# Introduction to Abstract Algebra

MATH 350, Yale University, Fall 2018

These are lecture notes for MATH 350a, "Introduction to Abstract Algebra," taught by Marketa Havlickova at Yale University during the fall of 2018. These notes are not official, and have not been proofread by the instructor for the course. These notes live in my lecture notes respository at

https://github.com/jopetty/lecture-notes/tree/master/MATH-350.

If you find any errors, please open a bug report describing the error, and label it with the course identifier, or open a pull request so I can correct it.

## Contents

# Syllabus

| | |
|---|---|
| **Instructor** | Marketa Havlickova, miki.havlickova@yale.edu |
| **Lecture** | MWF 10:30–11:20 AM, LOM 205 |
| **Recitation** | TBA |
| **Textbook** | Dummit and Foote. *Abstract Algebra*. 3rd ed. John Wiley & Sons, 2004 |
| **Midterms** | Wednesday, October 10, 2018<br>Wednesday, November 14, 2018 |
| **Final** | Monday, December 17, 2018, 2:00–5:30 PM |

Abstract Algebra is the study of mathematical structures carrying notions of "multiplication" and/or "addition". Though the rules governing these structures seem familiar from our middle and high school training in algebra, they can manifest themselves in a beautiful variety of different ways. The notion of a group, a structure carrying only multiplication, has its classical origins in the study of roots of polynomial equations and in the study of symmetries of geometrical objects. Today, group theory plays a role in almost all aspects of higher mathematics and has important applications in chemistry, computer science, materials science, physics, and in the modern theory of communications security. The main topics covered will be (finite) group theory, homomorphisms and isomorphism theorems, subgroups and quotient groups, group actions, the Sylow theorems, ring theory, ideals and quotient rings, Euclidean domains, principal ideal domains, unique factorization domains, module theory, and vector space theory. Time permitting, we will investigate other topics. This will be a heavily proof-based course with homework requiring a significant investment of time and thought. The course is essential for all students interested in studying higher mathematics, and it would be helpful for those considering majors such as computer science and theoretical physics.

Your final grade for the course will be determined by

$$\max \left\{ \begin{array}{l} 25\% \text{ homework} + 20\% \text{ exam } 1 + 20\% \text{ exam } 2 + 35\% \text{ final} \\ 25\% \text{ homework} + 10\% \text{ exam } 1 + 20\% \text{ exam } 2 + 45\% \text{ final} \\ 25\% \text{ homework} + 20\% \text{ exam } 1 + 10\% \text{ exam } 2 + 45\% \text{ final} \end{array} \right\}.$$

# References

[DF04] Dummit and Foote. *Abstract Algebra*. 3rd ed. John Wiley & Sons, 2004.

# 1 August 31, 2018

As always, Miki began class at precicely 10:25 AM. She wrote a review of last lecture on the bard, and then posed the following question as a warm up. She also talked about how the DUS department is arguing over whether money should be spent on T-shirts or chocolate (Miki thinks chocolate).

**Problem 1** (Warm Up)**.** Are these groups?
(a) $(\mathbb{Z}/n\mathbb{Z}, \times)$;
(b) $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \times)$

*Solution.* The solutions to the warm-up

*Solution to* (a). No, since 0 has no inverse. □

*Solution to* (b). No, this only works when $n$ is prime. For any factors $a, b$ of $n$, $a \times b = 0$, which isn't in the group. We say that $(\mathbb{Z}/p\mathbb{Z}, \times)$ is a group for all prime $p$. □

■

**Theorem 1** (Fermat's little theorem)**.** *For prime $p$ and composite $a = np$, then* $a^{p-1} \equiv 1 \pmod{p}$.

**Lemma 1.** *If $\bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, then $\bar{a}$ has an inverse in $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times)^*$.*

*Units*

**Definition 1** (Units)**.** A unit is something which has an inverse. The units of a group are denoted by putitng an asterisk after teh group, eg $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times)^*$.

**Example 1.** For integers modulo 4, $(\mathbb{Z}/4\mathbb{Z}, \times)^* = \{\bar{1}, \bar{3}\}$.

**Problem 2** (On Homework)**.** What are the conditions for determining the units of a group? We know it must have an inverse, but that's hard to check. Instead, we know that $a$ is a unit if and only if $\gcd(a, n) = 1$. Prove this.

## 1.1 Symmetries of a regular $n$-gon

Miki is angry with the book because she doesn't like how it treats symmetries, I think because she wants $D_{2n}$ to be called $D_n$.

Miki drew a triangle on the board, and began talking about the different operations we can preform on that triangle to preserve symmetries. She introduced $s$ to mean a reflection, and $r$ to mean a rotation. For a triangle, there are three distinct reflections,

$$s = \{s_1, s_2, s_3\},$$

where $s_i$ is the reflection across the line $OA_1$. We can also rotate the triangle in two directions.

We know that these are all the symmetries, since we can count the permutations of the triangle. We've exhauseted then, so we know that there can't be any more elements of the triangle-symmetry group $D_6$. In fact, because of the permutation fact, we konw that $|D_{2n}| = 2n$. Some other observations about $D_{2n}$:

- $s^2 = e \implies s = s^{-1}$;
- rotating twice clockwise is the same as rotating counterclockwise, so these aren't unique elememnts;
- $r^n = e$
- $rs = s_2$, so $s_n$ is just a combination of $r$ and $s$ — then we can generate the entire group with just $r$ and $s$.

These things lead us to discover a new object.

*Generators*

**Definition 2** (Generators)**.** For a group $G$, the generators of $G$ is a set $S = \{a, b, \ldots : a, b, \ldots \in G\}$ where $G$ is equal to all possible sombinations of elements of $S$. For $D_{2n}$, we could say that $D_{2n}$ is generated by $r$ and $s$. Usually there isn't a way to guess the generators of a group easily.

*Relations*

**Definition 3** (Relations)**.** A relation is a way of writing equivalent elements of groups. For example, in $D_{2n}$,

$$r^3 \equiv 1, \qquad s^2 \equiv 1, \qquad sr \equiv r^2 s.$$

Relations allow us to define how we can commute elements of the group.

*Presentation*

**Definition 4** (Presentation)**.** A presentation of a group are the generators combined with the relations necessary to create the group. The largest group which is generated from the generators and which satisfies the relations, and has no other relations, is our group. A presentation

is written as $\langle a, b \mid \text{relations between } a \text{ and } b \rangle$, where $a$ and $b$ are the generators of the group.

Now Miki told us that the group of the symmetires of a regular $n$-gon is the dihedral group of order $2n$, written either as $\{D_{2n}$ or $D_n\}$, depending on if you are a representation theorist or not.

**Problem 3** (HW)**.** Why is the order of $D_{2n}$ always $2n$?

## 1.2 Symmetric group on $n$ elements

Miki defined the symmetric group on $n$ elements $S_n$, which is just the permutations of $n$ elemnts. Notice that $D_{2n}$ is a subgroup of $S_n$. We know that the order of $S_n = n!$ and the order of $D_{2n} = 2n$.

[Insert diagrams of different ways to denote permuations, like the cycle notation]

# 2 September 4, 2018

**Definition 5.** For a set $\Omega$, the symmetric group on $\Omega$ is $S_\Omega = \{\text{bijective maps } \Omega \to \Omega\}$. For $n \in \mathbb{N}$, we say that $S_n = S_{\{1,\dots,n\}}$. This is usually called the symmetric group on $n$ letters.

Let's consider this example for $S_4$ (warning, there's some cyclic decomposition for $g_1, g_2$?)

**Example 2.** Consider the following maps $g_1, g_2 \in S_4$,

| $g_1$ | $g_2$ |
|---|---|
| $1 \to 2$ | $1 \to 3$ |
| $2 \to 1$ | $2 \to 1$ |
| $3 \to 4$ | $3 \to 2$ |
| $4 \to 2$ | $4 \to 4$ |

We can also write these as $g_1 = (12)(34)$ and $g_2 = (132)(4)$. In this notation, how to we multiply things? E.g., what is $g_2 g_1$? Well, we can write this naïvely as $(132)(4)(12)(34)$, but we don't want to repeat any numbers. Let's see what happens to 1:

$$(132)(4)(12)(34) \cdot 1 = (132)(4)(12) \cdot 1 = (132) \cdot 2 = 1.$$

For 2, we get

$$(132)(4)(12)(34) \cdot 2 = 3.$$

For 3, this comes $g_2 g_1 \cdot 3 = 4$, and for 4 we have $g_2 g_1 \cdot 4 = 2$. Then $g_2 g_1 = (1)(234)$. Unfortunately, doing this sort of element-wise reduction is the fastest way to multiply anything.

**Problem 4.** Someone asked the question "does order matter?" E.g., is it true that $(12)(34) = (34)(12)$ always?

*Solution.* No. They are the same. Also, $(abc) = (bca)$; as long as the sign of the permutation of the cycle elements is $+1$, it won't matter how you order the elements of a cycle. ■

**Problem 5.** Does order matter when there is a number repeated (when the cycles are not disjoint)? E.g. does $g_1g_2 = g_2g_1$?

*Solution.* Yeah, order does matter. Consider that $(12)(13) \neq (13)(12)$. This means that, in general, $S_n$ is not abelian. ■

**Problem 6.** Consider $S_5$, where $g = (123)(45)$ and $h = (12345)$. Find $g^2, g^{-1}, h^{-1}$. Fun fact, it's easy.

These facts lead us to an interesting and useful conclusion.

**Proposition 1.** *For any $g \in S_n$, we can write $g$ as a product of disjoint cycles.*

This gives us an interesting observation for $S_n$.

**Proposition 2.** *Let $g \in S_n$ be written as the product of disjoint cycles. Then the order of $g$ is the least common multiple of the orders of the disjoint cycles.*

## 2.1 Fields $n$ stuff

**Definition 6.** A field $k$ is a triple $(F, +, \times)$ where $(F, +)$ and $(F \setminus \{0\}, \times)$ are groups where $F^\times = F \setminus \{0\}$ and where multiplication distributes over addition. Some cannonical examples are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for prime $p$.

A brief note on finite fields: for a finite field $\mathbb{F}$, we know that $|\mathbb{F}| = p^n$ for some prime $p$ and some $n \geq 1$.

Now that we have fields, we can get matrices for free. Consider the cannonical matrix group $\mathrm{GL}_n(k)$ of invertible matrices with entries in $k$.

**Example 3.** Consider $\mathrm{GL}_2(\mathbb{F}_2)$ where $\mathbb{F}_2 = \{\bar{1}, \bar{2}\}$ (note that this is just $\mathbb{Z}/2\mathbb{Z}$). What is the order of $\mathrm{GL}_2(\mathbb{F}_2)$?

*Proof.* There are six. Any element cannot have three or four zeros in it, nor two zeros in the same row or column. Then just count the total possibilities. ■

# 3 September 7, 2018

Some facts about finite fields.

1. For all prime $p$, there exists a field $\mathbb{F}_p$ where $|\mathbb{F}_p| = p$;
2. For all prime $p$ and $n > 0$, there exists a field $\mathbb{F}$ where $|\mathbb{F}| = p^n$;
3. Every finite field has order $p^n$ for some prime $p$ and some $n > 0$.

From last time, we know for for all prime $p$ and all $n > 0$, there exists a field with $p^n$ elements. However, the naïve choice for this field isn't always right.

**Example 4.** Consider $\mathbb{F}_4$; what could it be?

*Solution.* It can't be $\mathbb{Z}/4\mathbb{Z}$, since inverses aren't unique as 4 isn't prime, and so $(\mathbb{Z}/4\mathbb{Z} \setminus \{0\}, \times)$ isn't a group. However, it could be the direct product of $\mathbb{Z}/2\mathbb{Z}$ with itself; i.e., $\mathbb{F}^4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Whatever it is, we know it has elements $\{\bar{0}, \bar{1}, x, x+1\}$ which satisfies $x^2+x+1 = 0$, $\bar{1}+\bar{1} = 0$, and $x+x = 0$. Then $x^2 = -x-1 = x+1$. ■

## 3.1 Homomorphisms

*Homomorphism*

**Definition 7** (Homomorphism)**.** A group homomorphism is a map $\varphi : (G, *) \to (H, \times)$ which preserves the operations between the groups, so $\varphi(a * b) = \varphi(a) \times \varphi(b)$. Usually, this is just abbreviated into $\varphi(ab) = \varphi(a)\varphi(b)$.

**Lemma 2.** *Let $\varphi$ be a homomorphism. Then $\varphi(1_G) = 1_H$, and $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

*Proof.* We know that $1 \cdot 1 = 1$. Then $\varphi(1 \cdot 1) = \varphi(1)\varphi(1) = \varphi(1)$. Then multiply by $\varphi(1)^{-1}$, and we have that $\varphi(1) = 1$. Consider then that $1 = aa^{-1}$, so $\varphi(1) = \varphi(a)\varphi(a^{-1}) = 1$ (by the previous result). Then $1 = \varphi(a)\varphi(a^{-1})$, so $\varphi(a^{-1}) = \varphi(a)^{-1}$ since inverses are unique. ■

**Example 5** (Examples of Homomorphisms)**.**

1. The identity map $g \mapsto g$;
2. The determinant $\det : \mathrm{GL}_n(\mathbb{R}) \to (R^\times, \times)$;
3. The map $(\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ where $a \mapsto \bar{a}$;
4. Let $g \in G$. Then we have a map $(\mathbb{Z}, +) \to G$ where $n \mapsto g^n$.

*Isomorphism*

**Definition 8** (Isomorphism)**.** An isomorphism is a bijective homomorphism. Note that the inverse of an isomorphism is also a group isomorphism.

What does it mean for two things to be isomorphic? Well, it means that anything you care about can be preserved under a sufficiently good map, so two isomorphic groups aren't the same, but they're "the same." As an example of why they aren't actually the same, consider that $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_3^\times, \times)$ are isomorphic. These groups don't have the same elements or the same operations, but they are isomorphic to one another.

**Lemma 3.** *Let $\phi : G \to H$ be a homomorphism where $g_i \mapsto h_i$. Then any relation on $\{g_i\}$ is satisfied by $\{h_i\}$. For example, if $G$ is abelian then $H$ is abelian as well.*

**Corollary 1.** *If $G = \langle g_1, \ldots, g_n \mid \text{relations} \rangle$, and if $h_1, \ldots, h_n \in H$ satisfy the same relations, then there exists a homomorphism $\phi : G \to H$ where $g_i \mapsto h_i$. However, any map which does preserve these relations need not be surjective nor injective. This means that presentations aren't enough to determine group isometry. Worse, minimal generating sets may not even have the same size for distinct generators. For example $\{1\}$ and $\{2, 3\}$ both generate $\mathbb{Z}_6$.*

**Corollary 2.** *Homomorphisms don't actually preserve order, since if $g^n = 1$ then $\phi(g^n) = 1$, but the order of $\phi(g^n)$ might just be a divisor of $n$, not $n$ itself.*

*Subgroup*

**Definition 9** (Subgroup)**.** A subgroup $H$ of $G$ is a group where the set of $H$ is a subset of $G$ and $H$ inherits its operation from $G$. Formally, $H$ is a subgroup of $G$ if the following are satisfied:

- $e \in G$;
- $a \in H \implies a^{-1} \in H$;
- $a, b \in H \implies ab \in H$.

# 4 September 10, 2018

A useful fact about orders a generated subgroups.

**Lemma 4.** *Let $x \in G$, and let $\langle x \rangle \subset G$. Then $|x| = |\langle x \rangle|$.*

Today, we're gonna connect the notion of a homomorphism and the notion of a group. Let $\phi : H \to G$ be a homomorphism. Then the image $\phi(H)$ is a subgroup of $G$. Why is this true? Well, trivially, $\phi(H)$ is a subset of $G$. Since $\phi$ is a homomorphism, we know that $\phi(1) = 1$ and so $1 \in \phi(H)$. Since $\phi$ is multiplicative, $\phi(a), \phi(b) \in \phi(H) \implies \phi(a)\phi(b) \in \phi(H)$. And since $\phi(a)^{-1} = \phi(a^{-1})$, $\phi(H)$ contains inverses for all $\phi(a) \in \phi(H)$. However, there's not much that we can say about $\phi(H)$ in relation to $G$, other than the fact that it must not be larger than $G$. However, if $\phi : H \hookrightarrow G$ is injective, then $H$ and $\phi(H)$ are isomorphic, so there's a copy of $H$ inside of $G$.

## 4.1 Representation Theory

Miki says that she's not supposed to talk about representation theory in this class but she can't resist mentioning it here when we discuss group actions.

*Group Action*

**Definition 10** (Group Action)**.** Let $G$ be a group. A group action is a map $\phi : G \times A \to A$, where $A$ is a set on which $G$ is acting, which obeys the following axioms.

1. The identity in $G$ becomes the identity map, so $\phi(1_G, a) = a$ for all $a \in A$;
2. The action $\phi$ is associative, so $\phi(g, \phi(h, a)) = \phi(gh, a)$.

The simplest example of a group action is the *trivial action*, which is simply the map $\phi(g, a) = a$ for any $a \in A$ and any $g \in G$. Another example is *translation*, where we map each $a$ to $a + n$ from some $n$. *Reflection* is where we map $a$ to $-a$.

**Example 6.** Some food for thought: the group operation is also an action on that group.

Some facts about group actions.

**Lemma 5.** *For all $g \in G$, we get a map $\sigma_g : A \to A$ where $a \mapsto g \cdot a$; then $\sigma_g$ is bijective since it's just a permutation of $a$; then we have a map $\pi : G \to S_A : g \mapsto \sigma_g$. This map $\pi$ is a group homomorphism. However, we don't know that $\pi$ is necessarily injective.*

*Proof.* We know that $\sigma_g$ is bijective since it has an inverse in $\sigma_{g^{-1}}$. Since it's bijective, we know that $\sigma_g$ is a permutation, and so is an element of $S_A$. Then consider that $\pi(gh)(a) = (gh)(a) = g \cdot (h \cdot a) = \pi(g)\pi(h)(a)$, so $\pi$ is multiplicative. ■

**Example 7.** Let $A = G$, so our action is left multiplication $* : G \times G \to G : (g, a) \mapsto ga$. Since multiplication already fulfills the requirements for group actions, we know this forms a valid action. For this action, look at the map $\pi : G \to S_G$. We know $\pi(g) = \sigma_g$ is bijective. Then $\pi$ is injective. This fact gives us that every finite group is isomorphic to a subgroup of $S_n$ for some $n$, since $G \cong \pi(G) \subset S_n$ for $n = |G|$.

*Proof.* Suppose $\sigma_g = \sigma_h$. Then $\sigma_g(a) = \sigma_h(a)$ for all $a \in A = G$. In particular, let $a = 1$. The $g = g \cdot 1 = h \cdot 1 = h$, so $g = h$. Then $\pi(g) = \pi(h)$ if and only if $g = h$. ■

## 4.2 Isomorphisms and Equality

Why do we bother saying that groups are isomorphic instead of just saying that groups are "equal." Consider $D_8$ acting on a square $\square$. There is a subgroup $H_1 = \langle r^2 \rangle = \{1, r^2\}$. We know that $H_1 \cong \mathbb{Z}/2\mathbb{Z}$. There is also the subgroup $H_2 = \langle s \rangle = \{1, s\}$. We know that $H_2$ is also isomorphic to $\mathbb{Z}/2\mathbb{Z}$. However, it's pretty clear that $H_1 \neq H_2$ even though $H_1 \cong H_2$. Then isomorphic groups can be distinguished by their group actions.

# 5 September 12, 2018

"Oh, I erased my smiley face. How sad." (she did not sound sad)

Miki

Today we'll officially state something we covered last time.

**Theorem 2** (Caley's Theorem)**.** *Every finite group $G$ is isomorphic to a subgroup of $S_n$ for some $n$.*

*Proof.* Let $n = |G|$. ■

## 5.1 Kernels

Let's discuss formally the idea of a kernel of a homomorphism and a kernel of a group action.

*Kernel*

**Definition 11** (Kernel)**.** Let $\phi : G \to H$ be a homomorphism. Then the kernel of $\phi$, written $\ker \phi$, is the set of all elements in $G$ which are mapped to the identity in $H$; i.e., $\ker \phi = \{g \mid \phi(g) = 1_h\}$.

**Definition 12.** Suppose $G$ acts on $A$ by $\pi$. Then the kernel of the action is the set of all elements of $g$ which act trivially on $A$; i.e., $\ker \pi = \{g \mid ga = a \text{ for all } a \in A\}$.

**Example 8.** Consider the action $\phi : \mathrm{GL}_2(\mathbb{R}) \to (\mathbb{R}^\times, \times) : A \mapsto \det A$. Then the kernel of $\phi$ are all matricies with determinant 1, called $\mathrm{SL}_2(\mathbb{R})$.

*Stabalizer*

**Definition 13** (Stabalizer)**.** Let $\pi : G \times A \to A$ be a group action, and fix $a \in A$. The *stabalizer* is $G_a = \{g \in G \mid ga = a\}$. By this definition, the kernel is contained within any stabalizer, and in fact is equal to the intersection of all stabalizers.

**Example 9.** Let $G = \mathrm{GL}_2(\mathbb{R})$ and let $A = \mathbb{R}^2$ defined with the usual action (vector-matrix multiplication). What is the kernel of this action? Then let $c = (0, 1)^\top \in \mathbb{R}^2$. What is the stabalizer of $c$?

**Corollary 3.** *The kernel of an action is a subgroup of $G$, and $G_a$ is a subgroup of $G$ for any fixed $a \in A$.*

*Orbit*

**Definition 14** (Orbit)**.** Fix $a \in A$. The orbit of $a$ is the image of $a$ under the group action; i.e., $O_a = \{ga \mid g \in G\}$. Intuitively, it's everywhere $a$ can go under a specific group action. Notice that the orbits partition $A$, and so are equivalence classes in $A$.

**Example 10.** Let $G = \mathrm{GL}_2(\mathbb{R})$ and let $A = \mathbb{R}^2$ defined with the usual action (vector-matrix multiplication). What is the orbit of $(1, 0)^\top$?

*Faithful*

**Definition 15** (Faithful)**.** An action is faithful if the kernel is the identity. This means that the base element of the action must be the identity. This tells us that $G$ is injective into $S_A$.

**Example 11.** Consider $D_8$ acting on a square (technically the set $A = \{1, 2, 3, 4\}$). The orbit $O_1$ is all possible vertices, since you can rotate any vertex to any position. The stabalizer is $\{1, s\}$.

**Lemma 6.** *As it turns out, for a fixed $a \in A$, we see that $|O_a||G_a| = |G|$. We'll prove this later. (Orbit-Stabalizer Theorem I think?)*

*Conjugation*

**Definition 16** (Conjugation)**.** Consider the action $\pi : G \times G \to G : (g, a) \mapsto gag^{-1}$. This action is known as *conjugation*.

*Centralizer*

**Definition 17** (Centralizer)**.** Let $S \subset G$. The *centralizer* of $S$ in $G$, written $C_G(S) = \{g \in G \mid gsg^{-1} = s \text{ for all } s \in S\}$. This is the set of things that fix $S$ in $G$ pointwise under conjucation. By definition, this is the set of elements in $G$ which commute with all elements in $S$. In the case that $S = \{s\}$ we see that $C_G(S) = G_S$.

*Normalizer*

**Definition 18** (Normalizer)**.** Let $S \subset G$. The *normalizer* of $S$ in $G$ is $N_G(S) = \{g \in G \mid gSg^{-1} = S\}$. Essentially, this is just a centralizer on a set, except that it may permute the elements of $S$. Then $C_G(S) \subset N_G(S)$.

**Example 12.** Suppose that $G$ is abelian. For any $S \subset G$, we see that $C_G(S) = N_G(S) = G$.

**Example 13.** Let $G = S_3$, and let $S = G$. What is the normalizer of $S$? (It's the whole thing since $G$ is closed under its operation.) What is the centralizer of $S$? (It's the identity.)

# 6 September 14, 2018

> "Why do we get struck by lightning when we reach a contradiciton? I don't know, it's usually a good thing." ϟ
>
> Miki

**Definition 19** (Center)**.** The center of a group $G$ is $Z(G) = \{g \in G \mid gs = sg \text{ for all } s \in G\}$; i.e., $Z(G) = C_G(G)$, so it's the centralizer of the whole group. *Center*

Why do we care so much about conjugation? We give all these special names to the sets of conjugation, like the Normalizer, Stabalizer, and Centralizer. We also know that conjugation preserves the order of an element, so $|a| = \left|gag^{-1}\right|$.

**Problem 7.** What is the center of $D_8$? We know the identity must be in the center. What about $r^2$? We know it commutes with $s$, and $sr^2 = r^{-2}s = r^2s$, so it commutes with $s$ as well; Since $r$ and $s$ generate the group, we know that it be in the center as well. So $Z(D_8) = \{1, r^2\}$.

## 6.1 Cyclic Groups

**Proposition 3.** *Let $G$ be a group, and let $x \in G$. For $m, n \in \mathbb{Z}$, if $x^n = x^m = 1$ then $x^d = 1$ where $d = \gcd(m, n)$.*

*Proof.* Use the Euclidean Algorithm. We know there are integers $a, b \in \mathbb{Z}$ where $d = am + bn$, so $x^d = x^{am+bn} = (x^a)^m(x^b)^n = 1^a 1^b = 1$. ■

**Corollary 4.** *If $x^m = 1$ then $|x|$ divides $m$ if $m$ is finite.*

*Proof.* If $m = 0$, we are done since everything divies zero. Assume that $1 \leq m < \infty$. Let $n = |x| \leq m < \infty$ be finite. Let $d = \gcd(m, n)$, so $x^d = 1$. We know that $d$ divides $n$, and since $n$ is the smallest power of $x$ to be the identity, we know that $d = n$. *A priori,* we know that $d$ divides $m$ so $d$ must divide $m$ as well. ■

**Proposition 4.** *Let $x \in G$, and let $a \in \mathbb{Z} \setminus \{0\}$.*

1. *If $|x| = \infty$, then $|x^a| = \infty$;*
2. *If $|x| = n < \infty$, then $|x^a| = n/\gcd(a, n)$.*

*Proof.* The proof of (1) is ommitted, and left as an exercise to the student. For (2), let's focus on the special case that $a$ divides $n$. If $x^n = 1$ then $(x^a)^{n/a} = x^n = 1$.

Then $|x^a|$ is at most $n/a$. Suppose by way of contraction that the order $d$ is strictly less than $n/a$. Then $x^{ad} = 1 \implies 1 \leq ad < n$, but $|x| = n$. This is a contradiction, so the order of $x^a$ must be exactly $n/a$. In the case that $a$ does not divide $n$, play around with this to get the more general conclusion (the logic is the same). ■

**Definition 20** (Cyclic Group)**.** A group $G$ is cyclic if there exists an $x \in G$ such that $G = \langle x \rangle$. As a note, it's not always easy to tell since there could be other presentaitons of a group which are not single elements. Always remember that presentations are not unique. *Cyclic Group*

**Problem 8.** Let $G = \langle a, b \mid a^2 = b^3 = 1, ab = ba \rangle$. Show that $G$ is cyclic.

**Corollary 5.** *All cyclic groups must be abelian, since any $g \in G$ is generated by some $x^a$, and $x$ always commutes with itself.*

**Example 14** (Infinite Cyclic Groups)**.** Throughout, let $G = \langle x \rangle$, and assume that $|x| = \infty$.

**Proposition 5.** *The order of $G$ is $\infty$. Then $x^m \neq x^n$ for all distinct $m, n \in \mathbb{Z}$.*

*Proof.* Let $m < n$. Suppose by way of contradiction that $x^m = x^n$. Then $x^{n-m} = 1$, which cannot happen since $n - m > 0$ and $|x| = \infty$. Then $|G| = \infty$. ■

**Proposition 6.** *Such $G$ must be isomorphic to $(\mathbb{Z}, +)$.*

*Proof.* Define a map $\phi : \mathbb{Z} \to G : n \mapsto x^n$. This map is well defined. It also respects multiplication since $m + n \mapsto x^m x^n$. It is injective by Proposition 1, and it is surjective by Proposition 1 since $G$ is generated completely by $x$. Then $\phi$ is an isomorphism. ■

**Proposition 7.** *Such a group $G$ is generated by $x^n$ if and only if $n = \pm 1$.*

*Proof.* Left as an exercise to the student. ■

**Proposition 8.** *Every subgroup of $G$ is cyclic of the form $H = \langle x^n \rangle$ for some $n \in \mathbb{Z}$.*

*Proof.* Suppose that $x^n = 1$. Then $H$ is obviously cyclic. On the other hand, if $H \neq \langle 1 \rangle$. Let $n = \min\{k > 0 \mid x^k \in H\}$. This can't be empty, so there is an $n$. Then $\langle x^n \rangle \subset H$. Take some other element $x^m \in H$, and let

$d = \gcd(m, n) = am + bn$. Then $x^d = (x^m)^a(x^n)^b \in H$ but $1 \leq d \leq n$, so $d = n$. Then $n$ divides $m$, and so $x^m \in \langle x^n \rangle$. The $\langle x^n \rangle = H$, and so $H$ is cyclic. ■

**Corollary 6.** *Every non-trivial subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.*

**Corollary 7.** *For some cyclic $G$, we know that $\langle x^n \rangle = \langle x^{-n} \rangle \subset G$. Then all non-trivial subgroups correspond to $\mathbb{Z}_{>0}$.*

# 7 September 17, 2018

"The only thing I learned for years was how to count hedgehogs in a field." (In the midst of a wonderful and inspirational talk about being a mathematician.)

Miki

## 7.1 Finite Cyclic Groups

Today, we'll cover finite cyclic groups. This will be very similar to the previous lecture on infinite cyclic groups. As a reminder, here are the propositions for infinite cyclic groups:

**Proposition 9** (Infinite Cyclic Groups)**.** *Let $G$ be an infinite cyclic group.*

1. *The order of $G$ is infinite, with $G = \{\dots, x^{-1}, 1, x, x^2, \dots\}$ all distinct.*
2. *The group $G$ is isomorphic to $\mathbb{Z}$.*
3. *The group $G$ is generated by $x^n$ if and only if $n = \pm 1$.*
4. *Every subgroup $G$ is cyclic.*

Now for the finite case.

**Proposition 10** (Finite Cyclic Groups)**.** *Let $G = \langle x \rangle$ with $|G| = n < \infty$.*

*P1. The group $G$ is exactly $\{1, x, \dots, x^{n-1}\}$.*

*P2. The group $G$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

*P3. The group $G$ is generated by $x^k$ if and only if $\gcd(k, n) = 1$.*

*P4. Every subgroup of $G$ is also cyclic. That is, for all $k > 0$ where $k$ divides $n$ we get a subgroup $H$ of order $k$ generated by $x^{n/k}$*

*Proof of P1.* We know that $1, \dots, x^{n-1}$ are all in $G$. Suppose that $x^a = x^b$ for some distinct $a, b$. Then $x^{b-a} = 1$ for $0 < b - a < n$, which is a contradiciton since $|x| = n$. In fact, this set enumerates $G$. Suppose that $x^k \in G$ for some $k \in \mathbb{Z}$. We use the divison algorithm to write that $k = an + r$ for some $a, r \in \mathbb{Z}$. Then $x^k = x^{an+r} = (x^n)^a x^r = x^r$, so $x^k$ is in $G$. ■

*Proof of P2.* Let $\phi : \mathbb{Z}/n\mathbb{Z} \to G : \bar{k} \mapsto x^k$ where $k$ is any representative of $\bar{k} \in \mathbb{Z}$. To show that $\phi$ is well-defined, consider another representative $\ell$ of $\bar{k} \in \mathbb{Z}$. Then $\ell = k + an$, so $x^\ell = x^{k+an} = x^k (x^n)^a = x^k$. To show that $\phi$ is a homomorphism,

consider that $\phi(\bar{m}+\bar{n}) = x^{m+n} = x^m x^n$, so $\phi$ is multiplicative. Finally, we know that $\phi$ is surjective and injective by P1. This tells us that, up to an isomorphism, there are only really two cyclic groups; $\mathbb{Z}$ if the group is of infinite order, or $\mathbb{Z}/n\mathbb{Z}$ if it is finite. ■

*Proof of P3.* This is more of a sketch. Recall that $\langle |x^k| \rangle = |x^k|$, and this is $n$ if and only if $\gcd(k,n) = 1$. In general, $|x^k| = n/\gcd(k,n)$. ■

*Proof of P4.* Exactly the same as the infinite case. ■

Now that we've covered cyclic groups, it's helpful to introduce some notation to represent them.

> **Notation** $(\mathbb{Z}_n, C_n)$**.** We write the multiplicative cyclic group of order $n$ as $\mathbb{Z}_n$. The additive cyclic group of order $n$, which we've been writing as $\mathbb{Z}/n\mathbb{Z}$, is commonly written as $C_n$. $\mathbb{Z}_n, C_n$

## 7.2 Subgroups

[DF04] uses the notation $S \subset G$ to mean that $S$ is a subset of $G$, and $H \leq G$ to mean that $H$ is a subgroup of $G$.

> **Definition 21** (Subgroup)**.** Let $S \subset G$ be nonempty. Let $H = \{a_1^{\varepsilon_1} \cdots a_k^{\varepsilon_k}\}$ where $a_i \in S$ and $\varepsilon_i = \pm 1$ for $k \in \mathbb{Z}_{\geq 0}$. This sequence of $a_i^{\varepsilon_i}$ is called a *word*. Note that $a_i$ need not be distinct. Then $H$ is a subgroup of $G$. *Subgroup*

*Proof.* First, we know that $H \subset G$. We know that $1 \in H$. Since any concatenation of words is also a word, we know that $H$ is closed under multiplication. Finally, since $((ab)^n)^{-1} = b^{-n}a^{-n}$ we know that the inverses of a word are words themselves, and so $H$ is closed under inversion. ■

# 8 September 19, 2018

"Funny things happen with groups, which is why they're fun!"

Miki

Recall from last time how we defined a subgroup $H$ of $G$ in terms of words where the powers of each element was $\pm 1$. If $G$ is abelian we can combine elements of like bases to get powers which can be any integral value. If we assume that $|a_i| = d_i$ is finite for all $a_i \in H$, then we know that $|H| \leq d_1 \cdots d_k$. This gives us a limit on the order of a subgroup; if $G$ is abelian then the order of a subgroup is bounded above by the product of the orders of the generating elements. On the other hand, if $G$ is not abelian then this does not always hold. Consider $G = \langle a, b \mid a^2 = b^2 = 1 \rangle$. If $G$ isn't commutative, then $(ab)^n \neq a^n b^n$ for all $n$ and so we can just create infinitely many words by appending $ab$ to one another and so the order is infinite.

**Lemma 7.** *Let $G = \{a_1^{n_1} \cdots a_k^{n_k}\}$ be abelian, and let each $a_i$ have finite order $d_i$. Then $|G| \leq d_1 \cdots d_i$.*

**Proposition 11.** *Let $G$ be a group and let $\mathcal{L}$ be a collection of subgroups of $G$. Then*

$$K = \bigcap_{L \in \mathcal{L}} L$$

*is a subgroup of $G$.*

*Subgroup*

**Definition 22** (Subgroup)**.** Let $S \subset G$ and let $\mathcal{L} = \{L \leq G \mid s \subset L\}$. Then the subgroup generated by $S$ is

$$K = \bigcap_{L \in \mathcal{L}} L.$$

What do we know from this definition? Well, $S \subset K$ and $K \leq G$. We want to say that $K \in \mathcal{L}$ is the minimal element, so $K = L_i$ for some $i$.

*Minimal Element*

**Definition 23** (Minimal Element)**.** Let $\mathcal{M}$ be a collection of subsets of $G$. A minimal element is an element $M$ of $\mathcal{M}$ such that if $M' \in \mathcal{M}$ and $M' \subset M$ then $M = M'$. It's like "the smallest element" except there could be multiple minimal elements.

We want to show that $K$ is *the* minimal element of $\mathcal{L}$.

*Proof $K$ is minimal.* Let $L \in \mathcal{L}$. Then $K \subset L$. Then either $K = L$ or $L$ is not minimal. ■

*Proof $K$ is* the *minimal element.* Suppose there is another minimal $M$ in $\mathcal{L}$. By definition $K \subset M$ so by minimality $M = K$. ■

**Proposition 12.** *Our two definitions for subgroup (generated by words $H$ and minimal element of collection $K$) containing elements of $S \subset G$ are equivalent.*

*Proof.* $H \leq G$ and $S \subset H$ by the construction of 1-letter words. Then $H \in \mathcal{L}$ so $K \subset H$. On the other hand, $S \subset K$ and $K$ is a group. Then $K$ contains all inverses and products of elements in $S$, so it contains all words and therefore contains $H$. Then $H \subset K$. Putting this together, we have that $K = H$. ■

*Lattice*

**Definition 24** (Lattice)**.** Given a group $G$, a lattice is a diagram showing all subgroups of $G$ which shows containment between the subgroups.

**Figure 1:** Lattice Diagram of $C_2$

Recall from last time that for $C_n$ the subgroups are paired with the divisors $k$ of $n$; then $\langle k \rangle$ generates subgroup of order $n/k$.

**Figure 2:** Lattice Diagram of $C_4$

**Figure 3:** Lattice Diagram of $C_8$

**Figure 4:** Lattice Diagram of $C_6$

**Figure 5:** Lattice Diagram of $S_3$