algebra   hw 5?

$\frac{35}{35}$

① (12.4.1) (long division done on scratch paper)

ⓐ factor $x^9 - x$, $x^9 - 1$ in $\mathbb{F}_3[x]$ PID ⇒ prime ⟷ irred.

$(x-1)^9 = \sum_{k=0}^{n} \binom{9}{k} x^k$.   note: $3 \mid \binom{9}{k} = \frac{9!}{k!(9-k)!}$ for $k \in \{1 \ldots 8\}$

$\Rightarrow \underbrace{(x-1)^9}_{\text{prime in } \mathbb{F}_3[x]} \equiv_3 x^9 - 1$. ✓

$x^9 - x = \underset{\text{prime}}{x}(x^8-1)$ so, does x^8-1 have a root mod 3? ie does (x^2-1)
yes, 2 and 1

$= x(x-1)(x^7+x^6+x^5+x^4+x^3+x^2+1)$ 1 not a root, 0 not a root. 2 must be a root by above

$= x(x-1)(x+1)(x^6+x^4+x^2+1)$ ← no more roots in $\mathbb{F}_3$, but note i is a root the. try $\underbrace{(x^2+1)}_{\text{irred in } \mathbb{F}_3[x]}$

5

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

$= x(x-1)(x+1)(x^2+1)(x^2+x-1)(x^2-x-1)$. ← all irred. (artin) ✓

ⓑ $x^{16} - x$ in $\mathbb{F}_2[x]$. again PID: irred ⟷ prime.

$x^{16} - x = x(x^{15}-1) = x(x-1)\underbrace{(x^{14}+x^{13}+\ldots+1)}_{\text{try } x^4+x^3+x^2+x+1}$ note $15 \equiv_2 1 \Rightarrow$ no more linear factors (1 not a root)

← irred from artin ✓

try x^2+x+1

$= x(x+1)\underbrace{(x^4+x^3+x^2+1)}_{\text{irred}}(x^{10}+x^5+1)$ +x

try $\cancel{x^3+x^2+1}$ x^4+x^3+1 ✓

$= x(x+1)(x^4+x^3+x^2+1)\underbrace{(x^2+x+1)}_{\text{irred}}(x^8+x^7+x^5+x^4+x^3+x+1)$ +x

$= x(x+1)(x^4+x^3+x^2+1)(x^2+x+1)\underbrace{(x^4+x^3+1)(x^4+x+1)}_{\text{irred}}$. +x

② (12.4.3) decide whether or not x^4+6x^3+9x+3 gen. a max ideal in $\mathbb{Q}[x]$

$\mathbb{Q}[x]$ is a PID. so, if (x^4+6x^3+9x+3) is irred. in $\mathbb{Q}[x]$, then gen. a max ideal.

x^4+6x^3+9x+3 primitive in $\mathbb{Z}[x]$, so sts irreducible in $\mathbb{Z}[x]$

suppose $x^4+6x^3+9x+3 = p(x)q(x)$ for some $p(x), q(x) \in \mathbb{Z}[x]$.

5

now consider in $\mathbb{Z}[x]/(2)$. $\overline{x^4+6x^3+9x+3} = x^4+x+1 = \overline{p(x)}\,\overline{q(x)}$. but, ✓

x^4+x+1 irred in $\mathbb{F}_2[x] \Rightarrow \overline{p(x)} = 1$ or $\overline{q(x)} = 1$. wlog. $\overline{p(x)} = 1$

$\Rightarrow 2 \mid \text{lead}(p(x)) \Rightarrow 2 \mid \text{lead}(p(x)q(x))$ # contradiction
(b/c x^4+6x^3+9x+3 primitive)

$\therefore$ x^4+6x^3+9x+3 irred in $\mathbb{Z}[x] \Rightarrow x^4+6x^3+9x+3$ irred. in $\mathbb{Z}[x]$

$\Rightarrow (x^4+6x^3+9x+3)$ is maximal in $\mathbb{Q}[x]$ (irred.) ✓

③ (12.4.5) which of the following are irreducible in $\mathbb{Q}[x]$?

recall: if irred. in $\mathbb{Z}[x]$ then irreducible in $\mathbb{Q}[x]$. Let $p(x) \in \mathbb{Z}[x]$. if $p(x) = q(x)r(x)$
so, our technique is to look at in $\mathbb{F}_p[x]$ st $\overline{p(x)} = \overline{q(x)}\,\overline{r(x)}$. if irreducible in $\mathbb{F}_p[x]$ then wlog assume $p \mid \text{lead}(q(x))$. if $p \nmid \text{lead}(p(x))$ then $p(x)$ irred in $\mathbb{Z}[x]$ and hence $\mathbb{Q}[x]$. otherwise use a reduction to reduce in $\mathbb{Q}[x]$

ⓐ $x^2 + 27x + 213 \in \mathbb{Q}[x]$. look at $x^2 + 27x + 213 \in \mathbb{Z}[x]$.

note: $2 \nmid \text{lead}(x^2+27x+213)$ so $x^2 + 27x + 213 \equiv x^2 + x + 1$ in $\mathbb{F}_2[x]$

$x^2 + x + 1$ irred $\Rightarrow$ by above logic, $x^2+27x+213$ irred in $\mathbb{Z}[x]$

$\Rightarrow x^2 + 27x + 213$ irred. in $\mathbb{Q}[x]$.

ⓑ $8x^3 - 6x + 1$ in $\mathbb{Q}[x]$. again $\rightsquigarrow \mathbb{Z}[x] \rightsquigarrow \mathbb{F}_7[x]$

5

$8x^3 - 6x + 1 \equiv_7 x^3 + x + 1$ if reducible, then has a root mod 7 (splits to linear and quad.)

so sts no roots. plugging in:

$\cancel{0}\to 1,\ \cancel{1}\to 3,\ \cancel{2}\to 3,\ \cancel{3}\to 3,\ \cancel{4}\to 6,\ \cancel{5}\to 5,\ \cancel{6}\to 6$ $\rightsquigarrow$ so, no roots. $\Rightarrow$ irred in $\mathbb{F}_7[x]$

$\Rightarrow$ irred. in $\mathbb{Q}[x]$.

ⓒ $x^3 + 6x^2 + 1 \rightsquigarrow \mathbb{F}_5[x]$ congr. to $x^3 + x^2 + 1$ again, sts no roots b/c cubic.

plugin: $\cancel{0}\to 1,\ \cancel{1}\to 3,\ \cancel{2}\to 3,\ \cancel{3}\to 2,\ \cancel{4}\to 1$ no roots so, irred in $\mathbb{Q}[x]$.

ⓓ $x^5 - 3x^4 + 3 \rightsquigarrow \mathbb{F}_2[x]$ congr. to $x^5 + x^4 + 1$ if it

show work

factors must be irred. of deg at most 2 $\cancel{x}$, $\cancel{x+1}$, $x^2 + \cancel{x} + 1$

these are all the irreducible poly deg ≤ 2 in $\mathbb{F}_2[x]$ so $x^5 + x^4 + 1$ irred.

$\Rightarrow x^5 - 3x^4 + 3$ irred. in $\mathbb{Q}[x]$

④ (12.4.12) determine

ⓐ monic irred. polynomials of deg 3 over $\mathbb{F}_3$.

possibilities: given 3 monic and 3 quad $\rightsquigarrow 3\cdot 3 + \frac{3^3}{3} \to 9$ irred. (look $a_0 \neq 0$ o.w. x is factor)
2 poss. for a_0, 3 for a_1, 3 for $a_2 \Rightarrow 18$

check for roots: $\cancel{x^3+1}$, $\cancel{x^3-1}$, $\cancel{x^3+x+1}$, $x^3+\cancel{x}-1$, x^3-x+1, x^3-x-1

$x^3+\cancel{x^2}+1$, x^3+x^2-1, $x^3+x^2+\cancel{x}+1$, x^3+x^2+x-1, x^3+x^2-x+1, $x^3+\cancel{x^2}-x-1$,

x^3-x^2+1, x^3-x^2-1, x^3-x^2+x+1, $x^3-\cancel{x^2}+x-1$, $x^3-\cancel{x^2}-x+1$, x^3-x^2-x-1

so irred: x^3-x+1, x^3-x-1, x^3+x^2-1, x^3+x^2+x-1, x^3+x^2-x+1,
x^3-x^2+1, x^3-x^2-1, x^3-x^2+x+1, x^3-x^2-x-1

0
0
0
1
1
1
-1
-1
-1

(b) monic irred. poly of deg 2 over $\mathbb{F}_5$

25 possibilities. 5 monic irred $\Rightarrow$ $\frac{5\cdot 4}{2}+5$ non-irred $\Rightarrow$ 10 irred. poly. deg 2 in $\mathbb{F}_5[x]$

again, skip $a_2=0$. so, 20 remaining note: squares: $1^2 \to 1$, $2^2 \to 4$, $4^2 \to 1$, $3^2 \to 4$

$\cancel{x^2+1}$, x^2+2, x^2+3, $\cancel{x^2+4}$, x^2+x+1, x^2+x+2, $\cancel{x^2+x+3}$, $\cancel{x^2+x+4}$,

$\cancel{x^2+2x+1}$, $\cancel{x^2+2x+2}$, x^2+2x+3, x^2+2x+4, $\cancel{x^2+3x+1}$, $\cancel{x^2+3x+2}$, x^2+3x+3

$\cancel{x^2+3x+4}$, x^2+4x+1, x^2+4x+2, $\cancel{x^2+4x+3}$, $\cancel{x^2+4x+4}$

so ~~irred. poly of deg 2 over~~ $\mathbb{F}_5$:

$$\boxed{x^2+2,\ x^2+3,\ x^2+x+1,\ x^2+x+2,\ x^2+2x+3,\ x^2+2x+4,\ x^2+3x+3,\ x^2+4x+1,\ x^2+4x+2}$$

(c) # of irred. poly over $\mathbb{F}_5$ deg 3. UFD so can deploy counting argument via irred. of deg 1 + 2 (I already have been doing this)

#possible poly deg 3: $5^3 = 125$

− #reducible cubics: $\#\{(\text{quad.})(\text{lin.})\} = 10\cdot 5 = 50$

$\#\{(\text{lin})(\text{lin})(\text{lin})\}$ (combination w/ rep. allowed)

$\underbrace{1\,1\,1\,0\,0\,0\,0\,0}_{n+r-1 \text{ choose } r}$ $\longrightarrow$ $= \frac{(3+5-1)!}{3!\,(5-1)!} = \frac{7\cdot 6\cdot 5}{3\cdot 6} = 35$.

$\therefore$ $125 - 85 = 40$ irred. cubics in $\mathbb{F}_5$

(5) (1R: 4.16) factor $x^{14}+8x^{13}+3$ in $\mathbb{Q}[x]$ using red. mod 3

in $\mathbb{F}_3[x]$: $x^{14}-x^{13} = x^{13}(x-1)$. suppose $x^{14}+8x^{13}+3$ factors in $\mathbb{Z}[x]$.

$\Rightarrow x^{14}+8x^{13}+3 = p(x)q(x) \equiv_3 x^{13}(x-1)$. wlog. $\overline{p(x)} = x^{13-i}$, $\overline{q(x)} = x^i(x-1)$ some $i \in \{0,\dots,13\}$

monic $\Rightarrow p(x), q(x)$ monic. if $i=0$, then $q(x) = x+8$ (b/c $p(x)$, $q(x)$ monic) but $8 \nmid 3$. ✗. contradiction.

so $i>0$. but then $\overline{p(x)} = x^{13-i} \Rightarrow$ const term $3m$, $m \neq 0$

but $\overline{q(x)} = x^{i+1} - x^i \Rightarrow$ const term $3n$, $n\neq 0$ but we only have one 3 in $x^{14}+8x^{13}+3$. ✗.

5 ✓

⑥ (15:1.2) let F be a field, not of characteristic 2, and let $x^2+bx+c=0$ be a quad equation w/ coefficients in F. ⓐ prove that if δ is an elt of F such that $\delta^2 = b^2-4c$, $x=(-b+\delta)/2$ solves the quad equ. in F
ⓑ prove also that if the discriminant b^2-4c is not a square, the poly has no root in F. (proceed as in quad formula?)

let F, field as above, $x^2+bx+c=0$ st $b, c \in F$

$$\Leftrightarrow x^2+bx=-c \overset{\text{not char. 2}}{\Leftrightarrow} x^2+bx+\underbrace{\left(\tfrac{1}{2}\right)^2}_{=1/4,\ \text{not } 0} b^2 \Leftrightarrow -c+\frac{b^2}{4} \Rightarrow \left(x+\frac{b}{2}\right)^2 \Leftrightarrow \frac{b^2-c}{4}$$

$$\Rightarrow \frac{(2x+b)^2}{4} = \frac{b^2-4c}{4} \Rightarrow (2x+b)^2 = b^2-4c \Rightarrow (2x+b)^2-(\underset{\delta^2}{b^2-4c})=0$$

ⓐ

if $\exists \delta \in F$ st $\delta^2=b^2-4c$. then, under $\varphi: F[x] \longrightarrow F$, $x \longmapsto \frac{(-b+\delta)}{2}$

5

$\Rightarrow \varphi((2x+b)^2-(b^2-4c))=0$

note: $\varphi\left(x-\frac{(-b+\delta)}{2}\right)=0 \leftarrow$ irred. (notice $ev_{\frac{-b-\delta}{2}}$ also works)

(ie $F[x]/\left(x-\frac{(-b+\delta)}{2}\right) \cong F$ by first iso and $x^2+bx+c \in \ker\varphi$.)

ⓑ else, $\forall \phi \in F$, $\phi^2 \neq b^2-4c$. suppose x^2+bx+c has a root, α.

the α satisfies $(2x+b)^2-(b^2-4c)=0 \Rightarrow (2\alpha+b)^2-(b^2-4c)=0$

but $(2\alpha+b)\in F \Rightarrow (2\alpha+b)^2-(b^2-4c)\neq 0$ □

⑦ (15:2.1) let α be a complex root of x^3-3x+4 (ie $x^3-3x+4 \in \ker ev_\alpha$)
find the inverse of $\alpha^2+\alpha+1$ in the form $a+b\alpha+c\alpha^2$.

note: x^3-3x+4 has no root (mod 5) $\Rightarrow$ irred. in $\mathbb{Q} \Rightarrow \ker ev_\alpha = (x^3-3x+4)$

5

($\Rightarrow \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(x^3-3x+4)$)

so must divide: $(x^2+x+1)(a+bx+cx^2)-1 = cx^4+(b+c)x^3+(c+b+a)x^2+(a+b)x+(a-1)$

$$\begin{array}{r l}
 & cx \quad + (b+c) \\
x^3-3x+4 \,\big) & cx^4+(b+c)x^3+(c+b+a)x^2+(a+b)x+(a-1) \\
 & -(cx^4+0 \quad -3cx^2 \quad +4cx) \\
\hline
 & (b+c)x^3+(b+a+4c)x^2+(a+b-4c)x+(a-1) \\
 & -((b+c)x^3 \quad -3(b+c)x \quad +4(b+c)) \\
\hline
 & (b+a+4c)x^2+(a+4b-c)x+(a-4b-4c-1)=0
\end{array}$$

this gives us:

alt, could have used generalized euclidean alg (probably way simpler...)

$$\begin{bmatrix} 1 & 1 & 4 \\ 1 & 4 & -1 \\ 1 & -4 & -4 \end{bmatrix}\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \Rightarrow \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 1 & 1 & 4 \\ 1 & 4 & -1 \\ 1 & -4 & -4 \end{bmatrix}^{-1}\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \frac{+1}{49}\begin{bmatrix} 20 & 12 & 17 \\ -3 & 8 & -5 \\ 8 & -5 & -3 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{49}\begin{bmatrix} 17 \\ -5 \\ -3 \end{bmatrix}$$

$\Rightarrow$ so, inverse is

$$\boxed{\frac{17}{49}-\frac{5}{49}\alpha-\frac{3}{49}\alpha^2}$$

co factors: $\begin{bmatrix} -20 & +3 & -8 \\ +12 & -8 & 5 \\ -17 & +5 & 3 \end{bmatrix}^{T}$

(8) show there exist $r \in \mathbb{R}$ st r is trans/$\mathbb{Q}$.
sts $A = \{r \in \mathbb{R} \mid r \text{ is alg}/\mathbb{Q}\}$ is countable.

$\forall q \in \mathbb{Q}$, q is alg/$\mathbb{Q}$ by min. poly. $(x-q) \Rightarrow \mathbb{Q} \subset A \Rightarrow |\mathbb{Q}| \leq |A|$.

so sts $|A| \geq |\mathbb{Q}|$, in otherwords injectivity is sufficient (repetitions don't matter b/c we have a lower bound on cardinality.) (a real number is algebraic over $\mathbb{Q}$ if it is the solution to an irreducible polynomial in $\mathbb{Q}$.

Claim: $P = \{a_0 + \cdots + a_n x^n \mid a_i \in \mathbb{Q}\}$ is countable.

pf: recall that $\mathbb{Z}$ is UFD. $\Rightarrow \forall n \in \mathbb{Z}, n = p_1^{m_1} \cdots p_k^{m_k}$, $\forall i$ p_i prime w/ mult. m_i.

let $\varphi : P \longrightarrow \mathbb{N} \subset \mathbb{Z}$ defined as follows: (note: $\mathbb{N} = \{1, 2, 3, \ldots\}$)

5

(i) $\mathbb{Q}$ countable $\Rightarrow \exists$ bij. $f : \mathbb{Q} \to \aleph_0$

(ii) inf. many primes proof given in hw. (unique up to unit, but we excluded their duals)
let $p_0\, p_1\, p_2\, p_3 \cdots p_n \cdots$ be an ordering (take one imposed by $\mathbb{N}, <$) of the primes in $\mathbb{Z}$.

now, $\varphi(a_0 + a_1 x + \cdots + a_{n-1} x^n) = p_0^{f(a_0)} \cdot p_1^{f(a_1)} \cdots p_{n-1}^{f(a_{n-1})}$

not nec $\Big($ φ surj: let $n \in \mathbb{N}$. $n = q_1^{m_1} \cdots q_k^{m_k}$ q prime (in $\mathbb{Z}$, UFD)
$= p_0^{n_0} \cdots\cdots p_\ell^{n_\ell}$ ← w/og.

$\Rightarrow n = \varphi(f^{-1}(n_0) + \cdots + f^{-1}(n_\ell) x^{n_\ell})$ $\Big)$

φ inj: let $p(x) = a_0 + a_1 x + \cdots + a_n x^n \Rightarrow \varphi(p(x)) = p_0^{f(a_0)} \cdots p_i^{f(a_i)} \cdots p_n^{f(a_n)}$
$q(x) = b_0 + \cdots b_m x^m \Rightarrow \varphi(q(x)) = p_0^{f(b_0)} \cdot p_i^{f(b_i)} \cdots p_m^{f(b_m)}$
$\exists i$ st $b_i \neq a_i$ $\Rightarrow \varphi(p(x)) \neq \varphi(q(x))$ again b/c UFD.

$Q = \{\text{irred. poly over } \mathbb{Q} \text{ (min. poly.)}\} \subseteq P \Rightarrow Q$ is at most countable.

each irreducible poly has finite degree $\Rightarrow$ can be reduced to at most finitely many linear factors in $\mathbb{R}[x] \Rightarrow$ the set of algebraic numbers for each irreducible poly is at most countable, call this $A_{q(x)}$.

$\Rightarrow A = \bigcup_{q(x) \in Q} A_{q(x)}$ is at most countable b/c the at most countable union of at most countable sets is at most countable.

$\therefore |A| = \aleph_0$ but, $|\mathbb{R}| = 2^{\aleph_0}$ $(>\aleph_0)$ (uncountable) $\Rightarrow \exists r \in \mathbb{R}$ st r is not alg/$\mathbb{Q} \Rightarrow \exists r$ trans/$\mathbb{Q}$ $\square$