Galois theory — Exercise sheet 2

https://www.maths.tcd.ie/~mascotn/teaching/2019/MAU34101/index.html

Version: October 29, 2019

Answers are due for Tuesday October 29th, 3PM.

Exercise 1 *Yes or no (35 pts)*

Let $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$ (you may assume without proof that f is irreducible over $\mathbb{Q}$), and let $L = \mathbb{Q}[x]/(f)$.

1. (10 pts) Is L a separable extension of $\mathbb{Q}$? Explain.
2. (20 pts) Is L a normal extension of $\mathbb{Q}$? Explain.

   Hint: What does the fact that $f : \mathbb{R} \longrightarrow \mathbb{R}$ is strictly increasing tell you about the complex roots of f?
3. (5 pts) Is L a Galois extension of $\mathbb{Q}$? Explain.

Solution 1

1. Yes, since all fields of characteristic 0 are perfect.
2. Since $f : \mathbb{R} \longrightarrow \mathbb{R}$ is strictly increasing, f has exactly one real root α (intermediate value theorem) and thus one complex-conjugate pair of roots β, $\bar{\beta}$. The images of L by its $[L : \mathbb{Q}] = 3$ $\mathbb{Q}$-embeddings into $\mathbb{C}$ are $\mathbb{Q}(\alpha) \subset \mathbb{R}$, $\mathbb{Q}(\beta) \not\subset \mathbb{R}$, and $\mathbb{Q}(\overline{\beta}) \not\subset \mathbb{R}$. Since some are $\subset \mathbb{R}$ but others are not, they do not all agree, so L is not normal over $\mathbb{Q}$.
3. No, since it is not normal over $\mathbb{Q}$.

Exercise 2 *Square roots (65 pts)*

Let $L = \mathbb{Q}(\sqrt{10}, \sqrt{42})$.

In this exercise, you may use without proof the fact that for all $a, b \in \mathbb{Q}^\times$,

$$\begin{aligned} \mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b}) &\iff \sqrt{b} \in \mathbb{Q}(\sqrt{a}) \\ &\iff a/b \text{ is a square in } \mathbb{Q} \\ &\iff \text{The numerator and denominator of } a/b \text{ are squares.} \end{aligned}$$

1. (5 pts) Prove that L is a Galois extension of $\mathbb{Q}$.
2. (10 pts) Prove that $[L : \mathbb{Q}] = 4$.
3. (15 pts) Describe all the elements of $\mathrm{Gal}(L/\mathbb{Q})$. What is $\mathrm{Gal}(L/\mathbb{Q})$ isomorphic to?
4. (20 pts) Sketch the diagram showing all intermediate extensions $\mathbb{Q} \subset E \subset L$, ordered by inclusion (you may re-use without proof the subgroup diagram of $\mathrm{Gal}(L/\mathbb{Q})$ seen in class). Explain clearly which field corresponds to which subgroup.
5. (15 pts) Does $\sqrt{15} \in L$? Use the previous question to answer.

Solution 2

1. L is the splitting field over $\mathbb{Q}$ of $(x^2 - 10)(x^2 - 42) \in \mathbb{Q}[x]$ which is separable (not multiple root), so it is Galois over $\mathbb{Q}$.

2. Since 10 is not a square, $\mathbb{Q}(\sqrt{10}) \neq \mathbb{Q}$, so $[\mathbb{Q}(\sqrt{10}) : \mathbb{Q}] = 2$. In order to conclude that $[L : \mathbb{Q}] = 4$, we need to prove that $[L : \mathbb{Q}(\sqrt{10})]$ is 2 and not 1, i.e. that $\sqrt{42} \notin \mathbb{Q}(\sqrt{10})$. This follows from the fact that $\frac{42}{10} = \frac{21}{5}$ is not a square in $\mathbb{Q}$.

3. We already know that $\#\,\mathrm{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 4$ since L is Galois over $\mathbb{Q}$. Besides, an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ must take $\sqrt{10} \in L$ to a root of $x^2 - 10 \in \mathbb{Q}[x]$, i.e. to $\pm\sqrt{10}$; and similarly $\sigma(\sqrt{42}) = \pm\sqrt{42}$. Since σ is completely determined by what it does to $\sqrt{10}$ and to $\sqrt{42}$, this leaves us with only 4 possibilities for σ. But since $\#\,\mathrm{Gal}(L/\mathbb{Q}) = 4$, all these possibilities must occur. Therefore, $\mathrm{Gal}(L/\mathbb{Q})$ is made up of

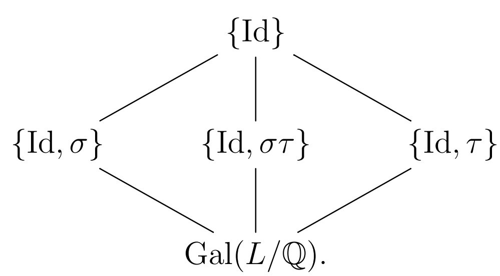
   - Id,
   - $\sigma : \sqrt{10} \mapsto -\sqrt{10},\ \sqrt{42} \mapsto \sqrt{42}$,
   - $\tau : \sqrt{10} \mapsto \sqrt{10},\ \sqrt{42} \mapsto -\sqrt{42}$,
   - $\sigma\tau : \sqrt{10} \mapsto -\sqrt{10},\ \sqrt{42} \mapsto -\sqrt{42}$.

   We see that $\sigma\tau = \tau\sigma$, and that $\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{Id}$. Therefore

   $$\begin{array}{ccc} (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & \longrightarrow & \mathrm{Gal}(L/\mathbb{Q}) \\ (a, b) & \longmapsto & \sigma^a \tau^b \end{array}$$

   is a group isomorphism.

4. We know from class that since $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, its subgroup diagram is

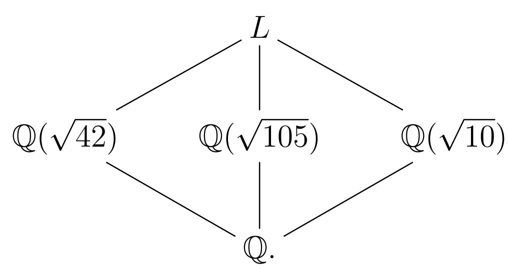
   Let us now find the corresponding fields.

- Clearly, $L^{\{\mathrm{Id}\}} = L$.
- We also have $L^{\mathrm{Gal}(L/\mathbb{Q})} = \mathbb{Q}$ since L is Galois over $\mathbb{Q}$.
- We know that $L^{\{\mathrm{Id},\sigma\}}$ is an extension of $\mathbb{Q}$ of degree $[\mathrm{Gal}(L/\mathbb{Q}) : \{\mathrm{Id}, \sigma\}] = 2$. It is the subfield of L formed of the elements fixed by σ, so it contains $\sqrt{42}$ and thus $\mathbb{Q}(\sqrt{42})$. Since the latter is already an extension of $\mathbb{Q}$ of degree 2, it must agree with $L^{\{\mathrm{Id},\sigma\}}$.
- Similarly, $L^{\{\mathrm{Id},\tau\}}$ is an extension of degree 2 of $\mathbb{Q}$, which contains $\sqrt{10}$ as it is fixed by τ, so $L^{\{\mathrm{Id},\tau\}} = \mathbb{Q}(\sqrt{10})$.
- Finally, $L^{\{\mathrm{Id},\sigma\tau\}}$ is an extension of degree 2 of $\mathbb{Q}$, but it contains neither $\sqrt{10}$ nor $\sqrt{42}$ since they are not fixed by $\sigma\tau$. However, $\sqrt{10}\sqrt{42} = \sqrt{420}$ is fixed by $\sigma\tau$ since

  $$\sigma\tau(\sqrt{10}\sqrt{42}) = (-\sqrt{10})(-\sqrt{42}),$$

  so $L^{\{\mathrm{Id},\sigma\tau\}} = \mathbb{Q}(\sqrt{420}) = \mathbb{Q}(\sqrt{105})$.

The field diagram is thus



5. No. Indeed, if $\sqrt{15} \in L$, then $\mathbb{Q}(\sqrt{15})$ is an intermediate field, but that contradicts the previous question since $\mathbb{Q}(\sqrt{15})$ is neither of $\mathbb{Q}(\sqrt{10})$, $\mathbb{Q}(\sqrt{42})$, $\mathbb{Q}(\sqrt{105})$ as neither $\frac{15}{10} = \frac{3}{2}$, $\frac{15}{42} = \frac{5}{14}$, $\frac{15}{105} = \frac{1}{7}$ are squares in $\mathbb{Q}$.