Mathematics 243, section 3 – Algebraic Structures
Review Sheet, Final Exam
December 7, 2012

General Information

The final examination for this course will be given at 11:30 a.m. on Saturday, December 15 in our regular class room, Swords 302. It will be a comprehensive exam, covering all the material we have studied this semester, divided *roughly* in thirds according to the topics from the three hour exams. Some questions on earlier material (e.g. the one-to-one and onto properties of mappings, binary operations, equivalence relations, etc.) may appear in the context of topics covered later in the semester, though. The exam will be roughly twice the length of one of the three midterms, but you will have the full 2.5 hour period from 11:30 am to 2:00 pm to work on it if you need that much time.

Topics to be Covered

1) Sets: set operations (union, intersection, difference, complement, Cartesian product, etc.) and their properties.
2) Mappings: the 1-1 and onto properties, direct and inverse images of sets under mappings,
3) Binary operations: identity elements, inverses, properties such as associativity, commutativity, key examples such as function composition, matrix addition and multiplication, addition and multiplication in $\mathbf{Z}$ and $\mathbf{Z}_n$, etc.
4) Relations: especially equivalence relations and the partition of a set into equivalence classes under an equivalence relation (key example: the congruence mod n relation on $\mathbf{Z}$ – the set of equivalence classes in that case is $\mathbf{Z}_n$).
5) Properties of $\mathbf{Z}$: the Well-Ordering Property, proof by mathematical induction, the division algorithm, divisibility, prime numbers and prime factorizations, the gcd and lcm of two integers, Euclid's algorithm for the gcd, and its use to find integers p, q satisfying $pm + qn = d$ when $d = \gcd(m, n)$ (especially for computing inverses mod n)
6) The congruence mod n relation on $\mathbf{Z}$ and the integers modulo n, addition and multiplication in $\mathbf{Z}_n$ and their properties.
7) Applications to cryptography (affine and RSA cryptosystems).
8) Groups: the definition, key examples such as $\mathbf{Z}_n$ under addition mod n, matrix groups such as $GL_2(\mathbf{R})$, the permutation group $\mathcal{S}(A)$, the group
$$\mathbf{Z}_n^\times = \{[x] \in \mathbf{Z}_n : [x]^{-1} \text{ (multiplicative inverse) exists}\} = \{[x] \in \mathbf{Z}_n : \gcd(x, n) = 1\}$$
under multiplication mod n
9) Subgroups of groups: know how to determine whether a given subset of a group is a subgroup. Cyclic subgroups.
10) Cyclic groups, generators, orders of elements, etc.
11) Homomorphisms of groups, kernel and image of a homomorphism, isomorphisms.

Proofs to Know

See the review sheets for Exams 1, 2, and 3. (These are reposted on the course homepage in case you need additional copies.)

Philosophical Comments and Suggestions on How to Prepare

- The reason we give final exams in almost all mathematics classes is to encourage students to "put whole courses together" in their minds. Preparing for the final should help to make the ideas "stick" so you will have the material at your disposal to use in later courses.
- You probably have noticed how things that seemed hard earlier in the semester seem easier now. That is because you have been using those concepts repeatedly and deepening your understanding with each "pass." The same thing should happen now with the course as a whole, if you have been approaching the problem sets, the definitions quizzes, and the hour exams in the right way.
- It may not be necessary to say this, but here goes anyway: *You should take this exam seriously* – it is worth 25% of your course average and it can pull your course grade up *or down* depending on how you do.
- Especially because our exam is so late in the exam week, you should get started reviewing early and do some work on this *every day* between now and the date of the final. Don't try to "cram" at the end. There's too much stuff that you need to know to approach preparing that way!
- Reread your class notes in addition to the text, especially for topics where you lost points on the midterms. There are a lot of worked-out examples and discussions of all of the topics we have covered there.
- Look over the midterm exams with the solutions. Go over your corrected problem sets. If there were questions where you lost a lot of points, be sure you understand why what you did was not correct, and how to solve those questions.
- Be sure you actually do enough practice problems so that you have the facility to solve exam-type questions in a limited amount of time. *Even if you have saved solutions for practice problems from the midterms*, it is going to be much more beneficial to do practice problems starting "from scratch" rather than just reading old solutions. Remember, the goal of the course is to get you to be able to develop solutions to these problems yourselves, not just to understand solutions that someone else has written down. Another analogy – as most of you know from your study of languages, it's much easier to understand another language passively than it is to actually use a language actively yourself (for instance, to form your own complete, grammatically correct sentences). The goal of this course is to make you reasonably proficient "algebra speakers" and there's no substitute for active practice on those skills.

Review Session

I will be happy to run a review session for the final exam during study week. We can discuss a time in class on Friday, December 7.

Some Sample Exam Questions

I.

A) Let $A = \mathbf{Z}$, the set of all integers. Consider $\varphi : A \to A$ be the mapping defined by

$$\varphi(x) = \begin{cases} 5x & \text{if } x \text{ is even} \\ x - 2 & \text{if } x \text{ is odd} \end{cases}$$

Is φ one-to-one? Why or why not? Is φ onto? Why or why not?

B) What is $\varphi^{-1}(\{3, 4, 5, 6, 7\})$ for the mapping in part A?

C) What is $\varphi(\{1, 2, 3\} \cap \{x \in A : x^2 < 5\})$?

II.

A) Give the precise statement and the proof of the Division Algorithm in $\mathbf{Z}$.

B) Find the integer $d = \gcd(753, 154)$ and express d in the form $d = 753m + 154n$ for some integers m, n.

C) Show that if a, b, c are integers, $a|(b \cdot c)$ and $\gcd(a, c) = 1$, then $a|b$.

III. Let $f_0 = 0, f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for all $n \geq 2$. The f_n are called the *Fibonacci numbers*; the first few of them are $1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$.

A) Let $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Compute the matrix powers A^2, A^3, A^4. Do you see a pattern developing?

B) (The pattern!) Show by mathematical induction:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$$

for all $n \geq 1$.

IV.

A) In an affine cipher on a 26-letter alphabet, “E” (the most common letter) is encrypted to “Z” and “T” (the next most common letter) is encrypted to “B”. What are the encryption and decryption functions?

B) In an RSA public key cryptosystem, the public key consists of the integer $m = 143$ and the encryption exponent $e = 29$. What is the decryption exponent d?

V. Consider the following set of all 2×2 matrices with real entries:

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbf{R} \right\}.$$

A) Show that G is a group under matrix *addition*.

B) Is the set

$$H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbf{Z} \right\}$$

a subgroup of the group from part A? Why or why not?

VI. All parts of this question refer to $\mathbf{Z}_{30}$, in which the operations are addition and multiplication mod 30.

A) Which elements of $\mathbf{Z}_{30}$ have *multiplicative* inverses in $\mathbf{Z}_{30}$?

B) Find all the elements of the additive group $(\mathbf{Z}_{30}, +)$ that generate the additive subgroup $\langle [24] \rangle$.

VII. Let G and H be groups and let $\varphi : G \to H$ be a group homomorphism.

A) Give the precise definition of the *kernel* of φ, $\ker(\varphi)$.

B) Show that if $K = \ker(\varphi)$ and $g \in G$ is an arbitrary fixed element, then $gKg^{-1} = \{gkg^{-1} \mid k \in K\}$ is equal to K.

C) Show that the relation R on G defined by

$$xRy \Leftrightarrow xy^{-1} \in \ker(\varphi)$$

is an *equivalence relation* on G.