Solution Galois Theory HT 2021

Problem 1

(a) Eisenstein criterion with $p=2$ or $p=5$ yields that f is irreducible $/\mathbb{Z}_4$ and so over $\mathbb{Q}$

(b) Let ζ a primitive 13 root of 1 and $\alpha = \sqrt[13]{10}$ the only positive real number such that $\alpha^{13} = 10$ then $L = \mathbb{Q}(\alpha, \zeta)$. In fact all the roots of $f(x)$ are of the form $\alpha\zeta^i$ for $i = 0 - 12$.

Thus $f(x)$ splits on $\mathbb{Q}(\alpha, \zeta)$ and $\mathbb{Q}(\alpha, \zeta) \supseteq L$. On the other side $L \supseteq \mathbb{Q}$ $\alpha \in L$ and $\alpha \cdot \zeta \in L$

Since L contains all the roots of $f(x)$

In particular $\alpha \in L$, $\frac{\alpha \cdot \zeta}{\alpha} = \zeta \in L$

$\Rightarrow \quad L \supseteq \mathbb{Q}(\alpha, \zeta)$

We deduce that $L = \mathbb{Q}(\alpha, \zeta)$

(c) $[L : \mathbb{Q}] = 13 \cdot 12$

$\mathbb{Q} \subseteq \mathbb{Q}(\alpha)$ is an extension of deg 13.

$\mathbb{Q} \subseteq \mathbb{Q}(\zeta)$ is an

an extension of order 12.

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\alpha, \zeta)$$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 13$ $\qquad$ $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] \leq 12$

$[L : \mathbb{Q}] \leq 13 \cdot 12$

On the other side $L \supseteq \mathbb{Q}(\alpha) \cdot \mathbb{Q}(\zeta)$

which has deg $13 \cdot 12$ / Φ since

$\gcd(13, 12) = 1$

$\Rightarrow [L : \mathbb{Q}] = 13 \cdot 12$

(d) L is the splitting field of

$x^{13} - 10$ which is irreducible

and so separable since $\text{char } \mathbb{Q} = 0$

So is Galois.

Problem 2

(a) we have the tower of exten

$|\text{Gal}(F)| = 13 \cdot 12$ since $L/\mathbb{Q}$

is Galois . . .

By Sylow thm $\text{Gal}(F)$ admits a unique, and hence normal subgp of order 13, N. $[\text{Gal}(F) : N] = 12$.

By the correspondence there is a unique (Galois) field extension $\mathbb{Q} \subseteq M \subseteq L$ with $[M : \mathbb{Q}] = 12$ and we have that $M = L^N$

Now $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ has deg 12

$\Rightarrow \mathbb{Q}(\zeta_3) = L^N$

(b)

Observe that $\langle 2 \rangle \cong \left(\mathbb{Z}/13\right)^*$

$Gal(f) \ni \sigma, \tau$ where

$\sigma(\alpha) = \alpha\zeta$ $\qquad$ $\tau(\alpha) = \alpha$

$\sigma(\zeta) = \zeta$ $\qquad$ $\tau(\zeta) = \zeta^2$

τ has order 12

$\sigma^2(\alpha) = \sigma(\alpha\zeta) = \alpha\zeta^2$

$\sigma^i(\alpha) = \alpha\zeta^i$ has order 13

Since $gcd(13,12) = 1$ we have that

$Gal(f) = \langle \sigma, \tau \rangle$

We have now to see what are the relations.

$\langle \sigma \rangle \trianglelefteq Gal(f)$ thus we have to see what is the action of $\langle \tau \rangle$ on $\langle \sigma \rangle$:

$$\tau\sigma\tau^{-1}(\alpha) = \tau\sigma(\alpha) = \tau(\alpha\zeta) = \alpha\zeta^2$$
$$\tau\sigma\tau^{-1}(\zeta) = \tau\sigma(\zeta^m) = \tau\tau^{-1}(\zeta) = \zeta$$

thus $\tau\sigma\tau^{-1} = \sigma^2$

$\mathrm{Gal}(f) = \langle \sigma, \tau \mid \sigma^{18} = \tau^{12} = 1 \quad \tau\sigma = \sigma^2\tau \rangle$

(c) L is clearly a radical extension.

So $\mathrm{Gal}(f)$ is solvable.

Problem 3

(a) Φ_{36} is irreducible & is separable since char $\mathbb{Q} = 0$

We have seen in class that $\mathbb{Q}(\zeta) = \mathrm{Spl}(\Phi_{36})$ which is Galois with Galois group

$\simeq (\mathbb{Z}/9)^* \times (\mathbb{Z}/4)^*$ (*)

$(\mathbb{Z}/9)^* \simeq \mathbb{Z}/3 \times \mathbb{Z}/2$

$(\mathbb{Z}/4)^* \simeq \mathbb{Z}/2$

thus $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is not

cyclic every element has order at most 6

(b) $p=3$ we have

$$x^{36}-1 = (x^{12}-1)^3 = (x^4-1)^3$$

has no irr factor of degree $24 = \deg \Phi_{36}$

$p=2$ $\quad (x^{36}-1) = (x^9-1)^4$

has no irred factor of deg 24

Let now $p \neq 3, 2$ so that $x^{36}-1$

is separable. We are going to show that $x^{36}-1$ has no irred factor of degree 24. Because of (*) we have that

$$p^6 \equiv 1 \bmod (36) \quad \text{for} \quad \text{thus.}$$

$$x^{36}-1 \mid x^{p^6-1}-1 \mid x^{p^6}-x$$

the right most polynomial splits in irred whose max degree is 6.

(c) Yes since $36 = 4 \cdot 3^2$ & 3 is a Hasseue prime

(d) Let ω a primitive 9-root root of 1 then.

$\mathbb{Q}(\omega)$ has a unique quadratic extension corresponding to the unique subgroup of index 3 of $(\mathbb{Z}/9)^* \simeq \mathbb{Z}/3 \times \mathbb{Z}/2$

We know that

$$\mathbb{Q}(\sqrt{-3}) \subseteq \mathbb{Q}(\omega') \subseteq \mathbb{Q}(\omega)$$

where ω' is a primitive 3-root of unity so we have that this extension is $\mathbb{Q}(\sqrt{-3})$

Observe that $i = \zeta^9$.

So that $\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta)$ is another quadratic extension. "$\mathbb{Q}(\sqrt{-1})$"

Also $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(-i\sqrt{-3}) \subseteq \mathbb{Q}(\zeta)$

Since $\mathbb{Z}/3 \times (\mathbb{Z}/2)^2$ has exactly

3 subgroups of index 6 we have that these are all the extensions

Problem 4

(a) $g_3 = x^4 + x^3 + x^2 + x + 1$

$g_3(x) \mid x^5 - 1$

$\frac{d}{dx} x^5 - 1 = 5x^4$

$\gcd(x^5 - 1, x^4) = 1$

$\Rightarrow x^5 - 1$ is separable and so g_3 is

$g_2(x) = x^4 + x = x(x+1)(x^2+x+1)$

$x^2 + x + 1$ is irreducible so x and 1 are not root

Since $\mathbb{F}_2$ is perfect x^2+x+1 is separable

$x^4 + x$ has no repeated roots.

(b) $g_3(x) \mid x^{2^4} - x$

So that

$$Spl(g_3(x)) \cong Spl(x^{p^4} - x)$$

$$\cong \mathbb{F}_{3^4}$$

$Gal(\mathbb{F}_{3^4} : \mathbb{F}_3) \cong \mathbb{Z}_4/4$

$Gal(Spl\, g_3(x) / \mathbb{F}_3)$ is a quotient of $\mathbb{Z}_4/4\mathbb{Z}_4$ thus it cyclic and the order divides 4

(c) Note that g_3 is the reduction mod 3 of $\Phi_5(x)$ the 5cyclotomic polynomial. Observe that 3 has order 4 in $(\mathbb{Z}_5)^*$

This means that

$5 \mid p^4 - 1$ but $5 \nmid p^k - 1$ for $k < 4$

In particular

$x^5 - 1 \nmid x^{p^k} - x$ for $k < 4$

and $x^5 - 1 \mid x^{p^4} - x$

If $g_3(x)$ where reducible, since it is separable we will have that $x^5 - 1$ splits as product of distinct polynom. of deg ≤ 2 that is $x^5 - 1 \mid x^{p^2} - x$ which is a contradiction

(d) with the info foran (a) - (c) we have either

D_8 or S_4

(enoug to get full points)

In fact thanks to the reduction of $f(x)$ mod $3^{\&}$ we know $Gal(f)$ contains a 4-cycle & a trasposition.

The correct answer is S_4
and you get one bonus point
if you give it motivating

(e) If the Galois group of f is
S_4 then the real roots of f are
not constructible with straight
edge & compass. Here an argument

$L = Spl(f)$ α a real root of f

$\mathbb{Q} \neq \mathbb{Q}(\alpha)$ $\subseteq L$

$\mathbb{Q}(\alpha)$ corresponds to a group of index
4 and so order 6

If α were to be constructible then
there should be an intermediate
extension $\mathbb{Q} \subsetneq k \subsetneq \mathbb{Q}(\alpha)$
such that $[k:\mathbb{Q}] = 2$ this corresponds

to a group of index 2 in S_4.
But there is only such a group which is A_4. This means that
$Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ is a subgroup of A_4 but A_4 has no subgroups of order 6.

For bonus points (1)

If $Gal(f) = D_8$ and α is a real root of f then α is constructible with straight edge and compass.

$L = Spl(f)$ then

$L = \mathbb{Q}(\alpha, \beta)$ with $[\mathbb{Q}(\alpha,\beta) : \mathbb{Q}(\alpha)] = 2$

this means that

$\therefore f = (x-\alpha)\cdot g$ with g of deg 3 now g has an irred factor of degree 2 so

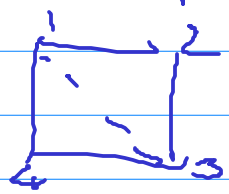
$f(x) = (x-\alpha)(x-\alpha')g_2(x)$ on $\mathbb{Q}(\alpha)$

Thus we know that

$Gal(Spl(f)/\mathbb{Q}(\alpha))$ has order 2 & is generated by the automorph. leaving fixed α, and α' and permuting the roots of $g_2(x)$

So is generated by a transposition

For example $(2,4)$



Consider now $\langle \rho^2, \rho\sigma \rangle \leq D_8$

Where $\rho = (1234)$ $\sigma = (12)(34)$

this is a group isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$ since the two generators have order 2 & commute

We have that, $(13) \in \langle \rho^2, \rho\sigma \rangle$

This corresponds to a quadratic

extension $L^6 \subseteq \mathbb{Q}(\alpha)$

So α is constructible.