Math 371, Exam 1, Study Guide

General information

(1) The exam will cover all of chapters 1–3 and 4.1–4.2.
(2) The exam will be in the testing center on Wednesday–Friday, February 2–4. After 2 pm on Friday the Testing Center will charge you a late fee. We suggest you take it earlier and save your money. Be sure to give yourself several hours to finish.
(3) Books, notes, and calculators will not be allowed.
(4) 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.

Basics

- Be able to do all homework problems.
- Know all the definitions discussed in the book, especially the definitions of
  - a prime number
  - a ring, a commutative ring, a ring with identity, an integral domain, a field
  - a zero divisor
  - a unit
  - a subring
  - a ring homomorphism and a ring isomorphism
  - the direct (Cartesian) product of two rings
  - the definition of $\mathbb{Z}_n$ and the definition of $+$ and $\cdot$ for $\mathbb{Z}_n$
  - $F[x]$, a monic polynomial, and an irreducible polynomial
  - the gcd of two integers or of two polynomials
- Know lots of examples of all the things we talked about, especially:
  (1) Examples of rings, both commutative and non-commutative, of every order and type
  (2) Examples of subrings with different properties.
  (3) Examples of polynomials.
  (4) Examples of all sorts of homomorphisms
    (a) A ring homomorphism that is injective but not surjective.
    (b) A ring homomorphism that is surjective but not injective.
    (c) A surjective homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.
    (d) A non-trivial ring isomorphism.
    (e) A map that preserves addition, but not multiplication.
    (f) A map that preserves multiplication, but not addition.

Theorems or Axioms you should know and be able to use

(1) The Well-Ordering Axiom
(2) The division algorithm for $\mathbb{Z}$ and $F[x]$
(3) The Euclidean algorithm for $\mathbb{Z}$ and $F[x]$
(4) In $\mathbb{Z}$ or in $F[x]$ the gcd of f and g can be written as $uf + vg$ for some u and v.
(5) The Fundamental Theorem of Arithmetic.

Theorems you should be able to prove and be able to use

(1) Every field is an integral domain.
(2) $\mathbb{Z}_p$ is a field.
(3) The equation $ax = b$ has solutions in $\mathbb{Z}_n$ if and only if $(a, n)|b$.
(4) The operations of $+$ and $\cdot$ in $\mathbb{Z}_n$ are well-defined.
(5) In any ring R, and for any $a \in R$, we have $0 \cdot a = a \cdot 0 = 0$.
(6) In any ring R, and for any $a \in R$, we have $-(-a) = a$.
(7) In any ring R, and for any $a, b \in R$, we have $(-a) \cdot b = -(ab)$.
(8) To check that a subset $S \subseteq R$ is a subring, it suffices to check that S is closed under subtraction and multiplication.

(9) If R is a commutative ring with multiplicative identity, then $R[x]$ is a commutative ring with multiplicative identity.
(10) If F is a field, then $F[x]$ is an integral domain.
(11) The image of a homomorphism $f : R \to S$ is a subring of S.
(12) 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. Also, note that the proof in the 3rd edition has a double typo: bc should be ac, twice.)
(13) A finite integral domain is a field.
(14) For any $f, g \in R[x]$ we have $\deg(fg) \leq \deg(f) + \deg(g)$. If R is an integral domain, then $\deg(fg) = \deg(f) + \deg(g)$. (Theorem 4.2)

Sample problems

(1) Prove or disprove: $\mathbb{Z}_{15}$ is a field.
(2) Prove or disprove: $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$.
(3) Prove or disprove: $\mathbb{Z}_8 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.
(4) Prove or disprove: If A and B are both subrings of C, then $A \cap B$ is a subring of A and of B and of C.
(5) Prove or disprove: If A and B are both subrings of C, then $A \cup B$ is a subring of C.
(6) Use the Euclidean algorithm to find $\gcd(63, 189)$. Write the gcd as a linear combination of the two integers:

$$\gcd(63, 189) = 63a + 189b.$$

(7) Find the gcd of $4x^4 + 2x^3 + 6x^2 + 4x + 5$ and $3x^3 + 5x^2 + 6x$ in $\mathbb{Z}_7[x]$.
(8) What is the last digit of the number 7^{2010}? (Hint: Use congruence $\pmod{10}$.)
(9) Prove or disprove: The set of functions which are differentiable on all of $\mathbb{R}$ forms a subring of the ring of all functions with domain $\mathbb{R}$, with the standard definitions of $+$ and $\cdot$.
(10) If there exists a ring isomorphism $A \to B$ we write $A \cong B$. Prove that $\cong$ is an equivalence relation on the class of all rings.
(11) Prove that an integer is divisible by 11 if and only if the alternating sum of its digits is congruent to 0 modulo 11; for example $132 \mapsto 1 - 3 + 2 \equiv 0 \bmod 11$, so $11|132$.
(12) Let T be the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Let $\theta : T \to \mathbb{R}$ be the function defined by $\theta(f) = f(5)$. Prove that θ is a surjective homomorphism. Is θ an isomorphism (prove or disprove)?