HOMEWORK 7

DUE 1 MARCH 2014

Read the Example on pages 549–550 of Dummit and Foote about finite fields with p^n elements.

1. Let $\mathbb{F}_q(t)$ be the rational function field in t over a finite field $\mathbb{F}_q$ of characteristic p. Let $K/\mathbb{F}_q(t)$ be a finite extension.

(a) Describe briefly why $K^{p^n} = \left\{x^{p^n}; x \in K\right\}$ is a field for any $n \in \mathbb{Z}$.

(b) Show that $K^{1/p} = K\left(\alpha^{1/p}\right)$ for any $\alpha \in K \setminus K^p$. (Hint: first show that $[K : K^p] = p$.)

2. (Optional, but good for you!) Let $F = \mathbb{F}_q$ be a finite field with q elements of characteristic p.

(a) Let $f(X_1, \ldots, X_n)$ be a polynomial in $F[X_1, \ldots, X_n]$ of degree d and assume that $f(0, \ldots, 0) = 0$. An element $a = (a_1, \ldots, a_n) \in F^n$ such that $f(a) = 0$ is called a zero of f. If $n > d$, show that f has at least one other zero in F^n. [Hint: Assume the contrary, and compare the degrees of the reduced polynomial belonging to

$$1 - f(X)^{q-1}$$

and $(1 - X_1^{q-1})(1 - X_2^{q-1}) \ldots (1 - X_n^{q-1})$. (The theorem is due to Chevalley.)

(b) Refine the above results by proving that the number N of zeros of f in F^n is divisible by p arguing as follows.

(i) Let i be a positive integer. Show that

$$\sum_{\alpha \in F} \alpha^i = \begin{cases} q - 1 = -1 & \text{if } q - 1 \mid i \\ 0 & \text{if } q - 1 \nmid i. \end{cases}.$$

0 otherwise.

(ii) Denote the preceding function of i by $\psi(i)$. Show that

$$N \equiv \sum_{x \in F^n} (1 - f(x)^{q-1})$$

(iii) Show that, for each n-tuple $(i_1, \ldots, i_n)$ of nonnegative integers,

$$\sum_{x \in F^n} x_1^{i_1} \ldots x_n^{i_n} = \psi(i_1) \ldots \psi(i_n).$$

(iv) Show that both terms in the sum for N above yield 0 mod p. (The above argument is due to Warning.)

(c) Extend Chevalley's theorem to r polynomials $f_1, \ldots, f_r$ of degrees $d_1, \ldots, d_r$ respectively, in n variables. If they have no constant term and $n > \sum d_i$, show that they have a non-trivial common zero.

(d) Show that an arbitrary function $f : F^n \longrightarrow F$ can be represented by a polynomial. (As before, F is a finite field.)

From Dummit and Foote: section **13.1** problem 2; section **13.2** problems 5, 7, 9; section **13.4** problem 1.