Math 601 – Spring 2026 – Harry Tamvakis

PROBLEM SET 9 – Due April 23, 2026

A1) Let K/F be a Galois extension whose Galois group is the symmetric group S_3. Is it true that K is the splitting field of an irreducible cubic polynomial over F? [Hint: Find an intermediate subfield $E = F(\alpha)$ of degree 3 over F and consider the minimal polynomial of α.]

A2) Let L/F be a Galois extension of degree 15.

(a) Show that every subextension K with $F \subset K \subset L$ is normal.

(b) Suppose that $f(x) \in F[x]$ is irreducible and its splitting field is L. Show that $\deg(f(x)) = 15$.

A3) Let F be an algebraically closed field. Show that there is an infinite subfield of F that is algebraic over the prime subfield of F, but is not algebraically closed.

A4) Suppose $K/\mathbb{Q}$ is a Galois extension such that $\mathrm{Gal}(K/\mathbb{Q}) = A_5$, the group of even permutations of 5 letters. Show that there is an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree 20 such that K is the splitting field of $f(x)$.

A5) Let α be algebraic over $\mathbb{Q}$ and let L be the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$, that is, the smallest Galois extension of $\mathbb{Q}$ which contains $\mathbb{Q}(\alpha)$. Let p be a prime dividing the order of $G(L/\mathbb{Q})$. Prove that there exists a subfield K of L with $[L : K] = p$ and $L = K(\alpha)$.

B1) Let $f \in \mathbb{Q}[x]$ be irreducible of degree p, where p is a prime. Let K be the splitting field of f and suppose that there are roots α and β of f such that $K = \mathbb{Q}(\alpha, \beta)$. We regard the Galois group $G = G(K/\mathbb{Q})$ as a subgroup of the symmetric group S_p.

(a) Show that $|G| \leq p(p-1)$.

(b) Show that G contains a p-cycle σ.

(c) Prove that the subgroup $H = \langle \sigma \rangle$ of G generated by σ is a normal subgroup of G.

(d) Prove that G/H is a cyclic group of order dividing $p - 1$. Deduce that G is solvable.

Remark: Galois proved the converse statement: If G is solvable for an irreducible polynomial f of prime degree, then the splitting field can be generated by two roots of f.

B2) Let F be a subfield of the real numbers $\mathbb{R}$. Suppose that $a \in F$, let $\sqrt[n]{a}$ be a real n-th root of a, and set $L = F(\sqrt[n]{a})$. Prove that if K is any Galois extension of F with $K \subset L$ then $[K : F] \leq 2$.

B3) Let $K \supset F$ be a finite extension of fields with Galois group $G = G(K/F)$. Then G acts on the elements of K. By a *Galois basis* of K over F we mean a linear basis of K over F that is the orbit under G of a single element of K.

(a) Show that if a Galois basis of K over F exists, then K is a Galois extension of F.

For the next three questions assume that $K \supset F$ is Galois and $G = \{\sigma_1, \ldots, \sigma_n\}$.

(b) Given $\alpha \in K$, show that the set $\{\sigma(\alpha) \mid \sigma \in G\}$ is a Galois basis of K over F if and only if the matrix

$$\{\sigma_i \sigma_j(\alpha)\}_{1 \leq i,j \leq n}$$

has non-zero determinant.

(c) If $f \in F[x_1, \ldots, x_n]$ and

$$f(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) = 0$$

for every $\alpha \in K$, prove that $f = 0$. [Hint: For a basis $\{b_i\}$ of K over F set

$$g(y_1, \ldots, y_n) := f\left(\sum_i y_i \sigma_1(b_i), \ldots, \sum_i y_i \sigma_n(b_i)\right),$$

and deduce that $g = 0$.]

(d) For each i define a variable x_{σ_i} indexed by σ_i and set

$$f(x_{\sigma_1}, \ldots, x_{\sigma_n}) := \det(x_{\sigma_i \sigma_j}).$$

Show that $f(1, 0, \ldots, 0) \neq 0$ and deduce that a Galois basis of K over F always exists.