MAT 612 **HW #8** Name _____

04/23/10, due Wednesday 04/28/10, 5 pm

25 points

1. Suppose E be a finite field of order q, with prime subfield $F \cong \mathbb{Z}_p, q = p^n$.

   (a) Prove that E is the splitting field over F of the polynomial $f(x) = x^q - x$.

   (b) Using (a), prove that, for any prime p and positive integer n, there exists a field E of order $q = p^n$, which is unique up to isomorphism.[1]

   (c) In the notation of part (a), prove that f is separable over F, and conclude that E is Galois over F.

   (d) Show that the mapping $x \mapsto x^p$ is an F-automorphism of E. Deduce that $\mathrm{Gal}(E, F)$ is isomorphic to $\mathbb{Z}_n$.

2. Prove that the Galois group of the polynomial $f(x) = x^4 - 2$ is isomorphic to the dihedral group D_4.

3. Suppose F is a field containing an element ω satisfying $\omega^n = 1$, and such that all roots of $x^n - 1$ are powers of ω. (ω is called a *primitive n^{th} root of unity.*) Let $E = F[\alpha]$, where $\alpha^n = a \in F$. Suppose $\mathrm{char}(F)$ does not divide n.

   (a) Show that E is Galois over F, and that $|\mathrm{Gal}(E, F)|$ divides n.

   (b) Show that there is an F-automorphism $\phi\colon E \to E$ satisfying $\phi(\alpha) = \alpha\omega^k$, for some $k, 0 < k < n$.

   (c) Choose ϕ so that k is minimal with $\phi(\alpha) = \alpha\omega^k$. Show that ϕ generates $\mathrm{Gal}(E, F)$, hence $\mathrm{Gal}(E.F)$ is cyclic.

4. Let $f(x, y) = x^2 + x^3 - y^2 \in \mathbb{C}[x, y]$.

   (a) Show f is irreducible. (Consider f as a polynomial in y over the PID $\mathbb{C}[x]$; apply Eisentein's Criterion.)

   (b) Let $I = (f)$ and $R = \mathbb{C}[x, y]/I$. Since f is irreducible, R is an integral domain. Let E be the quotient field of R. Show that E is (up to isomorphism) an extension field of $\mathbb{C}$.

   (c) Show that x represents a transcendental element of E over $\mathbb{C}$, and E is algebraic over $\mathbb{C}(x)$.

   (d) Show that F is Galois over $\mathbb{C}(x)$ and identify the Galois group.[2]

---

[1] This field is called "the Galois field of order q," denoted $\mathrm{GF}(q)$.

[2] The inclusion $\mathbb{C}(x) \hookrightarrow E$ corresponds to the projection from the curve $f(x, y) = 0$ onto the x axis.