Math 4000 – Final Exam Review Sheet

Exam time/location: Monday, December 14, 12:00 PM–3:00 PM, usual classroom

The exam is **cumulative**. The following is a "summary of course topics"; this list was discussed in class on Tuesday, December 8. Note that the material on Cauchy sequences is not examinable.

For material covered before Thanksgiving break, please refer to review sheets for midterms #1 – #3. For the material on geometric constructions, you should (a) be able to state the theorems listed in the topical outline (b) be able to apply them to determine, given a real number or a point in the plane, whether or not it is constructible.

Topical outline

Part I: The Integers

- Axioms: $\mathbb{Z}$ is a commutating ring with $1 \neq 0$, ordered, satisfies the well-ordering principle
- 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
- There are infinitely many prime numbers
- Congruences
  - basic definitions
  - congruence mod m is an equivalence relation
  - tests for divisibility (by 2, 5, 9)
  - 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 $\mathbb{R}$: **not examinable!**
- Definition of $\mathbb{C}$ from $\mathbb{R}$
- Basic properties of complex numbers
  - basic concepts: complex conjugation, absolute value, polar form
  - multiplication of complex numbers in polar form
  - de Moivre's theorem
  - n distinct nth roots of 1 for every n
  - solving linear, quadratic, and cubic equations over $\mathbb{C}$

Part III: Polynomials over commutative rings

- Definition of the polynomial ring $R[x]$
- Basic properties
  - $R[x]$ is a domain $\iff R$ is a domain
  - if R is a domain, u is a unit in $R[x] \iff u$ is a unit in R
  - if R is a domain, $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$
- 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 case $F = \mathbb{C}$: The Fundamental Theorem of Algebra
- testing irreducibility for polynomials with integer coefficients
  - rational root test
  - method of undetermined coefficients
  - reduction modulo p
  - Eisenstein's criterion

Part IV: Field extensions, part 1

- definition of a field extension
- definition of $F[\alpha]$, where α belongs to an extension of F
- definition of $f(x)$ splitting completely; definition of a splitting field for $f(x) \in F[x]$ over F
- $F[\alpha]$ is a field if α is the root of some nonzero 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
- definition of the minimal polynomial of α over F, where α belongs to a field extension of F
- construction of the quotient ring R/I, for an ideal I of R
- ring isomorphisms (basic properties) and the fundamental homomorphism theorem

Part VII: Gaussian integers

- Division algorithm in $\mathbb{Z}[i]$
- Theory of gcds, primes, Euclid's lemma, unique factorization
- Determination of which primes in $\mathbb{Z}$ stay prime in $\mathbb{Z}[i]$: p stays prime in $\mathbb{Z}[i] \iff p$ cannot be written in the form $x^2 + y^2 \iff p \equiv 3 \pmod 4$

Part VI: Field extensions, part 2

- If $f(x) \in F[x]$ is irreducible, then $K = F[x]/\langle f(x) \rangle$ is an extension of F that contains at least one root of $f(x)$ (namely, $\bar{x}$)
- If $f(x) \in F[x]$, there is an extension K of F over which f splits; moreover, there is a splitting field for $f(x)$ over F
- definition of the degree of a field extension
- degree is multiplicative in towers
- if K/F is a finite extension of fields, then every $\alpha \in K$ is the root of a nonzero polynomial in $F[x]$ of degree dividing $[K : F]$

- if $K = F[\alpha]$ and the min. poly of α over F has degree n, then $[K : F] = n$
- every finite field is an extension of $\mathbb{Z}_p$ for some prime p, and has size p^n for a positive integer n

Part VII: Constructions

- The constructible numbers form a field $\mathbb{K}$
- $\alpha \in \mathbb{R}$ is constructible $\iff$ α satisfies the "chain-of-fields criterion"
- if $\alpha \in \mathbb{R}$ is constructible, then $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ is a power of 2
- the set of constructible points $\mathbb{CK}$ forms a subfield of $\mathbb{C}$, and $\mathbb{CK} = \mathbb{K}[i]$

Additional practice problems

1. Let a, b, and c be three positive integers.

   (a) Show that $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.

   (b) Let d denote the common value of the expressions in part (a). Show that there are integers x, y, and z with $d = ax + by + cz$.

   (c) Show that the following equation of ideals holds in $\mathbb{Z}$: $\langle a, b, c\rangle = \langle d\rangle$.

2. Recall that an element x of a ring R is **nilpotent** if there is a positive integer n with $x^n = 0$. Let m be an integer with $m > 1$.

   (a) Show that in $\mathbb{Z}_m$, the element $\bar{a}$ is nilpotent if and only if every prime dividing m also divides a.

   (b) How many distinct nilpotent elements are there in $\mathbb{Z}_m$ if $m = 2 \cdot 3^2 \cdot 5^3$?

3. (a) If p is prime, how many solutions are there to the equation $x^2 = \bar{1}$ in $\mathbb{Z}_p$? Justify your answer.

   (b) Let $m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$. How many solutions are there to the equation $x^2 = \bar{1}$ in $\mathbb{Z}_m$?
   Hint: Use the Chinese remainder theorem.

4. Let F be a field. Suppose $f(x)$ and $g(x)$ are nonconstant polynomials in $F[x]$. Let K be a field containing F over which the product $f(x)g(x)$ splits.

   (a) Show that if $f(x)$ and $g(x)$ are relatively prime in $F[x]$, then $f(x)$ and $g(x)$ have no common roots in K.

   (b) Prove the converse of (a): If $f(x)$ and $g(x)$ have no common roots in K, then $f(x)$ and $g(x)$ are relatively prime in $F[x]$.

5. Suppose that $\phi \colon R \to S$ is an isomorphism of rings. Give a detailed proof that if R is an integral domain, so is S.

6. It can be shown that the number $\pi = 3.1415926\ldots$ is not the root of any nonzero polynomial $p(x) \in \mathbb{Q}[x]$.

   (a) Show that the map $\phi\colon \mathbb{Q}[x] \to \mathbb{Q}[\pi]$ given by $f(x) \mapsto f(\pi)$ is an isomorphism.

   (b) Is $\mathbb{Q}[\pi]$ a field? Why or why not?

7. Let F be any field. Show that there are infinitely many monic irreducible polynomials in $F[x]$.

8. Let R be a commutative ring, and let U be the collection of units in R. Fix an element $u \in U$.

   (a) Show that if $x \in U$, then $ux \in U$.

   (b) From part (a), it makes sense to define a map $\phi\colon U \to U$ by the equation $\phi(x) = ux$, for every $x \in U$.

   Show that ϕ is a bijection from U to U.

   (c) Now assume that U is a finite set, say $\#U = n$, where n is a positive integer. Deduce from (b) that $u^n = 1$.

   Hint: How does $\prod_{x \in U} \phi(x)$ compare with $\prod_{x \in U} x$?

   (d) If $R = \mathbb{Z}_p$, part (c) gives another proof of a theorem discussed in class. Which theorem?

   (e) More generally than (d), suppose R is a finite field. What conclusion do you draw from (c)?

9. Is $\mathbb{Q}[x]/\langle x^2 - 2\rangle$ isomorphic to $\mathbb{Q}[x]/\langle x^2 - 3\rangle$? Why or why not?

10. What is the degree of (a) $\mathbb{Q}[\sqrt[7]{16}]$ as an extension of $\mathbb{Q}$? b) $\mathbb{Q}[\sqrt[12]{2}, \sqrt[18]{2}]$ as an extension of $\mathbb{Q}$?

11. (a) Prove that $\cos(3\theta) = 4\cos(\theta)^3 - 3\cos(\theta)$ for every real θ.

    (b) Decide whether or not the point $(\cos(\pi/9), \sin(\pi/9))$ is constructible.