14-1100 Oct 30, hour 22: The isomorphism theorems for rings, "better rings"

October-10-14 1:09 PM

Reminders Ideal: $0 \in I$, $I+I \subset I$, $-I \subset I$, $RI \subset I$, $IR \subset R$

R/I, Iso 1: Given $\varphi: R \to S$, $R/\ker\varphi \cong \operatorname{im}\varphi$

---

2. $\frac{A+I}{I} \cong \frac{A}{A \cap I}$ $A \subset R$ 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, $F\setminus\{0\}$ of 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.

Example. $S = \{\text{bndd seq's in } \mathbb{R}\}$ $I = \{(a_n) : a_n \to 0\}$ [$a_n = 0$ a.e. is enough]

J - a maximal ideal containing I.

Lin: $S \to S/J = \mathbb{R}$ [$\mathbb{R} \to S/J$ is obvious;

$\mathrm{Lim}: S \to S/J = \mathbb{R}$? [$\mathbb{R} \to S/J$ is obvious; the other direction is not]

Theorem Lim satisfies:

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.... □

done line

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.

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

target line

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 irred (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 irred. is decomposed, the decomposition must have length 1.

Thm. UFD $\Leftrightarrow$ every $x \neq 0$ has a unique decomposition

PF next irred $\Rightarrow$ prime. If x is irred & $x|ab$, then

into irreducibles. $x = a_1 \cdots a_n b_1 \cdots b_m$ (a_i, b_j irreds) $\Rightarrow x \sim a_i$ or $x \sim b_j \Rightarrow x \mid a \vee x \mid b$

Thm. In a UFD gcd's always exist.