AUTOMORPHISMS OF FORMAL POWER SERIES UNDER SUBSTITUTION

BY

BENJAMIN MUCKENHOUPT

1. Introduction. The purpose of this paper is to show that for most cases the only automorphisms of a certain group of formal power series are what might be called the obvious ones. The power series to be considered will be of the form $\sum_1^\infty a_i x^i$ where $a_1 \neq 0$ and the coefficients are all members of a given field. The composition to be considered is that of substitution or functional composition. Given the series $f = \sum_1^\infty a_i x^i$ and $g = \sum_1^\infty b_i x^i$, then $fg = \sum_1^\infty a_i (g)^i = a_1 b_1 x + (a_1 b_2 + a_2 b_1^2) x^2 + \cdots$. Given a field, the series of this type clearly form a group with this law of composition. Furthermore, besides the inner automorphisms it is clear that any field automorphism $a \rightarrow \bar{a}$ induces an automorphism $\sum_1^\infty a_i x^i \rightarrow \sum_1^\infty \bar{a}_i x^i$ of the group. Such automorphisms of the group will be called simply field automorphisms. Showing that combinations of these and inner automorphisms are the only automorphisms of the group of power series for most base fields is the main part of this paper.

The original interest in this subject stemmed from the hope that automorphisms other than the obvious ones might be found and that they might have applications to the theory of iteration of analytic functions. The usual way of solving, for example, the functional equation $g[g(z)] = f(z)$ where $f(z) = \sum_1^\infty a_i z^i$ and $|a_1| \neq 1$ is to find an inner automorphism that simplifies $f(z)$. The solution h of $h^{-1}(f[h(z)]) = a_1 z$ is found and then $g(z) = h[(a_1)^{1/2} h^{-1}(z)]$. Proving that h exists and is analytic is not difficult. The method was originally used by Schroeder([1]). If the first coefficient of $f(z)$ is 1, however, no such simple automorphism gives results. No other automorphisms are suggested by this paper, but the present results do have independent interest.

In §2 some useful lemmas and definitions will be given.

In §3 the following will be proved.

THEOREM 1. *Over a field of characteristic* 0 *every automorphism of the group of formal power series under substitution can be written as the succession of an inner automorphism and a field automorphism* ([2]).

Received by the editors October 18, 1960.

[1] See E. Schroeder, *Über iterierte Functionen*, Math. Ann. vol. 3 (1871) pp. 296–322. For a simpler presentation see H. Kneser, *Reele analytischer Lösungen der Gleichung $\phi[\phi(z)] = e^z$ und verwandter funktionalgleichungen*, J. Reine Angew. Math. vol. 187 (1949) pp. 56–67; see p. 58.

[2] This result was announced for the case when the base field is the complex numbers by N. J. Fine and Bertram Kostant in an abstract, *The group of formal power series under iteration*, Bull. Amer. Math. Soc. vol. 61 (1955) pp. 36–37. Their proof has not yet appeared.

The method of proof will be to consider an arbitrary automorphism and to reduce it by stages to the desired form.

In §§4 to 6 the case for fields of characteristic $p\neq 0$ will be considered. The principal result is the following.

THEOREM 2. *Over an infinite field of characteristic not* 2, *every automorphism of the group of formal power series under substitution can be written as the succession of an inner automorphism and a field automorphism.*

Whether this can be extended to the case of finite fields or fields of characteristic 2 remains an open question. However, the following partial results can be proved for more general cases.

THEOREM 3. *If a series has first coefficient* 1, *then under any automorphism the transformed series has first coefficient* 1. *Hence the first coefficient of a series determines the first coefficient of the transformed series.*

THEOREM 4. *Any automorphism of a group of formal power series can be written as the succession of an inner automorphism and one that takes series of the form ax into series of the same type.*

THEOREM 5. *Over a field of characteristic not* 2 *the first k coefficients of a series determine the first k coefficients of the transformed series under an automorphism. In addition, the relation between first coefficients is a field automorphism.*

These results will be proved by methods similar to those of §3.

2. **Basic lemmas and definitions.** Throughout this paper the basic form of composition by substitution will be used. If $f=\sum_1^\infty a_ix^i$ and $g=\sum_1^\infty b_ix^i$, then

$$fg = a_1b_1x + \cdots + [a_1b_n + \cdots + a_j(jb_1^{j-1}b_{n-j+1} + \text{terms of lower } b_i\text{'s}) \\ + \cdots + a_nb_1^n]x^n + \cdots .$$

LEMMA 1. *If $f=\sum_1^\infty a_ix^i$ and a_1 has (multiplicative) order q, f may be written in the form $h^{-1}[a_1x+\sum_{i=1}^\infty b_{qi+1}x^{qi+1}]h$.*

Let $h=\sum_1^\infty c_ix^i$ and $g=a_1x+\sum_{i=1}^\infty b_{qi+1}x^{qi+1}$ where the b_{qi+1} and c_i are to be determined. In the series hf the coefficient of x^n is: $c_na_1^n+$(terms in lower c_i's), n not of the form $qj+1$, $c_{qi+1}a_1+$(terms in lower c_i's), $n=qj+1$, j an integer. In the series gh the coefficient of x^n is: a_1c_n+(terms in lower c_i's and b_i's), n not of the form $qj+1$, $a_1c_{qj+1}+b_{qj+1}a_1^n+$(terms in lower b_i's and c_i's), $n=qj+1$. From these it is clear that the c_n may be chosen successively to make the nth terms of hf and gh equal provided that n is not of the form $qj+1$. These latter terms may be made equal by proper successive choice of the b_{qj+1}'s. Thus, by proper choice of the b_{qj+1}'s and the c_n's the equation $hf=gh$ can be obtained. Multiplying this by h^{-1} gives the desired result.

The following special case is the one usually needed.

Lemma 2. *If $f=\sum_1^\infty a_i x^i$ and a_1 is not a root of unity, then f may be written in the form $h^{-1}[a_1 x]h$.*

Lemma 3. *If $f=\sum_1^\infty a_i x^i$, $a_1=1$, a_j is the second nonzero term and p is the characteristic of the field, then by proper choice of h, $h^{-1}fh$ may be given arbitrary terms from the $(2j)$th on except possibly for the $(2j-1+kp)$th ones, k an integer.*

Let $g=\sum_1^{2j-1} a_i x^i+\sum_{2j}^\infty b_i x^i$ and $h=x+\sum_j^\infty c_i x^i$. Then for $n\geqq 2j$, the nth coefficient of fh has the form $c_n+ja_jc_{n-j+1}+$(terms in lower c_i's). Again, for $n\geqq 2j$, the nth coefficient of hg has the form $c_n+(n-j+1)a_jc_{n-j+1}+b_n$ $+$(terms in lower c_i's and b_i's). From these it is clear that for $n\neq 2j-1+kp$ the nth terms may be made equal by proper successive choice of the c_{n-j+1} regardless of the choice of the b_n. For $n=2j-1+kp$ proper choice of b_n can make the terms equal. This gives the asserted arbitrariness.

Definition. For characteristic $p\neq 2$ let

$$P_1(x,r)=\sum_0^\infty r^i x^{i+1}\left(=\frac{x}{1-rx}\text{ for the real field and } x \text{ small}\right),$$

$$P_2(x,r)=\sum_0^\infty 2^{-i}C_i^{2i}r^i x^{2i+1}\left(=\frac{x}{(1-2rx^2)^{1/2}}\text{ for the reals and } x \text{ small}\right),$$

$$P_n(x,r)=P_1\left(x,\frac{r}{2-n}\right)P_{n-1}(x,1)P_1^{-1}\left(x,\frac{r}{2-n}\right)P_{n-1}^{-1}(x,1)$$

$$\text{for } n>2 \text{ and not of the form } 2+kp,$$

$$P_n(x,r)=P_2\left(x,\frac{r}{4-n}\right)P_{n-2}(x,1)P_2^{-1}\left(x,\frac{r}{4-n}\right)P_{n-2}^{-1}(x,1)$$

$$\text{for } n>2 \text{ and of the form } 2+kp.$$

The binomial coefficient C_i^{2i} being an integer is defined for any field.

The reason for considering these particular series is that $P_1(x,r)$ and $P_2(x,r)$ have the properties of Lemma 5. These properties are essentially preserved under automorphisms so that these series are essentially transformed into themselves under any automorphism. Knowing the images of $P_1(x,r)$ and $P_2(x,r)$, of course, determines the images of the other $P_n(x,r)$. However, because of the form of the P_n's shown in Lemma 4, any series can be written in some sense as the product of these series and one of the form ax. The precise statement of these ideas will be the main part of the proofs.

Lemma 4. *$P_n(x,r)$ has the form $x+rx^{n+1}+\cdots$.*

This is clearly true for $n=1$ and $n=2$. It follows in general by induction with a simple calculation.

LEMMA 5. *$P_1(x, r)^n = P_1(x, nr)$, $P_1(x, r)P_1(x, s) = P_1(x, r+s)$, $P_1(x, r) = (rx)^{-1}P_1(x, 1)(rx)$, $P_2(x, r)^n = P_2(x, nr)$, $P_2(x, r)P_2(x, s) = P_2(x, r+s)$, and $P_2(x, r^2) = (rx)^{-1}P_2(x, 1)(rx)$.*

With base field the real numbers and x sufficiently small, induction shows that $[P_1(x, r)]^n = x/(1-rnx) = P_1(x, nr)$. The identity of the two outer expressions does not depend on the field so that it holds generally. The other expressions are proved in a similar manner.

LEMMA 6. *Given an integer $n > 2$ and a series f over a field of characteristic $p \neq 2$, f can be written in the form $H(ax)\prod_{j=1}^{n-1} P_j(x, a_j)$, H having the form $SRS^{-1}TP_m(x, 1)T^{-1}$ where m is greater than $n-1$ and R is a finite product of P_i's with subscripts greater than $n-1$.*

First choose a to be the first coefficient of f. Choose the a_j's so that $g = (ax)\prod_{j=1}^{n-1} P_j(x, a_j)$ has the same first n coefficients as f. This is possible by choosing the a_j's successively, for since the P_j's have the form of Lemma 4, proper choice of an a_j will give the $(j+1)$st coefficient of the product any desired value while the previous coefficients are not affected. Now if fg^{-1} is the identity, the proof is finished. Otherwise fg^{-1} has a second nonzero term, c_m, where $m > n$. There is a product $R = \prod_{m-1}^{2m-1} P_i(x, b_i)$ and series S and T such that $(SRS^{-1})(TP_m(x, 1)T^{-1}) = fg^{-1}$. This follows from the fact that by proper choice of the b_i, R can be given arbitrary coefficients from order m to order $2m$, and by Lemma 3 proper choice of S will give arbitrary coefficients to SRS^{-1} from order $2m$ on except possibly for the $(2m-1+kp)$th ones. Again by Lemma 3, $TP_m(x, 1)T^{-1}$ can be given arbitrary terms from the $(2m+2)$nd on except for the $(2m+1+kp)$th ones. Since the characteristic is not 2, one or the other of these series can adjust any term.

3. **The characteristic 0 case; proof of Theorem** 1. Given an arbitrary automorphism, A, denote the image of a series f under the automorphism as f^A. The proof will proceed in steps as indicated.

A. If f has first coefficient 1, f^A does also.

The series $(2x)f$ may be written in the form $g^{-1}(2x)g$ by Lemma 2. Consequently, $f = (2x)^{-1}g^{-1}(2x)g$. Then f^A is of the form $h^{-1}k^{-1}hk$, and therefore will have first coefficient 1.

B. There exists h such that $h^{-1}(2x)^Ah = bx$ where b is the first coefficient in $(2x)^A$.

Let $(2x)^A = bx + \cdots$. Now suppose that some power of b, the nth, were such that $b^n = 1$. Then $(2^nx)^A = [(2x)^A]^n = (bx + \cdots)^n = x + \cdots$. Since the inverse of A is also an automorphism, $2^n = 1$ by part A. This is impossible since the base field is of characteristic 0. Therefore, b is not a root of 1 and Lemma 2 gives the desired result.

C. Now define an automorphism B by $f^B = h^{-1}f^Ah$, h the series of part B. Then $(2x)^B = bx$.

D. A series of the form ax is transformed by B into one of the form $\bar{a}x$.

Clearly $(2x)(ax)=(ax)(2x)$. Applying B gives $(bx)(ax)^B=(ax)^B(bx)$. Let $(ax)^B=\bar{a}x+\sum_2^\infty a_ix^i$. Then comparing nth terms of the last equality gives $ba_nx^n=a_nb^nx^n$. Now as shown in part B, b is not a root of unity. Therefore, $a_n=0$ for $n>1$.

E. $(2x)^B = 2x$, $[P_1(x, a)]^B = x + a^*x^2 + \cdots$, and $[P_2(x, c)]^B =x+c^\sharp x_3+ \cdots$, where a^* and $c^\sharp$ are not 0 provided that a and c are not 0.

By the definition of P_1 and Lemma 5, $(2x)^{-1}P_1(x, a)(2x)=P_1(x, 2a) =[P_1(x, a)]^2$. Applying B to the outer terms gives $(bx)^{-1}[P_1(x, a)]^B(bx) =([P_1(x, a)]^B)^2$. Now if $[P_1(x, a)]^B$ has the form $x+a_nx^n+ \cdots$, $a_n\neq 0$, then $([P_1(x, a)]^B)^2$ has the form $x+2a_nx^n+ \cdots$. Then comparing nth terms in the above equation gives $a_nb^{n-1}x^n=2a_nx^n$ so that $b^{n-1}=2$. Since the field has characteristic 0, n must be a constant independent of a.

Again, by the definition of P_2 and Lemma 5, $(2x)^{-1}P_2(x, c)(2x)=[P_2(x, c)]^4$. Applying B gives $(bx)^{-1}[P_2(x, c)]^B(bx)=([P_2(x, c)]^B)^4$. $[P_2(x, c)]^B$ has the form $x+c_mx^m+ \cdots$, $c_m\neq 0$, so that $([P_2(x, c)]^B)^4$ has the form $x+4c_mx^m + \cdots$. Comparing mth terms in the preceding equation shows that $b^{m-1}=4$. Since the field has characteristic 0, this shows that $m=2n-1$.

Using their definition it is now clear that $[P_k(x, d)]^B$ has second coefficient 0 for $k\geqq 2$. Now if $n\neq 2$, all the $[P_k(x, d)]^B$ for $k\geqq 1$ have second coefficient 0. Using Lemma 6, this would show that no series is transformed into one with second coefficient not 0. This is impossible since B is an automorphism; therefore $n=2$. This immediately gives the conclusions of this section.

F. Now if $[P_1(x, 1)]^B=x+ax^2+ \cdots$, define an automorphism C by $f^C=(ax)f^B(ax)^{-1}$.

G. $[P_1(x, 1)]^C=P_1(x, 1)$.

Apply C to the equation $(2x)[P_1(x, 1)]^2=[P_1(x, 1)](2x)$ to obtain $(2x)[x+x^2+\sum_3^\infty a_nx^n]^2=[x+x^2+\sum_3^\infty a_nx^n](2x)$. Comparing nth coefficients of this equality gives $4a_n+$(terms in lower a_i) $=2^na_n+$(terms in lower a_i). For $n\geqq 3$ the coefficients are uniquely determined. However, $P_1(x, 1)$ satisfies the above equation. Therefore, $[P_1(x, 1)]^C=P_1(x, 1)$.

H. Denote $(ax)^C=\bar{a}x$. Then $[P_1(x, a)]^C=P_1(x, \bar{a})$ and the transformation $a\dashrightarrow\bar{a}$ is a field automorphism.

Since $P_1(x, a) = (ax)^{-1}P_1(x, 1)(ax)$, applying C gives $[P_1(x, a)]^C =[(\bar{a})^{-1}x]P_1(x, 1)(\bar{a}x)=P_1(x, \bar{a})$. Now $(\overline{ab})x=(abx)^C=(ax)^C(bx)^C=(\bar{a}x)(\bar{b}x) =\bar{a}\bar{b}x$ and $P_1(x, \overline{a+b})=[P_1(x, a+b)]^C=[P_1(x, a)]^C[P_1(x, b)]^C=P_1(x, \bar{a}+\bar{b})$. Since the transformation has an inverse, it is a field automorphism.

I. Let D denote the power series automorphism induced by the inverse of the field automorphism obtained in H, and let $f^E=[f^C]^D$.

J. The second nonzero term of $[P_k(x, a)]^E$ is of order not less than $k+1$.

This follows from the definition of P_k and the forms of $[P_1]^E$ and $[P_2]^E$.

K. The first p terms of a series f determine the first p terms of f^E.

Apply Lemma 6 with $n=p$. The product H^E will have first coefficient 1 and the next $n-1$ coefficients zero since the $[P_k]^E$ in it will contribute nothing to these terms by part J and the other functions have their terms of order less than $p+1$ canceled by their inverses. Therefore, the first p terms of f^E are determined by the other product which in turn is determined by the first p terms of f.

L. $[P_2(x, 1)]^E$ has the form $x+cx^3+\sum_4^\infty c_nx^n$ where $c\neq 0$ by part E. Then applying E to the equation $(2x)[P_2(x, 1)]^4 = [P_2(x, 1)](2x)$ gives $(2x)[x+cx^3+\sum_4^\infty c_nx^n]^4=[x+cx^3+\sum_4^\infty c_nx^n](2x)$. Comparing nth coefficients gives $8c_n+(\text{terms in lower } c_i)=2^nc_n+(\text{terms in lower } c_i)$. Thus for $n>3$, c_n is uniquely determined. Since $P_2(x, c)$ satisfies the above equation, $[P_2(x, 1)]^E=P_2(x, c)$.

Now computation shows that $[P_3(x, 1)]^E=x+cx^4+cx^5+(c-(1/2)c^2)x^6 + \cdots$, and $[P_5(x, 1)]^E=x+cx^6+\cdots$. It may also be verified that $P_2(x, 1)P_3(x, 1)P_5(x, 1)$ has the same first six terms as $P_3(x, 1)P_2(x, 1)$. Applying E to both, the sixth terms must be equal by part K. This gives $2c+(5/2)c^2 =c+(7/2)c^2$ whence $c=1$ since $c\neq 0$.

M. $[P_2(x, a)]^E=P_2(x, a)$.

First, $[P_2(x, b^2)]^E=[(bx)^{-1}P_2(x, 1)(bx)]^E=(bx)^{-1}P_2(x, 1)(bx)=P_2(x, b^2)$. For the case when a is not a square observe the fact that

$$P_2(x, a) = P_2\left(x, \left(\frac{a+1}{2}\right)^2\right)\left[P_2\left(x, \left(\frac{a-1}{2}\right)^2\right)\right]^{-1}.$$

N. E is the identity.

E is certainly the identity on the series ax and $P_k(x, c)$ by the previous sections and the definitions. By part K it is the identity on the first p elements of any series. Since p is arbitrary, the conclusion follows.

This completes the proof of Theorem 1 since the given automorphism, A, was reduced to the identity by use of inner automorphisms and field automorphism.

4. Results valid for any field of finite characteristic; proof of Theorems 3 and 4. Let f^A denote the image of a series f under an arbitrary automorphism A. Let $p\neq 0$ be the characteristic of the base field.

LEMMA 7. *For a series $f=\sum_1^\infty a_ix^i$ with $a_1=1$, and for an integer n not divisible by p, there exists one and only one nth root of f with first coefficient* 1.

Let the second nonzero term of f be the kth. Consider $g=x+\sum_k^\infty b_ix^i$. Then $g^n=x+\sum_k^\infty (nb_i+\text{terms in lower } b_j\text{'s})x^i$. From this it is clear that the b_i may be determined successively to make $g^n=f$ since n is not divisible by p. If $h^n=g^n$, the above form shows that the second nonzero term of h must be the kth. Thereafter, h must have the same terms as g since the equations for the terms are linear and have unique solutions.

LEMMA 8. *Given a series $f = \sum_1^\infty a_i x^i$ with $a_1 \neq 1$, then*

$$f^n = a_1^n x + \frac{a_2(a_1^{2n} - a_1^n)}{a_1^2 - a_1} x^2 + \cdots .$$

This follows immediately by induction.

LEMMA 9. *If $f = \sum_1^\infty a_i x^i$, $a_1 = 1$, and $a_2 \neq 0$, then for all n not divisible by p there exists one and only one nth root of f.*

There is one and only one starting with x as shown in Lemma 7. Suppose there were another nth root of f, $g = \sum_1^\infty b_i x^i$ with $b_1 \neq 1$. Now

$$g^n = b_1^n x + \frac{b_2(b_1^{2n} - b_1^n)}{b_1^2 - b_1} x^2 + \cdots = x + 0x^2 + \cdots$$

since $b_1^n = 1$. However, the coefficient of x^2 in f is not zero by hypothesis. Therefore, the only nth root of f is the one starting with x.

Now to prove Theorem 3 let $f = \sum_1^\infty a_i x^i$, $a_1 = 1$, and $f^A = \sum_1^\infty b_i x^i$ and consider three separate cases.

CASE 1. There exists a field element, b, of infinite order. Then by Lemma 2, $(bx)f$ may be written as $h^{-1}(bx)h$ so that $f = (bx)^{-1}h^{-1}(bx)h$. As in the characteristic 0 case f^A has the form $g^{-1}k^{-1}gk$ so that f^A has first coefficient 1.

CASE 2. All the field elements are of finite order and $a_2 \neq 0$. Suppose b_1 is of order $q \neq 1$. The characteristic p does not divide q for if it did $(b_1)^{q/p}$ would satisfy $y^p = 1$. This, however, has only the solution 1 and would contradict the fact that q is the order of b_1. Now

$$[f^A]^q = b_1^q x + \frac{b_2(b_1^{2q} - b_1^q)}{b_1^2 - b_1} x^2 + \cdots = x + 0x^2 + \cdots ,$$

and $f^q = x + qa_2x^2 + \cdots$. The first series has at least two qth roots, the one starting with x given by Lemma 7 and f^A. The second can have only one qth root by Lemma 9 since its second coefficient is not zero. Since the series correspond under the automorphism, this is a contradiction. Therefore $q = 1$ and $b_1 = 1$.

CASE 3. All of the field elements are of finite order and $a_2 = 0$. Now if $g = f(x + x^2)$, g has first coefficient 1 and second coefficient 1. Therefore g^A has first coefficient 1 by Case 2 and so does $(x + x^2)^A$. Consequently, $f^A = g^A[(x + x^2)^{-1}]^A$ also has first coefficient 1.

To prove Theorem 4, again consider three cases.

CASE 1. There is a field element, b, of infinite order. As in part 3B for the characteristic 0 case it follows easily that if $(bx)^A = cx + \cdots$, then c is of infinite order. Then there is a series h such that $h^{-1}(bx)^Ah = cx$ by Lemma 2. The reasoning of part 3D then gives the result.

CASE 2. The field is infinite but has no element of infinite order. Choose an infinite sequence of field elements b_i with orders q_i so that $q_{i+1} > q_i$. Now if $(b_ix)^A = c_ix + \cdots$, b_i and c_i have the same orders, for if one were of lower order, s, the sth iterates of these series would violate Theorem 3. Then by Lemma 1 there exist series h_i with first coefficient 1 such that $h_i^{-1}(b_ix)^Ah_i = c_ix + \sum_{j=1}^{\infty} d_{i,j}x^{jq_i+1}$. As shown by the proof of Lemma 1 these h_i are uniquely determined up to the q_ith term. Now for any constant c, h_i has the property that $h_i^{-1}(cx)^Ah_i$ has zero coefficients from the second to the q_ith. This follows from the fact that $[h_i^{-1}(cx)^Ah_i][h_i^{-1}(b_ix)^Ah_i] = [h_i^{-1}(b_ix)^Ah_i] \cdot [h_i^{-1}(cx)^Ah_i]$. If $h_i^{-1}(cx)^Ah_i$ had the form $d_1x + d_kx^k + \cdots$ with $d_k \neq 0$ and $k \leq q_i$, a comparison of kth terms in the above equation would yield $d_kc_i^kx^k = c_id_kx^k$. This is impossible since c_i has order q_i.

Now for $i < j$, h_j has the same terms of order less than q_i as h_i since the terms of h_i are uniquely determined for order less than q_i, and $h_j^{-1}(b_ix)^Ah_j$ has the same terms as $h_i^{-1}(b_ix)^Ah_i$ for orders up to q_i. Therefore, it is possible to define a series h which coincides with each h_i up to the q_ith term. Since the q_i are arbitrarily large, h is defined and clearly has the desired property.

CASE 3. The field is a finite field. Let the field be of order $q+1$ and let b be a generator of the field. Then if $(bx)^A = \sum_1^{\infty} c_ix^i$, it follows as in Case 2 that c_i has order q. By Lemma 1 there is a series h such that $h^{-1}(bx)^Ah = c_1x + \sum_1^{\infty} d_ix^{qi+1}$. If the d_i are not all zero call the first nonzero one d_k. Then $[h^{-1}(bx)^Ah]^q = h^{-1}(b^qx)^Ah = h^{-1}h = x$. Therefore

$$x = [c_1x + d_kx^{kq+1} + \cdots]^q = (c_1x)^q\left[x + \frac{d_k}{c_1}x^{kq+1} + \cdots\right]^q$$
$$= x + \frac{qd_k}{c_1}x^{kq+1} + \cdots.$$

This is impossible since q is not divisible by the characteristic. Therefore, the d_i are all zero and $h^{-1}(bx)^Ah = c_1x$. Since for any a in the field, $(ax)^A$ may be written as a power of $(bx)^A$, it is clear that $h^{-1}(ax)^Ah$ has all coefficients beyond the first equal to zero.

5. **Results valid when the base field has finite characteristic p not equal to 2; proof of Theorem** 5. Because of §4 only automorphisms that take series of the form ax into series of the form $\bar{a}x$ need be considered. Let f^B denote the image of a series f under such an automorphism B.

LEMMA 10. *$[P_2(x, a)]^B$ does not have the form $x + bx^2 + \cdots$ where $b \neq 0$, provided that the base field characteristic, p, is not* 2.

Suppose that $[P_2(x, a)]^B$ had the given form. Let c be a generator of the prime field of the given field. Then if $(cx)^B = dx$, d also has order $p-1$. Then applying B to $(cx)^{-1}P_2(x, a)(cx) = [P_2(x, a)]^{c^2}$ gives $(dx)^{-1}(x+bx^2+ \cdots)(dx) = (x+bx^2+ \cdots)^{c^2} = x+bc^2x^2+ \cdots$. Comparing second coefficients of these expressions gives $bd=bc^2$ whence $d=c^2$. This is impossible for since c is of order $p-1$, this shows that d has order $(p-1)/2$.

LEMMA 11. *$P_1(x, a)$ has the form $x+bx^2+ \cdots$ where $b\neq 0$, provided that $a\neq 0$ and the base field characteristic, p, is not* 2.

Since for $a\neq 0$, $P_1(x, a) = (ax)^{-1}P_1(x, 1)(ax)$, the lemma must be true for all of these series or none. If it were true for none, Lemma 10 would show that no series $[P_k(x, a)]^B$ has second coefficient not equal to zero. Then using Lemma 6 with $n=3$ and applying B would show that no series would be transformed into one with nonzero second coefficient. This contradiction proves the lemma.

Now the reasoning of §3 parts J and K proves the first part of Theorem 5.

Letting $(ax)^B = \bar{a}x$ and $[P_1(x, 1)]^B = x+bx^2+ \cdots$, the fact that $P_1(x, a) = (ax)^{-1}P_1(x, 1)(ax)$ implies that $[P_1(x, a)]^B = x+b\bar{a}x^2+ \cdots$. Now $(\overline{ac})x = (acx)^B = (ax)^B(cx)^B = (\bar{a}x)(\bar{c}x) = (\bar{a}\bar{c}x)$, and $[P_1(x, a+c)]^B = x+b\overline{(a+c)}x^2+ \cdots = [P_1(x, a)]^B[P_1(x, c)]^B = x+b(\bar{a}+\bar{c})x^2+ \cdots$.

Since $b\neq 0$ and the field transformation has an inverse, these equations show that $a\rightarrow\bar{a}$ is a field automorphism. This completes the proof of Theorem 5.

6. **Results valid when the base field is infinite and has finite characteristic p not equal to** 2; **proof of Theorem** 2. Because of §§4 and 5, any automorphism can be reduced by use of inner automorphisms and a field automorphism to an automorphism C such that $(ax)^C = ax$ and $[P_1(x, a)]^C = x+abx^2+ \cdots$, $b\neq 0$. Now let $f^D = (bx)f^C(bx)^{-1}$.

LEMMA 12. *$[P_1(x, a)]^D = P_1(x, a)$.*

Let $[P_1(x, 1)]^D = \sum_1^\infty a_ix^i$. Since $P_1(x, a) = (ax)^{-1}P_1(x, 1)(ax)$, it will be sufficient to show that for any k the first k a_i's are equal to one. In any case $a_1=a_2=1$. Now choose c so that c is not the root of any polynomial with integral coefficients of degree less than k. This is possible since there are only a finite number of such polynomials and there are an infinite number of field elements. Then applying D to the equation $(cx)^{-1}P_1(x, 1)(cx)P_1(x, 1) = [(c+1)^{-1}x]P_1(x, 1)[(c+1)x]$ shows that the same equation holds with $P_1(x, 1)$ replaced by $\sum_1^\infty a_ix^i$. Comparing nth terms yields $c^{n-1}a_n+a_n$ $+$(terms in lower a_i) $=a_n(c+1)^{n-1}$. Because of the way c was chosen, this equation successively determines a_n if $n\leqq k$ and $n\neq 1+p^m$, $m=0, 1, 2, \cdots$.

Now it is also true that

$$(cx)^{-1}P_1(x, 1)(cx)P_1(x, 1) = P_1(x, 1)(cx)^{-1}P_1(x, 1)(cx).$$

Again, an application of D gives an equation for $\sum_1^\infty a_ix^i$. Comparing $(n+1)$st terms gives

$$c^n a_{n+1} + c^{n-1}a_n n + 2ca_{n-1} + a_{n+1} + \text{(terms in lower } a_i\text{'s)}$$
$$= a_{n+1} + ca_n n + 2a_n c^{n-1} + c^n a_{n+1} + \text{(terms in lower } a_i\text{'s)}.$$

This determines a_n successively if $n<k-2$ and $n\neq 2+mp$, $m=0, 1, 2, \cdots$. This and the preceding paragraph show that a_n is uniquely determined for $3\leqq n<k-2$. Since $P_1(x, 1)$ satisfies the given equations, this shows that the a_n are all 1 for $3\leqq n<k-2$. Since k is arbitrary, this completes the proof.

LEMMA 13. $[P_2(x, a)]^D=P_2(x, a)$.

Since

$$P_2(x,a) = \left[\left(\frac{a+1}{2}\right)x\right]^{-1} P_2(x, 1)\left[\left(\frac{a+1}{2}\right)x\right]\left[\left(\frac{a-1}{2}\right)x\right]^{-1}$$
$$\cdot[P_2(x, 1)]^{-1}\left[\left(\frac{a-1}{2}\right)x\right],$$

it is sufficient to prove that $[P_2(x, 1)]^D=P_2(x, 1)$. By Lemma 10 $[P_2(x, 1)]^D$ has a second coefficient of zero. If its third term were also zero, the second and third terms of all the $[P_k(x, a)]^D$ for $k\geqq 2$ would be zero. Using Lemma 6, all series with first coefficient one would be transformed by D into ones with their third coefficient equal to the square of their second coefficient. No series would be transformed into $x+x^3$. This contradiction shows that the third coefficient of $[P_2(x, a)]^D$ is not zero.

Choose an arbitrary integer $k\geqq 2$ and c in the field such that c is not the root of any polynomial with integral coefficients of degree less than $2k$. Let $[P_2(x, 1)]^D=\sum_1^\infty b_i x^i$. It is already known that $b_1=1$, $b_2=0$, and $b_3\neq 0$. The equation $(cx)^{-1}P_2(x, 1)(cx)P_2(x, 1)=P_2(x, 1)(cx)^{-1}P_2(x, 1)(cx)$ when transformed by D gives the following equation when $(n+2)$nd coefficients are compared:

$$c^{n+1}b_{n+2} + c^{n-1}b_n nb_3 + 3c^2b_3b_n + b_{n+2} + \text{(terms in lower } b_i\text{)}$$
$$= b_{n+2} + nb_nc^2b_3 + 3b_3c^{n-1}b_n + c^{n+1}b_{n+2}.$$

These determine b_n successively for $3<n\leqq 2k+3$ and $n\neq 3+mp$, $m=1, 2, \cdots$.

It is also true that

$$\left[\left(\frac{c^2-1}{2c}\right)x\right]^{-1} P_2(x, 1)\left[\left(\frac{c^2-1}{2c}\right)x\right] P_2(x, 1)$$
$$= \left[\left(\frac{c^2+1}{2c}\right)x\right]^{-1} P_2(x, 1)\left[\left(\frac{c^2+1}{2c}\right)x\right].$$

Applying D and comparing nth terms gives

$$\left[\frac{c^2-1}{2c}\right]^{n-1} b_n + b_n + (\text{terms in lower } b_i) = b_n\left[\frac{c^2+1}{2c}\right]^{n-1}.$$

For $3<n\leqq k$ and $n\neq 1+2p^m$, $m=1, 2, \cdots$, these equations determine the b_n successively.

Combining the last two results and the fact that k is arbitrary shows that all the b_n are determined except the third. Since $P_2(x, b_3)$ satisfies the given equations, $[P_2(x, 1)]^D=P_2(x, b_3)$. Now the reasoning of the second paragraph of §3 part L and §3 part M completes the proof of the lemma.

The reasoning of §2 part N shows that D is the identity. Since D was obtained from an arbitrary automorphism by inner automorphisms and a field automorphism, this completes the proof of Theorem 2.

Rutgers, The State University,
New Brunswick, New Jersey