



## Why

We generalize the algebraic structure of addition and multiplication over the integers.<sup>1</sup>

## Definition

A *ring* (or *ring with identity*)  $(A, f, g)$  is a set  $A$  and two operations on  $A$  satisfying the following set of conditions.

(A) (i)  $f$  is associative. (ii)  $f$  is *commutative*, (iii)  $A$  has an identity for  $f$  (i.e., is  $e \in A$  with  $f(a, e) = f(e, a) = a$  for all  $a \in A$ ) (iv)  $A$  has inverse elements for  $f$  (i.e., for any  $a \in A$ , there is  $\tilde{a}$  satisfying  $f(a, \tilde{a}) = f(\tilde{a}, a) = e$ )

(B) (i)  $g$  is associative; (ii)  $A$  has an identity element for  $g$  (i.e., there is  $\tilde{e} \in A$  satisfying  $g(a, \tilde{e}) = g(\tilde{e}, a) = a$ )

(C) (i)  $g$  left distributes:  $g(f(a, b), c) = f(g(a, c), g(b, c))$ ; (ii)  $g$  right distributes:  $g(c, f(a, b)) = f(g(c, a), g(c, b))$ .

Conditions (A) concern  $f$ , conditions (B) concern  $g$ , and conditions (C) relate the two. Define  $\psi : \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$  by  $\psi(a, b) = a + b$  and  $\pi : \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}$  by  $\pi(a, b) = a \cdot b$ . We have defined a ring so that  $(\mathbf{Z}, \psi, \pi)$  is one. The element referred to in (A.2) is  $0 \in \mathbf{Z}$ , so we refer to this element in any ring as the *additive identity*. That referred to (A.3) is  $1 \in \mathbf{Z}$ , so we refer to this element in any ring as the *multiplicative identity*. We refer to the elements mentioned in (A.4) as *additive inverses*. We call to  $f$  *ring addition* and  $g$  *ring multiplication*. Although integer products are commutative, we have not required this aspect (future editions will elaborate).

---

<sup>1</sup>Future editions will likely modify this sheet, and give a genetic treatment involving the solution of polynomial equations by Galois.

## Notation

The notation commonly adopted in discussing rings relies on analogy with the set of integers  $\mathbf{Z}$ . We denote the ring addition by  $+$  and ring multiplication by  $\cdot$ . Moreover, we denote the ring's additive identity by  $0$  and the ring's multiplicative identity by  $1$ . Finally, we denote the additive inverse of  $a \in A$  by  $-a$ .

Rewriting the conditions (A), (B), (C) in this notation gives familiar-looking relations, from when the objects involved were integers. (A) (1)  $a + (b + c) = (a + b) + c$ ; (2)  $a + b = b + a$ ; (3)  $a + 0 = 0 + a = a$ ; (4)  $a + (-a) = 0$ . (B) (1)  $a(bc) = (ab)c$ ; (2)  $1a = a1 = a$ . (C) (1)  $(a + b)c = ac + bc$ ; (2)  $c(a + b) = ca + cb$ .

## Immediate consequences

We need not require that  $0x = 0$ , because we can deduce it:

$$0x + x = (0 + 1)x = 1x = x.$$

Similarly,  $(-a)b = -(ab)$  since

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

Other familiar relations among the integers, e.g.  $(-a)(-b) = ab$ , may be deduced.

