MA3D5 Galois Theory
Sheet 3 Solutions

Peize Liu

22 Oct 2024

Exercise 3.1

Find the minimal polynomials $f \in K[x]$ of the given elements of the given extensions L/K:

(a) γ in $\mathbb{Q}(\gamma)/\mathbb{Q}$, where $\gamma = \sqrt{5}$.

(b) $\gamma + 1$ in $\mathbb{Q}(\gamma)/\mathbb{Q}$ (same γ as (a)).

(c) ω (a primitive cube root of unity) in $\mathbb{C}/\mathbb{Q}$.

(d) ω (a primitive cube root of unity) in $\mathbb{C}/\mathbb{Q}(\sqrt{-3})$.

(e) $\delta = \sqrt{2} + \sqrt{3}$ in $\mathbb{C}/\mathbb{Q}$. (No need to prove irreducibility in this case, unless you want to - will discuss more later.)

(f) $\delta = \sqrt{2} + \sqrt{3}$ in $\mathbb{C}/\mathbb{Q}(\sqrt{2})$.

(a) $\gamma = \sqrt{5}$ implies that γ is a root of $f_1(x) = x^2 - 5$. f_1 is irreducible over $\mathbb{Q}$ because it has no rational roots. Hence f_1 is the minimal of γ.

(b) Let $\alpha = \gamma + 1 = \sqrt{5} + 1$. Then $5 = (\alpha - 1)^2$. Hence $\gamma + 1$ is a root of $f_2(x) = x^2 - 2x - 4$ because it has no rational roots. Hence f_2 is the minimal of $\gamma + 1$.

(c) ω satisfies $\omega^3 = 1$ and $\omega \neq 1$. Note that $0 = \omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1)$. Hence ω is a root of $f_3(x) = x^2 + x + 1$. f_3 is irreducible because it has no rational roots (in fact its roots $\omega, \omega^2 \notin \mathbb{R}$). Hence f_3 is the minimal of γ.

(d) We take $\omega = \exp\left(\dfrac{2\pi i}{3}\right) = \dfrac{-1 + \sqrt{-3}}{2}$. Then $\omega \in \mathbb{Q}(\sqrt{-3})$. The minimal polynomial of ω in $\mathbb{Q}(\sqrt{-3})[x]$ is just $f_4(x) = x - \omega$.

(e) Since $\delta = \sqrt{2} + \sqrt{3}$, then $\sqrt{3} = \sqrt{2} - \delta$. Taking the square of both sides gives $3 = 2 + \delta^2 - 2\delta\sqrt{2}$. Rearrange: $2\delta\sqrt{2} = \delta^2 - 1$. Again taking the square: $8\delta^2 = \delta^4 - 2\delta^2 + 1$. Hence δ is a root of $f_5(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. We claim that f_5 is the minimal polynomial of δ over $\mathbb{Q}$. It suffices to show that $[\mathbb{Q}(\delta) : \mathbb{Q}] = \deg f_5 = 4$. Observe that

$$\delta^3 = (\sqrt{2} + \sqrt{3})^3 = 11\sqrt{2} + 9\sqrt{3}.$$

Then we have

$$\sqrt{2} = \frac{1}{2}\left((\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3})\right) \in \mathbb{Q}(\delta) \qquad \sqrt{3} = \frac{1}{2}\left(11(\sqrt{2} + \sqrt{3}) - (\sqrt{2} + \sqrt{3})^3\right) \in \mathbb{Q}(\delta).$$

This shows $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\delta)$. The reverse inclusion is obvious. We deduce that $\mathbb{Q}(\delta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Suppose that $\sqrt{2} \in \mathbb{Q}(\sqrt{3})$. Every element of $\mathbb{Q}(\sqrt{3})$ is of the form $a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$. Write $\sqrt{2} = a + b\sqrt{3}$. Taking the square of both sides gives $\sqrt{3} = \dfrac{2 - a^2 - 3b^2}{2ab}$. Note that RHS is a rational number, thus giving a contradiction.

Therefore we obtain a tower of non-trivial extensions $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\delta)$. Hence by tower law, $[\mathbb{Q}(\delta) : \mathbb{Q}] = [\mathbb{Q}(\delta) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \geqslant 2 \cdot 2 = 4$. We conclude that $[\mathbb{Q}(\delta) : \mathbb{Q}] = 4$ and f_5 is the minimal polynomial of δ over $\mathbb{Q}$.

(f) Recall that we have shown that δ satisfies $\delta^2 - 2\sqrt{2}\delta - 1 = 0$. Hence δ is a root of $f_6(x) = x^2 - 2\sqrt{2}x - 1 \in$

$\mathbb{Q}(\sqrt{2})[x]$. f_6 is irreducible over $\mathbb{Q}(\sqrt{2})$, as $\mathbb{Q}(\delta)$ is a non-trivial extension of $\mathbb{Q}(\sqrt{2})$. Hence f_6 is the minimal polynomial of δ over $\mathbb{Q}(\sqrt{2})$.

Exercise 3.2

(From Ian Stewart's book.) Consider complex numbers α, β whose minimal polynomials over $\mathbb{Q}$ are $x^2 - 2$ and $x^2 - 4x + 2$ respectively. Show that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are isomorphic.

Observe that the change of variable $x \longmapsto t = x + 2$ changes $x^2 - 2$ to $(t-2)^2 - 2 = t^2 - 4t + 2$. This implies that $\beta = \alpha + 2$. So $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha + 2) = \mathbb{Q}(\alpha)$. These two fields are not only isomorphic but in fact equal as subfields of $\mathbb{C}$.

Exercise 3.3

Let $\alpha = \sqrt[3]{2} \in \mathbb{R}$ and $\beta = \alpha\omega$ where ω is a primitive cube root of unity. Show that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are isomorphic (but distinct subfields of $\mathbb{C}$).

Find a third distinct subfield of $\mathbb{C}$ that is isomorphic to them both. Is there a fourth one?

Let $\varphi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ be a $\mathbb{Q}$-algebra homomorphism such that $\varphi(\alpha) = \beta$. This is well-defined as $\alpha^3 = \beta^3 = 2$. This is an isomorphism with inverse given by $\varphi^{-1}(\beta) = \alpha$.

$\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ because $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ while $\mathbb{Q}(\alpha) \not\subseteq \mathbb{R}$.

A third distinct subfield of $\mathbb{C}$ isomorphism to them would be $\mathbb{Q}(\alpha\omega^2)$. These are pairwise distinct by the same argument as Question 7(c) of Sheet 2.

Suppose that K is a subfield of $\mathbb{C}$ isomorphic to $\mathbb{Q}(\alpha)$. Let $\varphi : \mathbb{Q}(\alpha) \to K$ be the field isomorphism and let $\delta := \varphi(\alpha)$. It follows that $\delta^3 - 2 = \varphi(\alpha^3 - 2) = \varphi(0) = 0$. So $\delta \in \{\alpha, \alpha\omega, \alpha\omega^3\}$. It follows that K contains $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha\omega)$ or $\mathbb{Q}(\alpha\omega^2)$ as a subfield. But $[K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. So K is equal to one of $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha\omega)$, $\mathbb{Q}(\alpha\omega^2)$. There is no a fourth distinct isomorphic subfield.

Exercise 3.4

Let $K = \mathbb{C}$. Are there any (non-trivial) algebraic field extensions L/K? [Hint: Let L/K be such an extension and $\alpha \in L \setminus K$. What is the minimal polynomial of α over $\mathbb{C}$? You may use the fundamental theorem of algebra.]

Are there any (non-trivial) field extensions L/K (again for $K = \mathbb{C}$)?

Suppose that $L/\mathbb{C}$ is a non-trivial algebraic extension. Take $\alpha \in L \setminus \mathbb{C}$. Since α is algebraic over K, there exists $f(x) \in \mathbb{C}[x]$ such that $f(\alpha) = 0$. In particular we take f to be the minimal polynomial $m_\alpha \in \mathbb{C}[x]$ of α. By the fundamental theorem of algebra, m_α splits into linear factors. In particular $m_\alpha(x) = (x - \alpha)g(x)$ for some $g(x) \in \mathbb{C}[x]$, contradicting the minimality. Hence $\mathbb{C}$ has no non-trivial algebraic extension.

But the field of rational functions over $\mathbb{C}$, $\mathbb{C}(x)$ is a non-trivial field extension of $\mathbb{C}$. It is in fact a transcendental extension. You will see a lot of such examples in the commutative algebra or algebraic geometry module.

Exercise 3.5

Give an example of two finite extensions $L_1, L_2 \subseteq \mathbb{C}$ of $\mathbb{Q}$ that have the same degree, $[L_1 : \mathbb{Q}] = [L_2 : \mathbb{Q}]$, but are not isomorphic (and not seen in lectures).

I am not sure if this is covered in the lectures but the simplest example is to take $L_1 = \mathbb{Q}(\sqrt{2})$ and $L_2 = \mathbb{Q}(\sqrt{3})$. Suppose that there exists a field isomorphism $\varphi : L_1 \to L_2$. Since $\mathbb{Q}$ is a prime subfield of both L_1 and L_2, the fact that $\varphi(1) = 1$ forces $\varphi|_{\mathbb{Q}} = \text{id}$. Since $\alpha = \sqrt{2} \in L_1$ satisfies $\alpha^2 - 2 = 0$, then $\varphi(\alpha^2 - 2) = \varphi(\alpha)^2 - 2 = 0 \in L_2$.

Hence L_2 contains a root of $x^2 - 2 \in \mathbb{Q}[x]$, which means $\alpha = \sqrt{2} \in L_2$. In Q1.(e) we have shown that this is impossible.

$\mathbb{F}_{\nvDash}$