

Prof. Valentin Blomer

University of Toronto
Department of Mathematics

Algebra

Problem Set 19 (due Mar 27, 2007)

19.1. (80%) Variations on a theme:

a) Let G be any finite group of order n . Show that there exists a Galois extension L/K with Galois group G . *Hint:* Let k be any field, and $L = k(x_1, \dots, x_n)$. Regard G as a subgroup of S_n and S_n as a subgroup of $\text{Aut } L$. Now choose K suitably.

b) Let k be any field. Let $L := k(x_1, \dots, x_n)$ and let $K \subseteq L$ be the subfield of all rational functions that are symmetric in x_1, \dots, x_n . For $0 \leq j \leq n$ let the *elementary-symmetric polynomial* $s_j^{(n)} \in k[x_1, \dots, x_n]$ be defined by

$$p(T) := \prod_{i=1}^n (T - x_i) =: \sum_{j=0}^n (-1)^j s_j^{(n)} T^{n-j} \in (k[x_1, \dots, x_n])[T].$$

Show that L/K is Galois with $\text{Gal}(L/K) = S_n$ and $K = k(s_1^{(n)}, \dots, s_n^{(n)})$. In other words, every symmetric rational function is a rational function in the elementary-symmetric polynomials, and L is the splitting field of p over $k(s_1^{(n)}, \dots, s_n^{(n)})$. Also show that the transcendence degree of $k(s_1^{(n)}, \dots, s_n^{(n)})$ over k is n ; in other words, $s_1^{(n)}, \dots, s_n^{(n)}$ are algebraically independent over k .

c) Let a_1, \dots, a_n be algebraically independent over k , and let

$$f(T) := a_n + a_{n-1}T + \dots + a_1T^{n-1} + T^n \in k(a_1, \dots, a_n)[T]$$

be the general polynomial of degree n . Show that its Galois group is S_n .

d) Let $f = \sum a_j x^j \in k[x]$ be any monic polynomial of degree $n \geq 1$. Its discriminant Δ_f is a symmetric polynomial in its roots x_1, \dots, x_n , hence by part (b) it can be written in terms of the coefficients $a_{n-j} = (-1)^j s_j^{(n)}$. Give an explicit formula for $n = 2$ and $n = 3$.

19.2. (40%) Sei L/K a finite Galois extension with cyclic Galois group $\text{Gal}(L/K) = \mathbb{Z}/n\mathbb{Z}$. Assume that $\text{char} K = 0$ or $\text{char} K \nmid n$, and assume that K contains all n -th roots of unity. Show that L is the splitting field of an irreducible polynomial $x^n - a \in K[x]$ for some $a \in K$.

Hint: Let ζ be a primitive n -th root of unity, and σ a generator of $\text{Gal}(L/K)$. Consider the map $\Psi := \text{id} + \zeta\sigma + \dots + \zeta^{n-1}\sigma^{n-1}$. Choose $a = \Psi(c)^n$ for some $c \in L$ with $\Psi(c) \neq 0$ (why is this possible?).