Abstract Algebra 1 (MATH 3140)

Review for the Final Exam

Summary of Topics

The Basics [See Review for the Midterm]

Algebraic Themes [See Review for the Midterm]

Cyclic Groups. Subgroups of a Group and Lagrange's Theorem (Lectures 2/22–3/01, 3/08, 3/17; Sections 2.1–2.3, 2.5)

- Subgroups of a group. Generating set. Cyclic group. The order of a group element. Every cyclic group is isomorphic to the additive group $\mathbb{Z}$ or to the additive group $\mathbb{Z}_n$ for some nonzero natural number n. Subgroups of cyclic groups.
- The dihedral groups D_n ($n \geq 3$).
- Left/right cosets of a subgroup. Lagrange's Theorem and its consequences on orders of elements and subgroups of finite groups. Groups of prime order are cyclic.

Group Homomorphisms. Normal Subgroups and Quotient groups. Homomorphism/Isomorphism Theorems (Lectures 3/10–3/26; Sections 2.4, 2.6 (p. 133), 2.7)

- Homomorphisms between groups. Subgroups and homomorphisms. Kernel of a homomorphism. Normal subgroups of a group. Characterizations of normal subgroups. Conjugation, conjugacy classes of a group.
- Quotient group of a group by a normal subgroup. The Homomorphism Theorem.
- Isomorphism Theorems: Correspondence Theorem, Diamond Isomorphism Theorem, quotient groups of a quotient group.

Direct Product, Semidirect Product (Lectures 3/29–4/05; Sections 3.1–3.2, parts of 3.6)

- Direct product of (finitely many) groups. Decomposing a group into an internal direct product of two (more generally, finitely many) normal subgroups.
- The Chinese Remainder Theorem for $\mathbb{Z}_n$ (as an additive group and also as a ring).
- Decomposing a group into an internal semidirect product of a subgroup and a normal subgroup. The (external) semidirect product construction.
- Finite abelian groups: the Primary Decomposition Theorem; statement of the Fundamental Theorem of Finite Abelian Groups.

Group Actions and Sylow's Theorems (Lectures 4/07–4/16; Sections 5.1, 5.3–5.4)

- Group actions. The action of a group on itself by left multiplication and by conjugation. The action of a group on the set of left cosets of a subgroup by left multiplication. Orbits of an action, transitive action. Stabilizer of an element, and the Orbit-Stabilizer Theorem.
- The automorphism group and the inner automorphism group of a group. The automorphism group of $\mathbb{Z}_n$.

- The Class Equation. Finite p-groups have a nontrivial center, groups of order p^2 are abelian (p prime). Sylow p-subgroups of a finite group (p prime). Sylow's 1st Theorem and Cauchy's Theorem.
- Statement of Sylow's 2nd and 3rd Theorems. The classification of finite groups of order pq ($p > q$ primes). Groups of order $n \leq 15$, $n \neq 8, 12$.

Polynomial Rings over Fields, and their Quotient Rings (Lectures 4/19–4/26; Sections 1.8, 3.6 (Thm. 3.6.25), parts of 6.2–6.3)

- The ring $K[x]$ of polynomials in one indeterminate x over a field K. The degree of a nonzero polynomial in $K[x]$. Divisibility, greatest common divisors (g.c.d.s), and the Division Algorithm. The Euclidean Algorithm and its consequences on divisibility and g.c.d.s. Irreducible polynomials and unique irreducible factorization in $K[x]$.
- Evaluation homomorphisms, roots of polynomials. A polynomial of degree $n\,(\geq 1)$ in $K[x]$ has at most n roots in K. Every finite subgroup of K^* is cyclic.
- The kernel of a ring homomorphism. Ideals and quotient rings of rings. The Homomorphism Theorem for rings.
- Ideals of $K[x]$. The quotient ring $K[x]/(f)$ is a field if $f \in K[x]$ is irreducible. Construction of finite fields of orders p^n (p prime).

Advice on how to prepare for the exam

- Know the definitions of the concepts, and understand what they mean.
- Know the major theorems, and understand what they mean.
- Understand the proofs done in class and in solutions to homework problems.
- Know how to correct mistakes made on homework problems and quizzes.

During the exam

- The final exam will be administered through Canvas, and we will be using the Proctorio Online Exam Proctoring Service.
- During the Final Exam you will be allowed to use your textbook, your notes, and any material posted for the course on the course web page or on Canvas.
  You will not be permitted to use any other sources during the Final Exam.
  In particular, you will not be permitted
  (i) to use any book other than the textbook or any other person's notes,
  (ii) to use any other information from the internet, or
  (iii) to communicate about the course material or the Final Exam with any person (other than the instructor for the course).
- When a problem asks you to give a detailed solution or a proof, justify each step of your argument by citing the assumption, definition, or theorem you are using. Specify your proof method (unless it is a direct proof), and state your assumption(s) and desired conclusion(s).
- Unless a problem specifies it otherwise, to prove a statement you may use any definitions and any statements proved in class, in the text assigned for reading (see the course web page), or in a homework problem.

Practice Problems

1. Find all finite groups that have
(a) exactly two conjugacy classes,
(b) exactly three conjugacy classes.

2. Recall that $V = \{\mathrm{id},\ (1\,2)(3\,4),\ (1\,3)(2\,4),\ (1\,4)(2\,3)\}$ is a normal subgroup of A_4; it is, in fact a normal subgroup of S_4 as well. (You may use this fact without proof.)
(a) Find a subgroup H of S_4 such that $H \cong S_3$ and S_4 is an internal semidirect product of $H \leq S_4$ and $V \trianglelefteq S_4$.
(b) Use the result in part (a) to show that $S_4/V \cong S_3$.

3. Let G be a group and H a subgroup of G. Let $\varphi\colon H \to \mathrm{Sym}(G)$ be the action of H on G by left multiplication; i.e., for each $h \in H$, $\varphi(h)$ is the permutation $G \to G$, $x \mapsto hx$ of G.
(a) What are the orbits of this action?
(b) What does the Orbit-Stabilizer Theorem tell us about this action?
(c) What is the relationship between the answers to the questions in parts (a)–(b) and Lagrange's Theorem?

4. Let H and K be finite groups, let $G = H \times K$, and let p be a prime that divides $|G|$. Prove that every Sylow p-subgroup of G is the direct product of a Sylow p-subgroup of H and a Sylow p-subgroup of K. (If $p \nmid |H|$, consider $\{e_H\}$ be the Sylow p-subgroup of H; similarly for K, if $p \nmid |K|$.)

5. Let R and S be rings with identity elements 1_R and 1_S, respectively, and let $\varphi\colon R \to S$ be a ring homomorphism. Verify that
(a) φ is unital (i.e., $\varphi(1_R) = 1_S$ holds for φ) if and only if $\varphi(S)$ is a subring of S with identity element 1_S.
(b) φ is unital, if it is surjective.

6. Let $f = x^4 + 2x^2 + 1 \in \mathbb{Z}_3[x]$. Show that
(a) the quotient ring $R = \mathbb{Z}_3[x]/(f)$ contains two nonzero elements whose product is the zero element of R (so, R is not a field), but
(b) the element $x^2 + x - 1 + (f)$ of R has a multiplicative inverse.
(c) Compute the multiplicative inverse of $x^2 + x - 1 + (f) \in R$.

7. Give an example of each of the following, or prove that such an example does not exist:
(a) A group G with a subgroup H of index 3 such that $H \ntrianglelefteq G$.
(b) A group with two subgroups of the same order that are not isomorphic.
(c) Two nonisomorphic groups of order 77.
(d) A finite group G that does not have a transitive action on any set of size $|G|$.
(e) A nonabelian group of order 121.
(f) A dihedral group D_n ($n \geq 3$) and an odd prime p dividing $|D_n| = 2n$ such that D_n has two or more Sylow p-subgroups.
(g) An irreducible polynomial $f \in \mathbb{Z}_2[x]$ of degree 5 in which the coefficient of x is 0.