Math 375, Fall 2005 — About the First Test

The first test for this course will be given in class on Monday, September 26. It will cover material from the textbook up to page 46, as well as the extra material that I introduced about symmetry groups. There will not be any questions that are specifically directed at the material in Chapter 0, but you should be familiar with that material as background.

There will be some proofs on the test, but they will be proofs that are fairly straightforward and that should not require a lot of thought. There will be some short answer questions to test your knowledge of definitions and theorems. And there will be a few computational questions, such as finding the order of a group element or applying the Euclidean algorithm. It is possible that there will be a longer essay-type question.

Here are some important things you should know about:

Binary operation on a set

Commutative binary operation

Associative binary operation

Closure of a binary operation (part of the definition)

Symmetric difference of two sets, $A \triangle B$

Group; identity of a group; inverse of a group element

Abelian group

Caley table of a group (also called simply a "multiplication" table)

Basic examples of groups, including $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^+, *)$, $(\mathbb{R}^+, *)$

The General Linear Group $\mathrm{GL}(\mathbb{R}, 2)$

Symmetries of a square or other regular polygon and the Dihedral groups $\mathcal{D}_n$

The "Division Algorithm": If $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$, then $\exists q, r \in \mathbb{Z}$ with $a = qn + r$ and $0 \leq r < n$

The group $(\mathbb{Z}_n, \oplus)$ of integers under addition modulo n

Uniqueness of identity and of inverses in a group

Additive vs. multiplicative group notation; e.g., in an additive group, the inverse of x is denoted $-x$

$(x^{-1})^{-1} = x$

Left cancellation law and right cancellation law

$(xy)^{-1} = y^{-1}x^{-1}$

Powers of a group element, x^n for $n \in \mathbb{Z}$; properties of exponents for group elements

Order of an element in a group, $o(x)$

Finite order vs. infinite order

Cyclic group; generator of a cyclic group; the notation $\langle a \rangle = \{a^n \mid a \in \mathbb{Z}\}$

Greatest common divisor, (a, b), of two integers

(a, b) can be written as $ax + by$ for some $x, y \in \mathbb{Z}$

Euclidean algorithm

Properties of $o(x)$ (Theorem 4.4), especially: if $o(x) = n$ and $m \in \mathbb{Z}$, then $o(x^m) = \frac{n}{(m,n)}$

Every cyclic group is abelian

Subgroups

Testing whether a subset is a subgroup

Subgroups of $(\mathbb{Z}, +)$ and of $(\mathbb{Z}_n, \oplus)$

Every subgroup of a cyclic group is cyclic