Abstract Algebra Assignment (5): Rings

Mostafa Hassanein

31 December 2023

1.

To show that the system $(I_m, +, \cdot)$ is an ideal in the ring $(I, +, \cdot)$, we must show that:
i. $(I_m, +)$ is a sub-group of $(I, +)$.

Proof.
$a, b \in I_m \implies a = mr_1 \ \wedge \ b = mr_2$
$\implies b^{-1} = -mr_2$
$\implies a + b^{-1} = mr_1 + (-mr_2) = m(r_1 - r_2) = mr'$
$\implies a + b^{-1} \in I_m$
$\implies (I_m, +)$ is a sub-group of $(I, +)$.

$\square$

ii. I_m is a left ideal: $r \cdot x \in I_m, \ \forall x \in I_m \ \wedge \ \forall r \in I$.

Proof.
Let $x \in I_m \implies \ x = mr_1, \ m, r_1 \in I$.
Let $r_2 \in I \implies r_2 \cdot x = r_2 \cdot mr_1 = m(r_1 + r_2) = mr'$
$\implies r_2 \cdot x \in I_m, \ \forall x \in I_m \ \wedge \ \forall r_2 \in I$
$\implies (I_m, +, \cdot)$ is a left ideal.

$\square$

iii. I_m is a right ideal: $x \cdot r \in I_m, \ \forall x \in I_m \ \wedge \ \forall r \in I$.

Proof.
Because I is commutative w.r.t. the second operation, and I_m is a left ideal, then I_m is also a right ideal.

$\square$

2.

To prove that the system $(R, \oplus, \otimes)$ is a field, we need to show that:
i. $(R, \oplus)$ is a commutative group.

Proof.
a. Closure: $a \oplus b = a + b - 1$
$\implies a \oplus b \in R$.

b. Associativity: $(a \oplus b) \oplus c = (a + b - 1) \oplus c = (a + b - 1) + c - 1 = a + (b + c - 1) - 1 = a \oplus (b + c - 1) = a \oplus (b \oplus c)$.

c. Existence of an identity: $a \oplus e = a \implies a + e - 1 = a$
$\implies e = 1$
$\implies e \in R$.

d. Existence of inverses: $a \oplus a^{-1} = e \implies a + a^{-1} - 1 = 1$

$\implies a^{-1} = 2 - a$
$\implies a^{-1} \in R.$

e. $\oplus$ is commutative: $\oplus$ is defined in terms of addition and addition is commutative $\implies$ $\oplus$ is commutative.

(a), (b), (c), (d), (e) $\implies$ $(R, \oplus)$ is a commutative group.

$\square$

ii. $(R^*, \otimes)$ is a commutative group.

Proof.
Let $\bar{e}$ be the identity for $\otimes$, then: $a \otimes \bar{e} = a$
$\implies a + \bar{e} - a\bar{e} = a$
$\implies \bar{e} - a\bar{e} = 0$
$\implies \bar{e}(1 - a) = 0$
$\implies \bar{e} = 0.$

Let $b \in R^*$, then: $b \otimes b^{-1} = \bar{e}$
$\implies b + b^{-1} - bb^{-1} = 0$
$\implies b^{-1}(1 - b) + b = 0$
$\implies b^{-1} = b/(b - 1)$
$\implies b^{-1}$ exists for all $b \in \{R - 1\} \ \wedge \ b^{-1} \neq e = 1$
$\implies b^{-1} \in R^*.$

Let $a, b \in R^*$, then: $a \otimes b^{-1} = ab/b - 1$
$\implies a \otimes b^{-1}$ exists for all $b \in \{R - 1\} \ \wedge \ a \otimes b^{-1} \neq e = 1$
$\implies a \otimes b^{-1} \in R^*$
$\implies (R^*, \otimes)$ is a group.

Finally, $\otimes$ is defined in terms of addition and multiplication which are both commutative $\implies$ $(R^*, \otimes)$ is a commutative group.

$\square$

iii. The binary operation $\otimes$ is both left and right distributive over $\oplus$.

Proof.

a. Left distributivity:

$$
\begin{aligned}
a \otimes (b \oplus c) &= a + (b \oplus c) - a(b \oplus c) \\
&= a + (b \oplus c) - a(b \oplus c) \\
&= a + (b + c - 1) - a(b + c - 1) \\
&= a + (b + c - 1) - ab + ac - a \\
&= 2a + b + c - ab - ac - 1 \\
&= (a + b - ab) + (a + c - ac) - 1 \\
&= (a \otimes b) + (a \otimes c) - 1 \\
&= (a \otimes b) \oplus (a \otimes c).
\end{aligned}
$$

b. Right distributivity:

$$
\begin{aligned}
(a \oplus b) \otimes c &= (a \oplus b) + c - (a \oplus b)c \\
&= (a + b - 1) + c - (a + b - 1)c \\
&= a + b - 1 + c - ac - bc + c \\
&= a + b + 2c - bc - ac - 1 \\
&= (a + c - ac) + (b + c - bc) - 1 \\
&= (a \otimes c) + (b \otimes c) - 1 \\
&= (a \otimes c) \oplus (b \otimes c).
\end{aligned}
$$

Therefore, the system $(R, \oplus, \otimes)$ is a field. $\square$

3.

We start by constructing the Cayley table for both operations:

$*$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$
$\bar{4}$	$\bar{4}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$
$\bar{6}$	$\bar{6}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{8}$	$\bar{8}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$

$*$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{8}$	$\bar{2}$	$\bar{6}$
$\bar{4}$	$\bar{0}$	$\bar{8}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{8}$
$\bar{8}$	$\bar{0}$	$\bar{6}$	$\bar{2}$	$\bar{8}$	$\bar{4}$

Proof.
From the Cayley table for the first operation we see that:
i. $*$ is closed over S.
ii. There's an identity element $e = 0$.
iii. All elements have an inverse.
iv. $*$ is commutative.
Additionally:
v. $*$ is associative (because addition is associative).

(i), (ii), (iii), (iv), (v) $\implies$ $(S, *)$ is a commutative group.

From the Cayley table for the second operation we see that:
a. Δ is closed over S.
b. Δ is commutative.
c. Δ has no zero divisors.
Additionally:
d. Δ is associative (because multiplication is associative).
e. Δ is distributive over $*$ (because multiplication is distributive over addition).

(a), (b), (c), (d), (e) $\implies$ Δ is an associative, distributive, and commutative binary operation on S with no zero divisors.

Therefore, $(S, *, \Delta)$ is a commutative ring with no zero divisors.

□

4.

To show that the system $(M_2, +, \cdot)$ is a ring, we need to show that:
i. $(M_2, +)$ is a commutative group.

Proof.

$$a, b \in M_2 \implies a = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \land b = \begin{bmatrix} w & z \\ -z & w \end{bmatrix}$$

$$\implies b^{-1} = \begin{bmatrix} -w & -z \\ z & -w \end{bmatrix}$$

$$\implies a + b^{-1} = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} + \begin{bmatrix} -w & -z \\ z & -w \end{bmatrix} = \begin{bmatrix} x - w & y - z \\ -(y - z) & x - w \end{bmatrix}$$

$$\implies a \cdot b = \begin{bmatrix} p & q \\ -q & p \end{bmatrix}$$

$$\implies a + b^{-1} \in M_2$$

$\implies$ $(M_2, +)$ is a commutative group (because matrix addition is commutative).

$\square$

ii. $\cdot$ is binary associative over M_2.

Proof.

$$a, b \in M_2 \implies a = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \land b = \begin{bmatrix} w & z \\ -z & w \end{bmatrix}$$
$$\implies a \cdot b = \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \cdot \begin{bmatrix} w & z \\ -z & w \end{bmatrix}$$
$$\implies a \cdot b = \begin{bmatrix} xw - yz & xz + yw \\ -(xz + yw) & xw - yz \end{bmatrix}$$
$$\implies a \cdot b = \begin{bmatrix} p & q \\ -q & p \end{bmatrix}$$
$$\implies a \cdot b \in M_2$$

Therefore, $\cdot$ is closed and associative (because matrix multiplication is associative) over M_2.

$\square$

iii. $\cdot$ is distributive over $+$.

Proof.
Since matrix multiplication is distributive, then it must also be satisfied for the subset of matrices M_2.

Therefore, $(M_2, +, \dot{})$ is a ring. $\square$