14-1100 Nov 6, hour 25: Finish rings, start modules

November-06-14 9:10 AM

HW. HW3 due, HW4 on web

Riddle along: A game: Player A writes the numbers 1-18 on the faces of three blank dice, to her liking. Player B takes one of the 3 dice. Player B takes one of the remaining two, and throws away the third. Player A and B then play 1,000 rounds of "dice war" with the dice they hold. Whom would you rather be, player A or player B?

Global goal: IT3C4W: M f.g. module over a PID $R \Rightarrow$ Uniquely

$$M \cong R^k \oplus \bigoplus R/(p_i^{s_i}) \qquad p_i \text{ prime},\ s_i \geq 1$$

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. Finish rings, start modules.

Reminders. Euc $\Rightarrow$ PID $\overset{?}{\Rightarrow}$ UFD

---

theorem. PID $\Rightarrow$ UFD.

Weak proof. Take $x = x_1$; unless $x_1 \in R^\times$, $x_1 \in M_1$ where M_1 is a maximal ideal containing $\langle x_1 \rangle$. $M_1 = \langle p_1 \rangle$, p_1 prime. So $x_1 = p_1 x_2$; unless $x_2 \in R^\times$ $x_2 \in \langle x_3 \rangle \subset M_2$ maximal $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3, \ldots$ if process was infinite,

$$\langle x_1 \rangle \subsetneq \langle x_2 \rangle \subsetneq \langle x_3 \rangle \subsetneq \cdots$$

$\langle x_n \rangle \subset \langle x_{n+1} \rangle$ as $x_n = p_n x_{n+1}$
if $x_{n+1} \in \langle x_n \rangle$, $x_{n+1} = a x_n$ so
$x_n = p_n a x_n$ & p's not prime.

But a PID is "Noetherian", so the process must terminate.

So $x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \cdots = p_1 p_2 \ldots p_n u$

theorem. In a PID $\langle a, b \rangle = \langle \gcd(a,b) \rangle$. (so $\gcd(a,b) = sa + tb$)

The Euclidean Algorithm. In a Euc. Domain, a practical algorithm for finding $s(a,b)$ & $t(a,b)$ as above: WLOG, $e(a) \geq e(b)$

If $\langle a, b \rangle = \langle b \rangle$, take $(s,t) = (0,1)$. Otherwise $a = bq + r$, $e(r) < e(b)$,

$\langle a,b\rangle = \langle b,r\rangle$ so if $g = s'b + t'r$, then

$$g = s'b + t'(a-bq) = \underbrace{t'}_{s}\, a + \underbrace{(s'-t'q)}_{t}\, b$$

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.

skipped.

---

target line

Definition. An R-module: "A vector space over a ring".

Examples. 1. V.S. over a field.

2. Abelian groups over $\mathbb{Z}$.

3. Given $T: V \to V$, V over $F[x]$.

4. Given ideal $I \subset R$, R/I over R.

5. Column vectors R^n over $M_{n\times n}$ (Left module R-mod)
   row vectors $(R^n)^T$ over (right module mod-R)

---

done line

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. $A, B \subset M \Rightarrow \dfrac{A+B}{B} \cong \dfrac{A}{A\cap B}$

3. $A \subset B \subset M \Rightarrow \dfrac{M/A}{B/A} \cong M/B$

4. Also dull.

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

$$\begin{tikzcd} M \arrow[dr] \arrow[drr, bend left] & & \\ & M\oplus N \arrow[r, dashed, "\exists!"] & P \\ N \arrow[ur] \arrow[urr, bend right] & & \end{tikzcd} \quad \text{sum}$$

$$\begin{tikzcd} & & M \\ P \arrow[r, dashed, "\exists!"] \arrow[urr, bend left] \arrow[drr, bend right] & M\oplus N \arrow[ur] \arrow[dr] & \\ & & N \end{tikzcd} \quad \text{product}$$

$$\left(\begin{tikzcd} & M \arrow[dr] & \\ P \arrow[ur] \arrow[dr] \arrow[rr, dashed, "\exists!"] & & M\oplus N \\ & N \arrow[ur] & \end{tikzcd} \text{ sum} \qquad \begin{tikzcd} & M \arrow[dr] & \\ M\oplus N \arrow[ur] \arrow[dr] \arrow[rr, dashed, "\exists!"] & & P \\ & N \arrow[ur] & \end{tikzcd} \text{ product}\right)$$

differ for infinite families!

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

Example: $\dim(V \oplus W) = \dim V + \dim W$.

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

$$\frac{R}{\langle a\rangle} \oplus \frac{R}{\langle b\rangle} \cong \frac{R}{\langle ab\rangle} \quad \text{via}$$

$$\begin{tikzcd}
R/\langle a\rangle \arrow[dr, "t\cdot b"] & & R/\langle a\rangle \\
\oplus & R/\langle ab\rangle \arrow[ur, "1"] \arrow[dr, "1"'] & \oplus \\
R/\langle b\rangle \arrow[ur, "s\cdot a"'] & & R/\langle b\rangle
\end{tikzcd}$$

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