Math 350, Spring 2026 Professor Rob Benedetto

Review Sheet for Exam 1

The exam (in class, Friday, March 6) will cover Sections 2–7 of Saracino, although of course some material from Sections 0 and 1 will be be needed as well. The following is a list of most of the topics covered. **THIS IS NOT A COMPREHENSIVE LIST, BUT MERELY AN AID.** Please note: when I list a given concept or definition below, I mean three things. First, you should know the official definition (not necessarily verbatim, but close enough). Second, you should have a decent intuition for it. Third, you should also be able to use that concept accurately in a proof.

You may bring one standard size (8.5x11") "cheat sheet" of notes to the exam

You MAY use both sides of the sheet of paper for your cheat sheet

You must HAND-WRITE your own cheat sheet directly on the paper. No printouts.

- Section 0 and the "Review of Sets and Proofs" handout: Set notation, union, intersection, subsets, the empty set. The "for all" meaning of $S \subseteq T$ and $S = T$. The sets of numbers $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Mathematical induction.

- Section 1: Binary operation on a set. Commutative. Associative.

- Section 2: The definition of a group. Abelian. Basic examples like $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^+, \cdot)$, $(GL(n, \mathbb{R}), \text{matrix mult})$, the group of $\mathbb{R}$-valued functions on $\mathbb{R}$ (under $+$), and of course, the finite cyclic group $(C_n, \oplus)$ (which the book calls $(\mathbb{Z}_n, \oplus)$). Various **non**-group examples: $\varnothing$ with any operation; $\mathbb{Z}_{\geq 1}$ or $\mathbb{Z}$ with $\cdot$, etc. The division algorithm (Lemma 2.1). The notation $a \equiv b \pmod{n}$. (The) trivial group.

- Section 3: Theorems 3.1–3.6, which include: uniqueness of identity and of inverses; the formula $(x^{-1})^{-1} = x$; the formula $(xy)^{-1} = y^{-1}x^{-1}$; and the cancellation laws. The various consequences of the cancellation laws: Theorem 3.5 (if $xy = e$, then $y = x^{-1}$), and the theorem from class that if $x, y \in G$ with $xy = x$, then $y = e$. (And also the mirror images of those results: that $yx = e$ implies $y = x^{-1}$, and that $yx = x$ implies $y = e$.) All of these statements are under the assumption that we are working in a *group*, of course.

- Section 4: The notation x^n. (Or if the operation is called $+$ or $\oplus$, then use nx instead of x^n.) Order of an element, and order of a group. (These two uses of "order" mean different things! Know the difference, and don't confuse them.) Theorems 4.1, 4.4, 4.5, and Corollary 4.6, which talk about the algebraic rules for exponents x^n, the order $o(x^n)$ in terms of $o(x)$, and the distinct elements in $\langle x \rangle$. (Feel free to use the slightly more general version of Theorem 4.5 that I stated in class, that $o(x) = |\langle x \rangle|$.) Various terms and results about integers: relatively prime, gcd, Theorem 4.2. Cyclic groups. (Not just C_n but also $\mathbb{Z}$.) Generator (of a cyclic group). Theorem 4.7 (that cyclic groups are abelian). The Klein 4-group (denoted V or V_4).

- Section 5: Subgroups: the definition, and Theorem 5.1, used to determine more quickly whether or not $H \subseteq G$ is actually a subgroup. (Don't forget to check that H is nonempty!) The terminology "closed under $*$" and "closed under inverses," as well as the precise "for all" language that these terms mean. Theorem 5.4, about intersections and unions of subgroups. Theorems 5.2, 5.5, 5.7, and Corollary 5.6, about subgroups of cyclic groups. The center $Z(G)$ of a group G. The group Q_8 of unit quaternions. (Feel free to use either my notation $\{\pm 1, \pm i, \pm j, \pm k\}$ or the book's notation $\{\pm I, \pm J, \pm K, \pm L\}$ for the elements of Q_8, but **don't mix and match**!)

- Section 6: Direct Products: Definition of $G_1 \times \cdots \times G_n$, and the fact that it is a group if each G_i is a group. Least common multiple. Theorem 6.1 about orders of elements in the product group, and about when a product of cyclic groups is still cyclic. The result of Exercises 6.4 (the order of a product group) and 6.6 (the product is abelian iff each G_i is abelian).
- Section 7 and the "Functions" handout: Functions f from S to T, and the notation $f : S \to T$ and $f : x \mapsto f(x)$. Domain, codomain (target set), and image of f. (Warning: the image $f(S)$ and codomain T may be different). One-to-one (injective) and onto (surjective). Two functions to be equal if: they have the same domain, and they agree at every point of the domain. Composing functions; composition is associative. The inverse of a function (if it has one); f has an inverse if and only if it is both one-to-one and onto (bijective). In that case, f^{-1} is unique; and f^{-1} is invertible with inverse $(f^{-1})^{-1} = f$. If both f and g are invertible and the composition $f \circ g$ makes sense, then $f \circ g$ is invertible with inverse $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Some things you don't need to know

Here are some results and concepts that appear in the book and/or optional videos but which I did not really cover. Although you are allowed to use them (if you know them from the videos, the book, or another course), I will design the exam with no expectation that you know any of them.

- Section 0: The well-ordering principle.
- Section 0: The "second form" of mathematical induction (sometimes called "strong induction") on page 6.
- Section 0: The Fundamental Theorem of Arithmetic (that all positive integers can be factored *uniquely* as a product of primes).
- Sections 1–2: The power set $P(X)$ of a set X, and the symmetric difference operator $\triangle$.
- Section 2: The notation $\overline{a}$ for the remainder of a modulo n.
- Section 3 (also in one of the Optional Videos): Right identity, right inverse, left identity, left inverse. Theorem 3.7, that associative, right identity, and right inverses implies group.
- Section 4: The Euclidean Algorithm, and Euclid's Theorem (Theorem 4.3).
- Section 5: Theorem 5.3: for a *finite* subset H of a group G, nonempty and closed under $*$ (but no need to check inverses) guarantees that H is a subgroup.
- Section 6: Direct products (and direct sums) of **infinitely** many groups, which I discussed in one of the Optional Videos.
- Section 7: The "precise" definition of a function as a set of ordered pairs satisfying some properties (page 59, near the bottom, and in another Optional Video).
- Section 7: The definition of the symmetric group S_X. (That'll be saved for the *next* exam.)
- Section 7: The notion of a function being *well-defined*. That concept (and being able to work with it in proofs) will be important on future exams, but not on Exam 1.

Tips

- **Review your notes**, and take the time to write down theorems and definitions again, especially the important ones. (How do you know what's important? Well, if it came up on any homework problems, it's probably important!)
- **Review old homework problems**. Look at my solutions on the website, as well as the graders' comments on your solutions on gradescope.
- **Practice**. Try some old homework problems again, and try some of the practice problems at the end of this handout. Skip around to make sure you cover a wide range of problems of different types — some proofs, some computational, and across different sections — rather than trying to do every problem in order and risking never getting to the later sections.
- As mentioned earlier, know all the relevant definitions **thoroughly**. They are vital for proofs, for example. Know the theorems pretty precisely, too.
- When invoking facts that we now take for granted (like that for $x \in G$, the set $\langle x \rangle$ is a subgroup of G, or any of Theorems 3.1–3.6), you don't have to specifically quote a theorem. For example, you may write $(x^{-1})^{-1} = x$ with no further explanation required. Similarly, if you have an equation $xyz = a$ and on the next line you write $xy = az^{-1}$ with no extra explanation, that's fine. Technically, you multiplied both sides on the right by z^{-1}, then used associativity to make the left side into $xy(zz^{-1})$, then used the inverses axiom to change that into xye, and then used the identity axiom to change *that* into xy. But who cares?

  You don't need to memorize theorem numbers; but if you quote a named result (like the Division Algorithm), please call it by its name. Otherwise, if you want to use an unnamed result (like Theorem 4.5), just say that you're using a theorem from the book (or from class). If necessary, say just a few words to describe it so I know what result you're talking about; but usually, the context alone is enough.

  For example, if you have a cyclic group G of order n and generator a, and if you've got a couple integers i and j floating around and you've just demonstrated that $a^i = a^j$, feel free to say simply, "Therefore $i \equiv j \pmod{n}$, by a Theorem." From the context, it's utterly clear to me which theorem you're talking about.

  (But be warned, if you try to slip something by me by magically quoting a "Theorem" that doesn't actually exist, that won't fly. I actually know what all the theorems we covered say!)
- When trying to craft a proof, focus on what you're *trying to prove*, not what the hypotheses are. [Of course, you may want to do some scratch work where you write out what *both* the hypotheses and the conclusions mean. But when trying to design the structure of the proof itself, temporarily ignore the hypotheses, and focus on the desired conclusion.]

  For example, regardless of the hypotheses, if you are trying to show that a function $f : S \to T$ is one-to-one, the proof will begin, "Given $x_1, x_2 \in S$ such that $f(x_1) = f(x_2)$," and it will end with "so $x_1 = x_2$". An onto proof begins, "Given $y \in T$," and shortly (often immediately) thereafter says, "let x be $\square$," and soon (often immediately) verifies that $x \in S$, and finally ends with "so $f(x) = y$." (To fill in the blank there, you probably *do* have to look at the hypotheses and maybe do some scratchwork doodling.) Similarly, a proof that the set A is contained in the set B begins with, "Given $x \in A$" and ends with "so $x \in B$." A proof that G is abelian begins with, "Given $x, y \in G$" and ends with "so $xy = yx$."

  And so on. Know how to do all these little things from set theory (equality of sets, equality of functions, uniqueness of an element with a certain property, etc.) and from basic group theory.

The same applies even to slightly more advanced concepts. Suppose you're trying to prove $x \in G$ has order 4. Well, what does that mean, **exactly**? A common mistake would be to prove only that $x^4 = e$, which is *part* of it but not all of it.

The point is, seeing it written on paper might then help you figure out what to do next. Even if it doesn't, having **me** see it written down might give you some partial credit. Don't just stare at a blank page and try to get it all to work in your head before you write anything. Scribble and doodle. But if you're really stuck, make sure you write down a skeleton of your proof (based on what the desired *conclusion* is, while essentially *ignoring* the hypotheses). Once you have that skeleton, try to fill in the gaps, using the hypotheses when they look like they might help. Perhaps you can then produce a clean (and hopefully short) writeup. But don't be afraid to write down half-formed ideas that may turn out to be false starts.

- Remember that for groups whose operation is written as $+$ (or something similar, like $\oplus$), the rest of our notation needs to go with this idea of "addition". So instead of writing xy, we write $x + y$. Instead of x^{-1} we write $-x$. And instead of x^n we write nx (where $n \in \mathbb{Z}$ is an integer).

  So for example, if G is a group for which we use the symbol $+$, then Theorem 4.1 part (i) applied specifically to G would instead read $mx + nx = (m + n)x$; part (ii) would read $-(nx) = (-n)x$; and part (iii) would read $n(mx) = (nm)x = m(nx)$

- You can't raise group elements to fractional powers. Whenever you write something like g^k, make *very* sure it's clear that k is an *integer*.

Some more practice problems

To get practice, **the main places you should look** are:

- old homework problems,
- examples from class, and
- examples from the book.

If you're looking for **more practice**, here are some **totally optional** problems you may attempt. Most of the higher-numbered problems are harder than anything I would put on a timed exam, but they are still good practice. It would probably be best to read most or all the problems but pick and choose just some of problems to try, rather than simply doing all of them in order.

Problems in **bold face** below are mainly computational. The rest are proof or theoretical problems. Problems in *italics* might look hard at first but have very short proofs if you think about them the right way or spend enough time thinking of the right trick or example. Problems with asterisks (*) are trickier than the others, though their answers/proofs might turn out to be pretty short.

Please be aware that these problems are **practice problems** and **NOT** sample exam problems. They certainly are **NOT** a practice exam. Many of these problems require more time — for both thinking and writing — than would be appropriate for a timed exam. But they are still good practice.

Section 0, #4, 6, 9

Section 1, #3(d,f), 6(a,f)

Section 2, #1(d,e,h), 10 (but feel free to use stuff from later sections, about subgroups)

Section 3, #10

Section 4, #**1, 2, 4, 7**, 11, 13, 19, 22

Section 5, # 1(b,g), **4(c)**, #6(a), **6(b)**, 9, **12, 13***, *16*, *17*, 22, 26

Section 6, #**1(a,b), 2(c)**, 3, 5, *7*

Section 7, #1(d,f,h,j), 2(b), 3, 7, 10(b), 11*