Section V.2.Appendix.

Symmetric Rational Functions

Note. Inspired by the symmetric way in which the coefficients of a polynomial are related to the zeros of that polynomial, we define symmetric rational functions and elementary symmetric functions. Some of the results of this appendix are used in the appendix to Section V.9 in which Abel's Theorem on the unsolvability of the quintic is proved.

Note. Let K be a field and let $f(x) \in K[x]$ be a polynomial of degree n with roots $-r_1, -r_2, \ldots, -r_n$ in some extension field F. Then by the Factor Theorem (Theorem III.6.6), we have that $f(x) = a\prod_{i=1}^n (x + r_i)$ for some $a \in F$. We suppose $a = 1$ and then $f(x) = \prod_{i=1}^n (x + r_i)$. Multiplying this out to get the coefficients of the powers of x we have:

$$f(x) = x^n + \underbrace{(r_1 + r_2 + \cdots + r_n)}_{\text{all roots}} x^{n-1}$$

$$+ \underbrace{(r_1r_2 + r_1r_3 + \cdots + r_{n-1}r_n)}_{\text{all products of pairs of roots}} x^{n-2}$$

$$+ \underbrace{(r_1r_2r_3 + r_1r_2r_4 + \cdots + r_{n-2}r_{n-1}r_n)}_{\text{all products of triples of roots}} x^{n-3}$$

$$+ \cdots + \underbrace{(r_1r_2 \ldots r_k + \cdots + r_{n-k+1}r_{n-k+2} \cdots r_n)}_{\text{all products of } k\text{-tuples of roots}} x^{n-k}$$

$$+\cdots+\underbrace{(r_1r_2\cdots r_{n-1}+r_1r_2\cdots r_{n-2}r_n+\cdots+r_2r_3\cdots r_n)}_{\text{all products of } (n-1)\text{-tuples of roots}}\,x$$

$$+\qquad \underbrace{(r_1r_2\cdots r_n)}_{\text{product of all } n \text{ roots}}$$

Notice that if we permute the roots (for example, if we interchange r_1 and r_2) then the coefficients remain unchanged. Since the permutations of the roots fixes the coefficients, the coefficients are said to be *symmetric* expressions of the roots. **This is where permutation groups enter the scene of algebraic solutions of polynomial equations!!!**

Note. In this appendix, we let K be a field, $K[x_1, x_2, \ldots, x_n]$ be the ring of polynomials (an integral domain since K is a field) in n indeterminates, and $K(x_1, x_2, \ldots, x_n)$ the field of quotients of $K[x_1, x_2, \ldots, x_n]$ (the elements of this field are rational functions). By interpreting a polynomial as a rational function with denominator 1_K, we have $K[x_1, x_2, \ldots, x_n] \subset K(x_1, x_2, \ldots, x_n)$. Recall that we denote the symmetric group on n letters as S_n.

Definition. A rational function $\varphi \in K(x_1, x_2, \ldots, x_n)$ is *symmetric* in $x_1, x_2, \ldots, x_n$ over K if for every $\sigma \in S_n$,

$$\varphi(x_1, x_2, \ldots, x_n) = \varphi(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

The *elementary symmetric functions* in $x_1, x_2, \ldots, x_n$ over K are defined to be

$$\begin{aligned} f_1 &= \sum_{i=1}^{n} x_i \\ f_2 &= \sum_{1 \leq i < j \leq n} x_i x_j \\ f_3 &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k \\ &\vdots \\ f_k &= \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k} \\ &\vdots \\ f_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

Note. If $g(y) \in K[x_1, x_2, \ldots, x_n][y]$ is $g(y) = (y - x_1)(y - x_2)(y - x_3) \cdots (y - x_n)$, then the coefficients of g are

$$g(y) = y^n - f_1 y^{n-1} + f_2 y^{n-2} - \cdots + (-1)^{n-1} f_{n-1} y + (-1)^n f_n.$$

If we permute the x_i's then $g(y)$ remains unchanged showing that the f_k actually are symmetric functions.

Note. The only essential material from this appendix needed in Appendix V.9 is the definition of elementary symmetric functions, the next "Observation," and Theorem V.2.18.

Observation. If $\sigma \in S_n$ then the mapping $x_i \mapsto x_{\sigma(i)}$ induces a K-automorphism (that is, K is fixed by the automorphism elementwise) of the field $K(x_1, x_2, \ldots, x_n)$ (we denote both of these as σ, though the K-automorphism is in $\mathrm{Aut}_K(F(x_1, x_2, \ldots, x_n)))$. With the mapping σ (in S_n) $\mapsto \sigma$ (in $\mathrm{Aut}_K(K(x_1, x_2, \ldots, x_n))$ we have a one to one group homomorphism (a monomorphism) and whence S_n may be considered as a subgroup of the Galois group $\mathrm{Aut}_K(K(x_1, x_2, \ldots, x_n))$. Of course, the fixed field E os S_n in $K(x_1, x_2, \ldots, x_n)$ consists precisely of the symmetric functions. By Theorem V.2.15, Artin's Theorem, $K(x_1, x_2, \ldots, x_n)$ is a Galois extension of E (with $G = S_n$, $F = K(x_1, x_2, \ldots, x_n)$, and $K = E$). Since $G = S_n$ is finite, then by Artin's Theorem, G is the Galois group of $F = K(x_1, x_2, \ldots, x_n)$ over $K = E$ and (see the proof of Artin's Theorem)

$$|G| = |S_n| = n! = [F : K] = [K(x_1, x_2, \ldots, x_n) : E];$$

that is, the dimension of $K(x_1, x_2, \ldots, x_n)$ over E is $n!$.

Note. The following result shows that (informally put) every finite group is the Galois group of some field extension.

Proposition V.2.16. If G is a finite group, then there exists a Galois field extension with Galois group isomorphic to G.

Note. In the remainder of this appendix, K is an arbitrary field, E is the subfield of symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$, and $f_1, f_2, \ldots, f_n$ are the elementary symmetric function in $x_1, x_2, \ldots, x_n$ over$K$. We have the "tower" of fields:

$$K \subset K(f_1, f_2, \ldots, f_n) \subset E \subset K(x_1, x_2, \ldots, x_n).$$

Our first goal is to prove that $E = K(f_1, f_2, \ldots, f_n)$ (that is, every rational symmetric function is in fact a rational function of the elementary symmetric functions $f_1 m f_2, \ldots, f_n$ over K).

Lemma V.2.17. Let K be a field, $f_1, f_2, \ldots, f_n$ the elementary functions in $x_1, x_2, \ldots, x_n$ over K and k an integer with $1 \leq k \leq n-1$. If $h_1, h_2, \ldots, h_k \in K[x_1, x_2, \ldots, x_n]$ are the elementary symmetric functions in $x_1, x_2, \ldots, x_n$, then each h_j can be written as a polynomial over K in $f_1, f_2, \ldots, f_n$ and $x_{k+1}, x_{k+2}, \ldots, x_n$.

Theorem V.2.18. If K is a field, E the subfield of all symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$ and $f_1, f_2, \ldots, f_n$ the elementary symmetric functions in $x_1, x_2, \ldots, x_n$, then $E = K(f_1, f_2, \ldots, f_n)$.

Note. We now turn our attention from symmetric rational functions to symmetric polynomial functions and give a result analogous to Theorem V.2.18, but for polynomials.

Note. The following preliminary lemma requires two results from Chapter IV (namely, Theorem IV.2.5 concerning a spanning set and the proof of Theorem IV.2.16). Since we may have skipped this chapter, we omit the proof of this lemma.

Lemma V.2.19. Let K be a field and E the subfield of all symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$. Then the set $X = \{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid 0 \leq i_k < k \text{ for each } k\}$ is a basis of $K(x_1, x_2, \ldots, x_n)$ over E.

Proposition V.2.20. Let K be a field and let $f_1, f_2, \ldots, f_n$ be the elementary symmetric functions in $K(x_1, x_2, \ldots, x_n)$.

(i) Every polynomial in $K[x_1, x_2, \ldots, x_n]$ can be written uniquely as a linear combination of the $n!$ elements $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ (for eac k with $0 \leq i_k < k$) with coefficients in $K[f_1, f_2, \ldots, f_n]$;

(ii) every symmetric polynomial in $K[x_1, x_2, \ldots, x_n]$ lies in $K[f_1, f_2, \ldots, f_n]$.

Revised: 12/28/2015