Daily Assignments and Lectures
for Abstract Algebra I—Groups and Rings
Based on
Shahriar Shahriari, *Algebra in Action. A course in Groups, Rings, and Fields*, AMS, 2017.

Courses Based on the Text . Depending on the curriculum of your department and the mathematical background and mathematical maturity of your students, a number of different courses based on this text are possible. Some possibilities are as follows:

- **A course on Group Theory**. A solid semester course on Group Theory would cover chapters 1 through 6 followed by chapters 10 and 11. These chapters cover examples of groups (dihedral, symmetric, $\mathbb{Z}/n\mathbb{Z}$, the general linear group), basic group theory (cyclic groups, direct products, isomorphisms, and subgroups), symmetric and alternating groups, group actions, cosets and Lagrange's Theorem, conjugacy classes and the class equation, normal subgroups and quotient groups, and group homomorphisms. Time permitting, one can go back and do Sylow theorems (chapter 7), and/or Burnside counting (chapter 8). Limiting yourself to group theory, will allow for a more leisurely pace, and the possibility of significant group work in class. You can also spend more time on prerequisites (induction, 1-1/onto functions, basic properties of integers). There is no need to cover chapter 9 (lattice diagrams of subgroups) but it is a good idea to read through the chapter yourself and to introduce basic subgroup diagrams throughout the course. For such a course, the plan presented in the next few pages can be modified, and you still may find my commentary about the material in each section useful.
- **Group Theory and some Ring Theory**. This is what I do in my institution for our Abstract Algebra I course. In what follows, I have described my students and my course, and have provided a detailed list of my assignments and lecture topics. As you see I cover most of chapters 1 through 12 and 15 through the middle of chapter 19. Thus in addition to the group theory material described above, I also do enough ring theory to prove that a Euclidean domain is a principle ideal domain, and a principal ideal domain is a unique factorization domain. For my students, this is a fast paced class, and, in particular, the ring theory is a bit rushed. For this reason, I try, if possible, to squeeze in at least one more Ring Theory lecture (by going through the group theory a bit faster).
- **Group Theory and Ring Theory**. If your students are more sophisticated mathematically (maybe this is not the first time that they see this kind of material), then it may be possible to go through the early material more quickly and either cover more group theory (e.g.,

semidirect products, solvable and nilpotent groups) or cover more ring theory (complete the chapter on polynomial rings, do application to number theory).

- **Galois Theory (with a review of ring theory)**. This constitutes our Abstract Algebra II course, and I have provided a detailed list of assignments and lectures in a separate document. This course begins with a quick review of the needed ring theory, completes the chapter on polynomial rings, and goes through a solid course in Galois theory (chapters 21–28).

Audience The class plan presented in the following pages—the readings, the homework assignments, the additional practice problems, and the brief lecture notes—is from an Abstract Algebra I (Groups & Rings) class that I have been teaching at Pomona College for a number of years. The formal prerequisite for the class is a rigorous linear algebra class but the students are urged to take some form of a proof-based transition class (e.g., Combinatorics, Number Theory & Cryptography, Introduction to Analysis) before taking Abstract Algebra. While their facility with proofs varies substantially, the students have all had a class where they were expected to do some proofs. They have seen induction, know what a proof by contradiction means, can discern the difference between an example and a proof, and have seen "if and only if" statements. They have also seen functions discussed as maps and should be—famous last words—familiar with the concepts of 1-1 and onto functions. This doesn't mean that they are sophisticated when it comes to proofs. They are beginners, get confused with complicated or tersely worded proofs, and have no experience with the process of building intuition for an abstract algebraic object that you are meeting for the first time. Their previous classes expected them to understand proofs presented by others and to produce some simple arguments, and they find the expectations of this class much higher and more challenging. The students have had no prior experience with groups, rings, or fields. In my institution, most students taking the class are sophomores and juniors. A strong majority are math majors, but there are also students majoring in computer science or physics, and there are others who are taking this class as part of their math minor.

Class Organization This particular syllabus is for a semester long class meeting 3 times a week. I have organized the material for 40 fifty minute lectures, and usually—except for the midterms, and three holidays (in weeks 1, 10, and 15)—assign 3 home works a week. I like breaking each week's assignment into three parts for two reasons. It makes time management easier for the students, and it will allow them to study the solutions for each set before attempting the next. I actually often teach the class on a twice a week schedule with 75 minute classes (idiosyncratically, I continue to assign 3 home works even then), but it is easy enough to adjust. The lectures described are the right length only approximately. Often, I finish a topic in the next lecture or start next day's topic earlier. My pace also varies depending on the students in the class. For each class, the students are asked to read the appropriate section and hand in the assigned homework. It is certainly possible—and often a good idea—to break up the class with worksheets and group work. I sometimes begin the class with a short worksheet meant for group work. There are many problems in the text that can be modified for this purpose.

Reading the Text I want the students to read the text. It is written with this goal in mind and it is quite conversational. Being able to read a math text, decipher the notation, and understand

what is going on is a skill that my students do not have entering the class. My hope is that they will become better at it by the end of the semester. I do not hesitate to assign homework problems on material that we haven't yet covered in class. In fact, my ideal is that the students read the text, and attempt some of the problems, before we talk about them in class. Given the abstract nature of the material, I don't carry out this ideal, but, often, I will have them read a definition or even a section on their own before doing a problem. The students don't initially like this approach, but after I have explained the reasoning (several times), they start to warm up to it. Struggling on problems and a bit of initial frustration does lead to learning.

Hints, Short Answers, and Complete Solutions Some problems have hints, others have a short answer, and yet a third group of problems have complete solutions in the appendices. The problem number for this last group of problems is italicized. Ideally students work on a problem until they are stuck, and then they look for hints. Sometimes, I even assign as homework a problem that has a complete solution in the back. My instructions to the students are that they should try the problem themselves before looking at the solutions, and, in any case, their write up should be in their own words. Many of these problems are proofs to useful results, and I think there is value in learning how to read the solution to a problem and understand it well enough to write it in your own words.

The assignments and lecture notes For each assignment a list of 5 problems is provided. I ask the students to hand in 4 but they are responsible for eventually understanding all 5. There is also two to three extra practice problems. For each lecture the topic to be covered and a bit of commentary is included. The commentary is meant to give you an idea of my approach to the material.

Mini-Projects There are many additional problems in the text. Quite a few of them have their own heading and can be used for small individual or group mini-projects.

Week 1. Introduction; Symmetries of a regular polygon

Assignment. Read Preface.
Lecture 1. Introductions.
A bit about History of Algebra (several different historical threads are precursors of modern algebra: the quest to solve fifth degree equation and the quest to solve diophantine equations such as the one in Fermat's last theorem). Algebra is a language that will allow us to talk about symmetries as well as collections of numbers that behave like the integers. I give examples of problems that we will be able to solve and go over the syllabus for the class.

The first chapter is to set the stage by introducing 4 groups (without formally defining groups): D_n, S_n, $\mathbb{Z}/n\mathbb{Z}$, and $\mathrm{GL}(n, F)$. The last one can be skipped and the instructor should not get bogged down in this chapter. Except for a few properties of the integers, we don't need a formal development at this point. We mostly want to develop some intuition about these groups by calculating.

Assignment. Read Sections 1.1.
Lecture 2. D_n (Section 1.1).
Start with D_8. What are the symmetries of a square? It is helpful to have a physical square made of cardboard and with its corners labeled. Discuss the multiplication, and the use of algebraic notation to streamline finding products. Define D_8. Informally, mention that D_8 is closed under the multiplication, is associative, has an identity, and inverses. Briefly, discuss the multiplication table and possible patterns. Without a formal definition talk about groups being a generalization of what we see with D_8. A set with an operation that is closed, associative, has an identity, and inverses. It is an abstract object because when we say we have a group, we don't know what the elements are or what the operation is. We want to study a group in the abstract even though we will constantly come back to specific examples to get intuition and to test our conjectures.

Week 2. 1-1, onto functions; Integers mod n; Division Algorithm; General Linear Group; Definition of a group

Assignment. Read Section 1.2. Do Problems *1.1.1*, 1.1.5, 1.1.6, 1.2.1, 1.2.20. Extra Practice Problems 1.1.4, 1.2.7.
Lecture 3. S_n (Section 1.2).
Review the definition of bijective functions quickly. Note that a function has an inverse iff it is bijective. Define $\mathrm{Perm}(\Omega)$ and S_n. Discuss cycle notation and multiplication for elements of S_n. Mention that S_n is also closed, associative, has an identity, and inverses. Point out that $D_8 \leq S_4$. Commutative diagrams do not play that important of a role at this level, but it is not a bad idea to get students thinking about maps and diagrams early.

A word of caution. At this point, our main aim is to have a working knowledge of examples of groups in order to build intuition about the more abstract results that are about to follow. For this purpose, being able to write down the cycle notation and multiply elements of S_n is important, but a thorough understanding of 1-1 and onto functions is not. Of course, a good understanding of these concepts—injective, surjective, and bijective maps—in important in many areas of mathematics, and becomes critical in Chapter 11. They will also appear in Chapter 2 when we discuss isomorphisms.

If your students are struggling with these concepts, then my suggestion would be to give the relevant definitions here but to focus on the finite case and on the permutations of a finite number of elements. Then gradually and through the following few weeks, assign problems (or worksheets) so as to slowly build the students' background. The point is that, in my opinion, you don't really want to get bogged down this early on but you don't want to ignore the issue either.

Assignment. Read Section 1.3 including pp. 22-28. Do Problems 1.2.4, 1.2.6, 1.2.11, 1.2.15, 1.3.1. Extra Practice Problems 1.2.5, 1.2.16.

Lecture 4. $\mathbb{Z}/n\mathbb{Z}$ (Section 1.3).

The arithmetic of integers mod n; $(\mathbb{Z}/n\mathbb{Z}, +)$ has the same properties as D_8 and S_4 albeit the addition also being commutative. The next motivating project is to find a subset of $\mathbb{Z}/n\mathbb{Z}$ that has the group properties under multiplication. 1 is the identity, and if a and b are invertible, then so is ab. So, accepting that multiplication is associative, and if we let $(\mathbb{Z}/n\mathbb{Z})^\times$ denote the set of invertible elements of $\mathbb{Z}/n\mathbb{Z}$, then $(\mathbb{Z}/n\mathbb{Z})^\times$ does have the four properties of a group. What are its elements? Prove the division algorithm, and the fact that $\gcd(a, b)$ is a linear combination of a and b, for their own right but also to prove that $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of those integers between 1 and n that are relatively prime to n. As a corollary $\mathbb{Z}/p\mathbb{Z}$, where p is a prime, is a field. The well-ordering principle—which is how many of the induction proofs in algebra are organized—the greatest common divisor, and the Euler ϕ function should be mentioned.

Assignment. Read Sections 1.4 and 2.1. Do Problems 1.3.2, 1.3.6, 1.3.9, 1.3.13, 1.4.2. Extra Practice Problems 1.3.4, 1.3.10, 1.4.1.

Lecture 5. GL(n, p), Definition of a group (Sectiosn 1.4 and 2.1).

Quickly and briefly talk about the general linear group. This section and the example of the general linear group can be completely skipped. Explain that the scalars in the matrices can be reals, complexes, rationals, or from $\mathbb{Z}/p\mathbb{Z}$ where p is a prime. In this early stage, when we say a field, we mean one of these four. Mention that a field is a set of elements where we can do all four arithmetical operations (addition, subtraction, multiplication, and division by non-zero elements). You may want to mention the more general concept of a field but introducing general fields at this stage is not recommended. Introduce the notation GL(n, p) and SL(n, p). If students have not had a solid course in linear algebra, then skip this example altogether (and do not assign any of the problems that include matrices). It is unrealistic to want to incorporate groups of matrices if the students don't already have a feel for matrix operations.

Start Chapter 2 by giving a formal definition of a group. This section should not take that much time, since we have already been discussing groups for a good part of two weeks. Note that D_8, S_4, $\mathbb{Z}/6\mathbb{Z}$, $(\mathbb{Z}/8\mathbb{Z})^\times$, and SL$(2, 3)$ are examples of groups. In fact, these are good examples of groups to try conjectures on. Just about any question should first be tried on these groups (SL$(2, 3)$ is harder to get to know than the others and could be ignored early on). The students should be encouraged to have an expanding set of examples that they know very well. Define abelian groups, and discuss two guiding questions: (1) How do we prove that a group is abelian? (2) How many "different" groups of order n are there?

HW Note. The strange group in Problem 1.3.6 is more fully explored in Problems 2.3.5, 2.5.12, and especially 2.7.11.

Week 3. Cancellation; Cyclic Groups; Isomorphisms; Direct Products; Subgroups.

Assignment. Read Sections 2.2 and 2.3. Do Problems 1.3.15, 1.4.4, 1.4.11, 1.5.6, 2.1.2. Extra Practice Problems 1.4.3, 2.1.3, 2.1.6.

Lecture 6. Cancellation & Cyclic Groups (Sections 2.2 and 2.3).

Do the cancellation properties, prove the elementary properties of Lemma 2.22, and mention that this lemma does explain the fact that in a multiplication table of a group no element is repeated in any row or column. (Theorems 2.24 and 2.25 show that, for finite semigroups, you can get inverses from the cancellation properties. This can be skipped even though the proof gives the students a chance to become familiar with the kind of element-wise argument that is possible for finite groups.)

Define cyclic groups and order of an element; Theorem 2.37 (If a is a generators of finite cyclic group, then you can start with a and find only positive powers of a, as soon as you hit e, you have all the elements of G) does have content and is used often. Contrast the multiplicative notation and the additive notation (used only for abelian groups). State (and either prove or assign as homework) the fact that if $x^s = e$ then $o(x) \mid s$.

HW Note. Problem 1.3.15—which has a hint in Appendix A—is a statement from number theory: $(p-1)! \equiv -1 \mod p$, for primes p. Here, however, the proof is group theoretic. This (that is, number theory facts proved through group theory) will be a thread through the problems.

Assignment. Read Sections 2.4 and 2.5. Do Problems *1.4.9*, 2.1.8, 2.2.1, 2.2.4, 2.3.1. Extra Practice Problems 2.2.2, *2.2.3*, 2.3.4.

Lecture 7. Isomorphisms & Direct Products (Sections 2.4 and 2.5).

Define isomorphisms, and drive home the idea that two groups are isomorphic if and only if we can relabel the elements of one of the groups so that the two multiplication tables become identical. Prove that two cyclic groups of the same order are isomorphic, and, so, for every order, we have exactly one cyclic group of that order. Mention homomorphisms, and time-permitting prove that the homomorphic image of an abelian group is abelian. The thorough study of homomorphisms is picked up in Chapter 11, but we do want to be able to say that this group is "different" than that group and so introducing the concept of isomorphic groups early is important.

Direct products allow us to construct new groups from ones we already know. Go over examples such as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and and the fact that it is *not* isomorphic to $\mathbb{Z}/4\mathbb{Z}$ (but is isomorphic to $(\mathbb{Z}/8\mathbb{Z})^\times$). Whenever you get a chance, stop and ask how many different groups of order n, for small positive integers n, we know. For each order there is the cyclic group of that order. We now know that there are at least two groups of order 4, and we have two groups of order 6 ($\mathbb{Z}/6\mathbb{Z}$ and D_6), and several of order 8. Eventually for various very small orders, we can prove that we know *all* groups of that order.

HW Note. Problem 2.1.8 may seem impossible at first. After all isn't the identity automatically a 1-1 function? The point is that if none of the functions are 1-1, then a function other than the

identity function plays the role of the identity element. You can find an example with two functions whose domain and codomain are $\{1, 2, 3\}$.

Assignment. Read Section 2.6. Do Problems *2.2.5*, 2.3.6, 2.3.15, 2.4.1, 2.4.6. Extra Practice Problems 2.3.9, 2.3.13, 2.4.3.

Lecture 8. Subgroups (Section 2.6).

Define a subgroup of a group G generated by a subset $X \subseteq G$. Discuss the fact that subgroups carry information about the bigger structure, and we have a strong preference for arguments that use subgroups in place of elements. Define Centralizer, and prove that it is a subgroup. In algebra, when faced with a binary question (those with a yes or no answer), we prefer to find an algebraic structure that encodes the answer and provides a spectrum of answers. For example, instead of "Is G abelian?" we ask "What is the center of G?" Instead of "is x in the center of G?" we ask "What is the centralizer of x?" Not only these the answers to these revised questions carry more information, they may even be easier to answer since restrictions that our theorems put on subgroups may help us answer the questions. Prove that for a finite subset of a group to be a subgroup, we only need to prove closure. Complete discussion of subgroups by proving that subgroups of cyclic groups are cyclic.

Week 4. The Alternating Group; Group Actions; Cayley Graphs

Assignment. Read Sections 3.1 and 3.2. Do Problems 2.3.16, *2.3.19*, 2.3.21, 2.4.8, 2.5.7. Extra Practice Problems 2.3.22, 2.5.5, 2.5.6.

Lecture 9. A_n (Sections 3.1, and 3.2).

Go over the material in 3.1 somewhat quickly since students are already familiar with S_n. No need to write formal proofs. The meat of this chapter is one theorem: Every permutation is either odd or even. Even before proving this fact, we define the alternating group as the collection of even permutations. We (easily) prove that it is a group and that the number of odd permutations is the same as the number of even permutations. We need a careful argument that there is no permutation that is both odd and even. It then follows that the size of A_n is $n!/2$.

HW Note. Problem 2.3.19—with a solution in Appendix C—is important. It tells us which powers of the generator in a cyclic group are generators themselves. As a result, we know that a cyclic group of order n has $\phi(n)$ generators. Problem 2.3.21 is not particularly profound, but it reminds the students that permutations and group theory concepts come up in many places. In Problem 2.4.8, the group Q_8, one of the two non-abelian groups of order 8, is introduced.

Assignment. Read Section 4.1. Do Problems *2.4.9*, 2.5.10, 2.6.2, 2.6.9, 2.6.22. Extra Practice Problems 2.6.3, 2.6.12, 2.6.13.

Lecture 10. Actions (4.1).

Define an action, and give examples. Actions will be the mainstay of this course and will actually give rhyme and reason to the study of group theory. One way to help students think about actions is to pretend that you hold the elements of the group in your hand, and that the set elements are sitting on the floor. To say that your group acts on the set, means that if you throw one element of the group into the set, the elements of the set switch places. The action of that one element gives a

permutation of the elements of the set. Moreover, if you throw the identity in nothing happens, and the action respects the group multiplication in the sense that instead of throwing in the element x and then the element y, you can just throw in the element yx.

Focus on actions of groups on groups. Discuss both Regular and Conjugation actions.

HW Note. Problem 2.4.9—with a solution in Appendix C—establishes by brute force that there are only two groups of order 4. In Problem 2.5.10, we show that if m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$. This is a little fact from number theory, but it is proved here by counting the number of generators for appropriate cyclic groups.

Assignment. Read Section 4.2. Do Problems 2.6.27, 2.6.32, 3.1.6, *3.1.9*, 3.2.4. Extra Practice Problems 3.1.4, 3.1.10, 3.2.1.
Lecture 11. Cayley digraphs (Section 4.2).

Cayley digraphs (optional) help visualize the action of a group on a set, and make the abstract concept easy to follow. (Section 4.2 is very short. Hence, this lecture is an opportunity to catch up or to forge ahead to Stabilizers and Orbits.)

HW Note. Problem 2.6.27 introduces conjugate subgroups. In section 2.6, conjugating is just a way of constructing new subgroups from the ones we already have. In chapter 4, however, conjugating subgroups is an action of the group on the set of all subgroups. Students's intuition sometimes leads them astray in Problem 3.1.6. One may not believe that the product of two three-cycles can be a five cycle or an element of order 2. Problem 3.1.9—with a solution in Appendix C—tells us how to conjugate in S_n. One of its consequences is that two elements of S_n are conjugate if and only if they have the same cycle type. This will allow us to count the size of conjugacy classes in S_n, for example, in Problem 4.4.16.

Week 5. Stabilizers; Orbits; Cosets & Lagrange's Theorem

Assignment. Read Sections 4.3 and 4.4. Do Problems 2.6.23, 3.2.7, 4.1.7, 4.2.4, *4.3.3*. Extra Practice Problems 3.2.5, 4.1.4, *4.1.5*.
Lecture 12. Stabilizers & Orbits (Sections 4.3 and 4.4).
When a group acts on a set, there are certain things we always ask. What are the stabilizers of elements? These are always subgroup of the group (and, in fact, a good way of constructing subgroups or proving that certain subsets are subgroups). What are the orbits? The orbits are subsets of the set and *partition* the set. Briefly go over equivalence relations but the main equivalence relation used in group theory is the one that comes from actions. Actions are the unifying theme for the group theory section of the class. Our approach is that groups reveal themselves not when they are sitting around but when they act. For the rest of the course, we analyze one action after another. For each such action, we use the general tools that we develop for actions (stabilizers and orbits are the most important) and ask "What does this action reveal about the group?"

HW Note. Problem 2.6.23 is another example of a number theory fact proved using group theory. In the paragraph before Problem 4.3.3, the normalizer of a subgroup is defined, and Problem 4.3.3—with

a solution in Appendix C—asks the students to compute two normalizers. In most texts, normalizers make an appearance after normal subgroups. In this text, normal subgroups are formally defined in Chapter 10, but normalizers appear early. Normalizers are just stabilizers of an action and so they are automatically a subgroup. We could define a normal subgroup right here as well. A subgroup is normal if and only if its normalizer is the whole group. In other words, a subgroup is normal iff it is fixed by the conjugation action of the group on the set of subgroups. By seeing and working with conjugate subgroups and normalizers early on (e.g., Problems 2.6.27, 4.1.5, 4.3.3), the students will be quite ready to grasp the import of normal subgroups.

Assignment. Read Sections 5.1, 5.2. Do Problems 2.6.24, *2.6.33*, 3.3.3, 4.4.6, 4.4.9. Extra Practice Problems *4.2.5*, 4.3.8, 4.4.13.

Lecture 13. Translation Action, Cosets, & Lagrange's Theorem (Sections 5.1 and 5.2).

A subgroup $H \leq G$ acts on G by left multiplication. As soon as a group acts, there are things to be learned. In this action, the stabilizers are trivial and uninteresting, but the orbits are *cosets* of the subgroup. One of the cosets is the subgroup itself and the other cosets can be thought of as translations of the subgroup and hence the action is called the *translation* action. We know orbits partition the set, and so cosets partition the group. Easy enough to show that two cosets have the same size, and so the size of the group is the number of cosets times the size of the subgroup. This is Lagrange's Theorem and puts severe restrictions on what subgroups are possible. A group of order 25 can't have a subgroup of order 7 and so it can't also have an element of order 7. This argument shows that the order of an element divides the order of the group. It also gives a classification of groups of order p, where p is a prime. Take a moment to reflect on the fact that we have proved that if you have a set with 47 elements, and a multiplication rule that follows the seemingly innocuous four properties of a group, then we have proved that there is just one possible multiplication rule. This is a problem that can be described to a layperson but without thinking structurally—e.g., through subgroups—it would not be so intuitive.

In discussing cosets emphasize Lemma 5.6 giving equivalent conditions for two cosets being the same. A particular coset may be called Hx or Hy. The fact that cosets have aliases means that whenever we make a definition for a coset, we have to be sure that it is independent of the particular alias. Discuss the index of a subgroup and prove that, for finite groups, they have a multiplicative property (Corollary 5.19).

Given the machinery of actions, the gist of sections 5.1 and 5.2 can be done quickly. If you have time, give further applications of Lagrange's Theorem. A really nice argument—that illustrates the value of using subgroups—proves that the index of the center cannot be a prime number.

HW Note. Problem 2.6.33 which follows 2.6.31 & 2.6.32 (and which has a solution in Appendix C) is an important result. It tells us that HK is a subgroup if and only if $HK = KH$. Problem 3.3.3 is part of a series of problems (3.3.3–3.3.5) that explore a curious and fascinating permutation puzzle.

Assignment. Read Section 5.3. Do Problems 3.3.4, 4.4.10, 4.4.16, 5.1.1, 5.1.6. Extra Practice Problems 5.1.2, 5.1.4, 5.1.9.

Lecture 14. Fermat's little Theorem (Section 5.3).

An application of Lagrange's Theorem is a quick proof of Euler's Theorem in number theory. The

group $(\mathbb{Z}/n\mathbb{Z})^\times$ has $\phi(n)$ elements and so raising any of the elements to the power $\phi(n)$ gives 1. That is basically it. There are a few details to fill in (e.g., the case $a > n$) but those are straightforward details, are done in the book, and could be left to the students. (This section optional, and this slot could be used to catch up or to allow more time for the FCP and conjugation action in Chapter 6.)

HW Note. Problem 5.1.6 is essentially saying that a subgroup of index 2 is normal in the group.

Week 6. FCP; Conjugation

Assignment. Read Sections 6.1 and 6.2. Do Problems 3.3.5, 5.1.17, 5.2.1, 5.2.4, 5.2.12. Extra Practice Problems 5.2.2, 5.2.3, 5.3.1.

Lecture 15. Fundamental Counting Principle (Section 6.1) & Conjugation Action (Sections 6.2).
State and prove the FCP. The relation between sizes of orbits and stabilizers can be seen as a generalization of Lagrange's Theorem, and can be employed as soon as we have an action of a group. In the rest of the chapter, we apply this to the conjugation action. Remind the students of the conjugation action of a group on itself and apply the FCP. We immediately get that the size of the conjugacy class of an element is the index of its centralizer, and so divides the size of the group.

HW Note. Problem 5.1.17 is a prelude to Problem 5.1.19 where we give a proof that A_4 does not have a subgroup of order 6. Problem 5.2.12 is the first of a sequence of problems (5.2.12–5.2.16) about the indices of two subgroups U and V of a group G. If you draw G, $\langle U, V\rangle$, U, V, and $U \cap V$, then always, and regardless of the context, the index of $U \cap V$ in V is less than or equal to the index of U in $\langle U, V\rangle$. By switching the roles of U and V, it is also true that $|U : U \cap V| \leq |\langle U, V\rangle, U|$. This is best remembered by Figure 9.14 of chapter 9. The legs of the quadrilateral going from the subgroups to the subgroup generated by them is at least as long as the legs going from the subgroup down to their intersection. And these two indices are actually equally if and only if UV is a group. Moreover, $UV = G$ is a group if $|G : U|$ and $|G : V|$ are relatively prime. This circle of ideas allows for some deeper investigation of specific examples. Many of these problems are actually solved in Chapter 9 and there is a recap there as well.

Assignment. Read Sections 6.3 and 7.1. Do Problems 5.1.10, 5.1.19, 5.2.5, 5.2.13, 6.1.3. Extra Practice Problems 5.2.7, 5.2.8, 6.1.1.

Lecture 16. Center of p-groups (Section 6.3) and Binomial Coefficients (Sections 7.1) .
The fact that conjugacy classes partition the group, and that their sizes are divisors of the size of the group immediately proves that a p-group has a non-trivial center. Since centers cannot have prime index, we have that every group of order p^2 is abelian. You can mention the class equation—just writing the order of a group as the sum of the sizes of conjugacy classes—but no need to make a big deal of it.

Actions allow us to move quickly and prove deeper results fast. This was already illustrated in the proof of Lagrange's Theorem and in proving that groups of order p^2 are abelian. We have the tools to prove Sylow's existence theorem now. I like doing that because it gives us a powerful tool early on. However, the instructor could postpone this till Chapter 12, there would be no real harm, just minor adjustments to some of the assignments. To be able to prove Sylow's theorem at this point, we have to know one fact about binomial coefficients. If $n = p^\alpha m$, where p is a prime and m an

integer not divisible by p, then $\binom{n}{p^\alpha}$ is not divisible by p. There is a complete proof of this fact in Section 7.1. Decide how much of the details to do in class.

HW Note. Problem 5.1.19 shows that A_4 has no subgroup of order 6 showing that the converse of Lagrange's Theorem is false.

Assignment. Midterm I—In Class Part.

Week 7. Sylow and Cauchy's Theorems; The Counting Lemma; Lattice Diagrams

Assignment. Read Sections 7.2. Midterm I—Take Home Part Due.
Lecture 17. Sylow's E Theorem, Cauchy's Theorem (Section 7.2).

Converse of Lagrange's theorem is not true (A_4, for example, does not have a subgroup of order 6) but Sylow's theorem salvages a partial converse. To prove Sylow's Theorem, we use Wielandt's brilliant and simple proof (that does not rely on quotient groups). Prove Sylow's theorem. Get Cauchy's theorem (if p divides the order of a group, then the group has an element of order p) as a corollary to Sylow's theorem.

Section 7.3 gives an outline of the proof of the other Sylow theorems and asks the reader to fill in the blanks. I don't cover this section at this time. Instead, I slowly assign the proofs for the students to do and struggle with (some of the problems have a complete proof in Appendix C). I come back to these when doing Chapter 12.

Assignment. Read Sections 8.1 and 8.2. Do Problems 5.2.14, 6.1.4, 6.2.13, 6.3.2, 7.2.3. Extra Practice Problems 6.2.1, *6.2.5*, *6.2.11*.
Lecture 18. The Cauchy-Frobenius counting lemma (Sections 8.1 and 8.2).

The counting lemma that is not due to Burnside (the Cauchy-Frobenius lemma) has applications to combinatorics. This chapter is optional and can be skipped if you are short of time. Otherwise, prove the counting lemma (Theorem 8.4) and do some applications from Section 8.2. I like counting the number of ways to color the faces of a cube using m colors.

HW Note. Problem 6.2.13 asks for the number and size of conjugacy classes of S_5. We know that each conjugacy class consists of elements of the same cycle type. Later, in Problem 6.2.15, we leverage what we found in Problem 6.2.13 and the fact that the size of a conjugacy class is the index of the centralizer to find the number of sizes of conjugacy classes of A_5. In chapter 10, we will use this information to prove that A_5 is simple.

Assignment. Read Section 9.1. Do Problems 4.5.1, *5.2.15*, 7.2.4, 7.2.6, 8.1.3. Extra Practice Problems 7.2.2, 7.2.5, *7.2.7*.
Lecture 19. The poset of subgroups (Section 9.1).
The set of subgroups of a group form a partially ordered set. Thinking of these subgroups as a poset and drawing partial Hasse diagrams of this poset helps tremendously in keeping track of arguments

about group theory. Having said that, you can touch on this topic at various levels of detail. Define a poset and its Hasse diagram. Explain that the subgroups of a group form a poset and that we like to draw partial lattice diagrams of this poset. Adding edge lengths to the edges in the Hasse diagram (if $H < K$, then the edge from H to K will have length $|K : H|$) is particularly helpful. Most of these ideas can be done via examples and with not as much detail as in the book. In particular, the "lattice" property of this poset can be skipped. Draw the lattice of subgroups of D_8 and use it to make some arguments (e.g., What is the centralizer of $\langle b\rangle$? Since this is a subgroup and contains $\langle b\rangle$, and the center of the group, by looking at the lattice of subgroups, we can limit the choices to $\langle a^2, b\rangle$ and D_8. Checking one element, then decides the issue.)

Week 8. Normal Subgroups and Normalizers

Assignment. Read Section 9.2. Do Problems 5.4.8, 7.2.8, *7.3.1*, 8.1.4, 8.2.1. Extra Practice Problems 7.2.9, 7.2.10, 8.1.1.

Lecture 20. When is HK a subgroup? (Section 9.2).

A few theorems that were Problems earlier in the book are reviewed in section 9.2 and they are very useful. Theorem 9.27 (the index of H in $\langle H, K\rangle$ is never smaller than the index of $H \cap K$ in K) is more memorable if accompanied by a diagram. If you have two subgroups H and K of a group, then in drawing them, an important question is whether HK is a subgroup. If it is, then we draw a parallelogram (and use as a mnemonic the fact that opposite sides of a parallelogram are equal). Proposition 9.28 and 9.30 give sufficient (and some necessary) conditions for HK to be a subgroup. Regardless of how much of Chapter 9 you do, and if you are going to do Chapter 12 later on (going somewhat deep into finite group theory), then you should make sure that the students are comfortable with the conditions for HK to be a subgroup. Depending on how far behind or ahead you are, you can decide how much of the proofs to do in class.

HW Note. Let G be a group of order 10^6 and assume that you check 4 randomly chosen elements and they are all in the center. Problem 5.4.8 asks you to prove that G is abelian with a very high probability. Problem 7.3.1 asks for a proof of the Sylow D Theorem. It is quite unreasonable to ask a student to do this. However, there is an outline of the proof in the text and a complete solution in Appendix C. I want the students to struggle with deciphering and understanding the proof. So this is more of a reading and understanding than a figure it out problem.

Assignment. Read Section 10.1. Do Problems *7.3.3*, 8.2.2, 8.2.7, 9.1.3, 9.2.6. Extra Practice Problems 8.2.5, 9.1.4, *9.2.5*.

Lecture 21. Normal subgroups (Section 10.1).

The center of a group could be defined as the elements of the group that were fixed by the conjugation action. Normal subgroups are the subgroups of G that are fixed by the conjugation action of G on the set of all subgroups. This is equivalent to right and left cosets being equal, and the two subgroups xHx^{-1} and H being equal for all $x \in G$. All three ways of looking at normal subgroups (via cosets, via conjugate subgroups, or as fixed points of an action) can be helpful. Give some examples, and prove that if $H \lhd G$ then HK is a subgroup for any other subgroup K of G. This is very helpful in drawing diagrams.

HW NOTE. Problem 7.3.3 asks for a proof of the fact that the number of Sylow subgroups is the index of the normalizer. Again there is an outline in the text and complete solution in Appendix C. Problem 9.2.6 wants the reader to get in the habit of drawing a partial lattice diagram of the subgroups involved.

Assignment. Read Section 10.2. Do Problems *7.3.5*, 9.2.7, 10.1.2, 10.1.9, 10.1.13. Extra Practice Problems 10.1.1, 10.1.6, 10.1.10.
Lecture 22. Normalizers (Section 10.2).
In the action of a group on its subgroups by conjugation, what are the stabilizers? The stabilizers in this action are called normalizers. Instead of asking "Is H normal in G?", we like to ask "What is the normalizer of H?" Theorem 10.18 brings together various characterizations of normality.

HW NOTE. Problems 7.3.5, 7.3.7, and 7.3.9 work through the proof of the last of the Sylow Theorems. All have a complete solution in Appendix C.

WEEK 9. QUOTIENT GROUPS; GROUP HOMOMORPHISMS

Assignment. Read Section 10.3. Do Problems 10.1.14, 10.1.18, 10.2.5, 10.2.11, *10.2.15*. Extra Practice Problems *10.1.17*, 10.2.4, 10.2.10.
Lecture 23. Quotient groups (Section 10.3).
The concept of a quotient group is sometimes difficult for students. Using examples show that if $N \lhd G$, we can turn the right cosets of N into a new group called the quotient group. This can't be done if N is not normal in G. Do examples (Figures 10.4, 10.5, and 10.6 drive home the idea), and mention simple groups and their role in group theory. An approach for studying groups is to first try to find a non-trivial normal subgroup, then study this subgroup and its quotient group. Both of these groups are smaller than the original group and easier to analyze. Maybe we can take information from the normal subgroup and the quotient group and make conclusions about the original group. In this scheme, finding non-trivial normal subgroups is crucial and the building blocks are simple groups. You have to know things about simple groups if you want this project to succeed.

HW NOTE. Problem 10.1.17 (among the extra practice problems) has a solution in appendix C and is a good warmup for Problem 10.1.18. In both cases, we draw an appropriate diagram. Problem 10.2.15—with a solution in Appendix C—says that a subgroup is normal if and only if it is a union of conjugacy classes. (It is possible to have a union of conjugacy classes not be a subgroup, but if it is a subgroup, it is normal.) This is a helpful result and it provides my preferred method (Problem 10.2.17) to prove that A_5 is not simple.

Assignment. Read Sections 11.1 and 11.2. Do Problems 10.2.17, 10.2.21, 10.3.1, 10.3.3, *10.3.11*. Extra Practice Problems 10.2.22, 10.3.6, 10.3.8.
Lecture 24. Group Homomorphisms; Kernel and image (Sections 11.1 and 11.2).
Define group homomorphisms, give examples, and prove elementary facts about them. Define the kernel and image of a group homomorphism, discuss the cosets of the kernel, and bring out the connection with being 1-1 and onto. Proposition 11.14 and the accompanying Figure 11.1 is helpful. Prove that the kernel is a normal subgroup.

HW Note. Problem 10.2.17 concludes that A_5 is a simple group. We know, by Problem 6.2.15, the sizes of conjugacy classes of A_5. If A_5 had a normal subgroup, it would be a union of these classes (Problem 10.2.15), but the only way the sizes of the classes add up to a number dividing 60 is if we get 1 or 60, and this completes the proof. The situation in Problem 10.2.21 comes up often. We have two normal subgroups with trivial intersection. In this problem, we prove that the elements of one normal subgroup commute with the elements of the other one. Problem 10.3.11 is a prelude to the homomorphism theorems as applied to the canonical homomorphism.

Assignment. Read Section 11.3. Do Problems *7.3.7*, 10.3.7, 10.3.9, 11.1.2, 11.1.10. Extra Practice Problems 11.1.5, 11.1.9, *11.1.11*.
Lecture 25. First isomorphism Theorem and Canonical Homomorphism (Section 11.3).
Discuss and prove: If $\phi\colon G \to H$ is a group homomorphism, then $G/\ker(\phi) \cong \phi(G)$. Give a preview of the homomorphism theorems that state that the lattice of subgroups of G that contain $\ker(\phi)$ is the same as the lattice of subgroups of $\phi(G)$. One way of thinking of this is that $G/\ker(\phi)$ is the part of the lattice diagram of G "above" $\ker(\phi)$.

Every kernel is a normal subgroup but every normal subgroup is also a kernel. Prove this by introducing the canonical homomorphism. This also points out that the "right" way of defining normal subgroups is to say that normal subgroups are those subgroups that are kernels of homomorphisms. In fact, we define the special objects of each algebraic structures this way. In ring theory, ideals will be the kernels of ring homomorphisms. Note that, for a vector space, all subspaces can be kernels of linear transformations and so, in this sense, every subspace is a "normal" subspace.

HW Note. Problem 7.3.7—with a solution in Appendix C—continues the proof of the last of Sylow theorems.

Week 10. Actions and Homomorphisms; Homomorphism Theorems

Assignment. Read Section 11.4. Do Problems *7.3.9*, 10.3.12, 11.1.12, 11.3.1, 11.3.6. Extra Practice Problems 11.2.1, *11.2.5*, 11.3.2.
Lecture 26. Actions and Homomorphisms (Section 11.4).
If we want a normal subgroup, we find a homomorphism of the group and find its kernel. But how do we construct homomorphisms. Of course, via actions! As soon as you have an action of a group on a set, you also have a homomorphism of the group into the group of permutations of the set. This is a win-win situation. Either the kernel of the homomorphism is not $\{e\}$, in which case we have found a non-trivial normal subgroup, or the kernel is just $\{e\}$, in which case we have found a copy of our group inside some symmetric group. This idea—used with the right action—proves Cayley's Theorem.

HW Note. Problem 7.3.9—with a solution in Appendix C—completes the proof of the last of the Sylow theorems. Problem 11.3.1 drives home the point that the kernel of a homomorphism is a *normal* subgroup.

Assignment. Read Section 11.5. Do Problems 10.3.14, 11.3.3, 11.3.8, 11.4.2, 11.4.5. Extra Practice Problems *10.3.13*, *11.3.9*, 11.4.1.
Lecture 27. Homomorphism Theorems (Section 11.5).

State the homomorphism theorem, Theorem 11.38, and point out that parts of it have already been proved (others were among the assigned problems). A complete proof, for the record, is in the text. Pick and choose which parts (if any) to prove in class. (At this point, the correspondence, between subgroups of the domain that contain the kernel and the subgroups of the image, should make sense to the students, and there is diminishing returns in laboriously going through the whole proof) Do discuss one example in detail, and possibly do the Direct Diamond theorem (theorem 11.43).

Section 11.6 on Inner Automorphisms, Automorphisms, and the N/C theorem (Theorem 11.47) is interesting, and brings lots of what we have done together. But it is quite optional. Do it only if you have time and are ahead of your schedule.

The third slot for this week is for a holiday or for catching up.

Week 11. Intro to Ring Theory; p-Groups

Assignment. Read Sections 15.1, 15.2, and 15.3. Do Problems 10.4.2, 11.4.8, 11.5.2, 11.5.5, 11.5.8. Extra Practice Problems *11.4.3*, 11.5.4, *11.5.7*.

Lecture 28. Introduction to Ring Theory (Sections 15.1 and 15.2).

I break the study of groups at this point to go through the first two introductory sections of ring theory. The students usually expect ring theory to have the same flavor as group theory, and they would like to be able to use the same guiding principles to study rings. At some general level this does work. We have rings and subrings, and the subrings that are kernels of homomorphisms—namely ideals—play a special role. We can mod out by ideals and we have basically the same homomorphism theorems as in groups. It is worthwhile to point out the similarities (and that they could be studied once and for all algebraic structures through category theory), but it is also important to see that each algebraic structure has its own guiding principles. For this reason, I like to spread out early ring theory problems in order to give the students a chance to gain some experience with rings before we delve into their study. You can, of course, rearrange the assignments, and finish group theory before starting ring theory.

The motivating question for commutative ring theory is to be able to do number theory in sets bigger than the ordinary integers. Do one of the examples in the text—not in the gory detail done there—to show that if we had unique factorization into primes in sets of numbers larger than integers, we could solve diophantine equations. Then define a ring, give examples, mention basic properties, and define integral domains, division rings, and fields. Note that we have made some common but not universal choices. Our definition of a ring does not assume the existence of a multiplicative identity (most of what we do is, however, for "rings with identity"), and as a result all ideals are subrings. We also do not consider $\{0\}$ as an integral domain (in our definitions, integral domains have to have more than one element). Hence, the expression "non-trivial integral domain", seen in many other texts, is redundant here. While in finite group theory, our prototypical group was the symmetric group S_n, in commutative ring theory, our prototypical ring is $\mathbb{Z}$, the ring of integers. We try to see which properties of the integers generalize to which classes of rings. While not that important in the rest of the course, the fact that finite integral domains are fields (section 15.3) explains why, unlike in

group theory, most rings that we consider are infinite. (You can mention this and refer the students to the text for the straightforward proof.)

Assignment. Read Sections 12.1 and 12.2. Do Problems 15.1.3, *15.2.1*, 15.2.4, 15.2.5, 15.2.12. Extra Practice Problems 15.2.2, 15.2.3, *15.2.7*.

Lecture 29. *p*-groups, Existence of normal subgroups (Sections 12.1 and 12.2).

For p-groups the converse of Lagrange's Theorem holds. This together with Sylow's Theorem means that if a power of a prime divides the size of the group, then the group will have a subgroup of that size. The proof illustrates the way we can use quotient groups and induction as a one-two punch. A quotient group gives us a smaller group and we can apply induction on the smaller group.

We like to find non-trivial normal subgroups. Theorem 12.4 helps in this endeavor. If $H \leq G$, then the theorem gives a normal subgroup with certain properties. The properties are used to sometimes prove that the normal subgroup obtained is not trivial. This theorem is proved using a common technique. First define an appropriate action of the group. This action gives a homomorphism from the group to a symmetric group and the kernel of the action is the sought after normal subgroup.

HW Note. Problem 15.1.3 is the multiplicative property of norms that will be very useful when we are looking for units and irreducible elements in quadratic integer rings. Students's attempt to bring their group theory intuition into ring theory sometimes backfires. In group theory, there was only one group—up to isomorphism—of order 3. But there is more than one ring of order 3 as Problem 15.2.1—with a solution in Appendix C—demands. In group theory, we often used direct products of groups as a way to create new groups from old ones. Problem 15.2.4 explains why this doesn't work as well in ring theory. The direct product of two integral domains is never an integral domain (recall that in our definition of integral domains, an integral domain has at least two elements and so $0 \neq 1$).

Assignment. In Class Midterm II.

Week 12. Structure of Finite Groups; Ideals, Ring Homomorphisms

Assignment. Read Section 12.3. Midterm II Take-Home Part due.

Lecture 30. Applying Sylow theorems to analyze the structure of groups (Section 12.3).

Recall the Sylow Theorems. We have already proved Sylow E in Chapter 7, and there were outlines of the other proofs (some were proved completely in Appendix C). Either assign the proofs to the students, do the proofs now yourself, or discuss the outlines of the proofs. All are again based on group actions. Then proceed to apply these theorems to show that a whole slew of groups are not simple. The examples in the text show different ways of using the Sylow theorems, and the arguments are typical of arguments in finite group theory. Do as many as you have time.

Assignment. Read Section 16.1. Do Problems 11.4.9, *11.5.11*, 12.1.4, 12.2.2, 15.2.14. Extra Practice Problems *12.1.3*, *12.2.3*, *12.2.5*.

Lecture 31. Ring Homomorphisms and Ideals (Section 16.1).

Given the similarity with groups, many of the details of arguments can be skipped. We define ring homomorphisms, state some basic properties, and then concentrate on subrings that can be kernels

of homomorphisms. These are called ideals, and using them we can find quotient rings. In fact, in ring theory, the ideals are the structure of choice, and we would like to translate statements about individual elements to those about ideals. For example, an integral domain is a field if and only if it has only trivial ideals. Define principal ideals, and a principal idea ring. Make sure that the students are comfortable with what an ideal is. In a first course, no reason to dwell on (or even mention) Zorn's lemma. Note that the elements of a quotient ring are cosets just as we defined them in group theory. Here we are just defining a multiplication for the same cosets.

HW NOTE. Problem 11.5.11—with a solution in Appendix C—is one of those problems that becomes a lot easier as soon as you draw the right diagram (Figure C4 in Appendix C).

Assignment. Read Section 16.2. Do Problems 11.5.13, 12.2.4, 12.2.8, 12.3.7, 16.1.9. Extra Practice Problems *12.3.3*, *16.1.1*, 16.1.6.

Lecture 32. Quotient rings and homomorphism theorems (Section 16.2).

Homomorphism theorems are just like the ones for groups, except the role of normal subgroups is taken up by ideals. The proofs of many theorems, due to similarity with groups, can be skipped, Use the occasion to solidify the students understanding of ideals, the definition of a quotient ring, and the interpretation of homomorphism theorems by drawing maps between partial lattice diagrams. Note results such as $R/\ker(\phi) \cong \mathrm{Im}(\phi)$, and R/M a field if and only if M maximal.

HW NOTE. Problem 11.5.13 through a series of steps guides the reader to use the machinery of actions and homomorphisms to prove that $\mathrm{PSL}(2,3) \cong A_4$. The group $\mathrm{SL}(2,3)$ acts on an appropriate set of size 4. This gives a homomorphism from this group to S_4. We then identify the kernel and the image and the result follows. One of the steps uses Problem 1.5.6 where the center of the general linear group was identified.

WEEK 13. CHARACTERISTIC OF A RING; FIELD OF FRACTIONS

Assignment. Read Section 16.3. Do Problems 12.3.12, 12.3.13, 12.3.16, 16.1.10, 16.1.20. Extra Practice Problems *12.3.15*, *16.1.17*, *16.1.23*.

Lecture 33. Characteristic of a ring; Prime subfields (Section 16.3).

Define characteristic of a ring and show that the characteristic of an integral domain is always a prime. Every ring (with identity) of characteristic zero contains a copy of $\mathbb{Z}$, every ring (with identity) of characteristic n contains a copy of $\mathbb{Z}/n\mathbb{Z}$. Every field, contains either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p. We can think of all characteristic 0 rings as extensions of $\mathbb{Z}$ and all characteristic n rings as extensions of $\mathbb{Z}/n\mathbb{Z}$.

Assignment. Read Section 17.1. Do Problems 12.3.22, 16.2.4, 16.2.8, 16.2.9, 16.2.11. Extra Practice Problems *12.3.17*, *16.2.5*, *16.2.7*.

Lecture 34. Field of Fractions and Localization (Section 17.1).

Explain the construction of the rationals from the integers, and the fact that a rational number is really an equivalence class of pairs of integers. Then say that the same construction works for integral domains and state Theorem 17.1. Give the appropriate definitions and do some of the proofs. When we have the field of fractions of an integral domain, then within the field of fractions we can find smaller rings where some of the elements of the original integral domain are invertible. These are

examples of localizations and a good source of examples for rings. (They are also very useful in algebraic number theory and in algebraic geometry). I usually cover this section quickly and move to chapter 18.

HW NOTE. Problem 16.2.4 gets the reader to calculate in a quotient ring of a polynomial ring. Problem 16.2.8 raises the ante and asks the reader to calculate in a quotient ring of the Gaussian integers.

Assignment. Read first half of Section 18.1. Do Problems 12.3.23, 16.1.14, 16.2.12, (16.3.1, 16.3.2), 17.1.1. Extra Practice Problems 16.3.4, 16.3.7, 17.1.2.
Lecture 35. Factorization in integral domains (Section 18.1).
Our project—to do number theory in rings that extend the integers—takes off in Section 18.1. Here we define divisibility, as well as irreducible and prime elements. These definitions are in terms of elements of a ring. We like to translate these concepts to two other languages. Once we translate what these mean in the language of ideals (Maximal and Prime ideals play an important role here). Our second translation is to see how to describe these notions in the language of quotient rings. Theorem 18.12 is the crux of this section, and it brings together most of the relevant results. In this Theorem concepts are presented in three different formats (in terms of properties of elements, ideals, or quotient rings). The rest of the section is devoted to proving (most of) this theorem. Many of the implications are true in more generality and the subsequent Theorems in the section bring them out.

HW NOTE. Problem 12.3.23 is probably the most involved of the assigned group theory problems that ask to show that a group of a certain order cannot be simple. I have received emails from students who shared their happiness after figuring out the convoluted argument. Guiding steps are provided and the argument is actually a respectable technique in finite group theory.

WEEK 14. FACTORIZATION IN INTEGRAL DOMAINS; PID ⇒ UFD

Assignment. Read second half of Section 18.1. Do Problems *16.2.7*, 17.1.4, 18.1.4, 18.1.6, 18.1.8. Extra Practice Problems 17.1.3, 18.1.2, *18.1.11*.
Lecture 36. Factorization and the norm map (Section 18.1); Definition of ED, PID, and UFD.
Complete your discussion of Section 18.1. You want the students to understand the relation between maximal ideals and irreducible elements as well as between prime elements and prime ideals. They should realize that there is advantage to passing to quotient rings as well. For quadratic integer rings, the norm map provides a very useful tool for determining units and irreducibles. Give one example of its use.

The ring of integers is a unique factorization domain, a principle ideal domain and a Euclidean domain. Define all three (PIDs have already been defined). As it shall become clear, not all integral domains have all three properties. Our aim for the rest of the course is to prove that ED ⇒ PID ⇒ UFD.

Assignment. Read Section 18.2. Do Problems 18.1.13, 18.1.16, 18.1.18, 18.1.20, 18.1.26. Extra Practice Problems *18.1.15*, 18.1.19, 18.1.22.
Lecture 37. Noetherian Rings (Section 18.2).

Define the ACC and noetherian rings. Prove that a commutative ring with identity is noetherian if and only if all of its ideals are finitely generated. As a results all PIDs are noetherian.

Assignment. Read Section 18.3. Do Problems 18.1.21, 18.1.27, 18.1.29, 18.2.5, 18.6.1. Extra Practice Problems *18.1.23*, 18.1.24, 18.2.1.
Lecture 38. PID ⇒ UFD (Section 18.3).
Our first aim is to prove that every principle ideal domain is a unique factorization domain. A unique factorization has two properties. (1) we can factor every non-zero, non-unit into a product of irreducibles and (2) this factorization is unique. The crucial theorem is that if a an integral domain satisfies the first of these two properties, then it has the second property if and only if every irreducible is prime. This latter condition was proved for PIDs in Section 18.1 as a corollary to the important Theorem 18.12. We also prove that in a noetherian domain (and PIDs are noetherian) the first condition is satisfied. This completes the proof.

HW Note. Problem 18.6.1, which is the starting point of Problems 18.6.1 through 18.6.4, explores local rings and DVRs.

Week 15. ED ⇒ PID; Polynomial Rings; Construction of Finite Fields

Assignment. Read Sections 18.4 and 19.1. Do Problems 18.3.9, *18.3.13*, 18.4.6, 18.6.2, 19.2.8. Extra Practice Problems 18.3.10, *18.6.3*, 19.2.1.
Lecture 39. ED ⇒ PID (Section 18.4); Polynomial rings (Section 19.1).
A Euclidean Domain is an integral domain with an appropriate division algorithm. Prove that ED ⇒ PID. In section 1.3, we gave a proof of the division algorithm for ordinary integers. Now, as a corollary to our main theorem, we have a proof that the integers are a PID and a UFD. We could, of course, prove this directly for the integers, but is satisfying to have a proof of the fundamental theorem of arithmetic as a consequence of our work.

Given a ring R, many properties of the ring R are reflected in the polynomial ring $R[x]$. Define the latter and mention a number of such properties (Theorems 19.17 and 19.18).

HW Note. For the last two homework assignments, by necessity, the homework is a bit ahead of the lectures. By this point, the students can handle reading on their own and doing the problems. Even so, I usually make these two assignments to be due one day later than usual.

Assignment. Read Sections 19.2, 19.3. Do Problems *18.4.1*, 18.4.7, 18.6.4, 19.3.4, 19.3.5. Extra Practice Problems *18.6.7*, *19.2.9*, *19.3.3*.
Lecture 40. K field ⇒ $K[x]$ is an ED (Section 19.2) Roots and Construction of finite fields (Section 19.3).
Outline the proof that if K is a field, then $K[x]$ is an ED, hence a PID, and a UFD. Here is one example of the use of this theorem. If A is a square matrix over $\mathbb{R}$, then consider the set of polynomials $p(x)$ such that $p(A) = 0$. This set is easily seen to be an ideal of $\mathbb{R}[x]$ and $\mathbb{R}[x]$ is a PID. Hence, this ideal is generated by one polynomial. Hence, there is a polynomial $m(x)$ such that $m(A) = 0$ and every other such polynomial is a multiple of $m(x)$. This was a quick proof that for every square matrix, we have a minimal polynomial.

As a proof of concept, show how the ideas developed in this chapter can be used to construct new fields. If K is a field and if $p(x) \in K[x]$ is irreducible, then $\langle p(x) \rangle$ is a maximal ideal of $K[x]$ and $K[x]/\langle p(x) \rangle$ is a field. Use this to construct a field of 4 elements.

As an optional lecture outside of class, I conclude with an expository lecture on the proof of Fermat's Last Theorem.