Math 546, Exam 1 Information.
9/18/09, LC 303B, 10:10 - 11:00.

Exam 1 will be based on:

- Sections 2.1, 2.2, 2.3, 3.1;
- The corresponding assigned homework problems
  (see http://www.math.sc.edu/~boylan/SCCourses/546Fa09/546.html)
  At minimum, you need to understand how to do the homework problems.
- Lecture notes: 8/21 - 9/11.

Topic List (not necessarily comprehensive):

You will need to know: theorems, results, and definitions from class.

§2.1: Functions.

1. Basic definitions relevant to functions including the definition of "function" itself: domain, codomain, image, preimage, composition of two functions.

2. What does it mean for a function to be one-to-one? onto? a one-to-one correspondence (bijection)?

3. Properties of compositions: The composition of one-to-one functions is one-to-one; the composition of onto functions is onto; the composition of bijections is a bijection; composition is associative, but not commutative; what is the inverse of a composition?

4. If \( f : S \rightarrow T \) is a function with \( |S| = |T| \) finite, then \( f \) one-to-one implies that \( f \) is onto; \( f \) onto implies that \( f \) is one-to-one.

5. When does a function have an inverse?

§2.2: Equivalence relations. A binary relation on a set \( S \) is an equivalence relation if and only if it satisfies the reflexive, symmetric, and transitive properties. If \( \sim \) is an equivalence relation on \( S \), then the equivalence class of \( a \in S \) is \( [a] \), a subset of \( S \) consisting of all \( b \in S \) with \( a \sim b \). The factor set of \( S \) modulo \( \sim \) is the set of all equivalence classes.

Key example. Let \( n \in \mathbb{N} \): Congruence modulo \( n \).

Key properties of equivalence relations. If \( \sim \) is an equivalence relation on \( S \), then the equivalence classes under \( \sim \) form a partition of \( S \). In other words, \( S \) is a disjoint union of the equivalence classes for \( \sim \).
§2.3: Permutations. A permutation of a set $S$ is a one-to-one and onto function (a bijection) $\sigma : S \rightarrow S$. The set of all permutations of a set $S$ is denoted $\text{Sym}(S)$. If $S = \{1, 2, \ldots, n\}$, then $\text{Sym}(S) = S_n$. Under the operation of composition, $\text{Sym}(S)$ is closed, associative, has an identity ($1_S$) and all elements have inverses. Therefore it is a group, called the symmetric group on $S$.

Be able to work with permutations in $S_n$:

1. Notation: 2-row arrays; cycles. What is a $k$-cycle? What are disjoint cycles?
2. How do you change from 2-row arrays to cycles?
3. How do you multiply (compose) permutations in cycle notation?
4. What is a transposition? How do you write $\sigma \in S_n$ as a product of transpositions?
5. What is an even permutation? An odd permutation? If $\sigma$ is a $k$-cycle, how do you determine whether it is even or odd?

Key facts:

1. Disjoint cycles commute. However, there are cycles that commute, but are not disjoint.
2. Every permutation $\sigma \in S_n$ is expressible as a product of disjoint cycles (i.e., it can be "factored" into disjoint cycles). Moreover, this factorization is unique up to the order in which the factors are multiplied.
3. Every permutation is expressible as a product of transpositions (i.e., it has a factorization into a product of transpositions). However, this factorization is not unique. Nevertheless, the parity (even- or odd-ness) of the number of transposition in any factorization of $\sigma \in S_n$ into is the same.

§3.1: Definition of a Group. What are the group axioms?

Key examples:

1. Let $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Then $(F, +)$, $(F^\times, \times)$ are commutative groups, so is $(\mathbb{Z}, +)$, but $(\mathbb{Z}, \times)$ is not (all but $\pm 1$ have inverses).
2. Let $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ with $M_n(F)$ the set of all $n \times n$ matrices with entries in $F$. Then $(M_n(F), +)$ is a group (commutative), but $(M_n(F), \times)$ is not (it lacks inverses). The set $\text{GL}_n(F)$ consisting of matrices in $M_n(F)$ with non-zero determinant is a group under matrix multiplication. It is not commutative.
3. The set $S_n$ of permutations of $\{1, \ldots, n\}$ is a group under composition.
4. Let $n \in \mathbb{N}$. Then $(\mathbb{Z}_n, +)$ is a commutative group.
5. Let $n \in \mathbb{N}$. Then $U_n = \{x : x^n = 1\}$ is a commutative group under multiplication.
6. The unit quaternions, $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$ form a non-commutative group under multiplication.
7. Let $n \in \mathbb{N}$. Then $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$ is a group under multiplication called the group of units modulo $n$. The key idea is that $a \in \mathbb{Z}_n$ has an inverse modulo $n$ if and only if $\gcd(a, n) = 1$. Ideas from number theory:
(a) If $a, b \in \mathbb{Z}$, not both zero, how is $\gcd(a, b)$ defined? Integers $a$ and $b$ are relatively prime if and only if $\gcd(a, b) = 1$.

(b) If $a, b \in \mathbb{Z}$ not both zero, then $\exists x, y \in \mathbb{Z}$ with $ax + by = \gcd(a, b)$.

(c) If $a, b \in \mathbb{Z}$, not both zero, then $\gcd(a, b) = 1$ if and only if $\exists x, y \in \mathbb{Z}$ with $ax + by = 1$.

(d) Let $n \in \mathbb{N}$. Then
\[
|\mathbb{Z}_n^\times| = \phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)
\]