# 3. The players: rings, fields, etc.



Here we introduce some basic terminology, and give a sample of a modern construction of a *universal object*, namely a polynomial ring in one variable.

---

## 1. *Rings, fields*

The idea of **ring** generalizes the idea of *collection of numbers*, among other things, so maybe it is a little more intuitive than the idea of **group**. A **ring** $R$ is a set with two operations, $+$ and $\cdot$, and with a special element 0 (**additive identity**) with most of the usual properties we expect or demand of *addition* and *multiplication*:
• $R$ with its addition and with 0 is an abelian group. [1]
• The multiplication is *associative*: $a(bc) = (ab)c$ for all $a, b, c \in R$.
• The multiplication and addition have left and right **distributive** properties: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Often the multiplication is written just as juxtaposition

$$ab = a \cdot b$$

Very often, a particular ring has some additional special features or properties:

• If there is an element 1 in a ring with $1 \cdot a = a \cdot 1$ for all $a \in R$, then 1 is said to be **the (multiplicative)**

[1] This is a compressed way to say that 0 behaves as an additive identity, that there are additive inverses, and that addition is associative.

**identity** or **the unit** [2] in the ring, and the ring is said to **have an identity** or **have a unit** or be a **ring with unit**. [3]

• If $ab = ba$ for all $a, b$ in a ring $R$, then the ring is a **commutative ring**. That is, a ring is called *commutative* if and only if the *multiplication* is commutative.

• In a ring $R$ with 1, for a given element $a \in R$, if there is $a^{-1} \in R$ so that $a \cdot a^{-1} = 1$ and $a^{-1} \cdot a = 1$, then $a^{-1}$ is said to be a **multiplicative inverse** for $a$. If $a \in R$ *has* a multiplicative inverse, then $a$ is called **a unit** [4] in $R$. The collection of all units in a ring $R$ is denoted $R^\times$ and is called **the group of units in** $R$. [5]

• A commutative ring in which every nonzero element is a *unit* is a **field**.

• A not-necessarily commutative ring in which every nonzero element is a unit is a **division ring**.

• In a ring $R$ an element $r$ so that $r \cdot s = 0$ or $s \cdot r = 0$ for some nonzero $s \in R$ is called a **zero divisor**. [6] A commutative ring *without* nonzero zero-divisors is an **integral domain**.

• A commutative ring $R$ has the **cancellation property** if, for any $r \neq 0$ in $R$, if $rx = ry$ for $x, y \in R$, then $x = y$.

If we take a ring $R$ with 0 and with its addition, forgetting the multiplication in $R$, then we get an abelian group, called **the additive group of** $R$. And the group of units $R^\times$ is a (possibly non-abelian) group.

[1.0.1] **Example:** The integers $\mathbb{Z}$ with usual addition and multiplication form a ring. This ring is certainly *commutative* and has a multiplicative identity 1. The group of units $\mathbb{Z}^\times$ is just $\{\pm 1\}$. This ring is an integral domain. The *even* integers $2\mathbb{Z}$ with the usual addition and multiplication form a commutative ring *without* unit. Just as this example suggests, sometimes the lack of a unit in a ring is somewhat artificial, because there is a larger ring it sits inside which *does* have a unit. There are no units in $2\mathbb{Z}$.

[2] Sometimes the word *unity* is used in place of *unit* for the special element 1, but this cannot be relied upon, and in any case does not fully succeed in disambiguating the terminology.

[3] We also demand that $1 \neq 0$ in a ring, if there is a 1.

[4] Yes, this usage is partly in conflict with the terminology for a special element 1.

[5] It is almost immediate that $R^\times$ truly is a group.

[6] The question of whether or not 0 should by convention be counted as a zero divisor has no clear answer.

**[1.0.2] Example:** The integers mod $m$, denoted $\mathbb{Z}/m$, form a commutative ring with identity. It is not hard to verify that addition and multiplication are well-defined. *As the notation suggests,* the group of units is $\mathbb{Z}/m^\times$. [7]

**[1.0.3] Example:** The ring $\mathbb{Z}/p$ of integers mod $p$ is a *field* for $p$ prime, since all non-zero residue classes have multiplicative inverses. [8] The group of units is $(\mathbb{Z}/p)^\times$. For $n$ non-prime, $\mathbb{Z}/n$ is definitely not a field, because a proper factorization $n = ab$ exhibits non-zero zero divisors.

**[1.0.4] Example:** Generally, a finite field with $q$ elements is denoted $\mathbb{F}_q$. We will see later that, up to isomorphism, there is at most one finite field with a given number of elements, and, in fact, none unless that number is the power of a prime.

**[1.0.5] Example:** The collection of $n$-by-$n$ matrices (for fixed $n$) with entries in a ring $R$ is a ring, with the usual matrix addition and multiplication. [9] Except for the silly case $n = 1$, rings of matrices over commutative rings $R$ are *non-commutative*. The group of units, meaning matrices with an inverse of the same form, is the group $GL(n, R)$, the **general linear group** of size $n$ over $R$.

**[1.0.6] Example:** The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are all examples of *fields*, because all their nonzero elements have multiplicative inverses. The integers $\mathbb{Z}$ do not form a field.

There are some things about the behavior of rings which we might accidentally take for granted.

Let $R$ be a ring.
• *Uniqueness of* 0 *additive identity:* From the analogous discussion at the beginning of group theory, we know that there is exactly one element $z = 0$ with the property that $r + z = r$ for all $r$ in $R$. And there is exactly one additive inverse to any $r \in R$. And for $r \in R$, we have $-(-r) = r$. Similarly, if $R$ has a unit 1, then, using the group $R^\times$, we deduce uniqueness of 1, and uniqueness of multiplicative inverses.

The following items are slightly subtler than the things above, involving the interaction of the multiplication and addition. Still, there are no surprises. [10]

Let $R$ be a ring.
• For any $r \in R$, $0 \cdot r = r \cdot 0 = 0$. [11]
• Suppose that there is a 1 in $R$. Let $-1$ be the additive inverse of 1. Then for any $r \in R$ we have $(-1) \cdot r = r \cdot (-1) = -r$, where as usual $-r$ denotes the additive inverse of $r$.
• Let $-x, -y$ be the additive inverses of $x, y \in R$. Then $(-x) \cdot (-y) = xy$.

*Proof:* Let $r \in R$. Then

$$\begin{aligned} 0 \cdot r &= (0+0) \cdot r \qquad (\text{since } 0+0=0) \\ &= 0 \cdot r + 0 \cdot r \qquad (\text{distributivity}) \end{aligned}$$

Then, adding $-(0 \cdot r)$ to both sides, we have

$$0 = 0 \cdot r - 0 \cdot r = 0 \cdot r + 0 \cdot r - 0 \cdot r = 0 \cdot r + 0 = 0 \cdot r$$

[7] Yes, we used the group-of-units notation in this case before we had introduced the terminology.

[8] Again, for a residue class represented by $x$ relatively prime to $p$, there are integers $r, s$ such that $rx + yp = \gcd(x, p) = 1$, and then the residue class of $r$ is a multiplicative inverse to the residue class of $x$.

[9] Verification of the ring axioms is not terrifically interesting, but is worth doing once.

[10] No surprises except perhaps that these things do follow from the innocent-seeming ring axioms.

[11] One can easily take the viewpoint that this universal assertion has very little *semantic content.*

That is, $0 \cdot r$. The proof that $r \cdot 0 = 0$ is identical.

To show that $(-1)r$ is the additive inverse of $r$, which by now we know is unique, we check that

$$r + (-1)r = 0$$

We have

$$r + (-1)r = 1 \cdot r + (-1) \cdot r = (1 - 1) \cdot r = 0 \cdot r = 0$$

using the result we just $0 \cdot r = 0$.

To show that $(-x)(-y) = xy$, prove that $(-x)(-y) = -(-(xy))$, since $-(-r) = r$. We claim that $-(xy) = (-x)y$: this follows from

$$(-x)y + xy = (-x + x)y = 0 \cdot y = 0$$

Thus, we want to show

$$(-x)(-y) + (-x)y = 0$$

Indeed,

$$(-x)(-y) + (-x)y = (-x)(-y + y) = (-x) \cdot 0 = 0$$

using $r \cdot 0 = 0$ verified above. Thus, $(-x)(-y) = xy$. ///

An **idempotent** element of a ring $R$ is an element $e$ such that

$$e^2 = e$$

A **nilpotent** element is an element $z$ such that for some positive integer $n$

$$z^n = 0_R$$

---

# 2. *Ring homomorphisms*

Ring homomorphisms are maps from one ring to another which respect the ring structures.

Precisely, a **ring homomorphism** $f : R \to S$ from one ring $R$ to another ring $S$ is a map such that for all $r, r'$ in $R$

$$\begin{array}{rcl} f(r + r') & = & f(r) + f(r') \\ f(rr') & = & f(r)\, f(r') \end{array}$$

That is, $f$ *preserves* or *respects* both addition and multiplication. [12] A ring homomorphism which has a two-sided inverse homomorphism is an **isomorphism**. If a ring homomorphism is a bijection, it is an isomorphism. [13]

[12] We do not make an attempt to use different notations for the addition and multiplication in the two different rings $R$ and $S$ in this definition, or in subsequent discussions. Context should suffice to distinguish the two operations.

[13] Since a bijective ring homomorphism has an inverse map which is a ring homomorphism, one could *define* an isomorphism to be a bijective homomorphism. However, in some other scenarios bijectivity of certain types of homomorphisms is *not* sufficient to assure that there is an inverse map of the same sort. The easiest example of such failure may be among continuous maps among topological spaces. For example, let $X = \{0, 1\}$ with the *indiscrete topology*, in which only the whole set and the empty set are open. Let $Y = \{0, 1\}$ with the *discrete* topology, in which all subsets are open. Then the identity map $X \longrightarrow Y$ is continuous, but its inverse is not. That is, the map is a continuous bijection, but its inverse is not continuous.

The **kernel** of a ring homomorphism $f : R \to S$ is

$$\ker f = \{r \in R : f(r) = 0\}$$

[2.0.1] **Example:** The most basic worthwhile example of a ring homomorphism is

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/n$$

given by

$$f(x) = x + n\mathbb{Z}$$

The assertion that this $f$ is a ring homomorphism is the combination of the two assertions

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z}) = (x + y) + n\mathbb{Z}$$

and

$$(x + n\mathbb{Z}) \cdot (y + n\mathbb{Z}) + n\mathbb{Z} = (x \cdot y) + n\mathbb{Z}$$

Even though it is slightly misleading, this homomorphism is called the **reduction mod** $m$ **homomorphism**.

[2.0.2] **Proposition:** Let $f : R \to S$ be a ring homomorphism. Let $0_R, 0_S$ be the additive identities in $R, S$, respectively. Then $f(0_R) = 0_S$.

*Proof:* This is a corollary of the analogous result for groups. ///

[2.0.3] **Proposition:** Let $f : R \longrightarrow S$ be a *surjective* ring homomorphism. Suppose that $R$ has a multiplicative identity $1_R$. Then $S$ has a multiplicative identity $1_S$ and

$$f(1_R) = 1_S$$

[2.0.4] **Remark:** Notice that, unlike the discussion about the additive identity, now we need the further hypothesis of surjectivity.

*Proof:* Given $s \in S$, let $r \in R$ be such that $f(r) = s$. Then

$$f(1_R) \cdot s = f(1_R) \cdot f(r) = f(1_R \cdot r) = f(r) = s$$

Thus, $f(1_R)$ behaves like a unit in $S$. By the *uniqueness* of units, $f(1_R) = 1_S$. ///

[2.0.5] **Example:** The image of a multiplicative identity $1_R$ under a ring homomorphism $f : R \to S$ is not necessarily the multiplicative identity $1_S$ of $S$. For example, define a ring homomorphism

$$f : \mathbb{Q} \to S$$

from the rational numbers $\mathbb{Q}$ to the ring $S$ of 2-by-2 rational matrices by

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

Then the image of 1 is

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

which is not the the multiplicative identity

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

in $S$. As another example, let $R = \mathbb{Z}/3$ and $S = \mathbb{Z}/6$, and define $f : R \longrightarrow S$ by

$$f(r \bmod 3) = 4r \bmod 6$$

(This is well-defined, and is a homomorphism.) The essential feature is that

$$4 \cdot 4 = 4 \bmod 6$$

Then

$$f(x \cdot y) = 4(x \cdot y) = (4 \cdot 4)(x \cdot y) = (4x) \cdot (4y) = f(x) \cdot f(y)$$

But $f(1) = 4 \neq 1 \bmod 6$.

---

# 3. *Vector spaces, modules, algebras*

Let $k$ be a field. A **$k$-vectorspace** $V$ is an abelian group $V$ (with operation written additively, referred to as **vector addition**) and a **scalar multiplication**

$$k \times V \longrightarrow V$$

written

$$\alpha \times v \longrightarrow \alpha \cdot v = \alpha v$$

such that, for $\alpha, \beta \in k$ and $v, v' \in V$,

$$\begin{array}{lrcl} \text{(Distributivity)} & \alpha \cdot (v + v') & = & \alpha \cdot v + \alpha \cdot v' \\ \text{(Distributivity)} & (\alpha + \beta) \cdot v & = & \alpha \cdot v + \beta \cdot v \\ \text{(Associativity)} & (\alpha \cdot \beta) \cdot v & = & \alpha \cdot (\beta \cdot v) \\ & 1 \cdot v & = & v \end{array}$$

[3.0.1] **Remark:** The requirement that $1 \cdot v = v$ does not follow from the other requirements. [14] By contrast, the zero element 0 in a field does reliably annihilate any vectorspace element $v$:

$$0_V = -(0 \cdot v) + 0 \cdot v = -(0 \cdot v) + (0 + 0) \cdot v = -(0 \cdot v) + 0 \cdot v + 0 \cdot v = 0 \cdot v$$

A $k$-vector **subspace** $W$ of a $k$-vectorspace $V$ is an additive subgroup closed under scalar multiplication.

A **$k$-linear combination** of vectors $v_1, \ldots, v_n$ in a $k$-vectorspace $V$ is any vector of the form

$$\alpha_1 v_1 + \ldots + \alpha_n v_n$$

with $\alpha_i \in k$ and $v_i \in V$. Vectors $v_1, \ldots, v_n$ are **linearly dependent** if there is a linear combination of them which is 0, yet not all coefficients are 0. They are **linearly independent** if they are not linearly *dependent*. [15]

---

[14] Sometimes the requirement that $1 \cdot v = v$ is given an unfortunate name, such as *unitary* property (in conflict with other usage), or *unital* property, which conjures up no clear image. The point is that the terminology is unpredictable.

[15] We will certainly continue this discussion of elementary linear algebra shortly, discussing the usual standard notions.

The pedestrian example of a vector space is, for fixed natural number $n$, the collection $k^n$ of ordered $n$-tuples of elements of $k$ with component-wise vector addition and component-wise scalar multiplication.

A **$k$-linear map** $T : V \longrightarrow W$ from one $k$-vectorspace $V$ to another $W$ is a homomorphism of abelian groups $T : V \longrightarrow W$

$$T(v + v') = Tv + Tv'$$

also respecting the scalar multiplication: for $\alpha \in k$

$$T(\alpha \cdot v) = \alpha \cdot Tv$$

The collection of all $k$-linear maps from $V$ to $W$ is denoted

$$\mathrm{Hom}_k(V, W) = \{ \text{ all } k\text{-linear maps from } V \text{ to } W\}$$

When $V = W$, write

$$\mathrm{End}_k(V, V) = \mathrm{End}_k(V)$$

This is the **ring of $k$-linear endomorphisms** of $V$.

The **kernel** $\ker T$ of a $k$-linear map $T : V \longrightarrow W$ is

$$\ker T = \{v \in V : Tv = 0\}$$

Let $R$ be a ring. An **$R$-module** [16] $M$ is an abelian group $M$ (with operation written additively) and a **multiplication**

$$R \times M \longrightarrow M$$

written

$$r \times m \longrightarrow r \cdot m = rm$$

such that, for $r, r' \in R$ and $m, m' \in M$

$$\begin{array}{lrcl} \text{(Distributivity)} & r \cdot (m + m') & = & r \cdot m + e \cdot m' \\ \text{(Distributivity)} & (r + r') \cdot m & = & r \cdot m + r' \cdot m \\ \text{(Associativity)} & (r \cdot r') \cdot m & = & r \cdot (r' \cdot m) \end{array}$$

The notion of module-over-ring obviously subsumes the notion of vectorspace-over-field.

A **$R$-linear combination** of elements $m_1, \ldots, m_n$ in a $R$ module $M$ is any module element of the form

$$r_1 m_1 + \ldots + r_n m_n$$

with $r_i \in R$ and $m_i \in M$. [17]

We specifically do *not* universally require that $1_R \cdot m = m$ for all $m$ in an $R$-module $M$ when the ring $R$ contains a unit $1_R$. Nevertheless, on many occasions we *do* require this, but, therefore, must say so explicitly to be clear.

An **$R$-submodule** $N$ of an $R$-module $M$ is an additive subgroup which is closed under scalar multiplication.

---

[16] In some older sources the word was *modul*, which is now obsolete. And, in some older sources, *module* was used for what we now call the multiplicative identity 1, as well as other things whose present names are otherwise.

[17] While one should think of linear algebra over fields as a prototype for some of the phenomena concerning modules more generally, one should at the same time be prepared for deviation from the simpler reasonable expectations.

An $R$**-linear map** $T : M \longrightarrow N$ from one $T$-module $M$ to another $N$ is a homomorphism of abelian groups $T : M \longrightarrow N$

$$T(m + m') = Tm + Tm'$$

also respecting the scalar multiplication: for $r \in R$

$$T(r \cdot m) = r \cdot Tm$$

The collection of all $R$-linear maps from $M$ to $N$ is denoted

$$\mathrm{Hom}_R(M, N) = \{ \text{ all } R\text{-linear maps from } M \text{ to } N\}$$

When $M = N$, write

$$\mathrm{End}_R(M, M) = \mathrm{End}_R(M)$$

This is the **ring of $R$-linear endomorphisms** of $M$.

The **kernel** $\ker T$ of an $R$-linear map $T : M \longrightarrow N$ is

$$\ker T = \{m \in M : Tm = 0\}$$

[3.0.2] **Example:** *Abelian groups are $\mathbb{Z}$-modules*: for $a \in A$ in an abelian group $A$, define the scalar multiplication by integers by

$$n \cdot a = \begin{cases} 0_A & (\text{for } n = 0) \\ \underbrace{a + \ldots + a}_{n} & (\text{for } n > 0) \\ -(\underbrace{a + \ldots + a}_{|n|}) & (\text{for } n < 0) \end{cases}$$

Observe that a homomorphism of abelian groups is inevitably $\mathbb{Z}$-linear.

[3.0.3] **Example:** A **(left) ideal** $I$ in a ring $R$ is an additive subgroup $I$ of $R$ which is also closed under left multiplication by $R$: for $i \in I$ and $r \in R$, $r \cdot i \in I$. It is immediate that the collection of left ideals in $R$ is identical to the collection of $R$-submodules of $R$ (with left multiplication).

Let $R$ be a *commutative* ring. [18] Let $A$ be a not-necessarily commutative ring which is a left $R$-module. If, in addition to the requirements of a module, we have the *associativity*

$$r \cdot (a \cdot b) = (r \cdot a) \cdot b$$

for $r \in R$ and $a, b \in A$, then say $A$ is an $R$-**algebra**. Often additional requirements are imposed. [19]

A ring homomorphism $f : A \longrightarrow B$ of $R$-algebras is an $R$-**algebra homomorphism** if it is also an $R$-module homomorphism.

---

# 4. *Polynomial rings I*

We should not be content to speak of *indeterminate* $x$ or *variable* $x$ to construct polynomial rings. Instead, we describe in precise terms the fundamental property that a polynomial ring is meant to have, namely, in

[18] The requirement that $R$ be commutative is not at all necessary to give a definition of $R$-algebra, but without that hypothesis it is much less clear what is best to offer as a first and supposedly general definition.

[19] One might require the commutativity $(ra)b = a(rb)$, for example. One might require that $R$ have a unit 1 and that $1 \cdot a = a$ for all $a \in A$. However, not all useful examples meet these additional requirements.

colloquial terms, the *indeterminate* can be replaced by *any value*, or that any value can be *substituted for* the indeterminate.

Fix a commutative ring $R$, and let $A$ be a *commutative* $R$-algebra with a distinguished element $a_o$. Say that $A$, or, more properly, the *pair* $(A, a_o)$, is a **free (commutative) algebra** on one **generator** $a_o$ if, for every commutative $R$-algebra $B$ and chosen element $b_o \in B$ there is a *unique* $R$-algebra homomorphism

$$f_{B,b_o} : A \longrightarrow B$$

such that

$$f(a_o) = b_o$$

This condition is an example of a **universal mapping property**, and the polynomial ring (once we show that it is this object) is thus a **universal object** with respect to this property.

[4.0.1] **Remark:** In different words, $a_o$ can be mapped *anywhere*, and specifying the image of $a_o$ completely determines the homomorphism.

[4.0.2] **Remark:** We are to imagine that $A = R[x]$, $a_o = x$, and that the $R$-algebra homomorphism *is* the substitution of $b_o$ for $x$.

The following uniqueness result is typical of what can be said when an object is characterized by universal mapping properties.

[4.0.3] **Proposition:** Up to isomorphism, there is *at most one* free commutative $R$-algebra on one generator. That is, given two such things $(A, a_o)$ and $(A', a'_o)$, there is a unique isomorphism

$$i : A \longrightarrow A'$$

sending $a_o$ to $a'_o$ and such that, given a commutative $R$-algebra $B$ with distinguished element $b_o$, the corresponding maps (as above)

$$f_{B,b_o} : A \longrightarrow B$$

$$f'_{B,b_o} : A' \longrightarrow B$$

satisfy

$$f = f' \circ i$$

[4.0.4] **Remark:** Despite the possible unpalatableness of the definition and the proposition, this setup does what we want, and the proposition asserts the *essential uniqueness* of what will turn out to be recognizable as the polynomial ring $R[x]$.

*Proof:* This proof is typical of proving that there is at most one thing characterized by a universal property. First, take $B = A$ and $b_o = a_o$. Then there is a *unique* $R$-algebra homomorphism $A \longrightarrow A$ taking $a_o$ to $a_o$. Since the identity map on $A$ does this, apparently *only* the identity has this property among all endomorphisms of $A$.

Next, let $B = A'$ and $b = a'_o$, and

$$f_{A',a'_o} : A \longrightarrow A' \quad (\text{with } a_o \longrightarrow a'_o)$$

the unique $R$-algebra homomorphism postulated. Reversing the roles of $A$ and $A'$, we have another *unique*

$$f'_{A,a_o} : A' \longrightarrow A \quad (\text{with } a'_o \longrightarrow a_o)$$

Consider $g = f' \circ f'$. It sends $a_o$ to $a_o$, so, by our first observation, must be the identity map on $A$. Similarly, $f \circ f'$ is the identity map on $A'$. Thus, $f$ and $f'$ are mutual inverses, and $A$ and $A'$ are isomorphic, by a *unique* isomorphism, [20] and $a_o$ is mapped to $a'_o$ by this map. ///

This slick uniqueness argument does not prove existence. Indeed, there seems to be no comparably magical way to prove existence, *but* the uniqueness result assures us that, whatever pathetic *ad hoc* device we do hit upon to construct the free algebra, the thing we make is *inevitably* isomorphic (and by a *unique* isomorphism) to what any *other* construction might yield. That is, the uniqueness result shows that particular choice of construction does not matter. [21]

How to construct the thing? On one hand, since the possible images $f(a_o)$ can be *anything* in another $R$-algebra $B$, $a_o$ ought not satisfy any relations such as $a_o^3 = a_o$ since a homomorphism would carry such a relation forward into the $R$-algebra $B$, and we have no reason to believe that $b_o^3 = b_o$ for every element $b_o$ of every $R$-algebra $B$. [22] On the other hand, since the image of $a_o$ under an $R$-algebra homomorphism is intended to determine the homomorphism completely, the free algebra $A$ should not contain more than $R$-linear combinations of powers of $a_o$.

For fixed commutative ring $R$ with identity 1, let $S$ be the set [23] of $R$-valued functions $P$ on the set $\{0, 1, 2, \ldots\}$ such that, for each $P$, there is an index $n$ such that for $i > n$ we have $P(i) = 0$. [24] Introduce an addition which is simply componentwise: for $P, Q \in S$,

$$(P + Q)(i) = P(i) + Q(i)$$

And there is the value-wise $R$-module structure with scalar multiplication

$$(r \cdot P)(i) = r \cdot P(i)$$

All this is obligatory, simply to have an $R$-module. We take the distinguished element to be

$$a_o = \text{ the function } P_1 \text{ such that } P_1(1) = 1 \text{ and } P_1(i) = 0 \text{ for } i \neq 1$$

A misleadingly glib way of attempting to define the multiplication is [25] as

$$(P \cdot Q)(i) = \sum_{j+k=i} P(j)\, Q(k)$$

---

[20] The virtues of there being a *unique* isomorphism may not be apparent at the moment, but already played a role in the uniqueness proof, and do play significant roles later.

[21] An elementary example of a construction whose internals are eventually ignored in favor of operational properties is *ordered pair*: in elementary set theory, the ordered pair $(a, b)$ is defined as $\{\{a\}, \{a, b\}\}$, and the expected properties are verified. After that, this set-theoretic definition is forgotten. And, indeed, one should probably not consider this to be *correct* in any sense of providing further information about what an ordered pair truly is. Rather, it is an *ad hoc* construction which thereafter entitles us to do certain things.

[22] While it is certainly true that we should doubt that this $a_o$ satisfies any relations, in other situations specification of universal objects *can* entail unexpected relations. In others, the fact that there *are* no relations apart from obvious ones may be non-trivial to prove. An example of this is the Poincaré-Birkhoff-Witt theorem concerning universal enveloping algebras. We may give this as an example later.

[23] This construction presumes that sets and functions are legitimate primitive objects. Thus, we tolerate possibly artificial-seeming constructions for their validation, while clinging to the uniqueness result above to rest assured that any peculiarities of a construction do not harm the object we create.

[24] We would say that $P$ is *eventually zero*. The intent here is that $P(i)$ is the coefficient of $x^i$ in a polynomial.

[25] If one is prepared to describe polynomial multiplication by telling the coefficients of the product then perhaps this is not surprising. But traditional informal discussions of polynomials often to treat them more as strings of symbols, *expressions*, rather than giving them set-theoretic substance.

using the idea that a function is completely described by its values. Thus, since $R$ is commutative,

$$P \cdot Q = Q \cdot P$$

For $P, Q, T$ in $S$, associativity

$$(P \cdot Q) \cdot T = P \cdot (Q \cdot T)$$

follows from rewriting the left-hand side into a symmetrical form

$$((P \cdot Q) \cdot T)(i) = \sum_{j+k=i} (P \cdot Q)(j)\, T(k)$$

$$= \sum_{j+k=i} \sum_{m+n=j} P(m)Q(n)T(k) = \sum_{m+n+k=i} P(m)Q(n)T(k)$$

Distributivity of the addition and multiplication in $S$ follows from that in $R$:

$$(P \cdot (Q+T))(i) = \sum_{j+k=i} P(j) \cdot (Q+T)(k) = \sum_{j+k=i} (P(j)Q(k) + P(j)T(k))$$

$$= \sum_{j+k=i} P(j)Q(k) + \sum_{j+k=i} P(j)T(k) = (P \cdot Q)(i) + (P \cdot T)(i)$$

The associativity

$$r \cdot (P \cdot Q) = (rP) \cdot Q$$

is easy. Note that, by an easy induction

$$P_1^i(j) = \begin{cases} 1 & (\text{if } j = i) \\ 0 & (\text{if } j \neq i) \end{cases}$$

So far, we have managed to make a commutative $R$-algebra $S$ with a distinguished element $P_1$. With the above-defined multiplication, we claim that

$$\sum_i r_i\, P_1^i$$

(with coefficients $r_i$ in $R$) is 0 (that is, the zero function in $S$) if and only if all coefficients are 0. Indeed, the value of this function at $j$ is $r_j$. Thus, as a consequence, if

$$\sum_i r_i\, P_1^i = \sum_j r'_j\, P_1^j$$

then subtract one side from the other, so see that $r_i = r'_i$ for all indices $i$. That is, there is only one way to express an element of $S$ in this form.

Given another $R$-algebra $B$ and element $b_o \in B$, we would like to define

$$f(\sum_i r_i P_1^i) = \sum_i r_i b_o^i$$

At least this is *well-defined*, since there is only one expression for elements of $S$ as $R$-linear combinations of powers of $P_1^i$. The $R$-linearity of this $f$ is easy. The fact that it respects the multiplication of $S$ is perhaps less obvious, but not difficult: [26]

$$f((\sum_i r_i P_1^i) \cdot (\sum_j r'_j P_1^j)) = f(\sum_{i,j} r_i r'_j P_1^{i+j}) = \sum_{i,j} r_i r'_j b_o^{i+j} = (\sum_i r_i b_o^i) \cdot (\sum_j r'_j b_o^j))$$

[26] The formulas for multiplication of these finite sums with many summands could be proven by induction if deemed necessary.

Thus, this $f$ is an $R$-algebra homomorphism which sends $a_o = P_1$ to $b_o$.

Finally, there is no *other* $R$-algebra homomorphism of $S$ to $B$ sending $a_o = P_1$ to $b_o$, since every element of $S$ is expressible as $\sum r_i P_1^i$, and the $R$-algebra homomorphism property yields

$$f(\sum r_i P_1^i) = \sum_i f(r_i P_1^i) = \sum_i r_i\, f(P_1^i) = \sum_i r_i\, f(P_1)^i$$

There is no further choice possible. [27]

[4.0.5] **Remark:** This tedious construction (or something equivalent to it) is necessary. The uniqueness result assures us that no matter which of the several choices we make for (this tiresome) construction, the resulting thing is the same.

# Exercises

**3.**[4.0.1] Let $r$ be nilpotent in a commutative ring. Show that $1 + r$ is a unit.

**3.**[4.0.2] Give an example of an integer $n$ such that $\mathbb{Z}/n$ has at least 4 different idempotent elements.

**3.**[4.0.3] Give an example of an integer $n$ such that $\mathbb{Z}/n$ has at least 4 different idempotent elements.

**3.**[4.0.4] Let $f \in k[x]$ for a field $k$. For indeterminates $x, y$, show that we have a Taylor-Maclaurin series expansion of the form

$$f(x+y) \;=\; f(x) + \sum_{i=1}^{n} f_i(x)\, y^i$$

for some polynomials $f_i(x)$. For $k$ of characteristic 0, show that

$$f_i(x) \;=\; \left(\frac{\partial}{\partial x}\right)^i f(x)/i!$$

**3.**[4.0.5] Show that a **local ring** $R$ (that is, a ring having a unique *maximal* proper ideal) has no idempotent elements other than 0 and 1.

**3.**[4.0.6] Let $p > 2$ be a prime. Show that for $\ell \geq 1 \geq \frac{p}{p-1}$ the power of $p$ dividing $(p^\ell)^n$ is larger than or equal to the power of $p$ dividing $n!$.

**3.**[4.0.7] *The exponential map modulo $p^n$:* Let $p > 2$ be prime. Make sense of the map

$$E : p\mathbb{Z}/p^n \to 1 + p\mathbb{Z} \bmod p^n$$

defined by the dubious formula

$$E(px) = 1 + \frac{px}{1!} + \frac{(px)^2}{2!} + \frac{(px)^3}{3!} + \dots$$

(*Hint:* cancel powers of $p$ before trying to make sense of the fractions. And only finitely-many of the summands are non-zero mod $p^n$, so this is a *finite* sum.)

[27] One may paraphrase this by saying that if $g$ were another such map, then $f - g$ evaluated on any such element of $S$ is 0.

**3.**[4.0.8] With the exponential map of the previous exercise, show that $E(px+py) = E(px)\cdot E(py)$ modulo $p^n$, for $x, y \in \mathbb{Z}/p^{n-1}$. That is, prove that $E$ is a group homomorphism from $p\mathbb{Z}/p^n\mathbb{Z}$ to the subgroup of $(\mathbb{Z}/p^n)^\times$ consisting of $a = 1 \bmod p$.

**3.**[4.0.9] Prove that $(\mathbb{Z}/p^n)^\times$ is *cyclic* for $p > 2$ prime.

**3.**[4.0.10] Figure out the correct analogue of the exponential map for $p = 2$.

**3.**[4.0.11] Figure out the correct analogue of the exponential maps modulo primes for the Gaussian integers $\mathbb{Z}[i]$.

**3.**[4.0.12] For which ideals $I$ of $\mathbb{Z}[i]$ is the multiplicative group $\mathbb{Z}[i]/I^\times$ of the quotient ring $\mathbb{Z}[i]/I$ *cyclic*?

**3.**[4.0.13] Show that there are no *proper* two-sided ideals in the ring $R$ of 2-by-2 rational matrices.

**3.**[4.0.14] (*Hamiltonian quaternions*) Define the **quaternions** $\mathfrak{H}$ to be an $\mathbb{R}$-algebra generated by $1 \in \mathbb{R}$ and by elements $i, j, k$ such that $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, and $ki = j$. Define the *quaternion conjugation* $\alpha \longrightarrow \alpha^*$ by

$$(a + bi + cj + dk)^* = a - bi - cj - dk$$

Show that $*$ is an *anti-automorphism*, meaning that

$$(\alpha \cdot \beta)^* = \beta^* \cdot \alpha^*$$

for quaternions $\alpha, \beta$. Show that $\mathfrak{H}$ is a *division ring*.

**3.**[4.0.15] Provide a *construction* of the quaternions, by showing that

$$a + bi + cj + dk \longrightarrow \begin{pmatrix} a+bi & c+di \\ c-di & a-bi \end{pmatrix}$$

is a ring homomorphism from the quaternions to a subring of the 2-by-2 complex matrices.