Math 371, Final Exam Review Sheet

General information

(1) The exam will be comprehensive, with some emphasis on material covered since the last exam.
(2) The exam will be in class on Tuesday December 17 from 11 AM–2 PM. Books and notes will not be allowed; you may use a scientific (non-graphing) calculator if you wish.
(3) WARNING: this study guide is not meant to be exhaustive. Just because something is not on the study guide does not mean it will not be on the exam.

Advice for your proofs

- Unless a problem explicitly asks for a heuristic argument, credit will not be given for rough outlines, picture "proofs," and arguments like "it is obvious that." Give careful, complete proofs of all your claims.
- Use complete English sentences in your proofs.
- Clearly indicate what your hypotheses are, what your conclusions are, the logical flow of your argument, and why each step is correct.
- If you write your conclusion into the proof before it is proved, your proof will be considered circular and will not get credit.

Basics

- Be able to do all homework problems.
- Know everything that was on the study guides for the first three exams.
- Know all the definitions discussed in the book, especially the definitions of
  - a group, an abelian group, a subgroup, and a cyclic group
  - the center of a group, direct product of groups, simple group
  - a ring, a field, an integral domain
  - a zero divisor, a subring, an ideal
  - a ring homomorphism and a ring isomorphism
  - the kernel and image of a homomorphism
  - quotient rings
  - maximal ideals
  - the direct product of two rings
  - a monic polynomial, an irreducible polynomial
- Know lots of examples of all the things we talked about, especially:
  - Examples of rings, both commutative and non-commutative, of every order.
  - Examples of subrings and ideals with many different properties (including subrings that are not ideals, maximal ideals, non-maximal ideals, etc.).
  - A ring with no subrings; a ring with no proper ideals.
  - A commutative ring that is not an integral domain.
  - An integral domain that is not a field.
  - A non-trivial ring homomorphism that is not surjective.
  - A non-trivial ring homomorphism that is not injective.
  - An automorphism of $F[x]$ that is non-trivial, where F is a field.
  - A maximal ideal that does not contain all proper ideals in the ring.
  - An infinite ring and an ideal with a finite quotient ring.
  - An infinite ring and an ideal with an infinite quotient ring.
  - A non-commutative ring and an ideal with a commutative quotient ring.
  - A field with 9 elements, and a ring with 9 elements that is not a field.
  - A field F that properly contains the rationals $\mathbb{Q}$ and is properly contained in the reals $\mathbb{R}$ (i.e., $\mathbb{Q} \subset F \subset \mathbb{R}$).
  - A subgroup of an infinite group that has finite index.

Things you should know and be able to use, but need not prove

- The fundamental theorem of finite Abelian groups, the Sylow theorems
- Every permutation is either even or odd, but not both
- A group G is isomorphic to the direct product $M \times N$ of two subgroups M and N if and only if the following conditions hold: (1) M and N are normal in G, (2) $M \cap N = \{e\}$ and (3) $MN = G$.

Theorems you should be able to state and prove and use

- Cancellation is valid in any integral domain R: if $a \neq 0_R$ and $ab = ac$, then $b = c$. (Theorem 3.10 in the second edition, and Theorem 3.7 in the third edition).
- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$. (Theorem 2.2 in the second edition, and Theorem 2.6 in the third edition.)
- Every finite integral domain is a field. (Theorem 3.11 in the second edition, and Theorem 3.9 in the third edition.)
- The First Isomorphism Theorem for rings (Theorem 6.13 in both editions).
- For a field F and an irreducible $p(x) \in F[x]$, the extension field $F[x]/(p(x))$ contains a root of $p(x)$ (Theorem 5.11 in both editions).
- Remainder and factor theorems (Theorems 4.14 and 4.15 in the second edition, or Theorems 4.15 and 4.16 in the third edition).
- The First Isomorphism Theorem for groups (Theorem 7.42 in Ed.2, Theorem 8.20 in Ed.3).
- The center of a group is a subgroup (Theorem 7.12 in Ed.2, Theorem 7.13 in Ed.3).
- Lagrange's theorem: the order of a subgroup of a finite group divides the order of the group (Theorem 7.26 in Ed.2, Theorem 8.5 in Ed.3).
- Cauchy's theorem: A finite group with order divisible by p contains an element of order p. (See proof available on course website.)

Other examples of things you should know well

- Every subgroup of a cyclic group is cyclic.
- Disjoint cycles in S_n commute.
- Every permutation in S_n is the product of disjoint cycles.
- Every k-cycle in S_n has order k.
- Every permutation is the product of transpositions.
- A_n is a normal subgroup of S_n of order $n!/2$.
- Inverses and identity are unique in a group.
- Groups of prime order are cyclic.
- The kernel of a homomorphism is a normal subgroup of the source group.
- If N is a normal subgroup of G, then the set G/N of all cosets of N in G forms a group with the induced operation.
- If N is a normal subgroup of G, then there is a (canonical) surjective homomorphism $G \to G/N$.
- $|G/N| = |G|/|N|$.
- All the things about 0 and negatives in rings that you thought were "obvious."
- If R is a commutative ring with unit, then $R[x]$ is a commutative ring with unit.
- If F is a field, then $F[x]$ is an integral domain.
- The division algorithm.
- Every element of $F[x]$ has unique (up to units) factorization as a product of irreducibles.

Sample problems

(1) Prove that A_n is a normal subgroup of S_n.
(2) Determine whether $(1234)(57)(689) \in S_{10}$ is even or odd.
(3) Is there an element in S_4 of order 6? Prove your answer is correct (either find one and prove it has the right order, or prove that none exists).
(4) Find a surjective group homomorphism $S_5 \to \mathbb{Z}_2$.
(5) If H is a finite subset of a group G such that H is closed under the operation of G, then H is a subgroup of G.
(6) Find all the subgroups of D_4.
(7) Prove there is no non-trivial group homomorphism $S_3 \to \mathbb{Z}_3$.
(8) True or false (prove your answer is correct): Every abelian group of order 35 is cyclic.
(9) True or false (prove your answer is correct): For every homomorphism $\phi : G \to G'$, the kernel of ϕ is trivial (equal to e) if and only if ϕ is injective.
(10) Prove that the kernel of a homomorphism is a subgroup of the source group.
(11) Prove that the image of a homomorphism is a subgroup of the target group.
(12) True or false (prove your answer is correct): For every group G and any element $a \in G$, the map $\psi_a : G \to G$ defined by $\psi_a(x) = a^{-1}xa$ is an automorphism of G.
(13) List all (isomorphism classes of) abelian groups of order 24, and prove that your list is complete and has no duplicates.
(14) Prove that every group of prime order is cyclic.
(15) Prove that $\mathbb{Z}_8 \times \mathbb{Z}_{30} \cong \mathbb{Z}_{24} \times \mathbb{Z}_{10}$ by giving an explicit isomorphism.
(16) Find all non-trivial homomorphisms from S_3 to $\mathbb{Z}_6$.
(17) Prove that $(\mathbb{Z} \times \mathbb{Z})/\langle(0,1)\rangle$ is an infinite cyclic group.
(18) If p and q are prime show that every proper subgroup of a group of order pq is cyclic.