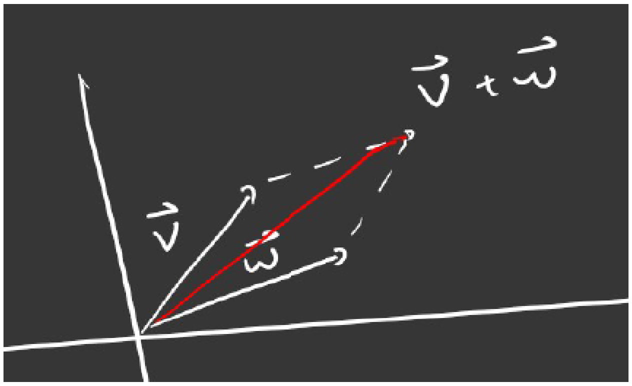
L15: Modules

Consider the vector space $\mathbb{R}^n := \{(a_1, \dots, a_n) \mid a_i \in \mathbb{R},\ i = 1, 2, \dots, n\}$. We know from our experiences in linear algebra that addition is defined as

$$\begin{array}{r} \mathbf{v} = (v_1, \dots, v_n) \\ \mathbf{w} = (w_1, \dots, w_n) \end{array} \implies \mathbf{v} + \mathbf{w} := (v_1 + w_1, \dots, v_n + w_n) \in \mathbb{R}^n$$



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

- (Additive identity) $\exists \mathbf{0} \in \mathbb{R}^n$ such that $\mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0} = \mathbf{v} \quad \forall \mathbf{v} \in \mathbb{R}^n$
- (Associative) $(\mathbf{v} + \mathbf{w}) + \mathbf{u} = \mathbf{v} + (\mathbf{w} + \mathbf{u}) \quad \forall \mathbf{v}, \mathbf{w}, \mathbf{u} \in \mathbb{R}^n$
- (Additive inverse) $\forall \mathbf{v} \in \mathbb{R}^n, \exists$ -$\mathbf{v} \in \mathbb{R}^n$ such that $\mathbf{v} + (-\mathbf{v}) = (-\mathbf{v}) + \mathbf{v} = \mathbf{0}$
- (Abelian) $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v} \quad \forall \mathbf{v}, \mathbf{w} \in \mathbb{R}^n$

$\mathbb{R}^n$ also has **scalar multiplication**: If $a \in \mathbb{R}$ and $\mathbf{v} \in \mathbb{R}^n$ then

$$a \bullet \mathbf{v} = (av_1, av_2, \dots, av_n) \in \mathbb{R}^n$$

We can think of scalar multiplication as a map

$$\begin{aligned} \mathbb{R} \times \mathbb{R}^n &\to \mathbb{R}^n \\ (a, \mathbf{v}) &\mapsto a \bullet \mathbf{v} \end{aligned}$$

Suppose $a, b \in \mathbb{R}$ and $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$, then scalar multiplication has the following properties

(1) $(a + b) \bullet \mathbf{v} = a \bullet \mathbf{v} + b \bullet \mathbf{v}$

(2) $(ab) \bullet \mathbf{v} = a \bullet (b \bullet \mathbf{v})$

(3) $a \bullet (\mathbf{v} + \mathbf{w}) = a \bullet \mathbf{v} + a \bullet \mathbf{w}$

(4) $1 \bullet \mathbf{v} = \mathbf{v}$

Definition 15.1: R-module

Let R be a ring.
A **(left) module over** R or (R-**module**) is a set M with

(1) a binary operation $+$ such that $(M, +)$ is an Abelian group,
(2) an action of R on M i.e a map

$$\begin{aligned} R \times M &\to M \\ (r, m) &\mapsto r \bullet m \end{aligned}$$

such that for $r, s \in R$ and $m, n \in M$

(i) $(r + s) \bullet m = r \bullet m + s \bullet m$
(ii) $(rs) \bullet m = r \bullet (s \bullet m)$
(iii) $r \bullet (m + n) = r \bullet m + r \bullet n$
(iv) If $1 \in R$ then $1 \bullet m = m$ and the module is called **Unital**.

Note: We can define a **right** R-module by $m \bullet r$ with scalar multiplication on the right.The only difference is associativity being $m \bullet (rs) = (m \bullet r) \bullet s$. Contrast this to property (ii) which says the action of rs on m is the action of s first and then acting by r , whereas now, it is the action of r first then acting by s and these two notions coincide only when R is commutative.
We will always be talking about left R-modules unless explicitly stated
Note: If R is a commutative ring then any left R-module has a natural right R-module structure as well:

$$(rs) \bullet m = (sr) \bullet m \longleftrightarrow m \bullet (sr) = m \bullet (rs) = (m \bullet r) \bullet s$$

Definition 15.2: F-vector space

If F is a field, then we refer to F-modules as F-**vector spaces**. In this sense $\mathbb{R}^n$ is an $\mathbb{R}$-vector space.

Observe If $R \subset S$ is as subring and M is an S-module then M is also a R-module by restricting scalar multiplication to R. For example, $\mathbb{C}^2$ is a $\mathbb{C}$-vector space but it is also an $\mathbb{R}$-vector space.
If $a \in \mathbb{R}$, $\mathbf{v} = (v_1, v_2) \in \mathbb{C}^2$ then $a \bullet \mathbf{v} = (av_1, av_2) \in \mathbb{C}^2$ still makes sense.

Example 15.1. For any ring R, consider

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

with component-wise addition

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

Exercise: $(R^n, +)$ is an abelian group.
Scalar multiplication is also component-wise, for $a \in R$ and $(a_1, \ldots, a_n) \in R^n$, defined as

$$a \bullet (a_1, \ldots, a_n) \coloneqq (a \bullet a_1, \ldots, a \bullet a_n)$$

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

This is called the **free R-Module of rank n**.

Example 15.2. The **trivial module** $0 \coloneqq \{\mathbf{0}\}$ which has $\forall r \in R$, $r \bullet \mathbf{0} \coloneqq \mathbf{0}$.

Example 15.3. Any ideal of a ring $I \subset R$ is an R-module with scalar multiplication as ring multiplication:

$$\begin{aligned} R \times I &\to I \\ (r, a) &\mapsto ra \end{aligned}$$

Example 15.4. Quotient rings of R are R-modules with scalar multiplication as ring multiplication:

$$\begin{aligned} R \times R/I &\to R/I \\ (r, \bar{a}) &\mapsto \overline{r \bullet a} \end{aligned}$$

Exercise: Module property (ii) $(rs) \bullet \bar{a} = r \bullet (s \bullet \bar{a})$ holds.

Recall a vector subspace $W \subset \mathbb{R}^n$ is a subset such that

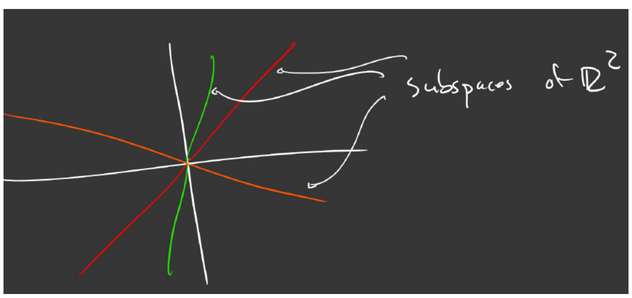
(i) $\mathbf{w}_1 + \mathbf{w}_2 \in W, \quad \forall \mathbf{w}_1, \mathbf{w}_2 \in W$

(ii) $\mathbf{0} \in W$

(iii) $a \bullet \mathbf{w} \in W, \quad \forall a \in \mathbb{R}, \mathbf{w} \in W$

(iv) $-\mathbf{w} \in W, \quad \forall \mathbf{w} \in W$

Example 15.5. $\mathbb{R}^2$ has subspaces $\mathbf{0}, \mathbb{R}^2, \text{Span}\left\{\begin{pmatrix} a \\ b \end{pmatrix} \mid a, b \in \mathbb{R}\right\}$



Definition 15.3: Submodule, Subspace

A **submodule** of an R-module M is a subgroup $N \subset M$ such that it is closed under scalar multiplication, i.e for all $r \in R, n \in N, r \bullet n \in N$.
If F is a field, we call F-submodules **F-subspaces**

Example 15.6. Every module is a submodule of itself.

Example 15.7. Every module has the 0-module.

Example 15.8. If we think about a ring R as a module over itself, then the submodules of R are the ideals of R.
Note: The only subspaces of $\mathbb{R}$ are 0 or $\mathbb{R}$ (since the only ideals in a field are 0 and the field itself).

Example 15.9. $\mathbb{Z}$**-modules**.
Let M be any abelian group. Define for all $n \in \mathbb{Z}$ and $a \in M$,

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

Exercise: $(n+m) \cdot a = n \cdot a + m \cdot a$ and $(nm) \cdot a = n \cdot (m \cdot a)$
This is a common sense way to come up with a $\mathbb{Z}$-module structure on any abelian group and so $\{\mathbb{Z}\text{-modules}\} = \{\text{Abelian groups}\}$ For example $\mathbb{Z}/4\mathbb{Z}$ is a $\mathbb{Z}$-module as

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

We can then immediately think of a large list of $\mathbb{Z}$-modules: $\mathbb{Z}^n$ for $n \geq 1$ and $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$.

Example 15.10. $(\mathbb{Z}/n\mathbb{Z})$**-module**
Let M be a $(\mathbb{Z}/n\mathbb{Z})$-module.
Then

$$\begin{aligned} &\underbrace{(1 + 1 + 1 + \cdots + 1)}_{n\text{-times}} \cdot a = 0 \cdot a = 0 \quad \forall a \in M \\ = &\underbrace{1 \cdot a + 1 \cdot a + 1 \cdot a + \cdots + 1 \cdot a}_{n\text{-times}} \\ = &\underbrace{a + a + a + \cdots + a}_{n\text{-times}} \end{aligned}$$

So in a $\mathbb{Z}/n\mathbb{Z}$-module, the sum of any element with itself n times is going to be equal to 0. For example $\mathbb{Z}/2\mathbb{Z}$ is a $(\mathbb{Z}/4\mathbb{Z})$-module because 1 added to itself four times is 0 as seen

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

A **linear transformation** $T \colon \mathbb{R}^n \to \mathbb{R}^m$ is a map between two vector spaces such that

$$T(\mathbf{v} + \mathbf{w}) = T\mathbf{v} + T\mathbf{w}$$
$$T(a\mathbf{v}) = a \cdot T\mathbf{v}$$

As an example,

$$\begin{aligned} T \colon \mathbb{R}^3 &\to \mathbb{R}^2 \\ (x, y, z) &\mapsto (2x + y - z, x + 2y) \end{aligned}$$

which, recall, we can represent as a matrix

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

Definition 15.4: R-module homomorphism, F-linear transformation

Let R be a ring and M, N be R-modules.
An R**-module homomorphism** from M to N is a map $f\colon M \to N$ such that

(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**.