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

Pf: Suppose $I \neq 0$. $M \overset{\neq 0}{\in} I$

$$\begin{bmatrix} 0 & & \\ & 1 & 0 \\ 0 & & 0 \end{bmatrix} M \begin{bmatrix} 0 & & 0 \\ & 1 & \\ 0 & & 0 \end{bmatrix} = \begin{bmatrix} 0 & & 0 \\ & M_{ij} & \\ 0 & & 0 \end{bmatrix} \in I$$

i,i-th entry $\quad j,j^{th}$-entry $\quad (i,j)^{th}$ entry

rescale: $\begin{bmatrix} 0 & 1 & 0 \\ 0 & & 0 \end{bmatrix}$ permute rows/columns $\begin{bmatrix} 0 & & \\ & 1 & 0 \\ 0 & & 0 \end{bmatrix}$

add these up to get $1 = \begin{bmatrix} 1 & & 0 \\ 0 & & 1 \end{bmatrix}$.

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

Show R is a subring of $\mathbb{C}$, integral domain, not UFD.

- subring: $0 \in R$, $1 \in R$, closed under $+, -, \cdot$
- $\mathbb{C}$ is an integral domain so so is R

$(a+3bi)(a-3bi) = a^2 + 9b^2$

$a = 4, b = 1$ is a good choice

$(4+3i)(4-3i) = 25 = 5^2$

unique factorization says if $p_1 \cdots p_k = q_1 \cdots q_l$ then differ by permutation and units

Look at $N : R \to \mathbb{Z}_{\geq 0}$ $\quad N(a+3bi) = a^2 + 9b^2 = |a+3bi|^2$

multiplicative

$N(5) = 5^2$ so if 5 factored, then either Norm 1 $\cdot$ Norm 25 or Norm 5 $\cdot$ Norm 5

if $a^2+9b^2=1$ then $a+3bi = \pm 1$

Impossible because $a^2 + 9b^2 \neq 5$

Any element of norm 25 is irreducible

Need to show that $4+3i$ and 5 don't differ by a unit. $\left(\frac{4+3i}{5} = \frac{4}{5} + \frac{3}{5} \notin R\right)$

Only units are ± 1 because $uv = 1$, then $N(u)N(v) = 1$ so $u, v = \pm 1$

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

Only unit... so $u, v = \pm 1$

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

Suppose $m \geq n$. Then

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

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

This is one step of the Euclidean algorithm applied to the exponents

By repeating this, we arrive at

$$(x^m - 1, x^n - 1) = \cdots = (x^{\gcd(m,n)} - 1, x^0 - 1)$$
$$= (x^{\gcd(m,n)} - 1)$$

principal.

If R is finite commutative ring with unity and no zero-divisors and not the zero ring, then R is a field.

If $x \in R$ nonzero, then $y \mapsto xy$ is injective (if $xy = xz$, then $x(y-z) = 0$ so $y - z = 0$)

so $y \mapsto xy$ surjective

so $1 = xy$ for some $y \in R$.

This problem is still true if R is not assumed to be commutative (Wedderburn's little thm)

$\begin{cases} I \text{ is prime} \iff R/I \text{ integral domain} \\ I \text{ is maximal} \iff R/I \text{ field} \end{cases}$

F field, X finite set, $R(X, F)$ pointwise operations.
What are the maximal ideals.

If we look at $ev_x = proj_x : R(X, F) \to F$, surjective,

so $R(X,F)/\ker ev_x \cong F$ so $\ker ev_x = \{f : f(x) = 0\}$ is maximal

$e_1, e_2, \ldots, e_n$ idempotents

$e_i(x) = \begin{cases} 1 & \text{if } x \text{ is the } i^{th} \text{ element} \\ 0 & \text{else} \end{cases}$

If $\varphi : R(X, F) \to$ field

$\left.\begin{matrix} \varphi(e_i) & i = j \\ 0 & \text{if } i \neq j \end{matrix}\right\} = \varphi(e_i e_j) = \varphi(e_i)\varphi(e_j) \implies$ Only one $\varphi(e_i)$ can be nonzero

$\varphi(e_i) = 1$

Then $\ker \varphi$ contains

ker ev_{x_i}

If $f \in \ker ev_{x_i}$

$f = f(e_1 + \dots + e_n) = fe_1 + \dots + fe_n$

all but $fe_i \xmapsto{\varphi} 0$

$fe_i \longmapsto 0$ too because $f \in \ker ev_{x_i}$

If I is an ideal, look at $f \in I$,

f will nonzero on some set $S \subseteq X$

For $x \in S$, $f \cdot e_x$ will just be supported at x

by rescaling, $e_x \in I$.

Claim: $I = \langle e_x$ for x s.t. $f(x) \neq 0$ for some $f \in I \rangle$

Claim': $I = \langle e_x$ for $e_x \in I \rangle$

$\geq$

If $f \in I$, then I contains e_x for $f(x) \neq 0$

so $f \in \langle e_x \rangle$ because $f = f(x_1) e_{x_1} + f(x_2) e_{x_2}$

Thus, ideals of $R(X,F) \xleftrightarrow{\text{bij}}$ subsets of X

$I \xleftrightarrow{\text{bij}}$ subset of X consisting of the points on which some $f \in I$ is nonzero.

$\langle e_x : x \in S \rangle$

$\{f : f(x) = 0 \text{ for } x \notin S\} \longleftarrow\!\!\mid S$

In particular, maximal ideals correspond to $X \setminus \{x_0\}$

$I = \{f : f(x_0) = 0\} = \langle e_x : x \neq x_0 \rangle$.

Vieta's formulas (symmetric polynomials)

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

where a_i is an elementary symmetric polynomial

$e_1 = a_{n-1} = r_1 + \dots + r_n$

$e_2 = a_{n-2} = r_1 r_2 + r_1 r_3 + \dots + r_{n-1} r_n$

$\vdots$

$e_n = a_0 = r_1 \cdots r_n$

Any symmetric poly is a poly in these $e_1, \dots, e_n$

$R[x_1, \dots, x_n]^{S_n} \cong R[e_1, \dots, e_n]$

$$e_i(x_1,\dots,x_n) \longleftarrow e_i$$

$$x^3+2x^2+7x+1 = (x-\alpha_1)\cdots(x-\alpha_n)$$

Compute $\alpha_1^3+\alpha_2^3+\alpha_3^3 = e_1^3 - 3e_1e_2 - 3e_3 = (-2)^3 - 3\cdot(-2)\cdot 7 - 3\cdot(-1) = 31$

$(\alpha_1+\alpha_2+\alpha_3)^3 - 3(\alpha_1+\alpha_2+\alpha_3)(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) - 3\alpha_1\alpha_2\alpha_3$

$e_1 = -2$

$e_2 = 7$

$e_3 = -1$

Irreducibility techniques.

- → Eisenstein's criterion $\quad f \in \mathbb{Z}[x]$, $= a_nx^n + \dots + a_1x + a_0$, $p \mid a_1,\dots,a_{n-1}$, $p^2 \nmid a_0$, $p \nmid a_n$ then f irred — also works for arbitrary prime ideals
- x^4+1 → Show irreducible mod p
- → Translate $x \mapsto x+c$
- → Deg 2,3 check if there is a root
- → Deg 4, check if root, and try to write as a product of two quadratic.

$I \trianglelefteq \mathbb{Z}[x]$ generated by $5, x^3+x+1$

Is I prime?

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

We just need to show x^3+x+1 irreducible mod 5 (so that the quotients are integral domains)

Check $x \equiv 0,1,2,3,4 \pmod 5$

$$f_n(x) = x^{n-1}+x^{n-2}+\dots+x+1 = (1+x+\dots+x^{d-1})(\dots)$$

irreducible $\Longleftrightarrow$ n prime

$(\Leftarrow)$ First shift $\dfrac{x^n-1}{x-1} = \dfrac{(y+1)^n-1}{y}$ (for $y = x-1$)

$$= y^{n-1} + \overbrace{\binom{p}{1}y^{n-2} + \binom{p}{2}y^{n-3} + \dots + \binom{p}{p-1}}^{\text{div by } p}$$

Eisenstein

$\binom{p}{p-1} = p$ so not div by p^2