Math 404 – Spring 2025 – Harry Tamvakis
PROBLEM SET 6 – Due March 27, 2025

Reading for this week: Chapters 5, 6 and Theorem 7.13.

Problems

1) Let α and β be complex numbers of degree 3 over $\mathbb{Q}$, and let $K = \mathbb{Q}(\alpha, \beta)$. What are the possible values of $[K : \mathbb{Q}]$? Give examples which illustrate that each of your values is indeed possible (with proof).

2) Let F be a subfield of the field $\mathbb{C}$ of complex numbers, and let $f(x) \in F[x]$ be an irreducible polynomial over F. Prove that $f(x)$ has no multiple root in $\mathbb{C}$.

3) Give an example of two different irreducible monic polynomials (a) in $\mathbb{Q}[x]$ and (b) in $\mathbb{F}_2[x]$ which have the same splitting field.

4) Factor the polynomials $x^9 - x$ and $x^{27} - x$ into a product of irreducible factors in $\mathbb{F}_3[x]$. Prove that your factors are indeed irreducible.

5) Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Determine all polynomials f in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$ for all $\alpha \in \mathbb{F}_q$.

6) Let n be an odd positive integer, and let F be a field of cardinality 2^n. Prove that if $a, b \in F$ and $a^2 + ab + b^2 = 0$, then $a = b = 0$.

7) Let F be a finite field. Prove that the product of all the nonzero elements of F is equal to -1.

8) Show that if F is an infinite field, then the multiplicative group $(F^\times, \cdot)$ is not cyclic.

Extra Credit Problems.

EC1) Let $\mathbb{C}(x)$ be the quotient field of the polynomial ring $\mathbb{C}[x]$. Let $t \in \mathbb{C}(x)$ be the rational function $t = p(x)/q(x)$, where $p, q \in \mathbb{C}[x]$ are relatively prime polynomials and $q \neq 0$. Then $\mathbb{C}(x)$ is an extension of the field $\mathbb{C}(t)$.

(a) Show that the polynomial $p(z) - tq(z)$ in the variable z and coefficients in $\mathbb{C}(t)$ is irreducible over $\mathbb{C}(t)$ and has x as a root. [Hint:

First show that this polynomial is irreducible in $(\mathbb{C}[t])[z]$; note that $(\mathbb{C}[t])[z] = (\mathbb{C}[z])[t]$. Then use the general form of Gauss' Lemma].

(b) Show that $[\mathbb{C}(x) : \mathbb{C}(t)] = \max(\deg p(x), \deg q(x))$.

EC2) (a) In the notation of problem EC1, prove that $\mathbb{C}(t) = \mathbb{C}(x)$ if and only if

$$t(x) = \frac{ax + b}{cx + d}$$

for some $a, b, c, d \in \mathbb{C}$ such that $ad - bc \neq 0$.

(b) An *automorphism* of a field F is a field isomorphism $\phi : F \to F$. Determine the group G of all automorphisms ϕ of $\mathbb{C}(x)$ which are the identity map on $\mathbb{C}$, that is, $\phi(w) = w$ for all $w \in \mathbb{C}$ (try to identify G with a certain matrix group).