ON THE INVERSE PROBLEM OF GALOIS THEORY OF DIFFERENTIAL FIELDS

A. BIALYNICKI-BIRULA

0. One can ask what algebraic groups are isomorphic to groups of automorphism of strongly normal extensions of a fixed ordinary differential field (see [2]). The purpose of the note is to give a contribution in this direction. We shall prove the following theorem.

THEOREM. *Let $\mathfrak{F}$ be an ordinary differential field with algebraically closed field of constants C and suppose that $\mathfrak{F}$ is of finite transcendence degree over C but is different from C. Let G be a connected nilpotent affine algebraic group defined over C. Then there exists a strongly normal extension $\mathcal{E}$ of $\mathfrak{F}$ such that the Galois group $\mathcal{G}(\mathcal{E}/\mathfrak{F})$ is isomorphic to $G(C)$.*

1. All fields considered here are of characteristic 0. Let F be a field, let C be an algebraically closed subfield of F. Let G be a connected algebraic group defined over C. $F(G)$ denotes the field of all rational functions on G defined over F. If $g \in G$ then $F(g)$ denotes the field generated by g over F. We shall say that a derivation of $F(G)$ commutes with $G^*(C)$ if it commutes with g^*, for every $g \in G(C)$, where g^* denotes the automorphism of $F(G)$ induced by the left translation by g, i.e., $(g^*f)(x) = f(gx)$, for any $x \in G$. $\mathfrak{G}_F$ denotes the Lie algebra of all derivations of $F(G)$ that are zero on F and which commute with $G^*(F)$. If G_1 is a normal subgroup of G defined over F then $F(G/G_1)$ is canonically isomorphic to a subfield of $F(G)$; we shall identify $F(G/G_1)$ and this subfield.

If R is an integral domain then (R) denotes the field of fractions of R. Every derivation d of R can be uniquely extended to a derivation of R (the extended derivation will be also denoted by d). If F_1, F_2 are two fields containing F as a subfield and if d_1, d_2 are derivations of F_1, F_2, respectively, such that $d_1|F = d_2|F$ and $d_1(F) \subset F$ then $d_1 \otimes d_2$ denotes the derivation of $F_1 \otimes_F F_2$ determined by $(d_1 \otimes d_2)(a \otimes b) = d_1(a) \otimes b + a \otimes d_2(b)$, for every $a \in F_1$ and $b \in F_2$.

d_0 denotes the zero derivation of a field (it will be always clear what field we have in mind). The underlying field of an ordinary differential field $\mathfrak{F}$ will be denoted by F.

2. LEMMA 1. *If d_1 belongs to the center of $\mathfrak{G}_C$ then the derivation $d_1 \otimes d_0$ of $(C(G) \otimes F)$ $(=F(G))$ commutes with every derivation d of $F(G)$ such that $d(F) \subset F$ and $dg^* = g^*d$ for every $g \in G(C)$.*

Received by the editors June 12, 1963.

PROOF. Let d be as in the lemma. Then $d-d_0\otimes(d|F)$ is zero on F and commutes with $G^*(F)$ and so $d-d_0\otimes(d|F)\in\mathfrak{G}_F$. But $d_1\otimes d_0$ belongs to the center of $\mathfrak{G}_F$ and commutes with $d_0\otimes(d|F)$. Thus $d_1\otimes d_0$ commutes with $d=d-d_0\otimes(d|F)+d_0\otimes(d|F)$.

LEMMA 2. *Let G_1 be a normal subgroup of G defined over C and let d^0 be a derivation of $F(G/G_1)$ such that $d^0(C)=0$ and d^0 commutes with any element from $(G/G_1)^*(C)$. Then there exists an extension d' of d^0 to a derivation of $F(G)$ that commutes with $G^*(C)$.*

PROOF. Let g be a generic point of G over $F(G)$. Extend d^0 to a derivation d_1 of $F(G)$ and let d_2 be the extension of d_1 to a derivation of $F(g)(G)$ which is trivial on $C(g)$. Let V be a nonempty affine open subset of G defined over C and let $C[x_1, \cdots, x_n]$ be the coordinate ring of V over C. Then there exists $h_0\in V(C)$ such that $d_1x_1, \cdots, d_1x_n$ are defined at h_0. Hence, if $a\in F(g)(G)$ is defined at h_0 then $d_2(a)$ is also defined at h_0. In particular, for any $a\in F(G)$, $d_2((gh_0^{-1})^*a)$ is defined at h_0 (since $((gh_0^{-1})^*a)(h_0)=a(g)$). Let, for any $a\in F(G)$, $d'(a)$ be the element of $F(G)$ such that $d'(a)(g)=d_2((gh_0^{-1})^*a)(h_0)$. One can easily see that the definition of d' does not depend on g. In particular, if g_1 is any point of G such that $C(g_1)=C(g)$, then g_1 is generic for G over F and so $d'(a)(g_1)=d_2((g_1h_0^{-1})^*a)(h_0)$. Hence, for any $h\in G(C)$ $(h^*d'(a))(g) = d'(a)(hg) = d_2((hgh_0^{-1})^*a)(h_0) = d_2((gh_0^{-1})^*h^*a)(h_0)$ $=d'(h^*a)(g)$, since $C(hg)=C(g)$. Thus $d_1h^*=h^*d_1$, i.e., d_1 commutes with $G(C)^*$. Moreover, d' is a derivation of $F(G)$. Indeed

$$\begin{aligned} d'(a+b)(g) & \\ &= d_2((gh_0^{-1})^*(a+b))(h_0) = d_2((gh_0^{-1})^*a)(h_0) + d_2((gh_0^{-1})b)(h_0) \\ &= d'(a)(g) + d'(b)(g) \end{aligned}$$

and

$$\begin{aligned} d'(ab)(g) &= d_2((gh_0^{-1})^*ab)(h_0) \\ &= d_2((gh_0^{-1})^*a)(h_0)\cdot(gh_0^{-1})^*b(h_0) + (gh_0^{-1})^*a(h_0)\cdot d_2((gh_0^{-1})^*b)(h_0) \\ &= d'(a)(g)\cdot b(g) + a(g)\cdot d'(b)(g). \end{aligned}$$

Finally, if $a\in F(G/G_1)$ then

$$\begin{aligned} d'(a)(g) &= d_2((gh_0^{-1})^*a)(h_0) = d^0((gh_0^{-1})^*a)(h_0) \\ &= (gh_0^{-1})^*d^0(a)(h_0) = d^0(a)(g), \end{aligned}$$

i.e., d' is an extension of d^0. This completes the proof of the lemma.

LEMMA 3. *Let G_1 be a connected central one-dimensional normal sub-*

group of an affine connected algebraic group G, both defined over F. Let $d_1 \in \mathfrak{G}_F$ be a derivation in the direction of G_1. Then, for any $a \in F(G)$, $d_1(a)=0$ if and only if $a \in F(G/G_1)$. Moreover, there exists an element $b \in F(G)-F(G/G_1)$ such that either $d_1(b)=c\cdot b$ or $d_1(b)=c$, where c is an element from $F(G/G_1)$.

PROOF. The first part of the lemma is well known. Let b' be a regular function on G such that $b' \in F(G)-F(G/G_1)$. Then $G_1^*(F)\cdot b'$ generates a finite-dimensional F-vector space. Since G_1 is one-dimensional and connected, hence we may assume that this space is either one-dimensional or two-dimensional with basis b_0, b', where $b_0 \in F(G/G_1)$ and $g^*(b')=\alpha(g)b_0+b'$, $\alpha \in F(G/G_1)$ and $\alpha(g)\neq 0$ if $g \neq$ identity e of G_1. Then it follows from Lemma 7 [1] that in the first case $d_1(b')=cb'$, where c is an element from $F(G/G_1)$ and we may take $b=b'$. In the second case (again by Lemma 7 [1]) $c_1d_1^2(b')+c_2d_1(b')+c_3b'=0$, for some c_1, c_2, $c_3 \in F(G/G_1)$ which do not vanish simultaneously. Then $0 = g^*(c_1d_1^2(b')+c_2d_1(b')+c_3b') = c_1d_1^2(b')+c_2d_1(b')+c_3(\alpha(g)b_0+b')$, for every $g \in G_1(F)$. Hence $c_3=0$ and $c_1\neq 0$. If $c_2\neq 0$, then $d_1(d_1(b'))=-c_2/c_1$, $d_1(b')\neq 0$, and we take $b=d_1(b')$. If $c_2=0$, then $d_1^2(b')=0$. Hence $d_1(b')\in F(G/G_1)$, and we take $b=b'$.

LEMMA 4. *Let $\mathfrak{F}$ be an ordinary differential field with derivation d, let C be the field of constants of $\mathfrak{F}$ and suppose that $\mathfrak{F}$ is of finite transcendence degree over C. Let $\mathfrak{F}_1$ be a (differential) subfield of $\mathfrak{F}$ which is not contained in C and let $c \in C$. Then there exist a_1, $a_2 \in \mathfrak{F}_1$, $a_1\neq 0\neq a_2$, such that there is no element $y \in \mathfrak{F}-C$ which satisfies either $dy=a_1\cdot c$ or $dy=a_2cy$.*

PROOF. We may suppose that $\mathfrak{F}_1$ contains an element x such that $dx=1$ (let $x\in\mathfrak{F}_1-C$; then $dx\neq 0$ and we may replace d by $1/dx\cdot d$). If $dy_n=c/(x+n)$, $y_n\in\mathfrak{F}-C$, where n is an integer, then, one can prove that the elements y_i, for different integers i, are algebraically independent over C. Similarly, if $dz_n=x^ncz_n$, then the elements z_i, for different integers i, are also algebraically independent over C. Hence F contains only a finite number of elements y_i and z_i. Thus, for some n, y_n, $z_n \notin \mathfrak{F}$ and the lemma is proved.

3. **Proof of the theorem.** Let d be the nonzero derivation of $\mathfrak{F}$. We shall show that one can extend d to a derivation d^* of $F(G)$ which commutes with $G^*(C)$ and has C as the field of constants. Proof by induction on the dimension of G.

If $\dim G=0$, then this is trivial.

Suppose that the above is true for connected nilpotent affine groups of dimension n and let $\dim G=n+1$. There exists a central connected normal subgroup G_1 of G defined over C and of dimension 1. Then G/G_1 is an affine nilpotent connected group of dimension n. Hence there exists an extension d^0 of d to a derivation of $F(G/G_1)$ such that C is the field of constants of d^0 and d^0 commutes with $(G/G_1)^*(C)$. It follows from Lemma 2 that d^0 can be extended to a derivation d' of $F(G)$ that commutes with $G^*(C)$. Let $d_1 \in \mathfrak{G}_F$ be a derivation of $F(G)$ in the direction of G_1. Then the field of constants of d_1 is $F(G/G_1)$ and it follows from Lemma 1 that d_1 commutes with every derivation ad', where $a \in F$. Therefore the set of all $b \in F(G)$, for which $d_1(b) = ad'(b)$, where a is fixed, is a subfield F_a of $F(G)$ closed under d_1 (and ad'). Indeed, it is easy to see that this is a field. Moreover, if $d_1(b) = ad'(b)$, then $d_1(d_1(b)) = d_1(ad'(b)) = ad'(d_1(b))$. C is the field of constants of $d_1 | F_a$ for $a \neq 0$, since the field of constants of d_1 is $F(G/G_1)$ and the field of constants of $ad' | F(G/G_1)$ is C. And we want to prove that $F_a = C$, for some $a \in F$. Let $a \in F$; consider the ordinary differential field $(F(G) \otimes_c F(G/G_1))$ together with the derivation $ad' \otimes d_0$ and the algebraic closure $(F(G) \otimes_c F(G/G_1))^*$ of $(F(G) \otimes_c F(G/G_1))$ with the unique extension $(ad' \otimes d_0)^*$ of $(ad' \otimes d_0)$. F_a is linearly disjoint from $F(G/G_1)$ over C since $F(G/G_1)$ is the field of constants of d_1 and C is the field of constants of $d_1 | F_a$ (see Proposition 1 in [3] or Lemma 1 in [1]). Hence there exists a subfield of $F(G)$ with d_1 which is canonically isomorphic to $(F_a \otimes_c F(G/G_1))$ with $(ad' | F_a) \otimes d_0$. $F(G)$ is an algebraic extension of the subfield unless $F_a = C$ and this isomorphism maps b onto $1 \otimes b$, for every $b \in F(G/G_1)$. Therefore $F_a \neq C$ implies that there exists an isomorphism α_a of $F(G)$ with d_1 into $(F(G)) \otimes_c F(G/G_1))^*$ with $(ad' \otimes d_0)^*$ such that $\alpha_a(b) = 1 \otimes b$, for every $b \in F(G/G_1)$. It follows from Lemma 3 that there exist elements $c \in F(G/G_1)$ and $y \in F(G) - F(G/G_1)$ such that either $d_1 y = c$ or $d_1 y = cy$. Therefore, for every $a \in G$, $a \neq 0$ for which $F_a \neq C$, we have that either $(ad' \otimes d_0)^* \alpha_a(y) = 1 \otimes c$ or $(ad' \otimes d_0)^* \alpha_a(y) = (1 \otimes c)\alpha_a(y)$, i.e., either $(d' \otimes d_0)^* \alpha_a(y) = 1 \otimes c/a \otimes 1$ or $(d' \otimes d_0)^* \alpha_a(y) = 1 \otimes c/a \otimes 1 \ \alpha_a(y)$. But it follows from Lemma 4 that there exist $a_1, a_2 \in F$ such that neither $(d' \otimes d_0)^* z = 1 \otimes c/a_1 \otimes 1$ nor $(d' \otimes d_0)^* z = (1 \otimes c/a_2 \otimes 1)z$ has a solution z in $(F(G) \otimes F(G/G_1))^*$. Then $a_1 \neq 0 \neq a_2$ and either $F_{a_1} = C$ or $F_{a_2} = C$. If $F_a = C$, then $a \neq 0$ and the field of constants of $d^* = (1/a)d_1 - d'$ is C. Moreover, d^* commutes with $G^*(C)$. Thus we have proved by induction that there exists an extension d^* of d that commutes with $G^*(C)$ and has C as the field of constants.

Now if d^* is such a derivation then $F(G)$ with d^* is a strongly normal extension of $\mathfrak{F}$ and $G(C)$ is the Galois group of the extension (see Proposition 1 and Theorem 1 in [1]).

REFERENCES

1. A. Bialynicki-Birula, *On Galois theory of fields with operators*, Amer. J. Math. 84 (1962), 89–109.

2. E. R. Kolchin, *Galois theory of differential fields*, Amer. J. Math. 75 (1953), 753–824.

3. ———, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. (2) 49 (1948), 1–42.

UNIVERSITY OF CALIFORNIA, BERKELEY AND
INSTITUTE OF MATHEMATICS, P.A.N., POLAND

ON A REALIZATION OF A COMPLEMENTED ALGEBRA

PARFENY P. SAWOROTNOW

In this note we intend to show that each simple complemented algebra is isomorphic to an algebra described in the example below (as in [6] we use the term "simple" to mean "simple and semisimple"). This paper can be considered as a continuation of [5] and [6].

In the example below (and in the proof of the theorem after it) we use terms "summable" and "integrable" in the sense defined in Chapter III of [3].

EXAMPLE. Let (S, μ) be a measure space. Let $K(s)$ be a real-valued function defined on S and having the following properties:

(i) $K(s)$ is finite almost everywhere,

(ii) there exists a positive number a such that $a \leqq K(s)$ for each $s \in S$,

(iii) the restriction of $K(s)$ to any summable subset of S is integrable (in particular $K(s)$ may be integrable).

Let A be the set of all complex-valued members x of $L^2(S\times S, \mu\times\mu)$ such that $\int\int|x(t, s)|^2K(s)dtds$ is finite. Then A is a complemented algebra in the scalar product $(x, y) = \int\int x(t, s)\bar{y}(t, s)K(s)\, dtds$ and the multiplication $(xy)(t, s) = \int x(t, r)y(r, s)dr$ (we consider pointwise addition and pointwise multiplication with a scalar). If $K(s)$ is bounded above then A is well complemented. Condition (ii) implies continuity of the multiplication (in both factors simultaneously); if $a = 1$ then $\|xy\| \leq \|x\| \, \|y\|$.

Presented to the Society, August 24, 1956, under the title *Diagonalization of a complemented algebra*; received by the editors July 15, 1963.