

CSCI 124 - Discrete Structures II - Fall 2009
George Washington University

Homework 3: 100 points

due 6 November 2009, by 6 pm in TA's mailbox.

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the quizzes, tests or final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

Any violations will be treated as violations of the Code of Academic Integrity.

1. Consider the set G of all invertible matrices of some fixed size $n \times n$. Let \diamond be the operation of matrix multiplication. Answer the following (you may assume properties about matrix multiplication; however, if you need a particular property, it should be stated clearly):
 - (a) (1 point) Is \diamond commutative? Explain briefly.
 - (b) (1 point) Is \diamond associative? Explain briefly.
 - (c) (15 points) G is a group with respect to the operation \diamond . Show that it satisfies all requirements of a group.
2. (15 points) Consider the group G of problem 1, with the operation \diamond of problem 1. Define a shift cipher on this group as follows. The sets of plaintexts, ciphertexts and keys are all the same, G . Encryption with a key K is $E_K(x) = K \diamond x$. Demonstrate how encryption may be inverted for this group, pointing out each instance when the requirements of a group are used. In particular, demonstrate that the four requirements of a group are all necessary for the cryptosystem to work. DO NOT use examples, state everything for the given group and operation. DO NOT use a specific value of n , show it for general n .
3. Consider some set G with some operation \diamond . (G and \diamond are not necessarily related to any set or operation mentioned earlier in this HW or elsewhere.). Suppose G is a group with respect to \diamond , with identity e . Let \bar{z} denote the inverse of z with respect to \diamond . Answer the following:
 - (a) Let a be a fixed element in G . Define another operation \square as follows:

$$\forall x, y \in G, x \square y = x \diamond y \diamond a$$

(You may recall that you saw a special case of this problem in HW 1, (no. 6)).

- i. (4 points) Is G closed with respect to \square ?
- ii. (4 points) Is \square associative?
- iii. (2 points) Is \square associative if \diamond is commutative? (DO NOT assume \diamond is commutative for any other part of this problem).

- iv. (4 points) Does \square have an identity in G ? If so, what is it?
- v. (4 points) Consider x , some element in G . Does the inverse of x with respect to \square exist in G ? If so, what is it?

(b) (12 points) Define another operation \blacklozenge on G as follows:

$$\forall x, y \in G, x \blacklozenge y = \overline{x \diamond y}$$

Show that G is not a group with respect to \blacklozenge . (Hint: First identify which property it would not satisfy. Recall a problem in Test 1 for specific instances of \diamond and \blacklozenge).

4. (25 points) Let f be a homomorphism from group G_1 with operation \diamond to group G_2 with operation \circ . Consider the subset of group G_1 : $H_1 = \{x | f(x) = e\}$. Show that H_1 is a subgroup of G_1 .
5. Provide clear reasoning for the following. There will be no credit without reasoning.
 - (a) Let f be a homomorphism from the group of integers \mathbb{Z} with operation integer addition, to itself. Suppose $f(1) = 2$. What are the values of:
 - i. (1 point) $f(2)$
 - ii. (1 point) $f(n)$
 - (b) Let f be a homomorphism from \mathbb{Z}_{11}^* with operation multiplication *modulo* 11, to itself. (Recall that \mathbb{Z}_p^* is the set of integers smaller than p that are relatively prime to p). Suppose $f(2) = 2$. What are the values of:
 - i. (1 point) $f(4)$?
 - ii. (2 points) $f(5)$?
 - (c) Let f be a homomorphism from $\mathbb{Z} \times \mathbb{Z}$ with operation component-wise addition, to itself. (Recall that you showed, in Quiz 3, that this is a group). Suppose $f((2, 1)) = (1, 1)$ and $f((1, 0)) = (0, 1)$. What are the values of:
 - i. (2 points) $f((1, 1))$
 - ii. (2 points) $f((3, 5))$
 - iii. (4 points) $f((n, m))$