Spring 2019 #5 (and Spring 2017 #8, ~~Spring 2016~~ #8)
Describe in terms of radicals all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{12})$

$\zeta := \zeta_n = e^{2\pi i/n}$

$\mathbb{K} = \mathbb{Q}(\zeta_{12})$ $\quad$ $\mathbb{K}/\mathbb{Q}$ is Galois since

$\mathbb{K} = \mathrm{split}_{\mathbb{Q}}(x^{12}-1)$

separable; has 12 different roots $1, \zeta, \zeta^2, \dots, \zeta^{11}$

$\left[\, 1 \overset{?}{=} \gcd\left(x^{12}-1, \frac{d}{dx}(x^{12}-1)\right) = \gcd(x^{12}-1, 12x^{11}) \,\right]$

$G = \underset{\text{Gal}}{\mathrm{Aut}}(\mathbb{K}/\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^{\times} = \underbrace{\{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}}_{\text{size}}$

$\left(\sigma_a(\zeta) = \zeta^a\right) \longleftarrow\!\!| \ \bar{a}$

uniquely defines such an element of G

size $\varphi(12) = \varphi(3)\varphi(4) = (3-1)(2^2-2^1) = 2 \cdot 2 = 4$ ✓

$\bar{5}^2 = \bar{1}$
$\bar{7}^2 = \bar{1}$
$\overline{11}^2 = \bar{1}$

$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = V_4$

$$\begin{tikzcd}
 & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma_5 \rangle \arrow[dr, dash] & \langle \sigma_7 \rangle \arrow[d, dash] & \langle \sigma_{11} \rangle \arrow[dl, dash] \\
 & 1 &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{K}^{\langle \sigma_5 \rangle} \arrow[dr, dash] & \mathbb{K}^{\langle \sigma_7 \rangle} \arrow[d, dash] & \mathbb{K}^{\langle \sigma_{11} \rangle} \arrow[dl, dash] \\
 & \mathbb{K} &
\end{tikzcd}$$

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\begin{tikzcd}[column sep=small]
& G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma_5 \rangle \arrow[dr, dash] & \langle \sigma_7 \rangle \arrow[d, dash] & \langle \sigma_{11} \rangle \arrow[dl, dash] \\
& 1 &
\end{tikzcd}$$

$$\begin{tikzcd}[column sep=small]
& \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
K^{\langle \sigma_5 \rangle} \arrow[dr, dash] & K^{\langle \sigma_7 \rangle} \arrow[d, dash] & K^{\langle \sigma_{11} \rangle} \arrow[dl, dash] \\
& K = \mathbb{Q}(\zeta) &
\end{tikzcd}$$

$\mathbb{Q}(\zeta^3) = \mathbb{Q}(\zeta + \zeta^5) = K^{\langle \sigma_5 \rangle} = \mathbb{Q}(\alpha)$

$\mathbb{Q}(\zeta^2) \neq K^{\langle \sigma_7 \rangle}$

$\mathbb{Q}(\zeta + \zeta^{-1}) = K^{\langle \sigma_{11} \rangle}$

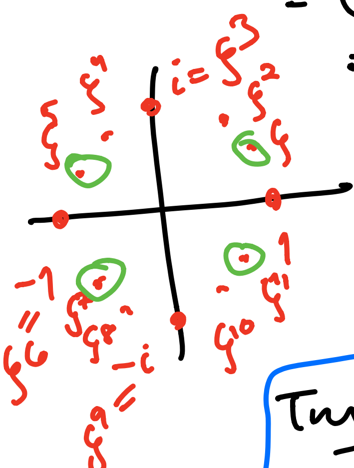
$\alpha \notin \mathbb{Q}$

$\sigma_5(\alpha) = \alpha$

$K = \mathbb{Q}(\zeta)$ $= \mathbb{Q}$-span of $\underbrace{\{1, \zeta, \zeta^2, \zeta^3\}}_{\text{a } \mathbb{Q}\text{-basis}}$

$\Phi_{12}(x)$ is a factor of

$$\begin{aligned}
x^{12} - 1 &= (x^6 - 1)(x^6 + 1) \\
&= (x^3 - 1)(x^3 + 1)(x^2 + 1)(x^4 - x^2 + 1) \\
&= \underbrace{(x-1)}_{\Phi_1}\underbrace{(x^2 + x + 1)}_{\Phi_3}\underbrace{(x+1)}_{\Phi_2}\underbrace{(x^2 - x + 1)}_{\Phi_6}\underbrace{(x^2 + 1)}_{\Phi_4}\underbrace{\boxed{(x^4 - x^2 + 1)}}_{\Phi_{12}}
\end{aligned}$$



$\zeta^4 - \zeta^2 + 1 = 0$

$\boxed{\zeta^4 = \zeta^2 - 1}$

Try $\alpha = \zeta + \sigma_5(\zeta) = \zeta + \zeta^5 = \zeta + \zeta\boxed{\zeta^4}$
$= \zeta + \zeta(\zeta^2 - 1)$
$= \zeta + \zeta^3 - \zeta = \zeta^3 \notin \mathbb{Q}$

$\zeta + \sigma_{11}(\zeta) = \zeta + \zeta^{-1} = \zeta - \zeta^5 = \zeta - \zeta(\zeta^2 - 1) = \zeta - \zeta^3 + \zeta = 2\zeta - \zeta^3 \notin \mathbb{Q}$

$\zeta + \sigma_7(\zeta) = \zeta + \zeta^7 = 0 \in \mathbb{Q}$

$\zeta^2 + \sigma_7(\zeta^2) = \zeta^2 + \zeta^{14} = 2\zeta^2 \notin \mathbb{Q}$

$$\begin{tikzcd}[column sep=small] & G \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle\sigma_5\rangle \arrow[dr, dash] & \langle\sigma_7\rangle \arrow[d, dash] & \langle\sigma_{11}\rangle \arrow[dl, dash] \\ & 1 & \end{tikzcd}$$

$$\begin{tikzcd}[column sep=small] & \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta^3) = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta+\zeta^5) = K^{\langle\sigma_5\rangle} = \mathbb{Q}(\alpha) \arrow[dr, dash] & \mathbb{Q}(\zeta^2) = \mathbb{Q}(\sqrt{-3}) = K^{\langle\sigma_7\rangle} \arrow[d, dash] & K^{\langle\sigma_{11}\rangle} = \mathbb{Q}(\zeta+\zeta^{-1}) = \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\ & K = \mathbb{Q}(\zeta) & \end{tikzcd}$$

Try it yourself

In terms of radicals,

$$(x-\zeta^3)(x-\sigma_{11}(\zeta^3)) = x^2 - (\overset{i}{\zeta^3} + \overset{-i}{\zeta^{-3}})x + \zeta^3\cdot\zeta^{-3}$$

all Galois images of ζ^3

$$= x^2 - (\ 0\ )x + 1$$

$$= x^2 + 1$$

$$(x-\zeta^2)(x-\sigma_{11}(\zeta^2)) = (x-\zeta^2)(x-\zeta^{-2})$$

$$= x^2 - (\zeta^2+\zeta^{-2})x + 1$$

$$= x^2 - (\zeta^2 - \zeta^4)x + 1$$

$$= x^2 - (\zeta^2 - (\zeta^2 - 1))x + 1$$

$$= x^2 - x + 1 \qquad (= \Phi_6(x))$$

$$\Rightarrow \zeta^2 = \frac{1 \pm \sqrt{1-4}}{2} = \frac{1 \pm \sqrt{-3}}{2}$$

$$\mathbb{Q}(\zeta^2) = \mathbb{Q}\left(\frac{1\pm\sqrt{-3}}{2}\right) = \mathbb{Q}(\sqrt{-3})$$

Spring 2018 #7

Determine all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_{10})$

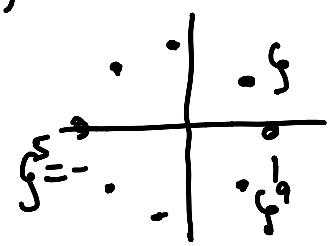
$\zeta = \zeta_{10}$

$$G = \mathrm{Aut}(\underset{\substack{\parallel \\ \mathbb{Q}(\zeta)}}{K}/\mathbb{Q}) \cong (\mathbb{Z}/10\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\} \cong \mathbb{Z}/4\mathbb{Z}$$

$\bar{3}^2 = \bar{9} = -\bar{1}$

$$\begin{array}{ccc}
1 & & K = \mathbb{Q}(\zeta) \\
| & & | \\
H = \langle \sigma_3^2 \rangle & & K^H = \mathbb{Q}(\alpha) = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\sqrt{5}) \\
| & & | \\
G = \mathbb{Z}/4\mathbb{Z} = \langle \sigma_3 \rangle & & \mathbb{Q}
\end{array}$$

check yourself!



$$x^{10} - 1 = (x^5 - 1)(x^5 + 1)$$
$$= \underbrace{(x-1)}_{\Phi_1}\underbrace{(x^4 + x^3 + x^2 + x + 1)}_{\Phi_5}\underbrace{(x+1)}_{\Phi_2}\boxed{\underbrace{(x^4 - x^3 + x^2 - x + 1)}_{\Phi_{10}}}$$

$\zeta^4 = \zeta^3 - \zeta^2 + \zeta - 1$

Try $\alpha = \zeta + \sigma_3^2(\zeta) = \zeta + \zeta^9 = \zeta + \zeta^{-1} = \zeta - \zeta^4 = \zeta - (\zeta^3 - \zeta^2 + \zeta - 1)$
$= -\zeta^3 + \zeta^2 + 2\zeta - 1 \notin \mathbb{Q}$

$(x - (\zeta + \zeta^9))(x - \sigma_3(\zeta + \zeta^9))$
$=$ an irred. quadratic giving $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Q}[x]$
solve via quadratic formula

Spring 2016 #8

Determine all intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\zeta_8)$

Try it; $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Spring 2019 #6

Show $x^4+x^3+x^2+x+1$ is irred. in $\mathbb{F}_3[x]$

It has no linear factors since $\mathbb{F}_3 = \{0, 1, -1\}$ has no roots for $f(x) = x^4+x^3+x^2+x+1$.

Only need to show no irred quadratic factors $g(x) \in \mathbb{F}_3[x]$.

Method 1: Brute force

Irred quadratics are:

x^2+1

$\cancel{x^2-1}$ $\quad x = \pm 1$

$\cancel{x^2+x+1}$ $\quad x = +1$

x^2+x-1

$\cancel{x^2-x+1}$ $\quad x = -1$

x^2-x-1

Check that $f(x)$ is not divisible by these!

Method 2:

If $f(x) = x^4 + x^3 + x^2 + x + 1$

$$= \frac{x^5 - 1}{x - 1}$$

has a quad. irred. factor $q(x)$ in $\mathbb{F}_3[x]$,

then α any root for $q(x)$

would have

$$\mathbb{F}_3(\alpha) \cong \mathbb{F}_3[x]/(q(x))$$

$$= \mathbb{F}_{3^2} = \mathbb{F}_9$$

so α is a root for $x^5 - 1$

so $\alpha^5 = 1$, and $\alpha \neq 1$ (since $\mathbb{F}_3(\alpha) \neq \mathbb{F}_3$)

but $\alpha \in \mathbb{F}_9^\times \cong (\mathbb{Z}/8\mathbb{Z})$

so its order divides 8.

Contradiction.

Fall 2018 #4

Show x^5+y^7+2y is irreducible in $\mathbb{C}[x,y]$

In $\mathbb{C}[x,y] = \mathbb{C}[y][x]$

$$x^5 + 0\cdot x^9 + 0\cdot x^3 + 0\cdot x^2 + 0\cdot x + \underbrace{y^7+2y}_{= y^1(y^6+2)}$$

in $\mathbb{C}[y]$

so Eisenstein applies

at the prime ideal

(y) in $\mathbb{C}[y]$

since $y^1(y^6+2) \notin \underset{\underset{(y^2)}{\shortparallel}}{(y)^2}$

Fall 2017 #4

Show x^5+y^7+11 is irreducible in $\mathbb{Z}[x,y]$

In $\mathbb{Z}[y][x]$,

$$x^5+y^7+11 =$$

$$x^5+0\cdot x^4+0\cdot x^3+0\cdot x^2+0\cdot x + \underbrace{y^7+11}$$

in $\mathbb{Z}[y]$

take any irred. factor $f(x)$ of y^7+11

and we know $y^7+11 \in (f(x))$,

but not $(f(x))^2$

since

$$1 \overset{?}{=} \gcd\left(y^7+11, \frac{d}{dy}(y^7+11)\right)$$

$$= \gcd(y^7+11, 7y^6) = 1 \checkmark$$

Fall 2016 #7

Show x^4+1 is irreducible in $\mathbb{Q}[x]$,
but reducible in $\mathbb{F}_p[x]$ for every prime p

$f(x) = x^4+1$ in $\mathbb{Q}[x]$

$= \Phi_8(x)$

$$x^8-1 = (x^4-1)(x^4+1)$$
$$= \underset{\Phi_1}{(x-1)}\underset{\Phi_2}{(x+1)}\underset{\Phi_4}{(x^2+1)}\underset{\Phi_8}{(x^4+1)}$$

cheat and say these are all irred. in $\mathbb{Q}[x]$?

To show it's irred.,
show no lin. factors by $\mathbb{Q}$ root test
which says only $\frac{\pm 1}{\pm 1} = \pm 1$
can be roots, but they're <u>not</u>,
For quad. factors in $\mathbb{Q}[x]$, it's same
$\mathbb{Z}[x]$ because $f(x)$ is <u>primitive</u>
and if $x^4+1 = (x^2+ax+b)(x^2+cx+d)$ in $\mathbb{Z}[x]$, $a,b,c,d \in \mathbb{Z}$

$\Rightarrow bd = \pm 1$

$$x^4+1 = (x^2+ax\pm 1)(x^2+cx\pm 1)$$

$$x^4 \pm 1 = (x^2 + ax \pm 1)(x^2 + cx \pm 1)$$
$$= x^4 + \underbrace{(a+c)}_{=0} x^3 + (ac \pm 2)\, x^2 \pm \underbrace{(a+c)}_{=0}\, x + 1$$

$a = -c$

$$\Downarrow$$

$$-a^2 \pm 2 = 0$$
$$a^2 = \sqrt{\pm 2} \quad a \in \mathbb{Z}$$
impossible.

Why is x^4+1 reducible in $\mathbb{F}_p[x]$?

$\underline{p=2}$: $x^4+1 = (x+1)^4$

For odd primes p, we suspect there should be an irred. quad factor $q(x)$ in $\mathbb{F}_p[x]$, whose roots α would give $\alpha \in \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(q(x))$
$\cong \mathbb{F}_{p^2}$

which is a root of $q(x) = \Phi_8(x)$ and have order 8 in $\mathbb{F}_{p^2}^\times$

Conversely, if $\exists\ \alpha \in \mathbb{F}_{p^2}^\times$ which has order 8, then $\alpha^8 = 1$

but $\alpha^4 = \pm 1$, not $+1$

so $\alpha^4 + 1 = 0$

α is a root of an irred. <u>linear</u> or <u>quadratic</u>

$m_{\mathbb{F}_p,\alpha}(x) = g(x)$ that divides x^4+1

$$\mathbb{F}_{p^2}^\times \cong \left(\mathbb{Z}/(p^2-1)\mathbb{Z}\right)^+$$

so such an α exists $\Longleftrightarrow p^2 - 1 \equiv 0 \mod 8$

$$p^2 - 1 \equiv \begin{cases} 0\cdot 2 \equiv 0 & \text{if } p \equiv 1 \mod 8 \\ 2\cdot 4 \equiv 0 & p \equiv 3 \\ 4\cdot 6 \equiv 0 & p \equiv 5 \\ 6 \cdot 8 \equiv 0 & p \equiv 7 \end{cases}$$

$p^2 - 1 = (p-1)(p+1)$

Fall 2019 #3 (and Fall 2016 #4)

Classify the $\mathbb{Z}[i]$-modules of cardinality 13

Fall 2016 #5

Show the ideal $I = (13, x^2+1) \subset \mathbb{Z}[x]$ is <u>not</u> maximal.

$\mathbb{Z}[i]$ is a PID, so any module M over $\mathbb{Z}[i]$ which has card 13 is certainly fin. gen'd, so

$$M = \underbrace{\mathbb{Z}[i]^r}_{r=0} \oplus \bigoplus_{j=1}^{t} \mathbb{Z}[i]/(\alpha_j) \qquad \alpha_i \in \mathbb{Z}[i]$$

since $\#M = 13$

$$\Downarrow$$

$$\#M = \prod_{j=1}^{t} \#\left[\mathbb{Z}[i]/(\alpha_j)\right]$$

$\#M = 13$ prime $\Rightarrow \mathbb{Z}[i]/(\alpha)$

Q: Which α in $\mathbb{Z}[i]$ have

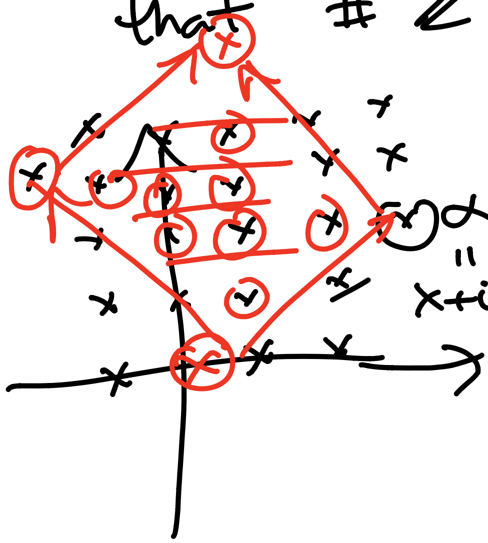
$\# \mathbb{Z}[i]/(\alpha) = 13$?

We showed in HW (or see Chap. 12)

that $\# \mathbb{Z}[i]/(\alpha) = N(\alpha)$ if $\alpha = x+iy$

$= x^2+y^2$

$= (x+iy)(x-iy)$



$13 = 2^2+3^2$

$= \underbrace{(2+3i)}_{\alpha_1}\underbrace{(2-3i)}_{\alpha_2}$

$M = \mathbb{Z}[i]/(2+3i)$

$M = \mathbb{Z}[i]/(2-3i)$

are the only two.

To show $I = (13, x^2+1) \subset \mathbb{Z}[x]$ is not maximal is equivalent to showing $\mathbb{Z}[x]/I$ is not a field.

But

$$\mathbb{Z}[x]/(13, x^2+1) \overset{\text{A Noether Thm.}}{\cong} \frac{\mathbb{Z}[x]/(x^2+1)}{(13, x^2+1)/(x^2+1)}$$

$$\cong \mathbb{Z}[i]/(13)$$

$$= \underbrace{\mathbb{Z}[i]/\underbrace{((2+3i)(2-3i))}_{\text{not a maximal ideal}}}_{\text{Not a field!}}$$

since

$$((2+3i)(2-3i)) \subsetneq (2+3i) \subsetneq \mathbb{Z}[i]$$

Spring 2019 #3
Show the ideal $I = (19, x^2+1) \subset \mathbb{Z}[x]$ is maximal.

Similarly to previous problem,

$I \subset \mathbb{Z}[x]$ is maximal

$\iff \mathbb{Z}[x]/I$ is a field

$$\mathbb{Z}[x]/I = \mathbb{Z}[x]/(19, x^2+1)$$

$$\cong \frac{\mathbb{Z}[x]/(x^2+1)}{(19, x^2+1)/(x^2+1)}$$

$$\cong \mathbb{Z}[i]/(19)$$

19 remains prime in $\mathbb{Z}[i]$ since $19 \equiv 3 \bmod 4$ (not $\equiv 1 \bmod 4$)

Hence (19) is maximal in $\mathbb{Z}[i]$ since it is a P.I.D.

and $\mathbb{Z}[i]/(19)$ is a field.

Fall 2019 # 7

Describe the prime ideals in $k[[x]]$, k a field

First recall who the units $k[[x]]^\times$ are, then who all the ideals are, then the prime ideals.

$f(x) = a_0 + a_1 x + a_2 x^2 + \dots \in k[[x]]$ is a unit whenever $a_0 \in k^\times$, since then one can write down a formula for $f(x)^{-1}$:

$$f(x)^{-1} = \frac{1}{a_0 + a_1 x + a_2 x^2 + \dots}$$

$$= a_0^{-1}\left(\frac{1}{1 + \frac{a_1}{a_0}x + \frac{a_2}{a_0}x^2 + \dots}\right)$$

$$= a_0^{-1}\left(1 - \underbrace{\left(\frac{a_1}{a_0}x + \frac{a_2}{a_0}x^2 + \dots\right)^1}_{} + \underbrace{\left(\frac{a_1}{a_0}x + \frac{a_2}{a_0}x^2 + \dots\right)^2}_{} - \dots\right)$$

which gives a well-defined element of $k[[x]]$

since this is divisible by x^1

this is divisible by x^2

$\vdots$

Once we've identified $k[[x]]^\times$, the nonzero, proper ideals $I \subset k[[x]]$ can be identified as all principal ideals $(x), (x^2), (x^3), \ldots$

since if I has nonzero element

$$f(x) = a_d x^d + a_{d+1} x^{d+1} + \ldots.$$

with $a_d \neq 0$ achieving the smallest such degree d,

then we claim $I = (x^d)$:

Note $f(x) = x^d \underbrace{(a_d + a_{d+1} x^1 + a_{d+2} x^2 + \ldots)}_{\text{a unit in } k[[x]]}$

$$\Rightarrow (f(x)) = (x^d) \subseteq I$$

but conversely $I \subseteq (x^d)$ by definition of d.

The only prime ideal among $(x), (x^2), (x^3), \ldots$ is (x) since any (x^d) for $d \geq 2$ has $x^1, x^{d-1} \notin (x^d)$ but $x^1 \cdot x^{d-1} \in (x^d)$

Note (x) is prime, since $k[[x]]/(x) \cong k$ a field, so a domain. Also $I = (0)$ is prime since $k[[x]]$ is a domain.

Fall 2018 #6

Show the ring $M_n(k) = k^{n\times n}$ for a field k has no proper 2-sided ideals.

Let's check that any non-zero 2-sided ideal $J \subseteq M_n(k)$ actually contains $1 = I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$.

Given any nonzero matrix $A = (a_{ij}) \in J$, assume the entry $a_{ij} \neq 0$. Then J also contains

$$\frac{1}{a_{ij}} E_{m,i} A E_{j,m} = \begin{array}{cc} & \text{column } m \\ & \downarrow \\ \text{row } m \rightarrow & \begin{bmatrix} 0 & & & & & \\ & \ddots & & & 0 & \\ & & 0 & & & \\ & & & \boxed{1} & & \\ & 0 & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \end{bmatrix} \end{array}$$

for each $m = 1, 2, \dots, n$

where

$$E_{a,b} = \begin{array}{cc} & \text{column } b \\ \text{row } a \rightarrow & \begin{bmatrix} 0 & 0 & 0 \\ & \vdots & \\ & \boxed{1} & \\ 0 \cdots 0 & 0 & 0 \cdots 0 \\ 0 & \vdots & 0 \end{bmatrix} \end{array}.$$

Hence J contains

$$\begin{bmatrix} 1 & & 0 \\ & 0 & \\ 0 & & \ddots \; 0 \end{bmatrix} + \begin{bmatrix} 0 & & 0 \\ & 1 & \\ & & 0 \\ 0 & & \ddots \; 0 \end{bmatrix} + \dots + \begin{bmatrix} 0 & & 0 \\ & \ddots & \\ 0 & & 0 \; 1 \end{bmatrix} = I_n.$$

Spring 2018 #6

Show $I=(x,y)\subset k[x,y,z]$ for k a field is not a principal ideal.

Suppose $I=(x,y)=(f(x,y,z))$ <u>was</u> principal.

Define for $g(x,y,z)=\sum_{a,b,c} g_{abc}\, x^a y^b z^c$

its minimum & maximum degrees

$$\text{mindeg}(g):=\min\{a+b+c : g_{abc}\neq 0\}$$
$$\text{maxdeg}(g):=\max\{a+b+c : g_{abc}\neq 0\}$$

and note $\text{mindeg}(fg)=\text{mindeg}(f)+\text{mindeg}(g)$
$\text{maxdeg}(fg)=\text{maxdeg}(f)+\text{maxdeg}(g)$

since k is a field (so $f_{abc}\,g_{\alpha\beta\gamma}\neq 0$ if $f_{abc}, g_{\alpha\beta\gamma}\neq 0$)

Since $f\in I=(x,y)$, one has $\text{mindeg}(f)\geq 1$.

Then since $x\in(x,y)=I=(f)$

implies $x=f\cdot g \Rightarrow$ $1=\text{mindeg}(f)+\text{mindeg}(g)$
$1=\text{maxdeg}(f)+\text{maxdeg}(g)$

one concludes that $\text{mindeg}(g)=\text{maxdeg}(g)=0$

i.e. $g\in k^\times$ and $f=g\cdot x$ is associate to x

Similarly $y\in(x,y)=I=(f)$ shows f is associate to y.

But then x,y are associates, which is false.

Fall 2017 #6

Let k be a field and show $I = (x,y,z) \subset k[x,y,z]$ is a maximal ideal.

This equivalent to showing that

$$k[x,y,z]/I \text{ is a field}$$

$$\|$$

$$k[x,y,z]/(x,y,z) \cong k, \text{ a field.} \checkmark$$

Spring 2016 #4

Prove that the set of nilpotent elements in a commutative ring is an ideal.

For R a commutative ring

and $I := \{$all nilpotent elements, i.e. $a \in R$ such that $\exists N \in \{1, 2, \dots\}$ with $a^N = 0\}$

one has $\forall\, a, b \in I$ and $r \in R$

that $\exists N_1$ with $a^{N_1} = 0$

N_2 with $a^{N_2} = 0$

so $ra \in I$ because

$$(ra)^{N_1} \underset{R \text{ commutative}}{=} r^{N_1} a^{N_1} = r^{N_1} \cdot 0 = 0$$

and $a+b \in I$ because

$$(a+b)^{N_1+N_2} = \sum_{\substack{(k,l): \\ k+l = N_1+N_2}} \binom{N_1+N_2}{k} \underbrace{a^k}\, \underbrace{b^l} = 0.$$

at least one of these vanishes since either $k \geq N_1$ or $l \geq N_2$ as $k + l = N_1 + N_2$

Spring 2016 #7

Give a prescription for a formula for an isomorphism (for integers $m,n>1$)

$$\mathbb{Z}/m \oplus \mathbb{Z}/n \to \mathbb{Z}/\gcd(m,n) \oplus \mathbb{Z}/\operatorname{lcm}(m,n)$$

If one factors $m = p_1^{a_1} \cdots p_r^{a_r}$
$n = p_1^{b_1} \cdots p_r^{b_r}$

for some list of distinct primes $p_1, \ldots, p_r$

and $a_i, b_j \in \{0,1,2,\ldots\}$, then

Chinese Remainder Theorem gives isomorphisms

$$\mathbb{Z}/m \oplus \mathbb{Z}/n \longrightarrow \bigoplus_{k=1}^{r} \mathbb{Z}/p_k^{a_k} \oplus \mathbb{Z}/p_k^{b_k}$$

$$\mathbb{Z}/\gcd(m,n) \oplus \mathbb{Z}/\operatorname{lcm}(m,n) \longrightarrow \bigoplus_{k=1}^{r} \mathbb{Z}/p_k^{\min(a_k,b_k)} \oplus \mathbb{Z}/p_k^{\max(a_k,b_k)}$$

Hence it suffices to exhibit for each k an isomorphism

$$\mathbb{Z}/p_k^{a_k} \oplus \mathbb{Z}/p_k^{b_k} \longrightarrow \mathbb{Z}/p_k^{\min(a_k,b_k)} \oplus \mathbb{Z}/p_k^{\max(a_k,b_k)}$$

which is either

$$(\bar{x}, \bar{y}) \longmapsto (\bar{x}, \bar{y}) \text{ if } a_k \leq b_k$$

or $$(\bar{x}, \bar{y}) \longmapsto (\bar{y}, \bar{x}) \text{ if } a_k > b_k$$