A NOTE ON THE GALOIS THEORY OF LINEAR HOMOGENEOUS DIFFERENCE EQUATIONS

CHARLES H. FRANKE

1. **Introduction.** We assume the following throughout. K is an inversive difference field of characteristic zero. f is a linear homogeneous difference equation of effective order n with coefficients in K. $\alpha=(\alpha^{(1)}, \cdots, \alpha^{(n)})$ is a fundamental system for f and $M=K\langle\alpha\rangle$. C is the subfield of M of constants, that is, solutions to $y_1=y$. K_M is the algebraic closure of $K(C)$ in M.

M is a normal extension of K if for each $z\in(M-K)$ there is a difference automorphism σ of M/K with $\sigma(z)\neq z$. The purpose of this note is to prove the following theorem.

THEOREM. *If $K=K_M$ then M is a normal extension of K.*

This result is of importance in several places in the Galois theory for linear homogeneous difference equations. Theorem 4 of [**3**] can now be stated in the following form.

Assume $K=K_M$ and G is the full Galois group of M/K. Then there is a one-to-one correspondence between connected algebraic subgroups of G and intermediate fields which are algebraically closed in M.

If we define f to be solvable in M by elementary operations over K if and only if M is contained in a qLE of K, [**4**, p. 241], then Theorems 2.1 and 2.2 of [**4**] can be combined and restated as follows.

f is solvable in M by elementary operations over K if and only if the Galois group of M/K_M is solvable.

2. **Preliminaries.** The following notation is used in the proof. $y=(y^{(1)}, \cdots, y^{(n)})$ is a vector of transformal indeterminates. $x=(x^{(i,j)})$ is an $n\times n$ matrix of ordinary algebraic indeterminates. If R is a difference ring then $R[x]$ denotes the difference over-ring of R in which the $x^{(i,j)}$ are constant. If L is a field then $V(L)$ denotes the set of nonsingular $n\times n$ matrices over L. If H is an algebraic matrix group with elements in $V(L)$ then dim H denotes the dimension of the ideal of polynomials in $L[x]$ vanishing on the component of the identity of H.

The term "algebraic automorphism" will be used to mean "an automorphism which is not necessarily a difference automorphism."

The proof uses the following lemma [**2**, Lemma 1, p. 530].

Received by the editors March 28, 1966.

LEMMA. *Assume that L is a field of characteristic zero and $\bar{L}$ is an algebraic closure of L. If H is an irreducible algebraic matrix group in $V(\bar{L})$ which is defined by a set of polynomials in $L[x]$ and $G=H\cap V(L)$ then* $\dim G=\dim H$.

3. Proof of the Theorem. Define G to be the transformal Galois group of M/K. We will show first that it is sufficient to prove that G is an algebraic matrix group and that $\dim G=\text{t.d.}(M, K)$. Assume that z is in the fixed field of G and L is the algebraic closure in M of $K\langle z\rangle$. Then L is in the fixed field of G_1, the component of the identity of G. Therefore G_1 is contained in the Galois group of M/L. Since $\dim G=\dim G_1$, $\text{t.d.}(M, K)=\text{t.d.}(M, L)$. Therefore $z\in K$, and M is a normal extension of K.

Define B as the prime reflexive ideal in $K\{y\}$ with generic zero α. Define a difference homomorphism F from $K\{y\}$ to $M[x]$ by $F(y^{(i)})=\sum x^{(i,j)}\alpha^{(j)}$. Define $J\subset M[x]$ as the image of B under F. Fix a vector space basis v of M/C. Define S to be the set of all $R^{(k)}\in C[x]$ which appear when each $I\in J$ is written in the form $I=\sum R^{(k)}v^{(k)}$. Define $\bar{S}$ as the ideal generated by S in $C[x]$.

G may be considered as a matrix group by assigning the matrix $(k^{(i,j)})$ to $\sigma\in G$ where $\sigma(\alpha^{(i)})=\sum k^{(i,j)}\alpha^{(j)}$. G is the set of solutions to $\bar{S}$ in $V(C)$ [**3**, Theorem 1]. $\bar{S}$ is prime and $\dim \bar{S}=\text{t.d.}(M, K)$ [**3**, Theorem 2].

Define P to be the subfield of M of all periodic elements of M. P is an algebraic extension of C so $P\subset K$. Choose an algebraic closure P^* of P. Since P is algebraically closed in K, P^* can be chosen compatible with K and with M. Since P^* is algebraic over K and K is algebraically closed in M, $K\langle P^*\rangle$ and M are linearly disjoint over K. Each periodic element of $M\langle P^*\rangle$ can be written uniquely in the form $q=\sum a^{(i)}p^{(i)}$ where $a^{(i)}\in M$ and p is a vector space basis of P^*/P. If j is a common period of q and the $p^{(i)}$ then $a_j^{(i)}=a^{(i)}$. Thus $a^{(i)}\in P$ and $q\in P^*$. Therefore, the set of periodic elements of $M\langle P^*\rangle$ is P^*.

Define $M^*=M\langle P^*\rangle$ and $K^*=K\langle P^*\rangle$. Define B^* to be the prime reflexive ideal in $K^*\{y\}$ with generic zero α. Extend F to $K^*\{y\}$ and define $J^*\subset M^*[x]$ as the image of B^* under F. Fix a vector space basis w of M^*/P^*. Define S^* to be the set of all $R^{(k)}\in P^*[x]$ which appear when each $I\in J^*$ is written in the form $I=\sum R^{(k)}w^{(k)}$. Define $\bar{S}^*$ as the ideal generated by S^* in $P^*[x]$.

Define H to be the set of all matrices $(p^{(i,j)})\in V(P^*)$ with the property that there is an algebraic automorphism A of M^*/K^* so that $A(\alpha_k^{(i)})=\sum p^{(i,j)}\alpha_k^{(j)}$. H is a group. We will show that H is an algebraic group defined by $\bar{S}^*$. Assume that $(p^{(i,j)})\in H$. The algebraic homomorphism of $K^*\{y\}$ to M^* defined by $y_k^{(i)} \to \alpha_k^{(i)} \to \sum p^{(i,j)}\alpha_k^{(j)}$ takes B^* to zero. Therefore, $(p^{(i,j)})$ is a solution to J^* and hence to $\bar{S}^*$. Conversely, if $(p^{(i,j)})$ is a solution to $\bar{S}^*$ in $V(P^*)$ then the algebraic homomorphism of $K^*\{y\}$ to M^* defined by $y_k^{(i)} \to \sum p^{(i,j)}\alpha_k^{(j)}$ sends B^* to zero. Therefore it induces an algebraic homomorphism A of $K^*\{\alpha\}$. Since the equations $A(\alpha_k^{(i)}) = \sum p^{(i,j)}\alpha_k^{(j)}$ can be solved for the $\alpha_k^{(j)}$, A is surjective. Since $K^*\{\alpha\}$ is an integral domain of finite transcendence degree over K^*, A is bijective [**6**, Lemma 5.3, p. 34]. By extending A to the quotient field of $K^*\{\alpha\}$ one obtains an element of H.

Next we will show that H is irreducible.

Since K^* is algebraically closed in M^* there is a generic zero β of B^* with $K^*\langle\beta\rangle$ and M^* linearly disjoint over K^*. Define B' to be the prime reflexive ideal in $M^*\{y\}$ with generic zero β. Extend F to $M^*\{y\}$ and define J' as the image of B' under F. Since the equations $F(y_k^{(i)}) = \sum x^{(i,j)}\alpha_k^{(j)}$ can be solved for the $x^{(i,j)}$, F is surjective. Define S' as the set of all $R^{(k)} \in P^*[x]$ which appear when each $I \in J'$ is written in the form $I = \sum R^{(k)}w^{(k)}$. Define $\bar{S}'$ as the ideal generated by S' in $P^*[x]$. Since $f(\beta^{(i)}) = 0$ there are constants $c^{(i,j)} \in M^*\langle\beta\rangle$ with $\beta^{(i)} = \sum c^{(i,j)}\alpha^{(j)}$. If $h \in M^*[x]$ and $h = F(g)$ for $g \in M^*\{y\}$ then $g(\beta^{(i)}) = h(c^{(i,j)})$. Therefore J' is a prime ideal with generic zero $c = (c^{(i,j)})$. Since the $w^{(j)}$ are linearly independent over the periodic elements of M^*, they are linearly independent over the periodic elements of any overfield of M^* [**5**, §3]. Therefore $\bar{S}'$ is a prime ideal with generic zero c.

If $D \in B'$ then we may write $D = \sum d^{(j)}u^{(j)}$ where $d^{(j)} \in K^*\{y\}$ and u is a vector space basis of M^*/K^*. Since $D(\beta) = 0$ and u is also a vector space basis of $M^*\langle\beta\rangle/K^*\langle\beta\rangle$, $d^{(j)}(\beta) = 0$ and $d^{(j)} \in B^*$. Therefore each $I \in J'$ can be written in the form $\sum I^{(j)}u^{(j)}$ with $I^{(j)} \in J^*$. Writing $I^{(j)} = \sum I^{(j,k)}w^{(k)}$, $I^{(j,k)} \in S^*$ we obtain

$$I = \sum I^{(j,k)}u^{(j)}w^{(k)}.$$

Finally we may write

$$u^{(j)}w^{(k)} = \sum p^{(j,k,l)}w^{(l)}, \qquad p^{(j,k,l)} \in P^*.$$

Thus,

$$I = \sum \sum p^{(j,k,l)}I^{(j,k)}w^{(l)}.$$

Therefore $S' \subset \bar{S}^*$, $\bar{S}^* = \bar{S}'$ and H is irreducible.

Next we will show that H is defined by $\bar{S}$.

Since $B \subset B^*$, β is a solution of B. Therefore c is a solution of J and hence of S. Therefore $\bar{S} \subset \bar{S}^*$, and H annuls $\bar{S}$.

Assume $p\in V(P^*)$ is a solution to $\bar{S}$. If ω is a vector space basis of K^*/K then each $D\in B^*$ can be written in the form $D=\sum d^{(j)}\omega^{(j)}$, $d^{(j)}\in K\{y\}$. Since ω is also a vector space basis of M^*/M, $d^{(j)}(\alpha)=0$ and $d^{(j)}\in B$. Therefore each $I\in J^*$ can be written in the form $I=\sum I^{(j)}\omega^{(j)}$, $I^{(j)}\in J$. Since p is a solution to S, p is a solution to J. Therefore, p is a solution to J^* and hence to $\bar{S}^*$. Thus $p\in H$ and H is the set of solutions to $\bar{S}$ in $V(P^*)$.

The hypotheses of the Lemma are satisfied and we obtain $\dim H=\dim(H\cap V(C))=\dim G$. Further, since P^* is algebraically closed, $\dim H=\dim \bar{S}^*$. Since c is a generic zero of $\bar{S}$, and P^* is an algebraic extension of C, t.d. $(M, K)=\dim \bar{S}=$ t.d. $(C(c), C)=$ t.d. $(P^*(c), P^*)=\dim \bar{S}^*$. Therefore $\dim G=$ t.d. (M, K), and the proof is complete.

References

1. R. Cohn, *Difference algebra*, Wiley, New York, 1965.

2. M. Epstein, *On the theory of Picard-Vessiot extensions*, Ann. of Math. **62** (1955), 528–547.

3. C. Franke, *Picard-Vessiot theory of linear homogeneous difference equations*, Trans. Amer. Math. Soc. **3** (1963), 491–515.

4. ———, *Solvability of linear homogeneous difference equations by elementary operations*, Proc. Amer. Math. Soc. **1** (1966), 240–246.

5. ———, *Reducible linear homogeneous difference equations*, (to appear).

6. I. Kaplanksy, *An introduction to differential algebra*, Hermann, Paris, 1957.

Seton Hall University

A NOTE ON ABSOLUTELY FREE ALGEBRAS

K.-H. DIENER AND G. GRÄTZER[1]

1. **Introduction.** A free algebra $\mathfrak{P}^{(\mathfrak{m})}(\tau)$ over the class $K(\tau)$ of *all* (universal) algebras of a fixed type τ is called an *absolutely free algebra*. The following is a simple characterization of absolutely free algebras.

THEOREM. *Let $\mathfrak{A}$ be an algebra of type τ, and let M be a generating set of $\mathfrak{A}$. Then the following two conditions are equivalent*:

(i) *$\mathfrak{A}$ is absolutely freely generated by M*;

(ii) *M is independent in every extension $\mathfrak{B}$ of $\mathfrak{A}$ with rank $\mathfrak{B}\leqq |M|$ and if there are nullary operations, then $\mathfrak{A}^c\cong\mathfrak{P}^{(0)}(\tau)$.*

Received by the editors May 10, 1966.

[1] Research supported by the National Science Foundation under grant number GP-4221.