Format and topics
Exam 2, Math 128A

General information. Exam 2 will be a timed test of 75 minutes, covering Chapters 4–8 of the text. No books, notes, calculators, etc., are allowed. Most of the exam will rely on understanding the problem sets and the definitions and theorems that lie behind them. If you can do all of the homework, and you know and understand all of the definitions and the statements of all of the theorems we've studied, you should be in good shape.

You should not spend time memorizing proofs of theorems from the book, though understanding those proofs does help you understand the theorems. On the other hand, you should defintely spend time memorizing the *statements* of the important theorems in the text.

The exam will contain the same four types of questions as the previous one. (Remember to be as specific as possible on the true/false questions.) The exam will not be cumulative, per se, as there will not be any questions that only concern material before Ch. 4. However, it will be assumed that you still understand the previous material; for example, it will be assumed that you know what groups and subgroups are, how to read the multiplication table of a group, what $U(25)$ is, and so on.

Definitions. The most important definitions we have covered are:

Ch. 4	Euler phi function $\varphi(n)$	subgroup lattice
Ch. 5	permutation of X	permutation group of X
	$\mathrm{Sym}(X)$	S_n, symmetric group of degree n
	array notation	cycle notation, cycle form
	cycle of length m, m-cycle	disjoint cycles
	transposition	even permutation
	odd permutation	A_n, alternating group of degree n
Ch. 6	isomorphism	isomorphic
	$G \approx \overline{G}$	left regular representation
	automorphism	inner automorphism induced by a
	$\mathrm{Aut}(G)$	$\mathrm{Inn}(G)$
Ch. 7	aH, Ha, aHa^{-1}	left coset of H in G containing a
	right coset of H in G containing a	coset representative
	index of H in G	$\lvert G : H \rvert$
	$\lvert aH \rvert$, $\lvert Ha \rvert$	$\mathrm{stab}_G(i)$, stabilizer of i in G
	$\mathrm{orb}_G(i)$, orbit of i in G	
Ch. 8	external direct product	$G_1 \oplus \cdots \oplus G_n$
	$U_k(n)$	

Examples. You will also need to be familiar with the key properties of the main examples we have discussed. The most important examples we have seen are:

Ch. 4 Z_n, Z; $\langle a \rangle$ where $\lvert a \rvert = n$, $\langle a \rangle$ where $\lvert a \rvert = \infty$.

Ch. 5 D_4 as a subgroup of S_4, rotations of a tetrahedron as A_4.

Ch. 6 Isomorphism: $\varphi : \mathbf{R} \to \mathbf{R}^+$ given by $\varphi(x) = 2^x$; cyclic groups isomorphic to either Z or Z_n; conjugation by $a \in G$. Non-isomorphisms: $U(10)$ vs. $U(12)$, Q vs. Q^*. Examples of automorphisms; $\mathrm{Inn}(D_4)$.

Ch. 7 Computations of left and right cosets (pp. 140–141, PS06). Cosets of $SL(2, \mathbf{R})$ in $GL(2, \mathbf{R})$. A_4 has no subgroup of order 6. Group of a cube, soccer ball, icosahedron.

Ch. 8 Classification of groups of order 4. Counting numbers of elements of a given order. Computation of $U(n)$ as a direct product of cyclic groups.

Theorems, results, algorithms. The most important theorems, results, and algorithms we have covered are listed below. You should understand all of these results, and you should be able to state any theorem clearly and precisely. You don't have to memorize theorems by number or page

number; however, you should be able to state a theorem, given a reasonable identification of the theorem (either a name or a vague description).

Ch. 4 When is $a^i = a^j$; $|a| = |\langle a \rangle|$, $a^k = e$ if and only if $|a|$ divides k. If $|a| = n$, $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$; when is $\langle a^i \rangle = \langle a^j \rangle$, which elements generate a cyclic group (e.g., Z_n). Fundamental Theorem of Cyclic Groups; subgroups of Z_n. Number of elements of each order in a cyclic group; number of elements of order d in a finite group.

Ch. 5 Disjoint cycles commute; order of a permutation. Every permutation in S_n is a product of 2-cycles. Permutations are either even or odd but not both; even permutations are a subgroup of S_n; $|A_n| = n!/2$.

Ch. 6 Cayley's Theorem. Element-wise properties of isomorphisms (Thm. 6.2), global properties of isomorphisms (Thm. 6.3). $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups. $\mathrm{Aut}(Z_n) \approx U(n)$.

Ch. 7 Properties of cosets. Lagrange's Theorem; $|G : H| = |G| / |H|$, $|a|$ divides $|G|$, prime order groups are cyclic, $a^{|G|} = e$, Fermat's Little Theorem. Classification of groups of order $2p$; groups of order $n \leq 7$. Orbit-Stabilizer Theorem.

Ch. 8 Order of an element of a direct product. Criterion for $Z_m \oplus Z_n$ to be cyclic. $U(n)$ as an external direct product.

Not on exam. (Ch. 5) Sliding disk puzzle/Rubik's cube, D_5 check digit scheme. (Ch. 8) Applications (cryptography, genetics, electric circuits). Gauss' classification of $U(p^n)$ for p prime (bottom of p. 160).

Good luck.