Appendix A
Algebraic Structures

This appendix is an elementary introduction to basic notions of set theory, together with those of group, ring and field. The reader is only supposed to know about numbers, more precisely natural (containing the zero 0), integer, rational and real numbers, that will be denoted respectively by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Some of their properties will also be recalled in the following. We shall also introduce complex numbers denoted $\mathbb{C}$ and (classes of) integers $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.

A.1 A Few Notions of Set Theory

Definition A.1.1 Given any two sets A and B, by $A \times B$ we denote their *Cartesian product*. This it is defined as the set of ordered pairs of elements from A and B, that is,

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Notice that $A \times B \neq B \times A$ since we are considering ordered pairs. The previous definition is valid for sets A, B of arbitrary cardinality. The set $A \times A$ is denoted A^2.

Exercise A.1.2 Consider the set $A = \{\diamondsuit, \heartsuit, \clubsuit, \spadesuit\}$. The Cartesian product A^2 is then

$$\begin{aligned} A^2 &= A \times A \\ &= \big\{(\diamondsuit, \diamondsuit), (\diamondsuit, \heartsuit), (\diamondsuit, \clubsuit), (\diamondsuit, \spadesuit), (\heartsuit, \diamondsuit), (\heartsuit, \heartsuit), (\heartsuit, \clubsuit), (\heartsuit, \spadesuit), \\ &\qquad (\clubsuit, \diamondsuit), (\clubsuit, \heartsuit), (\clubsuit, \clubsuit)(\clubsuit, \spadesuit), (\spadesuit, \diamondsuit), (\spadesuit, \heartsuit), (\spadesuit, \clubsuit), (\spadesuit, \spadesuit)\big\}. \end{aligned}$$

Definition A.1.3 Given any set A, a *binary relation* on A is any subset of the Cartesian product $A^2 = A \times A$. If such a subset is denoted by $\mathcal{R}$, we say that the pair of elements a, b in A are *related* or *in relation* if $(a, b) \in \mathcal{R}$ and write it as $a \mathcal{R} b$.

G. Landi and A. Zampini, *Linear Algebra and Analytic Geometry for Physical Sciences*, Undergraduate Lecture Notes in Physics,
https://doi.org/10.1007/978-3-319-78361-1

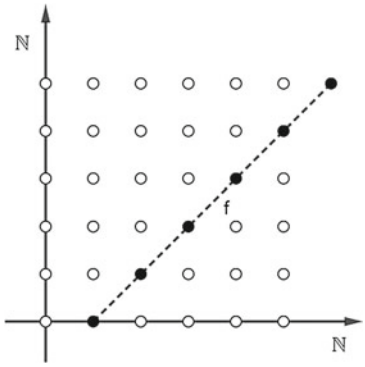

Fig. A.1 A binary relation in $\mathbb{N}^2$

Example A.1.4 Consider $A = \mathbb{N}$, the set of natural numbers, with $\mathcal{R}$ the subset of $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ given by the points as in the Fig. A.1. We see that $2\mathcal{R}1$, but it is not true that $1\mathcal{R}1$. One may easily check that $\mathcal{R}$ can be written by the formula

$$n\mathcal{R}m \Leftrightarrow m = n - 1, \qquad \text{for any} \quad (n, m) \in \mathbb{N}^2.$$

Definition A.1.5 A binary relation on a set A is called an *equivalence relation* if the following properties are satisfied

- $\mathcal{R}$ is *reflexive*, that is $a\mathcal{R}a$ for any $a \in A$,
- $\mathcal{R}$ is *symmetric*, that is $a\mathcal{R}b \Rightarrow b\mathcal{R}a$, for any $a, b \in A$,
- $\mathcal{R}$ is *transitive*, that is $a\mathcal{R}b$ and $b\mathcal{R}c \Rightarrow a\mathcal{R}c$ for any $a, b, c \in A$.

Exercise A.1.6 In any given set A, the equality is an equivalence relation. On the set T of all triangles, congruence of triangles and similarity of triangles are equivalence relations. The relation described in the Example A.1.4 is not an equivalence relation, since reflexivity does not hold.

Definition A.1.7 Consider a set A and let $\mathcal{R}$ be an equivalence relation defined on it. For any $a \in A$, one defines the subset

$$[a] = \{x \in A \mid x\mathcal{R}a\} \subseteq A$$

as the *equivalence class* of a in A. Any element $x \in [a]$ is called a *representative* of the class $[a]$. It is clear that an equivalence class has as many representatives as the elements it contains.

Proposition A.1.8 *With $\mathcal{R}$ an equivalence relation on the set A, the following properties hold:*

(1) If $a\,\mathcal{R}\,b$, then $[a] = [b]$.

(2) If $(a, b) \notin \mathcal{R}$, *then* $[a] \cap [b] = \emptyset$.
(3) $A = \bigcup_{a \in A} [a]$*; this is a disjoint union.*

Proof (1) One shows that the mutual inclusions $[a] \subseteq [b]$ and $[b] \subseteq [a]$ are both valid if $a \mathcal{R} b$. Let $x \in [a]$; this means $x \mathcal{R} a$. From the hypothesis $a \mathcal{R} b$, so by the transitivity of $\mathcal{R}$ one has $x \mathcal{R} b$, that is $x \in [b]$. This proves the inclusion $[a] \subseteq [b]$. The proof of the inclusion $[b] \subseteq [a]$ is analogue.
(2) Let us suppose that $A \ni x \in [a] \cup [b]$. It would mean that $x \mathcal{R} a$ and $x \mathcal{R} b$. From the symmetry of $\mathcal{R}$ we would then have $a \mathcal{R} x$, and from the transitivity this would result in $a \mathcal{R} b$, which contradicts the hypothesis.
(3) It is obvious, from (2). □

Definition A.1.9 The decomposition $A = \bigcup_{a \in A} [a]$ is called the *partition* of A associated (or corresponding) to the equivalence relation $\mathcal{R}$.

Definition A.1.10 If $\mathcal{R}$ is an equivalence relation defined on the set A, the set whose elements are the corresponding equivalence classes is denoted $A/\mathcal{R}$ and called the *quotient of* A *modulo* $\mathcal{R}$. The map

$$\pi : A \to A/\mathcal{R} \qquad \text{given by} \qquad a \mapsto [a]$$

is called *the canonical projection* of A onto the quotient $A/\mathcal{R}$.

A.2 Groups

A set has an algebraic structure if it is equipped with one or more operations. When the operations are more than one, they are required to be compatible. In this section we describe the most elementary algebraic structures.

Definition A.2.1 Given a set G, a *binary operation* $*$ on it is a map

$$* : G \times G \longrightarrow G.$$

The image of the operation between a and b is denoted by $a * b$. One also says that G is *closed*, or *stable* with respect to the operation $*$. One usually writes $(G, *)$ for the algebraic structure $*$ defined on G, that is for the set G equipped with the binary operation $*$.

Example A.2.2 It is evident that the usual sum and the usual product in $\mathbb{N}$ are binary operations.

As a further example we describe a binary operation which does not come from usual arithmetic operations in any set of numbers. Let T be an equilateral triangle whose vertices are ordered and denoted by ABC. Let R be the set of rotations on a plane under which each vertex is taken onto another vertex. The rotation that takes the vertices ABC to BCD, can be denoted by

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}.$$

It is clear that R contains three elements, which are:

$$e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \qquad x = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \qquad y = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}.$$

The operation—denoted now $\circ$—that we consider among elements in R is the composition of rotations. The rotation $x \circ y$ is the one obtained by acting on the vertices of the triangle first with y and then with x. It is easy to see that $x \circ y = e$. The Table A.1 shows the composition law among elements in R.

$\circ$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

(A.1)

Remark A.2.3 The algebraic structures $(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$ have the following well known properties, for all elements $a, b, c \in \mathbb{N}$,

$$a + (b + c) = (a + b) + c, \qquad a + b = b + a,$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \qquad a \cdot b = b \cdot a\,.$$

The set $\mathbb{N}$ has elements, denoted 0 and 1, whose properties are singled out,

$$0 + a = a, \qquad 1a = a$$

for any $a \in \mathbb{N}$. We give the following definition.

Definition A.2.4 Let $(G, *)$ be an algebraic structure.

(a) $(G, *)$ is called *associative* if

$$a * (b * c) = (a * b) * c$$

for any $a, b, c \in G$.

(b) $(G, *)$ is called *commutative* (or *abelian*) if

$$a * b = b * a$$

for any $a, b \in G$.

(c) An element $e \in G$ is called an *identity* (or a *neutral element*) for $(G, *)$ (and the algebraic structure is often denoted by $(G, *, e)$) if

$$e * a = a * e$$

for any $a \in G$.

(d) Let $(G, *, e)$ be an algebraic structure with an identity e. An element $b \in G$ such that

$$a * b = b * a = e$$

is called the *inverse* of a, and denoted by a^{-1}. The elements for which an inverse exists are called invertible.

Remark A.2.5 If the algebraic structure is given by a 'sum rule', like in $(\mathbb{N}, +)$, the neutral element is usually called a *zero* element, denoted by 0, with $a + 0 = 0 + a = a$. Also, the inverse of an element a is usually denoted by $-a$ and named the *opposite* of a.

Example A.2.6 It is easy to see that for the sets considered above one has $(\mathbb{N}, +, 0)$, $(\mathbb{N}, \cdot, 1)$, $(R, \circ, e)$. Every element in R is invertible (since one has $x \circ y = y \circ x = e$); the set $(\mathbb{N}, \cdot, 1)$ contains only one invertible element, which is the identity itself, while in $(\mathbb{N}, +, 0)$ no element is invertible.

From the defining relation (c) above one clearly has that if a^{-1} is the inverse of $a \in (G, *)$, then a is the inverse of a^{-1}. This suggests a way to enlarge sets containing elements which are not invertible, so to have a new algebraic structure whose elements are all invertible. For instance, one could define the set of *integer* numbers $\mathbb{Z} = \{\pm n : n \in \mathbb{N}\}$ and sees that every element in $(\mathbb{Z}, +, 0)$ is invertible.

Definition A.2.7 An algebraic structure $(G, *)$ is called a *group* when the following properties are satisfied

(a) the operation $*$ is associative,
(b) G contains an identity element e with respect to $*$,
(c) every element in G is invertible with respect to e.

A group $(G, *, e)$ is called *commutative* (or *abelian*) if the operation $*$ is commutative.

Remark A.2.8 Both $(\mathbb{Z}, +, 0)$ and $(R, \circ, e)$ are abelian groups.

Proposition A.2.9 *Let $(G, *, e)$ be a group. Then*

(i) the identity element is unique,
(ii) the inverse a^{-1} of any element $a \in G$ is unique.

Proof (i) Let us suppose that e, e' are both identities for $(G, *)$. Then it should be $e * e' = e$ since e' is an identity, and also $e * e' = e'$ since e is an identity; this would then mean $e = e'$.

(ii) Let b, c be both inverse elements to $a \in G$; this would give $a * b = b * a = e$ and $a * c = c * a = e$. Since the binary operation is associative, one has $b * (a * c) = (b * a) * c$, resulting in $b * e = e * c$ and then $b = c$. □

A.3 Rings and Fields

Next we introduce and study the properties of a set equipped with two binary operations—compatible in a suitable sense—which resemble the sum and the product of integer numbers in $\mathbb{Z}$.

Definition A.3.1 Let $A = (A, +, 0_A, \cdot, 1_A)$ be a set with two operations, called sum $(+)$ and product $(\cdot)$, with two distinguished elements called 0_A and 1_A. The set A is called a *ring* if the following conditions are satisfied:

(a) $(A, +, 0_A)$ is an abelian group,
(b) the product $\cdot$ is associative,
(c) 1_A is the identity element with respect to the product,
(d) one has $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for any $a, b, c \in A$.

If moreover the product is abelian, A is called an *abelian* ring.

Example A.3.2 The set $(\mathbb{Z}, +, 0, \cdot, 1)$ is clearly an abelian ring.

Definition A.3.3 By $\mathbb{Z}[X]$ one denotes the set of *polynomials* in the indeterminate (or variable) X with coefficients in $\mathbb{Z}$, that is the set of formal expressions,

$$\mathbb{Z}[X] = \left\{ \sum_{i=0}^{n} a_i X^i = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \,:\, n \in \mathbb{N},\ a_i \in \mathbb{Z} \right\}.$$

If $\mathbb{Z}[X] \ni p(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ then $a_0, a_1, \ldots, a_n$ are the *coefficients* of the polynomial $p(X)$, while the term $a_i X^i$ is a *monomial* of degree i. The *degree* of the polynomial $p(X)$ is the highest degree among those of its non zero monomials. If $p(X)$ is the polynomial above, its degree is n provided $a_n \neq 0$, and one denotes $\deg p(X) = n$. The two usual operations of sum and product in $\mathbb{Z}[X]$ are defined as follows. Let $p(X), q(X)$ be two arbitrary polynomials in $\mathbb{Z}[X]$,

$$p(X) = \sum_{i=0}^{n} a_i X^i, \qquad q(X) = \sum_{i=0}^{m} b_i X^i.$$

Let us suppose $n \leq m$. One sets

$$p(X) + q(X) = \sum_{j=0}^{m} c_j X^j,$$

with $c_j = a_j + b_j$ for $0 \leq j \leq n$ and $c_j = b_j$ for $n < j \leq m$. One would have an analogous results were $n \geq m$. For the product one sets

$$p(X) \cdot q(X) = \sum_{h=0}^{m+n} d_h X^h,$$

where $d_h = \sum_{i+j=h} a_i b_j$.

Proposition A.3.4 *Endowed with the sum and the product as defined above, the set $\mathbb{Z}[X]$ is an abelian ring, the ring of polynomials in one variable with integer coefficients.*

Proof One simply transfer to $\mathbb{Z}[X]$ the analogous structures and properties of the ring $(\mathbb{Z}, +, 0, \cdot, 1)$. Let $0_{\mathbb{Z}[X]}$ be the null polynomial, that is the polynomial whose coefficients are all equal to $0_{\mathbb{Z}}$, and let $1_{\mathbb{Z}[X]} = 1_{\mathbb{Z}}$ be the polynomial of degree 0 whose only non zero coefficient is equal to $1_{\mathbb{Z}}$. We limit ourselves to prove that $(\mathbb{Z}[X], +, 0_{\mathbb{Z}[X]})$ is an abelian group.

- Clearly, the null polynomial $0_{\mathbb{Z}[X]}$ is the identity element with respect to the sum of polynomials.
- Let us consider three arbitrary polynomials in $\mathbb{Z}[X]$,

$$p(X) = \sum_{i=0}^{n} a_i X^i, \quad q(X) = \sum_{i=0}^{m} b_i X^i, \quad r(X) = \sum_{i=0}^{p} c_i X^i.$$

We show that

$$\big(p(X) + q(X)\big) + r(X) = p(X) + \big(q(X) + r(X)\big).$$

For simplicity we consider the case $n = m = p$, since the proof for the general case is analogue. From the definition of sum of polynomials, one has

$$\begin{aligned} A(X) &= (p(X) + q(X)) + r(X) \\ &= \sum_{i=0}^{n} (a_i + b_i) X^i + \sum_{i=0}^{n} c_i X^i = \sum_{i=0}^{n} [(a_i + b_i) + c_i] X^i \end{aligned}$$

and

$$\begin{aligned} B(X) &= p(X) + (q(X) + r(X)) \\ &= \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} (b_i + c_i) X^i = \sum_{i=0}^{n} [a_i + (b_i + c_i)] X^i. \end{aligned}$$

The coefficients of $A(X)$ and $B(X)$ are given, for any $i = 0, \dots, n$, by

$$[(a_i + b_i) + c_i] \qquad \text{and} \qquad [a_i + (b_i + c_i)]$$

and they coincide being the sum in $\mathbb{Z}$ associative. This means that $A(X) = B(X)$.

- We show next that any polynomial $p(X) = \sum_{i=0}^{n} a_i X^i$ is invertible with respect to the sum in $\mathbb{Z}[X]$. Let us define the polynomial $p'(X) = \sum_{i=0}^{n} (-a_i) X^i$, with $(-a_i)$ denoting the inverse of $a_i \in \mathbb{Z}$ with respect to the sum. From the definition of the sum of polynomials, one clearly has

$$p(X) + p'(X) = \sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{n} (-a_i) X^i = \sum_{i=0}^{n} (a_i - a_i) X^i.$$

  Since $a_i - a_i = 0_{\mathbb{Z}}$ for any i, one has $p(X) + p'(X) = 0_{\mathbb{Z}[X]}$; thus $p'(X)$ is the inverse of $p(X)$.
- Finally, we show that the sum in $\mathbb{Z}[X]$ is abelian. Let $p(X)$ and $q(X)$ be two arbitrary polynomials in $\mathbb{Z}[X]$ of the same degree $\deg p(X) = n = \deg q(X)$ (again for simplicity); we wish to show that

$$p(X) + q(X) = q(X) + p(X).$$

  From the definition of sum of polynomials,

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

$$V(X) = q(X) + p(X) = \sum_{i=0}^{n} (b_i + a_i) X^i :$$

  the coefficients of $U(X)$ and $V(X)$ are given, for any $i = 0, \dots, n$ by

$$a_i + b_i \qquad \text{and} \qquad b_i + a_i$$

  which coincide since the sum is abelian in $\mathbb{Z}$. This means $U(X) = V(X)$.

We leave as an exercise to finish showing that $\mathbb{Z}[X]$ with the sum and the product above fulfill the conditions (b)–(d) in the Definition A.3.1 of a ring. □

Remark A.3.5 Direct computation show the following well known properties of the abelian ring $\mathbb{Z}[X]$ of polynomials. With $f(X), g(X) \in \mathbb{Z}[X]$ it holds that:

(i) $\deg(f(X) + g(X)) \leq \max\{\deg(f(X)), \deg(g(X))\}$;
(ii) $\deg(f(X) \cdot g(X)) = \deg(f(X)) + \deg(g(X))$.

It is easy to see that the set $(\mathbb{Q}, +, \cdot, 0, 1)$ of rational numbers is an abelian ring as well. The set $\mathbb{Q}$ has indeed a richer algebraic structure than $\mathbb{Z}$: any non zero element

$0 \neq a \in \mathbb{Q}$ is invertible with respect to the product. If $a = p/q$ with $p \neq 0$, then $a^{-1} = q/p \in \mathbb{Q}$.

Definition A.3.6 An abelian ring $K = (K, +, 0, \cdot, 1)$ such that each element $0 \neq a \in K$ is invertible with respect to the product $\cdot$, is called a *field*. Equivalently one sees that $(K, +, 0, \cdot, 1)$ is a field if and only if both $(K, +, 0)$ and $(K, \cdot, 1)$ are abelian groups and the product is *distributive* with respect to the sum, that is the condition (d) of the Definition A.3.1 is satisfied.

Example A.3.7 Clearly $(\mathbb{Q}, +, 0, \cdot, 1)$ is a field, while $(\mathbb{Z}, +, 0, \cdot, 1)$ is not. The fundamental example of a field for us will be the set $\mathbb{R} = (\mathbb{R}, +, 0, \cdot, 1)$ of real numbers equipped with the usual definitions of sum and product.

Analogously to the Definition A.3.3 one can define the sets $\mathbb{Q}[X]$ and $\mathbb{R}[X]$ of polynomials with rational and real coefficients. For them one naturally extends the definitions of sum and products, as well as that of degree.

Proposition A.3.8 *The set $\mathbb{Q}[X]$ and $\mathbb{R}[X]$ are both abelian rings.* □

It is worth stressing that in spite of the fact that $\mathbb{Q}$ and $\mathbb{R}$ are fields, neither $\mathbb{Q}[X]$ nor $\mathbb{R}[X]$ are such since a polynomial need not admit an inverse with respect to the product.

A.4 Maps Preserving Algebraic Structures

The Definition A.2.1 introduces the notion of algebraic structure $(G, *)$ and we have described what groups, rings and fields are. We now briefly deal with maps between algebraic structures of the same kind, which preserve the binary operations defined in them. We have the following definition

Definition A.4.1
A map $f : G \to G'$ between two groups $(G, *_G, e_G)$ and $(G', *_{G'}, e_{G'})$ is a *group homomorphism* if

$$f(x *_G y) = f(x) *_{G'} f(y) \qquad \text{for all} \quad x, y \in G.$$

A map $f : A \to B$ between two rings $(A, +_A, 0_A, \cdot_A, 1_A)$ and $(B, +_B, 0_B, \cdot_B, 1_B)$ is a *ring homomorphism* if

$$f(x +_A y) = f(x) +_B f(y), \qquad f(x \cdot_A y) = f(x) \cdot_B f(y) \qquad \text{for all} \quad x, y \in A.$$

Example A.4.2 The natural inclusions $\mathbb{Z} \subset \mathbb{Q}, \mathbb{Q} \subset \mathbb{R}$ are rings homomorphisms, as well as the inclusion $\mathbb{Z} \subset \mathbb{Z}[x]$ and similar ones.

Exercise A.4.3 The map $\mathbb{Z} \to \mathbb{Z}$ defined by $n \mapsto 2n$ is a group homomorphism with respect to the group structure $(\mathbb{Z}, +, 0)$, but not a ring homomorphism with respect to the ring structure $(\mathbb{Z}, +, 0, \cdot, 1)$.

To lighten notations, from now on we shall denote a sum by $+$ and a product by $\cdot$ (and more generally a binary operation by $*$), irrespectively of the set in which they are defined. It will be clear from the context which one they refers to.

Group homomorphisms present some interesting properties, as we now show.

Proposition A.4.4 *Let $(G, *, e_G)$ and $(G', *, e_{G'})$ be two groups, and $f : G \to G'$ a group homomorphism. Then,*

(i) $f(e_G) = e_{G'}$,
(ii) $f(a^{-1}) = (f(a))^{-1}$, *for any* $a \in G$.

Proof (i) Since e_G is the identity element with respect to the sum, we can write

$$f(e_G) = f(e_G * e_G) = f(e_G) * f(e_G),$$

where the second equality is valid as f is a group homomorphism. Being $f(e_G) \in G'$, it has a unique inverse (see the Proposition A.2.9), $(f(e_G))^{-1} \in G'$, that we can multiply with both sides of the previous equality, thus yielding

$$f(e_G) * (f(e_G))^{-1} = f(e_G) * f(e_G) * (f(e_G))^{-1}.$$

This relation results in

$$e_{G'} = f(e_G) * e_{G'} \quad \Rightarrow \quad e_{G'} = f(e_G).$$

(ii) Making again use of the Proposition A.2.9, in order to show that $(f(a))^{-1}$ is the inverse (with respect to the product in G') of $f(a)$ it suffices to show that

$$f(a) * (f(a))^{-1} = e_{G'}.$$

From the definition of group homomorphism, it is

$$f(a) * (f(a))^{-1} = f(a * a^{-1}) = f(e_G) = e_{G'}$$

where the last equality follows from (i).

If $f : A \to B$ is a ring homomorphism, the previous properties are valid with respect to both the sum and to the product, that is

(i') $f(0_A) = 0_B$ and $f(1_A) = 1_B$;
(ii') $f(-a) = -f(a)$ for any $a \in A$, while $f(a^{-1}) = (f(a))^{-1}$ for any invertible (with respect to the product) element $a \in A$ with inverse a^{-1}. □

If A, B are fields, a ring homomorphism $f : A \to B$ is called a *field homomorphism*. A bijective homomorphism between algebraic structures is called an *isomorphism*.

A.5 Complex Numbers

It is soon realised that one needs enlarging the field $\mathbb{R}$ of real numbers to consider zeros of polynomials with real coefficients. The real coefficient polynomial $p(x) = x^2 + 1$ has 'complex' zeros usually denoted $\pm\mathrm{i}$, and their presence leads to defining the field of complex numbers $\mathbb{C}$. One considers the smallest field containing $\mathbb{R}$, $\pm\mathrm{i}$ and all possible sums and products of them.

Definition A.5.1 The set of complex numbers is given by formal expressions

$$\mathbb{C} = \{z = a + \mathrm{i}b \mid a, b \in \mathbb{R}\}.$$

The real number a is called the *real part* of z, denoted $a = \Re(z)$; the real number b is called the *imaginary part* of z, denoted $b = \Im(z)$.

The following proposition comes as an easy exercise.

Proposition A.5.2 *The binary operations of sum and product defined in* $\mathbb{C}$ *by*

$$\begin{aligned}(a + \mathrm{i}b) + (c + \mathrm{i}d) &= (a + c) + \mathrm{i}(b + d),\\ (a + \mathrm{i}b) \cdot (c + \mathrm{i}d) &= (ac - bd) + \mathrm{i}(bc + ad)\end{aligned}$$

make $(\mathbb{C}, +, 0_{\mathbb{C}}, \cdot, 1_{\mathbb{C}})$ *a field, with* $0_{\mathbb{C}} = 0_{\mathbb{R}} + \mathrm{i}0_{\mathbb{R}} = 0_{\mathbb{R}}$ *and* $1_{\mathbb{C}} = 1_{\mathbb{R}} + \mathrm{i}0_{\mathbb{R}} = 1_{\mathbb{R}}$. □

Exercise A.5.3 An interesting part of the proof of the proposition above is to determine the inverse z^{-1} of the complex number $z = a + \mathrm{i}b$. One easily checks that

$$(a + \mathrm{i}b)^{-1} = \frac{a}{a^2 + b^2} - \mathrm{i}\frac{b}{a^2 + b^2} = \frac{1}{a^2 + b^2}\,(a - \mathrm{i}b).$$

Again an easy exercise establishes the following proposition.

Proposition A.5.4 *Given* $z = a + \mathrm{i}b \in \mathbb{C}$ *one defines its conjugate number to be* $\bar{z} = a - \mathrm{i}b$. *Then, for any complex number* $z = a + \mathrm{i}b$ *the following properties hold:*

(i) $\bar{\bar{z}} = z$,
(ii) $\bar{z} = z$ *if and only if* $z \in \mathbb{R}$,
(iii) $z\bar{z} = a^2 + b^2$,
iv) $z + \bar{z} = 2\Re(z)$. □

Exercise A.5.5 The natural inclusions $\mathbb{R} \subset \mathbb{C}$ given by $\mathbb{R} \ni a \mapsto a + \mathrm{i}0_{\mathbb{R}}$ is a field homomorphism, while the corresponding inclusion $\mathbb{R}[x] \subset \mathbb{C}[x]$ is a ring homomorphism.

Remark A.5.6 We mentioned above that the polynomial $x^2 + 1 = p(x) \in \mathbb{R}[x]$ cannot be decomposed (i.e. cannot be factorised) as a product of degree 1 polynomials in $\mathbb{R}[x]$, that is, with real coefficients. On the other hand, the identity

$x^2 + 1 = (x - \mathrm{i})(x + \mathrm{i}) \in \mathbb{C}[x]$ shows that the same polynomial can be decomposed into degree 1 terms if the coefficients of the latter are taken in $\mathbb{C}$. This is not surprising, since the main reason to enlarge the field $\mathbb{R}$ to $\mathbb{C}$ was exactly to have a field containing the zero of the polynomial $p(x)$.

What is indeed surprising is that the field $\mathbb{C}$ contains the zeros of *any* polynomial with real coefficients. This is the result that we recall as the next theorem.

Proposition A.5.7 (Fundamental theorem of algebra) *Let $f(x) \in \mathbb{R}[x]$ be a polynomial with real coefficients and* $\deg f(x) \geq 1$. *Then, $f(x)$ has at least a zero (that is a root) in $\mathbb{C}$. More precisely, if* $\deg f(x) = n$, *then $f(x)$ has n (possibly non distinct) roots in $\mathbb{C}$. If $z_1, \ldots, z_s$ are these distinct roots, the polynomial $f(x)$ can be written as*

$$f(x) = a(x - z_1)^{m(1)}(x - z_2)^{m(2)} \cdots (x - z_s)^{m(s)},$$

with the root multiplicities $m(j)$ for $j = 1, \ldots s$, such that

$$\sum_{j=1}^{s} m(j) = n.$$

That is the polynomial $f(x)$ it is completely factorisable on $\mathbb{C}$. □

A more general result states that $\mathbb{C}$ is an *algebraically closed* field, that is one has the following:

Theorem A.5.8 *Let $f(x) \in \mathbb{C}[x]$ be a degree n polynomial with complex coefficients. Then there exist n complex (non distinct in generall) roots of $f(x)$. Thus the polynomial $f(x)$ is completely factorisable on $\mathbb{C}$.* □

A.6 Integers Modulo A Prime Number

We have seen that the integer numbers $\mathbb{Z}$ form only a ring and not a field. Out of it one can construct fields of numbers by going to the quotient with respect to an equivalence relation of 'modulo an integer'. As an example, consider the set $\mathbb{Z}_3$ of integer modulo 3. It has three elements

$$\mathbb{Z}_3 = \{[0], [1], [2]\}$$

which one also simply write $\mathbb{Z}_3 = \{0, 1, 2\}$, although one should not confuse them with the corresponding classes.

One way to think of the three elements of $\mathbb{Z}_3$ is that each one represents the equivalence class of all integers which have the same remainder when divided by 3. For instance, [2] denotes the set of all integers which have remainder 2 when divided by 3 or equivalently, [2] denotes the set of all integers which are congruent to 2

modulo 3, thus $[2] = \{2, 5, 8, 11, \dots\}$. The usual arithmetic operations determine the addition and multiplication tables for this set as show in Table A.2.

$$\begin{array}{c|c|c|c} + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ \hline 1 & 1 & 2 & 0 \\ \hline 2 & 2 & 0 & 1 \end{array} \quad \text{and} \quad \begin{array}{c|c|c|c} * & 0 & 1 & 2 \\ \hline 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 2 \\ \hline 2 & 0 & 2 & 1 \end{array} . \tag{A.2}$$

Thus $-[1] = [2]$ and $-[2] = [1]$ and $\mathbb{Z}_3$ is an abelian group for the addition. Furthermore, $[1] * [1] = [1]$ and $[2] * [2] = [1]$ and both nonzero elements have inverse: $[1]^{-1} = [1]$ and $[2]^{-1} = [2]$. All of this makes $\mathbb{Z}_3$ a field.

The previous construction works when 3 is substituted with any *prime* number p. We recall that a positive integer p is called prime if it is only divisible by itself and by 1. Thus, for any prime number one gets the field of integers modulo p:

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{[0], [1], \dots, [p-1]\}.$$

Each of its elements represents the equivalence class of all integers which have the given remainder when divided by p. Equivalently, each element denotes the equivalence class of all integers which are congruent modulo p. The corresponding addition and multiplication tables, defines as in $\mathbb{Z}$ but now taken modulo p, can be easily worked out. Notice that the construction does not work, that is $\mathbb{Z}_p$ is not a ring, if p is not a prime number: were this the case there would be divisors of zero.

Index

G. Landi and A. Zampini, *Linear Algebra and Analytic Geometry for Physical Sciences*, Undergraduate Lecture Notes in Physics,
https://doi.org/10.1007/978-3-319-78361-1