Practice Midterm 2

MAT 312

April 8, 2024

List of topics

1. Permutations. Composition of permutations, cycle decomposition. Order of a permutaiton.
2. Sign of a permutation. Even and odd permutations.
3. Groups, subgroups, group isomorphism. Examples of groups, including S_n and the dihedral group (symmetries of an n-gon).
4. Order of an element. Subgroups generated by a single element. Cyclic groups.
5. Cosets. Lagrange Theorem and its corollaries (order of an element divides the order of the group). Using Lagrange theorem to prove Little Fermat's theorem and Euler's theorem.
6. Normal subgroups and quotient groups.
7. Examples of groups of small order. Klein 4-group, cartesian product of groups.
8. Binary codes. Distance between codewords and number of errors the code can detect/correct. Linear codes and generating matrix. Hammings (7,4) code.

Practice problems

Note that the actual exam will be shorter than this collection of problems.

1. Let $s \in S_{12}$ be the permutation

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 6 & 4 & 11 & 1 & 9 & 2 & 10 & 7 & 12 & 8 & 3 & 5 \end{pmatrix}$$

(a) Write s as a product of disjoint cycles.
(b) Find the sign of s.
(c) Find the order of s.
(d) Write s^3 as product of disjoint cycles.

2. Let G be a group and H a subgroup. For an element $g \in G$, let $gHg^{-1} = \{ghg^{-1}, h \in H\}$. Show that gHg^{-1} is also a subgroup in G.

3. (a) Let g be an element of a group G, and let n be the order of g. Show that the order of g^k is equal to n/d, where $d = \gcd(n, k)$.
(b) Show that in the group $\mathbb{Z}_n$ (with respect to addition), there are $\varphi(n)$ elements of order exactly equal to n.

4. Let $ABCD$ be a square in the plane, with center at the origin. Let G be the group of all symmetries of this square (i.e., rigid motions of the plane that send the square to itself), and let $H \subset G$ consist of those elements that send the diagonal AC to itself.
(a) Find the order of G.
(b) Show that H is a subgroup of G and find the order of H. Is H a cyclic group? a cartesian product of two cyclic groups?
(c) Is H a normal subgroup in G? if so, what is the quotient group G/H (i.e., is it commutative, is it cyclic, a product of cyclic groups, ...)

5. Let the coding function $f\colon \mathbf{B}^3 \to \mathbf{B}^6$ be given by the following generator matrix:

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

(a) What is the maximum number of errors this code can detect? how many errors it can correct?
(b) The messages received, possibly with errors, are (i) 110111 and (ii) 011100. What codewords should these messages be decoded to?