Definition: Inverse Element

An **inverse element** of an element under a Binary Operation is another element that, when combined with the original, yields the Identity Element.

Formal Definition

Let $(S, *)$ be a set with a binary operation $*$ and identity element e. For an element $a \in S$:

Left Inverse

An element $b \in S$ is a **left inverse** of a if:

$$b * a = e$$

Right Inverse

An element $b \in S$ is a **right inverse** of a if:

$$a * b = e$$

Two-Sided Inverse (or simply Inverse)

An element b is an **inverse** of a if it is both a left and right inverse:

$$b * a = a * b = e$$

We denote the inverse of a as a^{-1}.

Uniqueness in Groups

In a Group (where the operation is associative), if an element has both a left inverse and a right inverse, they are equal and unique.

Proof: Let l be a left inverse and r be a right inverse of a: - $l = l * e = l * (a * r) = (l * a) * r = e * r = r$

Examples

Arithmetic

- **Addition on** $\mathbb{R}$: The inverse of a is $-a$
  - $a + (-a) = (-a) + a = 0$
- **Multiplication on** $\mathbb{R} \setminus \{0\}$: The inverse of a is $\frac{1}{a}$
  - $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$

Matrices

- **Addition**: The inverse of matrix $\mathbf{A}$ is $-\mathbf{A}$
- **Multiplication**: For invertible matrix $\mathbf{A}$, the inverse is $\mathbf{A}^{-1}$
    - $\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}$

Functions

- For bijective function $f : X \to Y$, the inverse is $f^{-1} : Y \to X$
- $(f \circ f^{-1})(y) = y$ and $(f^{-1} \circ f)(x) = x$

Modular Arithmetic

- In $\mathbb{Z}_n$ under addition: inverse of a is $n - a$
- In $\mathbb{Z}_n^*$ under multiplication: inverse exists iff $\gcd(a, n) = 1$

Properties

1. **Involution**: $(a^{-1})^{-1} = a$
2. **Anti-homomorphism**: $(a * b)^{-1} = b^{-1} * a^{-1}$ (note the order reversal)
3. **Identity is self-inverse**: $e^{-1} = e$

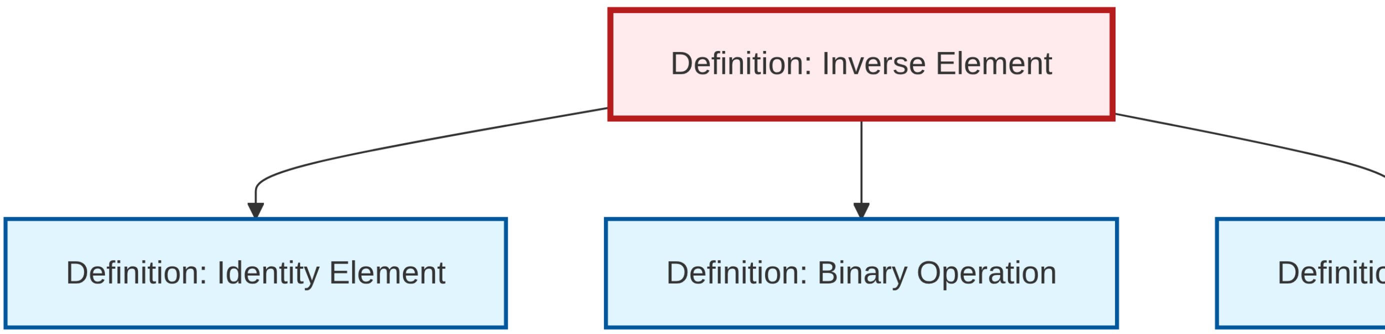
Non-Examples

- In $(\mathbb{Z}, \cdot)$: Only 1 and -1 have multiplicative inverses
- In $(\mathbb{N}, +)$: No element except 0 has an additive inverse
- Zero has no multiplicative inverse in any ring

Related Concepts

- **Invertible element**: An element that has an inverse
- **Unit**: In ring theory, an element with multiplicative inverse
- Group: A monoid where every element has an inverse
- **Quasi-inverse**: Weaker notions in semigroup theory

Dependency Graph



Local dependency graph