Math 404 – Spring 2025 – Harry Tamvakis
PROBLEM SET 9 – Due April 17, 2025

Reading for this week: Chapter 7.

Problems

1) (10 points) Let K be the splitting field of $f(x) = x^6 - 5$ over $\mathbb{Q}$. Work out the Galois correspondence for $K \supset \mathbb{Q}$. You should:

(a) Compute the degree $[K : \mathbb{Q}]$.

(b) Find $G(K/\mathbb{Q})$ and make a diagram of its subgroups and the containment relations between them.

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

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

2) Suppose that p is a prime and $\mathbb{F}_{p^n}$ is the finite field with p^n elements, for some $n \geq 1$. Show that $\mathbb{F}_{p^n} \supset \mathbb{F}_p$ is a Galois extension. Prove that the Galois group $G(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is a cyclic group, generated by the automorphism ϕ of $\mathbb{F}_{p^n}$ with $\phi(x) = x^p$, for all $x \in \mathbb{F}_{p^n}$.

3) Let $K \supset F$ be a finite field extension such that for any two subfields E_1 and E_2 of K containing F, either $E_1 \subset E_2$ or $E_2 \subset E_1$.

(a) Prove that there exists an element $\alpha \in K$ such that $K = F(\alpha)$.

(b) Show by example that $K \supset F$ need not be a Galois extension.

4) Let $K \supset F$ be a finite Galois extension with Galois group G, and let E be the fixed field of a subgroup H of G. Let

$$N := \{\sigma \in G \mid \sigma H \sigma^{-1} = H\}$$

be the *normalizer* of H in G. Observe that N is the largest subgroup of G in which H is normal.

(a) If $\sigma \in G(K/F)$, prove that $\sigma(E) = E$ if and only if $\sigma \in N$.

(b) Prove that the group $G(E/F)$ of all F-automorphisms of E is N/H.

5) Let $K \supset F$ be a Galois extension with Galois group $G = \{\sigma_1, \ldots, \sigma_n\}$. Let $\alpha \in K$ and let $\mathcal{O}_\alpha := \{\sigma_i(\alpha) \mid 1 \leq i \leq n\}$ be the orbit of α under the action of G on K. Let

$$G_\alpha := \{\sigma \in G \mid \sigma(\alpha) = \alpha\} = G(K/F(\alpha)).$$

Prove that

(a) $|\mathcal{O}_\alpha| = |G : G_\alpha| = [F(\alpha) : F]$;

(b) If $f(x)$ is the minimal polynomial of α over F, then we have

$$\prod_{\sigma \in G} (x - \sigma(\alpha)) = f(x)^{|G_\alpha|}.$$

6) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree three, with roots given by the complex numbers z_1, z_2, and z_3. Let $K = \mathbb{Q}(z_1, z_2, z_3)$.

(a) Show that $[K : \mathbb{Q}]$ is equal to 3 or 6.

(b) If $[K : \mathbb{Q}] = 6$, then prove that $G(K/\mathbb{Q})$ is isomorphic to S_3.

(c) Prove that $[K : \mathbb{Q}] = 6$ if and only if $(z_1 - z_2)(z_1 - z_3)(z_2 - z_3) \notin \mathbb{Q}$.

7) (a) Let a and b be rational numbers such that the polynomial $f(x) = x^3 + ax + b$ is irreducible over $\mathbb{Q}$. Find necessary and sufficient conditions on a and b so that the splitting field of $f(x)$ has degree exactly 3 over $\mathbb{Q}$. [Hint: Try to use the previous problem.]

(b) Compute the Galois groups over $\mathbb{Q}$ of the cubics (i) $x^3 - 39x + 26$, (ii) $x^3 - 12x + 8$, and (iii) $x^3 - 84x + 56$.

Extra Credit Problem.

EC) Let p be a prime number and let x, y be independent variables. Suppose that $F := \overline{\mathbb{F}}_p$ is the algebraic closure of the finite field $\mathbb{F}_p$. Prove that that the extension $F(x, y) \supset F(x^p, y^p)$ is of finite degree but is not a simple extension (i.e., is not generated over $F(x^p, y^p)$ by a single element). Do this by explicitly exhibiting an infinite number of fields E such that $F(x^p, y^p) \subset E \subset F(x, y)$.