Honours Algebra - Week 1 - Vector Spaces

Antonio León Villares

January 2022

Contents

Based on the notes by Iain Gordon, Sections 1.1 - 1.6

1 Fields

1.1 Defining Fields

- **What is a field?**
  - a **field** $\mathbb{F}$ is a set of elements equipped with 2 functions:
    * **addition**: an operation $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, such that:
    $$(\lambda, \mu) \to \lambda + \mu$$
    (where the meaning of $\lambda + \mu$ is defined by the specific field)
    * **multiplication**: an operation $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$, such that:
    $$(\lambda, \mu) \to \lambda\mu$$
    (where the meaning of $\lambda\mu$ is defined by the specific field)

- **Are fields groups?**
  - a **field** is an **abelian group**[1] under both **addition** $[(\mathbb{F}, +)]$ and **multiplication** $[(\mathbb{F}, \cdot)]$

- **What are the properties of elements in a field?**
  - *Distributive Property*
  $$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu, \qquad \lambda, \mu, \nu \in \mathbb{F}$$
  (notice, $\lambda(\mu + \nu)$ is just $\lambda \cdot (\mu + \nu)$)
  - *Commutative Property*
  $$\lambda + \mu = \mu + \lambda$$
  $$\lambda\mu = \mu\lambda$$
  - *Existence of Neutral Elements*: a field $\mathbb{F}$ is equipped with $0_{\mathbb{F}}$ (neutral element for addition) and $1_{\mathbb{F}}$ (neutral element for multiplication):
  $$\lambda + 0_{\mathbb{F}} = \lambda$$
  $$\lambda \cdot 1_{\mathbb{F}} = \lambda$$
  - *Existence of Inverse Elements*: a field $\mathbb{F}$ is equipped with inverse elements for both addition and multiplication, which when applied result in the neutral elements:
  $$\lambda + (-\lambda) = 0_{\mathbb{F}}$$
  $$\lambda \cdot (\lambda^{-1}) = 1_{\mathbb{F}}$$
  (the inverse multiplicative element exists provided that $\lambda \neq 0$)

1.2 Examples of Fields

- $\mathbb{R}, \mathbb{C}, \mathbb{Q}$.
- the set $0, 1$ is a field (also known as $\mathbb{Z}_2$). In particular, $\mathbb{Z}_p$ with p prime forms the field $\mathbb{F}_p$.
- however, $\mathbb{Z}$ is not a field, since for example 2 does **not** have a multiplicative inverse (since $0.5 \notin \mathbb{Z}$)

[1] Recall, an abelian group is a group such that its elements commute under the group operation, so if $a, b \in G$, then $a *_G b = b *_G a$.

2 Solutions of Simultaneous Linear Equations

2.1 Systems of Linear Equations

- **What is a system of linear equations?**
  - a group of n equations in m variables:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1m}x_m &= b_1 \\ \vdots \;+\; \vdots \;+\; \ldots \;+\; \vdots &= \vdots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nm}x_m &= b_n \end{aligned}$$

  - we typically consider systems in which a_{ij}, x_k are part of a **field**
  - we solve the system by finding the **m-tuple**:

$$(x_1, x_2, \ldots, x_m)$$

    (with all elements in $\mathbb{F}$) which satisfies the n equations

- **When is a system of linear equations homogeneous?**
  - when each of the $b_1, b_2, \ldots, b_n$ are 0
- **What is the solution set of a system?**
  - the subset $L \subseteq \mathbb{F}^m$ of all **m-tuples** which satisfy the system

2.2 Defining a Matrix

- **What is a matrix?**
  - we can think of a **matrix** as a mapping of the form:

$$\{1, \ldots, n\} \times \{1, \ldots, m\} \to Z$$

    where Z is just a set. Succintly:

$$Mat(n \times m : Z) := Maps(\{1, \ldots, n\} \times \{1, \ldots, m\}, Z)$$

  - this is known as an $\boldsymbol{n \times m}$**-matrix with coefficients in** $\boldsymbol{Z}$
  - this is just an overextended way of saying that a **matrix** is a collection of elements organised at certain indices (i, j) in a table like structure
- **What is an element of a matrix?**
  - a matrix element can be described using a_{ij}. where:
    * **i** is the **row-index**
    * **j** is the **column-index**

2.3 Gaussian Elimination

- **What is a coefficient matrix?**
  - a matrix in which we display the coefficients of a system
  - a_{ij} corresponds to the ith coefficient in the jth equation
  - for example, if we have the system:

$$\begin{aligned} x + 3y &= 0 \\ 2x + 2y + z &= 2 \\ 4x + 6y = z &= 8 \end{aligned}$$

    its corresponding coefficient matrix is:

$$\begin{pmatrix} 1 & 3 & 0 \\ 2 & 2 & 1 \\ 4 & 6 & 1 \end{pmatrix}$$

- **What is an extended coefficient matrix?**
  - a coefficient matrix, but with an added column, containing the values of the RHS terms $(b_1, b_2 \ldots .)$
- **What is Gaussian Elimination?**
  - **Gaussian Elimination** is the use of 3 operations which simplify the system, without changing its solution set
  - the operations are:
    * *row addition*: adding a row of the matrix to another row
    * *scalar multiplication*: multiplying the row of a matrix by a scalar
    * *row swap*: swap 2 rows
- **What is echelon form?**
  - a special form of an **extended coefficient matrix**, such that it allows for the system to be solved trivially
  - a matrix is in echelon form if:
    * any row consisting entirely of zeros occurs at the bottom of the matrix
    * for two successive (non-zero) rows, the leading non-zero entry in the higher row is further left than the leading non-zero entry in the lower row

2.4 Theorem: Solution Sets of Inhomogeneous Systems of Linear Equations

> *If the **solution set** of a linear system of equations is **non-empty**, then we obtain **all** solutions by adding **componentwise** an **arbitrary solution** of the associated homogenised system to a **fixed solution** of the system. [Theorem 1.1.4]*

Proof. Consider 2 particular solutions:

$$a = (a_1, \ldots, a_m)$$

$$b = (b_1, \ldots, b_m)$$

These solutions satisfy a possibly inhomogeneous system. If we subtract pairwise:

$$h = (b_1 - a_1, \ldots, b_m - a_m)$$

By construction, h solves the homogeneous system. But then it follows that the particular solution b (and since b was arbitrary, any other particular solution) can be found via the pairwise addition:

$$b = a + h$$

as required.

$\square$

3 Vector Spaces

3.1 Defining Vector Spaces

- **What is a vector space?**
  - for this, forget any notion of what a vector is, it makes it easier to understand the abstract definition
  - we define a **vector space over a field**, as a pair consisting of an **abelian group** $(V, \dot{+})$ and a mapping:
    $$\mathbb{F} \times V \to V \quad : \quad (\lambda, \underline{v}) \to \lambda\underline{v}$$
    where $\mathbb{F}$ is a **field**, $\lambda \in \mathbb{F}$ and $\underline{v} \in V$.
  - we use $\dot{+}$ as a way to distinguish from the "addition operator" $(+)$ for fields (however, I might be inconsistent, but hopefully whether I use it to add elements of the vector space or from a field will be clear from context)
- **What is an F-Vector Space?**
  - saying an F-Vector Space is the same as saying a vector space defined over the field F
- **What is a vector?**
  - an element of a **vector space**
  - this need not be a vector as we know it. For example, matrices and functions can be elements of a vector space.
- **What is a ground field?**
  - the naming convention we use to refer to the field $\mathbb{F}$ defining a vector space
- **What is multiplication by scalars?**
  - the mapping defining the vector space:
    $$(\lambda, \underline{v}) \to \lambda\underline{v}$$
  - this is also known as the **action of the field $\mathbb{F}$ on V**
- **What identities define a vector space?**

– *Distributive Law*: we can distribute a scalar across vectors

$$\lambda(\underline{v}\dot{+}\underline{w}) = \lambda\underline{v}\dot{+}\lambda\underline{w}, \qquad \underline{v}, \underline{w} \in V, \lambda \in \mathbb{F}$$

or a vector across scalars:

$$(\lambda + \mu)\underline{v} = \lambda\underline{v}\dot{+}\mu\underline{v}, \qquad \underline{v} \in V, \lambda, \mu \in \mathbb{F}$$

– *Associative Law*:

$$\lambda(\mu\underline{v}) = \mu(\lambda\underline{v}), \qquad \underline{v} \in V, \lambda, \mu \in \mathbb{F}$$

– *Applying the Multiplicative Identity*:

$$1_{\mathbb{F}}\underline{v} = \underline{v}, \qquad \underline{v} \in V, 1_{\mathbb{F}} \in \mathbb{F}$$

- **What is the trivial vector space?**
  - the one element abelian group $V = \{0\}$
  - in particular, this is a vector space over **any** field

3.2 Properties of Vector Spaces

3.2.1 Lemma: Product With 0 Scalar

If V is a vector space and $\underline{v} \in V$, then $0_{\mathbb{F}}v = \underline{0}$, where $\underline{0} \in V$ is the 0-vector. [Lemma 1.2.2]

Proof.

$$\begin{aligned} 0_{\mathbb{F}}\underline{v} &= 0_{\mathbb{F}}\underline{v} \\ &= (0_{\mathbb{F}} + 0_{\mathbb{F}})\underline{v} \\ &= 0_{\mathbb{F}}\underline{v} + 0_{\mathbb{F}}\underline{v} \\ \implies 0_{\mathbb{F}}\underline{v} - 0_{\mathbb{F}}\underline{v} &= 0_{\mathbb{F}}v \\ \implies \underline{0} &= 0_{\mathbb{F}}\underline{v} \end{aligned}$$

□

3.2.2 Lemma: Product With -1 Scalar

If V is a vector space and $\underline{v} \in V$, then $(-1)\underline{v} = -\underline{v}$, where $-\underline{v} \in V$ is the additive inverse of $\underline{v}$. [Lemma 1.2.3]

Proof.

$$\begin{aligned} &\underline{v}\dot{+}(-1)\underline{v} \\ =&1\underline{v}\dot{+}(-1)\underline{v} \\ =&(1 + (-1))\underline{v} \\ =&0_{\mathbb{F}}\underline{v} \\ =&\underline{0} \end{aligned}$$

So it follows that $(-1)\underline{v}$ must be the additive inverse of $\underline{v}$, as required. □

3.2.3 Lemma: Product With The Zero Vector

If V is a vector space and $\underline{v} \in V$, then:

- $\lambda \underline{0} = \underline{v}, \qquad \underline{0}, \underline{v} \in V, \forall \lambda \in \mathbb{F}$
- $\lambda \underline{v} = \underline{0} \implies \lambda = 0_{\mathbb{F}}$ *or* $\underline{v} = \underline{0}$

[Lemma 1.2.4]

Proof. (This is independently developed by me, without checking with professors or online, so take with a grain of salt)

$$\begin{aligned} \lambda 0 &= \lambda(0 \dot{+} 0) \\ \implies \lambda 0 &= \lambda 0 \dot{+} \lambda 0 \\ \implies \lambda 0 \dot{+} (-\lambda 0) &= \lambda 0 \\ \implies 0 &= \lambda 0 \end{aligned}$$

For the second part, notice that we have:

- $\underline{0} = \lambda \underline{0}$
- $\underline{0} = 0_{\mathbb{F}} \underline{v}$

Hence, if $\lambda \underline{v} = \underline{0}$, it must be so either because:

- $\lambda \underline{v} = \underline{0} \implies \lambda \underline{v} = \lambda \underline{0} \implies \underline{v} = \underline{0}$
- $\lambda \underline{v} = \underline{0} \implies \lambda \underline{v} = 0_{\mathbb{F}} \underline{v} \implies \lambda = 0_{\mathbb{F}}$

□

3.3 Examples

- the set $V = \mathbb{F}^n$, where:
$$\mathbb{F}^n = \{(a_1, a_2, \ldots, a_n) | a_i \in \mathbb{F})\}$$
also forms a vector space over the field $\mathbb{F}$, where scalar multiplication is defined elementwise:
$$\lambda(a_1, a_2, \ldots, a_n) = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n)$$
- for $n = 1$, we can see that this is true, since fields are abelian groups, and scalar multiplication is defined as multiplication in $\mathbb{F}$, so $V = \mathbb{F}$ constitutes a valid F-vector space
- a matrix with each $a_{ij} \in \mathbb{F}$ is also a vector space over $\mathbb{F}$, with addition and scalar multiplication defined componentwise. In fact, the set V of all such $m \times n$ matrices is **isomorphic** to $\mathbb{F}^{mn}$.

3.4 Exercises

1. **Given a set X and a vector space V over $\mathbb{F}$, show that the set $Maps(X;V)$ of all mappings $X \to V$ is an F-vector space, if we define addition by $(f+g)(x) = f(x)+g(x)$ and multiplication by scalars by $(\lambda f)(x) = \lambda(f(x))$.**

   To prove that this is a F-vector space, we can check the properties. For example, for the dsitributive law, we want to show that:

   $$(\lambda(f+g))(x) = (\lambda f + \lambda g)(x)$$

   Indeed:

   $$\begin{aligned} &(\lambda(f+g))(x) \\ =&\lambda \cdot (f+g)(x) \\ =&\lambda \cdot (f(x)+g(x)) \\ =&\lambda \cdot (f(x)) + \lambda \cdot (g(x)) \\ =&(\lambda f)(x) + (\lambda g)(x) \\ =&(\lambda f + \lambda g)(x) \end{aligned}$$

   The second distributive property:

   $$((\lambda+\mu)f)(x) = (\lambda f + \mu f)(x)$$

   Indeed:

   $$\begin{aligned} &((\lambda+\mu)f)(x) \\ =&(\lambda+\mu)f(x) \\ =&\lambda(f(x)) + \mu(f(x)) \\ =&(\lambda f)(x) + (\mu f)(x) \\ =&(\lambda f + \mu f)(x) \end{aligned}$$

   Associativity:

   $$(\lambda(\mu f))(x) = (\mu(\lambda f))(x)$$

   Indeed:

   $$\begin{aligned} &(\lambda(\mu f))(x) \\ =&((\lambda\mu)f)(x) \\ =&((\mu\lambda)f)(x) \\ =&(\mu(\lambda f))(x) \end{aligned}$$

   where we have used the associativity of $\lambda, \mu \in \mathbb{F}$.

   Finally, the multiplicative identity is just the identity of the field.

4 The Cartesian Product

4.1 Defining the Cartesian Product

- **What is the cartesian product?**

- an **operator** which produces new sets from a set of other sets
- given n sets $X_1, X_2, \ldots, X_n$, the cartesian product of these sets is a set of **n-tuples**:

$$X_1 \times X_2 \times \ldots \times X_n = \{(x_1, x_2, \ldots, x_n) | x_i \in X_i, i \in [1, n]\}$$

- **What is a component of an n-tuple?**
  - an individual entry x_i in the n-tuple $(x_1, x_2, \ldots, x_n)$
- **What does the notation X^n mean?**
  - we have taken the cartesian product of the set X with itself n times
- **Can we take cartesian products of cartesian products?**
  - since cartesian products operate on sets, we can apply the cartesian product to sets produced by the cartesian product
  - for example:
  $$X^n \times X^m = \{((x_{n1}, x_{n2}, \ldots, x_{nn}), (x_{m1}, x_{m2}, \ldots, x_{mm}))\}$$
  - in fact, there exists a bijection $X^n \times X^m \to X^{n+m}$, such that:
  $$((x_{n1}, x_{n2}, \ldots, x_{nn}), (x_{m1}, x_{m2}, \ldots, x_{mm})) \to (x_{n1}, x_{n2}, \ldots, x_{nn}, x_{m1}, x_{m2}, \ldots, x_{mm})$$
- **What is a projection of a cartesian product?**
  - a way of extracting a component of an n-tuple:
  $$pr_i : X_1 \times X_2 \times \ldots \times X_n \to X_i$$
  such that:
  $$pr_i : (x_1, x_2, \ldots, x_n) \to x_i$$

4.2 Exercises

1. **Consider a field $\mathbb{F}$, and a number of F-vector spaces $V_1, V_2, \ldots, V_n$. Show that the cartesian product $V_1 \times V_2 \times \ldots \times V_n$ is an F-vector space, with addition and multiplication defined componentwise. This new vector space is written using special notation:**

$$V_1 \oplus V_2 \oplus \ldots \oplus V_n$$

This is known as the *external direct sum* (or *direct sum* or *product*). Notice that technically, $\mathbb{F}^n$ is the external direct sum of the 1 dimensional F-vector space $\mathbb{F}$.

For this, the external direct product is a set of n-tuples, in which each entry is a vector $\underline{v}_i \in V_i$, with addition defined as:
$$(\underline{v}_1, \ldots, \underline{v}_n) + (\underline{w}_1, \ldots, \underline{w}_n) = (\underline{v}_1 + \underline{w}_1, \ldots, \underline{v}_n + \underline{w}_n)$$
and scalar multiplication:
$$\lambda \cdot (\underline{v}_1, \ldots, \underline{v}_n) = (\lambda\underline{v}_1, \ldots, \lambda\underline{v}_n)$$
These definition ensure closure under addition and multiplication. We consider the remaining properties for only 2 vector spaces, V, W. For example, for *Distributivity of a Scalar*: we want to show that

$$\lambda((\underline{v}_1, \underline{w}_1) + (\underline{v}_2, \underline{w}_2)) = \lambda(\underline{v}_1, \underline{w}_1) + \lambda(\underline{v}_2, \underline{w}_2)$$

Indeed:

$$\begin{aligned}
&\lambda((\underline{v}_1, \underline{w}_1) + (\underline{v}_2, \underline{w}_2)) \\
=&\lambda(\underline{v}_1 + \underline{v}_2, \underline{w}_1 + \underline{w}_2) \\
=&(\lambda(\underline{v}_1 + \underline{v}_2), \lambda(\underline{w}_1 + \underline{w}_2)) \\
=&(\lambda\underline{v}_1 + \lambda\underline{v}_2, \lambda\underline{w}_1 + \lambda\underline{w}_2) \\
=&(\lambda\underline{v}_1, \lambda\underline{w}_1) + (\lambda\underline{v}_2, \lambda\underline{w}_2) \\
=&\lambda(\underline{v}_1, \underline{w}_1) + \lambda(\underline{v}_2, \underline{w}_2)
\end{aligned}$$

5 Vector Subspaces

5.1 Defining Subspaces

- **What is a vector subspace?**
  - consider a vector space V, and a subset $U \subseteq V$
  - U is a **vector subspace** if and only if:
    * $\underline{0} \in U$
    * $\underline{a}, \underline{b} \in U \implies \underline{a} + \underline{b} \in U$
    * $\underline{a} \in U, \lambda \in \mathbb{F} \implies \lambda\underline{a} \in U$

5.1.1 Examples

- the trivial space, $\{\underline{0}\}$ is a subspace
- the whole vector space itself is a subspace
- if we have a homogeneous system, and L is the solution set, then $L \subseteq \mathbb{F}^m$ is a vector subspace, since:
  - $(0, 0, \dots, 0)$ is clearly a solution
  - adding 2 homogeneous solutions leads to another homogeneous solution
  - scaling a homogeneous solution by a constant factor is still a solution
- any straight line or plane passing through the origin (since scaling or adding vectors in a line/plane just results in another element of the line/plane)
- however, a line which doesn't go through the origin is not a subspace. For example, $y = 1$ in the vector space $\mathbb{R}^2$ over $\mathbb{F} = \mathbb{R}$:
  - it doesn't contain $\underline{0}$
  - take 2 elements, they have the form $(a, 1)$ and $(b, 1)$. Clearly,

    $$(a, 1) + (b, 1) = (a + b, 2)$$

    which is not in the line $y = 1$
  - scaling doesn't work either:

    $$\lambda(a, 1) = (\lambda a, \lambda)$$

    which is not in the line $y = 1$

- similarly, a (filled) sphere in $\mathbb{R}^3$ is not a vector subspace. A sphere of radius r is defined by:

$$S = \{(x, y, z) | x^2 + y^2 + z^2 \leq r^2\}$$

Whilst $S \subseteq \mathbb{R}^3$ contains $(0, 0, 0)$, it doesn't satisfy closure under addition:

$$(r, 0, 0), (0, r, 0) \in S, \qquad (r, r, 0) \notin S$$

or scalar multiplication:

$$(r, 0, 0) \in S, \lambda > 1, \qquad (\lambda r, 0, 0) \notin S$$

5.2 Linear Combinations

- **What is a linear combination?**
  - a linear combination is **finite** sum of vectors, each of which can be multiplied by a **scalar**:

$$a_1 \underline{v}_1 + a_2 \underline{v}_2 + \ldots + a_n \underline{v}_n$$

    where $a_i \in \mathbb{F}, v_i \in V$

- **What is span?**
  - given a set of vectors S, we define the span $span(S)$ as the **set of all linear combinations** of vectors in S
  - for example, $span(\{(0, 1), (1, 0)\})$ is the set of all vectors of the form (α, β) (in fact, notice that $span(\{(0, 1), (1, 0)\}) = \mathbb{R}^2$)
  - notice, the span always contains the 0 vector

5.3 Proposition: Generating a Vector Subspace From a Subset

*Let $T \subseteq V$, where V is a vector space over a field. Amongst all subspaces containing T, define the smallest such subspace as $\langle T \rangle$. Then, $\langle T \rangle$ is the span of T (where the span of the empty set is just the zero vector). We call $\langle T \rangle$ the **vector subspace generated by** T. [Proposition 1.4.5]*

Proof. Since $\langle T \rangle$ contains all possible linear combinations of vectors in T, then addition or scalar multiplication of any element in $\langle T \rangle$ must still be a member of $\langle T \rangle$, so it is a subspace.

Moreover, any subspace containing T must be such that it contains all possible linear combinations of T. □

5.4 Generating Sets

- **What is a generating set of a vector space?**
  - let $T \subseteq V$, where V is a vector space
  - T is a **generating set** of V if $span(T) = V$ (so the span of T is the whole vector space)
- **What is a finitely generated vector space?**
  - a vector space that can be generated by a **finite** subset T
  - for example, when discussing span, we noticed that $\mathbb{R}^2$ is finitely generated by:

$$T = \{(0, 1), (1, 0)\}$$

5.4.1 Examples

- this example illustrates the importance of a field to define a vector space. For example, consider $V = \mathbb{R}$ and $\mathbb{F} = \mathbb{Q}$. Consider the set $U = \{1\}$. Then,

  $$span(U) = \{\lambda \cdot 1 | \lambda \in \mathbb{Q}\} = \mathbb{Q} \neq \mathbb{R}$$

  In fact, the span of any finite set U over the field $\mathbb{Q}$ will be countable, so in particular, $\mathbb{R}$ can never be finitely generated over $\mathbb{Q}$.

5.4.2 Exercises (TODO)

1. **A subset of a vector space is called a linear hyperplane if it is a (proper) subspace of the vector space, and such that the hyperplane, alongside some other vector (not belonging to the hyperplane), generates the whole vector space. Prove that a hyperplane and a vector not contained in the hyperplane are sufficient to generate the original space.**

5.5 Example: Span Unchanged After Adding One of its Elements

If $\underline{v} \in span(T) = \langle T \rangle$, then $span(T \cup \{\underline{v}\}) = span(T)$. [Example 1.4.6]

Proof. It is clear that $span(T) \subseteq span(T \cup \{\underline{v}\})$, since the latter is the span of a (potentially) larger set, so all elements of $span(T)$ must be contained in it.

Similarly, pick $\underline{w} \in span(T \cup \{\underline{v}\})$. Then we can write:

$$\underline{w} = \sum a_i \underline{v}_i + b\underline{v}$$

But since $\underline{v} \in span(T)$,

$$\underline{v} = \sum c_i \underline{v}_i$$

So:

$$\underline{w} = \sum a_i \underline{v}_i + \sum (bc_i)\underline{v}_i = \sum (a_i + bc_i)\underline{v}_i$$

Hence, $span(T \cup \{\underline{v}\}) \subseteq span(T)$. Overall, both sets must be equal, as required. □

5.6 Union and Intersection

- **What is a power set?**
  - consider a set X
  - the **power set** of X, denoted by $\mathcal{P}(X)$, is the set obtained from all the subsets of X
  - we shall call a subset of the power set a **system of sets** (to avoid saying a set of sets)
- **How can we create subsets from the pwoer set (I still understand what the point of this was)?**
  - consider a system $\mathcal{U} \subseteq \mathbb{P}(X)$
  - define the **union** and **intersection** of sets in $\mathcal{U}$ via:

$$\bigcup_{U \in \mathcal{U}} U = \{x \in X | there\ is\ U \in \mathcal{U}\ with\ x \in U\}$$

$$\bigcap_{U \in \mathcal{U}} U = \{x \in X | if\ x \in U\ for\ all\ U \in \mathcal{U}\}$$

- what is "interesting" about this is that if we take $\mathcal{U}$ to be an empty system of subsets of X:
  * the union of U is just the empty set (easy to see, since the empty set contains no element, so no x will be part of the union)
  * the intersection of U is all of X (this due to a **vacuous truth**, by which, since there are no U, the requirement is always true, so all x get added)

5.6.1 Exercises (TODO)

1. **Show that: each intersection of vector subspaces of a vector space is again a vector subspace. Note that this has the following consequence: for a subset T of a vector space V over $\mathbb{F}$ the intersection of all vector subspaces of V that contain T is obviously the smallest vector subspace of V that contains T. This provides us with a new proof of Proposition 1.4.5 on the existence of such a smallest subspace. This proof has the advantage that it is easier to generalise.**

6 Linear Independence

6.1 Defining Linear Independence and Dependence

- **What is linear independence of vectors?**
  - consider a subset $L \subseteq V$ of a vector space V
  - we say L is **linearly independent** if the only way for a linear combination of all pairwise distinct vectors in L to be 0 is if each scalar coefficient is 0:

$$\sum_{i=1}^{r} a_i \underline{v}_i = \underline{0} \implies a_1 = a_2 = \ldots = a_r = 0$$

- **What is linear dependence of vectors?**
  - a subset $L \subseteq V$ is **linearly dependent** if it isn't linearly independent
  - in other words, there exist non-zero scalars such that:

$$\sum_{i=1}^{r} a_i \underline{v}_i = \underline{0}$$

- **What does it mean if a generating set is linearly dependent?**
  - that there are terms in the generating set that are **redundant**
  - for example, if L is a generating set, we can reduce its number of elements, since:

$$\sum_{i=1}^{r} a_i \underline{v}_i = \underline{0} \implies \underline{v}_1 = a_1^{-1} \left(- \sum_{i=2}^{r} a_i \underline{v}_i \right)$$

    Hence, with $r-1$ terms, we can generate everything that the previous r terms could generate
  - this illustrates that a set is linearly dependent if at least one of its vectors can be written as a linear combination of the remaining vectors

6.2 Examples

- the empty set is **linearly independent** in every vector space
  - think about it: the empty set is a valid subset of any vector space
  - consider any linear combination of elements in $\emptyset$
  - since there are no elements, no coefficients can be used to make the linear combination 0
  - hence, the empty set must be a linearly independent set
- the singleton set $\{\underline{0}\}$ is always **linearly dependent**, since for any $\lambda \in \mathbb{F}, \lambda \neq 0_{\mathbb{F}}$ we have:

$$\lambda\underline{0} = \underline{0}$$

- however, any singleton set containing a non-zero vector is always **linearly independent** (this follows by (3.2.3), since a scalar applied to a non-zero vector is 0 if and only if the scalar itself is 0)
- a two-element subset of a vector space is **linearly independent** if neither of its vectors is a multiple of the other
-

7 Bases

7.1 Defining a Basis of a Vector Space

- **What is a basis of a vector space?**
  - given a vector space V, a **basis** of V is a **linearly independent** generating set of V

7.1.1 Exercises

1. **Consider the vector space $V = \mathbb{R}^2$ over the field $\mathbb{F} = \mathbb{R}$. Is the subset:**

$$T = \{(4, 2), (1, 2)\}$$

a basis for V?

Consider $(a, b) \in V$. Since the elements of T are not multiples of each other, T forms a basis if there exists some linear combination of its elements that can generate (a, b). In other words, we want:

$$\lambda(4, 2) + \mu(1, 2) = (a, b)$$

In other words, we have a linear system, which we can solve for λ, μ:

$$\begin{aligned}
&\left(\begin{array}{cc|c} 4 & 1 & a \\ 2 & 2 & b \end{array}\right) \\
\iff &\left(\begin{array}{cc|c} 4 & 1 & a \\ 0 & 3 & 2b-a \end{array}\right) \\
\iff &\left(\begin{array}{cc|c} 4 & 1 & a \\ 0 & 1 & \frac{2b-a}{3} \end{array}\right) \\
\iff &\left(\begin{array}{cc|c} 4 & 0 & a - \frac{2b-a}{3} \\ 0 & 1 & \frac{2b-a}{3} \end{array}\right) \\
\iff &\left(\begin{array}{cc|c} 1 & 0 & \frac{a}{4} - \frac{2b-a}{12} \\ 0 & 1 & \frac{2b-a}{3} \end{array}\right)
\end{aligned}$$

In other words, given (a, b), we can use:

$$\lambda = \frac{a}{4} - \frac{2b-a}{12}$$

$$\mu = \frac{2b-a}{3}$$

and T can generate it. In other words, T must be a basis for V.

(To check linear independence, we can do the same thing, but using $a = b = 0$, and check whether $\lambda = \mu = 0$ is the only solution)

7.2 Defining a Family of Elements

- **What is a family of elements?**
  - consider two sets I (for indices) and A (a set of elements)
  - the mapping $I \to A$ is known as the **family of elements of A indexed by I**
  - such a family is succinctly described by:

$$(a_i)_{i \in I}$$

- **How do subsets an families of elements differ?**
  - (apparently) a family allows for the same vector to be described by 2 different indices
- **How does terminology for sets transfer to families?**
  - if the set $\{\underline{v}_i | i \in I\}$ is generating, then the family $(\underline{v}_i)_{i \in I}$ is also **generating**
  - a **linearly independent family** is one such that for pairwise distinct indices $(i(1), i(2), \dots, i(r))$ we have:

$$\sum_{j=1}^{r} a_j \underline{v}_{i(j)} = 0$$

    only if each $a_j = 0$. Notice, if two indices refer to the same vector, the family won't be linearly independent
  - a **linearly dependent family** is one which isn't linearly independent

- a linearly independent, generating family of vectors is a **basis** (or **basis indexed by** $i \in I$)

- **What is an ordered basis?**
  - if we index a basis, we obtain an **ordered basis**
  - this can be useful, for example when defining the basis vectors in $\mathbb{R}^n$, where $\underline{e}_1, \ldots, \underline{e}_n$ defined by having a 1 at index i, and 0 otherwise, is the **standard basis**, which is an **ordered basis**

7.3 Theorem: Linear Combination of Basis Elements

This theorem gives us a condition to check whether a family is a valid basis for a vector space.

> *Let $\mathbb{F}$ be a field, V a vector space over $\mathbb{F}$ and consider the vectors $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_r \in V$. The family $(\underline{v}_i)_{1 \leq i \leq r}$ is a basis of V* ***if and only if*** *the following "evaluation" mapping is a bijection:*
>
> $$\Phi : \mathbb{F}^r \to V$$
>
> $$(\alpha_1, \alpha_2, \ldots, \alpha_r) \to \sum_{i=1}^{r} \alpha_i \underline{v}_i$$
>
> *Hence, a family is a basis if each element in V is* ***uniquely*** *constructed by using a single r-tuple of coefficients.*
> *If such a mapping is done with ordered family $\mathcal{A} = (\underline{v}_1, \ldots, \underline{v}_r)$, the mapping can be written as $\Phi_{\mathcal{A}} : \mathbb{F}^r \to V$ [Theorem 1.5.11]*

Proof. We first claim that the family $(\underline{v}_i)_{1 \leq i \leq r}$ is a generating set **if and only if** Φ is a surjection:

- $(\Longrightarrow)$: if the family is a generating set, Φ will clearly be surjective, since this is the definition of a generating set: all elements in V are mapped to using linear combinations of elements in the generating set

- $(\Longleftarrow)$: similarly, if Φ is surjective, then every element in V must be mapped to under its application, so by definition, the family must constitute a basis

Secondly, we claim that the family $(\underline{v}_i)_{1 \leq i \leq r}$ is linearly independent **if and only if** Φ is injective:

- $(\Longrightarrow)$: consider that the family is linearly independent. We proceed by contradiction: assume that Φ is not injective. In this case, then there must exist 2 distinct r-tuples which map to the same element in V. In other words:

  $$\sum_{i=1}^{r} \alpha_i \underline{v}_i = \sum_{j=1}^{r} \beta_j \underline{v}_j \implies \sum_{i=1}^{r} (\alpha_i - \beta_i) \underline{v}_i = \underline{0}$$

  Since the 2 r-tuples are distinct, at least one of the $(\alpha_i - \beta_i)$ must be non-zero, which then implies that the family is linearly dependent, a contradiction. Hence, it follows that if the family is linearly independent, Φ must be injective.

- $(\Longleftarrow)$: now assume that Φ is injective. Notice, Φ maps the r-tuple containing only 0's to $\underline{0}$. Injectivity means that this is the only r-tuple which achieves this; in other words, the family must be linearly independent.

From the equivalences above, we can see that a family $(\underline{v}_i)_{1 \leq i \leq r}$ is a generating set **and** linearly independent **if and only if** the mapping Φ is surjective **and** injective. In other words, the family $(\underline{v}_i)_{1 \leq i \leq r}$ is a basis **if and only if** the mapping Φ is bijective, as required.

□

7.4 Theorem: Characterisation of Bases

This theorem provides us with equivalences that can be used to verify whether a subset is indeed a basis.

> *The following are equivalent for a subset E of a vector space V:*
>
> 1. *The subset E is a* ***basis*** *(linearly independent, generating set)*
> 2. *E is* ***minimal amongst all generating sets*** *(if we remove any element of E (i.e $V \setminus \{\underline{v}\}$), it will no longer generate V)*
> 3. *E is* ***maximal amongst all linearly independent subsets*** *(if we add any element to E (i.e $E \cup \{\underline{v}\}$) it will no longer be linearly independent)*
>
> *In other words, when looking for a basis, we look for the smallest generating subset with the largest number of linearly independent vectors. [Theorem 1.5.12]*

Proof. We show the equivalence of 1 and 2, and of 1 and 3.

- $1 \iff 2$
  - ($\Longrightarrow$): assume E is a basis. We proceed by contradiction: say E is not minimal, such that $span(E \setminus \{\underline{v}\}) = V$, $\underline{v} \in V$. Then, using $\underline{v}_i \in E \setminus \{\underline{v}\}$, we can write:

    $$\underline{v} = \sum_{i=1}^{r} a_i \underline{v}_i \implies \sum_{i=1}^{r} a_i \underline{v}_i - \underline{v} = \underline{0}$$

    This then means that E is a linearly dependent subset, which contradicts the fact that it is a basis. Hence, if E is a basis, E must be minimal.
  - ($\Longleftarrow$): assume E is minimal. We again proceed by contradiction, assuming that E is a generating set which is linearly dependent. In other words, there are some $a_i \neq 0$ such:

    $$\sum_{i=1}^{r} a_i \underline{v}_i = \underline{0}$$

    (again vectors are pairwise distinct, and $r \geq 1$). Without loss of generality, lets assume that, in particular, $a_1 \neq 0$. Then, we can rearrange, to see that:

    $$\underline{v}_1 = a_1^{-1} \left(- \sum_{i=2}^{r} a_i \underline{v}_i \right)$$

    In other words, $E \setminus \{\underline{v}_1\}$ would be a generating set too, which contradicts the fact that E was minimal. Hence, if E is minimal, E must be a basis.
- $1 \iff 3$
  - ($\Longrightarrow$): since E is a basis, consider $\underline{v} \in V \setminus E$. There exists some non-zero scalars, such that:

    $$\underline{v} = \sum_{i=1}^{r} a_i \underline{v}_i \implies \sum_{i=1}^{r} a_i \underline{v}_i - \underline{v} = 0$$

    In other words, the set defined by $E \cup \{\underline{v}\}$ is linearly dependent, as required.

– ($\Longleftarrow$): we now assume that E is maximal, and proceed by contradiction: assume that E is a linearly independent set, but it doesn't generate V. Then, $\exists \underline{v} \in V$ such that $\underline{v} \notin span(E)$. But now consider $E \cup \{\underline{v}\}$. Assume there are scalars, such that a linear combination of this set is equal to $\underline{0}$:

$$\sum_{i=1}^{r} a_i \underline{v}_i + b\underline{v} = \underline{0}$$

Since E doesn't generate $\underline{v}$, this is only possible if $b = 0$. And if this is the case, by linear independence of the $\underline{v}_i$, the a_i must be 0 too. Hence, it implies that $E \cup \{\underline{v}\}$ is linearly independent, contradicting the fact that E is maximal.

□

7.5 Corollary: The Existence of a Basis

Let V be a finitely generated vector space over a field $\mathbb{F}$. Then V has a finite basis. [Corollary 1.5.13]

Proof. The proof is simple. Say E is a generating set of some vector space V. While E is not linearly independent, we remove vector, so long as E remains a generating set. For example, at the second step, we redefine $E = E \setminus \{\underline{e}_{i(1)}\}$. If we continue this until we reach linear independence, we will have produced a linearly independent, generating set - a basis!

□

7.6 Theorem: Variant of the Characterisation of Bases

Let V be a vector space. Then:

1. *If:*
   - *$L \subset V$ is a **linearly independent** subset*
   - *E is **minimal** amongst all **generating** sets with the property that $L \subseteq E$*

   *Then, E is a **basis**.*

2. *If:*
   - *$E \subseteq V$ is a **generating** set*
   - *L is **maximal** amongst all **linearly independent** subsets with the property that $L \subseteq E$*

   *Then, L is a **basis**.*

This says that a minimal generating set which contains all linearly independent subsets is a basis. Alternatively, a linearly independent subset which is maximal and contained within any generating set is a basis. [Theorem 1.15.14]

7.7 The Free Vector Space

- **What is the set of mappings?**
  - define the set $Maps(X, \mathbb{F})$, where X is a set, and $\mathbb{F}$ is a field
  - this is the set of all functions $f : X \to \mathbb{F}$
  - under pointwise addition and scalar multiplication, this is a vector space
- **What is a free vector space?**
  - the **free vector space over $\mathbb{F}$ on the set** X is the subset of all mappings in $Maps(X, \mathbb{F})$ which send almost all elements to 0
  - we denote the free vector space via $\mathbb{F}\langle X \rangle$
  - $\mathbb{F}\langle X \rangle$ is a vector subspace
- **What does "almost all" mean in this context?**
  - only finitely many inputs are mapped to non-zero outputs
  - for example, if $X = \mathbb{Z}$ and $\mathbb{F} = \mathbb{R}$, then $f : X \to \mathbb{F}$ defined by $f(x) = x + 1$ is not an element in $\mathbb{F}\langle X \rangle$. However, $f(x) = 2$ if $|x| < 10$ and 0 otherwise is an element in $\mathbb{F}\langle X \rangle$.
- **How can we concisely write an element in $\mathbb{F}\langle X \rangle$?**
  - whilst we could simply list the elements in $\mathbb{F}\langle X \rangle$, they are oftentimes represented as a linear combination, known as a **formal linear combination of elements in** X
  - for a function $a \in \mathbb{F}\langle X \rangle$, we can write it as:

$$\sum_{x \in X} a(x)x$$

  - for example, if $f \in \mathbb{Q}\langle X \rangle$, and $X = \{$😂, 🤑, 🥶$\}$, such that:
    - $f($😂$) = \frac{17}{3}$
    - $f($🤑$) = -4$
    - $f($🥶$) = \frac{22}{7}$

    we could summarise this using the linear combination:

$$\frac{17}{3}\text{😂} - 4\text{🤑} + \frac{22}{7}\text{🥶}$$

  - notice, whilst we might not be able to explicitly sum elements in X, adding elements in $\mathbb{F}\langle X \rangle$ is possible, since these are just elements of a field

7.8 Theorem: Variant of the Linear Combination of Basis Elements

Let $\mathbb{F}$ be a field, V an F-vector space and $(\underline{v}_i)_{i \in I}$ a family of vectors from the vector space V. The following are equivalent:

1. *The family $(\underline{v}_i)_{i \in I}$ is a* ***basis*** *for V*
2. *For each vector $\underline{v} \in V$ there is precisely* ***one*** *family $(a_i)_{i \in I}$ of elements of our field $\mathbb{F}$, almost all of which are zero and such that:*

$$\underline{v} = \sum_{i \in I} a_i \underline{v}_i$$

We require almost all to be zero to avoid an infinite sum. [Theorem 1.5.16]

8 Dimension of a Vector Space

8.1 Theorem: The Fundamental Estimate of Linear Algebra

No ***linearly independent subset*** *of a given vector space has* ***more elements*** *than a* ***generating set****.*
If V is a ***vector space****, $L \subset V$ is a linearly independent subset, and $E \subseteq V$ is a generating set, then:*

$$|L| \leq |E|$$

We use the convention that an infinite set has $|X| = \infty$, so this is generally useful only for finitely generated sets.
The idea is the "smallest" generating sets will be linearly independent, so any linearly independent set will be of the same size or smaller than any generating set. [Theorem 1.6.1]

Proof. I don't really understand, so check notes □

8.2 Exchange Lemma

The Exchange Lemma is used to prove the **Steinitz Exchange Theorem**.

Let:

- V *be a vector space*
- $M \subset V$ *a linearly independent subset*
- $E \subseteq V$ *a generating set*

By the Fundamental Estimate, $M \subseteq E$*. If* $\underline{w} \in V \setminus M$ *and* $M \cup \{\underline{w}\}$ *is linearly independent, then* $\exists \underline{e} \in E \setminus M$ *such that:*

$$(E \setminus \{\underline{e}\}) \cup \{\underline{w}\}$$

is a ***generating set*** *of* V*.*
What this says is that we can change an element in a generating set for another element in a linearly independent set, and still keep the "generativeness" of a set. [Lemma 1.6.3]

Proof. Consider $\underline{w} \in V \setminus M$ such that $M \cup \{\underline{w}\}$ is linearly independent. Since E is a generating set, pick $\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_n$ with $\forall i \in [1, n], \lambda_i \neq 0$ such that:

$$\underline{w} = \sum_{i=1}^{n} \lambda_i \underline{e}_i$$

Notice, since $M \cup \{\underline{w}\}$ is linearly independent, at least one of the $\underline{e}_i$ must be such that $\underline{e}_i \in E \setminus M$. If all the $\underline{e}_i$ were part of M, since $\underline{w}$ wasn't originally in M, adding $\underline{w}$ to M would make the set $M \cup \{\underline{w}\}$ linearly dependent (since elements in M would be able to generate $\underline{w}$).

Without loss of generality, assume $\underline{e}_1 \in E \setminus M$. Then we can write:

$$\underline{e}_1 = \lambda_1^{-1} \left(\underline{w} - \sum_{i=2}^{n} \lambda_i \underline{e}_i \right)$$

In other words, the set $(E \setminus \{\underline{e}_1\}) \cup \{\underline{w}\}$ is also generating (anything generated using $\underline{e}_1$ can be generated using $\underline{w}$ and $\{\underline{e}_i\}_{i \in [2,n]}$).

$\square$

8.3 Theorem: Steinitz Exchange Theorem

Let:

- *V be a vector space*
- *$L \subset V$ a finite, linearly independent subset*
- *$E \subseteq V$ a generating set*

*Then, there exists an **injection** $\phi : L \to E$, such that:*

$$(E \setminus \phi(L)) \cup L$$

*is also a **generating set** of V.*
*What this says is that we can **swap** elements from a generating set using elements of a linearly independent set, and still maintain a generating set.[Theorem 1.6.2]*

Proof. Repeatedly (inductively) apply the Exchange Lemma, swapping elements on by one. □

8.4 Corollary: Cardinality of Bases

Let V be a finitely generated vector space. Then:

1. *V has a **finite** basis*
2. *V cannot have an infinite basis*
3. *Any 2 bases of V have the same **cardinality** (number of elements)*

[Corollary 1.6.4]

Proof. We prove each one sequentially:

1. This is just (7.5) (the existence of a finite basis)
2. Say V has an infinite basis E. It also has a finite basis, say of size r. Pick a subset of E with $r + 1$ elements. Then, this subset must be linearly independent. However, this violates the Fundamental Estimate of Linear Algebra, since we are saying that a linearly independent subset exists which has a greater cardinality than a basis.
3. Consider 2 bases, B_1, B_2. By the FELA, since B_2 is a generating set and B_1 is linearly independent, then $|B_2| \geq |B_1|$. By the FELA, since B_1 is a generating set and B_2 is linearly independent, then $|B_2| \leq |B_1|$. In other words:
$$|B_2| = |B_1|$$

□

8.5 Defining the Dimension of a Vector Space

- **What is the dimension of a vector space?**
  - the dimension of a vector space V (called $dimV$) is the **cardinality** of any of its bases
  - use $dim_{\mathbb{F}}V$ to denote the dimension of an F-vector space
- **What is an infinitely dimensional vector space?**
  - a vector space which is not finitely generated

8.5.1 Examples

- the empty set is the basis for the 0-vector space, so its dimension is 0
- the dimension of $\mathbb{F}^n$ is n, since the standard basis (using $\underline{e}_1, \dots, \underline{e}_n$) is composed of n vectors

8.6 Corollary: Cardinality Criterion for Bases

*Let V be a **finitely generated** vector space. Then:*

1. - *each **linearly independent** subset $L \subset V$ has **at most** $\dim V$ elements*
   - *if $|L| = dimV$, then L is a **basis***
2. - *each **generating set** $E \subseteq V$ has **at least** $dimV$ elements*
   - *if $|E| = dimV$, then E is a **basis***

[Corollary 1.6.7]

Proof. We know, using the Fundamental Estimate, that if:

- L is a linearly independent subset
- B is a basis
- E is a generating set

then:

$$|L| \leq |B| \leq |E|$$

If $|L| = |B|$, then L must be a maximal linearly independent subset (since no other linearly independent subset has a greater cardinality than it), and so, a basis.

If $|E| = |B|$, then E must be a minimal generating set (since no other generating set has a smaller cardinality than it), and so, a basis.

□

8.7 Corollary: Dimension Estimate for Vector Subspaces

*A **proper vector subspace** of a finite dimensional vector space has itself a strictly smaller dimension. [Corollary 1.6.8]*

8.8 Remark: Dimension of Subspace vs Dimension of Space

> *If $U \subseteq V$ is a subspace of the vector space V, then $dimU \leq dimV$. Moreover, if $dimU = dimV < \infty$, we must have $U = V$. [Remark 1.6.9]*

Proof. Proof (I think) has mistakes/worded weirdly, so check notes. □

8.8.1 Exercises

1. **Show that each one dimensional vector space has exactly two vector subspaces.**

   Let V be a one dimensional vector space. Without loss of generality, say it is $\{1\}$. By Remark 1.6.9, if U is a subspaces, we must have $dimU \leq 1$. Since V only has 2 subsets ($\emptyset$ and V), these must be the only possible subspaces.

8.9 Joining Vector Subspaces

- **In what sense can we join vector subspaces?**
  - if V is a vector space with subspaces U, W, we can define the new subspace $U + W$ given by:

$$span(U \cup W) = \{\underline{v} | \exists \underline{u} \in U, \underline{w} \in W, \underline{v} = \underline{u} + \underline{w}\}$$

  - for example, if $V = \mathbb{R}^2$, U and W can be the subspaces generated by two lines; $U + W$ is the set of all linear combinations of elements produced by combining lines in U and W

8.10 Theorem: The Dimension Theorem

> *Let V be a vector space with subspaces $U, W \subseteq V$. Then:*
>
> $$dim(U + W) + dim(U \cap W) = dimU + dimW$$
>
> *[Theorem 1.6.10]*

Proof. Let E be a basis for $U \cap W$:

$$E = \{\underline{e}_1, \ldots, \underline{e}_r\}$$

Notice, E will be a linearly independent subset of both U and W by construction, so in particular, we can add elements to it from both sets to generate bases:

$$E_U = \{\underline{e}_1, \ldots, \underline{e}_r\} \cup \{\underline{u}_1, \ldots, \underline{u}_s\}$$

$$E_W = \{\underline{e}_1, \ldots, \underline{e}_r\} \cup \{\underline{w}_1, \ldots, \underline{w}_k\}$$

Hence, we have that:

- $dim(U \cap W) = r$
- $dimU = r + s$

- $dimW = r + k$

We want to show that:

$$dim(U + W) = dimU + dimW - dim(U \cap W) = r + s + k$$

To do this, we claim that $E_U \cup E_W$ is a basis for $U + W$. We need to check 2 things: whether this set generates all elements in $U + W$, and whether it is linearly independent.

Let $\underline{v} \in U + W$. By definition, it follows that $\exists \underline{u} \in U, \exists \underline{w} \in W : \underline{v} = \underline{u} + \underline{w}$. But then it trivially follows that $\underline{v} \in span(E_U \cup E_W)$, as required.

Now, consider $a_i, b_i, c_i \in \mathbb{F}$, and consider:

$$\sum_{i=1}^{r} a_i \underline{e}_i + \sum_{i=1}^{s} b_i \underline{u}_i + \sum_{i=1}^{k} c_i \underline{w}_i = \underline{0}$$

If we rearrange:

$$\sum_{i=1}^{r} a_i \underline{e}_i + \sum_{i=1}^{s} b_i \underline{u}_i = -\sum_{i=1}^{k} c_i \underline{w}_i$$

Notice, $-\sum_{i=1}^{k} c_i \underline{w}_i \in W$ (since each $\underline{w}_i \in W$, and W is a subspace). Moreover, $\sum_{i=1}^{r} a_i \underline{e}_i + \sum_{i=1}^{s} b_i \underline{u}_i \in U$, since the $E_U = \{\underline{e}_1, \ldots, \underline{e}_r\} \cup \{\underline{u}_1, \ldots, \underline{u}_s\}$.

This then implies that $-\sum_{i=1}^{k} c_i \underline{w}_i \in U \cap W$. But notice, since all the $\underline{w}_i$ lie entirely in W, and outside of E (which is the basis generating $U \cap W$), this is not possible, unless each $c_i = 0$. But then this means that:

$$\sum_{i=1}^{r} a_i \underline{e}_i + \sum_{i=1}^{s} b_i \underline{u}_i = \underline{0}$$

But recall, this is a linear combination of elements in the basis E_U. Since they are linearly independent, this is only possible if $a_i = b_i = 0$. Hence, if

$$\sum_{i=1}^{r} a_i \underline{e}_i + \sum_{i=1}^{s} b_i \underline{u}_i + \sum_{i=1}^{k} c_i \underline{w}_i = \underline{0}$$

then $a_i = b_i = c_i = 0$, and so, the set $E_U \cup E_W$ must be linearly independent. Hence, $E_U \cup E_W$ is a basis for $U + W$. Moreover, it is easy to check that:

$$|E_U \cup E_W| = r + s + k$$

so $dim(U + W) = r + s + k$, as required.

$\square$

8.10.1 Examples

We can verify this theorem. For example, consider $V = \mathbb{R}^3$, and lets U, W be two non-parallel planes. These intersect in a line, so:

- $dimU = 2$
- $dimW = 2$
- $dim(U + W) = 3$ (their combination spans the whole space)
- $dim(U \cap W) = 1$ (a line is 1 dimensional)

and indeed:

$$dimU + dimW = 2 + 2 = 4$$
$$dim(U + W) + dim(U \cap W) = 3 + 1 = 4$$

8.10.2 Exercises (TODO)

1. **Given F-Vector Spaces $V_1, V_2, \dots, V_n$, show that:**

$$dim(V_1 \oplus V_2 \oplus \dots \oplus V_n) = dimV_1 + \dots + dimV_n$$

2. **Show that for some vector space V:**

$$dim_{\mathbb{R}}V = 2dim_{\mathbb{C}}V$$

Let A be a basis for $\mathbb{C}$:

$$A = \{\underline{v}_1, \dots, \underline{v}_n\}$$

Now consider a set:

$$B = \{\underline{v}_1, i\underline{v}_1, \dots, \underline{v}_n, i\underline{v}_n\}$$

We claim that B is a basis for $\mathbb{R}$. To see why, B is linearly independent, since:

$$\sum_{j=1}^{n} \alpha_j(\underline{v}_j + i\underline{v}_j) = 0 \implies (1+i)\sum_{j=1}^{n} \alpha_j \underline{v}_j = 0$$

Since $i + 1 \neq 0$, this is only possible if:

$$\sum_{j=1}^{n} \alpha_j \underline{v}_j = 0$$

But A is a basis, so this is true only if $\alpha_j = 0$, so it follows that the set B is linearly independent.

Moreover, A generates $\mathbb{R}$. To see why, if $v \in V$, then $\exists \lambda_i = a_1 + ib_i \in \mathbb{C}$ such that:

$$v = \sum_{i=1}^{n} \lambda_i v_i = \sum_{i=1}^{n} a_i v_i + \sum_{i=1}^{n} b_i(iv_i)$$

Hence:

$$dim_{\mathbb{R}}V = 2dim_{\mathbb{C}}V$$

9 Workshop

1. **True or False: It is not possible to find a basis $\{p_1, p_2, p_3, p_4\}$ of the vector space $\mathbb{R}[x]_{<4}$ such that none of the polynomials p_i has degree 1.**

We are considering the vector space of polynomials of degree at most 3. In other words, a "standard basis" is the 4 element set:

$$\{1, x, x^2, x^3\}$$

This statement is **False**, and the set:

$$\{1, x^2, x^2 - x, x^3\}$$

is a counterexample.

Clearly, each element is linearly independent:

$$\lambda_0 + \lambda_1 x^2 + \lambda_2(x^2 - x) + \lambda_3 x^3 = 0 \implies \lambda_0 - \lambda_2 x + (\lambda_1 + \lambda_2)x^2 + \lambda_3 x^3 = 0$$

and looking at powers, this is 0 only when each λ_i is 0.

Moreover, each element of the basis $\{1, x, x^2, x^3\}$ can be constructed with elements from the basis $\{1, x^2, x^2 - x, x^3\}$. The only element in which they don't coincide is the linear term, but:

$$x^2 - (x^2 - x) = x$$

Thus, $\{1, x^2, x^2 - x, x^3\}$ spans the same space as the standard set. Since it is also linearly independent, it is a basis.

2. (a) **Let V be the vector space of real functions.**

   i. **Is the set $\{\cos(x), \sin(x), e^x\}$ linearly independent?**

   Yes. Assume that they are linearly dependent. Then, $\forall x \in \mathbb{R}$ we have $a, b, c \in \mathbb{R}$, not all of which non-zero, such that:

$$a\cos(x) + b\sin(x) + ce^x = 0$$

   Evaluating at $x = 0$:

$$a + c = 0 \implies a = -c$$

   Evaluating at $x = \pi$:

$$-a + ce^\pi = 0 \implies a = ce^\pi$$

   In other words, if we assume that $c \neq 0$ we require that:

$$-c = ce^\pi \iff e^\pi = -1$$

   But the exponential is always positive, so this is impossible. Hence, the only possibility is that $c = 0$, so in particular $a = 0$.
   Thus, $\forall x \in \mathbb{R}$:

$$a\cos(x) + b\sin(x) + ce^x = 0 \implies b\sin(x) = 0$$

   with $b \neq 0$. But this is clearly false (for example, if $x = \frac{\pi}{2}$, we would get $b = 0$).
   Hence, our initial assumption was false, and $a = b = c = 0$, so the set is linearly independent.

   ii. **Is the set $\{\cos^2(x), \sin^2(x), 1\}$ linearly independent?**

   No, since $\forall x \in \mathbb{R}$:

$$\cos^2(x) + \sin^2(x) = 1`$$

(b) **Let $S = \{\underline{u}_1, \ldots, \underline{u}_n\}$ and $T = \{\underline{u}_1, \ldots, \underline{u}_n, \underline{u}_{n+1}\}$.**

   i. **T/F: If S is LiD, then T is LiD**

   This is **false**. If we set $\underline{u}_{n+1} = \underline{0}$, then even if S is LiD, T will be LD, since it contains the 0 vector

   ii. **T/F: If T is LiD, then S is LiD**

   This is **true**. Consider:

$$\sum_{i=1}^{n} \lambda_i \underline{u}_i = 0$$

   We can rewrite this as:

$$0\underline{u}_{n+1} + \sum_{i=1}^{n} \lambda_i \underline{u}_i = 0$$

   Notice, this is in terms of the linearly independent basis T, so $\forall i \in [1, n+1], \lambda_i = 0$, which implies that S is linearly dependent.

(c) **Consider:**

$$S = \left\{ \begin{pmatrix} 1 \\ 2 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 1 \\ 1 \end{pmatrix} \right\} \subset F^4$$

Is S LiD?

We can't know: this depends on the field F.

For example, if $F = \mathbb{R}$, then consider $a, b, c \in \mathbb{R}$. We need to satisfy:

$$\begin{aligned}
&a + b + 2c = 0 \\
&a + c = 0 \\
&b + c = 0 \\
&2a + 2b + c =
\end{aligned}$$

The above middle 2 equations imply that $a = -c = b$, but then the last equation would imply that $c = -4a = -4b$. This is only true if $a = b = c = 0$, so S is linearly independent.

If $F = \mathbb{F}_3$, then for example $a = b = 1$ and $c = 2$ gives a solution to the system, so the vector will be linearly dependent.

(d) **Consider $\underline{v}_1, \underline{v}_2, \underline{v}_3, \underline{v}_4 \in V$ and suppose that:**

$$\langle \underline{v}_1, \underline{v}_2, \underline{v}_3, \underline{v}_4 \rangle = \langle \underline{v}_1, \underline{v}_2, \underline{v}_3 \rangle$$

Which of the following are *necessarily* true?

i. $\underline{v}_4 = \underline{0}$
We could have $\underline{v}_4$ as a non-zero element of $\langle \underline{v}_1, \underline{v}_2, \underline{v}_3 \rangle$ and the result would follow.

ii. $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$ **is a LiD subset of** V
We could have that $\underline{v}_2$ is a scalar multiple of $\underline{v}_2$, and the result would follow.

iii. $\underline{v}_4 \in \langle \underline{v}_1, \underline{v}_2, \underline{v}_3 \rangle$
This is true; it is the only possibility which would allow for $\langle \underline{v}_1, \underline{v}_2, \underline{v}_3, \underline{v}_4 \rangle = \langle \underline{v}_1, \underline{v}_2, \underline{v}_3 \rangle$

iv. $\{\underline{v}_1, \underline{v}_2, \underline{v}_3\}$ **is a LD subset of** V
This is false. For example, they could be a standard basis of $\mathbb{R}^3$, with $\underline{v}_4$ as an element of $\mathbb{R}^3$.

(e) **Consider:**

$$S = \left\{ \begin{pmatrix} 1 \\ 2 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 1 \\ 1 \end{pmatrix} \right\} \subset F^4$$

where $F = \mathbb{F}_3$, the field of 3 elements. What is the dimension of the space spanned by S?

Above we showed that over $\mathbb{F}_3$, these vectors are linearly dependent. The set:

$$\left\{ \begin{pmatrix} 1 \\ 2 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix} \right\}$$

is linearly independent however, and spans a 2-dimensional space.

3. **In this question we begin by thinking of the field $F = \mathbb{F}_3$.**

(a) i. **Write out all the elements of the vector space $\mathbb{F}_3^2$.**
There are 9 elements:

$$\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix} \right\}$$

ii. **Find all the one-dimensional subspaces of $\mathbb{F}_3^2$. How many different bases does each of these subspaces have?**

There are 4 one-dimensional subspaces, each of which has 2 possible basis vectors:

$$\left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} \;\middle|\; a \in \mathbb{F}_3 \right\}$$

$$\left\{ \begin{pmatrix} 0 \\ a \end{pmatrix} \;\middle|\; a \in \mathbb{F}_3 \right\}$$

$$\left\{ \begin{pmatrix} a \\ a \end{pmatrix} \;\middle|\; a \in \mathbb{F}_3 \right\}$$

$$\left\{ \begin{pmatrix} a \\ 2a \end{pmatrix} \;\middle|\; a \in \mathbb{F}_3 \right\}$$

iii. **Given a non-zero vector $\underline{v}_1 \in \mathbb{F}_3^2$, how many vector $\underline{v}_2 \in \mathbb{F}_3^2$ are there such that $\{\underline{v}_1, \underline{v}_2\}$ is a linearly independent family?**

To construct a linearly independent family, $\underline{v}_1$ would need to be associated with a non-zero vector outside of its span. This leaves 6 possibilities (there are 9 vectors, and we can't have the 0 vector, $\underline{v}_1$ or $2\underline{v}_2$).

iv. **Count the number of indexed bases of $\mathbb{F}_3^2$. Forgetting indexing, how many bases are there?**

There are 8 possible $\underline{v}_1$ (can't have the 0 vector). Each $\underline{v}_1$ can be associated with 6 potential $\underline{v}_2$, so there are 48 possible ordered bases.

If we remove ordering, notice that $\{\underline{v}_1, \underline{v}_2\} = \{\underline{v}_2, \underline{v}_1\}$, so the indexed basis overcounts a basis twice. Hence, there are 24 unordered bases.

(b) **Now let V be an arbitrary two-dimensional vector space over $\mathbb{F}_3$. How many indexed bases are there for V?**

Notice, any vector space of dimension n over a field F is isomorphic to F^n, so V will be isomorphic to $\mathbb{F}_3^2$. Thus, V has the same number of bases as $\mathbb{F}_3^2$.

(c) i. **Let $n \in \mathbb{N}$ with $n \geq 2$. How many non-zero vectors are there in $\mathbb{F}_3^n$?**

$\mathbb{F}_3^n$ has 3^n total elements, one of which is the 0 vector, so there are $3^n - 1$ non-zero vectors.

ii. **How many one-dimensional subspaces of $\mathbb{F}_3^n$ are there? Check it agrees with your answer above with $n = 2$.**

For each non-zero vector $\underline{v}_1$, we have that $\langle \underline{v}_1 \rangle = \langle 2\underline{v}_2 \rangle$. There are $3^n - 1$ non-zero vectors, so there are:

$$\frac{3^n - 1}{2}$$

one-dimensional vector spaces (with $n = 2$, we get 4, as expected)

iii. **How many two-dimensional subspaces of $\mathbb{F}_3^n$ are there? Check you get the correct answer when $n = 2$.**

Such a space is the span of $\{\underline{v}_1, \underline{v}_2\}$. Picking a non-zero $\underline{v}_1$ has $3^n - 1$ choices. For a basis, we require $\underline{v}_2$ to not be in the span of $\underline{v}_2$, for which we have $3^n - 3$ possibilities. Thus, there are $(3^n - 1)(3^n - 3)$ ordered bases for a 2-dimensional subspace. If we don't consider order, recall we showed that there $\mathbb{F}_3^2$ (and so any 2-dimensional space over $\mathbb{F}_3$ has 48 unordered bases, so we have overcounted. The unordered number of basis is thus:

$$\frac{(3^n - 1)(3^n - 3)}{48}$$

If $n = 2$, we get 1, as expected (since the only 2-dimensional subspace of $\mathbb{F}_3^2$ is the space itself)

(d) **Now, consider $\mathbb{R}$ to be the ground field. Can the questions above be answered?**
No, since $\mathbb{R}$ is infinite dimensional.

4. **Let U, W be 6-dimensional subspaces of $\mathbb{R}^{11}$. Show that $U \cap W \neq \{\ 0\}$.**

Recall the Dimension Theorem:

$$dim(U + W) + dim(U \cap W) = dim(U) + dim(W)$$

Then, we have that:

$$dim(U + W) + dim(U \cap W) = 12 \implies dim(U \cap W) = 12 - dim(U + W)$$

But now, $U + W$ is a subspace of $\mathbb{R}^{11}$, so $dim(U + W) \leq 11$ which means that:

$$dim(U \cap W) = 12 - dim(U + W) \geq 12 - 11 = 1$$

Thus, we must have that $dim(U \cap W) \geq 1$, so in particular, $U \cap W$ can't be empty.