Chapter 1

Fields

1.1 Motivation

Recall the times when you learned to solve a linear equation is one unknown, say,

$$3X + 6 = 18. \tag{1.1}$$

An equation "asks a question": which number x yields an equality between both sides of the equation when substituted for the unknown X. What did you do? As a first step, you determined that if "something" plus 6 equals 18, then that "something" had to be equal 12, namely, that every solution of (1.1) is also a solution of the equation

$$3X = 12.$$

Stated differently, you used the fact that since the two sides of an equation are by definition equal, then the equation will remain true if you subtract 6 from both sides. As a second step, you determined that if 3 times "something" equals 12, then by solving an unknown-factor problem, that "something" has to be equal 4, finally, leading to the solution

$$x = 4.$$

In fact, 4 is the unique solution to (1.1).

Note that there are quite a few underlying assumptions in this way of solving an equation. First, there is a notion of the two sides of an equation being

in some sense "the same". Second, this notion of equality justifies the fact that if the same operation is applied on both sides, then the results of this operation preserve the sameness of the two sides. Third, we assume the existence of the operations of addition and multiplication, and their inverses, subtraction and division. We used the fact if "unknown + number = number" then "unknown" can be determined uniquely, and similarly for "unknown × number = number" (unless if the first number is zero).

But even before that, what are numbers? In the above example, we make do with the natural numbers,

$$\mathbb{N} = \{1, 2, 3, \dots\},$$

with which we are acquainted since early childhood.

Does every linear equation with coefficients in $\mathbb{N}$ have a solution in $\mathbb{N}$? No. Consider the equation

$$X + 6 = 6.$$

It does not have solutions in $\mathbb{N}$. If we want this equation to be solvable, we must add to the natural numbers a new element, which we call *zero*, forming now a set of numbers $\mathbb{N} \cup \{0\}$.

Does every linear equation with coefficients in $\mathbb{N} \cup \{0\}$ have a solution in $\mathbb{N} \cup \{0\}$? No. Consider the equation

$$X + 8 = 6.$$

It does not have solutions in $\mathbb{N} \cup \{0\}$. If we want this equation to be solvable, we must introduce the **negative integers**, which together with the natural numbers and zero form the set of **integers** (**המספרים השלמים**),

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

(The letter "Z" stands for the German word *zahl*, which means number.)

Does every equation with coefficients in $\mathbb{Z}$ have a solution in $\mathbb{Z}$? No. The equations

$$4X = 3 \qquad \text{and} \qquad 4X = (-3)$$

do not have solutions in $\mathbb{Z}$. Requiring these equation to be solvable requires the introduction of the **rational numbers** (**המספרים הרציונליים**), which are denoted by $\mathbb{Q}$ (for *quotients*).

The set of rational numbers gives us already the ability to solve any equation of the form

$$aX + c = b,$$

where $a, b, c \in \mathbb{Q}$ as long as $a \neq 0$ (we will discuss the case of $a = 0$ later). Thus, the rational numbers are "complete" in the sense that any linear equation with coefficients in that set has a solution within that set.

The rational numbers are however not "complete" in other respects. More than two millennia ago, it was discovered that the quadratic equation $X^2 = 2$ does not have a solution within the set of rational numbers, leading eventually to the definition of the set of **real numbers** (**המספרים הממשיים**), which we denote by $\mathbb{R}$. The set of real numbers *extends* the set of rational numbers in a sense described in your Calculus class. And yet, even with this extension, there still exist "simple" equations that are not solvable, such as

$$X^2 = (-1).$$

This observation has eventually led to the further extension of the set of real numbers into the set of **complex numbers** (**המספרים המרוכבים**), which we denote by $\mathbb{C}$. The complex numbers are defined by introducing a new "number" $\imath$, satisfying $\imath^2 = (-1)$, and then considering all combinations $a + b\imath$, with $a, b \in \mathbb{R}$.

It should be noted that in the context of linear equations, denoting either $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ by the generic notation $\mathbb{F}$, every equation of the form

$$aX + c = b,$$

where $a, b, c \in \mathbb{F}$ has a unique solution in $\mathbb{F}$, provided that $a \neq 0$.

1.2 Definition of a field

This course starts with the problem of solving systems of linear equations; as we progress to higher levels of mathematics, we tend to abstract out concepts that were formerly used without a formal definition. By the end of the day, we want to do mathematics in a way that is independent of meaning. Thus, we ask ourselves what is it that we want "numbers" to satisfy in order to be able to solve linear equations featuring those numbers as coefficients. The answer is partly given above: whatever those numbers are, we want to be able

to perform on them all the operations we would do with "school numbers" to solve linear systems of equations.

This brings us to defining an algebraic structure called a **field** (שדה):

A field $\mathbb{F}$ is a set containing at least two *different* elements, which we call **zero** and **one**, and denote by $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$. These elements are endowed with two binary operations (**פעולות דו מקומיות**), which we call **addition** (חיבור) and **multiplication** (כפל).

A binary operation on a set can be viewed as a "machine" taking for input two elements in the set (in a prescribed order!), and returning for output an element in that set, such that the output is uniquely determined by the input. In the case where $a \in \mathbb{F}$ and $b \in \mathbb{F}$ are inputs for the addition operation, we denote the output by $a+b$. The statement that the output be determined by the input can be formalized into stating that to every $a, b \in \mathbb{F}$ there corresponds a unique $c \in \mathbb{F}$, such that $c = a + b$[1]. Likewise, if $a \in \mathbb{F}$ and $b \in \mathbb{F}$ are inputs for the multiplication operation, we denote the output by $a \cdot b$; to every $a, b \in \mathbb{F}$ there corresponds a unique $c \in \mathbb{F}$, such that $c = a \cdot b$.

For $\mathbb{F}$ to be a field, more structure has a to be incorporated: addition and multiplication have to satisfy nine properties, called the **axioms of field** (**אקסיומות השדה**). Before stating the axioms, we should note that both addition and multiplication only act, by definition, on pairs of elements. Thus, there is no meaning at this point to adding or multiplying three or more elements. A binary operation can be extended to an operation on any (finite) number of elements in a **recursive** way. Let $a, b, c \in \mathbb{F}$. Their sum can be defined by taking the sum of $a+b$ and adding it to c. This repeated application of the binary operation of addition is denoted using parentheses,

$$(a + b) + c.$$

This is however not the only alternative: we could have also added a to the sum of b and c, the result of this compound action being denoted by

$$a + (b + c).$$

With that, we spell out the first four axioms, which are pertinent to addition:

[1] Throughout this text we will use the standard notation of set theory: if A is a set, then $a \in A$ means that a is an element in A, or that a belongs to A. For two sets A and B, the relation $A \subseteq B$ means that A is a subset of B, implying that every element in A is also an element in B; note that this relation holds also if $A = B$. In fact $A = B$ means that both $A \subseteq B$ and $B \subseteq A$.

1. Addition is **associative** (**קיבוצי**): for all $a, b, c \in \mathbb{F}$,

$$(a + b) + c = a + (b + c). \tag{A1}$$

2. Addition is **commutative** (**חילופי**): for all $a, b \in \mathbb{F}$,

$$a + b = b + a. \tag{A2}$$

3. Zero is **neutral** to addition: for all $a \in \mathbb{F}$,

$$a + 0_{\mathbb{F}} = a. \tag{A3}$$

4. Every element $a \in \mathbb{F}$ has an **additive inverse** (**איבר נגדי**), which we denote by $(-a) \in \mathbb{F}$, satisfying

$$a + (-a) = 0_{\mathbb{F}}. \tag{A4}$$

The next four axioms are analogous (with one big difference!) and pertinent to multiplication:

5. Multiplication is associative: for all $a, b, c \in \mathbb{F}$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c). \tag{M1}$$

6. Multiplication is commutative: for all $a, b \in \mathbb{F}$,

$$a \cdot b = b \cdot a. \tag{M2}$$

7. One is neutral to multiplication: for all $a \in \mathbb{F}$,

$$a \cdot 1_{\mathbb{F}} = a. \tag{M3}$$

8. Every non-zero (!!!) element $0_{\mathbb{F}} \neq a \in \mathbb{F}$ has a **multiplicative inverse** (**איבר הפכי**), which we denote by $a^{-1} \in \mathbb{F}$, satisfying

$$a \cdot a^{-1} = 1_{\mathbb{F}}. \tag{M4}$$

Finally, the ninth axiom links between addition and multiplication:

9. Multiplication is **distributive** (פילוגי) over addition: for all $a, b, c \in \mathbb{F}$,
$$a \cdot (b + c) = a \cdot b + a \cdot c. \tag{D}$$

Comments:

(a) Elements of a field are called **scalars** (סקלרים) (rather than numbers).

(b) When no ambiguity occurs, we may denote the product of two elements by ab rather than by $a \cdot b$.

(c) We denoted the elements zero and one by $0_{\mathbb{F}}$ and $1_{\mathbb{F}}$ to emphasize that they may differ from the *numbers* zero and one. Nevertheless, when no confusion arises, we may revert to the more standard notation 0 and 1.

(d) A priori, a scalar may be its own additive and/or multiplicative inverse. In fact, $0_{\mathbb{F}}$ is always its own additive inverse and $1_{\mathbb{F}}$ is always its own multiplicative inverse. We will shortly see an example in which $1_{\mathbb{F}}$ is also its own additive inverse.

(e) **Subtraction** (חיסור) is defined as the addition of the additive inverse,
$$a - b = a + (-b),$$
whereas **division** (חילוק) (by a nonzero divisor) is defined as the multiplication by the multiplicative inverse,
$$a \div b = ab^{-1}.$$

Exercises

(easy) 1.1 S is a set. S claims to be a field. List all the properties you should check in order to verify whether S's claim is correct.

(easy) 1.2 Draw an "addition machine", which is a box having two input ports (labeled Input 1 and Input 2) and one output port. Combine two such machines to generate the output $(a + b) + c$. Combine two such machines to generate the output $a + (b + c)$.

(easy) 1.3 Let $\mathbb{F}$ be a field. Prove that for every $a \in \mathbb{F}$,
$$0_{\mathbb{F}} - a = (-a).$$
Likewise, prove that for every $\mathbb{F} \ni a \neq 0_{\mathbb{F}}$,
$$1_{\mathbb{F}} \div a = a^{-1}.$$

1.3 Examples

Example: We are already acquainted with three fields, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. Since

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

this may give the impression that all the fields in the world form a hierarchy of inclusions. This is not the case, as the next example shows. ▲▲▲

Example: A field is fully determined by its elements, and its tables of addition and multiplication. The smallest possible field is one consisting of just two elements, zero and one, along with the addition and multiplication tables:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

It takes some explicit verification to check that this is indeed a field (do you recognize it?). This field is commonly denoted by $\mathbb{F}_2$. That addition and multiplication are commutative is apparent by the symmetry of the tables. The neutrality of zero and one is also apparent. For associativity and distributivity we actually have to examine all the cases. Finally, 0 is its own additive inverse and 1 is both its own additive and multiplicative inverses. ▲▲▲

Exercises

(intermediate) 1.4 Consider a set consisting of three elements $\{0, 1, 2\}$ along with two binary operations defined by

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

How many verifications need to be done to determine whether it is a field (without taking shortcuts)? Verify that this is indeed a field (and you may take shortcuts). This field is commonly denoted by $\mathbb{F}_3$.

(harder) 1.5 Construct a field having four elements. Hint: construct first the multiplication table. Then, construct addition tables and show that only one of them is consistent with all axioms.

(easy) 1.6 Consider the following set

$$S = \{(1, a) \ : \ a \in \mathbb{R}\},$$

along with two binary operations,

$$(1, a) \oplus (1, b) = (1, a + b) \qquad \text{and} \qquad (1, a) \odot (1, b) = (1, ab),$$

where the addition and the multiplication on the right-hand sides are the standard addition and multiplication in $\mathbb{R}$.

(a) Does S have an element neutral to $\oplus$?

(b) Does S have an element neutral to $\odot$?

(c) Is S with $\oplus$ and $\odot$ a field.

(intermediate) 1.7 Consider the following set

$$T = \{(a, b) \ : \ a, b \in \mathbb{R}\},$$

along with two binary operations,

$$(a, b) \oplus (c, d) = (a + c, b + d) \qquad \text{and} \qquad (a, b) \odot (c, d) = (ac, bd),$$

where the addition and the multiplication on the right-hand sides are the standard addition and multiplication in $\mathbb{R}$.

(a) Does T have an element neutral to $\oplus$?

(b) Does T have an element neutral to $\odot$?

(c) Is T with $\oplus$ and $\odot$ a field.

1.4 Solvability of linear equations

We next show that every linear equation in one unknown with parameters in a field has a unique solution within that field:

Theorem 1.1 *Let $\mathbb{F}$ be a field and let $a, b, c \in \mathbb{F}$ with $a \neq 0_{\mathbb{F}}$. Then, the linear equation*

$$aX + c = b$$

has a solution and this solution is unique.

Proof: There are two claims to be proved: first, that there exists an $x \in \mathbb{F}$ such that

$$ax + c = b,$$

and second, that if $x, y \in \mathbb{F}$ both satisfy

$$ax + c = b \qquad \text{and} \qquad ay + c = b,$$

then $x = y$.

For existence, $x = a^{-1}\big(b + (-c)\big)$ is a solution, as

$$\begin{aligned} a\left(a^{-1}\big(b + (-c)\big)\right) + c &\overset{(M1)}{=} (aa^{-1})\big(b + (-c)\big) + c \\ &\overset{(M4)}{=} 1_{\mathbb{F}} \cdot \big(b + (-c)\big) + c \\ &\overset{(M3)}{=} \big(b + (-c)\big) + c \\ &\overset{(A1)}{=} b + \big(c + (-c)\big) \\ &\overset{(A4)}{=} b + 0_{\mathbb{F}} \\ &\overset{(A3)}{=} b. \end{aligned}$$

(Be sure to understand the justification of each passage.)

To prove uniqueness, suppose that

$$ax + c = b \qquad \text{and} \qquad ay + c = b.$$

Since both left-hand sides equal to b, they are equal, i.e.,

$$ax + c = ay + c.$$

We now proceed with the following deductions:

$$\begin{aligned}(ax + c) + (-c) &= (ay + c) + (-c)\\ ax + (c + (-c)) &= ay + (c + (-c))\\ ax + 0_{\mathbb{F}} &= ay + 0_{\mathbb{F}}\\ ax &= ay\\ a^{-1}(ax) &= a^{-1}(ay)\\ (a^{-1}a)x &= (a^{-1}a)y\\ 1_{\mathbb{F}} \cdot x &= 1_{\mathbb{F}} \cdot y\\ x &= y.\end{aligned}$$

(Be sure you understand why we had to assume that $a \neq 0_{\mathbb{F}}$ both for the existence and the uniqueness.) ■

The above proposition has a number of implications pertinent to any field:

Corollary 1.2 (Uniqueness of zero) *If there exist $b, x \in \mathbb{F}$ such that*

$$x + b = b,$$

then $x = 0_{\mathbb{F}}$.

Proof: Consider the linear equation

$$X + b = b.$$

Since $x = 0_{\mathbb{F}}$ is a solution of this equation, it follows from the uniqueness property that $x + b = b$ implies that $x = 0_{\mathbb{F}}$. ■

Corollary 1.3 (Uniqueness of the additive inverse) *If there exist $b, x \in \mathbb{F}$ such that*

$$x + b = 0_{\mathbb{F}},$$

then $x = (-b)$ (in other words, the additive inverse is unique).

Proof: Consider the linear equation

$$X + b = 0_{\mathbb{F}}.$$

Since $x = (-b)$ is a solution of this equation, it follows from the uniqueness property that $x + b = 0_{\mathbb{F}}$ implies that $x = (-b)$. ■

Exercises

(easy) 1.8 Prove that if there exist $a, x \in \mathbb{F}$, $a \neq 0$, such that

$$x \cdot a = a,$$

then $x = 1_{\mathbb{F}}$.

(easy) 1.9 Prove that if there exist $a, x \in \mathbb{F}$ such that

$$x \cdot a = 1_{\mathbb{F}},$$

then $x = a^{-1}$ (in other words, the multiplicative inverse is unique).

(harder) 1.10 Let $\mathbb{F}$ be a field. Prove that for every $a \in \mathbb{F}$,

$$a \cdot 0_{\mathbb{F}} = 0_{\mathbb{F}}.$$

Hint: consider the equation $X + a \cdot 0_{\mathbb{F}} = a \cdot 0_{\mathbb{F}}$ and show that $x = 0_{\mathbb{F}}$ and $x = 0_{\mathbb{F}} \cdot a$ are both solutions, hence must be equal.

(harder) 1.11 Let $\mathbb{F}$ be a field. Prove that for every $a, b \in \mathbb{F}$,

$$ab = 0_{\mathbb{F}} \qquad \text{if and only if} \qquad a = 0_{\mathbb{F}} \quad \text{or} \quad b = 0_{\mathbb{F}}.$$

Comment: the word *or* has a different meaning in mathematics than in our daily language. The "mathematical" *or* is inclusive: in this case, either $a = 0_{\mathbb{F}}$, or $b = 0_{\mathbb{F}}$ or both $a = b = 0_{\mathbb{F}}$. Hint: there are two separate claims to prove; formulate each claim separately.

(intermediate) 1.12 Let $\mathbb{F}$ be a field. Prove that for every $a, b, c, d \in \mathbb{F}$

(a) $-(-a) = a$.
(b) $(a^{-1})^{-1} = a$.
(c) $(-1)a = (-a)$.
(d) $(-0) = 0$.
(e) $a \neq 0$ if and only if $(-a) \neq 0$.
(f) $a = b$ if and only if $a - b = 0$.
(g) $-(a + b) = -a - b$.

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

(i) $(-a)b = a(-b) = -(ab)$.

(j) $(-a)(-b) = ab$.

(k) $a \cdot a = 1$ if and only if $a = 1$ or $a = -1$.

(l) $a \cdot a = b \cdot b$ if and only if $a = b$ or $a = -b$.

(m) If $a, b \neq 0$ then $(ab)^{-1} = a^{-1}b^{-1}$.

(n) If $a \neq 0$ then $0/a = 0$.

(o) $a/1 = a$.

(p) If $b, d \neq 0$ then $a/b = c/d$ if and only if $ad = bc$.

(q) If $b, d \neq 0$ then $(b/d)^{-1} = d^{-1}/b^{-1}$.

(r) If $b, d \neq 0$ then $(a/b)(c/d) = (ac)/(bd)$.

(s) If $b, d \neq 0$ then $a/b + c/d = (ad+bc)/(bd)$.

1.5 Equality as an equivalence relation

One of the hidden assumptions throughout this section is the properties of the equality sign, and its consistency with the operations of addition and multiplication. Equality is an instance of an **equivalence relation** (יחס שקילות). By that we mean the following:

(a) Every element in a set is equal to itself, i.e., for every $a \in \mathbb{F}$,

$$a = a.$$

(This property of being equivalent to oneself called **reflexivity**.)

(b) Equality is **symmetric**: for all $a, b \in \mathbb{F}$,

$$a = b \qquad \text{implies} \qquad b = a.$$

(c) Equality is **transitive**: for every $a, b, c \in \mathbb{F}$,

$$a = b \quad \text{and} \quad b = c \qquad \text{imply} \qquad a = c.$$

You will encounter many equivalence relations throughout your studies, including in this course.

Moreover, we assume that addition and multiplication are consistent with this notion of equivalence, namely, for all $a, b, c \in \mathbb{F}$,

$$a = b \qquad \text{implies} \qquad a + c = b + c,$$

and

$$a = b \qquad \text{implies} \qquad a \cdot c = b \cdot c.$$

This assumption is the basis for the practice of adding the same term to both sides of an equation.

Exercises

(easy) 1.13 Show that

$$a = b \quad \text{and} \quad c = d \qquad \text{implies} \qquad a + c = b + d,$$

and

$$a = b \quad \text{and} \quad c = d \qquad \text{implies} \qquad a \cdot c = b \cdot d.$$

1.6 Extended associativity and commutativity

Associativity for finite sums The associativity of addition (and similarly of multiplication) assert that for every three scalars $a, b, c \in \mathbb{F}$

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

What about the addition of four scalars. Without switching the order of the addends, we have the following alternative ways of adding up four addends $a, b, c, d \in \mathbb{F}$,

$$\begin{gathered} ((a + b) + c) + d \qquad (a + (b + c)) + d \qquad (a + b) + (c + d) \\ a + ((b + c) + d) \qquad a + (b + (c + d)) \end{gathered} \tag{1.2}$$

The associativity of addition generalizes to any number of addends. If there are n addends, then $n-2$ pairs of parentheses are needed in order to prescribe

the order of summation. The generalized law of associativity (which follows from the associativity for 3 addends) asserts that addends may be grouped in any order, always yielding the same sum.

The summation sign Let $a_1, \ldots, a_n \in \mathbb{F}$, where n may be any natural number. We may denote their sum by

$$a_1 + a_2 + \cdots + a_n.$$

While this notation may be self-explanatory. there may be cases where the use of an ellipsis (three dots) is ambiguous. The more formal way or writing this sum is

$$\sum_{i=1}^{n} a_i \qquad \text{or} \qquad \sum_{1 \le i \le n} a_i,$$

which we read as "the sum of all a_i's where i ranges from one to n". Formally, this sum is defined inductively (**הגדרה אינדוקטיבית**) as follows:

$$\sum_{i=1}^{1} a_i = a_1,$$

and for all $n > 1$,

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n-1} a_i + a_n.$$

Note that such a definition is meaningful even if the operation is nor associative nor commutative.

Example: Let's follow the inductive definition for

$$x = \sum_{i=1}^{4} i(i+1).$$

Unfolding the recursion we obtain

$$\begin{aligned}
\sum_{i=1}^{4} i(i+1) &= \sum_{i=1}^{3} i(i+1) + 4 \cdot 5 \\
&= \left(\sum_{i=1}^{2} i(i+1) + 3 \cdot 4 \right) + 4 \cdot 5 \\
&= \left(\left(\sum_{i=1}^{1} i(i+1) + 2 \cdot 3 \right) + 3 \cdot 4 \right) + 4 \cdot 5 \\
&= ((1 \cdot 2 + 2 \cdot 3) + 3 \cdot 4) + 4 \cdot 5.
\end{aligned}$$

▲ ▲ ▲

Commutativity for finite sums Commutativity is inherently a binary property. As such it can only be generalized to multiple addends (or factors) when combined with associativity. The generalized law of commutativity and associativity can be formalized as follows: let $a_1, \ldots, a_n \in \mathbb{F}$ be a collection of scalars. Let σ be a **permutation** (תמורה): σ is a function taking for input an index $\{1, \ldots, n\}$ and returning an index is that same set, such that every index is mapped to a distinct index. That is, $a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}$ is a reordering of $a_1, \ldots, a_n \in \mathbb{F}$. The generalized law of commutativity asserts that

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} a_{\sigma(i)}.$$

Example: Let $n = 5$ and let $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, $\sigma(4) = 2$ and $\sigma(5) = 5$. Then,

$$\sum_{i=1}^{5} a_{\sigma(i)} = a_3 + a_1 + a_4 + a_2 + a_5.$$

▲ ▲ ▲

Let $a_1, a_2, \ldots, a_n \in \mathbb{F}$ and $b_1, b_2, \ldots, b_n \in \mathbb{F}$. It can be shown inductively on n that

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i + b_i).$$

Likewise, for $c \in \mathbb{F}$,

$$c\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} (c\, a_i).$$

n-tuples of field elements We consider the set of all ordered n-tuples of element of a field, i.e., elements of the form

$$(a_1, \ldots, a_n),$$

where $a_i \in \mathbb{F}$ for all $i = 1, \ldots, n$. We denote this set by

$$\mathbb{F}^n = \{(a_1, \ldots, a_n) \ : \ a_i \in \mathbb{F}, \ \ i = 1, \ldots, n\}.$$

More generally, let S be a set, then

$$S^n = \{(s_1, \ldots, s_n) \ : \ s_i \in S, \ \ i = 1, \ldots, n\}.$$

For reasons that will become apparent later in this course, we will sometimes write n-tuples of scalars as columns delimited by square brackets; we denote this set by

$$\mathbb{F}^n_{\text{col}} = \left\{ \begin{bmatrix} x^1 \\ \vdots \\ x^n \end{bmatrix} \ : \ x^i \in \mathbb{F}, \ \ i = 1, \dots, n \right\}.$$

At other times, the scalars will be arrange in a row delimited by square brackets, and we denote this set by

$$\mathbb{F}^n_{\text{row}} = \left\{ \begin{bmatrix} a_1 & \dots & a_n \end{bmatrix} \ : \ a_i \in \mathbb{F}, \ \ i = 1, \dots, n \right\}.$$

At times, when writing columns is calligraphically annoying we will write

$$\begin{bmatrix} x^1 & \dots & x^n \end{bmatrix}^T = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

The reasons for this apparent nonsense (who cares about the form of parentheses and why write scalars in columns?) will be clarified later on.

Exercises

(easy) 1.14 Let S be a set. Describe the sets $(S^2)^3$ and $(S^3)^2$.

(easy) 1.15 Prove that all five ways of adding four addends in (1.2) yield the same sum.

(intermediate) 1.16 Prove using an inductive argument that

$$\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i + b_i).$$

(intermediate) 1.17 Prove that for every $1 < k < n$.

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{k} a_i + \sum_{i=k+1}^{n} a_i.$$

Hint: use an inductive argument on k.

(intermediate) 1.18 Calculate the following sums

(a) $\sum_{n=3}^{20} (k \cdot k - (k-1) \cdot (k-1))$.
(b) $\sum_{n=1}^{99} \frac{1}{n(n+1)}$.

Hint: you're not supposed to carry out tedious calculations.

(intermediate) 1.19 Unfold and evaluate the following sum,

$$S = \sum_{i=1}^{3} \left(\sum_{j=1}^{i} (i + 2j) \right).$$

(harder) 1.20 Let

$$\{a_{ij} \in \mathbb{F} \ : \ 1 \leq i \leq n, \quad 1 \leq j \leq m\}$$

be a set of mn scalars. Show that

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} \right) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij} \right).$$

(This equality is an instance of **Fubini's theorem** which you will encounter later in your studies in different contexts.)

(harder) 1.21 Let

$$\{a_{ij} \in \mathbb{F} \ : \ 1 \leq i \leq n, \quad 1 \leq j \leq n\}$$

be a set of n^2 scalars. Show that

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{i} a_{ij} \right) = \sum_{j=1}^{n} \left(\sum_{i=j}^{n} a_{ij} \right).$$

(harder) 1.22 True or false? For every $n \in \mathbb{N}$ and sequences $a_1, \ldots, a_n$, $b_1, \ldots, b_n$,

$$\left(\sum_{i=1}^{n} a_n \right) \left(\sum_{i=1}^{n} b_n \right) = \sum_{i=1}^{n} a_n b_n.$$