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 · 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 \( n \)th roots of every nonzero complex number
  – 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
  – reduction modulo \( p \)
  – Eisenstein’s criterion

Part IV: Field extensions, part 1

• definition of a field extension
• definition of \( F[\alpha] \), where \( \alpha \) 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 \( \alpha \) 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
- \( \mathbb{Z}, F[x], \) and \( \mathbb{Z}[i] \) 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
- if \( K = F[\alpha] \) and \( \alpha \) is a root of a degree \( n \) irreducible polynomial over \( F \), then \( [K : F] = n \)