03 January 2024 11:00

14 Rings and Modular Arithmetic

14.1 The Ring structure: Definition and Examples

Ring: Let R be a nonempty set on which we have two closed binary operations, denoted by $+$ and $\cdot$. Then $(R, +, \cdot)$ is a ring if for all $a, b, c \in R$, the following conditions are satisfied:

(a) $a + b = b + a$ — Commutative Law of $+$

(b) $a + (b + c) = (a + b) + c$ — Associative Law of $+$

(c) There exists $\mathbb{Z} \in R$ such that $a + \mathbb{Z} = \mathbb{Z} + a = a$ for every $a \in R$. — Existence of Identity for $+$

(d) For each $a \in R$ there is an element $b \in R$ with $a + b = b + a = \mathbb{Z}$. — Existence of Inverses under $+$

(e) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ — Associative Law of $\cdot$

(f) $a \cdot (b + c) = a \cdot b + a \cdot c$

$(b + c) \cdot a = b \cdot a + c \cdot a$ — Distributive Law of $\cdot$ over $+$

- We call $+$ addition and $\cdot$ multiplication.
- Multiplication need not be commutative.
- A ring need not have an identity under multiplication.

Examples of Rings

1. $(\mathbb{Z}, +, \cdot)$; $(\mathbb{Q}, +, \cdot)$; $(\mathbb{R}, +, \cdot)$; $(\mathbb{C}, +, \cdot)$ are all rings.
2. $(2\mathbb{Z}, +, \cdot)$ is a ring.
3. The set $M_2(\mathbb{Z})$ of 2×2 matrices with integer entries is a ring.

- Show that $(\mathbb{Z}, +, \cdot)$ is a ring.

Solution: $\mathbb{Z}$ has operations $+$ (addition) and $\cdot$ (multiplication). It is closed under those operations, in that if $a, b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$ and $a \cdot b \in \mathbb{Z}$.

1. Addition is commutative: If $a, b \in \mathbb{Z}$, then $a+b = b+a$.
2. Addition is associative: If $a, b, c \in \mathbb{Z}$, then $a+(b+c) = (a+b)+c$.
3. There is an additive identity $0 \in \mathbb{Z}$: For all $a \in \mathbb{Z}$, $a+0 = 0+a = a$.
4. Every element has an additive inverse: If $a \in \mathbb{Z}$, then there is an element $-a \in \mathbb{Z}$ such that $a+(-a) = (-a)+a = 0$.
5. Multiplication is associative: If $a, b, c \in \mathbb{Z}$, then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

6. The Distributive Laws hold: If $a, b, c \in \mathbb{Z}$, then

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Therefore $(\mathbb{Z}, +, \cdot)$ is a ring.

Similarly we can show that $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$ are all rings.

- Let $M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ be the set of all 2×2 matrices with integer entries. Now if we define $+$ and $\cdot$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}, \text{ then}$$

$+$ and $\cdot$ are closed binary operations.

Let us show that $(M_2(\mathbb{Z}), +, \cdot)$ is a ring.

1. '+' is commutative : If $A, B \in M_2(\mathbb{Z})$, then

$A + B = B + A$ [Matrix addition is commutative]

2. '+' is associative : If $A, B, C \in M_2(\mathbb{Z})$, then

$A + (B + C) = (A + B) + C$ [Matrix addition is associative]

3. There is an additive identity $O_{2\times 2} \in M_2(\mathbb{Z})$: For all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$,

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

4. Every element has an additive inverse : If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$, then

there exists $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} \in M_2(\mathbb{Z})$ such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

5. Multiplication is commutative: If $A, B, C \in M_2(\mathbb{Z})$, then

$A \cdot (B \cdot C) = (A \cdot B) \cdot C$ [Matrix multiplication is associative]

6. The Distributive Laws hold: If $A, B, C \in M_2(\mathbb{Z})$, then

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

$$(B + C) \cdot A = B \cdot A + C \cdot A$$

[Multiplication of matrices is distributive with respect to the matrix addition.]

Note: It is not the case that $AB = BA$ for all $A, B \in M_2(\mathbb{Z})$.
For example, if $A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$, then

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ and}$$

$$BA = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \neq AB.$$

Commutative ring: Let $(R, +, \cdot)$ be a ring. If $ab = ba$ for all $a, b \in R$, then R is called a commutative ring.

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are all commutative rings.
- $(2\mathbb{Z}, +, \cdot)$ is a commutative ring.

To prove this, we know that $(2\mathbb{Z}, +, \cdot)$ is a ring; and let $a, b \in 2\mathbb{Z}$. Then $a = 2k$, $b = 2l$ for some $k, l \in \mathbb{Z}$.

Then $a.b = (2k).(2l) = (2l).(2k) = b.a$.

Therefore, $2\mathbb{Z}$ is a commutative ring under ordinary addition and multiplication with **additive identity** 0.

- $(M_2(\mathbb{Z}), +, \cdot)$ is a non commutative ring.

$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$, but $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$.

A ring with no proper divisors of zero: Let $(R, +, \cdot)$ be a ring. If $ab = z \Rightarrow a = z$ or $b = z$, then the ring is said to have no proper divisors of zero.

- $(\mathbb{Z}, +, \cdot)$, $(2\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are all rings with no proper divisors of zero.

To see that $(\mathbb{Z}, +, \cdot)$ is a ring with no proper divisors of zero, we know that $(\mathbb{Z}, +, \cdot)$ is a ring; and let $a, b \in \mathbb{Z}$.

If $ab = 0$, then $a = 0$ or $b = 0$.

Therefore $(\mathbb{Z}, +, \cdot)$ is a ring with no proper divisors of zero.

- However, the ring $M_2(\mathbb{Z})$ does contain proper divisors of zero.

$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \in M_2(\mathbb{Z})$

$AB = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, but none of them is $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Ring with unity: Let $(R,+,\cdot)$ be a ring. The ring R is called a ring with unity if there is an element $u \in R$ with $u \neq z$ and

$au = ua = a$ for all $a \in R$.

Here u is called a unity or multiplicative identity.

- $(\mathbb{Z},+,\cdot)$ is a ring with unity.
  $z = 0$ is the additive identity.
  $u = 1$ is the unity or multiplicative identity.
- $(2\mathbb{Z},+,\cdot)$ is a ring **with no unity**.
  In $2\mathbb{Z}$, there is no element u with
  $au = ua = a$ for all $a \in 2\mathbb{Z}$.

- $(M_2(\mathbb{Z}),+,\cdot)$ is a ring with unity.
  $z = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the additive identity.

$U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unity.

Multiplicative Inverse: Let $(R, +, \cdot)$ be a ring with unity u. If $a \in R$ and there exists $b \in R$ such that $ab = ba = u$, then b is called multiplicative inverse of a. An element of R with multiplicative inverse is called unit of R.

Note that if $ab = ba = u$, then a and b are multiplicative inverse of each others and hence both are units.

- -1 and 1 are the units of $(\mathbb{Z}, +, \cdot)$.
- All nonzero elements of $(R, +, \cdot)$ are units.

Integral domain: Let R be a commutative ring with unity. Then R is called an integral domain if R has no proper divisors of zero.

- A zero-divisor is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Thus, in integral domain, a product is 0 (zero) only when one of the factors is 0 (zero).

- The ring of integers is an integral domain.

Field : Let R be a commutative ring with unity. Then R is called a field if every non zero element of R is a unit.

- $(\mathbb{Z}, +, \cdot)$ is NOT a field.
  2 is nonzero but it is not a unit i.e., Here is no element $b \in \mathbb{Z}$ with $2b = b2 = 1$.
- $(\mathbb{R}, +, \cdot)$ is a field.
  $\mathbb{R}$ is a commutative ring with unity $u = 1$.
  Every nonzero element of R is a unit.
  For example, 2 is a unit because $\frac{1}{2} \in R$ with $2 \cdot \frac{1}{2} = \frac{1}{2} \cdot 2 = 1$.

Exercises 14.1

Q.2 Determine whether or not each of the following sets of numbers is a ring under ordinary addition and multiplication.

(a) R = the set of positive integers and zero.

Solution: $R = \mathbb{Z}^+ \cup \{0\} = \{0, 1, 2, 3, \dots\}$.

$(R, +, \cdot)$ is NOT a ring.

1. $a + b = b + a \quad \forall\, a, b \in R$. ✓

2. $a + (b + c) = (a + b) + c \quad \forall\, a, b, c \in R$. ✓

3. $0 \in R$ s.t. $a + 0 = 0 + a = a \quad \forall\, a \in R$. ✓

4. Does not hold.

$1 \in R$ but there is no element $b \in R$ s.t.

$1 + b = b + 1 = 0$.

(b) $R = \{kn \mid n \in \mathbb{Z}, k \text{ is a fixed positive integer}\}$.

Solution: $R = k\mathbb{Z}$.

Let $a, b, c \in R$. Then

$a = kn_1$, $b = kn_2$, $c = kn_3$ for some $n_1, n_2, n_3 \in \mathbb{Z}$.

1. $a + b = kn_1 + kn_2 = kn_2 + kn_1 = b + a$.

2. $a + (b + c) = kn_1 + (kn_2 + kn_3)$

$= (kn_1 + kn_2) + kn_3$

$= (a+b)+c.$

3. $z = k(0) = 0 \in R$ s.t. $0 + a = a + 0 = a$ if $a = kn_1 \in R$.

4. For $a = kn_1 \in R$, there is an element $b = -kn_1$ s.t.
$a + b = kn_1 + (-kn_1) = (-kn_1) + kn_1 = b + a = 0.$

5. $a \cdot (b \cdot c) = kn_1 \cdot (kn_2 \cdot kn_3) = (kn_1 \cdot kn_2) \cdot kn_3 = (a \cdot b) \cdot c.$

6. $a \cdot (b+c) = kn_1 \cdot (kn_2 + kn_3) = kn_1 \cdot kn_2 + kn_1 \cdot kn_3 = a \cdot b + a \cdot c$
$(b+c) \cdot a = (kn_2 + kn_3) \cdot kn_1 = kn_2 \cdot kn_1 + kn_3 \cdot kn_1 = b \cdot a + c \cdot a.$

All the six properties hold. Therefore R is a ring.

(c) $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

Solution. Let $a_1 + b_1\sqrt{2}$, $a_2 + b_2\sqrt{2}$, $a_3 + b_3\sqrt{3}$ be any three elements of R.
Then

1. $(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2}).$ ✓

2. $(a_1 + b_1\sqrt{2}) + ((a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{3}))$

$= ((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) + (a_3 + b_3\sqrt{3})$. ✓

3. $\exists\ 0 = 0 + 0\cdot\sqrt{2} = 0 \in R$ s.t.

$0 + (a_1 + b_1\sqrt{2}) = (a_1 + b_1\sqrt{2}) + 0 = a_1 + b_1\sqrt{2}$. ✓

4. For $a_1 + b_1\sqrt{2} \in R$, there is an element
$-a_1 - b_1\sqrt{2} \in R$ s.t.

$(a_1 + b_1\sqrt{2}) + (-a_1 - b_1\sqrt{2}) = (-a_1 - b_1\sqrt{2}) + (a_1 + b_1\sqrt{2}) = 0$. ✓

5. $(a_1 + b_1\sqrt{2}) \cdot ((a_2 + b_2\sqrt{2}) \cdot (a_3 + b_3\sqrt{2}))$

$= (a_1 + b_1\sqrt{2})(a_2 a_3 + 2 b_2 b_3 + (a_2 b_3 + a_3 b_2)\sqrt{2})$

$= a_1(a_2 a_3 + 2 b_2 b_3) + 2 b_1 (a_2 b_3 + a_3 b_2)$

$+ (b_1(a_2 a_3 + 2 b_2 b_3) + a_1(a_2 b_3 + a_3 b_2))\sqrt{2}$

$$= (a_1 a_2 a_3 + 2a_1 b_2 b_3 + 2 a_2 b_1 b_3 + 2 a_3 b_1 b_2)$$
$$+ (a_2 a_3 b_1 + 2 b_1 b_2 b_3 + a_1 a_2 b_3 + a_1 a_3 b_2)\sqrt{2}$$

Similarly, $((a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2})) \cdot (a_3 + b_3\sqrt{2})$

$$= ((a_1 a_2 + 2 b_1 b_2) + (a_1 b_2 + a_2 b_1)\sqrt{2}) \cdot (a_3 + b_3\sqrt{2})$$
$$= (a_1 a_2 + 2 b_1 b_2) a_3 + 2 (a_1 b_2 + a_2 b_1) b_3$$
$$+ ((a_1 a_2 + 2 b_1 b_2) b_3 + (a_1 b_2 + a_2 b_1) a_3)\sqrt{2}$$

$$= (a_1 a_2 a_3 + 2 a_3 b_1 b_2 + 2 a_1 b_2 b_3 + 2 a_2 b_1 b_3)$$
$$+ (a_1 a_2 b_3 + 2 b_1 b_2 b_3 + a_1 a_3 b_2 + a_2 a_3 b_1)\sqrt{2}$$

clearly, $(a_1 + b_1\sqrt{2}) \cdot ((a_2 + b_2\sqrt{2}) \cdot (a_3 + b_3\sqrt{3}))$

$$= ((a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2})) \cdot (a_3 + b_3\sqrt{2}) \cdot$$

6. Similarly we can show that

$$(a_1 + b_1\sqrt{2}) \cdot ((a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{2}))$$

$$= (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) + (a_1 + b_1\sqrt{2}) \cdot (a_3 + b_3\sqrt{2}) \quad \&$$

$$((a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{2})) \cdot (a_1 + b_1\sqrt{2})$$

$$= (a_2 + b_2\sqrt{2}) \cdot (a_1 + b_1\sqrt{2}) + (a_3 + b_3\sqrt{2}) \cdot (a_1 + b_1\sqrt{2}) .$$

(d) $R = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b \in \mathbb{Z}, c \in \mathbb{R}\}$.

Solution: R is not a ring.

$(1 + \sqrt{2} + \sqrt{3}), (-1 + \sqrt{2} + \sqrt{3}) \in R$ but

$$(1 + \sqrt{2} + \sqrt{3}) \cdot (-1 + \sqrt{2} + \sqrt{3})$$

$$= (\sqrt{2} + \sqrt{3})^2 - 1^2$$

$$= 2 + 3 + 2\sqrt{6} - 1$$

$$= 4 + 2\sqrt{6} \notin R$$ as it cannot be written

in the form $a + b\sqrt{2} + c\sqrt{3}$ with $a, b \in \mathbb{Z}$, $c \in \emptyset$.

Therefore R is not closed under '.'.

Hence, R is not a ring.

Q.3 Let $(R, +, \cdot)$ be a ring with a, b, c, d elements of R. State the conditions that are needed to prove each of the following results.

(a) $(a+b)+c = b+(c+a)$

Solution: $(a+b)+c = (b+a)+c$ [Commutative Law of +]

$= b+(a+c)$ [Associative Law of +]

$= b+(c+a)$ [Commutative Law of +].

(b) $d + a(b+c) = ab + (d+ac)$

Solution: $d+a(b+c) = d+(ab+ac)$ [Distributive Law of · over +]

$= (d+ab)+ac$ [Associative Law of +]

$= (ab+d) + ac$ [Commutative Law of +]

$= ab + (d+ac)$ [Associative Law of +]

(c) $c(d+b) + ab = (a+c)b + cd$

(d) $a(bc) + (ab)d = (ab)(d+c)$.

Q.6 Define the binary operations $\oplus$ and $\odot$ on $\mathbb{Z}$ by $x \oplus y = x+y-7$, $x \odot y = x+y-3xy$, for all $x, y \in \mathbb{Z}$. Explain why $(\mathbb{Z}, \oplus, \odot)$ is not a ring.

Solution.

$1, 2, 3 \in \mathbb{Z}$

$1 \odot (2 \oplus 3) = 1 \odot (2+3-7) = 1 \odot (-2) = 1+(-2)-3(1)(-2) = 5$

$(1 \odot 2) \oplus (1 \odot 3) = (1+2-3(1)(2)) \oplus (1+3-3(1)(3))$

$= (-3) \oplus (-5)$

$= (-3)+(-5)-7$

$= -15$

$1 \odot (2 \oplus 3) \neq (1 \odot 2) \oplus (1 \odot 3)$.

The left Distributive Law of $\odot$ over $\oplus$ does not hold.

Q.12 [H.W.]

14.2 Ring Properties and Substructures

Theorem 1. In any ring $(R,+,\cdot)$,

(a) The zero element z is unique, and

(b) the additive inverse of each ring element is unique.

Theorem 2. The Cancellation Law of Addition. For all $a,b,c \in R$,

a) $a+b = a+c \Rightarrow b = c$, and

b) $b+a = c+a \Rightarrow b = c$.

Theorem 3. For any ring $(R,+,\cdot)$ and any $a \in R$, we have $az = za = z$.

Theorem 4. Given a ring $(R,+,\cdot)$, for all $a,b \in R$,

a) $-(-a) = a$

b) $a(-b) = (-a)b = -(ab)$, and

c) $(-a)(-b) = ab$.

Theorem 5. For a ring $(R, +, \cdot)$,

a) if R has a unity, then it is unique, and

b) if R has a unity, and x is a unit of R, then the multiplicative inverse of x is unique.

Theorem 6. Let R be a commutative ring with unity. Then R is an integral domain if, for all $a, b, c \in R$ where $a \neq 0$, $ab = ac \Rightarrow b = c$.

Subring: A subset S of a ring R is a subring of R if S is itself a ring with the operations on R.

- $\{0 \text{ (zero)}\}$ and R are subrings of any ring R. $\{0\}$ is called the trivial subring of R.

- For each positive integer n, the set

  $nZ = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$ is a subring of Z under ordinary addition and multiplication.

- The set $D_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$ of diagonal matrices is a subring of $M_2(\mathbb{Z})$.

Exercises 14.2

Q.4 Prove that a unit in a ring cannot be a proper divisor of zero.

Solution - Let R be a ring. Let x be a unit of R.

Then there exists an element y such that

$$xy = yx = u \text{ (unity)}. \quad \text{— (1)}$$

Suppose that x is a proper divisor of zero.

Then there must exist a nonzero element $w \in R$ with

$$x \cdot w = w \cdot x = z \text{ (zero)}. \quad \text{— (2)}$$

So $y \cdot (x \cdot w) = (y \cdot x) \cdot w$ [Using associativity]

$= u \cdot w$ [From (1)]

$= w$ — (3)

Also, $y \cdot (x \cdot w) = y \cdot (z)$ [From (2)]

$= z$ — (4).

$xy = yx = u$ (unity). — (1)

Suppose that x is a proper divisor of zero.

Then there must exist a nonzero element $w \in R$ with

$x \cdot w = w \cdot x = z$ (zero). — (2)

So $y \cdot (x \cdot w) = (y \cdot x) \cdot w$ [Using associativity]

$= u \cdot w$ [From (1)]

$= w$ — (3)

Also, $y \cdot (x \cdot w) = y \cdot (z)$ [From (2)]

$= z$ — (4).

From (3) and (4), we have $w = z$ contradicting the fact that w is nonzero.

Therefore the unit x cannot be a proper divisor of zero.

H.W. Q.2, Q.3.