Rings I

Thursday, August 3, 2023

Ideals $\longleftrightarrow$ kernels of ring homomorphisms

subset

$+, -, 0,$

$a \in I$

$b \in R$

$ab \in I$

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

Show that there are no 2-sided ideals. (besides $0, R$).

Pf: Suppose $M \in I$, $M \neq 0$.

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

- rescale $\begin{bmatrix} 0 & & 0 \\ 0 & 1_{(i,j)} & 0 \end{bmatrix} \in I$
- multiply by permutation matrix

$\begin{bmatrix} 1_{(i',j')} \end{bmatrix} \in I$

$$\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & \\ & 0 & \\ & & \ddots & \\ & & & 0 \end{bmatrix} + \cdots + \begin{bmatrix} 0 & & \\ & \ddots & \\ & & 1 \end{bmatrix} \in I.$$

So $I = M$.

Fields $\subsetneq$ Euclidean Domains $\subsetneq$ Principle Ideal Domain

Fields: every element $\neq 0$ is invertible

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

Principle Ideal Domain: Every ideal is principle $(a) = \{ar : r \in R\}$.

$\subsetneq$ Unique Factorization Domain

Every $r \neq 0$ can be written as unit $\cdot$ primes

(prime $\Longleftrightarrow$ irreducible here, but not in general)

$\subsetneq$ Integral Domain

If $ab = 0$ then $a = 0$ or $b = 0$

$\subsetneq$ Integral Domain
If $ab=0$ then $a=0$ or $b=0$.

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

$(a+3bi)(c+3di) =$
$(ac-9bd)+3(ad+bc)i.$

Subring of $\mathbb{C}$, ✓
Integral Domain, ✓ (because subring of an integral domain)
Not UFD.

$\underbrace{(a+3bi)(a-3bi)}_{a^2+9b^2}$ = a different factorization

$a=4,\ b=1$
$25 \quad = \quad 5 \cdot 5$

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

- Need to show different
- Need to show that they don't factor further.

Use $N(a+3bi) = |a+3bi|^2 = a^2+9b^2$

If $uv=1$
then $\underbrace{N(u)}_{a^2+9b^2}N(v)=1$

$a=\pm 1,\ b=0 \Rightarrow$ only units are ± 1.

$4\pm 3i, 5$ have norm 25, so if they factored further, they would have to factor as norm 5 · norm 5, but $a^2+9b^2 \neq 5$.

Ideal $(x^m-1,\ x^n-1)$ in $\mathbb{Z}[x]$ is principal $(m,n>0)$

If $m \le n$, $(x^m-1,\ x^n-1) = (x^m-1,\ x^n-1-x^{n-m}(x^m-1))$
(key: Sum of exponents strictly decreases) $= (x^m-1,\ x^{n-m}-1)$

Repeat this until some exponent reaches 0.

E.g., $(x^n-1, x^0-1) = (x^n-1, 0) = (x^n-1)$ is principal.

$I \qquad\qquad R/I$ is a ring

I is prime $\Longleftrightarrow$ R/I is an integral domain
$(ab \in I \Rightarrow a \in I$ or $b \in I)$

I is maximal $\Longleftrightarrow$ R/I is a field.

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

F is a field, X is a finite set,
$R(X,F)$ is the ring of functions $X \to F$,
with pointwise operations. What are the maximal ideals of $R(X,F)$?

Idea: A maximal ideal m will be the kernel of the ring homomorphism $R(X,F) \to \underbrace{R(X,F)/m}_{\text{a field}}$.

So let $\varphi: R(X,F) \to (F'$ a field$)$ be a ring homomorphism

$R(X,F)$ has "basis vectors"/"idempotents"

$$e_{x_0} = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{if } x \neq x_0 \end{cases}$$

$$e_x e_y = 0 \quad \text{if } x \neq y$$

$$\varphi(e_x)\varphi(e_y) = \varphi(e_x e_y) = \varphi(0) = 0$$

so $\varphi(e_x) = 0$ or $\varphi(e_y) = 0$

$\Rightarrow$ At most one $\varphi(e_x) \neq 0$.

$$e_{x_1} + \dots + e_{x_n} = 1$$
$$\varphi(e_{x_1}) + \dots + \varphi(e_{x_n}) = \varphi(1) = 1$$

$\Rightarrow$ Exactly one $\varphi(e_x) = 1$

Any $f \in R(X,F)$ with $f(x) = 0$ will get mapped to 0
$(f = c_1 e_{x_1} + c_2 e_{x_2} + \dots)$

$\ker ev_x \leq \ker \varphi$

$\ker ev_x$ is maximal,
so $\ker \varphi = \ker ev_x$.

$$ev_x : R(X,F) \twoheadrightarrow F \qquad f \longmapsto f(x)$$

$\dfrac{R(X,F)}{\ker ev_x} \cong \operatorname{im} ev_x = F$ is a field

Only maximal ideals are $\ker ev_x$.

Vieta's formulas

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_2 x^2 + a_1 x + a_0$$
$$= (x - r_1)(x - r_2)\cdots(x - r_n)$$

Equate coefficients:

$$e_n = r_1 r_2 \cdots r_n = (-1)^n a_0$$

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

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

$$e_1 = r_1 + \cdots + r_n = (-1)^1 a_{n-1}$$

Any symmetric polynomial in $r_1, \dots, r_n$ is a polynomial in $e_1, \dots, e_n$.

$x^3 + 2x^2 + 7x + 1 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, compute $\alpha_1^3+\alpha_2^3+\alpha_3^3$.

$$e_3 = \alpha_1\alpha_2\alpha_3 = -1$$

$$e_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = 7$$

$$e_1 = \alpha_1 + \alpha_2 + \alpha_3 = -2$$

$$e_1^3 - 3e_1e_2 + 3e_3 = (-2)^3 - 3(-2)(7) + 3(-1) = -8 + 42 - 3 = 31$$

$$\underbrace{\alpha_1^3+\alpha_2^3+\alpha_3^3 + 6\alpha_1\alpha_2\alpha_3 + 6(\alpha_1^2\alpha_2 + \cdots)}_{e_1^3} - 3\Big(\big(2(\alpha_1^2\alpha_2 + \cdots)\big) + 3(\alpha_1\alpha_2\alpha_3)\Big) + 3\alpha_1\alpha_2\alpha_3$$

Methods for showing irreducibility

- Mod p (e.g., x^2+x+1 is irreducible mod 2, so irreducible in $\mathbb{Z}$)
- Eisenstein's criterion (e.g., $x^3+6x^2+9x+12$ irreducible; $p \nmid a_n$, $p \mid a_{n-1}, \dots, a_0$, $p^2 \nmid a_0$)
- Translate: $f(x)$ vs $f(x \pm c)$
- Try to factor

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = (x^2 + b_1x + b_0)(x^2 + c_1x + c_0)$$

(e.g., $a_3 = b_1 + c_1$)

Show $x^{p-1} + x^{p-2} + \cdots + x + 1$ irreducible

$$= \frac{x^p - 1}{x-1} \xleftrightarrow{\text{translate}} \frac{(x+1)^p - 1}{x}$$

$$x^{p-1} + \underbrace{\binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + \overbrace{\binom{p}{p-1}}^{=p}}_{\text{all div by } p}$$

Show $x^{n-1} + x^{n-2} + \cdots + x + 1$ irreducible $\iff$ n prime.

Show $x^{n-1} + x^{n-2} + \cdots + x + 1$ irreducible $\Longleftrightarrow$ n prime.
(over $\mathbb{Q} \Longleftrightarrow$ over $\mathbb{Z}$, by Gauss' Lemma, since monic)

($\Longleftarrow$) done above

($\Longrightarrow$) If $n = ab$, then

$$x^{ab-1} + x^{ab-2} + \cdots + x + 1 = (x^{a-1} + x^{a-2} + \cdots + x + 1)(1 + x^{a} + x^{2a} + \cdots + x^{(b-1)a})$$

Show $I = (5, x^3+x+1) \leq \mathbb{Z}[x]$ prime.

$$\frac{\mathbb{Z}[x]}{(5, x^3+x+1)} \cong \frac{\mathbb{Z}[x]/(5)}{(5, x^3+x+1)/(5)} \cong \frac{\mathbb{Z}/5\mathbb{Z}\,[x]}{(x^3+x+1)}$$

(just show x^3+x+1 irred mod 5).