November 22, hours 29-30: Proof of the Structure Theorem - Existence

November-20-11
12:22 PM

IT2C2W: [M f.g./R PID $\Rightarrow M \cong R^k \oplus \bigoplus R/\langle p_i^{s_i}\rangle$]

$\Rightarrow$ structure of f.g. Abelian groups, J.C.F.

Goal: The existence part, the "ring" of modules.

Read Along: You tell me!

Let R be a PID...

Sketch $\{\text{matrices}\}/\text{row \& col. ops \& more} \xrightarrow{\text{onto}} \{\text{f.g. modules}\}$

finite by infinite, but the infinity is just a nuisance.

So we're back to Gaussian elimination!

Def M is "finitely generated" if $\exists\, g_1 \dots g_n \in M$ s.t. $M = \{\sum a_i g_i : a_i \in R\}$.

$$R^X \xrightarrow{A} R^g \xrightarrow{\pi} M \qquad \ker \pi = \langle r_x : x \in X\rangle$$

$$A = \underbrace{\left(\qquad\qquad\right)}_{X}\}g \qquad A \in M_{gX}(R)$$

... In general, every $g \times X$ matrix determined a f.g. module, and every f.g. modules arises in this way.

Exercise. If $C = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B\end{array}\right)$, then $M_C = M_A \oplus M_B$

$$\begin{array}{ccc} R^X & \xrightarrow{A} & R^g \\ \uparrow Q & \circlearrowleft & \downarrow P \\ R^X & \xrightarrow{A'} & R^g \end{array}$$

Claim if P, Q are invertible on the left, then $M = R^g/\operatorname{im} A$ and $M' = R^g/\operatorname{im} A'$ are isomorphic.

Pf $\Phi: M \to M'$ by $[\alpha]_{\operatorname{im} A} \to [P\alpha]_{\operatorname{im} A'}$

P can be interpreted as $g \times g$ matrix
Q can be interpreted as an $X \times X$ column-finite matrix; $A' = PAQ$

.... Can do arbitrary, ~~row~~ invertible row operations on A, and arbitrary invertible column ops, provided each column is touched finitely many times.

Of all the matrices reachable from A, let A' be the one having an entry with the smallest D-H norm; wlog, that entry is a_{11}.

Claim a_{11} divides all other entries in its row & column.

Pf 1 For a Euclidean domain.

Pf 2 In a PID, if $q = \gcd(a,b) = sa + tb$, then

$$(a \ b)\begin{pmatrix} s & -b/q \\ t & a/q \end{pmatrix} = (q \ 0), \text{ while } \begin{pmatrix} s & -b/q \\ t & a/q \end{pmatrix}^{-1} = \begin{pmatrix} a/q & b/q \\ -t & s \end{pmatrix} \quad \square$$

$\Longrightarrow$ W.l.o.g, the row & column of a_{11} are 0 (except for a_{11})

$\Longrightarrow$ all entries of A are divisible by a_{11}:

$$A = \begin{pmatrix} a_{11} & \text{---} \ 0 \ \text{---} \\ 0 & \\ \vdots & A_1 \ \substack{\text{all entries} \\ \text{divisible} \\ \text{by } a_{11}} \\ 0 & \end{pmatrix}$$

Continue to get $A \sim \left(\begin{array}{cc|c} a_{11} & & \\ & a_{22} & 0 \\ \hline & 0 & 0 \end{array}\right)$ (w.l.o.g., A is square) continue to get $A \sim \left(\begin{array}{c|c} \ddots & 0 \\ \hline 0 & 0 \end{array} \right)$ (is square)

So $M \cong \bigoplus_{i=1}^{g} R/\langle a_{ii} \rangle \cong R^k \oplus \bigoplus R/\langle a_i \rangle$

$a_1 | a_2 | \dots | a_n$

Claim. If $\gcd(a,b)=1$ $\quad 1 = sa+tb$ [e.g., if R is a PID]

then $\frac{R}{\langle a \rangle} \oplus \frac{R}{\langle b \rangle} \cong \frac{R}{\langle ab \rangle}$.

Aside: $\mathbb{Z}/_7 \oplus \mathbb{Z}/_{11} \oplus \mathbb{Z}/_{13} \cong \mathbb{Z}/_{77} \oplus \mathbb{Z}/_{13} \cong \mathbb{Z}/_{1,001}$

"the chinese remainder theorem"

Proof 1. as before, use

$$\begin{array}{ccccc} R/\langle a \rangle & \xrightarrow{t \cdot b} & & \xrightarrow{1} & R/\langle a \rangle \\ & & R/\langle ab \rangle & & \oplus \\ R/\langle b \rangle & \xrightarrow{s \cdot a} & & \xrightarrow{1} & R/\langle b \rangle \end{array} \quad \square$$

Proof 2. Using the techniques above, $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix}$. $\square$ $\quad \square$

done line

Recall that $(R\text{-mod}, \oplus)$ is an "Abelian group" (really, an Abelian semi-group, and even this is not precise)

Tensor Products. Given M, N

$$M \otimes_R N := \left\{ \sum_{i=1}^{n} a_i (m_i \otimes n_i) : n \in \mathbb{N}, a_i \in R \right\} \Big/ \begin{array}{l} (am) \otimes n = a(m \otimes n) = m \otimes (an) \\ (m_1+m_2) \otimes n = \dots \\ m \otimes (n_1+n_2) = \dots \end{array}$$

$\uparrow$ bilinear

$M \times N$

Example. $\dim V \otimes W = (\dim V) \cdot (\dim W)$

Example. If $q \in \gcd(a,b)$, $q = sa+tb$, $\quad \frac{R}{\langle a \rangle} \otimes \frac{R}{\langle b \rangle} \cong \frac{R}{\langle q \rangle}$

pf. $[r_1]_a \otimes [r_2]_b \longrightarrow [r_1 \cdot r_2]_q \qquad [q] \otimes [1] = [sa+tb] \otimes [1] = 0$

$[r]_q \longrightarrow [r]_a \otimes [1]_b \qquad [r_1 r_2] \otimes [1] = [r_1][r_2]$

theorem. $(R\text{-mod}, \oplus, \otimes)$ is a "ring".

theorem. $(M,N) \longmapsto M \otimes N$ is a "bifunctor".