Algebra 4 (2004-05) – Assignment 6

Instructor: Dr. Eyal Goren

Submit by Monday, March 7, 24:00 by mail-box on 10^{th} floor.

1.)

(1) Prove the following formula:

$$x^{p^n} - x = \prod f(x),$$

where the product is taken over all f irreducible monic polynomials in $\mathbb{F}_p[x]$ of some degree d dividing n. (Hint: group the elements of $\mathbb{F}_{p^n}$ according to their minimal polynomial.) Also, write this down explicitly for $p = 2$ and $n = 4$.

(2) Define the *Möbius function* μ as follows. It is a function on the positive integers and

$$\mu(n) = \begin{cases} 1, & n = 1; \\ 0, & p^2 \text{ divides } n \text{ for some prime } p; \\ (-1)^r, & n \text{ is a product of } r \text{ distinct primes.} \end{cases}$$

Let $f : \mathbb{N}^+ \longrightarrow \Gamma$ be a function, where $\mathbb{N}^+ = \{1, 2, 3, \dots\}$ and Γ is an abelian group. Let

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

(The summation is always over positive divisors, including 1 and n.) Prove the *Möbius inversion formula*:

$$f(n) = \sum_{d|n} \mu(n/d)F(d).$$

(3) Apply the results above to deduce that the number of irreducible monic polynomials in $\mathbb{F}_p[x]$ of degree n is

$$\frac{1}{n}\sum_{d|n} \mu(n/d)p^d.$$

2). Find the degree of the splitting field of the polynomial $x^3 - 3$ over $\mathbb{Q}$, over $\mathbb{Q}[i]$, and over the finite fields with $2, 3, 4, 5, 7$ elements. The same with $x^4 - 1$.