Math 103A Fall 2012 Final review sheet

(This is a slightly revised version of a review sheet from Fall 2006. I tried to remove anything that did not apply to our course as it was taught in 2012, but I may have missed something here or there. Don't be alarmed if the review sheet refers to something we did not cover; just ignore it in that case.)

The following is meant to give you an overview of the course, arranged by topics. This is not the same order as these topics appear in the textbook, or the order we covered them. The idea is that the list may jar your memory about certain topics you feel shaky on, so you can review those for the exam. Don't forget to also review your homework exercises.

The final exam will be like the two midterms, but about twice as long. Since you have 3 hours to complete it, my hope is that time pressure will not be an issue. The final is cumulative. The topics we have covered since midterm 2 will form about a third of the final; they will not be specially emphasized.

1 I. Fundamentals

A. Definition of $\gcd(m,n), \operatorname{lcm}(m,n)$ for $m,n \geq 0$. Relationship between them: $\gcd(m,n)\operatorname{lcm}(m,n) = mn$.

B. Definition of equivalence relations on a set S and equivalence classes. Knowing that S is a disjoint union of equivalence classes.

2 II. Group Basics

A.1. (Definition of a group). A group G is a set with a *binary operation* which is (i) associative, (ii) has an identity element, and for which (iii) every

element has an inverse. A *Cayley table* is a nice way to display the definition of the binary operation if the group is small.

2. (Very basic properties of groups). The identity element is unique. The inverse of an element is unique. Left and right cancelation hold. The rules for exponents hold for powers of elements, so $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$ when this equation is interpreted properly. A group G is *Abelian* if $gh = hg$ for all $g, h \in G$.

3. (Definitions of order of groups and elements in groups.) $|G|$ is the number of elements in G. For $g \in G$, the order of g, written $|g|$, is the smallest *positive* integer n such that $g^n = e$, or ∞ if no such n exists.

B.1. (Definition of subgroup). a subset H of a group G is called a *subgroup* if it is a group in its own right with the same binary operation, restricted to H. (Subgroup test) H is a subgroup if it is closed under products and closed under inverses— be able to apply this to examples.

2. (Cosets) For a fixed subgroup H of G, for $g \in G$, the left coset of H containing g is $gH = \{gh | h \in H\}$, and the right coset of H containing g is $Hg = \{hg | h \in H\}$. You should know the basic properties of cosets, especially: G is the disjoint union of the distinct left cosets, and all of those left cosets have the same size. The index of H in G, $|G : H|$, is defined to be $|G|/|H|$. Alternatively, $|G : H|$ is the size of every left coset of H in G.

3. (Lagrange's theorem and corollaries) If H is a subgroup of G, then $|H|$ divides $|G|$. *You should understand the basic idea of the proof of Lagrange's Theorem, assuming some basic facts about cosets.* If $x \in G$ is any element, then $|x|$ divides the order of $|G|$. *Understand why.* Fermat's little theorem: $x^p \equiv x (\mathrm{mod}\, p)$ for all $x \in \mathbb{Z}$ if p is prime.

C. (Special kinds of subgroups of any group).

1. The center of G, $Z(G) = \{g \in G | xg = gx \text{ for all } x \in G\}$. $Z(G) = G$ if and only if G is Abelian.

2. For $x \in G$, the centralizer of x, $C(x) = \{g \in G | gx = xg\}$. Be able to calculate this in examples. *Understand the proofs that $C(x)$ and $Z(G)$ are subgroups of G.*

3. For $x \in G$, the cyclic subgroup generated by x is $\langle x \rangle = \{x^n | n \in \mathbb{Z}\}$. The order of this subgroup is the same as the order $|x|$ of x.

D. 1. (Cyclic groups). Any cyclic group of order n is isomorphic to $\mathbb{Z}_n$. Any infinite cyclic group is isomorphic to $\mathbb{Z}$. You should understand why, and given a cyclic group G of order n, understand how to find an isomorphism from $\mathbb{Z}_n$ to G.

2. (Subgroups of cyclic groups). If G is cyclic, then every subgroup of G is cyclic. If $G = \langle x \rangle$ is cyclic with $|G| = n$, then there is exactly one subgroup of G with order d, for each number d dividing n, and that subgroup is $\langle x^{n/d} \rangle$.

3. (Orders of elements in cyclic groups). If $G = \langle x \rangle$ is cyclic of order n, then the order of x^m can be calculated from the formula $|x^m| = n/\gcd(m, n)$. In particular $\langle x^m \rangle = \langle x \rangle$ (i.e., x^m is a generator of $\langle x \rangle$) if and only if $\gcd(m, n) = 1$. However, you shouldn't need to memorize these formulas.

E. 1. (Normal Subgroups) Normal subgroups H of G are special subgroups that have the property that the right and left cosets of H in G are the same sets. (Normal subgroup test) If H is a subgroup of G, then H is normal if and only if $xhx^{-1} \in H$ for all $h \in H$ and $x \in G$.

2. For any group G, $Z(G)$ is a normal subgroup of G. If G is an abelian group, then any subgroup of G is normal.

3 III. Important examples of groups

For all of these groups, you should know what they are well enough to be able to do calculations in them, such as multiply elements, find inverses of elements, calculate centers and centralizers, find orders of elements, decide if subsets are subgroups and if so, if they are normal, find cosets of a given subgroup.

A. (Groups of numbers). $\mathbb{Q}, \mathbb{Z}$, and $\mathbb{R}$ under addition. $\mathbb{Q} \setminus \{0\}$ and $\mathbb{R} \setminus \{0\}$ under multiplication. For $n \geq 2$, $\mathbb{Z}_n$, the integers under addition modulo n. $U(n)$, the group of integers relatively prime to n, under multiplication modulo n.

B. (Matrix groups). the group $\mathrm{GL}(2, \mathbb{R})$ of 2×2 matrices with nonzero determinant and the group $\mathrm{SL}(2, \mathbb{R})$ of matrices with determinant 1.

C.1. (Dihedral groups). For $n \geq 3$, D_n is the group of symmetries of a regular n-gon in the plane. D_n has n reflections and n rotations. Be able to

multiply in this group by drawing pictures (and remember the convention that the product M_1M_2 means first do the motion M_2 and *then* the motion M_1.)

2. (Properties of elements in Dihedral groups). Reflections have order 2, and the set of rotations in D_n form a cyclic subgroup isomorphic to $\mathbb{Z}_n$, so the orders of rotations are calculated using properties of cyclic groups. Know why the product of a rotation and a reflection is a reflection, why the product of two rotations is a rotation, and why the product of two reflections is a rotation.

D.1. (Permutation groups). For $n \geq 2$, S_n is the group of all permutations of $\{1, 2, \ldots, n\}$, with the binary operation of function composition. If α and β are permutations, then $\alpha\beta$ means first do β, then do α. $|S_n| = n!$.

2. (Properties of permutation groups.) Every permutation is a product of disjoint cycles—and you should be able to put a permutation in this form if is not already so written. When written in this form, the order of the permutation is the lcm of the lengths of the cycles. Every permutation is a product of (not necessarily disjoint) 2-cycles. When written in this form, the permutation is called even if there are an even number of 2-cycles, and odd otherwise. The set A_n of even permutations is a normal subgroup of S_n, and $|A_n| = n!/2$, i.e. $|S_n : A_n| = 2$.

4 IV. Constructing new groups from old

A.1. (Direct products) Given groups $G_1, G_2, \ldots, G_n$, know the definition of the external direct product $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$. The order $|G|$ is the product $|G_1||G_2| \ldots |G_n|$.

2. (Properties of direct products). The order of the element $(a_1, \ldots, a_n) \in G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$ is given by the lcm of the orders $|a_1|, \ldots, |a_n|$, where $|a_i|$ means the order of a_i in the group G_i. One can use this to find the number of elements of a given order in a direct product, if one can find the number of elements of a given order in each factor. G is cyclic if and only if each G_i is cyclic and the orders of the G_i are pairwise relatively prime.

3. (Decomposing special groups into direct products of cyclic groups.) If $n = p_1^{i_1} \ldots p_n^{i_n}$ is the prime factorization of n, then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus \mathbb{Z}_{p_n^{i_n}}$. Similarly, $U(n) \cong U(p_1^{i_1}) \oplus \cdots \oplus U(p_n^{i_n})$. $U(p^m)$ where p is a prime can be

decomposed into a direct product of cyclic groups via formulas: $U(2) = \{e\}$, $U(4) \cong \mathbb{Z}_2$, $U(2^m) \cong \mathbb{Z}_{2^{m-2}} \oplus \mathbb{Z}_2$ for $m \geq 3$, and $U(p^m) \cong \mathbb{Z}_{p^m - p^{m-1}}$ for $m \geq 1$ when p is odd. Then the cyclic groups appearing may decompose further into direct products of cyclic groups of prime power order. Be able to use these decompositions to decide if two U-groups (Or two $\mathbb{Z}$-groups) are isomorphic or not.

B.1. (Factor groups) If K is a normal subgroup of G, can form the factor group G/K. Understand why if K is *not* normal this construction fails to make sense. The order of G/K is $|G|/|K| = |G : K|$. The elements of G/K are left cosets aK and the product is defined by $(aK)(bK) = abK$. If G is cyclic, then G/K is cyclic; If G is abelian, then G/K is abelian; know why these facts are true. The order of aK in G/K divides the order of a in G; *understand why*. Be able to calculate the order of aK in G/K.

5 V. Relationships among groups

A. (Homomorphisms) A homomorphism $\phi : G \to \overline{G}$ is a function such that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. The properties of G and $\overline{G}$ are related in this case: see the many theorems in chapter 10; you should have a general understanding of what these theorems say, but you don't have to memorize every individual property. Here are a few of the facts: $\phi(G)$ is a subgroup of $\overline{G}$. $K = \operatorname{Ker}\phi = \{g \in G | \phi(g) = e\}$ is a normal subgroup of G. $\phi(a) = \phi(b)$ if and only if $aK = bK$. if $|K| = m$, then ϕ is an m-to-1 function in the sense that G is divided into sets of elements of size m (which are in fact the left cosets of K in G), and all elements of each set are sent to the same element of $\overline{G}$ by ϕ.

B. (Isomorphisms) If ϕ is a homomorphism which is also one-to-one and onto, then ϕ is called an isomorphism and we write $G \cong \overline{G}$. In this case G and $\overline{G}$ have *all* of the same properties and we think of them as virtually the same. To prove two groups are isomorphic you need to construct a one-to-one and onto homomorphism from one to the other. One way to check that two groups are *not* isomorphic is to show that they have different numbers of elements of order d for some d. Another way is to show that one is cyclic and the other isn't, or that one is abelian and the other isn't.

C. (First isomorphism theorem) The first isomorphism theorem says that if $\phi : G \to \overline{G}$ is a homomorphism, and $K = \operatorname{Ker}\phi$, then $G/K \cong \phi(G)$.

In particular, $|\phi(G)| = |G|/|K|$. Also, $|\phi(G)|$ divides $|\overline{G}|$ by Lagrange's theorem.

D. (Homomorphisms between Z-groups) A homomorphism $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ is uniquely determined by the value of $\phi([1]) = [x]$, by the formula $\phi([a]) = [ax]$ for all $[a]$, which follows from the definition of a homomorphism (you should understand why). There exists a homomorphism ϕ such that $\phi([1]) = [x]$ if and only if for all $a, b \in \mathbb{Z}$, $a \mod n = b \mod n$ implies $ax \mod m = bx \mod m$ (you should understand why). In fact this happens if and only if n divides mx (but you needn't memorize this.) Using these facts one can understand all homomorphisms from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. Review your exercises along these lines.

6 VI. Classification of special kinds of groups

A. (Groups of prime order) If G is a group of order p where p is a prime, then G is isomorphic to $\mathbb{Z}_p$. *Understand why.*

B. (Groups of order p^2) If G is a group of order p^2 where p is an odd prime, then G is abelian. (We didn't cover this, but it is a nice fact to know.) In this case G is isomorphic to either $\mathbb{Z}_p \oplus \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$ by part C below.

C. (Fundamental Theorem of finite abelian groups.) If G is a finite abelian group of order n, then G is isomorphic to $\mathbb{Z}_{p_1^{i_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{i_k}}$ for some prime powers $p_1^{i_1}, \ldots, p_k^{i_k}$, where the list of prime powers (which might contain repeats) is uniquely determined up to rearrangement, and $n = p_1^{i_1} p_2^{i_2} \ldots p_k^{i_k}$. For given n, you should be able to write down the list of all possible abelian groups of order n up to isomorphism. Given a particular abelian group of order n, one can decide which group on the list it is isomorphic to by examining orders of elements, as in several of your homework problems.