Math 612 Homework 2

Paul Hacking

February 26, 2014

Reading: Dummit and Foote, 13.5,14.1,14.2,14.3.
Justify your answers carefully.

(1) Let $f = x^3 + x + 1 \in \mathbb{F}_2[x]$ and $K = \mathbb{F}_2(\alpha)$ be the field obtained by adjoining a root α of f. Then K is a finite field of order 8 with $\mathbb{F}_2$-basis $1, \alpha, \alpha^2$ (why?). For each of the elements of K, determine its minimal polynomial over $\mathbb{F}_2$.

(2) Let $f = x^4 + x + 1 \in \mathbb{F}_2[x]$ and $g = x^4 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$. The polynomials f and g are irreducible in $\mathbb{F}_2[x]$. Let $K = \mathbb{F}_2(\alpha)$ be the field obtained by adjoining a root α of f and $L = \mathbb{F}_2(\beta)$ the field obtained by adjoining a root β of g. Then K and L are finite fields of order 16, so according to the classification of finite fields they are isomorphic. Describe an isomorphism $\varphi\colon K \to L$ explicitly.

(3) Let F be a field, $f \in F[x]$ a polynomial of degree n, and K the splitting field of F. Show that the degree $[K : F]$ divides $n!$.

(4) Let $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$. Then f is irreducible over $\mathbb{Q}$ (why?). Show directly that if α is a root of f in some extension field then so is $\beta = \alpha^2 - 2$. Deduce that the splitting field K of f over $\mathbb{Q}$ is given by $K = \mathbb{Q}(\alpha)$ and so $[K : \mathbb{Q}] = 3$.

(5) Let F be a field of characteristic 2 and $F \subset K$ a field extension of degree $[K : F] = 2$. Show that there exists $\alpha \in K$ such that $K = F(\alpha)$ and either (a) $\alpha^2 \in F$ or (b) $\alpha^2 + \alpha \in F$. Show that the field extension $F \subset K$ is not separable in case (a) and is separable in case (b).

(6) Recall the following result (proved in class): Let K be a field and G a finite group of automorphisms of K. Let

$$K^G = \{\alpha \in K \mid g(\alpha) = \alpha \text{ for all } g \in G\}$$

be the fixed field of G. Then the extension $K^G \subset K$ is Galois with Galois group G. In particular, $[K : K^G] = |G|$. Moreover, if $\alpha \in K$, then the minimal polynomial of α over K^G is

$$f(x) = \prod_{i=1}^{r}(x - \alpha_i)$$

where $\{\alpha_1, \ldots, \alpha_r\}$ is the orbit of α under G.

Let $K = \mathbb{C}(t)$, the field of rational functions in the variable t with complex coefficients. Let $\zeta \in \mathbb{C}$ be a primitive nth root of unity. Consider the automorphisms σ and τ of K over $\mathbb{C}$ defined by $\sigma(t) = \zeta t$ and $\tau(t) = t^{-1}$. Let $G \subset \mathrm{Aut}(K)$ be the subgroup generated by σ and τ.

(a) Show that G is isomorphic to the dihedral group D_n of order $2n$.

(b) Determine the minimal polynomial of t over K^G.

(c) Show that the fixed field K^G equals $\mathbb{C}(u)$ for some $u \in \mathbb{C}(t)$ (to be determined explicitly).

[Hint: For part (c), it suffices to exhibit an element $u \in K^G$ such that $[K : \mathbb{C}(u)] = [K : K^G] = |G|$, then $\mathbb{C}(u) = K^G$. The degree $[K : \mathbb{C}(u)] = [\mathbb{C}(t) : \mathbb{C}(u)]$ can be computed either using part (b) or using the general result described in DF 13.2, Exercise 18, p. 530.]

(7) (Optional) Let $K = \mathbb{C}(t)$ and consider the automorphisms σ and τ of K over $\mathbb{C}$ given by $\sigma(t) = \frac{t+i}{t-i}$ and $\tau(t) = \frac{it-i}{t+1}$. Let G be the subgroup of $\mathrm{Aut}(K)$ generated by σ and τ. Prove that G is isomorphic to A_4 and show that $K^G = \mathbb{C}(u)$ for some $u \in \mathbb{C}(t)$ (to be determined explicitly).

(8) Let $K = \mathbb{C}(x_1, \ldots, x_n)$ be the field of rational functions in n variables $x_1, \ldots, x_n$ with complex coefficients.

(a) Describe an injective homomorphism from the symmetric group S_n to the group $\mathrm{Aut}(K)$ of automorphisms of the field K.

(b) Using part (a) or otherwise, show that for any finite group G there exists a field extension $F \subset K$ which is Galois with Galois group isomorphic to G.

[Remark: The following related problem is open: Given a finite group G, does there exist a field extension $\mathbb{Q} \subset K$ which is Galois with Galois group isomorphic to G?]

(9) Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$.

(a) Find a basis of K as a vector space over $\mathbb{Q}$.

(b) Describe the Galois group of K over $\mathbb{Q}$.

(c) Determine all the intermediate fields L, $\mathbb{Q} \subset L \subset K$.

(d) Let $\gamma \in K$, and write $\gamma = \sum a_i \alpha_i$ where $a_i \in \mathbb{Q}$ and $\{\alpha_i\}$ is the basis of K over $\mathbb{Q}$ found in part (a). Use part (c) to give an explicit criterion for γ to be a primitive element for the field extension $\mathbb{Q} \subset K$ (i.e., $K = \mathbb{Q}(\gamma)$) in terms of the coefficients a_i.

(10) Let $f \in \mathbb{Q}[x]$ be an irreducible cubic polynomial. Suppose f has exactly one real root. Let K be the splitting field of f over $\mathbb{Q}$. Prove that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_3.

(11) Let $F \subset K$ be a Galois extension with Galois group G. Determine the number of intermediate fields L such that $[L : F] = 2$ when G is isomorphic to (a) D_4 (the dihedral group of order 8) (b) A_4.

(12) Let $F \subset K$ be a Galois extension with Galois group G isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$. Determine the number of intermediate fields L such that (a) $[L : F] = 4$, (b) $[L : F] = 9$, (c) $\mathrm{Gal}(K/L) \simeq \mathbb{Z}/4\mathbb{Z}$.

(13) Let $F \subset K$ be a Galois extension with Galois group isomorphic to S_6.

(a) Determine the number of intermediate fields L such that $[K : L] = 9$.

(b) Let M be the intersection of the fields L enumerated in part (a). Compute $[M : F]$.

(14) Let F be a field and $f = x^4 + bx^2 + c \in F[x]$. Suppose f is separable, i.e., has distinct roots in the algebraic closure of F. Let K be the

splitting field of f over F. Show that the Galois group $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of D_4, the dihedral group of order 8.