Math 553 Homework 13

Due Mon. Dec. 3, 2012.

1. D& F, p. 622, #40(c).

2. D& F, p. 623, #48.

3. Let $L \supset K$ be finite fields, $c := |K|$, and let $f(X) \in K[X]$ be irreducible, of degree e dividing $[L : K]$. Show that there is an $a \in L$ such that in $L[X]$,

$$f(X) = (X - a)(X - a^c)(X - a^{c^2}) \cdots (X - a^{c^{e-1}}).$$

How many such a are there?

4. Let $p \neq q$ be odd primes, and let $\mathbb{F}_{q^n}$ be a field of cardinality q^n where n is such that the multiplicative group $\mathbb{F}_{q^n}^*$ has order divisible by p (e.g., $n = p - 1$). Let ζ be an element of order p in $\mathbb{F}_{q^n}^*$. For any integer a, let

$$g_a = \sum_{t=1}^{p-1} (t/p)\zeta^{at}$$

$$\text{where} \qquad \begin{cases} (t/p) = 1 & \text{if } t \text{ is a square in } \mathbb{Z}/p, \\ (t/p) = -1 & \text{if } t \text{ is not a square in } \mathbb{Z}/p. \end{cases}$$

Write g for g_1.

(a) Prove that if p doesn't divide a then $g_a = (a/p)g$.

(b) Prove that $g^q = g_q$; and assuming $g \neq 0$, deduce from (a) that

$$g \in \mathbb{F}_q \Leftrightarrow (q/p) = 1.$$

(c) It can be shown that $g^2 = (-1/p)p = \text{(say) } p^*$.[1] Assuming this, show that

$$g \in \mathbb{F}_q \Leftrightarrow (p^*/q) = 1.$$

(The equality $(q/p) = (p^*/q)$ resulting from (b) and (c) is *quadratic reciprocity*).

---

[1] See Ireland and Rosen, *A Classical Introduction to Modern Number Theory,* p. 71, Prop. 6.3.2; or D&F, p. 637, #11.

5. Notation remains as in 4. Set

$$\Delta := \prod_{p>b>a>0} (\zeta^b - \zeta^a).$$

Let $f(X)$ be the polynomial

$$f(X) := X^{p-1} + X^{p-2} + \cdots + X + 1 = (X^p - 1)/(X - 1) = \prod_{a=1}^{p-1} (X - \zeta^a).$$

(a) Show that the discriminant of f is

$$\Delta^2 = (-1)^{(p-1)/2} \prod_{a=1}^{p-1} f'(\zeta^a) = (-1/p)p^{p-2}.$$

(b) Let r be the order of q in the multiplicative group $(\mathbb{Z}/p)^*$. Let φ be the automorphism $x \mapsto x^q$ of $\mathbb{F}_{q^n}$, and let σ be the corresponding permutation of the roots of f. Show that σ is a product of $(p-1)/r$ cycles of length r, and deduce that σ is an odd permutation iff $(p-1)/r$ is odd.

(c) Deduce from (b) that $\varphi(\Delta) = (q/p)\Delta$.

(d) Deduce quadratic reciprocity from (a) and (c).