4/29/2019

(109) # Chapter 14 Modules (= Linear algebra) over a ring

It is surprisingly useful to generalize vector spaces V over a field $\mathbb{F}$ to something over a ring R

DEF'N: For a (commutative) ring R (with 1), an R-module V is an abelian
(14.1.1) group $(V,+)$ together with a scalar multiplication $R\times V \to V$
$(r,v)\mapsto rv$

satisfying
$$1\cdot v = v$$
$$(rs)v = r(sv)$$
$$(r+s)v = rv+sv \qquad \forall r,s\in R$$
$$r(v+v') = rv+rv' \qquad v,v'\in V$$

An R-submodule $V'\subset V$ is a subgroup $(V',+)$ closed under scalar multiplication,
i.e. $r\in R,\ v'\in V' \Rightarrow rv'\in V'$

An R-module homomorphism is a map $V_1 \xrightarrow{\varphi} V_2$ that is
an abelian group homomorphism $V_1^+ \xrightarrow{\varphi} V_2^+$
respecting scalar mult: $\varphi(rv) = r\varphi(v)\quad \forall r\in R,\ v\in V_1$

It's an isomorphism of R-modules if it's bijective

EXAMPLES: ① When $R=\mathbb{F}$ is a field, R-modules V are $\mathbb{F}$-vector spaces
R-submodules $V'\subset V$ are ($\mathbb{F}$-linear) subspaces
R-module homoms $V_1\xrightarrow{\varphi}V_2$ are $\mathbb{F}$-linear transformations

② When $R=\mathbb{Z}$, it (somewhat surprisingly) turns out that
$\mathbb{Z}$-modules V are nothing more than abelian groups $V=V^+$,
i.e. the scalar mult. adds no extra structure since one is
forced to define $\mathbb{Z}\times V\to V$
$$(n,v)\mapsto nv = \underbrace{(1+1+\dots+1)}_{n}v = 1\cdot v+1\cdot v+\dots+1\cdot v$$
$$= v+v+\dots+v$$

It will still turn out to be useful to view abelian groups as $\mathbb{Z}$-modules!
$\mathbb{Z}$-module homoms/isomorphisms are just group homoms/isos. $\mathbb{Z}$-submodules are subgroups.

③ When $R=\mathbb{F}[x]$ for a field $\mathbb{F}$, an R-module
i.e. $\mathbb{F}[x]$-module V
also has a surprising reformulation: it's an $\mathbb{F}$-vector space V,
together with an $\mathbb{F}$-linear transformation $V \xrightarrow{T} V$
that describes the scalar multiplication $(x,v) \longmapsto x\cdot v = T(v)$

(since $x(v+v') = xv + xv'$
$x(cv) = (xc)v = (cx)v = c(xv)$
so it is $\mathbb{F}$-linear)

and then any $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{F}[x]$

has $f(x)v = a_0v + a_1xv + a_2x^2v + \cdots + a_nx^nv$

$$= a_0v + a_1T(v) + a_2T^2(v) + \cdots + a_nT^n(v)$$

$$= (a_0 + a_1T + a_2T^2 + \cdots + a_nT^n)(v)$$

An $\mathbb{F}[x]$-submodule $V'\subset V$ is a T-stable $\mathbb{F}$-linear subspace $V'\subset V$
meaning $T(V')\subseteq V'$.

($\Rightarrow T^2(V') = T(T(V')) \subseteq T(V') \subseteq V'$
$\vdots$
$T^n(V') \subseteq V' \ \forall n$)

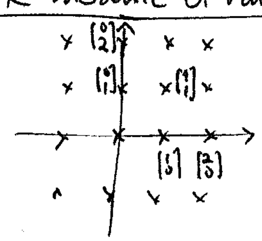
④ One can consider $V=R$ itself as an R-module via $V=R^+$

and $\underbrace{R\times V}_{=R\times R} \longrightarrow \underbrace{V}_{=R}$

$(r,s) \longmapsto rs$

and then an R-submodule $V'\subset R$ is just an ideal $V'\subset R$
since $r\cdot v'\in V' \ \forall v'\in V'$

⑤ $R^n := \left\{ \text{column vectors } \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} : x_i \in R \right\}$ with usual $+$ and R-scaling
is called a free R-module of rank n.

e.g. $\mathbb{Z}^2 =$ 

These are the most similar R-modules to vector spaces $V=\mathbb{F}^n$ over a field $\mathbb{F}$

How to recognize when an R-module $V \cong R^n$?

DEF'N: • Given $\{v_1,\dots,v_n\} \subset V$ an R-module,

$\mathrm{span}_R\{v_1,\dots,v_n\} := Rv_1 + \dots + Rv_n = \{r_1v_1+\dots+r_nv_n : r_i \in R\}$

= the R-submodule spanned by $\{v_i\}_{i=1}^n$

• Say $\{v_1,\dots,v_n\} \subset V$ are (R-linearly) independent if

$r_1v_1+\dots+r_nv_n = 0 \implies r_1=\dots=r_n=0$

• Say $\{v_1,\dots,v_n\} \subset V$ are an R-basis for V if they both span V and are independent.

PROPOSITION: Given $\{v_1,\dots,v_n\} \subset V$ an R-module,

the map $R^n \xrightarrow{\varphi} V$ is an R-module homomorphism,

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \longmapsto x_1v_1+\dots+x_nv_n$$

which is
- surjective $\iff V = \mathrm{span}_R\{v_i\}_{i=1}^n$
- injective $\iff \{v_i\}_{i=1}^n$ are independent
- bijective (i.e. an R-module isomorphism) $\iff \{v_i\}_{i=1}^n$ is an R-basis for V.

proof: Just think about it ∎

EXAMPLES:

① V is called a finitely generated R-module if it has a finite spanning set $\{v_i\}_{i=1}^n$ with $V = \mathrm{span}_R\{v_i\}_{i=1}^n$

e.g. $V = \mathbb{Q}^+$ is not finitely generated as a $\mathbb{Z}$-module (EXERCISE)

$V = \mathbb{Z}^2$ is fin. gen'd as $\mathbb{Z}$-module, since $V = \mathbb{Z}\begin{bmatrix}1\\0\end{bmatrix} + \mathbb{Z}\begin{bmatrix}0\\1\end{bmatrix}$

$V = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ is fin. gen'd as $\mathbb{Z}$-module, since $V = \mathbb{Z}\begin{bmatrix}\bar{1}\\0\\0\end{bmatrix} + \mathbb{Z}\begin{bmatrix}0\\\bar{1}\\0\end{bmatrix} + \mathbb{Z}\begin{bmatrix}0\\0\\\bar{1}\end{bmatrix}$

$V = \mathbb{Z}^\infty = \left\{ \begin{bmatrix} x_1 \\ x_2 \\ \vdots \end{bmatrix} : x_i \in \mathbb{Z} \right\}$ is not finitely gen'd as a $\mathbb{Z}$-module (EXERCISE)

② Many (most) finitely gen'd R-modules will have no basis, since they are not free R-modules

e.g. $V = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ has none

$4\begin{bmatrix}\bar{1}\\0\\0\end{bmatrix} = \begin{bmatrix}\bar{4}\\0\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\end{bmatrix} = 0$, but $4 \neq 0$ in $\mathbb{Z}$.