LECTURE 28: GENERATION OF MODULES, DIRECT SUMS, RANK

Let R be a ring with unity 1.

Def^n/ Let M be an R-module and $N_1, \dots, N_n$ be submodules of M.

(1.) $N_1 + \cdots + N_n = \{a_1 + \cdots + a_n \mid a_i \in N_i \text{ for all } i = 1, \dots, n\}$ is the sum of the submodules $N_1, \dots, N_n$.

(2.) For any subset $A \subseteq M$ we let

$$RA = \{r_1 a_1 + r_2 a_2 + \cdots + r_m a_m \mid r_1, \dots, r_m \in R,\ a_1, \dots, a_m \in A,\ m \in \mathbb{Z}^+\}$$

where $R\emptyset = \{0\}$ by convention and if A is the finite set $\{a_1, a_2, \dots, a_n\} = A$ then

$$RA = Ra_1 + Ra_2 + \cdots + Ra_n$$

If N is submodule and $N = RA$ for some subset A of M then A is a generating set for N and N is generated by A.

(3.) A submodule N of M is finitely generated if there is some finite set $A \subseteq M$ such that $N = RA$.

(4.) A submodule N of M is cyclic if there exists an element $a \in M$ such that $N = Ra = \{ra \mid r \in R\}$

Remark: if $1 \notin R$ then the def^n above can still be made however we wouldn't have $A \subseteq RA$ in that context.

Def^n/ If N is finitely generated then there is a smallest $d \in \mathbb{Z}^+$ for which $A = \{a_1, a_2, \dots, a_d\}$ generates N, such a set A is minimal generating set for N.

Examples

(1.) $R = \mathbb{Z}$ and M any R-module. Hence M forms abelian group.

$$\mathbb{Z}a = \langle a \rangle = \{ na \mid n \in \mathbb{Z} \}$$

finitely generated $\mathbb{Z}$-modules are same as finitely generated abelian groups.

(2.) Let R be ring with unity 1. Consider $M = R$

$$M = R \cdot 1 = \{ r1 \mid r \in R \} = R$$

Then submodule $N \subseteq R$ needs $r \cdot x \in N$ for each $r \in R$ and $x \in N$ which means N is LEFT IDEAL.

$$N = Ra = \{ ra \mid r \in R \} = (a)$$

cyclic submodules of $M = R$ are principal ideals of R.

cyclic submodules: might have R noncommutative

principal ideals of R: usually assumes R commutative

When R commutative $Ra = aR$ and $RA = RA$ with the natural meaning.

R is PID is commutative integral domain with 1 in which every R-submodule of R is cyclic

Remark: we can trade study of principal ideals for cyclic submodules. Much of this at the moment is just semantics.

Def^n Let R be ring with unity 1 and let $M = R^n$ be the free-R-module of rank n over R, we define $(e_i)_j = \delta_{ij} = \begin{cases} 1 & \text{for } i=j \\ 0 & \text{for } i \neq j \end{cases}$ for $1 \leq i, j \leq n$.

That is $e_1 = (1, 0, \ldots, 0)$ and $e_2 = (0, 1, 0, \ldots, 0)$ etc.

Suppose R is commutative ring and $S = (s_1, s_2, \ldots, s_n) \in R^n$ then calculate,

I don't think this is needed Exercise 2 assumes R commutative to allow field calculation, Ex27 is not a finitely gen. $\mathbb{Z}$-module.

$$\begin{aligned} S &= (s_1, s_2, \ldots, s_n) \\ &= (s_1, 0, \ldots, 0) + (0, s_2, \ldots, 0) + \cdots + (0, \ldots, 0, s_n) \\ &= s_1(1, 0, \ldots 0) + s_2(0, 1, \ldots 0) + \cdots + s_n(0, \ldots, 1) \\ &= \sum_{i=1}^{n} s_i e_i \end{aligned}$$

Proposition: $R\{e_1, \ldots, e_n\} = Re_1 + Re_2 + \cdots + Re_n = R^n$ given R is a ring with unity 1 and $(e_i)_j = \delta_{ij}$ as above.

Even if R is not commutative, we still require that $1r = r = r1$ for all $r \in R$ when R has multiplicative identity 1.

Conjecture: given R with unity 1 and $n \in \mathbb{Z}^+$ if $(e_i)_j = \delta_{ij}$ defines $e_i \in R^n$ then

$$R^n = Re_1 + Re_2 + \cdots + Re_n = e_1R + e_2R + \cdots + e_nR$$

(which is **not** to say that $AR = RA$ for any old A when R non commutative)

Th^m/ Suppose R is commutative and $m, n \in \mathbb{Z}^+$.
$$R^n \cong R^m \iff m = n$$

Proof: ($\Leftarrow$) Suppose $m=n$ then $R^n = R^m$ hence $R^n \cong R^m$ by $Id : R^m \longrightarrow R^n$ which is an R-module isomorphism.

($\Rightarrow$) Suppose R is commutative then recall there exists a maximal ideal I for R and thus $F = R/I$ is a field.

Suppose $R^n \cong R^m$ then

$$\frac{R \times R \times \cdots \times R}{I \times I \times \cdots \times I} \cong \left(R/I\right) \times \left(R/I\right) \times \cdots \times \left(R/I\right)$$

hence $R^n \cong R^m \Rightarrow F^n \cong F^m \Rightarrow n = m$ (by Linear Algebra)

it would be good to expand on why this implication holds.

(3.) $R^m = \text{span}_R\{e_1, e_2, \ldots, e_m\}$, ($R$ commutative)

$R^m = Re_1 + Re_2 + \cdots + Re_m$ is finitely generated R-module with minimal generating set $\{e_1, e_2, \ldots, e_n\}$.

Examples Continued

(4.) F field, V a vector space over F

$T : V \to V$

V forms $F[x]$-module via $\boxed{f(x) \cdot v = f(T)v}$

for all $f(x) \in F[x]$ and all $v \in V$

What does it mean for V to be cyclic $F[x]$-module?

$$V = \{ p(x) \cdot v \mid p(x) \in F[x] \}$$ ← generator v for some $v \in V$

$$= \{ c_0 v + c_1 T(v) + \cdots + c_n T^n(v) \mid c_0, \ldots, c_n \in F, n \in \mathbb{Z}^+ \}$$

$$= \text{Span} \{ T^n(v) \mid n \in \mathbb{Z}, n \geq 0 \}$$

That is $\{ v, T(v), T^2(v), T^3(v), \ldots \}$ is a generating or <u>spanning</u> set over F for V.

(for most $T : V \to V$, V is not a cyclic $F[x]$-module)

E1 $T : \mathbb{R}^3 \to \mathbb{R}^3$ via $T(x, y, z) = (z, x, y)$

$T(e_1) = T(1, 0, 0) = (0, 1, 0) = e_2$

$T(e_2) = T(0, 1, 0) = (0, 0, 1) = T^2(e_1) = e_3$

$T(e_3) = T(0, 0, 1) = (1, 0, 0) = T^3(e_1) = e_1$

Then $\{ e_1, T(e_1), T^2(e_1), \ldots \}$ reduces to $\{ e_1, T(e_1), T^2(e_1) \}$

$\mathbb{R}^3$ is $\mathbb{R}[x]$-cyclic subspace with generator e_1.

(choice of e_1 certainly not unique)

Def^n/ Let $M_1, M_2, \ldots, M_k$ be R-modules. Then $\{(m_1, m_2, \ldots, m_k) \mid m_i \in M_i \text{ for } i = 1, 2, \ldots, k\}$ with component-wise addition and R-action is called the (external) direct product of $M_1, \ldots, M_k$ and we denote it via $M_1 \times M_2 \times \cdots \times M_k = M$

The notation $M_1 \oplus M_2 \oplus \cdots \oplus M_k$ may also be used to denote this external direct sum of modules $M_1, \ldots, M_k$

$$\left[\begin{array}{l} X, Y \in M \text{ then } (X+Y)_i = X_i + Y_i \quad \forall i = 1, 2, \ldots, k \\ \qquad\qquad\quad (rX)_i = rX_i \quad \forall i = 1, \ldots, k, r \in R \end{array}\right]$$

You may recall the following Th^m from its analog in Math 321,

Proposition (5) Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then TFAE

(1.) $\pi : N_1 \times N_2 \times \cdots \times N_k \longrightarrow N_1 + N_2 + \cdots + N_k$ defined by $\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$ is an isomorphism of R-modules.

(2.) $N_j \cap (N_1 + N_2 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_k) = \{0\} \quad \forall j = 1, \ldots, k.$

(3.) Every $x \in N_1 + N_2 + \cdots + N_k$ can be written uniquely in the form

$$x = a_1 + a_2 + \cdots + a_k$$

with $a_i \in N_i$ for $i = 1, 2, \ldots, k$.

Def^n/ When $M = N_1 + \cdots + N_k$ and (1.) or (2.) or (3.) hold then $M = N_1 \oplus \cdots \oplus N_k$ is internal direct sum of $N_1, \ldots, N_k$

Remark: to say $M = N_1 \oplus N_2 \oplus \cdots \oplus N_k$ for submodules $N_1, N_2, \ldots, N_k$ of the R-module M means $M \cong N_1 \times N_2 \times \cdots \times N_k$ (1.). In other words, the modules $N_1, \ldots, N_k$ are *independent* (2.)

When $M = N_1 \oplus N_2 \oplus \cdots \oplus N_k$ then we can uniquely decompose M into independent components; $x \in M$ then $\exists!\ a_1 \in N_1, \ldots, a_k \in N_k$ s.t. $x = a_1 + \cdots + a_k$.

We're injected some of the language below into previous def^n's where the word "rank" appeared. Good news, it conforms to the def^n below:

Def^n An R-module F is said to be *free* on the subset A of F if for every nonzero $x \in F$ there exist *unique nonzero* $r_1, r_2, \ldots, r_n \in R$ and *unique* $a_1, a_2, \ldots, a_n \in A$ for which

$$x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$$

for $n \in \mathbb{Z}^+$. In this case we say A is a *basis* or set of *free generators* for F. If R is a commutative ring then cardinality of A is rank of F

E2 $N_1 = N_2 = \mathbb{Z}_2$ over $\mathbb{Z}_2$ gives free module $N_1 \times N_2$ of rank 2 with basis $\{(1,0), (0,1)\}$

E3 $N_1 = N_2 = \mathbb{Z}_2$ over $\mathbb{Z}$ is not free $\mathbb{Z}$-module when we think about $N_1 \times N_2$. $(a_1, a_2) = (a_1, 0) + (0, a_2)$

continued ?

E3 $M = \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2 e_1 + \mathbb{Z}_2 e_2$

thus M finitely generated as $\mathbb{Z}$-module by $A = \{(1,0),(0,1)\} = \{e_1, e_2\}$.

Indeed $M = \mathbb{Z}_2 e_1 \oplus \mathbb{Z}_2 e_2 = N_1 \oplus N_2$ $\left(N_1 = \mathbb{Z}_2 e_1,\ N_2 = \mathbb{Z}_2 e_2\right)$

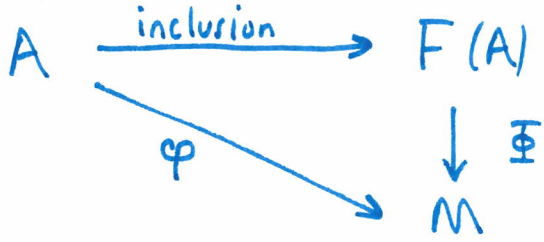
However, A is <u>not a basis</u>

for M as a $\mathbb{Z}$-module. For example,

$$x = (1,1) = (3,11) = \underbrace{3\cdot(1,0) + 11\cdot(0,1)}_{r_1 = 3,\ r_2 = 11} = \underbrace{1\cdot(1,0) + 1\cdot(0,1)}_{r_1 = 1,\ r_2 = 1}$$

$$x = (1,1) = \underbrace{(1,0)}_{a_1} + \underbrace{(0,1)}_{a_2} \qquad a_1 \in N_1 = \mathbb{Z}_2 e_1,\quad a_2 \in N_2 = \mathbb{Z}_2 e_2$$

Thm (6) For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following universal property: if M is any R-module and $\varphi : A \longrightarrow M$ is any map of sets, then $\exists!$ R-module homomorphism $\Phi : F(A) \longrightarrow M$ such that $\Phi(a) = \varphi(a)$ for all $a \in A$, that is the following diagram commutes,



When A is the finite set $\{a_1, a_2, .., a_n\}$ then $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.

Proof: see p. 354 – 355, hopefully we work through in-class.

Corollary 7

(1.) If F_1 & F_2 are free modules on A, there is a unique isomorphism between F_1 & F_2 which is the identity map on A.

(2.) If F is any free R-module with basis A then $F \cong F(A)$. In particular, F enjoys same universal property as $F(A)$ in Thm 6

"extend linearly" → for free module F over R with basis A, we can define R-mod. homomorphism from F into M by fixing values for A.

Th^{n} (6) For any set A there exists a free R-module $F(A)$ which satisfies the following universal property

If M is any R-module and $\varphi: A \to M$ is any map of sets then $\exists!$ R-module homomorphism $\Phi: F(A) \to M$ such that $\Phi(a) = \varphi(a)$ $\forall a \in A$.

Proof: Let $F(A) = \{0\}$ in the case $A = \emptyset$. Otherwise $A \neq \emptyset$ and $\exists a \in A$. Construct

$$F(A) = \{ f: A \to R \mid f(a) = 0 \ \forall \text{ but finitely many } a \in A \}$$

Define R-module structure on $F(A)$ by

$$(f+g)(a) = f(a) + g(a)$$
$$(rf)(a) = r f(a)$$

for all $a \in A$ and $r \in R$, we see $f+g, rf \in F(A)$ since these also have only finitely many nonzero values. Let

$$f_a(x) = \delta_{a,x} = \begin{cases} 1 & \text{for } a = x \\ 0 & \text{for } a \neq x \end{cases}$$

Suppose f takes value r_i at a_i for $i = 1, 2, .., n$ then

$$f = r_1 f_{a_1} + r_2 f_{a_2} + \cdots + r_n f_{a_n}$$

Notice the selection of $r_1, r_2, .., r_n$ is unique to given f. Identifying $a \in A$ with f_a we find $F(A)$ is free on $\{ f_a \mid a \in A \}$

Suppose $\varphi: A \to M$ is map into R-module M, define

$$\Phi: F(A) \to M \quad \text{by} \quad \Phi\left(\sum_{i=1}^{n} r_i f_{a_i} \right) = \sum_{i=1}^{n} r_i \varphi(a_i)$$

$$\Phi\left(r \left(\sum_{i=1}^{n} r_i f_{a_i} \right) \right) = \Phi\left(\sum_{i=1}^{n} r r_i f_{a_i} \right) = \sum_{i=1}^{n} r r_i \varphi(a_i) = r \sum_{i=1}^{n} r_i \varphi(a_i)$$
$$= r\, \Phi\left(\sum_{i=1}^{n} r_i f_{a_i} \right).$$

Additivity of Φ proved similarly. Note,

$$\Phi(f_{a_i}) = \varphi(a_i) \quad \text{hence } \Phi(a) = \varphi(a) \text{ provided}$$

we identify a with f_a. Uniqueness follows since values of Φ on A fix the necessary output on $F(A)$ for Φ on R-mod. homom. //