Sunday 3/8/20. MATH 612 HW3 SOLUTIONS.

1. a) By the structure theorem for f.g. modules over a PID,

$$A \simeq \mathbb{Z}^{\oplus r} \oplus \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}$$

for some $r, s \geq 0$, $p_1, \dots, p_s$ primes, & $\alpha_1, \dots, \alpha_s \in \mathbb{N}$.

(Note: an abelian group is naturally a $\mathbb{Z}$-module)

Also, $(M_1 \oplus M_2) \otimes_R N \cong M_1 \otimes_R N \oplus M_2 \otimes_R N$ for R-modules M_1, M_2, N

(& $M \otimes_R N \cong N \otimes_R M$ for R-modules M & N)

So, to prove $A \otimes_{\mathbb{Z}} A \neq 0$ for $A \neq 0$, it's enough to show

1. $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \neq 0$ & 2. $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \neq 0$ for $n \in \mathbb{N}$

1.:- in fact $R \otimes_R M \simeq M$ for R-modules M,

so $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} \simeq \mathbb{Z}. \neq 0.$

2.:- recall $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\gcd(m,n)\mathbb{Z}$ for $m, n \in \mathbb{N}$,

so $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \neq 0.$ □.

b. Following the hint, let $A = \mathbb{Q}/\mathbb{Z}$, and consider a pure tensor $\overline{\left(\frac{a}{b}\right)} \otimes \overline{\left(\frac{c}{d}\right)} \in A \otimes_{\mathbb{Z}} A$

Now
$$\overline{\left(\frac{a}{b}\right)} \otimes \overline{\left(\frac{c}{d}\right)} = \overline{\left(d \cdot \frac{a}{bd}\right)} \otimes \overline{\left(\frac{c}{d}\right)} = d \cdot \overline{\left(\frac{a}{bd}\right)} \otimes \overline{\left(\frac{c}{d}\right)}$$
$$= \overline{\left(\frac{a}{bd}\right)} \otimes d \cdot \overline{\left(\frac{c}{d}\right)} = \overline{\left(\frac{a}{bd}\right)} \otimes \overline{c} = \overline{\left(\frac{a}{bd}\right)} \otimes 0 = 0.$$

So $A \otimes_{\mathbb{Z}} A = \{0\}$. (<u>Note</u>: $M \otimes_R N$ is generated as an R-module by pure tensors $m \otimes n$.)

2. $R = \mathbb{C}[x,y]$, $M = (x,y) \subset R$, $t := x\otimes y - y \otimes x \in M \otimes_R M$.

a. $$\begin{aligned} x\cdot t &= x\cdot(x\otimes y) - x\cdot(y\otimes x) \\ &= x^2\otimes y - xy\otimes x \\ &= x\cdot(x\otimes y) - y\cdot(x\otimes x) \\ &= x\otimes xy - x\otimes yx = 0. \end{aligned}$$

Similarly, $y\cdot t = 0$.

b. $\varphi : M\times M \to \mathbb{C}$, $\varphi(f,g) = \frac{\partial f}{\partial x}(0,0)\cdot\frac{\partial g}{\partial y}(0,0)$

Regard $\mathbb{C}$ as an R-module via $f\cdot\lambda \underset{\dagger}{=} f(0,0)\cdot\lambda$ for $f\in R$, $\lambda\in\mathbb{C}$.

Show φ is R-bilinear:

Clearly $\varphi(f_1+f_2, g) = \varphi(f_1,g) + \varphi(f_2,g)$
& $\varphi(f, g_1+g_2) = \varphi(f,g_1) + \varphi(f,g_2)$ (b/c $\frac{\partial}{\partial x}$ & $\frac{\partial}{\partial y}$ are $\mathbb{C}$-linear)

For $h\in R$ & $f,g\in M$
$$\begin{aligned}\varphi(h\cdot f, g) &= \frac{\partial(h\cdot f)}{\partial x}(0,0)\cdot\frac{\partial g}{\partial y}(0,0) \\ &= \Big(\frac{\partial h}{\partial x}\Big|_{(0,0)}\cdot \underbrace{\cancel{f(0,0)}}_{f\in M} + h(0,0)\cdot\frac{\partial f}{\partial x}\Big|_{(0,0)}\Big)\cdot\frac{\partial g}{\partial y}\Big|_{(0,0)} \\ &= h(0,0)\cdot\varphi(f,g) \underset{\dagger}{=} h\cdot\varphi(f,g)\end{aligned}$$

Similarly $\varphi(f, h\cdot g) = h\cdot\varphi(f,g)$ for $h\in R$, $f,g\in M$. $\square$

c.
$$\begin{tikzcd} (f,g)\in M\times M \arrow[r, "\varphi"] \arrow[d] & \mathbb{C} \\ f\otimes g\in M\otimes_R M \arrow[ur, dashed, "\exists!\,\theta\ R\text{-module hom.}"'] & \end{tikzcd}$$

Now $\theta(t) = \theta(x\otimes y) - \theta(y\otimes x) = \varphi(x,y) - \varphi(y,x) = 1 - 0 = 1 \neq 0$

$\Rightarrow t \neq 0$. $\square$

4.

$$\mathrm{Hom}_S(M\otimes_R S, N) \underset{G}{\overset{F}{\rightleftarrows}} \mathrm{Hom}_R(M, {}_RN)$$

$$\theta \longmapsto (m \mapsto \theta(m\otimes 1))$$

$$(m\otimes s \mapsto s\cdot\psi(m)) \longleftarrow\!\shortmid\ \psi$$

First, check F & G are well defined :-

$F(\theta)$ is an R-module hom :- $\quad F(\theta)(m_1+m_2) = \theta((m_1+m_2)\otimes 1) = \theta(m_1\otimes 1 + m_2\otimes 1)$

$$= \theta(m_1\otimes 1) + \theta(m_2\otimes 1) = F(\theta)(m_1) + F(\theta)(m_2)$$

$$F(\theta)(rm) = \theta((rm)\otimes 1) = \theta(r\cdot(m\otimes 1))$$

$$= r\cdot\theta(m\otimes 1) = r\cdot F(\theta)(m)$$

$G(\psi)$ is well defined R-module hom :

$$M\times S \longrightarrow {}_RN \qquad (m,s) \longmapsto s\cdot\psi(m)$$

is R bilinear (where S is an R-module via $r\cdot s := \varphi(r)\cdot s$) :-

$$(m_1+m_2, s) \mapsto s\cdot\psi(m_1+m_2) = s\cdot(\psi(m_1)+\psi(m_2)) = s\cdot\psi(m_1) + s\cdot\psi(m_2)$$

$$(m, s_1+s_2) \mapsto (s_1+s_2)\cdot\psi(m) = s_1\cdot\psi(m) + s_2\cdot\psi(m)$$

$$(rm, s) \mapsto s\cdot\psi(rm) = s\cdot(r\cdot\psi(m)) = s\cdot\varphi(r)\psi(m) = \varphi(r)\cdot s\psi(m)$$

$$= r\cdot s\psi(m)$$

$$(m, r\cdot s) \mapsto r\cdot s\cdot\psi(m) = \varphi(r)\cdot s\cdot\psi(m) = r\cdot(s\cdot\psi(m)).$$

So, induces hom $\quad G(\psi): M\otimes_R S \longrightarrow {}_RN \quad$ of R-modules.

$$m\otimes s \mapsto s\cdot\psi(m)$$

Finally, check hom of S-modules :-

$$s'\cdot(m\otimes s) = m\otimes s's \mapsto s's\cdot\psi(m) = s'\cdot(s\cdot\psi(m)) \ \checkmark.$$

Now, compute $G\circ F = id$ & $F\circ G = id$.

$$\theta \overset{F}{\longmapsto} (m \mapsto \theta(m\otimes 1)) \overset{G}{\longmapsto} (m\otimes s \mapsto s\cdot\theta(m\otimes 1) = \theta(s\cdot(m\otimes 1)) = \theta(m\otimes s)). \ \checkmark$$

$$\psi \overset{G}{\longmapsto} (m\otimes s \mapsto s\cdot\psi(m)) \overset{F}{\longmapsto} (m \mapsto 1\cdot\psi(m) = \psi(m)) \ \checkmark\!/\!/ . \ \square.$$

(Lastly, check F & G homs of abelian groups (i.e. $F(\theta_1+\theta_2) = F(\theta_1)+F(\theta_2)$, $G(\psi_1+\psi_2) = G(\psi_1)+G(\psi_2)$ – clear.).

5. R local ring, $\mathfrak{m} \subset R$ the unique maximal ideal, M R-module, $m_1, \dots, m_n \in M$,

such that $\bar{m}_1, \dots, \bar{m}_n$ generate $M/\mathfrak{m}M = M \otimes_R R/\mathfrak{m} = M \otimes_R k$ as a k vector space.

Then $m_1, \dots, m_n$ generate M as an R-module :-

Let $\varphi : R^n \longrightarrow M$ be the R-module hom determined by the m_i.
$$e_i \longmapsto m_i$$

Let $C = \operatorname{coker}(\varphi)$, so $R^n \xrightarrow{\varphi} M \longrightarrow C \longrightarrow 0$ is exact.

Apply $- \otimes_R R/\mathfrak{m} = - \otimes_R k$: $k^n \longrightarrow M \otimes_R k \longrightarrow C \otimes_R k \longrightarrow 0$ exact
$e_i \longmapsto \bar{m}_i$ (right exactness of $(\cdot) \otimes_R N$ for N an R-module)

By our assumption, $k^n \to M \otimes_R k$ is surjective, so $C \otimes_R k = 0$ by exactness.

$C \otimes_R k = C/\mathfrak{m} \cdot C$, so $\mathfrak{m} \cdot C = C$.

C is f.g. R-module (b/c M is f.g. R-module & $M \twoheadrightarrow C$ by definition of C).

So $C = 0$ by Nakayama's lemma, i.e. φ is surjective, $m_1, \dots, m_n$ generate M as an R-module. $\square$

6. Recall the Dehn invariant of a polytope $P \subset \mathbb{R}^3$:

$$D(P) = \sum_{i=1}^{r} l_i \otimes \alpha_i \in \mathbb{R} \otimes_{\mathbb{Z}} \mathbb{R}/\pi\cdot\mathbb{Z}$$

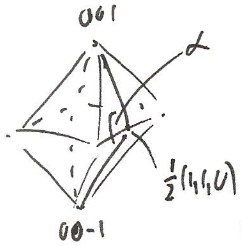
where $l_1, \dots, l_r$ are the lengths of the edges of P & α_i is the dihedral angle along edge i.

If P is subdivided into P_1 & P_2 by a plane cut, then

$D(P) = D(P_1) + D(P_2)$.

The Dehn invariant of a cube equals 0.

So, to show that an octahedron P cannot be dissected by plane cuts & reassembled to form a cube, it suffices to show $D(P) \neq 0 \in \mathbb{R} \otimes_{\mathbb{Z}} \mathbb{R}/\pi\cdot\mathbb{Z}$.



$D(P) = (12\, l) \otimes \alpha$

where l = edge length & α = dihedral angle.

So, by Lemma proved in class, $D(P) = 0 \iff \alpha \in \mathbb{Q}\cdot\pi$.

To compute α, can take octahedron w/ vertices $\pm e_1, \pm e_2, \pm e_3$.

Then α = angle between vectors $\begin{pmatrix} -1/2 \\ -1/2 \\ 1 \end{pmatrix}$ & $\begin{pmatrix} -1/2 \\ -1/2 \\ -1 \end{pmatrix}$

$$= \cos^{-1}\left(\frac{\begin{pmatrix} -1/2 \\ -1/2 \\ 1 \end{pmatrix}\cdot\begin{pmatrix} -1/2 \\ -1/2 \\ -1 \end{pmatrix}}{\left\|\begin{pmatrix} -1/2 \\ -1/2 \\ 1 \end{pmatrix}\right\|\cdot\left\|\begin{pmatrix} -1/2 \\ -1/2 \\ -1 \end{pmatrix}\right\|}\right) = \cos^{-1}\left(\frac{-1/2}{3/2}\right) = \cos^{-1}\left(-1/3\right)$$

recall $\underline{a}\cdot\underline{b} = \|\underline{a}\|\cdot\|\underline{b}\|\cos\theta$

Now, as stated in class, $\cos\left(\frac{m}{n}\cdot\pi\right) \in \mathbb{Q} \Rightarrow \cos(m/n\,\pi) = 0, \pm\frac{1}{2}, \pm 1$

Proof later using Galois theory.

Thus $\cos^{-1}(-1/3) \notin \mathbb{Q}\cdot\pi$. $\square$.

7. If F is a field then either $\mathbb{Z}/p\mathbb{Z} \subset F$ or $\mathbb{Q} \subset F$

some prime p — $\times$ if F finite.

Now F finite dimensional v.s. / $\mathbb{Z}/p\mathbb{Z}$ (using F finite again)

$\Rightarrow F \cong (\mathbb{Z}/p\mathbb{Z})^n$, some $n \geq 1$, as $\mathbb{Z}/p\mathbb{Z}$ v.s.

$\Rightarrow |F| = p^n$. $\square$.

8. $F = \text{ff}\,(\mathbb{Z}/p\mathbb{Z}\,[t]) = \mathbb{Z}/p\mathbb{Z}\,(t) := \left\{ \frac{a_0 + \dots + a_n t^n}{b_0 + \dots + b_m t^m} \;\middle|\; a_i, b_j \in \mathbb{Z}/p\mathbb{Z},\ b_j \text{ not all zero.} \right\}$

"fraction field".

9. $f = x^3 - x + 1$.

a. f irred over $\mathbb{Q}$:- since $\deg f \leq 3$, suffices to show f has no roots in $\mathbb{Q}$.

If $\alpha = a/b$ is a rational root of $f = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ then $b \mid a_n$ & $a \mid a_0$.
$\gcd(a,b) = 1$. Our case: $\alpha = \pm 1$. Just check $f(\pm 1) \neq 0$. So f irred $/\mathbb{Q}$.

b.

$$\alpha \leftrightarrow x$$

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha] \simeq \mathbb{Q}[x]/(f)$$

α alg. $/\mathbb{Q}$ basis $1, x, x^2$ $/\mathbb{Q}$

$\Rightarrow$ K has basis $1, \alpha, \alpha^2$ $/\mathbb{Q}$

$$(1+\alpha+\alpha^2)^{-1} = c_0 + c_1\alpha + c_2\alpha^2 \quad ?$$

$$g(x) = 1 + x + x^2$$

$\gcd(f,g) = 1 \Rightarrow \exists\, a, b \in \mathbb{Q}[x] . \; af + bg = 1$
E.A.

b/c f irred, $f \nmid g$ $\Rightarrow$ $\bar{b} \cdot \bar{g} = 1$ mod f

$\Rightarrow$ $b(\alpha) \cdot g(\alpha) = 1 \in \mathbb{Q}(\alpha)$, $\quad b(\alpha) = g(\alpha)^{-1}$.

E.A.:-

$$f = x^3 - x + 1 = q \cdot g + r$$

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

$$(x^2+x+1) = (-x-3)\cdot(-x+2) + 7$$

$$7 = (x^2+x+1) + (x+3)\cdot(-x+2) = (x^2+x+1) + (x+3)\cdot\left((x^3-x+1) - (x-1)(x^2+x+1)\right)$$

$$= (x+3)\cdot f + (1 - (x+3)(x-1))\underbrace{(x^2+x+1)}_{g}$$

$$1 = \frac{(x+3)}{7} \cdot f + \underbrace{\tfrac{1}{7}(4 - 2x - x^2)}_{b} \cdot g$$

$$\therefore \; (1+\alpha+\alpha^2)^{-1} = g(\alpha)^{-1} = b(\alpha) = \tfrac{1}{7}(4 - 2\alpha - \alpha^2) \quad \square.$$

10. $\alpha = \sqrt{2} + i$

a. $(\alpha - \sqrt{2})^2 = -1$,

$\alpha^2 - 2\sqrt{2}\alpha + 2 = -1$, $\quad (\alpha^2+3)^2 = (2\sqrt{2}\alpha)^2$, $\quad \alpha^4 + 6\alpha^2 + 9 = 8\alpha^2$, $\quad \alpha^4 - 2\alpha^2 + 9 = 0$.

We claim $f = x^4 - 2x^2 + 9$ is irred $/\mathbb{Q}$, so f is the min poly of α $/\mathbb{Q}$.

One can infer from the previous calc. that the roots of f in $\mathbb{C}$ are $\pm\sqrt{2} \pm i$. $\notin \mathbb{Q}$.

Also, given two roots α_1, α_2 of f, $\alpha_1 + \alpha_2 \notin \mathbb{Q}$ unless $\alpha_2 = -\alpha_1$,

in which case $\alpha_1 \alpha_2 \notin \mathbb{Q}$. So $(x-\alpha_1)(x-\alpha_2) \notin \mathbb{Q}[x]$.

So f is not the product of two quadratic factors in $\mathbb{Q}[x]$.

Thus f is irreducible $/\mathbb{Q}$.

b. $\alpha^2 - 2\sqrt{2}\alpha + 3 = 0$.

$x^2 - 2\sqrt{2}x + 3 \in \mathbb{Q}(\sqrt{2})[x]$ is the min poly of α $/ \mathbb{Q}(\sqrt{2})$

(<u>Note</u>: $\alpha \notin \mathbb{Q}(\sqrt{2})$ because $\alpha \notin \mathbb{R}$, so this poly is irred $/\mathbb{Q}(\sqrt{2})$)

c. $(\alpha - i)^2 = 2$

$\alpha^2 - 2i\alpha + i^2 = 2$

$\alpha^2 - 2i\alpha - 3 = 0$.

$x^2 - 2ix - 3 \in \mathbb{Q}(i)[x]$ is the min poly of α $/\mathbb{Q}(i)$

(<u>Note</u>: $\alpha \notin \mathbb{Q}(i)$ (because $[\mathbb{Q}(\alpha):\mathbb{Q}] = 4$ by a, but $[\mathbb{Q}(i):\mathbb{Q}] = 2$),

so this poly is irred. $/\mathbb{Q}(i)$).

d. $\alpha^2 = 2 + 2\sqrt{2} \cdot i + i^2 = 1 + 2\sqrt{-2}$

$x^2 - (1 + 2\sqrt{-2}) \in \mathbb{Q}(\sqrt{-2})[x]$ is the min poly of α $/\mathbb{Q}(\sqrt{-2})$

(<u>Note</u>: $\alpha \notin \mathbb{Q}(\sqrt{-2})$ so this poly irred $/\mathbb{Q}(\sqrt{-2})$)

as in c.

11. $\alpha = \sqrt[3]{2}$. min poly of α $/\mathbb{Q}$ is $f = x^3 - 2$ (E.C.)

$\beta = 1 + \alpha^2$. Min poly of β $/\mathbb{Q}$?

$\mathbb{Q}(\alpha)$ has basis $1, \alpha, \alpha^2$

$\beta \in \mathbb{Q}(\alpha) \Rightarrow [\mathbb{Q}(\beta):\mathbb{Q}] \leq [\mathbb{Q}(\alpha):\mathbb{Q}] = 3$

$\underset{\deg g,\ g \text{ min poly of } \beta / \mathbb{Q}.}{\overset{\shortparallel}{}}$

Now compute in basis $1, \alpha, \alpha^2$ of $\mathbb{Q}[\alpha]$:-

$$1 = 1$$

$$\beta = 1+\alpha^2$$

$$\beta^2 = 1+2\alpha^2+\alpha^4 \overset{\alpha^3=2}{=} 1+\cancel{}2\alpha+2\alpha^2$$

$$\beta^3 = 1+3\alpha^2+3\alpha^4+\alpha^6 = 5+6\alpha+3\alpha^2$$

$$\begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 0 & 2 & 6 \\ 0 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = 0. \quad \text{---} \quad c_3\beta^3 + \dots + c_0 = 0.$$

$$\begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 0 & 2 & 6 \\ 0 & 1 & 2 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 2 & 6 \end{pmatrix} \div 2 \xrightarrow{-R2} \begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \end{pmatrix} \xrightarrow[-2R3]{+R3} \begin{pmatrix} 1 & 0 & -1 & 2 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 3 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 5 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

$\rightsquigarrow$ $c_0 = -5c_3$, $c_1 = 3c_3$, $c_2 = -3c_3$ $\rightsquigarrow$ min poly x^3-3x^2+3x-5 of β / $\mathbb{Q}$. $\square$.

(Alternative approach (in this example): $(\beta-1)^3 = (\alpha^2)^3 = \alpha^6 = (\alpha^3)^2 = 4.$

$\Rightarrow \beta^3-3\beta^2+3\beta-5=0.$

Now check x^3-3x^2+3x-5 irred.

(in fact suffices to observe $\beta \notin \mathbb{Q}$ by Q14.)

17. Obviously $x = \zeta_n = e^{2\pi i/n}$ satisfies $x^n - 1 = 0$.

$n=4$: $\quad x^4-1 = (x^2-1)(x^2+1) = (x-1)(x+1)\underbrace{(x^2+1)}_{\text{min poly of } \zeta_4 = i}$

$n=6$: $\quad x^6-1 = (x^3-1)(x^3+1) = (x-1)(x^2+x+1)(x+1)\underbrace{(x^2-x+1)}_{\text{min poly of } \zeta_6.}$

$n=8$: $\quad x^8-1 = (x^4-1)(x^4+1) = \underbrace{(x-1)(x+1)(x^2+1)}_{n=4} \cdot \underbrace{(x^4+1)}_{\text{min poly of } \zeta_8}$

$\left(\zeta_8 = \frac{1+i}{\sqrt{2}},\ \zeta_8^2 = \zeta_4 = i \Rightarrow i, \sqrt{2} \in \mathbb{Q}[\zeta_8] \overset{Q10a}{\Rightarrow} [\mathbb{Q}[\zeta_8]:\mathbb{Q}] \geq 4 \Rightarrow x^4+1 \text{ irred } / \mathbb{Q} \right).$

$n=9$: $x^9-1 = (x^3-1)(x^6+x^3+1)$

$= (x-1)(x^2+x+1)\underbrace{(x^6+x^3+1)}_{\text{min poly of } \zeta_9}$

$\left(\frac{1}{2}(\zeta_9+\zeta_9^{-1}) = \cos^{2\pi}/9,\ \zeta_9^3 = \zeta_3 \Rightarrow \zeta_3, \cos\frac{2\pi}{9} \in \mathbb{Q}(\zeta_9) \Rightarrow [\mathbb{Q}(\zeta_9):\mathbb{Q}] \geq 6\right.$

$\left.\Rightarrow x^6+x^3+1 \text{ irred.}\right)$

$[\mathbb{Q}(\zeta_3):\mathbb{Q}]=2,\ [\mathbb{Q}(\cos^{2\pi}/9):\mathbb{Q}]=3$ cf. Q18,
& $\gcd(2,3)=1$.

$n=10$. $x^{10}-1 = (x^5-1)(x^5+1)$

$= (x-1)(x^4+\dots+1)(x+1)\underbrace{(x^4-x^3+x^2-x+1)}_{\text{min poly of } \zeta_{10}.}$

$\left(\zeta_{10}^2 = \zeta_5 \Rightarrow [\mathbb{Q}(\zeta_{10}):\mathbb{Q}] \geq [\mathbb{Q}(\zeta_5):\mathbb{Q}] \overset{\text{E.C.}}{=} 4 \Rightarrow x^4-x^3+x^2-x+1 \text{ irred}\right)$

$n=12$ $x^{12}-1 = (x^6-1)(x^6+1) = \underbrace{(x-1)(x^2+x+1)(x+1)(x^2-x+1)}_{n=6}(x^2+1)\underbrace{(x^4-x^2+1)}_{\text{min poly of } \zeta_{12}}$

$\left(\zeta_{12}^3 = \zeta_4 = i,\ \zeta_{12}^2 = \zeta_6 = \frac{1+\sqrt{3}i}{2} \Rightarrow i, \sqrt{3} \in \mathbb{Q}(\zeta_{12}) \Rightarrow [\mathbb{Q}(\zeta_{12}):\mathbb{Q}] \geq 4 \Rightarrow x^4-x^2+1 \text{ irred}\right).$

Rk: In fact, we will prove later that the min poly $\Phi_n(x)$ of ζ_n over $\mathbb{Q}$ has degree

$\phi(n) = \#\{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n)=1\} = |(\mathbb{Z}/n\mathbb{Z})^\times|$

& $\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x-\zeta^a).$

13. a. $i \in \mathbb{Q}(\sqrt{-2}) \Rightarrow i = a+b\sqrt{-2}$ $a,b \in \mathbb{Q}$

$\Rightarrow -1 = (a^2-2b^2)+2ab\sqrt{-2}$

$\Rightarrow a^2-2b^2=-1$ & $2ab=0$ $(1, \sqrt{-2}$ is basis of $\mathbb{Q}(\sqrt{-2})/\mathbb{Q})$

$\Rightarrow a=0$ & $b^2=\frac{1}{2}$ #

OR $b=0$ & $a^2=-1$ #. So $i \notin \mathbb{Q}(\sqrt{-2})$.

b. $\mathbb{Q}(\sqrt[4]{-2}) = \mathbb{Q}(e^{i\pi/4}\cdot\sqrt[4]{2}) = \mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\cdot\sqrt[4]{2}\right)$

& $(\sqrt[4]{-2})^2 = \sqrt{-2} = i\cdot\sqrt{2}$.

So if $i \in \mathbb{Q}(\sqrt[4]{-2}) \Rightarrow i, \sqrt{2} \in \mathbb{Q}(\sqrt[4]{-2}) \Rightarrow \sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{-2})$ #

because $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{-2}):\mathbb{Q}] = 4$ (E.C.)

& $\mathbb{Q}(\sqrt[4]{2}) \neq \mathbb{Q}(\sqrt[4]{-2})$ (e.g. b/c $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$, $\mathbb{Q}(\sqrt[4]{-2}) \not\subset \mathbb{R}$).

$\therefore\ i \notin \mathbb{Q}(\sqrt[4]{-2})$

c. x^3+x+1 is irred / $\mathbb{Q}$ (cf. Q4a)

so $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$. Now $[\mathbb{Q}(i):\mathbb{Q}] = 2$, & $2 \nmid 3 \Rightarrow i \notin \mathbb{Q}(\alpha)$. □

14. $F \subsetneq F(\alpha) \subset K$, $[K:F] = p$, prime.

$[K:F(\alpha)]\cdot[F(\alpha):F] = [K:F]$, $\underbrace{[F(\alpha):F] \neq 1}_{\text{Q15a}} \Rightarrow \begin{cases} [F(\alpha):F] = p \Rightarrow K = F(\alpha). \\ [K:F(\alpha)] = 1 \quad \text{(Q15a)} \end{cases}$

15 a. $F \subset K$

$[K:F] = \dim_F K = 1$.

Now $\dim_F F = 1$, $F \subset K \Rightarrow F = K$.

b. $[K:F] = 2$, $\operatorname{char} F \neq 2$.

Let $\alpha \in K \setminus F$ ($F \neq K$ b/c $[K:F] \neq 1$)

Then $1, \underset{\in K}{\alpha}$ are linearly independent over F $\underset{[K:F]=2}{\Rightarrow}$ $1, \alpha$ is a basis of K as F v.s.

Now $\alpha^2 = a + b\alpha$, $a, b \in F$. using $\operatorname{char}(F) \neq 2$, so $2 \neq 0 \in F$.

Complete the square: $\alpha' := (\alpha - b/2) \leadsto \alpha'^2 = (a + b^2/4) \in F$. $K = F(\alpha')$.

$= \{0, 1, \alpha, 1+\alpha\}$'s

(. $F = \mathbb{F}_2 \subset K = \mathbb{F}_4 \simeq \mathbb{F}_2[x] / (x^2+x+1)$

$\alpha \leftarrow\!\shortmid x$

$\alpha^2 = \alpha + 1$

Check $\alpha^2 = \alpha+1 \notin F$

$(1+\alpha)^2 = \alpha \notin F.$

16.

$$\begin{tikzcd}
& F(\alpha,\beta) & \\
F(\alpha) \arrow[ur, phantom, "\subset" sloped] & & F(\beta) \arrow[ul, phantom, "\supset" sloped] \\
& F \arrow[ul, phantom, "\supset" sloped] \arrow[ur, phantom, "\subset" sloped] &
\end{tikzcd}$$

$$[F(\alpha,\beta):F] = \overset{\substack{n \\ \vee\!|}}{[F(\alpha,\beta):F(\alpha)]} \cdot \overset{\substack{m \\ \shortparallel}}{[F(\alpha):F]} \qquad (*)$$

$$= \underset{\substack{\wedge\!| \\ m}}{[F(\alpha,\beta):F(\beta)]} \cdot \underset{\substack{\shortparallel \\ n}}{[F(\beta):F]}$$

$\rightsquigarrow$ $m, n \mid [F(\alpha,\beta):F]$, $[F(\alpha,\beta):F] \leq mn$

$\gcd(m,n) = 1 \implies [F(\alpha,\beta):F] = mn.$

Basis for $F(\alpha)$ over F : $1, \alpha, \dots, \alpha^{m-1}$

Basis for $F(\alpha,\beta)$ over $F(\alpha)$: $1, \beta, \dots, \beta^{n-1}$ (using $[F(\alpha,\beta):F(\alpha)] = n$ by $(*)$)

$\rightsquigarrow$ Basis for $F(\alpha,\beta)$ over F: $\{\alpha^i\beta^j \mid 0 \leq i \leq m-1,\ 0 \leq j \leq n-1\}$. $\square$.

17. $F \subset F(\alpha^2) \subset F(\alpha) = K.$

$[F(\alpha):F(\alpha^2)] = 1$ or 2 because α satisfies poly eq. $\underbrace{x^2 - \alpha^2}_{} = 0$ w/ coefficients in $F(\alpha^2)$.

$[F(\alpha):F(\alpha^2)] \mid [K:F]$, odd $\implies [F(\alpha):F(\alpha^2)] = 1$

$\implies F(\alpha) = F(\alpha^2).$ $\square$.

18. $e^{i\theta} = \cos\theta + i\sin\theta$

$\implies \cos 3\theta = \mathrm{Re}\left((e^{i\theta})^3\right) = (\cos\theta)^3 - 3(\sin\theta)^2 \cdot \cos\theta = (\cos\theta)^3 - 3(1-(\cos\theta)^2)\cdot\cos\theta$

$= 4(\cos\theta)^3 - 3\cos\theta.$

$\cos \pi/3 = 1/2$ ($\implies \pi/3$ constructible). So $\cos \pi/9 =: \alpha$ satisfies $1/2 = 4\alpha^3 - 3\alpha$

$0 = 8\alpha^3 - 6\alpha - 1$

Check $8x^3 - 6x - 1$ irred / $\mathbb{Q}$ (cf. Q9a)

$\Rightarrow$ $[\mathbb{Q}(\alpha):\mathbb{Q}] = 3$ $\Rightarrow$ angle $\pi/9$ not constructible $\Rightarrow$ angle $\pi/3$ not trisectable $\square$.

19. $\zeta = e^{2\pi i/5}$. $\alpha := \cos 2\pi/5 = \frac{1}{2}(\zeta + \zeta^{-1})$.

Min poly of ζ over $\mathbb{Q}$: $x^4 + x^3 + x^2 + x + 1 = 0$ (E.C.)

So $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$.

$\zeta^2 + \zeta + 1 + \zeta^{-1} + \zeta^{-2} = 0$.

$$\underbrace{\left(2\cos 2\pi/5\right)^2}_{\zeta^2 + 2 + \zeta^{-2}} + \underbrace{\left(2\cos 2\pi/5\right)}_{\zeta + \zeta^{-1}} - 1 = 0.$$

$4\alpha^2 + 2\alpha - 1 = 0$.

$$\underset{\text{QF}}{\alpha =} \frac{-2 \pm \sqrt{4 + 16}}{8} \underset{\alpha > 0}{=} \frac{\sqrt{5} - 1}{4}$$

$\Rightarrow$ $\overset{\cos(2\pi/5)}{\alpha}$ constructible length

$\Rightarrow$ $2\pi/5$ constructible angle

$\Rightarrow$ regular pentagon is constructible. $\square$

20.

$$\begin{array}{ccccc} \omega\sqrt[3]{2} & \longleftarrow & x & \longmapsto & \sqrt[3]{2} \\ \mathbb{Q}(\omega\sqrt[3]{2}) & \xleftarrow{\sim} & \mathbb{Q}[x]/(x^3 - 2) & \xrightarrow{\sim} & \mathbb{Q}(\sqrt[3]{2}) \end{array}$$

$\varphi: \mathbb{Q}(\omega\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$

$x^3 - 2$ irred / $\mathbb{Q}$ (E.C.)

i.e. have isomorphism of fields $\mathbb{Q}(\omega\sqrt[3]{2}) \xrightarrow{\sim} \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$.

Now (-1) cannot be written as a sum of squares in $\mathbb{Q}(\sqrt[3]{2})$ (because $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$),

so same is true in $\mathbb{Q}(\omega\sqrt[3]{2})$ $\square$.