PROBLEM SET 14

DUE: June 9

Problem 1

Let F be a finite field with $q = p^n$ elements, where p is a prime. $f(x) \in F[x]$ is an irreducible polynomial. Show that $f(x)$ has multiple zeros if and only if there exists $g(x) \in F[x]$ such that $f(x) = g(x^p)$.

Problem 2

Let F be a finite field with $q = p^n$ elements, where p is a prime. Let H be a subgroup of $Aut(F)$ of order m. $K = \{a \in F | \forall \sigma \in H,\ \sigma(a) = a\}$. Prove that:

(1). $m|n$.

(2). K is the unique subfield of F of order $p^{\frac{n}{m}}$.

Problem 3

Let Ω_p be the algebraic closure of the finite field F_p where p is a prime, and the unique subfield of Ω_p of order p^n is denoted by F_{p^n}. Show that:

(1). $F_{p^m} \subset F_{p^n}$ if and only if $m|n$.

(2). Suppose that $F_{p^m} \subset F_{p^n}$. Let $G = \{\sigma \in Aut(F_{p^n}) | \forall a \in F_{p^m},\ \sigma(a) = a\}$. Then G is a cyclic group of order $\frac{n}{m}$.

Problem 4

Let K be a field, $\sigma \in Aut(K)$. Show that K/K^σ is a separable extension.

Problem 5

Show that for $n \leq m$, there exist n matrices $A_1, A_2, ..., A_n \in M_{m\times m}(F_q)$ such that $\forall (x_1, x_2, ..., x_n) \neq 0$,we have

$$x_1A_1 + x_2A_2 + ... + x_nA_n \neq 0.$$

Problem 6

(1). Show that any functions $f : F_q^n \to F_q$ can be represented by an element in $F_q[x_1, ..., x_n]$. That is, there exists a polynomial $g \in F_q[x_1, ..., x_n]$ such that $\forall x \in F_q^n,\ g(x) = f(x)$.

*(2). For the given f as above, $g \in F_q[x_1, ..., x_n]$ is uniquely determined after modulo the ideal $(x_1^q - x_1, ..., x_n^q - x_n)$.

Problem 7

Let $E = \boldsymbol{Q}(\sqrt{2}, \sqrt{3}, u),\ u^2 = (9 - 5\sqrt{3})(2 - \sqrt{2})$. Show that $E/\boldsymbol{Q}$ is a Galois extension and determine its Galois group.