Definition of a ring

A **ring** is a set R with binary operations $+$ and $\cdot$, satisfying the following axioms.

Part 1: The first four axioms establish that $+$ and $-$ work as they do with real numbers.

(+ assoc) For all $a, b, c \in R$, $(a+b)+c = a+(b+c)$.

(+ comm) For all $a, b \in R$, $a+b = b+a$.

(Zero) There exists $0 \in R$ such that for all $a \in R$, $a+0 = a$.

(Neg) For all $a \in R$, there exists $(-a) \in R$ such that $a+(-a) = 0$.

Rings, part 2

Part 2: The next three axioms ensure that multiplication works as it does for real numbers, including interaction with $+$, except that we are not guaranteed that $a \cdot b = b \cdot a$.

- ($\cdot$ assoc) For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (Unit) There exists $1 \in R$ s.t. for all $a \in R$, $a \cdot 1 = 1 \cdot a = a$.
- (Distrib) For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

As we'll see later, we allow the possibility that $ab \neq ba$ to expand the definition of ring to sets of matrices.

Rings we have seen so far include $\mathbf{Z}$, $\mathbf{R}$, and $\mathbf{C}$.
$\mathbf{N}$ is not a ring (why not?).

Commutative rings and fields

A **commutative ring** R is a ring that also satisfies the axiom:

($\cdot$ comm) For all $a, b \in R$, $a \cdot b = b \cdot a$.

All rings we have seen so far are commutative; we will later briefly see a non-commutative example (again, matrices).

A **field** is a commutative ring F that also satisfies the axiom:

(Reciprocals) For all $a \neq 0$ in F, there exists $(1/a) \in F$ such that $a \cdot (1/a) = 1$.

$\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$ are fields; $\mathbf{N}$ and $\mathbf{Z}$ are commutative rings, but not fields.