Galois Theory Workshop 1

Revision; overview of Galois theory

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. Keep the other ones for practice another day.

1. In this course, *ring* means commutative ring with multiplicative identity, 1. By definition, ring *homomorphisms* φ preserve multiplicative identities: $\varphi(1) = 1$.

   (i) Let R be a ring. What is an *ideal* of R? Write down the definition.

   (ii) Let I be an ideal of a ring R. Write down the definition of the *quotient ring* (factor ring) R/I and the *canonical homomorphism* (natural homomorphism or quotient map) $\pi_I : R \to R/I$.

   (iii) Let I be an ideal of a ring R. Write down a precise statement of the universal property of the quotient ring R/I. (If you've forgotten what it is, look in Section 3.6 of your Honours Algebra notes.)

   (iv) Briefly *sketch* the proof of the universal property. Don't write out the whole proof: just summarize it in a few short bullet points.

2. Let f be a quadratic polynomial over $\mathbb{Q}$, and let α_1, α_2 be its roots in $\mathbb{C}$ (which may be equal). Show that it is impossible that $\alpha_1 \in \mathbb{Q}$ but $\alpha_2 \notin \mathbb{Q}$.

3. Let f be a quadratic polynomial over $\mathbb{Q}$. Using the definition of Galois group in Chapter 1 of the notes, prove that $\mathrm{Gal}(f)$ is S_2 if f has two distinct irrational roots, and trivial otherwise.

   (Here 'irrational' means not in $\mathbb{Q}$, so any non-real complex number is irrational. Hint: use an argument like the first proof of Example 1.1.5, replacing $\sqrt{2}$ by the square root of the discriminant of f.)

4. Let R be a ring and let $\varphi : 1 \to R$ be a homomorphism, where 1 denotes the trivial ring. Prove that R is trivial too and that φ is an isomorphism.

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

6. Let K be a field such that for $\alpha, \beta \in K$,

   $$\alpha \text{ is a square root of } \beta \iff \beta \text{ is a square root of } \alpha.$$

   How many elements does K have? Justify your answer fully.