

1. BASIC NOTIONS

Definition 1.1. A binary operation on a set S is a function $f : S \times S \rightarrow S$.

Definition 1.2. A *field* is a set \mathbb{F} together with two binary operations $+$, and \cdot called addition and multiplication (respectively) such that

1. For all $a, b, c \in \mathbb{F}$ we have

$$a + (b + c) = (a + b) + c$$

and

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

2. For all $a, b \in \mathbb{F}$ we have

$$a + b = b + a$$

and

$$a \cdot b = b \cdot a.$$

3. There exists an element $0 \in \mathbb{F}$, called an additive identity, such that for all $a \in \mathbb{F}$ we have $a + 0 = a$.
4. There exists an element $1 \in \mathbb{F}$, called a multiplicative identity, such that for all $a \in \mathbb{F}$ we have $a \cdot 1 = a$.
5. For all $a \in \mathbb{F}$ there exists an element $b \in \mathbb{F}$, called an additive inverse, such that $a + b = 0$.
6. For all $a \in \mathbb{F}$ such that $a \neq 0$ there exists an element $c \in \mathbb{F}$, called a multiplicative inverse, such that $a \cdot c = 1$.
7. For all $a, b, c \in \mathbb{F}$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Note: Fields have a unique additive and multiplicative identity denoted 0 and 1 respectively. Moreover, when the additive and multiplicative inverses exist they are unique.

Some examples: All of the following examples are with their standard operations.

1. \mathbb{Q} (rational numbers)
2. \mathbb{R} (real numbers)
3. \mathbb{C} (complex numbers)
4. $\mathbb{Z}/p\mathbb{Z}$ for p prime (Integers modulo p)

Non example: \mathbb{Z} is not a field, it lacks multiplicative inverses.

Definition 1.3. A *vector space* V over a field \mathbb{F} is a set V with two operations called *vector addition* and *scalar multiplication* where vector addition is a function $+$: $V \times V \rightarrow V$ and scalar multiplication is a function \cdot : $\mathbb{F} \times V \rightarrow V$ such that

1. For all $u, v \in V$ we have

$$u + v = v + u$$

2. For all $u, v, w \in V$ and for all $a, b \in \mathbb{F}$ we have

$$(u + v) + w = u + (v + w)$$

and

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

3. There exists a vector $0 \in V$, called an additive identity, such that for all $v \in V$ we have

$$v + 0 = v$$

4. For all $v \in V$ we have a vector $w \in V$, called an additive inverse, such that

$$v + w = 0$$

5. For all $v \in V$ we have

$$1 \cdot v = v$$

6. For all $a, b \in \mathbb{F}$ and for all $u, v \in V$ we have

$$a \cdot (u + v) = a \cdot u + a \cdot v$$

Some examples: All of the following examples are with their standard operations.

1. $\mathbb{F}^n = \left\{ \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} : a_i \in \mathbb{F} \right\}$ where \mathbb{F} is a field.
2. Polynomials with coefficients in a field \mathbb{F} .
3. Polynomials (with coefficients in a field \mathbb{F}) of degree $\leq n$
4. Continuous functions $f : X \rightarrow Y$, $C(X, Y)$, where X and Y are fields.
5. Functions from a field X into a field Y .
6. $\mathbb{F}^\infty = \{(a_1, a_2, a_3, \dots) : a_i \in \mathbb{F}\}$.

Proposition 1.1. *Every vector space V has a unique additive identity. The unique additive identity is denoted 0 .*

Proposition 1.2. *Every element $v \in V$ has a unique additive inverse. For all $v \in V$ its unique additive inverse is denoted $-v$.*

Proposition 1.3. *For all $v \in V$ we have $0 \cdot v = 0$.*

Proposition 1.4. *For all $a \in \mathbb{F}$ and $0 \in V$ we have $a \cdot 0 = 0$.*

Proposition 1.5. *For every $v \in V$ we have $(-1) \cdot v = -v$*

2. BASIS FOR A VECTOR SPACE

Definition 2.1. A *linear combination* of a list of vectors v_1, \dots, v_m in V is a vector of the form

$$a_1v_1 + \dots + a_mv_m$$

where $a_1, \dots, a_m \in \mathbb{F}$.

Definition 2.2. The set of all linear combinations of a list of vectors v_1, \dots, v_m in V is called the *span* of v_1, \dots, v_m denoted by $\text{span}\{v_1, \dots, v_m\}$.

$$\text{span}\{v_1, \dots, v_m\} = \{a_1v_1 + \dots + a_mv_m \mid a_i \in \mathbb{F}\}$$

Definition 2.3. If V is a vector space and $V = \text{span}\{v_1, \dots, v_m\}$ then we say that v_1, \dots, v_m span V .

Definition 2.4. We say that a vectors space is *finite dimensional* if there exists a finite list of vectors v_1, \dots, v_m such that

$$\text{span}\{v_1, \dots, v_m\} = V$$

Otherwise we say that V is *infinite dimensional*.

Definition 2.5. A list of vectors v_1, \dots, v_m in V is called *linearly independent* if the only choice of $a_1, \dots, a_m \in \mathbb{F}$ such that

$$a_1v_1 + \dots + a_mv_m = 0$$

is $a_1 = a_2 = \dots = a_m = 0$. A list is called *linearly dependent* if it is not linearly independent.

Lemma 2.6. Suppose that v_1, \dots, v_m is a linearly dependent list in V . There exists a $j \in \{1, \dots, m\}$ such that

- 1) $v_j \in \text{span}\{v_1, \dots, v_{j-1}\}$
- 2) $\text{span}\{v_1, \dots, v_{j-1}, v_j, v_{j+1}, \dots, v_m\} = \text{span}\{v_1, \dots, v_{j-1}, v_{j+1}, \dots, v_m\}$

Proposition 2.1. In a finite dimensional vector space the length of every linearly independent list of vectors is less than or equal to the length of every spanning list of vectors.

Definition 2.7. A basis for a vector space V is a list of vectors $\{v_1, \dots, v_n\}$ such that

1. $\{v_1, \dots, v_n\}$ is linearly independent
2. $\text{span}\{v_1, \dots, v_n\} = V$.

Proposition 2.2. A list of vectors $\{v_1, \dots, v_n\}$ in V is a basis for V if and only if every vector $v \in V$ can be written uniquely in the form

$$v = a_1v_1 + \dots + a_nv_n$$

for some $a_1, \dots, a_n \in \mathbb{F}$.

Proposition 2.3. Every spanning list of vectors in V can be reduced down to a basis.

Proposition 2.4. Every linearly independent list of vectors in V can be extended to a basis.

Proposition 2.5. Any two basis of a finite dimensional vector space V have the same length.

Definition 2.8. The dimension of a finite dimensional vector space is the length of any basis of the vector space. Denoted $\dim(V)$.

Proposition 2.6. *Suppose V is finite dimensional. Every list of linearly independent vectors whose length is equal to the dimension of V is a basis.*

Proposition 2.7. *Suppose V is finite dimensional. Every spanning list vectors whose length is equal to the dimension of V is a basis.*

3. SUBSPACES

Definition 3.1. A subspace of a vector space V is a subset H such that H is a vector space under the same binary relations and field as V .

Proposition 3.1 (Subspace Test). *A subset H is a subspace of V if and only if*

1. $0 \in H$.
2. For all $u, v \in H$ we have $u + v \in H$
3. For all $u \in H$ and $a \in \mathbb{F}$ we have $au \in H$.