Math 371, Exam 1, Study Guide

GENERAL INFORMATION

(1) The exam will cover all of chapters 1–4, through section 4.4.
(2) The exam will be in the testing center on Thursday and Friday, February 9–10. For a fee, the testing center will also let you take it on Saturday the 11th (note that the testing center closes at 4 PM on Saturday). Be sure to give yourself several hours to finish.
(3) Books and notes will not be allowed; testing center calculators will be allowed, but may not be of much help.
(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 ring, a field, an integral domain
  – a zero divisor
  – a subring
  – a ring homomorphism and a ring isomorphism
  – the direct (Cartesian) product of two rings
  – a monic polynomial
  – a prime number and an irreducible polynomial
  – a unit
  – the gcd of a pair of polynomials or of a pair of integers
  – the definition of $\mathbb{Z}_n$ and the definition of $+$ and $\cdot$ for $\mathbb{Z}_n$
• 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 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.
  (3) Examples of all sorts of polynomials
     (a) A ring $R$ and an irreducible polynomial $f$ in $R[x]$ of degree 2.
     (b) A ring $R$ and a polynomial of degree 2 with 4 roots.

THEOREMS OR AXIOMS YOU SHOULD KNOW AND BE ABLE TO USE

(1) The Well-Ordering Axiom
(2) The division algorithm for both $\mathbb{Z}$ and $F[x]
(3) The Euclidean algorithm for both $\mathbb{Z}$ and $F[x]
(4) In both $\mathbb{Z}$ and $F[x]$, the gcd of $f$ and $g$ can be written as $uf + vg$ for some $u$ and $v$.
(5) The Fundamental Theorem of Arithmetic for $\mathbb{Z}$ and its counterpart for $F[x]
(6) A finite integral domain is a field, and every field is an integral domain.
(7) $\mathbb{Z}_p$ is a field.
(8) The equation $ax = b$ has solutions in $\mathbb{Z}_n$ if and only if $(a, n)|b$.
(9) The operations of $+$ and $\cdot$ in $\mathbb{Z}_n$ are well-defined.
(10) In any ring $R$, and for any $a \in R$, we have $0 \cdot a = a \cdot 0 = 0$.
(11) In any ring $R$, and for any $a \in R$, we have $-(a) = a$
(12) In any ring $R$, and for any $a, b \in R$, we have $(-a) \cdot b = -(ab)$
(13) To check that a nonempty subset $S \subseteq R$ is a subring, it suffices to check that $S$ is closed under subtraction and multiplication.
(14) If $R$ is a commutative ring with multiplicative identity, then $R[x]$ is a commutative ring with multiplicative identity.

(15) If $F$ is a field, then $F[x]$ is an integral domain.

(16) If $F$ is a field then for any $f \in F[x]$ and any $a \in F$, the element $a$ is a root of $f$ if and only if $(x - a)$ divides $f$.

(17) The image of a homomorphism $f : R \to S$ is a subring of $S$.

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

(1) Cancellation is valid in any integral domain $R$: if $a \neq 0_R$ and $ab = ac$, then $b = c$. (Theorem 3.10).

(2) For any $f, g \in R[x]$ we have $\deg(fg) \leq \deg(f) + \deg(g)$. If $R$ is an integral domain, then we have $\deg(fg) = \deg(f) + \deg(g)$. (Theorem 4.2)

(3) Remainder and factor theorems (Theorem 4.14 and Theorem 4.15)

**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: $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

(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 $\gcd(x^7 - 128, x^2 - 4)$, where the polynomials are in $\mathbb{Q}[x]$. Write the $\gcd$ as a linear combination of the two polynomials:

$$\gcd(x^7 - 128, x^2 - 4) = a(x^7 - 128) + b(x^2 - 4).$$

(7) What is the last digit of the number $7^{2010}$?

(8) 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 $\cdot$.

(9) If there exists a ring isomorphism $A \cong B$ we write $A \cong B$. Prove that $\cong$ is an equivalence relation on the class of all rings.

(10) Find the $\gcd$ of $4x^4 + 2x^3 + 3x^2 + 4x + 5$ and $3x^3 + 5x^2 + 6x$ in $\mathbb{Z}_7[x]$.

(11) 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 $\theta$ is a surjective homomorphism. Is $\theta$ an isomorphism?