Review info for the final (Fall 2015)

Below is a list of all the sections we've covered, along with definitions and theorems from each section. If theorems are not listed in the "Proofs" section, then you will not be asked to prove them without hints. It should not be necessary to try to memorize the proofs listed, as they will be natural "follow-your-nose" proofs, not tricky ones, so if you know the relevant definitions and previous results, they will be straightforward. If an important theorem is in the exercises and you should know its proof, I will also list it in the proofs section.

As always, pay attention to examples! I also recommend reviewing the true/false question in each section.

Some sections have a lot of problems listed. Usually, these are a good source of examples, and they should be quick and relatively easy. (Don't feel that you need to carefully write out all the suggested problems, or even do them all. These are just good ones to try if you feel you need more practice on a topic. Especially for the computation problems, you might find it's enough to do the odds and check your answers.) The problems listed are mostly computational. There will be a separate handout of short proofs to practice.

Obviously there are way more things than I can reasonably put on the final exam, but this is a pretty good summary of what you should have learned this semester.

Section 0

- Definitions: set, subset, Cartesian product, relation, function/map, domain, codomain, range, one-to-one, onto, partition, equivalence relation
- Suggested problems: 27, 31, 32

Section 1

- Special note: know the examples U_n and U from this section. Be able to work with complex numbers in polar form.

Section 2

- Definitions: binary operation, closure under a binary operation, associative/commutative binary operation, well-definedness for binary operations
- Theorems + proofs: 2.13
- Suggested problems: 7-11, 17-22

Section 3

- Definitions: homomorphism property, identity element
- Theorems + proofs: sort of 3.13, 3.14, which show up later for group homomorphisms
- Suggested problems: 1-5, 11-14 (note that these are all groups; think about whether you have group isomorphisms).
- Special notes: Don't worry too much about this section with regards to binary structures – just think about how the results pertain to group homomorphisms and ring homomorphisms.

Section 4

- Definitions: group, abelian group
- Theorems + proofs: 4.15, 4.16, 4.17, 4.18
- Suggested problems: 1-18
- Special notes: Skip semigroups and monoids, as well as one-sided identities and inverses.

Section 5

- Definitions: order of a group, subgroup, proper/improper subgroup, nontrivial subgroup, cyclic subgroup, generator of a cyclic group
- Theorems (statements only): 5.14, #45 (subgroup criterion)
- Theorems + proofs: 5.17, #41, #54
- Suggested problems: 8-13, 14-19, 26

Section 6

- Definitions: order of an element in a group, division algorithm for $\mathbb{Z}$, gcd and lcm of two integers
- Theorems (statements only): 6.7, 6.10, 6.14, 6.16
- Theorems + proofs: 6.1, 6.6 (proof idea)
- Suggested problems: 1-7, 17-21, 23-29, 49

Section 8

- Definitions: permutation of a set, symmetric group, permutation group, dihedral group (use any sensible notation)
- Theorems (statements only): 8.16 (Cayley's Theorem)
- Theorems + proofs: 8.5, #46
- Suggested problems: 1-9, 11-13, 17, 30-34
- Special notes: Ignore left/right regular representations.

Section 9

- Definitions: orbits of a permutation, cycle, 2-line notation, disjoint cycle notation, transposition, even/odd permutations, alternating group
- Theorems (statements only): 9.8, 9.15
- Theorems + proofs: 9.20
- Suggested problems: 1-12, 14-18
- Special notes: Unlike cosets, orbits do not all have to be the same size. Use disjoint cycle notation for permutations on the exam. Don't forget that permutations are functions, so we work from right to left, as with function composition.

Section 10

- Definitions: left/right cosets, index of a subgroup in a group
- Theorems + proofs: 10.1, 10.10 (Lagrange's Theorem), 10.11, 10.12, 10.14, #39, #40
- Suggested problems: 1-5, 20-24, 30-32

Section 11

- Definitions: direct product of groups
- Theorems (statements only): 11.9, 11.12 (FTFGAG), 11.16 (don't worry about a formal proof – just be able to construct such a subgroup given a particular example),
- Theorems + proofs: 11.5, 11.17
- Suggested problems: 1-25
- Special notes: Be absolutely sure you can use the FTFGAG to determine whether two abelian groups are isomorphic or not. Don't worry about the definition of (in)decomposable groups.

Section 13

- Definitions: group homomorphism, image/inverse image/kernel of a homomorphism, normal subgroup
- Theorems + proofs: 13.12, 13.15, 13.18, 13.20
- Suggested problems: 1-24, 33-43
- Special notes: LOTS of examples in this section.

Section 14

- Definitions: factor/quotient group,
- Theorems (statements only): 14.1 (realize this is a consequence of 14.4; you just need to know how to prove the latter), 14.13
- Theorems + proofs: 14.4, 14.5, 14.9, 14.11 (First isomorphism theorem for groups. You have the map – be able to check it's an isomorphism.)
- Suggested problems: 1-16
- Special notes: The big idea of this section is that normal subgroups of G are exactly those subgroups which can be the kernel of a group homomorphism $\phi : G \to G'$, and these are precisely the ones we can quotient by to make a factor group. Skip automorphisms, conjugation.

Section 15

- Theorems (statements only): 15.6 (converse of Lagrange is false)
- Theorems + proofs: 15.8, 15.9
- Suggested problems: 1-12
- Special notes: Skip the end of the section, starting with simple groups.

Section 18

- Definitions: ring (which for us always has 1), ring homomorphism, kernel of a ring homomorphism, ring isomorphism, commutative ring, unit, division ring, field, subring, subfield
- Theorems (statements only): 18.8, #48 (subring criterion)
- Suggested problems: 1-20

Section 19

- Definitions: zero divisor, integral domain, characteristic of a ring
- Theorems (statements only): 19.3, 19.4, 19.15
- Theorems + proofs: 19.5, 19.9
- Suggested problems: 1-10

Section 20

- Definitions: Euler phi-function
- Theorems (statements only): 20.6, 20.8, 20.10, 20.11, 20.12, 20.13
- Theorems + proofs: 20.1 (Fermat's Little Theorem)
- Suggested problems: 4-5, 11-22
- Special notes: Don't worry about formal proofs about solving congruences, but do be able to justify your work as you actually solve a particular one.

Section 22

- Definitions: indeterminate, polynomial, coefficients, degree, zero/root of a polynomial
- Theorems (statements only): 22.2, 22.4
- Suggested problems: 1-17

Section 23

- Definitions: polynomials which are (ir)reducible over F
- Theorems (statements only): 23.1 (division algorithm for $F[x]$), 23.11, 23.12, 23.15 (Eisenstein Criterion), 23.18, 23.19
- Theorems + proofs: 23.3 , 23.5 (proof summary), 23.10, 23.20 (unique factorization in $F[x]$ – know a summary of the proof)
- Suggested problems: 1-4, 9-16, 18-21

Section 26

- Definitions: ideal, factor/quotient ring
- Theorems (statements only): 26.7, 26.9, 26.14
- Theorems + proofs: 26.3, 26.5, 26.6, 26.16, 26.17 (First isomorphism theorem for rings – again, you have the map, check it's an isomorphism.)
- Suggested problems: 2-4, 12-15
- Special notes: The big idea of this section is that ideals of R are exactly those subsets which can be the kernel of a ring homomorphism $\phi : R \to R'$, and these are precisely the ones we can quotient by to make a factor ring.

Section 27

- Definitions: maximal ideal, prime ideal, prime field, principal ideal
- Theorems (statements only): 27.24, 27.25, 27.17, 27.18, 27.19 (note: if F has a subring isom to $\mathbb{Z}$, then it has a subfield isom to $\mathbb{Q}$)
- Theorems + proofs: 27.5, 27.6, 27.9, 27.11, 27.15, 27.16, 27.27
- Suggested problems: 1-9, 15-19
- Special notes: We didn't specifically discuss prime fields much in lecture, but you can see the basics from the reading.

Section 29

- Definitions: extension field, algebraic/transcendental over F, irreducible polynomial for α over F, $F(\alpha)$ – see Cases I-II on p.270, simple extension
- Theorems (statements only): 29.12, 29.18
- Theorems + proofs: 29.3 (I could ask for an outline or 1-2 steps of this proof), 29.13 (idea only)
- Suggested problems: 1-5, 9-16
- Special notes: The big highlight of this section is Case I on p.270, since this is how we build finite simple extensions.

Section 30

- Definitions: vector space, basis, span, linear (in)dependence, linear combination, finite-dimensional
- Theorems (statements only): 30.16, 30.17, 30.18, 30.20, 30.23
- Most of these we use rather implicitly (versus explicitly), but it is important to know the foundations that let us build 30.23.

Section 31

- Definitions: algebraic extension, finite extension, algebraically closed, algebraic closure
- Theorems (statements only): 31.4 (know the rough idea – use two “small” bases to find the “big” basis), 31.17, 31.18 (Fundamental Theorem of Algebra)
- Theorems + proofs: 31.3, 31.7, 31.15, 31.16
- Suggested problems: 1-13
- Special notes: Skip Theorem 31.12 and the algebraic closure of F in E. Skip everything after the statement of the Fundamental Theorem of Algebra. You may use the fact that $F(\alpha_1, \ldots, \alpha_k)$ is the smallest subfield of $\overline{F}$ which contains F and all α_i.