

HW. HW3 due, HW4 on wed

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: M f.g. module over a PID $R \Rightarrow$ Uniquely
 IT3C4W
 $M \cong R^k \oplus \bigoplus R/(p_i^{s_i})$ 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. Finish rings, start modules.

Reminders. Euc \Rightarrow PID $\not\Rightarrow$ UFD

theorem. PID \Rightarrow UFD.

What proof. Take $x = x_1$ unless $x_1 \in R^\times$, $x_1 \in M_1$ where M_1 is a maximal ideal containing $\langle x \rangle$. $M_1 = \langle p_1 \rangle$,

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 $M_2 = \langle p_2 \rangle$, $x_2 = p_2 x_3, \dots$ if process was infinite,

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

But a PID is "Noetherian",

so the process must terminate.

$$\text{So } x = x_1 = p_1 x_2 = p_1 p_2 x_3 = \dots = p_1 p_2 \dots p_n u$$

$\langle x_n \rangle \subset \langle x_{n+1} \rangle$ 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.

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, $\ell(a) \geq \ell(b)$

If $\langle a, b \rangle = \langle b \rangle$, take $(s, t) = (0, 1)$. Otherwise

$$a = bq + r, \ell(r) < \ell(b),$$

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

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

Theorem. R is a PID iff it has a "Dedekind-Hasse" norm: $d: R - \{0\} \rightarrow \mathbb{N}_{>0}$ [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/ $d(x) < d(b)$.

skipped.

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

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 $T: V \rightarrow V$, 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 $M_{n \times n}$ (right module $\text{mod-}R$)

done
line

Def/claim. R -mod & $\text{mod-}R$ are categories.

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

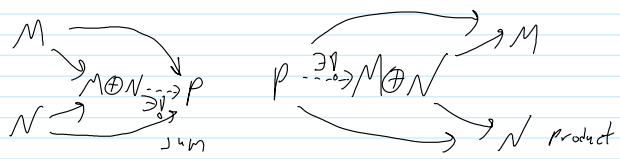
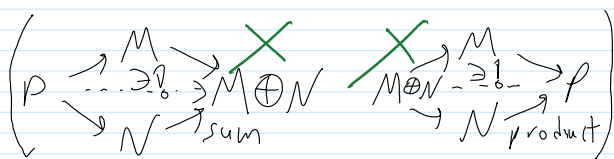
Basic Theorems. 1. $\phi: M \rightarrow N \Rightarrow M/\ker \phi \cong \text{im } \phi$

2. $A, B \subset M \Rightarrow A+B/B \cong A/A \cap B$

3. $A \subset B \subset M \Rightarrow M/A/B/A \cong M/B$

4. Also dual.

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



differ for infinite families!

$$\text{Hom}(\bigoplus N_i, \bigoplus M_i) = \left\{ \begin{pmatrix} \dots & \dots \\ a_{1j} & a_{2j} \\ \dots & \dots \end{pmatrix} : a_{ij} \in \text{Hom}(M_i, N_j) \right\}$$

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

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

$$\frac{R}{\langle a \rangle} \oplus \frac{R}{\langle b \rangle} \cong \frac{R}{\langle ab \rangle} \quad \text{via} \quad \begin{array}{ccc} R/\langle a \rangle & \xrightarrow{t \cdot b} & R/\langle ab \rangle & \xrightarrow{1} & R/\langle a \rangle \\ \oplus & & & & \oplus \\ R/\langle b \rangle & \xrightarrow{s \cdot a} & R/\langle ab \rangle & \xrightarrow{1} & R/\langle b \rangle \end{array}$$

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