1 Fields

Fields are an abstract structure that describes sets of "numbers" and their operations.

Definition 1.1 (Fields)
A set $\mathcal{F}$ together with two binary operations

- $+ : \mathcal{F} \times \mathcal{F} \to \mathcal{F}$ (Addition)
- $\cdot : \mathcal{F} \times \mathcal{F} \to \mathcal{F}$ (Multiplication)

$\forall x, y, z \in \mathcal{F}$

- $x + (y + z) = (x + y) + z$ (Associativity)
- $x(yz) = (xy)z$ (Associativity)
- $x + y = y + x$ (Commutatitivity)
- $xy = yx$ (Commutatitivity)
- $\exists 0 \in \mathcal{F}$ such that $x + 0 = x \; \forall x \in \mathcal{F}$ (Neutral additive element)
- $\exists 1 \in \mathcal{F}$ such that $x \cdot 1 = x \; \forall x \in \mathcal{F}$ (Neutral scalar multiplication element)
- $\forall x \in \mathcal{F} \; \exists - x \in \mathcal{F} \quad x + (-x) = 0$ (Additive Inverse)
- $\forall y \in \mathcal{F} \backslash \{0\} \exists y^{-1} \exists \mathcal{F} \quad yy^{-1} = 1$ (Multiplicative inverse)
- $x(y + z) = xy + xz$ (Distributivity)

Example of fields: Rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$. Another example is the set $\mathcal{F} = \{0, 1\}$. The set $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is also an example.

Definition 1.2
For any field $\mathcal{F}$ we denote the set of n-tuples by $\mathcal{F}^n$. We define two important operations on $\mathcal{F}^n$.

- Addition: Given two elements $x = (x_1, \dots, x_n)$ $y = (y_1, \dots, y_n)$ $x + y = (x_1 + y_1, \dots, x_n + y_n)$
- Scalar multiplication: Given an element $\lambda \in \mathcal{F}$ and a n-tuple $x \in \mathcal{F}^n$ we define $\lambda x := (\lambda x_1, \dots, \lambda x_n)$

We often write $0 \in \mathcal{F}^n$ for the n-tuple consisting of n zeros.
Let $x \in \mathcal{F}^n$ we define $-x := (-x_1, \dots, -x_n)$ and we see that $x + (-x) = 0$.

For any $x \in \mathcal{F}^n$ we have $0 + x = x$

2 Vector Spaces

Definition 2.1 (Vector Space)
Let V be a set and $\mathcal{F}$ be a field.

Let $+ : V \times V \to V$ and $\cdot : \mathcal{F} \times V \to V$ be two binary operations. We say V is a vector space (with respect to these operations) over $\mathcal{F}$, or an $\mathcal{F}$-vector space (VS) if

- Addition is commutative: $\forall u, v \in V \quad u + v = v + u$.
- Addition is associative: $\forall u, v, w \in V \quad u + (v + w) = (u + v) + w$.
- Multiplication is associative: $\forall \lambda, \mu \in \mathcal{F} \forall v \in V \quad (\lambda\mu)v = \lambda(\mu v)$.
- Neutral additive: $\exists 0 \in V$ such that $\forall v \in V \quad 0 + v = v$.
- Inverse addition: $\forall v \in V \exists - v \in V \quad v + (-v) = 0$.
- Neutral scalar multiplication: $1 \in \mathcal{F}$ it holds that $1 \cdot v = v \quad v \in V$.
- Distributivity: $\forall u, v \in V \ \forall \lambda\mu \in \mathcal{F} \quad \lambda(u + v) = \lambda u + \lambda v$ and $(\lambda + \mu)v = \lambda v + \mu v$.

Example 2.1
a) $\mathcal{F}^n$ is an $\mathcal{F}$-VS, it holds that $\forall n \in \mathbb{N}$ especially $\mathcal{F}$ is an $\mathcal{F}$-VS.

b) $V = \{0\} \subseteq \mathcal{F}$ is an $\mathcal{F}$-VS.

c) $\mathcal{F}^\infty := \{(x_1, x_2, \dots) : x_i \in \mathcal{F} \ i \in \mathbb{N}\}$, the set of all infinite sequences is an $\mathcal{F}$-VS

d) Let $V := \{f : S \to \mathcal{F}\}$ be the set of functions from a set S into $\mathcal{F}$ then V is an $\mathcal{F}$-VS with $f, g \in V$ for which $(f + g)(s) := f(s) + g(s) \forall s \in S$. Similiarly $\forall \lambda \in \mathcal{F} \quad (\lambda f)(s) = \lambda(f(s))$. Sometimes you will see this notation:

$$V = \mathcal{F}^S$$

Example. $\mathbb{R}^{[0,1]}$.

Theorem 2.1
Let V be an $\mathcal{F}$-VS. Then the additive neutral element is unique.

Proof 2.1
Suppose there is another additive neutral element: 0 and $0'$ are both neutral. Then

$$\begin{aligned} 0 &= 0 + 0' \text{ since } 0' \text{ is neutral} \\ &= 0' \text{ since } 0 \text{ is neutral} \end{aligned}$$

Hence $0 = 0'$ and there is an unique neutral.

∎

Theorem 2.2
Let V be an $\mathcal{F}$-VS. Then every element in V has a unique additive inverse.

Proof 2.2
Let $v \in V$ and suppose w and w' are both additive inverse for v.

$$w' = 0 + w' = (w + v) + w' = w + (v + w') = w + 0 = w$$

We will from now on decide the unique inverse of v be $-v$ and write $w + (-v) := w - v$.

Theorem 2.3
Let V be an $\mathcal{F}$-VS. Then $\forall v \in V$

$$0 \in \mathcal{F} \quad v = 0 \in V$$

Proof 2.3
We see that

$$0 \cdot v = (0 + 0)v = 0v + 0v$$

Add $-0v$ on both sides

$$0 = 0v.$$

$\blacksquare$

Theorem 2.4
Let V be an $\mathcal{F}$-VS. Then $\forall \lambda \in \mathcal{F}$

$$\lambda \cdot 0 = 0.$$

Proof 2.4

$$\lambda 0 = \lambda(0 + 0) = \lambda 0 + \lambda 0$$

Add $-\lambda 0$ on both sides

$$0 = \lambda 0.$$

$\blacksquare$

Theorem 2.5
Let V be an $\mathcal{F}$-VS and $-1 \in \mathcal{F}$ is the additive inverse of the multiplicative neutral in $\mathcal{F}$. Then

$$(-1)v = -v \quad \forall v \in V$$

Proof 2.5

$$1 \cdot v + (-1)v = (1-1) \cdot v = 0v = 0$$

by Theorem 2.3.

■

For any VS V the subset $\{0\}$ is also a VS. We generalise this notion.

Definition 2.2 (Subspaces)
Let V be an $\mathcal{F}$-VS then a subset $U \subseteq V$ is called a subspace if U is also an $\mathcal{F}$-VS with respect to the same operations.

Theorem 2.6 (Proposition)
A subset $U \subseteq V$ of an $\mathcal{F}$-VS V is a subspace iff (=if and only if)

- $0 \in U$
- $\forall u, w \in U \quad u + w \in U$
- $\forall \lambda \in \mathcal{F} \quad \forall u \in U \quad \lambda u \in U$

Proof 2.6
$\Rightarrow$ If U is a VS then all these conditions hold.

$\Leftarrow$ Condition 1 implies neutral additive of VS.

By condition 3 we know that $(-1)u \in U$, $(-1)u = -u$ and thereby implies the additive inverse of VS.

■

Example 2.2
1) For any VS V, $\{0\}$ and V itself are subspaces.

2) The set of all polynomials with coefficients in some field $\mathcal{F}$ is a VS, called $\mathcal{F}[x]$. For every $0 \leq d \in \mathbb{N}_0$ the set of polynomials of degree at most d is a subspace.

3) We have seen that $\mathbb{R}^{[0,1]}$ is a $\mathbb{R}$-VS. The sets of continuous or differentiable functions form subspaces.

4) We can classify all subspaces of $\mathbb{R}^3$ in a hierarchy: $\mathbb{R}^3 >$ planes containing the origin $>$ lines going through the origin $> \{0\}$.

Definition 2.3
Let $U_1, U_2, \dots, U_m$ be subspaces of a VS V. Then we define their sum.

$$U_1 + \cdots + U_m := \{u_1 + \cdots + u_m : u_i \in U_i\}$$

Theorem 2.7 (Proposition)
Finite sums of subspaces are subspaces again.

Proof 2.7
We only need to show this for two subspaces.

Let $U_1, U_2 \subseteq V$ be subspaces. Then since $0 \in U_1$ and $0 \in U_2 \Rightarrow 0 + 0 = 0 \in U_1 + U_2$.
Let $u_1 + u_2, u_1' + u_2' \in U_1 + U_2$ then $u_1 + u_2 + u_1' + u_2' = (u_1 + u_1') + (u_2 + u_2') \in U_1 + U_2$
Let $\lambda \in \mathcal{F}$ then

$$\lambda(u_1 + u_2) = \lambda u_1 + \lambda u_2 \in U_1 + U_2.$$

■

Theorem 2.8 (Proposition)
Let $U_1, U_2 \subseteq V$ be subspaces, then $U_1 + U_2$ is the smallest subspace of V containing both.

Proof 2.8
We see that $U_1 \subseteq U_1 + U_2$ because $\forall u_1 \in U_1 \quad u_1 + 0 = u_1 \in U_1 + U_2$, the same applies to U_2.

Assume there exists $W \subseteq U_1 + U_2$ that contains U_1 and U_2. Then there must exist an element $u_1 + u_2 \notin W$. But $u_1 \in W$ and $u_2 \in W \rightarrow W$ is not a subspace.

EX: Functions and reals can be split into subspaces of even and odd reals.

EX: L_1, L_2 lies in $\mathbb{R}^n$ $L_1 + L_2 = \begin{cases} P \text{ plane} \\ L_1 \text{ if } L_1 = L_2 \end{cases}$

EX: P is a plane in $\mathbb{R}^3$ and L is a line in $\mathbb{R}^3$:

$$P + L = \begin{cases} \mathbb{R}^3 \text{ if } L \subsetneq P \\ P \text{ if } L \subseteq P \end{cases}$$

Definition 2.4 (Direct Sum)
Let $U_1, \ldots, U_m \subseteq V$ be subspaces. Then their sum is called a direct sum if $U_1 + \cdots + U_m$ has a unique representation as a sum $u_1 + \cdots + u_m$. We then write $U_1 \oplus \cdots \oplus U_m$ for this sum.

Theorem 2.9 (Proposition)
The sum $U_1 + \cdots + U_m$ is direct iff there is a unique way to write 0 as a sum $u_1 + \cdots + u_m$.

Proof 2.9
$\Rightarrow$ check

$\Leftarrow$

If the sum is not direct then there exists an element that has two different representations

$$u_1 + \cdots + u_m = u_1' + \cdots + u_m'$$

where not all $u_i = u_i'$. Then

$$(u_1 - u_1') + (u_2 - u_2') + \cdots + (u_m - u_m') = 0$$

and at least one different $u_i - u_i' \neq 0$.

■

Theorem 2.10 (Lemma)
$U + W$ is direct iff

$$U \cap W = \{0\}$$

Proof 2.10
$\Rightarrow$: Let $v \in U \cap W$ and $v \neq 0$ then

$$0 + 0 = 0 = v + (-v)$$

and hence the sum is not direct.

$\Leftarrow$: $0 = u + w \Rightarrow -u \in U - w \in W \Rightarrow u = w = 0$

3 Bases and Dimension

A list is an n-tuple.

Definition 3.1 (2.3 and 2.5)
Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be a list of vectors in an $\mathcal{F}$-VS. Then for any $\lambda_i \in \mathcal{F}$ we call $\lambda_1\mathbf{v}_1 + \cdots + \lambda_m\mathbf{v}_m$ a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_m$. (Note that λ_i can be zero)

The set of all linear combinations is called the span of $\mathbf{v}_1, \ldots, \mathbf{v}_m$ and denoted $\operatorname{span}(\mathbf{v}_1, \ldots, \mathbf{v}_m)$. For consistency we let $\operatorname{span}() = \{0\}$.

Theorem 3.1 (Proposition 2.7)
Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a list of vectors. Then $\operatorname{span}(\mathbf{v}_i)$ is a subspace and it is the smallest subspace containing all $\mathbf{v}_i$.

Proof 3.1
We show that span is a subspace.

1. $0 \in \operatorname{span}(\mathbf{v}_i)$, just let $\lambda_i = 0 \ \forall\, i$
2. $\sum_{i=1}^m \lambda_i\mathbf{v}_i + \sum \mu_i\mathbf{v}_i = \sum(\lambda_i + \mu_i)\mathbf{v}_i \in \operatorname{span}(\mathbf{v}_i)$
3. $\sum \lambda_i\mathbf{v}_i = \sum(\mu\lambda_i)\mathbf{v}_i \in \operatorname{span}(\mathbf{v}_i)$

$$\mathbf{v}_i = 0\mathbf{v}_1 + 0\mathbf{v}_2 + \cdots + 1\mathbf{v}_i + \cdots + 0\mathbf{v}_m \in \operatorname{span}(\mathbf{v}_i)$$

Assume $W \subseteq \operatorname{span}(\mathbf{v}_i)$ such that $\mathbf{v}_i \in W \ \forall\, i$. Then $\exists x \in \operatorname{span}(\mathbf{v}_i) \setminus W \quad x = \sum \lambda_i\mathbf{v}_i \in W$ which is a contradiction.

■

Definition 3.2 (2.17)
We say a list $\mathbf{v}_i$ of vectors is <u>linearly independent</u> if

$$0 = \lambda_1\mathbf{v}_1 + \cdots + \lambda_m\mathbf{v}_m \Rightarrow \forall\, \lambda_i = 0.$$

Theorem 3.2 (Lemma 20)
A list $\mathbf{v}_i$ is linearly independent iff every vector in $\operatorname{span}(\mathbf{v}_i)$ has a unique representation as a linear combination.

Proof 3.2
$\Rightarrow$(direct proof) Assume that $\sum \lambda_i \mathbf{v}_i = \sum \mu_i \mathbf{v}_i$ then

$$\sum(\lambda_i - \mu_i)\mathbf{v}_i = 0 \Rightarrow \lambda_i - \mu_i = 0 \Rightarrow \lambda_i = \mu_i$$

because $\mathbf{v}_i$ is linear independent.

■

Remark:

1. If a list $\mathbf{v}_i$ is linearly dependant then there exist λ_i not all zero, such that $\sum \lambda_i \mathbf{v}_i = 0$
2. A single $\mathbf{v}$ is linearly dependant iff $\mathbf{v} = 0$. Because then $1\mathbf{v} = 1 \cdot 0 = 0$, note that $1 \in \mathcal{F}, v \in V, 0 \in V$.

Definition 3.3 (2.27)
Let V be an $\mathcal{F}$-VS. Then

1. A list $\mathbf{v}_i$ such that $V = \text{span}(\mathbf{v}_i)$ is called a generating set (spanning set). If the list is finite (always assumed here) then we say V is finitely generated.
2. A list $\mathbf{v}_i$ is called a basis for V if it is a linearly independent generating set.

Example 3.1

1. $$\lambda_1 \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \lambda_1 = 0 = \lambda_2$$
2. Let $V = \mathcal{F}^n$ and denote by e_i the vector with a one in the i-th coordinate and zero elsewhere.
3. Let $V = \mathbb{R}[x]^{\leq m} (= \mathcal{P}_m(\mathbb{R}))$ then $1, x, x^2, \ldots, x^m$ are a basis with $m + 1$ elements.

The $e_1, \ldots e_n$ are the so-called standard basis vectors.

Theorem 3.3 (Lemma)
Let $\mathbf{v}_1, \ldots, \mathbf{v}_m$ be linearly dependent. Then $\exists j$ such that $\mathbf{v}_j \in \text{span}(\mathbf{v}_1, \ldots, \mathbf{v}_{j-1})$ and $\mathbf{v}_1, \ldots, \mathbf{v}_m$ without $\mathbf{v}_j$ spans the same space.

Proof 3.3
Since $\mathbf{v}_i$ is linearly dependent $\exists \lambda_i \in \mathcal{F}$, not all zero such that $\sum_{i=1}^m \lambda_i \mathbf{v}_i = 0$. Let j be the max index such that $\lambda_j \neq 0$. Then

$$\sum_{i=1}^{j-1} -\frac{\lambda_i}{\lambda_j}\mathbf{v}_i = \mathbf{v}_j \Rightarrow \mathbf{v}_j \in \operatorname{span}(\mathbf{v}_1, \dots, \mathbf{v}_{j-1}). \tag{1}$$

Let $\sum_{i=1}^m \mu_i \mathbf{v}_i \in \operatorname{span}(\mathbf{v}_i)$. Substitute equation (1) for $\mathbf{v}_j$

$$\begin{aligned}\mu_1\mathbf{v}_1 + \dots + \mu_j\mathbf{v}_j + \dots + \mu_m\mathbf{v}_m &= \mu_1\mathbf{v}_1 + \dots + \mu_j\left(\sum_{i=1}^{j-1} -\frac{\lambda_i}{\lambda_j}\mathbf{v}_i\right) + \dots + \mu_m\mathbf{v}_m \\ &= \left(\mu_1 - \frac{\mu_j\lambda_1}{\lambda_j}\right)\mathbf{v}_1 + \left(\mu_2 - \frac{\mu_j\lambda_2}{\lambda_j}\right)\mathbf{v}_2 + \dots + \left(\mu_{j-1} - \frac{\mu_j\lambda_{j-1}}{\lambda_j}\right)\mathbf{v}_{j-1} + \mu_{j+}\end{aligned}$$

Theorem 3.4 (Steinitz)
Let V be a finitely generated VS. Then the length of any linear independent list is smaller or equal to the length of any generating list.

Proof 3.4
Let $\mathbf{u}_1, \dots, \mathbf{u}_m$ be linearly independent and $\mathbf{w}_1, \dots, \mathbf{w}_n$ a generating set.

$$\operatorname{span}(\mathbf{w}_j) = V, \mathbf{u}_1 \in V.$$

Then $(\mathbf{u}_1\mathbf{w}_1, \dots, \mathbf{u}_1\mathbf{w}_m)$ is linearly dependent. Then for $\sum \lambda_j \mathbf{w}_j = \mathbf{u}_1 \quad wlog \quad \lambda_1 \neq 0 \Rightarrow \frac{1}{\lambda_1}\mathbf{u}_1 - \frac{\lambda_2}{\lambda_1}\mathbf{w}_2 - \frac{\lambda_m}{\lambda_1} = \mathbf{w}_1$ (without loss of generality) point being

$$\operatorname{span}(\mathbf{u}_1, \mathbf{w}_2, \dots, \mathbf{w}_n) = \operatorname{span}(\mathbf{w}_1, \dots, \mathbf{w}_n) = V.$$

The new list $S_1 = (\mathbf{u}_1, \mathbf{w}_2, \dots, \mathbf{w}_n)$ also spans V. Then $(\mathbf{u}_1, \mathbf{u}_2, \mathbf{w}_2, \dots, \mathbf{w}_n)$ and

$$\mathbf{u}_2 = \lambda_1\mathbf{u}_1 + \lambda_2\mathbf{w}_2 + \dots + \lambda_n\mathbf{w}_n$$

assume $\lambda_2 \neq 0$ and thus an element $\mathbf{w}_2$ can be pulled out of the set without loss:

$$\Rightarrow S_2 = (\mathbf{u}_1, \mathbf{u}_2, \mathbf{w}_3, \dots, \mathbf{w}_n)$$

also spans V and we can keep going.

Remark: This shows that no list that is bigger than a generating set can be linearly independent. Also any list that is shorter than a linearly independent list can not generate the whole space.

Theorem 3.5 (Basis)
A list of vectors is a basis for V iff every $\mathbf{v} \in V$ can be uniquely be written as a linear combination.

Proof 3.5
Lemma 20. If you can write every element uniquely then you can write zero uniquely.

Theorem 3.6
Let $\operatorname{span}(\mathbf{v}_1, \ldots, \mathbf{v}_n) = V$. Then there is a subset of $\mathbf{v}_i$ that is a basis.

Proof 3.6
We construct the basis in n-steps.

We add a vector $\mathbf{v}_i$ to our basis if $\mathbf{v}_i \notin \operatorname{span}(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1})$. Let $\mathbf{w}_1, \ldots, \mathbf{w}_m$ be the basis acquired this way. Assume

$$\sum \lambda_i \mathbf{w}_i = 0.$$

Let j be max such that $\lambda_j \neq 0$ then $\sum_{i=1}^{j-1} \lambda_i \mathbf{w}_i = \lambda_j \mathbf{w}_j$, contradiction.

Therefore $\mathbf{w}_i$ is linearly independent and it still spans V.

Theorem 3.7 (Corollary)
Every finitely generated VS has a basis.

Theorem 3.8 (Corollary)
Every linearly independent set can be extended to a basis.

Proof 3.7
Let $(\mathbf{u}_1, \ldots, \mathbf{u}_m)$ be linearly independent and let $(\mathbf{w}_1, \ldots, \mathbf{w}_n)$ be a generated set. Then $(\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{w}_1, \ldots, \mathbf{w}_n)$ is a geenerating set. Use Theorem 3.6 to acquire a basis.

Theorem 3.9 (2.35)
Every basis of a finitely generated VS has the same length.

Proof 3.8
Let B_1 and B_2 be two bases. Since B_1 is linearly independent and B_2 generates V.

$$\begin{aligned} |B_1| &\leq |B_2| \\ |B_2| &\leq |B_1| \\ \Rightarrow |B_1| &= |B_2| \end{aligned}$$

Definition 3.4 (Dimension)
Let V be an $\mathcal{F}$-VS. Then we define dimension as

$$\dim_{\mathcal{F}}(V) = \begin{cases} \text{length of the basis if } V \text{ is finitely generated} \\ \infty \quad \text{otherwise} \end{cases}$$

Theorem 3.10 (Corollary)
Let $U \subseteq V$ be a subspace. Then $\dim(U) \leq \dim(V)$.

Proof 3.9
A basis of U is a linear set in V. Hence it is shorter or equal in length to any generating set of V, especially a basis of V.

Theorem 3.11 (Corollary 2.39)
A linearly independent list of size $\dim(V)$ is already a basis.

Proof 3.10
We can extend the list to a basis. But it is already of length $\dim(V)$ hence nothing is added.

Theorem 3.12 (Corollary 2.42)
Let $\dim(V) = n$ then every generating set of length n is already a basis.

Two sets A, B with size $|A|, |B|$. The union has size: $|A \cup B| = |A| + |B| - |A \cap B|$

Theorem 3.13
Let A, B be subspaces of a finite dimensional space V. Then $\dim(A+B) = \dim(A) + \dim(B) - \dim(A \cap B)$.

Proof 3.11
Let $c_1, \dots, c_l$ be a basis for $A \cap B$. We extend to a basis $c_1, \dots, c_l, a_1, \dots, a_m$ of A and to a basis $c_1, \dots, c_l, b_1, \dots, b_n$ of B.

We want to show that $c_i a_j b_k$ is a basis for $A + B$. This is a generating set, now we need to check that it is linearly independent.

Now let

$$\begin{aligned}
0 &= \sum \alpha_i a_i + \sum \beta_j b_j + \sum \mu_k c_k \\
-\sum \alpha_i a_i &= \sum \beta_j b_j + \sum \mu_k c_k \in A \cap B \\
-\sum \alpha_i a_i &= \sum \delta_k c_k \\
0 &= \sum \alpha_i a_i + \sum \delta_k c_k \\
\Rightarrow \alpha_i &= 0 \quad \delta_k = 0 \\
\Rightarrow 0 &= \sum (\beta_j b_j + \sum \gamma_k c_k) \\
\Rightarrow \beta_j &= 0 \quad \gamma_k = 0
\end{aligned}$$