UNIVERSITY OF SOUTH CAROLINA

MATH-546 Algebraic Structures I Homework X

Problems

Problem 1:

Let G be a group with $|G| = 6$ ($|G|$ denotes the number of elements of G). Assume that $a, b \in G$ are elements that are not equal to the identity and satisfy $a^3 = e, b^2 = e$.

(a) Prove that e, a, a^2, b, ab, a^2b are all distinct.

(b) The result from part (a) guarantees that $G = \{e, a, a^2, b, ab, a^2b\}$. Assume that $ba \neq ab$. Which of the 6 elements of G is equal to ba? Justify.

(c) Fill in the multiplication table of G. Justify.

Answer 1:

(a)

(1)	$a \neq e$	given
(2)	$a^2 \neq e$	$a^2 = e \Rightarrow a^3 = a = e$ contradicts (1)
(3)	$a^2 \neq a$	$a^2 = a \Rightarrow a = e$ contradicts (1)
(4)	$b \neq e$	given
(5)	$b \neq a$	$b = a \Rightarrow e = b^2 = a^2$ contradicts (2)
(6)	$b \neq a^2$	$b = a^2 \Rightarrow e = b^2 = a^4 = a$ contradicts (1)
(7)	$ab \neq e$	$ab = e \Rightarrow b = a^3b = a^2$ contradicts (6)
(8)	$ab \neq a$	$ab = a \Rightarrow b = e$ contradicts (4)
(9)	$ab \neq a^2$	$ab = a^2 \Rightarrow b = a$ contradicts (5)
(10)	$ab \neq b$	$ab = b \Rightarrow a = e$ contradicts (1)
(11)	$a^2b \neq e$	$a^2b = e \Rightarrow b = a$ contradicts (5)
(12)	$a^2b \neq a$	$a^2b = a \Rightarrow ab = e$ contradicts (7)
(13)	$a^2b \neq a^2$	$a^2b = a^2 \Rightarrow b = e$ contradicts (4)

(14) $a^2b \neq b$ $\quad$ $a^2b = b \Rightarrow a^2 = e$ contradicts (2)

(15) $a^2b \neq ab$ $\quad$ $a^2b = ab \Rightarrow a = e$ contradicts (1)

(b) $ba = a^2b$ by elimination:

$ba \neq e$ $\quad$ $ba = e \Rightarrow a = b$

$ba \neq a$ $\quad$ $ba = a \Rightarrow b = e$

$ba \neq a^2$ $\quad$ $ba = a^2 \Rightarrow a = b$

$ba \neq b$ $\quad$ $ba = b \Rightarrow a = e$

$ba \neq ab$ $\quad$ given

(c) Cayley table:

	e	a	a^2	b	ab	a^2b
e	e	a	a^2	b	ab	a^2b
a	a	a^2	e	ab	a^2b	b
a^2	a^2	e	a	a^2b	b	ab
b	b	a^2b	ab	e	a^2	a
ab	ab	b	a^2b	a	e	a^2
a^2b	a^2b	ab	b	a^2	a	e

Problem 2:

Let G be a group and $a, b \in G$ be arbitrary elements.

(a) Prove that $o(a) = o(a^{-1})$, where $o(a)$ denotes the order of the element a.

(b) Prove that $o(ab) = o(ba)$ (note: we are not assuming that a and b commute).

(c) Prove that $o(aba^{-1}) = o(b)$.

Answer 2:

(a) Let $p = o(a)$ then

$$\begin{aligned} e &= a^p (a^{-1})^p \\ &= e(a^{-1})^p \\ &= (a^{-1})^p \\ o(a) &\le o(a^{-1}) \end{aligned}$$

Interchange a and a^{-1} to get $o(a^{-1}) \le o(a)$ and $o(a^{-1}) = o(a)$

(b) Let $p = o(ab)$ and $q = o(ba)$ with $p >= q$.

$$\begin{aligned} e &= (ab)^p \\ bea &= b(ab)^p a \\ ba &= (ba)^p (ba) \\ e &= (ba)^p \\ o(ba) &\le o(ab) \end{aligned}$$

Interchange a and b to get $o(ab) \le o(ba)$ and so $o(ba) = o(ab)$

(c) Let $o(b) = p$ then

$$\begin{aligned} (aba^{-1})^p &= aba^{-1}aba^{-1} \cdots aba^{-1} \\ &= ab^p a^{-1} \\ &= aea^{-1} \\ &= e \\ o(aba^{-1}) &\le o(b) \end{aligned}$$

Reverse to get $o(b) \le o(aba^{-1})$ and so $o(b) = o(aba^{-1})$

Problem 3:

Let $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$. Prove that $o(A) = \infty$ by finding a formula for A^n. Use induction to prove that your formula holds for all n.

Answer 3:

Consider the Fibbonacci series defined:

$$F_0 = 0$$
$$F_1 = 1$$
$$F_k = F_{k-1} + F_{k-2}$$

We assert that $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ and therefore $o(A) = \infty$ since the Fibbonacci series is monotonically increasing.

$$A^1 = \begin{bmatrix} F_2 & F_1 \\ F_1 & F_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

If

$$A^{k-1} = \begin{bmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{bmatrix}$$

then

$$\begin{aligned} A^k &= \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{bmatrix} \\ &= \begin{bmatrix} F_k + F_{k-1} & F_{k-1} + F_{k-2} \\ F_k & F_{k-1} \end{bmatrix} \\ &= \begin{bmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{bmatrix} \end{aligned}$$

Problem 4:

Find the orders of all the elements in each of the following groups:
(a) $\mathbb{Z}_5$ (b) $\mathbb{Z}_6$ (c) $\mathbb{Z}_{12}^*$ (d) $\mathbb{R}^*$ (e) $\mathbb{Z}$

Answer 4:

Showing only $o(x)$ for $x \neq e$ and omitting brackets and subscripts:

(a) $\mathbb{Z}_5$:
$o(x) = 5$

(b) $\mathbb{Z}_6$:
$o(1) = o(5) = 6$
$o(2) = o(4) = 3$
$o(3) = 2$

(c) $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$:
$o(5) =$o$(7) = o(11) = 2$

(d) $\mathbb{R}^*$:
$o(-1) = 2$
$o(x) = \infty$

(e) $\mathbb{Z}$:
$o(x) = \infty$

Theoretical Problems

Problem 5:

Prove that there is only one possible multiplication table for groups with 3 elements up to labeling the elements.

Answer 5:

Problem 6:

Prove that there are only two possible multiplication tables for groups with 4 elements up to labeling the elements.

Answer 6:

Problem 7:

Let G be a group and $a \in G$ an element. Assume that $o(a) = n$. Let k be an arbitrary integer. Prove that $a^k = e \iff n \mid k$.

Answer 7:

Problem 8:

Let G be a group and $a \in G$ an element. Assume that $o(a) = n$. Let k_1, k_2 be integers. Prove that $a^{k_1} = a^{k_2}$ if and only if $n \mid (k_1 - k_2)$.

Answer 8: