Instructor's Guide for Discovering Abstract Algebra

Dr. John K. Osoinach, Jr.
University of Dallas

Contents

Preface

Framework for using a theorem sequence

Using a theorem sequence for the first time can seem daunting, even a bit scary. This is true for many types of inquiry-based or active learning approaches, where the instructor cedes much of the control to the students. My first foray into using theorem sequences came after I had been teaching for over a decade and took a new position at the University of Dallas. Even with a great deal of experience and confidence in the classroom, I still found myself craving guidance and reassurance from my new colleagues about what I was being asked to do. Would my students actually "buy into" this structure? What happens when they're not prepared? How do I cover all the material I need to get through?

The first time I tried it, things went fairly well, but what I wasn't prepared for was the realization of exactly what could be accomplished by using a theorem sequence. Prior to using a theorem sequence, my approach to teaching was mostly content oriented: a course in Calculus, or Topology, or Number Theory, had certain expectations of topics that students need to be shown. Hence, I designed my course around completing a set of topics that would be faithful both to my vision of what would be expected from a student taking that course as well as the student needs and abilities. All was well.

But after I used a theorem sequence for the first time, I quickly realized that my students learned *far* more and retained much more when I relaxed such strict control over the course. What became more important to me was not what I perceived as what is expected of me to cover in my course, but rather with what I wanted my students to come away after taking the course. The *process* of learning mathematics immediately became more important the the *content* of the course itself. I might not have covered absolutely everything I had usually taught, but my students learned more.

Of course, that doesn't mean that anything goes, or that I didn't keep guiding the students along a reasonable pace with reasonable content. But I stopped panicking if I didn't cover everything I used to. I was much more satisfied when I knew that student had actually learned what we covered, and that they now had the tools to continue their investigations on their own. They also enjoyed the subject much, much more than if they were simply shown the material. They *owned* it. It was *theirs*.

How to use this guide

My purpose in writing this guide, then, is to provide one instructor's experience and opinions – mine – in using this theorem sequence. It should not be considered a definitive approach or even a correct one, either. Think of it as a snapshot of how it *can* be used, rather than how it *should* be used. Nonetheless, the narrative that accompanies the theorems and some of the exercises reflects my own opinion of what should be emphasized, based primarily on the 2015 CUPM guide (see below).

Hence, what you'll see in the guide is an explanation of why the theorems are there, which theorems are essential for students to work through and present, which ones are necessary to at least discuss, either for later use or simply as a key consequence of other facts, and which ones are optional for a first course. I've also included what I think are the most important exercises for students to work through as well. But again, these are simply my own opinions. So, as you read this guide, you'll see that I preface each chapter with a pace that I use in my course, a list of what I consider the essential, necessary, and optional theorems in that chapter, and a list of important exercises for students to work. But every instructor needs to decide for themselves what their own goals are, what they consider to be important to achieve those goals, and then which theorems and exercises they should have their students work out.

Finally, in separate documents called Solutions Manuals I also have proofs of the theorems and solutions to the exercises for each part. Feel free to use them to give students hints as you deem necessary. In particular, as you decide which theorems and exercises to give the students to work on, look over the particular proofs and solutions in those documents as a guide to see if you want your students to wrestle with those particular issues.

Course Structure and Goals

As I mentioned in the To The Instructor foreword to the book, there's no one right way to structure a course around a theorem sequence. The philosophy of using a theorem sequence is to allow students to develop their own proofs and solutions, followed by discussion (or debate!) and refinement of the proofs. How you get your students to engage the theorems and exercises is entirely up to you based on your goals and your professional judgement (and your own personality, too). But creating a structure that's student centered requires any instructor to address four questions:

- Will my students be actively engaged in understanding the mathematics encountered?
- Will there be regular opportunities for my students either to share their work with or to collaborate with their peers and instructors?
- Will I be able to inquire as to my students' thinking?
- Will my structure and assessment treat all students equitably?

For instance, when I meet my students for the first time, I emphasize that working through the theorems isn't "glorified homework." They won't earn a grade simply by turning in correct proofs or exercises for me to grade. Getting right answers isn't the goal; I need to see *how* they understand the proof or the way they solved an exercise. I need to see how they *think* about the subject and how I can help them improve their understanding.

There's also no one particular method of assessment that needs to be adopted either. Including a participation or presentation grade is appropriate and very much in line with inquiring into your students' thinking. The use of projects, submitted theorems or exercises for "traditional" grading, take-home tests, or oral exams are all examples of ways to structure a course around the theorem sequence.

There are many groups and organizations (well, as of 2020) dedicated to helping instructors use inquiry-based approaches to mathematics. For help in setting up or implementing this theorem sequence, consider reaching out to one of the following groups, based on your vision and goals of how you want to use this book:

- The Academy of Inquiry Based Learning
- The COMMIT network
- The IBL SIGMAA
- The Initiative for Mathematics Learning By Inquiry (MLI)

Guidelines for topics and pace

This instructor's guide is aimed primarily at giving guidance for a single, first course in abstract algebra for undergraduates. As noted in the To The Instructor portion of the book, the topics included in the book were guided in part by the MAA's Curriculum Guide that the Committee on the Undergraduate Program in Mathematics (CUPM) published in 2015. Not all topics suggested are included, but what is included has been scaffolded carefully so that topics flow fairly naturally from one to the next. Hence, rather than provide a topic dependency chart, I'll summarize any required sequencing here.

- As a general rule, the material in Appendices A and B are absolutely necessary for the entire book, except Chapter 1. Appendix C, dealing with complex numbers, can either be covered explicitly in class or assigned as reading. It's possible to skip exercises dealing with complex numbers, but students will really be missing out on a lot if that happens. Reference to complex numbers occurs often enough in the text that at least a rudimentary knowledge of their arithmetic (section C.1) is needed.
- The chapters in Part I – Chapters 1 through 5 – must be covered in that order. Any particular sections that can be safely skipped (that is, the subsequent sections don't rely on them) will be articulated in the particular chapter guides below.
- Many instructors may desire to have students learn about groups of permutations earlier that the book does, in Chapters 10 and 11. If you find that more to your liking, the earliest in which you can bring in those chapters is after your students have completed Chapter 4.

- The theorems in chapters in part II – chapters 6 through 11 – follow a natural progression in the order given. I don't recommend inserting topics or material (such as permutation groups) between Chapters 5 and 6, as Chapter 6 is a very nice (and strong) continuation of the difficult topic of cosets. Likewise, the material in Chapters 7, 8, and 9 all build up to provide good examples of using the First Isomorphism Theorem. Any of these particular sections that can be safely skipped (that is, the subsequent sections don't rely on them) will be articulated in the particular chapter guides below.

- You'll notice that the material in Part III – Chapters 12 through 15 – deals with rings, but that polynomials are interwoven over those four chapters. The increasing structure on rings has specific implications for how polynomials behave, which is frequently lost on students when polynomials are treated as a "special" object. That said, if you prefer to teach polynomials on their own, you can safely skip those sections until you're ready to treat them separately.

- As I indicated in the To The Instructor forward, parts IV through VI are some of the topics recommended by the 2015 CUPM curriculum guide for a second course. Part IV is required for Part V, but students can explore Part VI as early as after completing Part II (having permutation groups is really important for understanding why group actions ought to be a natural idea to explore).

The remainder of this instructor's guide is my personal opinion of what's important and what's optional; what theorems must be covered and which are peripheral; and where students are likely to struggle and where students like to wallow. There are also a few exercises that are really crucial, and those I do highlight as well.

I try to give a sense of how long to spend, but obviously that depends a great deal on the students in your class. I give time spent in terms of "days;" this measure of time is a typical 50-minute class period. In particular, if you add up the suggested times I propose for each of the first 15 chapters, it comes to a total 37-38 days. This allows for a few extra days for topics in group theory or the material in the appendices, if needed. I also give my own commentary and experience with common pitfalls and errors you can expect. But the 2015 CUPM guide gives absolutely stellar advice as to the core content of just about any first semester Abstract Algebra course. If you're like me and begin "falling behind" of where you'd hope the students should be, you can use this guide to decide what topics are, well, less important than you might have first thought. I've included the relevant portions of that CUPM guide below.

Excerpts from the 2015 CUPM guide

Guiding Principles

The diversity of the student community and the richness of algebra as an area of study imply a diversity of topics that could be covered in a course in Abstract Algebra. While some topic may be of prime importance for a student pursuing one goal, that topic might be relatively unimportant to a student with different goals. Moreover, some of the learning goals we articulate below can be achieved regardless of the specific concepts a given course in Abstract Algebra treats. We therefore adopt the view that there are few topics that *must* be included in any given course in Abstract Algebra.

Although we refrain from specifying pedagogical practices, we do feel that active student engagement is necessary for a mastery of algebraic ideas. In particular, it is essential that students should wrestle with hard problems and communicate their solutions with care, in writing and in speaking. In addition, problem-based, inquiry-based and collaborative learning activities are appropriate means of maintaining student engagement.

Suggested Topics for a General First Course

Groups.

- Definitions and examples of groups and subgroups. Examples should include but not be limited to groups of rotations and reflections of planar figures and rotations of 3-dimensional objects, symmetric groups, integers modulo n with respect to addition and unit groups of integers modulo n with respect to multiplication, invertible 2×2 real matrices under multiplication.
- Cyclic groups and their subgroups, and the orders of elements.
- Symmetric groups, cycle notation, parity of a permutation and the alternating group. (See the remarks below.)
- Isomorphisms and Cayley's Theorem.
- Cosets and Lagrange's Theorem, the falsity of the converse of Lagrange's Theorem, and if time permits, the statement of the Sylow existence theorem.
- External direct products, if time permits.
- Normal subgroups and factor groups, conjugates of a subgroup and of an element.

- Homomorphisms, and the Fundamental Homomorphism Theorem. (See the remarks below.)
- Statement of the structure theorem for finite abelian groups, if time permits.

Rings.

- Definitions and examples of rings and fields. Examples should include but not be limited to the integers and integers modulo n (including the fact that if n is prime, then one gets a field), rational, real and complex fields, polynomial rings, Gaussian integers and matrix rings. Also, if time permits, some finite fields of non-prime order can be discussed. (See the remarks below.)
- Ideals and factor rings.
- Principal ideals, integral domains, principal ideal domains, maximal and prime ideals.
- Homomorphisms, the Fundamental Homomorphism Theorem, the theorem that a commutative ring modulo a maximal ideal is a field.
- Polynomial rings and irreducible polynomials.

Remarks. Some instructors may prefer to omit the proof that the parity of a permutation is well defined. Students should understand, however, that some argument is needed; that this fact is not "obvious". We note that several proofs of this are available which avoid the tedious subscript bookkeeping required in the usual argument involving the polynomial $\prod(x_i - x_j)$.

We referred to the "Fundamental Homomorphism Theorem". By this we mean the result (in both group theory and ring theory) that the image of a homomorphism is isomorphic to the original object modulo the kernel.

We do not feel that general finite fields can be covered in this course, but it is possible to give explicit constructions of fields with 4 or 9 elements. For the field of order 9, consider objects of the form $a + bi$, where a and b are integers modulo 3 and $i^2 = -1 \equiv 2$.

Suggested topics for a second semester course

Groups.

- Group actions and their orbits, the orbit-stabilizer theorem and the orbit counting formula (erroneously) attributed to Burnside and Polya counting. (See the remarks below.)
- If time permits, some of the following: conjugacy class sizes, the class equation, and the fact that nontrivial p-groups have nontrivial centers. Also the Sylow existence theorem and the simplicity of the alternating group A5 can be included here.

Linear algebra.

- A quick review of vector spaces, bases and dimension, linear transformations and their matrices, eigenvalues and eigenspaces.
- Minimal and characteristic polynomials and the Cayley-Hamilton theorem.
- Nilpotent linear operators and the Jordan canonical form.
- Linear functionals and dual spaces.

Fields.

- Algebraic extensions, finite degree extensions and minimal polynomials. Multiplicativity of degrees of extensions.
- Adjoining a root of a polynomial and existence of splitting fields. Repeated roots and formal derivatives. Uniqueness of splitting field. (Needed for uniqueness of finite fields.)
- Finite fields, existence and uniqueness.
- Discussion of geometric constructions. The impossibility of trisecting an angle, squaring a circle and doubling a cube. The construction of regular n-gons. (See the remarks below.)

Module theory.

- Modules, submodules, module-homomorphisms and factor modules.
- Modules over PIDs and the fundamental theorem of abelian groups. (See the remarks below.)

- The rational canonical form for linear operators.

Galois theory (brief introduction)

- Galois groups.
- Solvability by radicals. (See the remarks below.)

Remarks. The so-called Burnside orbit counting formula is

$$N = (1/|G|) \sum \chi(g),$$

where N is the number of orbits and $\chi(g)$ is the number of fixed points of the group element g, and where the sum runs over $g \in G$. As historical research by P. M. Neumann showed, this formula is more properly attributed to Cauchy and Frobenius. An example of Polya counting is the use of this formula to count the number of essentially different ways that the faces of a cube can be colored using a palette of n colors.

At this level one cannot prove all of the relevant facts about compass and straightedge constructions. The impossibility of each the three classical hard problems comes down to the fact that a certain complex number α does not lie in a field extension of 2-power degree over the rationals. For squaring a circle, $\alpha = \sqrt{\pi}$ and for doubling a cube, $\alpha = \sqrt[3]{2}$. To see that general angle trisection is impossible, it suffices to show that a 40 deg angle cannot be constructed, and for that, we can take $\alpha = e^{2\pi/0}$. At least some part of this theory could be presented at the level of Algebra B. Also, it seems that students in Algebra B should learn about Gauss' necessary and sufficient condition that a regular n-gon can be constructed. (The condition is that n is a power of 2 times a product of distinct Fermat primes.)

There was much discussion within the working group about whether or not module theory should be included in a second course. One argument in favor of including it is that modules provide a natural setting for the fundamental theorem of abelian groups. This theorem can be presented, however, without the general theory of modules over PIDs, and in addition, there is a fairly easy inductive argument that can be used to show that every *finite* abelian group is a direct sum of cyclic subgroups.

As is the case with compass and straightedge constructions, it is also true that Galois theory cannot be presented with complete proofs in this course, but still, it seems appropriate for students in a second course to learn what a Galois group is, what it means for a group to be solvable, what it means for a polynomial to be solvable by radicals, and the connections between these ideas.

Part I

Group Theory

Chapter 1

Introduction

Suggested time: 1-2 days.
Essential theorems for presentation: 1.2, 1.4, 1.5, 1.6
Necessary theorems for later use: 1.8, 1.9

This chapter can be introduced on the very first day of class and completed the next. When possible, have students read the To The Student forward and section 1.1 (A brief backstory) before the first day of class.

1.1 A brief backstory

There's no way to do justice to the vast history of algebra with a short summary like this. But I require my students to read this on or before the first day for one and only one reason: to let them know the subject is all about building the machinery to solve equations. That's the context for the whole book. There's no way a student should be able to see how topics like homomorphism, or normal subgroups, or zero divisors, should have any connection to the math they've seen before. Giving them a meaningful reason for the subject's existence provides a needed context as they progress through the theorem sequence.

1.2 Properties of the integers

The three properties of the integers provided lay the groundwork for the repeated need for using closure of binary operations. I insist that any time they use the fact that the sum, difference, or product of two integers is an integer, they must cite this property as the reason. The well-ordering property makes students anxious, but you can't let them remain fearful of its use. I also require its citation any time it's used in a proof.

Theorem 1.2. *Let $m, n \in \mathbb{Z}^+$. Then there is a smallest positive integer belonging to $n\mathbb{Z} \cap m\mathbb{Z}$.*

Make sure they use the well-ordering property carefully and correctly. For instance, I'm very picky that they identify the positive integers in the set, and that it's not empty. But it's important that you use these first few theorems to clarify your expectations for writing proofs.

Theorem 1.4. *Let S be a nonempty set of integers. If there exists an integer m such that $m < s$ for all $s \in S$, then S has a least element.*

This useful little theorem is another good theorem to insist they use the well-ordering property correctly. Many students will be uncomfortable defining the relevant set to which the well-ordering property applies. They just don't believe that *they* get to create their own useful circumstance that provides the desired result!

Lemma 1.5. *Let m and n be integers, with $n > 0$. Then the set $\{m - x \mid x \in n\mathbb{Z}\}$ has a least nonnegative element.*

Remind them to get in the habit of using previous results to prove theorems; in this case, using Theorem 1.4 is the direct way to prove this lemma. Don't be surprised if they still chafe at being asked to construct the set to which to apply the theorem.

Theorem 1.6 (The Division Algorithm)**.** *Let m and n be integers, with $n > 0$. Then there exist unique integers q and r such that $m = nq + r$, where $0 \leq r < n$.*

This is the first major theorem for them to prove. I require my students to memorize the statement of this theorem, and I always require them to recite it either on the first test or the final exam. Be prepared to spend the whole class on this one, if necessary. I almost always give two students the job of presenting this: one for existence, and the other for uniqueness. Spending time getting a really precise, complete proof is essential. Whatever level of precision you want from your students, this is the time to make that clear.

Corollary 1.8. *Let m and n be integers, with $n > 0$. Then m is a multiple of n if and only if the remainder of m divided by n in the Division Algorithm is 0.*

This doesn't need presentation. Have students give an oral proof or justification of this useful fact. But do highlight its utility in how to show something is a multiple of an integer. This idea will be used frequently in later chapters.

Theorem 1.9. *Let $a, b, n \in \mathbb{Z}$ with $n > 0$. If r_a and r_b are the remainders of a and b divided by n, respectively, then the remainder of $a + b$ divided by n equals the remainder of $r_a + r_b$ divided by n, and the remainder of ab divided by n equals the remainder of $r_a r_b$ divided by n.*

This relevant theorem will be very useful when constructing the operation of addition and multiplication modulo n. This is frequently the first homework problem I ask them to submit for assessment. This lets them know how careful and precise I expect their work to be, and I'll get my first glimpse of the relative strengths and weaknesses of the students in my class.

Chapter 2

Binary Operations

Suggested time: 2-3 days
Essential theorems for presentation: 2.16 or 2.17, 2.19, 2.21, 2.25
Necessary theorems for later use: 2.14, 2.24
Important exercises: 2.3, 2.5, 2.8, 2.9, various parts in section 2.3

The three sections that constitute this chapter can be covered in two days, but students will find that pace uncomfortable. On the other hand, if you spend three days on this chapter, the later material in the book might feel somewhat fast, so you'll need to judge if the students really don't get it or if they're just unsure of themselves. A good plan is to anticipate a total of 5 days for students to work through both Chapters 2 and 3.

All of this chapter's theorems are in the third section, so the exercises will be the focus of the first two sections. A really good plan is to assign sections 2.1 and 2.2 for one day, since there are no theorems in these sections – it's all about developing intuition and experience. You can then see how it goes and assign section 2.3 next. You can then decide if you need another half-day on this chapter or if your students are ready to move on to Groups.

2.1 Closure

As remarked above, there aren't any theorems in this section. This section is all about the exercises, along with working out the definitions with the examples.

If you look at the given definition of closure, you'll see that it's written differently than many other authors. In particular, a typical exercise is to "define" an operation on a set, and then ask if the set is closed under this operation. But the definition of the operation must come first, which means you must specify both the domain and the codomain *before*

you can even define the operation. Hence, I've found that defining binary operation and closed in terms of the range of the function is a better way to present this topic.

It's also worth the time to go out of your way to emphasize the difference between $f+g$ and $f(x)+g(x)$ in example 2.2.3. Highlighting this example reinforces to students that this issue isn't going away any time soon. This will come back when dealing with permutations, for instance.

Exercise 2.3. For each set below, determine if the proposed operation on the set G is a binary operation. If not, explain if the operation isn't well-defined, if it's undefined, or if it's not closed.

1. $G = \mathbb{Z}; a * b = a^b$
2. $G = \mathbb{Q}; \frac{a}{b} * \frac{c}{d} = \frac{a+c}{bd}$
3. $G = \mathbb{R}; a * b = |b - a|$.
4. $G = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}, a^2 + b^2 \neq 0\}; z * w = z/w$
5. G is the set of dyadic rationals; $a * b = a + b$.
6. $G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax + b, a, b \in \mathbb{R}\}; f * g = f \circ g$
7. $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b, c, d \text{ are odd integers} \right\}; A * B = AB$
8. $G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \;\middle|\; a, b \in \mathbb{R}, ad \neq bc \right\}; A * B = AB$

   There is a typo in this problem (2.3.8): all four entries a, b, c, d should be real numbers.

Exercise 2.5. Identify which of the binary operations in Example 2.2 and Exercise 2.3 are commutative and which are not.

Exercise 2.8. Go back to the less usual examples from Example 2.2 as well as Exercise 2.5, and determine which of those operations are associative.

Although these exercises are fairly routine, it's good for them to get their hands a bit dirty. The most important ones to have them work correctly are 2, 6, and one of 7 or 8.

Students really don't want to deal with the issue of well-defined, so press them on that with exercise 2. Exercise 6 is a good way to insist they're comfortable with manipulating composition. Finally, exercises 7 and 8 remind students that they really do need to know how matrix multiplication works. If you're looking for four exercises that mix and match commutativity and associativity, exercise 3 is commutative but not associative, exercises 6 and 8 are associative but not commutative, exercise 5 is both, and exercise 4 is neither. The four "less usual" examples also represent three of these four possible combinations.

2.2 Binary tables

Once again, there are no theorems in this section. It shouldn't be skipped, and exercise 2.10 is fun for students (it feels like a puzzle they have to solve, but isn't strictly needed). But this isn't at all worthy of a day's discussion, so combining this section with the previous one is a good plan. And while this is a good section for developing intuition, its content isn't nearly as important as other issues. Exercise 2.9 is the only exercise you need spend time discussing in class.

Exercise 2.9. Let $G = \{a, b, c\}$. Suppose we define a binary operation on G with the following table:

$*$	a	b	c
a	a	c	c
b	b	b	b
c	a	a	b

(So, for instance, $c * a = a$.)

1. Compute $a * b$, $b * a$, $b * b$, $(a * c) * b$, $a * (c * b)$, $c * (c * c)$, and $(c * c) * c$.
2. Determine if the operation is commutative, associative, neither, or both.

This exercise need not much discussion. Just make sure everyone knows how to read and interpret tables. Constructing binary tables will be important when they derive the Klein four-group in the next chapter.

2.3 Isomorphic structures

Many texts wait until much later to introduce the idea of isomorphisms, but I'm convinced that introducing this notion now is the best way to go. Getting students used to the abstract notion of "sameness by means of algebraic properties, not by notation or name" is really important early on, so that they are comfortable with this concept as they progress through the theorem sequence. They'll learn about homomorphisms in the proper context later.

Now, while the theorems aren't hard, students typically get anxious about algebraic properties. Furthermore, I introduce the notions of identity and inverse elements in this context. It's not unreasonable to spend more than a day on this section, especially considering the number of definitions, theorems, and exercises. Finally, while no single exercise is particularly important, don't skip them entirely either. The exercises that I find help students the most are 2.13.1, 2.13.4, 2.22.3, 2.22.4, 2.27.2, 2.27.4, and 2.27.5. Help them talk through how they've already experienced these in different contexts.

Theorem 2.14. *Let $\langle G, * \rangle, \langle G', *' \rangle$, and $\langle G'', *'' \rangle$ be binary structures. Then:*

1. *$\langle G, * \rangle$ is isomorphic to itself;*
2. *If $\langle G, * \rangle$ is isomorphic to $\langle G', *' \rangle$, then $\langle G', *' \rangle$ is isomorphic to $\langle G, * \rangle$;*
3. *If $\langle G, * \rangle$ is isomorphic to $\langle G', *' \rangle$ and $\langle G', *' \rangle$ is isomorphic to $\langle G'', *'' \rangle$, then $\langle G, * \rangle$ is isomorphic to $\langle G'', *'' \rangle$.*

This theorem is necessary for later use, but if you needed to, it can be discussed without presenting. When I have my class present this, I usually have one student present parts 1 and 3 and one student present part 2. Part 2 is the only really messy one here, and that's because students struggle with how to use inverse functions. You can decide if this is worth a class presentation or not.

Theorem 2.16. *The property "$*$ is commutative" is an algebraic property.*

Theorem 2.17. *The property "$*$ is associative" is an algebraic property.*

It's essential that one of these two theorems is presented, but only because students need to know how to prove something is an algebraic property. Choose one for presentation; the other is great for them to turn for homework to check their understanding.

Theorem 2.19. *If a binary structure $\langle G, * \rangle$ has an identity element, then that identity element is unique.*

This is a classic that needs to be presented. Everyone should have to know how to prove this theorem.

Theorem 2.21. *If $\langle G, * \rangle$ and $\langle G', *' \rangle$ are isomorphic binary structures, and $\langle G, * \rangle$ has an identity element $e \in G$, then $\phi(e)$ is the identity element for G', where $\phi : G \to G'$ is any isomorphism from G to G'. Consequently, the property "$\langle G, * \rangle$ has an identity element" is an algebraic property.*

This is another crucial theorem that needs to be presented. Indeed, this will come back when homomorphisms are introduced in Chapter 6. There the students will refer back to this proof and notice that they never needed to use the bijective properties of the function!

Theorem 2.24. *Let $\langle G, * \rangle$ be a binary structure with an identity element e. If a' is a left inverse for a, then a is a right inverse for a'; if a' is a right inverse for a, then a is a left inverse for a'; and if a' is an inverse for a, then a is an inverse for a'.*

A brief oral discussion should suffice, rather than a class presentation. I wouldn't bother assigning this for homework.

Theorem 2.25. *If $\langle G, * \rangle$ and $\langle G', *' \rangle$ are isomorphic binary structures with an identity such that every element in $\langle G, * \rangle$ has an inverse, then whenever $a' \in G$ is an inverse of $a \in G$, the element $\phi(a') \in G'$ is an inverse for $\phi(a) \in G'$ for any isomorphism $\phi : G \to G'$. Consequently, the property "Every element in $\langle G, * \rangle$ has an inverse" is an algebraic property.*

This theorem is another classic that ought to be presented. Everyone should have to know how to prove this result. If you really wanted to, you could assign this for homework after they see the idea from theorem 2.21. This will be extremely important when groups are developed in the next chapter.

Chapter 3

Groups

Suggested time: 2-3 days
Essential theorems for presentation: 3.6, 3.8, 3.10, 3.12
Necessary theorems for later use: 3.13, 3.16
Optional theorems: 3.7
Important exercises: Parts of 3.4, one of 3.11 or 3.15, 3.22

Although this chapter seems like it should take a long time, most of the work has been done in the previous chapter. Depending on the class, you only need two or at most three days for this chapter. The length of the chapter is due to the large number of examples of groups in the first section that the students will need to have for the course. This chapter has a nice balance of theorems and exercises.

3.1 Basic properties of groups

So much of this first section is for them to read on their own, so anticipate a longer than usual time for discussion before the theorems. I frequently wind up with much of the first day dealing with examples and exercises and only get to presenting one theorem (occasionally not even that, especially if students are finishing up section 2.3). I can then judge if I need one or two additional days for the next sections.

Exercise 3.4. Which, if any, of the following are groups? For those that are, give the identity element of the group. (Hint: check associativity *last*.)

1. $G =$ the nonnegative integers; $\quad m * n = m + n$.
2. $G = \mathbb{Z}$; $\quad x * y = x + y - 2$.
3. $G = \mathbb{Q}$; $\quad r * s = rs$.
4. $G = \{1, 2, 3, 4\}$, $\quad a * b = r$, where r is the unique remainder of ab divided by 5.
5. $G =$ the set of all $n \times n$ diagonal matrices over $\mathbb{R}$; $\quad A * B = AB$.
6. $G = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) \geq 0\}$; $\quad (f * g)(x) = |f(x) - g(x)|$.
7. $G = \{a + bi \in \mathbb{C} \mid a^2 + b^2 = 1\}$; $\quad z * w = zw$.
8. Let X be a set, and let $G = \mathcal{P}(X)$, the power set of X; $\quad S * T = (S \cup T) - (S \cap T)$.

The first 5 problems in this exercise are my favorites. Look over the solutions provided for Part I to see the issues each of these problems raise, but at the very least assign problem 4 for students to work and discuss. Students really need practice with the algebra of remainders, and it foreshadows the ring of integers modulo n. In particular, ask them about the integers $\{1, 2, 3, 4, 5\}$ divided by 6 and the integers $\{1, 2, 3, 4, 5, 6\}$ divided by 7. Get them to play and make a conjecture to foreshadow Ring Theory!

Theorem 3.6. *Let $\langle G, * \rangle$ be a group, and let $g \in G$. Then there exists exactly one inverse for g.*

This theorem is essential only because the previous section demonstrated that inverses need not be unique. If you're pressed for time, you can safely skip this, but it's best if you can have it presented. Assigning this for homework is also a reasonable option.

Corollary 3.7. *If $\langle G, * \rangle$ is a group, then the equations $a * x = b$ and $y * a = b$ have a unique solution for each $a, b \in G$, namely $x = a' * b$ and $y = b * a'$, where a' is the inverse of a.*

This corollary doesn't need a full presentation. It gives a formula for the solution to the equation, which isn't really central. Either skip this entirely or have a brief discussion in class. If you like, you could also use it as a homework problem to verify that they're using the group properties with the care and precision you want.

Theorem 3.8 (The Cancellation Laws)**.** *Let $\langle G, * \rangle$ be a group, and let $a, b, c \in G$. Then the following hold:*

1. *(Left Cancellation Law) If $c * a = c * b$, then $a = b$.*
2. *(Right Cancellation Law) If $a * c = b * c$, then $a = b$.*

It's absolutely essential that this crucial theorem is presented to the class. Doing just one part is fine, since the other part is identical. Insist that they use associativity carefully, as this reinforces why we need all the properties in our definition of a group.

3.2 Group notation

This section is all about careful notation and understanding what the laws of exponents do. It's tempting to just have a discussion about this, but it's important for students to be precise about such matters. You probably won't need an entire day with this, though.

Theorem 3.10. *Let G be a group, and let $a, b \in G$. Then $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.*

This is a huge theorem. Have students present this one, and make sure they appreciate how the inverse of a product isn't simply the product of the inverses: it's the product of the inverses in the reverse order. It's worth asking your students (don't tell them!) if they've seen this fact in another course; hopefully, someone will recall this important property of invertible matrices from their linear algebra course. Finally, many instructors call this fact the "socks and shoes" theorem: you put your socks on first, then your shoes, but to remove them, you must take them off in the reverse order. It's a great way to help students remember this!

Exercise 3.11. Prove that if G is a group, then $(ab)^{-1} = a^{-1}b^{-1}$ for all $a, b \in G$ if and only if G is abelian.

This is a fabulous homework problem, or a really good one to have them do a proof sketch for discussion. If you like, see if students can come up with two fundamentally different proofs!

Theorem 3.12. *Let G be a group and $a \in G$. Then for any nonnegative integer n, we have $(a^{-1})^n = (a^n)^{-1}$.*

Presenting this theorem ensures that everyone understands the notation. It's also a great way to see how well students can use induction.

Theorem 3.13 (Laws of Exponents)**.** *Let G be a group and $a \in G$. Then for any integers n, m, we have $a^n a^m = a^{n+m}$ and $(a^m)^n = a^{nm}$.*

This needs class discussion but not necessarily the full presentation in class. A formal proof would be unnecessarily tedious and doesn't shed any light at all on the theorem, while a semi-formal intuitive argument really does a better job here. Don't assign this for homework – the grading will drive you crazy.

Corollary 3.14 (Laws of Coefficients)**.** *Let G be an abelian group under addition, and let $a \in G$. Then for any integers n, m, we have $na + ma = (n + m)a$ and $n(ma) = (nm)a$.*

As much as I assumed that students would have no problem applying the Laws of Exponents in an additive sense, long experience has taught me that this is not the case. This theorem should be discussed along with the Laws of Exponents, but not presented. However, do *not* let students call this a "distributive" law or property. That will come with Ring Theory; what is being given here is a *notational* theorem.

Exercise 3.15. Prove that if G is a group, then $(ab)^2 = a^2b^2$ for all $a, b \in G$ if and only if G is abelian.

Much like Exercise 3.11, this really hammers home the point that not all the laws of exponents they think they know work. Both exercises get this (same) point across.

3.3 Group tables and the order of a group

This section really gets students to work out their own first examples of small groups. It doesn't need a full day, so you might combine this section with the previous one. Theorem 3.16 will be used to help create tables of small groups, so at least a sketch of a proof is in order. But the most important issue in this section is the definition of the order of a group. In particular, since order is used in two different ways in algebra – the order of a set and the order of an element – it's important to begin getting this terminology straight now.

Finally, exercise 3.22 is really, really important. It shows that there are exactly two non-isomorphic groups of order 4. And asking students to play around to see what they get with groups of order 5 or 6 is a good way to get messy with the subject!

Theorem 3.16. *Let G be a group. Then for every $g \in G$, the functions $\lambda_g : G \to G$ and $\rho_g : G \to G$ defined by $\lambda_g(x) = gx$ and $\rho_g(x) = xg$ are bijections.*

You can either have this presented or just sketched as part of class discussion, especially since it's so short. Some of my students like to call this the "Sudoku Theorem," since it says that in every row and in every column of a group table, each element of the group must appear once and only once, just like in a Sudoku puzzle.

Exercise 3.22. In this exercise, you will create the only two groups of order 4 (up to isomorphism). One of them must be isomorphic to $\mathbb{Z}_4$, so the other will be a new group, called the *Klein four-group*, denoted V. Use the set $\{e, a, b, c\}$, with e denoting the identity element, to create two nonisomorphic group tables in the following way. First, create the unique group table for which every element is its own inverse. Since not every element in $\mathbb{Z}_4$ is its own inverse, this will be the Klein four-group V. Then create a group table for which some element is not its own inverse. In so doing, explain why any choices you make are either forced or arbitrary. This shows that every group of order 4 is either isomorphic to $\mathbb{Z}_4$ or to V. Are either, both, or neither groups abelian?

The construction of the Klein four-group and the analysis of its features is utterly necessary for what follows. It provides a good, new example of a group for students to use throughout the book. Emphasize that they'll need to reference this group often.

Chapter 4

Subgroups and Generating Sets

Suggested time: 3 days.
Essential theorems for presentation: 4.9, 4.10, 4.13, 4.20, 4.24, 4.25, 4.28, 4,34, 4.35 parts 1 and 2
Necessary theorems for later use: 4.7, 4.29, 4.30
Optional theorems: 4.15, 4.16, 4.18, 4.32, 4.35 part 3
Important exercises: Parts of 4.12, parts of 4.22 and 4.27, parts of 4.33

This chapter can be tricky to navigate. On the one hand, the concept of a subgroup is easy enough, so most of the theorems should be straightforward. On the other hand, there are so many important theorems, exercises, and examples that spending a lot of time seems both necessary and natural. You'll have to judge the needs of the class carefully and balance it against the time constraints you're under at this point. Some topics and several theorems can be safely omitted, so don't expect (or even try) to cover everything.

4.1 Subgroups

There's a lot of reading in this section, and the preliminary theorems and exercises are a good way to get them used to the way subgroups work. Expect a good deal of discussion before theorem presentations.

Theorem 4.7. *Let G be a group and H a subset of G. Then H is a subgroup of G if and only if*

1. *H is closed under the operation induced by the operation on G;*
2. *H contains the identity element e of G; and*
3. *For all $a \in H$, its inverse a^{-1} is also in H.*

As important as this theorem is, you really don't need to have this presented. The proof isn't enlightening, and you can easily justify this in the discussion. That's the best place to develop this theorem and not in a presentation of its proof.

Theorem 4.9. *Let G and G' be groups and $\phi : G \to G'$ be an isomorphism. If $H < G$, then $\phi(H) < G'$.*

This is a good, straightforward theorem to show how subgroups work under isomorphisms.

Theorem 4.10. *Let G be a group and $\mathcal{H}$ be a nonempty collection of subgroups of G. Then $\bigcap_{H \in \mathcal{H}} H$ is a subgroup of G.*

Another good theorem to present, but if the notation isn't familiar, then just have them prove that the intersection of two subgroups is a subgroup. I've found that the proofs of this and the previous theorem are nice and short, so you can fit these proofs in with only 15 minutes to spare. On the other hand, if you're really pressed for time, you can skip this one. Make sure, though, that if it's presented, that they see where the subtle condition of $\mathcal{H}$ is not empty comes in!

Exercise 4.12. Determine if the following subsets H are subgroups of the given group G under the operation induced from G. Provide either a proof or a counterexample to justify your answers.

1. $G = \mathbb{Q}; H =$ the set of dyadic rationals.
2. $G = \mathbb{R}; H = \{2^\alpha \mid \alpha \in \mathbb{Q}\}$.
3. $G = \mathbb{Z}_9; H = \{0, 2, 4, 6, 8\}$.
4. $G = GL_2(\mathbb{R}); H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \;\middle|\; a, b, d \in \mathbb{R}, ad \neq 0 \right\}$.
5. $G = S_{\mathbb{Z}}; H = \{f \in S_{\mathbb{Z}} \mid f(\mathbb{Z}^+) \subset \mathbb{Z}^+\}$.
6. $G = \mathbb{C}^*; H = \{a + bi \in \mathbb{C}^* \mid a, b \in \mathbb{Q}\}$.

The point of problems 1 and 2 is to confirm that they know the correct operation: addition! I highly recommend problem 3 to reinforce their understanding of modular computations. And problem 5 is fairly challenging for many students, but I think it's worth seeing how my the class as a whole wrestles with it.

4.2 The center of a group

I frequently only cover part of this section and combine it with the beginning of the next section on cyclic groups. In particular, I've always skipped the material on the centralizer of an element and focused only on the center of a group. Centralizers play a very little role at this level of algebra, while the center of a group will appear with some frequency later in algebra.

Theorem 4.13. *Let G be a group. Then the subset $Z(G) = \{g \in G \mid xg = gx \text{ for all } x \in G\}$ is a subgroup of G.*

You could probably assign this for homework, if you're pressed for time. But it's vital to make sure everyone knows what the center of a group is. So, if you really had to choose, it's better to skip Theorem 4.10 and present this one instead.

Corollary 4.15. *Let G be a group. Then G is abelian if and only if $Z(G) = G$.*

Just mention this result in class discussion as an obvious consequence to Theorem 4.13. There's no need for a full presentation.

Theorem 4.16. *Let G be a group and $a \in G$. Then the subset $C(a) = \{g \in G \mid ga = ag\}$ is a subgroup of G.*

I usually don't cover centralizers in a first semester course. I like returning to this topic in a second course when dealing with group actions.

Theorem 4.18. *Let G be a group. Then $Z(G) = \bigcap_{a \in G} C(a)$.*

This is a cool theorem that relates the individual centralizers to the global center of a group. This is a natural theorem to assign for homework if (or when) you cover centralizers.

4.3 Generating sets

I usually combine the first part of this section with the previous one, and then spend the next day on what the students didn't complete. The technical details of cyclic groups is worth their time, but the technical details of general generating sets isn't. Emphasize cyclic subgroups over subgroups generated by an arbitrary subset, but don't omit it either.

Theorem 4.20. *Let G be a group and $a \in G$. Then the subset $\{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.*

This theorem is very easy, but it motivates so much of what follows.

Exercise 4.22. List or give a formula that describes the elements in the cyclic subgroups given below.

1. $G = \mathbb{Z}; H = \langle 4 \rangle$.
2. $G = \mathbb{Q}^*; H = \left\langle -\frac{1}{2} \right\rangle$.
3. $G = \mathbb{Z}_{12}; H = \langle 10 \rangle$.
4. $G = SL_2(\mathbb{Z}); H = \left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \right\rangle$.
5. Let $A = \mathbb{R} - \{0, 1\}$, and let $G = S_A; H = \langle f \rangle$, where $f(x) = 1 - \frac{1}{x}$.
6. $G = \mathbb{C}^*; H = \langle i \rangle$.
7. $G = U_8; H = \langle \zeta_2 \rangle$.
8. $G = U_8; H = \langle \zeta_3 \rangle$.

Each exercise here highlights different issues. Problem 1 forces students to translate the definition to additive notation, whereas problem 2 is really straightforward. Problem 3 is more practice with modular arithmetic. Problem 4 has a really nice geometric interpretation as a shear transformation of the plane. And exercise 5 is one of my favorites in the whole book – a function of order 3! You can skip 7 and 8 without much problem, but problem 6 is just so classic. I'd recommend having students work out 1, 3, and 5, at the least. I'd also pair this with exercise 4.27.

Lemma 4.24. *Let G be a group, and let $a \in G$. Then a has finite order if and only if $a^i = a^j$ for some integers $i \neq j$.*

This is really straightforward, but you'd be surprised how this really helps students gain insight. You can either present this or sketch the main idea, but everyone needs to see this little fact.

Theorem 4.25. *Let G be a group.*

1. *If $a \in G$, then $|a| = |\langle a \rangle|$.*
2. *If G is finite, then any element of G has finite order.*

This essential theorem needs presentation. There are two parts, so having two students present this works well.

Exercise 4.27. Go back to Exercise 4.22 and find the order of the element used to generate each cyclic subgroups listed.

Pair this exercise with 4.22. If you can, ask students about the orders of the other elements in problem 3 and see if they notice anything.

Theorem 4.28. *Let G be a group and let $a \in G$ be an element of finite order n. Then $a^k = a^l$ if and only if $k - l$ is a multiple of n.*

This theorem isn't obvious, so the proof is very enlightening. If you like, it's not unreasonable to suggest (or give a hint) using Corollary 1.8 to show something is a multiple of n.

Corollary 4.29. *Let G be a group and let $a \in G$. If $a^k = e$ for some positive integer k, then $|a|$ divides k.*

This is really the main takeaway from Theorem 4.28. It's one of the most useful tools for students to have, so emphasize this corollary right after the presentation of Theorem 4.28.

Theorem 4.30. *Let G be a group and $A \subset G$. Then the subset*

$$\{a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \mid a_i \in A, k \in \mathbb{Z}^+, n_i \in \mathbb{Z}\}$$

is a subgroup of G.

You don't need to present the proof of this, but get them to talk through why this theorem is true. Students will get this, and the exercises will illuminate the principle more that the proof.

Theorem 4.32. *Let G be a group, $A \subset G$, and $\mathcal{H} = \{H < G \mid A \subset H\}$. Then $\bigcap_{H \in \mathcal{H}} H$ is the subgroup generated by A.*

It's a nice result but really inconsequential in a first course. You can safely skip this one.

Exercise 4.33. List or describe the elements in the subgroup generated by the given set A.

1. $G = \mathbb{Q}^*$; $\quad A = \{2, 3\}$
2. $G = \mathbb{Z}$; $\quad A = \{4, 6\}$
3. $G = S_{\mathbb{R}}$; $\quad A = \{f, g\}$ where $f(x) = x + 1$ and $g(x) = -x$.
4. $G = \mathbb{R}$; $\quad A = \{\frac{1}{n} \mid n \in \mathbb{Z}^+\}$
5. $G = \mathbb{Q}$; $\quad A = \{2^{-n} \mid n \in \mathbb{Z}^+\}$
6. $G = SL_2(\mathbb{C})$; $\quad A = \left\{ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}$

Many of these problems foreshadow important ideas to come. The ones that do this best are problems 2 (greatest common divisors) and 6 (the quaternion group). For a little more fun, problem 4 connects to Egyptian fractions, and problem 5 generates the dyadic rationals. The only one that really needs attention, though, is problem 2; choose as many or as few of the others as you deem needed.

Lemma 4.34. *Let G and G' be groups and let $\phi : G \to G'$ be an isomorphism. Then $\phi(a^n) = \phi(a)^n$ for all $a \in G$ and $n \in \mathbb{Z}$.*

If you want the presenter to deal only with $n \geq 0$, for a cleaner induction, that's fine, but make everyone discusses how to complete the proof for negative exponents.

Theorem 4.35. *Let G and G' be groups and let $\phi : G \to G'$ be an isomorphism.*

1. *If $a \in G$ has (finite) order n, then $\phi(a)$ has (finite) order n. If $a \in G$ has infinite order, then so does $\phi(a)$.*
2. *If H is a cyclic subgroup of G generated by a, then $\phi(H)$ is a cyclic subgroup of G' generated by $\phi(a)$.*
3. *If A is a generating set for a subgroup $H < G$, then $\phi(A)$ is a generating set for $\phi(H)$.*

Part 1 is hugely important for presentation. The issue with which students routinely struggle is the part of the definition of order dealing with the smallest positive integer. Part 2 isn't nearly as problematic, as it follows directly from the lemma. If students believe part 2, they'll believe part 3 too, so don't spend time on the third part.

Chapter 5

Applications of Subgroups

Suggested time: 3 days.
Essential theorems for presentation: 5.3, 5.5, 5.6, 5.8, 5.9, 5.12, 5.13, 5.17
Necessary theorems for later use: 5.4, 5.20
Optional theorems: 5.21, 5.24
Important exercises: 5.2, 5.14, 5.23

This is likely the first place where many students will get truly lost. After all the buildup with groups and subgroups, we throw them a curve ball and talk about non-closed subsets (cosets) without any obvious justification. This chapter tries to motivate their importance, but this will take a lot of patience on both the instructor's and the students' part. Don't even think about rushing through the material on cosets. Spend three solid days on this chapter, either a day on each section, or two and a half days on the first two sections and dealing with conjugation lightly.

5.1 Cosets

Go super slow on this section. The theorems aren't hard, but students don't remember them as important, primarily because cosets don't seem relevant to them.

Exercise 5.2. Each subgroup of the given group below has a finite number of left cosets. Please list all its distinct left cosets, and for each coset, describe the cosets using two different elements from the group.

1. $G = \mathbb{Z}; \quad H = 5\mathbb{Z}.$
2. $G = \mathbb{Z}_{12}; \quad H = \langle 8 \rangle .$
3. $G = GL_2(\mathbb{R}); \quad H = \{A \mid \det(A) \geq 0\}.$
4. $G = \left\langle \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}, \begin{bmatrix} 0 & \pm 1 \\ \pm 1 & 0 \end{bmatrix} \right\}, \cdot \right\rangle; \quad H = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \right\}.$
5. $G = U_8; \quad H = \{\zeta_0, \zeta_4\}.$
6. $G = \mathbb{Z}[i]; \quad H = \langle \{2, 2i\} \rangle .$

This exercise is the key motivator for the next theorem. You don't have to have students work all the problems, but at the very least problems 1 and 2 need to be dealt with, and while problem 3 won't seem easy to students, it's possibly the most helpful one of the bunch.

Theorem 5.3. *Let G be a group and $H < G$.*

1. *Let $aH, bH \in G/H$. Then $aH = bH$ if and only if $a^{-1}b \in H$ if and only if $b^{-1}a \in H$*
2. *Let $Ha, Hb \in H\backslash G$. Then $Ha = Hb$ if and only if $ba^{-1} \in H$ if and only if $ab^{-1} \in H$.*

You don't need both parts presented. Since left cosets are the preferred object of study, have them present part 1. Then ask them what changes would need to be made to prove part 2.

Corollary 5.4. *Let G be a group and $H < G$. Then $aH = H$ if and only if $a \in H$.*

You don't need to have them present this, but do emphasize this one a lot. They'll need this all the time when dealing with quotient groups.

Theorem 5.5. *Let G be a group and $H < G$. If $aH, bH \in G/H$, then either $aH = bH$ or $aH \cap bH = \emptyset$.*

This must be presented. Insist on a careful, rigorous proof. Every student of mathematics should be expected to know and understand this argument.

Theorem 5.6. *Let G be a group and $H < G$.*

1. *The relation defined by*
$$a \sim b \text{ if and only if } a^{-1}b \in H$$
is an equivalence relation on G whose equivalence classes are the left cosets of H in G.

2. *The relation defined by*
$$a \sim b \text{ if and only if } ba^{-1} \in H$$
is an equivalence relation on G whose equivalence classes are the right cosets of H in G.

If you skip this theorem, it won't really harm them, but they'll miss a classic of the subject. It's a good theorem that ties a central mathematical principle (equivalence relations) with the new object (cosets). You only need to have them do part 1, then ask them what to change for a proof of part 2.

5.2 Lagrange's theorem

This is a key section. Nothing is to be skipped.

Theorem 5.8. *Let G be a group and $H < G$. If $aH, bH \in G/H$, then the function $f : aH \to bH$ given by $f(ah) = bh$ is a bijection.*

Very straightforward, but very important.

Theorem 5.9. *Let G be a group and H be a subgroup. The function $f : G/H \to H\backslash G$ given by $f(gH) = Hg^{-1}$ is a well-defined bijection.*

Not quite as important, but its technique is. Students will struggle often with what it means for a function to be well-defined, and this is a low-stakes theorem to help them develop this proof technique. Make sure they present this one.

Exercise 5.11. Go back and find $|G : H|$ for the subgroups in Exercise 5.2.

This is a standard exercise, just to make sure they can apply the definition. Nothing deep.

Theorem 5.12 (Lagrange's Theorem)**.** *Let G be a finite group and $H < G$. Then $|H|$ divides $|G|$, and $|G| = |G : H| \cdot |H|$.*

This is the biggest theorem so far, and naturally it must be presented.

Corollary 5.13. *Let G be a finite group. Then the order of any element of G must divide $|G|$, and $g^{|G|} = e$ for all $g \in G$.*

This crucial ramification of Lagrange's theorem needs to be presented, as it requires students to combine orders of elements with subgroup ideas. They're always still growing in this area, so its presentation is important for everyone to see and discuss.

Exercise 5.14. For each finite group below, list all the possible orders of subgroups, and find an element of that order, if possible.

1. $G = \mathbb{Z}_{20}$
2. $G = U_7$
3. $G = \left\langle \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm i \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \pm i \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}, \cdot \right\rangle$

This important exercise forces them to play around with the key application of Lagrange's theorem. Problems 1 and 2 are really the most important ones to have them work out thoroughly.

5.3 Conjugation

This section isn't as central as the other topics in the chapter, so you can decide how much or little time to spend on this section. Just don't skip it entirely, or many of the ideas that come later will seem somewhat mystifying.

Theorem 5.17. *Let G be a group and $H < G$. Then for any $g \in G$, the set $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G.*

In case anyone is still struggling with proving something is a subgroup, this is a good confidence builder. Otherwise, have them sketch a proof and present the next theorem instead (time permitting).

Theorem 5.20. *Let G be a group and $a \in G$. Then for any $g \in G$ and any integer $n \in \mathbb{Z}$, we have $(gag^{-1})^n = ga^ng^{-1}$. In particular, conjugate elements have the same order.*

This is a great theorem to assign for homework, or if you have time, to have them present. On the other hand, if you choose to discuss inner automorphisms below, you can have them prove this as a corollary to Theorem 5.21 by citing Theorem 4.35.

Theorem 5.21. *Let G be a group and $g \in G$. Then the function $\phi_g : G \to G$ given by $\phi_g(a) = gag^{-1}$ is an automorphism of G.*

It's not all that unusual to have to treat inner automorphisms lightly, and I've frequently skipped the topic entirely. It seems unnatural to omit such a fundamental object, but for a first course in algebra, it's safe to skip this. When students need it later, they can return to it.

Exercise 5.23. There's a neat trick to remember when dealing with conjugation that's frequently useful. Suppose you have a product of elements $a_1a_2 \dots a_n$ in a group, and you conjugate this product by an element g. Show that you can write the result as a product of conjugates of the elements $a_1, a_2, \dots, a_n$.

This exercise is just a generally useful fact, but if you don't see the idea, it often seems like "magic." Make sure everyone sees how this works.

Theorem 5.24. *Let G be a group. Then $Inn(G) < Aut(G)$.*

This is just such a cool result, so if you've chosen to cover inner automorphisms, then it's worth including this.

Part II

Types of Groups

Chapter 6

Quotient Groups

Suggested time: 3 days.
Essential theorems for presentation: 6.5, 6.7, 6.10, 6.11, 6.13, 6.19, 6.26
Necessary theorems for later use: 6.2, 6.17, 6.21, 6.22, 6.23, 6.28, 6.30. 6.32
Optional theorems: 6.22, 6.25, 6.34
Important exercises: Parts of 6.3 and 6.8, 6.9, parts of 6.16 and 18, parts of 6.20

This is a big, big chapter. Its content is denser than most, and there are more theorems in this chapter than most. Let the class guide the pace here, as the idea of cosets as elements that form a group is shrouded in mystery. Don't fret if only two theorems are presented on any given day. Get the students to play with the exercises to help them along. Anticipate a solid three days.

6.1 Homomorphisms and kernel

This section on homomorphisms is preparatory for quotient groups, obviously. The exercises provide the needed motivation, and the theorems begin to make connections with other topics already seen.

Theorem 6.2. *Let $\phi : G \to G'$ be a group homomorphism and let $H < G$.*

1. *The image of the identity of G under ϕ is the identity of G'.*
2. *$\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.*
3. *$\phi(g^n) = (\phi(g))^n$ for all $g \in G$ and integers n.*
4. *If $g \in G$ has finite order, then $\phi(g)$ has finite order and is a divisor of the order of g.*
5. *$\phi(H) < G'$.*
6. *If H is abelian, then $\phi(H)$ is abelian.*
7. *If $A \subset H$ generates H, then $\phi(A)$ generates $\phi(H)$.*

Honestly, this does not need a full, formal presentation. There are several ways to handle this theorem: assign parts for homework, sketch a few for short proofs, or even refer to these facts proved in the context of isomorphisms, and note when the bijective nature of the map was never needed. But don't waste valuable class time for a presentation of this (or just have them present part 4). Have a healthy discussion of this theorem at the start of the class or in the context of the exercises.

Exercise 6.3. Which, if any, of the following functions are homomorphisms? You might also see if any are secretly isomorphisms, while you're at it. (Hint: consider using Theorem 6.2 to identify those that aren't homomorphisms.)

1. $\phi : \mathbb{Z} \to \mathbb{Z}; \quad \phi(x) = 2x.$
2. $\phi : \mathbb{Q} \to \mathbb{Q}; \quad \phi(x) = |x|.$
3. $\phi : \mathbb{R} \to \mathbb{C}; \quad \phi(x) = \sqrt{x}.$
4. $\phi : \mathbb{Z} \to \mathbb{Z}_5; \quad \phi(x) = x.$
5. $\phi : \mathbb{Z}_5 \to \mathbb{Z}; \quad \phi(x) = x.$
6. $\phi : \mathbb{Z}[i] \to \mathbb{Z}; \quad \phi(a + bi) = b - a.$
7. $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*; \quad \phi(A) = \det(A).$
8. $\phi : U \to SL_2(\mathbb{C});$
   $\phi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$

This straightforward exercise gets their feet wet for what's coming. I'd especially emphasize the difference in problems 4 and 5, and problem 7 really makes an important connection to linear algebra.

Theorem 6.5. *Let $\phi : G \to G'$ be a group homomorphism. If $H' < G'$, then $\phi^{-1}(H') < G$.*

Because students typically struggle with inverse images of sets, the presentation is worthwhile.

Theorem 6.7. *Let $\phi : G \to G'$ be a group homomorphism. Then ϕ is injective if and only if $Ker(\phi) = \{e\}$.*

Another classic. Emphasize that this is a very short, convenient way to detect if a homomorphism is injective (and don't use the word monomorphism – they've got far too much terminology already).

Exercise 6.8. Find the kernel of the maps in Exercise 6.3 that are homomorphisms. Of those, which are injective?

This exercise gets students used to finding the kernel of a homomorphism and how to use it to detect isomorphisms.

Exercise 6.9. Each function below is a homomorphism (you need not verify that). Compute and compare the kernel of each homomorphism to the given inverse images. (To compare means to see if there is a computation you can specify that relates the kernel to each inverse image.)

1. $\phi : \mathbb{Z} \to \mathbb{Z}_5$; $\phi(x) = r$, where r is the remainder of x divided by 5. Compute and compare $Ker(\phi), \phi^{-1}(1)$, and $\phi^{-1}(2)$.
2. $\phi : \mathbb{Z}[i] \to \mathbb{Z}$; $\phi(a+bi) = b-a$. Compute and compare $Ker(\phi), \phi^{-1}(1)$, and $\phi^{-1}(-1)$.
3. $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*$; $\phi(A) = \det(A)$. Compute and compare $Ker(\phi)$ and $\phi^{-1}(-1)$. (Hint: do your answers to the first two exercises suggest how these two might also compare?)

This is a really key exercise. It motivates why we should care (or even consider) the next theorem.

Theorem 6.10. *Let $\phi : G \to G'$ be a group homomorphism with kernel K, and let $a' \in G'$. Then $\phi^{-1}(a') = aK = Ka$ for any element $a \in \phi^{-1}(a')$.*

Super important, as it motivates normal subgroups in the next section.

6.2 Normal subgroups

Here it comes – quotient group time! They'll be fine with normal subgroups, but *not* with quotient groups. Furthermore, they'll see $aH = Ha$ and assume that means $ah = ha$ for all $h \in H$. You're going to have to be patient with this mistake, as it'll take time for them to absorb the difference between those two equations. You'll need at least 1.5 days on this topic, and you can combine this with the next section if need be.

Theorem 6.11. *Let G be a group and $H < G$. Then the binary operation on G/H given by $(aH)(bH) = (ab)H$ is well defined if and only if $gH = Hg$ for all $g \in G$.*

Man, will they struggle with this one, but it's essential that math majors know how to deal with this issue. Make sure they're very careful and precise with the proof. I usually have two students present this, one presenting one direction and another presenting the other direction.

Theorem 6.13. *Let G be a group and $H \lhd G$. Then G/H is a group under the operation $(aH)(bH) = (ab)H$.*

Once Theorem 6.11 is complete, this is pretty easy.

Exercise 6.14. It should be obvious that every subgroup of an abelian group is normal, which means that the quotient group G/H is defined for every subgroup H of an abelian group G. Let's practice some basic quotient group computations with abelian groups. We'll use some of the same subgroups from Exercise 5.2, so go back and review that first.

1. In the group $\mathbb{Z}/5\mathbb{Z}$, compute $(2 + 5\mathbb{Z}) + (4 + 5\mathbb{Z})$.
2. In the group $\mathbb{Z}_{12}/\langle 8 \rangle$, compute $(1 + \langle 8 \rangle) + (3 + \langle 8 \rangle)$.
3. In the group $U_8/\{\zeta_0, \zeta_4\}$, compute $(\zeta_2\{\zeta_0, \zeta_4\})(\zeta_3\{\zeta_0, \zeta_4\})$.
4. In the group $\mathbb{Z}[i]/H$, where $H = \langle \{2, 2i\} \rangle$, compute $(1 + H) + ((1 + i) + H)$.

Students have *got* to get messy with cosets. At the very least, have them work out problems 1 and 2 – for many students, that suffices.

Theorem 6.15. *Let G be a group and $H \lhd G$.*

1. *The element $aH \in G/H$ has finite order n if and only if n is the least positive integer such that $a^n \in H$.*
2. *If $a \in G$ has finite order k, then the element $aH \in G/H$ has finite order, and its order is a divisor of k.*
3. *If H has finite index $m = |G : H|$, then $a^m \in H$ for all $a \in G$.*

This is almost an essential theorem, but the results are only used sporadically. This is a good theorem to reinforce the concept of order in the context of quotient groups. If you spend extra time on quotient groups, this is great for presentation; otherwise, assign this for homework.

Exercise 6.16. Find the order of the coset in the given quotient group.

1. In the group $\mathbb{Z}/5\mathbb{Z}$, find the order of $3 + 5\mathbb{Z}$.
2. In the group $\mathbb{Z}_{12}/\langle 8 \rangle$, find the order of $2 + \langle 8 \rangle$.
3. In the group $U_8/\{\zeta_0, \zeta_4\}$, find the order of $\zeta_1\{\zeta_0, \zeta_4\}$.
4. In the group $\mathbb{Z}[i]/H$, where $H = \langle \{2, 2i\} \rangle$, find the order of $(1 + i) + H$.

Parts of this exercise are needed for students to put together the idea of order and how quotient groups work. Problems 1 and 2 really work well for that purpose.

Theorem 6.17. *Let G be a group and $H < G$. Then the following are equivalent:*

1. *H is normal in G.*
2. *$gHg^{-1} = H$ for all $g \in G$.*
3. *$ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.*

Have different students present different implications (except 2 implies 3, which is too easy for a presentation).

Exercise 6.18. We now have three ways to determine if a subgroup H is a normal subgroup of a group G : use the definition directly or either of the two conditions in the above theorem. Practice using them by determining if the given subgroup H is a normal subgroup of the nonabelian group G.

1. $G = GL_2(\mathbb{R}), H = SL_2(\mathbb{R})$.
2. $G = SL_2(\mathbb{Z}), H = \left\{ \begin{bmatrix} 2a+1 & 2b \\ 2c & 2d+1 \end{bmatrix} \in G \,\middle|\, a, b, c, d \in \mathbb{Z} \right\}$.
3. $G = GL_2(\mathbb{R}), H = \left\{ \begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix} \right\}$.
4. $G = GL_2(\mathbb{R}), H = \left\{ \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \in G \,\middle|\, k \in \mathbb{R} \right\}$.
5. $G = S_{\mathbb{R}}, H = \{f \in G \mid f(x) = ax + b, a, b \in \mathbb{R}, a \neq 0\}$.
6. $G = \{f \in S_{\mathbb{R}} \mid f(x) = ax + b, a, b \in \mathbb{R}, a \neq 0\}, H = \{f \in G \mid f(x) = x + b, b \neq 0\}$.

This exercise requires them not only to get messy, but it also helps their intuition as to a good criterion to use to detect normal subgroups.

Theorem 6.19. *Let G be a group and $\mathcal{H}$ be a nonempty collection of normal subgroups of G. Then $\bigcap_{H \in \mathcal{H}} H$ is a normal subgroup of G.*

This is also a good homework problem. Very straightforward.

Theorem 6.20. *Let G be a group and $H < G$. If $|G : H| = 2$, then $H \lhd G$.*

This is a good in-class discussion problem, but not really good for homework (if they don't see the idea, it's really hard to grade).

Theorem 6.21. *Let G be a group and H a finite subgroup of G of order n. If H is the only subgroup of order n, then $H \lhd G$.*

If you assign this for homework, you might want to give them a hint about using conjugation. If you skipped conjugation entirely, don't bother at all with this theorem.

Theorem 6.22. *The center of a group is a normal subgroup of G.*

Nice fact, good exercise, but not important.

Theorem 6.23. *Let G be a group. Then $Inn(G) \lhd Aut(G)$.*

If you had them prove that $Inn(G) < Aut(G)$, you might as well fill in this detail too. Otherwise, it's not needed.

6.3 The natural projection homomorphism

I once skipped this entire chapter (well, I assigned the first theorem), and everyone did just fine (it was a weaker than usual class). If you have to treat this briefly, that's fine, but try not to omit it entirely. You definitely don't need a full day for this.

Theorem 6.24. *Let $\phi : G \to G'$ be a group homomorphism. If $H \lhd G$, then $\phi(H) \lhd \phi(G)$, and if $H' \lhd \phi(G)$, then $\phi^{-1}(H') \lhd G$.*

They really need to see how inverse images work, especially in the context of subgroups.

Theorem 6.26. *Let G be a group and $H \lhd G$. Then the function $\phi : G \to G/H$ given by $\phi(g) = gH$ is a homomorphism with $Ker(\phi) = H$.*

This isn't hard, so you can discuss it in class. It's too easy to assign as a homework problem.

Theorem 6.28. *Let G be a group and $K \lhd G$. Let $\phi : G \to G/K$ be the natural projection homomorphism and H' a subgroup of G/K.*

1. *$H = \phi^{-1}(H')$ is a subgroup of G containing K, and if $H' \lhd G/K$, then $H \lhd G$.*
2. *$H' = H/K$.*
3. *If H' and K are both finite, then H is finite and $|H| = |H'| \cdot |K|$.*

This theorem, on the other hand, is a great one for homework (at least parts 1 and 2), and if you can squeeze this in for class presentation, it's really worthwhile.

Theorem 6.30. *Groups of prime order are simple.*

Too easy for homework. It's enough to discuss this in class.

Theorem 6.32. *Let G be a group and $H \lhd G$. Then G/H is simple if and only if H is a maximal normal subgroup of G.*

Boy, does this set up the parallel theorem on fields and quotient rings nicely. But creating simple groups this way comes out of nowhere, so it's probably best to go ahead and skip it.

Chapter 7

Cyclic Groups

Suggested time: 3 days.
Essential theorems for presentation: 7.4, 7.7, 7.9, 7.13, 7.16, 7.18, 7.23
Necessary theorems for later use: 7.3, 7.5, 7.6, 7.10, 7.11, 7.17.1, 7.21, 7.22
Optional theorems: 7.17.2
Important exercises: 7.8, 7.19

This big chapter is comparatively easy for students (with the exception of theorem 7.18), as they return briefly to the realm of the semi-familiar. Encourage them to review the group $\mathbb{Z}_n$ before this section. You can spend days and days getting every little detail accurate, so try to focus their attention on the most important issues. Spend no more than three days total on this chapter.

7.1 Properties of cyclic groups

This section simply gets students familiar with properties common to all cyclic groups. Nothing major here, but exercise 7.8 is especially helpful for students.

Theorem 7.3. *Let G be a cyclic group. If a is a generator of G, then so is a^{-1}.*

Just discuss this in class. It's not worth assigning for homework.

Theorem 7.4. *Let G be a cyclic group generated by a. If H is a nontrivial subgroup of G, then a^n is a generator of H, where n is the least positive integer such that $a^n \in H$.*

This gives students a way to identify at least one generator of a nontrivial subgroup of a cyclic group.

Corollary 7.5. *If G is a cyclic group, then every subgroup of G is cyclic.*

Have students explain this after the presentation of Theorem 7.2.

Theorem 7.6. *Let G be a cyclic group generated by a and $H < G$. Then G/H is cyclic and is generated by aH.*

This isn't hard, but students are anxious about quotient groups. You can either discuss this in class or perhaps give this for homework.

Theorem 7.7. *Let G be a cyclic group generated by a, and let G' be any group.*

1. *If a has infinite order, then for any $g' \in G'$, there exists a unique homomorphism $\phi : G \to G'$ such that $\phi(a) = g'$.*
2. *If a has finite order n, then for any $g' \in G'$ whose order divides n, there exists a unique homomorphism $\phi : G \to G'$ such that $\phi(a) = g'$.*

Two parts, two students. They'll probably need some nudges on how to define the homomorphism, and maybe a hint on how to prove the homomorphism is unique.

Exercise 7.8. Given the information below, determine if there exists a homomorphism ϕ between the groups indicated. If so, compute $\phi(3)$ and $Ker(\phi)$.

1. $\phi : \mathbb{Z} \to \mathbb{Z}_5$, given that $\phi(1) = 2$.
2. $\phi : \mathbb{Z}_5 \to \mathbb{Z}$, given that $\phi(1) = 2$.
3. $\phi : \mathbb{Z} \to \mathbb{Z}$, given that $\phi(2) = -1$.
4. $\phi : \mathbb{Z} \to \mathbb{Z}$, given that $\phi(-1) = 2$.
5. $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_5$, given that $\phi(1) = 4$.
6. $\phi : \mathbb{Z}_5 \to \mathbb{Z}_{20}$, given that $\phi(4) = 1$.
7. $\phi : \mathbb{Z} \to GL_2(\mathbb{R})$, given that $\phi(1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.
8. $\phi : \mathbb{Z}_4 \to GL_2(\mathbb{R})$, given that $\phi(1) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Students don't need to work all of these, but it gives them good practice in understanding how to evaluate homomorphisms defined in this way.

7.2 Infinite cyclic groups

Students who have taken Number Theory will love this section, especially the last theorem. The definition of greatest common divisor is hugely important, but the exercise that follows isn't really necessary.

Theorem 7.9. *Let G be an infinite cyclic group. If $a \in G$ is not the identity element, then the order of a is infinite, and if a generates G, then only a and a^{-1} generate G.*

This is a really good theorem for students to see how everything gets put together carefully.

Theorem 7.10. *Let G be an infinite cyclic group. Then $G \cong \mathbb{Z}$, and there are exactly two isomorphisms from G to $\mathbb{Z}$.*

This need not have a formal presentation, as the theorem is intuitive plausible. You can assign this for homework, or you can have someone define the isomorphisms and sketch why they work, and then have them discuss why there's only two isomorphisms possible.

Theorem 7.11. *The only subgroups of $\mathbb{Z}$ are $n\mathbb{Z}$, for all $n \in \mathbb{Z}$.*

Just have a quick discussion about this one.

Theorem 7.13. *Let $a, b \in \mathbb{Z}$, not both zero, and let $d \in \mathbb{Z}$. Then there exist integers x and y such that $d = ax + by$ if and only if d is a multiple of $\gcd(a, b)$. Furthermore, $|ab|/\gcd(a, b)$ is the least common multiple of a and b.*

This is the really important result of the section. If students get confused about the absolute value, allow them to prove this when a and b are both nonnegative.

7.3 Finite cyclic groups

This section will take them a bit longer, primarily because of how messy it can get. The Structure Theorem will take time, so you might want to have two or three students present different parts of this theorem. Students who have had a course in Number Theory should be slightly more comfortable with this section, of course. It's easy to get bogged down in this section, so if you need to save a bit of time, you could consider starting this section the day before to leave extra time.

Theorem 7.16. *Let G be a finite cyclic group of order n, and let a be a generator of G. Then a^k is a generator of G if and only if n and k are relatively prime.*

This really gets the ball rolling. The careful use of the definition of greatest common divisor and Theorem 7.9 should be stressed, as it makes everything work clearly and ties into the previous section.

Theorem 7.17. *Let G be a finite cyclic group of order n. Then $G \cong \mathbb{Z}_n$, and there are exactly k isomorphisms from G to $\mathbb{Z}_n$, where k is the number of integers in $\mathbb{Z}_n$ that are relatively prime to n.*

If you feel a formal presentation will help the class, then by all means do so. But the intuition on how to see the isomorphism rather than getting bogged down in details is frequently a better way to do this. Counting the number of isomorphisms is nice, but ultimately unnecessary.

Theorem 7.18 (The Structure Theorem of Finite Cyclic Groups)**.** *Let G be a finite cyclic group of order n generated by a, and let $k \in \mathbb{Z}$. Then the order of a^k is n/d, where $d = \gcd(k, n)$. Furthermore, for any $l \in \mathbb{Z}$, then $\langle a^l \rangle = \langle a^k \rangle$ if and only if $\gcd(l, n) = \gcd(k, n)$.*

This is difficult for most students. This lengthy but important theorem is best done with two or three people presenting it. Encourage them to use Theorems 4.28 and Corollary 4.29, as those theorems make the proof precise.

Exercise 7.19. These rather tedious exercises are quite important to understand the nature of the subgroups of a finite cyclic group. For each group listed below, please list its generators and all its subgroups, along with all the elements that generate each subgroup. Then draw a subgroup lattice for G which shows the nature of its subgroup relationships.

1. $G = \mathbb{Z}_7$
2. $G = \mathbb{Z}_{12}$
3. $G = \mathbb{Z}_{15}$
4. $G = \mathbb{Z}_{16}$
5. $G = \mathbb{Z}_{36}$
6. $G = \mathbb{Z}_{42}$

Creating a subgroup lattice is one of the best ways for students to solidify their understanding of how subgroups relate. This is especially true for finite cyclic groups, as constructing the lattice really highlights how prime factorizations dictate the lattice structures. You don't need to have students work all of them, but do give them a variety, including at least one "messy" one to play with!

Theorem 7.21. *Let G be a group of order p^k, where p is a prime and k is a positive integer. Then G has an element of order p.*

This is a great theorem for to assign for homework.

Corollary 7.22. *Any group of prime order p is cyclic and is isomorphic to $\mathbb{Z}_p$.*

A nice in-class remark is all that's needed here.

Theorem 7.23. *Let $n > 0$ be a positive integer. Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.*

This simple theorem continues to stump students, primarily because they're still developing their intuition as to what exactly quotient groups do. Emphasize the use of previous results to prove this theorem.

Chapter 8

Direct Products

Suggested time: Varies; 1 day minimum (plus 2 optional days).
Essential theorems for presentation: 8.7, 8.8, (8.11, 8.15, 8.22)
Necessary theorems for later use: 8.1, 8.4, 8.5.1, 8.9, (8.19, 8.20, 8.23, 8.24, 8.25)
Optional theorems: 8.5.2
Important exercises: 8.6, 8.10, (8.21, 8.26)

For many students, this will be the first time they will deal with products of sets in a meaningful way (or at all). It's not hard, but you should be prepared to nurse them through notation a bit. Believe it or not, the second section really helps students understand what quotient groups do; I focus almost entirely on computation rather than the theorems in that section. Three days are needed to do this chapter justice. However, it's worth noting that the CUPM recommendations don't include this material as part of the essential core of Abstract Algebra. So, if you're worried about having enough time to get to enough of Ring Theory, but you still want them to wrestle with product groups, just have students work through section 8.1 through Exercise 8.10, as Theorem 8.8 is (in my opinion) crucial for every math major to know and understand. If you choose this route, plan on 1.5 days for this material and 1.5 for the complementary material in Chapter 9, for 3 days total for the two chapters combined.

8.1 External direct products

The major theorem in this section is showing that the product of finite cyclic groups is cyclic iff the orders are relatively prime. It's not uncommon that this section will take a day and a half to work through. I advise using the first day focusing mostly on examples and the easy theorems, and the second day to really hammer home the remaining theorems.

Theorem 8.1. *Let $\langle G_1, *_1\rangle$ and $\langle G_2, *_2\rangle$ be groups. Then the binary structure $\langle G_1 \times G_2, *\rangle$ defined by $(g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$ is a group.*

Yes, its obviously a required theorem, but it doesn't need to be presented. Examples suffice.

Theorem 8.4. *Let G_1 and G_2 be groups.*

1. *If $H_1 \lhd G_1$ and $H_2 \lhd G_2$, Then $H_1 \times H_2 \lhd G_1 \times G_2$.*
2. *If G_1 is generated by A_1 and G_2 is generated by A_2, then $G_1 \times G_2$ is generated by the set $(A_1 \times \{e\}) \cup (\{e\} \times A_2)$.*
3. *If $G_1 \times G_2$ is generated by A, then G_1 is generated by $A_1 = \{a \in G_1 \,|\, (a, b) \in A \text{ for some } b \in G_2\}$ (and similarly for G_2).*

This really ought to be an essential theorem, but going through the details of a formal proof isn't the best way to see what's going on. Have them talk through a sketch of why it's true, and supplement with exercise 8.6.

Corollary 8.5. *Let G_1 and G_2 be groups.*

1. *$G_1 \times \{e\} \lhd G_1 \times G_2$.*
2. *$G_1 \times G_2$ is finitely generated if and only if G_1 and G_2 are finitely generated.*

Part 1 will come back in the next chapter, so at least mention it. Part 2 isn't worth your time.

Exercise 8.6. This exercise is a warning about a common misreading of the above theorem. Prove that $(1, 1)$ does *not* generate $\mathbb{Z} \times \mathbb{Z}$, and that $\mathbb{Z} \times \mathbb{Z}$ isn't cyclic. Then show that the set $\{(1, 0), (0, 1)\}$ does generate $\mathbb{Z} \times \mathbb{Z}$.

This important exercise clarifies how ordered pairs really work.

Theorem 8.7. *Let G_1 and G_2 be groups, and let $g_i \in G_i$ for $i = 1, 2$. If either g_1 or g_2 have infinite order, then so does $(g_1, g_2) \in G_1 \times G_2$. If g_1 has finite order n_1 and g_2 has finite order n_2, then the order of $(g_1, g_2) \in G_1 \times G_2$ is the least common multiple of n_1 and n_2.*

This leads right into the big Theorem 8.8.

Theorem 8.8. *Let m and n be positive integers. Then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.*

This needs to be presented very precisely. Getting the details correct here is essential. (They'll see this idea again with orders of permutations.)

Corollary 8.9. *$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if m and n are relatively prime.*

Definitely draw their attention to this *huge* fact after the big proof of Theorem 8.8. The exercises that follow will help flesh out its utility.

Exercise 8.10. In each exercise, two groups are given. Decide if they are isomorphic or not.

1. $G_1 = \mathbb{Z}_4; \quad G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$.
2. $G_1 = \mathbb{Z}_6; \quad G_2 = \mathbb{Z}_2 \times \mathbb{Z}_3$.
3. $G_1 = \mathbb{Z}_3 \times \mathbb{Z}_4; \quad G_2 = \mathbb{Z}_2 \times \mathbb{Z}_6$.
4. $G_1 = \mathbb{Z}_6 \times \mathbb{Z}_{15}; \quad G_2 = \mathbb{Z}_3 \times \mathbb{Z}_{30}$.
5. $G_1 = \mathbb{Z}_{12} \times \mathbb{Z}_{36}; \quad G_2 = \mathbb{Z}_3 \times \mathbb{Z}_{12} \times \mathbb{Z}_{12}$.
6. $G_1 = \mathbb{Z}_{165} \times \mathbb{Z}_{182}; \quad G_2 = \mathbb{Z}_{26} \times \mathbb{Z}_{33} \times \mathbb{Z}_{35}$.

This really pushes students to understand the meaning of the previous theorem and its corollary. Have them work most (if not all) of these problems.

Theorem 8.11. *Let G_1, G_2 be cyclic groups generated by a_1, a_2, respectively, and let H be any group. Then for any $h_1, h_2 \in H$ (with order a divisor of the order of a_1 or a_2, when a_1 or a_2 have finite order) with $h_1h_2 = h_2h_1$, there exists a unique homomorphism $\phi : G_1 \times G_2 \to H$ such that $\phi(a_1, e_2) = h_1$ and $\phi(e_1, a_2) = h_2$.*

This theorem really, really helps students define homomorphisms on their own, so it needs presentation. Make sure they understand the exercise that follows, too.

8.2 Finitely generated abelian groups

I've always been ambivalent about this section of the book. On the one hand, I've tried to improve student understanding by including some nice motivating theorems. On the other hand, what I crave most for students to experience is the computation using the Fundamental Theorem, rather than a deep understanding of the proof. Hence, I've always come down on the side of vigorous hand waving, with lots and lots of computation (like exercise 8.26.) In particular, the proofs of Theorems 8.23 and 8.24 are beyond the capabilities of most students at this point, so simply state the result without proof and have them understand its meaning through the exercise that follows.

Theorem 8.15. *Let G be an abelian group. If T is the set of all elements of G with finite order, then T is a subgroup of G.*

This is an easy theorem that preps them for what's coming. Have students highlight where they use the fact that G is abelian, since this theorem isn't necessarily true for non-abelian groups.

Theorem 8.19. *Let G be an abelian group of order p^2, where p is a prime. If $a \in G$ generates a cyclic subgroup H of order p, then for any $b \notin H$, the p distinct cosets of H in G are $\{H, bH, b^2H, \ldots, b^{p-1}H\}$.*

You might even skip this; you only need it for the messy details of what follows.

Theorem 8.20. *Let G be an abelian group of prime power order p^k. Then G is isomorphic to a direct product of cyclic groups $\mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \cdots \times \mathbb{Z}_{p^{k_n}}$, where $k_1 + k_2 + \cdots + k_n = k$.*

This is a good theorem to discuss, but not to prove, as the proof is very, very difficult (I've not provided a proof in the instructor's guide, although a proof is technically possible with the tools they have at this point). They'll use this a lot in applying the Fundamental Theorem, so justify it intuitively.

Exercise 8.21. How many abelian groups of order 8 are there? Of order 81?

It's simple, but it prepares them for the important computations to come.

Lemma 8.22. *Let G be an abelian group. Then for each prime p, the set of elements whose order is a power of p forms a subgroup of G.*

Again, another straightforward theorem.

Theorem 8.23 (The Fundamental Theorem of Finite Abelian Groups)**.** *Let G be a finite abelian group of order $|G| = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, where $p_1, \ldots, p_n$ are distinct primes. Then there exist unique groups $H_{p_1}, H_{p_2}, \ldots, H_{p_n}$ such that*

$$G \cong H_{p_1} \times H_{p_2} \times \cdots \times H_{p_n}$$

where the group H_{p_i} is a direct product of cyclic groups $H_{p_i} = \mathbb{Z}_{p_i^{k_1}} \times \mathbb{Z}_{p_i^{k_2}} \times \cdots \times \mathbb{Z}_{p_i^{k_n}}$, where $k_1 + k_2 + \cdots + k_n = a_i$.

The book itself doesn't expect students to prove this theorem. I've provided a proof in the case of groups of order the product of two primes, in case you really want students to have a glimpse of what it takes. But it not reasonable to ask students to prove this one, and proving this for the students for the sake of rigor isn't warranted.

Theorem 8.24 (The Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let G be a finitely generated abelian group with torsion subgroup T. Then there exists a unique integer $b \geq 0$ such that $G \cong T \times \mathbb{Z}^b$.*

Emphasize that there's a torsion part and an infinite part. As before, a proof just isn't a viable option, nor is it even desirable at this level.

Corollary 8.25. *Every finitely generated abelian group is a product of cyclic groups.*

A nice summary statement of what just happened.

Exercise 8.26. A very scant description of an abelian group G is given below. Based on the information given, identify all possible finitely generated abelian groups, if any, to which the group G might be isomorphic.

1. $|G| = 11$.
2. $|G| = 25$.
3. $|G| = 35$; G is not cyclic.
4. $|G| = 48$; G is not cyclic.
5. $|G| = 64$; every element of G has order 1 or 2.
6. $|G| = 90$; every element of G has order $1, 2, 3, 4$, or 5.
7. $G \cong T \times \mathbb{Z}^b$; $|T| = 120$; $\mathbb{Z}^b$ is cyclic.
8. $G \cong T \times \mathbb{Z}^b$; $|T| = 210$; $\mathbb{Z}^b$ does not need more than 3 generators.

If you've decided to cover this section, then solving these kinds problems is probably your goal of the section. Hence, I'd have students work all of these.

Chapter 9

The Isomorphism Theorems

Suggested time: Varies; 1 day minimum (with up to 2 optional days).
Essential theorems for presentation: 9.1, 9.4, (9.5, 9.6, 9.10, 9.12), 9.15
Necessary theorems for later use: 9.2, (9.11, 9.13)
Optional theorems: 9.7, 9.18, 9.19, 9.21, 9.22
Important exercises: (9.14, 9.17)

Of the isomorphism theorems, the only important one for a first semester of Abstract Algebra at the undergraduate level is the First Isomorphism Theorem. You can skip section 3 entirely, as the only material relevant to a first course in abstract algebra in this chapter is in the first two sections. In that case, while in theory you can cover these sections in two days, experience has shown students really need three days to absorb what's happening. On the other hand, if you skipped product groups entirely, then all you need have the students work on is section 1. In that case, plan on 1.5 days for this material, for a total of 3 days for sections 8.1 and 9.1 combined.

9.1 The First Isomorphism theorem

This first section isn't too bad. It continues the development of how to think about quotient groups, with the obvious main theorem proved right off the bat.

Theorem 9.1 (The First Isomorphism Theorem)**.** *Let $\phi : G \to G'$ be a homomorphism with kernel K. Then the function $\overline{\phi} : G/K \to \phi(G)$ given by $\overline{\phi}(gK) = \phi(g)$ is a well-defined isomorphism.*

Make sure everyone understands the proof, especially the part about the map being well-defined.

Corollary 9.2. *Let $\phi : G \to G'$ be a surjective homomorphism with kernel K. Then G' is isomorphic to G/K.*

It's easy enough to talk through this one without presenting it.

Theorem 9.4. *Let G be a group with identity e. Then $G/G \cong \{e\}$ and $G/\{e\} \cong G$.*

As easy as this is, this theorem (and the next, if you covered section 8.1) are excellent applications of Corollary 9.2. The main thrust of these theorems is to force the students to come up with the relevant surjective homomorphisms on their own. After all, if you tell them what to use, then the First Isomorphism Theorem (FIT) tells them what to do with it.

Theorem 9.5. *Let G_1 and G_2 be groups, with e' the identity of G_2. Then $(G_1 \times G_2)/(G_1 \times \{e'\}) \cong G_2$.*

This too is just an application of the First Isomorphism Theorem.

Theorem 9.6. *Let G_1 and G_2 be groups, with e' the identity of G_2. If $H \lhd G_1$, then $(G_1 \times G_2)/(H \times \{e'\}) \cong (G_1/H) \times G_2$.*

This is a good one to help then develop an understanding what the process of quotienting out by a subgroup does.

Theorem 9.7. *Let G be a group. Then $G/Z(G) \cong Inn(G)$.*

This makes the intuition from Exercise 5.25 precise, if you covered that material.

9.2 Quotients of finitely generated abelian groups

Theorem 9.15 should be covered regardless, but only cover the rest of this section if you also covered Section 8.1, of course. Be prepared for a *lot* of confusion, but the point of this section is to expose their continued trepidation with quotient groups and to help them finally come to terms with what a quotient group does. A really good way to do this is spend one day on products of infinite cyclic groups, and if you covered section 8.2, you can then spend the next day on products of finite cyclic groups.

Exercise 9.9. Before attempting the following theorem, prove that $\mathbb{Z} \times \mathbb{Z}/\langle (1,1) \rangle \cong \mathbb{Z}$.

This exercise helps them to see what's coming. Don't skip it.

Theorem 9.10. *Let $n \in \mathbb{Z}$. Then $\mathbb{Z} \times \mathbb{Z}/\langle (n,1) \rangle \cong \mathbb{Z}$.*

The exercise just before this is a really good computation that might get them to think about this theorem's proof.

Theorem 9.11. *Let $a, b \in \mathbb{Z}$ be relatively prime integers. Then $\mathbb{Z} \times \mathbb{Z}/\langle (a,b) \rangle \cong \mathbb{Z}$.*

Once they've got Theorem 9.10 done, see if they can modify its proof just enough to justify this theorem.

Theorem 9.12. *Let $n \in \mathbb{Z}^+$. Then $\mathbb{Z} \times \mathbb{Z}/\langle (n,n) \rangle \cong \mathbb{Z}_n \times \mathbb{Z}$.*

Same issue, but trickier. Don't be surprised if they don't get this one; you might give them the homomorphism that works.

Theorem 9.13. *Let $a, b \in \mathbb{Z}$ be integers, and let $d = \gcd(a,b)$. Then $\mathbb{Z} \times \mathbb{Z}/\langle (a,b) \rangle \cong \mathbb{Z}_d \times \mathbb{Z}$.*

Much harder to do, but see if they can modify the proof of the previous theorem. Like before, if you want, you might give them the homomorphism that works.

Exercise 9.14. Classify the following according to the Fundamental Theorem of Finitely Generated Abelian Groups.

1. $\mathbb{Z} \times \mathbb{Z}/\langle(0,7)\rangle$
2. $\mathbb{Z} \times \mathbb{Z}/\langle(1,7)\rangle$
3. $\mathbb{Z} \times \mathbb{Z}/\langle(3,7)\rangle$
4. $\mathbb{Z} \times \mathbb{Z}/\langle(7,7)\rangle$
5. $\mathbb{Z} \times \mathbb{Z}/\langle(14,21)\rangle$
6. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/\langle(1,1,0)\rangle$
7. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/\langle(1,1,1)\rangle$
8. $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/\langle(2,2,2)\rangle$

Even if the students didn't come up with proofs of the relevant theorems, it's still worth having students work through this exercise.

Theorem 9.15. *Let n be a positive integer, and let $a \in \mathbb{Z}_n$. If $d = \gcd(a,n)$, then $\mathbb{Z}_n/\langle a\rangle \cong \mathbb{Z}_d$.*

This theorem is worth presenting, as it only relies on Chapter 7.

Exercise 9.17. Use the Fundamental Theorem of Finite Abelian Groups to classify the following quotient groups.

1. $G = \mathbb{Z}_3 \times \mathbb{Z}_{12}/\langle(0,8)\rangle$
2. $G = \mathbb{Z}_2 \times \mathbb{Z}_4/\langle(1,2)\rangle$
3. $G = \mathbb{Z}_4 \times \mathbb{Z}_6/\langle(2,3)\rangle$
4. $G = \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8/\langle(1,2,4)\rangle$

This gives needed practice in applying what the previous theorems provide, even if they didn't prove them.

9.3 The Second and Third Isomorphism theorems

For a first semester course, this entire section is optional, unless you're doing a groups-only course. In that case, spend a day on these four theorems. Emphasize the careful and precise use of the First Isomorphism Theorem in their proofs.

Lemma 9.18. *Let G be a group and H, K be subgroups of G. Then if either H or K is normal in G, then the set $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup of G, and if both H and K are normal in G, then HK is normal in G.*

This is a great, straightforward lemma.

Theorem 9.19 (The Second Isomorphism Theorem)**.** *Let G be a group and H, K be subgroups of G. If $K \lhd G$, then $(HK)/K \cong H/(H \cap K)$.*

Because both groups are quotient groups, it's not clear exactly how to use the First Isomorphism Theorem. One way to do it requires them to prove their map is well-defined, so if they do it that way, don't let them brush over that issue.

Lemma 9.21. *Let G be a group and H, K be normal subgroups of G. If $K \lhd H$, then $H/K \lhd G/K$.*

Another straighforward computation, but because it's about quotient groups, students will likely get anxious.

Theorem 9.22 (The Third Isomorphism Theorem)**.** *Let G be a group and H, K be normal subgroups of G. If $K \lhd H$, then $(G/K)/(H/K) \cong G/H$.*

This is a really good one to help them get insight into quotient groups.

Chapter 10

The Symmetric Groups

Suggested time: 2 days.
Essential theorems for presentation: 10.6, 10.10, 10.13, 10.14, 10.15
Necessary theorems for later use: 10.2
Optional theorems: 10.8, 10.12
Important exercises: 10.4, 10.5, 10.9

This chapter isn't too bad for students and can be covered easily in two days (and even one day if you skip Cayley's Theorem). Even the proofs are mostly computational, and students usually enjoy the relief of the intense theory they just got through.

10.1 Permutations

Don't spend an entire day on this one section. Combine it with part or all of the next.

Theorem 10.2. *Let A be a set. The binary structure $\langle S_A, \circ \rangle$ given by function composition is a group.*

Mention to them that this was proved in Example 3.2, so don't have them present it. It's here just for completion and context.

Exercise 10.4. It's important to remember that our objects in S_n are bijections, and that our operation on those objects is function composition. Practice this operation by finding the order and the inverse of the given permutation $\sigma \in S_n$ for some $n \geq 5$.

1. $\sigma(1) = 2, \sigma(2) = 1, \sigma(a) = a$ for all other $a \in \{1, 2, \ldots, n\}$.
2. $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1, \sigma(a) = a$ for all other $a \in \{1, 2, \ldots, n\}$.
3. $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 3, \sigma(a) = a$ for all other $a \in \{1, 2, \ldots, n\}$.
4. $\sigma(1) = 2, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 5, \sigma(5) = 3, \sigma(a) = a$ for all other $n \in \{1, 2, \ldots, n\}$.

I like this "messy" exercise, so that student come to crave a simple notation that they'll get in the next chapter.

Exercise 10.5. To help us understand how a symmetric group's elements behave, let's really dig into the symmetric group S_3. In a manner similar to Exercise 10.4, list all the permutations that constitute the group S_3. What is the order of S_3? Is S_3 abelian?

This is a classic exercise to get them to apply everything they've learned about groups so far.

Theorem 10.6. *Let A be a set with n elements. Then S_A is isomorphic to S_n, and the order of S_A is $n!$.*

This simple theorem sets the stage for the notation to come.

Theorem 10.8. *Let $n \geq 3$ be an integer. Then the center $Z(S_n)$ of S_n is trivial.*

While this theorem isn't important for the theorems that follow, it does let the students know how highly noncommutative permutations groups are.

10.2 Dihedral groups

Use lots and lots of pictures to guide the discussion and the theory here. Make sure the students see the connection between geometric transformations and permutations.

Exercise 10.9. Let's make sure you've got a good grip on your geometry by exploring D_3, the symmetries of a triangle, and D_4, the symmetries of a square.

1. D_3 has six elements: the trivial rotation, two nontrivial rotations, and three reflections. Find the orders of each of these six elements. Then show that if you take two different reflections in D_3, their product (composition) is an element of D_3 with order 3. Is D_3 closed under composition?

2. D_4 has eight elements: the trivial rotation, three nontrivial rotations, and four reflections. Find the orders of each of these eight elements. If you take two different reflections in D_4, what are the various orders you can come up with for their product? Is D_4 closed under composition?

Do you have a conjecture about the orders of rotations and reflections in D_n? What about a conjecture for the product of two reflections in D_n? Do you think that D_n is closed under composition?

Theorem 10.10. *Let $n \geq 3$ be an integer. Then D_n is a subgroup of S_n of order $2n$.*

This theorem allows everyone to see how symmetries can be described using permutations. I wouldn't worry too much about technical accuracy; using well-explained pictures is a really good idea.

Theorem 10.12. *Let $n \geq 3$ be an integer. Then any reflection of P_n is not in $Z(D_n)$. In particular, D_n is not abelian for all $n \geq 3$.*

Just use a geometric argument to show that D_n isn't abelian. The fact that reflections aren't in the center isn't crucial.

Theorem 10.13. *Let n be a positive integer. Then the subset of all rotations of P_n is a cyclic subgroup of D_n of order n.*

This nice theorem allows everyone to see how a particular subcollection of transformations is encoded in a cyclic subgroup. Definitely present this.

10.3 Cayley's theorem

This is the one section that really requires a lot of motivation. There's nothing natural that Cayley's theorem answers that came before, so for students it really seems like a result in search of a problem. It's not at all unreasonable to skip this result now and cover it in a second semester when discussing group actions.

Lemma 10.14. *Let G be a group. For each $g \in G$, define $\lambda_g : G \to G$ by $\lambda_g(x) = gx$, and let $\Lambda = \{\lambda_g \mid g \in G\}$. Likewise, for each $g \in G$, define $\rho_g : G \to G$ by $\rho_g(x) = xg$, and let $P = \{\rho_g \mid g \in G\}$. Then both Λ and P are subgroups of S_G.*

This lemma does all the heavy lifting for Cayley's theorem.

Theorem 10.15 (Cayley's Theorem)**.** *Let G be a group. Then G is isomorphic to a subgroup of S_G. In particular, every finite group of order n is isomorphic to a subgroup of S_n.*

If they see how to use the lemma, it's pretty easy.

Chapter 11

Alternating Groups

Suggested time: 3 days for sections 1-3.
Essential theorems for presentation: 11.6, 11.7, 11.8.1, 11.17, 11.18, 11.24, 11.27
Necessary theorems for later use: 11.2, 11.8.2, 11.14, 11.15, 11.19, 11.26, 11.28
Optional theorems: (11.22, 11.29, 11.32, 11.33, 11.34, 11.36, 11.38, 11.39, 11.40, 11.41, 11.42, 11.43)
Important exercises: 11.4, 11.10, 11.11, 11.16, 11.21, (11.44, 11.45)

This chapter is a great way to end group theory, as it's a combination of computation and theory. You can do the first three sections in two days if you push, but it's best done over the span of three days. Sections 11.4 and 11.5 are there for completeness, or for the students who just want to do it, so you can save those two sections for a second semester.

11.1 Orbits and cycles

This sets terminology, notation, etc. If you need, you can skip the theory in favor of computational justifications. But the exercises are the key thing for the students to understand best.

Theorem 11.2. *Let A be a set, and let $\sigma \in S_A$. Then the relation $\sim$ on A defined by*

$$a \sim b \text{ if and only if } b \text{ is in the orbit of } a \text{ under } \sigma$$

is an equivalence relation on A whose equivalence classes are the orbits of the elements of A under σ.

You can just talk through this one. No presentation is needed.

Exercise 11.4. List all the orbits of the given element of S_6. Which are cycles? Which are transpositions?

1. $f(1) = 5, f(2) = 2, f(3) = 1, f(4) = 6, f(5) = 3, f(6) = 4.$
2. $f(1) = 2, f(2) = 4, f(3) = 1, f(4) = 5, f(5) = 6, f(6) = 3.$
3. $f(1) = 1, f(2) = 5, f(3) = 3, f(4) = 6, f(5) = 2, f(6) = 4.$
4. $f(1) = 4, f(2) = 2, f(3) = 3, f(4) = 1, f(5) = 5, f(6) = 6.$
5. $f(1) = 3, f(2) = 1, f(3) = 6, f(4) = 4, f(5) = 5, f(6) = 2.$
6. $f(1) = 1, f(2) = 2, f(3) = 3, f(4) = 4, f(5) = 5, f(6) = 6.$

This messy exercise preps students well for why cycle notation is so nice.

Theorem 11.6. *Let A be a set, and let $\sigma, \tau \in S_A$ be disjoint cycles. Then $\sigma\tau = \tau\sigma$.*

This is a good theorem to see how the definitions work.

Theorem 11.7. *Every permutation of a finite set is a product of disjoint cycles, and this product is unique up to the order of the cycles.*

This is a bigger theorem than it seems at first. It requires students to identify the orbits as the candidates for the decomposition into a product of cycles. Be generous with this presentation, so they don't get bogged down in notation. But *do* ask them where they used the fact that A is finite. You could even ask them to give an example of a permutation of the integers that isn't a product of cycles (for instance, the permutation that swaps each even integer and its its successor).

Theorem 11.8. *Let A be a set and let $\sigma \in S_A$. If σ is a cycle of finite length, then the order of σ is its length. If σ is the product of disjoint cycles $\sigma_1, \sigma_2, \ldots, \sigma_n$, of finite length, then the order of σ is the least common multiple of the length of the cycles $\sigma_1, \sigma_2, \ldots, \sigma_n$.*

The first part of this theorem asks students to understand how to apply the order of an element in this context, so its presentation is very useful. For the second part, though, you can just talk with them about how this is identical to the order of an ordered pair in a product group, if you covered that material.

Exercise 11.10. Your turn. Write each of the following as a product of disjoint cycles.

1. $(3, 5, 7, 2, 1)(5, 6, 3, 4)$
2. $(6, 2, 1, 4)(2, 8, 4, 1, 3)(3, 1, 2, 6, 4, 8)$
3. $(2, 1, 5, 4)(1, 3)(1, 2, 4, 5)$
4. $(1, 2, 3, 4, 5, 6)^4$

This is necessary practice with the notation. Don't skip it.

Exercise 11.11. What is $(a_0, a_1, \ldots, a_{k-1})^{-1}$? Prove your conclusion.

This exercise asks students to have a modicum of comfort with abstractly writing down a cycle and then proving something about it. It's worth having them work it out.

11.2 Transpositions and the parity of a permutation

The only hard part about this section is the proving that the parity of a permutation is well-defined. The proof is interesting, but not essential. You can wave your hands, if you really need to (see the recommendations from the CUPM).

Lemma 11.14. *For $n > 1$, the cycle $(a_1, a_2, \ldots, a_n)$ can be written as*

$$(a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \cdots (a_1, a_2)$$

and as

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2)(a_2, a_3) \cdots (a_{n-1}, a_n).$$

It's just a computation. No need to present it.

Theorem 11.15. *Every permutation of a finite set is a product of transpositions.*

Again, it follows from Theorem 11.7 and the lemma. No need to present.

Exercise 11.16. Express the identity permutation as a product of transpositions in as many different ways as you can. Ensure that in at least one of your expressions, no transposition appears twice in the product.

This exercise motivates why there's something to prove about the parity of a permutation. Regardless of if you have students prove that fact, students should work through this exercise.

Lemma 11.17. *Let $\sigma \in S_n$ be a cycle. If $\tau \in S_n$ is a transposition, then the number of orbits of $\sigma\tau$ is either one more or one less than the number of orbits of σ.*

Although this lemma as stated is correct, it's incomplete as a fully useful tool for the following theorem. (In other words, think of this lemma's statement as having a typo.) I advise modifying the hypothesis of the lemma as follows:

Let $\sigma \in S_n$ be a permutation.

Now, a proof of this lemma will almost certainly get messy. I suggest you let students get creative here and allow them to be more intuitive than rigorous (but not entirely unjustified either). In particular, good diagrams can be more effective than a careful proof.

Theorem 11.18. *The identity permutation of S_n cannot be written as the product of an odd number of transpositions.*

This follows nicely from the lemma.

Corollary 11.19. *A permutation of a finite set cannot be written as a product of both an odd and an even number of transpositions.*

It follows from the previous theorem, so just discuss it.

Exercise 11.21. Write each permutation as a product of transpositions and classify each as either an even or odd permutation.

1. $(1,3,4,7,2)(5,6)$
2. $(1,2,3,4,5,6)^4$
3. $(1,2,3,4)(2,3,4,5)(3,4,5,1)(4,5,1,2)(5,1,2,3)$
4. $(1,2,3)(2,3,4)(3,4,5)(4,5,1)(5,1,2)$

This is a necessary exercise to get them to apply what they've learned.

11.3 The alternating group

This section has some good results. It's not unreasonable to combine this section with the previous one.

Theorem 11.22. *Let n be a positive integer, and let U_2 be the group $\{-1,1\}$ under multiplication. Then the function $sgn : S_n \to U_2$ given by $sgn(\sigma) = \begin{cases} 1, & \sigma \in A_n \\ -1, & \sigma \in B_n \end{cases}$ is a homomorphism with kernel A_n.*

It's a nice fact, but a peripheral one. It's here mostly because the signum map is used sporatically outside the subject, and being familiar with the concept of the sign of a permutation is useful. It makes the next theorem super simple, but if you skip this theorem, the next theorem is still pretty easy (just tedious).

Corollary 11.24. *A_n is a subgroup of S_n.*

It's absolutely essential that this gets presented. It's not hard, but the alternating group is what this section's all about.

Lemma 11.26. *Let $n > 1$ be an integer, and let $\tau \in S_n$ be any transposition. Then the function $f : A_n \to B_n$ given by $f(\sigma) = \sigma\tau$ is a bijection.*

Really straightforward; if you're pressed for time, a sketch can suffice. But this simple lemma is needed for the more important theorem that follows, so don't skip it entirely.

Theorem 11.27. *Let $n > 1$ be an integer. Then $|A_n| = |B_n| = \dfrac{n!}{2}$.*

These combinatorial arguments are really good for students to see. Definitely have them present this.

Corollary 11.28. *Let $n > 1$ be an integer. Then $A_n \lhd S_n$, and $S_n/A_n \cong \mathbb{Z}_2$.*

Remind them how this follows from Theorem 6.22, but don't bother with a presentation.

Theorem 11.29. *Every even permutation is a product of cycles of length three.*

This theorem is just a nice parallel to Theorem 11.6, but it isn't useful for students.

11.4 Generating sets for symmetric groups

At best, mention this to them in class, or have them just read the theorems on their own. Unless you're taking a groups-only approach, don't assign work from this section; just skip it. Rather, come back to this (and the next section) in a second semester course in Abstract Algebra.

Lemma 11.30. *S_n is generated by the set $\{(1,2),(2,3),\ldots,(n-1,n),(n,1)\}$.*

This is a first simplification of how to create permutations.

Lemma 11.31. *Let $n > 2$ be an integer. Then*

$$(1,2,\cdots,n)^m(1,2)(1,2,\cdots,n)^{-m} = (1+m, 2+m)$$

for any integer $0 \leq m < n-1$, and

$$(1,2,\cdots,n)^{-1}(1,2)(1,2,\cdots,n) = (n,1).$$

This is a technical lemma that sets up the big theorem that comes next.

Theorem 11.32. *Let $n > 1$ be an integer. Then S_n is generated by the set $\{(1,2),(1,2,\ldots,n)\}$.*

This is the classic result that makes this section worthwhile.

Theorem 11.36. *Let $n > 2$ be an integer.*

1. *If n is even, then D_n is generated by the set*
$$\{(1,2,\ldots,n),(1,n-1)(2,n-2)\cdots(\frac{n}{2}-1,\frac{n}{2}+1)\}.$$
2. *If n is odd, then D_n is generated by the set*
$$\{(1,2,\ldots,n),(1,n-1)(2,n-2)\cdots(\frac{n-1}{2},\frac{n+1}{2})\}.$$

A technically precise and correct algebraic proof really obscures what's going on. The better way to prove this is with pictures. After all, getting every rotation is easy; getting every reflection is harder. Pictures are the key here, and I'd encourage geometric proofs, justified with algebra. Indeed, showing how conjugation has a geometric interpretation makes such an approach really worthwhile.

11.5 The simplicity of A_5

In a one-semester course that covers both groups and rings, there's just no time for this section. You can safely skip it entirely and return to it in a second course.

Lemma 11.37. *Let $\sigma \in A_5$. Then σ is either the trivial element, a cycle of length 3, a cycle of length 5, or a product of two disjoint transpositions.*

This sets the stage for the analyzing the various elements.

Lemma 11.38. *Let $\sigma = (a_1, a_2, a_3, a_4, a_5) \in A_5$ be a cycle of length 5, and let $\rho = (a_1, a_2)(a_3, a_4)$. Then $\rho\sigma\rho^{-1}$ is a cycle of length 5, and $(\rho\sigma\rho^{-1})\sigma$ is a cycle of length 3.*

This one gets us ready to deal with conjugates.

Lemma 11.39. *If $\sigma \in A_5$ is a product of two disjoint transpositions, and if $\rho \in A_5$ is a product of two disjoint transpositions, then σ and ρ are conjugate in A_5.*

Yes, you can simply compute all conjugates of σ and discover you get every other product of two disjoint transpositions, but that's not really insightful. A clever student (hopefully) might try something like the proof I've provided in the solutions manual.

Theorem 11.40. *Any nontrivial normal subgroup of A_5 contains a cycle of length 3.*

There's the first key insight!

Lemma 11.41. *Any two cycles of length 3 in A_5 are conjugate in A_5.*

And now we've got conjugates in the mix!

Theorem 11.42 (The Simplicity of A_5)**.** *A_5 is a simple group.*

If they've made it this far, they can put all the pieces together.

Exercise 11.43. Consider the permutation $\sigma = (1,2,3)(2,3,4) \in A_5$. Let's use this permutation to demonstrate how some of the above lemmata work.

1. Express σ as a cycle of length 3, a cycle of length 5, or a product of two disjoint transpositions.
2. Next, show that $\rho = (1,2)(3,5)$ is a conjugate of σ in A_5.
3. Now show that $\tau = \rho\sigma$ is a cycle of length 3.
4. Finally, explicitly show that every cycle of length 3 is a conjugate of τ in A_5.

This exercise forces them to get messy and see how to track through the lemmata.

Exercise 11.44. This time, consider the permutation $\sigma = (1,2,3)(3,4,5) \in A_5$.

1. Express σ as a cycle of length 3, a cycle of length 5, or a product of two disjoint transpositions.
2. Next, show that $\rho = (1,4,3,5,2)$ is a conjugate of σ in A_5.
3. Now show that $\tau = \rho\sigma$ is a cycle of length 3.

Same idea, but now with different cases.

Part III

Ring Theory

Chapter 12

Rings

Suggested time: 3 days.
Essential theorems for presentation: 12.5, 12.9.1, 12.23, 12.31.3, 12.31.4, 12.35
Necessary theorems for later use: 12.6, 12.7, 12.9.2, 12.9.3, 12.11, 12.19, 12.21, 12.27, 12.31.1, 12.31.2, 12.32, 12.33
Optional theorems: 12.15, 12.17
Important exercises: 12.13, 12.22, 12.24, 12.36

Believe it or not, getting students comfortable with rings isn't as hard as it was with groups, precisely because of their experience with groups. Of major importance is the emphasis on the distributive laws, which I require students to cite each and every time it's used in a proof. Furthermore, since many of the results parallel those from groups, many of the theorems may be skipped in their entirety, as students frequently can repeat the ideas from group theory. This chapter and the three that follow require one week each, at most.

12.1 Basic Properties of Rings

This introductory section gives the basic definitions and properties of rings, of course. Believe it or not, the focus here is not on the theory, but rather on the contrast between rings and groups, which students discover through the examples and exercises. Expect to discuss more than usual. Since subrings are less important (right now) than subgroups, proofs many theorems given here can be omitted without loss of content.

Theorem 12.5. *Let R be a ring, and let $a, b \in R$.*

1. $a\mathbf{0} = \mathbf{0}a = \mathbf{0}$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(na)b = a(nb) = n(ab)$ *for all* $n \in \mathbb{Z}$.

This is an excellent theorem to force students to use the Distributive Law(s) accurately. You can decide if you want them to do a formal induction on part 3 or not (I personally think the induction is worth the time, as it really demonstrates the difference between the laws of coefficients and the distributive laws).

Corollary 12.6. *Let R be a ring, and let $a, b \in R$.*

1. $(-a)(-b) = ab$.
2. *If R has unity, then* $(-\mathbf{1})a = -a$.
3. *If R has unity* $\mathbf{1} \neq \mathbf{0}$, *then* $\mathbf{0}$ *is never a unit.*

Discuss these results, and emphasize part 3.

Theorem 12.7. *If R is a ring with unity, then the set of all units of R forms a group under the operation induced by ring multiplication.*

Have them discuss a proof sketch.

Theorem 12.9. *Let R be a ring.*

1. *Let $a, b \in R$. Then $(a+b)^2 = a^2 + 2ab + b^2$ if and only if $ab = ba$.*
2. *$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$ for all $a_i, b_j \in R$.*
3. *If R is a commutative ring, then $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$ for all integers $n \geq 1$, where $a^n b^0 = a^n$ and $a^0 b^n = b^n$.*

Part 1 of this theorem really needs a presentation to see why their high school rules rely on commutative rings. Part 2 isn't too bad, and presenting a proof is less enlightening that the discussion about its meaning. But the real reason to avoid presenting part 3 is the messy notation. A proof by induction for part 3 requires them to also know facts about binomial coefficients, which most students probably won't know. That means that a combinatorial approach, explaining how many times the element $a^{n-i}b^i$ appears, will be a much better way to understand the binomial theorem.

Theorem 12.11. *Let R be a ring and S a subset of R. Then S is a subring of R if and only if S is an additive subgroup of R and S is closed under multiplication.*

Have them come up the a sketch of the proof. It's easy.

Exercise 12.13. Be careful not to assume that everything you know about subgroups is the same for subrings. Consider the ring $R = \mathbb{Z} \times \mathbb{Z}$ and the subset $S = \mathbb{Z} \times \{0\}$. Show that R has a unity element, that S is a subring of R, that the unity element of R is not in S, and that S is a subring *with unity* (in other words, show that S has a unity element different from the unity element of R)!

Theorem 12.15. *Let R be a ring and $\mathcal{C}$ be a nonempty collection of subrings of R. Then $\bigcap_{S \in \mathcal{C}} S$ is a subring of R.*

This is a parallel theorem from group theorem and isn't particularly relevant.

Theorem 12.17. *Let R be a ring and $r \in R$. Then the subring generated by r is the set*

$$\{n_0 + n_1 r + n_2 r^2 + \cdots + n_k r^k \mid k, n_i \in \mathbb{Z}, k \geq 0\}.$$

There is a typo in the statement of this theorem. The initial n_0 should not be there, and elements of R raised to the 0 power need not be defined, so that the correct set should read

$$\{n_1 r + n_2 r^2 + \cdots + n_k r^k \mid k, n_i \in \mathbb{Z}, k \geq 1\}.$$

Fortunately, this theorem is really unimportant, but it does set up the idea of polynomials nicely. If students need it later, just have them refer to it without proof.

12.2 Homomorphisms

This is really a continuation of the introductory material on rings, so there shouldn't be much anxiety about this section. An ambitious instructor (or one short on time) might even combine this with the previous section, as there's only one essential theorem to present, but I'd advise against it. Once again, emphasize the points of contrast with groups.

Theorem 12.19. *Let $\phi : R \to R'$ be a ring homomorphism.*

1. *$\phi(a^n) = \phi(a)^n$ for all $a \in R$ and $n \in \mathbb{Z}^+$.*
2. *If S is a subring of R, then $\phi(S)$ is a subring of R', and if S is commutative, then $\phi(S)$ is also commutative.*
3. *If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.*

This is an exact parallel with the result from group theory. There's no need for a formal proof presentation.

Theorem 12.21. *Let $\phi : R \to R'$ be a ring homomorphism. Then ϕ is injective if and only if $Ker(\phi) = \{\boldsymbol{0}\}$.*

Remark that this *is* the result from group theory, not just a parallel!

Exercise 12.22. Which, if any, of the following functions are ring homomorphisms? Of those that are (if any), what is the kernel of the homomorphism? Are any isomorphisms?

1. $\phi : \mathbb{Z} \to \mathbb{Z}; \quad \phi(x) = 2x.$
2. $\phi : \mathbb{Z} \to \mathbb{Z}_5; \quad \phi(x) = r_x$, where r_x is the remainder of x when divided by 5.
3. $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n; \quad \phi(x) = (r_x, s_x)$, where r_x and s_x are the remainders of x when divided by m and n, respectively.
4. $\phi : M_n(\mathbb{R}) \to \mathbb{R}; \quad \phi(A) = \det(A).$

This exercise is here primarily to emphasize the contrast between group and ring homomorphisms. It's important that students recognize that something different is going on.

Theorem 12.23. *Let $\phi : R \to R'$ be a ring homomorphism. If R is a ring with unity element $\mathbf{1}$ and $\phi(\mathbf{1}) \neq \mathbf{0}$, then $\phi(\mathbf{1})$ is the unity element of the subring $\phi(R)$ of R'.*

The reason this is important to present is how it contrasts with group theory. The exercise that follows pairs nicely with this result.

Exercise 12.24. Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ be the function given by $\phi(a, b) = (a, 0)$. Verify that ϕ is a ring homomorphism, and that $\phi(1, 1) \neq (1, 1)$, but that $\phi(1, 1)$ is the unity element for the range of ϕ.

Again, students really need this kind of contrast. Otherwise, they're likely to assume that everything that's true from group theory is still true for rings.

12.3 Polynomials

I treat polynomials in the context of particular rings over several chapters, rather than in an entire chapter devoted to polynomials themselves. This gives students the chance to see how new properties of rings really influence what happens to polynomials, which is what I think is important. There's lots of terminology here, but it's not hard.

Theorem 12.27. *Let R be a ring. Then given any $f(x) = \sum_{i=0}^{\infty} a_i x^i$ and $g(x) = \sum_{i=0}^{\infty} b_i x^i$ in $R[x]$, the set $R[x]$ is a ring under the following two binary operations:*

1. $f(x) + g(x) = \sum_{i=0}^{\infty} (a_i + b_i) x^i$.
2. $f(x)g(x) = \sum_{i=0}^{\infty} c_i x^i$ *where* $c_i = \sum_{j=0}^{i} a_j b_{i-j} = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0$.

This theorem just affirms what students expect from polynomials. No presentation is necessary at this point, unless you really want to work on notation (and how to rewrite double sums).

Theorem 12.31. *Let R be a ring and $f(x), g(x) \in R[x]$ be nonzero polynomials.*

1. *If R is commutative, then $R[x]$ is commutative.*
2. *If R is a subring of R', then $R[x]$ is a subring of $R'[x]$.*
3. *If $f(x) \pm g(x) \neq 0$, then* $\deg(f(x) \pm g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.
4. *If $f(x)g(x) \neq 0$, then* $\deg(f(x)g(x)) \leq \deg(f(x)) + \deg(g(x))$.

Parts 1 and 2 are expected results whose justification can be discussed in class without proof. However, parts 3 and 4 are worthwhile to present. Since the degree of a polynomial is really, really important, getting clarity on how degree works (and where intuition can fail) is worthy of a presentation.

Corollary 12.32. *Let R be a ring with unity and $f(x), g(x) \in R[x]$ be nonzero polynomials. If the leading coefficient of $f(x)$ or $g(x)$ is a unit, then* $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.

This corollary will be important for Theorem 12.35, but its presentation isn't crucial. All that's needed is a sketch why the leading coefficient of the product can't be zero.

Theorem 12.33. *Let R be a ring. Then the map $\iota : R \to R[x]$ given by $\iota(r) = r$ is an injective ring homomorphism.*

This gives content to the idea that constant polynomials are the natural way to find a ring inside polynomials. Just talk this one through.

Theorem 12.35. *Let R be a ring with unity, and let $f(x), g(x) \in R[x]$ be polynomials, where the leading coefficient of $g(x)$ is a unit. Then there exist unique polynomials $q(x), r(x) \in R[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

This is the big one, naturally. Students will almost certainly struggle with precision on using degree as the way to find the quotient and remainder, so be prepared to give some help here.

Exercise 12.36. Yep – it's time to make sure you know your long division. Find the quotient $q(x)$ and remainder $r(x)$ when the polynomial $f(x)$ is divided by $g(x)$. Pay close attention to the particular polynomial ring!

1. $f(x) = 3x^3 + x^2 - x + 3; \quad g(x) = x^2 - 2$ in $\mathbb{Z}[x]$.
2. $f(x) = 3x^3 + x^2 - x + 3; \quad g(x) = x^2 - 2$ in $\mathbb{Z}_5[x]$.
3. $f(x) = 4x^5 - 4x^4 - 5x^3 - 2; \quad g(x) = 2x^2 + x - 1$ in $\mathbb{Q}[x]$.
4. $f(x) = 4x^5 - 4x^4 - 5x^3 - 2; \quad g(x) = 2x^2 + x - 1$ in $\mathbb{Z}_7[x]$.
5. $f(x) = -3x^4 + 2i; \quad g(x) = ix^2 + 3x + 2 + i$ in $(\mathbb{Z}[i])[x]$.
6. $f(x) = x^n - 1; \quad g(x) = x - 1$ in $R[x]$ for any ring R with unity and any positive integer n.

It's totally worth having them slog through the tedium of at least a couple of these. You'd be surprised how many math majors still struggle with long division.

Chapter 13

Commutative Rings

Suggested time: 3 days.
Essential theorems for presentation: 13.6, 13.10, 13.12, 13.13, 13.23, 13.25, 13.26
Necessary theorems for later use: 13.17, 13.19, 13.27, 13.28
Optional theorems: 13.15, 13.16, 13.18
Important exercises: 13.3, 13.11, 13.14, 13.21

The emphasis in this chapter really needs to be on polynomials, as that section contains the most critical results about polynomials. If you're pressed for time, you can omit much (but not all) of section 2 by covering sections 1 and 2 together. But the importance of integral domains is hard to understate, as they'll create fields of quotients/fractions in the next chapter. Spend two to three days on this chapter (but no more).

13.1 Integral Domains

There's a lot of terminology and examples here, but only two theorems. Gauge the class and the time remaining in the semester to see if you want to spend an entire day on this section or if you wish to combine it with the next one.

Exercise 13.3. Let R be a commutative ring and $a \in R$. Let $S = \{r \in R \mid ar = \mathbf{0}\}$, called the *annihilator* of a. Show that S is a subring of R, and that if $a \neq \mathbf{0}$, then no element in the annihilator of a is a unit (assuming R has unity). Conclude that if a is a zero divisor of R, then a can never be a unit of R.

This is sets the stage for the content in this chapter (and why we care so much about it).

Theorem 13.6 (The Ring Cancellation Law)**.** *Let R be a commutative ring and let $a, b, c \in R$ such that $ab = ac$. If $a \neq \mathbf{0}$ and is not a zero divisor, then $b = c$.*

The cancellation law is huge and must be presented. Make sure the proof is precise and uses the definitions accurately.

Theorem 13.10. *Every field is an integral domain, and every finite integral domain is a field.*

This is hard for students, so don't be surprised if they need some extra hints. While it's not unreasonable to skip the second part of this theorem, the idea of where the finiteness condition is used is really useful for students to understand.

Exercise 13.11. This important exercise will require you to come up with a list of examples that identify different types of rings. Provide an example of each type of ring listed.

1. A field.
2. An integral domain that is not a field.
3. A commutative ring with unity that is not an integral domain.
4. A commutative ring without zero divisors that is not an integral domain.
5. A noncommutative ring with unity.
6. A noncommutative ring without unity.

This is one of my favorite exercises to give students.

13.2 The Ring $\mathbb{Z}_n$

Depending on the semester, I've either spent an entire day on this, or I've just covered the first two theorems. It all depends on my time situation, the ability of the class, and what I think the class will do with this. Students who have taken a course in Number Theory should go wild with excitement.

Theorem 13.12. *Let $n > 1$ be an integer and a be a nonzero element of $\mathbb{Z}_n$. If a and n are relatively prime, then a is a unit. If a and n are not relatively prime, then a is a zero divisor.*

Every math major ought to know and understand a proof of this, so a complete, precise proof is important here.

Theorem 13.13. *Let $n > 1$ be an integer. If n is prime, then $\mathbb{Z}_n$ is a field; if n is not prime, then $\mathbb{Z}_n$ is not an integral domain.*

This is almost a corollary of the prior theorem, but there's enough original content to make a presentation worthwhile.

Exercise 13.14. Classify each nonzero element in the following rings as either a zero divisor or a unit. If an element a is a zero divisor, find a corresponding nonzero element b such that $ab = 0$. If an element is a unit, find its multiplicative inverse.

1. $\mathbb{Z}_3$ 2. $\mathbb{Z}_4$ 3. $\mathbb{Z}_6$ 4. $\mathbb{Z}_7$ 5. $\mathbb{Z}_9$ 6. $\mathbb{Z}_{10}$

This gives students the chance to apply the previous theorems.

Theorem 13.15. *Let $n > 1$ be an integer and let $a, b \in \mathbb{Z}_n$. Then the equation $ax = b$ has a solution if and only if the greatest common divisor of a and n divides b. Furthermore, if d is the greatest common divisor of a and n and d is a divisor of b, then the equation $ax = b$ has exactly d solutions.*

This obviously nice result doesn't affect what comes afterwards, despite it's very satisfying statement. If you only have time to prove the first half, that's a reasonable way to tie in Chapter 7 to Ring Theory. Counting solutions is really optional.

Corollary 13.16. *If p is prime, then the equation $ax = b$ has a unique solution in $\mathbb{Z}_p$ if and only if $a \neq 0$.*

If you don't cover 13.5, then its corollary won't be needed either.

Theorem 13.17 (Fermat's Little Theorem)**.** *Let p be a prime and a be a nonzero element in $\mathbb{Z}_p$. Then $a^{p-1} = 1$.*

Because of what's just been covered, this titan of a result can be given full recognition as an application of prior results.

Theorem 13.18 (Euler's Theorem)**.** *Let $n > 1$ be an integer and $a \in \mathbb{Z}_n$. If a and n are relatively prime, then $a^{\phi(n)} = 1$, where $\phi(n)$ is the number of elements in $\mathbb{Z}_n$ that are relatively prime to n.*

How can I possibly call Euler's theorem optional? Simply because it has little bearing on the last two chapters of Ring Theory. But feel free to use this as a hook for getting students interested in Number Theory!

13.3 Polynomials Over Integral Domains

This fundamentally important section shows why the classic results of high school algebra need an integral domain. That's the way to frame this topic: by emphasizing that the proofs need to reference the properties of an integral domain. Make sure the presenters highlight where those properties are used in their proofs.

Theorem 13.19. *Let D and D' be integral domains with D a subdomain of D', and let $\alpha \in D'$. Then the function $\phi_\alpha : D[x] \to D'$ given by $\phi_\alpha(f(x)) = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a^n\alpha^n$ where $f(x) = \sum_{i=0}^{\infty} a_i x^i$ is a polynomial of degree at most n, is a homomorphism.*

This proof of this theorem is too messy for a presentation. You'll want to discuss it, of course.

Exercise 13.21. Consider the polynomial $p(x) = x^2 + 3x + 2 \in \mathbb{Z}_6[x]$. Use long division to divide $p(x)$ first by $x - 1$, and then by $x - 4$. Use your result to factor $p(x)$ is two different ways.

This too is one of my favorites. Students think they know how polynomials work; this exercise should make them uneasy about what they believe is true. Students need to work this one out.

Theorem 13.23 (The Remainder Theorem)**.** *Let D be an integral domain and $f(x) \in D[x]$. Then for any $a \in D$ there exists a unique $q(x) \in D[x]$ such that $f(x) = q(x)(x-a) + f(a)$.*

This sets up the important Factor Theorem next.

Theorem 13.25 (The Factor Theorem)**.** *Let D be an integral domain and let $f(x) \in D[x]$. Then $a \in D$ is a zero of $f(x)$ if and only if there exists a polynomial $q(x) \in D[x]$ such that $f(x) = q(x)(x-a)$.*

A precise proof uses the evaluation homomorphism, so make sure it's done correctly.

Theorem 13.26. *Let D be an integral domain, and let $f(x) \in D[x]$ have degree n. Then $f(x)$ has at most n zeros in D.*

A false proof by induction is common (see the solution manual for a correct induction proof). What must occur is why there can't be more than n, and that requires the fact that D is an integral domain. To emphasize this, you should ask them to find a counterexample (in a previous exercise) that shows how if D is not an integral domain, there can be polynomials that have more zeros than the degree. Every math major should have such a counterexample in their back pocket.

Theorem 13.27. *Let D be an integral domain. Then $D[x]$ is an integral domain, and $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$ for all nonzero $f(x), g(x) \in D[x]$.*

The justification of this theorem can be done as a sketch on the board or in discussion.

Corollary 13.28. *If D is an integral domain, then the units of $D[x]$ are the units of D.*

Again, this satisfying corollary can be justified from previous results in discussion.

Chapter 14

Fields

Suggested time: 3 days.
Essential theorems for presentation: 14.1, 14.2.1, 14.2.4, 14.4, 14.8, 14.12, 14.13,
Necessary theorems for later use: 14.2.2, 14.2.3, 14.5, 14.9, 14.14, 14.20
Optional theorems: 14.18, 14.21, 14.24, 14.25, 14.26
Important exercises: 14.19, 14.22

This chapter is full of some of the best content in ring theory. Having students build fractions from scratch is particularly satisfying. Each section takes about a day, so this is a three-day chapter.

14.1 The Field of Quotients

While there's a lot going on here, many of the tedious details can be assigned for homework, or simply justified in discussion. What's truly important is the process of building a field. If need be, you can skim the derivation of knowing when a field is, in fact, a field of quotients of an integral domain.

Theorem 14.1. *Let D be an integral domain, and let D^* be the set of nonzero elements of D. Then the relation $\sim$ on $D \times D^*$ given by*

$$(a, b) \sim (c, d) \text{ if and only if } ad = bc$$

is an equivalence relation.

This foundational theorem is essential for this entire section. Transitivity is the key discussion point, and make certain that they know *why* they're allowed to cancel – never let them get away with "dividing."

Theorem 14.2. *Let D be an integral domain and $F = \{a/b \,|\, a, b \in D, b \neq \mathbf{0}\}$. Then:*

1. *$a/b + c/d = (ad + bc)/(bd)$ and $a/b \cdot c/d = (ac)/(bd)$ are well-defined binary operations on F.*
2. *Under these two operations, F is a field.*
3. *The subset $\{a/\mathbf{1} \,|\, a \in D\} \subset F$ is isomorphic to D.*
4. *$a/b = (a/\mathbf{1})\,(b/\mathbf{1})^{-1}$.*

Presenting careful proofs of parts 1 and 4 are enlightening for students. On the other hand, I routinely give some of the elements of part 2 and/or part 3 as homework. Mention that part 3 makes rigorous the high school notion that all integers are fractions with denominator 1.

Theorem 14.4. *Let D be an integral domain and $F = \{a/b \,|\, a, b \in D, b \neq \mathbf{0}\}$. If F' is any field also containing D, then the function $\phi : F \to F'$ given by $\phi(a/b) = ab^{-1}$ is a well-defined, injective homomorphism; if F' is also a field of quotients of D, then ϕ is an isomorphism.*

I've often skipped this theorem for the sake of time, but if you're going to cover the uniqueness of the field of quotients, this theorem's presentation is the key.

Corollary 14.5. *If F is a field, then F is isomorphic to its field of quotients.*

This can either be omitted or explained as the consequence of the preceding theorem.

14.2 The Characteristic of a Ring

The main consequence of discussing the characteristic of a ring is to show that every field is an extension of $\mathbb{Q}$ or of $\mathbb{Z}_p$. Hence, this material should focus on that corollary. It's not hard stuff.

Theorem 14.8. *Let R be a ring with unity and let n be a positive integer. Then R has characteristic n if and only if n is the smallest positive integer such that $n\mathbf{1} = \mathbf{0}$, and R has characteristic 0 if and only if $n\mathbf{1} \neq \mathbf{0}$ for all positive integers n.*

This emphasizes the role that the unity element plays in the characteristic of a ring.

Theorem 14.9. *Let R and R' be rings with unity. If R has characteristic $n > 0$ and R' has characteristic $m > 0$, then the characteristic of $R \times R'$ is the least common multiple of n and m; if either R or R' has characteristic 0, then $R \times R'$ has characteristic 0.*

A nice result that should be intuitively obvious from group theory.

Theorem 14.12. *If D is an integral domain, then its characteristic is either prime or 0.*

This shows why we care almost exclusively about rings of characteristic 0 or prime characteristic. But do watch for carelessness in their proof when using coefficients versus ring multiplication.

Theorem 14.13. *Let D be an integral domain and let $D' = \{n\mathbf{1} \mid n \in \mathbb{Z}\}$.*

1. *If D has characteristic 0, then the map $\phi : \mathbb{Z} \to D'$ given by $\phi(n) = n\mathbf{1}$ is an isomorphism;*
2. *If D has characteristic $p > 0$, then the map $\phi : \mathbb{Z}_p \to D'$ given by $\phi(n) = n\mathbf{1}$ is an isomorphism.*

This is the key theorem that leads into the result about prime fields.

Corollary 14.14. *Every field of characteristic* 0 *contains a field isomorphic to* $\mathbb{Q}$*, and every field of characteristic* $p > 0$ *contains a field isomorphic to* $\mathbb{Z}_p$*.*

This follows immediately from theorem 14.8, but it's worth highlighting.

14.3 Polynomials over a Field

Now, the highlight of the entire theorem sequence is the last section of the next chapter, which needs polynomials over a field. Irreducibility is the key concept here, and almost none of the theorems in this section are used in the next chapter. Hence, you can actually cover this section lightly if you need, but don't omit it entirely. The idea of irreducibility is really what needs attention.

Theorem 14.18. *Let* F *be a field and let* $f(x) \in F[x]$ *be a polynomial of degree* 2 *or* 3*. Then* $f(x)$ *is reducible over* F *if and only if* $f(x)$ *has a zero in* F*.*

This is a good exercise in putting together prior facts, but if they don't see this, it won't hurt them.

Exercise 14.19. Many students erroneously think that if a polynomial in $F[x]$ lacks a zero in F, then the polynomial is irreducible. Show this is false by verifying that the polynomial $x^4 + 1 \in \mathbb{R}[x]$ has no zero in $\mathbb{R}$ but is reducible in $\mathbb{R}[x]$.

This is another favorite exercise. Even seasoned mathematicians can forget that reducibility and having zeros are, in fact, not equivalent. This also shows that irreducibility depends on the field in which your coefficients lie. It's my professional opinion that all future high school math teachers *must* work this exercise out.

Theorem 14.20. *Let* F *be a field. Then every polynomial can be written as a product of irreducible polynomials. Furthermore, the polynomials in this product are unique up to the order of the polynomials and multiplication by units.*

This proof is unnecessarily complex at this point, so I don't ask students to prove it, nor is a presentation enlightening.

Theorem 14.21 (Freshman Exponentiation)**.** *Let F be a field of characteristic $p > 0$. Then $x^p + a^p = (x + a)^p$ for all $a \in F$.*

Yes, if they take more Abstract Algebra, they'll need this, but not now. It's a great one to come back to in a subsequent course.

Exercise 14.22. Since we're looking at fields of characteristic p, let's practice factoring polynomials in $\mathbb{Z}_p[x]$. Express each polynomial as a product of irreducibles in the given polynomial ring.

1. $x^2 + 2x + 2 \in \mathbb{Z}_5[x]$.
2. $x^3 + 3x^2 + 2x + 1 \in \mathbb{Z}_5[x]$.
3. $x^5 + x^3 + 2x^2 + 2 \in \mathbb{Z}_3[x]$.
4. $x^7 + 5 \in \mathbb{Z}_7[x]$. (Hint: Fermat's Little Theorem might prove useful.)

This exercise helps students develop computations in less familiar fields.

Theorem 14.24. *Let $p(x), q(x) \in \mathbb{Q}[x]$. If $p(x)q(x)$ is a polynomial with integer coefficients, then there exists polynomials $f(x), g(x) \in \mathbb{Q}[x]$ with integer coefficients and rational numbers a, b such that $f(x) = a \cdot p(x), g(x) = b \cdot q(x)$, and $p(x)q(x) = f(x)g(x)$.*

This result is truly a high school math result, but I almost always skip it, mostly because a precise proof is so tedious. The traditional way of saying this is that if you can factor a polynomial in $\mathbb{Z}[x]$ over $\mathbb{Q}$,, then you can factor it in such a way that the factors also have integer coefficients.

Theorem 14.25 (The Rational Root Test)**.** *Let $p(x) \in \mathbb{Q}[x]$ be a nonzero polynomial with integer coefficients and nonzero constant term. Then any rational zero of $p(x)$ must be of the form $\pm\frac{r}{s}$, where r is a divisor of the constant term and s is a divisor of the leading coefficient.*

I love this famous result, and high school teachers ought to know this too. But it's so specific to factoring high school polynomials that you can safely omit it.

Corollary 14.26. *The only rational zeros of monic polynomials with integer coefficients are integers.*

Nice to know, but safe to skip.

Chapter 15

Quotient Rings

Suggested time: 3 days.
Essential theorems for presentation: 15.1, 15.4, 15.7, 15.13, 15.19, 15.23, 15.26, 15.27, 15.29
Necessary theorems for later use: 15.5, 15.8, 15.9, 15.10, 15.16, 15.17, 15.21, 15.28
Optional theorems: 15.11
Important exercises: 15.3, 15.15, 15.30 or 15.31, 15.32

Since students have had to prove so much about quotient groups, these theorems are a really good reinforcement on how they work. But this chapter is really the big payoff of why they're so useful – they get to construct zeros of polynomials! One day each on the three sections is what's needed.

15.1 Ideals

Although the goal of the theorem sequence is to use quotient rings to construct fields, this first section's emphasis need only be on the definition of an ideal and its use in constructing quotient rings. The parallel results from group theory can be covered in a second course in Abstract Algebra. Indeed, you could even start the next section along with this one, if you felt it appropriate.

Theorem 15.1. *Let R be a ring and I a subring of R. The binary operation $(a+I)(b+I) = (ab)+I$ is well-defined on R/I if and only if $aI \subset I$ and $Ib \subset I$ for all $a, b \in R$.*

This proof really shows why we have to define ideals the way we do. It's a must for presentation.

Exercise 15.3. Determine if the following subsets I are ideals of the given ring R.

1. $R = \mathbb{Z}; \quad I = n\mathbb{Z}$
2. $R = \mathbb{Z} \times \mathbb{Z}; \quad I = \{(n, n) \,|\, n \in \mathbb{Z}\}$
3. $R = \mathbb{Z}_{18}; \quad I = \{0, 3, 6, 9, 12, 15\}$
4. $R = M_2(\mathbb{Z}); \quad I = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \,\middle|\, a, b \in \mathbb{Z} \right\}$

This addresses the basics of how to test if a subgroup is an ideal or not.

Theorem 15.4. *Let R be a ring and I, N ideals of R. Then $I + N = \{i + n \,|\, i \in I, n \in N\}$ is an ideal of R containing both I and N.*

This is useful in proofs in the next section, but I give this as a homework problem all the time when I don't have time for a presentation.

Theorem 15.5. *Let R be a ring and I an ideal of R. Then R/I is a ring under coset addition and multiplication.*

You can have them sketch a proof of this after theorem 15.2. Going through this carefully isn't particularly productive.

Theorem 15.7. *Let $\phi : R \to R'$ be a ring homomorphism. If I is an ideal of R, then $\phi(I)$ is an ideal of $\phi(R)$, and if I' is an ideal of $\phi(R)$, then $\phi^{-1}(I')$ is an ideal of R.*

This can be relevant in the next section on maximal ideals, but if you simply want to refer to the proof from group theory, it's not a bad compromise.

Theorem 15.8. *Let R be a ring and I an ideal of R. Then the function $\phi : R \to R/I$ given by $\phi(r) = r + I$ is a ring homomorphism with $Ker(\phi) = I$.*

Again, a sketch or discussion about this fact is all that's really necessary.

Theorem 15.9 (The First Isomorphism Theorem for Rings)**.** *Let $\phi : R \to R'$ be a ring homomorphism with kernel I. Then the function $\overline{\phi} : R/I \to \phi(R)$ given by $\overline{\phi}(r + I) = \phi(r)$ is a well-defined isomorphism.*

Rather than prove this (again), it's enough to show students the parallels to group theory.

Corollary 15.10. *Let $\phi : R \to R'$ be a surjective ring homomorphism with kernel I. Then R' is isomorphic to R/I.*

Again, it's a parallel theorem from group theory. Just reference that.

Theorem 15.11. *Let $n \in \mathbb{Z}$. Then $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.*

For practice using the First Isomorphism Theorem, get them to define the relevant homomorphism, then have them apply the First Isomorphism Theorem.

15.2 Ideals in Commutative Rings

This is where the concept of an ideal is really developed. Creating maximal ideals and principal ideals is paramount, so proceed carefully.

Theorem 15.13. *Let R be a commutative ring with unity and let $a \in R$. Then the set $\{ra \,|\, r \in R\}$ is an ideal of R containing a.*

Very important, and it's easy to present.

Exercise 15.15. For each evaluation homomorphism, show that its kernel is the principal ideal indicated.

1. $\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{R}; \quad Ker(\phi_{\sqrt{2}}) = \langle x^2 - 2 \rangle$.
2. $\phi_{\sqrt[3]{2}} : \mathbb{Q}[x] \to \mathbb{R}; \quad Ker(\phi_{\sqrt[3]{2}}) = \langle x^3 - 2 \rangle$.
3. $\phi_i : \mathbb{Q}[x] \to \mathbb{C}; \quad Ker(\phi_i) = \langle x^2 + 1 \rangle$.
4. $\phi_{e^{\frac{2\pi}{3}}} : \mathbb{Q}[x] \to \mathbb{C}; \quad Ker(\phi_{e^{\frac{2\pi}{3}}}) = \langle x^2 + x + 1 \rangle$.

Students really need the exposure to how principal ideas are special. This also preps them for the big finale exercises at the end of the chapter.

Theorem 15.16. *Let R be a ring with unity and let I be an ideal of R. If I contains a unit of R, then $I = R$.*

This is easily sketched and need not be given a full presentation.

Corollary 15.17. *Fields have no nontrivial proper ideals.*

This motivates what comes next, so it's a good lead-in fact.

Theorem 15.19. *Let R be a commutative ring with unity and $I \neq R$ a proper ideal of R. Then R/I is a field if and only if there does not exist an ideal N of R such that $I \subsetneq N \subsetneq R$.*

This establishes how to get fields: build maximal ideals. It's a biconditional, so two students can present this, one for each direction.

Corollary 15.21. *Every simple commutative ring with unity is a field.*

Emphasize that we keep looking for connections to fields.

Theorem 15.22. *Let R be a commutative ring with unity and $I \neq R$ a proper ideal of R. Then R/I is an integral domain if and only if whenever $ab \in I$, then $a \in I$ or $b \in I$ for all $a, b \in R$.*

A parallel theorem to the above (obviously), but less important. Present if possible; otherwise, just sketch.

15.3 Ideals in Polynomial Rings

This is it – the big payoff. Each of the first three theorems leads into the final result, so most will need presentation. The last exercise is also very cool!

Theorem 15.26. *If F is a field, then every ideal of $F[x]$ is a principal ideal.*

This tells us what the only ideals in $F[x]$ look like. It's a super important result that needs to be presented.

Theorem 15.27. *Let F be a field and $f(x) \in F[x]$ be an irreducible polynomial. Then $\langle f(x) \rangle$ is a maximal ideal.*

This tells us what to look for to create fields.

Theorem 15.28. *Let F be a field and $f(x) \in F[x]$ be an irreducible polynomial. Then the subset $\{r + \langle f(x) \rangle \mid r \in F\} \subset F[x]/\langle f(x) \rangle$ is a subfield of $F[x]/\langle f(x) \rangle$ isomorphic to F.*

This should be natural, so just bring this up as part of the discussion, rather than having students present this.

Theorem 15.29. *Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial. Then the coset $\alpha = x + \langle f(x) \rangle$ is a zero of $f(x)$.*

The use of the evaluation homomorphism is necessary, so hold their feet to the fire one last time.

Exercise 15.30. Let's practice with a well-known irreducible polynomial: $(x^2 - 2) \in \mathbb{Q}[x]$. We "know" what its zeros are: $\pm\sqrt{2}$. Prove that the subfield $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\} \subset \mathbb{R}$ is isomorphic to $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ by showing that the evaluation homomorphism $\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{2})$ is surjective, computing its kernel, and then using the First Isomorphism Theorem.

Until students put the theorems into practice, they won't really understand what they've done. Having them work through this exercise or the next is important.

Exercise 15.31. Construct the complex numbers by using another well-known irreducible polynomial: $(x^2 + 1) \in \mathbb{R}[x]$. Repeat the steps used above, but this time, use the evaluation homomorphism $\phi_i : \mathbb{R}[x] \to \mathbb{C}$.

As mentioned above, either this exercise or the previous one is important for students to work through.

Exercise 15.32. Finally, it's important to work out at least one example with fields of characteristic $p > 0$. This time, consider the polynomial $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$.

1. First, verify that $p(x)$ is irreducible over $\mathbb{Z}_3$.
2. Second, if we call i one of the zeros of $p(x)$, verify that $2i$ is its other zero. Furthermore, verify that $p(x) = x^2 - 2$, and if we call $\sqrt{2}$ one of its zeros, then $2\sqrt{2}$ is its other zero. Conclude that $i = \sqrt{2}$.
3. Third, let $F = \{a + bi \,|\, a, b \in \mathbb{Z}_3\} = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}_3\}$. You may assume that F is a field, so instead, count the number of elements in F.
4. Finally, show that the evaluation homomorphism $\phi_i : \mathbb{Z}_3[x] \to F$ is surjective, compute its kernel, and then use the First Isomorphism Theorem.

Congratulations: you've just constructed a field with nine elements!

This is one of the few exercises that the 2015 CUPM guide mentions, so assign this for students to work through, if at all possible.

Appendices

Appendix A

Relations and functions

Suggested time: .5 - 1 day per section
Essential theorems for presentation: A.7, A.12, A.17, A.20, A.21
Necessary theorems for later use: A.10, A.22, A.24, A.26
Optional theorems: A.13, A.27
Important exercises: A.8, A.16

This appendix includes all of the definitions about relations and functions a student needs to succeed in using this theorem sequence. However, a couple of exercises and theorems rely on the Division Algorithm from Chapter 1, so starting the course off with this Appendix is unwise. If you decide to cover part or all of this appendix, I recommend that you begin with Chapter 1 and use this appendix right before Chapter 2, since that's when they'll need it for the first time. No matter how much you decide to cover, don't spend any more than one day per sections, and ideally, spend one day on sections 2 and 3 together.

A.1 Equivalence relations

Don't spend a lot of time on the definitions; that's for them to digest as the theorems are presented.

Theorem A.7. *Let $\sim$ be an equivalence relation on a set X, and let $x, y \in X$. Then $\overline{x}$ and $\overline{y}$ are either disjoint or equal, and $\overline{x} = \overline{y}$ if and only if $x \sim y$.*

This has two parts to it, so giving this to two different students is a great way to have this presented. Whatever else, make sure that they are *explicit* in their use of the properties of an equivalence relation in their proofs.

Exercise A.8. Let $n \in \mathbb{Z}^+$, and define a relation on $\mathbb{Z}$ by $a \sim b$ if and only if $a - b \in n\mathbb{Z}$. Prove that this defines an equivalence relation on $\mathbb{Z}$. How many distinct equivalence classes are there? Write down those equivalence classes for $n = 5$.

Because of the relationship between this relation and the integers modulo n, this exercise ought to be given when covering this section of the appendix.

Theorem A.10. *Let $n \in \mathbb{Z}^+$. Then every integer $k \in \mathbb{Z}$ is congruent modulo n to exactly one integer in the set $\{0, 1, \ldots, n-1\}$.*

I usually assign this theorem as a homework problem after once they've worked through the Division Algorithm.

Theorem A.12. *Let $\sim$ be an equivalence relation on a set X. Then the collection of distinct equivalence classes of the relation forms a partition of X.*

This idea comes back later, so if students haven't seen this, presenting it now is important.

Theorem A.13. *Let $\{X_i\}_{i \in I}$ be a partition of X. Then the relation $\sim$ on X defined by*

$$x \sim y \text{ if and only if there exists a cell } X_i \text{ such that } x \in X_i \text{ and } y \in X_i$$

is an equivalence relation on X whose equivalence classes are the cells of the partition.

While this theorem is a natural complement to what's just been proved, this particular result doesn't make its appearance at all in this course. I either skip this result or have an oral discussion in class, if I have time at the end of a class.

A.2 Functions

Ah, the mountain of terminology! Although there's "only" one theorem in this section, the terminology and the exercises will be the highlight of the section. Graphs are fine here, but make sure everyone understands what's going on. My experience has always been that students actively avoid how inverse images work, so be patient with them on that, but insist that they understand what's going on.

Exercise A.16. Four functions from $\mathbb{R}$ to $\mathbb{R}$ are given below. Identify the range of the function, the image of the set $[-1, 1]$ under the function, the image of the set $[0, 1]$ under the function, the inverse image of the elements $-1, 0$, and 1 under the function, and the inverse image of the set $[-1, 1]$ under the function.

1. $f(x) = x^2$
2. $g(x) = ax + b, \quad a > 0$
3. $h(x) = b$
4. $k(x) = \frac{1}{x}$ when $x \neq 0$, and $k(0) = 0$

As mentioned above, the problems in this exercise force students to address all the definitions and notations introduced. It's worth going slowly to ensure that everyone knows how to deal with them all.

Theorem A.17. *Let $f : X \to Y, g : Y \to Z$, and $h : Z \to W$ be functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

The associativity of composition is a key computation that everyone needs to see. In particular, students have rarely been forced to distinguish between a function f and its image $f(x)$. This is an excellent time to begin to make this distinction precise. Make sure they go slowly and carefully through the order of composition.

A.3 Bijections and inverse functions

I've written the definitions for injective and surjective specifically as solutions to equations, as that's what the theme of the theorem sequence is. The theorems on cardinality are optional.

Theorem A.20. *Let $f : X \to Y$ and $g : Y \to Z$ be functions. If f and g are injective, surjective, or bijective, then so is $g \circ f$, accordingly.*

The proofs of composite functions regarding injective and surjective functions are what's needed for presentation; compositions of bijections is a trivial corollary. Insist they are precise with the use of existence and uniqueness language.

Lemma A.21. *Let $f : X \to Y$ be a function. Then f is injective if and only if for all $a, b \in X$, $f(a) = f(b)$ implies $a = b$.*

After this is proved, guide students to use this lemma every time they want to prove a function is injective.

Lemma A.22. *Let $f : X \to Y$ be a bijection, and let $y \in Y$. Then there is a unique element $x \in X$ such that $f(x) = y$.*

Don't bother assigning this. Have a student give an oral justification. It's trivial.

Theorem A.24. *If $f : X \to Y$ is bijective, then so is its inverse function f^{-1}.*

This is a really good exercise in working through the definitions and understanding what it means for a function to be everywhere defined and to be well-defined.

Theorem A.26. *Let A and B be disjoint finite sets. Then $|A \cup B| = |A| + |B|$.*

I skip this theorem and its corollary all the time. They're here because there are some important results (like Lagrange's theorem) that use these two specific counting arguments. But most students accept this as nearly obvious, so it's easy and safe to skip these two. But this theorem is the only one that you might want to have presented, or you can assign it as homework, or just have them do it together.

Corollary A.27. *Let A and B be finite sets. Then $|A \cup B| = |A| + |B| - |A \cap B|$.*

This only needs a brief discussion on how to use the previous theorem to derive this.

Appendix B

Matrices

Suggested time: .5 - 1 day per section
Essential theorems for presentation: B.10, B.14, B.15, B.17
Necessary theorems for later use: B.4, B.6, B.7, B.20, B.21
Optional theorems: B.12
Important exercises: B.8, B.11, B.18, B.22

For students who have never taken a Linear Algebra course, this appendix contains only that material which is necessary to succeed using this theorem sequence. The motivation and computations are covered quickly to get to the main theoretical results needed in abstract algebra. Much of what's needed is better done with examples than with careful derivations of general facts, and computations can safely be limited to the 2×2 case. But the content of inverses and determinants is necessary for completing the theorem sequence. Hence, for students who have never studied matrix algebra, it takes about 3 days to work through this material. If you use this as a review, you can spend 1 or 1.5 days to remind students of what they need.

B.1 Matrix Algebra

Writing down these formal definitions doesn't really convey to students how to read and manipulate matrices. This needs to be done visually.

Theorem B.4. *Let $A, B, C \in M_{m,n}(\mathbb{C})$, and let $c, d \in \mathbb{C}$.*

1. *(A+B)+C=A+(B+C).*
2. ***0**+A=A+**0**=A.*
3. *A+B=B+A.*
4. *c(dA)=(cd)A.*
5. *c(A+B)=cA+cB.*
6. *(c+d)A=cA+dA.*

Do not go through a careful proof of this theorem. Instead, highlight that matrix addition and scalar multiplication behave as we think they should.

Theorem B.6. *Let $A \in M_{m,n}(\mathbb{C})$ with $A = [a_{i,j}]$ and $B \in M_{n,p}(\mathbb{C})$ with $B = [b_{i,j}]$. If $c_{i,j}$ denotes the entry in the i^{th} row and j^{th} column of AB, then*

$$c_{i,j} = \sum_{k=1}^{n} a_{i,k} b_{k,j} = a_{i,1} b_{1,j} + a_{i,2} n_{2,j} + \cdots + a_{i,n} b_{n,j}.$$

Likewise, don't go through a formal, algebraic derivation of this fact. Indeed, working concrete examples is better for understanding.

Theorem B.7. *Let $A \in M_{m,n}(\mathbb{C})$ and $c \in \mathbb{C}$.*

1. *If $B \in M_{n,p}(\mathbb{C})$ and $C \in M_{p,q}(\mathbb{C})$, then $A(BC) = (AB)C$.*
2. *If $B \in M_{n,p}(\mathbb{C})$, then $c(AB) = (cA)B = A(cB)$ for any $c \in \mathbb{C}$.*
3. *If $B \in M_{n,q}(\mathbb{C})$ and $C \in M_{n,q}(\mathbb{C})$, then $A(B + C) = AB + AC$.*
4. *If $B \in M_{p,m}(\mathbb{C})$ and $C \in M_{p,m}(\mathbb{C})$, then $(B + C)A = BA + CA$.*
5. *$\mathbf{0}A = A\mathbf{0} = \mathbf{0}$.*

Students need the facts this theorem asserts, not its proof, so just talk through what the theorem says.

Exercise B.8. To emphasize this point, find two 2×2 matrices A and B such that AB and BA are different.

This exercise is a good first computation to show or remind them of the differences between numerical and matrix multiplication.

Theorem B.10. *Let $A \in M_{m,n}(\mathbb{C})$. Then $I_m A = A$ and $AI_n = A$. In particular, if $m = n$, then $I_n A = AI_n = A$.*

This is a main result of this section, and it's worthwhile and simple enough to present.

B.2 Matrix Inverses

This section contains the first set of truly important results about matrices students need to know for the theorem sequence. Make sure there's no confusion about how inverses work.

Exercise B.11. For each equation, find all 2×2 matrices $X \in M_{2,2}(\mathbb{R})$ that solve the equation, or determine that no such matrix exists.

1. $\begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix} X = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
2. $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} X = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
3. $\begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix} X = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$
4. $\begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix} X = \begin{bmatrix} 1 & 0 \\ 2 & 0 \end{bmatrix}$

Now repeat these same exercises, but reverse the order of the matrices in the product on the left hand side. Do your answers change?

This is a really good set of problems for students to work through, regardless of their familiarity with linear algebra.

Theorem B.12. *Let A and B be $n \times n$ matrices. Then $AB = I_n$ if and only if $BA = I_n$, and if C is any $n \times n$ matrix such that $AC = AB = I_n$ or $CA = CB = I_n$, then $B = C$.*

Students don't see the relevance of this theorem, so just make sure they know its statement; its proof is really not needed. Indeed, the techniques needed to prove this theorem are best learned in a complete Linear Algebra course, so there's no proof provided in the solutions manual.

Theorem B.14. *Let A be an invertible $n \times n$ matrix. Then for any $n \times n$ matrix B, the matrix equation $AX = B$ has a unique solution, $X = A^{-1}B$, and the matrix equation $XA = B$ has a unique solution, $X = BA^{-1}$.*

This theorem, however, is an important prep for the similar result students will prove in Chapter 3. If you're covering this appendix, this is great one to present.

Theorem B.15. *Let* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2,2}(\mathbb{C})$. *Then* A *is invertible if and only if* $ad - bc \neq 0$, *and when* $ad - bc \neq 0$, *we have* $A^{-1} = \dfrac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

The proof here can be done computationally, and although the formula isn't really needed, it's good to remind students how inverses of 2×2 matrices work. Since it's a biconditional, have two students present this, one for each direction.

Theorem B.17. *Let* A, B *be* $n \times n$ *invertible matrices.*

1. AB *is invertible, and* $(AB)^{-1} = B^{-1}A^{-1}$.
2. I_n *is invertible, and* $I_n^{-1} = I_n$.
3. A^{-1} *is invertible, and* $\left(A^{-1}\right)^{-1} = A$.

This is the last essential theorem for students to work through, as these results are echoed in Chapter 3. It must be presented.

Exercise B.18. It's easy to dismiss this theorem as obvious or irrelevant, especially part 1. To help you appreciate that there's really something there, take the following two matrices:

$$A = \begin{bmatrix} 2 & 1 \\ 3 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 2 \\ -1 & -1 \end{bmatrix}.$$

1. Compute AB, and use the formula for the inverse of a 2×2 matrix to compute $(AB)^{-1}$.
2. Next, compute A^{-1} and B^{-1}.
3. Finally, compute both $A^{-1}B^{-1}$ and $B^{-1}A^{-1}$.
4. Based on your answers, does $(AB)^{-1} = A^{-1}B^{-1}$? How important is the order in which you multiply A^{-1} and B^{-1} to compute $(AB)^{-1}$?

This computation is a great way for students to internalize the previous theorem.

B.3 Determinants

The definition of the determinant is so burdensome that proofs dealing with them are unnecessarily dense. Don't prove any of the results here; rather, have students accept the results, perhaps justifying them with you sketching proofs of the 2×2 case.

Theorem B.19. *Let* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *be a* 2×2 *matrix. Then* $\det A = ad - bc$.

This is the only theorem that you might consider having them prove. But since they won't be actually computing determinants in this theorem sequence, you don't really need to spend that time on it.

Theorem B.20. *Let* A, B *be* $n \times n$ *matrices.*

1. *A is invertible if and only if* $\det A \neq 0$.
2. $\det(AB) = \det(A)\det(B)$.
3. *If* $c \in \mathbb{C}$, *then* $\det(cA) = c^n \det(A)$.
4. $\det(I_n) = 1$.
5. *If A is invertible, then* $\det(A^{-1}) = 1/\det(A)$.

This is the set of facts every student must know. But the proofs are really ugly and don't shed light on what's going on. It might even be better to have them reference a standard linear algebra textbook for proofs, if you felt they needed it. But it's this result that they will need and use throughout the theorem sequence.

Exercise B.21. As a corollary of Theorem B.20, prove that if A is an $n \times n$ matrix, then $\det(A^k) = (\det(A))^k$ for all positive integers k. Furthermore, when A is invertible, prove that $\det(A^k) = (\det(A))^k$ for all integers k, where A^0 is defined to be I_n.

This exercise is a good way to have students practice the properties of determinant without the slog of computing them.

Appendix C

Complex Numbers

Suggested time: 2 days
Essential theorems for presentation: C.15, C.17
Necessary theorems for later use: C.2, C.18
Optional theorems: C.5, C.6, C.16, C.21
Important exercises: C.7, C.8, C.11, C.12, C.13, C.20

This appendix is included almost exclusively for its computational necessity in the book. Yes, the theorems are important, but not so much for the students to present. The computations in the exercises are what students need for this book, so keep that as the main focus. If you choose to have students present theorems, just use those theorems whose derivation will help with student understanding of the upcoming computations.

C.1 Complex Arithmetic

This first section shouldn't take a full day; indeed, pairing it with part or all of the second section is quite natural.

Lemma C.2. *Let $z = a + bi$ be a complex number. Then $(a + bi)(a - bi) = a^2 + b^2$.*

It's just a computation to get anyone who hasn't ever seen complex numbers before comfortable with simple arithmetic.

Theorem C.5. *Let z, w be complex numbers. Then $\overline{z+w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$.*

This (and its corollary) are needed if you want to talk about complex solutions to polynomials occurring in conjugate pairs. I'd skip it.

Corollary C.6. *Let z be a complex number. Then $\overline{z^n} = \overline{z}^n$ for all nonnegative integers n.*

If you had them do the previous theorem, then have them talk through the quick induction here.

Exercise C.7. Let's practice to get these computations down. For each pair of complex numbers z, w, compute $z + w, z - w, z \cdot w$, and z/w.

1. $z = 3 + 4i, w = 2 - i$
2. $z = 6, w = 3i$
3. $z = -7 - 2i, w = \sqrt{5} + 2i$
4. (Note: the imaginary part of w should be $1/\sqrt{2}$.) $z = -8 + 8i, w = (1/\sqrt{2}) + (1/\sqrt{2})i$

Students will need to be able to do all of these computation, especially division. I'd have them work all of these.

Exercise C.8. One of the really fun things about this imaginary unit i is the properties it has under exponentiation. Specifically, prove that for all integers k, we have $i^{4k} = 1, i^{4k+1} = i, i^{4k+2} = -1$, and $i^{4k+3} = -i$. (In other words, show that the powers of i cycle through the numbers $1, i, -1$, and $-i$.) *Solution:* $i^1 = i, i^2 = -1, i^3 = i^2 i = -i, i^4 = i^2 i^2 = (-1)(-1) = 1$. So, $i^{4k} = (i^4)^k = 1$, and therefore $i^{4k+1} = i^{4k} i = i, i^{4k+2} = i^{4k} i^2 = 1$, and $i^{4k+3} = i^{43} i^3 = -i$.

This classicly cool pattern has ramifications for cyclic groups in the theorem sequence, and just generally, math majors should know this anyway. Definitely worth assigning.

C.2 The Geometry of Complex Numbers

The main result for students to know in this section is Euler's formula and the polar form of a complex number. As mentioned before, focus on computations, not on theory.

Exercise C.11. For each complex number, identify its modulus and its nonnegative angle less than 2π.

1. $z = -2 + 2i$
2. $z = \sqrt{3} + i$
3. $z = -\frac{1}{\sqrt{12}} - \frac{1}{2}i$
4. $z = -5i$

This exercise, along with the next two, provide the computational play students need for using complex numbers in the theorem sequence.

Exercise C.12. Rewrite each of the complex numbers in Exercise C.11 in its standard polar form.

Comfort using Euler's formula to get the polar form is important for many of the exercises in the theorem sequence.

Exercise C.13. Once again, go back to the four complex numbers in Exercise C.11. Practice adding and multiplying several of them, but express this geometrically using rectangular coordinates for the sum and polar coordinates for the product.

This exercise emphasizes why comfort with both forms of a complex number are important.

Theorem C.15. *Let z, w be complex numbers. If $|z| = |w| = 1$, then $|zw| = 1$.*

This easy but important fact is used frequently as an example of a closed subset of $\mathbb{C}$ under multiplication. If you decide to present something from this appendix, this is a great choice.

C.3 Complex Solutions of Equations

This section's focus needs to be on the notation and form of the roots of unity. Many exercises use this section's results explicitly.

Theorem C.16. *Suppose $p(x) = a_n x^n + \cdots + a_1 x + a_0$ is a polynomial with real coefficients. If z is a solution to the equation $p(x) = 0$, then so is $\overline{z}$.*

This theorem can be safely skipped, but it does provide a very easy proof of why you always get complex solutions to polynomials occurring in conjugate pairs.

Theorem C.17. *Let $c = re^{i\theta}$ be any nonzero complex number, with $r > 0$. Then for any nonnegative integer n, the n distinct solutions to the equation $z^n = c$ are given by $z = r^{1/n} e^{i(\theta + 2\pi k)/n}$ for $0 \leq k < n$.*

This is the most important result in this appendix, one which most students probably don't know (or if they do, they don't know it well). This is the only other theorem worth presenting in this appendix. There is a small error, though. The integer n should be positive, not nonnegative.

Corollary C.18. *The n distinct solutions to the equation $z^n = 1$ are the complex numbers $\zeta_k = e^{i(2\pi k/n)}, k = 0, 1, \ldots, n-1$.*

This is a direct consequence of the previous theorem.

Exercise C.20. Solve the following equations, and graph the solutions.

1. $z^4 = 625$
2. $z^7 = -128$
3. $z^3 = -48i$
4. $z^6 = 27i$
5. $z^2 = \sqrt{3} - i$
6. $z^4 = -9 - 9i$
7. $z^6 = 1$
8. $z^{11} = 1$

This puts together the various pieces of this appendix. Don't have them work all of them; a few should suffice.

Theorem C.21. *Let* $\zeta_k = e^{i(2\pi k)/n}, k = 0, 1, \ldots, n-1$ *be an* n^{th} *root of unity. Then* $(\zeta_1)^k = \zeta_k$ *for* $0 \leq k \leq n-1$.

This is a minor observation, but it teases what's coming in the book.