14-1100 Oct 27, hours 20-21: Rings, Cayley-Hamilton, quotients and isomorphism theorems

October-10-14 1:09 PM

HW3 2 questions added!

Riddle Along $\boxed{1}\ \boxed{2}\ \boxed{3}\ \boxed{4}\ \boxed{5}\ \boxed{6}\ \boxed{7}\ \boxed{8}\ \boxed{9}$

Two players alternate drawing cards from the above deck. The first player to have 3 cards that add up to 15, wins. Would you like to be the first to move or the second?

Reminders 1. Rings: $(R, +, \times, 0 \neq 1)$

2. $R[x]$, $M_{n\times n}(R)$, RG

3. Morphisms (make rings a "category") $\boxed{F(1)=1}$

Further examples.

1. If $\varphi: G \to H$, $\varphi_*: RG \to RH$
2. $M_{n\times n}(R[x]) \cong M_{n\times n}(R)[x]$

Cayley-Hamilton A matrix annihilates its characteristic poly: Let $A \in M_{n\times n}(R)$, R commutative. Set

$\chi_A(t) = \det(tI - A)$. Then $\chi_A(A) = 0$

Wrong proof. $\chi_A(A) = \det(AI - A) = \det(0) = 0$

Nonsense! Would have worked for trace just as well! $\chi_A^{tr} = tr(tI-A) = nt - tr(A)$

So $A = \frac{trA}{n} I$

The issue:

$$\begin{array}{ccc} M_{n\times n}(R)[t] & \xrightarrow{\det} & R[t] \\ \downarrow ev_A & & \downarrow ev_A \\ M_{n\times n}(R) & \xrightarrow{?} & M_{n\times n}(R) \end{array}$$

not mentioned.

Right proof.

in $M_{n\times n}(R[t])$ in $M_{n\times n}(R)[t]$

$\det(tI-A)\cdot I = adj(tI-A)(tI-A) = (\sum B_i t^i)(tI-A)$ in

now substitute $t=A$. The B_i's commute with A because $(tI-A)\,adj(tI-A) = adj(tI-A)(tI-A)$.

See 2015-12

---

im, subring, ker, ideal. (ideals are subrings but never subrings)

Q. Is every proper ideal a kernel?

Ans. Define R/I.

Example. $\mathbb{R}[x]/\langle x^2+1\rangle = R_1$

The Isomorphism Theorems. 1. $\varphi: R \to S \Rightarrow R/\ker\varphi = \operatorname{im}\varphi$.

(Example: $ev_i : \mathbb{R}[x] \to \mathbb{C} \Rightarrow R_1 \cong \mathbb{C}$)

done line

2. $\frac{A+I}{I} \cong A/A\cap I$ $A \subset R$ subring, $I \subset R$ proper ideal.

3. $I \subset J \subset R$ ideals $\Rightarrow \frac{R/I}{J/I} \cong R/J$

4. Given an ideal I of R, there's a bijection between ideals $I \subset J \subset R$ & ideals of R/I.

From this point, our goal is "modules over PID"

Better Rings. 1. The ultimate:

Field [commutative, $F \setminus \{0\}$ a group]

("division ring", if not commutative

Example: $\mathbb{H} = \{a+bi+cj+dk\}/\begin{matrix} i^2=j^2=k^2=-1 \\ ij=k \end{matrix}$

useful for 3D rotations, etc...)

[almost all of high-school & freshman algebra carries through]

2. (Integral) domains: commutative, has no 0-divisors.

How make? For ideals which, R/I is a field or a domain?

.... from now on, R is commutative.

Maximal Ideals. 1. Definition.

2. $I \subset R$ is maximal $\iff R/I$ is a field.

Fishy proof: Use the 4th isomorphism theorem.

Honest proof: $\Rightarrow$: $x \notin I \Rightarrow Rx + I = R \Rightarrow \exists y \in R\ yx + I = 1 + I$

$\Leftarrow$ $J \supsetneq I$, $x \in J \setminus I \Rightarrow [x]_I \neq 0 \Rightarrow \exists y\ xy - 1 \in I \Rightarrow 1 \in J$

Examples. 1. $p\mathbb{Z}$ is a maximal ideal in $\mathbb{Z}$.

2. $S = \ell^\infty = \{\text{bndd seq's in } \mathbb{R}\}$ $A_n = \{(a_i) : a_n = 0\}$

Fishy **Theorem.** Every ideal is contained in a maximal ideal.

Proof using Zorn's Lemma.

Theorem There exists a function

$\mathrm{Lim} : \{\text{bndd seq's in } \mathbb{R}\} \to \mathbb{R}$ s.t.

1. If (a_n) is convergent, $\lim a_n = \mathrm{Lim}\, a_n$.
2. $\mathrm{Lim}(a_n + b_n) = \mathrm{Lim}(a) + \mathrm{Lim}(b_n)$
3. $\mathrm{Lim}(a_n b_n) = \mathrm{Lim}(a_n) \cdot \mathrm{Lim}(b_n)$

+ more....

Proof. $S = \{\text{bndd seq's in } \mathbb{R}\}$ $I = \{(a_n) : a_n \neq 0 \text{ for finitely many } n\text{'s}\}$

J - a maximal ideal containing I.

$\mathrm{Lim} : S \to S/J \underset{?}{=} \mathbb{R}$

Prime Ideals. 1. Definition $P \subset R$ is prime if $ab \in P$ $\Rightarrow a \in P$ or $b \in P$.

2. Theorem. R/P is a domain iff P is prime.

Proof $\Rightarrow$ $ab \in P \Rightarrow [ab] = 0 \Rightarrow [a][b] = 0 \Rightarrow$ $[a]=0 \Rightarrow a \in P$ or $[b]=0 \Rightarrow b \in P$.

$\Leftarrow$ $[a][b] = 0 \Rightarrow [ab] = 0 \Rightarrow ab \in P \Rightarrow$ $a \in P \Rightarrow [a]=0$ or $b \in P \Rightarrow [b]=0$

Theorem. A maximal ideal is prime.

target line

From this point on, R is a commutative integral domain.

Primes. 1. $a|b$ $[a \neq 0, \exists q \text{ s.t. } aq = b]$ $(a|b \wedge b|a \Rightarrow a = ub)$ "a, b are associates"

2. $\gcd(a,b) = q$; $\gcd = q$ & $\gcd = q' \Rightarrow q' = uq$.

3. Primes: $p \neq 0$ non-unit $p|ab \Rightarrow p|a$ or $p|b$

p is prime iff $\langle p \rangle$ is prime ideal.

4. Irreducible $x = ab \Rightarrow a \in R^* \vee b \in R^*$

Claim. prime $\Rightarrow$ irreducible

$p = ab \Rightarrow p|a \Rightarrow a = pc$

$\Rightarrow p = pcb \Rightarrow cb = 1 \Rightarrow b \in R^*$

Counterexample: in $\mathbb{Z}[\sqrt{-5}]$, 2 is irrd (for norm reasons) but not prime, as $2 \mid (1-\sqrt{-5})(1+\sqrt{-5}) = 6$

UFDs. Def. Every non-zero element can be factored into primes.

Thm. Uniqueness up to units & a permutation.

Thm. In a UFD, prime $\Leftrightarrow$ irreducible.

pf If an irrd. is decomposed, the decomposition must have length 1.

Thm. UFD $\Longleftrightarrow$ every $x \neq 0$ has a unique decomposition into irreducibles.

Pf need irred $\Rightarrow$ prime. If x is irred & $x | ab$, then $zx = \underbrace{a_1 \ldots a_n b_1 \ldots b_m}_{\text{irreds}} \Rightarrow x \sim a_i$ or $x \sim b_j \Rightarrow x|a \vee x|b$

Thm. In a UFD gcd's always exist.