ACTUALITÉS SCIENTIFIQUES ET INDUSTRIELLES

1251

PUBLICATIONS DE L'INSTITUT DE MATHÉMATIQUE
DE L'UNIVERSITÉ DE NANCAGO

V

IRVING KAPLANSKY

AN INTRODUCTION TO DIFFERENTIAL ALGEBRA

HERMANN

6, RUE DE LA SORBONNE, PARIS V

PUBLICATIONS DE L'INSTITUT DE MATHÉMATIQUE DE L'UNIVERSITÉ DE NANCAGO

(1) Numéros d'ordre dans la collection: Actualités Scientifiques et Industrielles.

Printed in France

CONTENTS

PREFACE

Differential algebra is easily described: it is (99 per cent or more) the work of Ritt and Kolchin.

I have written this little book to make the subject more easily accessible to the mathematical community. Ritt was at heart an analyst; but the subject is algebra. As a result he wrote in a style that often makes the road rough for both analysts and algebraists.

Kolchin's basic paper [3] on the Picard-Vessiot theory is admirably clear and elegant. However it is not entirely self-contained. In particular, there is a crucial reference to an earlier paper [2], which in turn makes use of the Ritt theory. Certain needed facts from algebraic geometry are also likely to be troublesome to the average reader.

I have sought to make the exposition as self-contained and elementary as possible. In addition to standard algebra (say the contents of Birkhoff and Mac Lane's *Survey of Modern Algebra*), a prospective reader needs only the Hilbert basis theorem, the Hilbert Nullstellensatz, the rudiments of the theory of transcendence degrees, and a smattering of point set topology. A discerning reader will notice several places where proofs can be shortened by the use of more sophisticated techniques (Kronecker products, linear disjointness, methods from algebraic geometry).

There are two main novelties.

(1) The Picard-Vessiot theory is developed without the use of the Ritt-Raudenbush basis theorem.

As a result the book really contains two introductions: Chapters I-VI are an introduction to Kolchin's papers, while Chapters I and VII can serve as an introduction to Ritt's two books and his numerous papers. (Chapter VII can be read directly after Chapter I).

(2) The necessary theory of algebraic matrix groups is developed entirely within the framework of point set topology. Chapter IV gives just the minimum needed in the next two chapters. But in the appendix (Chapter VIII) I have inserted the natural analytic continuation of these ideas.

There are in addition two minor points to which I would like to call attention.

(3) A brisk account of classical Galois theory, slightly generalized, occurs at the beginning of Chapter III. I am indebted to Mr. George Morgan for straightening me out on the proof of Lemma 3.2.

(4) In Chapter VI a « concrete » example of an equation $(y'' + xy=0)$ not solvable by quadratures is carried through in full. Investigations of this kind can be found scattered in the older literature, going back to Liouville. Pertinent references can be located in the extensive bibliography given by Kolchin in [3].

I gratefully acknowledge the aid of the Office of Ordnance Research. Work on this book was done in part with the support of a contract with that agency.

CHAPTER I

GENERALITIES CONCERNING DIFFERENTIAL RINGS

1. DERIVATIONS. — A derivation of a ring A is an additive mapping $a \to a'$ of A into itself satisfying

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

We write a'', a''', ..., $a^{(n)}$ for the successive derivatives. By induction one proves Leibnitz's rule:

$$(ab)^{(n)} = a^{(n)}b + \cdots + {}_nC_i a^{(n-i)} b^{(i)} + \cdots + ab^{(n)}.$$

If a' commutes with a, we have $(a^n)' = na^{n-1}a'$. If A has a unit element, its derivative is necessarily O. If a is regular (has a twosided inverse a^{-1}) we find by differentiating $aa^{-1} = 1$ that

$$(a^{-1})' = -a^{-1}a'a^{-1}.$$

Theorem 1.1. — *A derivation of an integral domain has a unique extension to the quotient field.*

Proof. The uniqueness is clear. In order to extend the derivation to the quotient field we define

$$\left(\frac{a}{b}\right)' = \frac{ba' - ab'}{b^2}.$$

We verify that this rule gives the same result for ac/bc, and so is a valid definition. To check additivity of the proposed derivation, we bring a/b and c/d to the common denominator bd, and then we use the linearity in a of the definition of $(a/b)'$. The proof of the product law involves a slightly longer computation.

2. DIFFERENTIAL RINGS. — A differential ring is a commutative ring with unit together with a distinguished derivation.

Examples. — 1. Any commutative ring with unit may be converted

into a differential ring by imposing the trivial derivation (the derivation sending everything into 0). In this way we may say that ordinary ring theory is covered as a special case of differential ring theory.

Note that on the ring of integers or the field of rational numbers the only possible derivation is the trivial one.

2. The ring of all infinitely differentiable functions on the real line, with the customary derivative. (Note that one must take infinitely differentiable functions in order to have a system closed under differentiation).

3. The ring of entire functions, with the usual derivative. Note that, unlike the preceding example, there are no divisors of 0, and hence there is a quotient field (the field of meromorphic functions). More generally, we may take the functions analytic in a domain of the complex plane.

4. Let A be any differential ring. We use the customary notation $A[x]$ for the ring of all polynomials, with coefficients in A, in an (ordinary) indeterminate. If A is a field, $A(x)$ denotes the field of rational functions in x. The derivation in A may be extended to a derivation of $A[x]$ by assigning x' arbitrarily, defining $(x^n)' = nx^{n-1}x'$, and extending by linearity. We have similar freedom in making $A(x)$ into a differential field (see Theorem 1.1).

5. Again let A be any differential ring. This time we form the ring $A[x_i]$ of polynomials in an infinite number of ordinary indeterminates $x_0, x_1, x_2, \ldots$ A unique derivation of $A[x_i]$ is determined by assigning x_{i+1} as the derivative of x_i. Change notation so that

$$x_0 = x, \; x_n = x^{(n)}.$$

We call this procedure the adjunction of a *differential indeterminate*, and we use the notation $A\{x\}$ for the resulting differential ring. The elements of $A\{x\}$ are called *differential polynomials* in x (= ordinary polynomials in x and its derivatives).

Suppose that A is a differential field. Then $A\{x\}$ is a differential integral domain, and its derivation extends uniquely to the quotient field (Theorem 1.1). We write $A\langle x\rangle$ for this quotient field; its elements are *differential rational functions* of x (quotients of differential polynomials).

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.

In any differential ring A the elements with derivative 0 form a subring C, called the ring of *constants*. If A is a field, so is C. Note that C contains the subring generated by the unit element of A.

Let I be an ideal in a differential ring. A. We say that I is a *differential ideal* if $a \in I$ implies $a' \in I$, or more briefly, if $I' \subset I$. In the ring A/I we introduce a differential structure by defining the derivative of the coset $a + I$ to be $a' + I$; this is independent of the choice of representative in the coset, and actually defines a derivation in A/I.

Let A and B be differential rings. A *differential homomorphism* from A to B is a homomorphism (purely algebraically) which furthermore commutes with derivative. 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 self-explanatory.

Theorem 1.2. *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.*

The proof is straightforward and is omitted.

3. Radical ideals. — As in ordinary commutative ring theory we define an ideal I to be a *radical ideal* if $a^n \in I$ implies $a \in I$.

Lemma 1.3. — *If* ab *lies in a radical differential ideal* I, *then* $ab' \in I$ *and* $a'b \in I$.

Proof. — We have $(ab)' = a'b + ab' \in I$. Multiplying by ab' we obtain $(ab')^2 \in I$ and hence $ab' \in I$.

Lemma 1.4. — *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. — T is an ideal by ordinary ring theory, and a differential ideal by Lemma 1.3. Suppose finally that $x^n \in T$. Then for any s in S we have $x^n s^n \in I$. Since I is a radical ideal, $xs \in I$, $x \in T$.

In any commutative ring the intersection of any collection of radical ideals is again a radical ideal. In a differential ring the intersection of any set of differential ideals is a differential ideal; hence the intersection of any set of radical differential ideals is a radical differential ideal. Therefore: for any set S in a differential ring there is a unique smallest radical differential ideal containing S; we write it $\{S\}$. (This is to be carefully distinguished from the use of braces for differential ring adjunction.)

Lemma 1.5. — *Let a be any element and* S *any subset of a differential ring. Then* $a\{S\} \subset \{aS\}$.

Proof. The set of all x with $ax \in \{aS\}$ is, by Lemma 1.4, a radical differential ideal. It contains S and hence contains $\{S\}$.

Lemma 1.6. — *Let* S *and* T *be any subsets of a differential ring. Then* $\{S\}\{T\} \subset \{ST\}$.

Proof. The set of all x with $x\{T\} \subset \{ST\}$ contains S by Lemma 1.5, is a radical differential ideal by Lemma 1.4, and hence contains $\{S\}$.

4. Ritt algebras. — The radical of an ideal is defined to be the set of all elements with some power in the ideal; it is a radical ideal. For the purposes of differential ring theory we need to supplement this with the result that the radical of a differential ideal is a differential ideal. But this is not true without a suitable additional hypothesis.

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 a unit element. By setting $1' = 0, x' = 1$ we define a derivation of A. The radical of the zero ideal is generated by x, and is not 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, infinite-dimensional in general.

Lemma 1.7. — *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. We have $(a^n)' = na^{n-1}a' \in I$. Since I admits multiplication by $1/n$, $a^{n-1}a' \in I$. This is the case $k = 1$ of the statement $a^{n-k}(a')^{2k-1} \in I$ which we assume by induction. Differentiate:

$$(n-k)a^{n-k-1}(a')^{2k-1} + (2k-1)a^{n-k}(a')^{2k-2}a'' \in 1.$$

After multiplying by a' we see that the second term lies in I. We can cancel the factor $n - k$ in the first term and we find $a^{n-k-1}(a')^{2k-1} \in I$, which is the case $k + 1$ of the statement we are proving inductively. Finally we arrive at $k = n$, which gives us $(a')^{2n-1} \in I$.

Lemma 1.8. — *In a Ritt algebra the radical of a differential ideal is a differential ideal.*

This is an immediate consequence of Lemma 1.7.

CHAPTER II

EXTENSION OF ISOMORPHISMS

5. KRULL'S THEOREM. — It is a standard theorem of ordinary commutative ring theory that any radical ideal is an intersection of prime ideals. It is a fact that the word « differential » can be inserted in both the hypothesis and conclusion of this theorem. The technique of the proof rests on the following lemma.

Lemma. — *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 on the contrary that $ab \in Q$, $a \notin Q$, $b \notin Q$. Then $\{Q, a\}$ and $\{Q, b\}$ are radical differential ideals properly larger than Q; hence they contain elements of T, say t_1 and t_2. We have

$$t_1 t_2 \in \{Q, a\}\{Q, b\} \subset Q$$

by Lemma 1.6, a contradiction.

Theorem 2.1. — *Let* I *be a radical differential ideal in a differential ring* A. *Then* I *is an intersection of prime differential ideals.*

Proof. — Given an element x not in I, we have to produce a prime differential ideal containing I but not containing x. Take T to be the set of powers of x; by Zorn's lemma, select a radical differential ideal Q containing I and maximal with respect to the exclusion of T. The lemma asserts that Q is prime.

6. EXTENSION OF PRIME IDEALS. — We now contemplate the following situation: A is a differential ring contained in B (which includes the tacit assumption that they have the same unit element), P is a prime differential ideal in A, and I is a radical differential ideal in B which contracts to P (thats is, $I \cap A = P$). We ask two questions:

(1) Can I be enlarged to a prime differential ideal which also contracts to P?

(2) Is I even the intersection of prime differential ideals contracting to P ?

The answer to the first question is an easy unconditional affirmative.

Theorem 2.2. — *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. — T is taken to be the complement of P in A and the lemma is applied.

To answer the second question affirmatively requires the additional hypothesis that $ab \in I$, $a \in A$, $b \in B$ implies a or b in I. The hypothesis is inescapable since any ideal I satisfying the conclusion of the theorem has this property.

Theorem 2.3. — *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 or b is 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. — Let x be an element in B but not in I. We must construct a prime differential ideal in B which contains I, contracts to P, and fails to contain x. Take T to be the set of all elements ax^n where a is in A but not in P. Then T is multiplicatively closed, and it follows from our hypothesis that it is disjoint from I. The lemma then provides us with a prime differential ideal Q which contains I and is disjoint from T. The element x is not in Q, since $x \in T$. Finally, to see that $Q \cap A = P$, let $a \in Q \cap A$. Then $ax \in Q$, and this is a contradiction unless $a \in P$. (I am indebted to Robert Macrae for this brief proof of Theorem 2.3.)

7. A LEMMA ON POLYNOMIAL RINGS. — For convenience we separate out in this section an elementary (non-differential) lemma.

Lemma 2.4. — *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 is in* P *or b is 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 which is in* L *but not in* K. *Then* $y - s$ *is not in* I.

Proof. — We look at L for the moment as merely a vector space over

K, and select a vector space basis u_α, α ranging over an index set. We write u_1, u_2 for two typical basis elements (although there is no suggestion that the index set is countable and of course no need to well order it). In particular we choose $u_1 = 1$. Every element of B has a unique expression $\Sigma a_\alpha u_\alpha$ where a_α is in A; and such an element lies in A only in case all coefficients except a_1 vanish. Now J evidently consists exactly of all elements $\Sigma p_\alpha u_\alpha$, $p_\alpha \in P$. It follows (for arbitrary P) that $J \cap A = P$.

a) We assume that P is a radical ideal and that b lies in $I \cap A$. Then a suitable power b^n lies in $J \cap A = P$. Since P is a radical ideal, $b \in P$. Thus $I \cap A = P$.

b) Suppose further that P is prime and that $ab \in I$, $a \in A$, $b \in B$. Then $a^n b^n \in J$. Say $b^n = \Sigma a_\alpha u_\alpha$. We find $\Sigma(a^n a_\alpha)u_\alpha \in J$, whence each $a^n a_\alpha \in P$. Either $a \in P$, or else every $a_\alpha \in P$, in which case $b^n \in J$, $b \in I$.

c) We shall assume that $y - s$ does lie in I and reach a contradiction. Some power $(y - s)^m$ lies in J. Let I_o denote the set of all polynomials in y (coefficients in L) which lie in J. I_o is a principal ideal whose generator divides $(y - s)^m$. This generator cannot be a constant (i.e. a non-zero element of L) for then J would be all of B, and $P = J \cap A$ would be all of A, contradicting our hypothesis. Thus the generator is of the form $(y - s)^r$ with $r \geq 1$. We now invoke again the vector space basis u_α, taking $u_1 = 1$, $u_2 = s$. When $(y - s)^r$ is expressed as a linear combination of the u's, each separate coefficient must be in P and hence in J. In particular this is true for the coefficient of u_1, a polynomial beginning with y^r and then having no term in y^{r-1}. This polynomial must coincide with $(y - s)^r = y^r - rsy^{r-1} \ldots$ Because of characteristic 0, this is impossible.

Remark. — Part (*c*) can be sharpened to the statement that (for characteristic 0) J is a radical ideal whenever P is. We shall not need this refined result for our later purposes.

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.

Admissible isomorphisms are going to play the role of temporary substitutes for automorphisms; that is, in suitable contexts we shall be able to prove that admissible isomorphisms are indeed automorphisms. Classical Galois theory can be developed in this way: if N is a finite-dimensional separable extension of K, then N is normal over K if and only if every admissible isomorphism of N, leaving K elementwise fixed, is an automorphism. In the usual modern treatment of Galois

theory, admissible isomorphisms are not mentioned; but they seem to be indispensable for differential Galois theory.

We shall now prove two basic theorems concerning the extension and existence of admissible isomorphisms. The reader may find it instructive to compare these theorems with their (much easier) analogues in ordinary field theory.

Theorem 2.5. — *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.

Proof. — By transfinite induction we reduce the problem to the following: given an element u in M but not in K, we seek to define an extension ot the isomorphism S to u, the image of u lying in a suitable extension of M. Let $K\{u\}$ be the differential integral domain obtained by adjoining u to 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 homomosphism from $K\{y\}$ onto $K\{u\}$ defined by sending y into u; P_1 is a prime differential ideal in $K\{y\}$. (P_1 is the differential substitute for the irreducible polynomial for u, which would be used at this point in ordinary field theory). Via the isomorphism S we transfer P_1 to a prime differential ideal P in $L\{y\}$. Let J be the ideal in $M\{y\}$ generated by P. Since J consists of all finite sums $\Sigma p_i m_i$ with $p_i \in P$, $m_i \in M\{y\}$, it is plain that J is a differential ideal. Let I be the radical of J. By Lemma1.8, I is a (radical) differential ideal in $M\{y\}$. By part (a) of Lemma 2.4, $I \cap L\{y\} = P$. (The K and L of Lemma 2.4 are to be replaced by L and M. Note that, from the point of view of ordinary algebra, $M\{y\}$ is obtained by adjoining a countable number of ordinary indeterminates to M). By Theorem 2.2, I can be enlarged to a prime differential ideal Q in $M\{y\}$ satisfying $Q \cap L\{y\} = P$.

Write v for the image of y in the natural homomorphism from $M\{y\}$ onto $M\{y\}/Q$. Next we define a differential homomorphism from $K\{y\}$ onto $L\{y\}$ in two steps: $K\{y\}$ to $L\{y\}$ via S, then $L\{y\}$ to $L\{y\}$ by sending y into v. The kernel of the second mapping is $Q \cap L\{y\} = P$. Hence the kernel of the product mapping is P_1. Thus we get a differential isomorphism between the differential integral domains $K\{u\}$ and $L\{v\}$, extending S. By Theorem 1.1, the isomorphism extends uniquely to a differential isomorphism between the quotient fields. This concludes the prof of Theorem 2.5.

Theorem 2.6. — *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. — The fundamental procedure is the same as that used in proving Theorem 2.5. For a differential indeterminate y, we let P be the kernel of the homomorphism from $K\{y\}$ onto $K\{s\}$. Of course, $P \neq K\{y\}$, for $s \neq 0$. Let J be the ideal in $L\{y\}$ generated by P, where $L = K<s>$. Let I be the radical of J. Then I is a radical differential ideal in $L\{y\}$ which contracts in $K\{y\}$ to P. Suppose that I has been expanded to a prime differential ideal Q in $L\{y\}$ which also contracts in $K\{y\}$ to P. Write t for the image of y in the homomorphism of $L\{y\}$ onto $L\{y\}/Q$. Then we can build an admissible differential isomorphism of $K<s>$ onto $K<t>$, sending s into t. When is t equal to s? Answer: only if $y - s \in Q$.

Now part (*b*) of Lemma 2.4 tells us that the hypotheses of Theorem 2.3 are fulfilled (with $K\{y\}$ and $L\{y\}$ playing the roles of A and B respectively). Consequently the intersection of Q's such as the above is I. If, therefore, we always find $y - s \in Q$, it would follow that $y - s$ is in I. But this contradicts part (*c*) of Lemma 2.4.

We have thus constructed a differential isomorphism of $K<s>$ into $L<t>$ which moves s. By Theorem 2.5 we may extend this to an admissible differential isomorphism defined on all of L.

CHAPTER III

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 (in other words, 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; H′ is automatically a differential field lying between K and M. We have (obviously) $L'' \supset L$, $L_1 \supset L_2$ implies $L_1' \subset L_2'$, and similar statements apply to subgroups. From just these facts one deduces $H''' = H'$, $L''' = L'$. Call a field or group *closed* if it is equal to its double prime. Then: *any primed object is closed, and priming sets up a one-one correspondence between closed subgroups and closed intermediate differential fields.* This of course leaves completely untouched the really important question: which subgroups or subfields are closed?

Classical Galois theory can be slightly sharpened by showing that the property of closure, of fields or of groups, is stable under « finite increases ». (From this discussion we shall actually use only the fact that the subgroup corresponding to a finite-dimensional extension is of finite index).

Lemma 3.1. — *Let* N *be a differential field with differential sub, field* K. *Let* L *and* M *be intermediate differential fields with* $M \supset L$. $[M:L] = n$. *Let* L′ *and* M′ *be the corresponding subgroups of the differential Galois group of N over* K. *Then: the index of* M′ *in* L′ *is at most n.*

Proof. — Since relative degrees of fields and relative indices of groups are both multiplicative, it is enough to prove the lemma for the

case of a simple extension. Say $M = L(u)$. Then the right cosets of L' mod M' correspond exactly to the possible images of u (in automorphisms keeping L fixed). There are at most n such images, namely the roots of the irreducible polynomial for u over L.

Lemma 3.2. — *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* $[J' : H'] \leqq n$.

Proof. — Suppose on the contrary that $u_1, \ldots, u_{n+1}$ are elements of J′ linearly independent over H′. Let $S_1, S_2, \ldots, S_n$ be any representatives of the right cosets of H mod J. We can suppose for convenience that $S_1 = I$. Form the equations

$$(*) \qquad \sum_{i=1}^{n+1} a_i(u_i S_j) = 0 \qquad (j = 1, \cdots, n).$$

Since these are n linear homogeneous equations in $n + 1$ variables, there exist non-trivial solutions in M. Among all such solutions pick one with a maximum number of zeros. Say this solution consists of the non-zero elements $a_1, \ldots, a_r$ followed by O's. We can suppose that $a_1 = 1$. It is not possible that all the a's lie in H′, for then the first of the equations (*) contradicts the linear independence of the u's. Suppose for definiteness that a_r is not in H′. Then some automorphism in H actually moves a_r; say this automorphism lies in the coset JS_k. It is harmless to make a change in the choice of a representative of the coset, for the u's are invariant under J. Thus we can suppose $a_r S_k \neq a_r$. Apply S_k to the equations (*) and then subtract. The result is a shorter solution of the equations, a contradiction.

By combining these two lemmas we obtain:

Lemma 3.3. — *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.*

Something can be said concerning the meaning of normality of subgroups even in this very general context.

Theorem 3.4. — *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 be a differential automorphism of M/K, $x \in H'$. We show that $xS \in H'$. For this we need $xST = xS$ for T in H, i.e., $xSTS^{-1} = x$. Since $STS^{-1} \in H$, this is true. We have thus shown that S sends H′ into itself. Since the same is true for S^{-1}, S actually sends H′ onto itself.

b) Proving that L′ is normal is the same computation as in (*a*), read backwards. There is a natural homomorphism of G into the differential Galois group of L/K, obtained by restricting the automorphisms to L. The kernel is L′, and the image consists of those differential automorphisms of L/K which can be extended to M.

One corollary of Theorem 3.4 is worth noting : the closure of a normal subgroup is normal.

We define M to be normal over K if any element in M but not in K can be actually moved by a differential automorphism of M/K; in the notation above, normality means that $K'' = K$ and that K is closed.

A subfield L that corresponds to a normal subgroup is normal over K, as one easily sees. The converse is not true. For later use we shall prove Lemma 3.6, a case where the converse holds because of additional hypotheses.

Lemma 3.5. — *Let* L *be a closed subfield,* H *the corresponding subgroup. Then the normalizer of* H (*the set of all* S *in* G *with* $SHS^{-1} = H$) *consists of all* S *in* G *that map* L *onto itself.*

The proof is by a computation like that in Theorem 3.4.

Lemma 3.6. — *Let* L *be a closed subfield of* M, L *normal over* K. *Let* H *be the subgroup corresponding to* L. *Assume that the normalizer* H_1 *of* H *is closed and that every differential automorphism of* L *over* K *can be extended to* M. *Then* H *is normal and moreover* G/H *is the full differential Galois group of* L *over* K.

Proof. — In order to prove H normal, we have to show that $H_1 = G$. If L_1 is the field corresponding to H_1 it is equivalent (since H_1 is closed) to prove $L_1 = K$. Now by Lemma 3.5, H_1 consists of just those S in G that map L onto itself. Among these we find all the differential automorphisms of L/K, for by hypothesis they can be extended to M. Since, further, L is assumed to be normal over K, it follows that no elements of L other than K are fixed under H_1. But this means that $L_1 = K$, as desired. The final statement of the lemma follows from the last portion of Theorem 3.4.

10. THE WRONSKIAN. — The *Wronskian* of n elements $y_1, y_2, \ldots y_n$ in a differential ring is defined as the determinant

$$\begin{vmatrix} y_1 & y_2 \cdots y_n \\ y_1' & y_2' \cdots y'_n \\ \vdots & \\ y_1^{(n-1)} & y_2^{(n-1)} \ldots y_n^{(n-1)} \end{vmatrix}$$

Theorem 3.7. — *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. Suppose $y_1, \ldots, y_n$ are linearly dependent over C, $\Sigma c_i y_i = 0$. On differentiating this equation $n - 1$ times we get n linear homogeneous equations for $c_1, \ldots, c_n$. Since the c's are not all 0, the determinant must vanish.

Conversely suppose the Wronskian of $y_1, \ldots, y_n$ vanishes. Then we can find in F a non-trivial solution $c_1, \ldots, c_n$ of the equations $\Sigma c_i y_i^{(j)} = 0$, $j = 0, \ldots, n - 1$. We may assume that $c_1 = 1$ and that the Wronskian of $y_2, \ldots, y_n$ does not vanish. Differentiating the first $n - 1$ of our equations and then cancelling the appropriate original equations, we arrive at $n - 1$ linear homogeneous equations in $c_2', \ldots, c_n'$ with determinant the Wronskian of $y_2, \ldots, y_n$. Hence $c_2' = \ldots = c_n' = 0$, and the $c's$ are constants.

Because of Theorem 3.1 we shall be able to use the phrase « linearly dependent over constants » unambiguously; it does not matter which differential field we think we are in, for the vanishing of the Wronskian is independent of the choice of field.

11. PICARD-VESSIOT EXTENSIONS. — Consider a linear homogeneous differential equation

$$(*) \qquad L(y) = y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0$$

with coefficients in a differential field K. Let $u_1, \ldots, u_{n+1}$ be solutions of the equation in a certain (possibly) larger differential field. We claim that $u_1, \ldots, u_{n+1}$ are linearly dependent over constants; for the equations $L(u_i) = 0$ show that the final row of the Wronskian of $u_1, \ldots, u_{n+1}$ is a linear combination of the preceding rows.

Definition. — Let (*) 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 (*)] if,

(1) $M = K < u_1, \ldots, u_n >$ where $u_1, \ldots, u_n$ are n solutions of (*) linearly independent over constants,

(2) M has the same field of constants as K.

If K is of characteristic O and has an algebraically closed field of constants, the basic existence question has an affirmative answer : there exists a Picard-Vessiot extension for any linear homogeneous differential equation over K. The difficult part of the proof is to maintain the field of constants — see [4]. The same ideas can be exploited to prove the uniqueness (up to differential isomorphism) of a Picard-Vessiot extension for a given equation (communication to the author from Kolchin).

Examples of Picard-Vessiot extensions. — 1. Two simple types (the adjunction of an integral and the adjunction of an exponential of an integral) are discussed in the next section.

2. If K is the field of all functions meromorphic in a domain of the complex plane, classical existence theorems reveal that a Picard-Vessiot extension exists corresponding to any linear homogeneous differential equation over K.

3. If we are free to select both the top and bottom fields, we can easily exhibit a Picard-Vessiot extension whose differential Galois group is the full linear group. Let K_o be any differential field. Let $M = K_o < x_1, \ldots, x_n >$ be the field obtained by adjoining n differential indeterminates to K_o. Let T be any non-singular linear transformations on the $x's$ with coefficients in the constant field C of K_o :

$$x_i T = \Sigma c_{ij} x_j, \qquad c_{ij} \in C.$$

We define T on all of M by agreeing that for any derivative

$$x_i^{(m)} T = \Sigma c_{ij} x_j^{(m)}.$$

Then T is a differential automorphism of M. Let K be the fixed field of M under all the T's. Define

$$L(y) = W(y, x_1, \cdots, x_n)/W(x_1, \cdots, x_n)$$

where W denotes the Wronskian. Then L $(y) = 0$ is a linear homogeneous differential equation in y with coefficients in K; $x_1, \ldots, x_n$ are linearly independent solutions; M is a Picard-Vessiot extension of K for the equation L $(y) = 0$; and the differential Galois group is the full linear group.

When the Galois theory is completed in Chapter v, we shall be able to amplify this example: by taking M over a suitable intermediate differential field we exhibit any algebraic matrix group as a Galois group.

Let M be a Picard-Vessiot extension of K, and S a differential automorphism of M over K. Then $u_i S$ is necessarily a linear combination

of the $u's$ with coefficients in the constant field C: $u_i S = \Sigma c_{ij} u_j$. The matrix c_{ij} is non-singular since the inverse automorphism gives rise to the inverse matrix. Thus the differential Galois group is isomorphic to a multiplicative group of non-singular matrices over C. The discovery of which matrix groups are eligible is one of the main questions on the agenda.

Lemma 3.8. — *Let* K $\subset$ L $\subset$ M *be differential fields. Suppose that* 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.*

The proof is immediate.

12. Two special cases. — We proceed to study two important types of building blocks for larger extensions. The first is the process of adjoining an integral. Naturally, we do this only for elements not yet possessing an integral; otherwise we would merely be adjoining a new constant.

Lemma 3.9. — *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 $< u >$ *is a Picard-Vessiot extension of* K, *and its differential Galois group is isomorphic to the additive group of constants in* K.

Proof. — If u satisfies a polynomial equation over K, take the irreducible equation, say

$$u^n + bu^{n-1} + \cdots = 0.$$

Differentiating, we get

$$nu^{n-1}a + b'u^{n-1} + \cdots = 0.$$

Hence $na = -b'$ and a is the derivative of $-b/n$ in K, a contradiction.

Next we show that K $< u >$ contains no new constants. First suppose that a polynomial $b_1u^n + b_2u^{n-1} + \ldots$ is a constant. On differentiating we find

$$b_1'u^n + (nb_1a + b_2')u^{n-1} + \cdots = 0.$$

Hence $b_1' = nb_1a + b_2' = 0$, a is the derivative of $-b_2/nb_1$. Suppose that the rational function $f(u)/g(u)$ is a constant, where this fraction is in lowest terms, g actually contains u, and its leading cefficient is 1. We find that $f/g = f'/g'$, where g' is a non-zero polynomial of lower degree than g. This contradicts our assumption that f/g is in lowest terms.

We observe that 1 and u are solutions of $y'' - (a'/a)y = 0$, linearly independent over constants. Hence $K < u >$ is a Picard-Vessiot extension of K.

In a differential automorphism of $K < u >$ over K, u must go into another element with derivative a. That is, u must be sent into $u + c$ with c in the constant field C. The mapping $u \to u + c$ induces an automorphism of $K < u >$ over K, at least in the purely algebraic sense. We verify directly that it is a differential automorphism of $K < u >$, and it is enough to do this on a polynomial $\Sigma\lambda_i u^i$. The latter is sent into $\Sigma\lambda_i (u + c)^i$ with derivative

$$\Sigma[i\lambda_i(u + c)^{i-1}a + \lambda'(u + c)^i].$$

But this is the image of the derivative $\Sigma(i\lambda_i u_i^{i-1}a + \lambda_i' u^i)$.

The second type of extension we refer to as the adjunction of the *exponential of an integral.* We prove a somewhat weaker result.

Lemma 3.10. — *Let* K *be a differential field, u an element satisfying the equation $y' - ay = 0$, $a \in K$. Suppose that* $K < u >$ *has the same field of constants as* K. *Then* $K < u >$ *is a Picard-Vessiot extension of* K, *and its differential Galois group is isomorphic to a subgroup of the multiplicative group of non-zero constants in* K.

Proof. — It is evident from the definition that $K < u >$ is a Picard-Vessiot extension of K. If v is any other solution of $y' - ay = 0$ we find $(v/u)' = 0$, *so* $v = cu$ with c a constant. Thus every differential automorphism 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 $K = K_1 \subset K_2 \subset \ldots \subset K_n = M$ such that each K_{i+1} is an extension of K_i by an integral or an exponential of an integral.

Theorem 3.11. — *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. — It follows from Lemmas 3.9, 3.10, and 3.8 that every differential automorphism of M over K automatically sends K_2 onto itself. Let G_2 be the subgroup of G corresponding to K_2 in the Galois correspondence. By Theorem 3.4, H_2 is a normal subgroup of G. Since G/H_2 is a subgroup of the differential Galois group of K_2/K (Theorem 3.4), and the latter is abelian, G/H_2 is abelian. In this way we see that G is solvable.

This result has two defects. First, it is desirable to prove a theorem of this kind for fields which are *embedded* in a Liouville extension.

Second, we ought to allow algebraic extensions as a further type of building block. It will require a lot more theory to cover these two objections.

14. TRIANGULAR AUTOMORPHISMS. — Theorem 3.12 is a preliminary step toward a converse of Theorem 3.11. We insert it at this point to emphasize that its proof does not require any of the deeper theory yet to be developed.

Theorem 3.12. — *Let the differential field* M *be normal over its differential subfield* K. *Suppose that* $u_1, \ldots u_n \in \mathrm{M}$ *are elements such that for every differential automorphism* σ *of* M *we have*

$$(*) \qquad u_i\sigma = a_{ii}u_i + a_{i,i+1}u_{i+1} + \cdots + a_{in}u_n \ (i = 1, \cdots, n)$$

with the a's constants in M (*depending on* σ). *Then* $\mathrm{K} < u_1, \ldots, u_n >$ *is a Liouville extension of* K.

Proof. — The last of the equations (*) reads $u_n\sigma = a_{nn}u_n$. Differentiating and dividing, we find that u_n'/u_n is invariant under σ (we can suppose $u_n \neq 0$ for otherwise u_n could simply be suppressed). By the normality of M over K, $u_n'/u_n \in \mathrm{K}$. Hence the adjunction of u_n to K is the adjunction of an exponential of an integral. Next divide each of the $n - 1$ preceding equations by the equation $u_n\sigma = a_{nn}u_n$, and differentiate. The result is

$$\left(\frac{u_i}{u_n}\right)'\sigma = \frac{a_{ii}}{a_{nn}}\left(\frac{u_i}{u_n}\right)' + \cdots + \frac{a_{i,n-1}}{a_{nn}}\left(\frac{u_{n-1}}{u_n}\right)'.$$

This is a set of equations of the same form in the elements $(u_i/u_n)'$ $(i = 1, \ldots, n - 1)$. By induction on n, the adjunction of $(u_i/u_n)'$ to K yields a Liouville extension. Then adjoining u_i/u_n themselves means adjoining integrals.

CHAPTER IV

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, i.e., the set of all n-ples with elements in F. Let $F[x_1, \ldots, x_n]$ be the polynomial ring in n indeterminates over F. By an *algebraic manifold* in V we mean the set of all zeros of a collection of polynomials in $F[x_1, x_2, \ldots, x_n]$. It is equivalent to say that an algebraic manifold is the set of zeros of an ideal in $F[x_1, \ldots, x_n]$. By the Hilbert basis theorem the ideals in $F[x_1 \ldots, x_n]$ satisfy the ascending chain condition. Hence the algebraic manifolds in V satisfy the descending chain condition.

One knows that the union of a finite number or the intersection of any number of algebraic manifolds is again an algebraic manifold. We are therefore able to use the algebraic manifolds as closed sets to define a T_1-topology on V, called the *Zariski topology.*

With this as motivation, we define a *Z-space* to be a T_1-space satisfying the descending chain condition on closed sets (or équivalently, the ascending chain condition on open sets).

Lemma 4.1. — *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.*

The first two parts of the lemma are immediate, while the third is a consequence of the known fact that an infinite Hausdorff space has an infinite number of disjoint open sets.

Lemma 4.2. — *A Z-space is the union of a finite number of disjoint open and closed connected subsets.*

Proof. — Let the Z-space be X. If X is not connected, it is the union of two disjoint open and closed sets. If either of these two

sets is disconnected, 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 connected component of X. In the complement of this we extract a second open and closed component, etc. The ascending chain condition on open sets causes this procedure also to terminate in a finite number of steps.

16. T_1-GROUPS AND Z-GROUPS. — The group G of all non-singular n by n matrices over a field F is a subset of n^2-dimensional space and, as such, carries the Zariski topology. The next lemma tells us that in this « topological group » multiplication is separately continuous in its variables, and that the inverse is continuous. Multiplication is not however jointly continuous in its variables (unless F is finite); for one knows that joint continuity would make G Hausdorff, and even completely regular. But Lemma 4.1 (*c*) says that a Hausdorff Z-space is finite.

The group $G \times G$ is a subset of $2n^2$-dimensional space and thus admits the Zariski topology induced by that space, a topology which is stronger than the Cartesian product of the individual Zariski topologies. Multiplication in G would indeed be jointly continuous if we used the Zariski product topology instead of the Cartesian product topology; but this would not fit our program of studying G as much as possible in the spirit of abstract topological groups.

Lemma 4.3. — *Let* V *and* W *be m-dimensional and n-dimensional spaces over* F, *taken in the Zariski topology. Let* $r_1, \ldots, r_n$ *be rational functions in m variables* $x_1, \ldots, x_m$. *Let* S *be the set where the denominators of* $r_1, \ldots, r_m$ *vanish, and let* T *be the complement of* S *in* V. *Then the mapping from* T *to* W, *defined by* $(x_1, \ldots, x_m) \to (y_1, \ldots, y_n)$ *with* $y_i = r_i(x_1, \ldots, x_m)$, *is continuous.*

Proof. — We have to show that the inverse image of a closed set is a closed set. A closed set in W consists of the zeros of a set of polynomials $g_j(y_1, \ldots, y_n)$. The inverse image consists of all zeros in T of the rational functions $g_j(r_1, \ldots, r_m)$, which is the same as the zeros of their numerators. This is a closed set in the Zariski topology for T.

The example of matrix groups under the Zariski topology motivates the next definition.

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 homeo-

morphisms of G onto itself. A Z-group is a T_1-group whose space is a Z-space.

The theory of the component of the identity works in any T_1-group.

Lemma 4.4. — *The component of the identity in a* T_1*-group is a closed normal subgroup.*

Proof. Let C be the component of the identity in the T_1-group G. C^{-1} is connected (being the continuous image of a connected set) and contains 1; hence $C^{-1} \subset C$. For $c \in C$ we have that $c\,C$ is connected and shares the element c with C; hence $c\,C \subset C$. Thus C is a subgroup. Since for any x in G, $x^{-1}Cx$ is connected and contains 1, $x^{-1}C\,x \subset C$ and C is normal.

Putting together Lemmas 4.2 and 4.4 we obtain :

Lemma 4.5. — *The component of the identity in a Z-group is a closed normal subgroup of finite index.*

17. C-GROUPS. — In a T_1-group, or even a Z-group, it may not be true that the center is closed. Further: the closure of an abelian subgroup need not be abelian. Most alarming for our immediate purposes is the fact that the commutator subgroup of a connected group need not be connected. Here is a method for constructing appropriate examples. Let G be an arbitrary group. Topologize G by declaring that the only closed sets are the finite ones and all of G. (Since this is the weakest possible T_1-topology on G, it is often referred to as the minimal T_1-topology). Then G is a Z-group. To get an example where, for instance, the center is not closed, we merely have to arrange that the center of G is infinite but not all of G (examples of such groups abound).

To get the results we require, we need not go all the way to a topological group. A weaker axiom will suffice.

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

Matrices under the Zariski topology form a C-group. For let X be a fixed matrix. The entries of the matrix $A^{-1}X\,A$ are rational functions of the entries in the matrix A. By Lemma 4.3 the mapping $A \to A^{-1}XA$ is continuous. More generally the mapping sending A into any « word » in A and other fixed matrices in continuous, but we shall not make use of any word except $A^{-1}XA$.

Lemma 4.6. — *Let* G *be a* C*-group whose component of the identity has finite index k. Then any finite conjugate class of* G *has at most k elements.*

Proof. — Suppose on the contrary that there exists an element x

with a finite conjugate class, the number of elements in the class exceeding k. The mapping $a \to a^{-1}xa$ is continuous. The inverse image of each conjugate is open and closed. This yields a decomposition of G into more than k open and closed sets, a contradiction.

For later use, we note a special case of Lemma 4.6:

Lemma 4.7. — *In a connected* C*-group any non-central element has an infinite conjugate class.*

Theorem 4.8. — *If* G *is a connected* C*-group, the commutator subgroup* G′ *is again connected.*

Proof. — Write D_k for the set of all productes of k commutators in G. Then $D_1 \subset D_2 \subset \ldots$ and the union of all the D's is G′. It will suffice for us to prove that each D_k is connected. Consider the mapping

$$a_1 \to a_1^{-1}b_1^{-1}a_1b_1a_2^{-1}b_2^{-1}a_2b_2 \cdots a_k^{-1}b_k^{-1}a_kb_k,$$

all elements other than a_1 being held fixed. The mapping is continuous and hence the image is connected. The image has a point in common with D_{k-1}, obtained when $a_1 = b_1$. Now let a_1 vary over G. As a result we express D_k as a union of connected sets, each having a point in common with the (connected by induction) set D_{k-1}. Hence D_k is connected.

We insert at this point two further results, to be used in Chapter v.

Lemma 4.9. — *Let* G *be a* C*-group,* H *a closed subgroup of* G. *Suppose that either* (1) H *is of finite index in* G, *or* (2) H *is normal and* G/H *abelian. Suppose further that the component of the identity in* H *is solvable. Then the component of the identity in* G *is solvable.*

Proof. — In case (1) the two components of the identity coincide.

Case (2). — Write K, K_1 for the components of the identity in G and H respectively. Write G′, K′ for the commutator subgroups of G and K respectively. Then H contains G′ and therefore K′. By Theorem 4.8, K′ is connected. Hence $K' \subset K_1$. By hypothesis K_1 is solvable, whence K′ is solvable and K is solvable.

Lemma 4.10. — *In a* C*-group the normalizer of a closed subgroup is closed.*

Proof. — Let S be the closed subgroup. For fixed s in S, consider the mapping $a \to a\,s\,a^{-1}$. The inverse image of S is closed and consists of all a with $a\,s\,a^{-1} \in S$. Take the intersection of these closed sets for all s in S; we see that the set of a with $a\,S\,a^{-1} \subset S$ is closed. Likewise the set of a with $a^{-1}Sa \subset S$ is closed. The intersection of these two closed sets is the normalizer of S.

18. SOLVABLE CONNECTED MATRIX GROUPS. — We proceed to prove a theorem wich plays a key role in the Picard-Vessiot theory.

Theorem 4.11. — *Let* G *be a solvable multiplicative group of non-singular matrices over an algebraically closed field. Suppose that* G *is connected in the Zariski topology. Then* G *can be put in simultaneous triangular form.*

Remarks. — 1. Lie's theorem in the theory of Lie groups says the same thing except that the field is the field of complex numbers, and connectedness is taken in the ordinary Euclidean topology. But the Zariski topology is weaker than the Euclidean topology, so that Euclidean connectedness implies Zariski connectedness. Thus Theorem 4.11 is stronger than Lie's theorem and extends it to any algebraically closed field.

2. Sometimes people mean by Lie's theorem the infinitesimal analogue : a solvable Lie algebra of matrices over an algebraically closed field admits simultaneous triangular form. This theorem is true for characteristic 0 but false for characteristic p. We have here an illuminating example of how groups sometimes behave better than Lie algebras.

3. If G is a commutative set (not necessarily a group) of matrices over an algebraically closed field it is a standard theorem that G can be put into simultaneous triangular form; connectedness is irrelevant. At the appropriate moment in the proof of Theorem 4.11 we shall use this fact.

4. However, connectedness cannot be dropped from the hypothesis of Theorem 4.11. For instance, any finite solvable group can be faithfully represented by unitary matrices, and a set of unitary matrices admits simultaneous triangular form only if it is commutative.

5. The appearance of the word « connected » in Theorem 4.11 is a blemish, in view of the highly algebraic nature of the subject. It is worth noting that we can state a purely algebraic corollary : *any* solvable multiplicative group of matrices over an algebraically closed field has a normal subgroup of finite index which admits simultaneous triangular form. If we wish to drop the hypothesis of algebraic closure, we can salvage the following fact : if G is a solvable group of matrices over any field, then G has a normal subgroup of finite index whose commutator subgroup is nilpotent.

Proof of Theorem 4.11. — We divide the proof into six steps.

(1) Suppose that G is reducible, i.e. that the vector space (say V) admits a non-trivial invariant subspace W. Take a basis of W and

expand it to a basis of V. Relative to this basis the matrices A_i of G take the form

$$A_i = \begin{pmatrix} B_i & O \\ * & C_i \end{pmatrix}$$

The mapping $A_i \to B_i$ is a homomorphism which, by Lemma 4.3, is continuous. Hence B_i is a connected solvable matrix group. By induction on the size of the matrices, B_i can be put in triangular form. A similar argument applies to C_i, and the result is that G reaches triangular form. Consequently we may assume that G is irreducible.

(2) By Theorem 4.8 the commutator subgroup G′ of G is connected. By an induction on the length of the derived series, we may assume that G′ is in triangular form.

(3) Let W be the subspace of V spanned by all joint characteristic vectors of G′. $W \neq O$ since the triangular form of G′ yields at least one joint characteristic vector. W is invariant under G. For let α be a joint characteristic vector of G′: $\alpha T = c(T)\alpha$ for $T \varepsilon G'$. Then for any S in G we have $STS^{-1} \varepsilon G'$, $\alpha STS^{-1} = c(STS^{-1})\alpha$, so that αST is a scalar multiple of αS and αS is a joint characteristic vector of G′. Since G is irreducible, W = V. This means that we can suppose that G′ is in diagonal form.

(4) Any element in G′ is now a diagonal matrix. Its conjugates in G are again in G′ and hence also diagonal. The only possible conjugates are thus obtained by permuting the characteristic roots. Hence each element of G′ has a finite conjugate class in G. By Lemma 4.7, G′ lies in the center of G.

(5) Suppose there is a matrix T in G′ which is not a scalar. Let c be a characteristic root of T, and define W to be the set of all α in V with $\alpha T = c\alpha$. Since T commutes with all of G we find that W is invariant under G. Hence W = V, T = cI. This contradiction proves that all the matrices of G′ are scalar.

(6) Since G′ is the commutator subgroup of G, its elements have determinant 1. Hence the entries down the diagonal must be n — th roots of 1. There are only a finite number of these, so that G′ is finite. But by Theorem 4.8, G′ is connected. Hence G′ = 1, G is commutative. But in the commutative case the theorem is known. This completes the proof of Theorem 4.11.

19. A SPECIAL RESULT. — For use in Chapter VI we insert at this point another result concerning solvable matrix groups.

Theorem 4.12. — *Let* G *be a group of* 2×2 *matrices with determinant* 1, *over an algebraically closed field. Assume that* G *is an algebraic*

group, i.e. *is closed in the Zariski topology, and that* K, *the component of the identity in* G, *is solvable. Then at least one of the following statements holds:*

(1) G *is finite,*

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

(3) G *can be put in simultaneous triangular form.*

Proof. — First we study 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 matrices for which a satisfies a certain polynomial equation. There are just two possibilities: either K is finite (whence G is finite) or K consists of all the above matrices. As in part (3) of the proof of Theorem 4.11, joint characteristic vectors of K are carried by G into joint characteristic vectors of K. Thus any element of G either leaves fixed or interchange the one-dimensional subspaces given by the two basis vectors. Hence the index of K in G is 1 or 2.

There remains the possibility that K does not admit diagonal form. By Theorem 4.11 it admits triangular form. Hence K must have just one characteristic vector. This must also be invariant under G, and so G admits triangular form.

CHAPTER V

THE GALOIS THEORY

20. THREE LEMMAS. — In this section we assemble for convenience three preliminary lemmas.

Lemma 5.1. — *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. Then: if the equations and inequality* $f_\alpha = 0$, $g \neq 0$ *have a solution in* D *they have a solution in* C.

Proof. — Take a vector space basis u_β of K over C. Each f_α has a unique expression $f_\alpha = \Sigma h_{\alpha\beta} u_\beta$, where $h_{\alpha\beta}$ is a polynomial with coefficients in C. The independence of the u's over constants survives in L. Therefore in a constant solution of $f_\alpha = 0$ we must have each $h_{\alpha\beta} = 0$. So the equations $h_{\alpha\beta} = 0$ have a solution in D. By the Hilbert Nullstellensatz they already have a solution in C.

We now show further that some solution fails to annul g. Write g in its expansion $\Sigma t_\gamma u_\gamma$. If every solution of $h_{\alpha\beta} = 0$ is also a solution of g (and hence a solution of each t_γ) we have, again by the Nullstellensatz, $t_\gamma^{r_\gamma} \in \mathrm{I}$, where r_γ is a suitable integer and I is the ideal generated by the h's. But then every solution of $f_\alpha = 0$ in D would annihilate g, a contradiction.

A similar argument leads to the next lemma.

Lemma 5.2. — *Let* K *be a differential field with constant field* C. *Let* $k_1, \ldots, k_r$ *be constants in some differential field extension of* K. *Then: if* $k_1, \ldots, k_r$ *are algebraically dependent over* K *they are algebraically dependent over* C.

Proof. — We have a polynomial relation $f(k_1, \ldots, k_r) = 0$ with coefficients in K. Again, let u_β be a basis of K over C, and write $f = \Sigma h_\beta u_\beta$.

Then $h_\beta(k_1, \ldots, k_r) = 0$, showing that the $k's$ are algebraically dependent over C.

Lemma 5.3. — *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* I. *Then the transcendence degree of* I/P *over* F *is strictly less than that of* I *over* F.

Proof. — Take any non-zero element u in P. It is impossible for u to be algebraic over F, for then the constant term in the equation for u would be in P, P would contain 1. So we may take u as the first element u_1 of a transcendence basis $u_1, \ldots, u_r$ of I. These elements map into 0, $v_2, \ldots, v_r$ in I/P. We claim that any element x in I/P is algebraically dependent on $v_2, \ldots, v_r$. Take y in I mapping on x. Then y satisfies a 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 coefficients polynomials in the $u's$, selected so that $f(x)$ is of minimal degree among polynomials lying in P. Mapping modulo P we get y to be dependent on the $v's$ unless all the $r's$ are in P. But then

$$(r_k x^{k-1} + r_{k-1} x^{k-2} + \cdots + r_1)x$$

lies in P, x does not, and we get a polynomial of lower degree in P.

21. Normality of Picard-Vessiot extensions. — Let $M = K < u_1, \ldots, u_n >$ be a Picard-Vessiot extension of K. Let σ be an admissible differential isomorphism of M over K; that is, σ is a differential isomorphism, leaving K elementwise fixed, of M onto another subfield of a given larger differential field N. Each $u_i\sigma$ is again a solution of the underlying differential equation and so must be of the form $\Sigma k_{ij}u_j$ with k_{ij} constants in N. Thus each σ gives rise to a non-singular matrix of constants. We now prove that the eligible matrices are determined by a set of polynomial equations.

Lemma 5.4. — *Let* K *be a differential field with constant field* C, $M = K < u_1, \ldots, u_n >$ *a Picard-Vessiot extension of* K. *There exists a set* S *of polynomials (in* n^2 *ordinary indeterminates) with coefficients in* C *such that:*

(1) *Every admissible differential isomorphism of* M *over* K *gives rise to a matrix of constants satisfying* S;

(2) *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* $\Sigma k_{ij}u_j$.

Proof. — Let $y_1, \ldots, y_n$ be differential indeterminates over K. Define a differential homomorphism of $K\{y_1, \ldots, y_n\}$ into M by keeping K fixed and sending y_i into u_i. The kernel Γ is a prime differential ideal in $K\{y_1, \ldots, y_n\}$.

Let $c_{ij}(i,j = 1, \ldots, n)$ be a set of n^2 ordinary indeterminates over M. Via the mapping $y_i \to \Sigma c_{ij}u_j$ we define a differential homomorphism of $K\{y_1, \ldots, y_n\}$ into $M[c_{ij}]$. Let Δ be the image of Γ in this mapping. Thus Δ is an ideal of (ordinary) polynomials with coefficients in the field M. Let w_α be a vector space basis of M over C. Write each polynomial in Δ as a linear combination of w's with coefficients polynomials over C. The collection S of all these polynomials over C is our candidate to fulfil the requirements of the lemma.

(1) Suppose that $u_i \to \Sigma k_{ij}u_j$ in an admissible differential isomorphism σ of M/K. Perform the homomorphism from $K\{y_1, \ldots, y_n\}$ into $K\{u_1, \ldots, u_n\}$ followed by σ. In the product homomorphism Γ gets sent into O. Again take the mapping given by $y_i \to \Sigma c_{ij}u_j$ followed by $c_{ij} \to k_{ij}$. The product is the same as before, and this time Γ goes into Δ evaluated at $c_{ij} = k_{ij}$. Hence all polynomials of Δ vanish at k_{ij}; after expression in terms of the basis w_α we see that the polynomials of S vanish at k_{ij}.

(2) Let us be given N and a non-singular matrix k_{ij} of constants in N satisfying S. We may define a homomorphism of $K\{y_1, \ldots, y_n\}$ into N by $y_i \to \Sigma k_{ij}u_j$ in the two steps $y_i \to \Sigma c_{ij}u_j$ and $c_{ij} \to k_{ij}$ The kernel contains Γ and so we get a homomorphism σ of $K\{u_1, \ldots, u_n\}$ onto $K\{u_1\sigma, \ldots, u_n\sigma\}$, $u_i\sigma = \Sigma k_{ij}u_j$. If we only knew that σ is one-one we could extend it to the quotient fields and the proof would be finished. Using Lemma 5,3 we shall argue that σ is one-one; assuming the contrary we have

$$(*) \qquad \partial K\langle u_1, \ldots, u_n\rangle/K > \partial K\langle u_1\sigma, \ldots, u_n\sigma\rangle/K$$

where ∂ denotes the transcendence degree (note that these transcendence degrees are finite since each u_i satisfies a differential equation). Let us abbreviate the notation by writing $K\langle u\rangle$ for $K\langle u_1, \ldots, u_n\rangle$ etc. From (*) we get, by the additivity of transcendence degrees

$$\partial K\langle u, u\sigma\rangle/K\langle u\rangle < \partial K\langle u, u\sigma\rangle/K\langle u\sigma\rangle.$$

We have

$$\begin{aligned}\partial K\langle u, u\sigma\rangle/K\langle u\rangle &= \partial K\langle u, k\rangle/K\langle u\rangle \\ &= \partial C(k)/C,\end{aligned}$$

the last step by Lemma 5.2. 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 $K\langle u\sigma\rangle$. Obviously $\partial C'(k)/C' \leqslant$

$\partial C(k)/C$ and we have a contradiction. This completes the proof of Lemma 5.4.

The main results of the Galois theory are now readily within our reach. The first is merely a special case of Lemma 5.4.

Theorem 5.5. — *The differential Galois group of a Picard-Vessiot extension is an algebraic matrix group over the field of constants.*

Lemma 5.6. — *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_α *and* y_α *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. — Let σ be the given differential isomorphism. Say

$$u_i\sigma = \Sigma k_{ij}u_j,$$

the k's being constants in the larger field. Consider any two elements x, y in M; each is a ratio of two differential polynomials in the u's, say $x = P(u)/Q(u)$, $y = R(u)/S(u)$. The condition that $y = x\sigma$ can be written

$$S(u)P(u\sigma) = R(u)Q(u\sigma).$$

Putting in $u_i\sigma = \Sigma k_{ij}u_j$, we get a polynomial equation in the k's with coefficients in M. We have one such equation for each α, saying that $x_\alpha\sigma = y_\alpha$. Combine these equations with the equations given by Lemma 5.4. Also we can combine the inequality given by

$$z\sigma \neq z \text{ with } |k_{ij}| \neq 0$$

into a single inequality. There is a constant solution in the larger field; hence, by Lemma 5.1 there is a constant solution in C. This gives us the differential automorphism we are seeking.

Theorem 5.7. — *Let* K *be a differential field of characteristic zero with an algebraically closed constant field. Then any Picard-Vessiot extension of* K *is normal.*

Proof. — We have to prove that for any z in M but not in K there exists a differential automorphism of M/K moving z. By Theorems 2.6 and 2.5 there exists an admissible differential isomorphism of M/K moving z. We then apply Lemma 5.6.

Theorem 5.8. — *Let* K *be a differential field of characteristic* O *with an algebraically closed constant field. Let* M *be a Picard-Vessiot extension of* K. *Then any differential isomorphism over* K *between two inter-*

mediate 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. — The given differential isomorphism is first extended to an admissible differential isomorphism defined on all of M, using Theorem 2.5. The theorem then follows from Lemma 5.6.

22. Completion of the Galois Theory. — Let us see where we stand. Let M be a Picard-Vessiot extension of K (characteristic 0, algebraically closed constant field). If L is any intermediate differential field, M is also a Picard-Vessiot extension of L. By Theorem 5.7, M is normal over L. In the language of the Galois theory of Chapter III all intermediate differential fields are closed.

Again, let H be a normal subgroup of the differential Galois group G, and let $L = H'$ be the corresponding differential field. Suppose that H is closed in the sense of Galois theory. By Theorem 5.8 all differential automorphisms of L/K are extendible to M. It follows from Theorem 3.4 that G/H is the full differential Galois group of L/K. Again (by Lemmas 3.6 and 4.10) if L is closed and normal over K, the corresponding subgroup is normal.

By Theorem 5.6, G is an algebraic matrix group, and so are all the subgroups corresponding to intermediate differential fields. Only one point remains to be settled : that the algebraic subgroups of G are Galois-closed.

The problem comes to this : given a subgroup H in G we must show that H is Zariski-dense in H''. If not, there exists a polynomial f (in n^2 variables, coefficients in C) which vanishes on H but not on H''. We now perform a construction which is adequately illustrated in the case $n = 2$. Say $M = K < u, v >$. The matrix

$$\begin{pmatrix} u & v \\ u' & v' \end{pmatrix}$$

is non-singular. Let

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

be its inverse. Let y and z be differential indeterminates over M. We define a differential polynomial F by

$$F(y,z) = f(Ay + By', Az + Bz', Cy + Dy', Cz + Dz').$$

In F we set $y = u\sigma$, $z = v\sigma$ where σ belongs to H. Since

$$\begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} u & v \\ u' & v' \end{pmatrix}\begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix}$$

where k_{ij} is the matrix for σ, we have

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} u\sigma & v\sigma \\ u'\sigma & v'\sigma \end{pmatrix} = \begin{pmatrix} k_{11} & k_{21} \\ k_{12} & k_{22} \end{pmatrix}.$$

Hence $F(u\sigma, v\sigma) = 0$ for σ in H but not for all σ in H″. Among all differential polynomials in $M\{y, z\}$ wi th this property, pick one, say E, with the smallest possible number of terms (when written out as a sum of monomials). We may assume that one of the coefficients of E is 1. For τ in H write E_τ for the polynomial obtained by replacing each coefficient by its image under τ. Then

$$E_\tau(u\sigma, v\sigma) = [E(u\sigma\tau^{-1}, v\sigma\tau^{-1})]\tau$$

which is 0 for every σ in H. The polynomial $E - E_\tau$ is shorter than E. Consequently it must vanish for every $u\sigma$, $v\sigma$ with σ in H″. If $E - E_\tau$ is not identically 0 we can find an element γ in M such that $E - \gamma(E - E_\tau)$ is shorter than E. Since $E - \gamma(E - E_\tau)$ shares with E the property of vanishing at $u\sigma$, $v\sigma$ for all σ in H but not all σ in H″, we have a contradiction unless $E - E_\tau \equiv 0$. This means that every coefficient of E lies in H′, the differential field corresponding to H, and is left invariant by H″. But then $E(u\sigma, v\sigma) = 0$ for all σ in H″, a contradiction.

We summarize our results in a single theorem.

Theorem 5.9. — *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-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 then the full differential Galois group of* L *over* K.

23. Liouville extensions. — As in ordinary Galois theory, it is important to study the effect on the differential Galois group of an enlargement of the base field.

Lemma 5.10. — *Let* M *be a Picard-Vessiot extension of* K *(characteristic* 0, *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. — It is immediate that N is a Picard-Vessiot extension of L, for they have the same constant field and N is generated over L by the

same solutions (of the underlying differential equation) that generate M over K. Any differential automorphism of N over K automatically sends M onto itself (Lemma 3.8). Thus we get a homomorphism of the differential Galois group of N/L onto a subgroup (say G_1) of the differential Galois group of M/K. Any automorphism in the kernel leaves fixed both M and L and hence also their union. The homomorphism is therefore an isomorphism, and the image G_1 is therefore an algebraic group of matrices (Theorem 5.5). Its fixed field is exactly $M \cap L$. By Theorem 5.9, G_1 is the whole group of differential automorphisms of M leaving $M \cap L$ fixed.

We now obtain the two main results concerning solvability of differential equations by quadratures.

Theorem 5.11. — *Let* M *be a Picard-Vessiot extension of* K *(characteristic* O, *algebraically closed constant field). Suppose that the differential Galois group of* M *over* K *has a solvable component of the 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 the identity. Let L be the intermediate differential field corresponding to C. Then L is a finite-dimensional normal extension of K, and C is the differential Galois group of M over L. That M is a Liouville extension of L follows at once from Theorem 4.11 and 3.12.

We say that 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 5.12. — *Let* M *be a Picard-Vessiot extension of* K *(characteristic* O, *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 the identity in the differential Galois group* G *of* M *over* K *is solvable (whence by Theorem* 5.11, M *can be obtained from* K *by a finite-dimensional normal extension followed by a Liouville extension).*

Proof. — We make an induction on the number of steps in the chain from K to N. Let $K < z >$ be the first step. Then by induction the differential Galois group of $M < z >$ over $K < z >$ has a solvable component of the identity. By Lemma 5.10 this group is isomorphic to the subgroup (say H) of G corresponding to $M \cap K < z >$. Suppose that z is algebraic over K. Then, by Lemma 3.1, H has finite index in G. Suppose on the other hand that z is either an integral or

an exponential of an integral. By Lemma 3.9 or Lemma 3.10, $K\langle z\rangle$ is a Picard-Vessiot extension of K with abelian Galois group. Thus all 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 with G/H abelian. In either case Lemma 4.9 tells us that the component of the identity in G is solvable.

To conclude this chapter we shall mention (with appropriate references to Kolchin's papers) several refinements of the theory.

1. One can detect from the Galois group the possibility of solving a linear homogeneous differential equation by integrals alone, or by exponentials of integrals alone. If we ignore the complications caused by the possible disconnectedness of the Galois group, the facts are as follows: solvability by integrals alone corresponds to the Galois group admitting special triangular form (1's on the diagonal and 0's below); solvability by exponentials of integrals alone corresponds to the Galois group admitting diagonal form. See [3].

2. Reducibility of the Galois group (or rather of the vector space on which it acts) is equivalent to an appropriate kind of factorisation of the differential equation ([3], § 22).

3. If an equation has a non-solvable Galois group, then it cannot be solved by quadratures even if one allows new constants [4].

4. The theory can be extended to partial differential fields, where one assumes from the start several commuting derivations [6].

5. A final touch can be added to Theorem 5.9: a normal intermediate field is again a Picard-Vessiot extension of the base field [8, p. 891].

6. Substantially the entire theory can be carried through for more general extensions which Kolchin calls *strongly normal* ([7], [8]). The generalisation corresponds exactly to replacing algebraic matrix groups by algebraic group varieties.

CHAPTER VI

EQUATIONS OF ORDER TWO

24. THE WRONSKIAN. — Let $M = K < u_1, ..., u_n >$ be a Picard-Vessiot extension and write W for the Wronskian of $u_1, ..., u_n$.

Lemma 6.1. — *Let σ be a differential automorphism of* M *over* K, with *corresponding matrix c_{ij}. Then* $W\sigma = |c_{ij}|\ W$.

Proof. — We have $u_i\sigma = \Sigma c_{ij}u_j$. It follows that the Wronskian matrix of the u's, multiplied by the matrix c_{ij}, yields the Wronskian matrix of the $u\sigma$'s. On taking determinants we get the result stated in the lemma.

Lemma 6.2. — *The field* $K < W >$ *corresponds to the unimodular subgroup of the differential Galois group.*

Proof. — By Lemma 6.1, W is fixed under σ if and only if $|c_{ij}| = 1$.

Lemma 6.3. *If the underlying differential equation reads*

$$y^{(n)} + ay^{(n-1)} + ... = 0,$$

then $W' = -a\,W$.

Proof. — Differentiate the determinant W by rows: the result is merely to differentiate the last row, converting it into $u_1^{(n)}, ..., u_n^{(n)}$. On substituting in the differential equation we get $W' = -a\,W$.

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

We note finally the classical method of removing the term $ay^{(n-1)}$, at the expense of an exponential of an integral. Let w be a solution of $nw' + aw = 0$, and set $y = wz$. The resulting equation in z has no term in $z^{(n-1)}$.

Thus in studying solvability of differential equations by quadratures, there is no loss of generality in supposing the coefficient of $y^{(n-1)}$ to be 0. The general equation of the second order can be taken as $y'' + ay = 0$.

25. CONNECTION WITH A RICCATI EQUATION.

Theorem 6.4. — *Let* K *be a differential field of characteristic* 0 *with an algebraically closed constant field, and let* a *be an element of* 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 in a quadratic extension of* K.

Proof. — By the corollary to Lemma 6.3, the differential Galois group G of M over K is an algebraic group of two by two matrices of determinant 1. By Theorem 5.12 the component of the identity in G is solvable. We are now able to apply Theorem 4.12. The case where G is finite has been ruled out. In each of the two remaining cases we can assert the following: there is a quadratic extension L of K such that the differential Galois group of M over L can be put in triangular form. This means there is a non-zero solution u of $y'' + ay = 0$ which is carried into a constant multiple of itself by every differential automorphism of M over L, and this in turn means $u'/u \in$ L. Set $t = -u'/u$. Then $u' = -ut$, $u'' = -u't - ut' = u(t^2 - t')$ whereas $u'' = -au$. Hence $t' = t^2 + a$.

We push the computation one step further.

Lemma 6.5. — *Let* K *be a differential field,* a *an element in* K, *and* t *an element 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. — Differentiate $t^2 + rt + s = 0$, using $t' = t^2 + a$. We find

$$2t^3 + rt^2 + (2a + r')t + ar + s' = 0.$$

Multiply $t^2 + rt + s = 0$ by $2t$ and subtract:

$$rt^2 + (2s - 2a - r')t - ar - s' = 0.$$

This yields $2s - 2a - r' = r^2$, $-ar - s' = rs$.
Hence $2s' = 2a' + r'' + 2rr$. Substituting for

$$2s \text{ and } 2s' \text{ in } 2rs + 2s' + 2ar = 0,$$

we get the result stated in the lemma.

26. *An example.* — Let us take the case $y'' + xy = 0$, done in classical style with base field the field K of all rational functions of x with complex coefficients. The solutions are entire functions and we get a well defined Picard-Vessiot extension M inside the field of functions meromorphic in the whole plane. It is not the case that [M:K] is

finite, for then the solutions would be algebraic; but an algebraic entire function is a polynomial and there are no polynomial solutions of

$$y'' + xy = 0.$$

We proceed to examine the possibility that $t' = t^2 + x$ has a solution in K. Say $t = f/g$ is the representation of t with f and g relatively prime polynomials. Then

$$gf' - fg' - f^2 = g^2x.$$

If the degree of f is larger than the degree of g, f^2 is the unique leading term in this equation and cannot be cancelled. If degree of $g \geqq$ degree of f, g^2x is the unique leading term.

There remains the case that $t' = t^2 + x$ has a solution in a quadratic extension of K but not in K. We quote Lemma 6.5. This time we shall use the partial fraction expansion. Let $\sum_{i=1}^{n} c_i (x-a)^{-i}$ be the portion of r occuring for the linear factor $x - a$. Then in order for the equation

$$r'' + 3rr' + r^3 + 4xr + 2 = 0$$

to hold we must have equality among the two highest of the numbers $n + 2$, $2n + 1$ and $3n$, which happens only for $n = 1$. Thus there can be no repeated linear factors. From a term $c/(x\text{-}a)$we get $2c/(x\text{-}a)^3$, $-3c^2/(x\text{-}a)^3$ and $c^3/(x\text{-}a)^3$ from r'', $3rr'$ and r^3 respectively. Hence $2c - 3c^2 + c^3 = 0$, $c = 1$ *or* 2.

This being settled, we switch to the representation $r = f/g$. Bringing everything to the common denominator g^4, we find the following terms in the numerator:

$$g^3f'', fg^2g'', g^2f'g', fg(g')^2, ff'g^2, f^2gg', f^3g, xfg^3, g^4.$$

If f and g have the same degree, the term xfg^3 cannot be cancelled. If the degree of f is strictly the larger of the two, f^3g is the unique highest term. But if the degree of g is the larger of the two the two leading terms xfg^3 and g^4 can cancel, provided the degree of f is smaller by just one.

Returning to the partial fraction decomposition, we see that r must have the form $\Sigma c_i/(x - a_i)$ with $c_i = 1$ or 2, and no polynomial component. Thus we have, say, $g(x) = x^k + \ldots$, $f(x) = \alpha x^{k-1} + \ldots$ with α a positive integer. But then the cancellation between the terms xfg^3 and g^4, arising from the terms $4xr$ and 2 will not occur: $4\alpha + 2$ is not 0.

In summary:

Theorem 6.6. — *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, adjunctions of integrals, and adjunctions of exponentials of integrals.

By supplementary considerations it can be established that the Galois group of this equation is the full unimodular group of two by two matrices. This follows, for instance, from the fact that any proper algebraic subgroup has a solvable component of the identity.

THE BASIS THEOREM AND APPLICATIONS

27. THE BASIS THEOREM. — The Hilbert basis theorem asserts that if R is a commutative ring with unit, satisfying the ascending chain condition on ideals, the same is true of the result $R[x]$ of adjoining an indeterminate.

In proposing an analogue for differential rings, one's first impulse would probably be to impose on R the ascending chain condition on differential ideals, and seek to prove that this is inherited by the ring $R\{x\}$ obtained by adjoining a differential indeterminate. However in this version the proposed analogue is false, even when R is a field: it can be shown that the differential ideals generated by x^2, x^2 and $(x')^2$, x^2, $(x')^2$ and $(x'')^2$, etc. form a properly ascending chain.

The proper result, just as adequate for applications, is:

Theorem 7.1. — *Let* R *be a Ritt algebra satisfying the ascending chain condition on radical differential ideals. Then the same is true for the result* $R\{x\}$ *of adjoining a differential indeterminate. (Ritt-Raudenbush basis theorem.)*

Remark. — There are two sources of difficulty in the proof. First, there are the « differential » difficulties which in particular force us to assume that R is a Ritt algebra and not a mere differential ring. Second there are the complications arising from the fact that radical ideals occur in the hypothesis and conclusion of the theorem. The reader might find it helpful to study the second difficulty by itself by extracting, from the proof below, a proof of the following theorem: if R is a commutative ring with unit satisfying the ascending chain condition on radical ideals, then the same is true of $R[x]$.

The proof requires various préparatory remarks and two lemmas We begin with a definition.

Definition. — A radical differential ideal I in a differential ring is of *finite type* if there exists a finite subset $a_1, \ldots, a_n$ of I such that $I = \{a_1, \ldots, a_n\}$, i.e. such that I is the smallest radical differential ideal containing $a_1, \ldots, a_n$.

Lemma 7.2. — *Let* S *be a subset of a Ritt algebra* A. *Let* a *be an element of* S *such that* $\{a,S\}$ *is of finite type. Then there exist elements* $b_1, \ldots, b_r$ *in* S *such that*

$$\{a, S\} = \{a, b_1, \cdots, b_r\}.$$

Proof. Let I be the differential ideal generated by a and S, and let J be the radical of I. By Lemma 1.8, J is a radical differential ideal, and consequently is equal to $\{a,S\}$. Say $\{a,S\} = \{c_1, \ldots, c_q\}$. For each c_i we have that some power of it is expressible as a linear combination (with coefficients in A) of a, elements of S, and their derivatives. Take for $b_1, \ldots, b_r$ all the elements of S that show up in this way.

Given a differential ring R, we refer to the elements of $R\{x\}$ as *differential polynomials* in x. For any such differential polynomial A there will be a highest derivative $x^{(r)}$ which actually occurs in A; we call r the *order* of A. The degree of A in $x^{(r)}$ will be referred to as the *degree* of A itself. Given a second differential polynomial A_1 we say that A_1 is *below* A if its order is smaller, or, in the event that A and A_1 have the same order, if the degree of A_1 is smaller.

We may write

$$A = B(x^{(r)})^d + C$$

where B is free of $x^{(r)}$ and C has lower degree than A in $x^{(r)}$. We call B the *leading coefficient* of A.

We write $S = \partial A/\partial x^{(r)}$ and call S the *separant* of A. (In taking this partial derivative one treats as constants the elements of R as well as the lower derivatives of x, including x itself if $r > 0$).

Note that both the separant and the leading coefficient of A are below A.

Lemma 7.3. — *Let* A *be a differential polynomial in* x *over a Ritt algebra* R. *Let* I *be the differential ideal in* $R\{x\}$ *generated by* A. *Let* B *and* S *be the leading coefficient and separant of* A. *Let* F *be any differential polynomial in* x. *Then we can find integers* m,n *and a differential polynomial* G *below* A *such that*

$$B^m S^n F \equiv G \pmod{I}.$$

Proof. Differentiating A we find

$$A' = Sx^{(r+1)} + T_1$$

where T_1 has order strictly less than $r + 1$; and after k successive differentiations we similarly find

$$A^{(k)} = Sx^{(r+k)} + T_k \qquad \text{(order of } T_k < r + k\text{)}.$$

Thus if F has order greater than r (say order $r + k$), a suitable power of S multiplied by F will have the property that subtraction of $A^{(k)}$ depresses the order. By repeated steps of this kind we reach the case where F has order r. Then if the degree of F is d or more (where d is the degree of A), a suitable power of B times F will admit the ordinary division algorithm relative to A, and we depress the degree below d.

Proof of Theorem 7.1. It is equivalent for us to prove that every radical differential ideal in $R\{x\}$ is of finite type. Suppose the contrary. Then by Zorn's lemma we may pick a radical differential ideal I which is maximal among those not of finite type. We claim that I is prime. Suppose that $ab \in I$, $a \notin I$, $b \notin I$. Then $\{I,a\}$ and $\{I,b\}$ are larger radical differential ideals and hence of finite type. By Lemma 7.1.

$$\{I, a\} = \{a, c_1, \cdots, c_r\}$$
$$\{I, b\} = \{b, d_1, \cdots, d_s\}$$

where the c's and d's are in I. By Lemma 1.6

$$\{I, a\}\{I, b\} \subset \{ab, \cdots, c_r d_s\} \subset I.$$

Now if z is any element of I, z^2 lies in $\{I, a\}\{I, b\}$, hence in $\{a\,b, \ldots, c_r d_s\}$. Therefore z lies in $\{a\,b, \ldots, c_r d_s\}$, the latter is equal to I, I is of finite type, a contradiction. Hence I is prime.

Now $I \cap R$ is a radical differential ideal in R, and hence by hypothesis it is of finite type. Let J denote the radical differential ideal in $R\{x\}$ generated by $I \cap R$; then J is also of finite type. If $J = I$ we have a contradiction and so J is properly contained in I. Take a differential polynomial A in I but not in J, of smallest possible order, and of smallest degree for that order. Let B the leading coefficient of A:

$$A = B(x^{(r)})^d + C.$$

B cannot be in I. If it were, it would be in J, since it is below A. But then C would be I but not in J, a contradiction since C is also below A. Let S be the separant of A. S cannot be in I. If it were, it would be in J since S is below A. But then

$$A - \frac{1}{d} x^{(r)} S$$

would be in I but not in J, a contradiction since it is below A. (Note

that the hypothesis that R is a Ritt algebra is used crucially here). Since I is prime, the product BS is not in I. Thus $\{BS, I\}$ is a radical differential ideal properly larger than I and consequently is of finite type. By Lemma 7.2, $\{BS, I\} = \{BS, C_1, ..., C_q\}$ where the C's are in I.

Let F be any element of I. By Lemma 7.3 we can find integers m, n and a differential polynomial G below A such that $B^m S^n F - G$ lies in the differential ideal generated by A, and all the more so lies in I. Thus G is an element of I and is below A; hence $G \in J$. It follows that BSF lies in $\{J, A\}$. This being true for all $F \in I$, we have $BSI \subset \{J, A\}$. We now find

$$\begin{aligned} I^2 &\subset I\{BS, I\} \\ &\subset \{BSI, IC_1, \cdots, IC_q\} \quad \text{by Lemma 1.6} \\ &\subset \{J, A, C_1, \cdots, C_q\} \subset I. \end{aligned}$$

From this we argue (as above) that $I = \{J, A, C_1, ..., C_q\}$, a contradiction since I is not of finite type.

Corollary. — *If* R *is a Ritt algebra satisfying the ascending chain condition on radical differential ideals, so is the result* $R\{x_1, ..., x_n\}$ *of adjoining a finite number of differential indeterminates.*

The most important instance of this corollary is the case where R is a differential field of characteristic zero.

28. SYSTEMS OF DIFFERENTIAL EQUATIONS. — An algebraic differential equation (over a differential field F) is the result of equating to O a differential polynomial with coefficients in F. A solution is a set of values (possibly in a differential extension field of F) satisfying the equation. The following theorem is a fairly immediate corollary of Theorem 7.1.

Theorem 7.4. — *Let* F *be a differential field of characteristic* O. *Let* S *be an infinite set of algebraic differential equations over* F *in a finite number of differential indeterminates. Then there exists a finite subset of* S *with the same solutions as* S.

29. THE DECOMPOSITION THEOREM. — The following theorem should be compared with Theorem 2.1. At the expense of a stronger hypothesis we achieve a better conclusion (a finite intersection of prime ideals).

Theorem 7. 5. — *In a differential ring satisfying the ascending chain condition on radical differential ideals, any radical differential ideal is*

expressible as the intersection of a finite number of prime differential ideals. In particular this is true for the ring $F\{x_1, ..., x_n\}$ *obtained by adjoining a finite number of differential indeterminates to a differential field of characteristic* 0.

Proof. — Suppose the contrary. Then (by the ascending chain condition, not by Zorn's lemma !) we can find a radical differential ideal I maximal with respect to the property that it is not an intersection of a finite number of prime differential ideals. Evidently I itself is not prime. Thus there exist elements a and b with $ab \in I$, $a \notin I$, $b \notin I$. The properly larger radical differential ideals $\{I,a\}$ and $\{I,b\}$ are expressible as intersections of a finite number of prime differential ideals. We shall achieve a contradiction by showing that $I = \{I,a\} \cap \{I,b\}$. By Lemma 1.6

$$\{I, a\}\{I, b\} \subset \{ab, I\} \subset I.$$

If c is any element in $\{I, a\} \cap \{I, b\}$ we have $c^2 \in \{I, a\}\{I, b\} \subset I$, $c \in I$. Hence $\{I, a\} \cap \{I, b\} \subset I$, and the reverse inclusion is trivial.

The uniqueness of the decomposition in Theorem 7.5 is a matter of non-differential algebra. Call a representation of I as an intersection of ideals *irredundant* if none of the ideals can be omitted.

Theorem 7.6. — *Let* I *be an ideal in a commutative ring with unit. Suppose that* I *can be expressed in two ways as an irredundant intersection of prime ideals*: $I = P_1 \cap ... \cap P_r = Q_1 \cap ... \cap Q_s$. *Then* $r = s$ *and, after perhaps renumbering,* $P_i = Q_i$.

Proof. — We have $P_1 \cap ... \cap P_r \subset Q_1$, hence $P_1 ... P_r \subset Q_1$, hence one of the $P's$ is contained in Q_1. We can suppose $P_1 \subset Q_1$. Similarly one of the $Q's$ is contained in P_1. By the irredundancy, this must be Q_1, and we have $Q_1 = P_1$. Similarly each Q_i gets equated to a unique P_i, and vice versa.

30. STUDY OF A SINGLE DIFFERENTIAL POLYNOMIAL. — In this section we shall observe how the theory obtained in the preceding sections works out in the special case of the radical differential ideal generated by a single polynomial.

Let A be a differential polynomial in one differential indeterminate y. Let A have order r, and let S be the separant: $S = \partial A/\partial y^{(r)}$. Define J to be the set of all B with $BS \subset \{A\}$. By Lemma 1.4, J is a radical differential ideal. We shall adhere to this notation in the succeeding discussion.

Lemma 7.7. — $\{A\} = \{A, S\} \cap J$.

Proof. That $\{A\}$ is contained in both $\{A, S\}$ and J is clear. Conversely suppose C lies in $J \cap \{A, S\}$. Then

$$C^2 \in C\{A, S\} \subset \{CA, CS\} \subset \{A\},$$

whence $C \in \{A\}$.

From this point on we must assume that the underlying differential field has characteristic O.

Lemma 7.8. — *Suppose that* A *is irreducible (in the ordinary algebraic sense, as a polynomial in an infinite number of indeterminates* $y, y', y'' \ldots$*). Suppose that* G *lies in the differential ideal generated by* A, *and that order of* $G \leqq$ *order of* A. *Then* A *divides* G.

Proof. — We have an equation of the form

$$(*) \qquad G = C_0A + C_1A' + \cdots + C_kA^{(k)}.$$

Further, $A^{(i)} = Sy^{(r+i)} + T_{r+i}$ for $i = 1,2, \ldots$, where the order of T_{r+i} is less than $r + i$. We look at (*) as an identity in the indeterminates $y, y', y'', \ldots$. The element $y^{(r+k)}$ may occur in the C's but it does not occur in G. We may replace $y^{(r+k)}$ *by* $-T_{r+k}/S$ in (*) and the result is still an identity (note that S is non-zero because of characteristic zero). After multiplying by a suitable power of S, the result is an equation of the form

$$S^jG = D_0A + D_1A' + \cdots + D_{k-1}A^{(k-1)}.$$

By induction on k we conclude that A divides S^jG. But A does not divide S (S is below A). Hence A divides G. (Note that from the point of view of ordinary algebra we are working in the integral domain obtained by adjoining a countable number of indeterminates to a field, and this is a unique factorization domain).

Lemma 7.9. — *Assume again that* A *is irreducible. Then* J *is prime.*

Proof. — Suppose that $FG \in J$; we shall prove that F or G is in J. Let I be the differential ideal generated by A. We can find integers m, n and differential polynomials F_1, G_1 with order at most the order of A such that

$$S^mF \equiv F_1, \; S^nG \equiv G_1 \pmod{I}.$$

(This portion of Lemma 7.3 is implicit in its proof). We have $SFG \in \{A\}$ by the definition of J. By Lemma 1.8, $\{A\}$ is the radical of I. We therefore have $(SFG)^k \in I$ for a suitable integer k. After multiplying by $S^{mk+nk-k}$ we find $(S^mF)^k(S^nG)^k \in I$. Hence $(F_1G_1)^k \in I$. By Lemma 7.8, A divides $(F_1G_1)^k$. Since A is irreducible, A must divide F_1 or G_1, say F_1. This means $S^mF \in I$, $S^mF^m \in I$, $SF \in \{A\}$, $F \in J$.

Therorem 7.10. — *Let* F *be a differential field of characteristic* O. *Let* A *be an irreducible differential polynomial in one indeterminate over* F. *Let* S *be the separant of* A, *and* J *the set of all differential polynomials* B *with* $BS \in \{A\}$. *Then* J *is a prime differential ideal. If* $\{A, S\} = P_1 \cap \ldots \cap P_r$ *is the irredundant representation of* $\{A, S\}$ *as an intersection of prime differential ideals, then the irredundant representation of* $\{A\}$ *has the form* J ∩ *(some of the* P's).

Proof. — Only the last sentence awaits proof. By Lemma 7.7, $\{A\} = J \cap P_1 \cap \ldots \cap P_r$. If it were possible to delete J from this representation we would have

$$J \cap P_1 \cap \cdots \cap P_r = P_1 \cap \cdots \cap P_r$$

whence $J \supset \{S, A\}$, $S \in J$, $S^2 \in \{A\}$, S to some power lies in the differential ideal generated by A, A divides S by Lemma 7.8, a contradiction.

The component J in the expression of A is called the *general solution ideal*, the other components being *singular solution ideals.*

31. Examples. — *a*) $A = (y')^2 - 4y$. Here $S = 2y'$. Then $\{S, A\}$ is the ideal generated by y and all its derivatives; it is a maximal ideal. $A' = 2y'(y'' - 2)$. Now y' is not in J; if it were, it would be in $\{A\}$ since $y' \in \{S, A\}$. This means some power of y' lies in the differential ideal generated by A and, by Lemma 7.8, is divisible by A. But A cannot be a factor of a power of y'. Hence $y' \notin J$, and it follows, since J is prime, that $y'' - 2 \in J$. Thus J contains $K = \{(y')^2 - 4y, y'' - 2\}$. Now the ordinary ideal generated by $(y')^2 - 4y$, $y'' - 2$, y''', ... is already a differential ideal. Moreover it is prime; for on mapping modulo it we suppress the variables y'', y''', ... and then map modulo the irreducible polynomial $(y')^2 - 4y$. Hence K is prime. We have the equation

$$\{A\} = J \cap \{S, A\} \cap K.$$

If J were properly larger than K we could delete J from this equation, contradicting Theorem 7.10. Hence $J = K$. We have thus identified the decomposition of $\{A\}$.

Let us find the solutions of $(y')^2 - 4y = 0$. If t is a solution, $t'(t'' - 2) = 0$. Either $t' = 0$ or $t'' = 2$.

In the first case $t = 0$. In the second $(t'/2)' = 1$. If we write x for a specific element with $x' = 1$, then $t'/2 = x + c$, $t = (t'/2)^2 = (x + c)^2$, where c is a constant. Classically, the solutions break into a family of parabolas, the solutions of J above, and their envelope, the line $y = 0$, which is the singular solution.

(*b*) $A = (y')^2 - 4y^3$. Again $S = 2y'$ and $\{A, S\}$ is the ideal gene-

rated by y and its derivatives. As above we argue that J is the ideal generated by $(y')^2 - 4y^3$, $y'' - 6y^2$ and the derivatives of the latter. But then $J \subset \{A, S\}$. Hence $\{A\} = J$ and is already prime.

The solutions are $y = 0$, $y = (x + c)^{-2}$.

An individual solution of A is said to be *singular* if it annuls the separant S of A. The above example (*b*) is one where the general solution contains a singular solution.

APPENDIX : MORE ON MATRIX GROUPS AND THEIR ABSTRACTION

32. SOLVABILITY. — We begin by noting a result valid even in T_1-groups.

Theorem 8.1. — *In a T_1-group the closure of a subgroup is a subgroup; the closure of a normal subgroup is a normal subgroup.*

Proof. Let G be the group, S the subgroup, S_1 the closure of S. For $s \in S$, the mapping $x \to sx$ is a homeomorphism of G onto itself. Hence the inverse image of S_1 is closed. Since this inverse image contains S, it contains S_1. Thus $sS_1 \subset S_1$. Again take t in S_1, and look for the inverse image of S_1 under the mapping $x \to xt$. We conclude that $S_1S_1 \subset S_1$. Since $S_1^{-1} = S_1$ by the continuity of the inverse, S_1 is a subgroup.

For fixed a in G the mapping $x \to axa^{-1}$ is a homeomorphism of G onto itself. Hence aS_1a^{-1} is closed. Assume now that S is normal. Then aS_1a^{-1} contains S and hence contains S_1. Thus $a^{-1}S_1a \subset S_1$, and S_1 is normal.

In a T_1-group it need not be true that the closure of an abelian subgroup is abelian-see § 17 for remarks on the construction of a counter-example. However this is true in a C-group. We prove a result slightly more general.

Theorem 8.2. — *Let* G *be a* C*-group,* S *and* T *subgroups with* $S \supset T$. *Suppose that* T *contains the commutator subgroup of* S. *Then the closure* T_1 *of* T *contains the commutator subgroup of the closure* S_1 *of* S.

Proof. — For fixed b in S the mapping $a \to aba^{-1}b^{-1}$ is continuous. The inverse image of T_1 contains S and therefore contains S_1. Next fix a in S_1. The mapping $b \to aba^{-1}b^{-1}$ is continuous. The inverse image of T_1 again contains S and therefore contains S_1. Hence T_1 contains all commutators of elements of S_1.

Corollary 1. — *In a* C*-group the closure of an abelian subgroup is abelian.*

Proof. — Take T = 1 in Theorem 8.2.

Corollary 2. — *In a* C*-group the closure of a solvable subgroup is solvable.*

Proof. — Let H be a solvable subgroup of a C-group, K its closure Let $H = H_1 \supset \ldots \supset H_n = 1$ be the derived series of H, and let K_i be the closure of H_i. By Theorem 8.2, K_{i+1} contains the commutator subgroup of K_i. Hence each K_i/K_{i+1} is abelian and K is solvable.

We close this section with a result proved by Kolchin [5] for matrix groups in the Zariski topology.

Call a T_1-group G *topologically solvable* if there exists a chain $G = G_1 \supset G_2 \supset \ldots \supset G_n = 1$ of *closed* subgroups, each normal in its predecessor, and such that each G_i/G_{i+1} is abelian. Of course any topologically solvable group is solvable. For C-groups we prove the converse.

Theorem 8.3. — *A solvable* C*-group* G *is topologically solvable.*

Proof. We argue by induction on the length of the derived series of G. Suppose it ends with $G_k = 1$. Then G_{k-1} is an abelian normal subgroup of G. Its closure H is abelian normal by Theorem 8.1 and Cor. 1 of Theorem 8.2. The group G/H is again a C-group and its derived series is shorter than that of G. By induction G/H is topologically solvable. Hence G is topologically solvable.

33. CZ*-groups.* — Any group is capable is being a C-group : take it in the discrete topology. Any group is capable of being a Z-group : take it in the minimal T_1-topology. But not every group can be a CZ-group. By Lemmas 4.5 and 4.6 :

Theorem 8.4. — *In a* CZ*-group, and in particular in any multiplicative group of matrices, there is a finite upper bound to the size of the finite conjugate classes.*

A more useful result follows from the descending chain condition on closed sets, when we recall that any centralizer in a C-group is closed.

Theorem 8.5. — *In a* CZ*-group, and in particular in any multiplicative group of matrices, the centralizers of subsets satisfy the descending chain condition.*

The group of finite even permutations on an infinite set rather obviously violates the descending chain condition on centralizers.

Moreover it is simple, so that any non-trivial matrix représentation must be faithful. Hence:

Theorem 8.6. — *The group of finite even permutations on an infinite set admits no matrix representations whatever (any field, any size of matrix) other than the representation sending every element into the identity matrix.*

The existence of a group with this property does not seem to have been previously noted in the literature.

34. IRREDUCIBLE SETS; THE ASCENDING CHAIN CONDITION. — In the theory of Chapter IV a major role was played by the concept of connectedness. But in algebraic geometry it is not connectedness that is important but rather irreducibility.

Definition. — A topological space X is *irreducible* if it cannot be expressed as the union of two proper closed subsets. A subset of X is irreducible if, in the induced topology, it is an irreducible topological space.

Remark. — It is easy to see that an irreducible Hausdorff space contains at most one point.

We collect in the next lemma some of the relevant facts; the proofs are easy and we omit them. (For a related exposition see [11]).

Lemma 8.7. — *a) A continuous image of an irreducible space is irreducible. b) The closure of an irreducible set is irreducible. c) Any Z-space can be expressed as a finite union* $S_1 \cup S_2 \cup \ldots \cup S_r$ *of closed irreducible subsets. If the expression is irredundant (i.e. if no* S_i *can be omitted), then it is unique.*

In Chapter IV we needed only to consider connected sets because for. groups connectedness and irreducibility coincide.

Lemma 8.8. — *Let* G *be a Z-group,* C *its component of the identity Then the unique irredundant decomposition of* G *into closed irreducible sets is obtained by resolving* G *into its cosets modulo* C.

Proof. — Let $G = S_1 \cup S_2 \cup \ldots \cup S_r$ be the decomposition. We begin by proving that the S's are disjoint. Suppose $a \in S_1 \cap S_2$. Any homeomorphism of G merely permutes the S's (because of the uniqueness of the decomposition). For any element b in G there is a homeomorphism (for instance, a right multiplication) carrying a into b. Hence b lies in two distinct S's. In particular any element of S_1 lies in at least one S with $i > 1$. Thus

$$S_1 = (S_1 \cap S_2) \cup \cdots \cup (S_1 \cap S_r).$$

Since each $S_1 \cap S_i$ is closed and properly smaller than S_1, we have contradicted the irreducibility of S_1. Therefore the S's are disjoint.

Let S_1 be the one containing the identity of G. For any a in S_1, $S_1 a$ intersects S_1 and is also one of the S's; hence $S_1 a = S_1$. Likewise $S_1^{-1} = S_1$. Hence S_1 is a subgroup. Of course S_1 is connected; it must be the component of the identity, and the other S's are its cosets.

Corollary. — *A connected Z-group is irreducible.*

Consider again an arbitrary field F and an n-dimensional vector space V over F, endowed with the Zariski topology. Then V satisfies the ascending chain condition on its irreducible closed subsets; this follows from the fact that each such irreducible closed subset has a dimension bounded by n, and the dimension is properly increasing. Moreover this ascending chain condition is inherited by the subsets of V. Hence: any matrix group is the Zariski topology satisfies the ascending chain condition on closed irreducible subsets and in particular (Corollary to Lemma 8.9) on closed connected subgroups. We can draw an interesting consequence from this.

Theorem 8.9. — *Let* G *be a connected* CZ*-group satisfying the ascending chain condition on closed connected normal subgroups. Then* G *has a unique largest connected solvable normal subgroup* M; M *is automatically closed. If* Z/M *is the center of* G/M *then* Z/M *is finite and* Z *is the unique largest solvable normal subgroup in* G.

Proof. — By the ascending chain condition we first pick M to be a maximal closed connected solvable normal subgroup of G. If H is any connected solvable normal subgroup, then HM is solvable normal by standard algebra and connected by easy point set topology. The closure of HM is solvable (Cor. 2 of Theorem 8.2), normal and connected. Hence $H \subset M$.

The group G/M (it is again a CZ-group) has no connected solvable normal subgroup. Hence any solvable normal subgroup is finite and therefore (Lemma 4.7) central. Thus Z/M is finite and Z is the unique largest solvable normal subgroup in G.

Lemma 8.11. — *Let* G *be a group with a normal subgroup* H. *If both* H *and* G/H *possess a unique largest solvable normal subgroup, the same is true of* G.

We leave the proof to the reader. As a corollary of Theorem 8.10 and Lemma 8.11 we have:

Theorem 8.12. — *Let* G *be a* CZ*-group satisfying the ascending chain condition on closed connected normal subgroups. In particular,* G

can be any matrix group (in the Zariski topology). Then G *has a unique largest solvable normal subgroup.*

For matrix groups this result was proved by Zassenhaus [12] in a different way.

35. IMAGES OF IRREDUCIBLE SETS. — Everything treated in Chapter IV and thus far in Chapter VIII applied to any matrix group, not necessarily algebraic. Naturally then we are not in a position to prove any result concerning matrix groups which actually requires the group to be algebraic. In this final section we shall invoke an additional axiom which makes possible some further progress.

Definition. — Let X be a topological space, S a subset with closure S_1. We say that S is *semi-closed* if S contains a subset T which is dense in S_1 and open in the relative topology of S_1. (Motivation from algebraic geometry: S is an algebraic manifold with a portion of a manifold of lower dimension deleted).

Lemma 8.13. — *Let* |G *be a connected Z-group and* U *a semi-closed dense subset of* G. *Then* UU = G.

Proof. — We have $U \supset V$ with V an open dense subset of G. We shall prove VV = G. For any x in G, V and $V^{-1}x$ are non-void open sets. Since G is irreducible (Cor. to Lemma 8.8), $V \cap V^{-1}x$ is non-void. Hence $x \in VV$.

By a *word* in a group, in variables $x_1, \ldots, x_r$, we mean a product of powers (positive or negative) of the x's and of other fixed group elements.

We now state the proposed axiom, labelling it (D).

(D). Let G be a T_1-group. We say that G satisfies axiom (D) if the following is true: for any closed irreducible sets $C_1, \ldots, C_r$ and any word $f(x_1, \ldots, x_r)$, the range of f as x_i runs over C_i $(i = 1, \ldots, r)$ is a semi-closed irreducible set.

That algebraic matrix groups under the Zariski topology (over an algebraically closed field) satisfy axiom (D) is implicit in Chevalley's volume on algebraic groups [1]. A brief proof from scratch can be given via elimination theory.

Theorem 8.14. — *Let* G *be a Z-group satisfying the ascending chain condition on closed irreducible sets and axiom* (D). *Let* $S_1, \ldots, S_r$ *be closed connected subgroups of* G. *Let* $f_i(x_1, \ldots, x_r)$, $i = 1, \ldots, k$, *be words each having the property that for some value of the variables* $x_j \in S_j$, f_i *takes the value* 1. *Let* H *be the subgroup generated by all elements* $f_1(x_1, \ldots, x_r), \ldots, f_k(x_1, \ldots, x_r)$ *as* x_j *ranges over* S_j. *Then*: H *is closed.*

Moreover there exists an integer n such that every element of H *is a product of at most n of the f's and their inverses.*

Proof. — It is harmless to adjoin to the *f's* the further polynomials $f_1^{-1}, \ldots, f_k^{-1}$. We suppose that this has already been done. Then H is merely the set of all products of *f's*.

Let $m_1, \ldots, m_t$ be any sequence of integers, each in the range 1 to k. By C $(m_1, \ldots, m_t)$ we denote the set of all elements $f_{m1} \ldots f_{mt}$, the arguments $x_1, \ldots, x_r$ of the *f's* of course ranging over $S_1, \ldots, S_r$.

Let $D(m_1, \ldots, m_t)$ be the closure of $C(m_1, \ldots, m_t)$. By axiom (D) we have that $D(m_1, \ldots, m_t)$ is irreducible. From the fact that the *f*'s take the value 1 for suitable values of the arguments, we see that $C(m_1, \ldots, m_{t-1}) \subset C(m_1, \ldots, m_t)$ and the same relation consequently holds for the D's.

Let H_1 be the union of all the D's. From the ascending chain condition on closed irreducible sets, plus a simple combinatorial argument, we deduce the existence of an integer p such that H_1 is already the union of those $D(m_1, \ldots, m_t)$ with $t \leqq p$. Hence H_1 is closed. Since H is dense in H_1, H_1 is simply the closure of H, and therefore it is a subgroup of G. Next, denote by H_0 the union of all $C(m_1, \ldots, m_t)$ with $t \leqq p$. By axiom (D), H_0 is semi-closed (with closure H_1). By Lemma 8.13, $H_0H_0 = H_1$. This proves that $H = H_1$ is closed, and that $n = 2p$ fulfils the requirements of the theorem.

We conclude by noting four special cases of Theorem 8.14.

Theorem 8.15. — *Let* G *be a Z-group satisfying the ascending chain condition on closed irreducible subsets and axiom* (D). *Let* $S_1, \ldots, S_r$ *be closed connected subgroups of* G. *Then the union of the subgroups* $S_1, \ldots, S_r$ *is closed. Moreover in forming this union we need only products of length* $\leqq n$ *for a certain integer n.*

Proof. — Apply Theorem 8.14 to the one polynomial $x_1x_2 \ldots x_r$.

Easy examples show that we cannot in Theorem 8.15 drop the hypothesis that the S's are connected. However this is possible if all but one of them is normal.

Theorem 8.16. — *Let* G *be a Z-group satisfying the ascending chain condition on closed irreducible subsets and axiom* (D). *Let* S, T *be closed subgroups of* G *with* S *normal. Then* ST *is closed.*

Proof. — Let S_0, T_0 be the components of the identity in S, T. Then S_0T_0 is closed by Theorem 8.15. Since it is of finite index in ST, the latter is closed.

Theorem 8.17. — *Let* G *be a connected Z-group satisfying the ascending chain condition on closed irreducible subsets and axiom* (D). *Let*

G_r be the subgroup of G generated by all r-th powers. Then G_r is closed. Moreover in forming G_r we need only products of r-th powers of length $\leq n$ for a certain integer n.

Proof. — Apply Theorem 8.14 to the one polynomial x_r.

I do not know whether one must assume in Theorem 8.17 that G is connected. For the next theorem, however, connectedness is not needed. (For connected algebraic matrix groups the theorem is due to Chevalley [1]; I am indebted to M. Rosenlicht for the present proof.)

Theorem 8.18. — *Let G be a Z-group satisfying the ascending chain condition on closed irreducible subsets and axiom* (D). *Let G′ be the commutator subgroup of G. Then G′ is closed. Moreover in forming G′ we need only products of commutators of length $\leq n$ for a certain integer n.*

Proof. — Let C be the component of the identity, and let $z_1, \ldots, z_h$ be representatives of the cosets of G modulo C. Define $f_i(x,y)$ to be the commutator of $z_i x$ and y ($1 \leq i \leq h$). Note that $f_i = 1$ when $x = y = 1$. Apply Theorem 8.14 to these h polynomials, with x and y ranging over C. The resulting subgroup (call it H) is closed, and moreover there is a bound on the length of the products of commutators needed in forming H. We note that C/H is central in G/H. The proof of the theorem is thereby reduced to the following purely group-theoretic theorem discovered independently by Baer, Neumann and Witt.

Theorem 8.19. — *If the center of a group G is of finite index, then the commutator subgroup of G is finite.*

The following proof of Theorem 8.19 is due to Donald Ornstein. Let $a_1, \ldots, a_m$ be representatives of the cosets of G modulo its center. Any commutator in G is then of the form $a_i^{-1} a_j^{-1} a_i a_j$, and there are at most m^2 of them. Our problem is to put a bound on the length of the products of commutators. Now in a sufficiently long product some commutator will get repeated m times. We can bring these m elements together; this harmlessly replaces some of the other commutators by conjugates. The following lemma then completes the proof.

Lemma 8.20. — *If $(ab)^m$ lies in the center of a group, then $(a^{-1} b^{-1} ab)^m$ can be expressed as a product of $m - 1$ commutators.*

Let us prove, for any integer r, that $(a^{-1}b^{-1}ab)^r$ can be written as the product of $(a^{-1} b^{-1})^r (ab)^r$ and $r - 1$ commutators. Assuming this for $r - 1$, we have

$$(a^{-1}b^{-1}ab)^r = a^{-1}b^{-1}ab(a^{-1}b^{-1})^{r-1}(ab)^{r-1}c_{r-2} \cdots c_1,$$

the $c's$ being commutators. Commutate ab past $(a^{-1}\,b^{-1})^{r-1}$; this introduces a new commutator which can be placed just before c_{r-2}, by switching it to a conjugate. We have proved the statement for r, and we proceed to apply it with $r = m$. Note that $(ba)^m$ is a conjugate of $(ab)^m$ and so is equal to it. Hence $(a^{-1}\,b^{-1})^m(ab)^m = 1$, and the lemma is proved.

GLOSSARY

The following is an informal list of the more important definitions, given (more or less) in the order in which they occur in the text.

Derivation. An additive mapping satisfying the product law for derivatives.

Differential ring. A commutative ring with unit and a distinguished derivation.

Differential ideal. An ideal closed under derivation.

Differential homomorphism (isomorphism, automorphism). A homomorphism (isomorphism, automorphism) commuting with derivative.

Constant. An element with derivative O.

Radical of an ideal. The set of all elements with some power in the ideal.

Radical ideal. An ideal equal to its own radical.

Ritt algebra. A differential ring containing the rational numbers.

Admissible isomorphism. An isomorphism between two fields when there is a superfield containing both.

Differential Galois group. The group of all differential automorphisms of the top field, leaving the bottom one elementwise fixed.

Wronskian of n *elements.* The n by n determinant having in its i-th row the $(i - 1)$-is derivatives of the elements.

Picard-Vessiot extension. An extension with no new constants, génétared by n linearly independent solutions of an n — *th* order linear homogeneous equation.

Adjunction of an integral. Adjunction of an element u with u' in the base field.

Adjunction of an exponential of an integral. Adjunction of an element u with u'/u in the base field.

Liouville extension. End result of a finite number of extensions, each the adjunction of an integral or an exponential of an integral.

Generalized Liouville extension. End result of a finite number of extensions, each the adjunction of an integral, the adjunction of an exponential of an integral, or a finite algebraic extension.

Zariski topology. The closed sets are the algebraic manifolds.

Algebraic matrix group. Group consisting of all non-singular matrices satisfying a set of polynomial equations (i.e.a closed subgroup of the full linear group in the Zariski topology).

Z-space. T_1-space with the descending chain condition on closed sets.

T_1*-group.* A group and a T_1-space, with the inverse continuous and multiplication separately continuous.

Z-group. A T_1-group which is a Z-space.

C-*group.* A T_1-group where the mapping $a \to a^{-1}xa$ (x fixed) is continuous.

CZ-*group.* A T_1-group which is both Z and C.

Differential polynomial. A polynomial in an element (say y) and its derivatives. The *order* is the highest derivative $y^{(r)}$ that actually occurs. The *degree* is the power d to which $y^{(r)}$ is raised. The *leading coefficient* is the coefficient of $[y^{(r)}]^d$. The *separant* is the partial derivative of the polynomial with respect to $y^{(r)}$.

Irreducible topological space. A space which cannot be expressed as the union of two proper closed subsets.

Notation for adjunction. Four kinds of adjunction occur, each with its own notation. We use [ ] for ordinary ring adjunction, ( ) for ordinary field adjunction, $\{\ \}$ for differential ring adjunction, $<\ >$ for differential field adjunction. The braces are also used to denote the smallest radical differential ideal containing a set; the context should make it clear which meaning is intended.

BIBLIOGRAPHY

[1] C. CHEVALLEY, Théorie des Groupes de Lie, Tome II: Groupes Algébriques, *Act. sc. et ind.*, 1152, Paris, 1951.

[2] E. R. KOLCHIN, Extensions of differential fields I, *Ann. of Math.*, 43, 724-729 (1942).

[3] E. R. KOLCHIN, Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, *Ann. of Math.*, 49, 1-42 (1948).

[4] E. R. KOLCHIN, Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations, *Bull. Amer. Math. Soc.*, 54, 927-932 (1948).

[5] E. R. KOLCHIN, On certain concepts in the theory of algebraic matric groups, *Ann. of Math.*, 49, 774-789 (1948).

[6] E. R. KOLCHIN, Picard-Vessiot theory of partial differential fields, *Proc. Amer. Math. Soc.*, 3, 596-603 (1952).

[7] E. R. KOLCHIN, Galois theory of differential fields, *Amer. J. of Math.*, 75, 753-824 (1953).

[8] E. R. KOLCHIN, On the Galois theory of differential fields, *Amer. J. of Math.*, 77, 868-894 (1955).

[9] J. F. RITT, Differential equations from the algebraic standpoint, *Amer. Math. Soc. Coll. Pub.*, vol. 14, New-York, 1932.

[10] J. F. RITT, Differential algebra, *Amer. Math. Soc. Coll. Pub.*, vol.33, New-York, 1950.

[11] J.-P. SERRE, Faisceaux algébriques cohérents, *Ann. of Math.*, 61. 197-278 (1955).

[12] H. ZASSENHAUS, Beweis eines Satzes über diskrete Gruppen, *Hamb. Abh.*, 12, 289-312 (1938).