



Why

We generalize the algebraic structure of *addition* and *multiplication* over the integers.¹

Definition

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

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

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

(C) (i) g *left distributes*:

$$g(f(x, y), \alpha) = f(g(\alpha, x), g(\alpha, y)) \quad \text{for all } x, y, \alpha \in R$$

(ii) g *right distributes*:

$$g(\alpha, f(x, y)) = f(g(\alpha, x), g(\alpha, y)) \quad \text{for all } x, y, \alpha \in R$$

Conditions (A) concern f , conditions (B) concern g , and conditions (C) relate the two.

Clearly, \mathbf{Z} with addition and multiplication is a ring. 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*.

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

A ring which for which multiplication is commutative is called a *commutative ring*. Note that a ring is *always* commutative with respect to addition, here the term commutative refers to multiplication. A ring for which there are inverse elements, excepting 0, is called a *division ring*).

Of course, the integers form a ring with the usual notion of addition and multiplication. For another trivial example, consider $\{0\}$ with $0+0 = 0$ and $0 \cdot 0 = 0$; this is called the *zero ring* (any ring isomorphic to this one is called a *trivial ring* or *zero ring*).

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.

