C. Fields

By a **field** one means a set $\mathbb{K}$ equipped with two operations: addition and multiplication. Both are assumed to be commutative and associative, and satisfying the distributive law: $a(b+c) = ab+ac$. Besides, it is required that there exist elements 0 and $1 \neq 0$ such that $a+0 = a$ and $1a = a$ for all $a \in \mathbb{K}$. Then, it is required that every $a \in \mathbb{K}$ has the opposite $-a$ such that $-a+a = 0$, and that every *non-zero* $a \in \mathbb{K}$ has its *inverse* a^{-1} such that $a^{-1}a = 1$. To the examples of fields $\mathbb{C}$ and $\mathbb{R}$, we can add (omitting many other available examples): the field $\mathbb{Q}$ of rational numbers; the field $\mathcal{A} \subset \mathbb{C}$ of all **algebraic numbers** (i.e. roots of polynomials in one variable with rational coefficients); the field $\mathbb{Z}_p$ of integers modulo a given prime number p (see Exercises). For instance, the set $\mathbb{Z}_2 = \{0, 1\}$ of remainders modulo 2 with the usual arithmetic of remainders ($0+0 = 0 = 1+1$, $0+1 = 1 = 1+0$, $0 \cdot 0 = 1 \cdot 0 = 0 \cdot 1 = 0$, $1 \cdot 1 = 1$) can be taken on the role of scalars. This gives rise to the definition of $\mathbb{Z}_2$-vector spaces useful in computer science and logic.

To reiterate: it is essential that division by all non-zero scalars is defined. Therefore the set $\mathbb{Z}$ of all integers and the set $\mathbb{F}[x]$ of all polynomials in one indeterminate x with coefficients in a field $\mathbb{F}$ are not fields, and do not qualify on the role of scalars in the definition of vector spaces, because the division is not always possible. However the field $\mathbb{Q}$ of all rational numbers and the field $\mathbb{F}(x)$ of all rational functions with coefficients in a field $\mathbb{F}$ are O.K.

EXERCISES

388. Can a field have only one element? ϟ

389. Verify that $\mathbb{Z}_2$ is a field.

390. Prove uniqueness of the zero element, the unit element, the opposite and the inverse to a given element. ϟ

391. Given two integers a and $b > 0$, let q and r be respectively the quotient and remainder from the division of a by b, i.e. $a = qb + r$, where $0 \leq r < b$. Show that the set of common divisors of a and b coincides with the set of common divisors of b and r.

392. Prove that for any two integers a and b, there exists a non-negative integer d (often denoted (a, b) and called the **greatest common divisor** of a and b) such that the set of common divisors of a and b coincides with the set of all divisors of d. ✓

393. Prove that the greatest common divisor (a, b) of two integers a and b is representable in the form $d = ka + lb$, where k, l are some integers. ✓

394. Let n be a positive integer. Call integers a and b **congruent modulo** n (and write $a \cong b \mod n$) if $a - b$ is divisible by n. Prove that if $a \cong b \mod n$ and $a' \cong b' \mod n$ then $a+a' \cong b+b' \mod n$ and $ab \cong a'b' \mod n$.

395. Denote by $\mathbb{Z}_n$ the set of congruence classes of integers modulo n. Show that addition and multiplication of integers descends to the addition and multiplication on $\mathbb{Z}_n$. ϟ

396. How many elements does $\mathbb{Z}_n$ have? ✓

397. Find all invertible elements and their multiplicative inverses in $\mathbb{Z}_5$.

398. The same for $\mathbb{Z}_8$. ✓

399. Prove that the congruence class of an integer a has a multiplicative inverse in $\mathbb{Z}_n$ if and only if a is relatively prime to n. ϟ

400. Prove that $\mathbb{Z}_n$ is a field if and only if n is prime.

401. By definition, a **homomorphism** $f : \mathbb{F} \to \mathbb{K}$ is a map respecting the operations: $f(a + b) = f(a) + f(b)$ and $f(ab) = f(ab) = f(a)f(b)$ for all $a, b \in \mathbb{F}$. Prove that a non-zero homomorphism between two fields is necessarily injective. ϟ

402. Show that numbers of the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Q}$, form a subfield in $\mathbb{R}$.

403. Prove that every field $\mathbb{K}$ contains a unique subfield isomorphic to $\mathbb{Q}$ or one of $\mathbb{Z}_p$, where p is prime. (One calls $\mathbb{K}$ a fields of **characteristic** p in the latter case, and of characteristic 0 in the former.) ϟ

404.* Show that there is a field $\mathbb{F}_4$ of four elements. ϟ

405. Find all roots of the polynomial $x^2 + x + 1$ in $\mathbb{F}_4$. ϟ

D. Examples of Vector Spaces

The axiomatic definition of vector spaces is *doubly* abstract: not only it neglects to specify the set $\mathcal{V}$ of vectors, but it does not even tell us anything explicit about the nature of the operations of addition of vectors and multiplication of vectors by scalars. To find various examples of vector spaces we should figure out which operations would be good candidates to satisfy the axioms (i–vii). It turns out that in the majority of useful examples, the operations are *pointwise addition of functions and multiplication of functions by scalars.*

`Example 1.` Let S be *any* set, and $\mathcal{V}$ be the set of *all* functions on S with values in $\mathbb{K}$. We will denote this set by $\mathbb{K}^S$. The sum and multiplication by scalars are defined on $\mathbb{K}^S$ as pointwise operations with functions. Namely, given two functions f, g and a scalar λ, the values of the sum $f+g$ and the product λf at a point $s \in S$ are

$$(f+g)(s) = f(s) + g(s),\ \ (\lambda f)(s) = \lambda(f(s)).$$

It is immediate to check that $\mathcal{V} = \mathbb{K}^S$ equipped with these operations satisfies the axioms (i–vii). Thus $\mathbb{K}^S$ is a $\mathbb{K}$-vector space.

`Example 1a.` Let S be the set of n elements $1, 2, ..., n$. Then the space $\mathbb{K}^S$ is the space $\mathbb{K}^n$ (e.g. $\mathbb{R}^S = \mathbb{R}^n$ and $\mathbb{C}^S = \mathbb{C}^n$) of **coordinate vectors**. Namely, each function on the set $\{1, \dots, n\}$ is specified by a string $\mathbf{x} = (x_1, ..., x_n)$ of its values, called **coordinates** or **components** of the coordinate vector. By tradition, the string is written as a **column**, and the pointwise operations with functions turn into termwise operations with the columns:

$$\lambda \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{bmatrix}, \quad \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}.$$

`Example 1b.` Let S be the set of all ordered pairs (i, j), where $i = 1, ..., m,\ j = 1, ..., n$. Then the vector space $\mathbb{K}^S$ is the space of $m \times n$-**matrices**. By tradition, a matrix is denoted by an upper-case letter, e.g. A, and is represented by a rectangular array whose **entry** at the intersection of the ith row and jth column is an element of $\mathbb{K}$ denoted by a_{ij} (the same lower-case letter with subscripts):

$$A = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & a_{ij} & \vdots \\ a_{m1} & \dots & a_{mn} \end{bmatrix}.$$

The pointwise operations with matrices as functions turn into elementwise addition of the arrays and their multiplication by scalars.

`Example 2.` Recall that a subset $\mathcal{W}$ in a vector space $\mathcal{V}$ is called a **linear subspace** (or simply **subspace**) if linear combinations $\lambda\mathbf{u} + \mu\mathbf{v}$ of vectors from $\mathcal{W}$ with arbitrary coefficients lie in $\mathcal{W}$, and that a subspace of a vector space is a vector space on its own with respect to the same operations as those in $\mathcal{V}$. Thus, a subspace of $\mathbb{K}$-vector space is an example of a $\mathbb{K}$-vector space.

`Example 2a.` An $m \times n$-matrix is called **square**, if $m = n$. A square matrix A is called **diagonal** (respectively, **upper-triangular**, or **lower-triangular**) if $a_{ij} = 0$ whenever $i \neq j$ (respectively, $i > j$, or $i < j$). Diagonal (respectively, upper-triangular, or lower-triangular) matrices form a subspace in the space of all $n \times n$-matrices, and therefore provide an example of a vector space.

`Example 2b.` The set of all polynomials (say, in one variable),[17] form a subspace in the space $\mathbb{R}^{\mathbb{R}}$ of all real-valued functions on the number line and therefore provide examples of real vector spaces. More generally, polynomials with coefficients in $\mathbb{K}$ (as well as such polynomials of degree not exceeding 7) form examples of $\mathbb{K}$-vector spaces.

`Example 3.` Let $\mathcal{V}$ be a $\mathbb{K}$-vector space. Consider the set $\mathcal{V}^S$ of all functions on a given set S with values in $\mathcal{V}$. Elements of $\mathcal{V}$ can be added and multiplied by scalars. Respectively the *vector-valued* functions can be added and multiplied by scalars in the pointwise fashion. Thus, $\mathcal{V}^S$ is an example of a $\mathbb{K}$-vector space.

Recall that a function $A : \mathcal{V} \to \mathcal{W}$ from a vector space $\mathcal{V}$ to a vector space $\mathcal{W}$ is called a **linear map** if it *respects* the operations with vectors, i.e. if it maps linear combinations of vectors to linear combinations of their images with the same coefficients:

$$A(\lambda\mathbf{u} + \mu\mathbf{v}) = \lambda A\mathbf{u} + \mu A\mathbf{v} \quad \text{for all } \mathbf{u}, \mathbf{v} \in \mathcal{V} \text{ and } \lambda, \mu \in \mathbb{K}.$$

`Example 3a.` Linear combinations $\lambda A + \mu B$ of linear maps $A, B : \mathcal{V} \to \mathcal{W}$ are linear. Therefore all linear maps from $\mathcal{V}$ to $\mathcal{W}$ form a subspace in the space $\mathcal{W}^{\mathcal{V}}$ of all vector-valued functions $\mathcal{V} \to \mathcal{W}$. The vector space of linear maps from $\mathcal{V}$ to $\mathcal{W}$ is usually denoted

[17] As well as sets of all continuous, differentiable, 5 times continuously differentiable, infinitely differentiable, Riemann-integrable, measurable, etc. functions, introduced in mathematical analysis.

by$\mathrm{Hom}(\mathcal{V},\mathcal{W})$ (from the word *homomorphism*, synonimous in our context to the term *linear map*.

`Example 3b.` By the very definition, $Hom(\mathcal{V},\mathbb{K})$ is the space of all $\mathbb{K}$-linear forms $\mathcal{V}\to\mathbb{K}$, which is called the **dual space** to $\mathcal{V}$ and is usually denoted by $\mathcal{V}^*$.

The following formal construction indicates that *every vector space can be identified with a subspace in a space of functions with pointwise operations of addition and multiplication by scalars.*

`Example 3c.` Given a vector $\mathbf{v}\in\mathcal{V}$ and a linear function $f\in\mathcal{V}^*$, the value $f(\mathbf{v})\in\mathbb{K}$ is defined. We can consider it not as a function f of $\mathbf{v}$, but as a function of f defined by $\mathbf{v}$. This way, to a vector $\mathbf{v}$ we associate the function $E_{\mathbf{v}}:\mathcal{V}^*\to\mathbb{K}$ defined by evaluating all linear functions $\mathcal{V}\to\mathbb{K}$ on the vector $\mathbf{v}$. The function $E_{\mathbf{v}}$ is linear, since $(\lambda f+\mu g)(\mathbf{v})=\lambda f(\mathbf{v})+\mu g(\mathbf{v})$. The linear function $E_{\mathbf{v}}$ is an element of the second dual space $(\mathcal{V}^*)^*$. The formula $f(\lambda\mathbf{v}+\mu\mathbf{w})=\lambda f(\mathbf{v})+\mu f(\mathbf{w})$, expressing linearity of linear functions, shows that $E_{\mathbf{v}}$ depends linearly on $\mathbf{v}$. Thus the **evaluation map** $E:\mathbf{v}\mapsto E_{\mathbf{v}}$ is a linear map $\mathcal{V}\to(\mathcal{V}^*)^*$. One can show that E ***is injective and thus provides an isomorphism between $\mathcal{V}$ and its range*** $E(\mathcal{V})\subset(\mathcal{V}^*)^*$***.***

The previous result and examples suggest that vector spaces need not be described abstractly, and raises the suspicion that the axiomatic definition is misleading as it obscures the actual nature of vectors as functions subject to the pointwise algebraic operations. Here are however some examples where vectors do not come *naturally* as functions.

Perhaps, the most important example of this kind is given by geometric vectors, (as well as by forces and velocities in physics). It provides the opportunity to use geometric intuition in contexts unrelated to geometry. That is, one can "visualize" functions as geometric vectors. Furthermore, taking the field $\mathbb{Q}$ of rational numbers, or the field $\mathbb{Z}_2=\{0,1\}$ on the role of scalars, one can apply geometric intuition to number theory or computer science. Later we will have a chance to see how this works.

Another justification for introducing vector spaces abstractly is that this approach provides great flexibility in constructing new vector spaces from given ones. Such constructions (e.g. direct sums) are used regularly, and it would be very awkward to constantly express the resulting vector spaces as spaces of functions, even when the given spaces are expressed this way. Here is another example.

Quotient spaces

The **quotient space** of a vector space $\mathcal{V}$ by a subspace $\mathcal{W}$ is defined as follows. Two vectors $\mathbf{v}$ and $\mathbf{v}'$ (Figure 23) are called *equivalent modulo* $\mathcal{W}$, if $\mathbf{v} - \mathbf{v}' \in \mathcal{W}$. This way, all vectors from $\mathcal{V}$ become partitioned into equivalence classes. These equivalence classes form the quotient vector space $\mathcal{V}/\mathcal{W}$.

In more detail, denote by $\pi : \mathcal{V} \to \mathcal{V}/\mathcal{W}$ the **canonical projection**, which assigns to a vector $\mathbf{v}$ its equivalence class modulo $\mathcal{W}$. This class can be symbolically written as $\mathbf{v} + \mathcal{W}$, a notation emphasizing that the class consists of all vectors obtained from $\mathbf{v}$ by adding arbitrary vectors from $\mathcal{W}$. Alternatively, one may think of $\mathbf{v} + \mathcal{W}$ as a "plane" obtained from $\mathcal{W}$ as *translation* by the vector $\mathbf{v}$. When $\mathbf{v} \in \mathcal{W}$, we have $\mathbf{v} + \mathcal{W} = \mathcal{W}$. When $\mathbf{v} \notin \mathcal{W}$, $\mathbf{v} + \mathcal{W}$ is not a linear subspace in $\mathcal{V}$. We will call it an **affine subspace** parallel to $\mathcal{W}$.

The set $\mathcal{V}/\mathcal{W}$ of all affine subspaces in $\mathcal{V}$ parallel to $\mathcal{W}$ is equipped with algebraic operations of addition and multiplication by scalars in such a way that the *canonical projection* $\pi : \mathcal{V} \to \mathcal{V}/\mathcal{W}$ *becomes a linear map*. In fact this condition leaves no choices, since it requires that for every $\mathbf{u}, \mathbf{v} \in \mathcal{V}$ and $\lambda, \mu \in \mathbb{K}$,

$$\lambda\pi(\mathbf{u}) + \mu\pi(\mathbf{v}) = \pi(\lambda\mathbf{u} + \mu\mathbf{v}).$$

In other words, the linear combination of given equivalence classes must coincide with the equivalence class containing the linear combination $\lambda\mathbf{u} + \mu\mathbf{v}$ of arbitrary representatives $\mathbf{u}, \mathbf{v}$ of these classes. It is important here that picking different representatives $\mathbf{u}'$ and $\mathbf{v}'$ will result in a new linear combination $\lambda\mathbf{u}' + \mu\mathbf{v}'$ which is however equivalent to the previous one. Indeed, the difference $\lambda(\mathbf{u} - \mathbf{u}') + \mu(\mathbf{v} - \mathbf{v}')$ lies in $\mathcal{W}$ since $\mathbf{u} - \mathbf{u}'$ and $\mathbf{v} - \mathbf{v}'$ do. Thus linear combinations in $\mathcal{V}/\mathcal{W}$ are well-defined.

The construction of the quotient space is admittedly one of the most abstract ones so far. Here is a hint to how one could think of elements of $\mathcal{V}/\mathcal{W}$ and the projection π.

`Example 4.` Projecting $3D$ images to a 2-dimensional screen is described in geometry by the canonical projection π from the $3D$ space $\mathcal{V}$ to the plane $\mathcal{V}/\mathcal{W}$ of the screen along the line $\mathcal{W}$ of the eye sight (Figure D1).

`Example 5.` The direct sum $\mathcal{V} \oplus \mathcal{W}$ contains $\mathcal{V}$ and $\mathcal{W}$ as subspaces consisting of the pairs $(\mathbf{v}, \mathbf{0})$ and $(\mathbf{0}, \mathbf{w})$ respectively. The quotient of $\mathcal{V} \oplus \mathcal{W}$ by $\mathcal{W}$ is canonically identified with $\mathcal{V}$, because each pair $(\mathbf{v}, \mathbf{w})$ is equivalent modulo $\mathcal{W}$ to $(\mathbf{v}, \mathbf{0})$. Likewise, $(\mathcal{V} \oplus \mathcal{W})/\mathcal{V} = \mathcal{W}$.

`Example 6.` Let $\mathcal{V} = \mathbb{R}[x]$ be the space of polynomials with real coefficients, and $\mathcal{W}$ the subspace of polynomials divisible by $x^2 + 1$. Then the quotient space $\mathcal{V}/\mathcal{W}$ can be identified with the plane $\mathbb{C}$ of complex numbers, and the projection $\pi : \mathbb{R}[x] \to \mathbb{C}$ with the map $P \mapsto P(i)$ of evaluating a polynomial P at $x = i$. Indeed, polynomials P and P' are equivalent modulo $\mathcal{W}$ if and only if $P - P'$ is divisible by $x^2 + 1$, in which case $P(i) = P'(i)$. *Vice versa*, if $P(i) = P'(i)$, then $P(-i) = P'(-i)$ (since the polynomials are real), and hence $P - P'$ is divisible by $(x - i)(x + i) = x^2 + 1$.

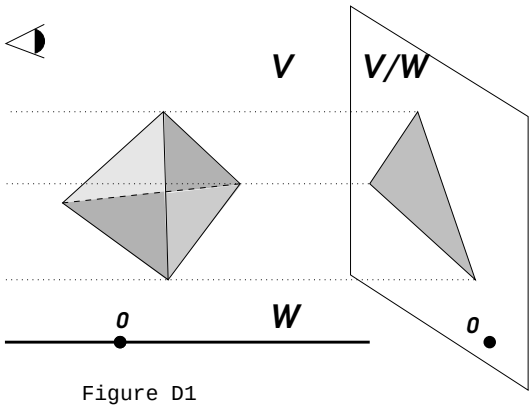

Figure D1

For every linear map $A : \mathcal{V} \to \mathcal{V}'$, there is a canonical isomorphism $\tilde{A} : \mathcal{V}/\operatorname{Ker} A \to A(\mathcal{V})$ between the quotient by the kernel of A, and its range. Namely, $A\mathbf{u} = A\mathbf{v}$ if and only if $\mathbf{u} - \mathbf{v} \in \operatorname{Ker} A$, i.e. whenever $\mathbf{u}$ is equivalent to $\mathbf{v}$ modulo the kernel. Thus, *one can think of every linear map as the projection of the source space onto the range along the null space.* This is a manifestation of a general **homomorphism theorem** in algebra, which in the context of vector spaces can be formally stated this way:

`Theorem.` ***Every linear map*** $A : \mathcal{V} \to \mathcal{V}'$ ***is uniquely represented as the composition*** $A = i\tilde{A}\pi$ ***of the canonical projection*** $\pi : \mathcal{V} \to \mathcal{V}/\operatorname{Ker} A$ ***with the isomorphism*** $\tilde{A} : \mathcal{V}/\operatorname{Ker} A \to A(\mathcal{V})$ ***followed by the inclusion*** $i : A(\mathcal{V}) \subset \mathcal{V}'$***:***

$$\begin{array}{ccc} \mathcal{V} & \xrightarrow{A} & \mathcal{V}' \\ \pi\downarrow & & \cup\, i \\ \mathcal{V}/\operatorname{Ker} A & \xrightarrow[\tilde{A}]{\cong} & A(\mathcal{V}) \end{array} .$$

This result, although called a theorem, is merely a rephrasing of the definitions (of vector spaces, subspaces, quotient spaces, linear maps, isomorphisms, etc.) and is in this sense *tautological*,[18] void of new knowledge.

EXERCISES

406. Verify that $\mathbb{K}^S$ and $\mathcal{V}^S$ are vector spaces.

407. How many vectors are there in $\mathbb{Z}_p$-vector space $\mathbb{Z}_p^n$? $\mathrm{Hom}(\mathbb{Z}_p^n, \mathbb{Z}_p^m)$? ✓

408. How many vectors are there in the $\mathbb{Z}_p$-vector space of strictly upper triangular $n \times n$-matrices? ✓

409. Show that the map $f \mapsto \int_a^b f(x)\,dx$ defined by integration of (say) polynomial functions is a linear form $\mathbb{R}[x] \to \mathbb{R}$.

410. Find the kernel and the range of the differentiation map $D = \frac{d}{dx} : \mathbb{K}[x] \to \mathbb{K}[x]$, when (a) $\mathbb{K} = \mathbb{R}$, (b) $\mathbb{K} = \mathbb{Z}_p$. ✓

411.* Let $\mathcal{V} = \mathbb{R}[x]$, and $\mathcal{W} \subset \mathcal{V}$ be the subspace of all polynomials divisible by $x^2 - 1$. Establish an isomorphism between $\mathcal{V}/\mathcal{W}$ and $\mathbb{R}^{\{1,-1\}}$, the space of all functions from $\{1, -1\}$ to $\mathbb{R}$. ϟ

412. Find the dimensions of spaces of: (a) diagonal $n \times n$-matrices; (b) upper-triangular $n \times n$-matrices. ✓

413. Find the dimension of the subspace in $\mathbb{R}^{\mathbb{R}}$ spanned by functions $\mathbf{cos}(x + \theta_1), \ldots, \mathbf{cos}(x + \theta_n)$, where $\theta_1, \ldots, \theta_n$ are given distinct angles. ✓

414. Let $\mathcal{W} \subset \mathcal{V}$ be any subset of $\mathcal{V}$. Define $\mathcal{W}^\perp \subset \mathcal{V}^*$ as the set of all those linear functions which vanish on $\mathcal{W}$. Prove that $\mathcal{W}^\perp$ is a subspace of $\mathcal{V}^*$. (It is called the **annihilator** of $\mathcal{W}$.)

415. Let $\mathcal{W} \subset \mathcal{V}$ be a subspace. Establish a canonical isomorphism between the dual space $(\mathcal{V}/\mathcal{W})^*$ and the annihilator $\mathcal{W}^\perp \subset \mathcal{V}^*$. ϟ

416. Show that a field $\mathbb{K}$ can be considered as an $\mathbb{F}$-vector space over any subfield $\mathbb{F} \subset \mathbb{K}$.

417. Prove that the number of elements in a finite field is a power of its characteristic. ϟ

[18] Dictionaries define **tautology** as "a representation of anything as the cause, condition, or consequence of itself."