JOURNAL OF ALGEBRA 25, 25–39 (1973)

The Structure of the Automorphism Group of Polynomial Rings

MARSHALL FRASER AND ADOLF MADER

Department of Mathematics, University of Hawaii, Honolulu, Hawaii 96822

Communicated by Saunders MacLane

Received July 13, 1971

1. INTRODUCTION

Let F be a field of characteristic 0, $R = F[X, Y]$. We investigate the structure of the group $\mathrm{aut}_F R$ of all automorphisms of R fixing F elementwise. The filtration $M = (X, Y) \supset M^2 \supset M^3 \supset \cdots$ of R induces a descending series $A_1 \supset A_2 \supset \cdots$ of normal subgroups of $\mathrm{aut}_F R$. In Section 2 we determine the structure of the quotients A_n/A_{n+1}. Each such group is isomorphic with a direct sum of $n + 3$ copies of the additive group of F. It was proved in [1] that the sequence $A_1 > A_2 > \cdots$ is a descending central series of A_1. We show in Section 3 that the series $A_1 > A_2 > \cdots$ is, in a sense, arbitrarily close to the lower central series of A_1, and we conjecture that equality holds. Similarly, the commutator subgroups A_n' can be shown to be arbitrarily close to A_{2n}. In Section 4 we consider the rings R^α of all polynomials left fixed by $1 \neq \alpha \in A_1$. We show that either $R^\alpha = F$ or $R^\alpha = F[f_0]$ for some nonconstant irreducible polynomial f_0. In our final Section 5 we collect a few additional observations and state some open questions.

The notation is standard. We consistently write maps on the right. The symbols D_X and D_Y denote formal partial differentiation with respect to X and Y, respectively.

2. THE STRUCTURE OF $\mathrm{Aut}_F F[X, Y]$

Let F be a field and consider $R = F[X, Y]$. The maximal ideal M generated by X and Y induces a filtration $R = M^0 \supsetneq M \supsetneq M^2 \supsetneq \cdots$. We denote by $\mathrm{aut}_F R$ the set of all (ring) automorphisms of R fixing F elementwise. Let $A_0 = \{\alpha \in \mathrm{aut}_F R : M\alpha \subset M\}$. Then A_0 is a subgroup of $\mathrm{aut}_F R$ and henceforth we confine our attention to A_0. We have $M^n A_0 \subset M^n$ for all n.

The maps $\varphi_n: A_0 \to \text{aut}_F\, M/M^{n+1}$ defined by $(f + M^{n+1})(\alpha\varphi_n) = f\alpha + M^{n+1}$ for $f \in R$, $\alpha \in A_0$, are group homomorphisms for each n. We define $A_n = \ker \varphi_n$. It is easy to see that $A_n = \{\alpha \in A_0: X\alpha - X \in M^{n+1}$ and $Y\alpha - Y \in M^{n+1}\}$, and $A_0 > A_1 > A_2 > \cdots$ is a descending series of normal subgroups of A_0 with $\bigcap_{n=1}^{\infty} A_n = \{1\}$.

The additive group of M is in a natural way a vector space over F and $\hom_F(M, M)$ has the structure of an F-algebra under the usual operations. If $\alpha \in A_0$ then the map $\xi = \alpha - 1$ is an element of $\hom_F(M, M)$.

LEMMA. *If $\alpha \in A_0$ and $\xi = \alpha - 1$ then for all $f, g \in M$,*

$$(fg)\xi = (f\xi)(g\xi) + f(g\xi) + (f\xi)g. \tag{2.1}$$

If $\alpha, \beta \in A_0$ and $\xi = \alpha - 1$, $\eta = \beta - 1$ then

$$\alpha\beta - 1 = \xi\eta + \xi + \eta. \tag{2.2}$$

$$A_n = \{\alpha \in A_0: M(\alpha - 1) \subset M^{n+1}\}. \tag{2.3}$$

If $\alpha_i \in A_{n_i}$ for $1 \leqslant i \leqslant s$, and $\xi_i = \alpha_i - 1$, then

$$M^k\xi_1 \cdots \xi_s \subset M^{k+n_1+n_2+\cdots+n_s} \qquad \text{for all } k. \tag{2.4}$$

The proof of the lemma is easy and left to the reader.

Let B be the subgroup of A_0 defined as

$$B = \{\alpha \in A_0: X\alpha = a_{11}X + a_{12}Y,\ Y\alpha = a_{21}X + a_{22}Y, \text{ and } \det(a_{ij}) \neq 0\}.$$

Then B is isomorphic to $GL(2, F)$ and $A_0 = B \cdot A_1$, the product being semidirect. Therefore we may fix our attention on the group A_1.

Now each M/M^n is a finite dimensional vector space over F under the operation $a(f + M^n) = af + M^n$. Let L_n^+ denote the additive group of $\hom_F(M/M^n, M/M^n)$. We examine the structure of A_n/A_m for $1 \leqslant n < m \leqslant 2n$ by looking at the map $A_n \to L_{m+1}^+$ defined by $\alpha \mapsto \overline{\alpha - 1}$ where $(f + M^{m+1})\,\overline{\alpha - 1} = f(\alpha - 1) + M^{m+1}$. This map is well defined by (2.4), a group homomorphism by (2.2)–(2.4), and has kernel A_m. This implies in particular that A_n/A_m is commutative for $1 \leqslant n < m \leqslant 2n$.

We use a certain class of automorphisms to study A_n/A_m. If $f \in F[Z]$ we define $\gamma \in A_1$ by

$$X\gamma = X + bf(aX + bY), \qquad Y\gamma = Y - af(aX + bY), \tag{2.5}$$

a and b being arbitrary elements of F. Then $(aX + bY)\gamma = aX + bY$ and

$$X\gamma^{-1} = X - bf(aX + bY), \qquad Y\gamma^{-1} = Y + af(aX + bY).$$

It is easy to see that any automorphism of the type (2.5) can be obtained from the automorphism $\alpha \in A_1$ with $X\alpha = X$, $Y\alpha = Y + f(X)$ by conjugation with an appropriate automorphism in B.

From now on we assume that $\operatorname{char} F = 0$.

We denote by C_n the subgroup of L^+_{n+2} generated by the images of all automorphisms of the type (2.5) under the natural injection $A_n/A_{n+1} \to L^+_{n+2}$.

PROPOSITION 2.6. *C_n is a subvector space of L^+_{n+2} of dimension $\geqslant n + 3$.*

Proof. Clearly C_n is a subvector space (and not merely a subgroup) of L^+_{n+2} since the f in (2.5) may be any element of the vector space $F[Z]$.

We produce $n + 3$ linearly independent functions in C_n. For $i = 1,..., n + 3$ consider γ_i of the type (2.5) defined by

$$X\gamma_i = X + b_i(a_iX + b_iY)^{n+1}, \qquad Y\gamma_i = Y - a_i(a_iX + b_iY)^{n+1},$$

the a_i, b_i still to be chosen. If we let $\xi_i = \gamma_i - 1$, then

$$X\xi_i = b_i(a_iX + b_iY)^{n+1}, \qquad Y\xi_i = -a_i(a_iX + b_iY)^{n+1}.$$

First choose $a_1 = 1$, $b_1 = 0$ and then choose $a_2 ,..., a_{n+3}$ any distinct elements of F and $b_i = 1$ for $i = 2,..., n + 3$. Suppose we have a dependency relation among the images of $\xi_1 , \xi_2 ,..., \xi_{n+3}$ in C_n. Lifting back to $\hom_F(M, M)$ we see that there exist $d_1 , d_2 ,..., d_{n+3} \in F$ so that

$$X(d_1\xi_1 + d_2\xi_2 + \cdots + d_{n+3}\xi_{n+3}) \in M^{n+2}, \tag{2.7}$$

and

$$Y(d_1\xi_1 + d_2\xi_2 + \cdots + d_{n+3}\xi_{n+3}) \in M^{n+2}. \tag{2.8}$$

From the definition of the ξ_i's we obtain from (2.7)

$$d_2(a_2X + Y)^{n+1} + \cdots + d_{n+3}(a_{n+3}X + Y)^{n+1} = 0.$$

By formal partial differentiation with respect to X we obtain

$$a_2d_2(a_2X + Y)^n + \cdots + a_{n+3}d_{n+3}(a_{n+3}X + Y)^n = 0.$$

We continue the partial differentiation with respect to X, and in each equation set $X = 0$, $Y = 1$. We obtain the system of equations

$$\begin{aligned} d_2 + \cdots + d_{n+3} &= 0, \\ a_2d_2 + \cdots + a_{n+3}d_{n+3} &= 0, \\ &\vdots \\ a_2^{n+1}d_2 + \cdots + a_{n+3}^{n+1}d_{n+3} &= 0. \end{aligned} \tag{2.9}$$

Since the determinant of coefficients is a Van der Monde determinant, we obtain $d_2 = \cdots = d_{n+3} = 0$. This together with (2.8) yields $d_1 = 0$. So the functions are independent, as asserted.

We wish to show now that C_n has dimension exactly $n + 3$. To this purpose, if α is an endomorphism of R define

$$\det \alpha = \det \begin{bmatrix} (X\alpha)\, D_X & (X\alpha)\, D_Y \\ (Y\alpha)\, D_X & (Y\alpha)\, D_Y \end{bmatrix}. \tag{2.10}$$

It is well known and easy to see that if α is an automorphism of R then $\det \alpha$ is a nonzero element of F. It is not known whether the converse is true. It fails for nonzero characteristic. Reference [3] is devoted to proving the converse for F the field of complex numbers. However, the referee informs us that, among experts, Engel's proof is not considered completely secured, and specifically he quotes p. 16, lines 9 to 11 as being incorrect as it stands.

THEOREM 2.11. *If F has characteristic 0 then the image of A_n/A_{n+1} under the natural injection $A_n/A_{n+1} \to L^+_{n+2}$ is a sub-vector space of dimension $n + 3$.*

Proof. Suppose $\alpha \in A_n$. By (2.3),

$$X\alpha = X + \sum_{i+j=n+1} a_{ij} X^i Y^j + \text{terms of degree} \geqslant n + 2,$$

$$Y\alpha = Y + \sum_{i+j=n+1} b_{ij} X^i Y^j + \text{terms of degree} \geqslant n + 2.$$

So

$$\det \alpha = 1 + \sum_{i+j=n+1} i a_{ij} X^{i-1} Y^j + \sum_{i+j=n+1} j b_{ij} X^i Y^{j-1} + \text{terms of degree} \geqslant n + 1$$

Since $\det \alpha$ is a nonzero element of F,

$$0 = \sum_{i+j=n+1} i a_{ij} X^{i-1} Y^j + \sum_{i+j=n+1} j b_{ij} X^i Y^{j-1} = \sum_{i+j=n} [(i+1)\, a_{i+1,j} + (j+1)\, b_{i,j+1}]\, X^i Y^j.$$

Thus

$$(i+1) a_{i+1,j} + (j+1) b_{i,j+1} = 0 \qquad \text{for} \quad i + j = n,\ 0 \leqslant i, j \leqslant n. \tag{2.12}$$

For $\alpha \in A_n$ its image $\overline{\alpha - 1} \in L^+_{n+2}$ is determined by the equations

$$\overline{X}(\overline{\alpha - 1}) = \sum_{i+j=n+1} a_{ij} \overline{X}^i \overline{Y}^j, \qquad \overline{Y}(\overline{\alpha - 1}) = \sum_{i+j=n+1} b_{ij} \overline{X}^i \overline{Y}^j.$$

Let F^{n+3} be the vector space of $(n+3)$-tuples over F. Define

$$\overline{\alpha - 1} \mapsto (a_{n+1\,0}, a_{n\,1}, \ldots, a_{0\,n+1}, b_{n+1\,0}).$$

It is easily checked that this is a homomorphism from the image of A_n/A_{n+1} in L^+_{n+2} to F^{n+3}. By (2.12) the map is a monomorphism. This shows the image of A_n/A_{n+1} in L^+_{n+2} generates a subvector space of dimension at most $n+3$. Since the image contains C_n, (2.6) shows it must be a subvector space of L^+_{n+2} of dimension $n+3$.

COROLLARY 2.13. *A_n/A_m, $1 \leqslant n < m \leqslant 2n$, is isomorphic with the additive group of a vector space over F of dimension $(m-n)(m+n+5)/2$.*

Proof. We induct on m for $m \geqslant n+1$. For $m = n+1$ the corollary coincides with (2.11). Consider the exact sequence

$$1 \to A_m/A_{m+1} \to A_n/A_{m+1} \to A_n/A_m \to 1.$$

Here A_n/A_{m+1} is known to be abelian for $m+1 \leqslant 2n$, and $A_m/A_{m+1} \cong F^+ \oplus \cdots \oplus F^+$ ($m+3$ copies). Since $\operatorname{char} F = 0$, A_m/A_{m+1} is divisible and hence $A_n/A_{m+1} \cong (A_m/A_{m+1}) \oplus (A_n/A_m)$. By induction hypothesis, A_n/A_m is isomorphic to the direct sum of $(m-n)(m+n+5)/2$ copies of F^+, hence A_n/A_{m+1} is isomorphic to the direct sum of

$$(m-n)(m+n+5)/2 + (m+3) = (m+1-n)(m+1+n+5)/2$$

copies of F^+. This proves the corollary.

COROLLARY 2.14. *A_m is torsion free for all m.*

This is true since A_n/A_{n+1} is torsion free and $\bigcap A_n = 1$.

3. CENTRAL SERIES

It was proved in [1] that the sequence $A_1 > A_2 > \cdots$ is a descending central series of A_1. We suspect that in fact $\{A_n\}$ is the lower central series of A_1, i.e., $A_{n+1} = [A_1, A_n]$, and that $A_{2n} = A_n'$. We are able to show that $[A_1, A_n]$ is arbitrarily close to A_{n+1}, and that A_n' is arbitrarily close to A_{2n} in a certain sense. Specifically we shall show that $A_{n+1} = [A_1, A_n] \cdot A_m$ for all $m \geqslant n+1$ and that $A_{2n} = A_n' \cdot A_m$ for all $m \geqslant 2n$.

For $\alpha \in A_1$ let $\xi_\alpha = \alpha - 1$. As usual $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ and we put $[\xi_\alpha, \xi_\beta] = \xi_\alpha\xi_\beta - \xi_\beta\xi_\alpha$.

LEMMA 3.1. *For* $\alpha, \beta \in A_1$, $\xi_{[\alpha,\beta]} = [\xi_\alpha, \xi_\beta] + \xi_{[\alpha^{-1},\beta^{-1}]}[\xi_\alpha, \xi_\beta]$.

Proof. Easy calculation.

PROPOSITION 3.2. $[A_n, A_m] \subset A_{n+m}$.

Proof. Combine (3.1), (2.4) and (2.3).

This says already that $\{A_n\}$ is a descending central series. We wish to show next that $A_{n+m} = [A_n, A_m]A_{n+m+1}$. This follows immediately from $A_{n+m}/A_{n+m+1} = [A_n, A_m]A_{n+m+1}/A_{n+m+1}$, and this latter equality is obtained by showing that these groups have equal images under the natural injection into L^+_{n+m+2}. Since the image of A_{n+m}/A_{n+m+1} is known to be a subvector space of L^+_{n+m+2} of dimension $n + m + 3$ (Theorem 2.11), we need to produce $n + m + 3$ commutators whose images in L^+_{n+m+2} are linearly independent. Several facts will be needed. Let ${}_t\alpha_0 \in A_t$ be the map defined by $X_t\alpha_0 = X$, $Y_t\alpha_0 = Y + X^{t+1}$. Put ${}_t\xi_0 = {}_t\alpha_0 - 1$.

LEMMA 3.3. $X^{r-s}Y^s{}_t\xi_0 - sX^{t+1+r-s}Y^{s-1} \in M^{r+2t}$ *for* $1 \leqslant r$, $0 \leqslant s \leqslant r$.

Proof. Put $\xi = {}_t\xi_0$. Induct on r. For $r = 1$, the claim follows from $X\xi = 0$, $Y\xi = X^{t+1}$. If $s \leqslant r$ then, using (2.1) and (2.4),

$$\begin{aligned} X^{r+1-s}Y^s\xi &= (X\xi)(X^{r-s}Y^s)\xi + X(X^{r-s}Y^s)\xi + (X\xi)(X^{r-s}Y^s) \\ &= X(X^{r-s}Y^s)\xi, \end{aligned}$$

and

$$\begin{aligned} &X^{r+1-s}Y^s\xi - sX^{t+1+r+1-s}Y^{s-1} \\ &\quad = X((X^{r-s}Y^s)\xi - sX^{t+1+r-s}Y^{s-1}) \in M^{1+r+2t} \text{ by induction hypothesis.} \end{aligned}$$

Finally,

$$Y^{r+1}\xi = (Y\xi)(Y^r\xi) + (Y\xi)Y^r + Y(Y^r\xi) = X^{t+1}(Y^r\xi) + X^{t+1}Y^r + Y(Y^r\xi),$$

and

$$\begin{aligned} &Y^{r+1}\xi - (r+1)X^{t+1}Y^r \\ &\quad = X^{t+1}(Y^r\xi) + Y(Y^r\xi - rX^{t+1}Y^{r-1}) \in M^{t+1+r+t} + M^{1+r+2t} \subset M^{(r+1)+2t}, \end{aligned}$$

by (2.4) and induction hypothesis.

LEMMA 3.4. $M^r({}_t\xi_0 - D_YX^{t+1}) \subset M^{r+2t}$.

Proof. Both ${}_t\xi_0$ and D_YX^{t+1} are linear transformations of M, and by (3.3) the claim is true for monomials.

LEMMA 3.5. *Let* $\alpha \in A_t$ *be the map given by* $X\alpha = X + (aX + Y)^{t+1}$, $Y\alpha = Y - a(aX + Y)^{t+1}$. *Put* $\xi = \alpha - 1$. *Then*

$$M^r(\xi - (D_X - aD_Y)(aX + Y)^{t+1}) \subset M^{r+2t}.$$

Proof. Let $\tau \in A_0$ be the map with $X\tau = aX + Y$, $Y\tau = X$. Then $X\tau^{-1} = Y$, $Y\tau^{-1} = X - aY$, $\alpha = \tau^{-1}{}_t\alpha_0\tau$ and $\xi = \tau^{-1}{}_t\xi_0\tau$. Now, for all $f \in M$,

$$f\tau^{-1}D_Y X^{t+1}\tau = f(Y, X - aY)\, D_Y\tau(aX + Y)^{t+1} = f(D_X - aD_Y)(aX + Y)^{t+1}.$$

Thus $M^r(\xi - (D_X - aD_Y)(aX + Y)^{t+1}) = M^r\tau^{-1}({}_t\xi_0 - D_Y X^{t+1})\tau \subset M^{r+2t}$ by (3.4).

LEMMA 3.6. *Let* ξ, ξ', η, η' *be linear transformations on* M *to* M *such that*

$$M^r\xi \subset M^{r+n}, \qquad M^r\xi' \subset M^{r+n}, \qquad M^r(\xi - \xi') \subset M^{r+2n};$$
$$M^r\eta \subset M^{r+m}, \qquad M^r\eta' \subset M^{r+m}, \qquad M^r(\eta - \eta') \subset M^{r+2m}.$$

Then $M^r([\xi, \eta] - [\xi', \eta']) \subset M^{(r+1)+n+m} \subset M^{n+m+2}$.

Proof.

$$\begin{aligned}[\xi, \eta] - [\xi', \eta'] &= \xi\eta - \eta\xi - \xi'\eta' + \eta'\xi' \\ &= \xi(\eta - \eta') + (\xi - \xi')\eta' + (\eta' - \eta)\xi - \eta'(\xi - \xi').\end{aligned}$$

Thus

$$\begin{aligned}M^r([\xi, \eta] - [\xi', \eta']) &\subset M^{r+n+2m} + M^{r+2n+m} + M^{r+2m+n} + M^{r+m+2n} \\ &\subset M^{(r+1)+n+m} \subset M^{n+m+2}.\end{aligned}$$

LEMMA 3.7. *Let* $\alpha \in A_n$ *be the map with* $X\alpha = X + (aX + Y)^{n+1}$, $Y\alpha = Y - a(aX + Y)^{n+1}$, *and let* $\beta \in A_m$ *be the map with*

$$X\beta = X + (bX + Y)^{m+1}, \qquad Y\beta = Y - b(bX + Y)^{m+1}.$$

Put $\alpha_0 = {}_n\alpha_0$. *Then*

$$M^r(\xi_{[\alpha,\beta]} - [(D_X - aD_Y)(aX + Y)^{n+1}, (D_X - bD_Y)(bX + Y)^{m+1}]) \subset M^{n+m+2},$$

and

$$M^r(\xi_{[\alpha_0,\beta]} - [D_Y X^{n+1}, (D_X - bD_Y)(bX + Y)^{m+1}]) \subset M^{n+m+2}.$$

Proof. Combine (3.5) with (3.6), and (3.4) with (3.6).

We are now ready to prove the essential result.

THEOREM 3.8. $A_{n+m} = [A_n, A_m] \cdot A_{n+m+1}$.

Proof. Consider $\alpha_0 = {}_n\alpha_0$, $\alpha_1, \ldots, \alpha_{n+2} \in A_n$ where

$$X\alpha_k = X + (a_kX + Y)^{n+1}, \quad Y\alpha_k = Y - a_k(a_kX + Y)^{n+1} \quad (1 \leqslant k \leqslant n+2),$$

and consider $\beta_1, \ldots, \beta_{m+2} \in A_m$ where

$$X\beta_k = X + (b_kX + Y)^{m+1}, \quad Y\beta_k = Y - b_k(b_kX + Y)^{m+1} \quad (1 \leqslant k \leqslant m+2).$$

We choose $a_1 = b_1 = 0$, all a_k different and all b_k different. We shall show that the $n + m + 3$ maps $\xi_{[\alpha_0,\beta_k]}$ $(1 \leqslant k \leqslant m+2)$, $\xi_{[\alpha_k,\beta_1]}$ $(2 \leqslant k \leqslant n+2)$ are linearly independent in L^+_{n+m+2}. Suppose

$$\sum \lambda_k \xi_{[\alpha_0,\beta_k]} + \sum \mu_k \xi_{[\alpha_k,\beta]} \equiv 0 \qquad \text{in } L^+_{m+n+2}. \tag{1}$$

By (3.7),

$$\begin{aligned} X\xi_{[\alpha_0,\beta_k]} &\equiv X(D_X - b_kD_Y)(b_kX + Y)^{m+1}D_YX^{n+1} \equiv (b_kX + Y)^{m+1}D_YX^{n+1} \\ &\equiv (m+1)(b_kX + Y)^mX^{n+1} \bmod M^{n+m+2}, \end{aligned}$$

and

$$\begin{aligned} X\xi_{[\alpha_k,\beta_1]} &\equiv X(D_X - a_kD_Y)(a_kX + Y)^{n+1}D_XY^{m+1} \\ &\quad - XD_XY^{m+1}(D_X - a_kD_Y)(a_kX + Y)^{n+1} \\ &\equiv (n+1)\,a_k(a_kX + Y)^nY^{m+1} + (m+1)\,a_kY^m(a_kX + Y)^{n+1} \\ &\equiv a_k((n+m+2)Y + (m+1)\,a_kX)(a_kX + Y)^nY^m \bmod M^{n+m+2}. \end{aligned}$$

Thus (1) implies that

$$\begin{aligned} &\sum \lambda_k(m+1)(b_kX + Y)^mX^{n+1} \\ &\quad + \sum \mu_ka_k((n+m+2)Y + (m+1)\,a_kX)(a_kX + Y)^nY^m = 0. \end{aligned} \tag{2}$$

We differentiate this equation with respect to X n-times, and each time put $X = 0$ and $Y = 1$. Since the left sum of (2) contains a factor X^{n+1}, it will not contribute to any of the equations which we obtain in this way. The 0-th to n-th derivatives of the right sum of (2) are:

$$\sum \mu_ka_k(n+m+2)(a_kX + Y)^nY^{m+1}$$

$$+ \sum \mu_k{a_k}^2(m+1)\sum_{t=0}^{n}\binom{n}{t}{a_k}^tX^{t+1}Y^{m+n-t}$$

$$\sum \mu_k{a_k}^2(n+m+2)\,n(a_kX + Y)^{n-1}Y^{m+1}$$

$$+ \sum \mu_k{a_k}^2(m+1)\sum_{t=0}^{n}\binom{n}{t}(t+1)\,{a_k}^tX^tY^{m+n-t}$$

$$\cdots$$

$$\sum \mu_k a_k^{1+r}(n+m+2)\,n(n-1)\cdots(n-r+1)(a_kX+Y)^{n-r}Y^{m+1}$$

$$+\sum \mu_k a_k^{2}(m+1)\sum_{t=r-1}^{n}\binom{n}{t}(t+1)\cdots(t+2-r)\,a_k{}^{t}X^{t+1-r}Y^{m+n-t}$$

$$\cdots$$

$$\sum \mu_k a_k^{1+n}(n+m+2)\,n!\,Y^{m+1}$$

$$+\sum \mu_k a_k^{2}(m+1)\sum_{t=n-1}^{n}\binom{n}{t}(t+1)\cdots(t+2-n)\,a_k{}^{t}X^{t+1-n}Y^{m+n-t}.$$

Putting $X=0$, $Y=1$, we get

$$\sum \mu_k a_k(n+m+2)=0 \qquad \text{or} \quad \sum \mu_k a_k=0,$$

$$\sum \mu_k a_k^{2}((n+m+2)n+(m+1))=0 \qquad \text{or} \quad \sum \mu_k a_k^{2}=0,$$

$$\cdots$$

$$\sum \mu_k a_k^{1+r}\left((n+m+2)\,n(n-1)\cdots(n-r+1)+(m+1)\binom{n}{r-1}r!\right)=0$$

$$\text{or} \quad \sum \mu_k a_k^{1+r}=0,$$

$$\cdots$$

$$\sum \mu_k a_k^{1+n}\left((n+m+2)\,n!+(m+1)\binom{n}{n-1}(n-1)!\right)=0$$

$$\text{or} \quad \sum \mu_k a_k^{1+n}=0.$$

We obtained a system of $n+1$ homogeneous linear equations for the $n+1$ unknowns μ_k whose coefficient matrix is clearly nonsingular. Thus $\mu_2=\mu_3=\cdots=\mu_{n+2}=0$. Equation (2) becomes $\sum \lambda_k(b_kX+Y)^m=0$. Here we differentiate with respect to Y, and obtain

$$\sum \lambda_k(b_kX+Y)^m=0,$$

$$\cdots$$

$$\sum \lambda_k m(m-1)\cdots(m+1-r)(b_kX+Y)^{m-r}=0,$$

$$\cdots$$

$$\sum \lambda_k m!=0.$$

Putting $X=1$, $Y=0$ we get

$$(3)\qquad \begin{cases} \sum \lambda_k b_k{}^{m}=0, \\ \cdots \\ \sum \lambda_k b_k^{m-r}=0, \\ \cdots \\ \sum \lambda_k b_k{}^{0}=0. \end{cases}$$

These are $m+1$ equations for the $m+2$ unknowns λ_k. An additional equation is obtained by evaluating (1) at Y. We get

$$\sum \lambda_k(X^{n+1}(D_X - b_kD_Y)(b_kX + Y)^{m+1} + b_k(b_kX + Y)^{m+1}D_YX^{n+1}) = 0$$

or

$$\sum \lambda_k((n+1)\,X^n(b_kX + Y)^{m+1} + (m+1)\,b_k(b_kX + Y)^mX^{n+1}) = 0.$$

Putting $X = 1$, $Y = 0$ we get $\sum \lambda_k b_k^{m+1}(n+m+2) = 0$ or $\sum \lambda_k b_k^{m+1} = 0$. This equation together with (3) shows that $\lambda_1 = \lambda_2 = \cdots = \lambda_{m+2} = 0$. We have shown that the images of the commutators $[\alpha_0, \beta_k]$ $(1 \leqslant k \leqslant m+2)$, $[\alpha_k, \beta_1]$ $(2 \leqslant k \leqslant n+2)$ in L^+_{n+m+2} are linearly independent. It is easy to see that the image of $[A_n, A_m]$ in L^+_{n+m+2} is actually a subvector space, and the theorem now follows as outlined after Proposition 3.2.

COROLLARY 3.9. *$A_{n+m} = [A_n, A_m]A_k$ for every $k \geqslant n+m$.*

Proof. We apply (3.8) repeatedly:

$$\begin{aligned} A_{n+m} &= [A_n, A_m]A_{m+n+1} = [A_n, A_m][A_n, A_{m+1}]A_{m+n+2} \\ &= [A_n, A_m]A_{m+n+2} = \cdots. \end{aligned}$$

COROLLARY 3.10. *$A_{2n} = A_n'A_k$ for every $k \geqslant 2n$, where A_n' is the commutator subgroup of A_n.*

Proof. $n = m$ in (3.9).

The group A_1 has trivial center (as is easily seen) while the intersection of the terms Z^n of its lower central series is the identity subgroup. We will next describe the structure of the factors ${}_nA_m = A_n/A_m$. We denote by $Z(G)$ the center of the group G.

THEOREM 3.11. *Let ${}_nA_m = A_n/A_m$ for $m \geqslant n$. Then*

(a) *${}_nA_m$ is torsion free.*

(b) *${}_nA_m' = {}_{2n}A_m$ if $m > 2n$ and ${}_nA_m' = \{1\}$ otherwise.*

(c) *$Z({}_nA_m) = {}_{m-n}A_m$ if $m > 2n$ and $Z({}_nA_m) = {}_nA_m$ otherwise.*

(d) *The terms of the upper central series of ${}_nA_m$ are ${}_mA_m$, ${}_{m-n}A_m$, ${}_{m-2n}A_m$, ...*

(e) *The terms of the lower central series of ${}_nA_m$ are ${}_nA_m$, ${}_{2n}A_m$, ${}_{3n}A_m$, ...*

(f) *${}_nA_m$ is nilpotent of class $[m/n]$ ($[x]$ denotes the greatest integer $\leqslant x$).*

(g) *The upper and lower central series of ${}_nA_m$ coincide (and ${}_nA_m$ has a unique central series) if and only in $n \mid m$.*

Proof. (a) Same argument as in (2.14). (b) Immediate consequence of (3.8). (c) From (3.9) we obtain $A_m = [A_n, A_{m-n}]A_m$ hence $[A_n, A_{m-n}] \subset A_m$. Therefore $Z({}_nA_m) = {}_nA_m$ if $m - n \leqslant n$ or $m \leqslant 2n$, and $Z({}_nA_m) \supset {}_{m-n}A_m$ if $m > 2n$. We will show that $\alpha \in A_n$ and $\alpha A_m \in Z({}_nA_m)$ implies that $\alpha \in A_{m-n}$. Let $\beta \in A_n$ be the map given by $X\beta = X$, $Y\beta = Y + X^{n+1}$. Let $\xi = \alpha - 1$ and $\eta = \beta - 1$. Since $\alpha A_m \in Z({}_nA_m)$ we have $[\alpha, \beta] \in A_m$ or $M\xi_{[\alpha,\beta]} \subset M^{m+1}$. It is easily calculated that $[\xi, \eta] = \beta\alpha\xi_{[\alpha,\beta]}$ and therefore $M[\xi, \eta] = M\beta\alpha\xi_{[\alpha,\beta]} = M\xi_{[\alpha,\beta]} \subset M^{m+1}$. In particular,

$$X\xi\eta = X(\xi\eta - \eta\xi) = X[\xi, \eta] \subset M^{m+1}. \tag{1}$$

Write $X\xi = \sum_{i+j\geqslant d} a_{ij}X^iY^j$ with $a_{id-i} \neq 0$ for some i. Then (2) $X\xi\eta - \sum_{i+j\geqslant d} ja_{ij}X^{i+n+1}Y^{j-1} \in M^{d+2n}$ by (3.3). If $m + 1 \geqslant d + 2n$ then it follows from (1) and (2) that $\sum_{i+j\geqslant d} a_{ij}jX^{i+n+1}Y^{j-1} \in M^{d+2n}$, and hence $d + n \geqslant d + 2n$, a contradiction. If $d + 2n > m + 1$ then it follows from (1) and (2) that $\sum_{i+j\geqslant d} a_{ij}jX^{i+n+1}Y^{j-1} \in M^{m+1}$, and hence $d + n \geqslant m + 1$ or $d \geqslant (m - n) + 1$. This says that $X\alpha - X \in M^{(m-n)+1}$. Using $\gamma \in A_n$ with $X\gamma = X + Y^{n+1}$ and $Y\gamma = Y$ we obtain analogously that $Y\alpha - Y \in M^{(m-n)+1}$ and so $\alpha \in A_{m-n}$. This completes the proof.

(d) follows immediately from (c), (e) follows from (3.9), and (f) and (g) follow from (d) and (e).

4. Fixed Rings

In the whole section we again assume that $\operatorname{char} F = 0$. If α is a nonidentity automorphism in A_1 then α has infinite order. If we let $R^\alpha = \{f \in R: f\alpha = f\}$, then R^α is an F-subalgebra of R which coincides with the ring of invariants under the cyclic subgroup of A_0 generated by α. In this section we prove that either $R^\alpha = F$ or $R^\alpha = F[f_0]$ for some nonconstant irreducible polynomial f_0 in R.

Lemma 4.1. *Let f, g be nonconstant polynomials in R with g dividing f. If $\alpha \in A_1$ and $f\alpha = f$ then $g\alpha = g$.*

Proof. Without loss of generality we can assume g is an irreducible factor of f. The image under α of an irreducible polynomial must be irreducible. So α permutes the irreducible factors of f and we obtain a homomorphism of $\langle\alpha\rangle$ into the symmetric group on the set of irreducible factors of f. Since the latter group is finite, there is a nontrivial kernel, in particular, $g\alpha^n = g$ for some $n > 0$.

Suppose $g \in M^i$ but $g \notin M^{i+1}$, $i \geqslant 1$. Set $\xi = \alpha - 1$. Then $0 = g(\alpha^n - 1) = \binom{n}{1}(g\xi) + \binom{n}{2}(g\xi^2) + \cdots + \binom{n}{n}(g\xi^n)$ and $g\xi^k \in M^i\xi^k \subset M^{i+k} \subset M^{i+2}$ for $k \geqslant 2$

by (2.4). So $g\xi \in M^{i+2}$. But now for $k \geqslant 1$, $(g\xi)\xi^k \in M^{i+2+k} \subset M^{i+3}$ and, as above, $g\xi \in M^{i+3}$. So we see that $g\xi \in \bigcap_{j=1}^{\infty} M^j = (0)$, i.e., $g\alpha = g$.

LEMMA 4.2. *If* $\alpha \in A_1$, $\alpha \neq 1$, *and* $R^\alpha \neq F$ *then* R^α *has transcendence degree one over* F.

Proof. $R^\alpha \neq F$ implies the transcendence degree is at least one. Suppose it is two. Then X satisfies an algebraic equation over R^α. So there exists a polynomial $p \in R^\alpha[Z]$ with $p(X) = 0$. But then $p(X\alpha^k) = 0$ for all k and, since p has finitely many roots, there exists an n so that $X\alpha^n = X$. By the proof of (4.1), $X\alpha = X$. Similarly, $Y\alpha = Y$ and so $\alpha = 1$, contradiction.

This lemma implies that each $\alpha \in A_1$ is determined by its effect on any two algebraically independent polynomials.

The following proposition was communicated to us by the referee together with an outline of the proof. The main theorem will then follow at once. We are grateful to the referee for pointing out this improvement of our original derivation.

THEOREM 4.3. *If* $R = F[X_1, \ldots, X_n]$ *is a polynomial ring over the field* F *and* K *is a field such that* $F \subset K \subset F(X_1, \ldots, X_n)$ *with* K/F *of transcendence degree one, then either* $R \cap K = F$ *or* $R \cap K$ *is a polynomial ring in one variable over* F.

Proof. If $R^* = R \cap K = F$ there is nothing to prove. So suppose $R^* \neq F$. By the generalized Lüroth theorem (see, for example, Nagata, *Nagoya Math. J.* **29** (1967), 87) the field of quotients of R^* is a simple transcendental extension of F, say $F(t)$. Notice that R^* is integrally closed and every unit of R^* is in F. By [6, Theorem 57], R^* is the intersection of valuation domains of $F(t)$ over F. By [6, Theorem 66], such a valuation domain is either $V(f) = F[t]_{(f)}$ for some irreducible $f \in F[t]$, or else $V(t^{-1}) = F[t^{-1}]_{(t^{-1})}$.

Case I. $R^* \not\subset V(t^{-1})$. We shall show that

$$R^* = \bigcap \{V(f) : f \text{ is irreducible}\} = F[t].$$

So suppose $g \in F[t]$ is irreducible and $R^* \not\subset V(g)$. Then, clearly, $g^{-1}, g \in V(f)$ for all f not associate with g. Since R^* is the intersection of such valuation rings we obtain that $g^{-1}, g \in R^*$, a contradiction.

Case II. $R^* \subset V(t^{-1})$. Notice that

$$V(t^{-1}) = \{g/h : g, h \in F[t] \text{ and } dg(g) \leqslant dg(h)\}.$$

Consider two non-associate, irreducible elements $g, h \in F[t]$. If $d = dg(g)$ and $e = dg(h)$ then it is easily seen that g^e/h^d and h^d/g^e belong to $V(t^{-1})$

and to each $V(f)$ different from $V(g)$ and $V(h)$. Hence R^* is contained either in $V(g)$ or $V(h)$ or else g^e/h^d is a nonconstant unit of R^* which is impossible. It follows that R^* is contained in all but one of the valuation domains $V(g)$. Let $V(f)$ be the exceptional domain. Then

$$R^* = \{g/f^k : g \in F[t] \text{ and } dg(g) \leqslant k\, dg(f)\}.$$

Write $t = r/s$, $r, s \in R$, $(r, s) = 1$, and let $f(t) = a_0 + a_1 t + \cdots + a_m t^m$. Since $1/f(t) = p \in R$, we obtain $s^m = p(a_0 s^m + a_1 s^{m-1} r + \cdots + a_m r^m)$. It follows that $1/f(t) = p = s^m$ and

$$a_0 s^m + a_1 s^{m-1} r + \cdots + a_m r^m = 1.$$

Here the left side is homogeneous in r and s and therefore factors into linear terms $ar + bs$ over the algebraic closure of F. It follows that $ar + bs = 1$ is solvable for a, b in the algebraic closure of F. But this is a system of linear equations with coefficients in F, and has therefore a solution in F. So suppose

$$ar + bs = 1, \qquad a, b \in F.$$

Then $1/at + b = s/ar + bs = s \in R^*$. Hence $s = g/f^k = gs^{km}$, which implies $m = k = g = 1$. Since $st = a^{-1}(1 - bs)$ it follows readily that $R^* = F[s]$. This proves the theorem.

THEOREM 4.4. *Suppose F has characteristic 0, $\alpha \in A_1$, $\alpha \neq 1$, with $R^\alpha \neq F$. Then there is an irreducible polynomial $f_0 \in R$ such that $R^\alpha = F[f_0]$.*

Proof. Let K be the quotient field of R^α in $F(X, Y)$. Then K has transcendence degree one over F by (4.2), and by (4.3) $R^\alpha = K \cap R = F[f_0]$ for some $f_0 \in R^\alpha$. The polynomial f_0 is irreducible by (4.1).

We could not decide whether the fixed ring of some automorphism can just be the field F. It also seems interesting to know which polynomials f_0 can occur as the generators of fixed rings R^α.

5. REMARKS

In the previous section we considered the fixed rings R^α for $\alpha \in A_1$. Conversely, we may consider the sets $A_f = \{\alpha \in A_1 : f\alpha = f\}$ for $f \in R$. The following facts are easily verified:

(5.1) A_f is a subgroup of A_1.

(5.2) $\beta^{-1} A_f \beta = A_{f\beta}$ for each $\beta \in A_0$.

(5.3) If α, β are non-identity elements of A_f, $f \notin F$, then $R^\alpha = R^\beta$. If $R^\alpha = R^\beta = F[f_0]$ then $A_f = A_{f_0}$.

By (5.3) we only need to consider groups A_{f_0} with $f_0 \in M$ and f_0 irreducible. For each polynomial f_0, $A_{f_0} = \{\alpha \in A_1 \colon R^\alpha = F[f_0]\} \cup \{1\}$.

(5.4) If $A_f \cap A_g \neq 1$ then $A_f = A_g$. If both f and g are in M and irreducible then $f \sim g$ (associates).

The following result follows at once from (5.2) and (5.4) using that $\beta \in A_1$ and $f\beta \sim f$ implies that $f\beta = f$.

(5.5) If $1 \neq \alpha \in A_f$ and $\beta^{-1}\alpha\beta \in A_f$ for $\beta \in A_1$ then $\beta \in A_f$. In particular, A_f contains the centralizer of each of its elements, and A_f is its own normalizer.

This is what we are able to say in general. We will next have a look at the prime example A_X.

(5.6) A_X is isomorphic with the direct sum of countably many copies of the additive group of F, and is a maximal abelian subgroup of A_1.

To what degree is the structure of A_X typical? Is each A_f, $f \notin F$, commutative? Of course, the conjugates $\alpha^{-1}A_X\alpha = A_{X\alpha}$ share the structure of A_X. If $R^\alpha = F[f_0]$, $f_0 \in M$, then is A_{f_0} conjugate to A_X?

Every $\alpha \in \mathrm{aut}_F R$ induces a "polynomial map" $\bar{\alpha}$ on the affine space F^2 onto itself defined by $\bar{\alpha}\colon F^2 \to F^2$: $(a, b)\bar{\alpha} = (X\alpha(a, b), Y\alpha(a, b))$. Let $V(f)$, $f \in R$, denote the algebraic curve of all points (a, b) satisfying $f(a, b) = 0$. The following fact is easily checked:

(5.7) $V(f)\bar{\alpha} = V(f\alpha^{-1})$ for each $f \in R$ and $\alpha \in \mathrm{aut}_F R$.

From now on we assume that F is algebraically closed. We clarify the connection between polynomials left fixed by $\alpha \in A_1$ and algebraic curves mapped into themselves by $\bar{\alpha}$.

(5.8) Let f be a nonconstant polynomial, and $\alpha \in A_1$. Then $f\alpha = f$ if and only if $V(f)\bar{\alpha} \subset V(f)$.

Proof. If $f\alpha = f$ then it follows at once from (5.7) that $V(f)\bar{\alpha} = V(f)$. Suppose $V(f)\bar{\alpha} \subset V(f)$. By (5.7) $V(f\alpha^{-1}) \subset V(f)$. By Hilbert's Nullstellensatz $f\alpha^{-1} \mid f^n$ for some n. Let f_k be the irreducible factors of f. Then $f_i\alpha \sim f_j$ for some j. Hence there is a natural number m such that $f_i\alpha^m \sim f_i$ for all i. By an earlier remark $f_i\alpha^m = f_i$ and hence $f_i\alpha = f_i$. So $f\alpha = f$.

COROLLARY 5.9. *If $1 \neq \alpha \in A_1$ and $V(f)\bar{\alpha} \subset V(f)$ then $\bar{\alpha}$ maps each irreducible component of $V(f)$ onto itself. Furthermore, $f = (f_0 + c_1) \cdots (f_0 + c_k)$ where $R^\alpha = F[f_0]$ and $c_i \in F$.*

Propositions (5.8) and (5.9) say that any polynomial map arising from some $\alpha \in A_1$ will either map no algebraic curve into itself or else there is

a family of irreducible nonintersecting algebraic curves $V(f_0 + c)$ which cover the plane and are all mapped onto themselves.

If $\alpha \in A_X$ then $\bar{\alpha}$ leaves $V(X)$ pointwise fixed. We observe the following fact:

(5.10) The algebraic curve $V(f)$ is left pointwise fixed by $\bar{\alpha}$ (where $\alpha \in A_1$) if and only if $f \mid (X\alpha - X, Y\alpha - Y)^n$.

Using (5.8) we obtain

(5.11) If $\alpha \in A_1$ and $(X\alpha - X, Y\alpha - Y) \neq 1$ then

$$(X\alpha - X, Y\alpha - Y) = (f_0 + c_1) \cdots (f_0 + c_k)$$

where $R^\alpha = F[f_0]$ and $c_i \in F$. In particular, $(X\alpha - X, Y\alpha - Y) \in R^\alpha$.

If $R^\alpha \neq F$, does α necessarily leave some curve pointwise fixed, i.e., does it follow that $(X\alpha - X, Y\alpha - Y) \neq 1$? If this question has an affirmative answer then it is very easy to exhibit automorphisms $\alpha \in A_1$ with $R^\alpha = F$. Using a deeper theorem of algebraic geometry [2, Theorem 8, p. 293] the following can be shown:

(5.12) If $1 \neq \alpha \in A_1$ and $\bar{\alpha}$ maps an irreducible algebraic curve of genus >1 into itself then some power of $\bar{\alpha}$ leaves the curve pointwise fixed.

This suggests an investigation of the genus of $V(f)$ for $F[f] = R^\alpha$ for some $\alpha \in A_1$. If $\bar{\alpha}^n$ fixes $V(f)$ pointwise, does $\bar{\alpha}$ already fix $V(f)$ pointwise?

References

1. S. Andreadakis, Automorphisms of the ring of polynomials and transformations of algebraic sets (Greek), *Bull. Soc. Math. Greece* **7** (1966), 1–49.
2. T. L. Coolidge, "A Treatise on Algebraic Plane Curves," Dover, New York, 1959.
3. W. Engel, Ein Satz über ganze Cremona-Transformationen der Ebene, *Math. Ann.* **130** (1955), 11–19.
4. W. Engel, Ganze Cremona-Transformationen von Primzahlgrad in der Ebene, *Math. Ann.* **136** (1958), 319–325.
5. H. Jung, Über ganze birationale Transformationen der Ebene, *J. R. U. A. Math.* **184** (1942), 161–174.
6. I. Kaplansky, "Commutative Rings," Allyn and Bacon, Boston, 1970.