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 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.

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 $2n$?

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 Ω, the symmetric group on Ω is $S_\Omega = \{\text{bijective maps } \Omega \to \Omega\}$. For $n \in \mathbb{N}$, we say that $S_n = S_{\{1,\dots,n\}}$. 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.*

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 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 $n \mapsto g^n$.

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:

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