1.1 definition: *complex numbers,* $\mathbf{C}$

- A *complex number* is an ordered pair (a, b), where $a, b \in \mathbf{R}$, but we will write this as $a + bi$.
- The set of all complex numbers is denoted by $\mathbf{C}$:

$$\mathbf{C} = \{a + bi : a, b \in \mathbf{R}\}.$$

- *Addition* and *multiplication* on $\mathbf{C}$ are defined by

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i;$$

here $a, b, c, d \in \mathbf{R}$.

$i^2 = -1$

$(a+bi)(c+di) = a(c+di) + bi(c+di)$
$= ac + adi + bci + bdi^2$
$= (ac - bd) + (ad + bc)i$

1.3 *properties of complex arithmetic*

commutativity
$\alpha + \beta = \beta + \alpha$ and $\alpha\beta = \beta\alpha$ for all $\alpha, \beta \in \mathbf{C}$.

associativity
$(\alpha + \beta) + \lambda = \alpha + (\beta + \lambda)$ and $(\alpha\beta)\lambda = \alpha(\beta\lambda)$ for all $\alpha, \beta, \lambda \in \mathbf{C}$.

identities
$\lambda + 0 = \lambda$ and $\lambda 1 = \lambda$ for all $\lambda \in \mathbf{C}$.

additive inverse
For every $\alpha \in \mathbf{C}$, there exists a unique $\beta \in \mathbf{C}$ such that $\alpha + \beta = 0$.

multiplicative inverse
For every $\alpha \in \mathbf{C}$ with $\alpha \neq 0$, there exists a unique $\beta \in \mathbf{C}$ such that $\alpha\beta = 1$.

distributive property
$\lambda(\alpha + \beta) = \lambda\alpha + \lambda\beta$ for all $\lambda, \alpha, \beta \in \mathbf{C}$.

1.5 definition: $-\alpha$, *subtraction,* $1/\alpha$, *division*

Suppose $\alpha, \beta \in \mathbf{C}$.

- Let $-\alpha$ denote the additive inverse of α. Thus $-\alpha$ is the unique complex number such that

$$\alpha + (-\alpha) = 0.$$

- *Subtraction* on $\mathbf{C}$ is defined by

$$\beta - \alpha = \beta + (-\alpha).$$

- For $\alpha \neq 0$, let $1/\alpha$ and $\frac{1}{\alpha}$ denote the multiplicative inverse of α. Thus $1/\alpha$ is the unique complex number such that

$$\alpha(1/\alpha) = 1.$$

α^{-1}

- For $\alpha \neq 0$, *division* by α is defined by

$$\beta/\alpha = \beta(1/\alpha).$$

For $\alpha \in \mathbb{C}$ and m a positive integer, we define α^m to denote the product of α with itself m times:

$$\alpha^m = \underbrace{\alpha \cdots \alpha}_{m \text{ times}}.$$

Definition

Definition 1 (Field)
*A **field** is a set $\mathbb{F}$ equipped with two binary operations (usually written as addition and multiplication) such that:*

1. *Addition and multiplication are associative: $\forall a, b, c \in \mathbb{F}$, we have*

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

2. *Addition and multiplication commute: $\forall a, b, c \in \mathbb{F}$, we have*

$$a + b = b + a$$
$$ab = ba$$

3. *There exist distinct additive and multiplicative identities in $\mathbb{F}$:*

$$\exists 1 \in \mathbb{F} \text{ such that } 1a = a \ \ \forall a \in \mathbb{F}$$
$$\exists 0 \in \mathbb{F} \text{ such that } a + 0 = a \ \ \forall a \in \mathbb{F}$$

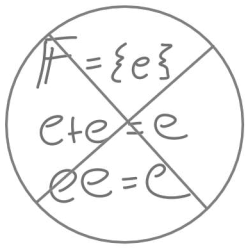
The distinctness requirement here means that $0 \neq 1$.

4. *Additive and multiplicative inverses exist in $\mathbb{F}$:*

$$\forall a \in \mathbb{F}, \exists (-a) \in \mathbb{F} \text{ such that } a + (-a) = 0$$
$$\forall a \neq 0 \in \mathbb{F}, \exists a^{-1} \in \mathbb{F} \text{ such that } aa^{-1} = 1$$

5. *Multiplication is distributive over addition:*

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



Definition

Definition 2 ($\mathbb{F}^n$)
For n a positive integer, we define:

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

Where the addition is component-wise.

Example

Example 3
Here is an example of addition in $\mathbb{F}^n$:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

What about multiplication? Can we define $(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n)$?

Sure, but we lose a nice property! mainly, multiplicative inverses: Ex: $(0, x_2, \ldots, x_n)$ does not have a multiplicative inverse! Even when $x_i \neq 0$ for some $i \in \{2, \ldots, n\}$ i.e. we have some $x \neq 0$ with no inverse wrt multiplication!

Notation

Notation 4
In $\mathbb{F}^n$, we let 0 denote the element $(0, 0, \ldots, 0) \in \mathbb{F}^n$, and for $x \in \mathbb{F}^n$, we let $(-x)$ denote the additive inverse of x–i.e., the element $(-x) \in \mathbb{F}^n$ such that $x + (-x) = 0$.

Definition

Definition 5 (Scaling)
For $\lambda \in \mathbb{F}$, define λx for $x \in \mathbb{F}^n$ to be:

$$\lambda x = (\lambda x_1, \ldots, \lambda x_n) \in \mathbb{F}^n$$

1.19 definition: *addition, scalar multiplication*

- An *addition* on a set V is a function that assigns an element $u + v \in V$ to each pair of elements $u, v \in V$.
- A *scalar multiplication* on a set V is a function that assigns an element $\lambda v \in V$ to each $\lambda \in \mathbf{F}$ and each $v \in V$.

1.20 definition: *vector space*

A *vector space* is a set V along with an addition on V and a scalar multiplication on V such that the following properties hold.

commutativity
$u + v = v + u$ for all $u, v \in V$.

associativity
$(u + v) + w = u + (v + w)$ and $(ab)v = a(bv)$ for all $u, v, w \in V$ and for all $a, b \in \mathbf{F}$.

additive identity
There exists an element $0 \in V$ such that $v + 0 = v$ for all $v \in V$.

additive inverse
For every $v \in V$, there exists $w \in V$ such that $v + w = 0$.

multiplicative identity
$1v = v$ for all $v \in V$.

distributive properties
$a(u + v) = au + av$ and $(a + b)v = av + bv$ for all $a, b \in \mathbf{F}$ and all $u, v \in V$.

different +'s!

1.21 definition: *vector, point*

Elements of a vector space are called *vectors* or *points*.

Example

$\mathbb{F}^n$ is a vector space for any field $\mathbb{F}$. If you take F^∞ to be all sequences of elements in $\mathbb{F}$, then so is F^∞.

Notation

For a set S and field $\mathbb{F}$, $\mathbb{F}^S$ denotes the set of all functions from S to $\mathbb{F}$.

Example

If we define $(f + g)(x) = f(x) + g(x)$ and $(\lambda f)(x) = \lambda(f(x))$ for all $f, g \in \mathbb{F}^S$ and $\lambda \in \mathbb{F}$, then $\mathbb{F}^S$ is a vector space.

Similar!

Notice: A function $f \in \mathbb{F}^S$ w/ $S = \{1, \ldots, n\}$ is basically just a list $(x_1, \ldots, x_n)$
ie. $f(i) = x_i$. Taking $S = \{1, \ldots\}$ we get $\mathbb{F}^\infty$ too!

1.26 *unique additive identity*

A vector space has a unique additive identity.

Proof

Let $0, 0' \in V$ be two additive identities. Then,

$0 + x = x$ and $0' + x = x$ for all $x \in V$. So,

$0' = 0 + 0'$ commutativity!

$= 0' + 0$

$= 0$.

1.27 *unique additive inverse*

Every element in a vector space has a unique additive inverse.

Proof Let V be a vector space & let $v \in V$.

& w, w' are two additive inverses of v. Then:

$$\begin{aligned} w &= w + 0 \\ &= w + (v + w') \\ &= (w + v) + w' \\ &= 0 + w' \\ &= w'. \end{aligned}$$

Therefore, additive inverses are unique.

1.28 notation: $-v$, $w - v$

Let $v, w \in V$. Then

- $-v$ denotes the additive inverse of v;
- $w - v$ is defined to be $w + (-v)$.

1.30 *the number* 0 *times a vector*

$0v = 0$ for every $v \in V$.

Proof

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

So,

$0 = 0v + (-(0v))$ ← Defn of additive inverses

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

$= 0v + (0v + (-(0v)))$ ← Associativity of addition

$= 0v + 0$ ← Defn of additive inverses

$= 0v$ ← Defn of additive identity.

1.31 *a number times the vector* 0

$a0 = 0$ for every $a \in \mathbf{F}$.

Proof

$$\begin{aligned} a0 &= a(0+0) \\ &= a0 + a0 \end{aligned}$$

Hence,
$$\begin{aligned} 0 &= a0 + (-(a0)) \\ &= (a0 + a0) + (-(a0)) \\ &= a0 + (a0 + (-(a0))) \\ &= a0 + 0 \\ &= a0. \end{aligned}$$

(Same reasons as before!)

1.32 *the number -1 times a vector*

$(-1)v = -v$ for every $v \in V$.

Proof For $v \in V$,

$$\begin{aligned} v + (-1)v &= (1)v + (-1)v \\ &= (1+(-1))v \\ &= 0v \\ &= 0 \end{aligned}$$

Hence, by the uniqueness of additive inverses,

$$(-1)v = -v.$$