



Añadir come referencia al Atiyah.

We will see, in the world of ring, that there are natural analogues brought from the world of groups. Indeed, we will generalize concepts from Group Theory as seamlessly as possible. But, a deeper engagement with the main references is needed to supplement the concepts displayed in the coming sections.

1. Definition of ring

Definition 1.1. A ring is a triple $(A, +, \cdot)$ that consist of a set A and two binary operations $+, \cdot: A \times A \rightarrow A$, called respectively sum and multiplication, such that

- (i) $(A, +)$ is an Abelian group,
- (ii) (A, \cdot) is a semigroup, and
- (iii) \cdot distributes over $+$, i.e.,

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

for all $a, b, c \in A$.

Recall that (A, \cdot) is a semigroup if \cdot is associative. Thus, in the definition above, we may well have replaced (ii) by the condition that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in A$. The **zero** of the ring $(A, +, \cdot)$ is the **additive neutral element** of $(A, +)$, denoted 0 . The **additive inverse** of an element $a \in A$ is denoted by $-a$. **Subtraction** is the internal operation $-: A \times A \rightarrow A$ on A defined by

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

Is $-$ associative? We usually say A is a ring to we mean $(A, +, \cdot)$ is a ring when the operations $+$ and \cdot are known. By convention, we write ab for $a \cdot b$. If there is an element $e \in A$ such that $e \cdot a = a \cdot e = a$ for all $a \in A$, we say A is a ring with unity¹ and, since such an element is unique, denote e by 1_A or simply 1 . If \cdot is commutative, i.e., $ab = ba$ for all $a \in A$, we say A is a *commutative ring*; and, if in addition, A has a unity, we say A is a commutative ring with unity.

Example 1. The basic examples of rings are $\mathbb{Z}/n\mathbb{Z}$, \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C} where the operations $+$ and \cdot are the usual addition and multiplication in each case.

Theorem 1.2. Let $(A, +, \cdot)$ be a ring and $a, b \in A$. Then

$$(i) \quad a0 = 0a = 0$$

$$(ii) \quad a(-b) = -a(b) = -(ab)$$

¹In Spanish, we say “con identidad” instead of “con unidad”. (Un anillo puede tener más de una unidad.)

$$(iii) \quad (-a)(-b) = ab$$

Proof. (i) We know $0 = 0 + 0$. By the distributivity of \cdot over $+$, we have

$$a0 = a(0 + 0) = a0 + a0.$$

Adding $-a0$ to both sides yields $0 = a0$. Similarly, we obtain $0a = 0$.

(ii) By the distributivity of \cdot over $+$ and by (i),

$$ab + a(-b) = a(b - b) = a0 = 0.$$

Additive inverses are unique, so $-(ab) = a(-b)$. Likewise, $-a(b) = -(ab)$.

(iii) Exercise.

□

Remark 1.2.1. If $1 = 0$, then

$$a = a1 = a0 = 0$$

for every $a \in A$. Thus, in this case, every element of A is zero, meaning $A = \{0\}$. We call this ring the *trivial ring*, and it is the unique ring with this property. Some authors write “ A is a ring with $1 \neq 0$ ” to express that $A \neq \{0\}$ is ring with unity.

Example 2. Let X be a nonempty set and A a ring. The set A^X of all functions from X to A is a ring with the operations given by

$$\begin{aligned} (f + g)(x) &= f(x) + g(x), \\ (f \cdot g)(x) &= f(x) \cdot g(x), \end{aligned}$$

for functions $f, g: X \rightarrow A$ and $x \in X$.

2. Types of rings

Let $(A, +, \cdot)$ be a ring. We say $a \in A$ is

- (i) a *zero divisor* if $a \neq 0$ and there is $b \in A, b \neq 0$, such that $ab = 0$ or $ba = 0$.
- (ii) *nilpotent* if $a^n = 0$ for some $n \in \mathbb{Z}^+$.
- (iii) *idempotent* if $a^2 = a$

If A is a ring with unity, $a \in A$ is *invertible* if there is $a' \in A$ such that $aa' = 1$ and $a'a = 1$. The set of units of A is denoted A^\times or $U(A)$. Verify that A^\times is a group under multiplication.

Exercise 1. Verify that a zero divisors is not invertible.

We say that a ring $(A, +, \cdot)$ is

- (i) an *integral domain* if A is a nontrivial commutative ring with unity and it has no zero divisors.

(ii) a ring with the *cancellation property* if for any $a, b \in A$, if $c \in A$ is nonzero, then

$$ac = bc \text{ or } ca = cb \text{ implies } a = b.$$

(iii) a *division ring* if A is a nontrivial ring with unity and every nonzero element is invertible.

(iv) a *field* if it is both commutative and a division ring.

Exercise 2. Verify that a field is an integral domain. Provide a counterexample that disproves the converse affirmation.

Proposition 2.1. *A ring has the cancellation property if and only if it has no zero divisors.*

Proof. (i) Suppose first that A is a ring with the cancellation property. Let $a, b \in A$ such that $a \neq 0$ and $ab = 0$, then $ab = a0$, but this implies that $b = 0$ due to the cancellation property. Thus, A has no zero divisors.

(ii) Conversely, suppose that A has no zero divisors. Let $ab = ac$ with $a \neq 0$, then $a(b - c) = 0$. Hence, $b - c = 0$ and $b = c$.

□

Example 3. (i) $\mathbb{Z}/4\mathbb{Z}$ is a ring with zero divisors. Note $2 \cdot 2 \equiv 0 \pmod{4}$.

(ii) The set \mathbb{R}^X of functions from a set X to \mathbb{R} is a commutative ring with unity. The unity is the constant function equal to $1 \in \mathbb{R}$. In this ring, an element is invertible if it never vanishes, i.e., $f: X \rightarrow \mathbb{R}$ is invertible if $f(x) \neq 0$ for every $x \in X$.

(iii) \mathbb{R} is a field with the usual addition and multiplication. Is \mathbb{R}^X a field?

(iv) \mathbb{Q} is a field with the usual addition and multiplication.

(v) \mathbb{Z} is a commutative ring with unity but not a field. The only invertible elements are 1 and -1 .

(vi) $\mathbb{Z}/n\mathbb{Z}$ is an integral domain. .

(vii) $\mathbb{Z}/p\mathbb{Z}$ is a field if and only if $p \in \mathbb{Z}^+$ is prime. This is an example of a finite field.

(viii) Let us show that there are infinitely many fields F such that $\mathbb{Q} \subsetneq F \subsetneq \mathbb{R}$. Let D be a rational number which is not a perfect square in \mathbb{Q} , i.e., $x^2 \neq D$ for any $x \in \mathbb{Q}$. Then

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

is a field with the operations:

$$\begin{aligned} (a_1 + b_1\sqrt{D}) + (a_2 + b_2\sqrt{D}) &= (a_1 + a_2) + (b_1 + b_2)\sqrt{D}, \\ (a_1 + b_1\sqrt{D})(a_2 + b_2\sqrt{D}) &= (a_1a_2 + b_1b_2D) + (a_1b_2 + a_2b_1)\sqrt{D}, \end{aligned}$$

for a_1, b_1, a_2 and b_2 in \mathbb{Q} . Since D is not a perfect square, every element of $\mathbb{Q}(\sqrt{D})$ is written in a unique way. Indeed, suppose that

$$a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D},$$

then

$$(a_1 - a_2) + (b_1 - b_2)\sqrt{D} = 0.$$

If $b_1 \neq b_2$ then

$$\sqrt{D} = \frac{a_2 - a_1}{b_1 - b_2} \in \mathbb{Q},$$

a contradiction. So, $b_1 = b_2$, and then, $a_1 = a_2$. The ring $\mathbb{Q}(\sqrt{D})$ is called the **quadratic field**. The rational number D could be written in the form

$$D = e^2 D',$$

for some rational number e and some rational number D' , such that D' is square free, this is, D' is not divisible for the square of any integer greater than 1. Then

$$\sqrt{D} = e\sqrt{D'},$$

and then,

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{D'}).$$

Therefore, it is possible to assume that in $\mathbb{Q}(\sqrt{D})$, D is square free.

- (ix) If A is a ring, the set of square matrices with entries in A and the usual operations of addition and multiplication of matrices is a noncommutative ring with unity. Exercise: Verify that this ring has zero divisors if A does.

We have already mention that an integral domain need not be a field. However, if the underlying set is finite, this is true.

Exercise 3. Prove this assertion.

This section ends up with important examples and a proposition.

Example 4. There is an important and familiar subset of that is a ring with a special operation of multiplication, this is, the set of polynomial functions $\mathcal{P}(\mathbb{R})$. This set contains all the functions of the form

$$\begin{aligned} p: \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto p(x) = a_0 + a_1x + \dots + a_nx^n, \end{aligned}$$

for $n \in \mathbb{N}$. $\mathcal{P}(\mathbb{R})$ is a ring with the operations inherited from $\mathcal{F}(\mathbb{R})$ which, for this particular situation, can be seen in the following way

$$\begin{aligned} p(x) + q(x) &= (a_0 + b_0) + (a_1 + b_1)x + \dots = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i, \\ p(x) \cdot q(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots = \sum_{i=0}^{n+m} C_i x^i, \end{aligned}$$

where

$$C_k = \sum_{i=0}^k a_i b_{k-i},$$

$b_j = 0$ if $j > m$, $a_j = 0$ if $j > n$, and $p(x), q(x)$ polynomial functions given by

$$\begin{aligned} p(x) &= a_0 + a_1x + a_2x^2 + \dots + a_nx^n, \\ q(x) &= b_0 + b_1x + b_2x^2 + \dots + b_mx^m. \end{aligned}$$

For example, taking $p(x), q(x) \in \mathcal{P}(\mathbb{R})$, given by $p(x) = 1 + 2x + x^2$ and $q(x) = 2 - x + x^3$, then

$$\begin{aligned} p(x) + q(x) &= (1 + 2x + x^2) + (2 - x + x^3) = 3 + x + 2x^2 + x^3, \\ p(x) \cdot q(x) &= (1 + 2x + x^2) \cdot (2 - x + x^3) = 2 + 3x + 2x^4 + x^5. \end{aligned}$$

p is called a polynomial function of degree n if $a_n \neq 0$. The term a_nx^n is called the leading term of $p(x)$.

Example 5. Let's recall the definition of cartesian product. Let $M \neq \emptyset$. Then

$$\begin{aligned} M^2 &= M \times M = \{(a_1, a_2) / a_1, a_2 \in M\} \\ M^3 &= M \times M \times M = \{(a_1, a_2, a_3) / a_1, a_2 \in M\} \\ &\vdots \\ M^n &= M \times \dots \times M = \{(a_1, a_2, \dots, a_n) / a_i \in M, \forall i = 1, \dots, n\} \end{aligned}$$

If $A = (A, +, \cdot)$ is a ring, then A^n is a ring with the componentwise operations:

$$\begin{aligned} (a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) &= (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n), \\ (a_1, a_2, \dots, a_n) \cdot (b_1, b_2, \dots, b_n) &= (a_1b_1, a_2b_2, \dots, a_nb_n). \end{aligned}$$

In fact, we can define the ring of all the sequences, $A^{\mathbb{N}}$, whose coordinates are filled with elements of A , i.e.,

$$A^{\mathbb{N}} = \{(a_n)_{n \in \mathbb{N}} = (a_1, \dots, a_i, \dots) : a_i \in M, \forall i \in \mathbb{N}\},$$

with the componentwise operations defined by

$$\begin{aligned} (a_1, a_2, \dots) + (b_1, b_2, \dots) &= (a_1 + b_1, a_2 + b_2, \dots), \\ (a_1, a_2, \dots) \cdot (b_1, b_2, \dots) &= (a_1b_1, a_2b_2, \dots). \end{aligned}$$

Example 6 (Important). There is a special subset of $A^{\mathbb{N}}$ denoted

$$A[x] = \{(a_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}} / \exists N \in \mathbb{N}, \forall m \geq N : a_m = 0\},$$

The notation $A[x]$ is used because an arbitrary element $p(x)$ of $A[x]$ is usually represented as a formal sum:

$$p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n,$$

which means that $a_i \in A$ for each $i \in \{1, \dots, n\}$, $a_n \neq 0$, and

$$n = \min \{N \in \mathbb{N} / \forall n \geq N : a_n = 0\}.$$

In this case,

1. $p(x)$ is called a polynomial in x .
2. n is called the degree of $p(x)$ and is denoted by $\deg(p(x))$,
3. the term $a_n x^n$ is called the leading term of $p(x)$,
4. if the leading term of $p(x)$ is $a_n = 1$, then $p(x)$ is called monic.

With this representation, if $p(x) = a_0 + a_1 x^1 + a_2 x^2 + \dots + a_n x^n$ and $q(x) = b_0 + b_1 x^1 + b_2 x^2 + \dots + b_m x^m$, assuming that $m \leq n$, the operations in this ring are defined by

$$p(x) + q(x) = \sum_{i=0}^n (a_i + b_i) x^i,$$

$$p(x) \cdot q(x) = \sum_{i=0}^{n+m} C_i x^i,$$

where

$$C_k = \sum_{i=0}^k a_i b_{k-i},$$

$b_j = 0$ if $j > m$ and $a_j = 0$ if $j > n$. The ring $A[x]$ usually found in the literature as the **polynomial ring** with coefficients in A and indeterminate x .

Remark 2.1.1. The ring A is identified in $A[x]$ with the set of polynomials of degree 0, i.e, the set A , is in bijective correspondence with the set of all the sequence of the form $(a, 0, 0, \dots)$, for $a \in A$. This observation allows us to write $A \subseteq A[x]$, as a commonly accepted abuse of notation.

Remark 2.1.2 (Polynomial function \neq polynomial). Although their construction is different, the rings $\mathcal{P}(\mathbb{R})$ and $\mathbb{R}[x]$ look very similar. In fact, there is a bijective correspondence between the polynomial functions and the (abstract) polynomials in x . This is quite obvious considering that every polynomial function of the form

$$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

can be viewed as the polynomial

$$\bar{p}(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

in the variable x . The big difference between $p(x)$ and $\bar{p}(x)$ is that we can evaluate $p(a) \in \mathbb{R}$, for every $a \in \mathbb{R}$, while $\bar{p}(a)$ has no sense.

Example 7. Let's recall that for any index set I , the cartesian product of an indexed family $\{A_i\}_{i \in I}$ of set is defined by

$$\prod_{i \in I} A_i = \{f: I \rightarrow \cup A_i / f(i) \in A_i, \forall i \in I\}.$$

If each A_i is a ring, then $\prod_{i \in I} A_i$, is a ring with the componentwise addition and multiplication.

$$(f + g)(i) = f(i) + g(i),$$

$$(fg)(i) = f(i)g(i),$$

for each $i \in I$. If $I = \mathbb{Z}^+ \cup \{0\}$, there is a special subset of $\prod_{i \in I} A_i$, called the coproduct of the family $\{A_i\}_{i \in I}$, and defined by the set of all functions $f \in \prod_{i \in I} A_i$ such that f is zero except for a finite number of elements in I . This set is a ring with the componentwise addition and multiplication and is denoted by

$$\coprod_{i \in I} A_i.$$

Example 8. Taking $I = \{1, 2\}$, the indexed family $\{A_1, A_2\}$ verifies that the set

$$\prod_{i \in I} A_i$$

is in bijection with the usual cartesian product $A_1 \times A_2$. For this, if $f: I \rightarrow A_1 \cup A_2$ is a function such that $f(1) \in A_1$ and $f(2) \in A_2$, then f corresponds with the element $(f(1), f(2)) \in A_1 \times A_2$. This correspondence is clearly a bijection. The operations defined above over $\prod_{i \in I} A_i$ in terms of the usual cartesian product are

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &= (x_1 + x_2, y_1 + y_2), \\ (x_1, y_1) \cdot (x_2, y_2) &= (x_1 x_2, y_1 y_2).\end{aligned}$$

In general, if $I = \{1, \dots, n\}$, then

$$\prod_{i \in I} A_i = A_1 \times \dots \times A_n$$

is a ring with componentwise operations. Moreover, if $I = \mathbb{N}$, then

$$\prod_{i \in \mathbb{N}} A_i = A^{\mathbb{N}}.$$

Remark 2.1.3. Polynomial rings are important because their structure provides them with many properties which are analogues to those of \mathbb{Z} . In particular, we can define “prime elements” among them and establish a generalized version of the division algorithm. It comes as no surprise then that they have many applications in multiple areas of mathematics such as algebraic geometry, number theory, and algebraic combinatorics.

Remark 2.1.4. Let’s give a look to polynomial rings with zero divisors.

1. For example, take $p(x) = x^2 + 1$ in $\mathbb{Z}_2[x]$, then

$$\begin{aligned}p(x) + p(x) &= (x^2 + 1) + (x^2 + 1), \\ &= 2x^2 + 2, \\ &= 0, \text{ mod } 2.\end{aligned}$$

This example shows that the sum of two polynomials does not preserve the degree of the polynomials.

2. Another interesting example is in the polynomial ring $\mathbb{Z}_6[x]$. Take $p(x) = 2x$ and $q(x) = 3x^2 + 1$. If the multiplication is in $\mathbb{Z}[x]$, then

$$p(x) \cdot q(x) = 6x^3 + 2x,$$

but in the ring \mathbb{Z}_6 , the operations module 6 implies that

$$p(x) \cdot q(x) = 6x^3 + 2x = 2x, \text{ mod } 6.$$

The last remark allows us to conclude that not always the degree of the sum of two polynomials is the maximum of the degree and that the degree of the product of two polynomials is not the sum of the degree, as usual in \mathbb{Z} . The next proposition determinates when the latter happens.

Proposition 2.2. *Let A be an integral domain and $p(x)$ and $q(x)$ polynomials in $A[x]$. Then*

1. $A[x]$ is an integral domain;
2. $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$;
3. considering A as the polynomials of degree 0, $(A[x])^\times = A^\times$.

Proof. Let A be a integral domain and $p(x)$ and $q(x)$ polynomials in $A[x]$, with leading term $a_n x^n$ and $b_m x^m$ respectively. The leading term of $p(x) \cdot q(x)$ is $a_n b_m x^{n+m}$, where $a_n b_m \neq 0$ because A is a integral domain. Then

$$\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x)),$$

and $A[x]$ is an integral domain, otherwise, if two polynomials $p(x) \neq 0$ and $q(x) \neq 0$, verifies that $p(x) \cdot q(x) = 0$,

$$0 = \deg(p(x)) + \deg(q(x)),$$

therefore, $\deg(p(x)) = \deg(q(x)) = 0$, and $p(x), q(x) \in A$, but this is a contraccition since A is an integral domain. This proves i) and ii).

For ii) it is easy to see that $A^\times \subseteq (A[x])^\times$. On the other hand, if $p(x)$ and $q(x)$ are invertibles in $A[x]$, then $p(x) \cdot q(x) = 1$, and for i), $\deg(p(x)) = \deg(q(x)) = 0$, and $p(x), q(x) \in A$, therefore, $p(x)$ and $q(x)$ are invertibles in A . \square