GROUPS

RINGS

FIELDS

Binary Operation:

A binary operation $*$ on a set G is a function $* : G \times G \longrightarrow G$.

$$\forall a,b \in G \quad [a * b := *(a,b)]$$

A binary operation $*$ on the set G is associative if

$$\forall a,b,c \in G \quad [(a*b)*c = a*(b*c)]$$

A binary operation $*$ on the set G is commutative if

$$\forall a,b \in G \quad [a*b = b*a]$$

Suppose $*$ is binary operation on a set G.
Consider a set H which is a subset of G.

$$\forall a,b \in H \quad [a*b \in H] \longrightarrow H \text{ is closed under } *$$

Observe if $*$ is an associative on G and $*$ is restricted to some subset H of G is a binary operation on H then $*$ is automatically associative on H.

Observe if $*$ is an commutative on G and $*$ to H is a binary operation on H where $H \subseteq G$. Then $*$ is automatically commutative on H.

Group:

A group is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms –

(i) (Closure) $\forall a, b \in G \left[a * b \in G \right]$

[implied automatically because of the definition of a binary operation $*$ defined on G.]

G is closed under $*$.

(ii) (Associative) $\forall a, b, c \in G \left[(a * b) * c = a * (b * c) \right]$

$*$ is associative on G.

(iii) (Identity) There exists an unique element $e \in G$ called the identity of G such that.

$\exists! e \in G, \forall a \in G \left[a * e = e * a = a \right]$

↳ Unique identity

(iv) (Inverse) For each element $a \in G$, there exists an unique element $a^{-1} \in G$ called inverse of element a such that

$$\forall a \in G \left[a^{-1} * a = a * a^{-1} = e \right]$$

A group $(G, *)$ is called Abelian (or commutative) group if and only if

$$\forall a, b \in G \left[a * b = b * a \right]$$

A group $(G, *)$ is called finite group if and only if G is a finite set.

A group $(G, *)$ is always a non-empty because of the fact that the group must contain the identity element 'e' (at least) within it.

Terminology: G is a group under $*$

$(G, *)$ is a group

G is a group (when operation $*$ is clear from the context)

Properties of Groups:

$(G, *)$ is a group.

(i) The identity e of G is unique.

proof: Assume identity of $G = e, f$ where $e \neq f$

Applying identity axiom,

$$\left.\begin{aligned} e * f &= e \\ f * e &= e \end{aligned}\right\} \text{ and } \quad \begin{aligned} f * e &= f \\ e * f &= f \end{aligned}$$

We are applying identity f on e — we are applying identity e on f

Note that $f * e = e$

$f * e = f$

Therefore $e = f$ but it is a contradiction of the assumption (Hence proved)

(ii) $\forall a \in G$ ($a^{-1} \in G$ is unique)

proof: Assume, $a^{-1} = x$ and $a^{-1} = y$ where $x \neq y$

Applying inverse axiom:

Assuming e = identity element of G

$$\left.\begin{aligned} a^{-1} * a &= e \\ a * a^{-1} &= e \end{aligned}\right\} \quad \begin{aligned} x * a &= e \\ y * a &= e \end{aligned}$$

Similarly, $a * x = e$

$a * y = e$

$x * a = y * a$

Post multiply by a^{-1} on both sides -

$x * a * a^{-1} = y * a * a^{-1}$

$\Rightarrow x * e = y * e$

$\Rightarrow x = y$

But it is a contradiction of the assumption (hence proved)

(iii) $(a^{-1})^{-1} = a$ for all $a \in G$.

proof: $a^{-1} = x$ (let) and

Applying axiom of inverse: $x * x^{-1} = e$

where e = identity element of G.

$$a^{-1} = x$$

$$\Rightarrow x^{-1} * a^{-1} = x^{-1} * x = e$$

$$\Rightarrow x^{-1} * a^{-1} * a = e * a = a$$

$$\Rightarrow x^{-1} * e = a$$

$$\Rightarrow x^{-1} = a$$

$$\Rightarrow (a^{-1})^{-1} = a \quad [\text{Hence Proved}]$$

(iv) $\forall a, b \in G \quad \left[(a*b)^{-1} = b^{-1} * a^{-1} \right]$

From inverse axiom,

$$(a*b) * (a*b)^{-1} = e \quad [e = \text{identity}]$$

Now we need to eliminate a & b so premultiply by a^{-1} and b^{-1}.

$$\Rightarrow (a^{-1}*a) * b * (a*b)^{-1} = a^{-1} * e = a^{-1}$$

$$\Rightarrow (e*b) * (a*b)^{-1} = a^{-1}$$

$$\Rightarrow b * (a*b)^{-1} = a^{-1}$$

$$\Rightarrow (b^{-1}*b) * (a*b)^{-1} = b^{-1} * a^{-1}$$

$\Rightarrow e * (a*b)^{-1} = b^{-1} * a^{-1}$

$\Rightarrow (a*b)^{-1} = b^{-1} * a^{-1}$ (Hence proved)

Note: Throughout the proofs, we do not change the order of operands in operation $*$ (unless it is permitted by inverse & identity axioms) since G may be non-Abelian group also.

Notations: $(G, *) \equiv (G, \cdot)$

$a*b \equiv a \cdot b \equiv ab$

$x \cdot x \cdot x \cdot \ldots \cdot x = x^n$

$x^{-1} \cdot x^{-1} \cdot x^{-1} \cdot \ldots \cdot x^{-1} = x^{-n}$

identity element, $e = 1$ for the abstract group $(G, \cdot)$

(v) Left Cancellation & Right Cancellation property.

$\forall a, b, x, y \in G \quad \left[\begin{array}{lll} au = av & \longrightarrow & u = v \\ ub = vb & \longrightarrow & u = v \end{array} \right]$

Proof: Use the proof of contradiction by assuming L.H.S as True & R.H.S as false.

$au = av$ [True] and $u \neq v$

Premultiply by a^{-1} on both side.

$a^{-1}au = a^{-1}av$

$\Rightarrow u = v$ [contradiction]

Rings:

(a) A ring R is a set together with 2 binary operations $+, \times$ (addition, multiplication) satisfying the following axioms –

(i) $(R, +)$ is an Abelian group.

(ii) $\forall a,b,c \in R \quad [\, a \times (b \times c) = (a \times b) \times c \,]$

$\times$ is associative on R.

(iii) The closedness of R under $\times$ is implied because $\times$ is a binary operation on R. $\times : R \times R \to R$

(iv) The distributive laws hold in R.

$$\forall a,b,c \in R \quad [\, (a+b) \times c = (a \times c) + (b \times c) \,]$$

$$\forall a,b,c \in R \quad [\, a \times (b+c) = (a \times b) + (a \times c) \,]$$

The distribution of multiplication over addition.

(b) A Ring R is called "commutative" ring if the multiplication is commutative.

$$\forall a,b \in R \quad [\, a \times b = b \times a \,]$$

(c) A Ring R is called "Ring with identity" if there exists an identity element for multiplication on R.

$$\exists!\, e \in R,\ \forall a \in R \quad [\, a \times e = a \wedge e \times a = a \,]$$

(d) A Ring R is called "commutative ring with identity" if there exist identity for multiplication and if the multiplication is commutative [(b)+(c) together]

Notation: $(R, +, \times) \equiv (R, +, \cdot)$

$$a \times b \equiv a \cdot b$$

Additive identity $= 0$

Additive inverse of $a = a^{-1} = -a$

Multiplicative identity $= 1$

We see that in the definition of ring, $(R, +)$ must be Abelian group. To see why "commutative" criteria on $+$ is enforced we follow the calculation.

1: Multiplicative identity
$a, b \in R$.
} currently assume $(R, +)$ is a group

$$(1+1)\cdot(a+b) = (1+1)\cdot a + (1+1)\cdot b$$

$$= 1\cdot a + 1\cdot a + 1\cdot b + 1\cdot b = a + a + b + b$$

$$(1+1)\cdot(a+b) = 1\cdot(a+b) + 1\cdot(a+b)$$
$$= 1\cdot a + 1\cdot b + 1\cdot a + 1\cdot b$$
$$= a+b+a+b$$

Look at the 2 results. If we don't assume commutativity of $+$ on R then the 2 results of distributive law of ring will be different. When we impose $a+b = b+a$ then we get the same result.

(e) A ring R with identity $1 \in R$ where $1 \neq 0$ [0 is additive identity] is called "division ring" if

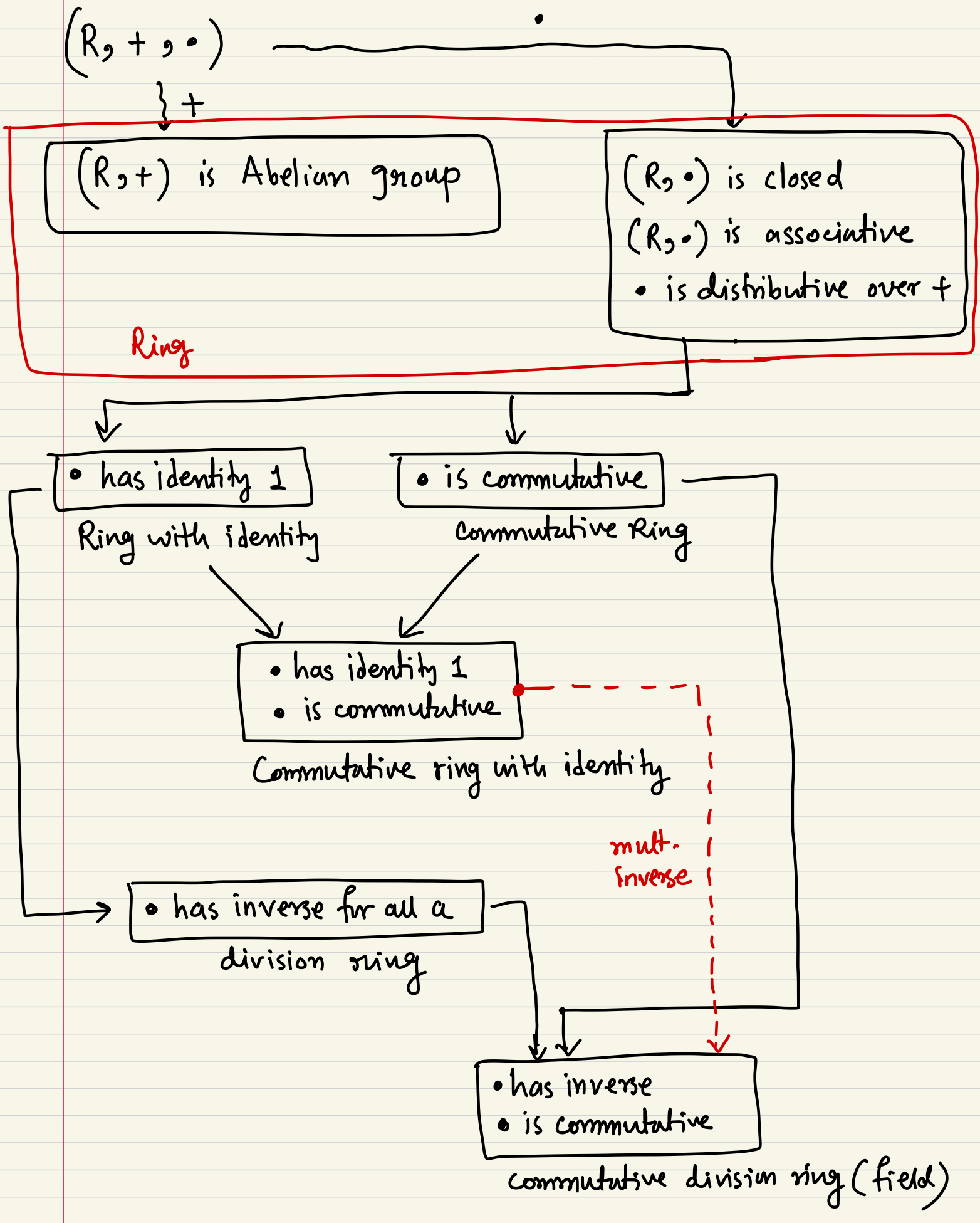
$$\forall a \in R, a \neq 0 \left[a^{-1}\cdot a = 1 \wedge a\cdot a^{-1} = 1 \right]$$

(there exists multiplicative inverse for all elements of R).

(f) A division ring R is called "Field" if

$$\forall a,b \in R \left[a\cdot b = b\cdot a \right]$$

meaning for-all elements (a,b), it is commutative under multiplication. So a commutative division ring is called field.


$(R, +, \cdot)$
$+$
$\cdot$
$(R, +)$ is Abelian group
$(R, \cdot)$ is closed
$(R, \cdot)$ is associative
$\cdot$ is distributive over $+$
Ring
• has identity 1
Ring with identity
• is commutative
Commutative Ring
• has identity 1
• is commutative
Commutative ring with identity
mult. inverse
• has inverse for all a
division ring
• has inverse
• is commutative
commutative division ring (field)

Ex1: Integer $\mathbb{Z}$ under usual operations $+$ and $\times$ is a commutative ring with identity.

(i) $(\mathbb{Z}, +)$ is an Abelian group.

- 1. Closeness of $+$. ✓
- 2. Associative of $+$. ✓
- 3. identity of $+$ (0) ✓
- 4. inverse of a $(-a)$ ✓
- 5. Commutative of $+$ ✓

(ii) Closeness of $\times$ ✓

(iii) Associative of $\times$ ✓

(iv) Distribution of $\times$ over $+$ ✓

$$(-2+3)\times 5 = (-2\times 5) + (3\times 5)$$
$$5\times(-2+3) = (5\times -2) + (5\times 3)$$

] same.

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

(v) Multiplicative identity (1) ✓

So $(\mathbb{Z}, +, \times)$ is ring with identity.

(vi) Multiplicative commutative ✓

So $(\mathbb{Z}, +, \times)$ is commutative ring with identity

(vii) Multiplicative inverse ×

For most of the elements multiplicative inverse doesn't exist

$3^{-1} = 0.33 \notin \mathbb{Z}$ so it is not a field.

3^{-1} is defined as: $3^{-1} \cdot 3 = 1$ and $3 \cdot 3^{-1} = 1$

There is no such $z \in \mathbb{Z}$ such that $z \cdot 3 = 1$ and $3 \cdot z = 1$.

So $(\mathbb{Z}, +, \times)$ is not a field.

Ex2: Set of real numbers $(\mathbb{R}, +, \times)$

Set of complex numbers $(\mathbb{C}, +, \times)$

These are commutative ring with identity and in fact they are fields.

$\mathbb{R}$ and $\mathbb{C}$ are fields because for every non-zero elements, the inverse will exist. Look at the definition that says, there exists the inverse for all non-zero elements. For every non-zero element, the multiplicative inverse must exist. That's why 0 is not checked for the multiplicative inverse.

In any field, the multiplicative inverse of the additive identity doesn't exist.

Motivation behind Ring:

Many sets have 2 operations — addition and multiplication. It can be integers, integers modulo n, real numbers, matrices and polynomials. When considering these sets as groups, we simply used addition and ignored the multiplication. Ring structure takes care of both operation.

Ring is Abelian group under addition.
Ring is closed under multiplication.
Ring is associative under multiplication.
Ring has distributive property of multiplication over addition.

Note: Although ring has left & right distribution of multiplication over addition, in general the multiplication operation is not commutative in ring.

Also ring need not have identity element under mult.
A ring with identity need not have multiplicative inverse when it has inverse we say it is division ring.

Ring is not a group under multiplication. Ring elements need not have multiplicative inverses. Ring structure need not have multiplicative identity.

Properties of Rings:

Let R be a ring. Then -

(i) $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$

where 0 is additive identity and $\cdot$ is multiplication

Distributive property of $\cdot$ over $+$

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

Let $x = a \cdot 0$

We have to show that $x = 0$

$$x = a \cdot (0+0) = a \cdot 0 + a \cdot 0 = x + x$$

Adding $(-x)$ on both sides-

$(x - x) = x + (x - x)$ [$x - x = 0$ by additive inverse]

$\Rightarrow 0 = x + 0$ [$x + 0 = x$ by additive identity]

$\Rightarrow 0 = x$ [Proved]

(ii) $\forall a, b \in R$ $[\ a \cdot (-b) = (-a) \cdot b = -(a \cdot b)\ ]$

($-b$ is additive inverse of b)

Let $y = a \cdot (-b)$

We have to show, $y = -(a \cdot b)$

or, $y + (a \cdot b) = -(a \cdot b) + (a \cdot b) = 0$

(Adding $(a \cdot b)$ in both sides of equation and additive inverse axiom follows)

or $y + (a \cdot b) = 0$ (to be proved)

$$y + (a \cdot b) = a \cdot (-b) + (a \cdot b)$$
$$= (a) \cdot (-b) + (a) \cdot (b)$$
$$= (a) \cdot [-b + b] \quad [\text{Distributive Law}]$$
$$= (a) \cdot 0 \quad [\text{additive inverse}]$$
$$= 0 \quad [\text{proved}]$$

(iii) $\forall a, b \in R \quad (-a) \cdot (-b) = a \cdot b$

Consider, $x = -a$, $y = -b$.

$\Rightarrow x + a = -a + a = 0$

$\Rightarrow y + b = -b + b = 0$

Prove that, $x \cdot y = a \cdot b$

$x \cdot b = (-a) \cdot b = -(a \cdot b)$

$a \cdot y = a \cdot (-b) = -(a \cdot b)$

$$(x+a)\cdot(y+b) = 0\cdot 0 = 0$$

$$\Rightarrow x\cdot y + x\cdot b + a\cdot y + a\cdot b = 0$$

$$\Rightarrow x\cdot y + (-a)\cdot b + a\cdot y + a\cdot b = 0$$

$$\Rightarrow x\cdot y - (a\cdot b) + a\cdot y + (a\cdot b) = 0$$

$$\Rightarrow x\cdot y + a\cdot y = 0$$

$$\Rightarrow x\cdot y + a\cdot y - (a\cdot y) = -(a\cdot y)$$

$$\Rightarrow x\cdot y = -(a\cdot y) = -(a\cdot(-b))$$

$$= -(-(a\cdot b)) = (a\cdot b) \quad [(p^{-1})^{-1} = p]$$

$$\Rightarrow x\cdot y = a\cdot b \quad [\text{proved}]$$

(iv) If R has an identity 1, then the identity is unique and $-a = (-1)\cdot a$

Suppose, there are 2 multiplicative identity e and f.

$$\forall a \in R \left[a\cdot e = a \wedge e\cdot a = a \right] \quad \text{—(1)} \quad (e \neq f)$$

$$\forall a \in R \left[a\cdot f = a \wedge f\cdot a = a \right] \quad \text{—(2)}$$

Applying (i) for element 'f'. $f\cdot e = f$

Applying (ii) for element 'e'. $f\cdot e = e$

Note that $f \cdot e = f = f \cdot e = e$

Therefore, $f = e$ which contradicts with the assumption.
Hence the multiplicative identity is unique and it is 1.

$(-a) + (a) = 0$ (additive inverse)

Since R is ring with identity so multiplicative identity exists.

$1 \cdot a = a$ and $a \cdot 1 = a$

Therefore, $(-a) + (a) = 0$

$\Rightarrow (-a) + (a) + (-a) = -a$

$\Rightarrow (-a) = (-a) \cdot 1 = 1 \cdot (-a) = (-1) \cdot a$

(Proved)

Zero Divisors and Units:

Let R be a ring.
A nonzero element a $(a \in R \wedge a \neq 0)$ is called a "zero divisor" if there is a nonzero element b $(b \in R \wedge b \neq 0)$ such that

either $a \cdot b = 0$ or $b \cdot a = 0$ where 0 is add ident.

A zero divisor is a non-zero element of the ring whose multiplication with another non-zero element results in additive identity.

if a is a zero divisor then $a \cdot b = \underbrace{0}_{\text{additive identity}}$

If a, b are 2 element of ring and $a \neq 0, b \neq 0$ then a is a zero divisor with respect to b and b is a zero divisor with respect to a.

Assume that R has an identity $1 \neq 0$ so R is now ring with identity. An element u of R is called a "unit" ($u \in R$) if there exists $v \in R$ such that.

$$u \cdot v = v \cdot u = \underbrace{1}_{\text{multiplicative identity.}}$$

The set of all units of R is denoted as $R^{\times}$

The units $R^{\times}$ in a ring R form a group under multiplication so $(R^{\times}, \times)$ is a group because they will have inverse but the ring itself will not form the group under multiplication.

Suppose $\left(R=\{0,1,2,3,4,5\}, \oplus_6, \odot_6\right) \equiv (R,+,\cdot)$

We have a zero divisor, a s.t. $a \cdot b = 0$

where $a \neq 0$, $b \neq 0$.

Consider 4 and 3 so, $4 \cdot 3 = (4 \times 3) \bmod 6$

$= 12 \bmod 6$

$= 0$

"A zero divisor can never be a unit:"

Zero divisor: $a \cdot b = 0 \rightsquigarrow$ [additive identity]

Unit: $u \cdot v = 1 \rightsquigarrow$ [multip. identity]

Here a, b are zero divisors (due to commutativity)

Here u, v are units (due to commutativity)

Suppose, 'a' is a unit in R and $a \cdot b = 1$

also assume that 'a' is also a zero divisor $a \cdot c = 0$

$(c \neq 0)$

Therefore we have $a \cdot c = c \cdot a = 0 \quad (c \neq 0)$

$a \cdot b = b \cdot a = 1 \quad (b \neq 0)$

$c = 1 \cdot c = b \cdot (a \cdot c) = b \cdot 0 = 0$

It is a contradiction of the assumption

Since we have seen a zero divison can't be an unit so in case of field, all the elements are units therefore, there exist no zero divisor in a field.

Integral Domain:

A commutative ring with identity $(1 \neq 0)$ is called an integral domain if it has no zero divisors.

In an integral domain, multiplication of 2 non zero elements is non-zero.

$$\forall a, b \neq 0, \in R \quad \left[\; a \cdot b \neq 0 \; \right]$$

$$\left[\begin{array}{l} \text{If } a, b \neq 0 \text{ then } a \cdot b \neq 0 \\ \qquad \equiv \\ \text{If } a \cdot b = 0 \text{ then either } a = 0 \text{ or } b = 0 \end{array} \right] \quad \text{equivalent statement}$$

Let $a, b, c \in R$ which is an integral domain.
If $a \neq 0$ and $a \cdot b = a \cdot c$ then $b = c$.
This cancellation property holds true in Integral domain

Proof:

Assume $a \neq 0$ and $a \cdot b = a \cdot c$ and $b \neq c$
Now we will lead to a contradiction.

$a \cdot b = a \cdot c$

Adding the additive inverse of $a \cdot c$ in both sides

$$a \cdot b + (-(a \cdot c)) = (a \cdot c) + (-(a \cdot c)) = 0$$

$$\Rightarrow a \cdot b + a \cdot (-c) = 0$$

$$\Rightarrow a \cdot (b + (-c)) = 0$$

Zero divisors: $a \neq 0, b \neq 0, \quad a \cdot b = 0$

In integral domain, zero divisor doesn't exist that means if $a \cdot b = 0$ then either $a = 0$ or $b = 0$. Otherwise a or b will become zero divisor.

In integral domain, $a \neq 0 \wedge b \neq 0 \longrightarrow a \cdot b \neq 0$

or $a \cdot b = 0 \longrightarrow a = 0 \vee b = 0$

Since we get $a \cdot (b + (-c)) = 0$ and $a \neq 0$ that means to not have zero divisor $b + (-c) = 0$ must be true.

Hence $b + (-c) = 0 \Rightarrow b = c$.

Therefore, in integral domain, the cancellation property is true.

Definition of Field:

① A commutative division ring is a field. That means a ring with identity where for all elements, the inverse exist and it is commutative also then it is called a field.

② A commutative ring with identity in which every non-zero elements is a unit (inverse exists) is called a field. That means in a field, there is no zero divisors because a unit can never be a zero divisor.

"Every field is an integral domain"

Proof: Suppose F is a field. We want to prove that F is an integral domain.

That means if $a, b \in F$ and $a \neq 0, b \neq 0 \rightarrow a \cdot b \neq 0$

So there exists no zero divisors.

Assume that F is not an integral domain. That means a zero divisor will exist in F. Say it is $(a \neq 0)$.

$a \neq 0$ and $b \neq 0$ such that $a \cdot b = 0$

then a is called zero divisor.

Since F is a field, for every element inverse will exist. That means every element is unit.

$a \neq 0, a^{-1} \neq 0$ such that $a \cdot a^{-1} = 1$

$b \neq 0, b^{-1} \neq 0$ such that $b \cdot b^{-1} = 1$

Since we have $a \cdot b = 0$

premultiply by a^{-1} on both sides - (mult. inverse)

$$a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0$$

$$\Rightarrow 1 \cdot b = 0$$

$$\Rightarrow b = 0$$

So it is a contradiction because we assumed $b \neq 0$. So the assumption was wrong.

Hence every field is an integral domain.

"Every integral domain is not field"

proof:

In an integral domain, there are no zero divisors. The integral domain will be called field if all the elements of the ID has mult. inverse or all the elements are units But in ID, some elements can be units (only some of

the elements are invertible) and other elements are not zero divisors and not invertible. So there can be an ID where it may happen that all elements are not invertible so it will not be called field.

$(\mathbb{Z}, +, \cdot)$ is an integral domain because there are no zero divisors.

Zero divisors: $a \neq 0, b \neq 0$ such that $a \cdot b = 0$
But it is not a field as 2^{-1} doesn't exist so there are many elements which are not units.

zero divisors	units	
×	×	→ Very frequent
✓	×	→ property
×	✓	
✓	✓	→ Impossible

Motivation behind integral domain:

We know that ring need not have multiplicative identity and multiplicative inverses. Because of this reason, we can't apply cancellation property to ring.

If a, b, c belong to a ring, $a \neq 0$ and $ab = ac$.
In a ring, we can't conclude that $b = c$ by cancelling a from both side of equation.

$a \cdot b = a \cdot c$

$\Rightarrow$ Multiply by a^{-1} (mult. inverse) on both side.

$a^{-1} \cdot a \cdot b = a^{-1} \cdot a \cdot c$

$\Rightarrow 1 \cdot b = 1 \cdot c$

$\Rightarrow b = c$

We can do this only when the multiplicative identity and inverse exist.

In ring, it need not have multiplicative cancellation and it need not have multiplicative identity.

In ring with identity, the existence of inverse is not guarented so there also cancellation property does't hold. The same thing is also true for commutative ring with identity as multiplicative inverse need not exist.

In division ring, integral domains, fields, the cancellation property holds. Integral domain is special as there mult. Inverse is not guarented still we can cancel the terms as we will see why this is the case.

A ring is not appropriate abstraction of integers. This is because the identity do not exist and that's why cancellation property doesn't hold. Even it is not commutative under multiplication.

Integral domain is a particular class of rings that have — identity, cancellation property and the commutativity.

In integral domain, there is no zero divisors.
Zero divisors: $a \neq 0$ and $b \neq 0$ such that $a \cdot b = 0$
Then a, b are called zero divisors of the structure.

In a commutative ring with identity, the integral domains are those where —

$$\forall_{a,b \in R} \left[a \neq 0 \wedge b \neq 0 \longrightarrow a \cdot b \neq 0 \right]$$

That means there is no zero divisor. In contrapositive sense, if $a \cdot b = 0$ then either $a = 0$ or $b = 0$.

$$\forall_{a,b \in R} \left[a \cdot b = 0 \longrightarrow a = 0 \vee b = 0 \right]$$

In an integral domain, multiplication of $a \cdot b = 0$ only when one of the factors a or b is 0.

Inspite of the fact that the elements need not form a group under multiplication in integral domain, still it enjoys the cancellation property.

a, b, c belong to an integral domain.

$a \cdot b = a \cdot c$ [comm. ring with identity and have no zero divisors]

$\Rightarrow a^{-1}$ need not exist

Add the add inverse of $a \cdot c$

$\Rightarrow a \cdot b + (-(a \cdot c)) = 0$

$\Rightarrow a \cdot b + a \cdot (-c) = 0$

$\Rightarrow a \cdot (b + (-c)) = 0$

The product of 2 elements are 0 in integral domain only when $a = 0$ or $b + (-c) = 0$ as there is no zero divisors.

Therefore, $b = c$ or $a = 0$. If we have $a \neq 0$ then $b = c$ which means cancellation of a. Even though a^{-1} may/may not exist in integral domain.

A field can be though of a kind of integral domain where every element is an units. That means for all the elements multiplicative inverse must exist.

In a commutative ring with identity, there is a property that rules out one of the categories you've listed:

1. **Not (Zero Divisor) ZD, Not (Unit) U**: This category includes nonzero elements that are neither zero divisors nor units. These are ordinary nonzero elements that are neither invertible (do not have a multiplicative inverse) nor multiply to zero with another nonzero element.
2. **Not ZD, U**: These are nonzero elements that are units. They have a multiplicative inverse within the ring.
3. **ZD, Not U**: These are nonzero elements that are zero divisors but not units. They can multiply to zero with another nonzero element but do not have a multiplicative inverse.
4. **ZD, U**: This category includes elements that are both zero divisors and units. This category is not possible.

The category that can never be possible is **ZD, U**. An element cannot simultaneously be a zero divisor and a unit in a commutative ring with identity. This is because units are elements with multiplicative inverses, meaning they have a nonzero product with another element that results in the multiplicative identity. On the other hand, zero divisors are elements that multiply to zero with another nonzero element. These two properties are contradictory, so an element cannot be both a zero divisor and a unit in the same ring.

In a structure, all 3 categories can be present

$\otimes_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

1 is multiplicative identity certainly it is commutative

Hence $\mathbb{Z}/6\mathbb{Z}$ is a commutative ring with identity.

Let's find the zero divisors: $a \neq 0, b \neq 0$ s.t $a \cdot b = 0$

$2 \cdot 3 = 0$, $3 \cdot 4 = 0$

Hence 2, 3, 4 are zero divisors and they are not units We can see element 1, 5 have identity element in it and they are invertible. That means 1, 5 are units but not zero divisors.

Element 0 is neither a zero divisor, nor an unit.

Theorem: "Every finite integral domains are fields"

proof: Suppose the finite integral domain = D

We have to show that.

$$\forall a, b \in D \quad \left[\left(a^{-1} \text{ exists} \right) \text{ or } \left(a \cdot b = 1 \wedge b \neq 0 \right) \right]$$

where $b = a^{-1}$

That means every non-zero element in D has a multiplicative inverse (to be proved)

Take any non-zero element in D (say a). Consider the set of powers of a:

$$\{ a, a \cdot a, a \cdot a \cdot a, a \cdot a \cdot a \cdot a, \ldots \}$$

$= \{a, a^2, a^3, a^4, \ldots\}$

Since the D is finite, eventually the powers will repeat under the modulo operation.

Suppose, $a^n = a^m$ for some m with $m > n$

Suppose n is the smallest power to which the repeatation of large power m happens.

$$\Rightarrow a^n = \underbrace{a \cdot a \cdot a \ldots \cdot a}_{m-n \text{ times}} \cdot \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ times}} = a^{m-n} \cdot a^n$$

$$\Rightarrow 1 \cdot a^n = a^{m-n} \cdot a^n$$

In an integral domain, the cancellation property holds

Therefore,

$$a^{m-n} = 1 \quad [\because a^n \neq 0]$$

$$\Rightarrow \underbrace{a \cdot a \cdot a \ldots \cdot a}_{m-n-1 \text{ times}} \cdot \underbrace{a}_{1 \text{ time}} = 1$$

$$\Rightarrow a^{m-n-1} \cdot a = 1$$

Therefore, $a^{-1} = a^{m-n-1} \quad [\neq 0]$

Hence a^{-1} exists therefore D must be a field.

Characteristic of a Ring :

Consider the ring of Gaussian integers.

$$Z_3[i] = \{ a+bi \mid a,b \in Z_3 \}$$

where $Z_3 = \{0,1,2\}$

The ring of elements are $\{0,1,2,i,1+i,2+i,2i,2i+1,2i+2\}$

The coefficients will be reduced to modulo 3 under the addition & multiplication. $Z_3[i]$ is ID and field also.

Table 13.1 Multiplication Table for $Z_3[i]^*$.

	$\mathbf{1}$	$\mathbf{2}$	i	$\mathbf{1+i}$	$\mathbf{2+i}$	$\mathbf{2i}$	$\mathbf{1+2i}$	$\mathbf{2+2i}$
$\mathbf{1}$	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
$\mathbf{2}$	2	1	$2i$	$2+2i$	$1+2i$	i	$2+i$	$1+i$
i	i	$2i$	2	$2+i$	$2+2i$	1	$1+i$	$1+2i$
$\mathbf{1+i}$	$1+i$	$2+2i$	$2+i$	$2i$	1	$1+2i$	2	i
$\mathbf{2+i}$	$2+i$	$1+2i$	$2+2i$	1	i	$1+i$	$2i$	2
$\mathbf{2i}$	$2i$	i	1	$1+2i$	$1+i$	2	$2+2i$	$2+i$
$\mathbf{1+2i}$	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	i	1
$\mathbf{2+2i}$	$2+2i$	$1+i$	$1+2i$	i	2	$2+i$	1	$2i$

For example, $(2+i)\cdot(2+2i) = (2+i)\cdot 2 + (2+i)\cdot 2i$

$= 2\cdot 2 + 2\cdot i + 2\cdot 2\cdot i + 2\cdot i\cdot i$

$= 4 + 2i + 4i - 2$

$= 2 + 6i \pmod 3$

$= 2 + 0i = 2$

Look, there is no zero divisors in the table [No 0 in entry]

For any element x in $Z_3[i]$, we have

$3 \cdot x = x + x + x = 0$

For example, $2+2i+2+2i+2+2i = 6+6i = 0$
Because it is (mod 3) that's why all the coefficients if added 3 times will eventually be 0 when (mod 3) is done.

The characteristic of a ring R is the least positive integer 'n' such that $n \cdot x = 0$ for all $x \in R$. If no such integer n exists then we say R has characteristic 0. It is denoted as $\text{char}[R]$.

$\text{char}[Z_3[i]] = 3$ because $\forall x [x+x+x = 3 \cdot x = 0]$

$(Z_n, \oplus_n, \odot_n)$ has characteristic n.

Order of a group:

The number of elements of a group (finite/infinite) is called its order. We will use $|G|$ to denote the order of group.

Order of an element: Consider $g \in G$ is an element.

The order(g) in a group G is the smallest positive integer

n such that $g * g * g * \cdots * g = e$ [identity = e]

$$\Rightarrow g^n = e$$

If no such integer exists then we say g has infinite order of element g is denoted as $|g|$.

To compute $|g|$, we have to compute $g, g^1, g^2, g^3, \ldots$ until we find $g^n = e$. If e is not obtained then we say order is infinite for g.

Characteristic of ring with identity, R:

Let R be a ring with identity 1. If the element 1 has infinite order under addition then the char[R] will be 0. If 1 has n order under addition then the char[R] will be n.

Proof: Element 1 has ∞ order under addition.

$$1 + 1 + 1 + \cdots \infty \text{ times} = \underbrace{0}_{\text{additive identity}}$$

$$\downarrow$$

Char[R] = n s.t. $\forall a \in R \; [n \cdot a = 0]$ for smallest n where no such n exists here char[R] = 0.

If 1 has ∞ order that means no such n exists such that,

$$1+1+1+\cdots\cdots+\underbrace{1}_{n \text{ times}} = 0$$

or $n \cdot 1 = 0$

Now for any arbitrary $x \in R$,

$$n \cdot x = x + x + x + \cdots\cdots + \underbrace{x}_{n \text{ times}}$$

$$= 1 \cdot x + 1 \cdot x + \cdots + 1 \cdot x \quad [R \text{ has identity } 1]$$

$$= (1 + 1 + \cdots\cdots + 1) \cdot x \quad [\text{Distributivity axiom}]$$

$$= (n \cdot 1) \cdot x$$

Since $n \cdot 1 \neq 0$ for any n $[\text{add. order}(1) = \infty]$

Therefore, $n \cdot x \neq 0$ for any n hence characteristic of R doesn't exist and it is denoted as 0.

Similarly if 1 has order n under addition then.
$n \cdot 1 = 0$ for $n < \infty$

Hence $n \cdot x = (n \cdot 1) \cdot x = 0 \cdot x = 0$ for $n < \infty$
Therefore, $\text{char}[R] = n$ for $n < \infty$.

Characteristic of an Integral Domain:

The characteristic of an integral domain is 0 or prime number.

$\text{char}[R] = n$ such that $\forall x \in R \left[n \cdot x = 0 \right]$ for smallest $n < \infty$

$= 0$ if $n = \infty$

Integral domain has the multiplicative identity 1. Sometimes we define the characteristic of a ring with identity as - n summation of multiplicative identity resulting into additive identity for smallest n.

$\text{char}[R] = n$ such that $\left[n \cdot 1 = 0 \right]$ for smallest $n < \infty$ (provided 1 exists)

$= 0$ if no such n exists such that $n \cdot 1 = 0$

The $\text{char}[D]$ (where D = Integral Domain) will be 0 only when, no such n exists such that $n \cdot 1 = 0$

$n \cdot 1 = 0$ for no positive integer n

That means the only way to satisfy the equation is $n = 0$

Therefore, we say for no such positive integer n, the $n \cdot 1 = 0$ can be satisfied hence no such +ve int n exists
Therefore $\text{char}[D] = 0$

Suppose when the $\text{char}[D] = n$ where $n \neq 0$ & $n < \infty$
In that case, the characteristic of ID exists. We need to prove that it is a prime number.

$\text{Char}[D] = n$ such that $[n \cdot 1 = 0]$ for $n < \infty$
and $n \neq 0$ and n = prime.

(To be proved)

Suppose n is a composite number. So n can be expressed as multiplication of a and b where $1 < a < n$ and $1 < b < n$. $a, b \in Z$ which itself is an ID.

n is the smallest integer such that $n \cdot 1 = 0$
$\Rightarrow a \cdot b \cdot 1 = 0$ } it is integral domain so no zero divisor must exist.
$\Rightarrow (a \cdot b) \cdot 1 = 0$

Since D is integral domain, $x \cdot y = 0 \longrightarrow x = 0 \vee y = 0$
Therefore,
$(a \cdot b) = 0$ since $1 \neq 0$

Since $a \neq 0, b \neq 0$ but $a \cdot b = 0$ so a, b are zero divisor

But it is the contradiction that we assumed $\mathbb{Z}$ being an integral domain. That means n can't be composite. So it has to be prime.

Ex: Show that if $m, n \in \mathbb{Z}$ and $a, b \in R$ where R is a ring then $(m \cdot a) * (n \cdot b) = (m * n) \cdot (a * b)$

In a ring, multiple for addition is written as $n \cdot a$ to stand for repeated addition. Let R be a ring.

$$n \in \mathbb{N}, \quad n \cdot a \overset{\text{def}}{=} \underbrace{a + a + \cdots + a}_{n \text{ times}} \quad \forall a \in R$$

This is not same as $n * a$ where $(R, +, *)$ is a ring. n is a completely different object where $n \in R$.

consider $R = (M_2(\mathbb{R}), +, *)$ where $M_2(\mathbb{R})$: all real 2×2 matrices.

For $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$ and $n \in \mathbb{N}$,

$$n \cdot A = \begin{bmatrix} n \cdot a & n \cdot b \\ n \cdot c & n \cdot d \end{bmatrix} \in R \text{ (where } \cdot \text{ operation is in } \mathbb{R})$$

but $n * A$ is not defined as $n \notin M_2(\mathbb{R})$. For $*$ operation n must be a 2×2 real matrix.

$n \cdot a$ and $n * a$ can't be compared if n is not an element of ring and also even if n is element if $*$ operation is different that $\cdot$ operation in $\mathbb{R}$ then it is not comparable.

$n \cdot a$ for repeated addition
$n * a$ for ring multiplication which has nothing to do with repeated addition. Ring multiplication is an operation given as part of the structure which is seperate from addition.

For a general ring element, $n * a$ may be undefined since $n \notin R$. But when the ring has identity element then we can say -

$$1_R + 1_R + \cdots + 1_R = n \cdot 1_R = n$$

So now we can say n also belongs to the ring with identity 1_R.

But be aware that in some rings of identity, we can add 1, n times still it will result to additive identity.

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{n \text{ times}} = 0_R$$

Proof: $\underline{(m \cdot a) \# (n \cdot b) = (m \# n) \cdot (a \# b)}$

where $(R, +, \#)$ is ring and $n \cdot a = \underbrace{a + a + \cdots + a}_{(n \text{ times})}$

$m, n, a, b \in R$ otherwise it doesn't make sense

$m, n \in \mathbb{Z}$ and $m \cdot n$ is the usual multiplication rule.

$$(m \cdot a) \# (n \cdot b)$$

$a \cdot b$

$$= \underbrace{(a + a + \cdots + a)}_{m \text{ times}} \# \underbrace{(b + b + \cdots + b)}_{n \text{ times}}$$

$$= (a + a + \cdots + a) \# b + (a + a + \cdots + a) \# b + \cdots + \underbrace{(a + a + \cdots + a) \# b}_{n \text{ times}}$$

$$= n \cdot \underbrace{(a + a + \cdots + a)}_{m \text{ times}} \# b$$

$$= n \cdot \underbrace{(a \# b + a \# b + \cdots + a \# b)}_{m \text{ times}}$$

$$= (m \cdot n) \cdot (a \# b)$$

$$= (m \# n) \cdot (a \# b)$$

(since $m, n \in R$ so $m \cdot n = m \# n$ are comparable.)