

ALGEBRA

Algebra is the “abstractization” (also called the *generalization*) of arithmetics. We will equip a set with abstract operations reminiscent of those from usual arithmetics. Imposing more and more axioms to those operations (and therefore, going to definitions that are more and more restrictive/less general), we arrive to vector spaces (of which the quintessential incarnation is $\mathbb{R}^n$). Then, we will talk a bit about their main properties, which is a branch called *linear algebra*.

2.1 Groups

Definition 11. A *group* $(G, *)$ is a set G equipped with a map $*$: $G \times G \rightarrow G$ such that:

- (i) it is *associative*: $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$,
- (ii) possesses a *neutral element* or *identity*, i.e.,

$$\exists e \in G : e * a = a = a * e \quad \forall a \in G.$$

- (iii) every element has an *inverse*, i.e.,

$$\forall a \in G \quad \exists b \in G : a * b = e = b * a.$$

If a subset $H \subseteq G$, when equipped with the restriction of $*$ to $H \times H$, still forms a group, we call $(H, *)$ a *subgroup* of G . ♦

Lemma 14. Let $(G, *)$ be a group. Then,

- (i) the identity element and the inverse of any element are unique. Hence, we call them *the* identity and *the* inverse. In general, we denote the identity e or Id and the inverse of $a \in G$ as a^{-1} .
- (ii) $(a^{-1})^{-1} = a$ for all $a \in G$.
- (iii) $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$. ♦

Definition 12. A group $(G, *)$ is said to be *abelian* (or *commutative*) when $*$ is commutative, i.e.,

$$a * b = b * a \quad \forall a, b \in G.$$

For an abelian group one usually denotes the operation $*$ with the symbol $+$ and calls it *addition*. Furthermore, one calls the identity “zero” and denotes it as $0 := e$, the inverse of $a \in G$ is denoted as $-a$ and one uses $a - b := a + (-b)$. ♦

Example 3. 1. The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ equipped with the usual $+$ are abelian groups where $e = 0$.

2. For a fixed $n \in \mathbb{N}$, consider the equivalence relation in $\mathbb{Z}$ such that for $a, b \in \mathbb{Z}$

$$a \approx b \quad :\Longleftrightarrow \quad a - b = qn \quad \text{for some } q \in \mathbb{Z},$$

that is, when the distance from a to b is a whole multiple of n . If you draw a picture, you will notice we are left with n equivalence classes $\mathbb{Z}_n := \{[0], [1], [2], \dots, [n-1]\}$, as a sort of discrete “pac-man” world with n sites. Then for each $[a], [b] \in \mathbb{Z}_n$, define

$$[a] \oplus_n [b] := [a + b].$$

This is called *addition modulo n* and it can be seen as taking the usual sum $a + b$ and then subtracting as many n ’s as necessary to bring the result back to $\{0, 1, \dots, n-1\}$. (Like a “pac-man-world” sum). Equivalently, it is the same as taking the residual of the whole division of $a + b$ by n for $a, b \in \{0, 1, \dots, n-1\}$. In any case, $(\mathbb{Z}_n, \oplus_n)$ is an abelian group.

3. For a fixed $n \in \mathbb{N}$, let $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ be a bijection. One can view it as a rule telling a rearrangement of the tuple $(1, \dots, n)$: for each $j \in \{1, \dots, n\}$, $\sigma(j)$ tells the new position of element j , i.e., σ transforms $(1, 2, \dots, n)$ into $(\sigma^{-1}(1), \dots, \sigma^{-1}(n))$. This is why,

$$S_n := \left\{ \sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \mid \sigma \text{ is a bijection} \right\}$$

is called the set of *permutations of n elements*. Note that for any pair $\sigma, \tau \in S_n$, their composition $\sigma \circ \tau \in S_n$. Then, it turns out that S_n equipped with the composition operation makes a group. It is called the *symmetric group*. For $n \geq 3$ it is not abelian.

4. The set of $n \times n$ matrices with real coefficients, $\mathcal{M}_{n \times n}(\mathbb{R})$, equipped with the matrix product does not make a group because not all matrices have an inverse. But:

- (a) $GL(n, \mathbb{R})$, defined as the set of invertible matrices, is a group —called, the *general linear group*.
- (b) $SL(n, \mathbb{R})$, composed by the invertible matrices with determinant 1 is a subgroup of $GL(n, \mathbb{R})$ —called, the *special linear group*.
- (c) $O(n, \mathbb{R})$, composed by the matrices $A \in \mathcal{M}_{n \times n}(\mathbb{R})$ such that $A^T A = \text{Id}$ is a subgroup of $GL(n, \mathbb{R})$ —called, the *orthogonal group*. ♦

Definition 13. Given groups $(G, *)$ and $(H, \cdot)$, a map $f : G \rightarrow H$ is called a *group homomorphism* when

$$f(a * b) = f(a) \cdot f(b) \quad \forall a, b \in G,$$

—informally, when it does not matter if we multiply the elements before or after applying f .

If f is moreover bijective, we call it a *group isomorphism*. When such a map exists between two groups, we say that they are *group-isomorphic* and denote $(G, *) \cong (H, \cdot)$. ♦

When two groups $(G, *)$, $(H, \cdot)$ are group-isomorphic, every proposition we can prove about $(G, *)$ that only depends on its group structure will also hold for $(H, \cdot)$ —indeed, in the proof of the proposition we could replace $g \in G$ by $f(g) \in H$ and $*$ by $\cdot$, then, the homomorphism and bijectivity properties would make it a proof of the proposition for $(H, \cdot)$. That is, *isomorphic groups are identical for all purposes of group theory*. This concept of identification of objects “for all purposes of a certain construction” appears everywhere in mathematics and we will see several examples more. It is the key concept of the so-called *category theory*, and it is always called “isomorphism” plus a term that tells which is the structure being preserved (in this case “group-”).

2.2 Rings and Fields

Let us add more structure to a group:

Definition 14. A *ring* $(G, +, \cdot)$ is an abelian group $(G, +)$ equipped with an additional operation $\cdot : G \times G \rightarrow G$ such that

- (i) $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$.
- (ii) $+$ and $\cdot$ satisfy the compatibility condition called *distributivity*:

$$\begin{cases} a \cdot (b + c) = a \cdot b + a \cdot c \\ (a + b) \cdot c = a \cdot c + b \cdot c \end{cases} \quad \forall a, b, c \in G.$$

We call $+$ and $\cdot$ respectively, *addition* and *multiplication*.

- When $\cdot$ is also commutative (i.e., $a \cdot b = b \cdot a \quad \forall a, b \in G$), we call G a *commutative ring*.
- When there is also a unit for $\cdot$, i.e., $\exists \mathbf{1} \in G$ such that $a \cdot \mathbf{1} = a = \mathbf{1} \cdot a$, we call it a *unital ring*. ♦

Note that in a ring $(G, +, \cdot)$, $(G, \cdot)$ is not necessarily a group, as we have not imposed the existence of inverses for the $\cdot$ operation.

- Example 4.**
1. $(\mathbb{Z}, +, \cdot)$ is a unital commutative ring. Note that $\cdot$ does not have all inverses, for instance 2 has no inverse (it would be $1/2$, which is not in $\mathbb{Z}$).
 2. For a fixed $n \in \mathbb{N}$, equip $\mathbb{Z}_n$ with the operation $\odot_n$ such that for $[a], [b] \in \mathbb{Z}_n$, $[a] \odot_n [b] := [a \cdot b]$. Then, $(\mathbb{Z}_n, \oplus_n, \odot_n)$ is a unital commutative ring. As you will prove in the exercises, every non-zero element has a multiplicative inverse *if and only if* n is prime. ♦

Let us add even more structure:

Definition 15. A *field* $(G, +, \cdot)$ is a unital, commutative ring where

- (i) the identity of $+$ and $\cdot$ are different: $0 \neq \mathbf{1}$,
- (ii) every non-zero element has an inverse for $\cdot$, i.e.,

$$\forall a \in G \setminus \{0\} \quad \exists b \in G : b \cdot a = \mathbf{1} = a \cdot b.$$

We denote the inverse of $a \in G \setminus \{0\}$ for $+$ as $-a$ and for $\cdot$ as a^{-1} or $\frac{1}{a}$. ♦

So, in a sense, a field is a set with two abelian group structures $+$ and $\cdot$ that are compatible (distributive)—just that 0 has no multiplicative inverse.

- Example 5.**
1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields under the usual operations.

2. As you will prove in the exercises, for $n \in \mathbb{N}$, $\mathbb{Z}_n$ is a field *if and only if* n is prime. ♦

2.3 Vector Spaces

With that, we arrive to the most present algebraic structure in the master program:

Definition 16. A $\mathbb{K}$ -*vector space* $((V, \tilde{+}), (\mathbb{K}, +, \cdot), \circ)$ (also called a *vector space over* $\mathbb{K}$) is:

- (i) an abelian group $(V, \tilde{+})$ whose elements we will call *vectors*,
- (ii) a field $(\mathbb{K}, +, \cdot)$ whose elements we will call *scalars*,
- (iii) an operation $\circ : \mathbb{K} \times V \rightarrow V$ (whcih we call *vector-scalar multiplication*) satisfying all the following compatibility conditions:
 - (a) it is distributive in $\tilde{+}$:

$$\lambda \circ (v \tilde{+} w) = (\lambda \circ v) \tilde{+} (\lambda \circ w) \quad \forall \lambda \in \mathbb{K}, \forall v, w \in V,$$

(b) it is distributive in $+$:

$$(\lambda + \mu) \circ v = (\lambda \circ v) \tilde{+} (\mu \circ v) \quad \forall \lambda, \mu \in \mathbb{K}, \forall v \in V,$$

(c) it is associative with $\cdot$:

$$(\lambda \cdot \mu) \circ v = \lambda \circ (\mu \circ v) \quad \forall \lambda, \mu \in \mathbb{K}, \forall v \in V,$$

(d) $\mathbb{1} \in \mathbb{K}$ is also a neutral element for $\circ$:

$$\mathbb{1} \circ v = v \quad \forall v \in V.$$

Abusing notation one usually uses the same symbol $+$ for both $+$ and $\tilde{+}$, and the same symbol $\cdot$ for both $\cdot$ and $\circ$. Then, to differentiate the neutral element of $+$ and $\tilde{+}$, one often writes $\vec{0}$ for the zero vector.

- If a subset $W \subseteq V$, when equipped with the restricted operations also forms a vector space, we call it a *vector subspace* or *linear subspace*.

- Given $n \in \mathbb{N}$ and some $(\lambda)_{j=1}^n \subseteq \mathbb{K}$, $(v_j)_{j=1}^n \subseteq V$, one denotes the vector

$$\sum_{j \in \{1, \dots, n\}} \lambda_j v_j := \sum_{j=1}^n \lambda_j v_j := \lambda_1 v_1 + \dots + \lambda_n v_n,$$

the *linear combination of the vectors $(v_j)_j$ with coefficients $(\lambda_j)_j$* .

- The branch of mathematics that studies vector spaces is called *linear algebra*. Note that one talks about a vector space as though it was an actual “*physical space*”, using the associated language such as “*in a vector space this or that property holds*”. There will be other constructions that will also be referred to as “*spaces*” (metric spaces, topological spaces etc) and the same will apply. ♦

Example 6. 1. For all $n \in \mathbb{N}$, given a field $(\mathbb{K}, +, \cdot)$, the set $\mathbb{K}^n$ can be equipped with the operation: for $(x_1, \dots, x_n), (y_1, \dots, y_n) \in \mathbb{K}^n$,

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n).$$

Then, $(\mathbb{K}^n, +)$ is an abelian group. Defining the operation

$$\lambda \cdot (x_1, \dots, x_n) := (\lambda x_1, \dots, \lambda x_n) \quad \forall \lambda \in \mathbb{K}, \forall (x_1, \dots, x_n) \in \mathbb{K}^n,$$

one gets that $((\mathbb{K}^n, +), (\mathbb{K}, +, \cdot), \cdot)$ is a vector space. In this context, one writes the tuples of $\mathbb{K}^n$ as columns instead of rows. You are likely used to $\mathbb{R}^n$ and $\mathbb{C}^n$ (and do not worry because for the master’s you will only need to know about $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$).

2. More in general, for any index set I , given a field $(\mathbb{K}, +, \cdot)$, the set tuples $\prod_{j \in I} \mathbb{K}$ can be equipped with the operation: for $(x_j)_{j \in I}, (y_j)_{j \in I} \in \prod_{j \in I} \mathbb{K}$,

$$(x_j)_{j \in I} + (y_j)_{j \in I} := (x_j + y_j)_{j \in I}.$$

Then, $(\prod_{j \in I} \mathbb{K}, +)$ is an abelian group. Defining the operation

$$\lambda \cdot (x_j)_{j \in I} := (\lambda x_j)_{j \in I} \quad \forall \lambda \in \mathbb{K}, \forall (x_j)_{j \in I} \in \prod_{j \in I} \mathbb{K},$$

one gets that $((\prod_{j \in I} \mathbb{K}, +), (\mathbb{K}, +, \cdot), \cdot)$ is a vector space. In particular, the set of tuples that only have a non-zero entry at most for finitely many slots, i.e.,

$$\prod_{j \in I}^0 \mathbb{K} := \left\{ (x_j)_{j \in I} \in \prod_{j \in I} \mathbb{K} \mid \exists J \subseteq I \text{ finite} : x_j = 0 \forall j \in I \setminus J \right\}$$

is a vector subspace of $\prod_{j \in I} \mathbb{K}$.

3. Note that item 2 can be restated as follows: given a set X and a field $\mathbb{K}$, the space of $\mathbb{K}$ valued functions over X ,

$$\prod_{x \in X} \mathbb{K} = \left\{ f : X \rightarrow \mathbb{K} \right\}$$

is a vector space with the vector sum and scalar multiplication defined *point-wise*, i.e. for $\lambda, \mu \in \mathbb{K}$, $f, g \in \prod_{x \in X} \mathbb{K}$,

$$(\lambda f + \mu g)(x) := \lambda f(x) + \mu g(x) \quad \forall x \in X.$$

Then, $\prod_{x \in X} {}^0\mathbb{K}$ is just the subspace of functions that only take non-zero value at most in finitely many $x \in X$. $\blacklozenge$

Lemma 15. In a vector space V , the scalar 0 is the only scalar that maps non-zero vectors to $\vec{0}$ i.e., for $\lambda \in \mathbb{K}$ and $v \in V \setminus \{\vec{0}\}$,

$$\lambda \cdot v = \vec{0} \iff \lambda = 0. \quad \blacklozenge$$

2.3.1 Linear Algebra

Definition 17. Given vector spaces V, W over the same field $\mathbb{K}$, a map $f : V \rightarrow W$ is said to be *linear* when

$$f(v + w) = f(v) + f(w) \quad \text{and} \quad f(\lambda v) = \lambda f(v), \quad \forall \lambda \in \mathbb{K}, \forall v, w \in V.$$

That is, it preserves the vector sum and scalar-vector product. Linear maps are usually denoted with capital letters, say A instead of f , and one omits the parenthesis when placing an argument, such that $f(v)$ is denoted Av .

- If a linear map $A : V \rightarrow W$ is bijective, we call it a *linear (or vector space) isomorphism*. When such a map exists between two vector spaces, we say that they are *linearly isomorphic* spaces. Following the remark after Def. 13, *linearly isomorphic vector spaces are identical for all purposes of linear algebra*.

- Given a linear map $A : V \rightarrow W$, its *kernel* is the set of vectors that are mapped to $\vec{0} \in W$, i.e.,

$$\ker(A) := \left\{ v \in V \mid Av = \vec{0} \right\} = A^{-1}(\{\vec{0}\}). \quad \blacklozenge$$

In the context of linear maps, one uses more $\text{Im} A := \text{range}(A)$ (the image set). The kernel and image are the quintessential sets to analyze a linear map.

Lemma 16. Let V, W be $\mathbb{K}$ -vector spaces and $A : V \rightarrow W$ a linear map. Then,

- (i) Necessarily, $A\vec{0} = \vec{0}$.
- (ii) $\ker A$ and $\text{Im} A$ are linear subspaces of V and W respectively.
- (iii) A is injective *if and only if* $\ker A = \{0\}$.
- (iv) Given another linear map $B : V \rightarrow W$, for each $\lambda, \mu \in \mathbb{K}$, the linear combination of maps $\lambda A + \mu B$, defined as the mapping

$$(\lambda A + \mu B)(v) := \lambda Av + \mu Bv \quad \forall v \in V$$

is still a linear map. $\blacklozenge$

The last item tells that the set of linear maps is a vector space itself:

Example 7. Given two vector spaces V, W over the same field $\mathbb{K}$, the set of all linear maps

$$\text{Lin}(V, W) := \left\{ A : V \rightarrow W \mid A \text{ is linear} \right\},$$

is a vector space when equipped with the vector sum and scalar multiplication:

$$(\lambda A + \mu B)(v) := \lambda Av + \mu Bv \quad \forall \lambda, \mu \in \mathbb{K}, A, B \in \text{Lin}(V, W). \quad \blacklozenge$$

Definition 18. Let V be a vector space, let I be an index set and let $B \subseteq V$ non-empty.

- We say that the vectors in B are (or abusing notation, B itself is) *linearly independent* when^[a]

$$\left(\text{given a finite } J \subseteq B \text{ and } \{\lambda_v\}_{v \in J} \subseteq \mathbb{K} \text{ for which } \sum_{v \in J} \lambda_v v = \vec{0} \right) \implies \left(\lambda_v = 0 \ \forall v \in J \right).$$

In words, when the only linear combination of B vectors that is zero is putting all coefficients to 0.

- We say the vectors in B are *linearly dependent* when they are not independent, i.e., when

$$\exists J \subseteq B \text{ finite and } (\lambda_v)_{v \in J} \subseteq \mathbb{K} \text{ with } \lambda_{v_0} \neq 0 \text{ for at least one } v_0 \in J \text{ such that } \sum_{v \in J} \lambda_v v = 0.$$

- We say that the vectors in B *span* V when

$$\forall v \in V \quad \exists n \in \mathbb{N}, (v_j)_{j=1}^n \subseteq B, (\lambda_j)_{j=1}^n \subseteq \mathbb{K} \quad \text{such that} \quad v = \sum_{j=1}^n \lambda_j v_j,$$

i.e., every vector in V can be written as a linear combination of vectors in B .

- In particular, we denote the set of possible (finite)^[b] linear combinations of B as its *span*:

$$\text{span}(B) := \left\{ \sum_{j=1}^n \lambda_j v_j \mid n \in \mathbb{N}, (v_j)_{j=1}^n \subseteq B, (\lambda_j)_{j=1}^n \subseteq \mathbb{K} \right\}.$$

It is trivially a vector subspace of V .

- B is said to be a (*Hamel*) *basis* of V when both:

$$(i) \ B \text{ is linearly independent.} \qquad (ii) \ \text{span}(B) = V. \qquad \blacklozenge$$

Lemma 17. Given a vector space V , a set of non-zero vectors $\{v_j\}_{j=1}^n \subseteq V$ is linearly dependent *if and only if* it is possible to write one of the vectors as a linear combination of the rest. $\blacklozenge$

Lemma 18. Given an index set I and a field $\mathbb{K}$, define

$$e_j^k := \begin{cases} 1 & \text{if } j = k \\ 0 & \text{if } j \neq k, \end{cases}$$

such that $e_j := (e_j^k)_{k \in I} \in \prod_{k \in I} \mathbb{K}$ is a tuple of all zeros and a single 1. Then, $\{e_j\}_{j \in I}$ is a basis of $\prod_{j \in I} {}^0\mathbb{K}$. (We call it the *canonical basis* of $\prod_{j \in I} {}^0\mathbb{K}$.) $\blacklozenge$

Lemma 19. For an arbitrary vector space V , if $B \subseteq V$ is a basis, for each non-zero $v \in V$ there exist a *unique* finite $J \subseteq B$ and unique non-zero coefficients $(\lambda_w)_{w \in J} \subseteq \mathbb{K}$ such that $v = \sum_{w \in J} \lambda_w w$. $\blacklozenge$

Theorem 5. Every vector space V has a (Hamel) basis^[c] and all bases of V have the same cardinality. We call the cardinality $|B|$ of any of its bases B , the *dimension* of V and denote it $\dim(V)$. $\blacklozenge$

Corollary 3. Given a $\mathbb{K}$ -vector space V and a basis B , there is a linear isomorphism from V to $\prod_{j \in B} {}^0\mathbb{K}$. One calls this B 's *coordinate representation*. Hence, every vector space is isomorphic to some $\prod_{j \in I} {}^0\mathbb{K}$. $\blacklozenge$

^[a]Let $J \subseteq V$ be finite and let $J = \{v_1, \dots, v_{|J|}\}$ be an enumeration with $v_j \neq v_k$ if $j \neq k$. Given $(\lambda_v)_{v \in J} \subseteq \mathbb{K}$, for $j \in \{1, \dots, n\}$ define λ_j as the λ_v for which $v = v_j$. Then, we denote $\sum_{v \in J} \lambda_v v := \sum_{j=1}^n \lambda_j v_j$.

^[b]Note that so-far we did not define what an “infinite sum of vectors” means. In fact, there will be one such notion per notion of “topology” we put on the vector space—to be explained in the following lectures.

^[c]One needs to assume the so-called *axiom of choice* in the set theory that is being used for this. We will see more later.

Corollary 4. Given vector spaces V, W over the same field $\mathbb{K}$, they are isomorphic *if and only if* they have the same dimension. ♦

Example 8. 1. For each $n \in \mathbb{N}$, $\mathbb{R}^n$ (with its standard operations) is an n dimensional real vector space and $(e_j)_{j=1}^n$ with $e_j := (\underbrace{0, \dots, 0}_j, 1, 0, \dots, 0)$ is a basis.

2. $\prod_{j \in \mathbb{N}} \mathbb{R} = \{(x_1, x_2, \dots) \mid x_j \in \mathbb{R}\}$ with “slot-wise” operations as in Example 6, is an infinite dimensional real vector space. We call it the *space of real sequences*.

3. $\mathbb{C}$, if we use complex numbers as scalars, is a 1 dimensional complex vector space. But, if we use real numbers as scalars, $\mathbb{C}$ is a 2 dimensional real vector space. Similarly, for each $n \in \mathbb{N}$, $\mathbb{C}^n$ is an n dimensional complex vector space, or a $2n$ dimensional real vector space.

4. Given $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$, the space of 1 variable $\mathbb{K}$ -valued polynomials on $\mathbb{K}$, namely, the space of functions

$$\left\{ P : \mathbb{K} \rightarrow \mathbb{K} \mid \exists n \in \mathbb{N}, (c_j)_{j=0}^n \in \mathbb{K}^{n+1} : P(x) = c_0 + c_1x + c_2x^2 + \dots + c_nx^n \quad \forall x \in \mathbb{K} \right\}$$

is a vector space of infinite dimension and the set of monomials B is a basis, where^[d]

$$B := \{1, x, x^2, x^3, \dots\}. \quad \blacklozenge$$

The following theorem, called the *rank nullity theorem* is key to analyze linear maps in finite dimensions.

Theorem 6. Given vector spaces V, W , where V is finite dimensional, for any linear map $f : V \rightarrow W$,

$$\dim(V) = \dim(\ker(f)) + \dim(\operatorname{Im}(f)). \quad \blacklozenge$$

Corollary 5. Let V, W be finite dimensional vector spaces of equal dimension and $A : V \rightarrow W$ an arbitrary linear map. Then, A is injective *if and only if* A is surjective. ♦

Hence, in finite dimensions, between spaces of same dimension injective and surjective (linear) maps are equivalent! If you draw a picture, you will understand why it should obviously be so. In infinite dimensions however, it may happen that although we have a linear map $A : V \rightarrow V$ that is injective (every vector is mapped to a different vector), the result does not cover the whole space. This is an instance of the so-called *Hilbert’s hotel* phenomenon:

Example 9. How can a linear map be injective, map to the same dimensions, say, to itself and still fail to be bijective? Welcome to Hilbert’s hotel! Consider the vector space of sequences $\prod_{j \in \mathbb{N}} \mathbb{R}$ and define the right shift operator $R : \prod_{j \in \mathbb{N}} \mathbb{R} \rightarrow \prod_{j \in \mathbb{N}} \mathbb{R}$:

$$R(x_1, x_2, \dots) := (0, x_1, x_2, \dots) \quad \forall (x_1, x_2, \dots) \in \prod_{j \in \mathbb{N}} \mathbb{R}.$$

It is certainly linear and trivially $\ker(R) = \{\vec{0}\}$ (only the 0 vector goes to the 0 vector), so, R is injective by Lemma 16. However,

$$\operatorname{Im}(R) = \left\{ (y_1, y_2, \dots) \in \prod_{j \in \mathbb{N}} \mathbb{R} \mid y_1 = 0 \right\},$$

which is clearly not the whole $\prod_{j \in \mathbb{N}} \mathbb{R}$. Hence, it is not surjective! Yet, $\operatorname{Im}(R)$ is clearly infinite dimensional (and even of the same cardinality as $\prod_{j \in \mathbb{N}} \mathbb{R}$), but it does not fill the whole space. ♦

Next, we need to mention the following notion, although you will greatly enlarge it in mathematical quantum theory.

^[d]By x^k here we mean the function $x \mapsto x^k$, not a particular value in $\mathbb{K}$.

Definition 19. Given a vector space V and a linear map $A : V \rightarrow V$, we say that $\lambda \in \mathbb{K}$ is an *eigenvalue* of A with *eigenvector* $v \in V \setminus \{\vec{0}\}$ when $Av = \lambda v$. The subspace $\ker(A - \lambda \text{Id})$ (namely, the space of all eigenvectors of λ , plus $\vec{0}$) is called the *eigenspace* of λ and its dimension is called the *(geometric) multiplicity or degeneracy* of λ . ♦

2.4 There is More in the Ladder of Algebra

To conclude, note that one can keep adding structure to a vector space (as we will do in future lectures), but there is one such additional structure that gives the space the name entitling this lecture, so it is worth mentioning it:

Definition 20. An *algebra* over $\mathbb{K}$ is a $\mathbb{K}$ -vector space V equipped with an additional operation $\star : V \times V \rightarrow V$ (called *vector product*) that is *bilinear* (linear in each slot), i.e. $\forall v, w, u \in V, \lambda, \mu \in \mathbb{K}$,

$$(\lambda \cdot v + \mu \cdot w) \star u = \lambda \cdot (v \star u) + \mu(w \star u),$$

$$u \star (\lambda \cdot v + \mu \cdot w) = \lambda \cdot (u \star v) + \mu(u \star w).$$

- We call it an *associative algebra* when $\star$ is also *associative*:

$$(v \star w) \star u = v \star (w \star u) \quad u, v, w \in V.$$

- We call it *unital* if $\exists \Omega \in V$ such that

$$\Omega \star v = v = v \star \Omega \quad \forall v \in V.$$

(So, an associative $\star$ makes the vector space a ring for vectors, which is a unital ring when the algebra is unital.) ♦

Example 10. Given a vector space V , the space of linear maps $\text{Lin}(V, V)$ equipped with the composition operation is an associative unital algebra. ♦

Exercise Sheet 2

1. Prove Lemma 14.

2. Let $((G, +), \cdot)$ be a ring. Prove the following statements:

- (i) For all $a, b \in G$

$$(-a) \cdot b = -(a \cdot b), \quad a \cdot (-b) = -(a \cdot b), \quad (-a) \cdot (-b) = a \cdot b.$$

- (ii) Denoting the neutral element for $+$ by 0 ,

$$a \cdot 0 = 0 \quad \forall a \in G$$

3. Let $((G, +), \cdot)$ be a field. Prove the following statements:

- (i) For all $a, b, c \in G$

$$\left(a \neq 0 \quad \text{and} \quad a \cdot b = a \cdot c \right) \implies \left(b = c \right).$$

- (ii) Let $n \in \mathbb{N}$. If $\mathbb{Z}_n$ is a field, then n must be prime.

(Hint: think of the definition of prime.)

(iii) Let $n \in \mathbb{N}$. Assume we know that $\mathbb{Z}_n$ is a unital commutative ring. If n is prime, then $\mathbb{Z}_n$ is a field.

(Hint: Consider all multiples of $a \in \mathbb{Z}_n$. What would happen if there were $n-1$ multiples? Use that every natural has a unique prime number factorization —the fundamental theorem of arithmetics.)

4. Prove Lemmas 15, 16, 17, 18 and 19. (In 18 if you want a simpler version, you can assume $I = \{1, \dots, n\}$, so that $\prod_{j \in I}^0 \mathbb{K} = \mathbb{K}^n$.)

5. Prove Corollaries 3 and 4. (If you want a simpler version, you can assume finite dimensional vector spaces. Then, substitute $\prod_{j \in I}^0 \mathbb{K}$ by $\mathbb{K}^n$.)