Part II Galois theory (2014–2015) Example Sheet 4

c.birkar@dpmms.cam.ac.uk

(1) Let $h = f/g$ be a non-constant rational function in $K(t)$ where f, g are coprime polynomials. Show that the polynomial $f(z) - hg(z)$ is irreducible as an element of $K(h)[z]$. Hence deduce that $[K(t) : K(h)] = \max\{\deg(f), \deg(g)\}$. (Hint: Gauss's Lemma.)

If $\varphi \in \mathrm{Aut}_K(L)$ where $L = K(t)$, show that there exist a, b, c, $d \in K$ with $ad \neq bc$ such that $\varphi(t) = (at + b)/(ct + d)$, and conversely that such elements of K do determine elements of $\mathrm{Aut}_K(L)$.

(2) Suppose $K \subseteq L$ is a Galois extension with $G = \mathrm{Gal}(L/K)$ and let $\alpha \in L$. Show that $L = K(\alpha)$ if and only if the images of α under the elements of G are distinct.

(3) Suppose that $K \subseteq L$ is a Galois extension with Galois group $\mathrm{Gal}(L/K) = \{\varphi_1, \ldots, \varphi_n\}$. Show that $\{\beta_1, \ldots, \beta_n\}$ is a basis for L as a K-vector space if and only if $\det[\varphi_i(\beta_j)]_{1 \leq i,j \leq n}$ is not zero.

(4) Express $\sum_{i \neq j} t_i^3 t_j \in K(t_1, \ldots, t_n)$ as a polynomial in the elementary symmetric polynomials.

(5) Let $L = K(t)$. We define maps φ and ψ by $\varphi(h(t)) = h(1/t)$ and $\psi(h(t)) = h(1 - 1/t)$ for $h \in K(t)$. Show that $\varphi, \psi \in \mathrm{Aut}_K(L)$ and that they determine an action of S_3 on L. Show that the corresponding fixed field is just $K(g)$, where $g(t) = \frac{(t^2-t+1)^3}{t^2(t-1)^2}$.

(6) Let L be the 15-th cyclotomic extension of $\mathbb{Q}$. Find all the degree two extensions of $\mathbb{Q}$ contained in L.

(7) *Reduction mod p.* Let $f \in \mathbb{Z}[t]$ with no repeated roots and write $f = t^n - a_1 t^{n-1} + a_2 t^{n-2} - \cdots + (-1)^n a_n$. Let p be a prime number and assume $\bar{f}$, the image of f in $\mathbb{F}_p[t]$, also has no repeated roots. In several steps we show $\bar{G} = \mathrm{Gal}(\bar{E}/\mathbb{F}_p)$ embeds into $G = \mathrm{Gal}(E/\mathbb{Q})$ where $\bar{E}$ (resp. E) is the splitting field of $\bar{f}$ (resp. f) over $\mathbb{F}_p$ (resp. $\mathbb{Q}$).

Let $x_1, \ldots, x_n$ be variables and $e_1, \ldots, e_n$ the symmetric polynomials in the x_i. Let $A = \mathbb{Z}[e_1, \ldots, e_n]$, $B = \mathbb{Z}[x_1, \ldots, x_n]$, $L =$ fraction field of A, and $F =$ fraction field of B. For $\sigma \in S_n$ define $R_\sigma = t - x_{\sigma(1)}u_1 - \cdots - x_{\sigma(n)}u_n$ where the u_i are a new set of variables. Put $R = \prod_{\sigma \in S_n} R_\sigma$.

(i) Considering R as an element of $B[u_1, \ldots, u_n, t]$, show that its coefficients belong to $B \cap L$. For the ambitious: show that in fact these coefficients belong to A (we will use this fact in the steps below).

(ii) Let $\mathrm{Root}_f(E) = \{\alpha_1, \ldots, \alpha_n\}$ and define a ring homomorphism $\theta\colon B \to E$ by $\theta(x_i) = \alpha_i$. Show that θ restricts to a homomorphism $A \to \mathbb{Z}$ sending e_i to a_i. Denoting the induced homomorphism $B[u_1, \ldots, u_n, t] \to E[u_1, \ldots, u_n, t]$ again by θ, deduce that $\theta(R) \in \mathbb{Z}[u_1, \ldots, u_n, t]$.

(iii) Let P be an irreducible factor of $\theta(R)$ in $\mathbb{Q}[u_1, \ldots, u_n, t]$. Assume $\theta(R_\sigma)|P$ in $E[u_1, \ldots, u_n, t]$ for some σ. Show that $P = \theta(R_{G\sigma}) := \prod_{\tau \in G} \theta(R_{\tau\sigma})$ where we consider $G = \mathrm{Gal}(L/\mathbb{Q}) \leq S_n$. (So the irreducible factors of $\theta(R)$ correspond to the cosets of G in S_n.)

(iv) Reprove (ii) and (iii) by replacing f with $\bar{f}$, that is, by considering $\mathrm{Root}_{\bar{f}}(\bar{E})$ and defining a homomorphism $\bar{\theta}\colon B \to \bar{E}$ which restricts to a homomorphism $A \to \mathbb{F}_p$, and by considering the irreducible factors of $\bar{\theta}(R)$, etc. Finally deduce that $\bar{G}$ can be identified with a subgroup of G.

(8) Show that t^4+1 is reducible over every finite field $\mathbb{F}_q$. (Hint: use the previous problem and consider the Frobenius) Let p be an odd prime. By considering the splitting field of t^2+1 over $\mathbb{F}_p$, show that -1 is a quadratic residue mod p iff $p \equiv 1 \bmod 4$. If ζ a root of t^4+1, show that $(\zeta + \zeta^{-1})^2 = 2$. Hence show that 2 is a quadratic residue mod p iff $p \equiv \pm 1 \bmod 8$.

(9) Show that the minimal polynomial of $\sqrt{3}+\sqrt{5}$ over $\mathbb{Q}$ is reducible modulo p for all primes p.

(10) Let L be the splitting field of $t^3 - 3t + c$ over $\mathbb{Q}$. Find the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ when $c = 1$ and 3. What happens when $c = 2$?

(11) Consider the polynomial $f = t^3 + 3t^2 - 1$ over $\mathbb{Q}$. Show that there exist $a \in \mathbb{Q}$ and $\alpha \in \mathbb{Q}(\sqrt{a})$ such that f splits over $L = \mathbb{Q}(\sqrt{a})(\sqrt[3]{\alpha})$.

(12) Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a Galois extension of $\mathbb{Q}$ and find its Galois group. Optional: show that $\mathbb{Q}(\sqrt{(2+\sqrt{2+\sqrt{2}})})$ is a Galois extension of $\mathbb{Q}$, and find its Galois group.

(13) Show that $t^4 + t^2 + t + 1$ is irreducible over $\mathbb{Q}$, and find the Galois group of its splitting field over $\mathbb{Q}$.

(14) Let $f \in K[X]$ be an irreducible separable quartic and L its splitting field over K. Consider the Galois group $\mathrm{Gal}(L/K)$ as a subgroup $G \leq S_4$. Let $V = \{1, (12)(34), (13)(24), (14)(23)\}$. Show that $G \cap V$ is either V or a subgroup of index 2 in V. In both cases, determine the various possibilities for G.

(15) Let L be the splitting field of $t^5 - 2$ over $\mathbb{Q}$. Investigate the Galois group $\mathrm{Gal}(L/\mathbb{Q})$.

(16) Suppose p is an odd prime, $\mu = \exp(2\pi i/p)$, and let $L = \mathbb{Q}(\mu)$. If F denotes the corresponding cyclotomic polynomial Φ_p, show that $F'(\mu) = p\mu^{p-1}/(\mu - 1)$. Prove that the norm $\mathrm{N}_{L/\mathbb{Q}}(F'(\mu)) = p^{p-2}$.

(17) Optional: Let $p_1, p_2, \ldots, p_n$ denote the first n primes, and let $L = \mathbb{Q}(\sqrt{p}_1, \sqrt{p}_2, \ldots, \sqrt{p}_n)$. Show that this is a Galois extension of degree 2^n with Galois group isomorphic to $(\mathbb{Z}/\langle 2 \rangle)^n$.