Final Preparation – MA521 – Fall 2019

Chapter 1. (DF §1.1-1.7)

- Definition of a group, types of group (finite, abelian)
- Order of group, and group elements
- Examples: $\mathbb{Z}/n\mathbb{Z}$, D_{2n}, S_n, $\mathrm{GL}_n(\mathbb{F})$
- Presentation of a group and relations,
- Group homomorphisms, isomorphisms, kernel
- Group action on a set, orbits, stabilizers

Chapter 2. (DF §2.1-2.5)

- Subgroup definition, criterion
- Special examples: centralizers, normalizers, stabilizers, kernels
- Intersections and generation of subgroups
- lattice of subgroups

Chapter 3. (DF §3.1-3.5)

- Normal subgroups, quotient group
- Cosets, Lagrange's Theorem
- Isomorphism Theorems
- Simple groups, composition series
- The alternating group A_n

Chapter 4. (DF §4.1-4.5)

- Group action terminology: kernel, stabilizer, faithful, transitive, orbit
- Cayley's Theorem
- Conjugacy classes, the class equation
- Conjugacy in S_n via cycle decomposition
- Automorphism group of a group
- Sylow p-subgroups, Sylow theorems

Chapter 5. (DF §5.1, 5.4, 5.5)

- Direct products, recognizing direct products
- Semi-direct products, constructing and recognizing semi-direct products
- Applications to groups of small sizes

Chapter 7. (DF §7.1-7.6)

- Definition of a ring types of ring (commutative, with an identity)
- Units, zero-divisors
- Division ring, field, integral domain
- Subring, Ideal
- Examples: Polynomial rings, matrix rings
- Ring homomorphism, isomorphism, kernels
- Ideals (left-sided, right-sided, two-sided)
- Quotient Rings, Isomorphism Theorems
- Properties of ideals (maximal, prime)
- Rings of fractions, quotient fields
- Chinese Remainder Theorem

Chapter 8. (DF §8.1-8.3)

- Euclidean domains, division algorithm, greatest common divisors
- Principal ideal domains
- Unique factorization domains, irreducible elements, prime elements
- Important examples: $\mathbb{Z}, \mathbb{Z}[i]$, polynomials rings

Chapter 13. (DF §13.1, 13.2, 13.4, 13.5)

- Characteristic of a field
- Field extensions, algebraic vs. transcendental, minimal polynomial
- Finite extensions, finitely generations extensions, degree of a field extension
- Composite fields
- Splitting fields, algebraic closure
- Multiplicity of roots, separable vs. inseparable extensions

Chapter 14. (DF §14.1- 14.4, 14.6, 14.7, 14.9)

- Automorphism $\mathrm{Aut}(K/F)$ group of a field extension
- Connection with minimal polynomials
- Fixed field of a subgroup of $\mathrm{Aut}(K/F)$
- Galois extensions, Galois group
- Connection with splitting fields of separable polynomials
- Fundamental theorem of Galois theory
- Applications to finite fields
- Application to composite extensions
- Primitive Element Theorem
- Elementary symmetric polynomials, fundamental theorem of symmetric polynomials
- Discriminant
- Solvable and radical extensions, connection with solvable and cyclic groups
- Transcendental elements, transcendence basis

Some practice problems (from material after the midterm)

(1) Find the greatest common divisor of $a = x^6 + x^2 + 1$ and $b = x^4 + x^3 + x^2 + x + 1$ in $\mathbb{F}_2[x]$ and polynomials $c, d \in \mathbb{F}_2[x]$ so that $ac + bd = \gcd(a, b)$.

(2) Let F be a field and suppose that $f, g \in F[x]$ are irreducible with $\gcd(f, g) = 1$. Is $F[x]/\langle f \cdot g \rangle$ an integral domain?

(3) Give the prime factorization of $65 = 5 \cdot 13$ in $\mathbb{Z}[i]$ and use it to write 65 as a sum of integer squares in two different ways.

(4) A ring R is called a Boolean ring if $a^2 = a$ for all $a \in R$. Prove that every Boolean ring is commutative.

(5) True or false: For $R = \mathbb{Q}[x]$ and $D = \{x^n : n \in \mathbb{Z}_+\}$, the ring of fractions $D^{-1}R$ equals $\mathbb{Q}(x)$.

(6) Let Γ be a subgroup of $\mathrm{GL}_n(\mathbb{Q})$. Show that $A \cdot f(\mathbf{x}) = f(A\mathbf{x})$ defines an action of Γ on the polynomial ring $R = \mathbb{Q}[x_1, \ldots, x_n]$ and that the set of polynomials fixed by this action form a subring of R. Does it form an ideal of R?

(7) True or false: Let R be a principal ideal domain, $I \subsetneq R$ be an ideal, and $f, g \in R$. If the images of f and g are the same in $R/(I^n)$ for every $n \in \mathbb{Z}_+$, then $f = g$. (Here I^n denotes the product of ideals $I \cdot I \cdots I$.)

(8) Are $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ isomorphic as fields?

(9) Let F be a field of characteristic $\neq 2$ and K/F a Galois field extension with $\mathrm{Gal}(K/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Show that there exist $D_1, D_2 \in F$ for which $K = F(\sqrt{D_1}, \sqrt{D_2})$.

(10) Let K be the splitting field of $(x^7 - 2)$ over $\mathbb{Q}$. What is the isomorphism type of the group $\mathrm{Gal}(K/F)$?

(11) Find minimal polynomial of $\sqrt{2} + \sqrt{5}$ over $\mathbb{Q}$.

(12) Any Galois extension K/F of degree 15 has an intermediate field extension $F \subsetneq E \subsetneq K$ for which E/F is also a Galois extension.

(13) Given an example of a finite field extension that is not separable.

(14) Give an example of a finite field extension that is separable but not Galois.