

Problems are due two class periods after we have covered the corresponding section in the textbook. (Once or twice, “covering” will mean me telling you to read the section yourself.) For example, if we finish §1.1 on a Monday, then the associated problems are due the following Friday.

---

## CHAPTER 1: GROUPS, THE BASICS

We’ll cover this quickly, since most of it should be familiar. In §1.1 we’ll recall some definitions and examples. Dihedral groups (§1.2) provide an example that will be important later. We won’t cover symmetric groups (§1.3) in class, since you’ve probably mucked about with these a lot. Of course, I’ll be happy to try to answer any questions about them, either in class or elsewhere. Matrix groups (§1.4) are so important that some courses use them (instead of symmetric groups) as the most basic example. We won’t cover §1.5 in class, but please read it, since you need to have a good store of examples of groups in your head. Group actions (§1.7) will be at the heart of this whole course. We’ll cover the basic definitions and examples, and see more later.

**Exercises:** §1.1: 8,12,22,34. §1.2: 3,4,10,14,15. §1.3: 1,5,9a,19. §1.4: 1,2,3,11. §1.5: 1. §1.6: 2,7,9,11,14,20. §1.7: 1,4,6,8,10a,11,16–19.

*Also, for each section above, let me know how long you spent on the exercises.*

---

## CHAPTER 2: SUBGROUPS

We’ll spend a little time on centralizers, normalizers, and stabilizers (§2.2).

**Exercises:** §2.1: 4. §2.2: 1,3,4,5a,14. §2.4: 2,8,14. §2.5: 11.

---

## CHAPTER 3: QUOTIENT GROUPS; HOMOMORPHISMS

We’ll quickly review what quotient groups are, as well as Lagrange’s theorem (§3.2) and the isomorphism theorems (§3.3). The Hölder Program (§3.4) is a two-step research program to classify all finite groups. Step one took about 100 years. Wanna start step two?

**Exercises:** §3.1: 1,3,4,5,6,8,9,17,36. Read 11,22,35,42. §3.2: 4,8,12,16,22 (see §0.3, #10), 23. Congratulations. You’ve just proved a main theorem of number theory. §3.3: 1,3,5,9.

Topic: Group extensions See §17.4.

Topic: Certificates of primality Suppose  $n$  is a large integer. If I want to prove to you that  $n$  is composite, all I have to do is tell you an alleged divisor  $d$  of  $n$ . It is then easy for you to verify that  $d$  is indeed a divisor of  $n$ . But suppose I want to prove to you that  $n$  is prime. How can I do it without giving you a zillion pages of failed attempts to find a divisor? The answer boils down to the fact that the size of  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$  determines the primality of  $n$ . See any recent number theory book, particularly one that includes applications to cryptography. I can lend you one or two.

---

## CHAPTER 4: GROUP ACTIONS

We define groups as sets with operations that satisfy various properties. However, groups don't arise in nature in this way, but as collections of symmetries of things. If we take this point of view, then we can prove many different theorems in pretty much the same way. For example, we will prove the Sylow theorems, even though you have already seen them.

**Exercises:** §4.1: 1,9. §4.2: 1,6 (“ $rH$ ” should be “ $rN$ ”), 7,10,12. Read 2,3. §4.3: 2,3b,5,10a,11a,19,23,29,31,35. Read 24,25. §4.4: 1,2,5,7,12,15. §4.5: 1,3,6,8,13,16,21,30,36,40.

Topic: For which  $n$  are all groups of order  $n$  cyclic?

---

## CHAPTER 5: PRODUCTS

You've seen direct products before. We'll look at them again, briefly. If there's time, we'll later cover semidirect products, another way to construct groups out of smaller ones. But in case we don't have time, think of this as another possible project for you.

**Exercises:** §5.1: 7,8,10,14. §5.2: 1,2,4b,7,9.

Topic: Semidirect products

Include a classification of all groups of order a product of two distinct primes.

---

## CHAPTER 6: FURTHER TOPICS IN GROUP THEORY

We will not cover this in class, but it's a good source of topics.

Topic:  $p$ -groups

Topic: Groups of order  $p^3$ , where  $p$  is a prime

One can either use semidirect products (§5.5) or the theory of  $p$ -groups (§6.1) to handle this.

Topic: Nilpotent groups

See the chapter.

Topic: Solvable groups

See the chapter.

Topic: Free groups

See the chapter.

Topic: Rubik's Cube

(Matt suggested this topic.) Discuss Rubik's Cube in terms of group theory, and address one or both of the following: What do we know about the particular group involved? What's a solution algorithm?

Topic: Anything that looks interesting to you

See me if something catches your fancy enough that you'd like to prepare a talk on it.

---

## CHAPTER 11: VECTOR SPACES AND MODULES

Here we study linear algebra in a general context. Instead of dealing with  $n$ -by- $n$  matrices and  $n$ -tuples of real numbers, we deal with vector spaces and linear transformations, and we replace real numbers with elements of any field you like. (Be careful when reading the book: when they define vector spaces,

the authors assume that you already know about modules, which we haven't covered yet.)

Though one can never know too much linear algebra, we will not go beyond §11.2 in this chapter. (And in §11.2, we won't look at tensor products.) However, we will then go back to §10.1, to see what all of the fuss was about. It turns out that modules simultaneously generalize abelian groups, vector spaces, and other things as well.

**Exercises:** §11.1: 2,3,7,8,9. §11.2: A good part of a beginning linear algebra course is contained in these exercises, so all of them that don't involve tensor products. Do 2,4,6,8,10,37. §10.1: 1,2,5,9,15,18.

Topic: Modules Direct sums, quotients, etc.

Topic: Tensor products of modules

Topic:  $K$ -theory of rings Modules are sort of like vector spaces.  $K$ -theory measures (among other things) the extent to which they are different. See the first few pages of *Algebraic K-theory*, by Sylvester.

## CHAPTER 13: FIELD THEORY

Suppose  $F$  is a field, and  $p(x)$  is a polynomial with coefficients in  $F$ . If  $p$  does not have a zero in  $F$ , is it possible to construct a larger field  $E$  in which  $p$  *does* have a root? If so, what can we say about the relationship between  $F$  and  $E$ ?

Application: Classical straightedge and compass constructions.

**Exercises:** §13.1: 1,3,7. §13.2: 1,2,3,7,19,20. §13.3: 1,5. §13.4: TBA. §13.5: TBA.

## CHAPTER 14: GALOIS THEORY

When Galois was your age, he had already invented this stuff.

We will cover all parts of this chapter except for §§14.5, 14.8, and 14.9.

**Exercises:** TBA.

Topic: Transcendental extensions

Topic: Inseparable extensions

Topic: Infinite Galois groups

Topic: Abelian extensions of  $\mathbb{Q}$

## CHAPTER 10: MODULES

If there is time, we will continue our study of modules far enough to classify the finitely-generated modules over a principle ideal domain. Special cases of this include:

- the classification of finitely generated abelian groups;
- rational canonical form (one of the important theorems in advanced linear algebra).