Math 503 Homework 6

Due Wed. Oct. 24

1. (a) Let k be a field. Prove there are infinitely many monic irreducible polynomials in the polynomial ring $k[X]$, in the following two ways:

(i) Starting with the statement (which should be justified) that if m and n are relatively prime positive integers then $(X^m - 1)/(X - 1)$ and $(X^n - 1)/(X - 1)$ are relatively prime in $k[X]$.

(ii) Starting with the statement (which should be justified) that for any $n > 0$ not divisible by the characteristic of k, the polynomial $X^n - 1$ has no multiple factors—i.e., if e is a positive integer and $f \in k[X]$ is a nonunit such that $f(X)^e$ divides $X^n - 1$, then $e = 1$. (Do not use part (a).)

(b) Show that if k is finite, then for each $n > 0$ there is an irreducible polynomial in $k[X]$ of degree n. Is a similar statement true for *all* fields?

(c) Let q be a power of a prime integer, and denote by $\mathbb{F}_q$ the finite field with q elements. Show that in $\mathbb{F}_q[X]$ the polynomial $X^{q^n} - X$ is the product of all the monic irreducible polynomials of degree d with d running through all divisors of n, each factor occurring with multiplicity 1.

(d) Factor $X^{15} - 1$ into irreducibles over $\mathbb{F}_2$ and over $\mathbb{F}_4$.

(e) With q as in (c), prove that if $N_q(d)$ is the number of monic irreducible polynomials of degree d in $\mathbb{F}_q[X]$ then for any $n > 0$,

$$q^n = \sum_{d|n} dN_q(d).$$

(f) [Extra Credit.] Let μ be the Möbius function, defined in Clark, 25$\boldsymbol{\beta}$.

(i) Look up the *Möbius inversion formula* via Google, and use it to show that

$$N_q(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d.$$

(ii) Calculate $N_4(12)$.

Do the following problems in Clark:

2. 108$\boldsymbol{\beta}$.

3. 110$\boldsymbol{\epsilon}$.

4. 112β.

5. Let K, E, F and G be fields, with $K \subset E \subset G$ and $K \subset F \subset G$. Prove:

(a) If E/K is finite (respectively, algebraic), then

$$EF := \{ \sum_{i=1}^{n} e_i f_i \mid e_i \in E,\ f_i \in F,\ n > 0 \} \subset G$$

is a finite (respectively, algebraic) field extension of F.

(b) If the extensions E/K and F/K are both algebraic, then so is the extension EF/K.