Abstract Algebra 1 (MATH 3140)

Review for the Midterm

Summary of Topics

The Basics (Lectures 1/25–2/03)

- Some axioms of set theory; set constructions. Relations and functions.
- Constructing and communicating proofs.
- The natural numbers: Definition of the set $\mathbb{N}$ of natural numbers (using the Infinity Axiom). The Induction Theorem. Definitions of $m < n$, $m + n$, mn, and m^n for $m, n \in \mathbb{N}$; basic properties of these operations and the relations $<$ and $\leq$.
- The definitions of a finite set and its cardinality. Properties of functions between finite sets. Subsets of finite sets.

Algebraic Themes (Lectures 1/20–1/22, 2/05–2/19; Sections 1.1–1.7, 1.10–1.11)

- Symmetries of a rectangle and a square. Symmetries and matrices. Symmetries and permutations.
- Permutations. Cycle decomposition of permutations in S_n. Transpositions. Even and odd permutations in S_n.
- The integers: Construction of $\mathbb{Z}$ from $\mathbb{N}$. Divisibility, gcd. The Euclidean algorithm and writing $\gcd(a, b)$ as an integer linear combination of a and b ($a, b \in \mathbb{Z}$). The existence and uniqueness of prime factorization for natural numbers > 1. Modular arithmetic.
- Definitions and examples of groups, rings, and fields. Isomorphism.

Theory of Groups (Lectures 2/22–3/01; Sections 2.1–2.2)

- 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.

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 midterm exam will be administered through Canvas, and we will be using the Proctorio Online Exam Proctoring Service.
- During the midterm you will be allowed to use your book, your notes, and any material posted for the course on the course web page or on Canvas. However, during the exam, you will not be permitted to (i) use any other information from the internet or (ii) communicate about the course material 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. Prove that if $f\colon A \to B$ and $g\colon B \to C$ are functions such that $g \circ f$ is injective and f is surjective, then g is injective.

2. Use only properties of natural numbers (no theorems on finite sets) and induction on n to prove the following statement for every $n \in \mathbb{N}$:

For any set A and for any $m \in \mathbb{N}$ such that there exist an injective function $f\colon A \to n$ and a bijective function $A \to m$, we have that $m \leq n$.[1]

You may use the statement proved in Problem 1, Homework 2.

3. Prove that if $p_1, p_2, \ldots, p_r$ are distinct primes and $a, b \in \mathbb{N} \setminus \{0\}$ have prime factorizations $a = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ and $b = p_1^{\ell_1} p_2^{\ell_2} \ldots p_r^{\ell_r}$, where $k_1, k_2, \ldots, k_r, \ell_1, \ell_2, \ldots, \ell_r \in \mathbb{N}$, then

$$\gcd(a, b) = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r} \quad \text{where} \quad m_i = \min(k_i, \ell_i) \text{ for all } i \ (1 \leq i \leq r).$$

(Note: $k_i = 0$ means that p_i does not occur in the prime factorization of a. Similarly, $\ell_i = 0$ means that p_i does not occur in the prime factorization of b.)

4. Let $G = \langle a \rangle$ be a cyclic group of order $1932 = 2^2 \cdot 3 \cdot 7 \cdot 23$.

(a) Show that $\langle a^{294} \rangle \subseteq \langle a^{189} \rangle$.

(b) Write a^{294} as a power of a^{189}. (That is, find an integer k such that $a^{294} = (a^{189})^k$.)

5. Let G be an arbitrary group.

(a) Show that for any two elements a, b of G, we have $(ab)^2 = a^2 b^2$ if and only if $ab = ba$.

(b) Use the result in part (a) to show that if G is a group such that $g^2 = e$ holds for all $g \in G$, then G is abelian.

6. Let n be a nonzero natural number, and let π be a nonidentity permutation in S_n. Prove that the order of π is the least common multiple of the lengths of the cycles in the cycle decomposition of π.
(For example: $o\big((1\ 2)(3\ 4\ 5)\big) = \operatorname{lcm}(2, 3) = 6$.)

7. Give an example of each of the following, or prove that such an example does not exist:

(a) a finite set A with a surjective function $A \to A$ that is not injective;

(b) two integers a, b such that $\operatorname{lcm}(a, b)$ does not exist;

(c) a subgroup H of S_4 such that H is not cyclic and H is different from S_4 and A_4;

(d) two permutations π, σ in S_4 such that $o(\pi\sigma) < o(\pi), o(\sigma)$;

(e) a cyclic group that is not abelian.

(f) an odd permutation $\pi \in S_n$ such that $o(\pi)$ is odd.

[1] This is statement (2) of Thm. 1.2 in the lecture notes "Background on Finite Sets and Infinite Sets".