Rings: Basic Definitions and Examples

Kevin James

Definition

1. A ring is a set together with two binary operations called addition and multiplication satisfying the following axioms:
   1. $(R, +)$ is an Abelian group.
   2. $\times$ is associative
   3. The following distributive laws hold:

$$(a+b)c = ac + bc \quad \text{and} \quad a(b+c) = ab + ac.$$

2. The ring R is commutative if multiplication is commutative.
3. The ring R is said to have an identity if there is an element $1_R \in R$ such that

$$1_R \times a = a = a \times 1_R \quad \forall a \in R.$$

Definition

1. A ring is a set together with two binary operations called addition and multiplication satisfying the following axioms:
   1. $(R, +)$ is an Abelian group.
   2. $\times$ is associative
   3. The following distributive laws hold:
   $$(a+b)c = ac + bc \quad \text{and} \quad a(b+c) = ab + ac.$$
2. The ring R is commutative if multiplication is commutative.
3. The ring R is said to have an identity if there is an element $1_R \in R$ such that
$$1_R \times a = a = a \times 1_R \quad \forall a \in R.$$

Definition

A ring with identity in which $0_R \neq 1_R$ is called a division ring if every $0_R \neq a \in R$ has a multiplicative inverse. A commutative division ring is called a field.

Proposition

Let R be a ring. Then,

1. $0_R a = a 0_R = 0_R, \quad \forall a \in R.$
2. $(-a)b = a(-b) = -(ab), \quad \forall a, b \in R.$
3. $(-a)(-b) = ab, \quad \forall a, b \in R.$
4. *if R has an identity then the identity is unique and* $-a = (-1_R)a, \quad \forall a \in R.$

Proposition

Let R be a ring. Then,

1. $0_R a = a 0_R = 0_R, \quad \forall a \in R.$
2. $(-a)b = a(-b) = -(ab), \quad \forall a, b \in R.$
3. $(-a)(-b) = ab, \quad \forall a, b \in R.$
4. *if R has an identity then the identity is unique and* $-a = (-1_R)a, \quad \forall a \in R.$

Definition

Let R be a ring.

1. An element $0_R \neq a \in R$ is called a zero divisor if there is $0_R \neq b \in R$ such that $ab = 0_R$ or $ba = 0_R$.
2. Suppose that R has an identity $1_R \neq 0_R$. An element $u \in R$ is called a unit in R if there is some $v \in R$ such that $uv = vu = 1_R$.
3. The set of units of R is denoted $R^\times$ or R^*. Thus fields contain no zero divisors.

Note

1. R^* is a group under multiplication referred to as the group of units.
2. A zero divisor can never be a unit.

Note

1. R^* is a group under multiplication referred to as the group of units.
2. A zero divisor can never be a unit.

Definition

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

Note

1. R^* is a group under multiplication referred to as the group of units.
2. A zero divisor can never be a unit.

Definition

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

Proposition

Suppose that $a, b, c \in R$ and that R has no zero divisors. If $ab = ac$ then either $a = 0_R$ or $b = c$.

Note

1. R^* is a group under multiplication referred to as the group of units.
2. A zero divisor can never be a unit.

Definition

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

Proposition

Suppose that $a, b, c \in R$ and that R has no zero divisors. If $ab = ac$ then either $a = 0_R$ or $b = c$.

Proposition

A finite integral domain is a field.

Definition

A subring of a ring R is a subgroup of R that is closed under multiplication.

Definition

A subring of a ring R is a subgroup of R that is closed under multiplication.