LINEAR ALGEBRA II
SPRING 2024 - HKU

ARON HELEODORO

These notes will be updated as the semester progresses. Their goal is to present the material from the textbook and the class in a more concise form. I will often try to give slightly different phrasing (and/or proofs) than the one provided in the textbook. The intent is to make you think the concepts through and to work the concepts by yourself.

You are strongly encouraged to do the exercises as you read. They will help you parse the definitions, examples, and concepts used in the proofs of the theory. Some of these exercises will be assigned as Homework or will be discussed in class.

Points in red and blue are still being edited.

I would appreciate any comments. If you find mistakes, which are probably present, please let me know too. I normally revise part of the notes after the class in which we discussed the material, so please refer frequently to the website for the most up-to-date version.

1. Jan. 15: Vector spaces

Plan:

- Introduce the word field, $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$.
- Define vector spaces over $\mathbb{F}$.
- Examples: $\mathbb{F}^S$ for S a set.
- Proposition with basic properties: uniqueness of additive identity and inverse, multiplication by 0 gives the zero vector, the zero vector is stable and -1 multiplication gives the additive inverse.

1.1. **Fields.** In your previous linear algebra class (Math 2101) you defined a vector space over the real numbers. The very same definition works in a slightly more general context, we start by introducing some terminology for that.

Date: Last updated January 17, 2024.

Definition 1. A *field* is a triple $(\mathbb{F}, +, \cdot)$, where $\mathbb{F}$ is a set, and we have operations (i.e. functions):

- addition $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$,
- multiplication $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$;

satisfying the following list of axioms:

(a) addition and multiplication are associative;

(b) addition and multiplication are commutative;

(c) there exists $0 \in \mathbb{F}$, such that $a + 0 = 0 + a = a$, for all $a \in \mathbb{F}$;

(d) there exists $1 \in \mathbb{F}$, such that $a \cdot 1 = 1 \cdot a = a$, for all $a \in \mathbb{F}$;

(e) $0 \neq 1$;

(f) every $a \in \mathbb{F}$ has an *additive inverse*, i.e. an element $b \in \mathbb{F}$ such that $a + b = b + a = 0$;

(g) every $a \in \mathbb{F}\backslash\{0\}$ has a multiplicative inverse;

(h) distributivity, i.e. for every $a, b, c \in \mathbb{F}$ one has: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Notation 1. We will omit the $\cdot$ when writing the multiplication operation, i.e. for any $a, b \in \mathbb{F}$ we will write ab for $a \cdot b$.

Example 1. (i) The real numbers $\mathbb{R}$ form a field with usual addition and multiplication.

(ii) The complex numbers $\mathbb{C}$ form a field with usual addition and multiplication.

(iii) The *rational numbers* $\mathbb{Q} := \{\frac{p}{q} \mid p \in \mathbb{Z},\ q \in \mathbb{Z}\backslash\{0\}\}$ are a field.

Exercise 1. Write out explicitly what conditions (a-b) and (g) above are and check them in one of the examples in Example 1.

Exercise 2. Let p be a prime number and consider $\mathbb{F}_p = \{0, 1 \ldots, p-1\}$, then for $a, b, c \in \mathbb{F}_p$ we define:

$a + b := c$ if $(a + b - c)$ is a multiple of p, $\qquad a \cdot b := c$ if $(a \cdot b - c)$ is a multiple of p.

(i) Check that $+ : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ and $\cdot : \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ are well-defined.

(ii) Prove that $\mathbb{F}_p$ is a field.

Exercise 3. Can you come up with another example of a field?

1.2. **Vector spaces.** In a previous Linear Algebra class you probably approached vector spaces by concrete examples. The main point of this class is to develop the theory from an abstract point of view focused on proofs, mostly basis-free, and applicable to general fields of characteristic zero, until later results that might require $\mathbb{F}$ to be the real or complex numbers.

Let $\mathbb{F}$ be a field.

Definition 2. A *vector space* over $\mathbb{F}$ is the data of

(i) a set V;

(ii) an operation $+ : V \times V \to V$;

(iii) a *scalar multiplication* operation $\cdot : \mathbb{F} \times V \to V$.

These are subject to the following axioms:

(a) the operation $+$ is associative, commutative, it admits an identity $0_V \in V$ and inverse;

(b) the operation $\cdot$ is associative;

(c) for every $v \in V$ one has $1 \cdot v = v$;

(d) scalar multiplication distributes over vector addition (i.e. the operation $+$ on V).

Example 2. (i) The set $\{0\}$ is a vector space over any field $\mathbb{F}$.

(ii) Given a set S consider $\mathbb{F}^S$ the set of functions $f : S \to \mathbb{F}$. The operations are defined by pointwise addition and multiplication, i.e. given $f, g \in \mathbb{F}^S$ and $a \in \mathbb{F}$ we let:

$$(f + g)(s) := f(s) + g(s), \qquad (a \cdot f)(s) := a \cdot f(s),$$

and $0_{\mathbb{F}^S}$ is the zero function.

(iii) For any $n \geq 1$, the set $\mathbb{F}^n$ is a vector space, where the operations are defined as follows. Let $v = (v_1, \ldots, v_n) \in \mathbb{F}^n$, $w = (w_1, \ldots, w_n) \in \mathbb{F}$, and $a \in \mathbb{F}$, then:

$$v + w := (v_1 + w_1, \ldots, v_n + w_n), \qquad a \cdot v := (av_1, \ldots, av_n),$$

and $0_{\mathbb{F}^n} := (0, \ldots, 0)$.

(iv) For any $n, m \geq 1$ the set $M_{m\times n}(\mathbb{F})$ of $m \times n$ matrices with coefficients in $\mathbb{F}$ equipped with matrix addition and scalar multiplication is a vector space over $\mathbb{F}$.

(v) The set of sequences with value in $\mathbb{F}$ is a vector space.

Remark 1. A set G equipped with an operation $+ : G \times G \to G$ satisfying condition (a) above is an *Abelian group*. These objects are very important in algebra and are studied in more detail in an abstract algebra course, e.g. Math3301 (Algebra I).

Lemma 1. *Let V be a vector space over $\mathbb{F}$.*

(1) Given $v \in \mathbb{F}$ such that $v + w = w$ for all $w \in \mathbb{F}$, then $v = 0_V$.

(2) The additive inverse is unique.

(3) For every $v \in V$, we have $0 \cdot v = 0_V$.

(4) For every $a \in \mathbb{F}$, we have $a \cdot 0_V = 0_V$.

(5) For every $v \in V$ we have $v + (-1) \cdot v = 0$, i.e. the additive inverse of v is given by $-v := (-1) \cdot v$.

Proof. (1) We have $v = v+0_V = 0_V$. First equality follows from Definition 2 (a) the second from the assumption of the Lemma.

(2) Assume there exists $u_1, u_2 \in V$ such that $u_1 + v = 0_V = u_2 + v$. Then we have: $u_1 = u_1 + 0_V = u_1 + u_2 + v = u_2 + u_1 + v = u_2 + 0_V = u_2$.

(3) Notice $v+0\cdot v = (1+0)\cdot v = 1\cdot v = v$. Thus by (1), we have $0\cdot v = 0_V$.

(4) For any $a \in \mathbb{F}$, we have: $a \cdot 0_V = a \cdot (0_V + 0_V) = a \cdot 0_V + a \cdot 0_V$. By (1), we have $a \cdot 0_V = 0_V$.

(5) Notice $v + (-1) \cdot v = (1 + (-1)) \cdot v = 0 \cdot v = 0_V$, where in the last step we used (3).

□

Notation 2. (1) Notice that for $a, b \in \mathbb{F}$ and $v \in V$ we have:

$$(ab) \cdot v = a \cdot (b \cdot v)$$

by Defintition 2 (b). Thus, we can omit the $\cdot$ for the operation of scalar multiplication as we omitted it for multiplication in a field (see) without causing ambiguity.

(2) We will denote the additive inverse of v by $-v$.

(3) We will denote 0_V simply by 0. This should not be confused with $0 \in \mathbb{F}$ the identity of the operation $+$ in $\mathbb{F}$, as these live in different sets, except when $V = \mathbb{F}$, in which case the notation is consistent.

Remark 2. (i) The empty set $\emptyset$ is not a vector space. Namely, it fails condition (a) from Definition 2.

(ii) Condition (a) from Definition 2 can be substituted by

(a)' the operation $+$ is associative, commutative, it admits an identity $0_V \in V$ and (3) from Lemma 1 holds.

Indeed, assume (a)', then we have $0_V = 0 \cdot w = (1+(-1)) \cdot w = w+(-1)w$ for every $w \in V$. Thus (a) holds.

Example 3. Let V be a vector space over $\mathbb{R}$. We can define a vector space over the complex numbers $V_{\mathbb{C}}$, called the *complexification* of V as follows:

- as a set we let $V_{\mathbb{C}} := V \times V$;
- $+ : V_{\mathbb{C}} \times V_{\mathbb{C}} \to V_{\mathbb{C}}$ is given by $(u_1, v_1) + (u_2, v_2) := (u_1 + u_2, v_1 + v_2)$;
- scalar multiplication is defined as $(a + bi) \cdot (u_1, v_1) = (au_1 - bv_1, bu_1 + av_1)$.

The reader should check that $V_{\mathbb{C}}$ is a vector space over $\mathbb{C}$.

Exercise 4. Universal property of complexification. Let V be a vector space over $\mathbb{R}$ and W a vector space over $\mathbb{C}$. Notice that W can be seen as a vector space over $\mathbb{R}$, where $a \cdot w := (a + i0) \cdot w$, i.e. using the natural inclusion of $\mathbb{R}$ into $\mathbb{C}$. Let $\mathrm{Hom}_{\mathbb{R}}(V, W)$ denote the set of linear operators between V and W, where W is seen as a vector space over $\mathbb{R}$ and let $\mathrm{Hom}_{\mathbb{C}}(V_{\mathbb{C}}, W)$ denote the set of linear operator between $V_{\mathbb{C}}$ and W as vector spaces over $\mathbb{C}$. Prove that there exists a bijection:

$$\mathrm{Hom}_{\mathbb{R}}(V, W) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{C}}(V_{\mathbb{C}}, W).$$

2. Jan. 18, 2024

Plan:

- define subspaces and give plenty of examples;
- define sum and direct sum of vector subspaces and prove their properties;

- define span, degree of a polynomial, and definition of finite-dimensional vector space;
- linear independence with properties;
- subspaces of finite-dimensional vector spaces are finite-dimensional.
- define basis, how to construct basis and every finite-dimensional vector space has a basis.

2.1. **Subspaces.**

Definition 3. Let V be a vector space, a subset $U \subseteq V$ is said to be a *subspace* if:

(a) $0 \in U$;

(b) the restrictions $+_U : U \times U \to V$ and $\cdot_U : \mathbb{F} \times U \to V$ factors as:

$$\begin{array}{ccc} U \times U & \xrightarrow{+'_U} & U \\ & \searrow^{+_U} & \downarrow \\ & & V \end{array} \qquad \begin{array}{ccc} \mathbb{F} \times U & \xrightarrow{\cdot'_U} & U \\ & \searrow^{\cdot_U} & \downarrow \\ & & V \end{array} .$$

Given a subspace $U \subseteq V$ we will simply write $+ : U \times U \to U$ and $\cdot : \mathbb{F} \times U \to U$ for $+'_U$ and $\cdot'_U$, respectively.

Exercise 5. (i) Check that Definition 3 agrees with Definition (1.33) from the textbook.

(ii) Show that only requiring condition (b) in Definition 3 would not agree with the notion as defined in the textbook.

Example 4. (i) let $U \subset \mathbb{F}^n$ defined as $U := \{(v_1, \ldots, v_n) \in \mathbb{F}^n \mid v_1 + 2v_2 + \cdots + nv_n = 0\}$;

(ii) let $p \in \mathbb{F}[x, y, z]$ be a polynomial of the form $p(x, y, z) = ax+by+cz$, for some constants $a, b, c \in \mathbb{F}$, then $U := \{(v_1, v_2, v_3) \in \mathbb{F}^3 \mid p(v_1, v_2, v_3) = 0\}$ is a subspace;

(iii) the subset of functions $f : [0, 1] \to \mathbb{R}$ which are continuous is a subspace of all the functions from $[0, 1]$ to $\mathbb{R}$;

(iv) let $U \subset \mathbb{F}[x]$ denote the subset of polynomials p such that $p(0) = p'(0) = \cdots = p^{(k)}(0) = 0$;

(v) the set of all sequences of complex numbers whose limit is 0 is a subspace of $\mathbb{C}^\infty$.

Exercise 6. (i) Let $p \in \mathbb{R}[x, y, z]$ be a polynomial of degree 1 and define the subset:

$$U_p := \{(v_1, v_2, v_3) \in \mathbb{R}^3 \mid p(v_1, v_2, v_3) = 0\}.$$

Show that U_p is a subspace if and only if p is of the form taken in (ii) of Example 4.

(ii) With the notation as in (i), assume that $p_1, p_2 \in \mathbb{R}[x, y, z]$ are polynomials of degree 1 with no constant term, prove that

$$U_{p_1} \cap U_{p_2} = U_{p_1 p_2}$$

is a subspace of $\mathbb{R}^3$.

(iii) Can you guess which types of polynomials $p \in \mathbb{R}[x, y, z]$ have the property that U_p is a subspace of $\mathbb{R}^3$.

Exercise 7. Let $\mathbb{F}^{\mathbb{N}}$ be the vector space of sequences over $\mathbb{F}$. For an integer $p \geq 1$, we define the subset $S_p \subset \mathbb{F}^{\mathbb{N}}$ of sequences $(a_n)_{n \geq 1}$ satisfying:

$$\sum_{n=1}^{\infty} |a_n|^p < \infty.$$

Proof or disproof S_p is a subspace for every integer $p \geq 1$.

Definition 4. Given $U_1, U_2 \subseteq V$ two subspaces of V we define the *sum* $U_1 + U_2 \subseteq V$ as the subset of elements $v \in V$ such that there exist $u_1 \in U_1$ and U_2 such that $u_1 + u_2 = v$. For $U_1, \ldots, U_k$ a collection of k subspaces of V, we inductively define:[1]

$$U_1 + \cdots + U_k := U_1 + (U_2(\cdots + U_k)).$$

Example 5. (i) let $U_i = \{(v_1, v_2, v_3, v_4) \in \mathbb{F}^4 \mid v_i \neq 0\}$ for $i = 1, 2, 3, 4$. Then

$$U_2 + U_3 + U_4 = \{(v_1, v_2, v_3, v_4) \in \mathbb{F}^4 \mid v_1 = 0\}, \qquad U_1 + U_2 + U_3 + U_4 = \mathbb{F}^4.$$

(ii) let $U_1 = \{(v_1, v_2, v_3, v_4) \in \mathbb{F}^4 \mid v_3 + v_4 = 0 \text{ and } v_1 + v_2 = 0\}$, let $U_2 = \{(v_1, v_2, v_3, v_4) \in \mathbb{F}^4 \mid v_1 = 0\}$, then $U_1 + U_2 = \mathbb{F}^4$.

[1] In fact, this definition is independent of the choice of parenthesization, hence justifying the notation.

Exercise 8. In the condition in Definition 4 are the vectors u_1 and u_2 uniquely determined? Compare (i) and (ii) in Example 4.

Definition 5. Given $U_1, U_2 \subseteq V$ two subspaces of V we say that $U_1 + U_2$ is a *direct sum* if u_1 and u_2 are uniquely determined. In this case, we use the notation $U_1 \oplus U_2$[2]. Similarly, given subspaces $U_1, \dots, U_k$ we define:

$$U_1 \oplus \cdots \oplus U_k := U_1 \oplus (U_2(\cdots \oplus U_k)).$$

Lemma 2. *Given subspaces $U_1, \dots, U_k$, then $U_1 + \cdots + U_k$ is a direct sum if and only if $U_i \cap U_j = \{0\}$ for all $i, j \in \{1, \dots, k\}$ with $i \neq j$.*

Proof. We start with $k = 2$.

First, we prove that the condition is necessary. Let $U_1 + U_2 = U_1 \oplus U_2$ and consider $v \in U_1 + U_2$, written as $v = u_1 + u_2$ for some $u_1 \in u_1$ and $u_2 \in u_2$. Assume by contradiction that $U_1 \cap U_2 \neq \{0\}$. Then there exists a non-zero vector $w \in U_1 \cap U_2$ such that

$$v = (u_1 + w) + (-w + u_2), \text{ where } u_1 + w \in U_1 \text{ and } -w + u_2 \in U_2.$$

This shows that u_1, u_2 are not unique, so we get a contradiction.

Now assume that $U_1 \cap U_2 = \{0\}$. Again by contradiction suppose that there exists $v \in U_1 + U_2$ which can be written as:

$$v = u_1 + u_2 \text{ and } v = u_1' + u_2',$$

for $u_1, u_1' \in U_1$ and $u_2, u_2' \in U_2$, such that $u_1 \neq u_1'$ and $u_2 \neq u_2'$. Then consider $w = u_1 - u_1'$. Notice that $w \in U_1$ and, since $w = u_2' - u_2$, we have that $w \in U_2$. As $w \neq 0$ we obtain a contradiction with $U_1 \cap U_2 = \{0\}$.

The general case follows by induction, we leave the details to the reader. □

Exercise 9. Let $V = \mathbb{F}^4$. Provide three distinct subspaces $U_1, U_2, U_3 \subseteq V$ such that:

$$V_1 + V_2 = V_1 \oplus V_2, V_2 + V_3 = V_2 \oplus V_3, \text{ but } V_1 + V_2 + V_3 \neq V_1 \oplus V_2 \oplus V_3.$$

2.2. **Span and linear dependence.**

Definition 6. Given a subset $S \subseteq V$ we define $\operatorname{Span} S$ the *span of S* to be the subset of V consisting of vectors $v \in V$ such that

$$v = a_1 u_1 + \ldots + a_k u_k$$

for some $k \in \mathbb{N}$, $a_1, \dots, a_k \in \mathbb{F}$, and $v_1, \dots, v_k \in S$. It is convenient to define $\operatorname{Span} \emptyset = \{0\}$. If $\operatorname{Span} S = V$ we say that S *spans* V.

[2]At the moment this notation might seem unmotivated, but it will be clearer when we consider this operation on vector spaces.

Remark 3. It is clear that Span S is a vector space and that it contains S. We claim that Span S is the smallest subspace of V containing S. Consider a subspace $U \subseteq V$ such that $S \subseteq U$, we claim that Span $S \subseteq U$. Indeed, given $v \in \operatorname{Span} S$ we have $v = v = a_1u_1 + \ldots + a_ku_k$ for some $a_1, \ldots, a_k \in \mathbb{F}$, and $v_1, \ldots, v_k \in S$. Since $u_1, \ldots, u_k \in U$ we have $v \in U$. Thus, it follows that Span S belongs to the intersection of all subspaces of V containing Span S.

Example 6. (i) Consider $\{e_1, \ldots, e_n\} \subseteq \mathbb{F}^n$, where $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ where 1 is in the ith position. Then Span $\{e_1, \ldots, e_n\} = \mathbb{F}^n$.

(ii) Let $a, b, c \in \mathbb{F}$ and consider $S = \{(b, -a, 0), (0, c, -b)\}$, then we have Span $S = U_p$, where U_p is defined as in Example 4 (ii).

Exercise 10. Let e_i be as in Example 6 (i) and consider the set $S = \{je_i - ie_j\}_{1=i<j=n}$, then

$$\operatorname{Span} S = \{(v_1, \ldots, v_n) \in \mathbb{F}^n \mid v_1 + 2v_2 + \cdots + nv_n = 0\}.$$

Definition 7. A vector space U is *finite-dimensional* if there exists a finite subset $S \subseteq U$ such that Span $S = U$.

Example 7. (i) $\mathbb{F}^n$ is finite-dimensional.

Exercise 11. Check which of the examples of vector spaces defined so far are finite-dimensional.

Definition 8. (1) A *polynomial* with coefficients in $\mathbb{F}$ is a function $p : \mathbb{F} \to \mathbb{F}$ such that

$$p(x) = a_0 + a_1x + \cdots a_nx^n \tag{1}$$

for some $n \in \mathbb{N}$ and $a_i \in \mathbb{F}$.

(2) We let $\mathbb{F}[x]$ denote the set of polynomials in $\mathbb{F}$[3].

(3) Given a polynomial $p \in \mathbb{F}[x]$ the *degree* of p is the smallest natural number $n \in \mathbb{N}$ such that p can be written as (1). By convention, we set the degree of the zero polynomial to be $-\infty$.

(4) Let $\mathcal{P}_n(\mathbb{F})$ denote the set of polynomials of degree at most n.

Exercise 12. Check that $\mathcal{P}_n(\mathbb{F})$ forms a vector space.

Exercise 13. Assume that $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$. Let $p : \mathbb{F} \to \mathbb{F}$ be a function. Check that $p \in \mathcal{P}_n(\mathbb{F})$ if and only if $p^{(n+1)} = 0$.

[3]The textbook uses the notation $\mathcal{P}(\mathbb{F})$.

Exercise 14. The set $\mathbb{F}[x] = \mathcal{P}(\mathbb{F})$ is a vector space. Think about how we can formally define this.

Definition 9. Let V be a vector space over $\mathbb{F}$. Given a finite subset $S = \{v_1, \dots, v_n\} \subset V$ we say that S is *linearly independent* if

$$a_1 v_1 + \cdots + a_n v_n = 0 \implies a_1 = \cdots = a_n = 0,$$

where $a_1, \cdots, a_n \in \mathbb{F}$. By convention, we declare that $S = \emptyset$ is linearly independent. We say that a subset $S \subset V$ is linearly dependent if it is not linearly independent.

Example 8. (i) For every $k \in \{1, \dots, n\}$, the set $S = \{e_1, \dots, e_k\} \subset \mathbb{F}^n$, where e_i's are defined as in Example 6 (i), is linearly independent.

(ii) For any $k \geq 0$ the set $S_k := \{1, x, \dots, x^k\} \subset \mathbb{F}[x]$ is linearly independent.

(iii) Given $\{v, w\} \subset V$, then $\{v, w\}$ is linearly independent if and only if $n \neq aw$ for every $a \in \mathbb{F}$.

Exercise 15. Given a finite subset $S \subset V$. Prove that S if $0 \in S$ then S is linearly dependent.

Example 9. (1) the subset $S = \{e_1 - e_2, e_2 - e_3, e_3 - e_1\} \subset \mathbb{F}^3$ is linearly dependent.

(2) the subset $S = \{x^2, x^2 - 2x, 3x\} \subset \mathbb{F}[x]$ is linearly dependent.

Exercise 16. Given $S = \{(2, 3, 1), (1, -1, 2), (7, 3, c)\} \subset \mathbb{F}^3$. Check that S is linearly independent if and only if $c = 8$.

Exercise 17. Given $\{v_1, v_2, v_3, v_4\} \subset V$ a linearly independent set. Prove that $\{v_1, v_1 + v_2, v_1 + v_2 + v_3, v_1 + v_2 + v_3 + v_4\}$ is a linearly independent set.

The next result is extremely useful in many future proofs since it allows one to make a linearly dependent set smaller.

Lemma 3. *Let $\{v_1, \dots, v_n\} \subset V$ be a linearly dependent subset of a vector space V. Then there exists $k \in \{1, \dots, n\}$ such that*

$$v_k \in \text{Span}\,\{v_1, \dots, v_{k-1}\}.$$

In this case, one has:

$$\text{Span}\,\{v_1, \dots, v_n\} = \text{Span}\,\{v_1, \dots, v_n\} \backslash \{v_k\}.$$

Proof. Since $\{v_1, \dots, v_n\}$ is linearly dependent there exists $a_1, \dots, a_n \in \mathbb{F}$ not all zero such that

$$a_1 v_1 + \cdots + a_n v_n = 0.$$

Thus, let $k \in \{1, \dots, n\}$ such that $a_k \neq 0$, then we have:

$$v_k = -a_k^{-1}(a_1 v_1 + \cdots + a_{k-1} v_{k-1} + a_{k+1} v_{k+1} + \cdots + a_n v_n),$$

where the expression on the right above works for $k \in \{2, \dots, n-1\}$, we leave it to the reader to write the correct expression for the edge cases. To prove the last assertion we notice that clearly $\operatorname{Span}\{v_1, \dots, v_n\} \backslash \{v_k\} \subseteq \operatorname{Span}\{v_1, \dots, v_n\}$. Now suppose that $w \in \operatorname{Span}\{v_1, \dots, v_n\}$ and let $w = a_1 v_1 + \cdots + a_n v_n$. Since $v_k \in \operatorname{Span}\{v_1, \dots, v_{k-1}\}$, there exists $b_1, \dots, b_{k-1} \in \mathbb{F}$ such that $v_k = b_1 v_1 + \cdots + b_{k-1} v_{k-1}$. Then

$$w = (a_1 + b_1) v_1 + \cdots + (a_{k-1} + b_{k-1}) v_{k-1} + \sum_{i=k+1}^{n} a_i v_i,$$

so $w \in \operatorname{Span}\{v_1, \dots, v_n\} \backslash \{v_k\}$. This finishes the proof. □

Definition 10. Let $T \subseteq S \subset V$ be two finite subsets of a vector space. We say that T is a *spanning subset of* S if

$$\operatorname{Span} T = \operatorname{Span} S.$$

Lemma 4. *Consider $R, T \subseteq S \subset V$ finite subsets of a vector space V. Suppose that $\operatorname{Span} T = \operatorname{Span} S$ and that R is linearly independent. Then $|R| \leq |T|$.*

Proof. See the textbook (2.22). □

Corollary 1. *Let $U \subseteq V$ be a subset of a finite-dimensional vector space V, then U is finite-dimensional.*

Proof. We do an induction on the number of vectors necessary to span U. The base case is $U = \operatorname{Span} \emptyset = \{0\}$, in which case U is finite-dimensional. Assume that $U \neq \{0\}$ and let $v_1 \in U$ be a non-zero vector. Then if $U = \operatorname{Span} v_1$ we are done, otherwise there exists $v_2 \in U$ such that $v_2 \notin \operatorname{Span} v_1$ and we can consider $\operatorname{Span}\{v_1, v_2\}$. We claim that repeating this step k times gives $\operatorname{Span}\{v_1, \dots, v_k\} = U$ for some $k \in \mathbb{N}$. Indeed, let $S \subset V$ be a finite set such that $\operatorname{Span} S = V$. Such a set exists since V is finite-dimensional. Then consider $\{v_1, \dots, v_k\} \subseteq \{v_1, \dots, v_k\} \cup S$. Since $S \subseteq \{v_1, \dots, v_k\} \cup S$ spans V, we have that $k \leq |S|$, thus k is finite. □

2.3. **Basis.** The following concept is extremely important in linear algebra. One could say that the main difference between this course and Math2101 is that in Math2101 one is choosing a basis for every vector space that is considered by default, whereas in Math2102 we are not.

Definition 11. A subset $S \subset V$ is a *basis* if it satisfies:

(a) $\operatorname{Span} S = V$;

(b) S is linearly independent.

Example 10. (i) The set $\{e_1, \dots, e_n\}$ as defined in Example 6 (i) is a basis of $\mathbb{F}^n$.

(ii) The set $\{1, \dots, x^4\}$ is a basis of $\mathcal{P}_4(\mathbb{F})$ the vector space of polynomials of degree at most 4.

(iii) The sets $\{(7,5), (-4,9)\}$ and $\{(1,2), (3,5)\}$ are both basis of $\mathbb{F}^2$.

Remark 4. A subset $S = \{v_1, \dots, v_n\} \subset V$ is a basis of V if and only if every element $u \in V$ can be written as:

$$u = a_1 v_1 + \cdots + a_n v_n$$

for an unique choice of $a_1, \dots, a_n \in \mathbb{F}$. Indeed, suppose that there are two n-uples $(a_1, \dots, a_n), (b_1, \dots, b_n) \in \mathbb{F}^n$ such that

$$u = a_1 v_1 + \cdots + a_n v_n, \qquad u = b_1 v_1 + \cdots + b_n v_n,$$

and $a_i \neq b_i$ for some $i \in \{1, \dots, n\}$. Then we have:

$$\begin{aligned} 0 = u - u &= (a_1 v_1 + \cdots + a_n v_n) - (b_1 v_1 + \cdots + b_n v_n) \\ &= (a_1 - b_1) v_1 + \cdots + (a_n - b_n) v_n. \end{aligned}$$

Since S is linearly independent, we have that $a_i = b_i$ for all $i \in \{1, \dots, n\}$.

One of the consequences of Lemma 3 is that any finite spanning set contains a subset which is a basis.

Lemma 5. *Let $T \subset V$ be a finite spanning subset of V. Then there exists $S \subseteq T$ such that S is a basis.*

Proof. We proceed by downward induction. If T is linearly independent we are done. If T is linearly dependent, by Lemma 3 there exists $v \in T$ such that $\operatorname{Span} T \backslash \{v\} = \operatorname{Span} T = V$ and $|T \backslash \{v\}| < |T|$. Since T is finite this process stops and we obtain a basis. □

We get two immediate consequences:

Corollary 2. *(1) Every finite-dimensional vector space V admits a basis.*

(2) Any linearly independent subset $S = \{v_1, \dots, v_k\} \subset V$ extends to a basis.

Proof. For (1) let T be a finite set such that $\operatorname{Span} T = V$. By Lemma 5 there exists $S \subseteq T$ such that S is a basis of V.

For (2) let $T = \{w_1, \dots, w_n\}$ be a finite set such that $\operatorname{Span} T = V$. Then $\operatorname{Span} S \cup T = V$. Order the set $T \cup S$ as follows $\{v_1 < v_2 < \cdots < v_k < w_1 < \cdots < w_n\}$, then running the argument in the proof of Lemma 5 we notice that we obtain a subset $R \subset V$ such that:

$$S \subseteq R \subset S \cup T \qquad \text{and} \qquad \operatorname{Span} R = V.$$

□

The following result is interesting because it uses that $\mathbb{F}$ is a field in a serious way. In other words, certain concepts so far would make sense for more general objects as (commutative) rings, i.e. the integers $\mathbb{Z}$, however, the following result is the first to fail.

Lemma 6. *Let V be a finite vector space and consider a subspace $U \subseteq V$. Then there exists a subspace $W \subseteq V$ such that $U \oplus W = V$.*

Proof. Notice that U is also finite-dimensional. Let T be a basis for U (it exists by Corollary 2 (1)). By Corollary 2 (2) we can find $T \subset R$ such that R is a basis of V. We claim that $W := \operatorname{Span} R \backslash T$ satisfies $U \oplus W = V$. Indeed, it is clear that $U + W = V$, by Lemma 2 we need to check that $U \cap W = \{0\}$. We give names to the elements of $U = \{v_1, \dots, v_k\}$ and $W = \{v_{k+1}, \dots, v_n\}$. Assume by contradiction that there exists a non-zero vector $v \in U \cap W$, then we have

$$v = a_1 v_1 + \cdots a_k v_k = a_{k+1} v_{k+1} + \cdots + a_n v_n.$$

Thus, $a_1 v_1 + \cdots a_k v_k - (a_{k+1} v_{k+1} + \cdots + a_n v_n) = 0$, and since $\{v_1, \dots, v_k, v_{k+1}, \dots, v_n\}$ is linearly independent, we have that $a_i = 0$ for all $i \in \{1, \dots, n\}$. So we get a contradiction with $U \cap W \neq \emptyset$. This finishes the proof. □