Galois Theory: GAL #05

Due on Mar 18, 2022 at 11:59pm

Prof Matyas Domokos Section 7

Xianzhi

2023

HW05
Exercise 7.2.5
Exercise 7.2.7
Exercise 7.2.8

Problem 1

Exercise 7.2.5 Let $\gamma = \sqrt{2+\sqrt{2}}$.

1. Show that $\mathbb{Q}(\gamma) : \mathbb{Q}$ is normal with cyclic Galois Group.

2. Show that $\mathbb{Q}(\gamma, i) = \mathbb{Q}(\phi)$ with $\phi^4 = i$.

Soln:
Part A

Let

$$\sqrt{2+\sqrt{2}} = X \tag{1}$$
$$\sqrt{2} = X^2 - 2 \tag{2}$$
$$2 = (X^2-2)^2 = X^4 - 4X^2 + 4 \tag{3}$$

Thus, $\sqrt{2+\sqrt{2}}$ is a root of $X^4 - 4X^2 + 2 =: f$ Since f is irreducible, by Eisenstein ($p = 2$), $\mathbb{Q}(\gamma)$ is degree 4 over $\mathbb{Q}$, we could find the roots of f:

$$f = \left(X + \sqrt{2+\sqrt{2}}\right)\left(X - \sqrt{2+\sqrt{2}}\right)\left(X + \sqrt{2-\sqrt{2}}\right)\left(X - \sqrt{2-\sqrt{2}}\right) \tag{4}$$

Let $\phi \in \Gamma(\mathbb{Q}(\gamma) : \mathbb{Q})$, we know ϕ permutes the roots of f.
If we can find an element ϕ with order strictly greater than 2, then since order of the element need to divide the order of the group, $|\phi|$ must be 4. Since up to isomorphism, group of order 4 is $\mathbb{Z}_4$ and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, we know once there exists $|\phi| = 4$, $\Gamma(\mathbb{Q}(\gamma) : \mathbb{Q})$ must be cyclic.
First, we show $\mathbb{Q}(\gamma)$ is splitting field of f that has no multiple roots, which would imply it is normal. since

$$\sqrt{2+\sqrt{2}} = \gamma \in \mathbb{Q}(\gamma) \implies -\sqrt{2+\sqrt{2}} \in \mathbb{Q}(\gamma) \tag{5}$$
$$2+\sqrt{2} = \gamma^2 \in \mathbb{Q}(\gamma) \tag{6}$$

so $\sqrt{2} \in \mathbb{Q}(\gamma)$. Since

$$\sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{2} \in \mathbb{Q}(\gamma) \implies \sqrt{2-\sqrt{2}} \in \mathbb{Q}(\gamma) \tag{7}$$

so $-\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\gamma)$.
Thus, all 4 roots of f are in $\mathbb{Q}(\gamma)$. And these roots are all distinct. so

$$\mathbb{Q}\left(\sqrt{2+\sqrt{2}}, -\sqrt{2+\sqrt{2}}, +\sqrt{2-\sqrt{2}}, -\sqrt{2-\sqrt{2}}\right) \subseteq \mathbb{Q}(\gamma) \tag{8}$$
$$\mathbb{Q}\left(\sqrt{2+\sqrt{2}}, -\sqrt{2+\sqrt{2}}, +\sqrt{2-\sqrt{2}}, -\sqrt{2-\sqrt{2}}\right) \supseteq \mathbb{Q}(\gamma) \tag{9}$$
$$\text{so } \mathbb{Q}\left(\sqrt{2+\sqrt{2}}, -\sqrt{2+\sqrt{2}}, +\sqrt{2-\sqrt{2}}, -\sqrt{2-\sqrt{2}}\right) = \mathbb{Q}(\gamma) \tag{10}$$
$$\tag{11}$$

Thus, $\mathbb{Q}(\gamma)$ is indeed splitting field of f with no multiple roots, so $\mathbb{Q}(\gamma) : \mathbb{Q}$ is Galois extension, and is normal extension. Now we find $\phi \in \Gamma(\mathbb{Q}(\gamma) : \mathbb{Q})$ that has order ≥ 3. Claim:

$$\sqrt{2+\sqrt{2}} \mapsto_\phi \sqrt{2-\sqrt{2}} \tag{12}$$

Problem 1 continued on next page. . .

does the job.
Why does such an automorphism exist? Answer: Galois group acts transitively on the roots of a minimal polynomial
Let

$$X_1 = -\sqrt{2+\sqrt{2}},\ X_2 = \sqrt{2+\sqrt{2}},\ X_3 = -\sqrt{2-\sqrt{2}},\ X_4 = \sqrt{2-\sqrt{2}} \tag{13}$$

Hence

$$\begin{aligned}
\phi \circ \phi\left(\sqrt{2+\sqrt{2}}\right) &= \phi\left(\sqrt{2-\sqrt{2}}\right) &(14)\\
&= \phi\left(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\right) &(15)\\
&= \frac{\phi(\sqrt{2})}{\phi\left(\sqrt{2+\sqrt{2}}\right)} &(16)\\
&= \frac{-\sqrt{2}}{\sqrt{2-\sqrt{2}}} &(17)\\
&= -\sqrt{2+\sqrt{2}} &(18)
\end{aligned}$$

We also have

$$\begin{aligned}
\phi(2)+\phi(\sqrt{2}) &= \phi(2+\sqrt{2}) &(19)\\
&= \phi\left(\sqrt{2+\sqrt{2}}\cdot\sqrt{2+\sqrt{2}}\right) &(20)\\
&= \phi\left(\sqrt{2+\sqrt{2}}\right)\cdot\phi\left(\sqrt{2+\sqrt{2}}\right) &(21)\\
&= \left(\sqrt{2-\sqrt{2}}\right)\cdot\left(\sqrt{2-\sqrt{2}}\right) &(22)\\
&= 2-\sqrt{2} &(23)
\end{aligned}$$

so $\phi(2)+\phi(\sqrt{2}) = 2-\sqrt{2}$, since $\phi(2) = 2$ implies $\phi(\sqrt{2}) = -\sqrt{2}$.
Since ϕ^2 is not identity automorphism, $|\phi| \geq 3$, and we found the desired ϕ.
We can check ϕ indeed permutes X_1, X_2, X_3, X_4.

$$\begin{aligned}
&X_2 \xrightarrow{\phi} X_4 &(24)\\
&\phi(X_1) = \phi(-\sqrt{2+\sqrt{2}} = -\sqrt{2-\sqrt{2}} = X_3 &(25)\\
&\phi(X_3) = \phi(-\sqrt{2-\sqrt{2}}) = (-1)\cdot(-\sqrt{2+\sqrt{2}}) = \sqrt{2+\sqrt{2}} = X_2 &(26)\\
&\phi(X_4) = -\sqrt{2+\sqrt{2}} = X_1 &(27)\\
&\phi : X_1 \to X_3 \to X_2 \to X_4 \to X_1 &(28)
\end{aligned}$$

Part B

Show $\mathbb{Q}(\gamma, i) = \mathbb{Q}(\phi)$ with $\phi^4 = i$.

Use formula

$$\cos(A) = 1 - 2\sin^2 \frac{A}{2} \tag{29}$$

$$1 - 2\sin^2(22.5°) = \cos 45° \tag{30}$$

$$\sin^2(22.5°) = \frac{\sqrt{2}-1}{2\sqrt{2}} \tag{31}$$

$$\sin^2(22.5°) = \frac{\sqrt{2-\sqrt{2}}}{2} \tag{32}$$

And also,

$$\cos(A) = 2\cos^2 \frac{A}{2} - 1 \tag{33}$$

$$\cos 45° = 2\cos^2 22.5° - 1 \tag{34}$$

$$\frac{1}{\sqrt{2}} + 1 = 2\cos^2(22.5°) \tag{35}$$

$$\sqrt{\frac{1+\sqrt{2}}{2\sqrt{2}}} = \cos(22.5°) \tag{36}$$

Problem 2

Exercise 7.2.7 Find the degree of

$$\sqrt[5]{81} + 29\sqrt[5]{9} + 17\sqrt[5]{3} - 16 \tag{37}$$

over $\mathbb{Q}$.

Soln:

Observe that if we adjoint $\sqrt[5]{3}$ to $\mathbb{Q}$, then

$$\gamma := (\sqrt[5]{3})^4 + 29(\sqrt[5]{3})^2 + 17\sqrt[5]{3} - 16 \in \mathbb{Q}(\sqrt[5]{3}). \tag{38}$$

since $\sqrt[5]{3}$ is root of $X^5 - 3$, which is irreducible by Eisenstein.

$$m_{\mathbb{Q}}(\sqrt[5]{3}) = X^5 - 3 \tag{39}$$

and $\mathbb{Q}(\sqrt[5]{3})$ is degree 5 extension.
Since $\gamma \in \mathbb{Q}(\sqrt[5]{3})$, we have $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ divides $[\mathbb{Q}(\sqrt[5]{3} : \mathbb{Q})] = 5$ so $\mathbb{Q}(\gamma)$ is either degree 1 or 5.
If it's degree 1, then $\gamma \in \mathbb{Q}$, so there exists $q \in \mathbb{Q}$ such that $\gamma = q$.

$$\left(\sqrt[5]{3}\right)^4 + 29\left(\sqrt[5]{3}\right)^2 + 17\sqrt[5]{3} - 16 - q = 0 \tag{40}$$

Thus, $\sqrt[5]{3}$ is a root of the above polynomial with coefficients in $\mathbb{Q}$, but this polynomial is degree 4, contradicting the minimal polynomial of $\sqrt[5]{3}$ having degree 5. Thus, $\mathbb{Q}(\gamma)$ is degree 5. so the degree of γ over $\mathbb{Q}$ is 5.

Problem 3

Exercise 7.2.8 Find the degree of $\sqrt[5]{81}$ over $\mathbb{Q}(\sqrt[81]{5})$.

Soln:

First we show $\mathbb{Q}(\sqrt[5]{81}) = \mathbb{Q}(\sqrt[5]{3})$.
Want to show $\sqrt[5]{81} \in \mathbb{Q}(\sqrt[5]{3})$. Write $\sqrt[5]{81} = (\sqrt[5]{3})^4 \in \mathbb{Q}(\sqrt[5]{3})$. So $\mathbb{Q}(\sqrt[5]{81}) \subset \mathbb{Q}(\sqrt[5]{3})$. Want to show $\sqrt[5]{3} \in \mathbb{Q}(\sqrt[5]{81})$: write $3^{1/5} = \left(3^{4/5}\right)^4 (3^{-1})^3 \in \mathbb{Q}\left(\sqrt[5]{81}\right)$ so $\mathbb{Q}(\sqrt[5]{3}) \subseteq \mathbb{Q}(\sqrt[5]{81})$
so $\mathbb{Q}(\sqrt[5]{81}) = \mathbb{Q}(\sqrt[5]{3})$
Since $X^5 - 3$ is irreducible by eisenstein, $\mathbb{Q}(\sqrt[5]{3})$ is degree 5 over $\mathbb{Q}$, so $\mathbb{Q}(\sqrt[5]{81})$ is degree 5 over $\mathbb{Q}$.
$\mathbb{Q}(\sqrt[81]{5})$ is degree 81 over $\mathbb{Q}$, since $X^{81} - 5$ is irreducible by Eisenstein.
By earlier exercise

$$[\mathbb{Q}(\sqrt[5]{81}, \sqrt[81]{5}) : \mathbb{Q}] \leq degm_{\mathbb{Q}}(\sqrt[5]{81}) \cdot degm_{\mathbb{Q}}(\sqrt[81]{5}) = 5 \cdot 81 \tag{41}$$

Also, since $[\mathbb{Q}(\sqrt[5]{81}) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\sqrt[81]{5} : \mathbb{Q}] = 81$ divide $[\mathbb{Q}(\sqrt[5]{81}, \sqrt[81]{5}) : \mathbb{Q}]$ by Tower law, $[\mathbb{Q}(\sqrt[5]{81}, \sqrt[81]{5}) : \mathbb{Q}]$ is a multiple of $5 \cdot 81$ so its exactly $5 \cdot 81$.
Use tower law again,

$$\begin{aligned} 5 \cdot 81 &= [\mathbb{Q}(\sqrt[5]{81}, \sqrt[81]{5}) : \mathbb{Q}(\sqrt[81]{5})] \cdot \left[\mathbb{Q}(\sqrt[81]{5} : \mathbb{Q}\right] &(42)\\ &= 5 \cdot 81 &(43)\end{aligned}$$

Thus, $\sqrt[5]{81}$ is degree 5 over $\mathbb{Q}(\sqrt[81]{5})$. And we are done.