Rings I

Monday, August 5, 2024

(Two-sided) Ideals are exactly the kernels of ring homomorphisms

$I \subseteq R$

$0 \in I$

$a, b \in I \Rightarrow a+b \in I$

$\left[\begin{array}{l} a \in I,\ b \in R \Rightarrow ab \in I \\ \text{(right-ideal)} \end{array}\right.$

$\varphi : R \to S$

$\ker \varphi = \{x \in R : \varphi(x) = 0\}$ is an ideal

Conversely, $I = \ker(R \to R/I)$

F is a field, $M_n(F) = n \times n$ matrices over F

Show $M_n(F)$ has no nontrivial two-sided ideals.

Suppose I is a nontrivial two-sided ideal

Then we can find $0 \neq M \in F$.

$$\begin{bmatrix} 1_{(i,i)} \end{bmatrix} \underbrace{\begin{bmatrix} \sim \boxed{M_{ij} \neq 0} \sim \end{bmatrix}}_{M} \begin{bmatrix} 1_{(j,j)} \end{bmatrix} = \begin{bmatrix} 0 & M_{ij} & 0 \\ & 0 & \end{bmatrix} \in I$$

- rescale by $\begin{bmatrix} 1/M_{ij} & & \\ & \ddots & \\ & & 1/M_{ij} \end{bmatrix}$ to make $\begin{bmatrix} 1 \end{bmatrix}$
- multiply by permutation matrices to make $\begin{bmatrix} 1 & & \\ & 0 & \\ & & \ddots & \\ & & & 0 \end{bmatrix}, \begin{bmatrix} 0 & & \\ & 1 & \\ & & 0 \\ & & & \ddots & 0 \end{bmatrix}, \cdots \begin{bmatrix} 0 & & \\ & 0 & \\ & & \ddots & \\ & & & 0 & \\ & & & & 1 \end{bmatrix}$
- add to get $\begin{bmatrix} 1 & & \\ & 1 & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$
- multiply by any matrix to get every element of $M_n(F)$.

What can you say about ring homomorphisms $M_n(F) \to R$?

Kernel is either 0 or $M_n(F)$

0: so $M_n(F) \to R$ injective.

$M_n(F)$: impossible

$m, n \geq 1$ integers $(x^m - 1, x^n - 1)$ in $\mathbb{Z}[x]$ is principal.

$m, n \geq 1$ integers

Show that $(x^m - 1, x^n - 1)$ in $\mathbb{Z}[x]$ is principal.

Suppose $m \geq n$. Then $x^m - 1 = x^{m-n}(x^n - 1) + x^{m-n} - 1$

Then $(x^m - 1, x^n - 1) = (x^{m-n} - 1, x^n - 1)$

Repeat until the smaller exponent reaches 0.

$$\cdots = (x^k - 1, x^0 - 1)$$
$$= (x^k - 1, 0) = (x^k - 1).$$

Fields $\subsetneq$ Euclidean Domains $\subsetneq$ Principal ideal domains

Fields (every nonzero element has a multiplicative inverse)

Euclidean Domains: $a, b \in R$, $b \neq 0$, $a = qb + r$, $N(r) < N(b)$

Principal ideal domains: Every ideal is principal

$\subsetneq$ UFDs: Every nonzero element is uniquely a product of irreducible elements

uniquely: up to rearrangement and multiplying by units

$\subsetneq$ Integral domains (if $ab = 0$ then $a = 0$ or $b = 0$)

$R = \{a + 3bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$

Show R is a subring of $\mathbb{C}$,

R is an integral domain

R is not a UFD.

$\to$ $(a+3bi)(c+3di) = (ac - 3bd) + 3(ad+bc)i \in R$

$\to$ $R \subseteq \mathbb{C}$ and $\mathbb{C}$ is an integral domain

$\to$ Strategy: $(a+3bi)(a-3bi) = a^2 + 9b^2 =$ different factorization

Eg., $a = 4$, $b = 1$.

$$(4+3i)(4-3i) = 25 = 5 \cdot 5$$

Check: That $4 \pm 3i, 5$ are irreducible

Check: That $4 \pm 3i, 5$ don't differ by a unit

$\to$ If $5 = xy$, $25 = |5|^2 = |x|^2 |y|^2$

or $4 \pm 3i = xy$, $25 = |4 \pm 3i|^2 = |x|^2 |y|^2$

But $|x|^2 \neq 5$ since $a^2 + 9b^2 = |a+3bi| \neq 5$

If $|x|^2 = 1$ then $x = \pm 1$ —

But $|x|^2 \neq 5$ since $a^2+4b^2=(a+2bi)\neq 5$

If $|x|^2=1$, then $x=\pm 1$.

If $4+3i=5\cdot u$, then $|4+3i|^2=|5|^2|u|^2$

$25=25|u|^2 \longrightarrow u=\pm 1$ X.

If I is an ideal of R, then

R/I is a field $\Leftrightarrow$ I is maximal
(no $I \subsetneq J \subsetneq R$)

R/I is an integral domain $\Leftrightarrow$ I is prime
(if $ab\in I$, then $a\in I$ or $b\in I$)

If F is a field, and X is a finite set,
and $R(X,F)=\{f: X\to F\}$ (pointwise addition & multiplication)
What are the maximal ideals of $R(X,F)$.

Maximal ideal $\longleftrightarrow$ quotient being a field
$\parallel$
$\ker \varphi \longleftrightarrow$ image being a field

If $\varphi: R(X,F) \twoheadrightarrow F'$ is a ring homomorphism that maps onto a field F' then $\ker \varphi$ will be a maximal ideal.

If $a\in X$

Ex: $ev_a: R(X,F) \twoheadrightarrow F$ has kernel is $\underbrace{\{f: f(a)=0\}}_{\text{maximal ideal}}$
$f \mapsto f(a)$

Let $a,b\in X$, then

$1_a(x)=\begin{cases}1 & \text{if } x=a\\ 0 & \text{if } x\neq a\end{cases}$, 1_b

$0=\varphi(0)=\varphi(1_a 1_b)=\varphi(1_a)\varphi(1_b)$ so 1_a or 1_b must map to 0.

So at most one 1_a that maps to something nonzero.

$\ker ev_a \leq \ker \varphi \Rightarrow \ker\varphi = \ker ev_a$

If $\ker ev_a \ni f = f(x_1)\underbrace{1_{x_1}} + f(x_2)\underbrace{1_{x_2}} + \cdots$

and $\varphi(f)=\varphi(f(x_1))\varphi(1_{x_1})+\cdots = 0$.

Vieta's Formulas

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x - r_1)\cdots(x - r_n)$$

$$a_0 = (-1)^n r_1 \cdots r_n$$

$$a_1 = (-1)^{n-1}(r_2 \cdots r_n + r_1 r_3 \cdots r_n + \cdots + r_1 \cdots r_{n-1})$$

$$a_{n-k} = (-1)^k \text{ (sum of products of } k \text{ roots)}$$

$$a_{n-1} = (-1)(r_1 + \cdots r_n)$$

$$r_1^3 + r_2^3 + r_3^3 = (r_1 + r_2 + r_3)^3 - 3(r_1 r_2 + r_1 r_3 + r_2 r_3)(r_1 + r_2 + r_3) + 3 r_1 r_2 r_3$$

Irreducibility

↳ Mod p (e.g., $x^2 + x + 1$ is irreducible mod 2)

↳ Eisenstein (if $p \nmid a_n$, $p \mid a_{n-1}, \ldots, a_0$, $p^2 \nmid a_0$ then irreducible)

↳ Gauss's lemma
Monic polynomial irreducible over $\mathbb{Q}$
$\Leftrightarrow$ irreducible over $\mathbb{Z}$