14-1100 Nov 10, hours 26-27: Modules, Main Theorem - Existence

November-09-14 10:27 AM

Office Hour this week Wed $1^{30}-2^{30}$ (not at 2^{30})

Global goal: IT3C4W M f.g. module over a PID $R \Rightarrow$ Uniquely
$M \cong R^k \oplus \bigoplus R/(p_i^{s_i})$ p_i prime, $s_i \geq 1$

Cor 1. A f.g. Abelian $\Rightarrow A \cong \mathbb{Z}^k \oplus \bigoplus \mathbb{Z}/p_i^{s_i}$

Cor 2. $A \in M_{n\times n}(\mathbb{C})$ has a "Jordan form"

Today. Further dull technicalities, then proof of existence side of Thm.

Euc $\Rightarrow$ PID $\Rightarrow$ UFD.
Many UFD's are not PID's.

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ is a PID but is not Euclidean.

Theorem. R is a PID iff it has a "Dedekind-Hasse" norm: $d: R-\{0\} \to \mathbb{N}_{>0}$ [or add $d(0)=0$]
s.t. if $a,b \neq 0$ either $a \in \langle b\rangle$ or $\exists 0 \neq x \in \langle a,b\rangle$ w/ $d(x) < d(b)$.

Pf. $\Leftarrow$ as before. $\Rightarrow$ Replace every prime by 2, get even a "multiplicative" D-H norm.

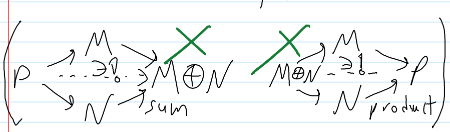
Reminder. Modules.

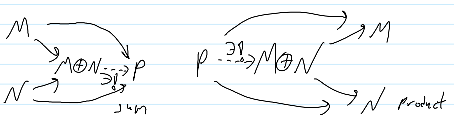
Def/Claim. R-mod & mod-R are categories.

Def/claim. Submodules, $\ker\phi$, $\operatorname{im}\phi$, M/N

Boring Theorems. 1. $\phi: M \to N \Rightarrow M/\ker\phi \cong \operatorname{im}\phi$
2. $A, B \subset M \Rightarrow \frac{A+B}{B} \cong A/A\cap B$
3 $A \subset B \subset M \Rightarrow {}^{M/A}\!/_{B/A} \cong M/B$
4. Also dull.

Direct sums. $M, N \Rightarrow M \oplus N$





differ for infinite families!

$\operatorname{Hom}\left(\bigoplus^n N_j, \bigoplus^m M_i\right) = \left\{\begin{pmatrix} a_{11} & a_{1n} \\ a_{m1} & a_{mn}\end{pmatrix} : a_{ij} \in \operatorname{Hom}(M_i, N_j)\right\}$

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

(d ca) (!)

PM. I should have done $l = \mathrm{lcm}$, $g = \gcd$
$\frac{R}{\langle a\rangle} \oplus \frac{R}{\langle b\rangle} \cong \frac{R}{\langle g\rangle} \oplus \frac{R}{\langle l\rangle}$

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

$$\frac{R}{\langle a\rangle}\oplus\frac{R}{\langle b\rangle}\cong\frac{R}{\langle ab\rangle} \text{ via } \begin{tikzcd} R/\langle a\rangle \oplus R/\langle b\rangle \arrow[r, "(tb\ \ sa)"] & R/\langle ab\rangle \arrow[r, "\binom{1}{1}"] & R/\langle a\rangle \oplus R/\langle b\rangle \end{tikzcd}$$

$$\mathbb{Z}/7\oplus\mathbb{Z}/11\oplus\mathbb{Z}/13\cong\mathbb{Z}/77\oplus\mathbb{Z}/13\cong\mathbb{Z}/1{,}001$$ "the chinese remainder theorem"

PM. I should have done $1 = \mathrm{lcm}$

$$\frac{R}{\langle a\rangle}\oplus\frac{R}{\langle b\rangle}\cong\frac{R}{\langle g\rangle}\oplus\frac{R}{\langle l\rangle} \qquad g=\gcd$$

in a way compatible w/ $\frac{R}{\langle ab\rangle}\to\frac{R}{\langle a\rangle}\oplus\frac{R}{\langle b\rangle}$ by $\binom{1}{1}$ in the case of $\gcd=1$.

Let R be a PID...

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

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. $M=\left\{\sum a_i g_i : a_i\in R\right\}$.

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

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

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

PM. I should have gone
1. $M_{n\times m} \longrightarrow$ modules w/ n gens & m rels.
2. $M_{n\times X} \longrightarrow$ f.g. modules
3. The above is surjective.

Examples. (1), (a), (0)

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

done line

Comment. May add/remove 0 columns.

$$\begin{tikzcd} R^X \arrow[r, "A"] & R^g \arrow[d, "P"] \\ R^X \arrow[u, "Q"] \arrow[r, "A'"] & R^g \end{tikzcd}$$

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 $[\alpha]_{\operatorname{im}A}\longrightarrow[P\alpha]_{\operatorname{im}A'}$

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

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

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

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

$\Rightarrow$ 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)

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

$a_1 \mid a_2 \mid \dots \mid a_n$