MATH 4000/6000 – 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
  - 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 and properties 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
  - 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
- 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 $F[x]$
- remainder theorem and root-factor theorem
- The Fundamental Theorem of Algebra (**proof** non-examinable, but understand the statement!)
- testing irreducibility of polynomials in $\mathbb{Q}[x]$
  - rational root test
  - reduction modulo p
  - Eisenstein's criterion

Part IV: Field extensions, part 1

- definition of a subfield/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 $f(x)$ over F
- if K/F is a field extension, and $\alpha \in K$ is the root of a nonzero polynomial in $F[x]$, then $F[\alpha]$ is a field

Part V: Ring homomorphisms

- definition of a ring homomorphism
- kernel of a homomorphism
- $\mathbb{Z}$, $F[x]$, and $\mathbb{Z}[i]$ have all their ideals principal; that is, 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
- description of the elements of $F[x]/\langle m(x) \rangle$; determination when $F[x]/\langle m(x) \rangle$ is a domain and when it is a field
- ring isomorphisms (basic properties)
- the fundamental homomorphism theorem
- direct product of two rings

Part VI: Gaussian integers

- definition of $\mathbb{Z}[i]$
- division algorithm in $\mathbb{Z}[i]$
- every ideal of $\mathbb{Z}[i]$ is principal
- definition of a prime in $\mathbb{Z}[i]$
- every prime number p (in $\mathbb{Z}$) with $p \equiv 1 \pmod 4$ is the norm of an element of $\mathbb{Z}[i]$, and hence a sum of two squares

Part VII: Field extensions, part 2

- If $f(x) \in F[x]$ is irreducible, then $K = F[t]/\langle f(t) \rangle$ is an extension of F that contains at least one root of $f(x)$ (namely, $\bar{t}$)
- 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 $L/K/F$; that is, $[L : F] = [L : K] \cdot [K : F]$
- if K/F is a field extension, and $\alpha \in K$ is the root of an irreducible polynomial of degree n in $F[x]$, then $[F[\alpha] : F] = n$
- if L/F has degree n, then every $\alpha \in L$ is the root of a nonconstant polynomial in $F[x]$; moreover, if $\alpha \in L$ is the root of $p(x) \in F[x]$ where $p(x)$ is irreducible, then the degree of $p(x)$ divides n

Part VIII: Finite fields (not examinable)

- Every finite field contains a subring isomorphic to $\mathbb{Z}_p$ for some prime p
- If F is a finite field, then F has p^n elements for some prime p and some positive integer n
- For each prime p, and positive integer n, there is a field F with p^n elements: namely, take a field K containing $\mathbb{Z}_p$ over which $x^{p^n} - x$ splits, and let F be the collection of roots of $x^{p^n} - x$ inside K
- Any two finite fields of size p^n are isomorphic