# 1. Vector spaces

**Def.** An <u>abelian group</u> $G$ is a set equipped with a binary operation

$$* : G \times G \longrightarrow G \qquad ( * (x,y) = x * y )$$

satisfying the following:

(i) $x * y = y * x \quad \forall x, y \in G$ (commutativity)

(ii) $\exists$ an element $e \in G$ s.t. $e * x = x * e = x \quad \forall x \in G$ (existence of identity)

(iii) for each $x \in G$, there exists an element $y_x \in G$ s.t. $x * y_x = y_x * x = e$ (existence of inverses)

(iv) $x * (y * z) = (x * y) * z \quad \forall x, y, z \in G$ (associativity)

**Rk**

- The identity $e$ in (ii) is unique, i.e., if $e' \in G$ is any element such that $e' * x = x * e' = x \quad \forall x \in G$, then $e' = e$.
- For each $x \in G$, the inverse $y_x$ in (iii) is unique, i.e., if $y_x' \in G$ is any element such that $x * y_x' = y_x' * x = e$, then $y_x' = y_x$.

  We denote $y_x$ by $x^{-1}$ (in multiplicative notation) or $-x$ (in additive notation) and call it the <u>inverse</u> of $x$.

**Examples** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are abelian groups under addition

$\{\pm 1\}$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ are abelian groups under multiplication

$\mathbb{N}$ is not an abelian group under addition

$\mathbb{Z} \setminus \{0\}$ is not an abelian group under multiplication

**Def.** A *field* $F$ is a set on which two binary operations $+$ ("addition") and $\cdot$ ("multiplication") are defined such that

(i) $F$ is an abelian group under addition. We denote by $0$ the (additive) identity.

(ii) $F \setminus \{0\}$ is an abelian group under multiplication. We denote by $1$ the (multiplicative) identity.

(iii) the distributive law holds:

$$\lambda \cdot (\mu + \nu) = \lambda \cdot \mu + \lambda \cdot \nu \qquad \forall \lambda, \mu, \nu \in F$$

**Examples** $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/2\mathbb{Z}$ with usual addition and multiplication are fields

Let $F$ be a field, $n > 0$ an integer. The set of (ordered) $n$-tuples of elements of $F$ is the set

$$F^n := \{ (x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in F \}$$

Define a binary operation "$+$" on $F^n$ as follows:

if $\vec{x} = (x_1, \ldots, x_n)$, $\vec{y} = (y_1, \ldots, y_n) \in F^n$, then

$$\vec{x} + \vec{y} = (x_1 + y_1, \ldots, x_n + y_n)$$

Clearly

$$\vec{x}+\vec{y} = \vec{y}+\vec{x} \qquad \forall \vec{x},\vec{y} \in F^n$$

$$\vec{x}+(\vec{y}+\vec{z}) = (\vec{x}+\vec{y})+\vec{z} \qquad \forall \vec{x},\vec{y},\vec{z} \in F^n$$

Define $\vec{0} = (0,\dots,0)$ and, for each $\vec{x} = (x_1,\dots,x_n) \in F^n$, define $-\vec{x} = (-x_1,\dots,-x_n)$.

Then

$$\vec{x}+\vec{0} = \vec{0}+\vec{x} = \vec{x} \qquad \forall \vec{x} \in F^n$$

$$\vec{x}+(-\vec{x}) = \vec{0} = (-\vec{x})+\vec{x} \qquad \forall \vec{x} \in F^n$$

Hence $F^n$ is an abelian group under $+$.

Define an operation

$$F \times F^n \longrightarrow F^n$$

$$(\lambda, \underset{\substack{\| \\ (x_1,\dots,x_n)}}{\vec{x}}) \longmapsto \lambda\vec{x} := (\lambda x_1,\dots,\lambda x_n)$$

Then

- $\lambda(\vec{x}+\vec{y}) = \lambda\vec{x}+\lambda\vec{y} \qquad \forall \lambda \in F,\ \forall \vec{x},\vec{y} \in F^n$
- $(\lambda+\mu)\vec{x} = \lambda\vec{x}+\mu\vec{x} \qquad \forall \lambda,\mu \in F,\ \forall \vec{x} \in F^n$
- $(\lambda\mu)\vec{x} = \lambda(\mu\vec{x}) \qquad \forall \lambda,\mu \in F,\ \forall \vec{x} \in F^n$
- $1.\vec{x} = \vec{x} \qquad \forall \vec{x} \in F^n$

This motivates the following definition.

**Def** An <u>F-vector space</u> (or a <u>vector space over F</u>) is an abelian group $V$ (written additively) together with a map $\begin{array}{l} F \times V \to V \\ (\lambda, x) \mapsto \lambda x \end{array}$ called <u>scalar multiplication</u> such that

(i) $\lambda(x+y) = \lambda x + \lambda y \quad \forall \lambda \in F, \ \forall x, y \in V$

(ii) $(\lambda+\mu)x = \lambda x + \mu x \quad \forall \lambda, \mu \in F, \ \forall x \in V$

(iii) $(\lambda\mu)x = \lambda(\mu x) \quad \forall \lambda, \mu \in F, \ \forall x \in V$

(iv) $1x = x \quad \forall x \in V$

**Convention** For $x, y \in V$, we write $x-y$ to mean $x+(-y)$.

**Examples**

1) $F^n$ is an F-vector space. In particular, $F$ is an F-vector space.

2) $\mathbb{R}$ is a $\mathbb{Q}$-vector space

$\mathbb{C}$ is an $\mathbb{R}$-vector space and also a $\mathbb{Q}$-vector space

3) Let $X$ be a set and let $F$ be a field. Let

$$V := \{\text{functions } X \to F\}.$$

For $f, g \in V$, $\lambda \in F$ define

$$(f+g)(t) = f(t) + g(t) \quad \forall t \in X$$

$$(\lambda f)(t) = \lambda \cdot f(t) \quad \forall t \in X$$

Then $f+g, \lambda f \in V$. The set $V$ is a vector space under these operations.

Rk (a) If $F = \mathbb{R}$, $X = [0,1]$, then $V$ is the space of real-valued functions on the interval $[0,1]$.

(b) If $F$ is any field and $X = \{1, 2, \dots, n\}$, then a function $f: X \to F$ is essentially an $n$-tuple of elements of $F$, so we can identify $V$ with $F^n$.

Prop. Let $V$ be an $F$-vector space. Then:

(a) $0_F \cdot x = 0_V \quad \forall x \in V$

(b) $\lambda \cdot 0_V = 0_V \quad \forall \lambda \in F$

(c) $\lambda \cdot x = 0_V \Rightarrow \lambda = 0_F$ or $x = 0_V$

(d) $(-\lambda)x = -(\lambda x) = \lambda(-x) \quad \forall \lambda \in F, \forall x \in V$

Proof.

(a) $0_F \cdot x = (0_F + 0_F) \cdot x = 0_F \cdot x + 0_F \cdot x$

This implies that

$$0_F \cdot x + (-0_F x) = (0_F \cdot x + 0_F \cdot x) + (-0_F \cdot x) = 0_F \cdot x + (0_F \cdot x + (-0_F \cdot x))$$

$$\Rightarrow 0_V = 0_F \cdot x + 0_V = 0_F \cdot x$$

(b) Exercise

(c) Suppose $\lambda \cdot x = 0_V$. If $\lambda = 0$, we are done. If $\lambda \neq 0$, then $\lambda^{-1} \in F \setminus \{0\}$ exists and so

$$x = 1_F \cdot x = (\lambda^{-1}\lambda)x = \lambda^{-1}(\lambda x) = \lambda^{-1} 0_V = 0_V.$$

(d) $\lambda \cdot x + (-\lambda)x = (\lambda + (-\lambda))x = 0 \cdot x = 0_V$

Adding $-(\lambda \cdot x)$ to both sides, we deduce $(-\lambda)x = -(\lambda x)$.

Similarly $\lambda(-x) = -(\lambda x)$ (exercise).