

Tutorial Sheet-ODD Semester 2022

15B11CI212 Theoretical Foundation of Computer Science

Tutorial 7 Solutions

Q1. Define an operation $*$ on R as $x * y = x + y + xy$. Prove or disprove: $(R, *)$ is a group

Solution:

- a. [Closure] Obvious.
 - b. [Associativity] We have $(x*y)*z = (x+y+xy)*z = (x+y+xy)+z+(x+y+xy)z = x+y+z+xy+xz+yz+xyz$
 $x*(y*z) = x*(y+z+yz) = x+(y+z+yz)+x(y+z+yz) = x+y+z+xy+xz+yz+xyz$, i.e., $(x * y) * z = x * (y * z)$.
 - c. [Identity] It is easy to check that 0 is the identity with respect to $*$.
 - d. [Inverse] Let $x \in R$ have the inverse $y \in R$, i.e., $x * y = x + y + xy = 0$, i.e., $y = -x / (1+x)$, i.e., y exists if and only if $x \neq -1$. Since -1 does not have an inverse under $*$, $(R, *)$ is not a group.
- Q2. Prove or disprove that the set $G = \{1, 3, 7, 9\}$ is a group under multiplication modulo 10.

Solution: The composition table of G with respect to \odot_{10} is as follows:

\odot_{10}	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

From the composition table, we have

- a. $a \odot b \in G \forall a, b \in G$
- b. $(a \odot b) \odot c = a \odot (b \odot c) \forall a, b \in G$
- c. $a \odot 1 = a \forall a \in G$
- d. The inverse elements of 1, 3, 7, 9 are 1, 7, 3, 9 respectively.

Q3. If G is a group such that $(ab)^2 = a^2b^2$ for all $a, b \in G$, then show that G must be abelian.

Solution: $abab = a^2b^2$ apply a^{-1} from left and b^{-1} from right. We obtain $ba = ab$ for all $a, b \in G$. Hence G is abelian.

Q4. Let $(A, +, \cdot)$ be a ring such that $a \cdot a = a$ for all a in A .

- a. Show that $a + a = 0$ for all a , where 0 is the additive identity.
- b. Show that the operation \cdot is commutative.

Solution:

$(A, +, \cdot)$ is a ring

a) Let 0 be the additive identity.
 Then $a \cdot 0 = 0 \cdot a = 0$ for all a in A
 $(a + a) \cdot a = a \cdot a + a \cdot a = a + a = a \cdot (a + a)$
 Hence $a + a = 0$

b) $(a + b) \cdot (a + b) = a + b$
 $a \cdot a + b \cdot a + a \cdot b + b \cdot b = a + b$
 $a + b \cdot a + a \cdot b + b = a + b$
 Hence $b \cdot a + a \cdot b = 0$
 But $a \cdot b + a \cdot b = 0$
 Hence $a \cdot b$ and $b \cdot a$ are additive inverse of $a \cdot b$.
 Since the additive inverse is unique $b \cdot a = a \cdot b$.
 Hence \cdot is commutative.

Q.5 Let $(Z, *)$ be an algebraic structure, where Z is the set of integers and the operation $*$ is defined by $n * m = \text{maximum of } (n, m)$. Show that $(Z, *)$ is a semi group. Is $(Z, *)$ a monoid ?. Justify your answer

Solution: Let a, b and c are any three integers. Closure property: Now, $a * b = \text{maximum of } (a, b) \in Z$ for all $a, b \in Z$ Associativity : $(a * b) * c = \text{maximum of } \{a, b, c\} = a * (b * c) \therefore (Z, *)$ is a semi group.
 Identity : There is no integer x such that $a * x = \text{maximum of } (a, x) = a$ for all $a \in Z \therefore$ Identity element does not exist. Hence, $(Z, *)$ is not a monoid.

Q.6 Show that the set of all strings S is a monoid under the operation concatenation of strings. Is S a group w.r.t the above operation? Justify your answer.

Solution: Let us denote the operation concatenation of strings by $+$. Let s_1, s_2, s_3 are three arbitrary strings in S . Closure property: Concatenation of two strings is again a string. i.e., $s_1 + s_2 \in S$
 Associativity: Concatenation of strings is associative. $(s_1 + s_2) + s_3 = s_1 + (s_2 + s_3)$ Identity: We have null string, $I \in S$ such that $s_1 + I = S$. $\therefore S$ is a monoid. Note: S is not a group, because the inverse of a non empty string does not exist under concatenation of strings.

Q.7 If $(G, *)$ is a group and $a \in G$ such that $a * a = a$, then show that $a = e$, where e is identity element in G .

Proof: Given that, $a * a = a$ $a * a = a * e$ (Since, e is identity in G) $a = e$ (By left cancellation law)
 Hence, the result follows. Ex. If every element of a group is its own inverse, then show that the group must be abelian . Proof: Let $(G, *)$ be a group. Let a and b are any two elements of G . Consider the identity, $(a * b)^{-1} = b^{-1} * a^{-1}$ $(a * b) = b * a$ (Since each element of G is its own inverse) Hence, G is abelian. Note: $a^2 = a * a$ $a^3 = a * a * a$ etc.