ACADEMIC PRESS

Available at WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE @ DIRECT•

J. Differential Equations 191 (2003) 323–347

Journal of Differential Equations

http://www.elsevier.com/locate/jde

Linear relations among algebraic solutions of differential equations

John Michael Nahay

25 Chestnut Hill Lane, Columbus, NJ 08022-1039, USA

Received August 18 2000; revised March 12 2002

Abstract

For any univariate polynomial with coefficients in a differential field of characteristic zero and any integer, q, there exists an associated nonzero linear ordinary differential equation (LODE) with the following two properties. Each term of the LODE lies in the differential field generated by the rational numbers and the coefficients of the polynomial, and the qth power of each root of the polynomial is a solution of this LODE. This LODE is called a qth power resolvent of the polynomial. We will show how one can get a resolvent for the logarithmic derivative of the roots of a polynomial from the αth power resolvent of the polynomial, where α is an indeterminate that takes the place of q. We will demonstrate some simple relations among the algebraic and differential equations for the roots and their logarithmic derivatives. We will also prove several theorems regarding linear relations of roots of a polynomial over constants or the coefficient field of the polynomial depending upon the (nondifferential) Galois group. Finally, we will use a differential resolvent to solve the Riccati equation.

MSC: 12H05; 13N15

Keywords: Algebraic; Differential equations; Linear; Resolvent

1. Introduction

The Riccati equation is a well-known example of a nonlinear differential equation which is solvable by means of the trick of replacing the dependent variable with (something close to) the logarithmic derivative of another dependent variable. One then gets a second-order homogeneous linear ordinary differential equation (LODE)

E-mail address: resolvent@juno.com.

PII: S0022-0396(02)00074-8

in the new dependent variable. One can then, in principle, solve the LODE for the new dependent variable, and then work backwards to find the original dependent variable. Conversely, the logarithmic derivative of any nonzero solution of a second-order homogeneous LODE can be realized as satisfying a Riccati equation over the field generated by the terms of the ODE.

As an example of the use of logarithmic derivatives to solve differential equations, we note that in 1917 (see [8]) P. Scalizzi solved the nonlinear Abel equation, $\frac{dy}{dx} = f_0 + f_1 y + f_2 y^2 + f_3 y^3$, under the condition that $2f_2^3 - 9f_1 f_2 f_3 + 27 f_0 f_3^2 + 9f_3^2 \cdot \frac{d}{dx}(\frac{f_2}{f_3}) = 0$. A complete and more modern algebraic treatment of the Abel equation has been given by Schwarz [9]. In the spring of 2001 the author had independently rediscovered Scalizzi's solution. The method involves solving the second-order homogeneous LODE $9f_3 \cdot t'' + (-9f_3' - 18 f_1 f_3 + 2f_2^2) \cdot t' + 12 f_0 f_2 f_3 \cdot t = 0$ for a new variable, t, in terms of x. One then solves for y in terms of x by the formula $y = -\frac{f_2}{3f_3} \pm \sqrt{\left(\frac{f_2}{3f_3}\right)^2 - \frac{1}{2f_3}\frac{t'}{t}}$, i.e. by solving the quadratic equation $3\frac{t'}{t} + (6f_3 \cdot y^2 + 4f_2 \cdot y) = 0$. This formula depends upon only the logarithmic derivative of t, not upon t itself. The form of this dependence is expected since, as with the Riccati, the solution of the LODE for t involves the introduction of two arbitrary constants of integration. The logarithmic derivative of t then reduces the dependence of y to one constant of integration. The author is currently trying various methods, many involving the dependence upon the logarithmic derivative of a new variable which may satisfy some LODE of second order, for solving the general Abel equation without the aforementioned condition on f_0, f_1, f_2 and f_3.

It is with this background that the author pursued the study of a particular class of LODEs associated with polynomials of a single variable whose coefficients lie in a differential field. These LODEs are known as *resolvents* of the polynomial. In this paper, we will show some interesting properties of the logarithmic derivatives of the roots of the polynomial, and therefore of the logarithmic derivatives of particular solutions of its resolvents. This author always starts with the polynomial and then computes the terms of a resolvent, the minimal polynomial of the logarithmic derivatives of the roots of the polynomial, and the resolvent of this minimal polynomial, in terms of the coefficients of the polynomial and their derivatives.

Most other authors have worked the other way, starting with the LODE. For instance, in Theorem 4.1 of [10], Singer determines, in a finite number of steps, if the LODE, $L(y) = 0$, has a liouvillian solution over $\mathbb{F}$, where $\mathbb{F}$ is a finite algebraic extension of $\mathbb{Q}(x)$ and the terms of the LODE lie in $\mathbb{F}$. If it does, Singer's algorithm finds the liouvillian solution, y. In other words, one can find u such that the logarithmic derivative of u equals y. Working the other way, authors have long ago studied the logarithmic derivative of y, rather than the exponential of its integral. For instance, in [7], Pepin gives an algorithm (with some mistakes) in 1881 to find the minimal polynomial of the logarithmic derivatives of a solution of a second-order LODE.

As demonstrated by the solution of the Riccati equation and by Scalizzi's solution of the particular Abel equation, it is also important to understand something about the number of arbitrary constants that arise when solving a differential equation, such as the resolvent of a polynomial. Many authors have already done this for LODEs. For instance, in [2], E'lie and Singer characterize the LODEs with coefficients in $\mathbb{C}(x)$ that have solutions linearly independent over $\mathbb{C}$ but linearly dependent over $\mathbb{C}(x)$. They give an algorithm to compute such LODEs. So, this paper will also pursue the study of the numbers of linear relations over constants of the solutions of LODEs, namely, of resolvents of a polynomial. In other words, we will study the number of linear relations that can arise over constants of the roots of the polynomial. More generally, we will study the number of linear relations that can arise over the coefficient field of the polynomial or extensions of it.

As mentioned in the previous paragraph, this author always considers the coefficients of the polynomial as the known or given variables. In contrast, most authors in differential algebra have not studied the properties of a LODE as being the resolvent of any particular polynomial, although it seems likely one could always construct such a polynomial trivially. Let $P(t) \equiv \prod_i (t - s_i)$ where we may take as many solutions, s_i, of the LODE as we wish. Then the given LODE will be a resolvent for P if and only if the terms of the LODE lie in the differential field generated by $\mathbb{Q}$ and the elementary symmetric functions of the $\{s_i\}$. The author has not studied those LODEs and their solutions which satisfy this condition.

Finally, to tie these results together, we will demonstrate how one can use the formula for a particular resolvent of a quadratic polynomial to solve the Riccati equation if one did not know a priori the change-of-variables "trick".

2. Notation

Let $\in$ denote "is an element of", $\forall$ denote "for all", $\exists$ denote "there exists", and $\ni$ denote "such that". We will denote the set of all integers by $\mathbb{Z}$, the set of all nonzero integers by $\mathbb{Z}^{\#}$, the set of all positive integers by $\mathbb{N}$, and the set of all nonnegative integers by $\mathbb{N}_0$. The set of all rational numbers will be denoted by $\mathbb{Q}$. For each positive integer, m, the symbol, $[m]$, will denote the set of m positive integers, $\{1, \dots, m\}$, and the symbol, $[m]_0$, will denote the set of $m + 1$ integers nonnegative integers, $\{0, 1, \dots, m\}$.

An *ordinary differential field*, or a *differential field*, or a *d-field*, $\mathbb{F}$, is a field equipped with a derivation, D, satisfying the Leibniz Rule on all elements of $\mathbb{F}$, $D(u \cdot v) = uDv + vDu$. A *constant* is an element, $c \in \mathbb{F}$, satisfying $Dc = 0$. The subset of all constants in $\mathbb{F}$ forms a d-field called the *subfield of constants*, or the *field of constants*, and is denoted by $\Bbbk$. We will later need to introduce an element, α, that is transcendental over $\mathbb{F}$, yet is constant.

An *ordinary differential ring*, or a *differential ring*, or a *d-ring* $\mathbb{R}$, is a ring equipped with a derivation, D, satisfying the Leibniz Rule on all elements of $\mathbb{R}$, $D(u \cdot v) = uDv + vDu$. All rings will be considered to be commutative, with unity, and of characteristic zero.

The small letter, t, will be our universal dummy variable. The choice of letter reflects it being "totally transcendental" over everything else you see on the page.

We will consider only monic polynomials $P(t) \equiv \sum_{i=0}^{n} (-1)^{n-i} e_{n-i} \cdot t^i$ in a single indeterminate, t, with coefficients, $\{e_{n-i}\}_{i=0}^{n-1}$, lying in a differential field, $\mathbb{F}$, of characteristic zero. The roots of P will be denoted by $\{z_i\}_{i=1}^{n}$. The coefficient e_{n-i} of t^i in P is the $(n-i)$th elementary symmetric function of the roots of P. We will denote the set of coefficients, $\{e_i\}_{i=1}^{n}$, by e when we wish to adjoin all of them and their derivatives to various fields and d-fields. When we wish to indicate that each of the roots $\{z_i\}_{i=1}^{n}$ of $P(t)$ satisfies a particular differential or algebraic equation, we will simply use z without subscripts to denote the dependent variable. The discriminant of P will be defined in the usual manner as the product of the squares of the differences of the roots, $\Delta \equiv \prod_{i<j} (z_i - z_j)^2$.

Let $q \in \mathbb{Z}$. A qth power *linear differential resolvent*, or *differential resolvent*, or simply *resolvent*, of such a polynomial, P, is a nonzero finite-order linear ordinary differential equation, $\sum_{j=0}^{m} B_j(q) \cdot D^j z^q = I(q)$, with *coefficient functions*, $B_j(q)$ and $I(q)$, which lie in the smallest differential field, $\mathbb{Q}\langle e \rangle$, generated by the coefficients of P, and whose solutions include the qth power of each of the roots of P, $z^q \equiv \{z_i^q\}_{i=1}^{n}$. If the coefficient functions $B_j(q)$ and $I(q)$ lie in the smallest differential ring, $\mathbb{Z}\{e\} \subset \mathbb{Q}\langle e \rangle$, generated by the coefficients of P, then we say that the resolvent is *integral*. We will find it particularly useful to deal mostly with homogeneous resolvents, $I(q) \equiv 0$, especially when we refer to the Powersum Formula for expressing the $B_j(q)$ in terms of the e and their derivatives. But, we will sometimes refer to inhomogeneous resolvents for computational purposes, since, given any homogeneous resolvent of P there exists an inhomogeneous resolvent of one lower order.

We say that the roots z of P are differentially independent over any ordinary differential ring, $\mathbb{R}$, with derivation, D, if there exists no nonzero multivariable polynomial, f, with coefficients in $\mathbb{R}$ such that $f(z_1, \dots, z_n, Dz_1, \dots, Dz_n, \dots) = 0$. Hence, if the z are differentially independent over $\mathbb{R}$, then the z are algebraically independent over $\mathbb{R}$. We will exclusively consider $\mathbb{R} = \mathbb{k}$, the constant subfield of $\mathbb{F}$. It has been shown in Theorem 1 (the ZEP Theorem) on p. 23 in [5] that the z are differentially independent over $\mathbb{k}$ if and only if the e are differentially independent over $\mathbb{k}$. Furthermore, differential independence over $\mathbb{k}$ is equivalent to differential independence over any field of constants, so we may sometimes simply say "differential independence over constants".

If the roots of P (similarly, if the coefficients of P) are differentially independent over $\mathbb{k}$, then the weight of the coefficient functions $B_j(q)$ in $\mathbb{Z}\{e\}$ is well defined as on pp. 17–19 in [5]. It has been shown in Theorem 3 on pp. 25–26 in [5] that, in this case, there exists an integral resolvent of lowest weight and with no common factors among all its terms, $B_j(q)$, except for ±1. This resolvent, unique up to multiplication by ±1, is called the *Cohnian* of P, in honor of Dr. Richard Cohn.

Let α be transcendental over $\mathbb{Q}\langle e\rangle$ with $D\alpha = 0$. For each root, z_j, of P define y_j to be a nonzero solution of the logarithmic differential equation, $\frac{Dy_j}{\alpha \cdot y_j} = \frac{Dz_j}{z_j}$. An *$\alpha$th power resolvent*, of such a polynomial, P, is a finite-order linear differential equation, $\sum_{j=0}^{m} B_j(\alpha) \cdot D^j y = 0$, with coefficient functions, $B_j(\alpha)$, which lie in the smallest differential field, $\mathbb{Q}\langle e\rangle(\alpha)$, generated by α and the coefficients of P, and whose solutions include the set $y \equiv \{y_i\}_{i=1}^{n}$. If the coefficient functions, $B_j(\alpha)$, lie in the smallest differential ring, $\mathbb{Z}\{e\}[\alpha] \subset \mathbb{Q}\langle e\rangle(\alpha)$, generated by the coefficients of P and α then we say that the resolvent is *integral*. If the roots of P are differentially independent over $\mathbb{k}$, then the weight of elements in the d-ring $\mathbb{Z}\{e\}[\alpha]$ is well defined, and there exists an αth power resolvent of lowest weight and with no common factor in $\mathbb{Z}\{e\}[\alpha]$ among its coefficient functions except for ± 1. This resolvent is called the *Cohnian* of P and is unique up to multiplication by ± 1.

As it has already been done in the abstract and introduction, we will abbreviate "linear ordinary differential equation" to LODE, "ordinary differential equation" to ODE, and "differential equation" to DE.

3. Resolvent for the logarithmic derivative

Define $\Omega \equiv \frac{n(n-1)}{2} + 1$. The author has already determined in [5] the existence and form of certain αth power resolvents of polynomials. We will assume this form in Theorem 1. Theorem 1 was suggested for the Quadratic by Dr. Richard Cohn, but it was generalized by the author. In order to guarantee that the same resolvents and identities in Theorem 1 and Observation 2 hold for the logarithmic derivative, $u_j \equiv \frac{Dz_j}{z_j}$, of each root, z_j, of P, we must assume that P is irreducible over its differential coefficient field, $\mathbb{Q}\langle e\rangle$. The hypothesis of Theorem 1, that the coefficients of P are differentially independent over constants, guarantees that P will be irreducible over $\mathbb{Q}\langle e\rangle$.

Theorem 1. *Let $\mathbb{F}$ be a differential field of characteristic 0 with derivation, D, and subfield of constants, $\mathbb{k}$. Let $P(t) \equiv \sum_{i=0}^{n} (-1)^{n-i} e_{n-i} \cdot t^i \in \mathbb{F}[t]$ be a monic polynomial of degree $n \geqslant 3$ in t whose coefficients, e, are differentially independent over $\mathbb{k}$. Let α be transcendental over $\mathbb{F}$ with $D\alpha = 0$. Let $\sum_{m=0}^{n} \sum_{i=0}^{\Omega-m} \theta_{i,m} \alpha^i D^m y = 0$ be the αth power Cohnian of P. Then the logarithmic derivative, $u_i \equiv \frac{Dz_i}{z_i}$, of z_i satisfies the nonzero inhomogeneous first-power differential equation, $R_u(u) = 0$, where $R_u(t) \equiv \sum_{m=1}^{n} \theta_{0,m} D^{m-1} t + \theta_{1,0}$. Furthermore, u satisfies the algebraic equation, $P_u(u) = 0$, where $P_u(t) \equiv \sum_{m=0}^{n} \theta_{\Omega-m,m} t^m$.*

Proof. We have $Dy = \alpha \cdot y \cdot u$. Then $D^2 y = \alpha \cdot Dy \cdot u + \alpha \cdot y \cdot Du = \alpha \cdot (\alpha \cdot y \cdot u) \cdot u + \alpha \cdot y \cdot Du$. So $D^2 y = y \cdot (\alpha^2 u^2 + \alpha Du)$. We need one more differentiation to start the induction that follows.

$$\begin{aligned}D^3y &= Dy\cdot(\alpha^2u^2+\alpha Du)+y\cdot(2\alpha^2u\cdot Du+\alpha D^2u)\\ &= y\cdot\alpha\cdot u\cdot(\alpha^2u^2+\alpha Du)+y\cdot(2\alpha^2u\cdot Du+\alpha D^2u)\\ &= y\cdot(\alpha\cdot D^2u+\alpha^2\cdot(3u\cdot Du)+\alpha^3u^3).\end{aligned}$$

Let $g_{2,3}\equiv 3u\cdot Du$. We have proven that there exist $g_{j,m}\in\mathbb{Z}\{e,u\}$ such that $D^my=y\cdot(\alpha\cdot D^{m-1}u+\sum_{j=2}^{m-1}\alpha^jg_{j,m}+\alpha^mu^m)$ when $m=3$.

Now assume that there exist $g_{j,m}\in\mathbb{Z}\{e,u\}$ such that $D^my=y\cdot(\alpha\cdot D^{m-1}u+\sum_{j=2}^{m-1}\alpha^jg_{j,m}+\alpha^mu^m)$ holds true for some $m\geqslant 3$. We will prove that there exist $g_{j,m+1}\in\mathbb{Z}\{e,u\}$ such that the formula is true for $m+1$. It should be emphasized that we are not simply rederiving the partial Bell polynomial formulae for the mth derivative of a power of z. We need to relate the derivatives of y and z to the derivatives of u, the logarithmic derivative of z.

$$\begin{aligned}D^{m+1}y &= y\cdot\left(\alpha\cdot D^mu+\sum_{j=2}^{m-1}\alpha^jDg_{j,m}+\alpha^mm\cdot u^{m-1}Du\right)\\ &\quad+(Dy)\cdot\left(\alpha\cdot D^{m-1}u+\sum_{j=2}^{m-1}\alpha^jg_{j,m}+\alpha^mu^m\right)\\ &= y\cdot\left(\alpha\cdot D^mu+\sum_{j=2}^{m-1}\alpha^j\cdot Dg_{j,m}+\alpha^mm\cdot u^{m-1}Du\right)\\ &\quad+(y\cdot\alpha\cdot u)\cdot\left(\alpha\cdot D^{m-1}u+\sum_{j=2}^{m-1}\alpha^jg_{j,m}+\alpha^mu^m\right)\\ &= y\cdot\left(\alpha\cdot D^mu+\sum_{j=2}^{m-1}\alpha^jDg_{j,m}+\alpha^mmu^{m-1}Du+\alpha^2u\cdot D^{m-1}u\right.\\ &\quad\left.+\sum_{j=2}^{m-1}\alpha^{j+1}g_{j,m}u+\alpha^{m+1}u^{m+1}\right)\\ &= y\cdot\left(\alpha\cdot D^mu+\sum_{j=2}^{m}\alpha^jg_{j,m+1}+\alpha^{m+1}u^{m+1}\right)\end{aligned}$$

where $g_{j,m+1}\equiv Dg_{j,m}+g_{j-1,m}u$ for each $j\in[m-1]$ with $j\geqslant 3$, $g_{m,m+1}\equiv m\cdot u^{m-1}\cdot Du+g_{m-1,m}u$, and $g_{2,m+1}\equiv Dg_{2,m}+u\cdot D^{m-1}u$. Hence $g_{j,m+1}\in\mathbb{Z}\{e,u\}$ for each $j\in[m]$ with $j\geqslant 2$.

Substitute this expression for $D^m y$ into the Cohnian of P, $\sum_{m=0}^{n} \sum_{i=0}^{\Omega-m} \theta_{i,m}\alpha^i D^m y = 0$. We get

$$\begin{aligned} 0 &= y \cdot \sum_{m=3}^{n} \sum_{i=0}^{\Omega-m} \theta_{i,m}\alpha^i \cdot \left(\alpha D^{m-1} u + \sum_{j=2}^{m-1} \alpha^j g_{j,m} + \alpha^m u^m \right) \\ &\quad + y \cdot \sum_{i=0}^{\Omega-2} \theta_{i,2} \cdot \alpha^i \cdot (\alpha D^1 u + \alpha^2 u^2) + y \cdot \sum_{i=0}^{\Omega-1} \theta_{i,1} \cdot \alpha^i \cdot (\alpha \cdot u) + y \cdot \sum_{i=1}^{\Omega} \theta_{i,0} \cdot \alpha^i \\ &\quad \text{if } n \geqslant 3. \end{aligned}$$

Since α is transcendental over $\mathbb{Z}\{e\}$, the coefficient in this expression of each power of α must be zero. The lowest power of α in this expression is 1. Setting the coefficient of α^1 to zero yields $\sum_{m=1}^{n} \theta_{0,m} D^{m-1} u + \theta_{1,0} = 0$, an inhomogeneous linear differential equation over $\mathbb{Z}\{e\}$ which u satisfies. The highest power of α in this expression is Ω. Setting the coefficient of α^{Ω} to zero yields $\sum_{m=0}^{n} \theta_{\Omega-m,m} u^m = 0$, an algebraic equation for u. The hypothesis that the z are differentially independent over $\Bbbk$ guarantees that $\theta_{i,m} \neq 0$, $\forall (i,m) \neq (0,0)$ such that $i \in [\Omega - m]_0$ for each $m \in [n]_0$ by Theorem 41 on pp. 74–91 in [5] or Theorem 4.1 on p. 726 in [6]. Hence, the inhomogeneous resolvent, $R_u(t) \equiv \sum_{m=1}^{n} \theta_{0,m} D^{m-1} t + \theta_{1,0}$, and the polynomial, $P_u(t) \equiv \sum_{m=0}^{n} \theta_{\Omega-m,m} t^m$, are not identically zero. $\square$

Theorem 1 shows that the lowest power of α in the Cohnian yields a LODE over $\mathbb{Z}\{e\}$ satisfied by u, while the highest power of α in the Cohnian yields an algebraic equation over $\mathbb{Z}\{e\}$ satisfied by u. It is worthwhile at this point to mention the various relations between the coefficients, e, of t in $P(t) \equiv \prod_{i=1}^{n} (t - z_i) = \sum_{i=0}^{n} (-1)^{n-i} e_{n-i} t^i$, the coefficient functions $\theta_{i,m} \in \mathbb{Z}\{e\}$ in the αth-power Cohnian, $\sum_{m=0}^{n} \sum_{i=0}^{\Omega-m} \theta_{i,m}\alpha^i D^m y = 0$, of P, and the coefficients, e^L, of t in the minimal polynomial, $P_L(t) \equiv h \cdot \prod_{i=1}^{n} (t - u_i) = h \cdot \prod_{i=1}^{n} (t - \frac{Dz_i}{z_i}) = h \cdot \sum_{i=0}^{n} (-1)^{n-i} e_{n-i}^L t^i$ of $u = \frac{Dz}{z}$ over $\mathbb{Z}[e, De]$. It is not hard to prove that $h \in \mathbb{Z}[\Delta, e_n]$. Here e_i^L is the ith elementary symmetric function of the u.

Observation 2. The polynomial, $P_u(t) \equiv \sum_{m=0}^{n} \theta_{\Omega-m,m} \cdot t^m$, defined in Theorem 1 is some $\mathbb{Z}\{e\}$-multiple of the minimal polynomial, $P_L(t)$, of u over $\mathbb{Z}[e, De]$, since $P_u(u) = 0$.

Observation 3. The LODE, $R_u(u) \equiv \sum_{m=1}^{n} \theta_{0,m} D^{m-1} u + \theta_{1,0} = 0$, is a first-power inhomogeneous resolvent for $P_u(t)$. It should follow that one could apply the Powersum Formula, p. 67 in [5], to the polynomial, $P_u(t)$, to get a first-power nth order homogeneous resolvent for u over the ring, $\mathbb{Z}\{e\}$. This resolvent will have a large common factor in $\mathbb{Z}\{e\}$ among all $n+1$ terms. After removing a sufficient portion of this factor, what remains will be a resolvent for $P_u(t)$ which will also be the derivative of $R_u(u) = 0$.

Observation 4. One can find $P_L(t)$ by taking the resultant of the polynomials, $\xi \cdot t - D\xi$, and $P(\xi)$, with respect to ξ. Here, $D\xi = \frac{-\sum_{i=0}^{n-1} (-1)^i De_{n-i} \cdot \xi^i}{\sum_{i=0}^{n-1} (-1)^i e_{n-1-i} \cdot (i+1) \cdot \xi^i}$ must be expressed as a polynomial in ξ. A formula for $D\xi$ as a polynomial in ξ of degree $n-1$ with coefficients in the ordinary ring, $\frac{1}{e_n \cdot \varDelta}\mathbb{Z}[e, De]$, can be obtained by a method identical to the method for obtaining a formula for $\frac{D\xi}{\xi}$ presented in Theorem 8 on p. 32 in [5].

It will be a fun exercise in Observation 6 to relate the coefficient, $\theta_{\Omega-m,m}$, of t^m in $P_u(t)$, as obtained from the Cohnian, to the $(n-m)$th elementary symmetric function, e_{n-m}^L, of the logarithmic derivatives, $\{u_i = \frac{Dz_i}{z_i}\}_{i=1}^n$. Let us give the coefficient, $\theta_{\Omega-m,m}$, the name g_m. First we need a well-known identity.

Lemma 5. *Let* $n \in \mathbb{N}$. *Let* $\{\eta_i\}_{i=1}^n$ *be* n *indeterminates algebraically independent over* $\mathbb{Z}$. *Let* $k \in [n]_0$. *Then* $F_k \equiv |\eta_i^j|_{\substack{i \in [n] \\ 0 \leqslant j \leqslant n, j \neq k}} = e_{n-k} \cdot a_\delta$, *where* $a_\delta = |\eta_i^j|_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant n-1}}$ *is defined on p. 40 in* [3] *as the alternant of* $\{\eta_i\}_{i=1}^n$, *and* e_{n-k} *is the* $(n-k)$*th elementary symmetric function of* $\{\eta_i\}_{i=1}^n$.

Proof. Let $P(t) \equiv \prod_{i=1}^n (t - \eta_i) = \sum_{k=0}^n (-1)^{n-k} e_{n-k} t^k$. Then $P(t) - t^n = \sum_{k=0}^{n-1} (-1)^{n-k} e_{n-k} t^k$. Replacing t with each of the indeterminates, $\{\eta_i\}_{i=1}^n$, yields a system of n equations, $-\eta_i^n = \sum_{k=0}^{n-1} (-1)^{n-k} e_{n-k} \eta_i^k$, for $i \in [n]$. Solving by Cramer's Rule for e_{n-k} yields $e_{n-k} = \frac{|\eta_i^j|_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant n, j \neq k}}}{|\eta_i^j|_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant n-1}}} = \frac{|\eta_i^j|_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant n, j \neq k}}}{a_\delta}$. Thus, $|\eta_i^j|_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant n, j \neq k}} = e_{n-k} \cdot a_\delta$. $\square$

Observation 6. Let $\mathbb{F}, \Bbbk, D, P, e_i, z_i, y_i, \alpha, u_i, P_u, P_L, e_i^L, t, g_m$ be as they were in Theorem 1 and in the remarks following Theorem 1. Let $\Delta_L \equiv \prod_{i<j}(u_i - u_j)^2 \in \dfrac{1}{e_n \cdot \Delta}\boldsymbol{Z}[e, De]$ be the discriminant of $P_L(\xi)$. Then we observe that $g_m = (-1)^m \sqrt{\frac{\varDelta_L}{\varDelta}} \varDelta^{2n-1} e_n^n e_{n-m}^L \div \vartheta$ where $\vartheta \in \mathbb{Z}\{e\}$ is the ratio of the resolvent, $\frac{(\sqrt{\varDelta})^{4n-3} e_n^{n-\alpha}}{\alpha^{n-1}} \cdot W_\alpha$, defined in Theorem 46 on pp. 95–98 in [5], to the Cohnian. This ratio, ϑ, is unknown, because the Cohnian is unknown for polynomials of degree greater than 3.

To see this, let y satisfy the differential equation, $\sum_{k=0}^n a_{k,\alpha} D^k y = 0$, where

$$a_{k,\alpha} = (-1)^k |D^i y_j|_{\substack{i \neq k \\ 1 \leqslant j \leqslant n}} = (-1)^k \left| y_j \sum_{l=1}^{i} (\alpha)_l B_{i,l} z_j^{-l} \right|_{i \neq k, 0} \left. y_j \right|_{1 \leqslant j \leqslant n}.$$

Here $p_{i,l}$ denotes the (i,x) partial Bell polynomial in $\{Dz_j, D^2z_j, \ldots, D^2z_j$ as defined on page 30 of [3]. This differential equation is not an αth-power resolvent for P, because its coefficient functions do not lie in $\mathbb{Z}\{e\}[\alpha]$. We have replaced q with α and z_j^q with y_j in Theorem 1. As explained in the proof of Theorem 46 on pp. 95–98 in [5], if we multiply $a_{k,\alpha}$ by $\frac{(\sqrt{\Delta})^{4n-3}e_n^{n-\alpha}}{\alpha^{n-1}}$ we get a differential resolvent of weight, $\varphi(n) = \frac{n(4n^2-5n+3)}{2}$. It is known that $\varphi(n)$ is strictly greater than the weight of the Cohnian for $n \in \{2,3\}$. Here, $e_n^{-\alpha} \equiv \prod_{j=1}^n y_j^{-1}$. Observe that the coefficient of the highest power of α in $a_{k,\alpha}$ is $(-1)^k e_n^\alpha |B_{i,i}z_j^{-i}|_{i \neq 0,k} \ 1|_{1 \leqslant j \leqslant n}$. So the coefficient of the highest power of α in $G_{k,\alpha} = a_{k,\alpha} \cdot \frac{(\sqrt{\Delta})^{4n-3}e_n^{n-\alpha}}{\alpha^{n-1}}$ is $G_k \equiv (-1)^k e_n^n (\sqrt{\Delta})^{4n-3} |B_{i,i}z_j^{-i}|_{i \neq 0,k} \ 1|_{1 \leqslant j \leqslant n}$. Since $B_{i,i} = (Dz)^i$, it follows that $G_k = (-1)^k e_n^n (\sqrt{\Delta})^{4n-3} |(Dz_j)^i z_j^{-i}|_{\substack{i \neq k \\ 1 \leqslant i \leqslant n}} \ 1|_{1 \leqslant j \leqslant n} = (-1)^k e_n^n (\sqrt{\Delta})^{4n-3} |(\frac{Dz_j}{z_j})^i|_{\substack{0 \leqslant i \leqslant n, i \neq k \\ 1 \leqslant j \leqslant n}}$.

There must exist a nonzero factor, $\vartheta \in \mathbb{Z}\{e\}$, such that $\vartheta \cdot \sum_{m=0}^n \sum_{i=0}^{\Omega-m} \theta_{i,m}\alpha^i D^m y = \sum_{k=0}^n G_{k,\alpha}D^k y$ whose weight equals the difference between the unknown minimal Cohnian weight, $w(\theta_{i,m})$, and $\varphi(n)$. Thus

$$g_k = (-1)^k e_n^n (\sqrt{\Delta})^{4n-3} \left| \left(\frac{Dz_j}{z_j} \right)^i \right|_{\substack{0 \leqslant i \leqslant n, i \neq k \\ j \in [n]}} \div \vartheta.$$

Then by Lemma 5 $|(\frac{Dz_j}{z_j})^i|_{\substack{0 \leqslant i \leqslant n, i \neq k \\ 1 \leqslant j \leqslant n}} = e_{n-k}^L \cdot \sqrt{\Delta_L}$. So, $g_k = (-1)^k e_n^n (\sqrt{\Delta})^{4n-3} e_{n-k}^L \cdot \sqrt{\Delta_L} \div \vartheta$, or

$$g_k = (-1)^k \sqrt{\frac{\Delta_L}{\Delta}} \Delta^{2n-1} e_n^n e_{n-k}^L \div \vartheta.$$

One can see that the form of g_k in Observation 6 is predictable, namely, that g_k equals the $(n-k)$th elementary symmetric function of $\{\frac{Dz_i}{z_i}\}_{i=1}^n$ times an expression that is independent of k. So $\sum_{k=0}^n g_k \cdot u^k = \left(\sqrt{\frac{\Delta_L}{\Delta}} \Delta^{2n-1} e_n^n \div \vartheta\right) \cdot \sum_{k=0}^n (-1)^k e_{n-k}^L \cdot u^k = \left(\sqrt{\frac{\Delta_L}{\Delta}} \Delta^{2n-1} e_n^n \div \vartheta\right) \cdot P_L(u) = 0$.

4. Linear relations of roots over the base field

For this section we will put aside differential algebra and deal only with the algebraic properties of a monic polynomial, $P(t) \equiv \sum_{i=0}^n (-1)^{n-i} e_{n-i} t^i$, whose coefficients, e, lie in some nondifferential field, $\mathbb{F}$, of characteristic 0. Let P be irreducible over $\mathbb{F}$ with transitive Galois group G. Let $q \in \mathbb{Z}^\#$. Let P have roots, $z \equiv \{z_i\}_{i=1}^n$, and let $y_i \equiv z_i^q$. For convenience, we will refer to the y_i as the roots themselves. One could probably prove the following theorems if one replaced the integer, q, with a differential indeterminate, α, satisfying $D\alpha = 0$ and y_i satisfying $\frac{Dy_i}{\alpha \cdot y_i} = \frac{Dz_i}{z_i}$. However, the Galois group is defined to act only on elements in the splitting field of P, i.e. only on integral powers of the roots, z. The Galois group of the minimal polynomial of y may be isomorphic to a proper subgroup of the Galois group, G, of P. So, it is important to keep in mind, in the following theorems, that G is a Galois group for the z, not the y, even though the linear relations appearing in the statements of the theorems involve the y.

Theorem 7. *Let $P, z, y, q, \mathbb{F}, G$ be as in the preceding paragraph. Let ω be a primitive nth root of unity. If G, as a permutation group on the roots, z, of P, contains an n-cycle, and the y are linearly dependent over $\mathbb{F}$, then $\exists j \in [n]$ such that $\sum_{i=1}^{n} \omega^{i \cdot j} \cdot y_i = 0$.*

Proof. Let g be an n-cycle in G. Let $\sum_{i=1}^{n} x_i \cdot y_i = 0$ be a nontrivial relation of the y over $\mathbb{F}$. For each $j \in [n]$ apply g^j to $\sum_{i=1}^{n} x_i \cdot y_i = 0$. We get $\sum_{i=1}^{n} x_i \cdot y_{g^j(i)} = 0$ for $j \in [n]$. This is a homogeneous system of n equations in the n elements, $\{x_i\}_{i=1}^{n}$, which are not all 0. Therefore, $|y_{g^j(i)}|_{(i \in [n]) \times (j \in [n])} = 0$.

But a determinant of this form, $|t_{g^j(i)}|_{i,j \in [n]}$, with $\{t_1, \ldots, t_n\}$ algebraically independent over $\mathbb{Q}$, is not identically zero. It is the determinant of a very special type of matrix, called a *circulant*. By a very elegant and simple proof given on pp. 486–487 in [4], we have the following formula for the determinant of a circulant, $|y_{g^j(i)}|_{(i \in [n]) \times (j \in [n])} = \prod_{j=1}^{n} \sum_{i=1}^{n} \omega^{i \cdot j} y_i$. Thus,

$$|y_{g^j(i)}|_{(i \in [n]) \times (j \in [n])} = 0 \Rightarrow \exists j \in [n] \ni \sum_{i=1}^{n} \omega^{i \cdot j} \cdot y_i = 0. \qquad \square$$

Corollary 8. *Let $P, z, y, q, \mathbb{F}, G, \omega$ be as in Theorem 7, with the added restrictions that $\omega \in \mathbb{F}$ and $\sum_{i=1}^{n} x_i \cdot y_i = 0$ is the only linear relation of the y over $\mathbb{F}$, up to multiples. Then $\exists j \in [n]$ and $\exists u \in \mathbb{F}$ such that $x_i = u \cdot \omega^{i \cdot j}$.*

Proof. If the y are linearly independent over $\mathbb{F}$, then $x_i = 0, \forall i \in [n]$ and $u = 0 \in \mathbb{F}$. Assume otherwise. By Theorem 7 $\exists j \in [n]$ such that $\sum_{i=1}^{n} \omega^{i \cdot j} \cdot y_i = 0$. Since $\omega \in \mathbb{F}$ it follows that $\omega^j \in \mathbb{F}$. By hypothesis, all other linear relations of the y over $\mathbb{F}$ are multiples of $\sum_{i=1}^{n} x_i \cdot y_i = 0$. Hence, $\exists u \in \mathbb{F}^{\#} \ni x_i = u \cdot \omega^{i \cdot j}$. $\square$

Corollary 8 suggests that it is necessary for a field, $\mathbb{F}$, to contain some root of unity in order for a unique nontrivial linear relation of the roots of an irreducible polynomial, P, to occur. Since $\text{char}(\mathbb{F}) = 0$ implies that $\mathbb{F}$ contains $\mathbb{Q}$, and hence ± 1, the existence (or possible nonexistence) of linear dependencies of the y over $\mathbb{F}$ becomes interesting only when $j \neq \frac{n}{2}$ or $j \neq n$ and $\mathbb{F}$ does not contain an nth root of unity. In this case, $\omega^j \notin \mathbb{Q}$, with $\omega \in \mathbb{C}$. Usually in differential algebra, the subfield of constants, $\mathbb{k}$, of $\mathbb{F}$ is chosen to be algebraically closed, so this situation does not arise. In order for Corollary 8 to hold for any irreducible polynomial over $\mathbb{F}$, it suffices to impose upon $\mathbb{F}$ the slightly more restrictive condition that $\Bbbk = \bar{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$.

We do not know how many of the relations, $\sum_{i=1}^{n} x_i \cdot y_{g^j(i)} = 0$, $\forall j \in [o(g)]$, where $o(g)$ is the order of g in G, for a given n-cycle, $g \in G$, or even how many of the relations, $\sum_{i=1}^{n} x_i \cdot y_{h(i)} = 0$, $\forall h \in G$, are linearly independent when G is transitive. It is unclear if the number of linearly independent relations depends upon particular properties of P itself or only upon its Galois group.

Theorem 7 has told us something about the form of linear relations of roots over $\mathbb{F}$ for those polynomials, P, whose Galois group, G, contains an n-cycle as a permutation group on the roots. Furthermore, we wish to return to the study of differential resolvents only of polynomials which are irreducible over the differential field generated by their coefficients, because a resolvent of a reducible polynomial may be constructed from resolvents of its irreducible factors. (For an idea of how this might be done, see Example 144, p. 219 in [5].) Hence, we will continue to examine polynomials only with transitive Galois groups. So, we now study those P with transitive G which do not contain an n-cycle. Let S_n denote the full symmetric group on n letters.

Example 9. $n = 2$. $G \approx S_2$ is the only transitive subgroup of S_2.

Example 10. $n = 3$. $G \approx S_3$ and $A_3 = \langle (123) \rangle$ are the only transitive subgroups of S_3. Both have an n-cycle = 3-cycle in them.

Example 11. $n = 4$. The transitive subgroups of S_4 are $S_4, A_4, V = \{I, (12)(34), (13)(24), (14)(23)\}$, $C = \langle (1234) \rangle$ and its conjugates, and $D = V \cup \{(12), (34), (1423), (1324)\}$ and its conjugates, which are Sylow 2-groups of order 8. All of these have a 4-cycle in them, except V.

Suppose $G \approx V$. If $\sum_{i=1}^{4} x_i \cdot y_i = 0$ is a nontrivial linear relation of the roots, y, of P, over $\mathbb{F}, x_i \in \mathbb{F}$, then $\sum_{i=1}^{4} x_i \cdot y_{g(i)} = 0, \forall g \in V$. Hence, we get the system of equations,

$$x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 = 0, \quad x_1y_2 + x_2y_1 + x_3y_4 + x_4y_3 = 0,$$

$$x_1y_3 + x_2y_4 + x_3y_1 + x_4y_2 = 0, \quad x_1y_4 + x_2y_3 + x_3y_2 + x_4y_1 = 0.$$

Hence, the following determinant, given on p. 489 in [4],

$$\begin{vmatrix} y_1 & y_2 & y_3 & y_4 \\ y_2 & y_1 & y_4 & y_3 \\ y_3 & y_4 & y_1 & y_2 \\ y_4 & y_3 & y_2 & y_1 \end{vmatrix} = (y_1 + y_2 - y_3 - y_4)(y_1 - y_2 + y_3 - y_4)(y_1 - y_2 - y_3 + y_4) \times (y_1 + y_2 + y_3 + y_4)$$

must be zero. Therefore, the sum of two of the roots must equal ± 1 times the sum of the other two roots. A similar relation holds on the x. Furthermore, the x must be square roots of unity, up to a common multiple. For example, $x_1 = x_2 = 1$ and $x_3 = x_4 = -1$.

So we have shown in Example 11 that a polynomial, P, of degree n, can have a regular, transitive, but not doubly transitive, Galois group, G, over a field, $\mathbb{F}$, such that G does not contain an n-cycle, and such that the coefficients in any nontrivial linear relation of the roots of P over $\mathbb{F}$ must be roots of unity up to a common multiple. In Example 16 we will construct a polynomial F of degree 6 over a field, $\mathbb{F}$, and a nontrivial linear relation of the roots of F which is not a multiple of a relation over roots of unity, such that the Galois group, G, of F over $\mathbb{F}$ is regular (i.e. $|G| = n = 6$), transitive but not doubly transitive, and contains no 6-cycle.

Example 12. $n = 5$. Here n is prime. With the help of the following lemma we may cover all cases where n is prime.

Lemma 13. *Let p be prime, and let $G \subseteq S_p$ be a transitive subgroup of S_p. Then G contains a p-cycle.*

Proof. Since G is transitive on $[p]$, we must have p divide the order of G. By Sylow's Theorems, G has a subgroup of order, p. Since p is prime, this subgroup is cyclic and must be generated by a p-cycle. $\square$

From Corollary 8 and Lemma 13 we immediately conclude that, if the degree, n, of P is prime, P is irreducible over its base field, $\mathbb{F}$, and there exists some nontrivial linear relation of the roots of P over $\mathbb{F}$, then there exists a linear relation of the roots of P over roots of unity. Hence, if the linear relation is unique, then it is a multiple of a relation over roots of unity, and $\mathbb{F}$ must contain the appropriate root of unity. We will show in the next section that when the Galois group is doubly transitive, an even more stringent condition than transitivity, then there exists at most one nontrivial relation over $\mathbb{F}$, up to multiples. In this relation, the roots of unity are all 1. In other words, the first powersum of the roots, p_1, is zero. Without any difficulty, we may generalize these statements to the qth powers of the roots to obtain the result that $p_q = 0$ is the only possible nontrivial relation of the roots over $\mathbb{F}$.

5. Doubly transitive Galois groups

Let g be a permutation on $[n]$. We say g *moves* an element, s, in $[n]$, if $g(s) = t \neq s$, $\{t, s\} \subset [n]$. We say g moves a subset, $\Gamma \subset [n]$, if g moves each $s \in \Gamma$, possibly out of Γ. Let G be a group acting on the set, $[n]$. Let $s \in [n]$. Then the *stabilizer of s in G* is defined to be $\{g \in G \ni g(s) = s\}$ and is denoted by G_s. A group, G, is said to be *regular* if G is isomorphic to a permutation group that acts transitively on $|G|$ elements.

Let $m \in \mathbb{N}$. A group, G, acting on a finite set, Γ, is said to be *m-transitive* on Γ if, for each pair of sets of m distinct elements, $\{a_i\}_{i=1}^{m} \subset \Gamma$ and $\{b_i\}_{i=1}^{m} \subset \Gamma$, there exists an element, $g \in G$, such that $g(a_i) = b_i$, $\forall i \in [m]$. A *2-transitive* group is said to be *doubly transitive*.

Lemma 14. *Let $n \in \mathbb{N}$ with $n \geqslant 3$. Let G act doubly transitively on the set $[n]$. Let $k \in [n]$. Then G_k, the stabilizer of k in G, acts transitively on $[n] - \{k\} \equiv \{j \in [n] \ni j \neq k\}$.*

Proof. Let $\{i,j\} \subset [n] - \{k\}$. Since G acts doubly transitively on $[n]$ there exists an element, $g \in G$, such that $g(i) = j, g(k) = k$. (Just let $m = 2, a_1 = i, a_2 = k, b_1 = j$, and $b_2 = k$ in the definition of doubly transitive.) But, $g(k) = k$ implies $g \in G_k$. Hence, $\exists g \in G_k \ni g(i) = j$. Hence, G_k acts transitively on $[n] - \{k\}$. □

Theorem 15 (Doubly Transitive Theorem). *Let $\mathbb{F}$ be a field of characteristic 0. Let $n \in \mathbb{N}$ with $n \geqslant 3$. Let $P(t) \equiv \sum_{i=0}^{n} (-1)^{n-i} e_{n-i} t^i \in \mathbb{F}[t]$ be a monic polynomial over $\mathbb{F}$ with roots, $z \equiv \{z_i\}_{i=1}^{n}$. Let G be the Galois group of P over $\mathbb{F}$. Suppose G acts doubly transitively on the roots, z. Let $q \in \mathbb{Z}^{\#}$. Define $y_i \equiv z_i^q$. Then $p_q \equiv \sum_{i=1}^{n} y_i = 0$ is the only possible nontrivial linear combination of the qth powers of the roots over $\mathbb{F}$, up to multiples.*

Proof. If one of the roots, say z_1, satisfied $z_1^q = f$ for some $f \in \mathbb{F}$, then the cyclotomic polynomial $t^q - f$ would have to divide $P(t)$ in the ring, $\mathbb{F}[t]$. Since $P(t)$ is monic and irreducible over $\mathbb{F}$ we would have $P(t) = t^q - f$. This is impossible unless we chose $q = n$. Even if $q = n$, by well-known theorems in abstract algebra usually proven for the cyclotomic polynomial, $\Phi_n(t) \equiv t^n - 1$, over the ground field, $\mathbb{Q}$, it is easy to conclude that $G \approx (\mathbb{Z}_n, +, 0)$, the cyclic additive group of order n. So G could not be doubly transitive. So from now on we may assume $y_i \equiv z_i^q \notin \mathbb{F}, \forall i \in [n]$.

The y could be linearly independent over $\mathbb{F}$. Suppose otherwise. Let $\sum_{i=1}^{n} x_i \cdot y_i = 0$ be a nontrivial linear combination of the qth powers of the roots over $\mathbb{F}$, so $x_i \in \mathbb{F}$, $\forall i \in [n]$. Let $\bar{e}_1 \equiv \sum_{k=1}^{n} x_k$ and $p_q \equiv \sum_{k=1}^{n} y_k$. Then $x_i \in \mathbb{F}$, $\forall i \in [n]$ implies $0 = g(0) = g(\sum_{i=1}^{n} x_i \cdot y_i) = \sum_{i=1}^{n} x_i \cdot y_{g(i)}$, $\forall g \in G$. For each $k \in [n]$, sum these equations over $g \in G_k$. Thus $\forall k \in [n]$, we have $\sum_{i=1}^{n} x_i \sum_{g \in G_k} y_{g(i)} = 0$.

For $i = k$, we have $\sum_{g \in G_k} y_{g(i)} = \sum_{g \in G_k} y_{g(k)} = \sum_{g \in G_k} y_k = |G_k| y_k = \frac{|G|}{n} y_k$. Thus $\forall k \in [n]$, we have $\frac{|G|}{n} y_k x_k + \sum_{i \neq k} x_i \sum_{g \in G_k} y_{g(i)} = 0$. Let $G_{ki} \equiv \{g \in G_k \ni g(i) = i\}$ be the stabilizer of i in G_k. By Lemma 14 G_k acts transitively on $[n] - \{k\}$. Hence $|G_{ki}| = \frac{|G_k|}{n-1} = \frac{|G|}{n(n-1)}$. Since G_k acts transitively on $[n] - \{k\}$, then for each integer, $j \in [n] - \{k\}$, there exists a $g_j \in G_k$ such that $g_j(i) = j$. Let $g_j G_{ki}$ be the coset of G_{ki} in G_k such that $h \in g_j G_{ki} \Rightarrow h(i) = j$. (So $g_i G_{ki} = G_{ki}$). Then, $\forall k \in [n], \frac{|G|}{n} y_k x_k +$

$\sum_{i\neq k} x_i \sum_{j\neq k} \sum_{h\in g_jG_{ki}} y_{h(i)} = 0 \Rightarrow \frac{|G|}{n} y_k x_k + \sum_{i\neq k} x_i \sum_{j\neq k} \sum_{h\in g_jG_{ki}} y_j = 0$

$$\Rightarrow \frac{|G|}{n} y_k x_k + \sum_{i\neq k} x_i \sum_{j\neq k} |g_jG_{ki}| y_j = 0 \Rightarrow \frac{|G|}{n} y_k x_k + \sum_{i\neq k} x_i \sum_{j\neq k} |G_{ki}| y_j = 0,$$

$$\Rightarrow \frac{|G|}{n} y_k x_k + \frac{|G|}{n(n-1)} \sum_{i\neq k} x_i \sum_{j\neq k} y_j = 0 \Rightarrow (n-1)\cdot y_k \cdot x_k + (\bar{e}_1 - x_k)\cdot(p_q - y_k) = 0,$$

$$\Rightarrow n\cdot y_k \cdot x_k + \bar{e}_1 \cdot p_q - x_k \cdot p_q - y_k \cdot \bar{e}_1 = 0.$$

If $p_q = 0$ then $0 = n\cdot y_k \cdot x_k - y_k \cdot \bar{e}_1 = y_k(n\cdot x_k - \bar{e}_1)$. Since $y_k \notin \mathbb{F}, \forall k \in [n]$, it follows that $y_k \neq 0$, $\forall k \in [n]$. Hence $n\cdot x_k - \bar{e}_1 = 0, \forall k \in [n] \Rightarrow \exists x \in \mathbb{F} \ni x_k = x$, $\forall k \in [n]$. Thus, other linear relations of the roots over the base field cannot exist.

If $p_q \neq 0$ then $n\cdot y_k \cdot x_k + \bar{e}_1 \cdot p_q - x_k \cdot p_q - y_k \cdot \bar{e}_1 = 0 \Rightarrow y_k = p_q \frac{\bar{e}_1 - x_k}{\bar{e}_1 - n\cdot x_k} \in \mathbb{F}$. But, this contradicts the hypothesis that $y_k \notin \mathbb{F}, \forall k \in [n]$. Hence, we must have both the numerators and the denominators of $p_q \cdot \frac{\bar{e}_1 - x_k}{\bar{e}_1 - n\cdot x_k}$ vanish. This implies $x_k = \bar{e}_1 = n\cdot x_k$, $\forall k \in [n] \Rightarrow x_k = 0$, $\forall k \in [n]$. □

6. Sextic example

Let G be the Galois group of the polynomial, $P(z) \equiv \sum_{i=0}^{n} (-1)^{n-i} e_{n-i} z^i$ over a field, $\mathbb{F}$, containing $\mathbb{Q}(e)$. Suppose G acts transitively on the roots, $\{z_i\}_{i=1}^{n}$, of P. Let $q \in \mathbb{Z}^{\#}$. Let $y_i \equiv z_i^q$. Let $\sum_{i=1}^{n} x_i \cdot y_i = 0$ be a linear combination of the qth powers of the roots over the base field, $x_i \in \mathbb{F}, \forall i \in [n]$. In Example 11 we had an example of a transitive, not doubly transitive, regular Galois group not containing an n-cycle in which the x had to be a common multiple of roots of unity. It is natural to ask if all the x always have to be a common multiple of roots of unity when these conditions are placed upon the Galois group. The following counterexample, suggested by Dr. Richard Cohn and developed by Nahay, disproves this conjecture. The x do not have to be a common multiple of roots of unity, when G is transitive, regular, not cyclic, and not doubly-transitive. However, in order to make this counterexample work, the base field, $\mathbb{F}$, must be a proper extension of the coefficient field, $\mathbb{Q}(e)$, of the polynomial.

Example 16. Let $\{a,b,c,u,v,w\}$ be algebraically independent over $\mathbb{Q}$. Let $e \equiv \{e_1,e_2,e_3\}$ and $p \equiv \{p_1,p_2,p_3\}$ be the first three elementary symmetric functions and powersums of $\{u,v,w\}$, respectively. Let $\bar{e} \equiv \{\bar{e}_1,\bar{e}_2,\bar{e}_3\}$ and $\bar{p} \equiv \{\bar{p}_1,\bar{p}_2,\bar{p}_3\}$ be the first three elementary symmetric functions and powersums of $\{a,b,c\}$, respectively. Define

$$\mu_1 \equiv au + bv + cw, \quad \mu_2 \equiv cu + av + bw, \quad \mu_3 \equiv bu + cv + aw,$$

$$\mu_4 \equiv bu + av + cw, \quad \mu_5 \equiv au + cv + bw, \quad u_6 \equiv cu + bv + aw.$$

Then $\mu \equiv \{\mu_1, \mu_2, \mu_3, \mu_4, \mu_5, \mu_6\}$ are the roots of the sixth degree polynomial $F(t) \equiv \prod_{g \in S_3} \left(t - \sum_{i=1}^{3} a_i u_{g(i)}\right)$ where we define $a_1 \equiv a,\ a_2 \equiv b,\ a_3 \equiv c,\ u_1 \equiv u,\ u_2 \equiv v$, and $u_3 \equiv w$. The coefficients of t in $F(t)$ are symmetric in $\{u, v, w\}$ and $\{a, b, c\}$ separately. Hence $F(t) \in \mathbb{Q}(e, \bar{e})[t]$.

Rather than choose our base field, $\mathbb{F}$, to be the coefficient field, $\mathbb{Q}(e, \bar{e})$, of F, we will choose $\mathbb{F}$ to be the larger field, $\mathbb{Q}(e, a, b, c)$. Then $[\mathbb{Q}(a, b, c, u, v, w) : \mathbb{F}] = 6$. We wish to prove that the Galois group, G, of $F(t)$ over $\mathbb{F}$ is isomorphic to S_3.

First let us prove that the splitting field, $\mathbb{F}(\mu)$, of $F(t)$ equals $\mathbb{F}(u, v, w)$. Clearly $\mathbb{F}(\mu) \subset \mathbb{F}(u, v, w)$. To prove the reverse inclusion, we must show that $\{u, v, w\}$ can be expressed in terms of μ and $\{a, b, c\}$. We can solve the system $\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} \cdot \begin{bmatrix} u \\ v \\ w \end{bmatrix} = \begin{bmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \end{bmatrix}$ for $\{u, v, w\}$ because $\det \begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix} = \bar{p}_3 - 3\bar{e}_3 \neq 0$. Furthermore, the μ are all conjugate under H, the Galois group of the polynomial $P(t) \equiv (t - u) \cdot (t - v) \cdot (t - w)$ over $\mathbb{Q}(e)$, by their construction as linear combinations of elements, $\{u, v, w\}$, which are conjugate under H. Therefore, the μ's automorphism group over $\mathbb{F}$, their Galois group, G, is isomorphic to $H \approx S_3$. Hence $[\mathbb{F}(\mu) : \mathbb{F}] = 6 = [\mathbb{F}(u, v, w) : \mathbb{F}]$. Combine this result with $\mathbb{F}(\mu) \subset \mathbb{F}(u, v, w)$ to get $\mathbb{F}(\mu) = \mathbb{F}(u, v, w)$.

We may also simply say that we are extending both the coefficient field, $\mathbb{Q}(e)$, and splitting field, $\mathbb{Q}(u, v, w)$, of P to a new base field, $\mathbb{F} = \mathbb{Q}(e)(a, b, c)$, and a new splitting field, $\mathbb{Q}(u, v, w)(a, b, c)$, by the adjunction of algebraically independent indeterminates, $\{a, b, c\}$. By a basic property of Galois groups, the Galois group of $\mathbb{Q}(u, v, w)$ over $\mathbb{Q}(e)$ is isomorphic to the Galois group of $\mathbb{F}(u, v, w)$ over $\mathbb{F}$.

We need to prove that G acts transitively on the set of roots, μ. By an elementary theory of groups acting on sets, we need to prove only that $G\mu_1 = \{\mu_1, \ldots, \mu_6\}$ for one of the roots, μ_1. But this follows directly from the definition of the μ.

Finally, G is not doubly transitive since $6 = |S_3| = |G| < n \cdot (n - 1) = 6 \cdot 5 = 30$. Let the letter, n, represent the degree of F, which is 6, and not the degree of P, which is 3. Then we have exhibited a sixth degree polynomial, F, whose Galois group is transitive but not doubly transitive, whose order equals the degree, $n = 6$, of the polynomial (a regular group), and which does not contain an n-cycle.

Now we must prove that there exists a linear relation, $\sum_{i=1}^{6} x_i \cdot \mu_i = 0$, of the roots of $F(t)$ over elements, $x \equiv \{x_i\}_{i=1}^{6}$, in $\mathbb{F}$ which is not a multiple of a relation, $\sum_{i=1}^{6} \tilde{x}_i \cdot \mu_i = 0$, in which the $\tilde{x} \equiv \{\tilde{x}_i\}_{i=1}^{6}$ are all roots of unity. Since the only roots of unity in $\mathbb{Q}$ are ± 1, this implies $\tilde{x} \subset \{\pm 1\}$.

Let $\sum_{i=1}^{6} x_i \cdot \mu_{g(i)} = 0$ be a set of six linear relations over elements, $x \in \mathbb{F}$. The first three of these six linear relations, say, generated by the subgroup $\langle (u \to v \to w \to u) \rangle \subset S_3$, are created by the action $\mu_1 \to \mu_2 \to \mu_3 \to \mu_1$ and $\mu_4 \to \mu_6 \to \mu_5 \to \mu_4$. They may be written as a system of three linear equations in the three variables, $\{x_1, x_2, x_3\}$,

$$\begin{bmatrix} \mu_1 & \mu_2 & \mu_3 \\ \mu_2 & \mu_3 & \mu_1 \\ \mu_3 & \mu_1 & \mu_2 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = - \begin{bmatrix} \mu_4 & \mu_5 & \mu_6 \\ \mu_6 & \mu_4 & \mu_5 \\ \mu_5 & \mu_6 & \mu_4 \end{bmatrix} \cdot \begin{bmatrix} x_4 \\ x_5 \\ x_6 \end{bmatrix}.$$

We note that

$$\det \begin{bmatrix} \mu_1 & \mu_2 & \mu_3 \\ \mu_2 & \mu_3 & \mu_1 \\ \mu_3 & \mu_1 & \mu_2 \end{bmatrix} = -(\mu_1^3 + \mu_2^3 + \mu_3^3 - 3\mu_1\mu_2\mu_3)$$
$$= -\bar{p}_3 \cdot p_3 - 9 \cdot \bar{e}_3 \cdot e_3 + 3 \cdot (\bar{e}_3 \cdot p_3 + \bar{p}_3 \cdot e_3) = -(p_3 - 3 \cdot e_3) \cdot (\bar{p}_3 - 3 \cdot \bar{e}_3)$$
$$= -e_1 \cdot \bar{e}_1 \cdot (e_1^2 - 3 \cdot e_2) \cdot (\bar{e}_1^2 - 3 \cdot \bar{e}_2).$$

Since $\{a, b, c\}$ are algebraically independent over $\mathbb{Q}$, their first three elementary symmetric functions are algebraically independent over $\mathbb{Q}$. So $\bar{e}_1 \neq 0$ and $(\bar{e}_1^2 - 3 \cdot \bar{e}_2) \neq 0$. Similarly, e_1 and e_2 are algebraically independent over $\mathbb{Q}$. Therefore $e_1 \neq 0$ and $e_1^2 - 3e_2 \neq 0$. Therefore $\det \begin{bmatrix} \mu_1 & \mu_2 & \mu_3 \\ \mu_2 & \mu_3 & \mu_1 \\ \mu_3 & \mu_1 & \mu_2 \end{bmatrix} \neq 0$.

To determine how many of the x may be chosen arbitrarily, we must determine the rank of the system, $\sum_{i=1}^{6} x_i \cdot \mu_{g(i)} = 0$. If the rank of the matrix, $[\mu_{g(i)}]_{g \times i}$, is 3, then we may solve for $\{x_1, x_2, x_3\}$ uniquely in terms of $\{x_4, x_5, x_6\}$, and $\{x_4, x_5, x_6\}$ may be chosen arbitrarily in $\mathbb{F}$. Define $d \equiv (\bar{p}_2 - \bar{e}_2) = (\bar{e}_1^2 - 3 \cdot \bar{e}_2)$, $k_a \equiv (a - b) \cdot (a - c)$, $k_b \equiv (b - c) \cdot (b - a)$, and $k_c = (c - a) \cdot (c - b)$. Note that $d \in \mathbb{Q}(a, b, c) \subset \mathbb{F}$.

According to the Mathematica program at the end of this article the first three equations are equivalent to the three equations $x_1 = -\frac{1}{d}(k_b \cdot x_4 + k_a \cdot x_5 + k_c \cdot x_6)$, $x_2 = -\frac{1}{d}(k_c \cdot x_4 + k_b \cdot x_5 + k_a \cdot x_6)$, and $x_3 = -\frac{1}{d}(k_a \cdot x_4 + k_c \cdot x_5 + k_b \cdot x_6)$. The transposition, $(u \leftrightarrow v)$, induces the action $(\mu_1 \leftrightarrow \mu_4)(\mu_2 \leftrightarrow \mu_5)(\mu_3 \leftrightarrow \mu_6)$ on the roots of F. Applying this action to the first three equations yields the last three equations. But the action of $(u \leftrightarrow v)$ on $d \cdot x_1 = -(k_b \cdot x_4 + k_a \cdot x_5 + k_c \cdot x_6)$, $d \cdot x_2 = -(k_c \cdot x_4 + k_b \cdot x_5 + k_a \cdot x_6)$, and $d \cdot x_3 = -(k_a \cdot x_4 + k_c \cdot x_5 + k_b \cdot x_6)$ leaves these equivalent equations unchanged. Therefore, the last three equations have the same equivalent equations as the first three. Therefore the rank of $[\mu_{g(i)}]_{g \times i}$ is 3. So we may choose x_4, x_5, x_6 arbitrarily in $\mathbb{F} = \mathbb{Q}(e, a, b, c)$.

Choosing $x_4, x_5, x_6 \in \mathbb{Q}(a, b, c)$ guarantees that $x_1, x_2, x_3 \in \mathbb{Q}(a, b, c)$ since $d \in \mathbb{Q}(a, b, c)$, so all x will lie in $\mathbb{F}$. Since we may choose $\{x_4, x_5, x_6\}$ not to be a common multiple of roots of unity, we have demonstrated the existence of a polynomial, F, a field, $\mathbb{F}$, containing the coefficient field of F, and a linear relation of the roots of F over $\mathbb{F}$ which is not a multiple of a relation over roots of unity and such that the Galois group of F over $\mathbb{F}$ is transitive, not doubly transitive, regular, and does not contain an n-cycle.

So we proved there exists a linear relation, $\sum_{i=1}^{6} x_i \cdot \mu_i = 0$, for the roots, μ, of F, over $\mathbb{F} = \mathbb{Q}(e, a, b, c)$ with coefficients which are not all roots of unity (in $\mathbb{Q}$ this means not all ± 1), up to a common multiple. However, the coefficients of $F(t)$ lie in the smaller field, $\mathbb{Q}(e, \bar{e})$. If we want all the x to lie in $\mathbb{Q}(e, \bar{e})$, then, as can be seen from the formulae $d \cdot x_1 = -(k_b \cdot x_4 + k_a \cdot x_5 + k_c \cdot x_6)$, $d \cdot x_2 = -(k_c \cdot x_4 + k_b \cdot x_5 + k_a \cdot x_6)$, $d \cdot x_3 = -(k_a \cdot x_4 + k_c \cdot x_5 + k_b \cdot x_6)$, we must take $x_1 = x_2 = x_3 = -x_4 = -x_5 = -x_6$, so that $\sum_{j=1}^{6} x_j \cdot \mu_j = 0$ is a multiple of the relation $\sum_{j=1}^{3} \mu_j - \sum_{j=3}^{6} \mu_j = 0$.

It remains a conjecture whether there exists a field, $\mathbb{F}$, and a polynomial, $F(t) \in \mathbb{F}[t]$, such that $\mathbb{F}$ is the smallest field containing the coefficients of F, the Galois group of F over $\mathbb{F}$ is transitive but not doubly-transitive, and there exist linear relations of the roots of F over $\mathbb{F}$ which are not multiples of relations over roots of unity.

7. Linear dependence over constants

We once again return to differential algebra. In Example 16 we may turn the ordinary field, $\mathbb{Q}(a, b, c, u, v, w)$, into the differential field, $\mathbb{Q}\langle a, b, c, u, v, w\rangle$, by adding a derivation, D, such that $Da = Db = Dc = 0$, and so $D\bar{e}_1 = D\bar{e}_2 = D\bar{e}_3 = 0$, and all the derivatives of $\{u, v, w\}$, which are assumed to be differentially independent over $\mathbb{Q}(a, b, c)$. Likewise, we add all the derivatives of the first three elementary symmetric functions of $\{u, v, w\}$, $e = \{e_1, e_2, e_3\}$, to the ordinary field, $\mathbb{F} = \mathbb{Q}(e, a, b, c)$, to get the differential field, $\mathbb{F} = \mathbb{Q}\langle e, a, b, c\rangle = \mathbb{Q}\langle e\rangle(a, b, c)$. We now say that the coefficients of the polynomial, $F(t) \equiv \prod_{i=1}^{6} (t - \mu_i)$, lie in the differential field, $\mathbb{Q}\langle e, \bar{e}\rangle = \mathbb{Q}\langle e\rangle(\bar{e}) \subset \mathbb{F}$. The constant subfield of $\mathbb{F}$ is $\mathbb{k} = \mathbb{Q}\langle a, b, c\rangle = \mathbb{Q}(a, b, c)$.

Can we find a linear relation, $\sum_{i=1}^{6} x_i \cdot \mu_i = 0$, for the roots μ of F over (any) constants (not just in $\mathbb{k}$), which is not a multiple of a relation over roots of unity? In Example 16, we showed that we could do this, that we could choose all $x \subset \mathbb{Q}(a, b, c)$ satisfying this property. However, if we seek constants, x, in the smaller field of constants, $\mathbb{Q}\langle \bar{e}\rangle = \mathbb{Q}(\bar{e}) \subset \mathbb{k}$, then, by the remarks following Example 16, the relation, $\sum_{j=1}^{6} x_j \cdot \mu_j = 0$, would be a $\mathbb{k}$-multiple of the relation, $\sum_{j=1}^{3} \mu_j - \sum_{j=3}^{6} \mu_j = 0$.

Likewise, we may rephrase the conjecture following Example 16 in the following way. Does there exist a differential field, $\mathbb{F}$, with subfield of constants, $\mathbb{k}$, and a polynomial, $F(t) \in \mathbb{F}[t]$, such that $\mathbb{F}$ is the smallest differential field containing the coefficients of F, the Galois group of F over $\mathbb{F}$ is transitive but not doubly transitive, and there exist linear relations of the roots of F over $\mathbb{k}$ which are not multiples of relations over roots of unity?

In Example 16, G is transitive but not doubly transitive and $\mathbb{k} = \mathbb{Q}(a, b, c)$ is not algebraically closed. As mentioned after Corollary 8, fields of constants are usually taken to be algebraically closed in differential algebra. We saw that there can exist a linear relation of the roots over constants which is not a multiple of a relation over roots of unity. But, in this example such constants could not lie in the smallest differential field, $\mathbb{Q}\langle e, \bar{e}\rangle$, generated by the coefficients of F. Even if we took $\Bbbk$ to be the algebraic closure of $\mathbb{Q}(a, b, c)$ and took the base field, $\mathbb{F}$, of the Galois group, G, of F to be $\Bbbk\langle e\rangle$, the result would be the same: any relation of the roots of F over constants in $\mathbb{Q}\langle e, \bar{e}\rangle$, i.e. over $\Bbbk \cap \mathbb{Q}\langle e, \bar{e}\rangle = \mathbb{Q}(\bar{e})$, will be a multiple of a relation over roots of unity.

However, we may conclude the following result concerning linear relations of the roots over constants. By Theorem 15, if G is doubly transitive and $p_q \neq 0$, then the qth powers of the roots are linearly independent over $\Bbbk$ (trivially, since Theorem 15 implies the z^q are linearly independent over $\mathbb{F}$, and $\Bbbk \subset \mathbb{F}$). We remind the reader that there may exist relations over constants in some extension of $\Bbbk$.

8. Finite number of powers for linear denpendencies

We now return to the previous notation where $\mathbb{F}$ is a differential field of characteristic 0, with derivation, D, and subfield of constants, $\Bbbk$, and $P(t) \in \mathbb{F}[t]$ is a monic polynomial of degree n with coefficients, $e \equiv \{e_i\}_{i=1}^n$, and roots, $z \equiv \{z_i\}_{i=1}^n$.

The next theorem, Theorem 17, demonstrates that the condition that there exist linear relations of the qth powers of the roots, $y \equiv \{z_i^q\}_{i=1}^n$, over $\Bbbk$ is a very rare condition indeed. A result similar to this has been proven recently by Cattani, D'Andrea and Dickenstein using A-hypergeometric series. In [1], they showed that for the trinomial polynomial, $z^n + (-1)^{n-r} e_{n-r} z^r + (-1)^n e_n = 0$, where r and n are coprime and e_{n-r} and e_n are differentially independent over $\mathbb{Q}$, the only possible linear relation among the y is $\sum_{i=1}^n y_i = 0$. We will combine our result with basic LODE theory (namely, that nth order LODEs have at most n solutions linearly independent over $\Bbbk$) to obtain a powerful result: the order of a qth power resolvent of a polynomial of degree n, for which no root is a constant multiple of another, is at least n for all but finitely many integers q and at least n for an αth power resolvent.

To do this we will now re-introduce some notation which was used in [5] to prove the existence and form of resolvents. For each $m \in \mathbb{N}_0$ let $\mathbb{Z}\{e\}_m$ denote the ordinary (non-differential) ring generated by the e and their derivatives up through mth order. Let $(t)_m \equiv \prod_{i=0}^{m-1}(t-i)$ if $m > 0$ and $(t)_0 \equiv 1$. The symbol Δ denotes the discriminant of the polynomial, P. By Theorem 32 on p. 60 in (5) for each $m \in \mathbb{N}$ there exists a polynomial, $G_m(t, \alpha) \in \mathbb{Z}\{e\}_m[(n! \cdot \Delta \cdot e_n)^{-1}, t, \alpha]$, independent of the choice of roots, z, such that $D^m y = \alpha \cdot y \cdot G_m(z, \alpha)$ holds for each of the roots, z, and $\deg_\alpha G_m(t, \alpha) = m - 1$ where $\deg_\alpha G_m(t)$ denotes the degree of α in the polynomial, $G_m(t, \alpha)$. Here, y depends on the choice of z through $\alpha \cdot y \cdot Dz - z \cdot Dy = 0$.

Define $G_0(t; \alpha) \equiv 1$.

Theorem 17. *Let* $\mathbb{F}$ *be a differential field of characteristic* 0 *with derivation*, D, *and subfield of constants*, $\Bbbk$. *Let* $P(t) \in \mathbb{F}[t]$ *be a polynomial of degree n which is irreducible over* $\mathbb{F}$. Let $\{z_i\}_{i=1}^n$ *be the roots of P. Then either*

(1) *$\{z_i^q\}_{i=1}^n$ are linearly independent over $\Bbbk$ for all but finitely many integers, $q \in \mathbb{Z}$, or*
(2) *one root is a constant multiple of another.*

These conditions are mutually exclusive.

Proof. For indeterminates, t and α, where α is a transcendental constant over $\mathbb{F}$, let $G_m(t,\alpha)$ be defined as in Theorem 32 on p. 60 in [5] and in the paragraph preceding this theorem. We will prove that if $|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ i\in U}} = 0$ for some $k \in [n]_0$ and some subset, $U \subset [n]$, such that $|U| = k+1$, then one root of P is a constant multiple of another. Here, $|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ i\in U}}$ denotes the determinant of the matrix whose rows are labelled by m and whose columns are labelled by i and whose entries are $G_m(z_i,\alpha)$. If $k=0$, then we have $0 = |G_0| = |1|$, a contradiction.

So suppose $|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ i\in U}} = 0$ for some $k \in [n]$ and some subset, $U \subset [n]$, such that $|U| = k+1$. This implies the coefficient of $\alpha^{\frac{k(k-1)}{2}}$ in $|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ 1\in U}}$ is zero. By the Y-Bell Theorem, Theorem 36 on p. 65 in [5], $G_m(z_i,\alpha) = \sum_{k=1}^m B_{m,k}(Dz_i,\ldots)\cdot(\alpha-1)_{k-1}\cdot z_i^{-k}$ for $m>0$. By Theorem 32 on p. 60 in [5] we have $\deg_\alpha G_m(z_i,\alpha) = m-1$ for $m>0$ and $\deg_\alpha G_0(z_i,\alpha) = 0$. So $\deg_\alpha(|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ i\in U}}) \leqslant \sum_{m=1}^k (m-1) = \frac{k\cdot(k-1)}{2}$. So the coefficient of $\alpha^{\frac{k\cdot(k-1)}{2}}$ in $|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ i\in U}}$ is $|B_{m,m}(Dz_i)\cdot z_i^{-m}|_{\substack{0\leqslant m\leqslant k\\ i\in U}} = |(\frac{Dz_i}{z_i})^m|_{\substack{0\leqslant m\leqslant k\\ i\in U}}$. This implies $|(\frac{Dz_i}{z_i})^m|_{\substack{0\leqslant m\leqslant k\\ i\in U}} = 0$. This implies $\frac{Dz_i}{z_i} = \frac{Dz_j}{z_j}$ for some roots, z_i and z_j with $i \neq j, \{i,j\} \subset U$. This implies there exists a constant, $\gamma \in \Bbbk$, such that $z_i = \gamma\cdot z_j$, i.e. one root is a constant multiple of another.

Therefore, if no root is a constant multiple of another root, then $|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ i\in U}} \neq 0$ for each $k \in [n]_0$ and any subset, $U \subset [n]$, such that $|U| = k+1$. But $|G_m(z_i,\alpha)|_{\substack{0\leqslant m\leqslant k\\ i\in U}}$ is a polynomial in α. Therefore, it can equal zero for only finitely many values of α, and therefore for only finitely many integer values, q, of α, if any. Therefore, if no root is a constant multiple of another root, then $|G_m(z_i,q)|_{\substack{0\leqslant m\leqslant k\\ i\in U}} \neq 0$ for each $k \in [n]_0$ and any subset, $U \subset [n]$, such that $|U| = k+1$ for all but finitely many integers, q.

Assume no root is a constant multiple of another. Assume there exists an infinite set, $\Gamma \subset \mathbb{Z}^\#$, such that the z_i^q are linearly dependent, $\sum_{i=1}^n c_i(q)\cdot z_i^q = 0$, over constants, $c_i(q)$, for all q in Γ. We will obtain a contradiction. The existence of Γ implies there exists a subset, U, of $[n]$ such that the roots, $\{z_i^q\}_{i\in U}$, are linearly dependent over constants for all q in some infinite subset, $\Lambda \subset \Gamma$, and no proper subset of U has this property. Choose the notation so that $U = [k+1]$ for some $k \in [n]_0$.

Differentiate the relations, $\sum_{i\in U} c_i(q)\cdot z_i^q = 0$, k times. One gets for each $m \in [k]$, after dividing out by one power of q, the relations, $\sum_{i\in U} c_i(q)\cdot z_i^q \cdot G_m(z_i,q) = 0$, where $G_m(t,q) \in \Bbbk[t,q] = \Bbbk[t]$. Since the hypothesis that no root is a constant multiple of another implies that no root is zero, and $z_i \neq 0,\ \forall i \in [n] \Leftrightarrow z_i^q \neq 0,\ \forall i \in [n],\ \forall q \in \Gamma$, it follows that $z_i^q \neq 0, \forall i \in U \subset [n], \forall q \in \Lambda \subset \Gamma$. So these relations imply that $0 = |c_i(q) \cdot G_m(z_i,q)|_{\substack{0 \leqslant m \leqslant k \\ i \in U}} = (\prod_{i=1}^n c_i(q))|G_m(z_i,q)|_{\substack{0 \leqslant m \leqslant k \\ i \in U}},\ \forall q \in \Lambda$. Since $|G_m(z_i,q)|_{\substack{0 \leqslant m \leqslant k \\ i \in U}} \neq 0$ for all but finitely many $q \in \Lambda$, it follows that there exists a root, $z_{i'}$, with $i' \in U$ such that $c_{i'}(q) = 0,\ \forall q \in \Lambda'$ for some infinite subset, $\Lambda' \subset \Lambda$. But this implies the $\{z_i^q\}_{i \in U, i \neq i'}$ are linearly dependent over constants $\forall q \in \Lambda'$, contradicting the minimality of U with this property. □

9. Minimal order of resolvents

If R_α is an αth power resolvent for an nth degree polynomial, P, over a d-field, $\mathbb{F}$, then, by definition of an αth power resolvent, R_α is a polynomial in α. Therefore, there exist at most finitely many $q \in \mathbb{Z}$ such that some or all of the coefficient functions of $R_q \equiv \phi_q(R_\alpha)$ vanish, where $\phi_q : \mathbb{F}(\alpha) \to \mathbb{F}$ is the differential specialization such that $\phi_q(\alpha) = q$ and $\phi_q(u) = u$ for each $u \in \mathbb{F}$. By the Powersum Satisfaction Theorem, Theorem 35 on p. 64 in [5], R_q is a qth power resolvent for P. This suggests, but does not prove, that if no roots of P have a constant ratio, then for all but finitely many integers, q, the order of a qth power resolvent of P is greater than or equal to n. Theorem 18 immediately asserts this result.

Theorem 18. *Let P be an nth degree polynomial over a d-field*, $\mathbb{F}$, *for which no two roots have a constant ratio. Then for all but finitely many integers*, q, *the order of any qth power resolvent of P is greater than or equal to n.*

Proof. By Theorem 17 for all but finitely many $q \in \mathbb{Z}$ there exist no nontrivial linear relations over constants of the qth power of the roots of P. By Theorem 37 on p. 67 in [5] the order of a resolvent of P with no nontrivial relations over constants of its roots is greater than or equal to n. Therefore for all but finitely many integers, q, the order of a qth power resolvent of P is greater than or equal to n. □

Theorem 19. *Let P be an nth degree polynomial over a d-field*, $\mathbb{F}$, *for which no two roots have a constant ratio. Then the order of any* α*th power resolvent is greater than or equal to n.*

Proof. Let R_α be an αth power resolvent of order, $m < n$. Since R_α is a polynomial in α, it follows that $R_q \equiv \phi_q(R_\alpha) \neq 0$ for all but finitely many integers q. But R_q is a nonzero qth power resolvent, by the Powersum Satisfaction Theorem, Theorem 35 on p. 64 in (5), of order $\leqslant m < n$, a contradiction with the assertion of Theorem 18 that the order of qth power resolvents is greater than or equal to n for all but finitely many integers, q. □

10. Fields of constants containing roots of unity

The final theorem in this paper asserts a result similar to that asserted in Theorem 7. Theorem 7 is a statement about algebra, whereas Theorem 20 is a statement about differential algebra. Unlike Theorem 7, Theorem 20 does not assume that the Galois group, G, of a polynomial, P, over a field, $\mathbb{F}$, contains an n-cycle. But Theorem 20 does assume that there exists at least one non-trivial linear relation over constants, and that the subfield, $\Bbbk$, of constants of $\mathbb{F}$ contains a sufficient number of roots of unity.

Theorem 20. *Let $\mathbb{F}$ be a differential field of characteristic 0 with derivation, D, and subfield of constants, $\Bbbk$. Let $P(t) \equiv \sum_{i=0}^{n}(-1)^{n-i}e_{n-i}t^i \in \mathbb{F}[t]$ with $n \geqslant 3$. Let G be the Galois group of P, over $\mathbb{F}$. Suppose G acts transitively on the n distinct roots, $z \equiv \{z_i\}_{i=1}^n$, of P. Suppose $\Bbbk$ contains all $2(n!)$th roots of unity. Let $q \in \mathbb{Z}$. Suppose there exists at least one nontrivial linear relation of $y \equiv \{z_i^q\}_{i=1}^n$ over $\Bbbk$. Then there exists a nontrivial linear relation of the y over roots of unity.*

Proof. Let $z_k^q = \sum_{i \neq k} c_i \cdot z_i^q$ be one of the nontrivial linear relations of $\{z_i^q\}_{i=1}^n$ over $\Bbbk$. Since G acts transitively on the roots of P, P is irreducible over $\mathbb{F}$. So no root of P is zero. So, at least one of the $c_{i \neq k}$ in this relation is not zero. Let it be c_m.

Let W_k be the Wronskian of $\{z_i^q\}_{i \neq k}$. By basic differential algebra, $D^j z_i^q \in \mathbb{F}(z_i^q)$, for each $j \in \mathbb{N}_0$. To prove this quickly for our purposes here, we remark that, for each $q \in \mathbb{Z}$ and each $i \in [n]$, there exists a minimal polynomial, $P_{q,i}(t) \in \mathbb{F}[t]$, for z_i^q. Hence, $0 = D(0) = D(P_{q,i}(z_i^q)) = H_{q,i} + S_{q,i} \cdot Dz_i^q$ where $H_{q,i}, S_{q,i} \in \mathbb{F}[z_i^q]$ and $S_{q,i}$ is the separant of $P_{q,i}$. Hence, $Dz_i^q = -\frac{H_{q,i}}{S_{q,i}} \in \mathbb{F}(z_i^q)$. Repeating this process shows that $D^j z_i^q \in \mathbb{F}(z_i^q)$ for each $j \in \mathbb{N}_0$. Hence $W_k = |D^j z_i^q|_{\substack{0 \leqslant j \leqslant n-2 \\ i \in [n], i \neq k}} \in \mathbb{F}(z_1^q, \dots, z_n^q)$.

Since G is transitive, there exists a $g \in G \ni g(k) = m$. Then $g(W_k) = |D^j z_{g(i)}^q| = |\cdots D^j z_k^q \cdots| = \pm W_m$ contains $D^j z_i^q$ for all $i \neq m$. But, $D^j z_k^q = \sum_{i \neq k} c_i \cdot D^j z_i^q$. Hence, $g(W_k) = \pm c_m \cdot W_k$. Since $g(k) = m \neq k$, it follows that $g \neq I$, the identity permutation. So g has a positive order, $|g| = o$, in G. Thus, $W_k = I(W_k) = g^o(W_k) = (\pm c_m)^o \cdot W_k$. Since $W_k \neq 0$, we have $(\pm c_m)^o = 1$, so $c_m^{2o} = (\pm c_m)^{2o} = 1$. Thus, c_m is a $2o$th root of unity.

Since this holds for all nonzero c_m on the right-hand-side of the equation, $z_k^q = \sum_{i \neq k} c_i \cdot z_i^q$, it follows that $z_k^q = \sum_{i \neq k} c_i \cdot z_i^q$ is a linear relation over roots of unity. □

Since $c_m \in \Bbbk$ by the hypothesis that $z_k^q = \sum_{i \neq k} c_i \cdot z_i^q$ is a linear relation over $\Bbbk$, since $2o$ divides $2|G|$, and since $2|G|$ divides $2(n!)$, it was necessary to include in the hypothesis of the theorem that $\Bbbk$ contains at least certain $2(n!)$th roots of unity, and it was sufficient that $\Bbbk$ contains all of them.

11. The Riccati equation

We will now use a linear differential resolvent to solve a familiar nonlinear differential equation. Consider nonlinear differential equations of the form, $Dw + \sum_{i=0}^{N} g_i \cdot w^i = 0$, where g_i are given differentiable real-valued functions of a real variable, x, such that $Dx = 1$. If we knew how to solve the equation, $D\bar{w} + \sum_{i=0}^{N} \bar{g}_i \cdot \bar{w}^i = 0$, where $\bar{g}_N \equiv 1$, then we could solve the equation, $Dw + \sum_{i=0}^{N} g_i \cdot w^i = 0$, by making the change of variables $\bar{w} = \sqrt[N-1]{g_N} \cdot w$, $\bar{g}_i = \sqrt[N-1]{g_N^{1-i}} \cdot g_i$ for $i = 0$ and $2 \leqslant i \leqslant N$, and $\bar{g}_1 = g_1 - \frac{1}{N-1}\frac{Dg_N}{g_N}$.

So, consider the Riccati equation, $Dw + \sum_{i=0}^{2} g_i \cdot w^i = 0$, with $g_2 = 1$. We know how to solve this equation by defining a new variable, v, which satisfies $w = \frac{Dv}{v}$. Then v satisfies $D^2 v + g_1 \cdot Dv + g_0 \cdot v = 0$, which we assume we know how to solve in principle.

But, suppose we did not know this change of variables. Specifically, suppose we had not known to introduce the logarithmic derivative of a new variable. Then, instead, we could have looked at a particular homogeneous resolvent of a quadratic polynomial, $P(t) \equiv t^2 - e_1 \cdot t + e_2$, whose properties will be determined momentarily. The discriminant of P is $\Delta = e_1^2 - 4e_2$. Define $\tilde{W} \equiv \begin{vmatrix} 1 \cdot e_1 & De_1 \\ 2 \cdot e_2 & De_2 \end{vmatrix}$, which is (up to sign) $\begin{vmatrix} 1 & 1 \\ z_2 & z_1 \end{vmatrix} = \sqrt{\Delta} = (z_1 - z_2)$ times the Wronskian, $\begin{vmatrix} z_1 & Dz_1 \\ z_2 & Dz_2 \end{vmatrix}$. The simplest homogeneous resolvent of P is $D^2 z + (\frac{1}{2}\frac{D\Delta}{\Delta} - \frac{D\tilde{W}}{\tilde{W}}) \cdot Dz + \frac{1}{2}(\frac{D\Delta}{\Delta} \cdot \frac{D\tilde{W}}{\tilde{W}} - \frac{D^2\Delta}{\Delta}) \cdot z = 0$. We know something about solving LODEs, provided we know something about the terms of the LODE, namely, $f_1 \equiv \frac{1}{2}\frac{D\Delta}{\Delta} - \frac{D\tilde{W}}{\tilde{W}}$ and $f_0 \equiv \frac{1}{2}(\frac{D\Delta}{\Delta} \cdot \frac{D\tilde{W}}{\tilde{W}} - \frac{D^2\Delta}{\Delta})$. We see that we may eliminate $\frac{D\tilde{W}}{\tilde{W}}$ between these two equations to get a differential equation in Δ alone, $4f_0 + 2\frac{D^2\Delta}{\Delta} + 2f_1\frac{D\Delta}{\Delta} - (\frac{D\Delta}{\Delta})^2 = 0$. We see now, by the square of the logarithmic derivative of the discriminant, how this variable might satisfy a Riccati equation. However, to get it into the Riccati form, one needs to know that $\frac{D^2\Delta}{\Delta} = D(\frac{D\Delta}{\Delta}) + (\frac{D\Delta}{\Delta})^2$. Allowing this knowledge, we get $2 \cdot Dv + v^2 + 2f_1 v + 4f_0 = 0$ where $v \equiv \frac{D\Delta}{\Delta}$. Making one more change of variables suggested earlier by the formula, $\bar{w} = \sqrt[N-1]{g_N} \cdot w$, let $v \equiv 2u$. Then $Du + u^2 + f_1 u + f_0 = 0$.

Hence, working backwards, if we are given the Riccati equation, $Du + u^2 + g_1 u + g_0 = 0$, let $f_0 = g_0$ and $f_1 = g_1$. Solve the linear differential equation $D^2 z + g_1 \cdot Dz + g_0 \cdot z = D^2 z + f_1 \cdot Dz + f_0 \cdot z = 0$ for two functions of x, called z_1 and z_2, each of which will depend upon two arbitrary constants. Then the solution of the Riccati will be $u = \frac{1}{2}v = \frac{1}{2}\frac{D\Delta}{\Delta} = \frac{Dz_1 - Dz_2}{z_1 - z_2}$, which will depend upon only one arbitrary constant.

So, the formula for the second-order homogeneous resolvent of a quadratic in terms of the logarithmic derivative of its discriminant shows why it is involved in the solution of the Riccati. In essence, this is nothing more than a fancy way of observing that a Riccati equation is associated to any nth-order LODE (see [10]). In the case $n=2$, if one divides the LODE, $D^2z+g_1\cdot Dz+g_0\cdot z=0$, by z one gets $\frac{D^2z}{z}+g_1\cdot\frac{Dz}{z}+g_0=0$. Letting $u\equiv\frac{Dz}{z}$ and observing that $\frac{D^2z}{z}=D(\frac{Dz}{z})+(\frac{Dz}{z})^2=Du+u^2$ we get back the Riccati, $Du+u^2+g_1\cdot u+g_0=0$. But, the formula does show the utility of the resolvent, which is defined for polynomials of any degree and therefore may possibly be useful for solving nonlinear ODEs of other orders and degrees in the dependent variable.

12. Mathematica program for the Sextic example

(* Example 16*)
(* In the notation of Example 16, $x=x_4, y=x_5$, and $z=x_6$. The variable, sol, is the vector, (x_1,x_2,x_3), expressed as a linear combination of x, y, and z over the field, $\mathbb{Q}(a,b,c)$. The variable, cy2, for instance, is the coefficient of x_2 in the expansion of $y=x_5$. Factor[cy2] is simply cy2 factored over $\mathbb{Q}(a,b,c)$.*)

```
a = .; b = .; c = .; u = .; v = .; w = .;
m1 = a*u + b*v + c*w;  m2 = c*u + a*v + b*w;  m3 = b*u + c*v + a*w;
m4 = b*u + a*v + c*w;  m5 = a*u + c*v + b*w;  m6 = c*u + b*v + a*w;
left = m1, m2, m3, m2, m3, m1, m3, m1, m2;
right = m4, m5, m6, m6, m4, m5, m5, m6, m4;
vec = right.x, y, z;
sol = -Together[LinearSolve[left, vec]]
```

```
-(abx - acx - bcx + c^2x + a^2y - aby-
    acy + bcy - abz + b^2z + acz - bcz)/
  (a^2 - ab + b^2 - ac - bc + c^2),
-(a^2x - abx - acx + bcx - aby + b^2y+
    acy - bcy + abz - acz - bcz + c^2z)/
  (a^2 - ab + b^2 - ac - bc + c^2),
-(-abx + b^2x + acx - bcx + aby - acy-
    bcy + c^2y + a^2z - abz - acz + bcz)/
  (a^2 - ab + b^2 - ac - bc + c^2)
```

```
cx3 = Coefficient[sol, x, 1][[3]];
cx2 = Coefficient[sol, x, 1][[2]];
cx1 = Coefficient[sol, x, 1][[1]];
cy3 = Coefficient[sol, y, 1][[3]];
cy2 = Coefficient[sol, y, 1][[2]];
cy1 = Coefficient[sol, y, 1][[1]];
cz3 = Coefficient[sol, z, 1][[3]];
cz2 = Coefficient[sol, z, 1][[2]];
cz1 = Coefficient[sol, z, 1][[1]];
```

```
Factor[cx3]
Factor[cx2]
Factor[cx1]
Factor[cy3]
Factor[cy2]
Factor[cy1]
Factor[cz3]
Factor[cz2]
Factor[cz1]
```

$$\frac{(a-b)(b-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$-\frac{(a-b)(a-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$-\frac{(a-c)(b-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$-\frac{(a-c)(b-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$\frac{(a-b)(b-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$-\frac{(a-b)(a-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$-\frac{(a-b)(a-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$-\frac{(a-c)(b-c)}{a^2-ab+b^2-ac-bc+c^2}$$
$$\frac{(a-b)(b-c)}{a^2-ab+b^2-ac-bc+c^2}$$

Acknowledgments

The author acknowledges the great assistance of Dr. Cohn, who was his doctoral dissertation adviser at Rutgers University.

References

[1] E. Cattani, C. D'Andrea, A. Dickenstein, The *A*-hypergeometric System Associated with a Monomial Curve, Duke Math. J. 99 (2) (1999) 179–207.

[2] E. Compoint, M. Singer, Relations line'aires entre solutions d'une e'quation diffe'rentielle, Ann. Fac. Sci. Toulouse VII (4) (1998) 659–670.

[3] I.G. Macdonald, Symmetric Functions and Hall Polynomials, Oxford Mathematical Monographs, 2nd Edition, Clarendon Press, Oxford, 1995, ISBN 0-19-853489-2.

[4] T. Muir, A Treatise on the Theory of Determinants, Revised and enlarged by William H. Metzler, Dover Publications, Inc. New York, NY, 1961. (Originally published in 1933 by Longmans, Green & Co. QA191.M95).

[5] J.M. Nahay, Linear Differential Resolvents, Doctoral Dissertation, Rutgers University, New Brunswick, NJ, May 23, 2000.

[6] J.M. Nahay, Powersum formula for polynomials whose distinct roots are differentially independent over constants, Internat. J. Math. Math. Sci. 32 (12) (2002) 721–738.

[7] P. Pepin, Me'thode pour obtenir les inte'grales alge'briques des e'quations diffe'rentielles line'aires du second order, Atti dell' Accad. Pont. De Nuovi Lincei XXXIV (1881) 243–388.

[8] P. Scalizzi, Soluzione di alcune equazioni del tipo di Abel, Atti Accad. Naz. Lincei, Ser. 5 (26) (1917) 60–64.

[9] F. Schwarz, Symmetry analysis of Abel's equation, Stud. Appl. Math. 100 (1998) 269–294.

[10] M. Singer, Liouvillian solutions of *n*th order homogeneous linear differential equations, Amer. J. Math. 103 (4) (1981) 661–682.