

## Example: Finite Field

### Example: The Finite Field $\mathbb{F}_5$

The integers modulo 5 form a [Field](#), denoted  $\mathbb{F}_5$  or  $\mathbb{Z}/5\mathbb{Z}$ .

#### Elements and Operations

The field  $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$  with operations:

##### Addition Table (mod 5)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

##### Multiplication Table (mod 5)

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

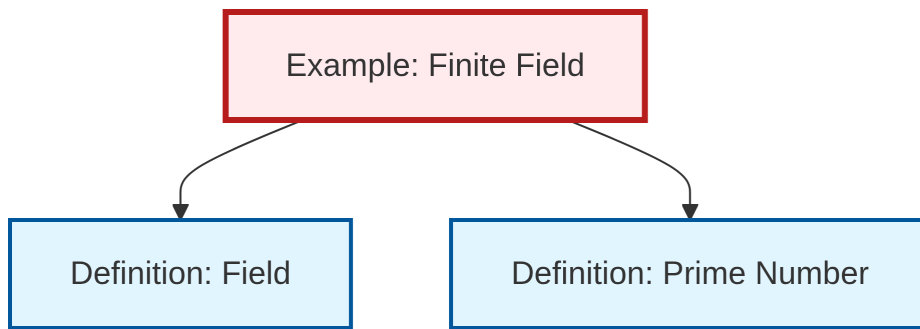
#### Verification

- **Additive identity:** 0
- **Multiplicative identity:** 1
- **Additive inverses:**  $-1 = 4$ ,  $-2 = 3$ ,  $-3 = 2$ ,  $-4 = 1$
- **Multiplicative inverses:**  $1^{-1} = 1$ ,  $2^{-1} = 3$ ,  $3^{-1} = 2$ ,  $4^{-1} = 4$

#### General Result

For any [Prime Number](#)  $p$ , the set  $\mathbb{F}_p = \{0, 1, \dots, p-1\}$  with arithmetic modulo  $p$  forms a field. This works because: - Every non-zero element has a multiplicative inverse (by Fermat's Little Theorem) - There are no zero divisors when  $p$  is prime

## Dependency Graph



Local dependency graph