612 Example Sheet 3

Paul Hacking

28 February 2011

Notation: For F a field and $f \in F[x]$ a separable polynomial, the *Galois group of f over F* is the Galois group $G = \mathrm{Aut}(K/F)$ of the splitting field K of f over F.

(1) Let K/F be a Galois extension with group $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Assume $\operatorname{char} F \neq 2$. Show that K/F is a biquadratic extension, that is, there exist $\alpha, \beta \in K$ such that $K = F(\alpha, \beta)$ and $\alpha^2, \beta^2 \in F$.

(2) Find the Galois groups of the following polynomials.

(a) $f(x) = x^3 - x - 1$ over $\mathbb{Q}$.

(b) $g(x) = x^3 + 2x + 1$ over $\mathbb{Q}(\sqrt{-59})$.

(c) $h(x) = x^3 + 3tx + t$ over $\mathbb{Q}(t)$ (the field of rational functions in the variable t).

(3) Let K/F be a Galois extension with group S_3. Show that K is the splitting field of an irreducible cubic over F.

(4) (a) Let F be a field, $\mathrm{char}(F) \neq 2$. Let $K = F(\alpha)$ where $\alpha^2 \in F$. Find all elements $\beta \in K$ such that $\beta^2 \in F$.

(b) Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[K : \mathbb{Q}]$. Show that $K/\mathbb{Q}$ is Galois and describe the Galois group. Find the intermediate fields $\mathbb{Q} \subset L \subset K$ such that $[L : \mathbb{Q}] = 2$.

(5) Find the Galois groups of the following polynomials over $\mathbb{Q}$.

(a) $f(x) = x^4 - 4x^2 - 1$.

(b) $g(x) = x^4 + 4x^2 + 2$.

(6) Let F be a field and $f(x) = x^4 + bx^2 + c \in F[x]$ a separable polynomial. Show that the Galois group G of f over F is a subgroup of the dihedral group D_4 of order 8.

(7) Let F be a field, $f \in F[x]$ a separable polynomial, K/F the splitting field of f over F, and $G = \mathrm{Aut}(K/F)$ the Galois group of f over F. Let $\alpha_1, \ldots, \alpha_n \in K$ be the roots of f.

(a) Show that the *discriminant*

$$D := \prod_{i \neq j} (\alpha_i - \alpha_j) = \left(\prod_{i<j} (\alpha_i - \alpha_j) \right)^2$$

lies in F. [Hint: $F = K^G$ and $G \subseteq S_n$.]

(b) Let $\delta := \prod_{i<j} (\alpha_i - \alpha_j)$. (So $D = \delta^2$.) Show that $G \subseteq A_n$ iff $\delta \in F$.

(8) Let k be a field. Let $K = k(u_1, \ldots, u_n)$ be the field of rational functions in n variables $u_1, \ldots, u_n$. For $i = 1, \ldots, n$, let s_i denote the *elementary symmetric function* of degree i in the u_i, that is,

$$s_i = \sum_{1 \leq j_1 < \cdots < j_i \leq n} u_{j_1} u_{j_2} \cdots u_{j_i}.$$

Let $F = k(s_1, \ldots, s_n)$. Show that K/F is Galois with group S_n. [Remark: In particular, $F = K^{S_n}$.]

(9) Let G be a finite group. Show that there exists a field F and a Galois extension K/F with Galois group G.

(10) (a) Let p be a prime. Let $\sigma \in S_p$ be a p-cycle and $\tau \in S_p$ be a transposition. Show that σ and τ generate S_p.

(b) Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of prime degree p. Suppose that f has exactly $(p-2)$ real roots. Show that the Galois group of f over $\mathbb{Q}$ is equal to S_p. [Hint: Use part (a).]

(11) Let p be an odd prime and let $\zeta = \exp(2\pi i/p) \in \mathbb{C}$, a primitive pth root of unity. In class we showed that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension with Galois group

$$G = \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Here the isomorphism

$$\theta \colon G \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$$

is given by $\sigma(\zeta) = \zeta^{\theta(\sigma)}$. Moreover, if $H \subset G$ is a subgroup then the fixed field $\mathbb{Q}(\zeta)^H$ equals $\mathbb{Q}(\alpha)$ where $\alpha := \sum_{h \in H} h(\zeta)$.

(a) Let $L = \mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\cos(2\pi/p))$. Show that $[L : \mathbb{Q}] = (p-1)/2$ and $L = \mathbb{Q}(\zeta) \cap \mathbb{R}$.

(b) Show that if p is a prime of the from $2^m + 1$ then necessarily m is a power of 2. (For example $p = 17 = 2^4 + 1$.) Show that in this case L can be obtained by repeated adjunction of square roots, that is, there is a tower

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots F_r = L$$

where for each $j = 1, \ldots, r$ we have $F_j = F_{j-1}(\alpha_j)$ for some α_j such that $\alpha_j^2 \in F_{j-1}$. [Remark: It follows that the regular p-gon can be constructed using only a straight-edge and compass.]

(12) Let p be a prime. Show that the Galois group of $x^p - 2$ over $\mathbb{Q}$ is a semidirect product $\mathbb{Z}/p\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z})^{\times}$.

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

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

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