1999

Algebraic theory of differential equations

Thomas J. Little
San Jose State University

Recommended Citation

Little, Thomas J., "Algebraic theory of differential equations" (1999). *Master's Theses*. 1882.
DOI: https://doi.org/10.31979/etd.9d2b-r3jb
https://scholarworks.sjsu.edu/etd_theses/1882

ALGEBRAIC THEORY OF DIFFERENTIAL EQUATIONS

A Thesis

Presented to

The Faculty of the Department of Mathematics and Computer Science

San Jose State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science

By

Thomas J. Little

August 1999

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

APPROVED FOR THE DEPARTMENT OF MATHEMATICS

AND COMPUTER SCIENCE

Brian Peterson

Dr. Brian Peterson

Eloise Hamann

Dr. Eloise Hamann

Richard P. Kubelka

Dr. Richard P. Kubelka

APPROVED FOR THE UNIVERSITY

William Fish

ABSTRACT

ALGEBRAIC THEORY OF DIFFERENTIAL EQUATIONS

By Thomas J. Little

The question of whether the indefinite integral of an elementary function is always elementary is the first of two investigations in this thesis. A precise criterion is developed that depends solely on elements, their derivatives and constants in a base field of a tower, starting with the original field and culminating in a field containing the indefinite integral. Several classical examples are given.

Similar to ordinary Galois theory, differential Galois theory addresses the nature of the differential field extensions generated by solutions of differential equations. The corresponding differential Galois group of automorphisms of an extension field, fixing the base field, provides insight to the solvability of a differential equation. We show that the differential Galois group corresponding to a Picard-Vessiot extension is an algebraic matrix group and there is a one-to-one correspondence between the intermediate differential fields and the algebraic subgroups of the differential Galois group. In the case of Airy's equation, we find that a generalized Liouville extension of the field of rational functions can give us no solutions.

Acknowledgments

This author wishes to express his appreciation to his thesis advisor, Dr. Brian Peterson, for his many suggestions, criticism and significant periods of consultation during this investigation and at other times. He also expresses his appreciation to his thesis committee, Dr. Eloise Hamann and Dr. Richard P. Kubelka, for the many helpful comments and suggestions.

CONTENTS

Introduction

The question is old: Is the indefinite integral of an elementary function always elementary? In other words, can the indefinite integral of an elementary function be expressed “explicitly” (or in “closed form” or “in finite terms”)? The answer, attributed to Liouville, is also old, and among mathematicians it is commonly known to be “no.” With the broadness of mathematics it seems very probable that a student may advance well into a career in mathematics only having heard that it is a familiar fact that a closed form solution to $\int e^{-\frac{x^2}{2}}dx$ is nonexistent. The lucky ones may know that the proof is among the many accomplishments of Liouville but still have not experienced a demonstration. Part I follows Rosenlicht’s paper closely with the motivation to make the material accessible to the interested upper division undergraduate by adding another level of detail and explanation. The original work is wonderfully organized and concise and every effort has been made to preserve those virtues.

We take elementary functions to be elements of fields of meromorphic functions, closed under differentiation, on given regions in the field of real numbers or the field of complex numbers. With careful formulation the problem becomes algebraic and the integral of an elementary function that is expressible in finite terms corresponds to a tower, starting with the original field and culminating in a field containing the indefinite integral. We develop a precise criterion for the existence of an elementary indefinite integral that depends solely on elements, their derivatives and constants in the base field. The result is expressed in an abstract generalization of Liouville's theorem. We show several examples of integrals of elementary functions that are not elementary, including perhaps the most famous $\int e^{-\frac{x^2}{2}}dx$ (a solution to the differential equation $y''+xy'=0$). Part I is divided into six sections.

Section 1 Elementary Functions: This section is devoted to specifying very clearly the notion of elementary function as described in the second paragraph of this Introduction.

Section 2 Differential Fields: Here we define a differential field to be a field together with a derivation mapping of the field into itself such that derivation sum and product rules hold. The development of the quotient and power rules follows immediately. We then are able to define the exponential of an element of the differential field as well as the logarithm of an element of the differential field.

Section 3 Algebraic Extensions of Differential Fields: This section is devoted to showing that a differential structure on a differential field may be uniquely extended to an algebraic extension of the original differential field.

Section 4 Differential Extension Fields: A differential extension field is an extension of a differential field such that the derivation on the extension field extends the derivation on the original field. A lemma and its proof are presented for central use in the proof of Liouville's theorem.

Section 5 Elementary Extensions: An elementary extension of a differential field is a differential extension defined by successive adjunction of elements, finite in number, such that each is algebraic over the previous field, or the logarithm of an element of the previous field, or the exponential of an element of the previous field. An abstract generalization of Liouville's theorem and proof are presented.

Section 6 Examples: The approach is to employ Liouville's theorem and the key lemma from Section 4 to show that $f(z)e^{g(z)}$ ($f(z)$, $g(z)$ rational functions) has an elementary integral if and only if the field of rational functions of a complex variable contains an element a such that $f = a' + ag'$. Several examples are then immediate.

Part II focuses on differential Galois theory and may be considered independent of Part I. Similar to ordinary Galois theory, differential Galois theory addresses the nature of the differential field extensions generated by solutions of differential equations. The corresponding differential Galois group of automorphisms of the extension field that fix the base field provides insight into the solvability of a differential equation. We show that the Galois group corresponding to a minimal differential extension field containing a solution space for a linear differential equation and no new constants over a base field of characteristic zero is an algebraic matrix group. Such an extension field is called a Picard-Vessiot extension and there is a one-to-one correspondence between the intermediate differential fields and the algebraic subgroups of the differential Galois group. Kaplansky observes that with additional refinements one can detect from the Galois group the possibility of solving a linear homogeneous equation by integrals alone, or by exponentials of integrals alone (40). Unfortunately there does not seem to be sufficient insight provided by the theory to detect the possibility of elementary integrals.

It is known that for a first order linear differential equation a field containing a solution (i.e. containing a solution subspace) may be obtained by finite adjunction of an integral or the finite adjunction of the exponential of an integral. Indeed classically a solution of $y' + a(x) = 0$ is $-\int a(x)dx$ and a solution of $y' + a(x)y = 0$ is $e^{-\int a(x)dx}$. What then should follow for a second order equation? Is it always possible to obtain a solution field for an equation by a similar process of adjunction? Again it is known from classical theory that the general homogeneous linear equation $y'' + a(x)y' + b(x)y = 0$ can be expressed in the form $u'' - f(x)u = 0$ where $y(x) = u(x)w(x)$, $w(x) = e^{-\int \frac{a(x)}{2}dx}$ and $f(x) = \left(\frac{a(x)}{2}\right)' + \left(\frac{a(x)}{2}\right)^2 - b(x)$. Hence for the general second order equation, the answer for the equation $u'' - f(x)u = 0$ will be sufficient. In particular we take a simple form, Airy's equation found in wave theory, $y'' + xy = 0$. We find that a generalized Liouville extension of the field of rational functions can give us no solutions to Airy's equation.

Part II may be viewed as a short course in differential algebra with emphases on differential Galois theory. Algebra intertwined with topology (to a lesser degree) in an interesting way is brought to bear on a seemingly classical elementary calculus and differential equation problem. Differential algebra emerged in the 19th century and during the first three-quarters of this century was advanced by Ritt and Kolchen. Their contribution was so dominant that some regarded the phrase "the work of Ritt and Kolchen" to be a description of differential algebra. Part II closely follows Kaplansky's book that, according to Kaplansky, is written to make the work of Ritt and Kolchin more accessible. The book, concise and short, has been acclaimed by many, but still its difficulty is such that many students will find it a little out of reach. There has been a resurgence of interest in differential Galois theory in recent years. Hopefully this effort will make a small contribution to the field that is worthy to be in the shadows cast by the leaders of the past and present. The presentation here reflects the portions of his book that Kaplansky attributes principally to the work of Kolchin.

Chapter 1 Differential Rings: The fundamental theory of differential rings is covered to the extent needed in later developments. The chapter begins with the basic definition and properties of derivations and extensions of derivations. The theory of differential rings, differential homomorphisms and differential ideals are developed and we get an isomorphism theorem analogous to an isomorphism theorem of ordinary ring theory. We discover that in a differential ring the condition of an algebra containing a copy of the field of rational numbers is necessary for the radical of a differential ideal to be a radical differential ideal.

Chapter 2 Extensions of Isomorphisms: As in ordinary ring theory any radical differential ideal is the intersection of prime ideals. An isomorphism between two fields both contained in the same larger field is defined to be an admissible isomorphism. There are several key results on extensions of admissible isomorphisms that underlie the remaining chapters.

Chapter 3 Preliminary Galois Theory: The rudiments of differential Galois theory are covered without the benefits of the theory of algebraic matrix groups or point set topology. If M is a differential field and K a differential subfield of M, the differential Galois group of M over K is the group of all differential automorphisms of M leaving K elementwise fixed. The foundational lemmas are developed which ultimately lead to the conditions for the existence of a one-to-one correspondence between the intermediate differential fields and algebraic subgroups of the differential Galois group. The essential steps to considering solutions of differential equations are taken here based on the introduction of two types of extensions of a differential field. First, a Picard-Vessiot extension of a differential field is defined to be one obtained by the adjunction of the solutions of a linear homogeneous differential equation, linearly independent over constants, and such that there are no new constants in the extension field. Second, a Liouville extension of a differential field is defined to be one obtained by a finite adjunction chain such that no new constants are added and where each adjunction consists of integrals of elements in the previous field in the chain or of the exponential of the integral of elements in the previous field in the chain.

Chapter 4 Algebraic Matrix Groups and The Zariski Topology: The focus of this section is putting into place the point set topology and algebraic matrix group machinery sufficient to complete the Galois theory of Chapter 5 and the application to equations of order two in Chapter 6. The topology of principal interest here is the Zariski topology, which may be derived by using algebraic manifolds as closed sets to define a T_1 topology on an n-dimensional vector space over any field (the finite union of algebraic manifolds is an algebraic manifold and the arbitrary intersection of algebraic manifolds is an algebraic manifold). The results are numerous and many are used later. Notable among them are 1) the conditions under which a C-group will have a solvable component of identity, and 2) a solvable, connected (in the Zariski topology) multiplicative group of nonsingular matrices over an algebraically closed field can be put in simultaneous triangular form.

Chapter 5 The Galois Theory: Here we reach our principal theoretical results. We find that the differential Galois group of a Picard-Vessiot extension is an algebraic matrix group over the field of constants and that the Galois Theory implements a one-to-one correspondence between the intermediate differential fields and the algebraic subgroups of the differential Galois group. And we develop the conditions under which a Picard-Vessiot extension field can be obtained by a generalized Liouville extension over the same base field.

Chapter 6 Equations of Order Two: This section addresses several special results with respect to the Wronskian of the solutions of a Picard-Vessiot extension. Included is the result discussed above for Airy's equation, $y'' + xy = 0$.

Part I — Differential Fields And Integration In Finite Terms

1) **Elementary Functions** — First we must be specific and careful concerning the notion of elementary functions. Following Rosenlicht, an **elementary function** may be constructed by using one variable and constants with repeated algebraic operations and taking exponentials and logarithms, e.g. $7x^{-3}e^{x}+10\ln(x^{2}+5)$. Take the variable to be complex, then $\sin z=\dfrac{e^{iz}-e^{-iz}}{2i}$, $\cos z=\dfrac{e^{iz}+e^{-iz}}{2}$, $\sin^{-1}z=-i\log[iz+(1-z^{2})^{1/2}]$, $\cos^{-1}z=-i\log[z+i(1-z^{2})^{1/2}]$ and $\tan^{-1}z=\dfrac{i}{2}\log\dfrac{i+z}{i-z}$. So the trigonometric functions and the inverse trigonometric functions are elementary. The integral of a rational function of one real variable is elementary since it is a linear combination of logarithms, inverse tangents and rational functions. For our purposes here we will agree without loss of generality that the exponential base and the logarithmic base are both the familiar number e. The awkward issue of multivaluedness may be handled in the most direct fashion by restricting the function's domain to nonempty connected open subsets in the real numbers **R** or complex numbers **C** in such a way that the function in question is unambiguous. We consider only meromorphic functions on the regions in question. A **meromorphic function** being the usual notion: a function such that in the neighborhood of any point z_0 the function may be represented as a convergent Laurent series in $z-z_0$, that is, a convergent power series in $z-z_0$ with at most a finite number of negative powers of $z-z_0$ added. Thus the

functions contained in the field of rational functions **C**(z), obtained by adjoining the identity function z to the field of constant functions **C** , are all meromorphic on all of **R** or **C**. The exponential function e^f of a function f meromorphic on a subregion A of **R** or **C** is a function meromorphic on a subregion obtained by deleting those points z_0 of A where $|f| \to \infty$ as $z \to z_0$ if A$\subset$**C** and in addition taking a connected component of A if A$\subset$**R**. The function $\log f$ may be considered meromorphic on a subregion A where $f \neq 0$ and $|f|$ is finite by choosing one of its many values at any point in A. Next consider a polynomial equation with coefficients functions $f_n(z)$ meromorphic on a region A, where the leading coefficient is not zero, $f_n(z)z^n + f_{n-1}(z)z^{n-1} + \cdots \ + f_1(z)z + f_0(z) = 0$, $f_n(z) \neq 0$. Hence we may write $F(f_n, f_{n-1}, \cdots, f_0, z) = 0$. Choosing $z \in$A such that $F_z(f_n, f_{n-1}, \cdots, f_0, z) \neq 0$, by the implicit function theorem we have the existence of a meromorphic solution $z = h(f_n, f_{n-1,} \cdots, f_0)$ on a suitable subregion of A. Thus an elementary function expressed as a complicated combination of algebraic operations, exponentials and logarithms is meromorphic on some region. Then under the operations of function multiplication and addition the totality of meromorphic functions on a region form a field and the restriction of these functions to a subregion gives an embedding of fields. That the derivative of a meromorphic function on a region is a meromorphic function on the region may be deduced from the Laurent series and if the integral exists, the integral of the function is also meromorphic. Thus we observe that the field of rational functions on a region is a field of meromorphic functions on the region that is closed under differentiation (restricting **C**(z) to the region in question). Suppose we are given a field of meromorphic functions on a region closed under differentiation and we adjoin the exponential or logarithm of a function in our field or a solution of a polynomial equation with coefficients in the field. The field obtained is a field of meromorphic functions on the region closed under differentiation. Thus our view is that **elementary functions** are elements of fields of meromorphic functions on **R** or **C**, closed under differentiation (963-965).

2) **Differential Field — A differential field** is defined to be a field F, together with a derivation on F. A **derivation** is a map of F into F, denoted $a \rightarrow a'$, and such that $(a+b)'=a'+b'$ and $(ab)'=a'b+ab'$ for every $a,b \in F$. The expected quotient rule, power rule for integers and derivation of constants follow with a little effort. Let $a,b,c \in F$ such that $c=\frac{a}{b}, b \neq 0$. Then

$a'=(cb)'=c'b+cb'=c'b+\left(\frac{a}{b}\right)b'$, and $a'b-ab'=c'b^2$. Therefore, $\left(\frac{a}{b}\right)'=\frac{a'b-ab'}{b^2}$.

Also, by repeated use of $(ab)'=a'b+ab'$, associativity, and commutativity, we have for $n>0$,

$(a^n)'=((a \cdot\cdot^{(n-1\,factors)} \cdot a)a'+((a \cdot\cdot^{(n-2\,factors)} \cdot a)a'a+\cdots+a'(a \cdot\cdot^{(n-1\,factors)} \cdot a))=na^{n-1}a'$. Then applying $(a^n)'=n(a^{n-1})a'$, $n>0$, to $1'=(1^2)'=2\cdot1\cdot1'$, we conclude $1'=0$. For $n<0$, let $m=-n$. Then,

$(a^n)' = \left(\frac{1}{a^m}\right)' = \left(\left(\frac{1}{a}\right)^m\right)' = m\left(\frac{1}{a}\right)^{m-1}\left(\frac{1}{a}\right)' = m\frac{1}{a^{m-1}}\left(\frac{1'a-1a'}{a^2}\right) = -\frac{ma'}{a^{m+1}} = na^{n-1}a'$. So,

$(a^n)' = n(a^{n-1})a'$ for every integer n. If we let the **constants** of F be all $c \in F$ such that $c' = 0$, then the constants form a subfield of F since $0,1 \in F$, $(a+b)' = a'+b' = 0$, $(ab)' = a'b + ab' = 0$ and if $b \neq 0$ then $\left(\frac{a}{b}\right)' = \frac{a'b-ab'}{b^2} = 0$, for all constants $a,b \in F$. For a constant the familiar rule $(ab)' = ab'$ is immediate.

Let $a,b \in F$, $a \neq 0$ and F a differential field. We define a to be the **exponential** of b, or b to be the **logarithm** of a, if $b' = \frac{a'}{a}$. We observe from the relations above that $(a_1^{v_1} \cdots a_n^{v_n})' = v_1(a_1^{v_1-1}a_2^{v_2} \cdots a_n^{v_n})a_1' + \cdots + v_n(a_1^{v_1} \cdots a_n^{v_n-1})a_n'$, for $a_1,\cdots,a_n \in F$, and $v_1,\cdots,v_n$ integers. Suppose $(a_1^{v_1} \cdots a_n^{v_n}) \neq 0$, then dividing by $(a_1^{v_1} \cdots a_n^{v_n})$ we have $\frac{(a_1^{v_1} \cdots a_n^{v_n})'}{(a_1^{v_1} \cdots a_n^{v_n})} = v_1\frac{a_1'}{a_1} + \cdots + v_n\frac{a_n'}{a_n}$, the **logarithmic derivative identity**.

3) **Algebraic Extensions of Differential Fields** — Continuing to follow Rosenlicht, we let K be an algebraic extension of the differential field F of characteristic zero. Then for every $x \in K$, x is algebraic over F and if $f(x) = 0$, $f(X) \in F[X]$, where X is an indeterminate and $F[X]$ a polynomial ring, we have $h(x) = c^{-1}f(x) = 0$ as well, where c is the nonzero leading coefficient of $f(X)$ and $h(X) \in F[X]$ is monic. So we will consider $f(x)$ monic

and irreducible over F. Let us define the maps $D_0, D_1 : F[X] \xrightarrow{\text{into}} F[X]$ by

$D_0\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} a_i{}' X^i$ and $D_1\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} i a_i X^{i-1}$, for $a_0\, a_1 \cdots a_n \in F$. Suppose K has a differential field structure extending that of F and that x is a simple root of the monic irreducible polynomial $f(X)$ over F, then $(f(x))' = (D_0 f)(x) + (D_1 f)(x) \cdot x' = 0$. But $(D_1 f)(x) \neq 0$. So $x' = -(D_0 f)(x)/(D_1 f)(x)$. Thus, if it exists, the differential structure on K that extends the differential structure on F is unique (965-966).

Addressing existence we presume that our extensions are finite, that is if $F(\alpha)$ is a simple extension of a differential field F, then $F(\alpha)$ may be viewed as a vector space over F with basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$, where n is the degree of the irreducible polynomial for α over F. Fraleigh provides the appropriate field theoretic Theorem 9.14 that we adapt to our notation: Let K be a finite separable extension of a field F. Then there exists $x \in K$ such that $K = F(x)$ (475). He also tells us in Theorem 9.12 that for every field of characteristic zero every finite extension is separable, that is, the irreducible polynomial for α over F of degree n has n distinct zeros in an algebraic closure for F (473).

Let $K = F(x)$ be a finite algebraic extension of F and $f(X)$ the monic irreducible polynomial of x in $F[X]$. Again using the maps D_0, D_1 defined above, for some $g(X) \in F[X]$, let the map $D: F[X] \to F[X]$ be defined by $DA = D_0 A + g(X) D_1 A$, for any $A \in F[X]$. Since $D_i(A+B) = D_i A + D_i B$ and

$D_i(AB) = (D_i A)B + A(D_i B)$ for $i = 0,1$, we have $D(A+B) = DA + DB$ and $D(AB) = (DA)B + A(DB)$ for all $A, B \in F[X]$. Also, $Da = a'$ for all $a \in F$. Next consider the surjective ring homomorphism $\phi: F[X] \rightarrow F(x)$, which is the identity on F and sends $X \rightarrow x$. We have that $Ker\phi = (f)$ and since $f(X)$ is irreducible (f) is maximal, thus $F[X]/(f) \cong \operatorname{Im}\phi = F[x]$ is a field. Hence $F[x] = F(x) = K$. Then the map D on $F[X]$ will induce a map on K extending that on F so long as $D(Ker\phi) \subset Ker\phi$. But $Ker\phi = (f)$. Thus we want to show that $D((f)) \rightarrow (f)$ which is equivalent to $(Df)(x) = 0$, that is, x is a root of the image of $f(X)$. Then $(D_0 f)(x) + g(x)(D_1 f)(x) = 0$. But we have $(D_1 f)(x) \neq 0$ and $F(x) = F[x]$, so a polynomial $g(X) \in F[X]$ can be found such that $(Df)(x) = 0$. Therefore we have found a unique differential structure on K extending the differential structure on F.

4) **Differential Extension Fields** — A differential field K that is an extension of a differential field F such that derivation on K extends the derivation on F is called a **differential extension field** of F. Rosenlicht introduces the next Lemma as a central element in the proof in Liouville's Theorem.

Lemma — Let F be a differential field of characteristic 0, $F(t)$ a differential extension field of F having the same field of constants, with t transcendental over F, and with either $t' \in F$ or $\frac{t'}{t} \in F$. If $t' \in F$, then for any polynomial $f(t) \in F[t]$of positive degree, $(f(t))'$ is a polynomial in $F[t]$ of the same degree as $f(t)$, or degree one less, according as the highest coefficient of $f(t)$ is not, or is, a constant c, i.e. $c' = 0$. If $\frac{t'}{t} \in F$, then for any nonzero $a \in F$ and any nonzero integer n we have $(at^n)' = ht^n$, for some nonzero $h \in F$, and furthermore with $\frac{t'}{t} \in F$, for any polynomial $f(t) \in F[t]$ of positive degree, $(f(t))'$is a polynomial in $F[t]$ of the same degree, and is a multiple of $f(t)$ only if $f(t)$ is a monomial.

Proof — For the case $t' = b \in F$we let $f(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0$for $n > 0$ with $a_0, \cdots, a_n \in F, a_n \neq 0$. Then $(f(t))' = a_n' t^n + (na_n b + a_{n-1}')t^{n-1} + \cdots$ is a polynomial in $F[t]$, since the coefficients are in F, and of degree n if a_n is not constant. If $a_n' = 0$ and $na_n b + a_{n-1}' = 0$ we have $(f(t))'$ of degree less than $n-1$ and $(na_n t + a_{n-1})' = na_n b + a_{n-1}' = 0$. Then $na_n t + a_{n-1} \in F$, since $F[t]$ and F have the same field of constants. Hence $t \in F$, which contradicts the hypothesis that t is transcendental over F. Therefore if a_n is constant, $(f(t))'$ has degree $n-1$.

Next let $t'/t = b \in F$. Consider the monomial $at^n \in F[t]$, where $a \in F, a \neq 0$and n a nonzero integer. Then $(at^n)' = a't^n + nat^{n-1}t' = (a' + nab)t^n$. If $a' + nab = 0$, then $(at^n)' = 0$ and $at^n \in F$ since it is constant, contradicting the hypothesis that t is transcendental over F. Hence $(at^n)' = ht^n$ for some $h \in F, h \neq 0$.

Still assuming $t'/t = b \in F$, let $f(t) \in F[t]$ be of positive degree. Let $a_n t^n$ be the leading term. By the analysis above we see that the degree of $f(t)$ and $(f(t))'$ are the same. Thus if $(f(t))'$ is a multiple of $f(t)$ it must be by a factor in F. Suppose that $f(t)$ is not monomial, $a_n t^n$ and $a_m t^m$ two different terms of $f(t)$, and $(f(t))'$ is a multiple of $f(t)$. Then, $(f(t))' = hf(t)$, for some $h \in F$ and $\cdots + ha_n t^n + \cdots + ha_m t^m + \cdots = \cdots (a_n' + na_n b)t^n + \cdots + (a_m' + ma_m b)t^m + \cdots$. But $a_n, a_m, (a_n' + na_n b), (a_m' + ma_m b) \in F$, so $ha_n = (a_n' + na_n b)$ and $ha_m = (a_m' + ma_m b)$. Hence $\frac{a_n' + na_n b}{a_n} = \frac{a_m' + ma_m b}{a_m}$. Then $\frac{a_n'}{a_n} + n\frac{t'}{t} = \frac{a_m'}{a_m} + m\frac{t'}{t}$. By the logarithmic derivative identity we have $\frac{(a_n t^n)'}{(a_n t^n)} = \frac{(a_m t^m)'}{(a_m t^m)}$, and $(a_n t^n)'(a_m t^m) - (a_n t^n)(a_m t^m)' = 0$. So dividing by $(a_m t^m)^2$, we see that $\left(a_n t^n / a_m t^m\right)' = 0$ and $a_n t^n / a_m t^m \in F$, again contradicting the transcendence of t over F. Therefore $(f(t))'$ is of the same positive degree as $f(t)$ and $(f(t))' = hf(t)$ for some $h \in F, h \neq 0$ only if $f(t)$ is monomial. The proof is complete (966-967).

5) **Elementary Extensions** — Let F be a differential field. An **elementary extension** of F is a differential extension of the form $F(t_1, \cdots, t_N)$, where for each $i = 1, \cdots, N$, the element t_i is either algebraic over the field $F(t_1, \cdots, t_{i-1})$ or the logarithm or exponential of an element of $F(t_1, \cdots, t_{i-1})$. Each intermediate field $F(t_1, \cdots, t_{i-1})$ is a differential field and an elementary extension of

F. Rosenlicht then presents an abstract generalization of Ostrowski's 1946 generalization of Liouville's 1835 theorem on the subject.

Theorem — Let F be a differential field of characteristic zero and $\alpha \in F$. If the equation $y' = \alpha$ has a solution in some elementary differential extension field of F having the same subfield of constants, then there are constants $c_1, \cdots, c_n \in F$ and elements $u_1, \cdots, u_n, v \in F$ such that $\alpha = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'$.

The essentiality that F and its elementary extension field have the same subfield of constants is quickly discerned from the example $F = \mathbf{R}(x)$, the field of real rational functions of a real variable where we let $x' = 1$ and $\alpha = 1/(x^2+1)$. Recall that $\tan^{-1} x$ is an elementary function (Section 1) and $(\tan^{-1} x)' = 1/(x^2+1)$. So $\int (1/(x^2+1))dx$ is an element of an elementary extension field of $\mathbf{R}(x)$. We now demonstrate that the assumption $\frac{1}{(x^2+1)} = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'$, where $c_1, \cdots, c_n \in \mathbf{R}$ and $u_1, \cdots, u_n, v \in \mathbf{R}(x)$ leads to a contradiction. Suppose $u_i = (x^2+1)^{v_i} g_i(x)$ such that x^2+1 does not occur in $g_i(x)$ for some $g_i(x) \in \mathbf{R}(x)$ and v_i a nonzero integer. Hence $\frac{u_i'}{u_i} = \frac{g_i'(x)(x^2+1)^{v_i} + g_i(x) 2 v_i x (x^2+1)^{v_i - 1}}{(x^2+1)^{v_i} g_i(x)} = \frac{g_i'(x)}{g_i(x)} + \frac{2 v_i x}{(x^2+1)}$, so $\frac{u_i'}{u_i} - \frac{2 v_i x}{(x^2+1)}$ is an element of $\mathbf{R}(x)$ without x^2+1 in its denominator. Consider now $\frac{1}{x^2+1} - \sum_{i=1}^{n} c_i \frac{2 v_i x}{(x^2+1)} = \sum_{i=1}^{n} \left(c_i \left(\frac{u_i'}{u_i} - \frac{2 v_i x}{(x^2+1)} \right) \right) + v'$. If x^2+1 occurs once in the denominator of v, it occurs twice in the denominator of v'. It does not occur twice in the denominator of $\sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$ for then $\frac{u_i'}{u_i} - \frac{2v_i x}{(x^2+1)}$ would have it in the denominator for some i. Since $v' = \frac{1}{x^2+1} - \sum_{i=1}^{n} c_i \frac{u_i'}{u_i}$, then x^2+1 does not occur in the denominator of v. But then x^2+1 divides $1 - \sum_{i=1}^{n} 2c_i v_i x$, which is impossible, therefore we have our contradiction. Now $\tan^{-1} x$ is an elementary extension of **R**(x) which does have new constants, e.g. the extension generated over **R**(x) by i, $\ln(i+x)$ and $\ln(i-x)$.

When our fields are fields of meromorphic functions on some subregion of **R** or **C**, the field F and the elementary extensions fields of F will automatically satisfy the conditions that the subfield of constants be the same so long as **C**$\subset F$, since any constant meromorphic function is a complex number (Rosenlicht 967-968).

Proof of Theorem — Following Rosenlicht's proof of Liouville's theorem, expanding on a few details, we let $F \subset F(t_1) \subset \cdots \subset F(t_1, \cdots, t_N)$ be an assumed tower of differential fields all with the same subfield of constants and each t_i being algebraic over $F(t_1, \cdots, t_{i-1})$, or the logarithm or exponential of an element of $F(t_1, \cdots, t_{i-1})$, such that there exists an element $y \in F(t_1, \cdots, t_N)$ for which $y' = \alpha$. The proof is by induction on N. Noting that the case $N = 0$ is trivial since then $v' = y' = \alpha$ meets the need, we assume that $N > 0$ and the theorem is true for

$N-1$. Thus for the fields $F(t_1) \subset F(t_1,\cdots,t_N)$ we have $\alpha = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'$ with $u_1,\cdots,u_n,v \in F(t_1)$. Putting $t_1 = t$, then t is algebraic over F, or the logarithm or exponential of an element in F and $\alpha = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'$, with $c_1,\cdots,c_n$ constants of F and $u_1,\cdots,u_n,v \in F(t)$. We now need a similar expression for α with all $u_1,\cdots,u_n,v \in F$ perhaps for another n.

Let t be algebraic over F. Then $F(t)$ may be viewed as a vector space over F with the basis $\{1,t,\cdots,t^{m-1}\}$ where m is the degree of t over F. Thus every element of $F(t)$ may be represented as a linear combination of $\{1,t,\cdots,t^{m-1}\}$ with coefficients in F. Hence there exist polynomials $U_1,\cdots,U_n,V$ over F such that $U_1(t) = u_1,\cdots,U_n(t) = u_n V(t) = v$. Let the distinct conjugates of t over F in some suitable algebraic closure of $F(t)$ be $\tau_1 = t, \tau_2,\cdots,\tau_s$ (In the event we are involved with meromorphic functions on **R** or **C**, the functions $\tau_1,\cdots,\tau_s$ are then taken as meromorphic on a suitable subregion.) Recall our result on the extension of the differential structure for an algebraic extension of a differential field in Section 3. Thus $\alpha = \sum_{i=1}^{n} c_i \frac{(U_i(\tau_j))'}{U_i(\tau_j)} + (V(\tau_j))'$ for $j = 1,\cdots,s$, since it is true for $j = 1$. Adding the s relations we have $s\alpha = \sum_{j=1}^{s}\sum_{i=1}^{n} c_i \frac{(U_i(\tau_j))'}{U_i(\tau_j)} + \sum_{j=1}^{s}(V(\tau_j))'$.

Then interchanging the summations in the first term on the right and applying the logarithmic derivative identity derived in Section 2 to the sum on j and rearranging the second term gives

$\alpha = \sum_{i=1}^{n} \frac{c_i}{s} \frac{(U_i(\tau_1)\cdots U_i(\tau_s))'}{U_i(\tau_1)\cdots U_i(\tau_s)} + \left(\frac{V(\tau_1)+\cdots+V(\tau_s)}{s}\right)'$. But $U_i(\tau_1)\cdots U_i(\tau_s)\in F$ and $V(\tau_1)+\cdots+V(\tau_s)\in F$ since $U_i(\tau_1),\cdots,U_i(\tau_s)$ and $V(\tau_1),\cdots,V(\tau_s)$ are symmetric polynomials in the conjugates $\tau_1,\cdots,\tau_s$ with coefficients in F. Hence for t algebraic over F we may express α in the desired form in F.

Now let us consider the cases where t is the logarithm or exponential of an element of F. We assume t is transcendental over F. Recalling our induction hypothesis, the circumstance is evidently special that there are constants $c_1,\cdots,c_n\in F$ and elements $u_1(t),\cdots u_n(t),v(t)\in F(t)$ of such form that the terms on the right side of $\alpha = \sum_{i=1}^{n} c_i \frac{(u_i(t))'}{u_i(t)} + (v(t))'$ add up to $\alpha\in F$. Now each $u_i(t) = a(g_1(t))^{v_1}\cdots(g_m(t))^{v_m}$, where $a\in F$ a nonzero element and $g_1(t),\cdots,g_m(t)\in F[t]$ all monic irreducible elements with $v_1,\cdots,v_m$ nonzero integers. Thus we may use the logarithmic derivative identity to write each $\frac{(u_i(t))'}{u_i(t)}$ in the form $\sum_{i=1}^{m} v_i \frac{g_i'}{g_i}$ so we may assume that $u_1(t),\cdots,u_n(t)$ are distinct each being an element of F or a monic irreducible element of $F[t]$, and no c_i is zero. Next we consider for later use the partial fraction decomposition of $v(t) = h(t) + \sum_{i=1}^{m} \frac{g_i(t)}{(f_i(t))^{r_i}}$, where $h(t)\in F[t]$, each $f_i(t)\in F[t]$ is monic and irreducible, each r_i is a positive integer, and each $g_i(t) \in F[t]$ not zero and of degree less than the degree of $f_i(t)$. We now separate the logarithm and exponential cases.

Continuing to follow Rosenlicht, suppose that t is the logarithm of an element of F, then $t' = \frac{a'}{a}$ for some $a \in F$. Let $f(t) \in F[t]$ be monic and irreducible over F. Then $(f(t))' \in F[t]$ and $(f(t))'$ has degree less than the degree of $f(t)$. Hence $f(t)$ does not divide $(f(t))'$. Thus if $u_i(t) = f(t)$, then $\frac{(u_i(t))'}{u_i(t)}$ is in lowest terms and the denominator is $f(t)$. So if $f(t)$ is one of the $u_i(t)$'s then $f(t)$ appears in α, a situation that cannot happen. Since this is true for every monic irreducible $f(t)$ we must then have each $u_i(t) \in F$. Now suppose $\frac{g(t)}{(f(t))^r}$ appears in the partial fraction decomposition for $v(t)$ and as above with $g(t) \in F[t]$ of lesser degree than $f(t)$ and $r > 0$ maximal for the given $f(t)$ (there may also be terms with $(f(t))^s$ the denominator, s an integer and $0 < s < r$). Then $(v(t))'$ will consist of terms having $f(t)$ in the denominator at most r times plus $-\frac{rg(t)(f(t))'}{(f(t))^{r+1}}$. Since $F[t]$ is a UFD and $f(t)$ is irreducible and hence a prime element in $F[t]$ not dividing $g(t)$ or $(f(t))'$, then $f(t)$ does not divide $g(t)(f(t))'$. Thus a term with the denominator $(f(t))^{r+1}$ appears in $(v(t))'$. Hence if $f(t)$ appears in the denominator of the partial fraction decomposition of $v(t)$ it will appear in α, which is not possible. Therefore $f(t)$

does not appear in the denominator of $v(t)$ for any irreducible $f(t)$ and we conclude $v(t) \in F[t]$. It must be that $(v(t))' \in F$ since $(v(t))' = \alpha - \sum_{i=1}^{n} c_i \frac{(u_i(t))'}{u_i(t)}$ and each $\frac{(u_i(t))'}{u_i(t)} \in F$, thus $(v(t))'$ is no more than one less in degree than $v(t)$. Hence by the lemma in Section 4 and the assumption $t' = \frac{a'}{a} \in F$, $v(t)$ is not a monomial and we conclude $v(t) = ct + d$ and $(v(t))' = ct' + d' = c\frac{a'}{a} + d'$, where $c, d \in F$ and c is a constant. Then we have an expression in the form desired $\alpha = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + c\frac{a'}{a} + d' \in F$ with $c_1, \cdots, c_n, c$ constants of F and $u_1, \cdots, u_n, a, d \in F$.

To complete the proof let $\frac{t'}{t} = b'$, $b \in F$, our final case to consider where t is the exponential of an element of F. The lemma in Section 4 and its proof imply that if $f(t) \in F[t]$ is a monic irreducible other than t itself, then $(f(t))' \in F[t]$, $(f(t))' \notin F$ and $f(t)$ does not divide $(f(t))'$ even though the degree of $f(t)$ is the same as the degree of $(f(t))'$. Thus the argument above, that no monic irreducible $f(t) \in F[t]$ can occur in the denominator of $v(t)$ and that no $u_i(t)$ can be equal to some monic irreducible $f(t) \in F[t]$, is the same here when t is the exponential of an element of F, with the possible exception that some $u_i(t) = t$; otherwise we will have $f(t)$ appear in α. Thus we write $v(t) = \sum_j a_j t^j$, where each $a_j \in F$ and j ranges over a finite set of integers, positive, negative, or zero, and we take each of the quantities $u_i(t) \in F$, with the possible exception of say $u_1(t) = t$. Then each $\frac{(u_i(t))'}{u_i(t)} \in F$ and we must have $v'(t) \in F$, so the lemma implies that $v(t) \in F$ since $t' = bt$. Hence we write $\alpha = c_1 \frac{t'}{t} + \sum_{i=2}^{n} \frac{u_i'}{u_i} + v' = \sum_{i=2}^{n} \frac{u_i'}{u_i} + (c_1 b + v)'$, with $u_2, \cdots u_n, c_1 b + v \in F$. The proof is finished (968-970).

6) **A Few Examples** — Before looking at selected non-elementary indefinite integrals let's consider the function $e^{g(z)}$, where the non-constant function $g(z) \in \mathbf{C}(z)$, the field of rational functions of a complex variable. Then $g(z)$ will have at least one pole in the entire complex plane or on the Riemann surface and thus $e^{g(z)}$ will have at least one isolated essential singularity, unlike an algebraic function. By Picard's theorem we know $e^{g(z)}$ assumes every value, with one possible exception, an unbounded number of times in every neighborhood of the isolated essential singular point. For instance consider $e^{\frac{1}{z}}$ at the origin: $e^{\frac{1}{z}} = i$ for an infinite sequence approaching zero, $\{z_k\} = \left\{ \frac{2}{(1+4k)\pi i} : k = 0, \pm 1, \cdots \right\}$. All this leads us to conclude $e^{g(z)}$ is transcendental.

An algebraic argument on the transcendental nature of $e^{g(z)}$ over $\mathbf{C}(z)$ is a little more tedious, but perhaps more satisfying. Consider the monic irreducible equation over $\mathbf{C}(z)$ that $e^{g(z)}$ would otherwise satisfy, say

$e^{ng}+a_1e^{(n-1)g}+\cdots+a_n=0$, where $a_1,\cdots,a_n \in \mathbf{C}(z)$. Differentiating the latter we have $ng'e^{ng}+(a_1'+(n-1)a_1g')e^{(n-1)g}+\cdots+a_n{}'=0$. Under these conditions we know that $\{(e^g)^{n-1},(e^g)^{n-2},\cdots,(e^g),1\}$ is a basis for a vector space over $\mathbf{C}(z)$. Hence $e^{ng}=-(a_1e^{(n-1)g}+\cdots+a_n)=-\frac{1}{ng'}((a_1'+(n-1)a_1g')e^{(n-1)g}+\cdots+a_n{}')$ are identical linear combinations so the coefficients must be equal. Hence $ng'=\frac{a_n{}'}{a_n}$. But $\frac{a_n{}'}{a_n}\in \mathbf{C}(z)$. So $\frac{a_n{}'}{a_n}$ is the ratio of polynomials over **C**. The denominator may be factored into linear factors and there exists a partial fraction decomposition with constants in the numerators and linear polynomials in the denominators, or $\frac{a_n{}'}{a_n}=0$. However ng' can have no linear factors to only the first power in its denominator so $g'=0$ is the only possibility, which contradicts the assumption that g is non-constant. Hence the assumption that $e^{g(z)}$ is algebraic over $\mathbf{C}(z)$ leads to a contradiction.

There is a criterion which Rosenlicht attributes to Liouville that will assist us in examining some of the classical cases: $\int f(z)e^{g(z)}dz$ is elementary if and only if there exists an $a \in \mathbf{C}(z)$ such that $f=a'+ag'$, where $f(z),g(z)\in \mathbf{C}(z)$, $f(z)\neq 0$ and $(g(z))'\neq 0$. First we derive the latter. Let $e^g=t$. Then $\frac{t'}{t}=g'$. Let $F=\mathbf{C}(z)$. Then $F(t)=\mathbf{C}(z,t)$ is a pure transcendental extension of $F=\mathbf{C}(z)$. If

$\int f(z)e^{g(z)}dz$ is elementary we have $ft=\sum_{i=1}^{n} c_i \frac{u_i'}{u_i}+v'$, where $c_1,\cdots,c_n \in \mathbf{C}$ and $u_1,\cdots,u_n,v \in F(t)$. Using the same argument we used in Section 5, each $u_i(t)=a(g_1(t))^{v_1}\cdots(g_m(t))^{v_m}$, where $a \in F$ a nonzero element and $g_1(t),\cdots,g_m(t) \in F[t]$ all monic irreducible elements with $v_1,\cdots,v_m$ nonzero integers. Thus we may use the logarithmic derivative identity to write each $\frac{(u_i(t))'}{u_i(t)}$ in the form $\sum_{i=1}^{m} c_i \frac{g_i'}{g_i}$, so we may assume that $u_1(t),\cdots,u_n(t)$ are distinct, each being an element of F or a monic irreducible element of $F[t]$, and no c_i is zero. Suppose v is expressed as a partial fraction decomposition with respect to $F(t)$. The Section 4 lemma and its proof imply that if $h(t) \in F[t]$ is a monic irreducible other than t itself, then $(h(t))' \in F[t]$ and $h(t)$ does not divide $(h(t))'$ even though the degree of $h(t)$ is the same as the degree of $(h(t))'$. Hence t is the only possible monic irreducible factor of a denominator in v and the only possible $u_i \notin F$. Thus $\sum_{i=1}^{n} c_i \frac{u_i'}{u_i} \in F$ and the form of v is $\sum b_j t^j$ for j ranging over some integers and $b_j \in F$. Hence we have $ft=(b_1'+b_1g')t$ since $f \in F$ and $t'=g't$. Changing the nomenclature we let $a=b_1$ and we have $f=a'+ag'$ with $a \in \mathbf{C}(z)$. Conversely, if there is an $a \in \mathbf{C}(z)$ such that $f=a'+ag'$, then one elementary integral of fe^g

is $\int fe^{g}dz = \int (a' + ag')e^{g}dz = \int d(ae^{g}) = ae^{g}$. Therefore fe^{g} has an elementary integral if and only if there is an $a \in \mathbf{C}(z)$ such that $f = a' + ag'$.

For $\int e^{-z^2}dz$, we have $g' = -2z$ and we are searching for an $a \in \mathbf{C}(z)$ such that $1 = a' - 2az$. But no $a \in \mathbf{C}(z)$ can be a solution to $1 = a' - 2az$ for $a = \dfrac{p(z)}{q(z)}$, $p,q \in \mathbf{C}[z]$. If q is not constant a has a partial fraction decomposition with powers of linear factors of q in the denominators and with constant numerators. Then a' will have terms with these same factors in the denominator to at least one higher degree, so that $1 \neq a' - 2az$. If q is constant then a' is at least one less degree than $2az$ and again $1 \neq a' - 2az$. Hence $\int e^{-z^2}dz$ is not elementary. Magid also demonstrates this result but employs a little different definition of an elementary function (80-82).

For $\int \dfrac{e^{z}}{z}dz$, we have $g' = 1$ and we are searching for an $a \in \mathbf{C}(z)$ such that $\dfrac{1}{z} = a' + a$. As before no $a = \dfrac{p(z)}{q(z)} \in \mathbf{C}(z)$, $p,q \in \mathbf{C}[z]$, can be a solution to $\dfrac{1}{z} = a' + a$. For q not constant, the denominators in the partial fraction decomposition of a are powers of linear factors of q and a' will have these same factors in the denominators to at least one degree higher so that

$\frac{1}{z} \neq a' + a$. For q constant $a' + a$ has no z in the denominator. Hence $\int \frac{e^z}{z} dz$ is not elementary.

Replacing z by e^z in $\int \frac{e^z}{z} dz$ we get $\int e^{e^z} dz$ since $\frac{d(e^z)}{e^z} = dz$. So $\int e^{e^z} dz$ is not elementary. And replacing z by $\log z$ we get $\int \frac{1}{\log z} dz$ since $e^{\log z} d(\log z) = dz$. So $\int \frac{1}{\log z} dz$ is not elementary.

For $\int \frac{\sin z}{z} dz$ we make the change in variables replacing z with $\sqrt{-1}z$. Recall that $\frac{\sin z}{z} = \frac{e^{\sqrt{-1}z} - e^{-\sqrt{-1}z}}{2\sqrt{-1}z}$. Then $\int \frac{\sin \sqrt{-1}z}{\sqrt{-1}z} d(\sqrt{-1}z) = \frac{\sqrt{-1}}{2} \int \frac{e^z - e^{-z}}{z} dz$. Thus we need to show that $\int \frac{e^z - e^{-z}}{z} dz$ is not elementary. To do so consider again $F = \mathbf{C}(z)$ and $F(t) = \mathbf{C}(z,t)$, where $t = e^z$. If the integral is elementary, Liouville's theorem tells us $\frac{t - t^{-1}}{z} = \frac{t^2 - 1}{tz} = \sum_{i=1}^{n} c_i \frac{u_i'}{u_i} + v'$, where $c_1, \cdots, c_n \in \mathbf{C}$ and $u_1, \cdots, u_n, v \in F(t)$. In the same manner as before we can have $u_i's$ either in F or monic irreducible elements of $F(t)$ and v expressed in its partial fraction form and then use the Lemma of section 4. And again we conclude that the only possible $u_i \notin F$ is t, hence $\sum_{i=1}^{n} c_i \frac{u_i'}{u_i} \in F$, and the only possible monic irreducible factor in the denominator of v is t. As before we write $v = \sum b_j t^j$, with each

$b_j \in F$, concluding $\frac{1}{z} = b_1' + b_1$ since $t = t'$ and for $v = b_1 t$ we have $v' = b_1't + b_1 t' = (b_1' + b_1)t$. By the same argument as before, there is no $b_1 \in \mathbf{C}(z)$ a solution to $\frac{1}{z} = b_1' + b_1$. Therefore $\int \frac{\sin z}{z} dz$ is not elementary (970-972).

Part II — Differential Algebra

Chapter 1

Differential Rings

1) **Derivation** — A **derivation** on a ring A is a map of A into A, denoted $a \rightarrow a'$ and such that $(a+b)' = a' + b'$ and $(ab)' = a'b + ab'$ for every $a,b \in A$. If A contains unity then $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 1' + 1'$, and we conclude $1' = 0$. Successive derivatives are written $a', a'', \cdots, a^{(n)}$. We note that

$(ab)'' = (a'b + ab')' = a''b + 2a'b' + ab''$,

$(ab)''' = (a''b + 2a'b' + ab'')' = a'''b + 3a''b' + 3a'b'' + ab'''$, and so on. Thus by induction we have Leibnitz's rule: $(ab)^{(n)} = a^{(n)}b + \cdots +{}_nC_i a^{(n-i)}b^{(i)} + \cdots + ab^{(n)}$. If A is commutative, by repeated use of $(ab)' = a'b + ab'$, associativity and commutativity, we have for $n > 0$,

$(a^n)' = ((a \cdot\cdot^{(n-1\, factors)} \cdot a)a' + ((a \cdot\cdot^{(n-2\, factors)} \cdot a)a'a + \cdots + a'(a \cdot\cdot^{(n-1\, factors)} \cdot a)) = na^{n-1}a'$. If $aa^{-1} = a^{-1}a = 1$ then $a'a^{-1} + a(a^{-1})' = 0$ so $(a^{-1})' = -a^{-1}a'a^{-1} = -a'(a^{-1})^2$.

Suppose D is an integral domain with a ring derivation as defined above and F the field of quotients with a field derivation as defined in Part I Section 2. Then for $a,b \in F, b \neq 0$, we have $(a+b)' = a' + b'$, $(ab)' = a'b + ab'$, and we showed for any field a direct consequence of the latter is $\left(\frac{a}{b}\right)' = \frac{a'b - ab'}{b^2}$ and $\left(a^{(n)}\right)' = na^{(n-1)}a'$ for every integer n. Next consider the ring isomorphism assured by ordinary ring theory from D onto $D_0 = \left\{ \frac{a}{1} \in F \middle| a \in D \right\} \subset F$ defined by $a \to \frac{a}{1}$. Then D_0 is an integral domain. But $D_0 \subset F$, so $\left(\frac{a}{1}\right)' = \frac{a' \cdot 1 - a \cdot 1'}{1^2} = \frac{a'}{1}$ and under the ring isomorphism a' is sent to $\left(\frac{a}{1}\right)'$ for every $a \in D$. It follows that the sum and product rules are preserved by the isomorphism. Hence D and D_0 are isomorphic with respect to the corresponding derivations of D and F.

The derivation on an integral domain has a natural extension to the field of quotients. As in ordinary field theory, elements in the field of quotients F are regarded as quotients of elements in D and equality of $\frac{a}{b}, \frac{c}{d} \in F$ defined by $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = cb$, $a,b,c,d \in D$, $b,d \neq 0$. Our extended derivation on F, defined by $\frac{a}{b} \to \left(\frac{a}{b}\right)'$, is well defined since $\left(\frac{a}{b}\right)' = \left(\frac{c}{d}\right)'$ if $\frac{a}{b} = \frac{c}{d}$. To see that the latter is true consider $\frac{a}{b} = \frac{c}{d} \in F$. Then $ad = cb \in D$. So $a'd + ad' = c'b + cb'$ and $a'd - cb' = c'b - ad'$. Hence $\frac{a'}{1}\frac{d}{1} - \left(\frac{a}{b}\right)\frac{d}{1}\frac{b'}{1} = \frac{c'}{1}\frac{b}{1} - \left(\frac{c}{d}\right)\frac{b}{1}\frac{d'}{1}$ and $\frac{a'b - ab'}{b^2} = \frac{c'd - cd'}{d^2}$. Thus $\left(\frac{a}{b}\right)' = \left(\frac{c}{d}\right)'$. To assert that our extension is indeed a derivation on F we need to verify that the sum and product rules work properly,

$\left(\frac{a}{b}+\frac{c}{d}\right)' = \left(\frac{a}{b}\right)' + \left(\frac{c}{d}\right)'$ and $\left(\frac{ac}{bd}\right)' = \left(\frac{a}{b}\right)'\left(\frac{c}{d}\right)+\left(\frac{a}{b}\right)\left(\frac{c}{d}\right)'$. To do so, on the left of the sum rule we apply the quotient derivation to the sum

$\left(\frac{ad+bc}{bd}\right)' = \left(\frac{(ad+bc)'(bd)-(ad+bc)(bd)'}{(bd)^2}\right)$ which reduces to $\frac{a'b-ab'}{b^2}+\frac{c'd-cd'}{d^2}$

after some tedium. In the product case with more tedium we show that

$\frac{(ac)'(bd)-(ac)(bd)'}{(bd)^2} = \left(\frac{a'b-ab'}{b^2}\right)\left(\frac{c}{d}\right)+\left(\frac{a}{b}\right)\left(\frac{c'd-cd'}{d^2}\right)$. Thus following Kaplansky we write the first theorem in Part II.

Theorem 1.1 — A derivation on an integral domain has a unique extension to the quotient field (9).

2) **Differential Rings** — A **differential ring** is a commutative ring with unity together with a derivation. Adopting the same examples as Kaplansky, we see that imposition of the trivial derivation, the map that sends every element into 0, will convert any commutative ring with unity into a differential ring. The ring of infinitely differentiable functions on the real line with the derivation we know from calculus meets the needs of our postulates and hence we have a differential ring. The ring of entire functions again with the customary derivation is the differential ring of entire functions. We recall that an entire function is analytic at each point in the entire finite complex plane and the zeros of a nonzero analytic function are isolated—none is a limit point. Let $f(z)$ and $g(z)$ be arbitrary entire functions. Then $f(z)g(z)=0$ if and only if $f(z)=0$ or $g(z)=0$. Thus there are no divisors of

zero and we have the differential integral domain of entire functions. Hence by our Theorem 1.1, the field of quotients of this integral domain, the field of meromorphic functions, is a differential field by the extension of the derivation from the differential integral domain of entire functions. Quotients of entire functions then have convergent Laurent series representations at every point in the finite plane so the notion of meromorphic here is consistent with the notion of meromorphic advanced in Part I. In fact we may take functions analytic in a domain of the complex plane.

Next we let A be any differential ring and $A[x]$ be the ring of all polynomials in the indeterminate x, with coefficients in A. If A is a differential field we have that $A[x]$ is an integral domain and we let $A(x)$ denote the field of rational functions in x. The derivation on A, that is the map A into A defined by $a \to a'$, may be extended to a map of $A[x]$ into $A[x]$ by assigning $x \to x'$ arbitrarily, defining $(x^n)' = nx^{n-1}x'$ and applying the rules of sum and product to the elements $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$ to give $(f(x))' = a_n' x^n + (na_n + a_{n-1}')x^{n-1} + \cdots + a_0'$. Then we have $(f(x) + g(x))' = (f(x))' + (g(x))'$ and $(f(x)g(x))' = (f(x))'g(x) + f(x)(g(x))'$ for every $f(x), g(x) \in A[x]$. Again if A is a differential field then by Theorem 1.1 with the latter extension to $A[x]$ we may extend the derivation to the field of quotients, $A(x)$ (9-10). This example is actually a special case of the next and there our treatment will be more careful.

To continue with Kaplansky we need additional notation. Let A be a differential ring and $A[x_i]$ be the polynomial ring in an infinite number of ordinary indeterminates $x_0, x_1, x_2 \cdots$. We extend the derivation on A to a unique derivation on $A[x_i]$ by the assigned relations $x_i' = x_{i+1}$ and changing the notation we have $x_0 = x$, $x_n = x^{(n)}$. Hence $\left(x^{(i)}\right)' = x^{(i+1)}$. This is called the adjunction of a differential indeterminate and we adopt the notation $A\{x\}$ for the resulting differential ring, elements being differential polynomials in x (or in other words, ordinary polynomials in x and its derivatives).

That the latter extension is indeed a derivation on $A\{x\}$ satisfying the sum and product postulates deserves a few comments and it seems appropriate to make them in a more general setting (Peterson suggested the approach taken here in private communication with the author.) Magid displays the Lemma below as an observation in a slightly different context (2). By definition the derivation on a differential ring is an additive group homomorphism satisfying the derivation product rule. Let R be a commutative ring. Let $\overline{R} = R[x]/\langle x^2 \rangle$ and let $\varepsilon = x + \langle x^2 \rangle \in \overline{R}$. Thus we have $\overline{R} = R[\varepsilon]$ with elements of the form $r + s\varepsilon$, $r, s \in R$ and $\varepsilon^2 = 0$. Let $D{:}R \to R$ be any additive group homomorphism. Then it follows that $\phi_D{:}R \to \overline{R}$ defined by $\phi_D(r) = r + D(r)\varepsilon$ is an additive group homomorphism.

Lemma 2.1 — The additive group homomorphism D is a derivation if and only if ϕ_D is a ring homomorphism.

Proof — For $r,s \in R$ we have $\phi_D(rs) = (rs) + D(rs)\varepsilon$ and $\phi_D(r)\phi_D(s) = (r + D(r)\varepsilon)(s + D(s)\varepsilon) = (rs) + (D(r)s + rD(s))\varepsilon$. So $\phi_D(rs) = \phi_D(r)\phi_D(s)$ if and only if $D(rs) = D(r)s + rD(s)$.

Let A be any differential ring with the derivation $d: A \to A$. Let $\{x_\alpha | \alpha \in \mathbf{A}\}$ be any family of (algebraically independent) indeterminates over A. Finally let $R = A[x_\alpha | \alpha \in \mathbf{A}]$ be the polynomial ring over A.

Theorem 2.2 — For any map $\gamma: \mathbf{A} \to R$, there exists a unique derivation $D: R \to R$ with $D(a) = d(a)$ for all $a \in A$ and $D(x_\alpha) = \gamma(\alpha)$ for all $\alpha \in \mathbf{A}$.

For the case at hand we take $\{x_\alpha | \alpha \in \mathbf{A}\}$ to be $\{x, x', x^{(2)}, \cdots\}$ and $\gamma(i) = x^{(i+1)}$ for $i = 0,1,2,\cdots$, the derivation extension from A to $A[x, x', x^{(2)}, \cdots] = A\{x\}$ follows. We note that $A\{x\}$ is an integral domain if A is a field. By Theorem 1.1 it follows that the derivation may be extended to the field of quotients containing elements that are quotients of differential polynomials. We denote the field of differential rational functions of x by $A\langle x \rangle$. The notation $\{\ \}$ and $\langle\ \rangle$ will also be used when the elements adjoined are not differential indeterminates, but rather elements of a larger differential ring or field. Elaborating, by the use of $\{\ \}$ we mean the adjunction of elements and all their derivatives from a larger differential ring or field so that the elements of the extended ring are all the polynomial expressions in the adjoined elements and derivatives of elements with coefficients from the original differential ring or field.

In the cases we use $\langle\ \rangle$ the elements of the extension are all the rational expressions in the adjoined elements and derivatives of elements from the larger differential ring or field over the original differential ring or field.

Proof of Theorem 2.2 — The set $\{x_a | \alpha \in \mathbf{A}\}$ generates R as a ring over A. If two derivations of R agree on A and agree at each x_a, the sum and product rules for derivations show that they agree on all of R. Thus if it exists, a derivation on R extending d is unique.

For existence, first let $\pi_1, \pi_2 : \overline{R} \to R$ be two projection maps given by $\pi_1(r + s\varepsilon) = r$ and $\pi_2(r + s\varepsilon) = s$ where like above $\overline{R} = R[\varepsilon]$ with $\varepsilon^2 = 0$. Then π_1 is a ring homomorphism and π_2 is an additive group homomorphism and for any $\overline{r} \in \overline{R}$ we have $\overline{r} = \pi_1(\overline{r}) + \pi_2(\overline{r})\varepsilon$.

Since $d: A \to A$ is a derivation, by Lemma 2.1 we have a ring homomorphism $\phi_d : A \to \overline{A} = A + A\varepsilon$ given by $\phi_d(a) = a + d(a)\varepsilon$ for $a \in A$. We may view this as the ring homomorphism $\phi_d : A \to \overline{R}$ since $\overline{A}$ is a subring of $\overline{R}$.

Now suppose a map $\gamma : \mathbf{A} \to R$ is given and we define $\overline{\gamma} : \mathbf{A} \to \overline{R}$ by $\overline{\gamma}(\alpha) = x_\alpha + \gamma(\alpha)\varepsilon$. By the universal mapping property for polynomial rings, there is a unique ring homomorphism $\phi : R \to \overline{R}$ such that $\phi(a) = \phi_d(a)$ for $a \in A$ and $\phi(x_a) = \overline{\gamma}(\alpha)$ for $\alpha \in \mathbf{A}$. Then $\pi_1(\phi(a)) = \pi_1(\phi_d(a)) = \pi_1(a + d(a)\varepsilon) = a$ for $a \in A$ and $\pi_1(\phi(x_\alpha)) = \pi_1(\overline{\gamma}(a)) = \pi_1(x_\alpha + \gamma(a)\varepsilon) = x_\alpha$ for $\alpha \in \mathbf{A}$. Thus $(\pi_1 \circ \phi)(a) = a$ and

$(\pi_1 \circ \phi)(x_\alpha) = x_\alpha$. But $\pi_1 \circ \phi$ is a ring homomorphism and $\{x_\alpha | \alpha \in \mathcal{A}\}$ generates R over A. So $(\pi_1 \circ \phi)(r) = r$ for every $r \in R$.

Next let $D = \pi_2 \circ \phi$. Then $D: R \to R$ is an additive group homomorphism. For any $r \in R$ we have $\phi(r) = \pi_1(\phi(r)) + \pi_2(\phi(r))\varepsilon = r + D(r)\varepsilon = \phi_D(r)$, and hence $\phi = \phi_D$. Since ϕ is a ring homomorphism Lemma 2.1 tells us D is a derivation. For any $a \in A$ we have $D(a) = \pi_2(\phi(a)) = \pi_2(\phi_d(a)) = \pi_2(a + d(a)\varepsilon) = d(a)$. Finally for any $\alpha \in \mathcal{A}$ we have $D(x_\alpha) = \pi_2(\phi(x_\alpha)) = \pi_2(\bar{\gamma}(\alpha)) = \pi_2(x_\alpha + \gamma(\alpha)\varepsilon) = \gamma(\alpha)$. Thus D is the required extension of d to R. This completes the proof of Theorem 2.2.

The elements of any differential ring A whose derivatives are zero form a subring C called the **ring of constants**. The latter follows immediately by application of the derivation sum and product rules. If A is a differential field then C is a subfield since $(a^{-1})' = -a'(a^{-1})^2$ (Section 1). It follows from $1' = 0$ that C contains the subring generated by 1, the unity of A.

If $I \subset A$ is an ideal in the differential ring A, we say that I is a **differential ideal** if $a \in I$ implies $a' \in I$, or equivalently $I' \subset I$. In the ring A/I we introduce the derivation $(a+I)' = a' + I$, that is, a map of A/I into A/I defined by $a + I \to a' + I$. Satisfaction of the sum and product rules is immediate:

$((a+I)+(b+I))' = (a+b)' + I = (a'+b') + I = (a'+I) + (b'+I) = (a+I)' + (b+I)'$, and

$((a+I)(b+I))' = (a'b + ab') + I = ((a'b) + I) + ((ab') + I) = (a+I)'(b+I) + (a+I)(b+I)'$

Next we have $a+I=b+I$ if and only if $a-b\in I$. Then $a'-b'=(a-b)'\in I$ if and only if $a'+I=b'+I$. Thus our derivation of a coset is independent of the choice of representative and we have defined a derivation on A/I.

Let A and B be differential rings. A **differential homomorphism** from A to B is a ring homomorphism that commutes with derivation. If I is a differential ideal in A the natural homomorphism from A to A/I is differential. The terms **differential isomorphism** and **differential automorphism** are defined as expected.

Theorem 2.3 "The First Isomorphism Theorem for Differential Rings" — Let I be the kernel of a differential homomorphism defined on a differential ring A. Then I is a differential ideal in A, and A/I is differential isomorphic to the image (Kaplansky 10-11).

Proof — That I is an ideal follows from regular quotient ring theory. To see that I is differential, let $\phi: A\to\phi[A]$ be the differential homomorphism in question (adopting Fraleigh's [ ] notation for the image of a set.) For $a\in I$ we have $\phi(a)=0$ and $(\phi(a))'=0$. Hence $\phi(a')=0$, and $a'\in I$. That A/I is differential follows from the definition of derivation on cosets above and the canonical homomorphism $\pi: A\to {}^{A}\!/_{I}$ that sends a' to $a'+I$ for every $a\in A$. We see that π is a differential homomorphism since $\pi(a')=a'+I=(a+I)'=(\pi(a))'$ for every $a\in A$. Again by regular quotient ring theory there exists an isomorphism $\mu\colon {}^{A}\!/_{I} \to \phi[A]$ such that $\mu(a+I) = \phi(a)$ for every $a \in A$. Then $(\mu(a+I))' = (\phi(a))' = \phi(a')$. But $\mu(a'+I) = \phi(a')$. So $(\mu(a+I))' = \mu(a'+I) = \mu((a+I)')$. Hence $\mu\colon {}^{A}\!/_{I} \to \phi[A]$ is a differential isomorphism.

3) **Radical Ideals** — An ideal I is defined to be a **radical ideal** if $a^n \in I$ implies $a \in I$, the usual definition.

Lemma 3.1 — If $ab \in I$, a radical differential ideal, then $ab' \in I$ and $a'b \in I$.

Proof — We have $ab \in I$. So $a'b + ab' = (ab)' \in I$, $ab'(ab)' \in I$, and $ab'(a'b) = a'b'(ab) \in I$. Thus $(ab')^2 = ab'((ab)' - (a'b)) = ab'(ab)' - ab'(a'b) \in I$. Therefore $ab' \in I$ and $a'b = (ab)' - ab' \in I$.

Lemma 3.2 — Let I be a radical differential ideal in a differential ring A, and let S be any subset of A. Define T to be the set of all x in A with $xS \subset I$. Then T is a radical differential ideal in A.

Proof — It follows that $0s = 0 \in I$ and for each $x \in T$, $z \in T$ and for every $s \in S$ we have $(x+z)s = xs + zs \in I$ and $-xs \in I$, so T is an additive subgroup of A. Suppose $y \in A$. Then $(yx)s = y(xs) \in I$ since $(xs) \in I$. Hence $yx \in T$ and T is an ideal in A. Next suppose $x \in T$ and $x' \notin T$. Then $x's \notin I$ and $xs \in I$ for some $s \in S$. So $(xs)' \in I$ since I is a radical differential ideal in A. Hence by Lemma 3.1 $x's \in I$. Thus the assumption that $x' \notin T$ leads to a contradiction. Thus T is a differential ideal in A. Finally, suppose $x^n \in T$. For any $s \in S$ it follows $x^n s^n = (x^n s^{n-1})s \in I$. But then $xs \in I$ since I is a radical differential ideal in A. Therefore $x \in T$ and T is a radical differential ideal in A.

Let $\{I_\alpha | \alpha \in \mathrm{A}\}$ be a collection of radical ideals in a commutative ring A. Let $a^n \in \bigcap_{\alpha \in \Lambda} I_\alpha$. Then $a \in I_\alpha$ for every $\alpha \in \mathrm{A}$ since each I_α is a radical ideal. Hence $\bigcap_{\alpha \in \Lambda} I_\alpha$ is a radical ideal. Similarly if $\{I_\alpha | \alpha \in \mathrm{A}\}$ is a collection of differential ideals in a differential ring A, then $\bigcap_{\alpha \in \Lambda} I_\alpha$ is a differential ideal in A. It follows that any intersection of radical differential ideals is a radical differential ideal. Therefore for any set S in a differential ring A there is a unique smallest radical differential ideal containing S, the intersection of all the radical differential ideals in A containing S, denoted $\{S\}$.

Lemma 3.3 — Let a be any element and S any subset of a differential ring A. Then $a\{S\} \subset \{aS\}$.

Proof — Let $\{a\}$ be the singleton subset containing the element a. The set $T = \{x \in A | ax \in x\{a\} \subset \{aS\}\}$ is a radical differential ideal by Lemma 3.2. We have $S \subset T$ since $as \in s\{a\} \subset \{aS\}$ for every $s \in S$. But $\{S\}$ is the intersection of all the radical differential ideals in A containing S. So $\{S\} \subset T$. Therefore $a\{S\} \subset \{aS\}$.

Lemma 3.4 — Let S and T be any subsets of a differential ring. Then $\{S\}\{T\} \subset \{ST\}$.

Proof — The set $P=\{x|x\{T\}\subset\{ST\}\}$ contains S, since for $s\in S$ by Lemma 3.3 $s\{T\}\subset\{sT\}\subset\{ST\}$. Now P is a radical differential ideal by Lemma 3.2. Hence $\{S\}\subset P$. Thus $\{S\}\{T\}\subset\{ST\}$.

4) **Ritt Algebras** — The radical of an ideal I is defined to be the set of all elements with some power in the ideal, denoted $Rad\,I$. Let H be the radical of an ideal I in the commutative ring A. We have $0\in H$ since $0\in I$. Suppose $h,g\in H$ then $h^n,g^m\in I$ for some n,m positive integers. Take $n\geq m$ and consider the binomial expansion of $(h+g)^{n+m}=h^{n+m}+\cdots+\binom{n+m}{m}h^n g^m+\cdots+g^{n+m}$. We have the term $\binom{n+m}{m}h^n g^m\in I$ and every term to its left can be written as a product of some element of A with h^n and every term to its right can be written as a product of some element of A with g^m. Hence $(h+g)^{n+m}\in I$ and $h+g\in H$. For every $h^n\in I$ then $-h^n\in I$, so H is an additive subgroup of A. For any $a\in A$ we have $(ah)^n=a^n h^n\in I$. Hence $ah\in H$ and H is an ideal in A. For the integer $n>0$, if $h^n\in H$ we have $h^{nm}=\left(h^n\right)^m\in I$ for some integer $m>0$ and hence $h\in H$. Therefore the radical of an ideal in A is a radical ideal in A.

A differential ideal example — Over a field of characteristic 2, let A be the two-dimensional algebra with basis $1,x$ where $x^2=0$ and 1 is unity. Define a derivation of A by setting $1'=0$ and $x'=1$. The radical of the zero ideal is generated by x but $x'=1$ is not an element of the radical since $1^n=1$ for every integer $n>0$. Thus the radical is not a differential ideal. With this example Kaplansky observes that it is not true without suitable additional hypothesises that the radical of a differential ideal is a differential ideal.

Definition — A **Ritt algebra** is a differential ring containing the field of rational numbers (which is necessarily a subfield of the ring of constants). A Ritt algebra is actually an algebra over the rational numbers in the usual sense.

Lemma 4.1 — Let I be a differential ideal in a Ritt algebra, and let a be an element with $a^n \in I$. Then $(a')^{2n-1} \in I$.

Proof — Applying our derivation power rule gives us $na^{n-1}a' = (a^n)' \in I$. Thus $a^{n-1}a' \in I$ since we have multiplication by $1/n$ in the Ritt algebra. The latter is the case $k=1$ of the statement $a^{n-k}(a')^{2k-1} \in I$. Assume the statement true for arbitrary k, then differentiating we have $(n-k)a^{n-k-1}(a')^{2k} + (2k-1)a^{n-k}(a')^{2k-2}a'' \in I$. Multiplying by a' and taking b as the result, $b = (n-k)a^{n-k-1}(a')^{2k+1} + (2k-1)a^{n-k}(a')^{2k-1}a'' \in I$. The second term of b is in I by the induction assumption. Hence $a^{n-k-1}(a')^{2k+1} = \frac{1}{n-k}\left(b-(2k-1)a^{n-k}(a')^{2k-1}a''\right) \in I$, the $k+1$ case of the statement we are proving by induction. Continuing we finally come to $k=n$ and we have the conclusion $(a')^{2n-1} \in I$.

Lemma 4.2 — In a Ritt algebra the radical of a differential ideal is a differential ideal.

Proof — Let I be a differential ideal in a Ritt algebra. We showed above that the radical of an ideal is a radical ideal. Thus it will suffice to show that the radical of I is differential. Let $a \in Rad\, I$. Then $a^n \in I$ for some integer $n > 0$. By Lemma 4.1 $(a')^{2n-1} \in I$. Then $a' \in Rad\, I$. Therefore the radical of I is a differential ideal (Kaplansky 11-12).

Chapter 2

Extension of Isomorphisms

5) **Krull's Theorem** — Like ordinary ring theory, in differential rings any radical differential ideal is the intersection of prime differential ideals. Kaplansky bases the proof of this theorem on the following lemma.

Lemma 5.1 — Let T be a multiplicatively closed subset of a differential ring A. Let Q be a radical differential ideal maximal with respect to the exclusion of T. Then Q is prime.

Proof — Suppose the contrary. Then there exist $ab \in Q, a \notin Q$ and $b \notin Q$. Then $\{Q,a\} = \{\{a\} \cup Q\}$ and $\{Q,b\} = \{\{b\} \cup Q\}$ are radical differential ideals properly larger than Q. Hence $\{Q,a\}$ and $\{Q,b\}$ contain $t_1, t_2 \in T$. But $(\{a\} \cup Q)(\{b\} \cup Q) \subset Q$ since its elements are finite sums of products of the form $aq_\lambda, bq_\lambda, q_\gamma q_\lambda$ and ab, all elements of Q, where $q_\lambda, q_\gamma \in Q$ and $\{a\}$, $\{b\}$ are singleton sets. So $t_1 t_2 \in \{Q,a\}\{Q,b\} \subset \{(\{a\} \cup Q)(\{b\} \cup Q)\} \subset Q$ by Lemma 3.4 a contradiction that Q is maximal with respect to the exclusion of the multiplicatively closed T.

Theorem 5.2— Let I be a radical differential ideal in a differential ring A. Then I is the intersection of prime differential ideals.

Proof — Let x be an element not in I. Our task is to find a prime differential ideal containing I but not containing x, for then I will equal the intersection of these various ideals. Let T be the set of powers of x. Consider the set $\{U_\lambda | \lambda \in \Gamma\}$ of all radical differential ideals containing I but not containing x. Zorn's Lemma says that if the nonempty partially ordered set Δ is such that every chain in Δ has an upper bound in Δ, then Δ contains a maximal element. Containment is a partial ordering on $\{U_\lambda | \lambda \in \Gamma\}$, $I \in \{U_\lambda | \lambda \in \Gamma\}$ and any chain $\{U_{\lambda_j} | j \in J\}$ in $\{U_\lambda | \lambda \in \Gamma\}$ has an upper bound in $\{U_\lambda | \lambda \in \Gamma\}$ namely $\bigcup_{j \in J} U_{\lambda_j}$. By Zorn's lemma we select a maximal radical differential ideal Q containing I and excluding x. But Q contains no powers of x, for otherwise $x \in Q$. Hence Q is a radical differential ideal maximal with respect to the exclusion of T. Lemma 5.1 asserts that Q is prime.

6) **Extension of Prime Ideals** — Let A be a differential ring contained in B. We tacitly assume that A and B have the same unity. Suppose P is a prime differential ideal in A and I is a radical ideal in B which contracts to P, that is $I \cap A = P$. In Theorems 6.1 and 6.2 respectively we address the conditions under which, (1) I may be enlarged to a prime ideal that contracts to P, and (2) I is the intersection of prime ideals contracting to P.

Theorem 6.1 — Let B be a differential ring with a differential subring A. Let I be a radical differential ideal in B such that $P = I \cap A$ is a prime differential ideal in A. Then I can be enlarged to a prime differential ideal in B which also contracts to P.

Proof — Take T to be the complement of P in A. Then T is a multiplicatively closed subset of A and hence of B, for if $t_1, t_2 \in T$ then $t_1 t_2 \in P$ is a contradiction since P is a prime differential ideal disjoint from T. We have I disjoint from T in B since T is a subset of A disjoint from $P = I \cap A$. Again Zorn's lemma guarantees the existence of a radical differential ideal Q in B containing I and maximal with respect to the exclusion of T. Then $Q \cap A = P$. Therefore by Lemma 5.1 Q is the prime differential ideal in B we seek that contains I and contracts to P.

Theorem 6.2 — Let B be a differential ring with a differential subring A. Let I be a radical differential ideal in B such that $ab \in I, a \in A, b \in B$ implies that $a \in I$ or $b \in I$ (Note that $P = I \cap A$ is consequently a prime differential ideal in A.) Then I can be expressed as an intersection of prime differential ideals in B, each of which also contracts to P.

Proof — First the parentheses: suppose $a,b \in A$ and $ab \in P = I \cap A$. Note that $a,b \in B$ hence $ab \in I, a \in A, b \in B$, which implies $a \in I$ or $b \in I$. Thus $a \in P$ or $b \in P$ and P is a prime ideal in A. We have P differential since it is the intersection of differential subrings. Next let $x \in B$ and $x \notin I$. We are searching for a prime ideal in B which contains I, contracts to P, and does not contain x. Let $T = \{ax^n | a \in A, a \notin P, n \geq 0 \text{an integer}\}$. We see that T is multiplicatively closed. We have $a \notin I$, $x \notin I$ and I is a radical differential ideal so $x^n \notin I$. Since $a \in A$ and $x^n \in B$ by our hypothesis $ax^n \notin I$ for every n so T is disjoint from I. Once again Zorn's lemma assures the existence of a radical differential ideal Q in B containing I and maximal with respect to the exclusion of T. By

Lemma 5.1 Q is a prime ideal in B. If $a \in Q \cap A$ and if $a \notin P$, then $a \in T$ and $a \in Q \cap T$, a contradiction. Hence $Q \cap A \subset P = I \cap A \subset Q \cap A$, and Q contracts to P. Finally, $x \notin Q$ since $x \in T$.

7) Lemma on Polynomial Rings —

Lemma 7.1 — Let K and L be fields with $K \subset L$. Let B be the ring obtained by adjoining a (possibly infinite) set of indeterminates to L, A the ring obtained by adjoining the same indeterminates to K. Let P be an ideal in A, J the ideal in B generated by P, and I the radical of J. Then: (a) If P is a radical ideal, $I \cap A = P$. (b) Suppose that P is a prime ideal and that $ab \in I$ with $a \in A$, $b \in B$. Then either $a \in P$ or $b \in I$. (c) Suppose that the characteristic is 0 and that $P \neq A$ (P need not be a radical ideal). Let y be one of the indeterminates and s an element that is in L but not in K. Then $y - s \notin I$.

Proof — Regard L as a vector space over K. Then for each $l_\lambda \in L$ we have a unique expression $l_\lambda = \sum_{\gamma \in \Gamma} k_{\gamma\lambda} u_\gamma$ where $\{u_\gamma \in L | \gamma \in \Gamma,\}$ is the basis of L over K, Γ an index set, and $k_{\gamma\lambda} \in K$, and all but finitely many $k_{\gamma\lambda}$ are 0. With no implication that Γ is of countable cardinality we let $u_1 = 1$. Then for $b \in B = L[x]$ where $x = (x_\nu | \nu \in \mathrm{N})$ we have

$$b = \sum_{\lambda \in \Lambda} l_\lambda (x_{\nu_1})^{j(\lambda,\nu_1)} \cdots (x_{\nu_n})^{j(\lambda,\nu_n)} = \sum_{\lambda \in \Lambda} \sum_{\gamma \in \Gamma} k_{\gamma\lambda} u_\gamma (x_{\nu_1})^{j(\lambda,\nu_1)} \cdots (x_{\nu_n})^{j(\lambda,\nu_n)} = \sum_{\gamma \in \Gamma} a_\gamma u_\gamma \text{ , where}$$

Λ is a finite indexing set and each $a_\gamma \in A$ is of the form

$\sum_{\lambda\in\Lambda} k_{\gamma\lambda}(x_{v_1})^{j(\lambda,v_1)}\cdots(x_{v_n})^{j(\lambda,v_n)}$. Hence $b \in A$ only when all $a_\gamma \in A$ vanish except a_1.

We observe that $J = \{b = \sum p_\gamma u_\gamma | p_\gamma \in P\}$. Hence $J \cap A = P$ (for arbitrary P).

a) Take P to be a radical ideal in A and $b \in I \cap A$. Then since I is the radical of J we have $b^n \in J$ for some integer $n > 0$. But $b^n \in A$. So $b^n \in J \cap A = P$. Since P is a radical ideal, $b \in P$. Hence $I \cap A \subset P$. For the reverse containment $P = J \cap A \subset I \cap A$ since I is the radical of J. Therefore $I \cap A = P$.

b) Suppose further that P is prime and that $ab \in I, a \in A, b \in B$. Then $a^n b^n \in J$ for some n since I is the radical of J. Take $b^n = \sum a_\gamma u_\gamma$. Thus $\sum (a^n a_\gamma) u_\gamma = a^n b^n \in J$. Then each $a^n a_\gamma \in P$ since $J = \{\sum p_\gamma u_\gamma | p_\gamma \in P\}$. Now P is prime, hence $a \in P$ or each $a_\gamma \in P$, in which case $b^n = \sum a_\gamma u_\gamma \in J$ and hence $b \in I$.

c) Presume that $y - s \in I$. We will find a contradiction. First, $(y-s)^m \in J$ for some m. Let $I_0 = \{f(y) \in L[y] | f(y) \in J\}$, the set of polynomials in y over L contained in J. Then $(y-s)^m \in I_0$. Now since J is an ideal in B, L is a field and I_0 involves only one indeterminate then I_0 is a principal ideal whose generator divides $(y-s)^m$. The generator cannot be a nonzero element of L (constant) for then J would be all of B, and $P = J \cap A$ would be all of A, contradicting our hypothesis. Thus the generator must be of the form $(y-s)^r$ with

$r \geq 1$. Again invoke the vector space basis $\{u_\gamma\}$, taking $u_1 = 1$ and $u_2 = s$. We have from above that when $(y-s)^r$ is expressed as a linear combination of the u_γ's, each separate coefficient must be in P and hence in $J = \{\sum p_\gamma u_\gamma | p_\gamma \in P\}$. In particular the polynomial coefficient of u_1, say p_1, is over K and $p_1 \in J$ since P is the generator of $J = \{f(y) = \sum p_\gamma u_\gamma | p_\gamma \in P\}$ in $B = L\{y\}$. Thus $p_1 \in I_0 = \{f(y) \in L[y] | f(y) \in J\} = \langle (y-s)^r \rangle$. But p_1 is over K, $s \notin K$ and by the binomial formula $p_1 = y^r + 0y^{r-1} + 0y^{r-2} + \cdots$ is monic of degree r in y, so $p_1 = (y-s)^r = y^r - rsy^{r-1} + \frac{1}{2}r(r-1)s^2y^{r-2}\cdots$. We have $rs \neq 0$ since the characteristic is 0. Hence we found our contradiction.

8) **Admissible Isomorphisms** — An isomorphism between two fields K and L will be called **admissible** if there exists a field M containing both K and L.

Theorem 8.1 — Let M be a differential field of characteristic 0, K and L differential subfields, and let there be given a differential isomorphism S of K onto L. Then S can be extended to an admissible differential isomorphism defined on M.

Kaplansky asserts that by the principal of transfinite induction it will suffice to show for $u \in M$ and $u \notin K$ that we can define an extension of the isomorphism S to u so that the image of u lies in a suitable extension of L. It is our purpose here to modestly expand the justification of the assertion by outlining a method employing Zorn's lemma after proving the following:

Lemma 8.2 — Let M be a differential field of characteristic 0, K and L differential subfields, and let there be given a differential isomorphism S of K onto L. Let $u \in M$ and $u \notin K$, then there exists an extension of the isomorphism S to u so that the image v of u lies in $L\{v\}$ and the fields of quotients of $K\{u\}$ and $L\{v\}$ are differential isomorphic.

Proof — Let $K\{u\}$ be the differential integral domain obtained by adjoining u to K where $u \in M$ and $u \notin K$, and let $K\{y\}$ be the differential integral domain obtained by adjoining the differential indeterminate y. Let P_1 be the kernel of the differential homomorphism ϕ from $K\{y\}$ onto $K\{u\}$ defined by sending y into u. Let $ab \in P_1$. Then $\phi(a)\phi(b) = \phi(ab) = 0$ and either $\phi(a) = 0$ or $\phi(b) = 0$ since $K\{u\}$ has no divisors of zero. Hence $a \in P_1$ or $b \in P_1$. Thus P_1 is a prime differential ideal in $K\{y\}$. If we apply the differential isomorphism S of K onto L to a map of $K\{y\} \to L\{y\}$ sending y to y and employ the commutative property of derivation and differential isomorphisms we can demonstrate that the result is a differential isomorphism from $K\{y\}$ onto $L\{y\}$ with the usual tedium. In this manner we apply the differential isomorphism S to P_1 and obtain a prime differential ideal P in $L\{y\}$. We let J be the ideal in $M\{y\}$ generated by P. Then J consist of all the finite sums $\sum p_i m_i$, $p_i \in P$ and $m_i \in M\{y\}$, so

$\left(\sum p_i m_i\right)' = \sum(p_i' m_i + p_i m_i') \in J$ and J is a differential ideal. Let I be the radical of J. Then I is a radical ideal for if $a^n \in I$ we have $(a^n)^m = a^{nm} \in J$ and $a \in I$. Since $M\{y\}$ contains M, a field of characteristic 0, it is a Ritt algebra, so by Lemma 4.2 I is a differential ideal. Thus I is a radical differential ideal in $M\{y\}$. Now P is a prime differential ideal in $L\{y\}$ so it is necessarily a radical differential ideal since if $a^{n-1}a = a^n \in P$ we conclude $a^{n-1} \in P$ or $a \in P$ and if it is $a^{n-1} \in P$ we continue and after at most $n-1$ tries $a \in P$. By Lemma 7.1(a), $I \cap L\{y\} = P$ (K and L are replaced by L and M respectively so B corresponds to $M\{y\}$ and A corresponds to $L\{y\}$). By Theorem 6.1 I can be enlarged to a prime differential ideal Q in $M\{y\}$ which contracts to P, $Q \cap L\{y\} = P$.

Let v be the image of y under the natural homomorphism from $M\{y\}$ onto $M\{y\}/Q$, a differential integral domain. Next we define a differential homomorphism from $K\{y\}$ onto $L\{v\}$ in two steps. The first step is from $K\{y\}$ onto $L\{y\}$ by means of the isomorphism S and the second step is from $L\{y\}$ onto the differential integral domain $L\{v\} = L\{y\}/Q \cap L\{y\}$ by sending y to v. Hence the kernel of the composite map $K\{y\}$ onto $L\{v\}$ is $P_1 \cong P = Q \cap L\{y\}$. But P_1 is the kernel of the differential homomorphism $K\{y\}$ onto $K\{u\}$. Thus we get a differential isomorphism between differential integral domains $K\{u\}$ and $L\{v\}$ extending S. By Theorem 1.1 the isomorphism extends uniquely to a differential isomorphisms between the quotient fields $K\langle u\rangle$ and $L\langle v\rangle$ of $K\{u\}$ and $L\{v\}$. We have $K\langle u\rangle \subset M$ and $L\langle v\rangle \subset {}^{M\{y\}}\!/_{Q}$. But M may be viewed as a differential subfield of ${}^{M\{y\}}\!/_{Q}$ by the natural injection $M \rightarrow {}^{M\{y\}}\!/_{Q}$ sending $m \in M$ into $m+Q$. So the quotient field N of the differential integral domain ${}^{M\{y\}}\!/_{Q}$ is a field containing both $K\langle u\rangle$ and $L\langle v\rangle$. This concludes the proof of Lemma 8.2.

Now we turn to the proof for Theorem 8.1. We will offer an outline containing enough details to comfortably continue beyond without further discourse (Peterson suggested the approach taken here in private communication with the author.) In doing so we will need a more robust notation than we currently have.

Proof of Theorem 8.1 (outline) —

1. Start by choosing a set $\overline{M}$ with $M \subset \overline{M}$ and $|\overline{M}| > |M|$.
2. Let *S* be the set of all 6-tuples $(E, F, +_F, \cdot_F, d_F, T)$ where
    a. E is a differential subfield of M containing K,

    b. $M \subseteq F \subseteq \overline{M}$,

c. $(F,+_F,\cdot_F,d_F)$ is a differential field having M as a differential subfield (i.e., $+_F$ and $\cdot_F$ are binary operations on F extending addition and multiplication in M and making $(F,+_F,\cdot_F)$ a field, and $d_F:F\to F$ is a derivation extending the derivation on M),

d. $T:E\to F$ is a differential isomorphism of E into (a differential subfield of) F extending S, the isomorphism from K to L in the theorem, and

e. F is generated over M by $T(E)$ (as a differential subfield of itself and hence, as one can prove, as a subfield), i.e., $F=M\langle T(E)\rangle=M(T(E))$.

3. Define a relation $\preceq$ on S by componentwise containment. That is $(E_1,F_1,+_{F_1},\cdot_{F_1},d_{F_1},T_1)\preceq(E_2,F_2,+_{F_2},\cdot_{F_2},d_{F_2},T_2)$ if and only if E_1 is a differential subfield of E_2, $(F_1,+_{F_1},\cdot_{F_1},d_{F_1})$ is a differential subfield of $(F_2,+_{F_2},\cdot_{F_2},d_{F_2})$ and T_2 is an extension T_1. If we view all binary operations as functions and all functions as sets (of ordered pairs), this means exactly that $E_1\subset E_2$, $F_1\subset F_2$, $+_{F_1}\subset +_{F_2}$, $\cdot_{F_1}\subset\cdot_{F_2}$, $d_1\subset d_2$, and $T_1\subset T_2$.

4. Show that $\preceq$ is a partial order on S (i.e. reflexive, transitive, antisymmetric). The steps here are straightforward and follow from the definitions above.

5. Show that the union of any chain in S is an upper bound in S for that chain. There are numerous verifications that lead to the result that for each chain $e=\{(E_\alpha,F_\alpha,+_{F_\alpha},\cdot_{F_\alpha},d_{F_\alpha},T_\alpha)|\alpha\in\mathbf{A}\}$ there exists an upper bound, namely

$\bigcup_{\alpha \in A}(E_\alpha, F_\alpha, +_{F_\alpha}, \cdot_{F_\alpha}, d_{F_\alpha}, T_\alpha) \in S$, where we take the union to mean componentwise union.

6. Now positioned to invoke Zorn's lemma, we conclude S has a maximal element, call it $(E, F, +_F, \cdot_F, d_F, T)$.

7. By Lemma 8.2 we have an extension of S to an admissible isomorphism of $K\langle u\rangle$ onto $L\langle v\rangle$. Then we may prove $E = M$ by assuming $E \neq M$ to obtain a contradiction to $(E, F, +_F, \cdot_F, d_F, T)$ being maximal in S.

8. Since $E = M$, $T: M \to T(M) \subseteq F$ is the required extension of S to an admissible differential isomorphism defined on M, and M is a differential subfield of F

Theorem 8.3 — Let K be a differential field of characteristic 0. Let s be an element in a larger differential field L, $s \notin K$. Then there exists an admissible differential isomorphism on L which actually moves s and is the identity on K.

Proof — Following the same approach used in the previous proof, for a differential indeterminate y let P be the kernel of a differential homomorphism from the differential integral domain $K\{y\}$ onto the differential integral domain $K\{s\}$. We have $K\{y\}/P \cong K\{s\}$, so P is a prime differential ideal in $K\{y\}$ and $P \neq K\{y\}$ since $s \neq 0$. Let J be the differential ideal in $L\{y\}$ generated by P, where we are taking $L = K\langle s\rangle$. Let I be the radical of J. Then I is a radical differential ideal in $L\{y\}$ and in $K\{y\}$ contracts to P by Lemma 7.1 (a). Invoking

Theorem 6.1 suppose that I has been expanded to a prime differential ideal Q in $L\{y\}$ which contracts in $K\{y\}$ to P. We will be in the position to construct an admissible differential isomorphism of $K\langle s\rangle$ onto $K\langle t\rangle$, sending s to t and equal to the identity on K, once we write t for the image of y in the homomorphism of $L\{y\}$ onto $L\{y\}/_{Q} \cong K\{s\}$. To meet our need we must move s and we have t equal to s only if $y-s \in Q$.

Lemma 7.1 (b) assures the hypotheses of Theorem 6.2 ($K\{y\}$and $L\{y\}$ in place of A and B respectively). Consequently the intersection of Q's such as above is I. So if we always have $y-s \in Q$, then $y-s \in I$. This is a contradiction to Lemma 7.1(c). Finally by Lemma 8.1 we may extend our admissible differential isomorphism to an admissible differential isomorphism moving s and equal to the identity on K defined on all of L (Kaplansky 13-17).

Chapter 3

Preliminary Galois Theory

9) **The Differential Galois Group** — Let M be a differential field, K a differential subfield of M. We define the differential Galois Group G of M/K to be the group of all differential automorphisms of M leaving K elementwise fixed. For any intermediate differential field L define L' to be the subgroup of G consisting of all automorphisms leaving L elementwise fixed (that is, L' is the differential Galois group of M/L). For any subgroup H of G define H' to be the set of all elements in M left fixed by H. Necessarily H' is an intermediate differential field between K and M. Evidently $L'' \supseteq L$ since it must lie between L and M. And $L_1 \supseteq L_2$ implies $L_1' \subseteq L_2'$. We have now $L'' \supseteq L$ implies $L''' \subseteq L'$. But the automorphisms of L' leave L'' fixed so $L' \subseteq L'''$. Hence $L' = L'''$. Similarly $H'' \supseteq H$, the set of all the automorphism that leave H' fixed contains H, $H_1 \supseteq H_2$ implies $H_1' \subseteq H_2'$, and $H' = H'''$. We say a field or group is **closed** if it is equal to its double prime. Thus we have the result that any primed object is closed, and priming sets up a one-to-one correspondence between closed subgroups and closed intermediate differential fields. Which subgroups or subfields are closed? This important question remains untouched.

Lemma 9.1 — Let N be a differential field with differential subfield K. Let L and M be intermediate differential fields with $M \supset L$ and $[M:L] = n$. Let

L' and M' be corresponding subgroups of the differential Galois group of N over K. Then the index of M' in L' is at most n, $(L':M') \le n$.

Proof — Since the relative degrees of fields and relative indices of groups are both multiplicative we need only to consider a simple extension, say $M = L(u)$. Then the right cosets of $L' \bmod M'$ correspond to the images of u under automorphisms keeping L elementwise fixed. There are at most n such images, namely the zeros of the irreducible polynomial for u over L.

Lemma 9.2 — Let G be the differential Galois group of a differential field extension M of K. Let H and J be subgroups of G with $H \supset J$ and J of index n in H. Let H' and J' be the corresponding intermediate differential fields. Then $[J':H'] \le n$.

Proof — Suppose $[J':H'] > n$. Then there exist $u_1, \cdots, u_{n+1} \in J'$ which are linearly independent over H'. Let $S_1, \cdots, S_n$ be any representatives of the right cosets of $H \bmod J$, cosets of automorphisms which fix the elements of M contained in H'. Suppose $S_1 = I$. Form the equations $\sum_{i=1}^{n+1} a_i(u_i S_j) = 0$, for $j = 1, \cdots, n$. We have n linear homogeneous equations in $n+1$ variables. Hence there exist nontrivial solutions in M and we choose one with a maximum number of zeros, say the nonzero elements $a_1, \cdots, a_r$ followed by 0's. We can suppose that $a_1 = 1$. It is not possible that all the a's lie in H', for then the first equation where $S_1 = I$ becomes $\sum_{i=1}^{n+1} a_i u_i = 0$ and contradicts the linear independence of the

u's. Suppose $a_r \notin H'$. Then some automorphism in H moves a_r, say this automorphism lies in the right coset JS_k. The u's are invariant under the automorphisms of J, so we are free to choose our representative of the coset. Thus we can suppose $a_r S_k \neq a_r$. Finally applying S_k to $\sum_{i=1}^{n+1} a_i(u_i S_j) = 0$ and subtracting the results from $\sum_{i=1}^{n+1} a_i(u_i S_j) = 0$, for $j = 1,\cdots,n$, we have a shorter solution since S_k does not move all the a's. Thus we have a contradiction to our choice of a solution with a maximum number of zeros.

A direct consequence of Lemma 9.1 and Lemma 9.2 follows:

Lemma 9.3 — Let G be the differential Galois group of a differential field extension M of K. Then any finite-dimensional extension of a closed intermediate differential field is closed. Also any subgroup of G having a closed subgroup of finite index is itself closed.

Proof — Let L and N be intermediate differential fields with $N \supset L$ and $[N{:}L] = n$ such that $L = L''$. Then $(L', N') \leq n$ by Lemma 9.1. Hence $[N''{:}L''] \leq n$ by Lemma 9.2. But $N \subseteq N''$ and $[N{:}L''] = n$ since $L = L''$. So $N = N''$. Next let H and J be subgroups of G with $H \supset J$, $(H{:}J) = n$ and such that $J = J''$. Then $[J'{:}H'] \leq n$ by Lemma 9.2. Hence $(H''{:}J'') \leq n$ by lemma 9.1. But $H'' \supset H$ and $(H{:}J'') = n$, since $J = J''$. So $H'' = H$.

Theorem 9.4 — Let M be a differential field, K a differential subfield, G the differential Galois group of M/K. (a) If H is a normal subgroup of G, then any differential automorphism of M / K sends H' onto itself. (b) If L is an intermediate differential field with the property that any differential automorphism of M / K sends L onto itself, then L' is a normal subgroup of G, and G / L' is the group of all differential automorphisms of L / K which can be extended to M.

Proof — (a) Let $S \in G$. We have $STS^{-1} \in H$ for every $T \in H$. Hence $xSTS^{-1} = x$ for every $x \in H'$. Thus $xST = xS$ and $H'S \subseteq H'$. Hence an automorphism of M / K sends H' into itself. The same argument is true for S^{-1}. Therefore an automorphism of M / K sends H' onto itself.

(b) — Let L be an intermediate differential field, $M \supset L \supset K$. Suppose that for $S \in G$ we have $LS = L$. Then for any $T \in L'$ we have $xST = xS$ for every $x \in L$. Hence $STS^{-1} \in L'$. Consider the homomorphism ϕ of G onto the differential Galois group of L / K defined by restricting the automorphisms of M to L. The kernel of ϕ is L', the automorphisms of M / K that fix L (that is, the differential Galois group of M / L). Then $G/_{L'} \cong \phi[G]$, differential automorphisms of L / K which can be extended to M.

Let H be a normal subgroup of the differential Galois group of M / K. By Theorem 9.4 (a) H' is an intermediate differential field with the property that any differential automorphism of M / K sends H' onto itself. By Theorem 9.4 (b) H'' is normal. **Hence the closure of a normal subgroup of a differential Galois group is normal.**

We define the differential field M to be **normal** over the differential subfield K if any element in M but not in K can be moved by a differential automorphism of M / K. Suppose M is normal, then elements of K'' not in K can be moved by differential automorphisms of M / K. But K'' is the set of elements fixed by the automorphisms of K', the automorphisms that fix K, hence $K'' = K$. **So if M is normal, K is closed.**

Suppose H is a normal subgroup of the differential automorphisms of M / K. Then H' is sent onto itself by any differential automorphism of M / K. Hence any element that lies in H' and not in K can be moved by differential automorphisms of M / K restricted to H', a differential automorphism of H' / K. **Hence the differential subfield corresponding to a normal differential Galois subgroup is normal.** The converse is not true unless we have additional hypotheses.

Lemma 9.5 — Let L be a closed subfield, H the corresponding subgroup. Then the normalizer of H $\left(N_H = \left\{S \in G \middle| SHS^{-1} = H\right\}\right)$ consists of all S in G that map L onto itself.

Proof — Let $S \in N_H$. Then $lSH_aS^{-1} = l$ for every $l \in L$ and $H_a \in H$. Hence $lSH_a = lS$ and $lS \in L$ since $L = L''$ and we have $LS = L$ (equality since S must be automorphism of L). The last argument works in reverse, so N_H contains every S in G that maps L onto itself.

Lemma 9.6 — Let L be a closed subfield of M, L normal over K. Let H be the subgroup corresponding to L. Assume that the normalizer N_H of H is closed and that every differential automorphism of L over K can be extended to M. Then H is normal and furthermore G/H is the full differential Galois group of L over K.

Proof — If $N_H = G$, then H is normal, so we need only to show $N_H = G$. Suppose L_{N_H} is the subfield corresponding to N_H. Then since N_H is closed, N_H contains all the automorphisms of G that fix L_{N_H} elementwise and we need only to show that $L_{N_H} = K$. We have that L_{N_H} is necessarily closed, thus by Lemma 9.5 N_H consists of just those $S \in G$ that map L onto itself. By hypothesis every differential automorphism of L/K can be extended to M. Hence N_H must contain all the differential automorphisms of L/K. Now we assumed L normal over K, so no elements of L other than elements of K are fixed under the automorphisms of N_H. Hence $L_{N_H} = K$, and $N_H = G$. Therefore H is normal. Then we have L with the property that that any differential automorphism of M/K sends L onto itself so by Theorem 9.4 G/H is the group of all differential automorphisms of L/K.

10) **The Wronskian** — The **Wronskian** W of n elements $y_1, y_2, \cdots, y_n$ in a differential ring is defined as usual $W(y_1, y_2, \cdots, y_n) = \det\begin{bmatrix} y_1 & y_2 & \cdots & y_n \\ y_1' & y_2' & \cdots & y_n' \\ \vdots & \vdots & & \vdots \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdots & y_n^{(n-1)} \end{bmatrix}$.

Theorem 10.1 — Let F be a differential field with field of constants C. Then n elements of F are linearly dependent over C if and only if their Wronskian vanishes.

Proof — Let $y_1,\cdots,y_n$ be linearly dependent over C. Then $\sum c_i y_i = 0$ with not all c's equal 0. Differentiating this equation $n-1$ times we have n linear homogeneous equations for $c_1,\cdots,c_n$, $\sum c_i y_i^{(j)} = 0$ for $j = 0,\cdots n-1$. The c's are not all zero, so $W(y_1,y_2,\cdots,y_n) = 0$.

Conversely, suppose $W(y_1,y_2,\cdots,y_n) = 0$. Then in F there exists a nontrivial solution $c_1,\cdots,c_n$ to the equations $\sum c_i y_i^{(j)} = 0$, $j = 0,\cdots,n-1$. If $c_1 = 0$ then we may rearrange terms of the equations so that $c_1 \neq 0$; otherwise there is no nontrivial solution. Take $c_1 = 1$ then we suppose $W(y_2,\cdots,y_n) \neq 0$. Otherwise $\sum\limits_{i\geq 2} c_i y_i^{(j)} = 0$ has a nontrivial solution and repeating the process we eventually arrive at a point with a nonzero Wronskian or all our y's may be expressed as a constant multiple of a single y and we are done (since then $c_1 = \cdots = c_{n-1} = 1$, $y_{n-1} = c_n y_n$, $y_{n-1}{}' = c_n y_n{}'$, and differentiating $y_{n-1} = c_n y_n$ we get $y_{n-1}{}' = c_n y_n{}' + c_n{}' y_n$ implying $c_n{}' = 0$). Taking $W(y_2,\cdots,y_n) \neq 0$ we have $-y_1^{(j)} = \sum\limits_{i\geq 2} c_i y_i^{(j)}$, $j = 0,\cdots,n-1$. Differentiating the first $n-1$ equations we have $-y_1^{(j)} = \sum\limits_{i\geq 2}\left(c_i y_i^{(j)} + c_i{}' y_i^{(j-1)}\right)$, $j = 1,\cdots,n-1$. Substituting $-y_1^{(j)} = \sum\limits_{i\geq 2} c_i y_i^{(j)}$ for $j = 1,\cdots,n-1$ into

$-y_1^{(j)} = \sum_{i\geq 2}\left(c_i y_i^{(j)} + c_i' y_i^{(j-1)}\right)$, $j = 1,\cdots,n-1$, we have $\sum_{i\geq 2} c_i' y_i^{(j)} = 0$, $j = 0,\cdots,n-2$.

Thus $c_2' =\cdots= c_n' = 0$ and the c's are constants since $W(y_2,\cdots,y_n) \neq 0$.

Theorem 10.1 makes it possible to discuss linear dependence over constants unambiguously since the vanishing of the Wronskian is independent of the choice of field.

11) **Picard-Vessiot Extensions** — Consider a linear homogeneous differential equation $L(y) = y^{(n)} + a_1 y^{(n-1)} +\cdots+ a_{n-1} y' + a_n y = 0$ with coefficients in the differential field K. Let $u_1,\cdots,u_{n+1}$ be solutions of the equation in a certain (possibly) larger differential field. The equation $L(y) = 0$ shows that the last row of the Wronskian $W(u_1,\cdots,u_{n+1})$ is a linear combination of the proceeding rows and $W(u_1,\cdots,u_{n+1}) = 0$. Thus $u_1,\cdots,u_{n+1}$ are linearly dependent over constants.

Definition — Let $L(y) = y^{(n)} + a_1 y^{(n-1)} +\cdots+ a_{n-1} y' + a_n y = 0$ be a linear homogeneous differential equation with coefficients in a differential field K. We say that a differential field M containing K is a **Picard-Vessiot extension** of K (for the equation $L(y) = 0$) if, (a) $M = K\langle u_1,\cdots,u_n\rangle$ where $u_1,\cdots,u_n$ are n solutions of $L(y) = 0$ linearly independent over constants, and (b) M has the same field of constants as K.

In regards to the issue of existence and uniqueness of Picard-Vessiot extensions, Kaplansky refers the issue to Kolchin both by works and personal communications. He observes that the existence and uniqueness are assured in the case where K is of characteristic 0 and has an algebraically closed field of constants. It seems appropriate to remind ourselves that when K is a differential field of meromorphic functions on a domain in the field of complex numbers $\mathbf{C}$ and $\mathbf{C} \subseteq K$, existence and uniqueness of Picard-Vessiot extensions follows from the theory of linear differential equations.

Let M be a Picard-Vessiot extension of K, and S a differential automorphism of M over K. Then $u_i S$ is a linear combination of the u's with coefficients in the constant field C, $u_i S = \sum c_{ij} u_j$, $i = 1, \cdots, n$. The matrix c_{ij} is non-singular since the inverse matrix may be derived from the inverse automorphism. Since $u_1, \cdots, u_n$ generate $M = K\langle u_1, \cdots, u_n \rangle$, the differential Galois group of M / K is isomorphic to a multiplicative group of non-singular matrices over C.

Lemma 11.1 — Let $K \subset L \subset M$ be differential fields. Suppose L is a Picard-Vessiot extension of K, and that M has the same field of constants as K. Then any differential automorphism of M over K sends L onto itself.

Proof — Suppose $L(u) = 0$ is the linear homogeneous differential equation of our Picard-Vessiot extension. For every differential automorphism S of M / K and every solution u_i of $L(u) = 0$, we have $L(u_i S) = L(u_i)S = 0S = 0$ since S commutes with derivation and K is elementwise fixed by S. Hence $u_i S \in L$ for every $u_i S$. Since $L = K\langle u_1, \cdots, u_n \rangle$ it follows that $lS \in L$ for every $l \in L$. Then we have $LS = L$ since S is an automorphism of M / K.

12) **Two Special Cases** — The first is adjoining an integral.

Lemma 12.1 — Let K be a differential field of characteristic 0. Let u be an element of a larger differential field with $u' = a \in K$, where a is not a derivative in K. Then u is transcendental over K, $K\langle u\rangle$ is a Picard-Vessiot extension of K, and its differential Galois group is isomorphic to the additive group of constants in K.

Proof — Suppose u satisfies an irreducible polynomial equation over K, take the equation $u^n + bu^{n-1} + \cdots = 0$. Differentiating, we get $nu^{n-1}a + b'u^{n-1} + \cdots = 0$, where we display only the terms of greatest degree, $n-1$. We have that u is a zero of an irreducible polynomial of degree n over K. Hence u is not the zero of a polynomial of degree less than n over K. Thus the coefficients of the polynomial $(na + b')u^{n-1} + \cdots$ are zero. Then $na = -b'$ and a is then the derivative of $\frac{-b}{n} \in K$, a contradiction to our hypothesis. Hence u is transcendental over K.

To show that $K\langle u\rangle$ has no new constants, first suppose that the polynomial $b_1u^m + b_2u^{m-1} + \cdots$ is a constant. On differentiating, $b_1'u^m + (mb_1a + b_2')u^{m-1} + \cdots = 0$. Hence $b_1' = mb_1a + b_2' = 0$ and

$a = \frac{-b_2'}{mb_1} = \frac{-mb_1b_2' + mb_1'b_2}{m^2b_1^2} = \left(\frac{-b_2}{mb_1}\right)'$ again a contradiction. Suppose now that the rational function $\frac{f(u)}{g(u)}$ is a constant, where $\frac{f(u)}{g(u)}$ is in lowest terms and $g(u)$

contains u with a leading coefficient of 1. Differentiating $\frac{f'g - fg'}{g^2} = 0$, and $\frac{f}{g} = \frac{f'}{g'}$. But g' is a polynomial of lower degree than g. So we have a contradiction to our assumption that $\frac{f(u)}{g(u)}$ is in lowest terms. Hence the assumption that we have new constants in $K\langle u\rangle$ leads to a contradiction to our hypothesis.

By hypothesis $\frac{u'}{a} = 1$. Thus differentiating , $\left(\frac{u'}{a}\right)' = \frac{u''a - u'a'}{a^2} = 0$. Hence u and 1 are solutions to the differential equation $y'' - \left(\frac{a'}{a}\right)y' = 0$, linearly independent over constants. Thus $K\langle u\rangle$ is a Picard-Vessiot extension of K.

In a differential automorphism of $K\langle u\rangle$ over K, u must be sent into another element with derivative a. Sending u into $u+c$ with $c \in C$ the field of constants and fixing K elementwise will do the job for us. That the mapping $u \to u+c$ induces an automorphism of $K\langle u\rangle$ over K in the usual algebraic sense is deduced by tediously showing that it is a bijection and preserves addition and multiplication. Let S be the name of our mapping $uS = u+c$. To show that S is a differential automorphism of $K\langle u\rangle$ we first demonstrate validity for the polynomial $\sum \lambda_i u^i$. The latter is sent to $\sum \lambda_i (u+c)^i$. Differentiating we have $\sum\left[i\lambda_i(u+c)^{i-1}a + \lambda_i'(u+c)^i\right]$, the image of $\left(\sum \lambda_i u^i\right)' = \sum\left[i\lambda_i u^{i-1}a + \lambda_i' u^i\right]$. Next for $\frac{f(u)}{g(u)} \in K\langle u \rangle$, where $f(u)$ and $g(u)$ are polynomials over K we have

$$\left(\left(\frac{f(u)}{g(u)}\right)'\right)S = \left(\frac{(f(u))'g(u) - f(u)(g(u))'}{(g(u))^2}\right)S = \left(\frac{(f(u+c))'g(u+c) - f(u+c)(g(u+c))'}{(g(u+c))^2}\right)$$

reducing to $\left(\left(\frac{f(u)}{g(u)}\right)'\right)S = \left(\frac{f(u+c)}{g(u+c)}\right)' = \left(\left(\frac{f(u)}{g(u)}\right)S\right)'$. Thus S is a differential automorphism. Since K is elementwise fixed by automorphisms of $K\langle u \rangle / K$, our automorphisms induced by the mappings $u \to u+c$, $c \in C$ cover all the possible images of u under differential automorphisms of $K\langle u \rangle / K$ and we have the desired result: the differential Galois group for $K\langle u \rangle / K$ is isomorphic to the additive group of constants in K, the fact that the given bijection between the differential Galois group and the additive group of constants preserves the group operation being immediate.

The second type of extension is the adjunction of an exponential of an integral.

Lemma 12.2 — Let K be a differential field, u an element satisfying the equation $y' - ay = 0$, $a \in K$. Suppose $K\langle u \rangle$ has the same field of constants as K. Then $K\langle u \rangle$ is a Picard-Vessiot extension of K, and its differential Galois group is isomorphic to a subgroup of the multiplicative group of nonzero constants in K.

Proof — By the definition, $K\langle u\rangle$ is a Picard-Vessiot extension. If v is another solution to $y'-ay=0$, we have $\left(\frac{v}{u}\right)'=\frac{v'u-u'v}{u^2}=\frac{avu-auv}{u^2}=0$. Hence $v=cu$ with c a constant. Thus every differential automorphism of $K\langle u\rangle / K$ is of the form $u \to cu$.

13) **Liouville Extensions** — We define M to be a Liouville extension of K if there exists a chain of intermediate differential fields $K=K_1 \subset K_2 \subset \cdots \subset K_n = M$ such that each K_{i+1} is an extension of K_i by an integral or an exponential of an integral.

Theorem 13.1 — Let M be a Liouville extension of the differential field K, having the same field of constants as K. Then the differential Galois group G of M over K is solvable.

Proof — Let the chain of intermediate differential fields be $K=K_1 \subset K_2 \subset \cdots \subset K_n = M$ such that each K_{i+1} is an extension of K_i by an integral or an exponential of an integral. By Lemmas 12.1 and 12.2, K_2 is a Picard-Vessiot extension of K. Then Lemma 11.1 tells us that an automorphism of M/K sends K_2 onto itself. Let H_2 be the Galois subgroup of G corresponding to K_2. By Theorem 9.4 H_2 is normal in G and G/H_2 is the group of all the differential automorphisms of K_2/K which can be extended to M. Hence G/H_2 is a subgroup of the differential Galois group of K_2/K. Again by Lemmas 12.1 and 12.2 the differential Galois group of K_2/K is isomorphic to the additive group of constants or multiplicative group of constants in K. Hence the differential Galois group of K_2 / K is abelian. So G / H_2 is abelian. Repeated application of the above argument to the automorphisms of $M / K_2, \cdots, M / K_{n-1}$ we have a chain $G \supset H_2 \supset H_3 \supset \cdots \supset H_{n-1} \supset \{1\}$, such that H_i is normal in H_{i+1} and H_{i+1} / H_i is abelian for every i. Therefore G is solvable.

14) **Triangular Automorphisms** — Until we have more machinery available to us we must settle with the next theorem, a partial step toward a converse to Theorem 13.1.

Theorem 14.1 — Let the differential field M be normal over its differential subfield K. Suppose that $u_1, \cdots, u_n \in M$ are elements such that for every differential automorphism σ of M / K we have $u_i\sigma = a_{ii}u_i + a_{i,i+1}u_{i+1} + \cdots + a_{in}u_n$, $i = 1, \cdots, n$, with the a's constants in M and depending on σ. Then $K\langle u_1, \cdots, u_n \rangle$ is a Liouville extension of K.

Proof — The equation for $i = n$ is $u_n\sigma = a_{nn}u_n$. Differentiating gives $u_n{}'\sigma = a_{nn}u_n{}'$ since σ is a differential automorphism. Taking $u_n \neq 0$, for otherwise we simply suppress u_n, and dividing gives us $\frac{u_n{}'\sigma}{u_n\sigma} = \frac{u_n{}'}{u_n}$. But $\frac{1}{u_n\sigma} = (u_n\sigma)^{-1} = u_n{}^{-1}\sigma$. So $\left(\frac{u_n{}'}{u_n}\right)\sigma = \frac{u_n{}'}{u_n}$, and $\frac{u_n{}'}{u_n}$ is invariant under σ. Hence $\frac{u_n{}'}{u_n} \in K$ since M is normal over K. Thus the adjunction of u_n to K is the adjunction of the exponential of an integral. Next dividing each of the equations $u_i\sigma = a_{ii}u_i + a_{i,i+1}u_{i+1} + \cdots + a_{in}u_n$, $i = 1,\cdots,n-1$, by $u_n\sigma = a_{nn}u_n$ we get $\left(\frac{u_i}{u_n}\right)\sigma = \frac{a_{ii}}{a_{nn}}\frac{u_i}{u_n} + \cdots + \frac{a_{i,n-1}}{a_{nn}}\frac{u_{n-1}}{u_n} + \frac{a_{in}}{a_{nn}}$. Differentiating gives us $\left(\frac{u_i}{u_n}\right)'\sigma = \frac{a_{ii}}{a_{nn}}\left(\frac{u_i}{u_n}\right)' + \cdots + \frac{a_{i,n-1}}{a_{nn}}\left(\frac{u_{n-1}}{n_n}\right)'$, $i = 1,\cdots,n-1$. The latter are of the same form as our original equations in the elements $\left(\frac{u_i}{u_n}\right)'$ for $i = 1,\cdots,n-1$. The process may be repeated and we have by induction on n, the adjunction of $\left(\frac{u_i}{u_n}\right)'$ to K yields a Liouville extension. Then the adjoining of $\frac{u_i}{u_n}$ means adjoining of integrals (Kaplansky 18-25).

Chapter 4

Algebraic Matrix Groups and The Zariski Topology

15) Z-**spaces** — Let F be any field. Let V be an n-dimensional vector space over F, specifically the set of n-tuples with elements in F together with the usual axioms of vector space addition and scalar multiplication. Let $F[x_1,\cdots,x_n]$ be the polynomial ring in n indeterminates over F. We define an **algebraic manifold** in V to be all the zeros of a collection S of polynomials in $F[x_1,\cdots,x_n]$, that is, the set of zeros common to every polynomial in S. Enlarging S to the set I of all polynomials which vanish on the manifold, we then have an ideal in $F[x_1,\cdots,x_n]$, since it is closed under polynomial addition and the product of any polynomial in $F[x_1,\cdots,x_n]$ with any member of the collection is again a polynomial possessing the set of common zeros. Thus an equivalent definition is that an algebraic manifold in V is the set of zeros of an ideal in $F[x_1,\cdots,x_n]$. Since ideals in F certainly satisfy the ascending chain condition, we know by the Hilbert basis theorem that ideals in $F[x_1,\cdots,x_n]$ satisfy the ascending chain condition. Each ideal in the chain corresponds to an algebraic manifold, so we conclude that algebraic manifolds of V must satisfy a descending chain condition, i.e. a descending chain of closed manifolds will stabilize in a finite number of steps.

We adopt the fact from algebraic geometry that a finite union of algebraic manifolds is an algebraic manifold and that an arbitrary intersection of algebraic manifolds is an algebraic manifold. Then we use algebraic manifolds as closed sets to define a T_1 topology on V, called the **Zariski topology** . We recall that the usual definition for a T_1 **topology** on V is given two distinct points in V each has an open neighborhood not containing the other. A familiar result of point set topology applicable here is that **points are closed sets if and only if the topology is T_1**. So we can see that the Zariski topology is indeed T_1 since any point $(a_1,\cdots,a_n)$ in V is the zero set of the collection of polynomials $\{x_1-a_1,\cdots,x_n-a_n\}$. It follows that any finite collection of points is closed since the finite union of closed sets is closed. It seems natural now to define a **Z-space** to be a T_1-space satisfying the descending chain condition on closed sets (or equivalently the ascending chain condition on open sets since the complement of a closed set in is open.)

Lemma 15.1 — a) Every subspace of a Z-space is a Z-space. b) If a T_1-space is a continuous image of a Z-space, it is itself a Z-space. c) A Hausdorff Z-space is finite (A space is **Hausdorff**, or T_2, if each two distinct points have nonintersecting respective open neighborhoods.)

Proof — a) Suppose we have a non-empty non-Z-subspace X of a Z-space Y. Suppose X does not satisfy the descending chain condition on closed sets. Then there exists an infinite descending chain of closed sets in X, say the sets C_n, $n=1,2,\cdots$. Each C_n is the intersection of some closed set D_n in Y with X. Thus we may construct an infinite descending chain of closed sets in Y since an arbitrary intersection of closed sets is closed. We display our chain: $D_1 \supset D_1 \cap D_2 \supset D_1 \cap D_2 \cap D_3 \cdots$. We are assured that it is not an empty descending chain since $D_1 \supset C_1$, $D_2 \supset C_2$, $D_3 \supset C_3 \cdots$ and $C_1 \supset C_2 \supset C_3 \supset \cdots$. Hence the assumption that the Z-subspace X does not satisfy the descending chain condition leads to a contradiction. Thus the subspace of a Z-space satisfies the descending chain condition. To see that X is T_1 note that for any point $p \in X$ we have that the set $\{p\}$ is closed in Y. Then $\{p\} \cap X = \{p\}$ is closed in X. Thus the subspace of a Z-space is a Z-space.

b) Suppose it is not. Then there exists an infinite descending chain of closed sets in the image T_1-space. But the pre-image of each closed set in the chain is a closed set in the Z-space since the image is the result of a continuous, surjective map and the totality of pre-images form a descending chain. Thus we have an infinite descending chain of closed sets in the Z-space, a contradiction. Therefore the continuous image of a Z-space that is a T_1-space is itself a Z-space.

c) It is a direct consequence of the Hausdorff axiom that every infinite Hausdorff space has an infinite number of disjoint open sets. For suppose not, then there exists an open set that is infinite and contains no disjoint open sets, a contradiction to the Hausdorff axiom. Thus we may construct inductively a countably infinite ascending chain of open sets. Therefore a Hausdorff Z-space is finite.

Lemma 15.2 — A Z-space is the union of a finite number of disjoint open and closed connected subsets.

Proof — Let X be a Z-space. If X is not connected it is the union of two disjoint open and closed sets. If either of these two is not connected, it may be similarly split. The descending chain condition on closed sets makes this process terminate in a finite number of steps, and we reach an open and closed component of X. In the complement we may similarly extract a second open and closed component, and so on until in a finite number of steps we have extracted all the open and closed components. In this way we may build an ascending chain of unions of open disjoint components of X which in a finite number of steps terminates with X by the ascending chain property.

16) **T_1-groups and Z-groups** — The group GL_n of all non-singular $n \times n$ matrices over a field F is a subset of n^2-dimensional space and thus "carries" the Zariski topology.

Lemma 16.1 — Let V and W be m-dimensional and n-dimensional spaces over F, taken in the Zariski topology. Let $r_1,\cdots,r_n$ be rational functions in m variables $x_1,\cdots,x_m$. Let S be the set where any of the denominators of $r_1,\cdots,r_n$ vanish, and let T be the complement of S in V. Then the mapping from T to W, defined by $(x_1,\cdots,x_m) \to (y_1,\cdots,y_n)$ with $y_i = r_i(x_1,\cdots,x_m)$, is continuous.

Proof — We have to show that the inverse image of a closed set is closed. Given a closed set on W, it is evidently the set of zeros of a collection of polynomials $g_j(y_1,\cdots,y_n)$. The inverse image of this set of zeros in W is the set of zeros of the rational functions $g_j(r_1(x_1,\cdots,x_m),\cdots,r_n(x_1,\cdots,x_m))$ in T, which is the same as the set of zeros of the numerator polynomials of $g_j(r_1(x_1,\cdots,x_m),\cdots,r_n(x_1,\cdots,x_m))$ in T, a closed set in the Zariski topology for T.

We may conclude by this last lemma that in the "topological group" G multiplication is separately continuous in its variables, and that the inverse is continuous. It can be shown that if multiplication is jointly continuous in its variables then the space Hausdorff and Lemma 15.2 tells that a Hausdorff Z-space is finite.

Definition — We say that G is a T_1**-group** if it is a group and a T_1-space in such a way that the inverse is continuous and multiplication is separately continuous in its variables. Equivalently, we may say that left multiplication, right multiplication and inversion are homeomorphisms of G onto itself. A Z**-group** is a T_1-group whose space is a Z-space.

We recall that **components** are equivalence classes that partition a space into connected disjoint subsets whose union equals the space. The equivalence relation is defined on a space X by taking $x \sim y$ if there is a connected subset of X containing both x and y. The component containing the identity element of a group is called the **component of identity.**

Lemma 16.2 — The component of identity in a T_1-group is a closed normal subgroup.

Proof — Let C be the component of identity in the T_1-group G. By C^{-1} we mean the set of multiplicative inverses of elements of C. Thus by definition of a T_1-group, C^{-1} is the continuous image of a connected set, hence C^{-1} is connected and contains 1. Thus $C^{-1} \subset C$ since every connected subset intersects only one component. Similarly, for $c \in C$ we have that cC is connected and shares the element c with C and so $cC \subset C$. Thus C is a subgroup. Now for any $x \in G$, $x^{-1}Cx$ is connected and contains 1. Hence $x^{-1}Cx \subset C$ and C is normal.

Recalling that the index of a subgroup in a group is the number of right cosets of the subgroup in the group, by Lemmas 15.2 and 16.2 we have:

Lemma 16.3 — The component of identity in a Z-group is a closed normal subgroup of finite index.

17) ***C*-groups** — Adopting a weaker axiom than for the Z-groups we obtain the next few results which will be sufficient for our needs.

Definition — A ***C*-group** is a T_1-group in which for fixed x the mapping $a \to a^{-1}xa$ is continuous.

Invertible matrices under the Zariski topology form a C-group. To see this let X be a fixed matrix. The entries of $A^{-1}XA$ are rational functions in the entries of the matrix A. By lemma 16.1 $A \to A^{-1}XA$ is continuous where A is taken in the subspace of invertible matrices, the complement of the subspace of non-invertible matrices.

Lemma 17.1 — Let G be a C-group whose component of identity has a finite index k. Then any finite conjugacy class of G has at most k elements.

Proof — Suppose there exists a finite conjugacy class of more than k elements for some $x \in G$. By definition of C-group, for every $a \in G$ the mapping $a \to a^{-1}xa$ is continuous. The image set $\{a^{-1}xa | a \in G\}$ is a finite subspace with the T_1 topology so each singleton subset is closed and open. Then the pre-image of each conjugate is an open and closed set in G since the mapping $a \to a^{-1}xa$ is continuous. Thus we have a decomposition of G into more than k disjoint open and closed sets, a contradiction.

Lemma 17.2 — In a connected C-group any non-central element has an infinite conjugacy class.

Proof — For elements in the center conjugation is the identity map. The Lemma follows immediately by the observation that if there were a finite conjugacy class then there would be a separation of the C-group since the pre-image of each element in the class is an open and closed set in the C-group, a contradiction.

Theorem 17.3 — If G is a connected C-group, the commutator subgroup G' is again connected.

Proof — Let D_k be the set of products of k commutators in G. Then $D_1 \subset D_2 \subset \cdots$ and the union of all the D's is G'. It will suffice to prove that each D_k is connected. Consider the mapping $a_1 \to a_1^{-1}b_1^{-1}a_1b_1a_2^{-1}b_2^{-1}a_2b_2 \cdots a_k^{-1}b_k^{-1}a_kb_k$ with all elements other than a_1 being held fixed. The mapping is continuous since conjugation $(a_1^{-1}b_1^{-1}a_1)$ is continuous and right multiplication

$a_1^{-1}b_1^{-1}a_1(b_1a_2^{-1}b_2^{-1}a_2b_2\cdots a_k^{-1}b_k^{-1}a_kb_k)$ is continuous. Thus the image is connected since the continuous image of a connected set is connected. When $a_1 = b_1$ the image has a point in common with D_{k-1}. Now let a_1 vary over G. In this way then we express D_k as the union of connected sets, each having a point in common with the set D_{k-1} and D_{k-1} is connected by induction by beginning the process with $k = 1$. Thus D_k is connected since the union of a collection of connected sets each with a point in common with a connected subset of the union is connected. (Proof of the latter assertion follows: Let $\{A_\alpha\}$ be a collection of connected subspaces of a space X each having a point in common with the connected subspace $A \subset Y = \bigcup A_\alpha$. Suppose Y has a separation. Then $Y = C \cup D$ where $C \cap D = \phi$, C and D are open and nonempty. Then $A \subset C$ or $A \subset D$ since A is connected. Say $A \subset C$. Each A_α is either in C or D, since each A_α is connected. But no A_α can be in D, since $A \subset C$ and $A_\alpha \cap A \neq \phi$ for every A_α. Hence $Y = \bigcup A_\alpha \subset C$ and $D = \phi$, a contradiction. Therefore $Y = \bigcup A_\alpha$ is connected.)

We include the next two results for later use.

Lemma 17.4 — Let G be a C-group, H a closed subgroup of G. Suppose that either (a) H is of finite index in G, or (b) H is normal and G/H is abelian. Suppose further that the component of identity in H is solvable. Then the component of identity in G is solvable.

Proof — (a) We know that component of identity C_H in H is a connected closed and open normal subgroup of H. Since H is closed in G, C_H is closed in G. There are finitely many closed right cosets of H in G since H is of finite index in G and right multiplication is a homeomorphism of G onto itself. The complement of C_H in H is closed in H and hence closed in G. Then the complement of C_H in G is closed in G since it is the finite union of all the right cosets of H in G other than H and the complement of C_H in H(all closed in G). Thus C_H is an open, closed, connected subgroup in G. Hence $C_H \subset C_G$, the component of identity in G, since both contain 1 and C_G is the largest connected subset of G containing 1. But the complement of C_H is open in G thus $C_H \cup (G - C_H)$ is a separation of G. So $C_G \subset C_H$ since $C_G \cap C_H \neq \phi$. Therefore C_H and C_G coincide and C_G is solvable.

(b) Again let C_G and C_H be the components of identity for G and H respectively. Let C_G' and G' be the commutator subgroups of C_G and G respectively. Then $H \supset G'$ since H in normal and G/H is abelian. Thus $H \supset G' \supset C_G'$. By Theorem 17.3 C_G' is connected. Hence $C_G' \subset C_H$, since they both contain 1 and C_H is the largest connected set in H containing 1. By hypotheses C_H is solvable, hence C_G' is solvable. Therefore C_G is solvable since C_G' is normal in C_G and C_G / C_G' is abelian.

Lemma 17.5 — In a C-group the normalizer of a closed subgroup is closed.

Proof — Let G be a C-group. Let S be a closed subgroup. For fixed s in S, consider the continuous mapping $a \to asa^{-1}$, say ϕ. The inverse image of S is closed and consists of all a with $asa^{-1} \in S$. We take the intersection of these closed sets for all $s \in S$. Thus the set of a with $aSa^{-1} \subset S$ is closed, since an arbitrary intersection of closed sets is closed. In the same manner we conclude that the set of a with $a^{-1}Sa \subset S$ is closed. The normalizer of S is $N_S = \{a \in G | a^{-1}Sa = S\}$ which is the intersection of our two closed sets of a. Therefore the normalizer of a closed subgroup of a C group is closed.

18) **Solvable Connected Matrix Groups —**

Theorem 18.1 — Let G be a solvable multiplicative group of nonsingular matrices over an algebraically closed field. Suppose that G is connected in the Zariski topology. Then G can be put in **simultaneous triangular form**.

Simultaneous triangular form is illustrated by the next proposition that we shall need in the proof of Theorem 18.1. We present it over the algebraically closed field F.

Proposition 18.2 — Let **F** be a family of commuting matrices in $M_n(F)$. Then there exists a matrix $P \in GL_n(F)$ such that PAP^{-1} is upper triangular for every $A \in \mathbf{F}$.

Lemma 18.3 — Let $A, B \in M_n(F)$ commute multiplicatively. Let λ be an eigenvalue of A and $E_\lambda(A)$ the corresponding eigenspace. Then B stabilizes $E_\lambda(A)$, that is for $v \in E_\lambda(A)$ we have $Bv \in E_\lambda(A)$.

Proof — Let $v \in E_\lambda(A)$. Then $Av = \lambda v$. Thus $BAv = B(\lambda v) = \lambda(Bv)$. But $BAv = A(Bv)$. So $Bv \in E_\lambda(A)$.

Lemma 18.4 — Any $C \in \mathbf{F}$ stabilizes any $E_\lambda(A) \cap E_\mu(B)$ for $A, B \in \mathbf{F}$.

Proof — Immediate from Lemma 18.3. Lemma 18.4 may be generalized to the any finite intersection of eigenspaces.

Lemma 18.5 — Let $\mathbf{F}$ be a family of commuting matrices in $M_n(F)$. Then there exists a non-zero $v \in F^n$ that is an eigenvector for all $A \in \mathbf{F}$.

Proof — Let $A \in \mathbf{F}$. Let λ be an eigenvalue of A and $V_1 = E_\lambda(A)$ the corresponding eigenspace. By Lemma 18.3 each $B \in \mathbf{F}$ operates on V_1. Case 1: Every $B \in \mathbf{F}$ has all of V_1 as a single eigenspace. Then take v be any non-zero element of V_1. Case 2: Some $B \in \mathbf{F}$ has for its operation on V_1 some eigenspace V_2 that is a proper subspace of $V_1 = E_\lambda(A)$. Repeat the operation procedure with each $B \in \mathbf{F}$ for subspace V_2, and so on ($n-1$ times at most) until Case 1 is achieved.

Proof of Proposition 18.2 — We use induction on n. Choose a basis for F^n which starts with $v_1 = v$, an eigenvector for all $A \in \mathbf{F}$ provided by Lemma 18.5. Take $P^{-1} \in GL_n(F)$ to have these basis vectors as column vectors. Thus

PAP^{-1} expresses the matrices $A \in \mathbf{F}$ in the new basis. They are all of the form $\begin{pmatrix} \lambda & * & \cdots & * \\ 0 & & & \\ \vdots & & A_1 & \\ 0 & & & \end{pmatrix}$, that is, another is like $\begin{pmatrix} \mu & * & \cdots & * \\ 0 & & & \\ \vdots & & B_1 & \\ 0 & & & \end{pmatrix}$, and so on. By induction hypotheses, the $A_1, B_1, \cdots$ can be put in simultaneous triangular form, say by some Q_1, then $\left[\begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{pmatrix} P\right] A \left[\begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{pmatrix} P\right]^{-1}$ is triangular.

Proof of Theorem 18.1 — We proceed by induction, first for the case that G is reducible and then for the case that G is irreducible.

(1) Suppose that G is reducible. By this we mean the vector space V has a proper, non-trivial invariant subspace W under the set of linear transformations of V onto V corresponding to G, each element of G being the matrix representation of a linear transformation in the set. It is a familiar result of linear algebra that if we take a basis of W and expand it to a basis of V, then relative to this basis the matrices of $A_t \in G$ take the form $A_t = \begin{pmatrix} B_t & * \\ 0 & C_t \end{pmatrix}$. By the rules of matrix multiplication we can easily determine that the set of matrices B_t selected in this manner above form a group say G_1. Then the mapping of G onto G_1 defined by $A_t \to B_t$ is a homomorphism. By Lemma 16.1 our homomorphism is continuous hence G_1 is connected. It is a familiar result that every (subgroup and) homomorphic image of a solvable group is solvable.

Hence, since G is connected and solvable G_1 is connected and solvable. Thus by induction on the size of the matrices, the matrices of G_1 can be put in simultaneous triangular form. A similar argument applies to C_t. Hence we have the result that G reaches triangular form. In the inductive process should we reach an irreducible matrix before achieving triangular form we switch to step 2).

(2) Next we assume G to be irreducible. Let G' be the commutator subgroup of G. Recall that matrices under the Zariski topology form a C-group, then by Theorem 17.3 G' is connected. Let $G^{(1)} = G'$ and in general $G^{(i)} = \left(G^{(i-1)}\right)'$. Then we have the so-called derived series $G > G^{(1)} > G^{(2)} \cdots$ where in the case at hand $G^{(n)} = \langle I \rangle$ for some n. Each $G^{(i-1)}$ is normal in $G^{(i)}$, connected and solvable, and each $G^{(i)} / G^{(i-1)}$ is abelian. Thus for every matrix $X_i \in G^{(i)}$ we have $X_i G^{(i-1)} X_i^{-1} \subset G^{(i-1)}$. It can be shown that for every homomorphism of G onto G that $G^{(i)}$ is invariant. Thus $G^{(i)}$ is normal in G. Hence by the above results by induction on the length of the derived series we may assume G' is in triangular form.

(3) Let W be the subspace of V spanned by all joint eigenvectors of G'. We have $W \neq 0$ since the triangular form of G' will yield at least one joint eigenvector. To see that W is invariant under G, let α be a joint eigenvector of G'. Then $\alpha T = \lambda_T \alpha$ for $T \in G'$. And for any $S \in G$ we have $STS^{-1} \in G'$, thus $\alpha STS^{-1} = \lambda_{STS^{-1}} \alpha$. Next we write $\alpha ST = \lambda_{STS^{-1}} \alpha S$. So αS is an eigenvector of G'

and W is invariant under G. But G is irreducible. So $W = V$. Hence we can suppose that G' is in diagonal form.

(4) We may take any element of G' to be a diagonal matrix. The conjugates in G of a matrix in G' are again in G' and hence diagonal. The only possible conjugates are obtained by permuting the eigenvalues. Hence each matrix of G' has a finite conjugacy class. By Lemma 17.2 G' lies in the center of G.

(5) Suppose there exists a non-scalar matrix $T \in G'$. Let λ be an eigenvalue of T. Define $W = \{\alpha | \alpha T = \lambda\alpha\}$. Let $S \in G$ and $\alpha \in W$. Then $(\alpha S)T = (\alpha T)S = (\lambda\alpha)S = \lambda(\alpha S)$, since T commutes with all of G. Thus $\alpha S \in W$ and W is invariant under G. Hence $W = V$ and $T = \lambda I$. This contradiction proves that the matrices of G' are scalar.

(6) The elements of G' are generated by elements of the form $aba^{-1}b^{-1}$, $a, b \in G$ and thus have determinants equal to 1. Hence the elements on the diagonal of a matrix must be n-th roots of unity. There are only a finite number of these, so G' is finite. G' is connected (Theorem 17.3). Hence $G' = \langle I \rangle$. But G is abelian if and only if $G' = \langle I \rangle$. We showed by Proposition 18.2 that sets of commuting matrices can be put in simultaneous triangular form. This completes the proof of Theorem 18.1.

19) **A Result To Use in Chapter 6** — The next result will be a key element in examples of equations of order two.

Theorem 19.1 — Let G be a group of 2×2 matrices with determinant 1, over an algebraically closed field. Assume G is an algebraic group, i. e. is closed in the Zariski topology, and that K, the component of identity in G, is solvable. Then at least one of the following statements holds:

(a) G is finite,

(b) K can be put in diagonal form and $[G:K] = 2$,

(c) G can be put in simultaneous triangular form.

Proof — We have that G is an algebraic group, hence a Z-group. First consider the case where K can be put in diagonal form. Then K consists of certain matrices $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Since K is closed in G, K is an algebraic group. Thus K consists of all the matrices for which the 2^2-tuples $(a,0,0,a^{-1})$ are zeros of some polynomials $f(w,x,y,z)$. Either K is finite and then G is finite or K consists of all the matrices $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. By lemma 16.3 K is normal in G. Thus as in part (3) of the proof of Theorem 18.1 the joint eigenvectors of K are carried by G into joint eigenvectors of K. Thus any element of G either leaves fixed or interchanges the one-dimensional subspaces given by the two basis vectors of F^2. If an element of G fixes both subspaces it lies in K. Hence $[G:K] = 1$ or 2.

Now consider the case that K does not admit diagonal form. By Theorem 18.1 K admits triangular form. So the elements of K have the form $\begin{pmatrix} a & 0 \\ b & a^{-1} \end{pmatrix}$.

Now $(1 \quad 0)$ is a joint eigenvector for K. If there were another joint eigenvector independent from $(1 \quad 0)$ then K would admit diagonal form, a contradiction. So again as in part (3) of the proof of Theorem 18.1 the span of $(1 \quad 0)$ must be invariant under G and G must admit triangular form.

Chapter 5

The Galois Theory

20) **Three Lemmas —**

Lemma 20.1 — Let K be a differential field with algebraically closed constant field C. Let L be a differential field extension of K, with constant field D. Let f_α, g be polynomials in a finite number of ordinary indeterminates over K, α ranging over a (possibly infinite) index set. If the equations $f_\alpha = 0$ and inequality $g \neq 0$ have a solution in D they have a solution in C.

Proof — Let $\{u_\beta\}$ be a vector space basis of K over C. Then there are unique expressions $f_\alpha = \sum h_{\alpha\beta} u_\beta$ where $h_{\alpha\beta} \in C[x_1, \cdots, x_n]$ and $x_1, \cdots, x_n$ are ordinary indeterminates. The u's are linearly independent in K over C. Hence the Wronskian of any finite set of the u's does not vanish. In section 10 we observed the consequence of Theorem 10.1 that the vanishing of the Wronskian is independent of the choice of fields. Thus the independence of the u's over constants survives in L. Suppose we have a solution to $f_\alpha = 0$ and $g \neq 0$ in D. Then there exists $a \in D^n$ such that $h_{\alpha\beta}(a) = 0$ for every α, β. Hence the ideal generated by $\{h_{\alpha\beta}\}$ in $D[x_1, \cdots, x_n]$ has a zero in D^n. If the ideal generated by $\{h_{\alpha\beta}\}$ in $C[x_1, \cdots, x_n]$ does not have a zero in C^n, then it is all of $C[x_1, \cdots, x_n]$ (follows from Hilbert's Nullstellensatz.) But then $\sum g_{\alpha\beta} h_{\alpha\beta} = 1$ for some

$g_{\alpha\beta} \in C[x_1, \cdots, x_n]$. Hence there are no zeros to all the $h_{\alpha\beta}$'s in D^n, a contradiction. Thus the $h_{\alpha\beta}$'s have a solution in C.

Similarly we have $g = \sum t_\gamma u_\gamma$ where $t_\gamma \in C[x_1, \cdots, x_n]$. If $g = 0$ where all the $h_{\alpha\beta}$'s equal 0 so each $t_\gamma = 0$ at all such points, then each t_γ is in the radical of the ideal I, generated by all the $h_{\alpha\beta}$'s in $C[x_1, \cdots, x_n]$. Thus each $t_\gamma^{r_\gamma} \in I$ for suitable r_γ, by Hilbert's Nullstellensatz. Then any point in D^n which is a zero of all f_α's will be a zero of all $h_{\alpha\beta}$'s, hence of all t_γ's, hence of g, a contradiction. Therefore we have some solution of $f_\alpha = 0$ and $g \neq 0$ in C.

Lemma 20.2 — Let K be a differential field with constant field C. Let $k_1, \cdots, k_n$ be constants in some differential extension field of K. If $k_1, \cdots, k_n$ are algebraically dependent over K they are algebraically dependent over C.

Proof — There exist a polynomial relation over K such that $f(k_1, \cdots, k_n) = 0$. Let $\{u_\beta\}$ be a vector space basis of K over C. Again consider the unique expression $f_\alpha = \sum h_{\alpha\beta} u_\beta$ where the $h_{\alpha\beta}$'s are nonzero polynomials over C. The u_β's are linearly independent over C, hence $h_{\alpha\beta}(k_1, \cdots, k_n) = 0$ for every α, β. Therefore $k_1, \cdots, k_n$ are algebraically dependent over C.

Lemma 20.3 — Let F be any field, I an integral domain over F with finite transcendence degree over F. Let P be a prime ideal in I, $P \neq 0$ or $P \neq I$. Then the transcendence degree of I / P over F is strictly less than that of I over F.

Proof — An element u of P cannot be algebraic over F. Otherwise there exists some relation $a_n u^n + a_{n-1}u^{n-1} + \cdots + a_1 u + a_0 = 0$, $a_i \in F$. We can take $a_0 \neq 0$. Hence $1 = -\frac{a_n}{a_0}u^n - \frac{a_{n-1}}{a_0}u^{n-1} - \cdots - \frac{a_1}{a_0}u \in P$. Thus $P = I$, a contradiction. Next we take $u = u_1$ the first element of a transcendence basis $\{u_1, \cdots, u_r\}$ of I over F ($u_1, \cdots, u_r$ are algebraically independent over F and I is algebraic over its subring $F[u_1, \cdots, u_r]$.) These elements map into $0, v_2, \cdots, v_r$ in the integral domain I/P. If we can show that any $y \in I/P$ is algebraically dependent on $v_2, \cdots, v_r$ then we are done. Take $x \in I$ mapping on $y \in I/P$. We know x satisfies some polynomial equation with coefficients polynomials in the u's. Let $f(X) = r_k X^k + r_{k-1}X^{k-1} + \cdots + r_1 X + r_0$ be a polynomial in X with the r's polynomials in the u's, such that $f(X)$ is of minimal degree among the nonzero polynomials with $f(x)$ lying in P. Mapping modulo P, the result gives us y dependent on the v's unless all the r's are in P. The latter event cannot be, since then $f(x) = (r_k x^{k-1} + r_{k-1}x^{k-2} + \cdots + r_1)x \in P$, but $x \notin P$, so $r_k x^{k-1} + r_{k-1}x^{k-2} + \cdots + r_1 \in P$, contradicting the minimality of the degree of the degree of $f(X)$.

21) **Normality of Picard–Vessiot Extensions** — Let $M = K\langle u_1, \cdots, u_n \rangle$ be a Picard-Vessiot extension of K. Then $u_1, \cdots, u_n$, linearly independent over constants, are solutions to some linear homogeneous differential equation in K, say $L(u) = u^{(n)} + a_1 u^{(n-1)} + \cdots + a_{n-1}u' + a_n u = 0$, and M has the same field of constants

as K. Let σ be an admissible differential isomorphism of M over K. Then there is a larger differential field $N \supset M$ and σ is a differential isomorphism of M onto another subfield of N leaving K elementwise fixed. Since σ commutes with differentiation then $L(u_i\sigma) = (L(u_i))\sigma = 0$, so every $u_i\sigma$ is a solution to the underlying differential equation of the Picard-Vessiot extension. Thus each $u_i\sigma = \sum k_{ij}u_j$ with constants k_{ij} in N. Hence each σ gives rise to a non-singular matrix of constants.

Lemma 21.1 — Let K be a differential field with constant field C. Let $M = K\langle u_1, \cdots, u_n \rangle$ be a Picard-Vessiot extension of K. There exists a set S of polynomials (in n^2 ordinary indeterminates) with coefficients in C such that, (a) every admissible differential isomorphism of M over K gives rise to a matrix of constants satisfying S, and (b) given a differential field extension N of M, and a non-singular matrix k_{ij} of constants of N satisfying S, there exists an admissible differential isomorphism of M/K into N sending u_i into $\sum k_{ij}u_j$.

Proof — Let $y_1, \cdots, y_n$ be differential indeterminates over K. Define a differential homomorphism of $K\{y_1, \cdots, y_n\}$ into $M = K\langle u_1, \cdots, u_n \rangle$ by keeping K fixed and sending y_i to u_i. The kernel Γ is a prime differential ideal in $K\{y_1, \cdots, y_n\}$ since it is a differential ideal by Theorem 2.3 and for $ab \in \Gamma$ letting ϕ be our differential homomorphism it follows that $\phi(ab) = \phi(a)\phi(b) = 0$ and either $\phi(a) = 0$ or $\phi(b) = 0$.

Let c_{ij} for $i,j=1,\cdots,n$ be a set of n^2 ordinary indeterminates over M. Define a differential homomorphism ψ of $K\{y_1,\cdots,y_n\}$ into $M[c_{ij}]$ by the mapping $y_i \to \sum c_{ij}u_j$. Let $\psi[\Gamma]=\Delta$. Then Δ is an ideal in the image of $K\{y_1,\cdots,y_n\}$ contained in $M[c_{ij}]$. Thus the elements of Δ are ordinary polynomials in n^2 ordinary indeterminates c_{ij} with coefficients in the field M, $\sum m_l\left(\prod c_{ij}^{t_{ijl}}\right)_l$ for $m_l \in M$. Let $\{w_\alpha\}$ be a vector space basis of M over C. Then each coefficient of the polynomials of Δ may be written as a linear combination of the w's with coefficients in C, $m_l=\sum k_{l\alpha}w_\alpha$ for $k_{l\alpha} \in C$. Next rearranging the polynomials of Δ we write each as a linear combination of w's with coefficient polynomials over C, $\sum_l m_l\left(\prod c_{ij}^{t_{ijl}}\right)_l=\sum_l\left(\sum_\alpha k_{l\alpha}w_\alpha\right)\left(\prod c_{ij}^{t_{ijl}}\right)_l=\sum_\alpha\sum_l\left(k_{l\alpha}\left(\prod c_{ij}^{t_{ijl}}\right)_l\right)w_\alpha$. The collection S of all these polynomials over C is our candidate to meet the needs of the lemma.

(a) Suppose there exists an admissible differential isomorphism σ of M/K such that u_i is sent into $\sum k_{ij}u_j$ with the k's constants of the larger field. We perform the homomorphism of $K\{y_1,\cdots,y_n\}$ into $K\{u_1,\cdots,u_n\}$ (by keeping K fixed and sending y_i into u_i) followed by σ. In the composite homomorphism y_i is sent to $\sum k_{ij}u_j$, K is fixed and Γ is sent to 0. Next consider the mapping given by sending y_i into $\sum c_{ij}u_j$ followed by a mapping sending c_{ij} into k_{ij}. This time as before in the composite homomorphism y_i is sent to $\sum k_{ij}u_j$, K is fixed but Γ goes to Δ evaluated at $c_{ij}=k_{ij}$. Hence all the polynomials of Δ vanish at k_{ij}. As above expressing each polynomial in terms of the vector space basis w_α of M over C, we have that the polynomials in our set S vanish at k_{ij}.

(b) Let N be a differential field extension of M. Let k_{ij} be a non-singular matrix of constants in N satisfying S. As before we define a homomorphism of $K\{y_1,\cdots,y_n\}$ into N by $y_i \to \sum k_{ij}u_j$ in two steps $y_i \to \sum c_{ij}u_j$ and $c_{ij} \to k_{ij}$. We know that the kernel contains Γ and so we have a homomorphism σ of $K\{u_1,\cdots,u_n\}$ onto $K\{u_1\sigma,\cdots,u_n\sigma\}$, where $u_i\sigma = \sum k_{ij}u_j$. We need now to show that σ is one-to-one, for then we can finish the proof by extending it to the quotient field of $K\{u_1,\cdots,u_n\}$. Assume σ is not one-to-one with the non-trivial kernel Γ_0. Let $\partial K\langle u_1,\cdots,u_n\rangle/K$ denote transcendence degree of $K\langle u_1,\cdots,u_n\rangle$ over K that we know to be finite since each u_i is the solution of a differential equation. Then $K\{u_1\sigma,\cdots,u_n\sigma\} \cong K\{u_1,\cdots,u_n\}/\Gamma_0$ and by Lemma 20.3 it follows that $\partial K\langle u_1,\cdots,u_n\rangle/K > \partial K\langle u_1\sigma,\cdots,u_n\sigma\rangle/K$. Adopt the abbreviation $K\langle u\rangle$ for $K\langle u_1,\cdots,u_n\rangle$, $K\langle u\sigma\rangle$ for $K\langle u_1\sigma,\cdots,u_n\sigma\rangle$ and $C(k)$ for $C(k_{ij}\text{'s})$. By the additivity of transcendence degrees we get $\partial K\langle u,u\sigma\rangle/K\langle u\rangle < \partial K\langle u,u\sigma\rangle/K\langle u\sigma\rangle$. And we have by Lemma 20.2 $\partial K\langle u,u\sigma\rangle/K\langle u\rangle = \partial C(k)/C$. Similarly $\partial K\langle u,u\sigma\rangle/K\langle u\sigma\rangle = \partial C'(k)/C'$ where C' is the field of constants in $K\langle u\sigma\rangle$. But $\partial C'(k)/C' \le \partial C(k)/C$. So the assumption that σ is not one-to-one leads to a contradiction. Therefore our proof is complete.

Recall that the differential Galois Group G of M/K is the group of all differential automorphisms of M leaving K elementwise fixed. Suppose that in part (a) of Lemma 21.1 each admissible differential isomorphism of M/K was actually a differential automorphism of M/K. Then each automorphism corresponds uniquely to a matrix of constants satisfying the polynomials of S. Thus the following is a special case of Lemma 21.1.

Theorem 21.2 — The differential Galois group of a Picard-Vessiot extension is an algebraic matrix group over the field of constants.

The issue now is existence.

Lemma 21.3 — Let K be a differential field with an algebraically closed field of constants. Let M be a Picard-Vessiot extension of K. Suppose that we are given an element z and two subsets $\{x_\alpha\}$ and $\{y_\alpha\}$ of M, α ranging over a (possibly infinite) index set. Suppose that there exists an admissible differential isomorphism of M over K sending x_α into y_α and moving z. Then there exists a differential automorphism of M over K sending x_α into y_α and moving z.

Proof — Suppose our admissible differential isomorphism σ is given by $u_i\sigma = \sum k_{ij}u_j$, the k's being constants in the larger field. Take any elements $x, y \in M = K\langle u_1, \cdots, u_n \rangle$. Then $x = P(u)/Q(u)$, $y = R(u)/S(u)$ where $P(u)$, $Q(u)$, $R(u)$ and $S(u)$ are polynomials in the u's and their derivatives. Suppose further that $y = x\sigma$. Then $R(u)/S(u) = (P(u)/Q(u))\sigma = P(u\sigma)/Q(u\sigma)$ and $S(u)P(u\sigma) = R(u)Q(u\sigma)$. By our hypothesis we have one such equation for each α, $x_\alpha\sigma = y_\alpha$. Substituting $u_i\sigma = \sum k_{ij}u_j$ we get a polynomial expression in the k's with coefficients in M for each α, $\sum m_{\alpha l}\left(\prod k_{ij}^{t_{ijl}}\right)_l = 0$. Include with these equations the equations of the set S of polynomials in Lemma 21.1. By hypotheses we have $z\sigma \neq z$ and $|k_{ij}| \neq 0$, k_{ij} the matrix representation of σ. So writing z as the ratio of polynomials in the u's and their derivatives, we can rewrite $z\sigma \neq z$ in the form $g(k_{ij}) \neq 0$, a polynomial in the k's with coefficients in M. Lemma 21.1(a) gives us a constant solution for the equations of the set S in the larger field, and we have $\sum m_{\alpha l}\left(\prod k_{ij}^{t_{ijl}}\right)_l = 0$ and $g(k_{ij}) \neq 0$. Thus there is a constant solution to all the equations combined in the larger field. By lemma 20.1 there is a constant solution in C. This and Lemma 21.1(b) gives us an admissible differential isomorphism of M/K onto $M \subset N$, the differential automorphism we are seeking.

Theorem 21.4 — Let K be a differential field of characteristic zero with an algebraically closed constant field. Then any Picard-Vessiot extension M of K is normal.

Proof — Let $z \in M$ and $z \notin K$. By Theorems 8.1 and 8.3 there exists an admissible differential isomorphism M/K moving z. Then by Lemma 21.3 there exists a differential automorphism of M/K moving z. Therefore M is normal.

Theorem 21.5 — Let K be a differential field of characteristic zero with an algebraically closed constant field. Let M be a Picard-Vessiot extension of K. Then any differential isomorphism over K between two intermediate differential fields can be extended to a differential automorphism of M. In particular any differential automorphism over K of an intermediate differential field can be so extended.

Proof — Using Theorem 8.1 we extend the given differential isomorphism to an admissible differential isomorphism defined on all of M. By Lemma 21.3 our theorem follows.

22) **Completion of the Galois Theory** —

Theorem 22.1 — Let K be a differential field of characteristic 0 with an algebraically closed constant field. Let M be a Picard-Vessiot extension of K. Then the Galois theory implements a one-to-one correspondence between the intermediate differential fields and the algebraic subgroups of the differential Galois group G. A closed subgroup H is normal if and only if the corresponding field L is normal over K and G/H is the full differential Galois group of L over K.

Proof — Let M be a Picard-Vessiot extension of K a differential field of characteristic 0 with an algebraically closed constant field. If L is any intermediate differential field, it follows from the existence and uniqueness that M is a Picard-Vessiot extension of L (adjunction of the solutions to L gets us M). Then by Theorem 21.4, M is normal over L. In section 9 chapter 3 we concluded that if a differential field is normal over a differential subfield then the subfield is closed. Hence all intermediate differential fields of a Picard-Vessiot extension are closed. If we can show that the corresponding differential Galois subgroups are Galois-closed (closed in the sense of Galois theory) then the correspondence is one-to-one (recall our discussion early in section 9 of Chapter 3).

Suppose H is a normal subgroup of the differential Galois group G. Then $L = H'$, the differential field corresponding to H, is sent onto itself by any differential automorphism of M / K, by Theorem 9.4(a). Hence any element that lies in H' and not in K can be moved by a differential automorphism of M / K restricted to H', a differential automorphism of H' / K. Hence the differential subfield corresponding to a normal differential Galois subgroup is normal. By Theorem 21.5 all differential automorphism of L/K are extendable to M. Next by Theorem 9.4(b) G/H is the group of all the automorphisms of L/K which can be extended to M. Thus L is normal over K and G/H is the full differential Galois group of L/K.

Now the converse. We observed in Chapter 4 section 17 in connection with the definition of C-groups that matrices under the Zariski topology form a C-group. By Theorem 21.2 G is an algebraic matrix group and hence a C-group. Then by Lemma 17.5 (if H is topologically closed then) the normalizer of H is topologically closed. Next it follows by Lemma 9.6 that if L is closed in M and normal over K then the corresponding subgroup H is normal in G. But since L is an intermediate field of a Picard-Vessiot extension, it is closed. Our hypotheses are that L is normal over K and G/H is the full differential Galois group of L over K. So we need only the closure of $\acute{H}$ to complete the proof.

Since G is an algebraic matrix group so are all the subgroups corresponding to the intermediate differential fields (Theorem 21.2). If we can show that the algebraic subgroups of G are Galois-closed then we will be finished.

Let H be a subgroup in G. Our task is to show that H is Zariski-dense in H'', i.e. $H'' \subset \overline{H}$, the algebraic closure of H. It will then follow that $H = H''$ since $H'' \subset \overline{H} = H \subset H''$. Suppose $H'' \not\subset \overline{H}$ then there exists a polynomial f in n^2 variables coefficients in C which vanishes on H but not on H''. Continuing with the supposition that H is not closed we follow Kaplansky's construction for the case $n = 2$ to arrive at a contradiction and give us the flavor of why it works in general. Let $M = K\langle u,v\rangle$. The matrix $\begin{pmatrix} u & v \\ u' & v' \end{pmatrix}$ is non-singular since the determinant is the Wronskian of linearly independent solutions of an ordinary differential equation. Let $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be the inverse. Let y and z be differential indeterminates over M. Let F be a differential polynomial defined by $F(y,z) = f(Ay + By', Az + Bz', Cy + Dy', Cz + Dz')$ where f is a polynomial in 2^2 variables with coefficients in C which vanishes on H but not on H''. Take $y = u\sigma$ and $z = v\sigma$ for some $\sigma \in H$. Then for the matrix k_{ij} of σ, we have

$\begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} u & v \\ u' & v' \end{pmatrix}\begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix}$. Multiplying by the inverse of $\begin{pmatrix} u & v \\ u' & v' \end{pmatrix}$ we get $\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix}$. Hence $F(u\sigma, v\sigma) = f(k_{11}, k_{21}, k_{12}, k_{22}) = 0$ for $\sigma \in H$ and not for all $\sigma \in H''$. Among all the differential polynomials in $M\{y,z\}$ with this property pick one which when written as the sum of monomials has the smallest possible number of terms. Name it E and take one of its coefficients to be 1. Let E_τ be the polynomial obtained by replacing the coefficients of E by the image of the same coefficient under some $\tau \in H$. Let $m(u\sigma)^s(v\sigma)^t(u'\sigma)^r(v'\sigma)^q$ be a term in $E(u\sigma, v\sigma)$. Replacing m by $m\tau$ and then applying $\tau^{-1}\tau$ gives us $\left(m\tau(u\sigma)^s(v\sigma)^t(u'\sigma)^r(v'\sigma)^q\right) = \left(m(u\sigma\tau^{-1})^s(v\sigma\tau^{-1})^t(u'\sigma\tau^{-1})^r(v'\sigma\tau^{-1})^q\right)\tau$. Hence $E_\tau(u\sigma, v\sigma) = \left[E(u\sigma\tau^{-1}, v\sigma\tau^{-1})\right]\tau$. But for $\sigma \in H$ then $\sigma\tau^{-1} \in H$. So $E_\tau(u\sigma, v\sigma) = \left[E(u\sigma\tau^{-1}, v\sigma\tau^{-1})\right]\tau = 0$ for every $\sigma \in H$. The polynomial $E - E_\tau$ is shorter than E since $1\tau = 1$. Thus it must vanish for every $u\sigma, v\sigma$ with $\sigma \in H''$. If $E - E_\tau$ is not identically 0, there exist $\gamma \in M$ such that $E - \gamma(E - E_\tau)$ is shorter than E. But $E - \gamma(E - E_\tau)$ shares with E the property that it vanishes at $u\sigma, v\sigma$ for all $\sigma \in H$ and not all $\sigma \in H''$ since $E - E_\tau$ vanishes for every $u\sigma, v\sigma$ with $\sigma \in H''$. So we have a contradiction, except when $E - E_\tau \equiv 0$. But in the case $E \equiv E_\tau$, every coefficient $m = m\tau$ lies in $L = H'$ the elements of M left fixed by the automorphism of H and H'' is all the automorphisms of G leaving $L = H'$ elementwise fixed. So $E(u\sigma, v\sigma) = 0$ for all $\sigma \in H''$, a contradiction. Therefore H is closed and the proof to Theorem 22.1 is complete.

23) **Liouville Extensions —**

Lemma 23.1 — Let M be a Picard-Vessiot extension of K where K is a differential field of characteristic 0 with an algebraically closed constant field. Let $N = M\langle z \rangle$ be an extension of M with no new constants. Write $L = K\langle z \rangle$. Then N is a Picard-Vessiot extension of L, and its differential Galois group is isomorphic to an algebraic subgroup of the differential Galois group of M over K, namely the subgroup leaving $M \cap L$ fixed.

Proof — Since there are no new constants in N, then N and L have the same constant field. The solutions of the underlying differential equation generating M over K also generate N over L since we may choose the order of adjunction. Hence N is a Picard-Vessiot extension of L. Since $K \subset L$ and $K \subset M$ any differential automorphism of N/L is a differential automorphism of N/K and hence sends M onto itself by Lemma 11.1. Thus we have a map of all of the differential automorphisms of N/L into the differential automorphisms of M/K. In other words we have a homomorphism of the differential Galois group of N/L onto a subgroup G_1 of the differential Galois group of M/K since the group operations are preserved by the map. Any automorphism in the kernel leaves M and L fixed and hence fixes $M \cup L$. But then it fixes all of N and is the identity. So our homomorphism is an isomorphism and the image G_1 is isomorphic with the Galois group of the Picard-Vessiot extension N of L. Then by Theorem 21.2 G_1 is an algebraic matrix group over a field of constants. All the automorphisms of G_1 fix at least K of M and are isomorphic to automorphisms of N/L that fix all of $L \supset K$. Hence the fixed field of G_1 is $M \cap L$. We note that the identity subgroup of G_1 is closed and normal so by Theorem 22.1, G_1 is the whole group of differential automorphisms of M leaving $M \cap L$ fixed. The proof is complete.

Theorem 23.2 — Let M be a Picard-Vessiot extension of K where K is a differential field of characteristic 0 with an algebraically closed constant field. Suppose that the differential Galois group of M over K has a solvable component of identity. Then M can be obtained from K by a finite-dimensional normal extension, followed by a Liouville extension.

Proof — Let G be the differential Galois group, C its component of identity. Let L be the intermediate differential field corresponding to C. By Theorem 16.3 C is a closed, normal subgroup of finite index in G. Hence L is closed and normal over K by Theorem 22.1 and its proof. Lemma 9.2 guarantees that L is a finite-dimensional extension of K. Since C is the group of all the automorphisms of M/K that fix L elementwise, then C is the differential Galois group of M/L and by Theorem 22.1 and its proof M is a Picard-Vessiot extension of L. Hence by hypothesis and Theorem 21.2 C is a solvable algebraic matrix group over the field of constants. Thus by Theorem 18.1 C can be put in simultaneous triangular form. Finally, Theorem 14.1 gives us that M is a Liouville extension of L.

Definition — A differential field N is a **generalized Liouville extension** of K if N can be obtained from K by a finite number of steps, each of which is a finite algebraic extension, or the adjunction of an integral, or the adjunction of an exponential of an integral.

Theorem 23.3 — Let M be a Picard-Vessiot extension of K where K is a differential field of characteristic 0 with an algebraically closed constant field. Suppose that M can be embedded in a differential field N, which is a generalized Liouville extension of K with no new constants. Then the component of identity of the differential Galois group G is solvable (whence by Theorem 23.2, M can be obtained from K by a finite-dimensional normal extension followed by a Liouville extension).

Proof — We use induction on the number of steps in the Liouville chain from K to N. Let $K\langle z\rangle$ be the first step of the chain. In the same manner as that used in the proof of Theorem 13.1 we conclude that the Galois group of $M\langle z\rangle$ over $K\langle z\rangle$ is solvable and hence has a solvable component of identity. By Lemma 23.1 this group is isomorphic to the subgroup H of G leaving $M \cap K\langle z\rangle$ fixed. Suppose z is algebraic over K. Then by Lemma 9.1 H is of finite index in G. It follows by Lemma 17.4 that the component of identity in G is solvable and we are done. Next suppose that z is either an integral or the exponential of an integral. By Lemmas 12.1 or 12.2 $K\langle z\rangle$ is a Picard-Vessiot extension of K with abelian Galois group (hence normal subgroups). Thus the differential fields between K and $K\langle z\rangle$ are normal over K. In particular $M \cap K\langle z\rangle$ is normal over K with an abelian differential Galois group. Thus H is normal in G and by Theorem 22.1 G/H is abelian. Again by Theorem 17.4 the component of identity in G is solvable (26-40).

Chapter 6

Equations of Order Two

24). **The Wronskian** — Let $W = W(u_1,\cdots,u_n)$ be the Wronskian of $u_1,\cdots,u_n$ where $M = K\langle u_1,\cdots,u_n\rangle$ is a Picard-Vessiot extension.

Lemma 24.1 — Let σ be a differential automorphism of M over K, with corresponding matrix c_{ij}. Then $W\sigma = |c_{ij}|W$.

Proof — We have $u_i\sigma = \sum c_{ij}u_j$. Thus

$$\begin{pmatrix} u_1\sigma & \cdots & u_n\sigma \\ \vdots & \vdots & \vdots \\ u_1^{(n-1)}\sigma & \cdots & u_n^{(n-1)}\sigma \end{pmatrix} = \begin{pmatrix} u_1 & \cdots & u_n \\ \vdots & \vdots & \vdots \\ u_1^{(n-1)} & \cdots & u_n^{(n-1)} \end{pmatrix} \begin{pmatrix} c_{11} & \cdots & c_{n1} \\ \vdots & \vdots & \vdots \\ c_{1n} & \cdots & c_{nn} \end{pmatrix}.$$ But

$$\det\begin{pmatrix} u_1\sigma & \cdots & u_n\sigma \\ \vdots & \vdots & \vdots \\ u_1^{(n-1)}\sigma & \cdots & u_n^{(n-1)}\sigma \end{pmatrix} = \left(\det\begin{pmatrix} u_1 & \cdots & u_n \\ \vdots & \vdots & \vdots \\ u_1^{(n-1)} & \cdots & u_n^{(n-1)} \end{pmatrix}\right)\sigma$$ since multiplication and addition are preserved by σ. So $W\sigma = |c_{ij}|W$.

Lemma 24.2 — The field $K\langle W\rangle$ corresponds to the unimodular subgroup of the differential Galois group.

Proof — Lemma 24.1 tells us that W is fixed if and only if $|c_{ij}| = 1$.

Lemma 24.3 — If the underlying differential equation reads $y^{(n)} + ay^{(n-1)} + \cdots = 0$, then $W' = -aW$.

Proof — The derivative of a determinant of a $n \times n$ matrix is given by the sum of determinants of the n matrices given by taking the derivative of rows in the original matrix a row at a time. In the case of a Wronskian taking the derivative of any row but the last gives a matrix with a determinant of 0 since it yields a matrix with two identical rows. Thus we have

$W' = \det\begin{pmatrix} u_1 & \cdots & u_{n-1} & u_n \\ \vdots & \vdots & \vdots & \vdots \\ u_1^{(n-2)} & \cdots & u_{n-1}^{(n-2)} & u_n^{(n-2)} \\ u_1^{(n)} & \cdots & u_{n-1}^{(n)} & u_n^{(n)} \end{pmatrix}$. Substituting the differential equation in to the last row gives $W' = \det\begin{pmatrix} u_1 & \cdots & u_{n-1} & u_n \\ \vdots & \vdots & \vdots & \vdots \\ u_1^{(n-2)} & \cdots & u_{n-1}^{(n-2)} & u_n^{(n-2)} \\ -au_1^{(n-1)} - h_1 & \cdots & -au_{n-1}^{(n-1)} - h_{n-1} & -au_n^{(n-1)} - h_n \end{pmatrix}$ where each h_i is a linear combination of the elements above it in the matrix. Evaluate the determinant by a cofactor expansion of the last row, the sum of the product of each row element with its cofactor. We see that the sum of the products of h's with cofactors contribute 0. Hence $W' = -aW$.

Corollary — If $a = 0$ then W is a constant and the differential Galois group consists only of unimodular matrices.

The classical method of removing the term $ay^{(n-1)}$ from an n-th order equation is at the expense of an exponential of an integral. The usual substitution is to let $y = wz$ where w is a solution to the equation $nw' + aw = 0$ ($w = e^{-\int \frac{a}{n}}$). The resulting equation in z has no term in $z^{(n-1)}$. For example in the case of the equation $y'' + x^2 y' = 0$ we note that the substitution removes $e^{\int \frac{x^2}{2}}$ and gives the equation $z''-\left(\frac{x^4}{4}+x\right)z=0$. We now consider the second order equations of the form $y''+ay=0$.

25) **Connection with a Riccati Equation —**

Theorem 25.1 — Let K be a differential field of characteristic 0 with an algebraically closed field of constants, and let $a\in K$. Let M be a Picard-Vessiot extension of K for the equation $y''+ay=0$. Suppose that M is a generalized Liouville extension of K but is not finite-dimensional over K. Then the equation $t'=t^2+a$ has a solution either in K or a quadratic extension of K.

Proof — By the corollary to Lemma 24.3, the differential Galois group G of M over K is an algebraic matrix group of 2×2 matrices with determinant equal to 1. By our hypothesis Theorem 23.3 tells us that the component of identity in G is solvable and by Theorem 23.2 M can be obtained from K by a finite dimensional normal extension followed by a Liouville extension. Our hypothesis ruled out the case of finite G and we consider the remaining two cases provided by Theorem 19.1 and its proof: (b) C the component of identity in G can be put in diagonal form and $[G{:}C]=2$, (c) G can be put in simultaneous triangular form. In case (b) there is a quadratic extension L of K (corresponding to C) such that the differential Galois group of M over L can be put in diagonal form (G/C is the full differential Galois group of L over K). In case (c) we may take $L=K$ (the degree of the extension is 1 since as we saw in the proof of Theorem 19.1 the triangular matrices have one joint eigenvector). Thus there is a non-zero solution u of $y''+ay=0$ carried to a constant multiple of itself by every automorphism of M over L. Thus $\frac{u'}{u}\in L$, since $u\sigma=bu$ for b a constant implies $\frac{u'}{u}\sigma=\frac{u'}{u}$. Put $t=-\frac{u'}{u}$. Then $u''=-u't-ut'=u(t^2-t')$. But $u''=-au$. So $t'=t^2+a$.

Lemma 25.2 — Let K be a differential field, a an element in K, and t an algebraic element over K satisfying $t'=t^2+a$, and having $t^2+rt+s=0$ as its irreducible equation over K. Then $r''+3rr'+r^3+4ar+2a'=0$.

Proof — We use computation only. Differentiate $\left(t^2+rt+s\right)'=2tt'+r't+rt'+s'=0$. Substitute $t'=t^2+a$, $2t^3+rt^2+(2a+r')t+ar+s'=0$. Next $2t\left(t^2+rt+s\right)=2t^3+2rt^2+2st=0$. Subtracting the last two equations, $rt^2+(2s-2a-r')t-ar-s'=0$. Then $r\left(t^2+rt+s\right)=rt^2+r^2t+rs=0$. Comparing the last two equations yields $r^2=2s-2a-r'$ and $rs=-ar-s'$ or $rs+ar+s'=0$. Write $2s=2a+r'+r^2$, differentiate $2s'=2a'+r''+2rr'$. Substitute the last two for $2s$ and $2s'$ into $2(rs+ar+s')=2rs+2ar+2s'=0$ we have $r''+3rr'+r^3+4ar+2a'=0$.

26) **An Example** — Consider the classical case $y''+xy=0$ (known as Airy's equation) with a base field K of all rational functions of x with complex coefficients. The solutions are entire functions and there is a well-defined Picard-Vessiot extension M inside the field of functions meromorphic in the whole

plane. Algebraic entire functions are polynomials and there are no polynomial solutions to Airy's equation, we conclude that $[M{:}K]$ is not finite.

We will show that it is not possible that $t' = t^2 + x$ has a solution in K or in a quadratic extension of K. Then by Theorem 25.1 a solution of $y'' + xy = 0$ cannot be obtained from the field of rational functions of x by any sequence of finite algebraic extensions, adjunction of integrals and adjunction of exponential of integrals.

Let $t = f/g$ where f and g are relatively prime polynomials. Then substituting into $t' = t^2 + x$ and clearing denominators we get $gf' - fg' - f^2 = g^2x$. Let $a =$ degree of f and $b =$ degree of g. If $a > b$ then f^2 is the unique leading term and the equation cannot be cancelled. If $b \geq a$ then g^2x is the unique leading term and the equation cannot be cancelled. Hence we have no solution of $t' = t^2 + x$ in K.

Now consider the case that $t' = t^2 + x$ has a solution in a quadratic extension of K but not in K. Lemma 25.2 gives us the equation $r'' + 3rr' + r^3 + 4xr + 2 = 0$ where $t^2 + rt + s = 0$. We take the partial fraction expansion of the rational function r. Let $\sum_{i=1}^{n} c_i(x-k)^{-i}$ be the portion of the expansion of r for the linear factor $(x-k)$ of the denominator of r. Substituting into $r'' + 3rr' + r^3 + 4xr + 2 = 0$, the highest degree term in the denominator of

$r'' = \left(\sum_{i=1}^{n} c_i (x-k)^{-i} \right)''$ is of degree $n+2$, for $3rr' = 3\left(\sum_{i=1}^{n} c_i (x-k)^{-i} \right)\left(\sum_{i=1}^{n} c_i (x-k)^{-i} \right)'$ the highest degree in the denominator is $2n+1$, and for $r^3 = \left(\sum_{i=1}^{n} c_i (x-k)^{-i} \right)^3$ the highest degree in the denominator is $3n$. We must have equality among at least two of the three highest so that $r'' + 3rr' + r^3 + 4xr + 2 = 0$ will hold. This can only be true for $n = 1$. Thus there can be no repeat linear factors in the denominator of r. Then for the term $\frac{c}{x-k}$ we get $\frac{2c}{(x-k)^3}$, $\frac{-3c^2}{(x-k)^3}$ and $\frac{c^3}{(x-k)^3}$ from r'', $3rr'$ and r^3 respectively. Hence $2c - 3c^2 + c^3 = 0$, so $c = 1$ or $c = 2$.

Next let's look at the representation $r = f/g$. $r' = \frac{gf' - fg'}{g^2}$ and $r'' = \frac{g^3 f'' - fg^2 g'' - 2g^2 g' f' + 2gf(g')^2}{g^4}$, $3rr' = \frac{3ff'g - 3f^2 g'}{g^3}$, $r^3 = \frac{f^3}{g^3}$ and $4xr = \frac{4xf}{g}$. Bringing every term to the common denominator g^4 we have the following terms in the numerator: $g^3 f''$, $fg^2 g''$, $g^2 f' g'$, $gf(g')^2$, $ff' g^2$, $f^2 gg'$, $f^3 g$, xfg^3, and g^4. Again we let degree of $f = a$ and degree of $g = b$. Then:

The degree of $g^3 f''$, $fg^2 g''$, $g^2 f' g'$, and $gf(g')^2$ $= a + 3b - 2$,

The degree of $ff' g^2$ and $f^2 gg'$ $= 2a + 2b - 1$,

The degree of $f^3 g$ $= 3a + b$,

The degree of xfg^3 $= a + 3b + 1$,

The degree of $g^4 = 4b$.

If $a = b$ then xfg^3 cannot be cancelled. If $a > b$ then f^3g is uniquely the highest term. But if $b > a$ and $a = b-1$, xfg^3 and g^4 can cancel and f^3g can cancel with g^3f'', fg^2g'', $g^2f'g'$, and $gf(g')^2$. If $b > a+1$, g^4 cannot be cancelled.

Hence in the partial fraction expansion of r there will be no polynomial term. And from above we must have the form $\sum \frac{c_i}{(x-a)^i}$ with $c_i = 1$ or $c_i = 2$.

Thus we must have $g(x) = x^b + \cdots$ and $f(x) = \alpha x^{b-1} + \cdots$ with α a positive integer. But then the cancellation between the terms xfg^3 and g^4, arising from the terms $4xr$ and 2 in $r'' + 3rr' + r^3 + 4xr + 2 = 0$, will not occur since $4\alpha + 2 \neq 0$. Hence it is not possible that $t' = t^2 + x$ has a solution in K or in a quadratic extension of K. Then by Theorem 25.1 we write:

Theorem 26.1 — The solutions of the equation $y'' + xy = 0$ cannot be obtained from the field of rational functions of x by any sequence of finite algebraic extensions, adjunction of integrals, or adjunction of exponentials of integrals.

Kaplansky observes that by additional considerations it can be established that the Galois group of the equation $y'' + xy = 0$ is the full unimodular group of 2×2 matrices. This follows from the fact that any proper algebraic subgroup has a solvable component of identity (41-44).

Works Cited

Fraleigh, John B. *A First Course In Abstract Algebra.* 5th ed. New York: Addison-Wesley, 1994.

Kaplansky, Irving. *An Introduction To Differential Algebra* . Paris: Hermann, 1957.

Kolchin, E. R. "Algebraic Matric Groups and the Picard-Vessiot Theory of Homogeneous Linear Ordinary Differential Equations." *Annals of Mathematics.* Vol. 49, No. 1, 1948: 1-42.

Magid, Andy R. *Lectures on Differential Galois Theory.* University Lecture Series Volume 7, Providence: American Mathematical Society, 1994.

Rosenlicht, Maxwell. "Integration In Finite Terms." *American Mathematical Monthly. Vol. 79,* November 1972: 963-972.