PROBLEM SET 13
DUE: June 2

Problem 1

Let K be a finite field with p^n elements. Show that every element of K must have a unique p-th root in K.

Problem 2

Write down the explicit structure of the finite field of order 8.

Problem 3

Let $f(x)$ be a monic irreducible polynomial in $F_p[x]$ of degree n.

(1). If u is a zero of $f(x)$, then $f(x)$ has n distinct zeros, $u, u^p, ..., u^{p^{n-1}}$.

(2). If a zero u is the generator of the multiplicative group of $F_p(u)$, then each zero of $f(x)$ is also the generator of $F_p(u)^*$.

(3). We say a polynomial $g(x)$ is primitive in $F_p[x]$, if one of its zero u is a generator of $F_p(u)^*$. Then show that the number of primitive polynomials in $F_p[x]$ of degree n is $\frac{\phi(p^n-1)}{n}$.

Problem 4

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

(2). Suppose $F_{p^m} \subset F_{p^n}$, compute the Galois group $Gal(F_{p^n}/F_{p^m})$.

Problem 5

Let E/F be a separable extension and M is a intermediate field. Show that E/M and M/F are separable.

Problem 6

Let K be a field of characteristic p and let u, v be algebraically independent over K. Show that

(1). $K(u, v)$ has degree p^2 over $K(u^p, v^p)$.

(2). $K(u, v)/K(u^p, v^p)$ is not a simple extension.

(3). There exist infinitely many intermediate field of $K(u, v)/K(u^p, v^p)$.

Problem 7

(1). Let $E = F(x)$ where x is transcendental over F. Let $K \neq F$ be a subfield of E which contains F. Show that x is algebraic over K.

(2). Let $E = F(x)$. Let $y = \frac{f(x)}{g(x)}$ be a rational function, with relatively prime polynomials $f, g \in F[x]$. Let $n = max\{deg(f), deg(g)\}$, and suppose $n \geq 1$. Prove that $[F(x) : F(y)] = n$.

Problem *8

Let P be the set of positive integers and R the set of functions defined on P with values in a commutative ring K. Define the sum in R to be the ordinary addition of functions and define the **convolution product** by the formula:

$$(f * g)(m) = \sum_{xy=m} f(x)g(y),$$

where the sum is taken over all pairs (x, y) of positive integers such that $xy = m$.

(1). Show that R is a commutative ring, whose unit element is the function δ such that $\delta(1) = 1$ and $\delta(x) = 0$ if $x \neq 1$.

(2). A function is said to be **multiplicative** if $f(mn) = f(m)f(n)$ whenever m, n are relatively prime. If f, g are multiplicative, show that $f * g$ is also multiplicative.

(3). Let μ be the **Mobius function** such that $\mu(1) = 1, \mu(p_1...p_r) = (-1)^r$ if $p_1, ..., p_r$ are distinct primes, and $\mu(m) = 0$ if m is divisible by p^2 for some prime p.

Show that $\mu * 1 = \delta$. The Mobius inversion formula of elementary number theory is then nothing else but the relation $\mu * 1 * f = f$.

(4). Let $f, g : P \to A$ be maps where A is an additive abelian group. Suppose that for all n,

$$f(n) = \sum_{d|n} g(d).$$

Let μ be the Mobius function. Prove that

$$g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d).$$

(5). Let K be a finite field of order q. Let $f(x) \in K[x]$ be irreducible. Show that $f(x)$ divides $x^{q^n} - x$ if and only if deg(f) divides n. And show the multiplication formula

$$x^{q^n} - x = \prod_{d|n} \prod_{f_d, irr} f_d(x),$$

where the inner product is over all irreducible polynomials of degree d with leading coefficient 1. Counting degrees, show that

$$q^n = \sum_{d|n} d\psi(d),$$

where $\psi(d)$ is the number of irreducible polynomials of degree d. Invert by (4), find that

$$n\psi(n) = \sum_{d|n} \mu(d) q^{\frac{n}{d}}.$$

(6). As a consequence, what is the number of irreducible polynomials of degree 6 over F_2?

(7). Furthermore, let p_n be the probability that a polynomial of degree n is irreducible. What is the limit of p_n? And what does it mean?