Edited: 5:30pm, May 2, 2018

DRAFT — DRAFT — DRAFT — DRAFT

Abstract Algebra I & II

David J. Hunter < Margaret L. Morrow

Westmont College

Contents

To the Instructor

These notes provide an introduction to abstract algebra for advanced undergraduate mathematics majors. There should be enough material for a two-semester sequence. At Westmont College, most mathematics majors and some minors take first semester of this sequence, which (ambitiously) covers Chapters 1–9. These chapters contain a fairly standard treatment of groups, rings, and fields. Some of the more motivated mathematics majors, including those destined for graduate school, will continue to the second semester, completing Chapters 10–13. The second semester includes some advanced group theory, including Sylow Theory, but its ultimate goal is to introduce students to Galois Theory.

This ultimate goal guides the selection of topics throughout these notes, beginning with the introductory activity. On the first day of class, students will discover how group operations can describe the symmetries of a polygon as permutations of the vertices. Analogously, by the end of the second semester, students will be using groups to describe automorphisms of splitting fields as permutations of the roots of a polynomial. It helps to keep the goal of the Galois correspondence in mind throughout both semesters, as it serves as a unifying theme.

At Westmont, enrollment for the first semester of this sequence is typically between 10 and 20, and second semester enrollment is much smaller. Regardless of class size, these notes are designed to be used with some form of the Moore method. Depending on the strength of the class, this method can be modified to provide additional support and scaffolding for students. I have found it very helpful to include the following components.

- **Prework.** Before class, students should work independently on a selection of problems. I like to collect these preliminary solutions, either via online submissions or by running them through a scanner at the beginning of class. I grade these very leniently, giving full credit for what appears to be honest engagement with the problems. Currently, solutions to nearly every problem in every abstract algebra text can be found by searching the Internet, so lenient grading at this stage is essential. I tell students not to use any outside resources during the Prework stage, because I would rather see a half-right attempt at a problem of their own construction than a regurgitation of somebody else's solution.

- **Class Discussion.** During class, students will benefit by explaining their solutions, or lack thereof, to each other. These conversations can be encouraged in a variety of ways, using small-group discussion, class presentations, or a combination of the two. The goal of these discussions is to come to some consensus about a correct solution to each problem.

- **Postwork.** After class, students should be able to write up complete and correct solutions to every problem. These write-ups can be posted on a class wiki, maintained in a code repository, collected through a course management system, or kept in a journal. I carefully grade some subset of these assignments, where the subset size is determined by the size

of the class.

Due to the abstract nature of the subject, it is important for instructors to provide some sort of regular framing and perspective on the material. Lectures will not be necessary, but students will appreciate hearing about why these techniques were developed and how these topics fit together.

The mathematical sophistication of the problems increases steadily throughout the sequence. Early on, students should be able to grapple with every detail of every proof. In later material, especially in the development of the Galois correspondence, some of the more difficult theoretical hurdles are given as theorems, with outlines, or "sketches," of proofs. Often undergraduate treatments of Sylow and Galois theory simply state the main theorems and have students do calculations. While these notes do not require students to construct proofs of every theorem, they are designed to expose students to the theoretical development of the important results.

Throughout the notes, you will notice superscripts at the end of some of the problems. These superscripts refer to endnotes in the last Chapter titled, "Notes to the Instructor."

Acknowledgements

Chapters 1–5 were originally written by Margaret Morrow and published on `jiblm.org`. These chapters have been modified, but retain much of her original content. The remainder of these notes were heavily influenced by some of my favorite algebra texts, including the following.

- *A First Course in Abstract Algebra*, by John Fraleigh.
- *A First Course in Abstract Algebra*, by Joseph Rotman.
- *Contemporary Abstract Algebra*, by Joseph Gallian.
- *Algebra*, by Thomas Hungerford.
- *Galois Theory*, by Joseph Rotman.

To the Student

Have you ever wondered how modern mathematics came to be? To what extent are the definitions and theorems that we find in the canonical textbooks the result of choices made by historical figures? Is there something intrinsic to the subject that forces modern mathematical theory down the path that it takes? Put another way, would Earthling mathematicians recognize the work of a community of mathematicians from a distant galaxy?

We can glean some insight into these questions by proceeding axiomatically: make as few assumptions and definitions as possible, and see where logical deduction leads. The material in these notes represents the consequences of some very low-level mathematical foundations: logic, sets, and the integers. These consequences have applications throughout pure and applied mathematics, and are part of the *lingua franca* of the discipline.

Historically, much of this subject was motivated by the search for solutions to polynomial equations: are there analogs to the quadratic formula for polynomials of degree greater than 2? It is easy to believe that our hypothetical space-alien mathematical colleagues would also be interested in this question. Throughout this semester and the next (should you persevere), you will be guided through a series of deductive discoveries along the path that modern mathematicians have blazed. Whether this path is the only reasonable one will be yours to judge once you have completed the journey.

> *That student is taught the best who is told the least.* —R. L. Moore

These notes (along with the sequel) give a comprehensive coverage of two semesters of advanced undergraduate or beginning graduate algebra. However, these notes contain mostly questions, and you must supply the answers. Your written accounts of your inquiry and our class discussions will produce a complete abstract algebra textbook of your own construction.

Introductory Activity

Redo the worksheet, and add cycle notation.

Chapter 1

Introduction to Groups

Definition 1.1. A **binary operation** $*$ on a set A is a function $A \times A \to A$, where $(a,b) \mapsto a*b$. In other words, a binary operation inputs two elements a, b of the set A, and outputs a well-defined element $a*b$ of the set A.

Problem 1. Which of the following are binary operations on the specified set? If not, explain why not.

1. Addition on $\mathbb{Z}$, the set of integers.
2. Subtraction on $\mathbb{Z}$, the set of integers.
3. Subtraction on $\mathbb{N}$, the set $\{1,2,3,\ldots\}$ of natural numbers.
4. Division on $\mathbb{R}$, the set of real numbers.
5. Division on $\mathbb{Z} \setminus \{0\}$.
6. Composition on D_4, the symmetries of the square.
7. Composition on the set of rotations in D_4.
8. Multiplication modulo 6 on $\mathbb{Z}_6$.

Definition 1.2. A binary operation is **associative** if $(a*b)*c = a*(b*c)$ for all $a,b,c \in A$. An operation is **commutative** if $a*b = b*a$ for all $a,b \in A$. An element e is said to be an **identity** for $*$ if $a*e = e*a = a$ for all $a \in A$. An element b is an **inverse** of the element a if $a*b = b*a = e$.

Problem 2. Refer back to those operations in Problem 1 that were binary operations. Do the following for each of these binary operations.

1. Determine whether the operation is associative, and if not, prove that the operation is not associative.
2. State whether there is an identity for the operation, and if so, identify it.
3. If there is an identity for the operation, determine which elements (if any) have inverses.

Problem 3. Determine which of the binary operations in Problem 1 are commutative, and if not, provide proof that the operation is not commutative.

Problem 4. Prove that if a binary operation $*$ on a set A has an identity element, then that identity element is unique.

Definition 1.3. A **group** is a set G together with a binary operation $*$ on G satisfying the following:

1. The operation $*$ is associative.
2. There is an element in G which is an identity for $*$.
3. Every element in G has an inverse with respect to $*$ in G.

We denote the group by $\langle G, * \rangle$. We refer to the set G as the **underlying set** of the group $\langle G, * \rangle$. (However if the specific operation is clear from the context, or is not important in the context, we sometimes simply write G instead of $\langle G, * \rangle$ for the group, and speak of "the group G.")

Problem 5. Which of the following are groups? If not, explain why not.

1. $\langle \mathbb{Z}, + \rangle$
2. $\langle \mathbb{Z}, - \rangle$
3. $\langle \mathbb{Z}, \times \rangle$
4. $\langle \mathbb{Z}, \div \rangle$
5. $\langle \mathbb{R}^+, \times \rangle$ ($\mathbb{R}^+$ denotes the set of positive real numbers.)
6. The set of symmetries of a regular pentagon with operation composition.
7. $\mathbb{Z}_6$ with operation addition mod 6.
8. $\mathbb{Z}_6$ with operation multiplication mod 6.
9. $\mathbb{Z}_6 \setminus \{0\}$ with operation multiplication mod 6.
10. $\mathbb{Z}_5 \setminus \{0\}$ with operation multiplication mod 5.

Problem 6. Prove that the following is, or is not a group, as appropriate. The set $S = \mathbb{R} \setminus \{1\}$ with operation defined by $a * b = a + b - ab$ for all a and b in S. (On the right side of the equation, the operations are the usual addition and multiplication in $\mathbb{R}$.)

Problem 7. Prove that the following is, or is not a group, as appropriate: The set $M_2(\mathbb{R})$ of all 2 by 2 matrices, with real numbers as entries, and operation matrix multiplication.

Definition 1.4.

- A group $\langle G, * \rangle$ is said to be **abelian** if $*$ is commutative.
- We say a group is **finite** if the underlying set contains finitely many elements. We say a group is **infinite** if the underlying set contains infinitely many elements.
- For a finite group G, the **order** of G is the number of elements in G.

Problem 8. Provide at least two examples of abelian groups.

Problem 9. Refer back to question 5. Identify the finite groups in that question, and for each of these state the order of the group.

Problem 10. Provide at least two examples of non-abelian groups. For one of these, prove that the group is non-abelian.

Problem 11. Suppose $\langle G, * \rangle$ is a group, with s, t and u in G. Prove or disprove as appropriate: If $s * t = u * s$, then $t = u$.

Remark: Using equations. Let a, b, c be elements of a group G. Since the binary operation in a group is well defined, it is OK to multiply both sides of an equation by the same element. In other words, $a = b$ implies that $c * a = c * b$ and $a * c = b * c$.

Problem 12. Let G be a group, and let $a \in G$. Prove that a has a unique inverse.

Problem 13. Suppose G is a group, with a and b in G. Prove that if $a * b = e$, then $b * a = e$. Use this to prove that if G is a group, with a and b in G and $ab = e$, then a is the inverse of b.

Notation: For convenience, instead of using "$*$" to denote the group operation, we often use multiplicative notation as follows:

- In place of $a * b$ write ab.
- Denote the inverse of a (the existence and uniqueness of which is ensured by Problem 12), by a^{-1}.
- Let a^1 denote a, and for $n \in \mathbb{N}$, with $n > 1$, define a^n to be aa^{n-1}.

It is important to note that we have simply introduced some notation; the operation "multiplication" in a group is NOT in general familiar old multiplication. Take care when working in an arbitrary group not to take for granted properties of exponents that are familiar from working with the real numbers. So for example, in the next two problems you may not assume that $a^m a^n = a^{m+n}$, nor that $(a^m)^n = a^{mn}$.

Problem 14. In a group G, if $a \in G$ and $n \in \mathbb{N}$, then both $(a^n)^{-1}$ and $(a^{-1})^n$ have unambiguous interpretations in terms of the definitions above. Prove that these two are in fact equal.

Problem 15. Prove that if G is a group, with $a \in G$, then $(a^{-1})^{-1} = a$.

You have shown in Problem 14 that $(a^n)^{-1}$ and $(a^{-1})^n$ have unambiguous meanings, and are in fact equal. The symbol a^{-n}, on the other hand, is not automatically defined by the definitions already given. It is convenient to define a^{-n} as simply another notation for $(a^n)^{-1}$ and $(a^{-1})^n$:

Definition: In a group G with $a \in G$, we define a^{-n} to be $(a^n)^{-1}$. Also we define a^0 to be the identity, e.

As we've said, we cannot simply assume that exponents will have the same properties in an arbitrary group as they do when working with real numbers. Some familiar properties of exponents for real numbers are in fact false in certain groups. The next problem establishes two basic principles that *do* apply in an arbitrary group.

Problem 16. Suppose G is a group, with $a \in G$. Using notation like

$$a^n = \underbrace{a * a * \cdots * a}_{n},$$

give a brief informal argument that $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$ for all integers m and n. (A formal proof requires a tedious but straightforward use of induction.)

Problem 17. Suppose G is a group, with a, b, and x in G. If $x = a^{-1}b$, can we conclude that $xa = b$? Either prove this conclusion true, or provide a counterexample.

Problem 18. Prove or disprove, as appropriate: Suppose G is a group, with a, b and c in G. If $ac = bc$, then $a = b$.

Problem 19. Prove or disprove, as appropriate: If G is a group, with a and b in G, then $(ab)^2 = a^2b^2$.

Problem 20. Prove or disprove, as appropriate: If G is a group, with a and b in G, then $(ab)^{-1} = a^{-1}b^{-1}$.

Problem 21. Prove or disprove, as appropriate: If G is a group, with a and b in G, then $(ab)^{-1} = b^{-1}a^{-1}$.

Historically, the central focus of abstract algebra was the solution of equations. The following problem gives an indication of the connection:

Problem 22. Suppose G is group, with a and b in G. Consider the equation $ax = b$.

1. Prove that $a^{-1}b \in G$.
2. Prove by substituting that $x = a^{-1}b$ is a solution for the equation.
3. Prove that $x = a^{-1}b$ is the *only* solution for the equation $ax = b$; that is, this solution is *unique*.

You have thus shown that if G is a group, then for all a and b in G, there is a unique solution in G for the equation $ax = b$. Similarly there is a unique solution in G for $xa = b$.

Chapter 2

Mandatory Reading

2.1 Getting Started

The base requirement is a LaTeX distribution. Once you have this, place the following three files from *www.jiblm.org/jiblm/info/authorinfo.aspx* into your working directory.

1. `JIBLM.tex` – This is the file containing additional LaTeX commands beyond those of the standard book class in order to typeset a JIBLM document. You should not need to edit this file.
2. `template.tex` – This file contains the text you are currently reading.
3. A copy of `template.tex`, named `myfile.tex` or whatever you like.

You are now ready to edit `myfile.tex` which will become your submission.

1. At the top of `myfile.tex`, locate

```
%%% Begin {Title Page} %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
\title{Author's Package}
\author{Paul J. Kapitza}
\affiliation{Berry College}
\maketitle
%%% End {Title Page} %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

   and replace “Author's Package", “Paul J. Kapitza" and “Berry College" with the title of your course notes, your name and your affiliation.

2. Delete any of the subsequent content of `myfile.tex` that you wish with the exception of the commands `\frontmatter`, `\mainmatter`, `\backmatter` and `\end{document}` commands. The blocks of statements to be removed are easily identified as follows:

```
%%%%%%%%%%%%%%%%%%%%%%BEGIN REMOVAL {n} %%%%%%%%%%%%%%%%%%%%%%
                    ....material to be removed....
%%%%%%%%%%%%%%%%%%%%%%END REMOVAL {n} %%%%%%%%%%%%%%%%%%%%%%%%
```

Your `myfile.tex` may now be filled in with your own course notes.

2.2 Student and Instructor Versions

You may wish to communicate with two different audiences, the students who will study the materials and the instructors who will teach from the materials. The `\annotation` environment enables you to create one document that serves as both a student and an instructor version. By toggling a single comment in the preamble, text and mathematics which is encased within the environment will be removed or restored upon compilation, providing two versions from the same document. Usage guidelines follow.

1. To change versions, toggle the comment symbol between the following two lines in `myfile.tex`.

```
%\StudentVersion
\InstructorVersion
```

2. Use the `\annotation` environment by placing opening and closing commands on lines separate from the material to be annotated, with no starting spaces or characters of any type on the lines containing the commands. For example:

```
\begin{annotation}
... your instructor-specific text goes here ...
\end{annotation}
```

3. If a large comment is required, place the text in a separate file and use the commands:

```
\begin{annotation}
\input{filename.tex}
\end{annotation}
```

4. Numbered sequences should be handled with caution since the automatic numbering of Chapters, Theorems, Equations, etc., is recalculated when material is removed by the environment.

5. While you may bracket anything you like using the `\annotation{}` environment, such as comments within the theorem sequence, you may wish to add annotations to the instructor as footnotes throughout the text which can be made to appear as a chapter-like component at the end of the document. [1] This document has such a component entitled *Notes to the Instructor* which will appear in the Instructor Version but not in the Student Version. [2] To do this:

   (a) Insert in the text itself footnotes to the instructor in the following format.

   ```
   \begin{annotation}
   \endnote{This is an example of a footnote to the instructor.}
   \end{annotation}
   ```

   (b) After the command `\backmatter`, add the chapter-like component *Notes to the Instructor* that you see following the `\backmatter` command in `template.tex`. Only do this if you have at least one endnote; otherwise you will get an error.

Chapter 3

Optional Reading

3.1 Theorem-like Environments

Theorem environments for declarations are provided and are numbered globally. As an example of the `\theorem{}` environment consider the following typesetting example.

Theorem 3.1. *(The Currant minimax principle.) Let T be completely continuous self adjoint operator in a Hilbert space H. Let n be an arbitrary integer and let $u_1,\ldots,u_{n-1}$ be an arbitrary system of $n-1$ linearly independent elements of H. Denote*

$$\max_{\substack{v\in H, v\neq 0 \\ (v,u_1)=0,\ldots,(v,u_n)=0}} \frac{(Tv,v)}{(v,v)} = m(u_1,\ldots,u_{n-1}) \tag{3.1}$$

Then the n-th eigenvalue of T is equal to the minimum of these maxima, when minimizing over all linearly independent systems $u_1,\ldots u_{n-1}$ in H,

$$\mu_n = \min_{u_1,\ldots,u_{n-1}\in H} m(u_1,\ldots,u_{n-1}) \tag{3.2}$$

Note: The above equations are automatically numbered as equation (3.1) and (3.2).

A number of theorem-like environments are included for structuring mathematical statements. Examples of these are given below in alphabetical order.

Axiom 3.2. This is an axiom

Definition 3.3. This is a definition

Lemma 3.4. This is a lemma

Problem 23. This is a problem

Theorem 3.5 (Main Theorem)**.** *This is a theorem*

Additionally, **acknowledgment**, **algorithm**, **case**, **claim**, **conclusion**, **condition**, **conjecture**, **corollary**, **criterion**, **example**, **exercise**, **notation**, **proposition**, **remark**, **solution**, **summary**, and **proof** are available.

3.2 Packages, Commands, Styles, and Libraries

1. The following packages are used by the Journal:
   - `book`–The base book class of LaTeX.
   - `time`–Make system time available.
   - `enumerate`–Extended enumeration package.
   - `amssymb`, `amsmath`, `latexsym`, `amsthm`–Symbol libraries.
   - `lettrine`–Drop-caps.
   - `mathptmx`–Times Roman type package for both math and text.
   - `fancyhdr`–Header customization.
   - `comment`–Base package for the annotation environment.
   - `endnotes`–End notes package.
2. The current Journal Style does not contain any packages which support graphics content. To include this facility, place a `\usepackage{pkg-choice}` command directly after the first command line in your text file, `\include{JIBLM}`. Popular packages available include `graphics`, `graphicx` and `epsfig`.
3. The following sectioning commands are available:
   - `\chapter{Chapter Title}` command produces a new chapter starting on a new page,
   - `\section{Section Title}` command for major sections, and
   - `\subsection{Subsection Title}` command for subsections.
4. Generally, all the styles available from LaTeX are available, including:
   - Typeset text shapes include *Emphasize*, **Bold**, *Italics* and *Slanted* texts.
   - You can also typeset Roman, Sans Serif, SMALL CAPS, and `Typewriter` families.
   - The size tags are available; tiny, scriptsize, footnotesize, small, normalsize, large 1, Large 2 , Large 3, Huge 1 and Huge 2.
5. The symbol libraries included within the journal package are the `amssymb`, `amsmath`, `latexsym` and `amsthm` packages. This collection provides for most of the commonly used mathematical typesetting tools to be directly accessed. Consult your favorite TeX reference for details. Of particular interest are the mathematical styles,
   (a) $\mathbb{BLACKBOARD}$, (e.g., $\mathbb{R}$,$\mathbb{Z}$,$\mathbb{C}$).
   (b) $\mathcal{CALLIGRAPHIC}$, (e.g. $\mathcal{S} = \emptyset$), and
   (c) $\mathfrak{Fraktur}$.

Notes to the Instructor

[1]This is an example of a footnote to the instructor which will appear at the very end of the document.

[2]This is another example of a footnote to the instructor, in case you missed the first one.

You can also add any text you want here.