BULL. AUSTRAL. MATH. SOC. 12E05, 12F05
VOL. 30 (1984), 335-356 (08A35)

DOES THE FROBENIUS ENDOMORPHISM ALWAYS GENERATE A DIRECT SUMMAND IN THE ENDOMORPHISM MONOIDS OF FIELDS OF PRIME CHARACTERISTIC?

PÉTER PRÖHLE

Let r be a given prime. Then a monoid M is the endomorphism monoid of a field of characteristic r if and only if either M is a finite cyclic group or M is a right cancellative monoid and M has an element of infinite order in its centre. The main lemma is the technical base of the present and other papers.

Introduction

J. De Groot [4] asked whether the automorphism groups of fields can be prescribed or, at least, whether there exists a field the automorphism group of which is isomorphic to the infinite group of integers. W. Kuyk [5] solved the special question of J. De Groot by proving the existence of a field in question. As a corollary of a much stronger result the original problem of J. De Groot is solved by E. Fried and J. Kollár [2]: A monoid is isomorphic to the endomorphism monoid of a field of characteristic zero if and only if the monoid is right cancellative. Moreover they proved that each group occurs as the automorphism group of a field of characteristic r, where r is a given odd prime. The mapping sending each element to its r^{th}-power is called the Frobenius endomorphism. Because of the difficulties occurring in the case of odd prime characteristic J. Kollár

Received 16 April 1984.

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

asked exactly the same question as the title above. The aim of the present paper is to prove as an answer the theorem which can be found in the abstract.

Review of the technique

For the basic notions and for the customary technique see the textbooks of G. Grätzer [3], of A. Pultr and V. Trnková [6] and of B. L. van der Waerden [9].

Up to now there was no result concerning the endomorphism monoids of fields of characteristic two, because the endomorphisms in that case can not be handled by adding square roots. Only the case $q = 2$ of the third lemma, that means the case of extensions by square roots, was known: the first lemma in E. Fried [1] and the sixteenth, the twenty-third and the twenty-fourth lemma in E. Fried and J. Kollár [2]. It was obvious that it should be enough to take third roots instead of square roots, but it seemed to be hopeless to calculate the occurring technical details. The case $q = 3$ of the third lemma solves these problems.

In order to make the generatum of the Frobenius endomorphism not to be a direct summand an essential change is needed in the conventional technique: at the process of extension, independent systems of new elements must be added instead of adding single elements. It must be done in such a way that the motion of the elements inside these systems must imitate the motion of the whole field. In consequence of the existence of the Frobenius endomorphism none of the single elements would be fixed, but such a system of elements can be fixed. This system of elements is nothing else but the unary algebra appearing in the main lemma.

Field theoretic investigations

ABEL'S THEOREM. *A polynomial* x^k-b *of prime degree* k *over a field* L *is reducible if, and only if,* b *is a* k^{th}*-power in* L.

A simple proof can be found in the textbook of L. Rédei [7].

FIRST LEMMA. *Let* L *be a field of characteristic* r. *Consider the pure algebraic extension* $L(t)$, *where* x^n-t^n *is an irreducible polynomial in the ring* $L[x]$, *and* n *is a prime different from* r. *Let* m *be an integer, where* $r \nmid m$ *and* $2 \leq m$. *Then the* m^{th}*-power of an element of* $L(t)$

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

belongs to the subfield L *if and only if the element is of the form* $c\cdot t^k$ *, where* $c \in L$ *,* $0 \leq k < n$ *and* $n|km$*. If in addition* $(m,n) = 1$ *then an element of* L *has an* m^{th}*-root in* $L(t)$ *if and only if it has one in* L*.*

Proof. Let K be the smallest algebraic extension of L containing all the n^{th}-roots of unity. The degree of the extension K/L is less than n. So the irreducibility of $x^n - t^n$ over L implies that t^n is never an n^{th}-power in K. Consequently by Abel's theorem $x^n - t^n$ is irreducible over K. So any element b of $K(t)$ can be uniquely written in the form: $b_0 + b_1t + b_2t^2 + \dots \quad \dots + b_{n-1}t^{n-1}$,

where all the coefficients belong to K. Obviously $L(t) \leq K(t)$, and an element b of $K(t)$ belongs to $L(t)$ if and only if each of the coefficients of b belongs to L. Let u be a primitive n^{th}-root of unity. The mapping $t \longrightarrow u\cdot t$ induces a relative automorphism of the extension $K(t)/K$, where the image of b is:

$$b_0 + b_1ut + b_2u^2t^2 + \dots + b_{n-1}u^{n-1}t^{n-1} .$$

If $b^m \in L$, then this image of b must be $v\cdot b$, where v is a suitable m^{th}-root of unity. The uniqueness of the coefficients of $v\cdot b$ gives the following equations: $b_i(u^i - v) = 0$ for $0 \leq i < n$. If $b \neq 0$, then there is an index k for which $b_k \neq 0$. Consequently $u^k - v = 0$, and $b_i = 0$ for $i \neq k$. So $b = b_k\cdot t^k$, where $b \in L(t)$ implies $b_k \in L$. Further $n|km$, since $u^{km} = v^m = 1$. Hence $(m,n) = 1$ yields $k = 0$. This completes the proof of the first lemma.

SECOND LEMMA. *Let* K *be a transcendental extension of* L *such that* K *is an algebraic extension of finite degree with respect to the simple transcendental extension* $L(y)$*. Let* s *be a prime different from the characteristic of* L*. An element is called s-high in a field, if the element has an* s^j*-root in the field for each* $j \in \omega$*. Then each s-high element of* K *belongs to* L*.*

Proof. Let $x \in K \setminus L$. Then y is algebraic over $L(x)$, so K is an algebraic extension of finite degree with respect to $L(x)$. Suppose, that x is s-high. Let ${}_ix$ be an s^i-th root of x. Consider the $L(x) \leq L({}_1x) \leq L({}_2x) \leq \dots \leq L({}_ix) \leq \dots$ infinite chain of fields. As the degree of $K/L(x)$ is finite, there exists an index n such that $L({}_nx) = L({}_{n+1}x)$. So the transcendental element ${}_nx$ has an s^{th}-root in $L({}_nx)$, but that is impossible. So any s-high element must belong to L. This completes the proof of the second lemma.

THIRD LEMMA. *Let p, q and r be three pairwise distinct primes. Let F be a field of characteristic r. Suppose that K is an extension of F generated by the set $\{{}_iz\ ,\ t_v : i \in \omega,\ v \in V\}$, where*

(a) ${}_oz$ *is transcendental over* F

(b) $({}_{i+1}z)^p = {}_iz \qquad i \in \omega$

(c) the elements $T_v = (t_v)^q$ are polynomials from the polynomial ring $F[{}_oz]$, where

- *none of them is constant*
- *none of them is divisible by* ${}_oz$
- *none of them has a multiply factor*
- *they are mutually prime.*

Denote the subfield $F(\{{}_iz\ ,\ t_v : i < j\ ,\ v \in V\})$ of K by $F(j,W)$, for $W \leq V$ and $1 \leq j \leq \omega$. Then the field K has the following properties:

(1) The polynomial $x^p - {}_iz$ is irreducible over $F(i+1,W)$, for $W \leq V$ and $i \in \omega$.

(2) The polynomial $x^q - T_v$ is irreducible over $F(j,W)$, for $W \leq V$, $v \in V \setminus W$ and $1 \leq j \leq \omega$.

(3) If the q^{th}-power of an element of $F(j,W)$ belongs to the subfield $F(k,\emptyset)$, where $W \leq V$ and $k \leq j \leq \omega$, then the element can be written in the form

$$c\cdot\frac{f({}_iz)}{g({}_iz)}\cdot\prod_{w\in W'}(t_w)^{n_w}\ ,$$

where $c \in F$, f and g are mutually prime polynomials over F and both of them have leading coefficients 1, $i \leq k$, W' is a suitable finite subset of W, and $0 < n_w < q$ for $w \in W'$.

(4) K is a transcendental extension of F.

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

(5) *Each s-high element of K belongs to F whenever s is a prime different from p, q and r.*

(6) *Each p-high element of K is of the form $c\cdot({}_iz)^m$, where c is a p-high element of F, $i \in \omega$ and m is an integer.*

Proof. First we prove the second and the third properties in the case of finite W and $j = k = 1$. We prove by induction on the size of the set W.

$F(1,\emptyset)$ is the quotient field of the polynomial ring $F[{}_oz]$, therefore the third property is true in the case of $W = \emptyset$ and $j = k = 1$. If the third property is true for W and $j = k = 1$, then $t_v \in F(1,W)$ would imply an equality of the form

$$g^q({}_oz)\cdot T_v = c^q\cdot f^q({}_oz)\cdot\prod_{w\in W}(T_w)^{n_w} \quad , \quad \text{if } v \in V\setminus W .$$

However, this contradicts one of the conditions on the polynomials T_w. But $t_v \notin F(1,W)$ yields the second property by Abel's theorem, for the case of the same W and $j = 1$. Now suppose that both of the second and the third properties are true for a finite W and $j = k = 1!$ Let $v \in V\setminus W$, $b \in F(1,W \cup \{v\})$ and $b^q \in F(1,\emptyset)$. As $x^q - T_v$ is irreducible over $F(1,W)$ by the assumption, $b = c\cdot(t_v)^n$ by the first lemma. Here $c \in F(1,W)$ and $c^q \in F(1,\emptyset)$, so the form of c is known by the assumption. Consequently b has the desired form, too. So we get the third property for the index-set $W \cup \{v\}$ and $j = k = 1$.

Second, we prove the first property in the case of finite W and $i = 0$, by induction on the size of the set W.

By Abel's theorem it is enough to show that ${}_oz$ has no p^{th}-root in $F(1,W)$. The existence of a p^{th}-root of ${}_oz$ in $F(1,\emptyset)$ would imply a polynomial equation $g^p({}_oz)\cdot{}_oz = c^p\cdot f^p({}_oz)$, where f and g are mutually prime. But this equation is a contradiction. The first lemma gives the inductive step of the proof, as we have seen the irreducibility of $x^q - T_v$ over $F(1,W)$ for finite W.

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

Third, we prove the first and the second properties. If we replace the elements ${}_0z, {}_1z, {}_2z$ .... with ${}_iz, {}_{i+1}z, {}_{i+2}z$ .... , then the conditions remain satisfied in the third lemma. So the polynomials $x^q - T_v$ and $x^p - {}_iz$ are irreducible over $F(i+1,W)$ for finite $W \leq V$, $v \in V \setminus W$ and $i \in \omega$. The reducibility of a polynomial over a field L needs only finitely many coefficients from L, therefore a reducible polynomial is also reducible over a suitable finitely generated subfield of L. So we get the first and the second properties by an indirect proof.

Fourth, we prove the third property. As the polynomial $x^p - {}_iz$ is irreducible over $F(i+1,W)$ for $i \in \omega$, the first lemma shows that if the q^{th}-power of an element of $F(i+2,W)$ belongs to $F(i+1,W)$, then the element also belongs to $F(i+1,W)$. So if an element of $F(1,\emptyset)$ has a q^{th}-root in $F(\omega,W)$, then this q^{th}-root lies in $F(1,W)$. On the other hand ${}_iz$ can play the role of ${}_0z$. Consequently we get the third property for finite j, k and W. Finally each element of $F(j,W)$ belongs to a field $F(i+1,W')$ for suitable finite $W' \leq W$ and $i < j$.

Fifth, we prove the fourth property. Let x be an algebraic element of K over F. Let $L = F(x)$. The element ${}_0z$ is transcendental over L, since x is algebraic. All the other conditions of the third lemma are also satisfied with respect to L instead of F. Therefore the system $1, t_v, t_v^2, \ldots, t_v^{q-1}$ form a basis of the field extension $L(\omega, W \cup \{v\})/L(\omega,W)$ for $v \in V \setminus W$, such that an element belongs to $F(\omega, W \cup \{v\})$ if and only if the coefficients of the element with respect to this basis belong to $F(\omega,W)$. Consequently $x \in F(\omega, W \cup \{v\})$ implies $x \in F(\omega,W)$, since the coefficients of x must belong to $F(\omega,W)$ and $x \in L \leq L(\omega,W)$. So $x \in F(\omega,\emptyset)$. Therefore $x \in F({}_iz)$ for a suitable $i \in \omega$. But $F({}_iz)$ is a pure transcendental extension of F, so $x \in F$.

Sixth, we prove the fifth property. Let x be s-high in K. Clearly $x \in F(i,W)$ for a suitable $i \in \omega$ and a finite $W \leq V$. Using the first lemma and the first and the second properties we get that x is s-high in $F(i,W)$ too. Now we can apply the second lemma for $F(i,W)$, so $x \in F$.

Seventh, we prove the sixth property. Let x be a p-high element of K. Then $x \in F(\omega,W)$ for a suitable finite $W \leq V$. By the first lemma and by the second property x is p-high in the subfield $F(\omega,W)$, too. So it is enough to prove the following statement by induction on the size of the set W: "For finite $W \leq V$ the p-high elements of $F(\omega,W)$ are of the form $c\cdot({}_iz)^m$." .

If $W = \emptyset$, then $x \in F(i+1,\emptyset) = F({}_iz)$ for suitable $i \in \omega$. So $x = ({}_iz)^m\cdot(f({}_iz)/g({}_iz))$, where m is an integer, ${}_iz \nmid f({}_iz)$ and ${}_iz \nmid g({}_iz)$. Here $(f({}_iz)/g({}_iz))$ must be p-high in $F(\omega,\emptyset)$. Suppose that there exists an element $y \in F(\omega,\emptyset)\setminus F(i+1,\emptyset)$ such that $y^p \in F(i+1,\emptyset)$ and some p^j-th power of y is $f({}_iz)/g({}_iz)$.

Let $k = \max\{n : y \notin F(n+1,\emptyset)\}$. By the first lemma and by the first property $y = ({}_{k+1}z)^b\cdot(u({}_kz)/v({}_kz))$, where u and v are polynomials over F, and $0 < b < p$. Now we arrive at the equation $({}_kz)^{b\cdot p^{j-1}}\cdot(u({}_kz))^{p^j}\cdot g({}_iz) = f({}_iz)\cdot(v({}_kz))^{p^j}$ in the polynomial ring $F[{}_kz]$. Consider the powers of the irreducible factor ${}_kz$ in that equation. As ${}_iz$ is irreducible in $F[{}_iz]$, therefore ${}_iz \nmid f({}_iz)$ implies $({}_iz,f({}_iz)) = 1$ in $F[{}_iz]$. So $({}_iz,f({}_iz)) = 1$ in $F[{}_kz]$ too. Consequently ${}_kz \nmid f({}_iz)$, and by a similar argument ${}_kz \nmid g({}_iz)$. The exponent of ${}_kz$ in $({}_kz)^{b\cdot p^{j-1}}\cdot(u({}_kz))^{p^j}\cdot g({}_iz)$ is congruent to $b\cdot p^{j-1}$ modulo p^j , while the exponent of ${}_kz$ in $f({}_iz)\cdot(v({}_kz))^{p^j}$ is divisible by p^j. This is a contradiction, and so the quotient $f({}_iz)/g({}_iz)$ must be p-high even in $F(i+1,\emptyset)$. Therefore by the second lemma $(f({}_iz)/g({}_iz)) \in F$, consequently x has the form $c\cdot({}_iz)^m$, which we had to prove.

Now we suppose that there exists a $w \in W$ and the statement is true for $W \setminus \{w\}$. Let $L = F(\omega,W\setminus\{w\})$ and $K = F(\omega,W)$. By the second property the degree of the extension K/L is q. Let $N(d)$ denote the norm of d with respect to K/L for $d \in K$. Only the following property of the norm will be used: N is a multiplicative mapping from K into L such that $N(d) = d^q$ for $d \in L$. For the details see L. Rédei [7] and B. L. van der Waerden [9]. $N(x)$ is p-high in L as x is p-high in K. So the element $y = x^q/N(x)$ is p-high in K. Clearly $y \in F(i+1,W)$ for a suitable $i \in \omega$. Suppose that there exists an element $u \in F(\omega,W) \setminus F(i+1,W)$ such that $u^p \in F(i+1,W)$ and y is a p^j-th power of u. Let $k = \max\{n : u \notin F(n+1,W)\}$. By the first lemma and by the first property $u = h\cdot({}_{k+1}z)^b$, where $h \in F(k+1,W)$ and $0 < b < p$. $N(u) = N(h)\cdot(N({}_{k+1}z))^b = N(h)\cdot({}_{k+1}z)^{bq}$. So $N(u) \notin F(k+1,W)$, as $N(h) \in F(k+1,W)$ and $p \nmid bq$. On the other hand, $N(y)$ is the p^j-th power of $N(u)$ and $N(y) = N(x^q/N(x)) = (N(x))^q/N(N(x)) = 1$. But this is a contradiction, because by the fourth property $N(u) \notin F(k+1,W)$ implies that $N(u)$ is a transcendental element, while its p^j-th power should be 1. Therefore y must be p-high even in $F(i+1,W)$. Consequently by the second lemma $y \in F$, and therefore $y\cdot N(x)$ is a p-high element of L. So by the induction hypothesis $y\cdot N(x)$ has the form $c\cdot({}_iz)^m$. Using the third property, we get:

$$c\cdot({}_iz)^m = y\cdot N(x) = x^q = d^q\cdot\frac{f^q({}_iz)}{g^q({}_iz)}\cdot\prod_{w\in W}(T_w)^{n_w} \ .$$

This implies that $n_w = 0$, $g({}_iz) = 1$, $q|m$ and $f({}_iz) = ({}_iz)^{(m/q)}$. So x also has the desired form: $x = d\cdot({}_iz)^{(m/q)}$. This completes the proof of the third lemma.

THE MAIN LEMMA (FIRST PART). *Let p, q and r be three pairwise distinct primes. Let F be a field of characteristic r. Let Y be a set disjoint to F. Let f be a unary operation over Y, where f is injective and none of the powers of f has a fix-point. Let E be a subset of $F \times Y$ such that $\langle a,y\rangle \in E$ if and only if*

$\langle a^r, f(y)\rangle \in E$, *and finally* $c \in F$ *has an* r^{th}*-root in* F *whenever* $\langle c, f(y)\rangle \in E$ *for some* $y \in Y$.

Let ${}_0y = y$ *for* $y \in Y$, $A(y) = \{a : \langle a,y\rangle \in E\}$ *and* $B(y) = \{1,\ a,\ a^{11} : \langle a,y\rangle \in E\}$. *Then the following property uniquely determines a field denoted by* $F(E,(Y,f),p,q)$:

"$F(E,(Y,f),p,q)$ *is the extension of* F *generated by the set* $R = \{{}_iy\ ,\ t(b,y) : i \in \omega\ ,\ b \in B(y)\ ,\ y \in Y\}$, *where:*

(a) y *is transcendental over the subfield* $F(X)$, *whenever the subset* X *of* Y *and the one element subset* $\{y\}$ *of* Y *generate disjoint subalgebras in the unary algebra* (Y,f)

$$\left.\begin{array}{ll} \text{(b)} & \left.\begin{array}{l} ({}_{i+1}y)^p = {}_iy \\ ({}_iy)^r = {}_i(f(y)) \end{array}\right\} i \in \omega \\ \\ \text{(c)} & \left.\begin{array}{l} (t(b,y))^q = y - b \\ (t(b,y))^r = t(b^r, f(y)) \end{array}\right\} b \in B(y) \end{array}\right\} y \in Y \qquad .''\ .$$

IMPORTANT DEFINITIONS. On the set R we define a *unary algebra* (R,g) as follows: $g({}_iy) = {}_i(f(y))$ and $g(t(b,y)) = t(b^r, f(y))$ for $i \in \omega$, $b \in B(y)$, and $y \in Y$. We will use the following occasional nomenclature:

$F(E,(Y,f),p,q)$	*special extension*
$F(E,(Y,f),p,q)\setminus F$	*the skin of the extension*
Y	*the variables of the skin*
(Y,f)	*the unar of the skin*
(F,E,Y)	*the bipartite graph of the skin*
R	*the roots of the skin*
(R,g)	*the unar of the roots.*

Let $F(E,(Y,f),p.q)$ and $F''(E'',(Y'',f''),p,q)$ be two special extensions, where both of F and F'' have the same characteristic. An injective mapping $m : F \cup Y \longrightarrow F'' \cup Y''$ is called a *pre-morphism*,

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

if the restrictions $m|_{F} : F \longrightarrow F''$, $m|_{Y} : (Y,f) \longrightarrow (Y'',f'')$ and $m|_{F\cup Y} : (F,E,Y) \longrightarrow (F'',E'',Y'')$ are field, unar and graph homomorphism respectively. An injective mapping $m : F\cup R \longrightarrow F'' \cup R''$ is called a *pre-homomorphism*, if the restriction $m|_{F\cup Y} : F\cup Y \longrightarrow F'' \cup Y''$ is a pre-morphism, the restriction $m|_{(R,g)} : (R,g) \longrightarrow (R'',g'')$ is a unar-homomorphism, $m({}_{i}y) = {}_{i}(m(y))$ and $m(t(b,y)) = t(m(b),m(y))$ for $i \in \omega$, $b \in B(y)$, and $y \in Y$. A field homomorphism of $F(E,(Y,f),p,q)$ into $F''(E'',(Y'',f''),p,q)$ sending the subfield F into F'' and sending the subset R into R'' , is called a *special-homomorphism*. If the two special extensions are the same, then we use the expression "*endo*" instead of "*homo*".

THE MAIN LEMMA (SECOND PART). *Let us take two special extensions: $F(E,(Y,f),p,q)$ and $F''(E'',(Y'',f''),p,q)$, where each of the sets $A(y)$ and $A(y'')$ is algebraically independent over the primefield for $y \in Y$ and $y'' \in Y''$. Then the following statements hold:*

(a) For each special homomorphism h of $F(E,(Y,f),p,q)$ into $F''(E'',(Y'',f''),p,q)$ the restriction $h|_{F\cup Y}$ is a pre-morphism, and the restriction $h|_{F\cup R}$ is a pre-homomorphism.

(b) Each pre-morphism has a unique extension among the special homomorphisms.

(c) The category whose objects are the special extensions and whose morphisms are the special homomorphisms is naturally equivalent to the category whose objects are the special extensions and whose morphisms are the pre-morphisms.

Proof of the first part of the main lemma. First of all we fix a well ordering $(Y,<)$ of the variables. For $y \in Y$ let $K_y = F_y(\{{}_{i}y, t(b,y) : i \in \omega , b \in B(y)\})$, where $F_y = F(\{{}_{i}u, t(b,u) : i \in \omega , b \in B(u) , u \in Y$ and $u < y\})$. The special extension $F(E,(Y,f),p,q)$ must be the union of the ascending chain of the subfield K_y , so it is enough to prove the unique existence of the subfields F_y and K_y by transfinite induction on $y \in (Y,<)$.

If $y \in Y$ is the least element of $(Y,<)$, then F_y must be F. If y is not the least element of $(Y,<)$, then F_y must be $\cup\{K_u : u \in Y \quad u < y\}$, where the subfields K_u form an ascending chain. Finally we show that K_y uniquely exists, if F_y does the same. Here we have three cases:

First case : the variable y belongs to the subalgebra generated by $\{u : u \in Y \quad u < y\}$ in (Y,f). So there is a $u < y$ and a $j \in \omega$ such that y is the j^{th} image of u under the operation f. By the conditions ${}_iy$ must be $({}_iu)^{r^j}$ for $i \in \omega$, and $t(b,y)$ must be $(t(\sqrt[r^j]{b},u))^{r^j}$ for $b \in B(y)$. So in this case $K_y = F_y$.

Second case : the variable y does not belong to the subalgebra generated by $\{u : u \in Y \quad u < y\}$ in (Y,f), but the subalgebras generated by $\{u : u \in Y \quad u < y\}$ and $\{y\}$ are not disjoint. So there is a $u < y$ and a $0 \neq j \in \omega$ such that u is the j^{th} image of y under the operation f. So $F_y(y)$ must be the pure inseparable extension of F_y by the polynomial $(x)^{r^j} - u$. Now ${}_iy$ must belong to $F_y(y)$ as the element $\sqrt[r^j]{{}_iu}$ does for $i \in \omega$, and $t(b,y)$ must belong to $F_y(y)$ as the element $\sqrt[r^j]{t(b^{r^j},u)}$ does for $b \in B(y)$. So in this case $K_y = F_y(y)$.

Third case : the subalgebras generated by $\{u : u \in Y \quad u < y\}$ and by $\{y\}$ are disjoint subalgebras of (Y,f). So y is transcendental over $F(\{u : u \in Y \quad u < y\})$. On the other hand F_y is an algebraic extension of $F(\{u : u \in Y \quad u < y\})$, therefore y is transcendental over F_y. By the conditions $({}_{i+1}y)^p = {}_iy$ for $i \in \omega$. The elements $y - b = (t(b,y))^q$ are polynomials from the polynomial ring $F_y[y]$ for $b \in B(y)$, where none of them is a constant, none of them is divisible by y, none of them has a multiply factor and they are mutually prime. So the third lemma can be used for the extension K_y of F_y. By the first property $F_y({}_{i+1}y)$ must be the simple algebraic extension of $F_y({}_iy)$ by the irreducible polynomial $x^p - {}_iy$ for $i \in \omega$. Further $F_y(\{{}_iy : i \in \omega\})$ must be the union of the ascending chain $F_y \le F_y(y) \le F_y({}_1y) \le F_y({}_2y) \le \dots \quad \dots \le F_y({}_iy) \le \dots$. Now we fix a well-ordering $(B(y),<)$. Let $F_{yb}^{\le} = F_{yb}^{<}(t(b,y))$, where

$F_{yb}^{<} = F_y(\{t(c,y) : c \in B(y) \quad c < b\})$ for $b \in B(y)$. Clearly K_y must be the union of the ascending chain of the subfields $F_{yb}^{\le}$, so it is enough to prove the unique existence of the subfields $F_{yb}^{<}$ and $F_{yb}^{\le}$ by transfinite induction on $b \in (B(y),<)$. If $b \in B(y)$ is the least element of $(B(y),<)$, then $F_{yb}^{<}$ must be F_y. If b is not the least element of $(B(y),<)$, then $F_{yb}^{<}$ must be $\cup\{F_{yc}^{\le} : c \in B(y) \quad c < b\}$, where the subfields $F_{yc}^{\le}$ form an ascending chain. Finally by the second property $F_{yb}^{\leqslant}$ must be the simple algebraic extension of $F_{yb}^{<}$ by the irreducible polynomial $x^q - (y - b)$. This completes the proof of the first part of the main lemma.

To prove the second part of the main lemma we need the following four sublemmas. The first three sublemmas have a common condition: "Let us take a special extension $F(E,(Y,f),p,q)$, where each set $A(y)$ is an algebraically independent system of elements over the primefield, for $y \in Y$." .

FIRST SUBLEMMA. *Let $Q(x)$ denote the following sentence: "There exists a non-zero element u in F and an element w in $F(E,(Y,f),p,q) \setminus F$, where w is p-high in $F(E,(Y,f),p,q)$, $w-u$ is the q^{th}-power of an element v of $F(E,(Y,f),p,q)$, and $x = u/w$." .*

Then $Q(x)$ is equivalent to the following: "The bipartite graph of the skin has an edge $<a,y>$ such that $x \in \{1/y \; , \; a/y \; , \; a^{11}/y\}$." .

Proof. First of all we fix a well ordering $(Y,<)$ of the variables. Now we use the same notation as in the proof of the first part of the main lemma. Suppose that x is an element satisfying $Q(x)$! Set $z = \min\{y : w$ is algebraic over $K_y\}$. Clearly w is transcendental over F_z , consequently z is transcendental over F_z. Let $Y_z = \{y :$ the subalgebras generated by $\{y\}$ and $\{z\}$ in (Y,f) are not disjoint}. By the fourth property the algebraic hull of K_z in the special extension is $F_z(\{R_y : y \in Y_z\})$, where $R_y = \{{}_iy, t(b,y) : i \in \omega, b \in B(y)\}$ for $y \in Y_z$. Since w belongs to this algebraic hull, there exists a $y \in Y_z$ such that $w \in F_z(R_y)$ but $w \notin F_z(R_{f(y)})$. As the algebraic hull in question is a pure inseparable extension of $F_z(R_y)$, w is p-high in $F_z(R_y)$ and $(w - u) \in F_z(R_y)$ yields $v \in F_z(R_y)$. So the third lemma can be used for the extension $F_z(R_y)$ of F_z, since y must be transcendental as the element z is. So $w = e\cdot({}_iy)^k$, where e is a non-zero p-high element of F_z, $i \in \omega$ and k is a non-zero integer. It can be supposed that $p|k$ occurs only if $i = 0$. Further

$$v = c\cdot\frac{G({}_iy)}{H({}_iy)}\sqrt[q]{({}_oy - b_1)^{k_1}\cdot({}_oy - b_2)^{k_2}\cdot \ldots \quad \ldots \cdot({}_oy - b_n)^{k_n}}$$

where $0 \neq c \in F_z$, G and H are mutually prime polynomials over F_z and both of them have leading coefficients 1, $n \in \omega$, $b_1, b_2 \ldots b_n$ are different from each other element from $B(y)$, and $0 < k_j < q$ for $j = 1, 2 \ldots n$. Set $t = {}_iy$. According to the sign of k we get one of the following equations in the polynomial ring $F_z[t]$:

$$H^q(t)\cdot(e\cdot t^k - u) = c^q\cdot G^q(t)\cdot(t^{p^i} - b_1)\cdot \ldots \cdot(t^{p^i} - b_n) \text{ if } k > 0$$
$$H^q(t)\cdot(e-(t^{-k})\cdot u) = c^q\cdot G^q(t)\cdot(t^{-k})\cdot(t^{p^i} - b_1)\ldots\cdot(t^{p^i} - b_n) \text{if } k < 0 .$$

$r|k$ would imply that $w \in F_z(R_{f(y)})$, therefore $r\nmid k$. By the assumptions none of the elements $e, u, b_1, b_2 \ldots b_n$ is zero. Therefore each of the binomials occurring in the equations is a proper binomial. So none of them has multiply factor, as $r\nmid k$ and $r\nmid p^i$. In both cases $G^q(t)$ divides the binomial standing at the left side, so $G^q(t) = 1$. In the first case a similar argument shows that $H^q(t) = 1$. In the second case

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

we get only that $H^q(t) \nmid t^{-k}$. But $e \neq 1$ yields that $t^{-k} | H^q(t)$, so $H^q(t) = t^{-k}$. Consequently $q|k$ if $k < 0$. Now in both cases the degree of the left side is $|k|$, and the degree of the right side is $n \cdot p^i$. So $n \neq 0$ and $i = 0$, since $k \neq 0$ and $i \neq 0$ implies $p \nmid k$. Now $n = 1$, since the quotient of any two different elements of $B(y)$ is never an nth-root of unity. The second case is impossible as $q|k = -n = -1$.

So the only possible case is the following: $e \cdot y - u = c^q(y - b)$. Consequently we have that $x = u/(ey) = b_1/y$. The other direction of the equivalence is trivial. This completes the proof.

SECOND SUBLEMMA. *Let $E(a,y)$ denote the following sentence: "The two elements a and y are transcendental over the primefield, $Q(1/y)$, $Q(a,y)$ and $Q(a^{11}/y)$."* .

Then $E(a,y)$ is equivalent to the following: "$\langle a,y \rangle$ is an edge of the bipartite graph of the skin." .

Proof. Let the elements a and y satisfy $E(a,y)$! Then by the first sublemma there are variables y_k and elements $b_k \in B(y_k)$, such that $a^k/y = b_k/y_k$ for $k = 0, 1, 11$. The equation $(a/y)^{11} = (1/y)^{10} \cdot (a^{11}/y)$ implies that:

$$\frac{b_1^{11}}{y_1^{11}} = \frac{b_0^{10}}{y_0^{10}} \cdot \frac{b_{11}}{y_{11}} \quad .$$

As the elements b_k are different from zero, each of these three variables y_k is algebraically dependent from the two others over F. So by the structure of the variables we get that $y_0 = (y_1)^{r^i}$ and $y_{11} = (y_1)^{r^j}$, where i and j are integers. Consequently $10r^i + r^j - 11 = 0$, since $y_1^{(10r^i + r^j - 11)} \in F$ and y is transcendental over F. $r^i = ((11 - r^j)/10) < (11/10) < 2$ implies that $i \leq 0$. Suppose that $i < 0$. Then $r^j = (11 - 10r^i) > (11 - 10) = 1$ implies $j > 0$. Consequently the element $10r^i = 11 - r^j$ must be an integer, so $i = -1$ and $r \in \{2,5\}$. But the equation $r^j = 11 - 10/r$ is a contradiction if

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

$r \in \{2,5\}$. So i must be zero. Therefore by $r^j = (11 - 10r^0) = 1$ the element j must also be zero. This means that $y_0 = y_1 = y_{11}$, and therefore $b_1^{11} = b_0^{10}.b_{11}$. Here the algebraic independence of $A(y_1)$ implies the existence of a suitable $c \in A(y_1)$ such that $\{b_0,b_1,b_{11}\} \leq \{1,c,c^{11}\}$. On the other hand b_0, b_1 and b_{11} are three pairwise distinct elements, because the three quotients $1/y$, a/y and a^{11}/y are also pairwise distinct. Consequently $\langle b_0,b_1,b_{11}\rangle$ is a permutation of $\langle 1,c,c^{11}\rangle$. So we have to solve the equation $11i = 10j + k$ where $\langle i,j,k\rangle$ is a permutation of $\langle 0,1,11\rangle$. The only solution is: $i = 1$, $j = 0$, $k = 11$. So we arrive at the equations $1/y = 1/y_1$, $a/y = c/y_1$ and $a^{11}/y = c^{11}/y_1$. Consequently $y = y_1$ is a variable, and $a = c \in B(y_1) = B(y)$. The other direction of the equivalence is trivially true. This completes the proof.

THIRD SUBLEMMA. *Let $V(y)$ denote the following sentence: "$y \neq 0$, and $Q(1/y)$, and for all a and z from $F(E,(Y,f),p,q)$, $E(a,z)$ implies that both of (a/z) and (a^{11}/z) are different from $(1,y)$." . Then $V(y)$ is equivalent to the following: "y is a variable of the skin."* .

Proof. Let y be an element satisfying $V(y)$! So by the first sublemma $(1/y) = (b/u)$, where u is a suitable variable of the skin and $b \in B(u)$. If $A(u) = \emptyset$, then $B(u) = \{1\}$, and therefore $b = 1$. If $A(u) \neq \emptyset$, then for $a \in A(u)$ $E(a,u)$ and $E(a^{11},u)$, and therefore both of (a,u) and (a^{11}/u) are different from (b/u). So even in the case of $A(u) \neq \emptyset$, the only possibility is $b = 1$. Consequently in both cases $y = u$ is a variable. The other direction of the equivalence is trivially true. This completes the proof.

FOURTH SUBLEMMA. *Under the condition of the second part of the main lemma, suppose that a given homomorphism h of $F(E,(Y,f),p,q)$ into $F''(E'',(Y'',f''),p,q)$ maps the subfield F into F'' ! Then the following implications hold:*

(a) if $h(x) \notin F''$ and $Q(x)$, then $Q''(h(x))$

(b) if $h(y) \notin F''$ and $E(a,y)$, then $E''(h(a),h(y))$

(c) if $h(y) \notin F''$ *and* $V(y)$ *, then* $Q''(1/h(y))$

(d) if none of the sets $A(y)$ *and* $A(y'')$ *is empty, then if* $h(y) \notin F''$ *and* $V(y)$ *, then* $V''(h(y))$.

Note: in particular, each of these implications holds if h *is a special homomorphism.*

Proof. (a) The validity of $Q(x)$ is certified by suitable elements u, v and w. The images of these elements certify the validity of $Q''(h(x))$, since $h(w) \notin F''$ by the assumption $h(x) \notin F''$.

(b) We have only to use the definition of $E(a,y)$ and the implication (a) of the present sublemma.

(c) We can use the implication (a), since $V(y)$ implies $Q(1/y)$.

(d) If none of the sets $A(y)$ is empty, then $V(y)$ is equivalent to the formula $\exists a(E(a,y))$. Using this equivalence and the implication (b) we get the implication (d). This completes the proof.

Proof of the second part of the main lemma. (a) Let y be an arbitrary variable from Y. Using the first sublemma and the implication (c) of the fourth sublemma we get $h(y) = x/b$, where $x \in Y''$ and $b \in B(x)$. But $h(y) \in R''$ implies that $b = 1$. Consequently each special homomorphism maps the set Y into Y''. Clearly the restriction $h|_{F\cup Y}$ is an injective mapping into $F'' \cup Y''$, and $h|_F$ is a field homomorphism of F into F''. The implication (b) of the fourth sublemma shows that $h|_{F\cup Y}$ is a homomorphism of the bipartite graph (F,E,Y) into (F'',E'',Y''). $h|_Y$ is a unar homomorphism of (Y,f) into (Y',f''), since $h(f(y)) = h(y^r) = (h(y))^r = f''(h(y))$. So the restriction $h|_{F\cup Y}$ is really a pre-morphism.

The restriction $h|_R$ is really a unar homomorphism of (R,g) into (R'',g''), since $h(g({}_iy)) = h(({}_iy)^r) = (h({}_iy))^r = g''(h({}_iy))$ and $h(g(t(b,y))) = h((t(b,y))^r) = (h(t(b,y)))^r = g''(h(t(b,y)))$. For $b \in B(y)$ $(h(t(b,y)))^q = h((t(b,y)^q)) = h(y - b) = h(y) - h(b) = (t(h(b),h(y)))^q$, therefore $(h(t(b,y))/t(h(b),h(y)))^q = 1$. But both elements of the quotient belong to R'' , so they must be equal. Now we prove that $h({}_iy) = {}_i(h(y))$ for $i \in \omega$. The case of $i = 0$ is clear, now we proceed by induction on i. $(h({}_{i+1}y))^p = h(({}_{i+1}y)^p) = h({}_iy) = {}_i(h(y)) = ({}_{i+1}(h(y)))^p$, therefore $(h({}_{i+1}y)/{}_{i+1}(h(y)))^p = 1$. But the quotient of two different elements from R'' is never a p^{th}-root of unity. So $h({}_{i+1}y) = {}_{i+1}(h(y))$. Summing up, we have proven that $h\big|_{F \cup R}$ is a pre-homomorphism.

(b) The uniqueness of the required extension is clear since the set R generates the field extension $F(E,(Y,f),p,q)/F$, further the restriction to $F \cup R$ of any possible extension must be a pre-homomorphism and this pre-homomorphism is uniquely determined by the given premorphism. So the only problem is the existence of the extension.

Let K be the subfield of $F''(E'',(Y'',f''),p,q)$ generated by the range of the pre-homomorphism generated by the given pre-morphism. By the first part of the main lemma there is an isomorphism of $F(E,(Y,f),p,q)$ onto K, which is an extension of the given pre-morphism. On the other hand there exists the natural embedding of K into $F''(E'',(Y'',f''),p,q)$. But the composition of that isomorphism and this natural embedding is just the special homomorphism we need.

(c) The restriction of the special homomorphisms to $F \cup Y$ is an identity and composition preserving bijection between the special homomorphisms and the pre-morphisms. This completes the proof of the second part of the main lemma.

Proof of the theorem which can be found in the abstract. The endomorphism monoid of a field is always right cancellative, since the endomorphisms of fields are injective. The transformation sending each element into its r^{th}-power is always an endomorphism, the so-called Frobenius endomorphism. The Frobenius endomorphism always belongs to the centre of the endomorphism monoid. If the order of the Frobenius endomorphism is finite, say k , then each element is equal to its own r^k-th power. Consequently the field must be finite in this case. But the endomorphism monoids of finite fields are finite cyclic groups.

Conversely if M is a finite cyclic group of order k , then it is isomorphic to the endomorphism monoid of the finite field having r^k elements. So it remains to prove that if M is a right cancellative monoid having an element φ of infinite order in its centre, then there exists a field F of characteristic r having an endomorphism monoid isomorphic to M.

The right multiplication by φ induces a unary operation f over M such that the non-identical polynomials of the unar (M,f) are injective and they have no fixpoints. We fix an undirected graph (M,E) having no non-trivial endomorphism and having no loops, see P. Vopenka and A. Pultr and Z. Hedrlín [8]. Now we define an infinite ascending chain of fields:

$$F_0 \leq F_1 \leq F_2 \leq F_3 \leq \dots \quad \dots \leq F_i \leq \dots \qquad i \in \omega.$$

Let F_0 be the prime field of characteristic r. Let $F_{i+1} = F_i(E_i,(Y_i,f_i),p_i,q)$ where r, q, p_0, p_1, p_2, $\dots$, p_i , $\dots$ are pairwise distinct primes, and the unars and the bipartite graphs of the skins are defined as follows:

$$Y_0 = \{0\} \times M \qquad\qquad f_0 = id\big|_{\{0\}} \times f$$

$$E_0 = \emptyset$$

$$Y_1 = \{1\} \times M \times M \qquad\qquad f_1 = id\big|_{\{1\}} \times id\big|_M \times f$$

$$E_1 = \{\langle\langle 0,m\rangle,\langle 1,n,m\rangle\rangle : m \in M \text{ and } n \in M\}$$

$$Y_2 = \{2\} \times E \times M \qquad\qquad f_2 = id\big|_{\{2\}} \times id\big|_E \times f$$

$$E_2 = \{\langle\langle 1,u,m\rangle,\langle 2,\langle u,v\rangle,m\rangle\rangle , \langle\langle 1,v,m\rangle,\langle 2,\langle u,v\rangle,m\rangle\rangle ,$$
$$\langle\langle 0,m\rangle,\langle 2,\langle u,v\rangle,m\rangle\rangle : \langle u,v\rangle \in E \text{ and } m \in M\}$$

$$Y_3 = \{3\} \times M \qquad\qquad f_3 = id\big|_{\{3\}} \times f$$

$$E_3 = \{\langle\langle 0,m\rangle,\langle 3,m\rangle\rangle : m \in M\}$$

$$(Y_4,f_4) = (M,f)$$

$$E_4 = \{\langle\langle 0,m\rangle,m\rangle : m \in M\}$$

$$Y_5 = \{5\} \times M \times M \qquad\qquad f_5 = id\big|_{\{5\}} \times id\big|_M \times f$$

$$E_5 = \{\langle\langle 0,n\rangle,\langle 5,m,n\rangle\rangle\ ,\ \langle\langle 1,m,m\cdot n\rangle,\ \langle 5,m,n\rangle\rangle\ ,\ \langle\langle 3,m\cdot n\rangle,\langle 5,m,n\rangle\rangle\ ,$$
$$\langle\langle 4,n\rangle,\langle 5,m,n\rangle\rangle : m \in M \text{ and } n \in M\}$$

Let (R_ig_i) denote the unar of the roots of the "i^{th}-skin" = $F_i(E_i,(Y_i,f_i),p_i,q)\setminus F_i$.

$$(Y_6,f_6) = (M,f) \times (R_0,g_0)$$

$$E_6 = \{\langle m,\langle m,t\rangle\rangle\ ,\ \langle t,\langle m,t\rangle\rangle : m \in M \text{ and } t \in R_0\}$$

$$(Y_{7+j},f_{7+j}) = (M_0,f_0) \times (R_{j+1},g_{j+1}) \qquad \text{for} \quad j \in \omega$$

$$E_{7+j} = \{\langle n,\langle n,t\rangle\rangle\ ,\ \langle t,\langle n,t\rangle\rangle : n \in M_0 \text{ and } t \in R_{j+1}\}\ .$$

Let F be the union of the above defined ascending chain of the fields F_i .

Now we prove that M is isomorphic to the endomorphism monoid of F. Let h be an arbitrary endomorphism of F. Each subfield F_i is mapped into itself by h for $i \in \omega$ because F_0 is the prime field and F_{i+1} is the algebraic hull with respect to F of the subfield generated by F_i and the p_i-high elements of F. None of the variables from Y_i is mapped into F_i since the variables from Y_i are p_i-high and each

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

p_i-high element belongs to the i^{th} skin. So the implication (b) of the fourth sublemma can be used for the extension F_{7+i} of F_{6+i}, and therefore the set R_i is mapped into itself by h. Summing up: we have proved that each endomorphism of F can be restricted to the subfield F_{i+1} and this restriction is a special endomorphism of the special extension F_{i+1}/F_i. So the second part of the main lemma can be used for these restrictions of the endomorphisms of F.

Let e be the unit element of the monoid M. So $h(e)$ is again an element of M since Y_4 is mapped into itself by h. Therefore we have a mapping $Q : \mathrm{End}(F) \longrightarrow M$, where $Q : h \longmapsto h(e)$. We want to show that Q is a monoid isomorphism.

First we prove that Q is surjective. Let $n \in M$ be arbitrary. We construct an ascending chain of endomorphisms $h_0 \leq h_1 \leq h_2 \leq \ldots \ldots \leq h_i \leq \ldots$ $i \in \omega$, where h_i is an endomorphism of F_i. Let h_0 be the identity of F_0. Using the second part of the main lemma we define h_{i+1} as follows: let h_{i+1} be a special endomorphism of F_{i+1} such that h_{i+1} is an extension of h_i and the action of h_{i+1} on the variables of the i^{th} skin is defined below:

(1) $h_1 : \langle 0,m\rangle \longmapsto \langle 0,m\cdot n\rangle$

(2) $h_2 : \langle 1,k,m\rangle \longmapsto \langle 1,k,m\cdot n\rangle$

(3) $h_3 : \langle 2,\langle u,v\rangle,m\rangle \longmapsto \langle 2,\langle u,v\rangle,m\cdot n\rangle$

(4) $h_4 : \langle 3,m\rangle \longmapsto \langle 3,m\cdot n\rangle$

(5) $h_5 : m \longmapsto m\cdot n$

(6) $h_6 : \langle 5,k,m\rangle \longmapsto \langle 5,k,m\cdot n\rangle$

(7+j) $h_{7+j} : \langle m,t\rangle \longmapsto \langle h_{6+j}(m),h_{6+j}(t)\rangle$ for $j \in \omega$.

Let h be the union of the above defined ascending chain of endomorphisms. Clearly $Q(h) = n$.

Secondly, we prove that Q is injective. By the second part of the main lemma it is enough to prove that the restrictions h_i of h to the subfields F_i satisfy the conditions *(1) (2) ... ... (7+j) ...* given above whenever $h(e) = n$. Observing the bipartite graph (F_2,E_2,Y_2) we see that h maps the sets $\{1\} \times \{m\} \times M$ and $\{2\} \times \{<u,v>\} \times M$ into itself for $m \in M$ and $<u,v> \in E$. The bipartite graph (F_5,E_5,Y_5) yields the condition (4). Consequently the bipartite graph (F_3,E_3,Y_3) yields the condition (1). The remaining conditions are easy consequences of the condition (1) and the structure of the bipartite graphs of the skins.

Thirdly, we prove that Q preserves the monoid structure. The condition (5) shows that each endomorphism h induces a right multiplication on the monoid M by the element $h(e)$, so Q preserves the multiplication. On the other hand $Q(id) = e$. This completes the proof of the theorem.

REFERENCES

[1] E. Fried, "Automorphism group of integral domains fixing a given subring", *Algebra Universalis* 7 (1977), 373-387.

[2] E. Fried and J. Kollár, "Automorphism groups of fields", Preprints of the Hungarian Academy of Sciences (1978).

[3] G. Grätzer, *Universal Algebra* (Springer-Verlag, 1979).

[4] J. De Groot, "Groups represented by homeomorphism groups I", *Math. Ann.* 138 (1959), 80-102.

[5] W. Kuyk, "The construction of fields with infinite cyclic automorphism group", *Canad. J. Math.* 17 (1965), 665-668.

[6] A. Pultr and V. Trnková, *Combinatorial algebraic and topological representations of groups, semigroups and categories* (Academia Prague, 1980).

[7] L. Rédei, *Algebra* (Pergamon Press, 1967).

[8] P. Vopenka, A. Pultr and Z. Hedrlín, "A rigid relation exists on any set", *Comment. Math. Univ. Carolinae* 6 (1965), 149-155.

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press

[9] B. L. van der Waerden, *Algebra* (Springer-Verlag, 1960).

Department of Algebra and Number Theory,
L. Eötvös University,
Budapest,
Hungary.

https://doi.org/10.1017/S0004972700002070 Published online by Cambridge University Press