Summer 2015

Generic Polynomials

Lucas Spencer Mattick
San Jose State University

GENERIC POLYNOMIALS

A Thesis

Presented to

The Faculty of the Department of Mathematics & Statistics

San José State University

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

by

Lucas S. Mattick

August 2015

The Designated Thesis Committee Approves the Thesis Titled

GENERIC POLYNOMIALS

by

Lucas S. Mattick

APPROVED FOR THE DEPARTMENT OF MATHEMATICS & STATISTICS

SAN JOSÉ STATE UNIVERSITY

August 2015

Dr. Roger Alperin	Department of Mathematics & Statistics
Dr. Richard Kubelka	Department of Mathematics & Statistics
Dr. Marilyn Blockus	Department of Mathematics & Statistics

ABSTRACT

GENERIC POLYNOMIALS

by Lucas S. Mattick

In Galois theory one is interested in finding a polynomial over a field that has a given Galois group. A more desirable polynomial is one that parametrizes all such polynomials with that given group as its corresponding Galois group. These are called generic polynomials and we provide detailed proofs of two theorems that give methods for constructing such polynomials. Furthermore, we construct generic polynomials for S_n, C_3, V, C_4, C_6, D_3, D_4, and D_6.

DEDICATION

I dedicate this to my family who has supported me more than I could ever ask, especially my Grandfather, Ben Loya, and my Mother, Laura Mattick.

ACKNOWLEDGEMENTS

I would like to thank my advisor Dr. Roger Alperin for always challenging me and providing me with motivation. I would also like to thank my committee for reading my thesis and providing feedback.

TABLE OF CONTENTS

CHAPTER 1

PRELIMINARY MATERIAL

1.1 Introduction

To study generic polynomials it is necessary to understand the theory of invariant subfields under a given group action. Inherently this requires the theory of symmetric polynomials and something called the Reynolds Operator. This paper is designed to provide detailed proofs of some of the main theorems regarding generic polynomials. These theorems are constructive and are discussed in depth in Kemper [KM00], which is used as a guideline for some of the proofs provided. We use these tools to construct generic polynomials for small groups.

1.2 Field Theory

In Galois Theory, a field extension is said to be Galois if it is algebraic, normal, and separable. Equivalently, we say an extension L/K is Galois if $|\operatorname{Aut}(L/K)| = [L : K]$, where $\operatorname{Aut}(L/K)$ is the group of automorphisms of L that fix K. We start with a review of field theory and symmetric polynomials.

Definition 1.2.1. A field extension of a field K is a field L containing K as a subfield; this is denoted by L/K (read "L over K").

Definition 1.2.2. A field extension L/K is algebraic if every element in L is algebraic over K, i.e., every element in L is a root of some polynomial in $K[x]$.

Definition 1.2.3. An algebraic field extension is called normal if it is the splitting field of a family of polynomials, i.e., if every irreducible polynomial in $K[x]$ that has one root in L has all of its roots in L.

Definition 1.2.4. An algebraic field extension L/K is called separable if the minimal polynomial for any $\alpha \in L$ over K is a separable polynomial, i.e, this minimal polynomial splits into distinct linear factors in L.

Galois Theory covers field extensions and automorphisms of these extensions. As described above, a Galois extension is an algebraic extension that is normal and separable. For example, the extension $\mathbb{Q}[\sqrt{2}]$ is algebraic as $\sqrt{2}$ is a root of the polynomial $x^2 - 2 \in \mathbb{Q}[x]$. Moreover, since $\mathbb{Q}[\sqrt{2}]$ contains all the roots of $x^2 - 2$ and they are distinct, $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ is normal and separable and thus a Galois extension. However this is assuming that $\mathbb{Q}[\sqrt{2}]$ is a field, which brings us to

Theorem 1.2.5. *Let L be an extension field of K. If $u \in L$ is algebraic over K then $K(u) = K[u]$.*

The proof of Theorem 1.2.5 is in [Hun12], pages 234-235.

Definition 1.2.6. Let K be a field and f a monic polynomial in $K[x]$. Then an extension field L/K is called a splitting field over K of f if

(i) $f(x) = (x - r_1)(x - r_2) \cdots (x - r_n)$ in $L[x]$ and

(ii) $L = K(r_1, \ldots, r_n)$.

Theorem 1.2.7 (Jacobson Theorem 4.3)**.** *Any monic polynomial of positive degree in $K[x]$ has a splitting field L/K.*

The proof of Theorem 1.2.7 is in [Jac09], page 225.

Theorem 1.2.8. *Let ϕ be an isomorphism of a field K onto a field K', $f \in K[x]$ be a monic of positive degree, f' the corresponding polynomial in $K'[x]$ (under the isomorphism which extends ϕ and maps $x \to x$), and let L and L' be splitting fields* *of f and f' over K and K' respectively. Then ϕ can be extended to an isomorphism of L onto L'. Moreover, the number of such extensions does not exceed $[L:K]$ and is precisely $[L:K]$ if f' has distinct roots in L'.*

The proof of Theorem 1.2.8 can be found in [Jac09], page 227.

1.3 Galois Theory

Let K be a field. An automorphism of K is a bijection $\phi : K \longrightarrow K$ such that $\phi(k_1 + k_2) = \phi(k_1) + \phi(k_2)$ and $\phi(k_1 k_2) = \phi(k_1)\phi(k_2)$ for all $k_1, k_2 \in K$. We denote the set of all automorphisms of K as $\mathrm{Aut}(K)$. The set $\mathrm{Aut}(K)$ forms a group under function composition. Given a field extension L/K, we denote $\mathrm{Aut}(L/K)$ as the subgroup of $\mathrm{Aut}(L)$ that fixes K. That is

$$\mathrm{Aut}(L/K) = \{\phi \in \mathrm{Aut}(L) | \phi(k) = k, \ \ \forall k \in K\}.$$

Moreover, if L/K is a Galois extension then $\mathrm{Aut}(L/K)$ is the corresponding Galois group denoted by $\mathrm{Gal}(L/K)$.

Definition 1.3.1. Let G be any group of automorphisms of a field L. Let

$$L^G = \{a \in L | \phi(a) = a, \ \phi \in G\}.$$

L^G is the set of elements of L which are not moved by any $\phi \in G$.

Using the properties of automorphisms one can show that L^G forms a subfield of L. Now let $G = \mathrm{Aut}(L/K)$. Take $\mathcal{K}$ to be the set of intermediate fields between L and K and take $\mathcal{H}$ to be the set of subgroups of G. The definitions of L^G and $\mathrm{Aut}(L/K)$ provide two maps,

$$H \mapsto L^H \qquad \text{for } H \in \mathcal{H}$$

$$F \mapsto \mathrm{Aut}(L/F) \qquad \text{for } F \in \mathcal{K}.$$

The basic properties of these maps are as follow:

(1) $H_1 \supset H_2 \Rightarrow L^{H_1} \subset L^{H_2}$

(2) $K_1 \supset K_2 \Rightarrow \mathrm{Aut}(L/K_1) \subset \mathrm{Aut}(L/K_2)$

(3) $L^{\mathrm{Aut}(L/K)} \supset K$

(4) $\mathrm{Aut}(L/L^G) \supset G$

In general $|\,\mathrm{Aut}(L/K)| \leq [L : K]$, and if equality holds then the extension is Galois and we denote the Galois group $\mathrm{Aut}(L/K)$ by $\mathrm{Gal}(L/K)$.

Given the field K and a polynomial $f \in K[x]$, f is said to be separable if it has no repeated roots in its splitting field. An extension field L/K is Galois if and only if it is the splitting field of a separable polynomial over K. Moreover, we refer to "the Galois group of a separable polynomial over K" as the Galois group of its splitting field over K.

Now we prove a corollary to Theorem 1.2.8.

Corollary 1.3.2. *If L/K is Galois, then the isomorphisms of L and L' given in Theorem 1.2.8 induce a group isomorphism of* $\mathrm{Gal}(L/K)$ *and* $\mathrm{Gal}(L'/K')$.

Proof. Let ϕ be any one of the isomorphisms mentioned in Theorem 1.2.8. If L/K is Galois then $f \in K[x]$ is separable, as must be $f' \in K'[x]$. Thus L'/K' is Galois and we may consider $\mathrm{Gal}(L'/K')$. We claim that the map given by $\Psi : \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L'/K')$ where $\sigma \mapsto \phi \circ \sigma \circ \phi^{-1}$ is an isomorphism. Let us first check that $\Psi(\sigma)$ is an element of $\mathrm{Gal}(L'/K')$. Let $\sigma \in \mathrm{Gal}(L/K)$ and consider $\phi \circ \sigma \circ \phi^{-1}$. Certainly $\phi \circ \sigma \circ \phi^{-1}$ is a map of L' into L'. Furthermore, ϕ, σ, and ϕ^{-1} are all bijective and operation preserving, thus $\phi \circ \sigma \circ \phi^{-1}$ is bijective and operation preserving as well. Hence $\phi \circ \sigma \circ \phi^{-1}$ is an automorphism of L'. Now let $k' \in K'$. As ϕ is an isomorphism of K and K', we have that $\phi^{-1}(k') \in K$. Then

$$(\phi \circ \sigma \circ \phi^{-1})(k') = \phi(\sigma(\phi^{-1}(k'))) = \phi(\phi^{-1}(k')) = k'$$

and $\phi \circ \sigma \circ \phi^{-1}$ fixes K'. Thus $\phi \circ \sigma \circ \phi^{-1} \in \mathrm{Gal}(L'/K')$.

Now we show that Ψ is a group isomorphism. Let $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$ and consider $\Psi(\sigma_1 \circ \sigma_2)$:

$$\begin{aligned}
\Psi(\sigma_1 \circ \sigma_2) &= \phi \circ (\sigma_1 \circ \sigma_2) \circ \phi^{-1} \\
&= (\phi \circ \sigma_1) \circ (\sigma_2 \circ \phi^{-1}) \\
&= (\phi \circ \sigma_1) \circ (\phi^{-1} \circ \phi) \circ (\sigma_2 \circ \phi^{-1}) \\
&= ((\phi \circ \sigma_1) \circ \phi^{-1}) \circ (\phi \circ (\sigma_2 \circ \phi^{-1})) \\
&= (\phi \circ \sigma_1 \circ \phi^{-1}) \circ (\phi \circ \sigma_2 \circ \phi^{-1}) \\
&= \Psi(\sigma_1) \circ \Psi(\sigma_2).
\end{aligned}$$

Hence Ψ is a group homomorphism. Consider $\mathrm{Ker}(\Psi)$. Let $\sigma \in \mathrm{Ker}(\Psi)$, then $\phi \circ \sigma \circ \phi^{-1}$ is the identity automorphism on L'. That is $(\phi \circ \sigma \circ \phi^{-1})(l') = l'$ for every $l' \in L'$. It follows that $\sigma(\phi^{-1}(l')) = \phi^{-1}(l')$ for every $l' \in L$. As ϕ^{-1} is a bijection between L and L' it follows that $\sigma(l) = l$ for every $l \in L$ and σ is the identity on L. Hence, $\mathrm{Ker}(\Psi)$ is trivial and Ψ is injective. As $\deg(f) = \deg(f')$ we have that $|\,\mathrm{Gal}(L/K)| = |\,\mathrm{Gal}(L'/K')|$ and Ψ is an isomorphism of $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L'/K')$. □

Theorem 1.3.3. *Let L be an extension field of a field K. Then the following conditions on L/K are equivalent:*

(1) L is a splitting field over K of a separable polynomial $f(x)$.

(2) $K = L^G$ for some finite group of automorphisms of L.

(3) L is finite dimensional, normal and separable over over K.

Moreover, if L and f are as in (1) and $G = \mathrm{Gal}(L/K)$ then $K = L^G$ and if G and K are as in (2), then $G = \mathrm{Gal}(L/K)$.

Theorem 1.3.4 (Fundamental Theorem of Galois Theory)**.** *Let L be an extension field of a field K satisfying any one (hence all) of the equivalent conditions of Theorem 1.3.3. Let G be the Galois group of L over K. Let $\mathcal{H}$ be the collection of subgroups of G, and $\mathcal{K}$, the set of intermediate fields between L and K (the subfields of L/K). The maps $H \mapsto L^H$, $F \mapsto \mathrm{Aut}(L/F)$, $H \in \mathcal{H}$, $F \in \mathcal{K}$, are inverses of each other and so bijections of $\mathcal{H}$ onto $\mathcal{K}$ and of $\mathcal{K}$ onto $\mathcal{H}$. Moreover, we have the following properties of the pairing:*

(1) $H_1 \supset H_2 \Leftrightarrow L^{H_1} \subset L^{H_2}$

(2) $|H| = [L : L^H]$, $[G : H] = [L^H : K]$

(3) H is normal in $G \Leftrightarrow L^H$ is normal over K. In this case

$$\mathrm{Gal}(L^H/K) \simeq G/H.$$

The proof of Theorems 1.3.4 and 1.3.3 can be found in [Jac09], pages 238-240.

Proposition 1.3.5. *If N/L is Galois with Galois group G, then $N(x_1, \ldots, x_n)/L(x_1, \ldots, x_n)$ is Galois with Galois group G where $x_1, \ldots, x_n$ are indeterminates.*

Proof. It is enough to show that $N(x_1)/L(x_1)$ is Galois with Galois group $\mathrm{Aut}(N(x_1)/L(x_1)) \cong G$.

We construct the homomorphism $\varphi : G \longrightarrow \mathrm{Aut}(N(x_1)/L(x_1))$ given by $\sigma \mapsto \sigma'$ where $\sigma'(n) = \sigma(n)$ for any $n \in N$ and $\sigma'(x_1) = x_1$. First we show that φ is a homomorphism. Consider $\varphi(\sigma_1\sigma_2) = (\sigma_1\sigma_2)'$ for some $\sigma_1, \sigma_2 \in G$. We have that

$$(\sigma_1\sigma_2)'|_N = \sigma_1\sigma_2 = \varphi(\sigma_1)|_N\varphi(\sigma_2)|_N$$

and

$$(\sigma_1\sigma_2)'(x_1) = x_1 = \sigma_2'(x_1) = \sigma_1'(\sigma_2'(x_1)) = (\sigma_1'\sigma_2')(x_1) = (\varphi(\sigma_1)\varphi(\sigma_2))(x_1).$$

Thus $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$ and φ is a homomorphism.

Suppose $\varphi(\sigma_1) = \varphi(\sigma_2)$. Then $\sigma_1' = \sigma_2'$ and $\sigma_1 = \sigma_1'|_N = \sigma_2'|_N = \sigma_2$. Thus φ is one to one. Let ρ be any automorphism in $\text{Aut}(N(x_1)/L(x_1))$. As ρ fixes $L(x_1)$, ρ must fix L and x_1. Thus $\rho|_N$ is an automorphism of N that fixes L. Hence $\rho|_N \in G$. It is readily seen that $\varphi(\rho|_N) = \rho$, and thus φ is onto. Therefore $\text{Aut}(N(x_1)/L(x_1)) \cong G$.

Now we show that the extension $N(x_1)/L(x_1)$ is Galois. Since N/L is a Galois extension, N is the splitting field over L of some separable polynomial $f \in L[x]$. The degree of this polynomial is some positive integer m. Take $u_1, \ldots, u_m \in N$ to be the roots of f. Then $N = L[u_1, \ldots, u_m]$. As $L \subset L(x_1)$ and $N \subset N(x_1)$, $f \in L(x_1)[x]$ and f splits in $N(x_1)$. However we need to show that the splitting field of f over $L(x_1)$ is in fact $N(x_1)$. That is, we need to show that $N(x_1)$ is the minimal field extension of $L(x_1)$ over which f splits. Indeed this splitting field is $L(x_1)[u_1, \ldots, u_n]$ and $L(x_1)[u_1, \ldots, u_n] \subset N(x_1)$. Now we show $N(x_1) \subset L(x_1)[u_1, \ldots, u_m]$. Let $g \in N(x_1)$, then $g = p/q$ for some $p, q \in N[x_1]$ with $q \neq 0$. Here the coefficients of p and q are in $N = L[u_1, \ldots, u_m]$. Thus $p/q = p'/q'$ where p' and q' are polynomials in $u_1, \ldots, u_m$ over $L[x_1]$. That is $p', q' \in L(x_1)[u_1, \ldots, u_m]$. Clearly $u_1, \ldots, u_m$ are algebraic over $L(x_1)$ and $L(x_1)[u_1, \ldots, u_m]$ is a field. Then $g = p'/q' \in L(x_1)[u_1, \ldots, u_m]$. Hence $N(x_1) \subset L(x_1)[u_1, \ldots, u_m]$ and $N(x_1) = L(x_1)[u_1, \ldots, u_m]$. Therefore $N(x_1)$ is the splitting field of f over $L(x_1)$ and $N(x_1)/L(x_1)$ is Galois with Galois group G. □

Applying this process again for the indeterminate x_2 we have that $N(x_1, x_2)/L(x_1, x_2)$ is Galois with Galois group G. We may apply this process a finite amount of times to conclude that $N(x_1, \ldots, x_n)/L(x_1, \ldots, x_n)$ is Galois with Galois group G.

Before we move on we need some results regarding bases for finite field extensions, which brings us to

Theorem 1.3.6. *Let E/F be finite dimensional and separable, with K/F its normal closure. Then the number of monomorphisms of E/F into K/F is $n = [E : F]$, and if these monomorphisms are $\eta_1 = 1, \eta_2, \ldots, \eta_n$, then a sequence of n elements $(u_1, \ldots, u_n)$, $u_i \in E$ is a basis for E/F if and only if*

$$\begin{vmatrix} u_1 & u_2 & \cdots & u_n \\ \eta_2(u_1) & \eta_2(u_2) & \cdots & \eta_2(u_n) \\ \vdots & \vdots & \ddots & \vdots \\ \eta_n(u_1) & \eta_n(u_2) & \cdots & \eta_n(u_n) \end{vmatrix} \neq 0.$$

The proof of Theorem 1.3.6 can be found in [Jac09], pages 292-293.

Corollary 1.3.7. *Suppose L/K is Galois for some fields L and K with Galois group $G = \{\sigma_1 = 1, \ldots, \sigma_n\}$. Then a sequence of n elements $(u_1, \ldots, u_n), u_i \in L$ is a base for L/K if and only if*

$$\begin{vmatrix} u_1 & u_2 & \cdots & u_n \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2(u_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \cdots & \sigma_n(u_n) \end{vmatrix} \neq 0.$$

Proof. L/K is finite dimensional, separable and normal by definition of a Galois extension. By Theorem 1.3.6 the number of monomorphisms (and hence automorphisms) of L/K into L/K is $n = [L : K]$. Moreover, we know these monomorphisms make up G. By Theorem 1.3.6, a sequence of n elements $(u_1, \ldots, u_n)$, $u_i \in L$ is a basis for L/K if and only if

$$\begin{vmatrix} u_1 & u_2 & \cdots & u_n \\ \sigma_2(u_1) & \sigma_2(u_2) & \cdots & \sigma_2(u_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & \cdots & \sigma_n(u_n) \end{vmatrix} \neq 0.$$

□

Definition 1.3.8. Let L/K be a finite Galois extension with basis B. Then B is a normal basis for L/K if there is a $z \in L$ such that $B = \{\sigma(z) | \sigma \in G\}$.

In fact, every finite Galois extension has a normal basis. This is given as the following theorem in [Jac09], pages 294-295.

Theorem 1.3.9. *Any (finite dimensional) Galois extension field L/K has a normal basis.*

This allows us to prove the following proposition, which will be useful in a later proof.

Proposition 1.3.10. *Suppose N/L is Galois with Galois group $G = \{\sigma_1 = 1, \ldots, \sigma_m\}$. We have some normal basis $B = \{\beta_1, \ldots, \beta_m\}$. Then $\overline{B} = \{\bar{\beta}_i := \sigma_i(\bar{\beta}_1) | 1 \leq i \leq m\}$ is a normal basis for $N(x_1, \ldots, x_m)/L(x_1, \ldots, x_m)$ where $\bar{\beta}_1 = x_1\beta_1 + \cdots + x_m\beta_m$ and $x_1, \ldots, x_m$ are indeterminates.*

Proof. By Proposition 1.3.5 $N(x_1, \ldots, x_m)/L(x_1, \ldots, x_m)$ is Galois with Galois group $\mathrm{Gal}(N(x_1, \ldots, x_m)/L(x_1, \ldots, x_m)) \cong G$. Thus $[N(x_1, \ldots, x_m) : L(x_1, \ldots, x_m)] = |G| = m$. By definition, the orbit of $\bar{\beta}_1$ forms $\overline{B}$ and $|\overline{B}| = m$, so we need only show that $\overline{B}$ is linearly independent.

Suppose we have some $f_1, \ldots, f_m \in L(x_1, \ldots, x_m)$ so that

$$f_1\bar{\beta_1} + \cdots + f_m\bar{\beta_m} = 0.$$

Then

$$\begin{aligned}
&[f_1\beta_1 + f_2\sigma_2(\beta_1) + \cdots + f_m\sigma_m(\beta_1)]x_1 \\
+&[f_1\beta_2 + f_2\sigma_2(\beta_2) + \cdots + f_m\sigma_m(\beta_2)]x_2 \\
&+ \\
&\vdots \\
&+ \\
+&[f_1\beta_m + f_2\sigma_2(\beta_m) + \cdots + f_m\sigma_m(\beta_m)]x_m = 0
\end{aligned}$$

and it follows that

$$A \cdot \mathbf{f} := \begin{bmatrix} \beta_1 & \sigma_2(\beta_1) & \ldots & \sigma_m(\beta_1) \\ \beta_2 & \sigma_2(\beta_2) & \ldots & \sigma_m(\beta_2) \\ \vdots & \vdots & \ddots & \vdots \\ \beta_m & \sigma_2(\beta_m) & \ldots & \sigma_m(\beta_m) \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

By Theorem 1.3.7 $\det(A^T) \neq 0$ so $\det(A) \neq 0$. Thus $\mathbf{f} = 0$. □

Definition 1.3.11. Suppose $G \neq 1$ is a permutation group on letters which can be divided into disjoint sets $S_1, \ldots, S_m$ such that every permutation of G either maps all letters of a set S_i onto themselves or onto the letters of another set S_j. Except for the trivial cases in which there is only one set or in which every set consists of a single letter, we say that G is imprimitive and we call $S_1, \ldots, S_m$ the sets of imprimitivity.

The proof of the following lemma is implicitly contained in [Hal76], pages 57-58, which was used as an outline for the proof provided below.

Lemma 1.3.12. *Suppose $G \leq S_n$ is a transitive permutation group on the set $Y = \{y_1, \ldots, y_n\}$ where $|G| = m$. Here G acts on $X = \{x_\sigma | \sigma \in G\}$ by $\sigma'(x_\sigma) = x_{\sigma'\sigma}$. Then we can divide up X into n sets of imprimitivity $X_1, \ldots, X_n$ such that the permutations of $X_1, \ldots, X_n$ under the action of G are the same as those in G.*

Proof. Take $H \leq G$ to be the stabilizer of y_1. Since G is transitive, for any $y_i \in Y$, there exists some $g_i \in G$ such that $g_i y_1 = y_i$. Then every element in the coset $g_i H$ sends y_1 to y_i. That is $g_i h y_1 = y_i$ for any $h \in H$. Moreover, the following n cosets of H are distinct

$$eH, g_2H, g_3H, \ldots, g_nH. \tag{1.1}$$

Suppose $g_iH = g_jH$. Then $g_j^{-1} g_j \in H$. It follows that $g_j^{-1} g_i y_1 = y_1$. Then $y_i = g_i y_1 = g_j y_1 = y_j$ and $i = j$ so $g_i = g_j$. Thus H has the n distinct cosets listed in 1.1. Let g be any element in G. Then $gy_1 = y_i$ for some $1 \leq i \leq n$ and $gy_1 = g_i y_1$. Then $g_i^{-1} g y_1 = y_1$. It follows that $g_i^{-1} g \in H$ and $gH = g_iH$. Therefore the n distinct cosets listed in 1.1 are all the distinct cosets of H and the index of H in G is n. Take $\mathscr{H}$ to be the set of distinct cosets of H in G.

For each $g \in G$ we have a permutation of the cosets of H given by $\pi : G \longrightarrow S_n$ where

$$\pi(g) = \begin{pmatrix} xH \\ gxH \end{pmatrix}, x \in G.$$

Here $\pi(g)$ maps each coset xH onto a distinct coset. Suppose $\pi(g)(g_1H) = \pi(g)(g_2H)$ for some fixed $g \in G$. Then $gg_1H = gg_2H$ and $(gg_2)^{-1} gg_1 \in H$. It follows that $g_2^{-1} g_1 \in H$ and $g_1H = g_2H$. Hence $\pi(g)$ is one to one and thus a bijection from $\mathscr{H}$ to $\mathscr{H}$. That is, $\pi(g)$ is in fact a permutation of the elements in $\mathscr{H}$.

Now we show that $\pi(G)$ is a transitive subgroup of S_n and is of the same permutations as G. Consider $\pi(g_1g_2)$ for any $g_1, g_2 \in G$,

$$\pi(g_1g_2)(xH) = g_1g_2xH = \pi(g_1)(g_2xH) = \pi(g_1)(\pi(g_2)(xH)) = (\pi(g_1)\pi(g_2))(xH)$$

for any cost xH. Hence $\pi : G \longrightarrow S_n$ is a homomorphism and $\pi(G) \leq S_n$. Let g_1H, g_2H be any cosets of H. Then $\pi(g_2g_1^{-1})(g_1H) = g_2g_1^{-1}g_1H = g_2H$ and $\pi(G)$ is transitive. Now suppose $\pi(g) = \iota$ were ι is the identity permutation. Then $\pi(g)(xH) = xH$ for any $x \in G$. Then $x^{-1}gx \in H$ for any $x \in G$. It follows that $x^{-1}gx(y_1) = y_1$ for any $x \in G$. Since G is transitive, for any $i = 1, \ldots, n$, we have some $x_i \in G$ so that $x_i(y_1) = y_i$. Then $x_i^{-1}gx_i(y_1) = y_1$ and

$$g(y_i) = gx_i(y_1) = x_i(y_1) = y_i$$

for $i = 1, \ldots, n$. It follows that $g(y_i) = y_i$ for $i = 1, \ldots, n$ and $g = e$. Thus π is a one to one homomorphism and $G \simeq \pi(G)$.

Lastly we show that the permutations of $\pi(G)$ coincide with G. Let g be any permutation in G. Then $g(y_i) = y_j$ for some $y_i, y_j \in Y$. We have that $g_j(y_1) = y_j$ and $g_i(y_1) = y_i$ so $g(g_i(y_1)) = g_j(y_1)$. It follows that $g_j^{-1}gg_i(y_1) = y_1$ and $g_j^{-1}gg_i \in H$. Therefore $\pi(g)(g_iH) = gg_iH = g_jH$. That is $\pi(g)$ is the permutation in $\pi(G)$ that takes x_iH to x_jH. Thus the permutations in $\pi(G)$ are the same as those in G.

This tells us how to partition X into the n desired sets of imprimitivity. Take $g_iH = \{g_{i1}, g_{i2}, \ldots, g_{il}\}$ where l is some positive integer so that $|H| = l$. Then $X_i = \{x_{g_{i1}}, x_{g_{i2}}, \ldots, x_{g_{il}}\}$ are the desired sets of imprimitivity (which we show). Let $g \in G$ and consider the action of g on the elements in the set X_i for some i. g sends y_i to y_j for some j. By what was shown $gg_iH = g_jH$. Then $gx_{g_{ik}} = x_{gg_{ik}}$ where gg_{ik} is some element in g_jH. Thus $x_{gg_{ik}}$ is some element in X_j. As x_{ik} was some arbitrary element in X_i, we have that g sends all the elements of X_i to all the elements of X_j. Therefore the permutations of $X_1, \ldots, X_n$ under G are the same as those in G. $\square$

Lastly we provide a theorem from Jacobson [Jac09], pages 259-260.

Theorem 1.3.13. *Let $f(x) \in F[x]$ have no multiple roots. Then $f(x)$ is irreducible in $F[x]$ if and only if the Galois group of $f(x)$ acts transitively on the roots of $f(x)$.*

1.4 The Jacobian & Transcendence Degree

A result regarding algebraic independence we will need later is contained in [For92], which is where the following proof is outlined from.

Theorem 1.4.1. *If K is a field of characteristic zero then $f_1, \dots, f_n \in K(x_1, \dots, x_n)$ are algebraically dependent only if the Jacobian matrix*

$$J(f) = \left(\frac{\partial f_i}{\partial x_j} \right)_{ij}$$

is (identically) singular, i.e. $\det(J(f)) \equiv 0$.

Proof. Suppose $f_1, \dots, f_n$ are algebraically dependent with dependency relation $P \in K[t_1, \dots, t_n]$. That is, $P(t_1, \dots, t_n) \not\equiv 0$ and $P(f_1, \dots, f_n) \equiv 0$. Then

$$\frac{\partial P(f_1, \dots, f_m)}{\partial x_i} = \frac{\partial P}{\partial t_1}\frac{\partial f_1}{\partial x_i} + \cdots + \frac{\partial P}{\partial t_n}\frac{\partial f_n}{\partial x_i} \equiv 0$$

for $i = 1, \dots, n$. It follows that $J(f)(\nabla P)^T \equiv 0$. As $P(t_1, \dots, t_n) \not\equiv 0$ we have that $(\nabla P)^T \not\equiv 0$. Thus $\det(J(f)) \equiv 0$. □

We will also need some definitions regarding transcendental extensions.

Definition 1.4.2. Let F be an extension field of K. If an element $u \in F$ is not a root of any nonzero $f \in K[x]$, u is said to be transcendental over K. F is called a transcendental extension if at least one element of F is transcendental over K.

Definition 1.4.3. Let F be an extension field of K. A transcendence base of F/K is a subset S of F which is algebraically independent over K and is maximal in the set of all algebraically independent subsets of F. The cardinality of S is called the transcendence degree of F/K, denoted $trd(F/K)$.

Theorem 1.4.4. *If F is an extension field of E and E an extension field of K, then*

$$trd(F/K) = trd(F/E) + trd(E/K).$$

The proof of Theorem 1.4.4 can be found in Hungerford [Hun12], page 316.

CHAPTER 2

SYMMETRIC FUNCTIONS

2.1 Symmetric Polynomials

To obtain the fundamental properties of symmetric polynomials, it is necessary to use the action of S_n on polynomial rings. To see this, let R be a ring and $x_1, \ldots, x_n$ indeterminates. S_n acts on $R[x_1, \ldots, x_n]$ by automorphisms that fix R and permute the indices of $x_1, \ldots x_n$. That is $\sigma(r) = r$ for any $r \in R$ and $\sigma(x_i) = x_{\sigma(i)}$ for $\sigma \in S_n$. A polynomial $f \in R[x_1, \ldots, x_n]$ is said to be symmetric if f is fixed under σ for every $\sigma \in S_n$. The set of symmetric polynomials is a subring Σ of $R[x_1, \ldots, x_n]$ containing R.

Take the ring $S = R[x_1, \ldots, x_n]$ and let $g(x) \in S[x]$ so that

$$g(x) = (x - x_1)(x - x_2) \cdots (x - x_n). \tag{2.1}$$

We show that the coefficients of $g(x)$ are symmetric polynomials by extending the action of $\sigma \in S_n$ to that of σ' on $S[x]$ by sending $x \longrightarrow x$. Since σ' permutes the $x_i's$ and fixes x we have that

$\sigma'(g(x)) = (x - x_{\sigma(1)})(x - x_{\sigma(2)}) \cdots (x - x_{\sigma(n)}) = (x - x_1)(x - x_2) \cdots (x - x_n) = g(x).$

Hence if we write

$$g(x) = x^n - p_1 x^{n-1} + \cdots + (-1)^n p_n \tag{2.2}$$

where $p_i \in R[x_1, \ldots, x_n]$, then $\sigma(p_i) = p_i$ for all $\sigma \in S_n$ and $i = 1, \ldots, n$. Thus $p_1, \ldots, p_n \in \Sigma$. Comparing (2.1) and (2.2) we get expressions for the p_i in the x_i, namely

$$p_1 = \sum_{1}^{n} x_i, \quad p_2 = \sum_{i<j} x_i x_j, \quad p_3 = \sum_{i<j<k} x_i x_j x_k, \ \ldots, \quad p_n = x_1 x_2 \ldots x_n. \tag{2.3}$$

Definition 2.1.1. The polynomials $p_1, \ldots, p_n$ in 2.3 are called the elementary symmetric polynomials in $x_1, \ldots, x_n$.

We now prove that $\Sigma = R[p_1, \ldots, p_n]$; that is, the elementary symmetric polynomials generate all symmetric polynomials over $R[x_1, \ldots, x_n]$, and that the $p_1, \ldots, p_n$ are algebraically independent over R.

The proofs of Propositions 2.1.2 and 2.1.3 are contained in [Jac09], pages 138-139, which was used as an outline for the proofs provided below.

Proposition 2.1.2. *The elementary symmetric polynomials generate* Σ*.*

We may view $R[x_1, \ldots, x_n]$ as a direct sum of abelian groups. More precisely let M_d be the span of all monomials of degree d in $x_1, \ldots, x_n$ then

$$R[x_1, \ldots, x_n] = \bigoplus_{d=1}^{\infty} M_d. \tag{2.4}$$

This representation of $R[x_1, \ldots, x_n]$ implies that for any $f \in R[x_1, \ldots, x_n]$ there is a unique sum so that

$$f = \sum_{d=0}^{n} f_d, \quad f_d \in M_d. \tag{2.5}$$

If f is symmetric then for any $\sigma \in S_n$, $\sigma(f) = f$. By the properties of homomorphisms we must have

$$\sigma(f) = \sum_{d=0}^{n} \sigma(f_d). \tag{2.6}$$

Since each f_d is unique if follows that $\sigma(f_d) = f_d$ for $0 \leq d \leq n$. Hence if f is symmetric, then so must be $f_0, \ldots, f_n$. Therefore it suffices to show proposition 2.1.2 for homogeneous symmetric polynomials.

Proof. Suppose f is a homogeneous symmetric polynomial of degree m in $R[x_1, \ldots, x_n]$. We introduce the lexicographic ordering in the set of monomials of degree m. We say that $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ is higher than $x_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ if $k_1 = l_1, k_2 = l_2, \ldots, k_s = l_s$ but $k_{s+1} > l_{s+1}$. Take $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ to be the highest monomial of degree m in f. Since f is symmetric it contains all the monomials obtained from $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ by permuting the x_i's. If we permute x_i with x_{i+1}, we know that $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ must be higher than $ax_1^{k_1}\cdots x_{i+1}^{k_i}x_i^{k_{i+1}}x_n^{k_n}$ by assumption. By the lexicographic ordering it follows that $k_i \geq k_{i+1}$. Since i was arbitrary we must have $k_1 \geq k_2 \geq \cdots \geq k_n$.

Consider now $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ where $p_1, \ldots, p_n$ are the elementary symmetric polynomials in $x_1, \ldots, x_n$. By expanding $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ we observe that the highest degree monomial is

$$x_1^{d_1+d_2+\cdots+d_n}x_2^{d_2+\cdots+d_n}\cdots x_n^{d_n}.$$

Hence the highest degree monomial in $ap_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_n^{k_n}$ coincides with the highest degree monomial in f. Furthermore, the highest degree monomial in $f_1 = f - ap_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_n^{k_n}$ is less than that of f. We repeat the process with f_1. Since there are a finite number of monomials of degree m, a finite number of applications of the process yields a representation of f as a polynomial in $p_1, \ldots, p_n$.

□

Proposition 2.1.3. *The elementary symmetric polynomials are algebraically independent.*

Proof. Suppose we have some algebraic expression of $p_1, \ldots, p_n$, where the coefficients are not all zero; that is, suppose

$$\sum a_{d_1d_2\cdots d_n}p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n} = 0 \tag{2.7}$$

where not all $a_{d_1d_2\cdots d_n} = 0$ and each set $\{d_1, d_2, \ldots, d_n\}$ is distinct. Consider $p_1^{d_1}p_2^{d_2}\cdots p_r^{d_n}$ expressed in terms of the x_i's for some set $\{d_1, \ldots, d_n\}$. The degree of one of its monomials $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ is $k_1+k_2+\cdots+k_n$. Expanding $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ in terms of the x_i's we observe that each term has the same degree, namely

$$m = d_1 + 2d_2 + \cdots + nd_n.$$

Now we introduce the same lexicographic ordering from earlier on the set of monomials of degree m. Take $k_i = d_i + d_{i+1} + \cdots + d_n$. Then $m = k_1 + k_2 + \cdots + k_n$. Moreover, the highest degree monomial in $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ must be $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ by the lexicographic ordering. By expanding $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ we observe that this term appears only once (suppressing lower degree terms),

$$\begin{aligned} p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n} &= (x_1+x_2+\cdots+x_n)^{d_1}(x_1x_2+x_1x_2+\cdots x_{n-1}x_n)^{d_2}\cdots(x_1x_2\cdots x_n)^{d_n} \\ &= (x_1^{d_1}+\cdots+x_n^{d_1})(x_1^{d_2}x_2^{d_2}+\cdots+x_{n-1}^{d_2}x_n^{d_2})\cdots(x_1^{d_n}\cdots x_n^{d_n}) \\ &= x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}+\cdots+x_1^{k_n}x_2^{k_{n-1}}\cdots x_n^{k_1}. \end{aligned}$$

Claim: The highest degree monomial in the x_i's is unique for each $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$. Consider $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ and $p_1^{d_1'}p_2^{d_2'}\cdots p_n^{d_n'}$. Then the highest degree monomials in the x_i's are $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ and $x_1^{k_1'}x_2^{k_2'}\cdots x_n^{k_n'}$ respectively. Suppose they are equal. Then $k_1 = k_1',\ k_2 = k_2',\ \ldots,\ k_n = k_n'$. It follows that $d_1 = d_1',\ d_2 = d_2',\ \ldots\ , d_n = d_n'$ and

$$p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n} = p_1^{d_1'}p_2^{d_2'}\cdots p_n^{d_n'}.$$

Thus the highest degree monomial in $x_1,\ldots,x_n$ in each $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ is unique. Since each highest degree monomial is unique we can compare them all in the lexicographic ordering and find the maximal highest degree monomial. Take the $p_1^{d_1}p_2^{d_2}\cdots p_n^{d_n}$ in the sum in 2.7 with the largest m so that $a_{d_1d_2\cdots d_n}\neq 0$ and so that its corresponding highest degree monomial $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ is maximal. Then expressing the sum in line 2.7 in $x_1,\ldots,x_n$ we get the monomial $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ only once with the nonzero coefficient $a_{d_1 d_2 \cdots d_n}$. This contradicts the algebraic independence of the $x_1, \ldots, x_n$. Hence the proposition is true. □

2.2 The Field of Symmetric Rational Expressions

Take a field F and consider the function field $F(x_1, \ldots, x_n)$ over n indeterminates. Recall that for any σ in S_n we have a unique automorphism σ of $F[x_1, \ldots, x_n]$ fixing the elements of F and sending $x_i \longrightarrow x_{\sigma(i)}$. This action of S_n can be extended uniquely to $F(x_1, \ldots, x_n)$ in one and only one way.

Definition 2.2.1. The elements of $F(x_1, \ldots, x_n)$ that are fixed under the action of S_n are called the symmetric rational expressions.

The proof of Proposition 2.2.2 is contained in [Jac09], pages 241-242, which was used as an outline for the proof provided below.

Proposition 2.2.2. *Let F be a field and $L = F(x_1, \ldots, x_n)$, the field F over n indeterminates. The symmetric rational expressions of L form a subfield L^{S_n} and are generated by the elementary symmetric polynomials in $x_1, \ldots, x_n$.*

Proof. Consider the polynomial ring $L[x]$ and the polynomial

$$g(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$$

which we can write as

$$g(x) = x^n - p_1 x^{n-1} + p_2 x^{n-2} - \cdots + (-1)^n p_n$$

where $p_1, \ldots, p_n$ are the elementary symmetric polynomials in $x_1, \ldots, x_n$. Consider some $\sigma \in S_n$. The automorphism σ can be extended to an automorphism σ' of $L[x]$ by fixing x. This maps $g(x)$ into $(x - x_{\sigma(1)})(x - x_{\sigma(2)}) \cdots (x - x_{\sigma(n)})$. Since σ is a permutation of the indices, this coincides with $g(x)$. Thus $\sigma'(g(x)) = g(x)$ for every $\sigma \in S_n$ and so $\sigma(p_i) = p_i$ for $i = 1, \ldots, n$ and for any $\sigma \in S_n$. Hence $p_1, \ldots, p_n \in L^{S_n}$, and the subfield over F they generate, $F(p_1, \ldots, p_n)$ is contained in L^{S_n}. Take $K = F(p_1, \ldots, p_n)$. It is clear from $L = F(x_1, \ldots, x_n) = F(p_1, \ldots, p_n, x_1, \ldots, x_n) = K(x_1, \ldots, x_n)$ that L is a splitting filed over $K = F(p_1, \ldots, p_n)$ of $g(x)$, and $g(x)$ has distinct roots. Hence L is Galois over K. Consider $\rho \in \mathrm{Gal}(L/K)$ and $g(x_i) = 0$ for some $1 \le i \le n$,

$$\rho(g(x_i)) = g(\rho(x_i)) = 0 \quad \text{because } \rho(p_i) = p_i.$$

Hence $\rho(x_i) = x_j$ for some $1 \le j \le n$. Since ρ is an automorphism, it follows that ρ must be some permutation of $x_1, \ldots, x_n$ and thus ρ coincides with some $\sigma \in S_n$. It follows that

$$\mathrm{Gal}(L/K) \subset S_n.$$

By definition, any $\sigma \in S_n$ fixes $p_1, \ldots, p_n$ and F. Thus $\sigma \in \mathrm{Aut}(F(x_1, \ldots, x_n)/F(p_1, \ldots, p_n)) = \mathrm{Gal}(L/K)$ and $S_n \subset \mathrm{Gal}(L/K)$. By inclusion

$$S_n = \mathrm{Gal}(L/K).$$

By the Fundamental Theorem of Galois Theory

$$L^{S_n} = L^{\mathrm{Gal}(L/K)} = K = F(p_1, \ldots, p_n).$$

□

2.3 The General Equation of the nth Degree

A general equation is one whose coefficients are distinct indeterminates. More precisely,

Definition 2.3.1. Let F be a field and let $t_1, \ldots, t_n$ be distinct indeterminates. Then the equation

$$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^n t_n = 0 \tag{2.8}$$

is called a general equation of the nth degree over F.

The proof of Theorem 2.3.2 is outlined from [Jac09], pages 262-264.

Theorem 2.3.2. *The general equation of the nth degree $f(x) = 0$ is irreducible in $K[x] = F(t_1, \ldots, t_n)[x]$ and has distinct roots. Let L be the splitting field of $f(x)$, then the Galois group of L/K is the symmetric group S_n.*

Proof. Take $K = F(t_1, \ldots, t_n)$ and let $f(x) \in K[x]$ so that

$$f(x) = x^n - t_1 x^{n-1} + t_2 x^{n-2} - \cdots + (-1)^n t_n. \tag{2.9}$$

Let L be the splitting field of f over K. Here $L = K(y_1, \ldots, y_n)$ where $y_1, \ldots, y_n$ are the roots of f in L. Hence f splits in L and $f(x) = (x - y_1)(x - y_2) \cdots (x - y_n)$ in $L[x]$. It follows that the coefficients of f are the elementary symmetric polynomials in the roots. That is

$$t_1 = \sum_1^n y_i, \quad t_2 = \sum_{i<j} y_i y_j, \quad t_3 = \sum_{i<j<k} y_i y_j y_k, \ \ldots, \quad t_n = y_1 y_2 \ldots y_n. \tag{2.10}$$

Furthermore, $L = K(y_1, \ldots, y_n) = F(t_1, \ldots, t_n, y_1, \ldots, y_n) = F(y_1, \ldots, y_n)$.

Now we obtain the Galois group of f by using the results obtained from Proposition 2.2.2. For Proposition 2.2.2 we introduced the field $F(x_1, \ldots, x_n)$, where $x_1, \ldots, x_n$ were n indeterminates. Then we constructed the polynomial $g(x) = (x - x_1)(x - x_2) \cdots (x - x_n) = x^n - p_1 x^{n-1} + p_2 x^{n-2} - \cdots + (-1)^n p_n$ and found that $F(x_1, \ldots, x_n)$ was a splitting field of g over $F(p_1, \ldots, p_n)$, where

$p_1, \ldots, p_n$ were the elementary symmetric polynomials in $x_1, \ldots, x_n$. Moreover, the Galois group of g was S_n.

We will carry over this result from the pair of fields $F(x_1, \ldots, x_n) \supset F(p_1, \ldots, p_n)$ to the pair we are interested in $F(y_1, \ldots, y_n) \supset F(t_1, \ldots, t_n)$. The difference here is that here we started with $F(t_1, \ldots, t_n)$ with $t_1, \ldots, t_n$ as distinct indeterminates, whereas in Proposition 2.2.2 we started with $F(x_1, \ldots, x_n)$, with $x_1, \ldots, x_n$ as indeterminates. To accomplish this we establish an isomorphism between $F(y_1, \ldots, y_n)$ and $F(x_1, \ldots, x_n)$.

Since $t_1, \ldots, t_n$ are indeterminates, we have a homomorphism $\sigma : F[t_1, \ldots, t_n] \longrightarrow F[p_1, \ldots, p_n]$, where σ is the identity on F and sends $t_i \longrightarrow p_i$ for $i = 1, \ldots, n$. Moreover, we have another homomorphism $\tau : F[x_1, \ldots, x_n] \longrightarrow F[y_1, \ldots, y_n]$ where τ is the identity on F and sends $x_i \longrightarrow y_i$ for $i = 1, \ldots, n$. Hence

$$\tau : F[x_1, \ldots, x_n] \longrightarrow F[y_1, \ldots, y_n], \qquad \sigma : F[t_1, \ldots, t_n] \longrightarrow F[p_1, \ldots, p_n]. \tag{2.11}$$

Now we form the composition $\tau\sigma$ and observe that

$$\tau\sigma(t_i) = \tau(p_i) = \tau\left(\sum_{j_1<j_2<\ldots<j_i} x_{j_1}x_{j_2}\cdots x_{j_i}\right) = \sum_{j_1<j_2<\ldots<j_i} y_{j_1}y_{j_2}\cdots y_{j_i} = t_i.$$

Here we show that the homomorphism σ is injective by showing that the kernel is trivial. Suppose $\sigma(h) = 0$ for some $h \in F[t_1, \ldots, t_n]$. Then $\tau\sigma(h) = 0$ as well. Moreover, $\tau\sigma(h) = h$. Hence $h = 0$ and 0 is the only element in the kernel of σ. It is clear that σ is surjective and it follows that σ is an isomorphism of $F[t_1, \ldots, t_n]$ and $F[p_1, \ldots, p_n]$. We saw earlier there is a unique extension of σ to an isomorphism of $K = F(t_1, \ldots, t_n)$ and $F(p_1, \ldots, p_n)$, we call this extension σ as well. Furthermore, we extend σ to σ' of $F(t_1, \ldots, t_n)[x]$ and $F(p_1, \ldots, p_n)[x]$ by fixing x. Here σ' maps the polynomial $f(x) = x^n - t_1x^{n-1} + t_2x^{n-2} - \cdots + (-1)^n t_n$ to the polynomial

$g(x) = x^n - p_1x^{n-1} + p_2x^{n-2} - \cdots + (-1)^n p_n$. Since $F(y_1, \ldots, y_n)$ is a splitting field over $F(t_1, \ldots, t_n)$ of f, and $F(x_1, \ldots, x_n)$ is a splitting field over $F(p_1, \ldots, p_n)$ of $g(x)$, σ can be extended to an isomorphism ρ of $F(y_1, \ldots, y_n)$ and $F(x_1, \ldots, x_n)$, by Theorem 1.2.8. Moreover, $\mathrm{Gal}(F(x_1, \ldots, x_n)/F(p_1, \ldots, p_n))$ is isomorphic to $\mathrm{Gal}(F(y_1, \ldots, y_n)/F(t_1, \ldots, t_n)) = \mathrm{Gal}(L/K) = S_n$, by Corollary 1.3.2. □

2.4 The Reynolds Operator

To construct generic polynomials, it will be useful to have the following tool.

Definition 2.4.1. Given a finite matrix group $G \subset GL(n, K)$, the Reynolds operator of G is the map $R_G : K[x_1, \ldots, x_n] \longrightarrow K[x_1, \ldots, x_n]$ defined by the formula

$$R_G(f(\mathbf{x})) = \frac{1}{|G|} \sum_{A \in G} f(A \cdot \mathbf{x})$$

for $f(\mathbf{x}) \in K[x_1, \ldots, x_n]$.

The Reynolds operator proves to be an efficient means of calculating invariant polynomial rings. This is discussed in depth in [CLO07], which is where the next Theorem is derived.

Theorem 2.4.2. *Given a finite matrix group $G \subset GL(n, K)$, we have*

$$K[x_1, \ldots, x_n]^G = K[R_G(x_1^{\beta_1} \cdots x_n^{\beta_n}) : \beta_1 + \cdots + \beta_n \leq |G|].$$

In particular, $K[x_1, \ldots, x_n]^G$ is generated by finitely many homogeneous invariants.

We now prove a proposition that lets us use the results of Theorem 2.4.2 on fields and invariant subfields. The proof of the following proposition was outlined from [DK02], pages 115-116.

Proposition 2.4.3. *Let $K(x_1, \ldots, x_n)$ be a function field in n indeterminates and let $G \subset GL_n(K)$ act on the indeterminates and hence on $K[x_1, \ldots, x_n]$. Then if $K[x_1, \ldots, x_n]^G = K[\varphi_1, \ldots, \varphi_m]$ it follows that $K(x_1, \ldots, x_n)^G = K(\varphi_1, \ldots, \varphi_m)$.*

Proof. Let $f \in K(\varphi_1, \ldots, \varphi_m)$. Then $f = p/q$ for some $p, q \in K[\varphi_1, \ldots, \varphi_m]$ where $q \neq 0$. Consider $\sigma(f)$ for any $\sigma \in G$,

$$\sigma(f) = \sigma(p/q) = \sigma(p)/\sigma(q) = p/q = f.$$

Thus $f \in K(x_1, \ldots, x_n)^G$ and $K(\varphi_1, \ldots, \varphi_m) \subset K(x_1, \ldots, x_n)^G$. It remains to show that $K(x_1, \ldots, x_n)^G \subset K(\varphi_1, \ldots, \varphi_m)$. Let $f \in K(x_1, \ldots, x_n)^G$. Then $f = p/q$ for some $p, q \in K[x_1, \ldots, x_m]$ with $q \neq 0$ and $\sigma(f) = f$ for any $\sigma \in G$. Consider now

$$f = p/q = \frac{p \prod_{\sigma \in G \setminus 1} \sigma(q)}{\prod_{\sigma \in G} \sigma(q)}.$$

Clearly $\prod_{\sigma \in G} \sigma(q)$ is invariant under G . As the entire expression must be invariant under G it follows that $p \prod_{\sigma \in G \setminus 1} \sigma(q)$ is invariant under G as well. Thus f can be expressed as a quotient of two polynomials that are G invariant and $f \in K(\varphi_1, \ldots, \varphi_m)$. Finally we get that $K(x_1, \ldots, x_n)^G \subset K(\varphi_1, \ldots, \varphi_m)$ and $K(x_1, \ldots, x_n)^G = K(\varphi_1, \ldots, \varphi_m)$. □

Now we show an example that demonstrates the Reynolds operator and Theorem 2.4.2. Consider the cyclic group of oder three and the representation given below.

$$G = \left\{ A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, A_3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\}.$$

with $G \subset GL(2, K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With Theorem 2.4.2, we can calculate the generators of the invariant subring given by $K[x,y]^G$. Consider the set of monomials of degree less than or equal to $|G| = 3$:

$$f_1(x,y) = x,\ f_2(x,y) = y,\ f_3(x,y) = x^2,\ f_4(x,y) = y^2,\ f_5(x,y) = xy,$$

$$f_6(x,y) = x^3,\ f_7(x,y) = y^3,\ f_8(x,y) = x^2y,\ f_9(x,y) = xy^2.$$

According to Theorem 2.4.2,

$$K[x,y]^G = K[R_G(f_i(x,y)) :\ i = 1,\ldots,9].$$

We use the notation $A \cdot (x,y)$ to represent the product of the matrix A and the vector (x,y) as shown below:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x,y) = (ax+by, cx+dy).$$

Below is an example of using Reynolds operator on the monomial $f_8(x,y) = x^2y$,

$$\begin{aligned} R_G(f_8(x,y)) &= \frac{1}{|G|}\sum_{A\in G} f_8(A\cdot(x,y)) \\ &= \frac{1}{3}(f_8(A_1\cdot(x,y)) + f_8(A_2\cdot(x,y)) + f_8(A_3\cdot(x,y))) \\ &= \frac{1}{3}(f_8(x,y) + f_8(-y,x-y) + f_8(y-x,-x)) \\ &= \frac{1}{3}(x^2y + (-y)^2(x-y) + (y-x)^2(-x)) \\ &= \frac{1}{3}(-x^3 - y^3 + 3x^2y). \end{aligned}$$

The remaining generators are as follows,

$$\begin{aligned} &R_G(f_1(x,y)) = 0 && R_G(f_6(x,y)) = x^2y - xy^2 \\ &R_G(f_2(x,y)) = 0 && R_G(f_7(x,y)) = xy^2 - x^2y \\ &R_G(f_3(x,y)) = \tfrac{2}{3}(x^2+y^2-xy) && R_G(f_8(x,y)) = \tfrac{1}{3}(-x^3-y^3+3x^2y) \\ &R_G(f_4(x,y)) = \tfrac{2}{3}(x^2+y^2-xy) && R_G(f_8(x,y)) = \tfrac{1}{3}(-x^3-y^3+3xy^2) \\ &R_G(f_5(x,y)) = \tfrac{1}{3}(x^2+y^2-xy). \end{aligned}$$

Now take

$$\varphi_1 = x^2 + y^2 - xy,\ \varphi_2 = x^2y - xy^2,\ \varphi_3 = x^3 + y^3 - 3x^2y.$$

It is readily seen that

$$K[x, y]^G = K[\varphi_1, \varphi_2, \varphi_3].$$

CHAPTER 3

GENERIC POLYNOMIALS

3.1 Generic Polynomials

In inverse Galois theory one is interested in obtaining a polynomial that has a given group as its Galois group. It is even more desirable to have a polynomial that parametrizes all polynomials with a given group, or at least all Galois field extensions having this group.

Definition 3.1.1. Let K be a field and G a finite group. A separable polynomial $g(t_1, \ldots, t_m, X) \in K(t_1, \ldots, t_m)[X]$ with coefficients in the rational function field $K(t_1, \ldots, t_m)$ is called generic for G over K if the following two properties hold:

(a) The Galois group of g (as a polynomial in X) is G.

(b) If L is an infinite field containing K and N/L is a Galois field extension with Galois group $H \leq G$, then there exists $\lambda_1, \ldots, \lambda_m \in L$ such that N is the splitting field of $g(\lambda_1, \ldots, \lambda_m, X)$ over L.

Before presenting the main theorems of this section we prove a lemma and a proposition. The proof of Lemma 3.1.2 is outlined from Kuyk [Kuy64], pages 34-35.

Lemma 3.1.2. *Let $G \leq S_n$ be a permutation group and N/L a Galois extension of infinite fields with Galois group G. Let $f \in N[x_1, \ldots, x_n]$ be a nonzero polynomial where $x_1, \ldots, x_n$ are indeterminates. Then there exists $\alpha_1, \ldots, \alpha_n \in N$ such that*

(i) $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ *for all* $\sigma \in G$ *where* $\sigma(\alpha_i)$ *denotes the Galois action, and*

(ii) $f(\alpha_1, \ldots, \alpha_n) \neq 0$.

Proof. As N/L is Galois, we have some normal basis $B = \{\beta_1, \ldots, \beta_m\}$ for N/L where $m = |G|$. Consider $N(x_1, \ldots, x_m)/L(x_1, \ldots, x_m)$, where $x_1, \ldots, x_m$ are indeterminates. By Proposition 1.3.5 $N(x_1, \ldots, x_m)/L(x_1, \ldots, x_m)$ is Galois with Galois group G. Moreover, by Proposition 1.3.10, $\overline{B}$ is a normal basis for $N(x_1, \ldots, x_m)/L(x_1, \ldots, x_m)$. Recall that

$$\overline{B} = \{\bar{\beta}_i = \sigma_i(\bar{\beta}_1) | \sigma_i \in G\}$$

and $\bar{\beta}_1 = \beta_1 x_1 + \cdots + \beta_m x_m$, with σ_1 being the identity. Note that G acts trivially on $x_1, \ldots, x_m$. Consider the action of G on $\overline{B}$. Let $\sigma \in G$ and $\bar{\beta}_i \in \overline{B}$. Then $\bar{\beta}_i = \sigma_i(\bar{\beta}_1)$ and $\sigma\sigma_i = \sigma_j$ for some σ_j, thus

$$\sigma(\bar{\beta}_i) = \sigma(\sigma_i(\bar{\beta}_1)) = \sigma\sigma_i(\bar{\beta}_1) = \sigma_j(\bar{\beta}_1) = \bar{\beta}_j.$$

Thus the action of G on $\overline{B}$ is the same as the action of G on X as described in Lemma 1.3.12. By Lemma 1.3.12 we can partition $\overline{B}$ into n sets $B_1, \ldots, B_n$ such that the permutations of $B_1, \ldots, B_n$ under G are the same as those in G (provided we label $B_1, \ldots, B_n$ appropriately).

Take $B_i = \{b_{i1}, \ldots, b_{il}\}$ and define $z_i = s(B_i)$ where $s(B_i)$ denotes the sum of the elements in B_i. Let $\sigma \in G$ and suppose $\sigma(B_i) = B_j$. Then $\sigma(z_i) = \sigma(b_{i1} + \cdots + b_{il}) = \sigma(b_{i1}) + \cdots + \sigma(b_{il}) = b_{j1} + \cdots + b_{jl} = z_j$. Hence G acts on z_i by permutations that are the same as those in G.

As the elements of $\overline{B}$ are algebraically independent over L so must be $z_1, \ldots, z_n$. Thus $f(z_1, \ldots, z_n) \neq 0$. As $\overline{B}$ is a normal basis, $\det(A) \neq 0$ (by Corollary 1.3.7) where $A = (a_{ij})$ and $a_{ij} = \sigma_i(\sigma_j(\bar{\beta}_1))$ for $\sigma_i, \sigma_j \in G$. However this determinant and $f(z_1, \ldots, z_n)$ are some nonzero polynomials $g, f' \in N[x_1, \ldots, x_m]$ respectively. Since $L < N$ is an infinite field, we can find $k_1, \ldots, k_m \in L$ so that $f'(k_1, \ldots, k_m)g(k_1, \ldots, k_m) \neq 0$. Let $\overline{\overline{B}}$ be the image of $\overline{B}$ under $x_i \mapsto k_i$. By construction $\bar{\bar{\bar{\beta}}}_i = \sigma_i(\bar{\bar{\bar{\beta}}}_1)$ and the determinant $g(k_1, \ldots, k_m) \neq 0$. It follows that $\bar{\bar{\bar{\beta}}}_i$ forms a normal basis for N/L. Moreover, $\alpha_i = s(\bar{\bar{\bar{B}}}_i)$ is the image under $x_i \mapsto k_i$ of z_i for $i = 1, \ldots, n$. Here $f(\alpha_1, \ldots, \alpha_n)$ is the image of $f(z_1, \ldots, z_n)$ under the same map and $f(\alpha_1, \ldots, \alpha_n) = f'(k_1, \ldots, k_m) \neq 0$. Moreover, the action of G on $\alpha_1, \ldots, \alpha_n$ is the same as G acting on $z_1, \ldots, z_n$ because G fixes $k_1, \ldots, k_m$. □

Proposition 3.1.3. *Let K be a field, G a group acting on the function field $K(x_1, \ldots, x_n)$ by permutations of the indeterminates and let F be a G-stable intermediate field between K and $K(x_1, \ldots, x_n)$. Then we can chose a finite G-stable subset $\mathcal{M} \subset F$ such that $F^G(\mathcal{M}) = F$. Moreover, the polynomial*

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) \in F^G[X].$$

Proof. Since G acts by permutations we have $G \leq S_n$. By Galois theory we have the following tower:

$$\begin{array}{c} K(x_1, \ldots, x_n) \\ | \\ F \\ | \\ K(x_1, \ldots, x_n)^G \\ | \\ F^G \\ | \\ K(x_1, \ldots, x_n)^{S_n} \\ | \\ K \end{array}$$

Moreover, we see in the proof of Theorem 2.3.2 that $[K(x_1, \ldots, x_n) : K(x_1, \ldots, x_n)^{S_n}] = n!$. By field theory if follows that $[K(x_1, \ldots, x_n) : F^G] \leq n!$ and $[F : F^G] \leq n!$. Hence there is some finite subset $\mathcal{M}' \subset F$ so that $F^G(\mathcal{M}') = F$. But is it G-stable? We construct a G-stable subset

$\mathcal{M} \subset F$ so that $\mathcal{M}' \subset \mathcal{M}$. Take $\mathcal{M}$ to be the set $\mathcal{M}'$ together with the orbit of all of its elements. Since G is finite and $\mathcal{M}'$ is finite, $\mathcal{M}$ must be finite as well. By construction $\mathcal{M}$ is a finite G-stable subset of F so that $F^G(\mathcal{M}) = F$.

Moreover, we show that $f(X)$ is in fact in the polynomial ring $F^G[X]$. Take $\mathcal{M} = \{y_1, \ldots, y_k\}$ for some positive integer k. Then the coefficients of $f(X)$ are symmetric in $y_1, \ldots, y_k$ by construction. Since $\mathcal{M}$ is a finite G-stable set, we can view the action of G on $\mathcal{M}$ as permutations of the indices's of $y_1, \ldots, y_k$. Therefore the coefficients of $f(X)$ are invariant under the action of G (by definition of symmetric polynomials) and lie in F^G. □

3.1.1 For Permutation Group Representations

The proof of Theorem 3.1.4 is in [KM00], pages 845-846, and is used as an outline for the proof below.

Theorem 3.1.4. *Let K be a field, G a group acting on the rational function field $K(x_1, \ldots, x_n)$ by permutations of the indeterminates, and let F be a G-stable intermediate field between K and $K(x_1, \ldots, x_n)$ such that G acts faithfully on F. Assume that the fixed field F^G is purely transcendental over K with transcendence degree m. Then there exists a generic polynomial for G over K.*

More precisely, let $\{\varphi_1, \ldots, \varphi_m\} \subset F^G$ be a transcendence base of F^G/K. Moreover, choose a finite, G-stable subset $\mathcal{M} \subset F$ such that $F = F^G(\mathcal{M})$. Set

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) \in F^G[X].$$

Then $f(X) = g(\varphi_1, \ldots, \varphi_m, X)$ with $g \in K(t_1, \ldots, t_m)$, and g is a generic polynomial for G over K.

Proof. Take $\mathcal{M} = \{y_1, \ldots, y_l\}$. By construction of $f(X)$ the splitting field of $f(X)$ is $F^G(\mathcal{M}) = K(\varphi_1, \ldots, \varphi_m)(\mathcal{M}) = F$. Moreover, $y_1, \ldots, y_l$ are distinct so

$f(X) = g(\varphi_1, \ldots, \varphi_m, X)$ is separable. Since $\varphi_1, \ldots, \varphi_m$ are algebraically independent, $K(\varphi_1, \ldots, \varphi_m)$ is isomorphic to $K(t_1, \ldots, t_m)$. Hence the splitting field of g is isomorphic to $F^G(\mathcal{M})$. It follows that the Galois group of g is

$$\mathrm{Gal}(F/F^G) = G.$$

It remains to prove property (b) of Definition 3.1.1. Let L be an infinite field containing K and N/L a Galois extension with Galois group $H \leq G$. To show what we need, we first construct a polynomial $h \in K[x_1, \ldots, x_n]$. We have that $f(X) = g(\varphi_1, \ldots, \varphi_m, X)$ is a polynomial in X whose coefficients are in $K(\varphi_1, \ldots, \varphi_m)$. Take $\mathcal{B} = \{\beta_0, \ldots, \beta_k\}$ to be said coefficients, where k is the degree of $f(X)$. Here each β_i is a rational expression in $\varphi_1, \ldots, \varphi_m$. That is

$$\beta_i = p_i/q_i \quad \text{for some} \quad p_i, q_i \in K[\varphi_1, \ldots, \varphi_m] \;\text{ with }\; q_i \neq 0.$$

Moreover, each $\varphi_1, \ldots, \varphi_m$ is a rational expression in $x_1, \ldots, x_n$, and it follows that $p_1, \ldots, p_k$ and $q_1, \ldots, q_k$ are as well. Thus

$$p_i = r_i/s_i, \;\; q_i = r_i'/s_i' \text{ for some } \;\; r_i, s_i, r_i', s_i' \in K[x_1, \ldots, x_n].$$

As $s_i \neq 0$, $r_i' \neq 0$, we can express the coefficients of $g(\varphi_1, \ldots, \varphi_m, X)$ as rational expressions in $x_1, \ldots, x_n$, namely

$$\beta_i = \frac{r_i \cdot s_i'}{s_i \cdot r_i'}.$$

Take $h_1 = \prod s_i \cdot r_i'$. Each $\varphi_1, \ldots, \varphi_m$ and $y_1, \ldots, y_l$ is a rational expression in $x_1, \ldots, x_n$. Take h_2 to be the product of the denominators of the $\varphi_1, \ldots, \varphi_m$ and $y_1, \ldots, y_l$. Moreover, $\mathrm{discr}_X(f(X)) = [\prod_{i<j}(y_i - y_j)]^2$ is a rational expression in $x_1, \ldots, x_n$. Take h_3 to be the product of the numerator and denominator of $\mathrm{discr}_X(f(X))$ (which is nonzero because the y_i are distinct). Finally take

$h \in K[x_1, \ldots, x_n]$ to be

$$h = h_1 \cdot h_2 \cdot h_3.$$

By Lemma 3.1.2 there exists $\alpha_1, \ldots, \alpha_n \in N$ such that

$$\sigma(\alpha_i) = \alpha_{\sigma(i)} \quad \text{for} \quad \sigma \in H, \quad \text{and} \quad h(\alpha_1, \ldots, \alpha_n) \neq 0.$$

Here $\sigma(i)$ is defined by the permutation action of G on $x_1, \ldots, x_n$. That is $\sigma(x_i) = x_{\sigma(i)}$. Define the homomorphism

$$\Psi : K[x_1, \ldots, x_n, h^{-1}] \longrightarrow N, \ x_i \mapsto \alpha_i.$$

By construction of h, $K[x_1, \ldots, x_n, h^{-1}]$ contains $\mathcal{M}$, all φ_i, $\mathrm{discr}_X(f(X))$ and $\mathrm{discr}_X(f(X))^{-1}$. Further more since $h(\alpha_1, \ldots, \alpha_n) \neq 0$, $\Psi(\varphi_i)$ is well defined. Take $\lambda_i := \Psi(\varphi_i)$ for $i = 1, \ldots, m$. Notice that the H-action commutes with Ψ, that is

$$\sigma(\Psi(x_i)) = \sigma(\alpha_i) = \alpha_{\sigma(i)} = \Psi(x_{\sigma(i)}) = \Psi(\sigma(x_i)).$$

Since $\varphi_1, \ldots, \varphi_m$ are invariant under G, they must be invariant under H as well. It follows that $\lambda_i \in N^H$. We have

$$\prod_{y \in \mathcal{M}} (X - \Psi(y)) = \Psi(f) = g(\lambda_1, \ldots, \lambda_m, X).$$

Therefore $N' := L(\Psi(\mathcal{M})) \subset N$ is the splitting field of $g(\lambda_1, \ldots, \lambda_m, X)$ over L. Note that $\Psi(y_i)$ is well defined because $h(\alpha_1, \ldots, \alpha_n) \neq 0$. However, we need $N' = N$. By way of contradiction, assume N' is properly contained in N. Since N is Galois over L, we have some $\sigma \in H, \sigma \neq 1$, that fixes N' element-wise. Moreover, there exists some x in F so that $\sigma(x) \neq x$ (because F is Galois over F^G). Since $F = F^G(\mathcal{M})$ we must have some y_0 in $\mathcal{M}$ so that $\sigma(y_0) \neq y_0$. It follows that $\sigma(y_0) - y_0 \neq 0$ and $\sigma(y_0) - y_0$ divides $\mathrm{discr}_X(f)$, which implies that $\Psi(\sigma(y_0) - y_0) = \sigma(\Psi(y_0)) - \Psi(y_0)$ divides $\Psi(\mathrm{discr}_X(f))$. Since $h(\alpha_1, \ldots, \alpha_n) \neq 0$ we have that $\Psi(\mathrm{discr}_X(f)) \neq 0$. Thus $\sigma(\Psi(y_0)) - \Psi(y_0) \neq 0$ and $\sigma(\Psi(y_0)) \neq \Psi(y_0)$, which contradicts the assumption that σ fixes N'. Therefore $N' = N$. □

From this result we can show that the polynomial given in the general equation of the n^{th} degree is generic for S_n. This is shown in Section 3.2.

3.1.2 For Linear Group Representations

[KM00] also provides a more general version of Theorem 3.1.4. However, this requires more material. Let K be a field and G a finite group so that $|G| = n$, for some positive integer n. We define the group algebra KG to be all formal linear combinations of elements of G over K. We write

$$KG = \{a_1g_1 + \cdots + a_ng_n | a_i \in K, g_i \in G\}.$$

It is readily seen that KG is an n-dimensional vector space with the basis G. Let $v_1, v_2 \in KG$. Then $v_1 = a_1g_1 + \cdots + a_ng_n$ and $v_2 = b_1g_1 + \cdots + b_ng_n$ for some $a_i, b_i \in K$. Here vector addition is given by

$$v_1 + v_2 = (a_1 + b_1)g_1 + \cdots + (a_n + b_m)g_n.$$

This defines an abelian group structure on KG where the identity is $0g_1 + \cdots + 0g_n$. Now define a product on KG by extending the product structure on G by distribution to obtain a ring structure. Let $a, b \in K$ and $g, h \in G$. Here the product of $(ag)(bh) := (ab)(gh)$ where ab and gh are the products defined on K and G

respectively. With that we have

$$\begin{aligned}
v_1 \cdot v_2 &:= (a_1g_1 + \cdots + a_ng_n)(b_1g_1 + \cdots + b_ng_n) \\
&= a_1g_1(b_1g_1 + \cdots + bng_n) + \cdots + a_ng_n(b_1g_1 + \cdots + b_ng_n) \\
&= [(a_1g_1)(b_1g_1) + \cdots + (a_1g_1)(b_ng_n)] + \cdots \\
&\qquad\qquad + [(a_ng_n)(b_1g_1) + \cdots + (a_ng_n)(b_ng_n)(b_ng_n)] \\
&= [(a_1b_1)(g_1^2) + \cdots (a_1b_n)(g_1g_n)] + \cdots + [(a_nb_1)(g_ng_1) + \cdots + (a_nb_n)(g_n^2)].
\end{aligned}$$

Lastly we collect like terms and are left with an element in KG. Thus KG is a ring which we call the group algebra of G over K and we may view it as a KG-module over itself. Furthermore, given some positive integer d, $(KG)^d$ is a KG-module as well.

Let V be an m-dimensional vector space over the field K with basis $\{v_1, \ldots, v_m\}$. Denote V^* as the set of all linear maps of V into K. It turns out V^* is also a m-dimensional vector space over K with the basis $\{v_1^*, \ldots, v_m^*\}$ where $v_i^*(v_j) = 1$ if $i = j$ and $v_i^*(v_j) = 0$ if $i \neq j$ (the dual basis). We denote the polynomial ring over V as $K[v_1^*, \ldots, v_m^*]$, the polynomial ring over K in m indeterminates, where the elements of the basis of V^* are the indeterminates. We refer to $K[v_1^*, \ldots, v_m^*]$ as $K[V]$ and the rational function field of $K[V]$ as $K(V)$.

The proof of Lemma 3.1.5 is in [JLY02], which was used as an outline for the proof below.

Lemma 3.1.5. *Let G be a finite group and V an m-dimensional, faithful linear representation of G over a field K. Then we have an injective KG-module homomorphism of V into $(KG)^m$ where KG is the group algebra of G over K defined above.*

Proof. As G acts linearly on V so does KG. That is, V is a KG-module. Take

$G = \{\sigma_1 = 1, \ldots, \sigma_n\}$, where $n = |G|$. Let $\varphi \in V^*$ and consider the map $h_\varphi : V \longrightarrow KG$ given by

$$h_\varphi(v) = \varphi(\sigma_1^{-1}v)\sigma_1 + \cdots + \varphi(\sigma_n^{-1}v)\sigma_n = \sum_{i=1}^{n} \varphi(\sigma_i^{-1}(v))\sigma_i.$$

Claim: h_φ is a KG-module homomorphism. Let $k_1, k_2 \in K$, $v_1, v_2 \in V$ and consider $h_\varphi(k_1v_1 + k_2v_2)$,

$$\begin{aligned}
h_\varphi(k_1v_1 + k_2v_2) &= \sum_{i=1}^{n} \varphi(\sigma_i^{-1}(k_1v_1 + k_2v_2))\sigma_i \\
&= \sum_{i=1}^{n} \varphi(k_1\sigma_i^{-1}(v_1) + k_2\sigma_i^{-1}(v_2))\sigma_i \\
&= \sum_{i=1}^{n} (k_1\varphi(\sigma_i^{-1}(v_1)) + k_2\varphi(\sigma_i^{-1}(v_2)))\sigma_i \\
&= \sum_{i=1}^{n} k_1\varphi(\sigma_i^{-1}(v_1))\sigma_i + k_2\varphi(\sigma_i^{-1}(v_2))\sigma_i \\
&= k_1 \sum_{i=1}^{n} \varphi(\sigma_i^{-1}(v_1))\sigma_i + k_2 \sum_{i=1}^{n} \varphi(\sigma_i^{-1}(v_2))\sigma_i \\
&= k_1h_\varphi(v_1) + k_2h_\varphi(v_2).
\end{aligned}$$

Thus h_φ is a K-homomorphism. However, we need to show that it is also a G-homomorphism. Let $\sigma \in G$, $v \in V$ and consider $h_\varphi(\sigma v)$,

$$h_\varphi(\sigma v) = \sum_{i=1}^{n} \varphi(\sigma_1^{-1}(\sigma v))\sigma_i \tag{3.1}$$

$$= \sum_{i=1}^{n} \varphi((\sigma_1^{-1}\sigma)v)\sigma_i. \tag{3.2}$$

Let $\tau_i = \sigma_i^{-1}\sigma$, then $\sigma_i = \sigma\tau_i^{-1}$ and

$$(3.2) = \sum_{i=1}^{n} \varphi(\tau_i v)\sigma\tau_i^{-1}. \tag{3.3}$$

Let $\rho_i^{-1} = \tau_i$, then

$$(3.3) = \sum_{i=1}^{n} \varphi(\rho_i^{-1} v)\sigma\rho_i \tag{3.4}$$

$$= \sigma \sum_{i=1}^{n} \varphi(\rho_i^{-1} v)\rho_i \tag{3.5}$$

$$= \sigma h_\varphi(v). \tag{3.6}$$

Thus h_φ is a KG-module homomorphism.

Consider the kernel of h_φ,

$$\begin{aligned}\ker(h_\varphi) &= \{v \in V | h_\varphi(v) = 0\} \\ &= \{v \in V | \varphi(\sigma_1^{-1}v)\sigma_1 + \cdots + \varphi(\sigma_n^{-1}v)\sigma_n = 0\} \\ &= \{v \in V | \varphi(\sigma_1^{-1}v) = \cdots = \varphi(\sigma_n^{-1}v) = 0\}.\end{aligned}$$

Notice that $\ker(h_\varphi) \subset \ker(\varphi)$.

V^* has the dual basis $v_1^*, \ldots, v_m^*$ and $\bigcap \ker(v_i^*) = \{0\}$. Then the map $\phi : V \longrightarrow (KG)^m$, where $v \mapsto (h_{v_1^*}(v), \ldots, h_{v_m^*}(v))$, is an injective KG-module homomorphism of V into $(KG)^m$. □

With Lemma 3.1.5 we can prove the following corollary. However, first we introduce some notation. Let G be a group and take $G = \{\sigma_1, \ldots, \sigma_n\}$. Let K be a field and let $K(mG) = K(x_{11}, \ldots, x_{1n}, \ldots, x_{m1}, \ldots, x_{mn})$ where x_{ij} are indeterminates. Let G act on $K(mG)$ by $\sigma(x_{ki}) = x_{kj}$ where $\sigma\sigma_i = \sigma_j$.

Corollary 3.1.6. *The injective KG-module homomorphism ϕ induces an injective field homomorphism of $K(V)$ into $K(mG)$.*

Proof. Take $\{v_1^*, \ldots, v_m^*\}$ to be the dual basis of V^*. As V^* itself is a vector space, we may consider V^{**} with the dual basis $\{v_1^{**}, \ldots, v_m^{**}\}$. Then we define

$$\phi^*(v_k^*) = \sum_{i=1}^{m} h_{v_i^{**}}(v_k^*).$$

where $h_{v_i^{**}}(v_k^*) = v_i^{**}(\sigma_1^{-1}v_k^*)x_{i1} + \cdots + v_i^{**}(\sigma_n^{-1}v_k^*)x_{in}$. Here the kernel of ϕ^* is $\bigcap \ker(v_i^*) = \{0\}$. Hence ϕ^* is injective.

Now we show the set $\{\phi^*(v_1^*), \ldots, \phi^*(v_m^*)\}$ is K-linearly independent. Suppose

$$a_1\phi^*(v_1^*) + \cdots + a_m\phi^*(v_m^*) = 0$$

for some $a_1, \ldots, a_m \in K$. Then

$$a_1 \sum_{i=1}^{m} h_{v_i^{**}}(v_1^*) + \cdots + a_m \sum_{i=1}^{m} h_{v_i^{**}}(v_m^*) = 0.$$

It follows that

$$\begin{aligned}
&(a_1v_1^{**}(\sigma_1^{-1}v_1^*) + a_2v_1^{**}(\sigma_1^{-1}v_2^*) + \cdots + a_mv_1^{**}(\sigma_1^{-1}v_m^*))x_{11}+\\
&\vdots\\
&+ (a_1v_1^{**}(\sigma_n^{-1}v_1^*) + a_2v_1^{**}(\sigma_n^{-1}v_2^*) + a_m \cdots + v_1^{**}(\sigma_n^{-1}v_m^*))x_{1n}+\\
&\vdots\\
&+ (a_1v_m^{**}(\sigma_1^{-1}v_1^*) + a_2v_m^{**}(\sigma_1^{-1}v_2^*) + \cdots + a_mv_m^{**}(\sigma_1^{-1}v_m^*))x_{m1}+\\
&\vdots\\
&+ (a_1v_m^{**}(\sigma_n^{-1}v_1^*) + a_2v_m^{**}(\sigma_n^{-1}v_2^*) + \cdots + a_mv_m^{**}(\sigma_n^{-1}v_m^*))x_{mn} = 0.
\end{aligned}$$

As the x_{ij} are indeterminates, we must have that

$$a_1v_i^{**}(\sigma_j^{-1}v_1^*) + a_2v_i^{**}(\sigma_j^{-1}v_2^*) + \cdots + a_mv_i^{**}(\sigma_j^{-1}v_m^*) = 0$$

for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. However,

$$a_1v_i^{**}(\sigma_j^{-1}v_1^*)+a_2v_i^{**}(\sigma_j^{-1}v_2^*)+\cdots+a_mv_i^{**}(\sigma_j^{-1}v_m^*) = v_i^{**}(\sigma_j^{-1}(a_1v_1^*+a_2v_2^*+\cdots+a_mv_m^*)).$$

Hence

$$v_i^{**}(\sigma_j^{-1}(a_1v_1^* + a_2v_2^* + \cdots + a_mv_m^*)) = 0$$

for $i = 1, \ldots, m$ and $j = 1, \ldots, n$.

Here $a_1 v_1^* + a_2 v_2^* + \cdots + a_m v_m^* = \mathbf{x}$ for some $\mathbf{x} \in V^*$. Now fix j at some value $1 \leq k \leq n$. Then

$$v_i^{**}(\sigma_k^{-1}(\mathbf{x})) = 0$$

for $i = 1, \ldots, m$ and it follows that $\sigma_k^{-1}(\mathbf{x}) = 0$. Since this must be true for any k we have that $\sigma_j^{-1}(\mathbf{x}) = 0$ for $j = 1, \ldots, n$. As V is a faithful representation we must have $\mathbf{x} = 0$. Hence

$$a_1 v_1^* + \cdots + a_m v_m^* = 0$$

which is true only if $a_1 = \cdots = a_m = 0$. Therefore $\{\phi^*(v_1^*), \ldots, \phi^*(v_m^*)\}$ is a linearly independent set and forms a basis for the image of V^* under ϕ^*. As $K(V)$ is defined in terms of the basis of V^*, we now have an injection of $K(V)$ into $K(mG)$. $\square$

The proof of Theorem 3.1.7 is in [KM00], pages 847-848, and is used as an outline for the proof below.

Theorem 3.1.7. *Let G be a finite group and V an m-dimensional, faithful linear representation of G over a field K. Assume that $K(V)^G$ is purely transcendental with transcendence degree m. More precisely take the transcendence base to be $\{\varphi_1, \ldots, \varphi_m\}$. Chose a finite, G-stable subset $\mathcal{M} \subset K(V)$ such that $K(V) = K(V)^G(\mathcal{M})$. Set*

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) \in K(V)^G[X],$$

so $f(X) = g(\varphi_1, \ldots, \varphi_m, X)$ with $g \in K(t_1, \ldots, t_m)[X]$. Then $g(X)$ is a generic polynomial for G over K.

Moreover, if the φ_i are homogeneous with

$$\deg(\varphi_1) = 1 \quad \textit{and} \quad \deg(\varphi_2) = \cdots = \deg(\varphi_m) = 0, \tag{3.7}$$

and if $\mathcal{M} \subset V^*$, then $g(1, t_2, \ldots, t_m, X)$ is also a generic polynomial (in $m-1$ parameters) for G.

Proof. To show that $g(X)$ is generic we show that the hypothesis of Theorem 3.1.4 is satisfied. By Corollary 3.1.6 we may view $K(V)$ as an intermediate field between K and $K(mG)$. The action of G on $K(mG)$ is given by $\sigma(x_{ki}) = x_{kj}$ where $\sigma\sigma_i = \sigma_j$. Hence the action of G on $K(mG)$ is by permutations of the indeterminates and we may consider Theorem 3.1.4.

Since G acts on V we have that $K(V)$ is a G-stable intermediate field between $K(mG)$ and K. Now we show the action of G on $K(V)$ is faithful. As the action of G on V is faithful, there exists some $v \in V$ so that $\sigma(v) \neq v$. It follows that $\sigma(v^*) \neq v^*$. As v^* is an element of $K(V)$, it follows that the action of G on $K(V)$ is faithful as well. Finally we have satisfied the hypothesis of Theorem 3.1.4 and $g(X)$ is a generic polynomial for G over K.

To prove the second assertion take $F = K(V)_0$, the field of homogeneous rational expressions of degree 0. We need to show that F is indeed a field and the the action of G is faithful on F. As $\deg(1) = 0$ and $\deg(0) = 0$ we have that $1, 0 \in F$. Now let $f, g \in F$. Then $f = p/q$ and $g = r/s$ for some $p, q, r, s \in K[V]$ with $q, s \neq 0$, $\deg(p) = \deg(q)$, and $\deg(r) = \deg(s)$. Then

$$f + g = p/q + r/s = (ps + rq)/qs, \quad \text{and} \quad fg = (p/q)(r/s) = (pr)/(qs).$$

Here $\deg(ps) = \deg(rq) = \deg(qs)$. Thus $\deg(ps + rq) = \deg(qs)$ and $f + g \in F$. Moreover, $\deg(pr) = \deg(qs)$ so $fg \in F$ as well. The additive inverse of f in $K(V)$ is $-f = -p/q$. Here $\deg(-p) = \deg(p) = \deg(q)$ so $-f \in F$. Suppose $f \neq 0$. The multiplicative inverse of $f \in K(V)$ is $f^{-1} = q/p$. As $\deg(p) = \deg(q)$, $f^{-1} \in F$ as well and F is a field.

To show that the action of G on F is faithful, we need to first show that G acts on F. As G acts linearly on $K(V)$, the action of G preserves the degree of polynomials, hence $\sigma(f) \in F$ for any $f \in F$ and $\sigma \in G$. Now we show that $K(V) = F(\varphi_1)$. Let $h \in K(V)$, then $h\varphi_1^{-\deg(h)} \in F$. Thus $K(V) = F(\varphi_1)$. As the action of $K(V)$ is faithful, there exists some $f \in K(V)$ so that $\sigma(f) \neq f$ for some $\sigma \in G$. Then

$$\sigma(f\varphi_1^{-\deg(f)}) = \sigma(f)\sigma(\varphi_1^{-\deg(f)}) = \sigma(f)\sigma(\varphi_1)^{-\deg(f)} = \sigma(f)\varphi_1^{-\deg(f)} \neq f\varphi_1^{-\deg(f)}.$$

As $f\varphi_1^{-\deg(f)} \in F$, the action of G on F is faithful.

Now we show that $F^G = K(\varphi_2, \ldots, \varphi_m)$. Take $N = K(\varphi_2, \ldots, \varphi_m)$ and let $f \in N$. Then $f = p/q$ for some $p, q \in K[\varphi_2, \ldots, \varphi_m]$ with $q \neq 0$. As $\deg(\varphi_2) = \cdots = \deg(\varphi_m) = 0$, it follows that $\deg(p) = \deg(q) = 0$ and $f \in F$. Further more since f is invariant under G we have that $f \in F^G$ as well. Thus $N \leq F^G$. As $F \leq K(V)$, we have that $F^G \leq K(V)^G = K(\varphi_1, \ldots, \varphi_m)$. Here we have the following tower of fields:

$$\begin{array}{c} K(V)^G = K(\varphi_1, \ldots, \varphi_m) \\ | \\ F^G \\ | \\ N = K(\varphi_2, \ldots, \varphi_m) \end{array}$$

As $\deg(\varphi_1) = 1$ and $\varphi_1 \notin F$, it follows that $\varphi_1 \notin F^G$. Now we claim that φ_1 is transcendental over F^G. Suppose it is not. Then $f(\varphi_1) = 0$ for some nonzero $f \in F^G[x]$. Take $f(x) = a_n x^n + \cdots + a_1 x + a_0$ with $a_n \neq 0$. If a_n is the only nonzero coefficient, then $a_n \varphi_1^n = 0$. Then either $a_n = 0$ or $\varphi_1^n = 0$ which is impossible because a_n and φ_1 are assumed to be nonzero. Let a_k be the first nonzero term in the list $a_0, a_1, \ldots, a_n$ where $k < n$. Then

$$a_n \varphi_1^n + \cdots + a_k \varphi_1^k = 0.$$

However, this implies that $a_k = -(a_n\varphi_1^{n-k} + \cdots + a_{k+1}\varphi_1)$. This is also impossible because $a_k \in F^G$ must have degree 0, while the RHS has degree $n-k > 0$. Therefore φ_1 must be transcendental over F^G. Hence the transcendence degree of $K(V)^G$ over F^G is greater than or equal to one. On the other hand $K(V)^G$ has transcendence degree 1 over N. By Theorem 1.4.4

$$trd(K(V)^G/N) = trd(K(V)^G/F^G) + trd(F^G/N) = 1$$

and it follows that $trd(F^G/N) = 0$. Thus F^G is algebraic over N. Moreover, since F^G is intermediate to a purely transcendental extension of N, $F^G = N$.

As $\mathcal{M} \subset V^*$, the elements of $\mathcal{M}$ are linear. Moreover, $\deg(\varphi_1) = 1$ so $\mathcal{M}' := \{y/\varphi_1 | y \in \mathcal{M}\} \subset F$. As $\mathcal{M}$ is G-stable and φ_1 is invariant under G, $\mathcal{M}'$ must be G-stable as well.

Now we show that $F^G(\mathcal{M}') = F$. As $F^G \subset F$ and $\mathcal{M}' \subset F$ it follows that $F^G(\mathcal{M}') \subset F$. Now we show the other containment. Let $f \in F$. Then $f \in K(V)$ and f is homogeneous of degree 0. Recall that $K(V) = K(\varphi_1, \ldots, \varphi_m)(\mathcal{M})$. Hence $f = p/q$ for some $p, q \in K(\varphi_1, \ldots, \varphi_m)[\mathcal{M}]$ with $q \neq 0$. Without loss of generality, we can assume that the coefficients of p and q are in $K[\varphi_1, \ldots, \varphi_m]$. For if they were not, we could find some nonzero polynomial $g \in K[\varphi_1, \ldots, \varphi_m]$ so that $gp, gq \in K[\varphi_1, \ldots, \varphi_m][\mathcal{M}]$. Take $\mathcal{M} = \{y_1, \ldots, y_r\}$ for some positive integer r. By assumption $\varphi_1, \ldots, \varphi_m$ and $y_1, \ldots, y_r$ are homogeneous. As f is homogeneous, we can assume that p and q are homogeneous in $\varphi_1, \ldots, \varphi_m$ and $y_1, \ldots, y_r$. For if p and q were not homogeneous in $\varphi_1, \ldots, \varphi_m$ and $y_1, \ldots, y_r$ then f would not be homogeneous. Moreover, as $\deg(\varphi_2) = \cdots = \deg(\varphi_m) = 0$, the degrees of p and q are determined by φ_1 and $y_1, \ldots, y_r$. By assumption $\deg(\varphi_1) = \deg(y_1) = \cdots = \deg(y_r) = 1$. As $\deg(f) = 0$, the degrees of p and q in $\varphi_1, y_1, \ldots, y_r$ must be equal. Take d to be the degree p and q. Consider some arbitrary term in p,

$$a\varphi_1^{\alpha_1}\cdots\varphi_m^{\alpha_m}y_1^{\beta_1}\cdots y_r^{\beta_r}$$

with $a \in K$ and $\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_r \in \mathbb{Z}_+$. Here $\alpha_1+\beta_1+\cdots+\beta_r = d$. If we factor φ_1^d out of this term we get

$$\varphi_1^d(a\varphi_1^{\alpha_1-d}\cdots\varphi_m^{\alpha_m}y_1^{\beta_1}\cdots y_r^{\beta_r}).$$

Since $\beta_1+\cdots+\beta_r = d-\alpha_1$ it follows that

$$\varphi_1^d(a\varphi_1^{\alpha_1-d}\cdots\varphi_m^{\alpha_m}y_1^{\beta_1}\cdots y_r^{\beta_r}) = \varphi_1^d\left(\varphi_2^{\alpha_2}\cdots\varphi_m^{\alpha_m}\left(\frac{y_1}{\varphi_1}\right)^{\beta_1}\cdots\left(\frac{y_r}{\varphi_1}\right)^{\beta_r}\right).$$

Therefore, if we factor out φ_1^d from p we get $p=\varphi_1^d p'$ for some $p' \in K(\varphi_2,\ldots,\varphi_m)[y_1/\varphi_1,\ldots,y_r/\varphi_1] = F^G[\mathcal{M}']$. Similarly, we can do the same for q and get $q=\varphi_1^d q'$ for some $q' \in F^G[\mathcal{M}']$. Hence

$$f=\frac{p}{q}=\frac{\varphi_1^d p'}{\varphi_1^d q'}=\frac{p'}{q'} \in F^G(M').$$

Therefore $F \subset F^G(\mathcal{M}')$ and $F = F^G(\mathcal{M}')$.

With $\mathcal{M}'$ we construct the following polynomial,

$$\begin{aligned}\prod_{y\in\mathcal{M}}(X-y/\varphi_1) &= \prod_{y\in\mathcal{M}}(1/\varphi_1)(\varphi_1 X-y)\\ &= \varphi_1^{-r}f(\varphi_1 X)\\ &= \varphi_1^{-r}g(\varphi_1,\ldots,\varphi_m,\varphi_1 X).\end{aligned}$$

We claim that $\varphi_1^{-r}g(\varphi_1,\ldots,\varphi_m,\varphi_1X) = g(1,\varphi_2,\ldots,\varphi_m,X)$. Consider the coefficient a_k of $(\varphi_1X)^k$ in $g(\varphi_1,\ldots,\varphi_m,\varphi_1X)$ for some $0\le k\le r$. By construction $a_k \in K(\varphi_1,\ldots,\varphi_m)$ and a_k is homogeneous in $y_1,\ldots,y_r$ of degree $r-k$. As $y_1,\ldots,y_r$ are elements of V^*, we have that a_k is homogeneous in $K(V)$ of degree $r-k$. Since $a_k \in K(\varphi_1,\ldots,\varphi_m)$ and $\varphi_1,\ldots,\varphi_m$ are homogeneous, a_k must be be homogeneous in $\varphi_1, \ldots, \varphi_m$. Take the numerator of a_k to be α and the denominator to be β. Then α and β are homogeneous in $\varphi_1, \ldots, \varphi_m$ and $\deg(\alpha) - \deg(\beta) = r - k$. As the degree is determined by φ_1, we may simplify α/β and assume that α is of degree $r - k$. That is, we may assume the degree of φ_1 in each term of α is $r - k$ and the degree of φ_1 in each term of β is zero. Now consider

$$\varphi_1^{-r} a_k (\varphi_1 X)^k = \varphi^{-r} a_k \varphi_1^k X^k = \frac{\alpha \varphi_1^{-(r-k)}}{\beta} X^k.$$

We get that the exponent of φ_1 in the coefficient of X^k is 0. However, this coefficient is precisely the coefficient of X^k in $\varphi_1^{-r} g(\varphi_1, \ldots, \varphi_m, \varphi_1 X)$. Hence

$$\varphi_1^{-r} g(\varphi_1, \ldots, \varphi_m, \varphi_1 X) = g(1, \varphi_2, \ldots, \varphi_m, X).$$

By Theorem 3.1.4, $g(1, t_2, \ldots, t_m, X)$ is generic for G over K. □

3.2 The Symmetric Group S_n

With Theorem 3.1.4 we can show

Corollary 3.2.1. *The polynomial given in the general equation of the n^{th} degree over a field K is generic for S_n.*

Proof. Let $G = S_n$ act on $K(x_1, \ldots, x_n)$ by permutations of the indeterminates $x_1, \ldots, x_n$. Take $F = K(x_1, \ldots, x_n)$. F is G-stable and F is an intermediate field between $K(x_1, \ldots, x_n)$ and K. Moreover, the action of G on F is faithful. Here $F^G = K(p_1, \ldots, p_n)$, where $p_1, \ldots, p_n$ are the elementary symmetric polynomials in $x_1, \ldots, x_n$ by Proposition 2.2.2. Take $\mathcal{M} = \{x_1, \ldots, x_n\}$. It is readily seen that $\mathcal{M}$ is a G-stable subset of F where $F^G(\mathcal{M}) = F$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.4,

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) \in F^G[X].$$

By construction $f(X) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n$. Take $g(p_1, \ldots, p_n, X) = f(X)$ with $g \in K(t_1, \ldots, t_n)[X]$. By Theorem 3.1.4, g is generic for G over K. Here

$$g(t_1, \ldots, t_n, X) = X^n - t_1X^{n-1} + \cdots + (-1)^n t_n$$

where $t_1, \ldots, t_n$ are indeterminates. Thus g is the polynomial given in the general equation of n^{th} degree and is generic for $G = S_n$ over K. □

With Theorem 3.1.7 we can obtain a generic polynomial for S_n in fewer parameters than in the one we constructed in Corollary 3.2.1. Let $K(x_1, \ldots, x_n)$ be the function field over K in n indeterminates. By Proposition 2.2.2, $K(x_1, \ldots, x_n)^{S_n} = K(\varphi_1, \ldots, \varphi_n)$, where φ_i are the elementary symmetric polynomials in $x_1, \ldots, x_n$. Moreover, by Proposition 2.1.3, $\varphi_1, \ldots, \varphi_n$ are algebraically independent and thus transcendental over K. Now take

$$\lambda_1 = \varphi_1, \quad \lambda_2 = \frac{\varphi_2}{\varphi_1^2}, \quad \ldots, \quad \lambda_n = \frac{\varphi_n}{\varphi_1^n}.$$

As $\varphi_1, \ldots, \varphi_n$ are algebraically independent, so must be $\lambda_1, \ldots, \lambda_n$. Moreover, since

$$\varphi_i = \lambda_1^i \lambda_i,$$

$K(x_1, \ldots, x_n)^{S_n} = K(\lambda_1, \ldots, \lambda_n)$. Here $\mathcal{M} = \{x_1, \ldots, x_n\}$ is a finite G-stable subset of $K(x_1, \ldots, x_n)$ so that $K(\lambda_1, \ldots, \lambda_n)(\mathcal{M}) = K(x_1, \ldots, x_n)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.4,

$$\begin{aligned} f(X) &= (X - x_1) \cdots (X - x_n) \\ &= X^n - \varphi_1 X^{n-1} + \varphi_2 X^{n-2} + \cdots + (-1)^n \varphi_n \\ &= X^n - \lambda_1 X^n + \lambda_1^2 \lambda_2 X^{n-1} + \cdots + (-1)^n \lambda_1^n \lambda_n. \end{aligned}$$

Take $g(\lambda_1, \ldots, \lambda_n, X) = f(X)$ with $g \in K(t_1, \ldots, t_n)[X]$. Since $\deg(\lambda_1) = 1$ and $\deg(\lambda_2) = \cdots = \deg(\lambda_n) = 0$, we may apply the second part of Theorem 3.1.7. Hence $g(1, t_2, \ldots, t_n X)$ is a generic polynomial for S_n over K as well. That is

$$g(1, t_2, \ldots, t_n, X) = X^n - X^{n-1} + t_2 X^{n-1} + \cdots + (-1)^n t_n$$

is generic for S_n over K. This gives us a generic polynomial for S_n in $n-1$ parameters.

CHAPTER 4

APPLICATIONS

We now consider applications of Theorems 3.1.4 and 3.1.7 to construct generic polynomials for some finite groups. Notice that the construction of generic polynomials in said theorems is based on the choice of $\mathcal{M}$. It turns out there are many choices of $\mathcal{M}$ that satisfy the prescribed conditions. Furthermore, how we pick such an $\mathcal{M}$ determines properties of the resulting generic polynomial which we state as

Proposition 4.0.2. *If the set $\mathcal{M}$ in Theorem 3.1.7 is formed using the orbit of one element in $K(V)$, then the resulting generic polynomial g is irreducible and G acts transitively on the roots of g.*

Proof. Suppose $\mathcal{M} = \{\sigma(r)|\sigma \in G\}$ for some $r \in K(x, y)$. By construction, $\mathcal{M}$ makes up the roots of $g(\varphi_1, \ldots, \varphi_m, X)$. As $\varphi_1, \ldots, \varphi_m$ are algebraically independent over K, we have that $K(\varphi_1, \ldots, \varphi_m)$ and $K(t_1, \ldots, t_m)$ are isomorphic where $\varphi_i \mapsto t_i$ for $i = 1, \ldots, m$. Call this isomorphism ϕ. Take L and L' to be the splitting fields of $g(\varphi_1, \ldots, \varphi_m, X)$ and $g(t_1, \ldots, t_m, X)$ respectively. Take $G' = \mathrm{Gal}(L'/K(t_1, \ldots, t_m))$.

By Theorem 1.2.8 ϕ can be be extended to an isomorphism of L and L'. Take $\mathcal{M}'$ to be the image of $\mathcal{M}$ under ϕ. It is readily seen that $\mathcal{M}'$ makes up the roots of $g(t_1, \ldots, t_m, X)$. Then $\mathcal{M}' = \{(\phi \circ \sigma)(r)|\sigma \in G\}$. As ϕ is an isomorphism, ϕ is a bijection from $\mathcal{M}$ to $\mathcal{M}'$. Then $r = \phi^{-1}(r')$ for some r' in $\mathcal{M}'$. Hence

$$\mathcal{M}' = \{(\phi \circ \sigma)(r)|\sigma \in G\} = \{(\phi \circ \sigma)(\phi^{-1}(r'))|\sigma \in G\} = \{(\phi \circ \sigma \circ \phi^{-1})(r'))|\sigma \in G\}.$$

Recall that we have the induced isomorphism under ϕ of G and G' given by $\phi \circ \sigma \circ \phi^{-1}$ for $\sigma \in G$ by Corollary 1.3.2. Then

$$\{(\phi \circ \sigma \circ \phi^{-1})(r'))|\sigma \in G\} = \{\sigma'(r'))|\sigma' \in G'\}$$

and G' is transitive on the roots of $g(t_1, \ldots, t_m, X)$. By Theorem 1.3.13 $g(t_1, \ldots, t_m, X)$ is irreducible. □

4.1 The Cyclic Group C_3

Consider the representation of the cyclic group of order three given by,

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

with $G \subseteq GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds Operator and Theorem 2.4.2, we calculate the invariant subring $K[x, y]^G$ is generated by

$$\varphi_1 = x^2 + y^2 - xy, \;\; \varphi_2 = x^2y - xy^2, \;\; \varphi_3 = x^3 + y^3 - 3x^2y, \;\; \varphi_4 = x^3 + y^3 - 3xy^2.$$

Hence $K[x, y]^G = K[\varphi_1, \varphi_2, \varphi_3, \varphi_4]$. As $\varphi_3 + 3\varphi_2 = \varphi_4$, we may take $\{\varphi_1, \varphi_2, \varphi_3\}$ as a generating set. Thus $K[x, y]^G = K[\varphi_1, \varphi_2, \varphi_3]$, and $K(x, y)^G = K(\varphi_1, \varphi_2, \varphi_3)$ by Proposition 2.4.3.

Now we construct a new generating set $\{\lambda_1, \lambda_2\}$ that is algebraically independent so that $\deg(\lambda_1) = 1$ and $\deg(\lambda_2) = 0$. Take $\lambda_1 = \varphi_2/\varphi_1$ and $\lambda_2 = \varphi_3/\varphi_2$ and consider $J(\lambda)$,

$$J(\lambda) = \begin{pmatrix} \frac{\partial \lambda_1}{\partial x} & \frac{\partial \lambda_1}{\partial y} \\ \frac{\partial \lambda_2}{\partial x} & \frac{\partial \lambda_2}{\partial y} \end{pmatrix}.$$

We get that $\det(J(\lambda)) = (-x^2 + xy - y^2)/(xy(x - y)) \not\equiv 0$. Thus λ_1 and λ_2 are algebraically independent by Theorem 1.4.1. Moreover,

$$\varphi_1 = \lambda_1^2(\lambda_2^2 + 3\lambda_2 + 9), \;\; \varphi_2 = \lambda_1^3(\lambda_2^2 + 3\lambda_2 + 9), \;\; \varphi_3 = \lambda_1^3(\lambda_2^3 + 3\lambda_2^2 + 9\lambda_2).$$

It follows that $\varphi_1, \varphi_2, \varphi_3 \in K(\lambda_1, \lambda_2)$ and $K(\lambda_1, \lambda_2) = K(x, y)^G$. Hence $\{\lambda_1, \lambda_2\}$ is a transcendence base for $K(x, y)^G$ over K.

4.1.1 Example 1

Now we form $\mathcal{M} = \{x, -y, y - x\}$ by taking the orbit of x. Here $\mathcal{M}$ is a finite G-stable subset of $K(x, y)$ so that $K(\lambda_1, \lambda_2)(\mathcal{M}) = K(x, y)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.7,

$$\begin{aligned} f(X) &= (X - x)(X + y)(X - y + x) \\ &= X^3 - (x^2 + y^2 - xy)X - (x^2y - xy^2) \\ &= X^3 - \varphi_1 X - \varphi_2 \\ &= X^3 - \lambda_1^2(\lambda_2^2 + 3\lambda_2 + 9)X - \lambda_1^3(\lambda_2^2 + 3\lambda_2 + 9). \end{aligned}$$

Take $g_1(\lambda_1, \lambda_2, X) = f(X)$ with $g_1(t_1, t_2, X) \in K(t_1, t_2)[X]$. By Theorem 3.1.7 $g_1(X)$ is generic for G over K. Since $\deg(\lambda_1) = 1$, $\deg(\lambda_2) = 0$ and $\mathcal{M}$ is a linear subset of $K(x, y)$, we can apply the second part of Theorem 3.1.7. Thus

$$g_1(1, t_2, X) = X^3 - (t_2^2 + 3t_2 + 9)X - (t_2^2 + 3t_2 + 9)$$

is generic for G over K. As t_2 is the only parameter, we get that $g_1 \in K(t, X)$ with

$$g_1(t, X) = X^3 - (t^2 + 3t + 9)X - (t^2 + 3t + 9)$$

is a generic polynomial for C_3 over K. Moreover, since $\mathcal{M}$ was formed as the orbit of x we have that $g_1(t, X)$ is irreducible and C_3 acts transitively on the roots, by Proposition 4.0.2.

4.1.2 Example 2

Another finite G-stable subset of $K(x, y)$ to consider is $\mathcal{M}' = \{x/y, y/(y - x), (x - y)/x\}$ which is formed by taking the orbit of x/y.

Moreover, $K(\lambda_1, \lambda_2)(\mathcal{M}') = K(x, y)$ which we show. It turns out

$$x = \frac{-\varphi_2 \cdot \left(\frac{x}{y} + \frac{y}{x} - 2\right) \cdot \left(\left(\frac{x-y}{x}\right)^{-3} - \left(\frac{y}{y-x}\right)^3\right)}{\varphi_1 \cdot \left(\frac{x}{y} - \left(\frac{x}{y} + \frac{y}{x} - 2\right) \cdot \left(\left(\frac{x-y}{x}\right)^{-3} + \left(\frac{y}{y-x}\right)^3\right)\right)}.$$

With $\mathcal{M}'$ we construct $f'(X)$,

$$\begin{aligned} f'(X) &= (X - x/y)(X - y/(y-x))(X - (x-y)/x) \\ &= X^3 + \left(\frac{x^3 - 3xy^2 + y^3}{x^2y - xy^2}\right) X^2 + \left(\frac{x^3 - 3x^2y + y^3}{x^2y - xy^2}\right) X + 1 \\ &= X^3 + \left(\frac{\varphi_3 + 3\varphi_2}{\varphi_2}\right) X^2 + \left(\frac{\varphi_3}{\varphi_2}\right) X + 1 \\ &= X^3 + \left(\frac{\varphi_3}{\varphi_2} + 3\right) X^2 + \left(\frac{\varphi_3}{\varphi_2}\right) X + 1 \\ &= X^3 + (\lambda_2 + 3)X^2 + \lambda_2 X + 1. \end{aligned}$$

Take $g_2(\lambda_1, \lambda_2, X) = f(X)$ with $g_2(t_1, t_2, X) \in K(t_1, t_2)[X]$. By Theorem 3.1.7 $g_2(X)$ is generic for G over K. That is

$$g_2(t_1, t_2, X) = X^3 + (t_2 + 3)X^2 + t_2 X + 1$$

is generic for G over K. As t_2 is the only parameter, we get that $g_2 \in K(t, X)$ with

$$g_2(t, X) = X^3 + (t + 3)X^2 + tX + 1$$

is a generic polynomial for C_3 over K. Moreover, since $\mathcal{M}'$ was formed as the orbit of x/y we have that $g_2(t, X)$ is irreducible and C_3 acts transitively on the roots, by Proposition 4.0.2.

4.2 The Klein-Four group

Consider the representation of the Klein-4 group given by,

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

with $G \subseteq GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds operator and Theorem 2.4.2, we get the invariant subring $K[x, y]^G$ is generated by the elements x^2, y^2. Hence $K[x, y]^G = K[x^2, y^2]$ and it follows that $K(x, y)^G = K(x^2, y^2)$ by Proposition 2.4.3. Clearly $\varphi_1 = x^2$ and $\varphi_2 = y^2$ are algebraically independent and $\{\varphi_1, \varphi_2\}$ forms a transcendence base for $K(x, y)^G$ over K.

4.2.1 Example 1

Now we form $\mathcal{M} = \{x, y, -x, -y\}$ by taking the orbit of x and y. Here $\mathcal{M}$ is a G-stable subset of $K(x, y)$ so that $K(x, y)^G(\mathcal{M}) = K(x, y)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.7,

$$\begin{aligned} f(X) &= (X - x)(X + x)(X - y)(X + y) \\ &= X^4 - (x^2 + y^2)X^2 + x^2y^2 \\ &= X^4 - (\varphi_1 + \varphi_2)X^2 + \varphi_1\varphi_2. \end{aligned}$$

Take $g(\varphi_1, \varphi_2, X) = f(X)$ with $g(t_1, t_2, X) \in K(t_1, t_2)[X]$. By Theorem 3.1.7

$$g(t_1, t_2, X) = X^4 - (t_1 + t_2)X^2 + t_1t_2 = (X^2 - t_1)(X^2 - t_2)$$

is generic for V over K. Since $\mathcal{M}$ was constructed with two disjoint orbits, it is reducible, which was shown.

4.2.2 Example 2

Consider the representation of the Klein-Four group given by,

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$$

with $G \in GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds operator and Theorem 2.4.2, we get the invariant subring $K[x, y]^G$ is generated by

$$x^2 + y^2, x^4 + y^4, xy, x^2y^2.$$

Since $x^2y^2 = (xy)^2$ and $x^4 + y^4 = (x^2 + y^2) - 2(xy)^2$ we have that $K[x, y]^G$ is generated by $\varphi_1 = x^2 + y^2$ and $\varphi_2 = xy$. Thus $K[x, y]^G = K[\varphi_1, \varphi_2]$ and it follows that $K(V)^G = K(\varphi_1, \varphi_2)$ by Proposition 2.4.3. It remains to show that φ_1 and φ_2 are algebraically independent. From the theory of symmetric functions we know that $x + y$ and xy are algebraically independent. That is, any algebraic expression of $x + y$ and xy is nonzero. Notice that $x^2 + y^2 = (x + y)^2 - 2xy$. Thus we may view any algebraic expression of $x^2 + y^2$ and xy as an algebraic expression of $(x + y)^2 - 2xy$ and xy which we know to be nonzero. Thus φ_1 and φ_2 are algebraically independent and $\{\varphi_1, \varphi_2\}$ forms a transcendence base for $K(x, y)^G$ over K.

Now we form $\mathcal{M} = \{x, y, -x, -y\}$ by taking the orbit of x. Here $\mathcal{M}$ is a finite G-stable subset of $K(x, y)$ so that $K(x, y)^G(\mathcal{M}) = K(x, y)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.7,

$$\begin{aligned} f(X) &= (X - x)(X + x)(X - y)(X + y) \\ &= X^4 - (x^2 + y^2)X^2 + x^2y^2 \\ &= X^4 - \varphi_1 X^2 + \varphi_2^2. \end{aligned}$$

Take $g(\varphi_1, \varphi_2, X) = f(X)$ with $g(t_1, t_2, X) \in K(t_1, t_2)[X]$. By Theorem 3.1.7,

$$g(t_1, t_2, X) = X^4 - t_1 X^2 + t_2^2$$

is generic for V over K. Moreover, since $\mathcal{M}$ was formed as the orbit of x we have that $g(t, X)$ is irreducible and G acts transitively on the roots, by Proposition 4.0.2.

4.3 The Cyclic group C_4

Consider the representation of C_4 given by

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

with $G \subseteq GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds operator and Theorem 2.4.2, we get the invariant subring $K[x, y]^G$ is generated by

$$\varphi_1 = x^2 + y^2,\ \ \varphi_2 = x^2y^2,\ \ \varphi_3 = xy(x^2 - y^2),\ \varphi_4 = x^4 + y^4.$$

Notice that $\varphi_4 = \varphi_1^2 - 2\varphi_2$. Thus $K[x, y]^G = K[\varphi_1, \varphi_2, \varphi_3]$ and it follows that $K(x, y)^G = K(\varphi_1, \varphi_2, \varphi_3)$ by Proposition 2.4.3. However $\{\varphi_1, \varphi_2, \varphi_3\}$ is not an algebraically independent set. It turns out

$$\varphi_1^2\varphi_2 - 4\varphi_2^2 - \varphi_3^2 = 0.$$

Take $\lambda_1 = \varphi_3/\varphi_2$, $\lambda_2 = \varphi_1/\varphi_2$ and consider $J(\lambda)$,

$$J(\lambda) = \begin{pmatrix} \frac{\partial \lambda_1}{\partial x} & \frac{\partial \lambda_1}{\partial y} \\ \frac{\partial \lambda_2}{\partial x} & \frac{\partial \lambda_2}{\partial y} \end{pmatrix}.$$

We get that $\det(J(\lambda)) = -(2(x^2 + y^2)^2)/(x^4y^4)) \not\equiv 0$. Thus λ_1 and λ_2 are algebraically independent by Theorem 1.4.1. Moreover,

$$\varphi_1 = (\lambda_1^2 + 4)/\lambda_2,\ \ \varphi_2 = (\lambda_1^2 + 4)/\lambda_2^2,\ \ \varphi_3 = (\lambda_1^3 + 4\lambda_1)/\lambda_2^2.$$

It follows that $\varphi_1, \varphi_2, \varphi_3 \in K(\lambda_1, \lambda_2)$ and $K(\lambda_1, \lambda_2) = K(x, y)^G$. Hence $\{\lambda_1, \lambda_2\}$ is a transcendence base for $K(x, y)^G$ over K.

Now we form $\mathcal{M} = \{x, y, -x, -y\}$ by taking the orbit of x. Here $\mathcal{M}$ is a G-stable subset of $K(x, y)$ so that $K(\lambda_1, \lambda_2)(\mathcal{M}) = K(x, y)$. With $\mathcal{M}$ we construct

$f(X)$,

$$\begin{aligned} f(X) &= (X-x)(X+x)(X-y)(X+y) \\ &= X^4 - (x^2+y^2)X^2 + x^2y^2 \\ &= X^4 - \varphi_1 X^2 + \varphi_2 \\ &= X^4 - ((\lambda_1^2+4)/\lambda_2)X^2 + (\lambda_1^2+4)/\lambda_2^2. \end{aligned}$$

Take $g(\lambda_1, \lambda_2, X) = f(X)$ with $g(t_1, t_2, X) \in K(t_1, t_2)[X]$. By Theorem 3.1.7

$$g(t_1, t_2, X) = X^4 - ((t_1^2+4)/t_2)X^2 + (t_1^2+4)/t_2^2$$

is generic for C_4 over K. Moreover, since $\mathcal{M}$ was formed as the orbit of x we have that $g(t, X)$ is irreducible and C_4 acts transitively on the roots, by Proposition 4.0.2.

4.4 The Cyclic Group C_6

Consider the representation of the cyclic group of order six given by,

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

with $G \subseteq GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds operator and Theorem 2.4.2, we get the invariant subring $K[x, y]^G$ is generated by

$$\varphi_1 = x^2 + y^2 - xy, \;\; \varphi_2 = (xy(x-y))^2, \;\; \varphi_3 = xy(x-y)(x^3+y^3-3x^2y).$$

By Proposition 2.4.3, $K(x, y)^G = K(\varphi_1, \varphi_2, \varphi_3)$. Take $\gamma_1 = \varphi_2/\varphi_1^2$ and $\gamma_2 = \varphi_3/\varphi_2$. Notice that $\gamma_1 = \lambda_1^2$ and $\gamma_2 = \lambda_2$ from section 4.1. As λ_1 and λ_2 are algebraically independent it follows that γ_1 and γ_2 are algebraically independent. Moreover,

$$\varphi_1 = \gamma_1(\gamma_2^2 + 3\gamma_2 + 9), \quad \varphi_2 = \gamma_1^3(\gamma_2^2 + 3\gamma_2 + 9)^2, \quad \varphi_3 = \gamma_1^3\gamma_2(\gamma_2^2 + 3\gamma_2 + 9)^2$$

and it follows that $K(x, y)^G = K(\gamma_1, \gamma_2)$. Hence $\{\gamma_1, \gamma_2\}$ is a transcendence base for $K(x, y)^G$ over K.

Now we form $\mathcal{M} = \{x, y, -x, -y, x - y, y - x\}$ by taking the orbit of x. Here $\mathcal{M}$ is a finite G-stable subset of $K(x, y)$ so that $K(\lambda_1, \lambda_2)(\mathcal{M}) = K(x, y)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.7,

$$\begin{aligned} f(X) &= (X - x)(X - y)(X + x)(X + y)(X - x + y)(X + x - y) \\ &= X^6 - (2x^2 + 2y^2 - 2xy)X^4 + (x^4 - 2x^3y + 3x^2y^2 - 2xy^3 + y^4)X^2 \\ &\qquad - (x^4y^2 - 2x^3y^3 + x^2y^4) \\ &= X^6 - 2\varphi_1 X^4 + \varphi_1^2 X^2 - \varphi_2 \\ &= X^6 - 2\gamma_1(\gamma_2^2 + 3\gamma_2 + 9)X^4 + \gamma_1^2(\gamma_2^2 + 3\gamma_2 + 9)^2 X^2 - \gamma_1^3(\gamma_2^2 + 3\gamma_2 + 9)^2. \end{aligned}$$

Take $g(\gamma_1, \gamma_2, X) = f(X)$ with $g(t_1, t_2,) \in K(t_1, t_2)[X]$. By Theorem 3.1.7

$$g(t_1, t_2, X) = X^6 - 2t_1\beta X^4 + t_1^2\beta^2 X^2 - t_1^3\beta^2$$

is a generic polynomial for C_6 over K, where $\beta = t_2^2 + 3t_2 + 9$. Moreover, since $\mathcal{M}$ was formed as the orbit of x we have that $g(t, X)$ is irreducible and C_6 acts transitively on its roots by Proposition 4.0.2.

4.5 The Dihedral Group D_3

Consider the representation of the dihedral group D_3 given by,

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \right.$$

$$\left.\begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\right\}$$

with $G \subseteq GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds operator and Theorem 2.4.2, we get the invariant subring $K[x, y]^G$ is generated by

$$\varphi_1 = x^2 + y^2 - xy, \quad \varphi_2 = (x + y)(x - 2y)(2x - y), \quad \varphi_3 = x^2y^2(x - y)^2.$$

So $K[x, y]^G = K[\varphi_1, \varphi_2, \varphi_3]$ and it follows that $K(x, y)^G = K(\varphi_1, \varphi_2, \varphi_3)$ by Proposition 2.4.3. However, $\varphi_1, \varphi_2, \varphi_3$ do not form an algebraically independent set. It turns out

$$\varphi_3 = (1/27)(4\varphi_1^3 - \varphi_2^2).$$

Hence $K(x, y)^G = K(\varphi_1, \varphi_2)$. However, we construct algebraically independent generators λ_1 and λ_2 to use Theorem 3.1.7 and obtain a generic polynomial in one parameter. Take $\lambda_1 = \varphi_2/\varphi_1$ and $\lambda_2 = \varphi_1^3/\varphi_2^2$ and consider $J(\lambda)$,

$$J(\lambda) = \begin{pmatrix} \frac{\partial \lambda_1}{\partial x} & \frac{\partial \lambda_1}{\partial y} \\ \frac{\partial \lambda_2}{\partial x} & \frac{\partial \lambda_2}{\partial y} \end{pmatrix}.$$

We get that

$$\begin{aligned} \det(J(\lambda)) = &- \frac{27x^2y(x - y)\left(-2x^4 + 4x^3y - 12x^2y^2 + 10xy^3 + y^4\right)}{(x - 2y)^3(2x - y)^3(x + y)^3} \\ &- \frac{27xy^2(x - y)\left(x^4 + 10x^3y - 12x^2y^2 + 4xy^3 - 2y^4\right)}{(x - 2y)^3(2x - y)^3(x + y)^3} \not\equiv 0. \end{aligned}$$

Thus λ_1 and λ_2 are algebraically independent by Theorem 1.4.1. Moreover,

$$\varphi_1 = \lambda_1^2\lambda_2, \quad \varphi_2 = \lambda_1^3\lambda_2.$$

It follows that $\varphi_1, \varphi_2 \in K(\lambda_1, \lambda_2)$ and $K(\lambda_1, \lambda_2) = K(x, y)^G$. Hence $\{\lambda_1, \lambda_2\}$ forms a transcendence base for $K(x, y)^G$ over K.

4.5.1 Example 1

Now we form $\mathcal{M} = \{x+y, x-2y, y-2x\}$ by taking the orbit of $x+y$. Here $\mathcal{M}$ is a finite G-stable subset of $K(x,y)$ so that $K(\lambda_1,\lambda_2)(\mathcal{M}) = K(x,y)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.7,

$$\begin{aligned} f(X) &= (X-x-y)(X-x+2y)(X-y+2x) \\ &= X^3 - (3x^2-3xy+3y^2)X + 2x^3 - 3x^2y - 3xy^2 + 2y^2 \\ &= X^3 - 3\varphi_1 X + \varphi_2 \\ &= X^3 - 3\lambda_1^2\lambda_2 X + \lambda_1^3\lambda_2. \end{aligned}$$

Take $g_1(\lambda_1,\lambda_2,X) = f(X)$ with $g_1(t_1,t_2,X) \in K(t_1,t_2)[X]$. By Theorem 3.1.7 $g_1(X)$ is generic for G over K. Since $\deg(\lambda_1) = 1$, $\deg(\lambda_2) = 0$ and $\mathcal{M}$ is a linear subset of $K(x,y)$, we can apply the second part of Theorem 3.1.7. Hence

$$g_1(1,t_2,X) = X^3 - 3t_2X + t_2$$

is generic for G over K. As t_2 is the only parameter, we get that $g_1 \in K(t,X)$ with

$$g_1(t,X) = X^3 - 3tX + t$$

is a generic polynomial for D_3 over K. Moreover, since $\mathcal{M}$ was formed as the orbit of $x+y$ we have that $g_1(t,X)$ is irreducible and D_3 acts transitively on its roots, by Proposition 4.0.2.

4.5.2 Example 2

Another finite G-stable subset of $K(x,y)$ to consider is $\mathcal{M}' = \{x, y, -x, -y, x-y, y-x\}$ which is formed by taking the orbit of x.

Furthermore, $K(x,y)^G(\mathcal{M}') = K(x,y)$. With $\mathcal{M}'$ we construct $f'(X)$,

$$\begin{aligned} f'(X) &= (X-x)(X+x)(X-y)(X+y)(X-x+y)(X+x-y) \\ &= X^6 + (2xy - 2x^2 - 2y^2)X^4 + (x^4 - 2x^3y + 3x^2y^2 - 2xy^3 + y^4)X^2 \\ &\qquad + (2x^3y^3 - x^2y^4 - x^4y^2) \\ &= X^6 - 2\varphi_1 X^4 + \varphi_1^2 X^2 + (1/27)(\varphi_2^2 - 4\varphi_1^3) \\ &= X^6 - 2\lambda_1^2\lambda_2 X^4 + (\lambda_1^2\lambda_2)^2 X^2 + (1/27)((\lambda_1^3\lambda_2)^2 - 4(\lambda_1^2\lambda_2)^3) \\ &= X^6 - 2\lambda_1^2\lambda_2 X^4 + \lambda_1^4\lambda_2^2 X^2 + (1/27)(\lambda_1^6\lambda_2^2 - 4\lambda_1^6\lambda_2^3). \end{aligned}$$

Take $g_2(\lambda_1, \lambda_2, X) = f'(X)$ with $g_2(t_1, t_2, X) \in K(t_1, t_2)[X]$. By Theorem 3.1.7, $g_2(X)$ is generic for G over K. However since $\deg(\lambda_1) = 1$, $\deg(\lambda_2) = 0$ and $\mathcal{M}'$ is a linear subset of $K(x,y)$, we can apply the second part of Theorem 3.1.7. Hence

$$g_2(1, t_2, X) = X^6 - 2t_2X^4 + t_2^2X^2 + (1/27)(t_2^2 - 4t_2^3)$$

is generic for D_3 over K. As t_2 is the only parameter, we get that $g_2 \in K(t, X)$ with

$$g_2(t, X) = X^6 - 2tX^4 + t^2X^2 + (1/27)(t^2 - 4t^3)$$

is a generic polynomial for D_3 over K. Moreover, since $\mathcal{M}'$ was formed as the orbit of x we have that $g_2(t, X)$ is irreducible and D_3 acts transitively on its roots, by Proposition 4.0.2.

Remark 1: Here we constructed two generic polynomials for D_3, one of degree 3 and one of degree 6. The degree 3 polynomial is a generic polynomial for D_3 as a transitive subgroup of S_3 and the degree 6 polynomial is a generic polynomial for D_3 as a transitive subgroup of S_6.

Remark 2: In Chapter 3 we constructed a generic polynomial for S_n in $n-1$ parameters. For S_3 this gives us a generic polynomial in 2 parameters. In this example we obtained a generic polynomial for $D_3 = S_3$ in one parameter, which is more desirable.

4.6 The Dihedral Group D_4

Consider the representation of the dihedral group D_4 given by,

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

with $G \subseteq GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds Operator we can determine that $K(x, y)^G = K(\varphi_1, \varphi_2)$ with $\varphi_1 = x^2 + y^2$ and $\varphi_2 = x^2y^2$. Earlier we saw that $x^2 + y^2$ and xy are algebraically independent. As $x^2y^2 = (xy)^2$, it is readily seen that φ_1 and φ_2 are algebraically independent as well. Hence $\{\varphi_1, \varphi_2\}$ forms a transcendence base for $K(x, y)^G$ over K.

4.6.1 Example 1

Now we form $\mathcal{M} = \{x, y, -x, -y\}$ by taking the orbit of x. Here $\mathcal{M}$ is a finite G-stable subset of $K(x, y)$ so that $K(\varphi_1, \varphi_2)(\mathcal{M}) = K(x, y)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.7,

$$\begin{aligned} f(X) &= (X - x)(X + x)(X - y)(X + y) \\ &= X^4 - \varphi_1 X^2 + \varphi_2. \end{aligned}$$

Take $g_1(\varphi_1, \varphi_2, X) = f(X)$ with $g_1(t_1, t_2, X) \in K(t_1, t_2)[X]$. By Theorem 3.1.7

$$g_1(t_1, t_2, X) = X^4 - t_1 X^2 + t_2$$

is generic for D_4 over K. Moreover, since $\mathcal{M}$ was formed as the orbit of x we have that $g_1(t_1, t_2, X)$ is irreducible and D_4 acts transitively on its roots, by Proposition

4.0.2.

4.6.2 Example 2

Another G-stable subset of $K(x,y)$ is $\mathcal{M}' = \{x, y, -x, -y, x+y, -x-y, x-y, -x+y\}$ which is formed by taking the orbit of x and $x+y$. Moreover, $K(x,y)^G(\mathcal{M}') = K(x,y)$. With $\mathcal{M}'$ we construct $f'(X)$,

$$\begin{aligned} f'(X) &= \prod_{\alpha \in \mathcal{M}'} (X - \alpha) \\ &= X^8 - 3(x^2+y^2)X^6 + 3(x^4+x^2y^2+y^4)X^4 \\ &\qquad - (x^6+x^4y^2+x^2y^4+y^6)X^2 + (x^6y^2 - 2x^4y^4 + x^2y^6) \\ &= X^8 - 3\varphi_1 X^6 + (3\varphi_1^2 - 3\varphi_2)X^4 - (\varphi_1^3 - 2\varphi_1\varphi_2)X^2 + (\varphi_1^2\varphi_2 - 4\varphi_2^2). \end{aligned}$$

Take $g_2(\varphi_1, \varphi_2, X) = f'(X)$ with $g_2(t_1, t_2, X) \in K(t_1, t_2, X)$. Then by Theorem 3.1.7,

$$g_2(t_1, t_2, X) = X^8 - 3t_1X^6 + (3t_1^2 - 3t_2)X^4 - (t_1^3 - 2t_1t_2)X^2 + (t_1^2t_2 - 4t_2^2)$$

is generic for D_4 over K. Note that since $\mathcal{M}'$ was formed using two disjoint orbits, $g_2(t_1, t_2, X)$ is a reducible polynomial and D_4 does not act transitively on its roots.

4.6.3 Example 3

Another G-stable subset of $K(x,y)$ is $\mathcal{M}'' = \{x+2y, 2x-y, -x-2y, y-2x, y+2x, -y-2x, x-2y, 2y-x\}$ which is formed by taking the orbit of $x+2y$. Moreover, $K(x,y)^G(\mathcal{M}'') = K(x,y)$. With

$\mathcal{M}''$ we construct $f''(X)$,

$$\begin{aligned} f''(X) &= \prod_{\alpha\in\mathcal{M}''}(X-\alpha) \\ &= X^8 - 10(x^2+y^2)X^6 + (33x^4+52x^2y^2+33y^4)X^4 \\ &\qquad - (40x^6+50x^2y^4+50x^4y^2+40y^6)X^2 \\ &\qquad + (16x^8-136x^6y^2+321x^4y^4-136x^2y^6+16y^8) \\ &= X^8 - 10\varphi_1X^6 + (33\varphi_1^2-14\varphi_2)X^4 - (40\varphi_1^3-70\varphi_1\varphi_2)X^2 \\ &\qquad + (16\varphi_1^4-200\varphi_1^2\varphi_2+625\varphi_2^2). \end{aligned}$$

Take $g_3(\varphi_1,\varphi_2,X) = f''(X)$ with $g_3(t_1,t_2,X) \in K(t_1,t_2,X)$. Then by Theorem 3.1.7,

$$\begin{aligned} g_3(t_1,t_2,X) = X^8 - 10t_1X^6 + (33t_1^2-14t_2)X^4 - (40t_1^3-70t_1t_2)X^2 \\ + (16t_1^4-200t_1^2t_2+625t_2^2) \end{aligned}$$

is generic for D_4 over K. Moreover, since $\mathcal{M}''$ was formed as the orbit of $x+2y$ we have that $g_3(t_1,t_2,X)$ is irreducible and D_4 acts transitively on its roots, by Proposition 4.0.2.

Remark: g_1 and g_3 are generic polynomials for D_4 of degree 4 and degree 8 respectively. Here g_1 is generic for D_4 as a transitive subgroup of S_4 and g_3 is generic for for D_4 as a transitive subgroup of S_8.

4.7 The Dihedral Group D_6

Consider the representation of the dihedral group D_6 given by,

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \right.$$

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix},$$
$$\begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}\Bigg\}$$

with $G \subseteq GL_2(K)$. Take $K(x, y)$ to be the function field over K in two indeterminates and let G act on $K(x, y)$. With the Reynolds Operator we can determine that $\varphi_1 = x^2 + y^2 - xy$ and $\varphi_2 = x^2y^2(x - y)^2$ generate $K(x, y)^G$. So $K(x, y)^G = K(\varphi_1, \varphi_2)$. Consider $J(\varphi)$,

$$J(\lambda) = \begin{pmatrix} \frac{\partial\varphi_1}{\partial x} & \frac{\partial\varphi_1}{\partial y} \\ \frac{\partial\varphi_2}{\partial x} & \frac{\partial\varphi_2}{\partial y} \end{pmatrix}.$$

We get that $\det(J(\varphi)) = 4x^5y - 10x^4y^2 + 10x^2y^4 - 4xy^5 \not\equiv 0$. Thus φ_1 and φ_2 are algebraically independent by Theorem 1.4.1. Hence $\{\varphi_1, \varphi_2\}$ forms a transcendence base for $K(x, y)^G$ over K.

4.7.1 Example 1

Now we form $\mathcal{M} = \{x, y, -x, -y, y - x, x - y\}$ by taking the orbit of x. Here $\mathcal{M}$ is a G-stable subset of $K(x, y)$ so that $K(\varphi_1, \varphi_2)(\mathcal{M}) = K(x, y)$. With $\mathcal{M}$ we construct $f(X)$ as in Theorem 3.1.7,

$$\begin{aligned} f(X) &= (X - x)(X + x)(X - y)(X + y)(X - x + y)(X + x - y) \\ &= X^6 + (2xy - 2x^2 - 2y^2)X^4 + (x^4 - 2x^3y + 3x^2y^2 - 2xy^3 + y^4)X^2 \\ &\qquad + (2x^3y^3 - x^2y^4 - x^4y^2) \\ &= X^6 - 2\varphi_1X^4 + \varphi_1^2X^2 - \varphi_2. \end{aligned}$$

Take $g_1(\varphi_1, \varphi_2, X) = f(X)$ with $g_1(t_1, t_2, X) \in K(t_1, t_2)[X]$. Then by Theorem 3.1.7

$$g_1(t_1, t_2, X) = X^6 - 2t_1X^4 + t_1^2X^2 - t_2$$

is a generic polynomial for D_6 over K. Moreover, since $\mathcal{M}$ was formed as the orbit of x we have that $g_1(t_1, t_2, X)$ is irreducible and D_6 acts transitively on its roots, by Proposition 4.0.2.

4.7.2 Example 2

Another G-stable subset of $K(x, y)$ is
$\mathcal{M}' = \{x, y, -x, -y, x-y, y-x, x+y, -x-y, 2x-y, 2y-x, y-2x, x-2y\}$ which is formed by taking the orbit of x and $x+y$. Moreover, $K(x, y)^G(\mathcal{M}') = K(x, y)$. With $\mathcal{M}'$ we construct $f'(X)$,

$$\begin{aligned} f'(X) &= \prod_{\alpha \in \mathcal{M}'} (X - \alpha) \\ &= X^{12} - 8\varphi_1 X^{10} + 22\varphi_1^2 X^8 - (28\varphi_1^3 - 26\varphi_2)X^6 + (17\varphi_1^4 - 48\varphi_1\varphi_2)X^4 \\ &\qquad - (4\varphi_1^5 - 18\varphi_1^2\varphi_2)X^2 + (4\varphi_1^3\varphi_2 - 27\varphi_2^2). \end{aligned}$$

Take $g_2(\varphi_1, \varphi_2, X) = f'(X)$ with $g_2(t_1, t_2, X) \in K(t_1, t_2)[X]$. Then by Theorem 3.1.7

$$\begin{aligned} g_2(t_1, t_2, X) = X^{12} - 8t_1 X^{10} + 22t_1^2 X^8 - (28t_1^3 - 26t_2)X^6 + (17t_1^4 - 48t_1t_2)X^4 \\ - (4t_1^5 - 18t_1^2t_2)X^2 + (4t_1^3t_2 - 27t_2^2) \end{aligned}$$

is a generic polynomial for D_6 over K. Note that since $\mathcal{M}'$ was formed using two disjoint orbits, $g_2(t_1, t_2, X)$ is a reducible polynomial and D_6 does not act transitively on its roots.

4.7.3 Example 3

Another G-stable subset of $K(x, y)$ is $\mathcal{M}'' = \{x+2y, 2x+y, 3y-2x, y-3x, -x-2y, 2x-3y, 3x-y, 3y-x, 2y-3x, -y-2x, x-3y, 3x-2y\}$ which is formed by taking the orbit of $x+2y$. Moreover, $K(x, y)^G(\mathcal{M}'') = K(x, y)$. With

$\mathcal{M}''$ we construct $f''(X)$,

$$\begin{aligned} f''(X) &= \prod_{\alpha \in \mathcal{M}''} (X - \alpha) \\ &= X^{12} - 28\varphi_1 X^{10} + 294\varphi_1^2 X^8 - (1444\varphi_1^3 - 286\varphi_2)X^6 \\ &\qquad + (3409\varphi_1^4 - 4004\varphi_1\varphi_2)X^4 - (3528\varphi_1^5 - 14014\varphi_1^2\varphi_2)X^2 \\ &\qquad\qquad + (1296\varphi_1^6 - 24696\varphi_1^3\varphi_2 + 117649\varphi_2^2). \end{aligned}$$

Take $g_3(\varphi_1, \varphi_2, X) = f''(X)$ with $g_3(t_1, t_2, X) \in K(t_1, t_2)[X]$. Then by Theorem 3.1.7

$$\begin{aligned} g_3(t_1, t_2, X) = X^{12} &- 28t_1 X^{10} + 294t_1^2 X^8 - (1444t_1^3 - 286t_2)X^6 \\ &+ (3409t_1^4 - 4004t_1t_2)X^4 - (3528t_1^5 - 14014t_1^2t_2)X^2 \\ &+ (1296t_1^6 - 24696t_1^3t_2 + 117649t_2^2) \end{aligned}$$

is generic for D_6 over K. Moreover, since $\mathcal{M}''$ was formed as the orbit of $x + 2y$ we have that $g_3(t_1, t_2, X)$ is irreducible and D_6 acts transitively on its roots, by Proposition 4.0.2.

Remark: g_1 and g_3 are generic polynomials for D_6 of degree 6 and degree 12 respectively. Here g_1 is generic for D_6 as a transitive subgroup of S_6 and g_3 is generic for D_6 as a transitive subgroup of S_{12}.

BIBLIOGRAPHY

[CLO07] D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd ed., Springer Science and Business Media, 2007.

[DK02] H. Derksen and G. Kemper, *Computatioinal Invariant Theory*, Encyclopedia of Mathematical Sciences, vol. I, Springer Science and Business Media, 2002.

[For92] K. Forsman, *Two Themes in Commutative Algebra*, 08 1992.

[Hal76] M. Hall, *The Theory of Groups*, AMS Chelsea Publishing, vol. 288, American Mathematical Soc., 1976.

[Hun12] T. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer Science and Business Media, 2012.

[Jac09] N. Jacobson, *Basic Algebra I*, 2nd ed., Dover Publications, INC., 2009.

[JLY02] C. Jensen, A. Ledet, and N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, 1st ed., Mathematical Sciences Research Institute, vol. 45, Cambridge University Press, 2002.

[KM00] G. Kemper and E. Mattig, *Generic Polynomials with Few Parameters*, J. Symbolic Computation **30** (2000), no. 6, 843–858.

[Kuy64] W. Kuyk, *On a theorem of E. Noether.*, Indagationes mathematicae **26** (1964), no. 1, 32–39.