(M1) For all $x, y \in F$, we have $x \cdot y = y \cdot x$

(multiplication is commutative)

(M2) For all $x, y, z \in F$, we have $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

(multiplication is associative)

(M3) For every $x \in F \setminus \{0\}$ there is an element $y \in F$ so that $x \cdot y = 1$

(inverse w.r.t. multiplication)

(D) For all $x, y, z \in F$, we have $(x+y) \cdot z = x \cdot z + y \cdot z$

(distributive law)

Remarks:

1) One can show (you should try!) that inverse elements w.r.t. addition and multiplication are unique. This allows us to write

$-x$ for the additive inverse of x and

x^{-1} for the multiplicative inverse of x (when $x \neq 0$)

2) other rules, e.g. $0 \cdot x = 0$ for all $x \in F$, are consequences of the rules above.

We also define the notion of a group, which we will need a little later:

Def: A set G with a binary operation $* : G \times G \to G$

is called a group if (A0), (A2) and (A3) are satisfied.

If in addition (A1) is also satisfied then $(G, *)$ is an

abelian group or commutative group.

Ex: If $(F, +, \cdot)$ is a field then $(F, +)$ is an abelian group and $(F \setminus \{0\}, \cdot)$ is also an abelian group.

Notation: Just as for vectors, we write

$$a - b := a + (-b) \quad \text{for } a, b \in F \qquad (F \text{ a field})$$

Ex: $\mathbb{F}_2$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

You can check that all rules are satisfied, so $(\mathbb{F}_2, +, \cdot)$ is a field.

2. Vector spaces

Def: Let $(F, +, \cdot)$ be a field.

A **vector space over F** is a set V with two operations

$$+ : V \times V \longrightarrow V \quad , \quad (v, w) \mapsto v + w \qquad \text{(addition)}$$

and

$$\cdot : F \times V \longrightarrow V \qquad (a, v) \mapsto a \cdot v \qquad \text{(scalar multiplication)}$$

so that the following hold:

(V) $(V, +)$ is a commutative group

(SM1) $a \cdot (v + w) = a \cdot v + a \cdot w$ for all $a \in F$, $v, w \in V$

(SM2) $(a + b) \cdot v = av + b \cdot v$ for all $a, b \in F$, $v \in V$

(SM3) $(a \cdot b) \cdot v = a \cdot (b \cdot v)$ for all $a, b \in F$, $v \in V$

(SM4) $1 \cdot v = v$ for all $v \in V$

The elements of V are then called **vectors**.

Notation/Rule: $(a-b)\cdot v = a\cdot v + (-b)\cdot v =: av - bv$

$(-1)\cdot v =: -v$

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

(0 in F; 0 in V)

Ex: $(F, +, \cdot)$ field

1) $(\{0\}, +, \cdot)$ is a vector space over F, the zero space

2) $(F, +, \cdot)$ is a vector space over F with the operations given on F.

3) $(\mathbb{C}, +, \cdot)$ is an $\mathbb{R}$-vector space w.r.t.

$$+ : \mathbb{C}\times\mathbb{C} \longrightarrow \mathbb{C}, \quad (x+iy, u+iv) \mapsto x+u + i(y+v)$$

$$\cdot : \mathbb{R}\times\mathbb{C} \longrightarrow \mathbb{C} \qquad a\cdot(x+iy) \mapsto a\cdot x + i\cdot(a\cdot y)$$

Theorem 1

Let M be a set, and let $(F, +, \cdot)$ be a field.

Then the set $F^M := \mathrm{Map}(M, F) = \{f : M \to F\}$ of maps from M to F

with addition

$$+ : F^M \times F^M \longrightarrow F^M \qquad (f, g) \mapsto f+g$$

defined by

$$(f+g)(m) := f(m) + g(m) \qquad \text{for all } m \in M$$

($+$: addition in F)

and scalar multiplication

$$\cdot : F \times F^M \longrightarrow F^M \qquad (a, f) \mapsto a\cdot f$$

defined by $(a \cdot f)(m) := a \cdot f(m)$ for all $m \in M$

($\cdot$: multiplication in F)

is a vector space over F.

Ex: F a field

1) $M = \{1, \dots, n\} \subseteq \mathbb{N}$

$\Rightarrow F^M =: F^n$

$f \in F^n$ is map from $\{1, \dots, n\}$ to F, so it is given by the ordered set of values $f(1), f(2), \dots, f(n) \in F$

$\Rightarrow F^n = \{(f(1), \dots, f(n)) \mid f \in F^n\}$

$= \{(f_1, \dots, f_n) \mid f_i \in F\}$

Vector spaces of this form are sometimes called <u>standard spaces</u>.

We have seen those for $F = \mathbb{R}$ in the introduction, e.g.

$M = \{1, 2, 3\}$, $F = \mathbb{R}$ gives $\mathbb{R}^3$.

2) $M = \mathbb{N}$

Then F^M is the vector space of sequences over F.

<u>Proof of Theorem 1</u>

We need to show that the properties of the definition are satisfied. Let $V := F^M$

1) $(V, +)$ is a commutative group:

$f, g \in V$, $m \in M \Rightarrow (f+g)(m) = f(m) + g(m) = g(m) + f(m) = (g+f)(m)$

(addition in F is commutative)

Since this holds for any $m \in M$, it implies $f+g = g+f$.

Let $f, g, h \in V$, $m \in M$. We similarly find:

$$((f+g)+h)(m) = (f+g)(m) + h(m) = f(m) + g(m) + h(m)$$

$$= f(m) + (g(m) + h(m)) = (f + (g+h))(m)$$

↑ addition in F is associative

Again, since $m \in M$ is arbitrary, this implies $(f+g)+h = f+(g+h)$

Let 0_V be the map defined by $0_V(m) = 0$ for all $m \in M$ (zero map)

It is then easy to check that this is a neutral element for addition.

We still need to show the existence of inverse elements:

Let $f \in V$. Define $g \in V$ by $g(m) := \underbrace{-f(m)}_{\text{inverse of } f(m) \text{ in } (F,+)}$

Then $(f+g)(m) = f(m) + g(m) = f(m) + (-f(m)) = 0$, for all $m \in M$.

Hence $f + g = 0_V$.

2) scalar multiplication:

(SM2) wts for $a, b \in F$, $f \in F^M$: $(a+b)\cdot f = a\cdot f + b\cdot f$

Let $m \in M$. Then

$$((a+b)\cdot f)(m) \overset{\text{df}}{=} (a+b) f(m) = a\cdot f(m) + b\cdot f(m) = (a\cdot f)(m) + (b\cdot f)(m)$$

↑ distributive law in F

so $(a+b)\cdot f = a\cdot f + b\cdot f$.

Similarly for (SM1), (SM3), (SM4)

□