**Format and topics**
**Exam 1, Math 128A**

**General information.** Exam 1 will be a timed test of 65 minutes, covering Chapters 0–4 of the text. You will be allowed to use one page of notes and the $n$-gons you have made, but no other aids (calculators, etc.). 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.

**Types of questions.** There are three types of questions that may appear on exams in this class, namely: computations; roofs; and true/false with justification.

**Computations.** These will be drawn from computations of the type you've done on the problem sets. You do not need to explain your answer on a computational problem, but show all your work.

**Proofs.** These will resemble some of the shorter problems from your homework. You may take as given anything that has been proven in class, in the homework, or in the reading. Partial credit may be given on proof questions, so keep trying if you get stuck (and you've finished everything else). If all else fails, at least try to write down the definitions of the objects involved.

**True/false with justification.** This type of question may be less familiar. You are given a statement, such as:

- If $G$ is a group, with its operation written multiplicatively, and $a, b \in G$, then $(ab)^{-1} = b^{-1}$.

If the statement is true, all you have to do is write "True". (However, see below.) If the statement is false (like the one above), not only do you have to write "False", but you must also give a reason why the statement is false. Your reason might be a very specific counterexample:

> False. For $G = \mathbf{R}^*$ (the nonzero real numbers), $a = 2$, and $b = 3$, $(ab)^{-1} = 1/6$, but $b^{-1} = 1/3$.

Your reason might also be a more general principle:

> False. In that case, we would have $ab = b$, which by cancellation means that $a = e$. So the statement fails for any $a \neq e$.

Either way, your answer should be as specific as possible to ensure full credit.

Depending on the problem, some partial credit may be given if you write "False" but provide no justification, or if you write "False" but provide insufficient or incorrect justification. Partial credit may also be given if you write "True" for a false statement, but provide some partially reasonable justification. (In other words, if you have time, it can't hurt to justify "True" answers.)

If I can't tell whether you wrote "True" or "False", you will receive no credit. In particular, please do not just write "T" or "F", as you may not receive any credit.

**Definitions.** The most important definitions we have covered are:

| | | |
|---|---|---|
| Ch. 0 | divisor, divisible | $t \mid s$, $t \nmid s$ |
| | prime | multiple |
| | quotient | remainder |
| | greatest common divisor | relatively prime |
| | least common multiple | $a \mod n$ |
| | equivalence relation, $a \sim b$ | equivalence class |

| | | |
|---|---|---|
| Ch. 0 | $[a]$ | partition |
| | domain | range |
| | image (of element or set) | composition |
| | one-to-one | onto |
| Ch. 1 | dihedral group of order 8 | Cayley table |
| | $D_n$, dihedral group of order $2n$ | reflection |
| | rotation | $C_n$, cyclic rotation group of order $n$ |
| Ch. 2 | binary operation | closure |
| | $\mathbf{Z}_n$ | group |
| | associativity | identity |
| | inverse | Abelian, non-Abelian |
| | $\mathbf{Q}^+$, $\mathbf{R}^+$ | $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ |
| | $GL(2,F)$ $(F = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p)$ | $SL(2,F)$ $(F = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p)$ |
| | $U(n)$ | $n$th roots of unity |
| | $\mathbf{R}^n$ | translations |
| Ch. 3 | order of a group $\lvert G\rvert$ | order of an element $\lvert g\rvert$ |
| | infinite order | subgroup |
| | proper subgroup | trivial/nontrivial subgroup |
| | $\langle a\rangle$ | cyclic subgroup of $G$ generated by $a$ |
| | cyclic group | generator of a cyclic group |
| | $Z(G)$, center of a group | $C(a)$, centralizer of $a \in G$ |
| Ch. 4 | Euler phi function $\varphi(n)$ | subgroup lattice |

**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. 0** Modular arithmetic: USPS, UPS, UPC, ISBN codes. Examples of equivalence relations.
**Ch. 1** Multiplying symmetries of a square; Cayley tables of $D_3$, $D_4$, $D_5$.
**Ch. 2** $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{R}^n$ (additive); $\mathbf{Q}^+$, $\mathbf{R}^+$, $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$, roots of unity (multiplicative); $Z_n$, $U(n)$. $GL(2,F)$, $SL(2,F)$. Non-groups: irrationals, $\{0,1,2,3\}$ with multiplication mod 4, $\mathbf{Z}$ under subtraction, all matrices (including non-invertible). Multiplicative vs. additive notation.
**Ch. 3** Computing orders of group elements. Examples of applying subgroup tests. Subgroup examples: $\langle a\rangle$, $Z(G)$, $C(a)$. Examples of cyclic subgroups, center of $D_n$, centralizers.
**Ch. 4** $Z_n$, $Z$; $\langle a\rangle$ where $|a| = n$, $\langle a\rangle$ where $|a| = \infty$.

**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. 0** Division algorithm (0.1), Euclidean algorithm. GCD is Linear Combination (0.2). Euclid's Lemma, Fundamental Theorem of Arithmetic (0.3). Equivalence Classes Partition (0.7).
**Ch. 2** Identity unique (2.1), Cancellation (2.2), Inverses unique (2.3). Socks-shoes (2.4).
**Ch. 3** One-step Subgroup Test (3.1), Two-Step Subgroup Test (3.2), Finite Subgroup Test (3.3). Subgroup proofs: (3.4) $\langle a\rangle$, (3.5) $Z(G)$, (3.6) $C(a)$.
**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.

**Not on exam.** (Ch. 0) Computing $\gcd(a,b)$ using Euclidean algorithm; mathematical induction. Also, while error-detecting schemes may be on the exam, you will not have to memorize how they work.

**Good luck.**