LAST TIME · Defined submodules of an R-module

· Proved: for a field F there is a bijection

$\{(V, T: V \to V) \mid V \text{ vector space over } F,\ T: V \to V \text{ linear map}\}$

$\longleftrightarrow$ $F[x]$-modules:

Given $T: V \to V$, $p(x) \in F[x]$, $p(x) \cdot v = p(T)v$

Conversely given $F[x] \times V \to V$, V is an F-module (since $F \subseteq F[x]$)

and the map $x \cdot - : V \to V$, $v \mapsto x \cdot v$ is F-linear.

· defined homomorphisms of R-modules

· Proved that if N is a submodule of an R-module M then the quotient abelian group $M/N = \{m + N \mid m \in M\}$ is an R-module with $r \cdot (m+N) = (r \cdot m) + N$. $\forall r \in R$

Thm (1st isomorphism theorem for modules). Let $\varphi: M \to N$ be a homomorphism of R-modules. Then

$\bar{\varphi}: M/\ker\varphi \longrightarrow \operatorname{im}\varphi$, $\bar{\varphi}(x + \ker\varphi) = \varphi(x)$

is a well-defined isomorphism of R-modules.

Proof Since $\varphi: M \to N$ is a homomorphism of abelian groups, the 1st iso Thm for abelian groups applies. $\Rightarrow$

$\bar{\varphi}: M/\ker\varphi \longrightarrow \operatorname{im}\varphi \equiv \varphi(M)$, $\bar{\varphi}(x + \ker\varphi) = \varphi(x)$

is a well-defined isomorphism of abelian groups.

Moreover, $\forall r \in R$, $\forall x \in M$

$$\bar{\varphi}(r \cdot (x + \ker\varphi)) = \bar{\varphi}((rx) + \ker\varphi) = \varphi(rx) = r\varphi(x) = r \cdot \bar{\varphi}(x + \ker\varphi)$$

$\Rightarrow$ $\bar{\varphi}$ is a bijective homomorphism of R-modules,

Hence $\bar{\varphi}$ is an isomorphism of R-modules.

Generators

"Recall" A vector space V over a field F is generated by a set $X \subseteq V$ iff every $v \in V$ is a finite linear combination of elements of X: $\forall v \in V \ \exists n>0, x_1 \dots x_n \in X, \lambda_1 \dots \lambda_n \in F$ so that

$$v = \lambda_1 x_1 + \dots + \lambda_n x_n.$$

Ex F a field, $V = F[x]$ $X = \{1, x, x^2, \dots, x^n, \dots\} \equiv \{x^n\}_{n \geq 0}$ generates $F[x]$ because $\forall p(x) \in F[x]$, $\exists n$ and $a_0 \dots a_n \in F$ s.t. $p(x) = a_0 \cdot 1 + a_1 x + \dots + a_n x^n$.

Definition Let M be an R-module. A subset $X \subseteq M$ generates M if $\forall m \in M \ \exists n>0, r_1 \dots r_n \in R, x_1 \dots x_n \in X$ s.t.

$$m = r_1 x_1 + \dots + r_n x_n$$

Ex $M = \mathbb{Z}$, a $\mathbb{Z}$-module. $X = \{5, 6\} \subseteq \mathbb{Z}$ generates $\mathbb{Z}$ since $1 = (-1)5 + 1 \cdot 6 \Rightarrow m = (-m) \cdot 5 + m \cdot 6 \ \forall m \in \mathbb{Z}$.

"Fancy" view of generating sets of modules (see homework)

1. $\forall$ R-module M, $\forall$ set $\mathcal{J}$ of submodules of M, $\bigcap_{N \in \mathcal{J}} N$ is a submodule of M.

2. $\forall$ R-module M, $\forall$ set $X \subseteq M$, $X \neq \emptyset$, $\mathcal{J} = \{N \subseteq M \mid N \text{ submodule and } X \subseteq N\} \neq \emptyset$ since $M \in \mathcal{J}$ and then $\langle X \rangle = \bigcap_{N \in \mathcal{J}} N = \bigcap_{X \subseteq N} N$ is a submodule of M.

3. $\langle X \rangle$ = set of finite linear combinations of elements of X

4. A set $X \subseteq M$ generates $M \iff M = \langle X \rangle$.

Definition An R-module M is finitely generated iff it is generated by a finite set

An R-module M is cyclic iff it is generated by a 1-element set $\{x\}$.

Ex Any finite dimensional vector space over a field F is a finitely generated F-module.

Ex For any ring R the module R is generated by the set $\{1_R\}$: $\forall\, r \in R$, $r = r \cdot 1_R$.

Ex Let R be a rng, $I \subseteq R$ an ideal. Then I is an R-module. I is a cyclic R-module $\Leftrightarrow$ I is principal.

Ex Cyclic abelian groups $\mathbb{Z}_n$ are generated by $[1]$: $[k] = k \cdot [1]$
Hence they are cyclic $\mathbb{Z}$-modules

Proposition 31.1 Let M be a cyclic R-module. Then M is isomorphic, as an R-module, to R/I for some ideal $I \subseteq R$.

Proof Suppose $x \in M$ generates M: $\forall\, m \in M\ \exists\, r \in R$ s.t. $m = r \cdot x$
Consider $\varphi: R \to M$, $\varphi(r) = r \cdot x$:
φ is surjective. Also: $\forall\, r_1, r_2 \in R$

$$\varphi(r_1 + r_2) = (r_1 + r_2)x = r_1 x + r_2 x = \varphi(r_1) + \varphi(r_2)$$

$$\varphi(ra) = (ra) \cdot x = r \cdot (a \cdot x) = r \cdot \varphi(a)$$

$\Rightarrow$ φ is a homomorphism of R-modules.
Let $I = \ker \varphi$. $I \subseteq R$ is a submodule, hence an ideal.
1st iso Thm for modules $\Rightarrow$

$$\overline{\varphi}: R/I \to M, \quad \overline{\varphi}(r + I) = r \cdot x$$

is a well-defined isomorphism of R-modules.

We would like to have a definition of a basis of an R-module. For that we need a notion of linear independence.

Def A subset X of an R-module M is linearly independent if $\forall n>0$, $\forall r_1, \dots r_n \in R$, $x_1, \dots x_n \in X$

$$r_1 x_1 + \dots + r_n x_n = 0 \Rightarrow r_1 = r_2 = \dots = r_n = 0.$$

Ex $M = F[x]$ (F a field), $X = \{x^i\}_{i=0}^{\infty}$ is linearly independent: $\forall n$, $\lambda_1 \cdot x^{k_1} + \dots + \lambda_k x^{k_n} = 0 \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_k = 0$ ($n \geq 1$)

Non Ex $M = \mathbb{Z}_n$, a $\mathbb{Z}$-module. $X = \{[1]\}$ is not linearly independent since $n \cdot [1] = [n] = [0]$ while $n \neq 0$.

Def Let M be an R-module. A subset $X \subseteq M$ is a basis if (1) X generates M and (2) X is linearly independent.

Note An R-module need not have a basis.

Eg. $\mathbb{Z}_n$ is a $\mathbb{Z}$-module with no basis, since $\forall x \in \mathbb{Z}_n$, $n \cdot x = 0$.

Eg Let F be a field, $V = F^n$, $T: V \to V$ linear map, $T \neq 0$. Then $Tv = Av$ for some $n \times n$ matrix A, $A \neq 0$.

Recall: $p_A(\lambda) = \det(\lambda I_n - A) \in F[x]$ has the property that $p_A(A) = 0$ (Cayley-Hamilton)

Hence $p_A(x) \cdot v = 0 \quad \forall v \in F^n$

$\Rightarrow$ no subset of F^n is linearly independent when we view F^n as an $F[x]$-module.