Binary operation:

Given a set, we assign to every ordered pair $(a, b) \in S \times S$ a unique element $c \in S$.

Special features:

Associative law: For every $a, b, c \in S$, we have $a(bc) = (ab)c$.

Commutative law: For every $a, b \in S$, we have $ab = ba$.

Identity: $e \in S$ satisfying $ea = ae = a$ for every $a \in S$.

Inverse: If S has an identity e, then the inverse of $a \in S$ is a^{-1} satisfying $aa^{-1} = a^{-1}a = e$.

(Refinement: If $ab = e$, then b is a *right* inverse of a, and $ca = e$ means that c is a *left* inverse of a.)

See Problem 18 about some important properties of identity and inverses.

Ring:

A set R with an addition and a multiplication where both are associative; addition is commutative; the two operations are connected by the *distributive* laws $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$; there is an identity for addition called zero; and every element has an additive inverse called its negative. (We have to prescribe both distributive laws as multiplication is not necessarily commutative.)

Special features:

A *field* is a ring where multiplication satisfies the following further properties: it is commutative; it has an identity; and every non-zero element has an inverse.

In a ring, an element $a \neq 0$ is a left *zero-divisor* if there exists some $b \neq 0$ satisfying $ab = 0$.

A field is zero-divisor free. See Problem 22 for the relation of zero-divisors and multiplicative inverses.

A commutative ring with identity and without zero divisors is called an *integral domain* (ID).

An invertible element can be called also a *unit*. Hence, in a field, every non-zero element is a unit.

Some important rings:

$\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ are fields.

The rings $\mathbf{Z}$ of the integers and $\mathbf{R}[x]$ of the polynomials with real coefficients are commutative, zero-divisor free, and have identities, so they are integral domains. Units: in $\mathbf{Z}$, only 1 and -1 have (multiplicative) inverses, and in $\mathbf{R}[x]$, exactly the non-zero constants are invertible (the same holds for polynomials over any field, but not for $\mathbf{Z}[x]$).

The ring $F^{n\times n}$ of square matrices over a field F is non-commutative and has an identity. A non-zero matrix has an inverse iff its determinant is not 0, and is a two-sided zero-divisor iff its determinant is 0.

The ring $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$ of the remainders obtained from the division algorithm by n is commutative and has an identity. A non-zero element c has an inverse iff $(c, n) = 1$, and is a zero-divisor iff $(c, n) > 1$.

This implies that $\mathbf{Z}_n$ is a field iff n is a prime.

Later we shall characterize all finite fields.