SOLUTION OF THE INVERSE PROBLEM OF DIFFERENTIAL GALOIS THEORY IN THE CLASSICAL CASE

By CAROL TRETKOFF and MARVIN TRETKOFF

In analogy with ordinary Galois theory, we may inquire ([7], [8], [9]): given a differential field K with field of constants k and an affine algebraic group G defined over k, does there exist a differential field extension E/K whose differential Galois group is isomorphic to G? Perhaps the most important case occurs when k is algebraically closed of characteristic zero and $K = k(z)$, the field of rational functions with coefficients in k. In this generality, the best answer presently available is due to J. Kovacic ([9], [8]), who proves, among other things, that the answer is affirmative provided G is *solvable.* The purpose of the present paper is to remove this restriction on G in the "classical case," that is, when $k = \mathbf{C}$, the complex numbers. More precisely, we shall prove:

THEOREM. *If $G \subset GL(n, \mathbf{C})$ is an arbitrary affine algebraic group, then there is a Picard-Vessiot extension E of $\mathbf{C}(z)$ whose differential Galois group is G.*

Our proof utilizes the availability in the classical case of topological notions and transcendental tools not at our disposal in differential algebra. In particular, we may associate a finitely generated group M, the monodromy group, to every homogeneous linear ordinary differential equation. If the equation is of Fuchsian type, the Zariski closure of M is the differential Galois group of the equation (Proposition III). Since every affine algebraic group G defined over $\mathbf{C}$ contains a finitely generated Zariski dense subgroup (Proposition I), the inverse problem of differential Galois theory is reduced to the problem of the existence of differential equations of Fuchsian type with prescribed finitely generated groups as their monodromy groups. Now, the latter is the famous Twenty First Hilbert Problem (formulated below as Proposition II); the complete solution was first obtained by Hilbert and Plemelj using the theory of integral equations. This powerful existence theorem can also be established by modern sheaf theoretic methods ([6]) which ex-

Manuscript received June 16, 1978

American Journal of Mathematics, Vol. 101, No. 6, pp. 1327-1332
0002-9327/79/1016-1327 $01.50

tend its validity from the Riemann sphere to more general algebraic varieties. Thus, *our Theorem remains valid if* $\mathbf{C}(z)$ *is replaced, for example, by the function field of any compact Riemann surface.*

Upon completing this paper, we examined the treatise [12] of Schlesinger, which appeared a decade before the solution of the Hilbert problem. We surmise that Schlesinger realized that the solution of the inverse problem of differential Galois theory would follow from that of the Hilbert problem by the method employed herein. In particular, he gives a proof of Proposition III which is virtually the same as the one presented here, but which, naturally, makes no reference to the Zariski topology. Professor M. Kuga has kindly informed us that he, too, has presented a proof of Proposition III in his Japanese book [10]. Finally, we note that the Lemma can be proved without the use of Schur's Theorem if one admits a more sophisticated knowledge of algebraic groups.

In the following discussion k shall denote an algebraically closed field of characteristic zero and, for brevity, we shall refer to an affine algebraic group as an algebraic group.

LEMMA. *If every element of the algebraic group* $G \subset GL(n, k)$ *has finite order, then* G *is finite.*

Proof. According to a well known theorem of Schur (c.f. [1], [2]), any periodic subgroup of $GL(n, k)$ contains a commutative subgroup of finite index. Thus, the connected component of the identity, G°, is commutative. Moreover, the periodicity of G implies that all its elements are semi-simple; and it is a standard result ([4]) that a connected commutative algebraic group whose elements are all semi-simple is isomorphic to the direct product of a finite number of copies of k^*, the multiplicative group of k. Applying this to G° and noting that k^* contains elements of infinite order, we conclude that $G^{\circ} = 1$ and G is finite.

COROLLARY. *An algebraic group* $G \subset GL(n, k)$ *of dimension at least one must contain a finitely generated subgroup* H *whose Zariski closure* $\overline{H}$, *is also of dimension at least one.*

Proof. Otherwise, the closure of every finitely generated subgroup is zero dimensional; it follows that G is periodic and, therefore, finite.

In fact, we have the following stronger result, which is essential for the proof of our theorem.

PROPOSITION 1. *Every algebraic group $G \subset GL(n, k)$ contains a finitely generated subgroup H whose Zariski closure $\overline{H} = G$.*

Proof. With no loss of generality, we may assume that G is connected. For, it is obvious that if the connected component of the identity, G°, contains a finitely generated Zariski dense subgroup R, then the subgroup generated by R and a system of coset representatives for G° in G is Zariski dense in G. Noting that the Proposition is trivial if the dimension of G is zero and that it reduces to the Corollary above if the dimension of G is one, we argue by induction on dim G, the dimension of G. Thus, we assume that the Proposition is valid for algebraic groups of dimension less than dim G, and we select a proper closed connected subgroup $H \subset G$ for which dim H is maximal.

Now, if H is normal in G, then there are finitely generated Zariski dense subgroups $R \subset H$ and $S \subset G/H$. If R is generated by $h_1, \ldots, h_r$ and if S is generated by the cosets of $g_1H, \ldots, g_sH$, we let L denote the subgroup of G generated by $h_1, \ldots, h_r, g_1, \ldots, g_s$ and note that S belongs to $\overline{LH/H} = \overline{L}/H$, the image of $\overline{L}$ in G/H. Moreover, since $\overline{L}/H$ is closed in G/H, it contains $\overline{S} = G/H$, and we see that $\overline{L} = G$.

If H is not normal in G, then there is an element $g \in G$ such that $H \neq gHg^{-1}$. Now, if R is a finitely generated Zariski dense subgroup of H, we let L denote the finitely generated subgroup of G generated by R and g. Since the closed connected subgroups H and gHg^{-1} both belong to $\overline{L}$, they are both contained in $\overline{L}^\circ$. Now, if dim $\overline{L}^\circ <$ dim G, dim $\overline{L}^\circ =$ dim $H =$ dim gHg^{-1} and, therefore, $\overline{L}^\circ = H$ and $\overline{L}^\circ = gHg^{-1}$. This is impossible because $H \neq gHg^{-1}$. Thus, dim $\overline{L}^\circ =$ dim G and $\overline{L} = \overline{L}^\circ = G$.

Now, suppose we are given an ordinary differential equation

$$w^{(n)} + a_1(z)w^{(n-1)} + \cdots + a_n(z)w = 0 \tag{*}$$

with coefficients which are single valued analytic functions on the domain Z obtained from the Riemann sphere by deleting the set $S = \{z_1, \ldots, z_t\}$ of singular points of the equation. Now, we select a base point $z_0 \in Z$ and n linearly independent solutions $w_1(z), \ldots, w_n(z)$ of (*) at z_0. We regard the latter as a column vector $\omega(z)$. Clearly, any solution of (*) at z_0 may be analytically continued along any path in Z which begins at z_0; and the resulting function satisfies (*) at every point where it is defined. Thus, analytic continuation of $\omega(z)$ along any loop l in Z beginning at z_0 yields another column vector whose components constitute n linearly independent solutions of (*) at z_0. It follows that the new column is of the form $m\omega(z)$ where $m \in GL(n, \mathbf{C})$ is called the *monodromy matrix* of $\omega(z)$ along l and is uniquely determined by the homotopy class of l. Next, we choose loops l_i ($i = 1, \ldots, t$) in Z based at z_0 such that:

(i) if $i \neq j$, l_i and l_j meet only at z_0
(ii) the product $l_1 \cdots l_t$ is null-homotopic
(iii) the winding number of l_i with respect to z_j is 1 if $i = j$ and 0 otherwise.

If we denote the monodromy matrix of $\omega(z)$ along l_i by m_i ($i = 1, \ldots, t$), then the subgroup of $GL(n, \mathbf{C})$ generated by $m_1, \ldots, m_t$ is called the *monodromy group* of (*) and denoted by M. Of course, $m_1 \cdots m_t = 1$ because $l_1 \cdots l_t$ is null-homotopic. Because of the choices made in its construction, the monodromy group is only determined up to conjugation as a subgroup of $GL(n, \mathbf{C})$.

Perhaps the most famous result about monodromy groups is the following ([3], [11]):

PROPOSITION II. (*Solution of Hilbert's Twenty First Problem*): *Let there be given matrices* $m_i \in GL(n, \mathbf{C})$ ($i = 1, \ldots, t$) *whose product* $m_1 \cdots m_t = 1$ *and points* $z_1, \ldots, z_t$ *on the Riemann sphere. Then there is an* nth *order homogeneous linear ordinary differential equation of* Fuchsian type *whose singularities are at* $z_1, \ldots, z_t$ *and whose monodromy matrices along a set of curves* l_i ($i = 1, \ldots, t$) *satisfying* (i), (ii), *and* (iii) *are* m_i ($i = 1, \ldots, t$).

We recall that a differential equation is said to be of *Fuchsian type* if each of its singular points z_i is a regular singular point. It follows that each solution of the differential equation approaches a limit as z approaches z_i in any sector formed by rays intersecting at z_i.

Next, we recall that a differential field E obtained from $\mathbf{C}(z)$ by adjunction of n linearly independent solutions $w_1, \ldots, w_n$ of (*) is called a *Picard-Vessiot extension* of $\mathbf{C}(z)$. The elements of E are quotients of polynomials in the w_i, the derivatives of the w_i, and z; and the automorphisms of E which commute with differentiation and which leave each element of $\mathbf{C}(z)$ fixed comprise the *differential Galois Group* G of $E/\mathbf{C}(z)$. Clearly, $G \subset GL(n, \mathbf{C})$; and it is a standard result ([5], [8]) that, in fact, G is an algebraic group.

Of course, each element of E can be represented uniquely by a power series solution of (*) at z_0. Since analytic continuation commutes with algebraic operations and with differentiation, we see that each element of the monodromy group M defines a differential automorphism of E. Because each element of $\mathbf{C}(z)$ is single valued, it is invariant under the action of M; it follows that M is a subgroup of G. In case (*) is of Fuchsian type, we have:

PROPOSITION III. *If* (*) *is of Fuchsian type, then the Zariski closure of M is G.*

Proof. Let F denote the subfield of E fixed by M. According to differential Galois theory ([5], [8]), $\overline{M}$ is the subgroup of G which fixes F. Thus the Proposition will be proved if we show that $F = \mathbf{C}(z)$.

Now, suppose $f(z)$ is an element of E fixed by each element of M. It follows that $f(z)$ is a single valued analytic function on the z-sphere whose singularities belong to the set $S = \{z_1, \ldots, z_t\}$ of singular points of (*). Since each z_i is a regular singular point, $f(z)$ approaches a limit as z approaches z_i. Consequently, $f(z)$ has no essential singularities, so it must be meromorphic on the z-sphere and, therefore, a rational function of z.

We note that Proposition III may fail when (*) is not of Fuchsian type. For example, the monodromy group of the equation $w' = w$ is trivial because the solution $w = e^z$ is single valued, but the Galois group of this equation is the multiplicative group of $\mathbf{C}$.

Acknowledgment. In the course of writing this paper we received valuable advice from many mathematicians. In particular, we would like to express our warm thanks to A. Adler, L. Goldman, I. Kaplansky, E. Kolchin, J. Kovacic, M. Kuga, J-P Serre, and M. F. Singer.

INSTITUTE FOR DEFENSE ANALYSIS
AND
PRINCETON UNIVERSITY

REFERENCES

[1] Curtis, C. and Reiner, I., *Representation Theory of Finite Groups and Associative Algebras*, Wiley-Interscience, New York, 1962

[2] Dixon, J. D., *The Structure of Linear Groups*, Van Nostrand Reinhold, London, 1971

[3] Hilbert, D., *Grundzuge Einer Allgemeinen Theorie der Linearen Integralgleichungen*, Chelsea Reprint, New York, 1953

[4] Humphreys, J. E., *Linear Algebraic Groups*, Springer-Verlag, New York, 1975

[5] Kaplansky, I., *An Introduction to Differential Algebra*, Hermann, Paris, 1957

[6] Katz, N., "An Overview of Deligne's Work on Hilbert's Twenty-First Problem," *Mathematical Developments Arising From Hilbert Problems*, American Mathematical Society, Providence, 1976

[7] Kolchin, E., "Some Problems in Differential Algebra," *Proc. Intl. Congress of Mathematicians* (Moscow, 1966), Mir, Moscow, 1968

[8] Kolchin, E., *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973

[9] Kovacic, J., "On the Inverse Problem in the Galois Theory of Differential Fields, I and II, *Annals of Math.*, **89**, pp. 583-608 (1969) and **93**, pp. 269-284 (1971)

[10] Kuga, M., *Galois No Yume* ("Galois' Dream", in Japanese) 1968

[11] Plemelj, J., *Problems in the Sense of Riemann and Klein*, Wiley-Interscience, New York, 1964

[12] Schlesinger, L., *Handbuch der Theorie der Linearen Differentialgleichungen*, Zweiter Band, Leipzig, 1897, Johnson Reprint, New York, 1968