# Modules over a ring

Nicolas Mascot

TCD

March 19, 2020

# Reminder: vector spaces

**Definition**

*Let $K$ be a field. A $K$-vector space is a set $V$ equipped with two composition laws*

$$\begin{array}{rcl} V \times V & \longrightarrow & V \\ (v, w) & \longmapsto & v + w, \end{array} \qquad \begin{array}{rcl} K \times V & \longrightarrow & V \\ (\lambda, v) & \longmapsto & \lambda v \end{array}$$

*such that $(V, +)$ is an Abelian group, and that for all $\lambda, \mu \in K$ and $v, w \in V$, we have*

$$\lambda(\mu v) = (\lambda\mu)v, \qquad 1v = v,$$

$$(\lambda + \mu)v = (\lambda v) + (\mu v), \qquad \lambda(v + w) = (\lambda v) + (\lambda w).$$

# Modules

## Definition

*Let $R$ be a ring. An <u>$R$-module</u> is a set $M$ equipped with two composition laws*

$$\begin{array}{rcl} M \times M & \longrightarrow & M \\ (m, n) & \longmapsto & m + n, \end{array} \qquad \begin{array}{rcl} R \times M & \longrightarrow & M \\ (\lambda, m) & \longmapsto & \lambda m \end{array}$$

*such that $(M, +)$ is an Abelian group, and that for all $\lambda, \mu \in R$ and $m, n \in M$, we have*

$$\lambda(\mu m) = (\lambda\mu)m, \qquad 1m = m,$$

$$(\lambda + \mu)m = (\lambda m) + (\mu m), \qquad \lambda(m + n) = (\lambda m) + (\lambda n).$$

# Modules: examples

## Example

Let $R$ be a ring, and let $n \in \mathbb{N}$. Then

$$R^n = \{(x_1, \cdots, x_n) \mid x_i \in R\}$$

is an $R$-module.

## Example

Let $(G, +)$ be an Abelian group. Then $G$ is actually a $\mathbb{Z}$-module:

$$ng = \underbrace{g + \cdots + g}_{n \text{ times}} \qquad (n \in \mathbb{Z}, g \in G).$$

# Submodules

**Definition**

*Let $M$ be an $R$-module. A submodule of $M$ is a subset of $M$ which is nonempty and closed under $+$ and under multiplication by $R$.*

**Example**

Let $M = R$, viewed as an $R$-module. Then the submodules of $M$ are the ideals of $R$.

# Generating sets of a module

## Definition

*Let $M$ be an $R$-module. Elements $m_1, \cdots, m_n \in M$ form a generating set if every $m \in M$ can be expressed in the form*

$$m = \sum_{i=1}^{n} \lambda_i m_i$$

*for some (not necessarily unique) $\lambda_i \in R$.*
*If such a finite generating set exists, then we say that $M$ is finitely generated.*

## Counter-example

Let $R$ be a commutative ring. Then $R[x]$ is an $R$-module, which is not finitely generated.

# Linear independence, free modules

## Definition

*Let $M$ be an $R$-module. Elements $m_1, \cdots, m_n \in M$ are linearly independent if the only $\lambda_1, \cdots, \lambda_n \in R$ satisfying*

$$\sum_{i=1}^{n} \lambda_i m_i = 0$$

*are $\lambda_1 = \cdots = \lambda_n = 0$.*

*If furthermore $m_1, \cdots, m_n$ form a generating set of $M$, we say that $M$ is a free $R$-module of rank $n$, and that the $m_i$ form a basis of $M$. In this case, every $m \in M$ can be expressed as*

$$m = \sum_{i=1}^{n} \lambda_i m_i$$

*for some unique $\lambda_i \in R$.*

# Free modules: examples

**Example**

$R^n$ is a free $R$-module of rank $n$, with basis

$$e_1 = (1, 0, \cdots, 0),\ e_2 = (0, 1, 0, \cdots, 0),\ \cdots, e_n = (0, \cdots, 0, 1).$$

**Counter-example**

The $\mathbb{Z}$-module $M = \mathbb{Z}/2\mathbb{Z}$ is finitely generated, but it is not a free module.

# Modules vs. vector spaces

In a vector space, one can extract a basis out of any generating set, and every linearly independent family can be extended into a basis.

**Counter-example**

$\{2, 3\}$ is a generating family of the $\mathbb{Z}$-module $M = \mathbb{Z}$, because $n = (-n)2 + (n)3$ for all $n \in \mathbb{Z}$. But one cannot extract a basis out of it.

**Counter-example**

In the $\mathbb{Z}$-module $M = \mathbb{Z}$, the linearly independent family $\{2\}$ cannot be extended into a basis.

# Morphisms

## Definition

*Let $M$ and $N$ be two $R$-modules. A map $f : M \longrightarrow N$ is a morphism if it is $R$-linear, meaning*

$$f(m + m') = f(m) + f(m') \text{ and } f(\lambda m) = \lambda f(m)$$

*for all $m, m' \in M$ and $\lambda \in R$.*
*A morphism is an isomorphism if it is bijective, in which case its inverse is automatically a morphism.*

# Morphisms: examples

## Example

An $R$-module $M$ is finitely generated iff. there exits $n \in \mathbb{N}$ and a surjective morphism $R^n \longrightarrow M$. It is free of rank $n$ iff. it is isomorphic to $R^n$.

## Remark

Let $I \subset R$ be a maximal ideal, and let $k = R/I$ be the corresponding field. Then

$$R^n \simeq R^m \Longrightarrow k^n \simeq k^m \Longrightarrow n = m,$$

so the rank of a free module is well-defined.

# Kernels and images

**Theorem**

*Let $M$ and $N$ be two $R$-modules, and $f : M \longrightarrow N$ be a morphism. Then*

$$\operatorname{Ker} f = \{m \in M \mid f(m) = 0\} \subseteq M$$

*is a submodule of $M$, and*

$$\operatorname{Im} f = \{f(m) \mid m \in M\} \subseteq N$$

*is a submodule of $N$.*

*$f$ is injective iff. $\operatorname{Ker} f = \{0\}$, surjective iff. $\operatorname{Im} f = N$, and an isomorphism if it is both.*

# Kernels and images: example

**Example**

Let

$$f: \begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ (x,y) & \longmapsto & x - y \bmod 2. \end{array}$$

Then

$$\operatorname{Im} f = \mathbb{Z}/2\mathbb{Z},$$

and

$$\operatorname{Ker} f = \{(x,y) \in \mathbb{Z}^2 \mid x \equiv y \bmod 2\}$$

is a free submodule of rank 2 of $\mathbb{Z}^2$ with basis $\{(1,1),(1,-1)\}$.

# Morphisms between free modules

Let $M$ be a free $R$-module with basis $m_1, m_2, \cdots$. Every $m \in M$ can be expressed uniquely as $m = \lambda_1 m_1 + \lambda_2 m_2 + \cdots$, and can thus be represented by its coordinates $\lambda_1, \lambda_2, \cdots \in R$.

Likewise, if $N$ is another free $R$-module with basis $n_1, n_2, \cdots$, then each morphism from $M$ to $N$ may be represented by it matrix with respect to these bases. Conversely, each matrix (of the appropriate size) corresponds to a morphism from $M$ to $N$.

Composition of morphisms corresponds to multiplication of matrices. In particular, a morphism from $M$ to $N$ is an isomorphism if and only if its matrix is invertible.

# $\mathrm{GL}_n(R)$: statement

Let $R$ be a commutative ring and $n \in \mathbb{N}$ be n integer. Write

$$M_n(R) = \{n \times n \text{ matrices with coefficients in } R\}$$

and

$$\mathrm{GL}_n(R) = M_n(R)^\times.$$

**Theorem**

$$\mathrm{GL}_n(R) = \{A \in M_n(R) \mid \det A \in R^\times\}.$$

# $\mathrm{GL}_n(R)$: proof and example

**Proof.**

If $A, B \in M_n(R)$ satisfy $AB = 1_n$, then

$$1 = \det(1_n) = \det(AB) = \det(A)\det(B)$$

so $\det(A) \in R^\times$.
Conversely, every $A \in M_n(R)$ satisfies

$$AA' = \det(A) I_n$$

where $A'$ is the adjugate matrix of $A$. □

**Example**

$$\mathrm{GL}_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}.$$

# Quotient modules

**Theorem**

*Let $M$ be an $R$-module, and $S \subseteq M$ be a submodule. Then the quotient set*

$$M/S = M/\sim, \quad \text{where } m \sim m' \iff m - m' \in S,$$

*inherits an $R$-module structure. The projection map*

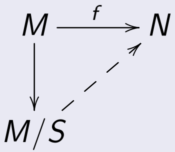
$$M \longrightarrow M/S$$

*is a surjective morphism whose kernel is $S$.*

# The isomorphism theorem for modules

**Theorem**

*Let $M$ and $N$ be two $R$-modules, $S \subseteq M$ a submodule, and $f : M \longrightarrow N$ be a morphism. Then $f$ factors as*




*iff.* $S \subseteq \operatorname{Ker} f$.

*In particular, $f$ induces an isomorphism $M/\operatorname{Ker} f \simeq \operatorname{Im} f$.*