MATH 4000/6000 – Final Exam Study Guide

Exam time/location: Friday, May 3, 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. At most 2 problems will test your knowledge of degrees of field extensions.

Course 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!**

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 in $F[x]$, Euclid's lemma, unique factorization theorem in $F[x]$
- root-factor theorem
- The Fundamental Theorem of Algebra (proof non-examinable)
- testing irreducibility of polynomials with integer coefficients
  - rational root test
  - reduction modulo p
  - Eisenstein's criterion

Part IV: Field extensions, part 1

- definition of $F[\alpha]$, where α belongs to a field extension of F
- definition of $f(x)$ splitting over F; definition of a splitting field for $f(x) \in F[x]$ over F
- $F[\alpha]$ is a field if α is is a root of nonconstant polynomial in $F[x]$

Part V: Ring homomorphisms

- 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
- ring isomorphisms (basic properties) and the Fundamental Homomorphism Theorem
- direct products of rings

Part VI: Field extensions, part 2

- If $f(x) \in F[x]$ is irreducible, then $K = F[x]/\langle f(x) \rangle$ is a field extension of F that also contains at least one root of $f(x)$ (namely, $\bar{x}$)
- If $f(x) \in F[x]$, there is a field extension K of F over which f splits; moreover, there is a splitting field for $f(x)$ over F
- definition of the degree $[K : F]$
- degrees multiply in towers
- if $p(x)$ is irreducible of degree n over F, then $K = F[x]/\langle p(x) \rangle$ is a field extension of F with $[K : F] = n$.
- if $K = F[\alpha]$ where α is a root of a degree n irreducible polynomial in $F[x]$, then $[K : F] = n$

Practice problems over §5.1

1. Find the degree $[K : F]$ in each of the following cases.

   (a) $F = \mathbb{Q}$, $K = \mathbb{Q}[\sqrt{2}]$,

   (b) $F = \mathbb{Q}[i]$, $K = \mathbb{Q}[\sqrt{3}, i]$,

   (c) $F = \mathbb{Q}[\sqrt{3} + i]$, $K = \mathbb{Q}[\sqrt{3}, i]$.

   (d) $F = \mathbb{Q}[i]$, $K = \mathbb{Q}[\sqrt[5]{8}, i]$,

2. (a) Find $[\mathbb{Q}[\sqrt[6]{2}, \sqrt[7]{2}] : \mathbb{Q}]$.

   (b) Show: $\mathbb{Q}[\sqrt[6]{2}, \sqrt[8]{2}] = \mathbb{Q}[\sqrt[24]{2}]$. What is $[\mathbb{Q}[\sqrt[6]{2}, \sqrt[8]{2}] : \mathbb{Q}]$?

3. One can show (you are not asked to do so) that the polynomial $p(x) = x^6 + x^3 + 1$ is irreducible over $F = \mathbb{Z}_2$. Let $K = \mathbb{Z}_2[x]/\langle p(x) \rangle$ and let $\alpha = \bar{x} \in K$.

   (a) Show that if F' is a field with $F \subsetneq F' \subsetneq K$, then $[F' : F] = 2$ or $[F' : F] = 3$.

   (b) Let $\beta = \alpha^3$. Find $[K : F[\beta]]$ and $[F[\beta] : F]$.

4. Let F be a field. Suppose $f(x) \in F[x]$ has degree 3. Prove that there is a field K containing F satisfying (a) $f(x)$ splits over K, (b) $\deg f(x) \leq 6$.