Math 476

Final Exam Review Sheet

Part I: Groups

A. Background

- Know the Well Ordering Principle and the Division Algorithm for integers. Also know the statement of Euclid's Lemma.
- Know the definitions of the terms: greatest common divisor, least common multiple, prime, and relatively prime.
- Understand Modular Arithmetic and be able to carry out addition and multiplication mod n.
- Know the definition of a binary operation and be able to both read and construct Cayley Tables.
- Understand the definition of associativity, commutativity, identity element, the inverse of an element, and a zero element and be able to determine whether or not which of these are satisfied or present in a given binary operation on a set.

B. Groups and Subgroups

- Know the definition of a group and be able to determine whether or not a binary operation on a set is a group.
- Be familiar with all of the examples of groups given in Table 2.1 in your textbook.
- Know the statements and proofs of Theorems 2.1, 2.2, 2.3, and 2.4 and be able to apply them.
- Know the definition of the order of a group and the order of an element of a group and be able to apply them.
- Know the definition of a subgroup of a group and be able to determine whether or not a subset of a group is a subgroup.
- Know the statements and proof of Theorem 3.4. Also know the definition of $Z(G)$ and $C(a)$.

C. Cyclic Groups and Permutation Groups

- Know the statements of Theorem 4.1, Theorem 4.2, Theorem 4.3 and their Corollaries.
- Be able to apply these results to find all generators for a cyclic group G, to find all possible orders of elements in G, to find all subgroups of G, and construct the subgroup lattice for G.
- Understand the definition of a permutation and be able to represent them in both double row and disjoint cycle notation.
- Be able to find the product of two (or more) permutations. Also be able to write a permutation as a product of 2-cycles.
- Know the proof of Theorem 5.2 and the statements of Theorems 5.1, 5.3, 5.4, 5.5, and 5.7.
- Know the definition of even and odd permutations and be able to determine whether a given permutation is even or odd.
- Be able to find the order of a given permutation. Also be able to determine the number of elements of a given order in S_n.
- Know the definition of A_n and be able to show that A_n is a subgroup of S_n for any n.

E. Group Isomorphisms and Homomorphisms

- Know the definition of group isomorphism and be able to determine whether or not a given function is an isomorphism.
- Given two groups, be able to either show that two groups are isomorphic or to prove that they cannot be isomorphic.
- Know the definition of a group homomorphism. Also be able to determine whether or not a given function between two groups is a homomorphism.
- Know the properties of isomorphisms and the properties of homomorphisms (see Theorems 6.2, 6.3, 10.1, and 10.2) It is highly likely that I will ask you to prove some of these properties.
- Know the definition of the kernel of a homomorphism and be able to find the kernel of a given homomorphism.
- Be able to determine all homomorphisms between two groups $\mathbb{Z}_n$ and $\mathbb{Z}_m$ and be able to investigate the properties or a specific homomorphism of this form.

F. Cosets, Normal Subgroups, and Factor Groups

- Know the definition of the left (right) cosets of a subgroup H of a group G. Also be able to find the cosets in a particular example.
- Know the properties of cosets in the main Lemma from page 139 in the textbook. It is likely that I will ask you to prove one or two of these properties.
- Know the statement of LaGrange's Theorem and its first 4 corollaries and be able to apply them.
- Know that the converse of Lagrange's theorem is false (also know a specific counterexample).
- Know the definition of a normal subgroup and be able to determine whether or not a subgroup of a given group is normal.
- Know the definition of a factor group. Know and be able to prove Theorem 9.2.
- Be able to build a Cayley table for a specific factor group and be able to carry out computations in a given factor group.

G. External Direct Products and Finite Abelian Groups

- Know the definition of the external direct product of a finite number of groups. Also be able to compute the order of elements in the direct product of two groups.
- Know and be able to apply Theorem 8.2 and its two corollaries.
- Know the statement of Theorem 11.1 and be able to apply it to analyze abelian groups of a given order.
- Know the statement of the Corollary to Theorem 11.1 and be able to apply it.

H. Conjugacy Classes and the Sylow Theorems

• Know the definition of the conjugacy class of an element and be able to prove that conjugacy is an equivalence relation.
• Be able to find the conjugacy classes of the elements of a group and/or conjugates of a subgroup of a group.
• Know the statements of the Sylow Theorems (24.3, 24.4, and 24.5 and the Corollary to Theorem 24.5).
• Be able to apply the Sylow Theorems in order to determine whether or not a group of a given order has a proper non-trivial normal subgroup.

Part II: Rings

A. Rings and Integral Domains

• Know the definitions of a ring, a commutative ring, a ring with unity, a unit, divisibility, and scalar multiplication.
• Know the properties of rings from Theorem 12.1. Also know the statement and proof of Theorem 12.2.
• Know the definition of a subring of a ring and be able to to determine whether or not a subset of a ring is a subring.
• Be familiar with standard examples of rings and their subrings.
• Know the definition of a zero divisor of a ring and the definition of an integral domain.
• Be able to find examples of zero divisors in various rings. Also be able to determine whether or not a given ring is an integral domain.
• Know the definition of a field and be able to determine whether or not a given ring is a field.
• Know the statements and proofs of both Theorem 13.1 and Theorem 13.2.
• Know the definition of the characteristic of a ring with unity. Also know the statements of Theorem 13.3 and Theorem 13.4.

B. Ideals and Factor Rings

• Know the definition of an ideal of a ring and be able to determine whether or not a given subset of a ring is an ideal.
• Know the definition of a factor ring. Also know the statement and proof of Theorem 14.2
• Be able to build the Cayley tables for a specific factor ring and be able to carry out computations in a given factor ring.
• Know the definitions of a prime ideal and maximal ideals. Be able to find the maximal ideals of a given ring.
• Know the statement and proof of Theorem 14.3 and the statement of Theorem 14.4.

C. Ring Homomorphisms

• Know the definition of a ring homomorphism. Also be able to determine whether or not a given function between two rings is a homomorphism.
• Know the definition of a ring isomorphism. Also be familiar with examples of ring homomorphisms and ring isomorphisms.
• Know and be able to prove the properties from Theorem 15.1. Also know the statements of Theorems 15.2, 15.3, and 15.4
• Know the the statement and proof of Theorem 15.6. I will not make you for the entire proof, but I may have prove one or more of the properties needed to verify that the construction of a field of quotients is well defined or that the resulting object is indeed a field.
• Be able to carry out computations in a field of quotients.

D. Polynomial Rings and Factorization

• Know the definition of a ring of polynomials $R[x]$, including the operations in $R[x]$, the degree of a polynomial, leading term, leading coefficient, constant term, monic polynomial, and the definition of a PID.
• Know the Division Algorithm and be able to carry it out in polynomial rings of any characteristic.
• Be able to prove the Remainder Theorem, The Factor Theorem, and Theorem 16.3
• Know the definition of reducible and irreducible polynomials in an integral domain D.
• Know both the statement and proof of both Theorem 17.1 and Theorem 17.3
• Given a polynomial in $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$, be able to use irreducibility tests to show that the polynomial is irreducible.
• Given a polynomial in $\mathbb{Z}_p[x]$ be able to either use irreducibility tests to show that the polynomial is irreducible, or be able to fully factor the polynomial.
• Know the statement of Theorem 17.5 and the statement of both of its corollaries. Be able to use Corollary 1 to construct a finite field.

E. Fields

• Know the definition of an extension field of a field $\mathbb{F}$. Also know the statement of Theorem 20.1 (The Fundamental Theorem of Field Theory).
• Know the statement of Theorem 22.1 and the definition of the Galois field of order p^n.
• Be able to construct a finite field of a given order. Also be able to construct the conversion tables for both addition and multiplication for the field you constructed.
• Know the statement of Theorem 22.3, and be able to draw the subfield lattice for a given Galois field.