Galois Theory Workshop 1

Overview of Galois theory; group actions, rings and 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. Keep the other ones for practice another day.

1. 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 $\alpha_2 \notin \mathbb{Q}$.

2. 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.)

3. Let G be a group acting on a set X. Let $S \subseteq G$, and write $\langle S \rangle$ for the subgroup of G generated by S. Prove that $\mathrm{Fix}(S) = \mathrm{Fix}(\langle S \rangle)$.

4. (i) Can C_6 act faithfully on a 4-element set? Give either an example or a proof that it is impossible.

   (ii) Let G be a finite group acting transitively on a nonempty finite set X. Prove that $|X|$ divides $|G|$. (Hint: orbit-stabilizer theorem.)

5. (i) Let R be a ring and let $I_0 \subseteq I_1 \subseteq \cdots$ be ideals of R. Prove that $\bigcup_{n=0}^{\infty} I_n$ is an ideal of R.

   (ii) Let R be a principal ideal domain and let $I_0 \subseteq I_1 \subseteq \cdots$ be ideals of R. Prove that there is some $n \geq 0$ such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

   (iii) Let R be an integral domain. Let $r, s \in R$ with $r \neq 0$ and s not a unit. Prove that $\langle rs \rangle$ is a proper subset of $\langle r \rangle$.

   (iv) Let R be a principal ideal domain. Let $r \in R$ be neither 0 nor a unit. Prove that some irreducible divides r.

   (Hint: if not then, writing $r_0 = r$, we have $r_0 = r_1 s_1$ for some non-units r_1 and s_1. Apply the same argument to r_1, and so on forever, then consider the ideals $\langle r_n \rangle$ to get a contradiction.)

   This result is the first step towards proving that in a principal ideal domain, every nonzero element can be expressed as a product of irreducibles in an essentially unique way. We won't need that fact except in rings of polynomials, where we'll use a different proof.

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.

7. Let R be a ring and let $\varphi\colon 1 \to R$ be a homomorphism, where 1 denotes the trivial ring (zero ring). Prove that R is trivial too and that φ is an isomorphism.

8. Let $f(t) = t^4 + t^3 + t^2 + t + 1$, which has roots $\omega, \omega^2, \omega^3, \omega^4$ where $\omega = e^{2\pi i/5}$. In the notes, you were told that one of the elements of $\mathrm{Gal}(f)$ is

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

   (i.e. $\omega \mapsto \omega^2 \mapsto \omega^4 \mapsto \omega^3 \mapsto \omega$). We didn't prove this, but for this question you can take it as given.

   Prove that $\mathrm{Gal}(f)$ is generated by σ, and deduce that $\mathrm{Gal}(f) \cong C_4$.

   (This question is maybe a bit harder.)