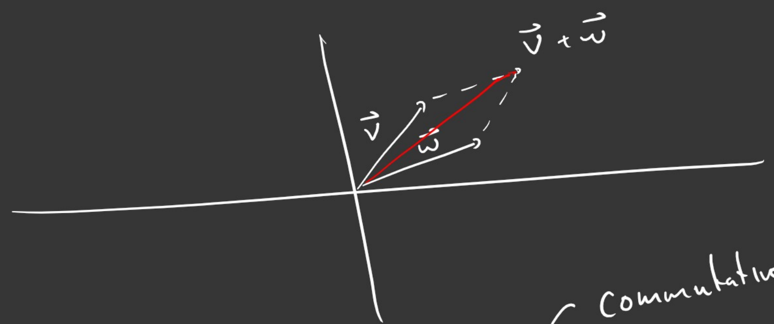
Modules

Motivating example:

The vector space $\mathbb{R}^n := \{ (a_1, \ldots, a_n) \mid a_i \in \mathbb{R},\ i = 1, 2, \ldots, n \}$

Addition: $\vec{v} = (v_1, \ldots, v_n)$
$\vec{w} = (w_1, \ldots, w_n)$ $\in \mathbb{R}^n$

$\vec{v} + \vec{w} := (v_1 + w_1, \ldots, v_n + w_n) \in \mathbb{R}^n$



commutative

Note: $(\mathbb{R}^n, +)$ is an abelian group with addition.

- $\exists\ \vec{0} \in \mathbb{R}^n$ s.t.
$$\vec{0} + \vec{v} = \vec{v} + \vec{0} = \vec{v} \qquad \forall\ \vec{v} \in \mathbb{R}^n$$

- $(\vec{v} + \vec{w}) + \vec{u} = \vec{v} + (\vec{w} + \vec{u}) \qquad \forall\ \vec{v}, \vec{w}, \vec{u} \in \mathbb{R}^n$

- $\forall\ \vec{v} \in \mathbb{R}^n,\ \exists\ -\vec{v} \in \mathbb{R}^n$ s.t.
$$\vec{v} + (-\vec{v}) = (-\vec{v}) + \vec{v} = \vec{0}$$

- (Abelian) $\vec{v} + \vec{w} = \vec{w} + \vec{v} \qquad \forall\ \vec{v}, \vec{w} \in \mathbb{R}^n$

$\mathbb{R}^n$ also has <u>scalar multiplication</u>:

If $a \in \mathbb{R}$, $\vec{v} \in \mathbb{R}^n$

$$a \cdot \vec{v} = (a v_1, a v_2, \ldots, a v_n) \in \mathbb{R}^n$$

<u>properties of scalar mult:</u>

⓪ We can think of scalar multiplication as a map

$$\begin{aligned} \mathbb{R} \times \mathbb{R}^n &\longrightarrow \mathbb{R}^n \\ (a, \vec{v}) &\longmapsto a \cdot \vec{v} \end{aligned}$$

Suppose $a, b \in \mathbb{R}$, $\vec{v}, \vec{w} \in \mathbb{R}^n$

① $(a+b) \cdot \vec{v} = a \cdot \vec{v} + b \cdot \vec{v}$

② $(a \cdot b) \cdot \vec{v} = a \cdot (b \cdot \vec{v})$

③ $a \cdot (\vec{v} + \vec{w}) = a \cdot \vec{v} + a \cdot \vec{w}$

④ $1 \cdot \vec{v} = \vec{v}$

Defn: Let R be a ring.

A **(left) module over R** (or **R-module**)

is a set M with

① a binary operation $+$

s.t. $(M, +)$ is an abelian group

② an action of R on M

i.e. a map $R \times M \longrightarrow M$

$$(r, m) \longmapsto r \cdot m$$

s.t. (i) $(r+s) \cdot m = r \cdot m + s \cdot m$

(ii) $(rs) \cdot m = r \cdot (s \cdot m)$

(iii) $r \cdot (m + n) = r \cdot m + r \cdot n$

(iv) If $1 \in R$, then $1 \cdot m = m$] M is a unital R-module

Note: we can define a right R-module by

$m \cdot r$.

Only difference $m \cdot (rs) = (m \cdot r) \cdot s$

Note: If R is a commutative ring then any left R-module has a natural right R-module structure as well.

$$(rs)\cdot m = (sr)\cdot m$$

$$\updownarrow$$

$$m\cdot(sr) = m\cdot(rs) = (m\cdot r)\cdot s$$

Defn: If F is a field, then we refer to F-modules as <u>F-vector spaces</u>

In this sense, $\mathbb{R}^n$ <u>is</u> an $\mathbb{R}$-vector space.

Obs: If $R \subset S$ is a subring

M an S-module

then M is also an R-module by restricting scalar multiplication.

e.g. $\mathbb{C}^2$ is a $\mathbb{C}$-vector space but is also an $\mathbb{R}$-vector space

If $a \in \mathbb{R}$, $\vec{v} = (v_1, v_2) \in \mathbb{C}^2$

then $a\cdot\vec{v} = (av_1, av_2) \in \mathbb{C}^2$ still makes sense.

Examples

① For any ring R, consider

$$R^n := \{ (a_1, \ldots, a_n) \mid a_i \in R,\ i = 1, 2, \ldots, n \}$$

with component-wise addition

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)$$
$$:= (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

Easy exercise: $(R^n, +)$ is an abelian group.

Scalar multiplication is also component-wise:

$$a \in R, \ (a_1, \ldots, a_n) \in R^n$$
$$a \cdot (a_1, \ldots, a_n) := (a \cdot a_1, \ldots, a \cdot a_n)$$

Easy exercise: $(R^n, +)$ is an R-module with this scalar multiplication

This is called the free R-module of rank n

② The trivial module $0 := \{0\}$

$$\forall r \in R, \ r \cdot 0 := 0$$

③ Any ideal of a ring $I \subset R$ is an R-module

$$R \times I \longrightarrow I$$
$$(r, a) \longmapsto ra$$

④ Quotient rings of R are R-modules

$$R \times R/I \longrightarrow R/I$$
$$(r, \bar{a}) \longmapsto \overline{r \cdot a}$$

<u>Check</u>: $(rs) \cdot \bar{a} = r \cdot (s\bar{a})$

<u>Back to motivating example</u>:

Recall a vector subspace $W \subset \mathbb{R}^n$ is a subset s.t.

① $\forall \vec{w}_1, \vec{w}_2 \in W$, $\vec{w}_1 + \vec{w}_2 \in W$

② $\vec{0} \in W$

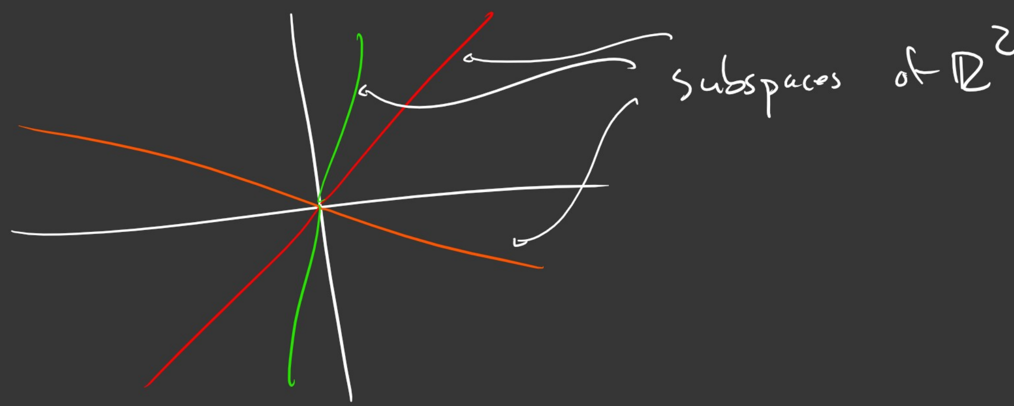
③ $\forall a \in \mathbb{R}, \vec{w} \in W$, $a \cdot \vec{w} \in W$

④ $\forall \vec{w} \in W$, $-\vec{w} \in W$

$-1 \cdot \vec{w} = -\vec{w}$

e.g. $\mathbb{R}^2$ has subspaces

$$0,\ \mathbb{R}^2,\ \text{Span}\left\{\begin{pmatrix} a \\ b \end{pmatrix} \,\middle|\, a,b\in\mathbb{R}\right\}$$



Defn: A <u>submodule</u> of an R-module M

is a subgroup $N \subset M$

s.t. $\forall r\in R,\ n\in N,\quad r\cdot n\in N$

If F is a field, we call F-submodules

<u>F-subspaces</u>

<u>Examples:</u>

① Every module is a submodule of itself

② Every module has the 0-submodule

③ If we think about R as a module over itself

Then the submodules of R are the ideals of R.

<u>Note:</u> The only subspaces of $\mathbb{R}$ are 0, $\mathbb{R}$.

Example: $\mathbb{Z}$-modules.

Let M be any abelian group.

Define $\forall n \in \mathbb{Z}$, $a \in M$

$$n \cdot a := \begin{cases} \underbrace{a + a + a + \ldots + a}_{n\text{-times}} & n > 0 \\ 0 & n = 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{(-n)\text{-times}} & n < 0 \end{cases}$$

Easy check: $(n+m) \cdot a = n \cdot a + m \cdot a$

$(n \cdot m) \cdot a = n \cdot (m \cdot a)$

So $\{\mathbb{Z}\text{-modules}\} = \{\text{abelian groups}\}$.

e.g. $\mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module

$n \cdot \bar{0} = \bar{0}$, $n \cdot \bar{1} = \bar{n}$, $n \cdot \bar{2} = \overline{2n}$, $n \cdot \bar{3} = \overline{3n}$

A large list of $\mathbb{Z}$-modules: $\mathbb{Z}^n$, $n \geq 1$

$\mathbb{Z}/n\mathbb{Z}$, $n \geq 2$

Example: $(\mathbb{Z}/n\mathbb{Z})$-module

Let M be a $(\mathbb{Z}/n\mathbb{Z})$-module.

Then $\underbrace{(1+1+1+ \_\_\_ +1)}_{n\text{-times}} \cdot a = 0 \cdot a = 0 \quad \forall a \in M.$

$$\| $$

$$\underbrace{1\cdot a + 1\cdot a + 1\cdot a + \_\_\_ + 1\cdot a}_{n\text{-times}}$$

$$\|$$

$$\underbrace{a + a + a + \_\_\_ + a}_{n\text{-times}}.$$

e.g. $\mathbb{Z}/2\mathbb{Z}$ is a $(\mathbb{Z}/4\mathbb{Z})$-module

because $\underbrace{(1 \bmod 2) + (1 \bmod 2)}_{0 \bmod 2} + \underbrace{(1 \bmod 2) + (1 \bmod 2)}_{0 \bmod 2}$

$= 0 \bmod 2.$

Back again to the motivating example:

A linear transformation is a map

$$T: \mathbb{R}^n \longrightarrow \mathbb{R}^m$$

s.t. $\begin{bmatrix} T(\vec{v}+\vec{w}) = T\vec{v} + T\vec{w} \\ T(a\vec{v}) = a \cdot T\vec{v} \end{bmatrix}$

e.g. $T: \mathbb{R}^3 \longrightarrow \mathbb{R}^2$

$$(x,y,z) \longmapsto (2x+y-z,\ x+2y)$$

which we can encode in a matrix

$$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 2 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2x+y-z \\ x+2y \end{pmatrix}$$

Defn: Let R be a ring. M, N R-modules

An R-module homomorphism from M to N

is a map $f: M \longrightarrow N$

s.t. ① $f(m+n) = f(m) + f(n)$ $\quad \forall m,n \in M$

② $f(a \cdot m) = a \cdot f(m)$ $\quad \forall a \in R,\ m \in M.$

If F is a field, we call F-module homomorphisms

F-linear transformations