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
	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 Wednesday, 29 August 2018

Most of today's lecture was administrata covering how the course will be run.

Towards the end of the period we began to play with the very basic concepts of group theory. First and foremost is the definition of a group.

> **Definition 1** (Group)**.** A group is an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G, which obeys the following axioms.
>
> - There exists an element $e \in G$ known as the *identity* with the property that $e \star g = g \star e = g$ for all $g \in G$.
> - For all $g \in G$ there exists a $g^{-1} \in G$ known as the *inverse* of g which has the property that $g \star g^{-1} = g^{-1} \star g = e$.
> - The operation $\star$ is associative.

Group

You will sometimes see a fourth axiom included in this list, namely that G is closed under $\star$, but since $\star$ is a binary operation on G which definitionally means it is a map $\star : G \times G \to G$, and so G is always implicitly closed under $\star$. When *checking* whether or not $(G, \star)$ is a group, though, it is a very good idea to check that $\star$ actually is a binary operation.

You're probably already familiar with lots of groups already. Consdier the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the set of symmetries of the square, and the integers (under addition, which is important).

2 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 $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times)^*$.*

Definition 2 (Units)**.** A unit is something which has an inverse. The units of a group are denoted by putitng an asterisk after teh group, eg $(\mathbb{Z}/p\mathbb{Z} \setminus \{0\}, \times)^*$. *Units*

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.

2.1 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.

Definition 3 (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. *Generators*

Definition 4 (Relations)**.** A relation is a way of writing equivalent elements of groups. For example, in D_{2n}, *Relations*

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

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

Definition 5 (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. *Presentation*

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 $2n$?

2.2 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]

3 September 4, 2018

Definition 6. For a set Ω, the symmetric group on Ω is $S_\Omega = \{\text{bijective maps } \Omega \to \Omega\}$. For $n \in \mathbb{N}$, we say that $S_n = S_{\{1,\ldots,n\}}$. 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 $g_1 g_2 = g_2 g_1$?

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.*

3.1 Fields n stuff

Definition 7. 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. ■

4 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 $x^2 = -x - 1 = x + 1$. ∎

4.1 Homomorphisms

Definition 8 (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 $\varphi(ab) = \varphi(a)\varphi(b)$. *Homomorphism*

Lemma 2. *Let φ 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 $n \mapsto g^n$.

Definition 9 (Isomorphism)**.** An isomorphism is a bijective homomorphism. Note that the inverse of an isomorphism is also a group isomorphism.

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 $G = \langle g_1, \dots, g_n \mid \textit{relations} \rangle$, and if $h_1, \dots, h_n \in H$ 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.*

Definition 10 (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:

Subgroup

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

5 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 ϕ is a homomorphism, we know that $\phi(1) = 1$ and so $1 \in \phi(H)$. Since ϕ 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.

5.1 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 11 (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 ϕ 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 σ_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 π is a group homomorphism. However, we don't know that π is necessarily injective.*

Proof. We know that σ_g is bijective since it has an inverse in $\sigma_{g^{-1}}$. Since it's bijective, we know that σ_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 π 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 π 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 $g = h$. ■

5.2 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.

6 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 $n = |G|$. ■

6.1 Kernels

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

Definition 12 (Kernel). Let $\phi : G \to H$ be a homomorphism. Then the kernel of ϕ, written $\ker \phi$, is the set of all elements in G which are mapped to the identity in H; i.e., $\ker \phi = \{g \mid \phi(g) = 1_h\}$. *Kernel*

Definition 13. Suppose G acts on A by π. 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 ϕ are all matricies with determinant 1, called $\mathrm{SL}_2(\mathbb{R})$.

Definition 14 (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. *Stabalizer*

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 $a \in A$.*

Definition 15 (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. *Orbit*

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 $(1, 0)^\top$?

Definition 16 (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. *Faithful*

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?)*

Definition 17 (Conjugation)**.** Consider the action $\pi : G \times G \to G : (g, a) \mapsto gag^{-1}$. This action is known as *conjugation.* *Conjugation*

Definition 18 (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 $C_G(S) = G_S$. *Centralizer*

Definition 19 (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 $C_G(S) \subset N_G(S)$. *Normalizer*

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.)

7 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." ↯

Miki

Definition 20 (Center)**.** The center of a group G is $Z(G) = \{g \in G \mid gs = sg$ 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 $|a| = |gag^{-1}|$.

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 $Z(D_8) = \{1, r^2\}$.

7.1 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 21 (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 ∞. 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 ϕ 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* $\mathbb{Z}_{>0}$.

8 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

8.1 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 ϕ is well-defined, consider another representative ℓ 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 ϕ is a homomorphism, consider that $\phi(\bar{m} + \bar{n}) = x^{m+n} = x^m x^n$, so ϕ is multiplicative. Finally, we know that ϕ 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. $\mathbb{Z}_n, C_n$

8.2 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 22 (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. ■

9 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 ± 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.

Definition 23 (Subgroup)**.** Let $S \subset G$ and let $\mathcal{L} = \{L \leq G \mid s \subset L\}$. Then the subgroup generated by S is

Subgroup

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

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.

Definition 24 (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.

Minimal Element

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 $M = K$. ∎

9 September 19, 2018

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 25 (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

9 September 19, 2018

Figure 4: Lattice Diagram of C_6

Figure 5: Lattice Diagram of S_3

10 September 21, 2018

"Oh I erased my smiley face again. How sad." (She did not sound sad.)

Miki

Problem 9 (Warm up). Draw the lattice diagram for C_{12}.

Figure 6: Lattice for C_{12}

Finish this

11 September 24, 2018

"This is where the fun begins." (slightly paraphrased)

Miki

11.1 Quotient Groups

For the rest of this section, keep in mind the example of $\mathbb{Z}/n\mathbb{Z}$. This is kind of like the prototypical example for quotient groups.

> **Definition 26** (Coset)**.** Let $H \leq G$. The left coset of H in G is a set of the form $aH = \{ah \mid h \in H\} \subset G$ for a fixed $a \in G$. The right coset of H in G is a set of the form $Hb = \{hb \mid h \in H\} \subset G$ for a fixed $b \in G$.

Coset

We said previously that left multiplication permutes the elements of H (this was called the left regular action), and in particular we know that $|aH| = |H|$. We can see this trivially by simply multiplying each ah by a^{-1}. Note that this coset is usually *not* a subgroup; if $a^{-1} \notin H$ then $e \notin aH$.

Example 15. Let $G = \mathbb{Z}$, and let $H = 2\mathbb{Z}$. Consider the cosets $0 + H$ and $1 + H$ (these are just the even integers and the odd integers). In particular, $0 \notin 1 + H$ and so $1 + H \not\leq G$.

The Right and Left cosets here are equal, which is always true of G is abelian.

Notice that in the above example, the cosets are disjoint and partition the group into equivalence classes. In general this is a true statement.

Lemma 8. *The costs of H partition G into equivalence classes, with the relation $a \sim b$ if and only if $a = bh$ for some $h \in H$. In particular, $a \sim b$ if and only if $aH = bH$, and so the cosets defined by those elements are identical.*

Corollary 8. *The order of the cosets divides the order of G. In particular, $|G| = |H| \cdot [G : H]$ where $[G : H]$ is the* index *of H in G and is the number of (left OR right) cosets of H in G.*

In the example with $\mathbb{Z}$ and $2\mathbb{Z}$, lets try to make these cosets behave like groups. Consider that $(0 + H) + (1 + H) = (1 + H)$ (which just says that and even plus an odd equals an odd). We also have a homomorphism $\pi : \mathbb{Z} \to 2\mathbb{Z} : n \mapsto \bar{n} = n + H$. This maps integers to cosets. Note that π respects the operations in each group! This is kind of what defines "adding even and odd integers" in the languages of sets.

Notation. Let $0+H = \pi^{-1}(\bar{0}) = \{n \in \mathbb{Z} \mid \pi(n) = \bar{0}\}$; this is the preimage of π or the fiber of π above 0. Yes this is overloaded notaiton, and no π does not have an inverse (it's pretty clearly *not* injective.)

Note that it doesn't really matter which elements we send into π as long as they are both of the same coset, so $\pi(a) = \pi(b)$ if and only if $a \sim b$. Additionally, note that since π is a homomorphism we can say that $\pi(\bar{1} + \bar{20}) = \pi(\bar{1}) + \pi(\bar{20})$.

Now, in making these cosets into groups we want them to inherit their operation from the parent group (so we can't just make up multiplications to suit our needs).

Definition 27. Let $A, B \subset G$. Then $AB = \{ab \mid a \in A, b \in B\} \subset G$. In particular, note that $HH = H$ and $(1H \cdot 1H = 1H)$.

Example 16 (Things Go Wrong)**.** Let $G = S_3$ and let $H = \langle (23) \rangle = \{1, (23)\}$. The cosets of H are $1H = (23)H$, $(12)H = (123)H = \{(12), (123)\}$, and $(13)H = (132)H = \{(13), (132)\}$. Now consider $1H \cdot (12)H = \{(12), (123), (132), (13)\}$. In particular, note that this isn't a coset (it has too many elements!). We would have wanted that $1H \cdot (12)H = (12)H$ but this doesn't happen. Then there is not quotient group G/H.

What just happened? Why can't we create a group out of the cosets of S_3? We wanted that $aH \cdot bH = abH$ but this didn't happen; essentially, we want b and H to commute, so we want that the left and right cosets to be equal to one another.

Example 17. Let $G = S_3$ and let $H = \langle (123) \rangle = A_3$. This is the alternating group on three letters. As always, $1H = H1 = H$. Note that $(12)H$ contains *the only other elements of* G which aren't in $1H$, and so $(12)H = H(12) = G \setminus 1H = G \setminus H1$. This happens when $[G : H] = 2$ even though G is not abelian. Then $S_3 \setminus A_3 = G \setminus H$ and $\bar{a}\bar{b} = \bar{ab}$ so multiplication is well defined.

12 September 26, 2018

> Let N be a group...I'll call it N suggestively
>
> Miki

Recall from last class that we found and example of a non-abelian group and a subgroup for which the left and right cosets of the group were the same; in this case, it was $G = S_3$ and $H = A_3$.

Definition 28 (Quotient Group)**.** Let $H \leq G$. The *quotient group* G/H is a group whose elements are the left cosets of H. The set for this group is known as the quotient set, and the operation for the group is inherited from G such that $gH \star kH = gkH$. Note that $(gH, \star)$ does not always form a group, so it isn't guaranteed that G/H exists for any G, H. *Quotient Group*

12.1 Mapping from G to G/H

Given a group G and a quotient group G/H we can find a very natural mapping $\pi : G \to G/H$ where $g \mapsto gH$. This map sends elements to their coset, and $\pi(a) = \pi(b)$ if and only if $aH = bH$; thenthe fibers of π are the left cosets of H, and $\ker \pi = H$. This is why we call it the quotient group — it's like we're dividing out by H. Note that this homomorphism is always going to be surjective since there's no member of G which isn't in some coset of H as they partition G.

Definition 29 (Normal Subgroup)**.** Let $N \leq G$. Then N is normal if and only if the left and right cosets are the same, so $gN = Ng$. If N is normal then G/N forms a quotient group. Note that this does not mean that $gn = ng$ so g and n do not commute necessarily, but the cosets are preserved. This is equivalent to saying that $\mathrm{N}_N(G) = G$ but $\mathrm{C}_N(G)$ is not necessarily G. *Normal Subgroup*

Notation ($\trianglelefteq$)**.** We write $N \trianglelefteq G$ to mean that N is a normal subgroup of G. $\trianglelefteq$

Theorem 3. *The quotient group G/N exists if and only if $N \trianglelefteq G$.*

Proof that $N \trianglelefteq G$ is sufficient. Observe that $(aN)(bN) = abN$ if N is normal. Then group multiplication is well defined. Observe also that $(aN)^{-1} = a^{-1}N$, so the group is closed under inversion, and by definition our multiplication is associative. Then G/N forms a group if N is normal in G. ■

Proof that $N \trianglelefteq G$ is necessary. Suppose $H \leq G$ is not normal. Then there is some $g \in G$ for which $gH \neq Hg$. Then we know that $1HgH \neq gH$, and our group operation $\star$ cannot hold. ■

Not that $|G/N| = |G|/|N| = [G : N]$ if G is finite, which we already knew but it's worth remembering it.

12.2 Testing Normality

Proposition 13. *The following are equivalent:*

- $N \trianglelefteq G$;
- $gNg^{-1} \subset N$ *for all* $g \in G$ *(note this implies they are equal since conjugation is injective);*
- N *is the kernel of some homomorphism* $\pi : G \to H$ *for some* $H \leq G$.

Proof that 1 $\implies$ 2. Let $g \in G$ and $n \in N$. We know that $gN = Ng$, so there exists $n' \in N$ such that $ng = n'g$. Multiply on the right by g^{-1} and we see that $gng^{-1} = n'$, and so $gng^{-1} \in N$ for all g, n. ■

Proof that 2 $\implies$ 1. Literally just reverse the above procedure. ■

Proof that 1 $\implies$ 3. Let $H = G/N$. Then we know that $\ker \pi = N$ where $\pi : G \to G/N : g \mapsto gN$. Then, rather trivially, we know N is the kernel for some homomorhpism if $N \trianglelefteq G$. ■

Proof that 3 $\implies$ 2. We know that $N = \ker \pi$ for some $\pi : G \to H$. Then take any $g \in G$ and $n \in N$, and consider that $\pi(gng^{-1}) = \pi(g)\pi(n)\pi(g^{-1}) = \pi(g)\pi(g^{-1})$ since $n \in \ker \pi$, and then we conclude that $\pi(g)\pi(g^{-1}) = 1$ and so we know that $gng^{-1} \in \ker \pi$ so $gng^{-1} \in N$ for all $n \in N$ and for all $g \in G$. ■

13 Friday, 28 September 2018

"I'll leave the cosets for later, where later means 15 seconds from now."

Miki

"Continuous math is not allowed...don't tell anyone I said that."

Miki

Recall Lagrange's Theorem, where if G is a finite group and $H \leq G$ then $|H|$ divides $|G|$; in fact, $|G|/|H| = [G : H]$.

Corollary 9. *Let G be a finite group and let $x \in G$. Then $|x|$ divides $|G|$ since x generates a cyclic subgroup of order $|x|$, so $|x| = |\langle x \rangle|$ which must divide $|G|$ by Lagrange.*

Corollary 10. *If $|G| = p$ is prime, then $|G| \cong Z_p$.*

Proof. Since $|G| \neq 1$ there exists $x \in G$ which is not the identity. Then consider $\langle x \rangle$. The order of this cyclic group must divide p, and since p is prime it must equal p, and so $G = \langle x \rangle$ which means it is isomorphic to Z_p. ∎

If we have some $n \in \mathbb{Z}_{>0}$ where n divides $|G|$ for some G, it isn't guaranteed that there exists some $H \leq G$ where $|H| = n$, and/or there isn't always an $x \in G$ where $|x| = n$. For example, consider $G = S_3$ and $n = 6$. However, if prime p divides $|G|$ then there exists an $x \in G$ where $|x| = p$ — Miki says she will prove this later.

13.1 Product Subgroups

Let G be a group and let $H, K \leq K$. Let's consider the product of HK, which we recall is defined as

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

This may or may not be a subgroup. In general it is not.

Example 18. Let $G = S_3$, and let $H = \langle (12) \rangle$ and let $K = \langle (13) \rangle$. Then $HK = \{1, (12), (13), (132)\}$ which is not a subgroup of S_3 since 4 does not divide 6.

What can we say about HK anyways?

Proposition 14. *The order of HK is at most $|H||K|$. In fact,*

$$|HK| = \frac{|K||K|}{|H \cap K|}.$$

Proof. We know that HK is the union of left cosets of K where

$$HK = \bigcup_{h \in H} hK.$$

Consider $a, b \in H$. We know that $aK = bK$ if and only if $a^{-1}b \in K$ which is true if and only if $a^{-1}b \in K \cap H$. This means that $aK \cap H = bK \cap H$. Then we've reduce the problem to counting the number of distinct cosets hK which is just the index, so it is $|H|/|K \cap H|$. Multiplying through by the size of K, we find that

$$|HK| = \frac{|H||K|}{|K \cap H|}. \qquad \blacksquare$$

Now we can answer when HK is a subgroup; it happens if and only if $HK = KH$. Intuitively, this happens only when $hkh'k' \in HK$ which can happen if and only if we can commute the h and k elements. It is sufficient to say that H is in the normalizer of K or vice-versa. Another sufficient condition is to say that $K \trianglelefteq G$, or the other way around. Note that neither of these conditions is necessary.

$$H \leq N_G H \implies hK = Kh \implies hk = k'h,$$

but we only need that $hk = k'h'$. That is, we only need that $hK = Kh'$ which is a weaker condition than being in the normalizer.

13.2 Isomorphism Theorems

Theorem 4 (First Isomorphism Theorem)**.** *Given a surjective homomorphism $\phi : G \to H$, we know that $H \cong G/\ker\phi$.*

Proof. This was the definition of $G/\ker\phi$, since $\ker\phi \trianglelefteq G$. See the previous lecture notes for a more in-depth explanation. $\blacksquare$

Example 19. Consider $\mathrm{GL}_2(\mathbb{F}_3)$ and let $\phi = \det : G \to \mathbb{F}_3^\times$. Then $\ker\phi = \mathrm{SL}_2(\mathbb{F}_3)$, and $\mathrm{GL}_2(\mathbb{F}_3)/\mathrm{SL}_2(\mathbb{F}_3) \cong \mathbb{F}_3^\times$. Since $\mathrm{GL}_2(\mathbb{F}_3)$ has 48 and $\mathbb{F}_3^\times$ has 2 elements then we know that $\mathrm{SL}_2(\mathbb{F}_3)$ is of order 2.

Theorem 5 (Second Isomorphism Theorem)**.** *Let G be a group with $H, K \leq G$ and let $H \leq N_G K$. Then $HK/L \cong H/H \cap K$.*

Proof. We know several things.

- $HK \leq H$ since $H \leq N_G K$;
- $K \leq HK$, since we know that $H \leq N_G K$ and $K \leq N_G K$ so $K \leq HK$;
- Now we can take the quotient HK/K, which is the left cosets of K in HK. We have shown that $hK = h'K$ if and only if $hH \cap K = h'H \cap K$. Then define the map $\pi : H \to HK/K$ defined by $h \mapsto HK$. This is a homomorphism since $hKh'K = hh'K$ since that's how we defined multiplication. Then $\ker \pi$ is all elements h of H which map to the identity coset which happens if and only if $h \in K$, so $\ker \pi = \{h \in H \cap K\}$. Then by the First Isomorphism Theorem, $H/H \cap K \cong HK/K$. ■

Example 20. Let $G = S_3$, let $K = A_3$, and let $H = \langle (12) \rangle$. We know that $HK = S_3$ and $H \cap K = \{e\}$. Then we know that $HK/K = S_3/A_3 \cong \langle (12) \rangle / 1 \cong Z_2$.

14 Monday, 1 October 2018

"I've got H's on the brain."

"That's the third isomorphism theorem, I knew you wouldn't like it. It should take you anywhere from a day to seven years to become comfortable with it."

Miki

"It's math....it keeps doing things like that."

Miki

14.1 Isomorphism Theorems Continued

Recall from last lecture we developed the first two isomorphism theorems. Today, we'll cover the last two (or one, depending on your perspective).

Theorem 6 (Third Isomorphism Theorem)**.** *Let G be a group and let H, N be normal subgroups of G with $N \subseteq H$. THen $G/N \big/ H/N \cong G/H$.*

Proof. Consider a map $\phi : G/N \to G/H : gN \mapsto gH$. We need this map to be well-defined. Suppose that $g_1 N = g_2 N$. Then $g_1^{-1} g_2 \in N$, but $N \subseteq H$, and so $g_1 H = g_2 H$ and ϕ is well defined. We also need to know that this is a homomorphism. Consider $\phi(g_1 N)\phi(g_2 H) = g_1 g_2 H = \phi(g_1 g_2 N)$, and in fact we also know that ϕ is surjective. Consider $gH \in G/H$ and suppose that $gH = \phi(gN)$. Since $N \subset H$ this is well defined. Consider then that $\ker \phi : \phi(gN) = gH$. This happens if and only if $g \in H$ so $gN \subset H$ is a coset of N in H and $gN \in H/N$, so $\ker \phi = H/N$. Then by the First Isomorphism Theorem, we know that $G/N \big/ \ker \phi \cong G/H$. ■

Example 21. Let $G = \mathbb{Z}$ with $N = \langle 10 \rangle$ and $H = \langle 2 \rangle$. Then $G/N = \{0 + N, \ldots, 9 + N\}$ and $G/H = \{0 + H, 1 + H\}$. Then $H/N = \{0 + N, 2 + N, \ldots, 8 + N\}$. The idea here is that if you take $\mathbb{Z} \pmod{10}$, and then modulo the result by 2, then it didn't really matter than we modded out by 10 to begin with.

Theorem 7. *The Totally not fourth isomorphism theorem Let $N \trianglelefteq G$. THere is a correspondence (bijection) between subgroups of G which contain N and subgroups of G/N. That* *is,*

$$\pi : H \mapsto \pi(H), \quad \bar{H} \mapsto \pi^{-1}(\bar{H}).$$

Note that for any $H \leq G$ we know that $\pi(H) \leq G/N$. We require normality to ensure that π is injective.

Example 22. Consider $G = S_3$ with $N = A_3$. Then $\pi(S_3) = G/N$ and $\pi(A_3) = N$. What is $\pi(\langle(12)\rangle)$? It's all of G/N.

14.2 Why do people care about normal groups?

Definition 30 (Simple)**.** A group G is simple if $|G| > 1$ and G contains no proper normal subgroups.

Simple

Definition 31 (Composition Series)**.** Consdier something like $1 = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = G$ where N_{i+1}/N_i is simple for all $0 \leq i \leq r-1$. As an example, $1 \trianglelefteq A_3 \trianglelefteq S_3$. Then $S_3/A_3 \cong Z_2$ and $A_3/1 \cong Z_3$. These series allow us to construct large groups whose multiplication is unknown, since normal subgroups multiply to form subgroups of something larger. For more information on this, see the *Holder Program*, which was started in 1890 to classify simple groups and it took 103 years to actually classify them all. These series are *almost* unique, where the quotient groups are unique up to a permutaiton, so the set of quotient groups are unique.

Composition Series

Definition 32 (Solvable groups)**.** A group G is solvalble is $1 = N_0 \trianglelefteq \cdots N_r = G$ and N_{i+1}/N is abelian. This kind of object shows up a lot in Galois Theory. As it turns out, A_1 through A_4 are solvalble but A_5 and higher is not solvable, which is why we can't solve arbitrary quintics.

Solvable groups

15 Wednesday, 3 October 2018

"I will not try to decide whether that was happy or sad."

Miki

"Try it if you don't believe me."

Miki

"If you don't have surjectivity, you have nothing."

Miki

Recall from last time that we defined a simple group to be a non-trivial group which has no proper normal subgroups. Observe that if G is abelian and simple then it has no proper subgroups at all, since all subgroups would be normal.

15.1 Permutations

We'll take a shortcut throught linear algebra to talk about the signs of permutaitons; the book constructs the notion from scratch. Recall that we can switch the rows of a matrix using the permutation matrix P_{mn}, by which left multiplication swaps the rows m and n. Now, we talk about this as the cycle (mn), so for example

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \sigma = (12) \in S_3.$$

Essentially, we start with I_n and permute the rows according to σ to yield the corresponding permutation matrix P_σ.

Definition 33 (Sign of Permutation)**.** Let $\varepsilon : S_n \to \{\pm 1\} \cong Z_2$ by $\varepsilon(\sigma) = \det P_\sigma$. Then ε is the *sign* of σ.

Sign of Permutation

Note that ε is actually a group homomorphism since the determinant is multiplicative; that is $\varepsilon(\tau\sigma) = \det(P_{\tau\sigma}) = \det(P_\tau)\det(P_\sigma) = \varepsilon(\tau)\varepsilon(\sigma)$. Then we can quite naturally ask, what is the kernel of ε. We define the terms *even* and *odd* to mean permutations whose sign is $+1$ and -1 respectively. Then $\ker \varepsilon = A_n \leq S_n$ is the set of all even permutations. This gives us a rigorous definition of the alternating group.

Let's note that a two-cycle in S_n is a transposition, and we have already proven on homework that every element in S_n can be written as the product of two-cycles. We can quite easily conclude that every transposition has a sign of -1.

Proposition 15. *Let $\sigma \in S_n$ be a k-cycle. Then $\varepsilon(\sigma) = (-1)^{k-1}$.*

> **Problem 10.** How large is A_n?

Since ε is surjective, we know by the First Isomorphism Theorem that $S_n/A_n \cong Z_2$ (since $\operatorname{Im} \varepsilon = Z_2$), so $|A_n| = n!/2$.

Theorem 8. *The alternating group on n letters is simple if $n \geq 5$. This was proven by Galois in the 1830's and is the reason for quintic insolubility.*

15.2 Actions

Recall that an action is a map $\phi : G \times A \to A$ by $\phi(g, a) = g \cdot a$. This yields a homomorphism $G \to S_A$ by $g \mapsto \sigma_g$, where σ_g is bijective for a fixed $g \in G$. Recall also for $a \in A$ the stabalizer G_a is the set of g for which $ga = a$, and the kernel of the action is the set of $g \in G$ for which $ga = a$ for all $a \in A$. We said that an action is *faithful* if the kernel of the action is the identity; that is, different elements of g give different permutaitons on A. Furthermore, the orbit of a is the set of ga for all $g \in G$. We proved on homework that the orbits partition A.

Definition 34 (Transitive)**.** An action is transitive if all elements of A are in a single orbit; i.e., $a \sim b$ for all $a, b \in A$.

Transitive

16 Friday, 5 October 2018

"I mean, ∞! is a big number!"

Miki

"Oh well, we'll cry later."

Miki

16.1 Orbits and Stabalizers

Miki introduced a new proposition today which I think is just the Orbit-Stabalizer theorem.

Proposition 16. *Given an action $G \times A \to A$ and an $a \in A$ we know that $|O_a| = [G : G_a]$ which tells us that $|G| = |O_a||G_a|$.*

Proof. Define a map $\pi : \{\text{cosets of } G_a \text{ in } G\} \to O_a$. Note that this is just a map, not a homomorphism. Define π to be $gG_a \mapsto g \cdot a$. We'll show it's well-defined and injective at the same time. Suppose we have that $gG_a = hG_a$ which happens if and only if $g^{-1}h \in G_a$ or $g^{-1}h \cdot a = a$, so $ha = ga$. Since anything in the orbit is $g \cdot a$ for some g, we also know that π is surjective; then π is a bijection and so $|O_a| = [G : G_a]$. ∎

16.2 Cycles in S_n

Let $\sigma \in S_n$ be or order k. We want to write it as the product of disjoint cycles. Consider the set $A = \{1, \dots, n\}$ and let $G = \langle \sigma \rangle$. We construct the action $\langle \sigma \rangle \times A \to A$. Consider the orbit O_a of $a \in A$ under $\langle \sigma \rangle$. We know by the orbit-stabalizer theorem that there is a bijection between the cosets G_a and the orbit of a. Since $\langle \sigma \rangle$ is cyclic we know that $G_a = \langle \sigma^r \rangle$ is also cyclic. By the definition of our map π from the Orbit-Stabalizer theorem, we know that $\pi(\sigma^i G_a) = \sigma^i a$. Then $O_a = \{a, \sigma a, \dots, \sigma^{r-1} a\}$ then on O_a we can say that σ acts as an r-cycle. Since the orbits collectively partition A we know that they are disjoint, and so we know that we can write σ as the product of disjoint cycles, which is unique up to the order of the cycles and up to cyclic permutation within each cycle. Note that since $\langle \sigma \rangle$ is cyclic (and therefore abelian) the cosets G_a are simply G/G_a.

16.3 Actions of G on itself

Previously we defined two cannonical actions of G on itself, via *left multiplication* where $G \times G \to G : (g, a) \mapsto g \cdot a$, and *conjugation*, where $G \times G \to G : (g, a) \mapsto gag^{-1}$. In the first case, we know that the action of left multiplication is faithful, and gave us an injective homomorphism from G to S_G (i.e., finite G always is isomorphism to a subgroup of S_n).

Example 23. Let $G = \mathbb{Z}$ and our action is $(i, j) \mapsto i + j$, so $\sigma_i(j) = i + j$. Let's consider the orbits of 0 and 1 under σ_2. Observe that $\cdots - 4 \to -2 \to 0 \to 2 \to 4 \to \cdots = O_0$ while O_1 is just the odd integers. Now consider $H = 4\mathbb{Z} \subset G$, and let's consider how σ_2 acts of G/H, or on the cosets of H in G. Well, we know that $H = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$. Note that σ_2 becomes $(\bar{0}\bar{2})(\bar{1}\bar{3})$.

Theorem 9. *Consider $G \times G \to G$ via left multiplication, and consider how this action acts on $H \leq G$. We know it acts like $g \cdot (aH) = gaH$. We can show this is well defined by noting that if $aH = bH$ then we know that $ga = gbh$ and so our action is well defined. Let A be set set of cosets of H in G, and we get a map $\pi : G \to S_A$. We know the following things.*

1. *G acts transitively on A;*
2. *$G_{1H} = H$;*
3. *The kernel of π is the intersection of all gHg^{-1} for all $g \in G$. This is actually the largest normal subgroup of G contained in H.*

Proof. Left as an exercize to the reader (me). ∎

17 Monday, 8 October 2018

"Remember that $1 + 1 = 2$."

Miki

"This proof should make you feel better after your exam."

Miki

Recall from last lecture we described how G can act on itself by either left multiplication or conjufgation. Today we'll cover in detail conjugation. Remember that conjugation is an action defined as

$$G \times G \to G : ga \mapsto gag^{-1}.$$

We define the orbit O_a of a under conjugation to be the *conjugacy class* of a. This is an equivalence relation (since we already know this holds for orbits). Then consider $S_1, S_2 \subset G$. There are conjugate if there exists a $g \in G$ such that $gS_1g^{-1} = S_2$. Note that these subsets better have the same cardinality.

For any $x \in G$, we know that $|O_x| = [G : G_x]$ where $G_x = G_G(x)$ is the centralizer of x in G, as it turns out.

Example 24 (Conjugacy Classes)**.**

1. Consider $G = C_6$. Since G is abelian, we know that $gxg^{-1} = x$ for all $x, g \in G$ so the orbit of x is simply $\{x\}$.
2. Consider $D_8 = \langle r, s \mid \cdots \rangle$. What is the center of G? It's $Z(G) = \{1, r^2\}$. Let's consider that orbit of 1 is 1 and the orbit of r^2 is just r^2. This tells us that if $x \in Z(G)$ then $O_x = \{x\}$ under conjugation. Then let's consider some $x \notin Z(G)$. The size of the orbit must be strictly greater than 1 (since otherwise it would commute with everything). Consider that the sabalizer must have at least three elements $(1, r^2, x)$, and so must have at least order four. It can't have order eight since the identity will not be in the centralizer, and so we know that $|O_x| = 2$. This tells us that the orbit of *any non-center* element has order two, which tells us that we can find the orbits of any elements *super quickly* since we just need to conjugate it *once* and get a new element and we are done!

Theorem 10 (Class Equation)**.** *Let G be a group. The center of the group contains all conjugacy classes of size 1. List the classes of size greater than or equal to 2 as $)_{x_1}, \ldots, O_{x_n}$.*

Then

$$|G| = |Z(G)| + \sum_{i=1}^{n} |O_{x_i}|$$

since the orbits partition G.

Theorem 11. *Let $|G| = p^n$ where p is prime. We know a few things about such a group.*

1. $|Z(G)| > 1$.

Proof of 1. We know from the class equation that

$$|G| = |Z(G)| + \sum_{i=1}^{n} |O_{x_i}|.$$

For all i we know that $O_{x_1} \geqslant 2$ and we know that it divides the order of the group. Then $|O_{x_1}| = p^k$ for some $1 \leqslant k \leqslant n$. Then p divides the order of the sum of the orders of the orbits, and so p must divide the order of the center. In fact, this tells us that $|Z(G)|$ is at least p. ■

Proposition 17. *For prime p, if $|G| = p^2$ then*

(a) G is abelian, and

(b) $G \cong C_{p^2}$ or $C_p \times C_p$.

Proof of (a). Let $x \in G$, and assume by way of contradiction that $x \notin Z(G)$. Consider $H = \langle Z(G), x \rangle$. Since G is a p group, we know that the center cannot be one, and so $|G| = p$ (since it must divide p^2 and if $|G| = p^2$ then $x \in Z(G)$). And we know that $|H| \geqslant |Z(G)|$ so we know that $p \leqslant |H| \leqslant p^2$ and the order must divide p, and so we know that $H = G$. But since x commutes with everything in H we know that $x \in Z(G)$. ■

Proof of (b). Left as an exercise to us. ■

17.1 Conjugation in S_n

If you take an arbitrary element σ of S_n, what can we reasonably expect the conjugacy class of σ to look like? For example, consider $\sigma = (123)$. Well, $(14)(123)(14) = (423)$. We also know that $(256)(123)(652) = (153)$. Notice that we've found two 3-cycles! We can hypothesis that $|\tau\sigma\tau| = |\sigma|$, and in fact we just replace the elements of the 3-cycle with "where the numbers in the conjugating cycles get sent." That is, if $\sigma = (a_1, \ldots, a_k)$ then $\tau\sigma\tau^{-1} = (\tau(a_1)), \ldots, \tau(a_k))$. We can infer a slightly stronger link here; in fact, σ is conjugate to σ' if and only if they have the same cycle structure.

18 Friday, 12 October 2018

"We have hope. But hope doesn't mean much."

Miki

Let's return to the proposition we described last time, where we said that the equivalency classes in S_n under conjugation are exactly the sets of permutations with the exact same cycle decomposition structure. That is, all elements of the form $(\cdot\cdot\cdot\cdot\cdot) \in S_n$ are conjugates with one another, and the same holds for $(\cdot\cdot\cdot)(\cdot\cdot)$ and all other cycle structures.

Proposition 18.

(d) *If $\sigma \in S_n$ is a $k-cycle$ where $\sigma = (a_1, \cdots, a_k)$, and $\tau \in S_n$, then $\tau\sigma\tau^{-1} = (\tau(a_1), \ldots, \tau(a_k))$.*

(e) *If σ is a product of disjoint cycles $\sigma_i \cdots \sigma_r$ then $\tau\sigma\tau^{-1}$ is the product of disjoint cycles $\tau\sigma_i\tau^{-1}$.*

(f) *Cycles σ, σ' are conjugate if and only if they have the same cycle structure.*

Proof of (d). Let $A = \{1, \ldots, n\}$ so that $\tau A = A$. Then $A = \{\tau(1), \ldots, \tau(n)\}$. ■ *FINISH THIS*

Proof of (e). Let $\sigma = \sigma_1 \cdots \sigma_r$. Then $\tau\sigma\tau^{-1}$ can be written as $\tau\sigma_1(\tau^1\tau)\cdots(\tau^1\tau)\sigma_r\tau^{-1}$, and by associativity the proposition holds. Since the cycles were disjoint to begin with, permuting each σ_i under τ ensure that the products are still disjoint. ■

Proof of (f). The forward direction follows immediately from the previous two proofs. Next, assume σ, σ' have the same cycle structure. Then

$$\sigma = (a_1^1 \cdots a_{k_1}^1)(a_1^2 \cdots a_{k_2}^2)\cdots(a_1^r \cdots a_{k_r}^r),$$

and

$$\sigma' = (b_1^1 \cdots b_{k_1}^1)(b_1^2 \cdots b_{k_2}^2)\cdots(b_1^r \cdots b_{k_r}^r).$$

Then $A = \{1, \ldots, n\} = \{a_i^j\} = \{b_i^j\}$. Then take $\tau(a_i^j) = b_i^j$, since this is just a permutation on the elements in A, so by (d) and (e) this holds. ■

18.1 Proving the simplicity of A_5

This is a big deal.

Proof. We want to show that A_5 (or any A_n, for that matter) has no proper normal subgroups. Recall the orbit stabalizer theorem, where $|G| = |G_x| \cdot |O_x|$ for any $x \in G$. Recall also that if $N \trianglelefteq G$ then N is the union of conjugacy classes. Let's start by finding the class equation for A_5. Since A_5 must have even sign, we know that the only cycles in A_5 are of the form e, $(\cdot\cdot)$, $(\cdot\cdot\cdot)$, and $(\cdot\cdot\cdot\cdot\cdot)$. Let $O_x^{S_5}$ be the orbit of an element x

in S_5 while $O_x^{A_5}$ is the orbit in A_5. Note that $\left|O_x^{A_5}\right| \leq \left|O_x^{S_5}\right|$. Similarly, anything in A_5 which fixes x must also fix x in S_5 so $|(S_5)_x| \geq |(A_5)_x|$. We also know by Orbit-Stabalizer that $|(A_5)_x| \cdot \left|O_x^{A_5}\right| = |A_5| = 60$ while $|(S_5)_x| \cdot \left|O_x^{S_5}\right| = |S_5| = 120$. Combining these inequalities with the Orbit-Stabalizer theorem (and recognizing that everything here is an integer), we are left with the option that either the orbits are the same size and the centralizer in A_5 is half of the centralizer in S_5, or that the centralizers are the same and the orbits in A_5 are half that of the orbits in S_5.

Let's figure out which of these cases is true. Consider $x = (\cdot\cdot\cdot) = (123) \in S_5$ without a loss of generality. What is the size of the orbit of x in S_5? Well, it's all three-cycles, so there are $2 \cdot \binom{5}{3} = 20$ elements in the orbit of x in S_5. By Orbit-Stabalizer, the size of the sabalizer is then $120/20 = 6$. Note that $(45) \in (S_5)_x$ since it doesn't move x, but because (45) is not in A_5 since it has the wrong sign, we know that it is the stablizer which has shrunk and the orbits have the same size.

Let's do the same thing with $x = (\cdot\cdot)(\cdot\cdot) = (12)(34)$ without a loss of generality. Then $\left|O_x^{S_5}\right| = \binom{5}{1} \cdot 3 = 15$ elements in the orbit of x in S_5. Since this is odd, we know that the orbit can't shrink so it *again* must be the case that the stabalizer has shrunk.

Now let $x = (\cdot\cdot\cdot\cdot\cdot)$. The orbit of x is then of order $5!/5 = 4!$ while the stabalizer is of order $5!/4! = 5$. In this case, it is now the *orbit* which has shrunk.

Then $|A_5| = 1 + 20 + 15 + 2 \cdot 12$ where 20 comes from the 3-cycles, 15 comes from the double 2-cycles, and the 24 comes from the two 5-cycles. Now suppose that $N \trianglelefteq A_5$. We know it is the union of conjugacy classes and it contains the identity, so $|N| = 1 + \{\text{some of } 12, 12, 15, 20\}$, and it must divide $|A_5| = 60$. Note that this can happen *only* if $|N| = 1$ or $|N| = 60$, so A_5 contains no proper normal subgroups and is simple. ■

19 Monday, 15 October 2018

"Perfectly balanced, as all things should be." (when referring to left and right actions)

Miki

"Our theorem is gone! Oh no!"

Miki

Problem 11. Does right multiplication define an action of S_4 on itself?

Solution. No, since we can find two elements for which $g_1(g_2(x)) \neq x \cdot (g_1 g_2)$. Consider (12) and (23) acting on the identity. In general, right multiplication is an action if and only if the group is commutative since we are "switching the order of the multiplication." ■

19.1 Right Actions

In order to fix this "unfairness," we often define something called a right action $A \times G \to A$, where the associativity of the action is specified as $a \cdot (gh) = (a \cdot g) \cdot h$. This turns right multiplication into a "right action." There really isn't any distinction between the two, which is why we just speak of "the action."

How do we turn left actions into right actions? Suppose we have a left action $g \cdot a$. Define $a \cdot g = g^{-1} \cdot a$; that is, the right action of g on a is just the left action by the inverse of g. This works since $(gh)^{-1} = h^{-1}g^{-1}$ so the order follows the rules for right multiplication/action.

Problem 12. Consider $\mathbb{Z}$ acting on itself through left addition, where $m \cdot n \mapsto m + n$, and consider that when we turn this into a right action. Then $n \cdot m \mapsto -m + n = n - n$, and we've just invented subtraction.

Example 25. Consider $A_3 \trianglelefteq S_3$, and consider conjugating $(123) \in A_3$ by something in S_3. We know we'll get either another three cycle or the identity, since we know that $gNg^{-1} = N$. Then if $g \in S_3$ there there exists a $\sigma_g : S_3 \to S_3$ which acts on g by conjugation. The consider $\sigma_g|_N$ restricted to acting on N. Then we have a map from N to itself. If $g \in N$ then we get the trivial map (since this is just Z_3), and otherwise we must not get the trivial map and so $(123) \mapsto (132)$ and *vice versa*. In the latter case, we've created not just a random map but a homomorphism from N to itself. This homomorphism $x \mapsto x^3$ in the group $\langle x \mid x^3 = 1\rangle$, which is both injective and surjective and we know that this is a homomorphism since the generators satisfy the relations under the map since $x^6 = 1$.

19.2 Group Automorphisms

Definition 35 (Automorphism)**.** A group automorphism is an isomorphism from G to itself. *Automorphism*

For every group G there is a group $\mathrm{Aut}(G)$ which is the group of all automorphism of G under composition. Miki told us to prove for ourselves that this is actually a group. Now consider G acting on itself through conjugation where $g \mapsto \sigma_g : x \mapsto gxg^{-1}$. For an normal subgroup of G we know that $\sigma_g|_N : N \to N$, and so we have a homomorphism ψ from G to $\mathrm{Aut}(N)$ where $g \mapsto \sigma_g|_N$. The kernel of ψ is the set of all elements in G which commute with N, and so $\ker \psi = C_G(N)$. Then $G/C_G(N)$ is isomorphic to a subgroup of $\mathrm{Aut}(N)$ by the First Isomorphism Theorem.

There are two things to unpack here. First, how to we know that ψ is actually a homomorphism? That is, why is $\sigma_g|_N \in \mathrm{Aut}(N)$? Well, consider that $\sigma_g(nn') = gnn'g^{-1} = gng^{-1} \cdot gn'g^{-1} = \sigma_g(n)\sigma_g(n')$, and so $\sigma_g|_N$ preserves the group operation. Next, how to we know that the map $g \mapsto \sigma_g$ is a homomorphism? That is, why does $\sigma_{gg'} = \sigma_g\sigma_{g'}$. Well, since conjugation is a well-defined action on G, this forms a homomorphism. Note that the restriction to N isn't important here, but the reason we require normality since we won't we able to compose the conjugations since $gHg^{-1} \neq H$.

Corollary 11. *Take $G = N$. Then we get a homomorphism from G to its own automorphism group, and so $G/C_G(G) = G/Z(G)$ is isomorphism to a subgroup of $\mathrm{Aut}(G)$.*

Corollary 12. *Let $H \leq G$ be any subgroup of G. Then for all $g \in G$, $gHg^{-1} \cong H$, but they are not necessarily equal to one another.*

Corollary 13. *Let $H \leq G$ be any subgroup of G. Then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$, since the centralizer is always normal in the normalizer. This is really just a general case of the preceeding statements.*

Proof. Since $H \trianglelefteq N_G(H)$, we just let $G' = N_G(H)$ and apply the result. ■

20 Monday, 22 October 2018

"You all look so unhappy."

Miki

"p is going to be prime for *at least* two more days."

Miki

20.1 Clasifying Automorphisms

Let's talk automorphisms!

Definition 36 (Inner Automorphism)**.** Let $g \in G$ and let $\sigma_g : G \to G : x \mapsto gxg^{-1}$ be an automorphism (i.e., an automorphism by conjugation). Then σ_g is an *inner automorphism.* The collection of all inner automorphisms forms a group $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$ which is isomorphic to $G/\mathrm{Z}(G)$ by the first isomorphism theorem.

Inner Automorphism

Example 26. Let $G = \mathbb{Z}/n\mathbb{Z}$. We proved on homework that $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, and so any $\sigma \in \mathrm{Aut}(G)$ is uniquely determined by the map which sends 1 to a for some unit a. Since G is commutative, conjugation doesn't really do anything, so $\mathrm{Inn}(G) = \sigma_1$. Put another way, $\mathrm{Z}(G) = G$, so $\mathrm{Inn}(G)$ is as small as it could be.

Example 27. Let $G = D_8$. The center of D_8 is $\mathrm{Z}(D_8) = \langle r^2 \rangle$. We know that $\mathrm{Inn}(G) \cong G/\langle r^2 \rangle \cong K_4$.

Definition 37 (Characteristic)**.** A subgroup $H \leq G$ is *characteristic* if $\sigma(H) = H$ for any $\sigma \in \mathrm{Aut}(G)$. This is like a normal subgroup, except that a normal subgroup need only be preserved under *inner automorphism* while a being characteristic subgroup is a stronger condition.

Characteristic

Example 28. Let $G = D_8$ and let $H = \langle r^2 \rangle$. Since H is the center, this is characteristic (this is true in general). Next let $K = \langle r \rangle \leq G$. Since $\mathrm{Im}(r)$ is either r or r^3 (check the order under isomorphism) then $\sigma(\langle r \rangle) = \langle r \rangle$ for any $\sigma \in \mathrm{Aut}(D_8)$ and so it is characteristic.

Just to make the point explicit, if H is characteristic in G then it must be normal in G, but the reverse is not true. Additionally, if H is the unique subgroup of a particular order in G then it must be characteristic since there's nothing else it could be sent to under an automorphism since it's image must be a subgroup of the same order.

20.2 Sylow p-subgroups

Definition 38. Let p be prime. A p-subgroup is a subgroupd of order p^n for $n \geq 0$.

Definition 39. Let $|G| = p^a m$ where p does not divide m. If there is a subgroup of order p^a (there is) then a subgroup of this order is called a Sylow p-subgroup. The set of all such groups is written as $\mathrm{Syl}_p(G)$. The number of such groups is written as $n_p(G) = \left|\mathrm{Syl}_p(G)\right|$.

Example 29. If p does not divide $|G|$ the the only Sylow p-subgroup is the trivial subgroup. If $|G| = p^a$ then the unique Sylow p-subgroup is $\mathrm{Syl}_p(G) = \{G\}$.

Example 30. Let $G = S_3$ which has order $2 \cdot 3$. Let $p = 2$, $m = 3$, and $a = 1$. Then the largest Syl_p subgroup is C_2, of which there are three such subgroups (things generated by 2-cycles). If we let $p = 3$, then there is one Sylow p-subgroup, generated by a 3-cycle.

20.3 Sylow Theorems

Throughout, let p be prime and let G be a group of order $p^a m$ where $a > 0$ and p does not divide m.

Theorem 12 (Sylow I)**.** *There exists a subgroup of $P \leq G$ where $|P| = p^a$.*

Theorem 13 (Sylow II)**.** *For each p, the Sylow p-subgroups are conjugate to one another.*

Theorem 14 (Sylow III). *The number of Sylow p-subgroups of G, written $n_p(G)$, divides m and is congruent to* $1 \bmod p$.

We'll prove these next time (with a lot of chocolate). Today we'll just talk about the implications of these theorems.

Corollary 14. *There must exist an $x \in G$ whose order is p.*

Proof. Let $y \in P$ be not the identity. Then $|y| = p$, so for some $0 < b \leq a$ we know that $x = y^{p^{b-1}}$. ■

Corollary 15. *The Sylow p-subgroups are all conjugate.*

21 Wednesday, 24 October 2018

Today was a presentation of the proof of the Sylow theorems found in the textbook. As such, notes are omitted in favor of reading the relevant section in the book (and I'm rather tired today and I don't want to type anything up).

22 Friday, 26 October 2018

Didn't go to class today! Something about direct products I think.

23 Monday, 20 October 2018

> "Let's write down all finitely generated abelian groups. What fun."
>
> Miki

We have two goals for today.

1. Is $Z_{20} \times Z_{18} \cong Z_{36} \times Z_{10}$?
2. How do we classify *all* finitely generatred abelian groups?

To start answering these, we'll begin with a proposition.

Proposition 19. $Z_n \times Z_m \cong Z_{mn}$ *if and only if* $\gcd(m, n) = 1$.

Proof. Let $d = \gcd(m, n)$, and let $Z_m = \langle x \rangle$ and let $Z_n = \langle y \rangle$. Consider $G = Z_m \times Z_n = \{(x^a, y^b)\}$. Consider $(c, f) \in G$. Then $|(c, f)| = \operatorname{lcm}(|c|, |f|)$. If $d = 1$ then $|(x, y)| = \operatorname{lcm}(m, n) = mn$, so $Z_{mn} \cong \langle (x, y) \rangle \leq G$. Since the orders are the same, it is isomorphic to the whole thing. On the other hand, if $d > 1$, let $(c, f) \in G$, and consider $(c, f)^{mn/d} = (c^{mn/d}, f^{mn/d}) = (e, e)$, so every element has order strictly less than mn since $d > 1$. Therefore $G \ncong Z_{mn}$. ∎

Example 31. Consider $Z_9 \times Z_6 \ncong Z_{54}$. Note that $Z_9 \times Z_6 \cong Z_9 \times Z_3 \times Z_2 = Z_{18} \times Z_3$.

Example 32. Use the proposition we just proved to "factor" the groups into the same decomposition. Ta-Da!

fdas

23.1 Classifying Finitely-Generated Abelian Groups

Definition 40 (Free Abelian Group)**.** Let $\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}$ (r times) be the free abelian group of rank r.

Free Abelian Group

Theorem 15 (Classification Theorem for Finitely Genreated Abelian Groups)**.** *Let G be a finitely generated abelian group. Then there is a unique decomposition of G satisfying*

1. $G \cong \mathbb{Z}^r \times Z_{n_1} \times \cdots Z_{n_s}$ *for* $r, n_i \in \mathbb{Z}$,

2. $n_i > 2$ *for all* i, *and*

3. n_{i+1} *must divide* n_i *for all* $1 \leq i \leq s-1$.

23.2 Classifying Finitely-Generated Abelian Groups 2, Electric Boogaloo

Example 33. Consider $Z_{60} \cong Z_{2^2} \times Z_3 \times Z_5$. Notice now that all the components are p-subgroups.

Theorem 16. *Let* $|G| = n = \prod p_i^{a_i}$, *where* $a_i \geq 1$. *Then we can write* G *uniquely (up to order of primes) as* $G \cong A_1 \times \cdots \times A_k$ *where* $|A_i| = p_i^{a_i}$, *and for all* $A = A_i$ *where* $|A| = p^a$, *we know that* $A \cong Z_{p^{b_1}} \times \cdots \times Z_{p^{b_\ell}}$ *where* $b_1 \geq b_2 \geq \cdots \geq b_\ell$, *where the sum of all* b_i *is* a.

24 Wednesday, 31 October 2018

"Oh. You are a gamer."

Miki

24.1 FGAGs for Dayyyyysssss

Miki started us off with some exercises to apply what we learned last lecture about classifying finite abelian groups.

Exercise 1. Conver $G = Z_{36} \times Z_{12}$ into elementary divisor notation.

Solution. $G \cong (Z_{2^2} \times Z_{3^2}) \times (Z_{2^2} \times Z_3) \cong (Z_{2^2} \times Z_{2^2}) \times (Z_{3^2} \times Z_3)$. ■

Exercise 2. Convert $(Z_{16} \times Z_4 \times Z_2) \times (Z_9 \times Z_3)$ into invariant factor notation.

Solution. Group up the i^{th} terms in each parenthetical term, so $G \cong (Z^{16} \times Z_9) \times (Z_4 \times Z_3) \times Z_2 \cong Z_{144} \times Z_{12} \times Z_2$. ■

Exercise 3. Classify all abelian groups of order 24.

Solution. Let's use the invariant factor notaion. If p divides the order of $|G|$ then p divides n_1. The factorization of 24 is $2^3 \times 3$. Then n_1 could be 24, and $G_1 \cong Z_{24}$. It could be that $n_1 = 4 \cdot 3$, so $n_2 = 2$ and $G_2 \cong Z_{12} \times Z_2$. It could be that $n_1 = 2 \cdot 3$, so $n_2 = 2$ and $n_3 = 2$, (can't be $n_2 = 4$ since 4 doesn't divide 6), so $G_3 \cong Z_6 \times Z_2 \times Z_2$. ■

Solution. Let's use the elementary divisor notation. Let $|H| = 24$. Then $H \cong A_1 \times A_2$ where $|A_1| = 2^3$ and $|A_3| = 3$. Then $A_2 \cong Z_3$. For A_1, we must take all non-increasing partitions of 3, so $3 = 3, 2+1, 1+1+1$. The the possibilities for A_1 are Z_{2^3}, $Z_{2^2} \times Z_2$, and $Z_2 \times Z_2 \times Z_2$. Then H is either $Z_3 \times Z^{2^4} \cong Z_2 4$ or $Z_3 \times Z_{2^2} \times Z_2 \cong Z_{12} \times Z_2$ or $Z_3 \times Z_2 \times Z_2 \times Z_2 \cong Z_6 \times Z_2 \times Z_2$. ■

24.2 The Shape of Things to Come

Over the next few lectures, we'll cover how to take the product of groups which aren't abelian, and understanding how we can "factor" non abelian groups in the same way that we now know how to factor abelian groups. Warning: it'll be the hardest single thing we do in this class.

24.3 Commutators

Let G be a group with $x, y \in G$. We defined the *commutator* to be $[x, y] = xyx^{-1}y^{-1}$. The commutator of any two elements of G is one if and only if $xy = yx$. The commutator subgroup $G' = \langle [x, y] \mid x, y \in G \rangle$, which is normal in G and the quotient G/G' is abelian.

Suppose we had a homomorphism ϕ from G to H, where H is abelian. Then it must be that $G' \leq \ker \phi$, since $\phi(x)\phi(y) = \phi(y)\phi(x)$, so $[\phi(x), \phi(y)] = \phi([x, y])$ for all $x, y \in G$.

The quotient of G by G' is the largest abelian quotient of G, which means that the commutator group is the smallest subgroup for which the quotient is abelian.

Example 34. Let $G = S_3$. What is G'? Given the sign map $\pi : S_3 \to Z_2$, we know that $\ker \pi = A_3$, so we know that $G' \leq A_3$ since Z_2 is commutative. Then $G' = A_3$.

Example 35. Let $G = D_{12}$. Is it a direct product of some proper subgroups? Consider $K = \langle r^3 \rangle \leq Z(G)$ and let $H = \langle s, r^2 \rangle$. Notice that $\langle H, K \rangle \leq G$ and $\langle H, K \rangle$ contains s and r, so it is equal to the whole group. It's also true that H and K commute with one another. As it turns out (note quite a proof yet) $G \cong K \times H$.

Theorem 17. *Let G be a group and let H, K be subgroups of G satisfying*

1. $H \trianglelefteq G$ *and* $K \trianglelefteq G$,
2. $H \cap K = \{e\}$, *and*
3. $\langle H, K \rangle = HK = G$.

Then $G \cong H \times K$.

Proof. First, we show that H and K commute with one another. Consdier $[h, k]$. Notice that $(hkh^{-1})k^{-1} \in K$ and $h(kh^{-1}k^{-1}) \in H$, so it's in both H and K, but the intersection of H and K is $\{e\}$ which means that the commutator is the identity, which happens if and only if H and K commute with one another. Next, consider that $|HK| = |H| \cdot |K| / |\{e\}| = |H| \cdot |K|$. Next, create a map $\phi : H \times K \to G$ where $(h, k) \mapsto hk$. We show that this is a homomorphism (and an isomorphism). Notice that $\phi(h, k)\phi(h', k') = hh'kk' = \phi(hh', kk')$ so ϕ is a homormphism. It is also injective. Suppose that $\phi(hk) = 1$, which tells us that $h = k^{-1}$, which means that $h = k = 1$ since $h \in H \cap K$. It is surjective, since the sizes of the groups are the same. Then $G \cong H \times K$ through ϕ. ■