Introduction to Abstract Algebra
Exam 1 Key

Instructions

1. Do NOT write your answers on these sheets. Nothing written on the test papers will be graded.
2. Do NOT write your name on any of your answer sheets.
3. Please begin each section of questions on a new sheet of paper.
4. Do not write problems side by side.
5. Do not staple test papers.
6. Limited credit will be given for incomplete or incorrect justification.

Questions

1. Quick Facts (4 each)
   (a) Prove $(\mathbb{R}, \times)$ is not a group.
   To be a group each element must have an inverse. However $0a \neq 1$ for any $a \in \mathbb{R}$.
   (b) Explain why there is no dihedral group of order 7. Be brief.
   The dihedral groups all have even order (n reflections and n rotations including the 0 rotation). 7 is odd.
   (c) Prove $\mathbb{Z}_6^*$ (the integers mod 6 without 0) with multiplication is not a group.
   Below is the multiplication table for $\mathbb{Z}_6^*$.

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

   Note multiple elements (e.g., 2,3,4) have products outside the set (0). Thus the operation is not closed on this set. Also multiple elements have no inverse (e.g., 2,3,4).

2. Stars (4 each)

The following are based on permutations of the five points of a regular pentagon. They are *not* symmetries.

$a = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix}$

(a) Calculate a^2.

$$\begin{aligned} a^2 &= (02413)(02413) \\ &= (04321). \end{aligned}$$

(b) Find a^{-1}.

$$a^{-1} = (03142)$$

(c) Calculate $(a^2)^{-1}$.

$$\begin{aligned} (a^2)^{-1} &= (a^{-1})^2 \\ &= (03142)(03142) \\ &= (01234) \end{aligned}$$

(d) Calculate a^3, a^4, a^5.

$$\begin{aligned} a^3 &= aa^2 \\ &= (02413)(04321) \\ &= (01234). \\ a^4 &= a^2a^2 \\ &= (04321)(04321) \\ &= (03142). \\ a^5 &= aa^4 \\ &= (02413)(03142) \\ &= e. \end{aligned}$$

(e) Prove that these form a subgroup of S_5.

These are a subset of S_5 so we use the subgroup theorem. They are closed as shown above (note $a^5 = e$ so all powers wrap around). Their inverses are all present as shown above.

3. Proofs

   For each proof below write the reason each statement is true.

   (a) Inverses when they exist are unique. See Figure 1.

   (b) $(a^m)^{-1} = (a^{-1})^m$ See Figure 2.

Suppose a_1^{-1} and a_2^{-1} are inverses of a.	
$a_1^{-1} = a_1^{-1} \circ e$	1. Definition of identity
$= a_1^{-1} \circ (a \circ a_2^{-1})$	2. Definition of inverse
$= (a_1^{-1} \circ a) \circ a_2^{-1}$	3. Associative
$= e \circ a_2^{-1}$	4. Definition of inverse
$= a_2^{-1}$	5. Definition of identity.

Figure 1: Inverses when they exist are unique.

This is a proof by induction on the power m.	
Basis step:	
$(a)^{-1} = a^{-1}$.	1. Given (def of notation).
Induction step:	
$a^{m+1} \circ (a^{-1})^{m+1} =$	
$a \circ a^m \circ (a^{-1})^m \circ a^{-1} =$	2. Definition of powers
$a \circ e \circ a^{-1} =$	3. Induction step
$a \circ a^{-1} =$	4. Definition of identity
e	5. Definition of inverse
Thus $(a^{m+1})^{-1} = (a^{-1})^{m+1}$ when $(a^m)^{-1} = (a^{-1})^m$.	
Thus the theorem is true.	6. by the principle of mathematical induction

Figure 2: Inverses in Finite Groups