Math 103A Homework 3

James Holden

January 25, 2019, Winter 2019

Question 1. *Find all subgroups of* $(Z_8, +_8)$.

Proof. $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Let G be a group. Let H be a subgroup of G. Lagrange theorem states that the order of subgroups of G divide the order of G. The subgroups of G are as follows:

$H_1 = \{\{0, 1, 2, 3, 4, 5, 6, 7\}, +_8\}$
$H_2 = \{\{0, 2, 4, 6, \}, +_8\}$
$H_4 = \{\{0, 4\}, +_8\}$
$H_\emptyset = \{\{\emptyset\}, +_8\}$

□

Question 2. *Let G be a group and let $g \in G$; assume that $ord(g) = n$. Show that $g^{-1} = g^{n-1}$.*

Proof. Let $g \in G$. We know since $ord(g) = n$, G has a finite number of elements. This means that there exists $n \in \mathbb{Z}^+$ such that $g^n = e$.

$$\begin{aligned} g^n &= e \\ g^{n-1+1} &= e \\ g^{n-1}g^1 &= e \\ g^{n-1} &= eg^{-1} \\ g^{n-1} &= g^{-1} \end{aligned}$$

The statement is proven. □

Question 3. *(a) Find the order of all the elements in* $(\mathbb{Z}_7, +_7)$.

Proof. $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$

W know for $a \in G$, $ord_G(a) = min\{n : a^n = e\}$. That is to say, the order of each element is the minimum number of times to apply the group operation to that element to get back to e.

For $a = 1$, $ord_G(a) \geq 1$

For $a = 2$, $ord_G(a) = 7$

For $a = 3$, $ord_G(a) = 7$

For $a = 4$, $ord_G(a) = 7$

For $a = 5$, $ord_G(a) = 7$

For $a = 6$, $ord_G(a) = 7$

This arises because 7 is prime.

□

(b) Let p be a prime number. Find the order of all the elements in $(\mathbb{Z}_p, +_p)$. (Hint: recall from Math 109 that if $g.c.d.(a, n) = 1$, then we have the following: $a|mn$ for some $m \in Z$ if and only if $a|m$.)

Proof. Since there is no integer in $2 \dots p$ which is coprime with p, the order of all the elements in $\mathbb{Z}_p$ is p. □

Question 4. *Let p be a prime number. Find all the subgroups of $(\mathbb{Z}_p, +_p)$. (Hint: use problem 3(b) above.)*

Proof. Using Lagrange's Theorem, the only subgroups of a prime-sized cyclic group are $\{\emptyset\}$ and $\{0, 1, , \dots, p\}$, the group itself. □

Question 5. *Exercise 4 page 45: 30, 32, 35, 36.*

(a) Question 30: *Let $\mathbb{R}^*$ be the set of all real numbers except* 0*. Define $*$ on $\mathbb{R}^*$ by letting $a * b = \mid a \mid b$.*

(a) Show that $*$ gives an associative binary operation on $\mathbb{R}^*$

Proof. Let $a, b, c \in \mathbb{R}^*$. Associative property states:
$(a * b) * c = a * (b * c)$

$$\begin{aligned} LHS &= (\mid a \mid * b) * c \\ &= (\mid\mid a \mid b \mid) c \\ &= (\mid ab \mid) c \end{aligned}$$

$$\begin{aligned} RHS &= a * (\mid b \mid * c) \\ &= \mid a \mid\mid b \mid c \\ &= (\mid ab \mid) c \end{aligned}$$

We note that $\mid ab \mid = \mid a \mid\mid b \mid$ which is easily verifiable by testing cases. Since the right hand side(RHS) of the associative rquation equals the left hand side(LHS) of the associative equation, the operator $*$ gives an associative binary property. □

*(b) Show there is a left identity for * and a right inverse for each element in $\mathbb{R}^*$*

Proof. Let $b \in \mathbb{R}^*$.
Left Identity: $e * b = \mid e \mid b = eb = b$
Right Inverse: $b * b^{-1} = \mid b \mid b^{-1} = bb^{-1} = e$ □

(c) Is $\mathbb{R}^*$ with this binary operation a group?

Proof. We have shown that $(\mathbb{R}^*, *)$ is associative and an identity and inverse element exists within the group for every member of the group. We also know it is closed under group operation. Therefore it is a group. □

(d) Explain the significance of this exercise.

Proof. To check if a binary operation paired with a set is a group you simply carry out the above steps/checks. □

(b) Question 32: *Show that every group G with identity e and such that $x * x = e$ for all $x \in G$ is abelian.*

Proof. Let $a, b \in G$. Since, G is a group, we know $(a * b), (b * a) \in G$.
Let $x = (a * b)$. Then $e = x * x = (a * b) * (a * b)$.

$$
\begin{aligned}
e &= (a * b) * (a * b) \\
e * (b * a) &= (a * b) * (a * b) * (b * a) \\
(b * a) &= a * b * a * (b * b) * a \text{ [by associativity]} \\
(b * a) &= a * b * a * e * a \\
(b * a) &= a * b * (a * a) \\
(b * a) &= a * b * e \\
b * a &= a * b
\end{aligned}
$$

which is the definition of an abelian group. □

(c) Question 35: *Show that if $(a * b)^2 = a^2 * b^2$ for $a, b \in G$, then $a * b = b * a$.*

Proof. We seek to prove that if $(ab)^2 = a^2b^2$, G is abelian.

$$
\begin{aligned}
(ab)^2 &= a^2b^2 \\
(ab)(ab) &= a^2b^2 \\
abab &= a^2b^2 \\
a^{-1}(abab)b^{-1} &= a^{-1}a^2b^2b^{-1} \\
ebae &= eabe \\
ba &= ab
\end{aligned}
$$

Thus, G is abelian.

□

(d) Question 36: *Let G be a group and let $a, b \in G$. Show that (a * b)' = a' * b' $\iff$ $a * b = b * a$. ' is left inverse.*

Proof. Again we want to show G is abelian.

$$
\begin{aligned}
ab &= ((ab)^{-1})^{-1} \\
&= (a^{-1}b^{-1})^{-1} \\
&= (b^{-1})^{-1}(a^{-1})^{-1} \\
&= ba
\end{aligned}
$$

Thus, G is abelian.

□