Galois Theory Workshop 3

Polynomials; field extensions; degree

There are more questions here than you'll have time for in the workshop. I suggest you start from the beginning and do whatever you do in the time, without hurrying. 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!

Warmup questions

1. Which of the following polynomials are irreducible over $\mathbb{Q}$? Don't forget Warning 3.3.2: 'has no roots' doesn't imply 'irreducible'!

   (i) $1 + 2t - 5t^3 + 2t^6$

   (ii) $4 - 3t - 2t^2$

   (iii) $4 - 13t - 2t^3$

   (iv) $1 + t + t^2 + t^3 + t^4 + t^5$

   (v) $1 + t + t^2 + t^3 + t^4 + t^5 + t^6$

   (vi) $2.2 + 3.3t - 1.1t^3 + t^7$ (where the dots are decimal points, not products)

   (vii) $1 + t^4$.

2. Find an irreducible polynomial $f \in \mathbb{R}[t]$ such that $\mathbb{R}[t]/\langle f \rangle \cong \mathbb{C}$.

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

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

Standard questions

5. Let $M : K$ be a field extension and $\alpha, \beta \in M$. Call α and β **conjugate** over K if for all $p \in K[t]$, we have $p(\alpha) = 0 \iff p(\beta) = 0$. (You saw this definition in Chapter 1 for $\mathbb{C} : \mathbb{R}$ and $\mathbb{C} : \mathbb{Q}$.)

   (i) Prove that α and β are conjugate over K if and only if *either* both are transcendental *or* both are algebraic and they have the same minimal polynomial.

   (ii) Show that if there exists an irreducible polynomial $p \in K[t]$ such that $p(\alpha) = 0 = p(\beta)$, then α and β are conjugate over K.

   (iii) Show that if α and β are conjugate over K then $K(\alpha) \cong K(\beta)$ over K.

6. (i) Let p be a prime number and put $\omega = e^{2\pi i/p}$. Prove that $\omega, \ldots, \omega^{p-1}$ are conjugate over $\mathbb{Q}$. (I claimed this in Example 1.1.8; now you can prove it.)

   (ii) Prove that $\mathbb{Q}(\pi) \cong \mathbb{Q}(e)$ over $\mathbb{Q}$. (You'll need a bit of mathematical general knowledge to do this.)

7. Let $M : L : K$ be field extensions, which you may *not* assume to be finite.

   (i) Let $\alpha \in M$. Prove that if α is algebraic over L and L is algebraic over K then α is algebraic over K.

   (ii) Deduce that if $M : L$ and $L : K$ are algebraic then so is $M : K$.

8. 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 7.)

9. (i) Here I will write $\langle X \rangle$ for the subfield generated by a subset X of a field K. Show that for all $X \subseteq K$ and homomorphisms of fields $\varphi\colon K \to L$,

$$\varphi\langle X \rangle = \langle \varphi X \rangle.$$

(Hints: use the characterization of $\langle X \rangle$ as the smallest subfield containing X, and use both parts of Lemma 2.3.6.)

(ii) Let $M : K$ and $M' : K$ be field extensions, and let $\varphi\colon M \to M'$ be a homomorphism over K. Show that $\varphi(K(Y)) = K(\varphi Y)$ for all subsets Y of M.

10. *Briefly* sketch the proof of the classification theorem for simple extensions—just the half about extensions by an algebraic element (Theorem 4.3.16(i)). Do not give details, and omit definitions that are in the notes. Your answer should be about three brief bullet points or half a page of handwriting.

11. Let f be a nonconstant polynomial over $\mathbb{Z}$. Prove that

$$f \text{ is primitive and irreducible over } \mathbb{Q} \iff f \text{ is irreducible over } \mathbb{Z}.$$

12. 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 σ in L, and that

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

(Don't get distracted by the hypothesis that $\operatorname{char} L \neq 2$, which is common in algebra. Put it to the back of your mind, and when you've done the question, look over your solution to see if you used it without realizing.)

(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 $d \in K$.

13. Prove that the field extension $\overline{\mathbb{Q}} : \mathbb{Q}$ is not finite. (Hint: use Exercise 3.3.15.) Deduce that $\overline{\mathbb{Q}} : \mathbb{Q}$ is not even finitely *generated*.

14. A field extension $M : K$ is said to be **simple algebraic** if there exists $\alpha \in M$ such that $M = K(\alpha)$ and α is algebraic over K. Prove that $M : K$ is simple algebraic if and only if it is simple and algebraic.

15. 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.

16. 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

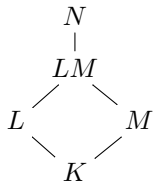
$$\mathbb{Q}(t_1, t_2, \ldots) : \mathbb{Q}(t_2, t_3, \ldots), \qquad \mathbb{Q}(t_2, t_3, \ldots) : \mathbb{Q}(t_2, t_3, \ldots)$$

(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 $\mathbb{Q}(t_2, t_3, \ldots)$.

17. 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.)

Challenge questions

18. Let K, L and M be subfields of a field N, with $K \subseteq L$ and $K \subseteq M$:



Here you will prove the 'diamond inequality', $[LM : L] \leq [M : K]$.

(i) As a warm-up, first suppose that $M = K(\beta)$ for some β algebraic over K. Show that $LM = L(\beta)$, then use a result in the notes to deduce that $[LM : L] \leq [M : K]$.

(ii) Now prove the diamond inequality when $M = K(\beta_1, \ldots, \beta_n)$ for some $\beta_1, \ldots, \beta_n$ algebraic over K. (Hint: tower law.)

(iii) Finally, prove the diamond inequality in full generality.

19. Figure 5.1 (p.70) 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

$$d(\alpha, \beta) = \log\big[K(\alpha, \beta) : K(\beta)\big].$$

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

20. 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 $z \in \mathbb{R}$.