April 22, 2011

**18.702 Problem Set 8**

due friday, April 29, 2011

1. Chapter 16, Problem 1.1. *(some symmetric functions)*

2. Chapter 16, Problem 2.4b. *(a discriminant)*

3. Chapter 16, Problem 3.2. *(splitting fields)*

4. Chapter 16, Problem 5.1d. *(a fixed field)*

5. Chapter 16, Problem 6.1. *(fields containing $\sqrt{-31}$)*

6. *(Galois theory for finite fields)* Let $K$ be a finite field of order $q = p^r$, and let $F = \mathbb{F}_p$ be its subfield of order $p$ ($p$ prime).

(a) Prove that the *Frobenius map* $f : K \to K$ defined by $f(\alpha) = \alpha^p$ is an automorphism of $K$.

(b) Show that $f^r$ is the identity map on $K$, and that no lower power of $f$ is the identity.

(c) There exist irreducible polynomials of degree $r$ in $F[x]$. By examining the roots of such a polynomial in $K$, show that every automorphism is a power of $F$.

(d) The fixed field of an automorphism $\phi$ of $K$ is the set of elements such that $\phi(\alpha) = \alpha$. Determine the fixed field of $f^k$ for $k = 1, ..., r-1$.