Mathematics 243, section 1 – Algebraic Structures
Information on Exam 3
November 17, 2006

General Information

The third exam this semester will be given the Friday after Thanksgiving, December 1. The exam will cover the material we have discussed since the second exam, through the material on isomorphisms and homomorphisms of groups from class on Monday, November 20. The relevant sections in Gilbert and Gilbert are 2.8, 3.1, 3.2, 3.3, 3.4, and 3.5. The topics to review are:

1) Applications to cryptography (affine and RSA encryption and decryption). I won't ask you to encrypt or decrypt long messages like the ones from Problem Set 8 with either type of system, but you should be prepared to carry out encryption or decryption of one or two characters with just a calculator.
2) The definition of a group; how to determine if a given set with a given binary operation has the structure of a group; key examples such as $\mathbf{Z}_m, +$, the group of invertible classes in $\mathbf{Z}_m$ under multiplication: $\mathbf{Z}_m^\times, \cdot$, the group of invertible 2×2 matrices, $GL(2, \mathbf{R})$ under the matrix product, groups of permutations, etc., what it means for a group to be abelian, which of the key examples are abelian and which are not.
3) Subgroups, the general subgroup criterion from Theorem 3.9, cyclic subgroups.
4) Cyclic groups, generators, orders of elements, the distinct subgroups of a cyclic group of order n.
5) Isomorphisms of groups and group homomorphisms, the kernel, other properties. *Note: we do not have time to "squeeze in" a problem set on this material before the exam, so it will be especially important to try at least a good sample of the review questions below from sections 3.4 and 3.5.*

Proofs to Know

1) Know how to prove Theorem 3.9 and how to apply it to show that subsets of groups are or are not subgroups, both in explicit examples and in cases where the subset is defined by a condition such as we saw in the problems about the center of a group, $K = \{x \in G : x = aha^{-1} for some h \in H\}$, the kernel of a homomorphism, etc.
2) Let $G = \langle a \rangle$ be a cyclic group. Then
   a) Every subgroup H of G is cyclic.
   b) If G is finite cyclic of order n and $H = \langle a^k \rangle$, then $H = \langle a^d \rangle$ where $d = \gcd(n, k)$.
3) If $\varphi : G \to H$ is a group homomorphism, then $\varphi(e_G) = e_H$, and for all $x \in G$, $\varphi(x^{-1}) = (\varphi(x))^{-1}$.
4) The kernel of a group homomorphism $\varphi : G \to G'$ is a subgroup of G.

Some Review Problems

From Gilbert and Gilbert:

1) Section 2.8: 9, 11, 19, 21 (see note 1 under General Information above)
2) Section 3.1: problems like 1-33, 48, 49.
3) Section 3.2: 7, 8, 9, 10, 11, 19, 30, 32 (take m fixed and argue by induction on n), 33 (induction on n)
4) Section 3.3: 1, 7, 10, 11, 16, 17, 18, 19
5) Section 3.4: 1, 2, 3, 7
6) Section 3.5: 1, 2, 3, 5, 13, 14

Review Session

I have off-campus commitments in Boston on the evenings of Tuesday and Wednesday, November 28 and 29. I will need to leave campus at 5:00 pm at the latest each of those days. Thus, if we are going to do an evening review session this time, it has to be Monday, November 27 or Thursday, November 30. I am happy to do a session either evening. I expect Thursday will be more popular. That's OK, but be aware that the better prepared you are that evening, the more valuable the session will be. *A word to the wise: Do not put off studying for this exam until the review session!*

Sample Exam Questions

I. An RSA public-key cryptographic system has $m = 143$ and the encryption exponent $e = 17$.

A) What is the corresponding decryption exponent d?
B) If you use a 26-letter alphabet, represented by the numbers $0, 1, \ldots, 25$, and 3-digit blocks to represent the encrypted symbols, what would be the encrypted form of the plaintext: HC?

Note: Be prepared for questions about affine ciphers as well – see review problems above!

II. Let $\mathbf{Q}$ be the set of rational numbers: $\mathbf{Q} = \{m/n : m, n \in \mathbf{Z}, n \neq 0\}$. Define a binary operation $*$ on $\mathbf{Q} - \{-1\}$ by $x * y = x + y + x \cdot y$ (where $\cdot$ is ordinary multiplication). Is $\mathbf{Q}$ a group under $*$? Why or why not?

III.

A) Find all generators of the group $G = \mathbf{Z}_{21}$, in which the operation is addition mod 21.
B) What are the possible orders of elements of the group G from part A?

IV. Let $G = \langle a \rangle$ be a cyclic group.

A) Show that every subgroup $H \subset G$ is cyclic.
B) Show that if G is finite, with $|G| = n$, then $\langle a^k \rangle = \langle a^d \rangle$ where $d = \gcd(n, k)$.

V. Let $G = \mathbf{Z}_{12}$ and $H = \mathbf{Z}_9$, which are both groups under addition. We write $[x]_{12}$ for the congruence class of x mod 12, and similarly $[x]_9$ for the class mod 9. Define $\phi : G \to H$ by $\phi([x]_{12}) = [3x]_9$.

A) Show that $[x]_{12} = [y]_{12}$ implies $[3x]_9 = [3y]_9$ (so that this mapping actually makes sense).

B) Show that ϕ is a *group homomorphism.*

C) Find all the elements of $\ker(\phi)$.

VI. Let G be a group and let $a \in G$ be a fixed element. Define

$$C(a) = \{x \in G : ax = xa\}$$

A) Is $b = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ in $C(a)$ for $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $G = GL(2, \mathbf{R})$ (a group under matrix multiplication)? Why or why not?

B) Show that $C(a)$ is a subgroup of G.