MATH 4000/6000 – Final Exam Study Guide

Exam time/location: Wednesday, April 30, 12:00 PM – 3 PM, usual classroom

The exam is **cumulative**. You should expect ≤ 10 questions, with a format similar to that used in the three midterms. For material covered on or before Exam #2, please consult the previous review sheets.

Basic definitions

You should be able to give precise descriptions of all of the following:

- isomorphism (and associated terminology/notation, such as "isomorphic" and the symbol "$\cong$")
- direct product $R \times S$ of the rings R and S
- group, abelian group
- order of an element in a group
- subgroup
- cyclic subgroup $\langle g \rangle$
- left coset of a subgroup

Big theorems

Give full statements of each of the following results, making sure to indicate all necessary hypotheses. For results proved in class or on HW, describe the components and main ideas of the proof.

- isomorphism is reflexive, symmetric, and transitive
- Fundamental Homomorphism Theorem
- ring-theoretic restatement of the Chinese Remainder Theorem
- if $g^m = 1$, then the order of g divides m
- Lagrange's theorem: The size of a subgroup of a finite group always divides the size of the group.

What to know how to do (not comprehensive!)

- Use the Euclidean algorithm to compute inverses of elements in $F[x]/\langle m(x) \rangle$
- Apply the ring-theoretic Chinese Remainder Theorem to answer questions about $\mathbb{Z}_m$ by decomposing $\mathbb{Z}_m$ into "similar pieces"
- Reason with direct products of rings (e.g., compute the number of units in a direct product based on the number of units in the component rings)
- Carry out multiplication of elements in explicitly given groups (e.g., S_3 and D_4)

Course outline/summary

Part I: The Integers

- Axioms: $\mathbb{Z}$ is a commutative ring with $1 \neq 0$, ordered, and satisfies the well-ordering principle (see the initial handout)
- Binomial theorem
- Theory of divisibility
  - basic definitions and properties of divisibility
  - definition of the gcd
  - Euclid's algorithm for computing the gcd
  - gcd can be written as a linear combination of starting numbers
- Euclid's lemma
- Unique factorization theorem
- Congruences
  - basic definitions
  - congruence mod m is an equivalence relation
  - Fermat's little theorem
  - inverses and cancelation; solving $ax \equiv b \mod m$
  - simultaneous congruences and the Chinese remainder theorem

Part II: Rings: First examples

- Ring axioms
- Definition of **fields** and **integral domains**
- Detailed discussion of $\mathbb{Z}_m$
  - $\bar{a}$ is a unit in $\mathbb{Z}_m \iff \gcd(a, m) = 1$
  - for positive integers m, $\mathbb{Z}_m$ is a field $\iff m$ is prime $\iff \mathbb{Z}_m$ is an integral domain
- Definition of $\mathbb{Q}$ from $\mathbb{Z}$ (ordered pairs up to cross-multiplication equivalence); verification that $+$ and $\cdot$ are well-defined
- Definition of $\mathbb{R}$ via Cauchy sequences: **not examinable!**
- Definition of $\mathbb{C}$ from $\mathbb{R}$
- Fundamental Theorem of Algebra (statement only)

Part III: Polynomials over commutative rings

- Definition of the polynomial ring $R[x]$
- Basic properties
  - if R is a domain, then $R[x]$ is a domain
  - if R is a domain, $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$
  - if R is a field, then u is a unit in $R[x] \iff u$ is a nonzero constant in R
- Division algorithm in $F[x]$ (F a field)
- gcds in $F[x]$ and their properties
- irreducibles (primes) in $F[x]$, Euclid's lemma, unique factorization theorem in $F[x]$
- Root-Factor theorem
- Testing irreducibility of polynomials with integer coefficients
  - rational root test
  - reduction modulo p
  - Eisenstein's criterion

Part IV: Ring homomorphisms and ideals

- Definition of a ring homomorphism
- Kernel of a homomorphism; $\ker \phi = \{0\} \iff \phi$ is injective
- definition of an ideal of a commutative ring
- $\mathbb{Z}$ and $F[x]$ are principal ideal domains: all ideals are of the form $\langle a \rangle$ for a single element a
- Construction of the quotient ring R/I, for an ideal I of R
- Definition of ring isomorphism and verification that isomorphism is an equivalence relation
- Direct products of rings
- Fundamental Homomorphism Theorem
- Chinese Remainder Theorem in ring-theoretic form

Part V: Introduction to groups

- Definition of a group and basic properties (such as uniqueness of identities and inverses)
- If R is a ring, then R is a group udner addition, and $R^\times = \{\text{units of } R\}$ is a group under multiplication
- For each set S, $\mathrm{Perm}(S) = \{\text{bijections } f\colon S \to S\}$ is a group under function composition
- Symmetry group of the square
- Order of an element in a group; proof that every element in a finite group has a finite order.
- The cyclic subgroup $\langle g \rangle$ generated by an element g; if g has finite order, then $|\langle g \rangle|$ is the order of g.
- (Left) cosets of a subgroup H; proof that every coset of a subgroup H is in one-to-one-correspondence (bijection) with H.
- Lagrange's theorem: If H is a subgroup of the finite group G, then the size of H divides the size of G.

Practice problems over material since Exam #2

1. For this problem, recall that if n is an integer and r belongs to the ring R, then

$$n \cdot r = \begin{cases} r + r + \cdots + r \ (n \text{ times}) & \text{when } n > 0, \\ 0 & \text{when } n = 0, \\ -r + -r + \cdots + -r \ (|n| \text{ times}) & \text{when } n < 0. \end{cases}$$

   For any ring R, the map $\phi\colon \mathbb{Z} \to R$ defined by $\phi(n) = n \cdot 1$ is a ring homomorphism. In fact, ϕ is the unique homomorphism from $\mathbb{Z}$ to $\mathbb{R}$. (You are being told these facts; you do not have to prove them.)

   For the rest of this problem, assume R is an integral domain.

   (a) Prove that $\operatorname{im}(\phi)$ is an integral domain.

   (b) State the Fundamental Homomorphism Theorem.

   (c) Using (a), (b), and results from class, show that $\ker(\phi) = \langle 0 \rangle$ or $\ker(\phi) = \langle p \rangle$ for some prime number p.

   (d) Give an example of a domain R for which $\ker(\phi) = \langle 0 \rangle$ and a different example where $\ker(\phi) = \langle 17 \rangle$.

2. (a) State the ring-theoretic version of the Chinese Remainder Theorem.

   (b) Prove that if p is a prime, there are precisely two solutions to the equation $x^2 = x$ in $\mathbb{Z}_p$.

   (c) How many solutions to $x^2 = x$ are there in $\mathbb{Z}_{210}$? Justify your answer. (Note that $210 = 2 \cdot 3 \cdot 5 \cdot 7$.)

3. Let G be a group.

   (a) What does it mean to say that G is abelian?

   (b) Suppose that G is an abelian group and that $g, h \in G$ with orders 2 and 3 respectively. Show that $(gh)^6 = 1$.

   (c) Continue with the assumptions of part (b). Prove that gh has order 6 in G.

4. (a) If g is a group and $g \in G$, what do we mean when we write $\langle g \rangle$?

   (b) A group G is said to be cyclic if there is a $g \in G$ for which $\langle g \rangle = G$. Prove that if G is cyclic, then G is abelian.

   (c) Prove that $\mathbb{Q}$, under addition, is not a cyclic group. (Don't be confused by the notation: Remember that the group operation here is addition!)