The exam is **cumulative**. The following is a "summary of course topics".

Topical outline

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 $\mathbb{C}$ 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

    - if R is a domain, $\deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$
    - if R is a domain, then $R[x]$ is a domain
    - 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
    - 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 algebraic over F

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

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 (proof not examinable)

- if $K = F[\alpha]$ and the min. poly of α over F has degree n, then $[K : F] = n$

Additional practice problems

Please refer to the review sheets for Exams #1–#3 for practice problems on the material covered in Chapters 1–4. The following problems concern (only) the material covered in Chapter 5.

1. We showed that if F is a field and $f(x) \in F[x]$ is irreducible of degree n, then $K = F[x]/\langle f(x) \rangle$ is a field extension of F. What is $[K : F]$ in this case?

2. Let K/F be an extension of fields with $[K : F] = p$, where p is prime. Show that if E is any field with $F \subseteq E \subseteq K$, then $E = F$ or $E = K$.

3. What is the degree of
   (a) $\mathbb{Q}[\sqrt[7]{2}]$ as an extension of $\mathbb{Q}$?
   (b) $\mathbb{Q}[\sqrt[7]{4}]$ as an extension of $\mathbb{Q}$? *Hint:* First show that $\mathbb{Q}[\sqrt[7]{4}]$ is a subfield of $\mathbb{Q}[\sqrt[7]{2}]$.
   (c) $\mathbb{Q}[\sqrt[7]{2}, \sqrt[9]{2}]$ as an extension of $\mathbb{Q}$?
   (d) $\mathbb{Q}[\sqrt[12]{2}, \sqrt[18]{2}]$ as an extension of $\mathbb{Q}$?
   (e) $\mathbb{Q}[\cos(2\pi/5) + i \sin(2\pi/5)]$ as an extension of $\mathbb{Q}$?
   (f) $\mathbb{Q}[\sqrt{3} + i]$ as an extension of $\mathbb{Q}[\sqrt{3}]$.

4. Recall the following fact from linear algebra: If V is an n-dimensional vector space, then any $n + 1$ vectors in V are linearly dependent.

(a) Use the quoted fact to prove that if K/F is a field extension of degree n, then every $\alpha \in K$ is algebraic over F. *Hint:* Look at the "vectors" $1, \alpha, \ldots, \alpha^n$.

(b) (continuation) Keep the assumption that K/F is a field extension of degree n. Show that if $\alpha \in K$, then $F[\alpha]$ is a field extension of F, and $[F[\alpha] : F]$ divides n.