This document summarizes the content that may appear on the final exam, as well as some suggestions as you review for it.
The middle portion of this guide was already posted as the review guide for midterm 2.

Exam format

- The exam will be Wednesday 12/19 at $9am$, and the time limit will be 3 hours.
- You are allowed one page of notes, front and back, prepared any way you wish (typing, copying, sharing, etc. are all fine).
- The exam will most likely be ten or so questions long.

Suggestions for your review

- Think hard about what to put on your note sheet, and how to organize it! This is a great way to study for the exam, since it will spur you to think holistically about the material, the most crucial ideas, and the places you've had the most trouble. It may well be that you won't even have to look at your sheet, because preparing it helped you thoroughy learn the material.
- Study your class notes in detail. Always *read actively.* Among other things, this means:
  1. Before reading a proof, try to summarize it on scratch paper. Even if you can't remember the details, this will help you prepare your brain to digest it.
  2. After each theorem, stop and ask yourself: what other theorems are similar or are proved in a similar way? Where do we apply it later in the course? What are some examples that we've done it class or on the homework?
  3. After each example, stop and ask yourself: what concepts of theorems is this illustrating? Can you generalize the example? What are similar examples elsewhere in the course?
- Review the homework assignments and posted solutions in detail, especially the problems you found challenging. When you review a problem, ask yourself: what concepts is this problem illustrating? What theorems from class does it apply or illustrate? What ideas do you need to come to mind in order to solve it?
- *After you've completing most of your review,* try the practice exam as a diagnostic and simulation of the timing. Remember that the practice exam, like the actual exam, will only cover essentially a random sample of the possible topics, so do not use it as a comprehensive review document!

Exam content

The list below provide a rough outline of the concepts we've studied in class or on the homework since the first midterm. I've provided references in many places to the spots where you can find more detail on the places where you need more review.

Content from midterm 1

- Binary operations and groups (§1, 2, PSet 1)
  - Definition of binary operation, "commutative," "associative." Can you think of examples that are associative, but not commutative, or vice versa, or neither?
  - A group is a set with an associative and invertible binary operation (implicit in "invertible:" there is an identity element).
  - Both the set and the operation matter! $(\mathbb{R}, +)$ is a group, but $(\mathbb{R}, \cdot)$ is not. $(\mathbb{R}, \cdot)$ is not a group, but $(\mathbb{R}^+, \cdot)$ is (so is $(\mathbb{R}^\times, \cdot)$, which we defined later in the rings unit). Make sure you understand why!
  - Other important examples: $GL(2, \mathbb{R})$, $SL(2, \mathbb{R})$, Klein 4-group V, Unit Quaternion group Q_8.
- Fundamental theorems on groups (§3, PSet 2)
  - Be able to write proofs, from the axioms, of the first six fundamental theorems from §3. These are: uniqueness of e_G; uniqueness of inverse; $(x^{-1})^{-1} = x$; the formula for $(xy)^{-1}$; if $xy = e_G$ then $x = y^{-1}$ (you can prove that $yx = e_G$ as well); the two cancellation laws.
  - The seventh theorem (3.7) from §3 is harder. It is a good review problem to come up with your own proof (or understand the proof in the book), but it would be too tricky for the exam.
  - Can you relax the hypotheses of any of these theorems and still prove them? For example (now that we know about rings), if R is a ring then $(R, \cdot)$ is *not* a group, and yet some of these theorems still hold for multiplication (uniqueness of inverses, for example). Which ones?
- Cyclic groups (§4, PSet 2)
  - Prototype of all finite cyclic groups: $\mathbb{Z}_n$. Prototype of all infinite cyclic groups: $\mathbb{Z}$.
  - Every element g in any group G defines a *cyclic subgroup* $\langle g \rangle$ (these aren't called "subgroups" until §5, but with hindsight this is what was going on in §4). The order (number of elements) of $\langle g \rangle$ is equal to the order of the element g (minimum positive n such that $g^n = e_G$). A group G is cyclic if it is equal to $\langle g \rangle$ for some g, in which case g is called a *generator* of G.
  - Subtle issue: in a *finite* cyclic group with generator g, every element can be written as g^n for $n \geq 0$, but in an *infinite* cyclic group you need negative exponents, too. (cf. PSet 3 # 1)
  - All cyclic groups are abelian.
  - Division algorithm for $\mathbb{Z}$: for all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exists a unique choice of $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r < q$.

  - Important number theory fact: for any two integers m, n, not both 0, there exist integers x, y such that $mx + ny = (m, n)$.
  - If $o(g) = n$, and m is any integer, then $o(g^m) = \frac{n}{(m,n)}$. More specifically, the subgroup $\langle g^m \rangle$ is equal to the subgroup $\left\langle g^{(m,n)} \right\rangle$. How do you prove this, using the "important number theory fact" above?
  - If $G = \langle g \rangle$ is a cyclic group of order n, how would you list all of the generators of G (besides g)? How would you list the elements of order d, for some other integer d? (cf. PSet 3 # 3,4)

- Subgroups (§5, PSets 2 and 3)
  - A subgroup is a subset that is a group in its own right. Equivalently (make sure you understand why it is equivalent), it is subset closed under multiplication and inverse.
  - Every subgroup of a cyclic group is cyclic (make sure you can prove this, using the division algorithm). (Theorem 5.2)
  - More specifically, if $G = \langle g \rangle$ has order $n < \infty$, then there is exactly one subgroup of order d for each $d \mid n$; the subgroup of order d can be described as $\left\langle g^{n/d} \right\rangle$.
  - Important special case: what are the subgroups of $\mathbb{Z}_n$?
  - Theorem 5.2 also applies to *infinite* cyclic groups. For example, what are the subgroups of $\mathbb{Z}$?
  - Given a group G, how might you go about trying to list all the subgroups of G? The key idea here is: try adding elements in one at a time, but always add any other elements that you are forced to include (by closure) every time.
  - If a subset H of a group G is *finite*, then closure under multiplication actually implies closure under inverse. This is a tricky point, but is a versatile idea, so make sure you understand the reasoning! (cf. Theorem 5.3; similar ideas are used in PSet 2 # 1, Midterm 1 # 4, and Theorem 16.7).

- Functions (§7, PSet 3)
  - Definitions: function; injective (one-to-one); surjective (onto); $f \circ g$; bijective; inverse function.
  - A function is bijective iff it has an inverse function.
  - Function composition is associative.
  - For any set X, the set of bijective functions $f : X \to X$ form a group $(S_X, \circ)$, where the operation is composition.
  - Useful fact to have in your back pocket: if X is a *finite* set, then a function $f : X \to X$ is injective iff it is surjective (why?).

- Symmetric groups (§8, PSet 3,4)
  - Defintions: S_n; A_n; cycle; disjoint cycles; transposition.
  - What is the order of S_n? Of A_n? (cf. Theorem 8.5)
  - Know how to write elements of S_n is both two-line notation and disjoint cycle notation (and how to convert between these), as well as how to compose two functions in either notation. Both of these notations are unique, with the caveat that two disjoint cycle decompositions are considered "the same" if the order is rearranged or if the starting point of a cycle is changed. (cf. PSet 4 # 8,9)

- Given $f \in S_n$, how would you find the order of f? Is this easier to do in two-line notation, or in disjoint cycle notation? (cf. PSet 4 # 1,2,3)
- Any element of S_n can be written as a product of transpositions. Such decomposition is not unique.
- *However,* the parity (odd versus even) of the number of transpositions is the same in any decomposition into transpositions.
- The dihedral groups D_n, which can be viewed as a subgroup of S_n or more abstractly as

  $$D_n = \{e, f, f^2, \cdots, f^{n-1}, g, gf, \cdots, gf^{n-1}\}$$

  where $fg = gf^{-1}$.
- What is the order of D_n?
- The group S_3 is the symmetry group of a triangle (where you are allowed to flip it over). The group A_4 is the symmetry group of a tetrahedron. The group D_n is the symmetry group of a regular n-gon (where you are allowed to flip it over).

Content from midterm 2

- Direct Products of groups (§6, PSet 5)
  - The definition of $G \times H$.
  - How is $o((g, h))$ related to $o(g)$ and $o(h)$? How can you use this to tell whether or not $G \times H$ is cyclic? (cf. Theorem 6.1)
  - How can you express the Klein 4-group as (isomorphic to) a direct product? (Example from class; we didn't use the word "isomorphism" at the time, of course)
  - Under what conditions can you deduce that $G \times H$ is abelian? Non-ablelian? Cyclic? (cf. Theorem 6.1, Exercise 6.2,6.6, PSet 5 # 2,3)
- Cosets and equivalence relations (§9, PSet 5)
  - The definition of an equivalence relation, and the definition of cosets of G under a subgroup H.
  - The definition of the equivalence relation $\equiv_H$. What does $x \equiv_H y$ mean in terms of cosets? (cf. Theorem 9.3 and Corollary 9.4, PSet 5 # 9)
  - Is a *coset* ever also a *subgroup*?
  - Three useful equivalent statements: $Ha = Hb \Leftrightarrow a \in Hb \Leftrightarrow ab^{-1} \in H$. How do we write these statements differently when discussing cosets in a ring?
- Lagrange's theorem (§10, PSet 5)
  - What is the definition of the index $[G : H]$? How is it related to $|G|$ and $|H|$ (when these are finite)? (cf. p. 89 in Saracino)
  - The statement and proof of Lagrange's theorem. (Theorem 10.1)
  - Why does Lagrange's theorem quickly imply each of the following statements (in a finite group G)? (Theorems 10.4 and 10.6)

- $*$ $g^{|G|} = e$ for all $g \in G$.
- $*$ $o(g)$ divides $|G|$ for all $g \in G$.
- $*$ If $|G|$ is prime, then G is cyclic.

- Quotient groups and normal subgroups (§11, PSet 6)
  - Define "normal subgroup."
  - Why are normal subgroups defined the way they are? Why would it be impossible to define a quotient group G/N without this definition ?(cf. discussion in Saracino beginning at the bottom of page 102)
  - Examples: what are the elements of $\mathbb{Z}/n\mathbb{Z}$? Of $Q_8/\{I, -I\}$? Which familiar groups are these isomorphic to?
  - Be comfortable doing computations in quotient groups (cf. PSet 6 #7 and 9; cf. also PSet 9 #7, where you do the same sort of thing in a quotient ring instead)
  - What is the order of G/N?
  - Examples of normal subgroups: $A_n \triangleleft S_n$, $SL(2, \mathbb{R}) \triangleleft GL(2, \mathbb{R})$, $Z(G) \triangleleft G$, any subgroup of an abelian group is normal.

- Group homomorphisms (§12, PSet 7)
  - Definitions: homomorphism, isomorphism.
  - Compositions of homomorphisms (resp. isomorphisms) are again homomorphisms (resp. isomorphisms). (cf. Theorem 12.1)
  - If $\phi : G \to K$ is a group homomorphism, what can you say about $\phi(g^{-1}), \phi(g^n), \phi(e_G)$ and $o(\phi(g))$? What can you say if you know that ϕ is an isomorphism? (cf. Theorems 12.4, 12.5)
  - There is a surjective group homomorphism from $\mathbb{Z}$ to any cyclic group. Why? (cf. example from class 10/23)
  - Any two cyclic groups of the same order are isomorphic. Why? (cf. Theorem 12.2)
  - Given a group homomorphism $\phi : G \to K$, and subgroups $H \leq G, J \leq K$, define the image $\phi(H)$ and inverse image $\phi^{-1}(J)$. These are subgroups; why? Under what hypotheses can you conclude that these are *normal* subgroups? (cf. Theorem 12.6)

- The fundamental theorem of group homomorphisms (§13, PSet 7)
  - Know the fundamental theorem, as stated in Saracino (Theorem 13.2). It is good to know the more general version stated in class (for non-surjective homomorphisms) especially if you are taking the Comps, but this will not be needed for this exam.
  - Define $\ker \phi$ (or a group homomorphism ϕ). Why is it a normal subgroup? (cf. Theorem 13.1)
  - We said (informally) in class that "$\ker \phi$ measures the failure of ϕ to be injective." What does this mean, more formally? What does $\ker \phi$ say about the cases where $\phi(x) = \phi(y)$?
  - Define the *induced homomorphism* $\overline{\phi}$ that we discussed in class. Why is it well-defined? Why is it a group homomorphism? Why is it injective? (cf. the proof of Theorem 13.2 in Saracino, especially the picture on page 123)

  - Examples: use the fundamental theorem to show that an order n cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$; the Klein 4-group is isomorphic to a quotient of Q_8 (by what normal subgroup?), the unit group of $\mathbb{R}$ is isomorphic to $GL(2, \mathbb{R})/SL(2, \mathbb{R})$ (we didn't call it the "unit group" at the time, of course; we wrote $(\mathbb{R} - \{0\}, \cdot)$ instead).

- Rings and field (§16, PSet 8)
  - Definitions: ring 0_R, 1_R, unit, unit group, field, integral domain, zero-divisor, nontrivial (ring, zero divisor).
  - Basic algebraic rules in rings for working with additive inverses, subtraction, and multiplication by integers (cf. Theorem 16.1, 16.4).
  - Specific comment: the book does not use the notation $R^\times$ for the unit group, but we use it frequently. Make sure you are familiar with it.
  - What are some examples of: integral domains, rings without unity, non-commutative rings, fields, rings with nontrivial zero-divisors?
  - Fix an integer n. Which elements of $\mathbb{Z}_n$ are units? When is $\mathbb{Z}_n$ a field? (cf. Exercise 16.9, and discussion in class on 10/31 and 11/2).
  - Under what circumstance does "cancellation" work for multiplication in rings? (cf. Theorem 16.5)
  - Definition of direct sums $R \oplus S$ of rings.

- Subrings, ideals, and quotient rings (§17, PSet 9,10)
  1. Know our definitions from class of rings and ideals (nonempty, closed under subtraction, and either closed under multiplication or sticky), and why they are equivalent to the definitions in the book.
  2. What are some examples of subrings? Of ideals? Of subrings that are not ideals?
  3. Why is R/I a well-defined ring when I is an ideal? (cf. our discussion from class, or the discussion in Saracino beginning in the second half of p. 167).
  4. Be comfortable doing computations in quotient rings by working with coset representatives (cf. PSet 9 #6, 7, 8).
  5. Definitions of prime and maximal ideals.
  6. I is a prime ideal iff R/I has what property? (cf. Theorem 17.5)
  7. If R is a commutative ring with unity: I is a maximal ideal if and only if R/I has what property? (cf. Theorem 17.7)
  8. What are the prime ideals of $\mathbb{Z}$? What are the maximal ideals of $\mathbb{Z}$? (cf. Example 1 on p. 172, or our discussion in class).

- Ring homomorphisms (§18, PSet 10)

  For the exam, you are only responsible for **the material up to the fundamental theorem (Theorem 18.5)** in §18.

  - Definitions of ring homomorphism and isomorphism.
  - Basic algebraic homomorphisms: what can you say about $\phi(0_R)$, $\phi(na)$ (where $n \in \mathbb{Z}$) and $\phi(a^n)$ (where $n \geq 1$)?

  - Criteria for $\phi(1_R) = 1_S$ (Theorem 8.2) and consequences (Theorem 18.1(iv)).
  - Why is $\ker \phi$ an *ideal* for a ring homomorphism ϕ?
  - Understand the statement and proof of the funamental theorem of ring homomorphisms (18.5).

Content from after midterm 2

- Polynomials (§19, PSet 11)
  - It is good to know the definition of the polynomial ring $R[X]$, where R is *any ring.*. However, **for our exam, I will limit any questions about polynomials to the case where R is a field.** Therefore you may feel free to ignore any more general hypotheses for theorems in the book. In all the following bullet points, I'll assume that F is a field and consider the ring $F[X]$.
  - Be comfortable adding and multiplying polynomials, and carrying out the division algorithm (to obtain quotient and remainder) (cf. Theorem 19.2, Example 2, PSet 11 # 6, and the worked example of long division from class on 12/5).
  - Know the definition of $\deg f(X)$. If you know $\deg f(X)$ and $\deg g(X)$, how do you find $\deg(f(X)g(X))$? Why does the formula work? (cf. Theorem 19.1)
  - What is a "constant polynomial?" How does $\deg f(X)$ help you identify the constants?
  - Definition of divisibility and irreducibility in $F[X]$.
  - The criterion for irreducibility in terms of roots; how to apply it when $F = \mathbb{Z}_p$ (cf. Theorem 19.8, Examples 1 and 2).
  - Polynomials can be used as functions. A "root" of $f(X)$ is a field element r where $f(r) = 0_F$. The element r is a root if and only if $(X - r)$ divides $f(X)$ (cf. Theorem 19.3, PSet 11 # 6).
  - You do **not** need to know anything from §19 after Example 4 on page 198 (it is beautiful mathematics! But it won't be on the exam.)

- Quotients of polynomial rings (§19, PSet 11)
  - The shorthand notations: $(f(X))$ for the principal ideal of $f(X)$; $\overline{f(X)}$ for the coset of $f(X)$ in a quotient ring $F[X]/(g(X))$.
  - All ideals in $F[X]$ are principal. How do you prove this using the division algorithm? (Suggestion: try writing out a proof of the analogous theorem in $\mathbb{Z}$: every ideal of $\mathbb{Z}$ is $n \cdot \mathbb{Z}$ for some integer n; the proof can be nearly line-by-line the same.) (cf Theorem 20.1, PSet 11 # 5)
  - An ideal $(g(X))$ in $F[X]$ is maximal iff $g(X)$ is irreducible (we didn't show the proof in full detail, and you don't need to be able to reproduce it). What does this mean about the quotients of $F[X]$ that are fields?
  - The field F can be viewed as a subring of $F[X]/(g(X))$. If $g(X)$ is irreducible, then this quotient ring is a *field extension* of F, in which $g(X) = 0$ has a solution (cf. PSet 11 # 7).

- Elements in $F[X]/(g(X))$ can all be written (uniquely!) as $\overline{r(X)}$, where $\deg r(X) < \deg g(X)$.
- Understand the isomorphism between $\mathbb{C}$ (complex numbers) and $\mathbb{R}[X]/(X^2+1)$, which is a good prototype for these "field extensions."