Math 612 Homework 3

Paul Hacking

March 5, 2014

Reading: Dummit and Foote, 14.4, 14.5, 14.6, 14.7.
Justify your answers carefully.

(1) For each of the following polynomials $f \in \mathbb{Q}[x]$, determine the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of the splitting field K of f over $\mathbb{Q}$.

(a) $x^3 - 5x - 1$.

(b) $x^4 - 10x^2 + 20$.

(c) $x^4 - 8x^2 + 9$.

(2) Let $f = x^5 - 7 \in \mathbb{Q}[x]$. Let K be the splitting field of f over $\mathbb{Q}$.

(a) Show that $[K : \mathbb{Q}] = 20$.

(b) Using part (a), deduce that for each $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ and $b \in \mathbb{Z}/5\mathbb{Z}$ there is an automorphism $\varphi_{a,b}$ of K over $\mathbb{Q}$ such that $\varphi_{a,b}(\zeta) = \zeta^a$ and $\varphi_{a,b}(\sqrt[5]{7}) = \zeta^b \sqrt[5]{7}$.

(c) Let $\mathrm{Aff}(\mathbb{Z}/5\mathbb{Z})$ denote the group of affine linear invertible maps f from $\mathbb{Z}/5\mathbb{Z}$ to itself. That is, $\mathrm{Aff}(\mathbb{Z}/5\mathbb{Z})$ is the set of maps $f\colon \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ such that $f(x) = ax + b$ for some $a \in (\mathbb{Z}/5\mathbb{Z})^\times$ and $b \in \mathbb{Z}/5\mathbb{Z}$, with the group operation being composition of maps. Show that the map

$$\mathrm{Aff}(\mathbb{Z}/5\mathbb{Z}) \to \mathrm{Gal}(K/\mathbb{Q}), \quad (f(x) = ax + b) \mapsto \varphi_{a,b}$$

is an isomorphism of groups.

(3) Let $\zeta = e^{2\pi i/13}$ and $K = \mathbb{Q}(\zeta)$. Then $\mathbb{Q} \subset K$ is a Galois extension with Galois group

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/13\mathbb{Z})^\times \simeq \mathbb{Z}/12\mathbb{Z}.$$

Let $\mathbb{Q} \subset L \subset K$ be the intermediate field such that $[L : \mathbb{Q}] = 2$. Show that $L = \mathbb{Q}(\sqrt{13})$.

(4) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

(a) Compute the Galois group $\mathrm{Gal}(K/\mathbb{Q})$.

(b) Determine the number of intermediate fields $\mathbb{Q} \subset L \subset K$ such that (i) $[K : L] = 2$, (ii) $[L : \mathbb{Q}] = 2$. Describe the fields L explicitly in case (ii).

(c) (Optional). Repeat for $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$, where $p_1, \ldots, p_n \in \mathbb{N}$ are distinct primes.

(5) Let $F \subset K$ and $K \subset L$ be Galois extensions. Is the extension $F \subset L$ Galois? (Give a proof or counterexample.)

(6) Let p be a prime.

(a) Let S_p be the symmetric group on p letters and $\sigma, \tau \in S_p$ be a p-cycle and a transposition. Prove that S_p is generated by σ and τ.

(b) Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p. Let K be the splitting field of f over $\mathbb{Q}$. Suppose that f has exactly $p - 2$ real roots. Show that $\mathrm{Gal}(K/\mathbb{Q}) = S_p$.

(c) Let $f = x^5 - 16x + 2$ and K be the splitting field of f over $\mathbb{Q}$. Show that $\mathrm{Gal}(K/\mathbb{Q}) = S_5$.

(7) Let $F \subset K$ be a Galois extension with group G. Let $H \subset G$ be a subgroup and $L = K^H$ the corresponding intermediate field. Show that the number of intermediate fields of the form $gL := \{g(\alpha) \mid \alpha \in L\}$ for some $g \in G$ is equal to $|G|/|N_G(H)|$, where

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}$$

is the normalizer of H in G.

(8) Let F be a field of characteristic p and $F \subset K$ a Galois extension with Galois group $G \simeq \mathbb{Z}/p\mathbb{Z}$. Let φ be a generator of G.

(a) Show that there exists $\alpha \in K$ such that $\varphi(\alpha) = \alpha + 1$.
[Hint: What are the eigenvalues of the F-linear map $\varphi : K \to K$? What is its Jordan normal form?]

(b) Deduce that $K = F(\alpha)$ and $\alpha^p - \alpha + a = 0$ for some $a \in F$.