Galois Theory Workshop 2

Polynomials and field extensions

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. In fact, your life will be much harder if you don't.

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

   (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. 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.

3. (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.)

4. (i) Let $f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{Z}[t]$. Let c/d be a rational root of f, where c and d are coprime integers. Prove the **rational roots theorem**: $c \mid a_0$ and $d \mid a_n$.

   (ii) Deduce that every rational root of a monic polynomial over $\mathbb{Z}$ is an integer.

   (iii) Show that $2t^5 + 4t + 3$ has no rational roots. (Don't forget about negative divisors.)

   (iv) Describe an algorithm that takes as input a polynomial over $\mathbb{Q}$ and produces as output its set of roots in $\mathbb{Q}$.

5. (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.

6. Prove that $\cos(\pi/9)$ is algebraic over $\mathbb{Q}$, and find its minimal polynomial. (Hint: begin by finding a general formula for $\cos 3\theta$.)

7. *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.

8. Let $f(t) \in \mathbb{Z}[t]$. Prove that

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

9. Does every field have a nontrivial extension?

10. Find an irreducible polynomial $f \in \mathbb{R}[t]$ such that $\mathbb{R}[t]/\langle f \rangle \cong \mathbb{C}$ (and prove it!).

11. Why do we tend to focus on $\mathbb{Q}$ as opposed to $\mathbb{R}$? One answer is that things over $\mathbb{R}$ tend to be a bit trivial, and this question demonstrates one aspect of that.

    (i) Let $x, y \in \mathbb{R}$. What is the minimal polynomial of $x + iy$ over $\mathbb{R}$?

    (ii) Which polynomials over $\mathbb{R}$ are irreducible? (This might sound like an open-ended question, but you have the tools to give a complete answer.)

12. Let K be a field. In this question, you'll find all the ring automorphisms of $K[t]$.

    (i) For $f \in K[t]$, there is a unique homomorphism $\theta_f \colon K[t] \to K[t]$ such that $\theta_f(t) = f$ and $\theta_f(a) = a$ for all $a \in K$. Which result in the notes guarantees this?

    (ii) For $f, g \in K[t]$, what is $\theta_f(g)$ in explicit terms? (There's a very short answer.) What is its degree?

    (iii) For $f_1, f_2 \in K[t]$, what can you say about the composite homomorphism

    $$K[t] \xrightarrow{\theta_{f_1}} K[t] \xrightarrow{\theta_{f_2}} K[t]?$$

    (iv) Using the previous parts, find all the isomorphisms $K[t] \to K[t]$.