Galois Theory: GAL #06

Due on Apr 01, 2022 at 11:59pm

Prof Matyas Domokos Section 9

Xianzhi

2023

HW06
Apr 01, 2022
Exercise 9.4.1
Exercise 9.4.2
Exercise 9.4.3

Problem 1

Exercise 9.4.1 Let L be the splitting field over $\mathbb{Q}$ of a cubic polynomial with rational coefficients, and ω a primitive cubic root of unity. Show that $L(\omega)$ is a radical extension of $\mathbb{Q}$, by exhibiting explicitly a radical sequence.
(Hint: recall Cardano's Method.)

Soln:

Let L be splitting field over $\mathbb{Q}$ of a cubic polynomial with radical coefficients $aX^3+bX^2+cX+d, a,b,c,d \in \mathbb{Q}$. WLOG, L is the same splitting field if the polynomial is monic

$$X^3 + \frac{b}{a}X^2 + \frac{c}{a}X + \frac{d}{a}, \tag{1}$$

so we could assume $a = 1$ from the beginning.
Also, L is the same if we shift by a rational amount $b/3$ of all the roots of this polynomial, because

$$X^3 + bX^2 + cX + d = (X + \frac{b}{3})^3 + (c - \frac{b^2}{3})(X + \frac{b}{3}) + d + \frac{b^3}{9} - \frac{cb}{3} - \frac{b^3}{27} \tag{2}$$

Thus, we could assume our polynomial is of the form:

$$X^3 + pX + q, \ p, q \in \mathbb{Q}. \tag{3}$$

$L(\omega)$ is radical extension, since

$$E := \mathbb{Q}\left(\sqrt{-3}, \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\right) = L(\omega). \ (*) \tag{4}$$

LHS of $(*)$ is a radical sequence, since

$$(\sqrt{-3})^2 \in \mathbb{Q} \tag{5}$$

$$\left(\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right)^2 \in \mathbb{Q}(\sqrt{-3}) \tag{6}$$

$$u^3 := \left(\sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\right)^3 \in \mathbb{Q}\left(\sqrt{-3}, \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right) \tag{7}$$

$$v := \frac{-p}{3u} = \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \tag{8}$$

$$\omega := -\frac{1}{2} + \frac{\sqrt{-3}}{2} \tag{9}$$

Now, we show the equality in $(*)$. By definition of u, v, ω, we have

$$L(\omega) = \mathbb{Q}(u + v, \omega u + \omega^2 v, \omega^2 u + \omega v, \omega) \tag{10}$$

First, we show $E \subset L(\omega)$, then we show $E \supset L(\omega)$. Since $\sqrt{-3} \in L(\omega)$, $\sqrt{-3} = 2\omega + 1$, observe

$$u + v, \frac{\omega u + \omega^2 v}{\omega} = u + \omega v \in L(\omega) \tag{11}$$

$$\implies (u + \omega v) - (u + v) = (\omega - 1)v \in L(\omega) \tag{12}$$

since $\omega - 1 \in L(\omega) \implies v \in L(\omega)$, similarly, we have $u \in L(\omega)$ or $u = (u+v) - v \in L(\omega)$. Hence,

$$\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = u^3 + \frac{q}{2} \in L(\omega) \tag{13}$$

Now, we show the other direction $E \supset L(\omega)$. We have $w = -\frac{1}{2} + \frac{1}{2} \cdot \sqrt{-3} \in E$, and $u \in E$, by definition, $v = \frac{-p}{3u} \in E$. Thus, $L(\omega) \subset E$. Hence, $E = L(\omega)$, and we have shown that $L(\omega)$ is a radical extension.

Problem 2

Exercise 9.4.2 Let L be the splitting field over $\mathbb{Q}$ of a monic irreducible cubic polynomial f in $\mathbb{Q}[x]$.

1. Show that $\Gamma(L:\mathbb{Q})$ has order 3 iff the discriminant of f is the square of a rational number. Recall that the discriminant of f is

$$\prod_{1\leq i<j\leq 3}(\alpha_i-\alpha_j)^2, \tag{14}$$

where α_i are the complex roots of f.

2. Give an example of a monic cubic polynomial f with $|\Gamma(L:\mathbb{Q})|=3$.
You may want to use the fact that the discriminant of $X^3+pX+q\in\mathbb{Q}[X]$ *is* $-4p^3-27q^2$.

Soln:
Part A

Part B

Problem 3

Exercise 9.4.3 Let L be a subfield of $\mathbb{C}$ such that $\Gamma(L)$ is the dihedral group D_4 (having 8 elements), and L a Galois extension of $\mathbb{Q}$. Show that L is a radical extension of $\mathbb{Q}$.

Proof. Let us denote the dihedral group D_4 this way:

$$D_4 = \langle f, t | \ f^4 = 1 = t^2, ft = tf^3 \rangle \tag{15}$$

We know degree 2 extension is obtained by adjoining an square root from previous homework. Since $\Gamma(L:\mathbb{Q})$ is $\cong D_4$, and is Galois, we can use Galois Correspondence. Normal subgroup corresponds to normal (Galois) extension.

$$\begin{array}{ccccccc} \{e\} & \triangleleft & \langle t \rangle & \triangleleft & \langle t, f^2 \rangle & \triangleleft & D_4 \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ L & \supset & E & \supset & F & \supset & \mathbb{Q} \end{array} \tag{16}$$

Where the up-down arrow $\updownarrow$ indicates the relationship being the field is fixed field of the group. Each of the subgroup has index 2 in the previous one, and it's a subnormal chain. So we have

$$\Gamma(F:\mathbb{Q}) \cong \Gamma(L:\mathbb{Q})/\Gamma(L:F) = |D_4/\langle t, f^2 \rangle| = 2 \tag{17}$$

So $\Gamma(F:\mathbb{Q})$ has order 2, so $F:\mathbb{Q}$ has degree 2. So $F = \mathbb{Q}(\alpha)$ where $\alpha^2 \in \mathbb{Q}$. Similarly,

$$\Gamma(E:F) \cong \Gamma(L:F)/\Gamma(L:E) = |\langle t, f^2 \rangle / \langle t \rangle| = 2 \tag{18}$$

So $|\Gamma(E:F)| = 2$ implies that $E:F$ has degree 2, so $E = F(\beta)$, where $\beta^2 \in F$.
$\Gamma(L:E) \cong \langle t \rangle$, $|\langle t \rangle| = 2$ implies that $L:E$ has degree 2.
$\implies L = E(\gamma)$, where $\gamma^2 \in E$.
$\implies L = \mathbb{Q}(\alpha, \beta, \gamma)$, so L is a radical extension.

□

Problem 6

Evaluate the integrals $\int_0^1 (1 - x^2) \mathrm{d}x$ and $\int_1^\infty \frac{1}{x^2} \mathrm{d}x$.