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

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

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 $a = np$, hen $a^{p-1} \equiv 1 \pmod{p}$.*

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

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 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. *Generators*

Definition 3 (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 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 *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]