Midterm 2 Solutions

MAT 312 - Lecture 1

April 17, 2014

Name: (please print)	**ID #**:

No notes or books. Calculators are allowed.

You must show your reasoning, not just the answer. Answers without justification will get only partial credit. If the problem ask you to solve some equation, you must find all solutions; if there are no solutions, you must explain why not.

Please cross out anything that is not part of your solution — e.g., some preliminary computations that you didn't need.

Each problem is worth 10 pts.

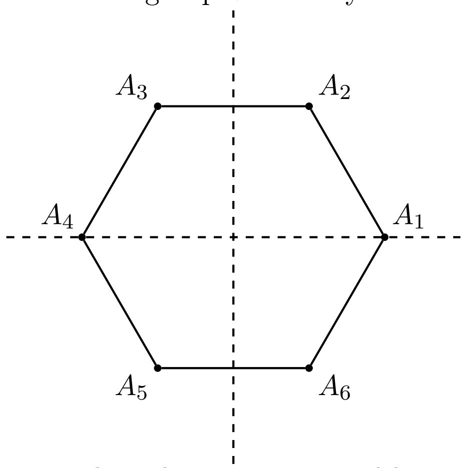
	1	2	3	4	5	**Total**
Grade						

1. Let π, $\sigma \in S(5)$ be given by

$$\pi = (12)(345)$$
$$\sigma = (13)(24)$$

(a) Compute $\pi\sigma$, $\sigma\pi$ (writing each of them in cycle notation).
(b) For each of the permutations π, σ, $\pi\sigma$, $\sigma\pi$, find the order and sign.
Solution: straightforward and left to the students.

2. Consider the group G of all symmetries (reflections and rotations) of a regular hexagon:



Let H be subgroup generated by two reflections around the dashed lines in the figure.

(a) Find orders of G, H

(b) Is H cyclic? if not, is it isomorphic to a Cartesian product of cyclic groups? Construct an isomorphism explicitly.

(c) How many H-cosets are there in G? Write one element from each coset. [Hint: each element of H sends the vertical dashed line to itself.]

Solution:

(a) The group G has 6 rotations (by multiples of 60 degrees) and 6 reflections (lines through vertices and middles of the sides). Thus, $|G| = 12$.
For H, if we denote the two reflections by r_x, r_y, then $r_x^2 = r_y^2 = e$, $r_x r_y = r_y r_x$, so

$$H = \{e, r_x, r_y, r_x r_y\}, \qquad |H| = 4$$

(b) H is not cyclic (it has order 4, but all elements have order 1 or 2). It is isomorphic to $C_2 \times C_2$, where $C_2 =< a >, a^2 = e$ is the cyclic group of order 2, written multiplicatively. The isomorphism is given by

$$\begin{aligned} \theta\colon H &\to C_2 \times C_2 \\ e &\mapsto (e, e) \\ r_x &\mapsto (a, e) \\ r_y &\mapsto (e, a) \\ r_x r_y &\mapsto (a, a) \end{aligned}$$

(c) There are $|G|/|H| = 12/4 = 3$ cosets. Since H sends the vertical dashed line to itself, all elements in a coset xH send the vertical dashed line to the same line. The following elements can be chosen as representatives of the three cosets:

$$\begin{gathered} e \\ \rho \\ \rho^2 \end{gathered}$$

where ρ is rotation by 60 degrees. All elements in the coset ρH send the vertical dashed line to the line through midpoint of A_3A_4. All elements in the coset $\rho^2 H$ send the vertical dashed line to the line through midpoint of A_4A_5.

Comment. The last part was intentionally made difficult. If you can not do it, it is OK. However, the first two parts are standard material.

3. Consider the group $\mathbb{Z}_9^*$ of invertible congruence classes mod 9 (with respect to multiplication)

(a) Show that $\mathbb{Z}_9^*$ is cyclic of order 6, by constructing an explicit isomorphism $\theta\colon \mathbb{Z}_6 \to \mathbb{Z}_9^*$. ($\theta$ will have to take sums to products).

(b) Is such an isomorphism θ unique?

Solution:

(a) $\mathbb{Z}_9^*$ consists of remainders relatively prime to 9, i.e. $\mathbb{Z}_9^* = \{[1],[2],[4],[5],[7],[8]\}$, and $|\mathbb{Z}_9^*| = 6$.

To show that it is cyclic, we need to find an element of order 6. After trying different elements, we see that [2] and [5] have order 6:

$$[2]^1 = [2],\ [2]^2 = [4],\ [2]^3 = [8],\ [2]^4 = [7],\ [2]^5 = [5],\ [2]^6 = [1],$$
$$[5]^1 = [5],\ [5]^2 = [7],\ [3]^3 = [8],\ [5]^4 = [4],\ [5]^5 = [2],\ [5]^6 = [1]$$

Thus,

$$\theta\colon \mathbb{Z}_6 \to \mathbb{Z}_9^*\colon a \mapsto [2]^a$$

is an isomorphism.

(b) No, it is not unique. Another isomorphism is given by

$$\theta\colon \mathbb{Z}_6 \to \mathbb{Z}_9^*\colon a \mapsto [5]^a$$

4. (a) Prove that in any finite group, the number of elements of order 3 is even.
(b) Prove that any group of order 12 must contain an element of even order.

Solution:

(a) If g is an element of order 3, then g^{-1} is also of order 3, and $g \neq g^{-1}$. Thus, elements of order 3 come in pairs.

(b) By Lagrange theorem, a group of order 12 can have elements of orders 1, 2, 3, 4, 6, 12. There is exactly one element of order 1 (identity); by part (a), there is even number of elements of order 3. Since the total number of elements is 12, there must be an element of order other than 1 or 3. But all other possible orders are even.

5. Consider the linear code

$$f\colon B^2 \to B^5$$
$$x \mapsto xG$$

with the generator matrix

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(a) Write explicitly all codewords for this code and find the minimal distance between codewords.

(b) Will this code be able to detect a single-bit error? two-bit error?

(c) Will this code be able to correct a single-bit error? two-bit error?

(d) After encoding some 2-bit word and transmission (with errors), the recipient got the word (10110). Can you decode it, i.e. find the original two-bit word?

Solution:

(a) The possible codewords are

$$(00)G = (00000)$$
$$(01)G = (01011)$$
$$(10)G = (10101)$$
$$(11)G = (11110)$$

The minimal distance is 3.

(b) To detect k errors, you need to have minimal distance at least $k + 1$. Thus, the code will detect 1- and 2-bit errors

(c) To correct k errors, you need to have minimal distance at least $2k + 1$. Thus, the code will correct 1-bit errors but not 2-bit errors.

(d) The closest codeword to (10110) is $(11)G = (11110)$ (distance 1). Thus, assuming that there was only one error during transmission, the original word was (11).