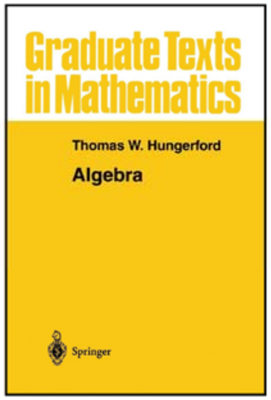
Modern Algebra

Chapter V. Fields and Galois Theory

V.2.Appendix. Symmetric Rational Functions—Proofs of Theorems



Proposition V.2.16

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

Proof. By Cayley's Theorem (Theorem II.4.6), with $|G| = n$, G is isomorphic to a subgroup of S_n. Let K be any field and E the subfield of symmetric rational functions in $K(x_1, x_2, \ldots, x_n)$. As discussed above, $K(x_1, x_2, \ldots, x_n)$ is a Galois extension of E with Galois group S_n. Here we have the fields and groups:

Fields	**Groups**
$K(x_1, x_2, \ldots, x_n)$	$\mathrm{Aut}_K(K(x_1, x_2, \ldots, x_n))$
$\cup$	$\cap$
E_1	G
$\cup$	$\cap$
E	S_n

Proposition V.2.16 (continued)

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

Proof (continued). Let E_1 (or G') be the fixed field of G. Since E_1 is an intermediate field, then by the Fundamental Theorem (Theorem V.2.5) part (ii), $K(x_1, x_2, \ldots, x_n)$ is Galois over E_1. We also know that, by the proof of the Fundamental Theorem (actually, by Theorem V.2.7), the one to one correspondence is between intermediate field E_1 and group $E_1' = \mathrm{Aut}_{E_1}(K(x_1, x_2, \ldots, x_n)) = G$ (the F of the Fundamental Theorem corresponds to our $K(x_1, x_2, \ldots, x_n)$ here). So G is the Galois group of the Galois extension of $K(x_1, x_2, \ldots, x_n)$ over E_1. □

Lemma V.2.17

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 $1 \le k \le n-1$. 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 $x_{k+1}, x_{k+2}, \ldots, x_n$.

Proof. The result is true when $k = n-1$ since in that case $h_1 = x_1 + x_2 + \cdots + x_{n-1} = (x_1 + x_2 + \cdots + x_{n-1} + x_n) - x_n = f_1 - x_n$ and for $2 \le j \le n$

$$h_j = \sum_{1 \le i_1 < i_2 < \cdots < i_j \le n-1} x_{i_1} x_{i_2} \cdots x_{i_j} (\text{all } j\text{-tuple products of } x_1, x_2, \ldots, x_{n-1})$$

$$= \sum_{1 \le i_1 < i_2 < \cdots < i_j \le n} x_{i_1} x_{i_2} \cdots x_{i_j} - x_n \left(\sum_{1 \le i_1 < i_2 < \cdots < i_{j-1} \le n-1} x_{i_1} x_{i_2} \cdots x_{i_{j-1}} \right).$$

Lemma V.2.17 (continued 1)

Proof (continued). The result is true when $k = n-1$ since in that case $h_1 = x_1 + x_2 + \cdots + x_{n-1} = (x_1 + x_2 + \cdots + x_{n-1} + x_n) - x_n = f_1 - x_n$ and for $2 \le j \le n$

$$\begin{aligned} h_j &= \sum_{1\le i_1<i_2<\cdots<i_j\le n} x_{i_1}x_{i_2}\cdots x_{i_j} - x_n \left(\sum_{1\le i_1<i_2<\cdots<i_{j-1}\le n-1} x_{i_1}x_{i_2}\cdots x_{i_{j-1}} \right) \\ &\quad \text{(all } j\text{-tuple products of } x_1, x_2, \ldots, x_{n-1}, x_n \text{ MINUS} \\ &\quad \text{all } j\text{-tuple products where one of the elements is } x_n \\ &\quad \text{and the other } j-1 \text{ are from } x_1, x_2, \ldots, x_{n-1}) \\ &= f_1 - x_n h_{j-1}. \end{aligned}$$

We now proceed by induction on k in reverse order. The base case is to assume the result is true for $k = r+1 \le n-1$; we then show the result holds for $k = r$. Assume the base case and let $g_1, g_2, \ldots, g_{r+1}$ be the elementary symmetric functions in $x_1, x_2, \ldots, x_{r+1}$ and $h_1, h_2, \ldots, h_r$ the elementary symmetric functions in $x_1, x_2, \ldots, x_r$.

Lemma V.2.17 (continued 2)

Proof (continued). We have $h_1 = x_1 + x_2 + \cdots + x_r = (x_1 + x_2 + \cdots + x_{r+1}) - x_{r+1} = g_1 - x_{r+1}$. For $2 \le j \le r$

$$\begin{aligned} h_j &= \sum_{1\le i_1<i_2<\cdots<i_j\le r} x_{i_1}x_{i_2}\cdots x_{i_j} \text{(all } j\text{-tuples of } x_1, x_2, \ldots, x_r) \\ &= \sum_{1\le i_1<i_2<\cdots<i_j\le r+1} x_{i_1}x_{i_2}\cdots x_{i_j} - x_{r+1} \left(\sum_{1\le i_1<i_2<\cdots<i_{j-1}\le r} x_{i_1}x_{i_2}\cdots x_{i_j} \right) \\ &\quad \text{(all } j\text{-tuples of } x_1, x_2, \ldots, x_{r+1} \text{ MINUS all } j\text{-tuples with} \\ &\quad \text{one element of } x_{r+1} \text{ and } j-1 \text{ elements from } x_1, x_2, \ldots, x_r) \\ &= g_j - x_{r+1} h_{j-1}. \end{aligned}$$

So the result holds for $k = r$. Therefore, it holds for all k with $1 \le k \le n-1$. □

Theorem V.2.18

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 $E = K(f_1, f_2, \ldots, f_n)$.

Proof. We have $[K(x_1, x_2, \ldots, x_n) : E] = n!$ since, as observed above, $\mathrm{Aut}_E K(x_1, x_2, \ldots, x_n) = S_n$. Since $f_1, f_2, \ldots, f_n$ involve *some* combinations of $x_1, x_2, \ldots, x_n$ and $K(f_1, f_2, \ldots, f_n)$ contains *some* of the symmetric rational functions, so $K(f_1, f_2, \ldots, f_n) \subset E \subset K(x_1, x_2, \ldots, x_n)$. By Theorem V.1.2, we have $[K(x_1, x_2, \ldots, x_n) : K(f_1, f_2, \ldots, f_n)] = [K(x_1, x_2, \ldots, x_n) : E][E : K(f_1, f_2, \ldots, f_n)]$ so to show that $[E : K(f_1, f_2, \ldots, f_n)] = 1$ (and hence $E = K(f_1, f_2, \ldots, f_n)$), if suffices to show that $[K(x_1, x_2, \ldots, x_n) : K(f_1, f_2, \ldots, f_n)] \le n!$ (which in turn implies that the value must equal $n!$).

Theorem V.2.18 (continued 1)

Proof. Let $F = K(f_1, f_2, \ldots, f_n)$ and consider the tower of fields: $F \subset F(x_n) \subset F(x_{n-1}, x_n) \subset \cdots \subset F(x_2, x_3, \ldots, x_n) \subset F(x_1, x_2, \ldots, x_n) = K(f_1, f_2, \ldots, f_n)(x_1, x_2, \ldots, x_n)$. Now $K \subset K(f_1, f_2, \ldots, f_n)$, so $K(x_1, x_2, \ldots, x_n) \subset K(f_1, f_2, \ldots, f_n)(x_1, x_2, \ldots, x_n)$. Also, each $f_1, f_2, \ldots, f_n \in K(x_1, x_2, \ldots, x_n)$, so $K(f_1, f_2, \ldots, f_n) \subset K(x_1, x_2, \ldots, x_n)$ and $K(f_1, f_2, \ldots, f_n)(x_1, x_2, \ldots, x_n) \subset K(x_1, x_2, \ldots, x_n)$ and $F(x_1, x_2, \ldots, x_n) = K(f_1, f_2, \ldots, f_n)(x_1, x_2, \ldots, x_n) = K(x_1, x_2, \ldots, x_n)$. Since $F(x_k, x_{k+1}, \ldots, x_n) = F(x_{k+1}, x_{k+2}, \ldots, x_n)(x_k)$, by Theorem V.1.2 and Theorem V.1.6(iii) it suffices to show that x_n is algebraic over F of degree $\le n$ and for each $k < n$, x_k is algebraic of degree $\le k$ over $F(x_{k+1}, x_{k+2}, \ldots, x_n)$ (then the factorial result will follows). To do this, let $g_n(y) \in F[y]$ be the polynomial $g_n(y) = (y - x_1)(y - x_2)\cdots(y - x_n) = y^n - f_1 y^{n-1} + \cdots + (-1)^n f_n$. Since $g_n \in F[y]$ has degree n and x_n is a root of g_n, then x_n is algebraic of degree at most n over $F = K(f_1, f_2, \ldots, f_n)$ by Theorem V.1.6(ii).

Theorem V.2.18 (continued 2)

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 $E = K(f_1, f_2, \ldots, f_n)$.

Proof. Now for each k with $1 \le k < n$ define a monic polynomial: $g_k(y) = g_n(y)/\{(y - x_{k+1})(y - x_{k+2}) \cdots (y - x_n)\} = (y - x_1)(y - x_2) \cdots (y - x_k)$. Then each $g_k(y)$ has degree k, x_k is a root of $g_k(y)$ and the coefficients of $g_k(y)$ are precisely the elementary symmetric functions in $x_1, x_2, \ldots, x_k$. By Lemma V.2.17, each $g_k(y)$ lies in $F(x_{k+1}, x_{k+2}, \ldots, x_n)[y]$, whence x_k is algebraic of degree at most k over $F(x_{k+1}, x_{k+2}, \ldots, x_n)$. This establishes the "$\le n!$" claim and hence the original claim. □

Proposition V.2.20

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 each k with $0 \le i_k < k$) 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 $K[f_1, f_2, \ldots, f_n]$.

Proof. (i) For each $k = 1, 2, \ldots, n$, let $g_k(y) = (y - x_1)(y - x_2) \cdots (y - x_k)$. As shown in the proof of Theorem V.2.18, the coefficients of $g_k(y)$ are polynomials over K is $f_1, f_2, \ldots, f_n$ and $x_{k+1}, x_{k+2}, \ldots, x_n$. Since g_k is monic of degree k and $g_k(x_k) = 0$ then x_k^k can be expressed as a polynomial over K in $f_1, f_2, \ldots, f_n, x_{k+1}, x_{k+2}, \ldots, x_n$ and the lower powers of x_k, x_k^i for $i \le k - 1$ (set $y = x_k$ and rearrange).

Proposition V.2.20(i)

Proof (continued). If we proceed step by step beginning with g_1 and solving for $x_1^1, \ldots, g_k$ and solving for $x_k^k, \ldots$, and solving for x_n^n, we can convert any polynomial $h \in K[x_1, x_2, \ldots, x_n]$ into a polynomial in $f_1, f_2, \ldots, f_n, x_1, x_2, \ldots, x_n$ in which the highest exponent of any x_k is $k - 1$ (powers of x_k can be reduced by multiples of k until the power is less than k). In other words, h is a linear combination of $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ (where for each k, $i_k < k$; so there are $n!$ such expressions) with coefficients in $K[f_1, f_2, \ldots, f_n]$. Furthermore, these coefficient polynomials are uniquely determined since $\{x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid 0 \le i_k < k \text{ for each } k\}$ is linearly independent over $E = K(f_1, f_2, \ldots, f_n)$ by Lemma V.2.19 (since the set is a basis for E). This proves (i).

Proposition V.2.20(ii)

Proof. (ii) So any polynomial $h \in K[x_1, x_2, \ldots, x_n]$ can be uniquely written as a linear combination of $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ (with $i_k < k$) with coefficients in $K(f_1, f_2, \ldots, f_n)$ and in fact this can be done, as shown above, with coefficients in $K[f_1, f_2, \ldots, f_n]$. So for h a symmetric polynomial we have $h \in E = K(f_1, f_2, \ldots, f_n)$ and the unique linear combination for h is $h = h1 = h x_1^0 x_2^0 \cdots x_n^0$, and the "coefficient" h must lie in $K[f_1, f_2, \ldots, f_n]$, as claimed in (ii). □