Galois Theory Workshop 3

Degree and splitting fields

There are more questions here than you're likely to have time for in the workshop. I suggest you start from the beginning and do whatever you do in the time, without hurrying, then keep the other ones for practice another day.

In all questions, you're strongly encouraged to use results from the notes—and this will make your life much easier!

1. Let $M : L : K$ be field extensions, with $M : K$ finite. Show that $[L : K] = [M : K] \iff L = M$.

2. Let $M : K$ be a finite field extension, let $\alpha \in M$, and let m be the minimal polynomial of α over K. Show that $\deg(m)$ divides $[M : K]$.

3. This question is about extensions of degree 2.

   (i) Let K be a field and $a \in K$. Show that

   $$[K(\sqrt{a}) : K] = \begin{cases} 1 & \text{if } a \text{ has a square root in } K \\ 2 & \text{otherwise.} \end{cases}$$

   (ii) This part is a general, careful version of the quadratic formula. Let L be a field with $\operatorname{char} L \neq 2$, and let $a, b, c, \alpha \in L$ with $a \neq 0$. Suppose that $a\alpha^2 + b\alpha + c = 0$. Prove that $b^2 - 4ac$ has a square root s in L, and that

   $$\alpha \in \left\{ \frac{-b+s}{2a}, \frac{-b-s}{2a} \right\}.$$

   (iii) Let $L : K$ be a field extension of degree 2, with $\operatorname{char} K \neq 2$. Prove that $L \cong K(\sqrt{d})$ for some $d \in K$.

4. Let $M : L : K$ be field extensions. Prove that if $M : L$ and $L : K$ are algebraic then so is $M : K$. (You may *not* assume that either extension is finite.)

5. Prove that $\overline{\mathbb{Q}}$, the subfield of $\mathbb{C}$ consisting of the complex numbers algebraic over $\mathbb{Q}$, is algebraically closed. (Hint: use question 4.)

6. Say whether each of the following statements is true or false, giving one sentence of justification. If you think the statement is false, your sentence should be a counterexample.

   (i) Let $M : K$ be a field extension of degree 10. Then it is not possible to find extensions $M : L_2 : L_1 : K$ that are all nontrivial.

   (ii) Let $f(t) \in K[t]$ be an irreducible polynomial of degree n. Then $[\mathrm{SF}_K(f) : K] \leq n$.

   (iii) Let $M : K$ be a field extension and $\alpha, \beta \in M$. Then $[K(\alpha\beta) : K] \leq [K(\alpha, \beta) : K]$.

   (iv) Let $(x, y) \in \mathbb{R}^2$ and suppose that x and y each have an annihilating polynomial of degree 4 over $\mathbb{Q}$. Then (x, y) is constructible by ruler and compass from $(0, 0)$ and $(1, 0)$.

   (v) For all nontrivial finite field extensions $M : \mathbb{Q}$, the Galois group $\mathrm{Gal}(M : \mathbb{Q})$ is nontrivial.

   (vi) For all finite extensions $M : K$ and $M' : K'$, every isomorphism $\psi\colon K \to K'$ can be extended to a homomorphism $\varphi\colon M \to M'$.

   (vii) A regular 1020-sided polygon can be constructed by ruler and compass, given two points in the plane.

(viii) Let $f \in \mathbb{Q}[t]$ and let $S = \mathrm{SF}_{\mathbb{Q}}(f)$. Then the splitting field of f over $\mathbb{Q}(\sqrt[3]{2})$ is $S(\sqrt[3]{2})$.

(ix) Let f be a polynomial over a field K and let $\theta, \varphi \in \mathrm{Gal}_K(f)$. If $\theta(\alpha) = \varphi(\alpha)$ for all roots α of f in the splitting field of f, then $\theta = \varphi$.

(x) The Galois group of $(t^4 - t^3 + t^2 - t + 1)^2$ over $\mathbb{Q}$ is solvable.

7. Let $M : K$ be a finite extension. Prove that every homomorphism $M \to M$ over K is an automorphism of M over K. (Hint: rank-nullity formula.)

8. Prove that the field extension $\overline{\mathbb{Q}} : \mathbb{Q}$ is not finite. (Hint: use Exercise 3.3.14.) Deduce that $\overline{\mathbb{Q}} : \mathbb{Q}$ is not even finitely *generated*.

9. This question gives you an example of two extensions $M : K$ and $M' : K$ such that M and M' are isomorphic, but not isomorphic over K.

   Let $\mathbb{Q}(t_1, t_2, \ldots)$ be the field of rational expressions in countably infinitely many symbols $t_1, t_2, \ldots$. (An element is a ratio of polynomials in these symbols, and can involve only finitely many of them.) It has a subfield $\mathbb{Q}(t_2, t_3, \ldots)$. So we have extensions

$$\mathbb{Q}(t_1, t_2, \ldots) : \mathbb{Q}(t_2, t_3, \ldots), \qquad \mathbb{Q}(t_2, t_3, \ldots) : \mathbb{Q}(t_2, t_3, \ldots)$$

   (the second being trivial). Prove that the fields $\mathbb{Q}(t_1, t_2, \ldots)$ and $\mathbb{Q}(t_2, t_3, \ldots)$ are isomorphic, but not isomorphic over $\mathbb{Q}(t_2, t_3, \ldots)$.

10. Figure 5.1 (p.55) suggests regarding the degree of a simple extension $[K(\beta) : K]$ as something like the 'distance' from β to K. It also warns you not to take that idea too seriously. This exercise explores whether it *could* be taken seriously.

    Let $M : K$ be a field extension. For $\alpha, \beta \in M$, put

$$d(\alpha, \beta) = \log\bigl(\deg_{K(\beta)}(\alpha)\bigr).$$

    Which of the metric space axioms are satisfied by d? (And why did I put a logarithm there?)

11. Imagine you're going for a walk with a friend in your year who has taken most of the same courses as you, but not Galois theory. How would you explain the proof that duplicating the cube with ruler and compass is impossible?

    Since you're out for a walk, you can't write anything down. Your mission is to explain as much as possible of the proof of the theorem (not just the statement) in intuitive terms.

12. Let F be the set of real numbers z such that z is a coordinate of some point in $\mathbb{R}^2$ constructible by ruler and compass from $(0, 0)$ and $(1, 0)$. ('A coordinate' means either the x-coordinate or the y-coordinate.) Prove that F is a subfield of $\mathbb{R}$, and, moreover, that F is the smallest subfield of $\mathbb{R}$ with the property that $z^2 \in F \Rightarrow z \in F$ for all $z \in \mathbb{R}$.

    This is a intended to be a more challenging question than the rest.