Math 601 – Spring 2026 – Harry Tamvakis
PROBLEM SET 8 – Due April 16, 2026

"Originally, the equation $x^2+1=0$ had no solution. Then the two solutions i and $-i$ were invented. But there is absolutely no way to tell who is i and who is $-i$. That is Galois Theory. Thus, Galois Theory tells you how far we cannot distinguish between the roots of an equation. This is codified in the Galois Group."

– Shreeram S. Abhyankar

A1) Let $L \supset \mathbb{Q}$ be the splitting field of $f(x) = x^4 - 2$. Work out the Galois correspondence for $L \supset \mathbb{Q}$. You should:

(a) Find $[L : \mathbb{Q}]$.

(b) Find $G(L/\mathbb{Q})$ and make a diagram of its subgroups and the containment relations between them. G is isomorphic to a group that we studied last semester. Which one?

(c) Make a corresponding diagram for the subfields of L, containment relations between them, and their degrees.

(d) Identify which subfields of L are Galois extensions of $\mathbb{Q}$.

A2) Suppose $L \supset F$ is a finite Galois field extension and m divides $[L : F]$. Prove that if m is prime, there is a subfield K of L containing F such that $[L : K] = m$. Show that this statement is false if m is not prime.

A3) Let k be an integer and let $f(x) := x^3 - kx^2 - (k+3)x - 1$.

(a) Show that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Show that if α is a root of $f(x)$, then $-1/(1+\alpha)$ is a root of $f(x)$.

(c) Let K be the splitting field of $f(x)$. Show that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.

A4) (a) Suppose that the fields K and K' are two finite Galois extensions of the rational numbers $\mathbb{Q}$. If K is isomorphic to K', prove that $K = K'$.

(b) Show that for every $n \geq 2$ there exist n isomorphic but different subfields of the complex numbers.

B1) This problem outlines a proof of the fundamental theorem of algebra using Galois theory. You should do parts (a) and (b) without appealing to either Galois theory or the fundamental theorem!

(a) Show that there are no irreducible polynomials of odd degree over $\mathbb{R}$.

(b) Show that there are no quadratic extensions of $\mathbb{C}$.

(c) Let $f \in \mathbb{R}[x]$ and suppose that K is the splitting field of f over $\mathbb{R}$. Let $G = G(K(i)/\mathbb{R})$ and show that $|G|$ is a power of two. [Hint: Use (a) to show that G is equal to its 2-Sylow subgroup.]

(d) Show that $[K(i) : \mathbb{C}]$ is a power of 2. Now use (b) to deduce that real polynomials split over $\mathbb{C}$.

(e) Show that any complex polynomial has a root in $\mathbb{C}$, hence splits over $\mathbb{C}$.

B2) (a) Let $f(x)$ be a monic irreducible polynomial in $\mathbb{Q}[x]$ and let K be a finite Galois extension of $\mathbb{Q}$. If g and h are monic irreducible factors of f in $K[x]$, show that there exists an automorphism σ of K over $\mathbb{Q}$ such that $g = \sigma(h)$ (applied coefficient-wise).

(b) Give an example where this conclusion is not valid if K is not Galois over $\mathbb{Q}$.

B3) Let F be a field and $F(x)$ the quotient field of $F[x]$. In this problem it will be useful to recall your work on problem (B3) from last week's set.

(a) Let $\mathrm{GL}_2(F)$ be the group of invertible 2×2 matrices with entries in the field F. For every $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{GL}_2(F)$, define

$$\rho x := \frac{ax + b}{cx + d} \in F(x).$$

Show that there is a unique F-automorphism $\overline{\rho} : F(x) \to F(x)$ so that $\overline{\rho}(x) = \rho x$.

(b) Show that $\rho \longmapsto \overline{\rho}$ defines a group homomorphism

$$\phi : \mathrm{GL}_2(F) \longrightarrow G(F(x)/F).$$

(c) Show that ϕ is *surjective*, that is, the F-automorphisms of $F(x)$ are all given by fractional linear transformations.

(d) Deduce that the Galois group $G(F(x)/F)$ is isomorphic to $\mathrm{PGL}_2(F) := \mathrm{GL}_2(F)/Z$, where Z is the center of $\mathrm{GL}_2(F)$.

(e) Define the elements $\sigma, \tau \in \mathrm{Aut}(F(x))$ by

$$(\sigma f)(x) = f\left(\frac{1}{1-x}\right) \quad \text{and} \quad (\tau f)(x) = f\left(\frac{1}{x}\right)$$

for $f \in F(x)$. Let $G = \langle \sigma, \tau \rangle$ be the group generated by σ and τ. Show that the function

$$g(x) := \frac{(x^2 - x + 1)^3}{x^2(x-1)^2}$$

is fixed by all the elements of G. Prove further that $F(g)$ is precisely the fixed field of G, and that $G \cong S_3$.

C problem

C1) Let $f \in \mathbb{C}[x]$ be a non-constant polynomial. When is $\mathbb{C}(x)$ a Galois extension of $\mathbb{C}(f)$?