qquad \{(12), (13), (23)\} \qquad \{(123), (132)\}$$

It's important to notice here that although different conjugacy classes have different orders, the number of elements in any conjugacy class is a divisor of the group. We will see that this is true in the general case as well.

But before we go any further, it might be beneficial to first address why any of this matters. Well, as mentioned previously, this chapter is *all* about the proofs of the Sylow Theorems.

In order to tackle these hard-bitting proofs, we need some new tools. It is important to note though that many of these tools can be generalized for all of group theory.

Anyway, let's continue! We start with a definition.

Definition (Centralizer)**.** Let G be a group and $a \in G$. The **centralizer** of a is denoted $C(a)$ and consists of all elements in G that commutes with a, that is

$$C(a) = \{g \in G : ga = ag\}$$

And just real quick as a confirmation, we have

Theorem 9.20.

Let G be a group and $a \in G$. The centralizer $C(a)$ is a subgroup of G.

The centralizer tells us something very important about conjugacy classes.

Theorem 9.21.

Let G be a group and $a \in G$. The number of elements in the conjugacy class of a is the index $[G : C(a)]$ and this number divides $|G|$.

Proof. Before we begin, let's get the facts straight. We know that $C(a) \leq G$, and that $[G : C(a)]$ refers to the number of right cosets of $C(a)$ in G.

We want to show that the number of elements in the conjugacy class of a is equal to $[G : C(a)]$.

Let $x^{-1}ax$ and $y^{-1}ay$ be two elements of the conjugacy class of a. Then,

$$\begin{aligned} x^{-1}ax = y^{-1}ay &\Leftrightarrow (xy^{-1})^{-1}a(xy^{-1}) = a \\ &\Leftrightarrow a(xy^{-1}) = (xy^{-1})a \\ &\Leftrightarrow xy^{-1} \in C(a) \\ &\Leftrightarrow C(a)x = C(a)y \end{aligned}$$

For every conjugate of a, we have a different coset of $C(a)$. □

Buliding off of this, it should make sense that

$$|G| = |C_1 \cup C_2 \cup \cdots \cup C_t| = |C_1| + |C_2| + \cdots + |C_t|$$

since, again, conjugacy classes are disjoint and the union of all of them should cover all of G. Using what we've just proved with **Theorem 9.21**, we can also say that

$$|G| = [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_t)]$$

where each $a_i \in C_i$. Both of these expressions for the order of G are known as the **class equations** of the group G. These class equations will prove to be crucial in our discussion of the proofs of the Sylow Theorems.

To expand further, recall that for $c, x \in G$, we have $cx = xc$ if and only if $x^{-1}cx = c$. Thus, c is in the center of G and commutes with every $x \in G$ if and only if its *only* conjugate is itself.

With this, we can introduce a third class equation as:

$$|G| = |Z(G)| + |C_1| + |C_2| + \cdots + |C_r|$$

where each C_i now is the distinct conjugacy classes of G that contains strictly more than one element. Note here that each $|C_i|$ should still divide $|G|$.

On top of the class equations, we need one more nontrivial result in order to start on the Sylow Theorem proofs. Here it is.

Lemma 19.4 (Cauchy's Theorem for Abelian Groups).
If G is a finite abelian group and p is a prime that divides the order of G, then G contains an element of order p.

This was actually already mentioned and proved in the previous section.

We can finally now get to the proofs of the Sylow Theorems. Let's start with the first one, and before we dive straight in, recall the theorem statement.

Theorem 9.13 (First Sylow Theorem).
Let G be a finite group. If p is a prime and p^k divides $|G|$, then G has a subgroup of order p^k.

Proof. We prove this statement by an induction on the order of G. For $|G| = 1$, we have trivially that only $p^0 = 1$ divides $|G|$, and G itself would be the subgroup of order $p^0 = 1$.

Now assume the statement holds for all groups with size less than $|G|$.

Combining the second and third class equations from above, we can express the order of G as

$$|G| = |Z(G)| + [G : C(a_1)] + \cdots + [G : C(a_r)]$$

where each $[G : C(a_i)]$ has order > 1 that divides $|G|$. Additionally, $|Z(G)| \geq 1$ since $e \in Z(G)$. Note once again that $|[G : C(a_i)]| < |G|$, which is implied when $|[G : C(a_i)]| > 1$. We now split into two cases.

Case 1: Suppose there exists an index j for which p does not divide $|[G : C(a_j)]|$. By the hypothesis of the statement, we know $p^k \mid |G|$, and since $|G| = |C(a_j)| \cdot |[G : C(a_j)]|$ by Lagrange's theorem, this directly implies that $p^k \mid |C(a_j)|$.

By the inductive hypothesis now, we know since $|C(a_j)| < |G|$, then $C(a_j)$ must have a subgroup of order p^k, implying that the same subgroup exists in G.

Case 2: If p divides the order of $C(a_i)$ for every i, then since p divides $|G|$ by the statement's hypothesis, we know that it must also divide $|G| - |[G : C(a_i)]| - \cdots - |[G : C(a_r)]| = |Z(G)|$.

From here, since $Z(G)$ is abelian, by **Cauchy's theorem for abelian groups**, we know there exists some $c \in Z(G)$ with order p. Then the cyclic subgroup generated by c necessarily have order p, and must be normal to G. Call this subgroup N.

Now consider the quotient group G/N, which has order $|G|/p$, meaning it's both $< |G|$ and divisible by p^{k-1}. By the inductive hypothesis then there must exist some subgroup $T \leq G/N$ such that T has order p^{k-1}.

Carrying on, by the **Correspondance Theorem 8.24**, we know there must exist some subgroup H of G such that $N \subseteq H$ and $T = H/N$. Lagrange's theorem now shows us that

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

thus H is the subgroup of G with order p^k in this case.

Cases are exhaustive, and we conclude by the principle of induction that the claim holds for all finite groups G. $\square$

20 Lecture 20: Mar. 2nd

summary

9.4 Conjugacy and Proof of the Sylow Theorems (cont'd)

Happy March! Last couple of lectures of the quarter left and wowza that last proof was something huh. Connected like 17 dots from all across the place for that.

Anyway, we move onwards and towards the proofs for the second and third theorems. But before we get too ahead of ourselves, we do need some extra tools again.

We begin with a definition.

Definition (H-conjugate)**.** Let G be a group and fix a subgroup H of G. Then let A, B be any two subgroups of G. We say that A **is H-conjugate to** B if there exists $x \in H$ such that

$$B = x^{-1}Ax = \{x^{-1}ax : a \in A\}$$

In the case that $H = G$, then we simply say that A is conjugate to B (or vise versa).

Theorem 9.23.

Let $H \leq G$. Then H-conjugacy is an equivalence relation

Definition (Normalizer)**.** Let G be a group and A a subgroup of G. The **Normalizer** of A is the set $N(A)$ defined by

$$N(A) = \{g \in G : g^{-1}Ag = A\}$$

Intuition. *the set of elements in G for which A acts like a normal subgroup*

Theorem 9.24.

If A is a subgroup of G, then $N(A)$ is a subgroup of G and A is normal to $N(A)$.

Proof. tbh this one should be trivial. □

Theorem 9.25.

Let H and A be subgroups of a finite group G. The number of H-conjugates of A (the number of sets that are congruent to A wrt H) is $[H : H \cap N(A)]$ and therefore divides $|H|$.

Proof. The proof of this is the exact same as **Theorem 9.21**, just replace the corresponding players. □

Lemma 20.4.

Let O be a Sylow p-group of a finite group G. If $x \in G$ has order a power of p and $x^{-1}Qx = Q$, then $x \in Q$.

We are now officially ready for the proof of the Second Sylow Theorem... Finally. To recall, we have

Theorem 9.15 (Second Sylow Theorem).
Let P and K be Sylow p-subgroups of a group G. Then there exists $a \in G$ such that $P = a^{-1}Ka$.

Proof. Since K is a Sylow p-subgroup of G, we know $|K| = p^n$ where $|G| = p^n m$ and $p \nmid m$. Now let $K = K_1, K_2, \ldots, K_t$ be the distinct conjugates of K in G. By **Theorem 9.25**, $t = [G : N(K)]$. Since $p^n m = |G| = |N(K)| \cdot [G : N(K)] = |N(K)| \cdot t$, and p^n divides $|N(K)|$ beacuse K is a subgroup of $N(K)$ (and by Lagrange's theorem implies so), then $p \nmid t$.

Our next goal is to show that the Sylow p-subgroup P is conjugate to K, that is, P is one of K_i.

nahhh lowkey fade this proof its too much □

21 Lecture 21: Mar. 4th

summary

9.5 The Structure of Finite Groups

You may wonder why there was a time skip (like what happened to the proof of the third sylow theorem?), and there is no explanation for that. I just got lazy.

Anyway, the professor contextualized this lecture as a "harvest" of *everything* we've learned this entire quarter. We will be applying theorems and corollaries from all over, with the goal of classifying groups of certain orders.

To begin, we once again introduce yet another tool.

Theorem 9.27.

If G is a group of order p^n for some prime p and an integer $n \geq 1$, then the center $Z(G)$ contains more than one element, ie $|Z(G)| = p^k$ for $1 \leq k \leq n$.

Proof. By Lagrange, we know that since $Z(G) \leq G$ is a subgroup, then it must have order dividing p^n. In other words, $|Z(G)| = p^k$ for some $0 \leq k \leq n$. Note here that, for now, k could necessarily be equal to 0.

We also know by one of our class equations as discussed from the previous section,

$$|Z(G)| = |G| - |C_1| - |C_2| - \cdots - |C_r|$$

where C_i is the i-th conjugacy class of G, which has order $[G : C(a_i)]$, where now $C(a_i)$ is the centralizer of a_i. Additionally, we've shown that in this class equation, each $|C_i| > 1$, and since $C_i \leq G$ is a subgroup, $|C_i|$ divides p^n.

Combining these facts, we can actually now factor out a p from the RHS of the class equation to have

$$|Z(G)| = p\left(\frac{|G|}{p} - \frac{|C_1|}{p} - \cdots - \frac{C_r}{p}\right)$$

where the RHS is still strictly an integer. We've thus shown that $p \mid Z(G)$, allowing us to conclude $|Z(G)| \geq p$, meaning $|Z(G)| = p^k$ for $1 \leq k \leq n$. □

Corollary 21.1.1.

There is no simple group of order p^n where $n > 1$.

Proof. Let G be a group of order p^n. We show that G cannot be simple. Recall that $Z(G) \trianglelefteq G$ is a normal subgroup. We've also just shown that it cannot be the trivial group, ie $|Z(G)| > 1$. If $Z(G) \neq G$, then we are done as $Z(G)$ is a nontrivial normal subgroup.

In the case that $Z(G) = G$, ie G is abelian, then since $|G| \geq p^2$, there must exist some elmeent $c \in G$ with order p, meaning $|\langle c \rangle| = p$. Since $\langle c \rangle \leq G$ which is abelian, it then must be nontrivially normal in G. □

Corollary 21.1.2.

If G is a group of order p^2, then it must be abelian. The only possible isomorphism types are then $\mathbb{Z}_p \oplus \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.

Proof. Assume for contradiction that G is a nonabelian group of order p^2. As proven above, we know $|Z(G)| \in \{p, p^2\}$, since it is nontrivial and must divide the order of G.

However, we cannot have $|Z(G)| = p^2$ since that would imply G is abelian, so $|Z(G)| = p$. From here, we see then that $|G/Z(G)| = p$, implying that $G/Z(G)$ is cyclic. We've previously shown that $G/Z(G)$ is cyclic if and only if G is abelian, a contradiction. □

Theorem 9.30.

Let p and q be distinct primes such that $q \not\equiv 1 \pmod{p}$ and $p^2 \not\equiv 1 \pmod{q}$. If G is a group of order p^2q, then G is isomorphic to $\mathbb{Z}_{p^2q}$ or $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$.

Proof. We will show this with an argument using the Sylow p-subgroups. Begin by noticing the possible divisors of $|G|$ being $\{1, p, p^2, q, pq, p^2q\}$. By the Third Sylow Theorem, the number of Sylow p-subgroups must be

$$\#P \in \{1 + kp\} \cap \{1, p, p^2, q, pq, p^2q\}$$

However, notice that if $1 + kp = pm$ for any integer m, this would imply $1 = pm - pk = p(m - k)$, implying $p \mid 1$, which is not possible. We can thus narrow down the possible number of Sylow p-subgroups to $\{1, q\}$.

Another however, if $1 + kp = q$, then $q \equiv 1 \pmod{p}$, which is also assumed to be not true. Thus we know that there only exists one Sylow p-subgroup, which we will denote P.

By a similar argument, we see that the only possible number of Sylow q-subgroups are $\{1, p, p^2\}$. A third however, if $1 + kq = p^2$, then $p^2 \equiv 1 \pmod{q}$, which is assumed to be not true. Same for $1 + kq = p$. Thus we also know that there only exists one Sylow q-subgroup, which we will denote Q.

Now, what do we know about P and Q? Well, we know that $P \trianglelefteq G$ and $Q \trianglelefteq G$, and that $P \cap Q = \{e\}$, since there doesn't exist an element of G that has order divding both p and q. These facts imply $|PQ| = |P| \cdot |Q| = |G|$, and since $PQ \subseteq G$, we know then $PQ = G$.

By **Theorem 9.3**, we can now conclude that $G = P \times Q$. Since $|P| = p^2$, by our previous corollary P is abelian. $|Q| = q$ implies it must also be cyclic and abelian. Thus G must be abelian as well since it's the direct product of two abelian groups.

To bring it all together, we've shown that $G = G(p) \times G(q)$, and since $|G(p)| = p^2$, by our previous corollary, we know its isomorphism types are $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$. This gives us the possible isomorphism types of G being $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ or $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$. □

Corollary 21.2.1.

If p and q are distinct primes, then there is no simple group of order p^2q.

Proof. Let G be a group of order p^2q for distinct primes p and q. We split into 3 cases:

(1) If $p^2 \not\equiv 1 \pmod{q}$, then by the proof of our previous corollary, we know there exists a unique Sylow q-subgroup, which by the Second Sylow Theorem means it must be a normal subgroup in G.

(2) If $q \not\equiv 1 \pmod{p}$, then by the proof of our previous corollary, we know there exists a unique Sylow p-subgroup, which then also must be normal.

(3) We now consider the case where $p^2 \equiv 1 \pmod{q}$ and $q \equiv 1 \pmod{p}$. Since $q \equiv 1 \pmod{p}$, we know then that $p \mid q-1$, which implies $p \leq q-1$, or in other words, $q \geq p+1$. q'' Since $p^2 \equiv 1 \pmod{q}$, we know then that $q \mid p^2 - 1 = (p-1)(p+1)$, implying $q \mid p-1$ or $q \mid p+1$. However, since we've established that $q \geq p+1$, we cannot have $q \mid p-1$. This leaves us with $q \mid p+1$, which implies $q \leq p+1$.

Notice that we've shown $q \geq p+1$ and $q \leq p+1$, meaning we must have $q = p+1$. Since p, q are primes, the only case for which this is true is if $p = 2$ and $q = 3$, giving us $|G| = 2^2 \cdot 3 = 12$.

Lastly, we can now use the Sylow Theroms to justify why groups of order 12 cannot be simple. This part of the proof will be omitted for space, but it is very much similar to proofs done in the previous section.

Finally, since our three cases are exhaustive, we conclude that G cannot be a simple group. □

22 Lecture 22: Mar. 9th

summary

9.5 The Structure of Finite Groups (cont'd)

Today we continue on our quest to classify all finite groups using everything we've learned thorughout the quarter. Specifically, we will be investigating groups of order $2p$.

To do this, we need the help of the dihedral groups D_n, which if we recall, is the group of symmetries of a n-sided regular polygon.

...

Theorem 9.33.
If G is a group of order $2p$, where p is an odd prime, then G is isomorphic to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p.

To back pedal a bit, recall that in section 8.1 we classified all groups up to order ≤ 7. Let's pick up from here using our newfound knowledge of dihedral groups.

Theorem 9.34.
If G is a group of order 8, then G is isomorphic to one of the following groups:

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q$$

where D_4 is the dihegral group and Q is the group of quaternions.

Remark. We will see that groups with order p^n, especially for small p, will have many(!) isomorphism types.