using the relations

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

(where the real number coefficients commute with i, j and k). For example,

$$\begin{aligned}(1+i+2j)(j+k) &= 1(j+k) + i(j+k) + 2j(j+k) = j + k + ij + ik + 2j^2 + 2jk \\ &= j + k + k + (-j) + 2(-1) + 2(i) = -2 + 2i + 2k.\end{aligned}$$

The fact that $\mathbb{H}$ is a ring may be proved by a straightforward, albeit lengthy, check of the axioms (associativity of multiplication is particularly tedious). The Hamilton Quaternions are a noncommutative ring with identity ($1 = 1+0i+0j+0k$). Similarly, one can define the ring of *rational* Hamilton Quaternions by taking a, b, c, d to be rational numbers above. Both the real and rational Hamilton Quaternions are *division rings*, where inverses of nonzero elements are given by

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}.$$

(6) One important class of rings is obtained by considering rings of functions. Let X be any nonempty set and let A be any ring. The collection, R, of all (set) functions $f : X \to A$ is a ring under the usual definition of pointwise addition and multiplication of functions: $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. Each ring axiom for R follows directly from the corresponding axiom for A. The ring R is commutative if and only if A is commutative and R has a 1 if and only if A has a 1 (in which case the 1 of R is necessarily the constant function 1 on X).

If X and A have more structure, we may form other rings of functions which respect those structures. For instance, if A is the ring of real numbers $\mathbb{R}$ and X is the closed interval $[0, 1]$ in $\mathbb{R}$ we may form the ring of all *continuous* functions from $[0, 1]$ to $\mathbb{R}$ (here we need basic limit theorems to guarantee that sums and products of continuous functions are continuous) — this is a commutative ring with 1.

(7) An example of a ring which does not have an identity is the ring $2\mathbb{Z}$ of even integers under usual addition and multiplication of integers (the sum and product of even integers is an even integer).

Another example which arises naturally in analysis is constructed as follows. A function $f : \mathbb{R} \to \mathbb{R}$ is said to have *compact support* if there are real numbers a, b (depending on f) such that $f(x) = 0$ for all $x \notin [a, b]$ (i.e., f is zero outside some bounded interval). The set of all functions $f : \mathbb{R} \to \mathbb{R}$ with compact support is a commutative ring without identity (since an identity could not have compact support). Similarly, the set of all continuous functions $f : \mathbb{R} \to \mathbb{R}$ with compact support is a commutative ring without identity.

In the next section we give three important ways of constructing "larger" rings from a given ring (analogous to Example 6 above) and thus greatly expand our list of examples. Before doing so we mention some basic properties of arbitrary rings. The ring $\mathbb{Z}$ is a good example to keep in mind, although this ring has a good deal more algebraic structure than a general ring (for example, it is commutative and has an identity). Nonetheless, its basic arithmetic holds for general rings as the following result shows.

Proposition 1. Let R be a ring. Then

(1) $0a = a0 = 0$ for all $a \in R$.

(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$ (recall $-a$ is the additive inverse of a).

(3) $(-a)(-b) = ab$ for all $a, b \in R$.

(4) if R has an identity 1, then the identity is unique and $-a = (-1)a$.

Proof: These all follow from the distributive laws and cancellation in the additive group R. For example, (1) follows from $0a = (0 + 0)a = 0a + 0a$. The equality $(-a)b = -(ab)$ in (2) follows from $ab + (-a)b = (a + (-a))b = 0b = 0$. The rest follow similarly and are left to the reader.

This proposition shows that because of the distributive laws the additive and multiplicative structures of a ring behave well with respect to one another, just as in the familiar example of the integers.

Unlike the integers, however, general rings may possess many elements that have multiplicative inverses or may have nonzero elements a and b whose product is zero. These two properties of elements, which relate to the multiplicative structure of a ring, are given special names.

Definition. Let R be a ring.

(1) A nonzero element a of R is called a *zero divisor* if there is a nonzero element b in R such that either $ab = 0$ or $ba = 0$.

(2) Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $uv = vu = 1$. The set of units in R is denoted $R^\times$.

It is easy to see that the units in a ring R form a group under multiplication so $R^\times$ will be referred to as the *group of units* of R. In this terminology a *field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F - \{0\}$.*

Observe that *a zero divisor can never be a unit*. Suppose for example that a is a unit in R and that $ab = 0$ for some nonzero b in R. Then $va = 1$ for some $v \in R$, so $b = 1b = (va)b = v(ab) = v0 = 0$, a contradiction. Similarly, if $ba = 0$ for some nonzero b then a cannot be a unit.

This shows in particular that fields contain no zero divisors.

Examples

(1) The ring $\mathbb{Z}$ of integers has no zero divisors and its only units are ± 1, i.e., $\mathbb{Z}^\times = \{\pm 1\}$. Note that every nonzero integer has an inverse in the *larger ring* $\mathbb{Q}$, so the property of being a unit depends on the ring in which an element is viewed.

(2) Let n be an integer ≥ 2. In the ring $\mathbb{Z}/n\mathbb{Z}$ the elements $\bar{u}$ for which u and n are relatively prime are units (we shall prove this in the next chapter). Thus our use of the notation $(\mathbb{Z}/n\mathbb{Z})^\times$ is consistent with the definition of the group of units in an arbitrary ring.

If, on the other hand, a is a nonzero integer and a is not relatively prime to n then we show that $\bar{a}$ is a zero divisor in $\mathbb{Z}/n\mathbb{Z}$. To see this let d be the g.c.d. of a and n and let $b = \frac{n}{d}$. By assumption $d > 1$ so $0 < b < n$, i.e., $\bar{b} \neq \bar{0}$. But by construction n

divides ab, that is, $\overline{ab} = \bar{0}$ in $\mathbb{Z}/n\mathbb{Z}$. This shows that *every nonzero element of* $\mathbb{Z}/n\mathbb{Z}$ *is either a unit or a zero divisor*. Furthermore, every nonzero element is a unit if and only if every integer a in the range $0 < a < n$ is relatively prime to n. This happens if and only if n is a prime, i.e., $\mathbb{Z}/n\mathbb{Z}$ *is a field if and only if* n *is a prime.*

(3) If R is the ring of all functions from the closed interval [0,1] to $\mathbb{R}$ then the units of R are the functions that are not zero at any point (for such f its inverse is the function $\frac{1}{f}$). If f is not a unit and not zero then f is a zero divisor because if we define

$$g(x) = \begin{cases} 0, & \text{if } f(x) \neq 0 \\ 1, & \text{if } f(x) = 0 \end{cases}$$

then g is not the zero function but $f(x)g(x) = 0$ for all x.

(4) If R is the ring of all *continuous* functions from the closed interval [0,1] to $\mathbb{R}$ then the units of R are still the functions that are not zero at any point, but now there are functions that are neither units nor zero divisors. For instance, $f(x) = x - \frac{1}{2}$ has only one zero (at $x = \frac{1}{2}$) so f is not a unit. On the other hand, if $gf = 0$ then g must be zero for all $x \neq \frac{1}{2}$, and the only *continuous* function with this property is the zero function. Hence f is neither a unit nor a zero divisor. Similarly, no function with only a finite (or countable) number of zeros on [0,1] is a zero divisor. This ring also contains many zero divisors. For instance let

$$f(x) = \begin{cases} 0, & 0 \leq x \leq \frac{1}{2} \\ x - \frac{1}{2}, & \frac{1}{2} \leq x \leq 1 \end{cases}$$

and let $g(x) = f(1 - x)$. Then f and g are nonzero continuous functions whose product is the zero function.

(5) Let D be a rational number that is not a perfect square in $\mathbb{Q}$ and define

$$\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$$

as a subset of $\mathbb{C}$. This set is clearly closed under subtraction, and the identity $(a + b\sqrt{D})(c + d\sqrt{D}) = (ac + bdD) + (ad + bc)\sqrt{D}$ shows that it is also closed under multiplication. Hence $\mathbb{Q}(\sqrt{D})$ is a subring of $\mathbb{C}$ (even a subring of $\mathbb{R}$ if $D > 0$), so in particular is a commutative ring with identity. It is easy to show that the assumption that D is not a square implies that every element of $\mathbb{Q}(\sqrt{D})$ may be written uniquely in the form $a + b\sqrt{D}$. This assumption also implies that if a and b are not both 0 then $a^2 - Db^2$ is nonzero, and since $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$ it follows that if $a + b\sqrt{D} \neq 0$ (i.e., one of a or b is nonzero) then $\dfrac{a - b\sqrt{D}}{a^2 - Db^2}$ is the inverse of $a + b\sqrt{D}$ in $\mathbb{Q}(\sqrt{D})$. This shows that every nonzero element in this commutative ring is a unit, i.e., $\mathbb{Q}(\sqrt{D})$ is a field (called a *quadratic field*, cf. Section 13.2).

The rational number D may be written $D = f^2 D'$ for some rational number f and a unique integer D' where D' is not divisible by the square of any integer greater than 1, i.e., D' is either -1 or ± 1 times the product of distinct primes in $\mathbb{Z}$ (for example, $8/5 = (2/5)^2 \cdot 10$). Call D' the *squarefree part* of D. Then $\sqrt{D} = f\sqrt{D'}$, and so $\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'})$. Thus *there is no loss in assuming that* D *is a squarefree integer* (i.e., $f = 1$) *in the definition of the quadratic field* $\mathbb{Q}(\sqrt{D})$.