Midterm 2. ①

Problem 1:

(1) Let $K := \mathbb{Q}(e^{2i\pi/35})$ and $G = Gal(K/\mathbb{Q})$

K is a cyclotomic extension of $\mathbb{Q}$ so

$$G \simeq (\mathbb{Z}/_{35\mathbb{Z}})^\times \underset{\substack{\uparrow \\ \text{Chinese} \\ \text{lemma}}}{\simeq} (\mathbb{Z}/_{5\mathbb{Z}} \times \mathbb{Z}/_{7\mathbb{Z}})^\times \simeq (\mathbb{Z}/_{5\mathbb{Z}})^\times \times (\mathbb{Z}/_{7\mathbb{Z}})^\times$$

$$\underset{\substack{\uparrow \\ \text{multiplicative} \\ \text{group of finite} \\ \text{field is cyclic}}}{\simeq} \mathbb{Z}/_{4\mathbb{Z}} \times \mathbb{Z}/_{6\mathbb{Z}}$$

$|G| = 24$ but the max order of the elements in G is 6 so G is not cyclic.

Let $(\bar{a}, \bar{b}) \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \setminus \{(0,0)\}$. If $(\bar{a}, \bar{b})$ has order 2 then $2\bar{a} = \bar{0}$ in $\mathbb{Z}/4\mathbb{Z}$

$2\bar{b} = \bar{0}$ in $\mathbb{Z}/6\mathbb{Z}$

so $2 | a$ and $3 | b$.

This gives: $(\bar{2}, \bar{0})$ $(\bar{0}, \bar{3})$ $(\bar{2}, \bar{3})$ are the only elements of order 2.

(2) G is commutative so any subgroup of G is normal. By Galois correspondence, the extensions $\mathbb{Q} \subseteq L \subseteq K$ such that $L/\mathbb{Q}$ is of degree 12 are in one-to-one correspondence with the ~~subgroups~~ subgroups of G of **ORDER** $\frac{|G|}{12} = 2$

By (1) there are 3 of them.

Problem 2: $P = X^5 + 20X + 6$.

(1) $\bar{P} = X^5 - X + 2 \mod 7$

$\bar{P}(\bar{0}) = 2$; $\bar{P}(\bar{1}) = 2$; $\bar{P}(\bar{2}) = 2^5 = 8 \times 2 \times 2 = \bar{4}$
$\bar{P}(\bar{3}) = 3^5 - 1 = 9 \times 9 \times 3 - 1 \equiv 2 \times 2 \times 3 - 1 \equiv -2-1 = -\bar{3}$
$\bar{P}(\bar{4}) = \bar{P}(-\bar{3}) = (-3)^5 + 5 = 2 + 5 = 7$. (use calculation in $\bar{P}(\bar{3})$)
$\bar{P}(\bar{5}) = \bar{P}(-\bar{2}) = (-2)^5 + 4 = -4 + 4 = \bar{0}$
use calculation in $\bar{P}(\bar{2})$)

$\bar{P}(\bar{6}) = \bar{P}(-1) = -1 + 1 + 2 = 2$.

So $\bar{P}$ has roots $\{\bar{4}, \bar{5}\}$ in $\mathbb{F}_7$.

and $\exists\ Q \in \mathbb{F}_7[X]$ $\underbrace{\deg Q = 3 \quad Q \text{ with no root in } \mathbb{F}_7}$
$\Rightarrow Q$ irreducible

$$\bar{P} = (X - \bar{4})(X - \bar{5})Q.$$

and $Gal(\bar{P}/\mathbb{F}_7) = Gal(Q/\mathbb{F}_7) \simeq Gal(\mathbb{F}_{7^3}/\mathbb{F}_7)$ is cyclic of order 3.

$Gal(\bar{P}/\mathbb{F}_7) \hookrightarrow S_3$
contains an element of order 3.
The only elements of order 3 in S_3 are the 3-cycles.

(2) $\bar{P} = X^5 - X + 1 \in \mathbb{F}_3[X]$

(a) $x \in \mathbb{F}_9$. If $x = 0$ then $x^5 = \pm x$ okay
Otherwise $x^8 - 1 = 0$ so $x^4 = \pm 1$ and $x^5 = \pm x$.

(b) Let $x \in \mathbb{F}_9$. $\bar{P}(x) = \pm x - x + 1$
so either $\bar{P}(x) = 1$ or $\bar{P}(x) = -2x + 1$. For $\bar{P}(x)$ to be 0 we then need $2x = 1$ so $x \in \mathbb{F}_3$ and $x = 2$
But $\bar{P}(2) = 2^5 - 2 + 1 = \bar{1} \neq 0$.

(c) If $\bar{P}$ is not irreducible over $\mathbb{F}_3$ it has

→ ~~either~~ a factor of degree 1 and a root in $\mathbb{F}_3$

But $\bar{P}(0) = 1$

$\bar{P}(1) = 1$ so this is impossible

$\bar{P}(2) = 1$

→ or an irreducible factor of degree 2 $\bar{P} = AB$

$\deg A = 2$

$A \in \mathbb{F}_3[X]$ A irreducible

$\Rightarrow$ $\bar{P}$ has a root in $\mathbb{F}_3[X]/_{(A)} \simeq \mathbb{F}_3[\zeta]$ where ζ is a root for A in $\overline{\mathbb{F}_3}$.

But $\mathbb{F}_3[X]/_{(A)} \simeq \mathbb{F}_9$

Contradiction.

So $\bar{P}$ is irreducible in $\mathbb{F}_3[X]$.

Problem 3

(1) (a) If $\mathrm{disc}(P)$ is a square in k then $\delta \in k$ and δ is fixed by any $\sigma \in G$.

So $\varepsilon(\sigma)\delta = \delta$ $\forall \sigma \in G$.

This means $\delta(\varepsilon(\sigma) - 1) = 0$ $\Rightarrow$ $\varepsilon(\sigma) = 1$ since k has characteristic different from 2

$\Rightarrow$ $G \subseteq A_n$.

If $G \subseteq A_n$ then $\varepsilon(\sigma) = 1$ $\forall \sigma \in G$ so δ is fixed under the action of G so δ is in the base field k.

(c) (i) The condition is $\mathrm{char}\, k \neq q$.

Indeed if $\mathrm{char}\, k = q$ then $P = (X-1)^q$ is not separable.

If char $k \neq q$ then $P' = qX^{q-1}$ has 0 as a unique root in $\bar{k}$ and $P(0) \neq 0$ so $\gcd(P, P') = 1$ and P is separable.

(ii) Note first : $\prod_{k=1}^{q} (e^{2i\pi/q})^k = e^{\frac{2i\pi}{q}(1+2+3\cdots+q)}$
$= e^{\frac{2i\pi}{q}\frac{q(q-1)}{2}}$

But $\frac{q-1}{2} \in \mathbb{N}$ so
$\left(e^{\frac{2i\pi}{q}}\right)^{q\left(\frac{q-1}{2}\right)} = 1.$

This proves that the product of all roots of P is equal to 1.

$$q^* = \mathrm{disc}(P) = (-1)^{q\left(\frac{q-1}{2}\right)} \prod_{i=1}^{q} q\, x_i^{q-1}$$

where $\{x_i\}$ is the set of roots of P.

$$\text{so } q^* = (-1)^{q\frac{(q-1)}{2}} \prod_{i=1}^{q} q\, x_i^{-1} \underset{\uparrow}{=} (-1)^{q\frac{(q-1)}{2}} q^q$$

by previous remark.

(2) (a) the valuation at q of q^* is q : it is an odd number so q^* is not a square in $\mathbb{Q}$.

(b) $G = \mathrm{Gal}(X^q - 1/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(e^{2i\pi/q})/\mathbb{Q})$
$= (\mathbb{Z}/q\mathbb{Z})^\times$
$\simeq \mathbb{Z}/(q-1)\mathbb{Z}.$