TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 304, Number 1, November 1987

ALL INFINITE GROUPS ARE GALOIS GROUPS OVER ANY FIELD

MANFRED DUGAS AND RÜDIGER GÖBEL

Dedicated to Bertram Huppert, on the occasion of his 60th birthday on October 22, 1987

ABSTRACT. Let G be an arbitrary monoid with 1 and right cancellation, and K be a given field. We will construct extension fields $F \supseteq K$ with endomorphism monoid End F isomorphic to G modulo Frobenius homomorphisms. If G is a group, then Aut $F = G$. Let F^G denote the fixed elements of F under the action of G. In the case that G is an infinite group, also $F^G = K$ and G is the Galois group of F over K. If G is an arbitrary group, and $G = 1$, respectively, this answers an open problem (R. Baer 1967, E. Fried, C. U. Jensen, J. Thompson) and if G is infinite, the result is an infinite analogue of the still unsolved Hilbert-Noether conjecture inverting Galois theory. Observe that our extensions $K \subset F$ are *not* algebraic. We also suggest to consider the case $K = \mathbf{C}$ and $G = \{1\}$.

1. Introduction. We want to investigate field extensions R of an arbitrarily fixed field K of characteristic char $K = p$ a prime or $p = 0$. Using some terminology from model theory, we will show that field extensions of K are a nonstructure theory in a very strong sense. The extension field R can be chosen quite arbitrary up to the obvious restrictions. Let us recall the related well-known facts. End R will denote the set of all endomorphisms of R. The product of endomorphisms makes End R = (End R)$^\cdot$ to a monoid, which is a set $G^\cdot$ with associative multiplication "$\cdot$" and identity $1 \in G$. A monoid G satisfies the law of right cancellations if $yx = zx$ for $x, y, z \in G$ implies $y = z$. The endomorphisms of R are necessarily injections, hence End R satisfies the law of right cancellations.

Observe that maps are acting from the right. Apparently not all endomorphisms are surjective. If $p \neq 0$, the field R always has a special semigroup Φ_p of such endomorphisms, the Frobenius homomorphisms. The cyclic group $\Phi_p \subseteq$ End R is generated by ex(p): $R \to R$ which takes $r \in R$ to r^p. Frobenius homomorphisms are surjective if and only if R is a perfect field. If $p = 0$, then $\Phi_0 = \{1\} = 1$. It is the object of this paper to prove the converse of these well-known facts.

THEOREM. *Let K be any field. Then the following conditions are equivalent.*
(1) *$G^\cdot$ is a monoid with right cancellation.*

Received by the editors October 14, 1986. Presented at the Annual AMS Meeting, San Antonio, January 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 20F29, 12A55, 12F20; Secondary 20C99, 20B27, 20F28, 20E36.

0002-9947/87 $1.00 + $.25 per page

(2) *For any cardinal* $\lambda \geq |G|$ *with* $\lambda > \kappa = |K| \cdot \aleph_0$, *and* $\lambda^\kappa = \lambda^{\aleph_0}$, *there exists a field extension* $K \subset R$ *such that* $|R| = \lambda^{\aleph_0}$ *and* $\operatorname{End} R^* = \Phi_p \times G^*$ *is a semidirect product with* Φ_p *central in* $(\operatorname{End} R)^*$.

The field R is not perfect ($\Phi^{*p} \cong N^*$) for $p \neq 0$ and Frobenius homomorphisms $\neq 1$ are not surjective in R.

We have the immediate

COROLLARY [7]. *Let* K *be any field,* G *be any group and* $\lambda \geq |G|$ *any cardinal with* $\lambda^\kappa = \lambda^{\aleph_0}$ *and* $\lambda > \kappa = |K| \cdot \aleph_0$. *Then there exists a field extension* $K \subset R$ *such that* $|R| = \lambda^{\aleph_0}$ *and* $\operatorname{Aut} R = G$. *Moreover, if* G *is infinite, then* G *is the Galois group* R *over* K.

The last remark follows from the group action on R, which is defined inductively in §3. By an easy support argument we have $R^G = K$, where R^G denotes the fixed field $\{r \in R\colon rg = r \text{ for all } g \in G\}$. The reader is invited to consider the special case $K = \mathbf{C}$, the field of complex numbers and the trivial group $G = \{1\}$. It is also clear in this case that the size $|R|$ of any extension field R of $\mathbf{C}$ with $\operatorname{Aut} R = 1$ must be larger than $|\mathbf{C}|$.

The corollary extends a recent result of the authors [**6**] in Gödel's universe $V = L$. The earlier construction in L depends on R. Jensen's diamond function and the prediction of maps on the union of ascending chains. Here we want to prove a similar result in ZFC—without any extra set theoretic hypothesis, cf. [7]. Hence it seems reasonable to imitate the prediction of Jensen functions. This is performed by a Black Box, prepared in §2. The role of the Jensen function is taken by partial maps associated with traps. The Black Box originates from a model theoretic result of S. Shelah [**31**]. It was used in Shelah's proofs on the existence of almost indecomposable abelian p-groups [**32, 33**] ten years ago and has been refined in [**34**]. Other proofs have been given in Corner, Göbel [**2**] and for cardinals of cofinality ω in Franzen, Göbel [**10**]. Observe that the Black Box is proved by simple but suitable counting arguments only. It is straightforward to carry over the arguments from [**2** and **10**] and to conclude (2.10). We also employ a simplification used in [**8**].

The reader will observe similarities with earlier theorems of the authors [**4, 5**] and jointly with A. L. S. Corner [**2**], S. Shelah [**18**] and A. Mader, C. Vinsonhaler [**8**] on ring and module theory. Modules M of certain categories over a class of commutative rings T have been constructed in such a way that a prescribed T-algebra A is realized as an endomorphism algebra; cf. [**2, 4, 5, 18**]. In a fixed module category we have unavoidable, so-called *inessential* endomorphisms, in general. Such endomorphisms have been collected in an ideal $\operatorname{Ines}(M)$ of the endomorphism algebra $\operatorname{End} M$; cf. [**2, 5**]. It turns out (after some calculations) that this ideal $\operatorname{Ines}(M)$ is well known in special categories; cf. [**2**]. In the case of abelian p-groups $\operatorname{Ines}(M)$ is the ideal of small endomorphisms of M, introduced by R. S. Pierce, for instance. In the case of cotorsion-free modules M we have $\operatorname{Ines}(M) = 0$. Other cases may be found in [**2**] or [**19**]. The general realization theorem for T-modules M reads as follows:

$$\operatorname{End} M = A \oplus \operatorname{Ines}(M),$$

cf. [2, p. 462, Main Theorem 5.2], in particular see the restrictions on T. In the context of field theory, the role of Ines(M) with respect to multiplication is taken by the semigroup Φ_p of all Frobenius homomorphisms, which cannot be killed by any extension. Therefore Φ_p naturally comes up in the theorem. However, $\Phi_p = 1$ if $p = 0$—which corresponds to the category of torsion-free T-modules.

The similarity can be pushed even further. The construction of T-modules is performed between a sufficiently large "relatively free" module and its T-adic completion. In the case of fields you do the same: The "relatively free" objects are large enough function fields and the T-adic completion is replaced by the algebraic closure. Now it is clear that a field should be cotorsion-free if it contains no algebraically closed subfield. The modules M are derived as pure submodules of the mentioned T-adic completion. Purity is achieved with the help of divisor chains [**2, 5**]. In the case of field theory we need an equivalent notion. Since multiplication in fields is more relevant than addition, the parallel construction of purity is carried out with root chains, compare §3. These root chains are motivated also by E. Fried and J. Kollar [**13**]; however, they are essentially different from the chains in [**13**]. They have been used in our earlier paper [**6**]. Hence the authors would like to understand this paper as a contribution of abelian groups to field theory, caused by the advances of the first theory in recent years; cf. [**19**].

The correlations cited between the two theories might help to detect other connections. However, and this is not surprising either; the actual computations in the following sections—although inspired by module theory—differ substantially from their origin [**2, 5**]. Besides the methods mentioned, the construction uses ideas from algebraic geometry, polynomial rings and (of course) from field theory. Finally we want to include some historical remarks concerning the solved problem. It was brought to our attention by C. U. Jensen (Kopenhagen) at a Colloquium at Essen University. We would like to thank him for a stimulating talk as well as for his support of \$25 on the solution in the case $K = \mathbf{C}$ and $G = 1$. The problem seems to be known to many experts. It is stated in E. Fried [**12**, p. 315] and it was earlier (1967) discussed in a seminar at Sheffield University by R. Baer as pointed out by P. Vamos. It also has been considered by J. Thompson in more recent talks. J. De Groot [**20**] asked a weaker question in 1959: Is any prescribed group G the automorphism group of some field? This was answered for $G = \mathbf{Z}$ by W. Kuyk [**23**]. The final answer to De Groot's problem was given by E. Fried and J. Kollar [**13**]. The characteristic of the field can be prescribed as well, see [**13**] for $p \neq 2$ and [**27**] for $p = 2$. The complication caused by a *prescribed* subfield K lies in the fact that Aut K might be very large. In order to find an extension field R with Aut $R = G$ we must kill the automorphisms on K simultaneously. In De Groot's special case we simply start with $K = \mathbf{Q}$ and recall that Aut $\mathbf{Q} = 1$.

There are similar problems known in field theory.

The famous still unsolved Hilbert [**22**]—E. Noether [**26**]—conjecture "inverting Galois theory" asks for realizations of finite groups as Galois groups over $K = \mathbf{Q}$; compare the reports by [**25, 36**] and references in these papers. The most important contribution in the finite case is the realization of all solvable groups by I. R. Safarevic [**29**]. Moreover, many of the finite simple groups have been realized—

including most of the sporadic simple groups, see B. H. Matzat [**25**] and in particular J. G. Thompson [**37**, **38**], W. Feit, P. Fong [**9**]. Our method contributes a solution of an infinite analogue of this problem. However, observe that our field extensions are not algebraic over the group field K. In fact algebraic extensions are impossible because K might be algebraically closed and if this is not the case, then G might be too large. Hence—unfortunately—this construction will be of no use in the finite case. There is also a weaker version of this problem asking for realizations of finite groups on *algebraic* extensions of $\mathbf{Q}$. This problem was essentially solved in [**14**] and corrected in [**15**]. A new simple proof is due to W. D. Geyer [**17**].

In a recent paper D. J. Madden and R. G. Valentini [**24**] constructed function fields F over a given algebraically closed field K with a prescribed finite relative automorphism group $G \cong \mathrm{Aut}(F/K)$. This was sharpened by H. Stichtenoth [**35**], who can prescribe the fixed field F^G as well. E. Fried [**11**] replaced fields by domains. In this case the answer can be obtained with less effort because of the rich ideal structure of domains.

2. The Black Box. We will use a simplified version of Shelah's "Black Box" adjusted to the construction of field extensions. The proof of the combinatorial tools is derived from Corner, Göbel [**2**], which is based on S. Shelah [**33**]. The simplification turned out to be useful in Dugas, Mader, Vinsonhaler [**8**]. The reader who is not willing to use the simplification, can also use [**2**] which makes no essential difference. In fact, we will adopt the terminology from [**2**] and will sometimes talk about "branches".

Let $G = (G, \cdot, 1)$ be a monoid with associative, multiplicative structure $(G, \cdot)$ with the law of right cancellation ($hg = h'g$ implies $h = h'$) containing the identity $1 \in G$; compare N. Bourbaki [**1**, p. 12]. Furthermore let K be any fixed field of characteristic $\mathrm{char}(K) = p$ with $p = 0$ or p a prime. Let $\kappa = |K| \cdot \aleph_0$, where $|K|$ denotes the cardinality of K. Choose any cardinal $\lambda > \kappa$, $|G|$ such that $\lambda^\kappa = \lambda^{\aleph_0}$. We want to construct an extension field R of K of cardinality $|R| = \lambda^{\aleph_0}$. Choose a set X of independent and commuting variables, and let

$$\lambda^\omega = \{u\colon u\colon \omega \to \lambda \text{ strictly increasing}\}.$$

Elements of λ^ω will be called "branches" occasionally, as in [**2**]. Consider

(2.1) $X = \{x_t\colon t \in \lambda \times \kappa \times G\}$ and $Y = \{y_u\colon u \in \lambda^\omega \times G\}$. The elements of the first set are called x-variables, the second ones y-variables.

We will write $t = (\alpha, k, g) \in \lambda \times \kappa \times G$ and $t_1 = \alpha$, $t_2 = k$, $t_3 = g$ for the components. Similarly $u = fg \in \lambda^\omega \times G$ and $u_1 = f$, $u_2 = g$ where $f \in \lambda^\omega$, $g \in G$. If $g = 1$, we also write $x_t = x_{\alpha k}$ and $y_u = y_f$. If F is any field, then let $\hat{F}$ be its algebraic closure. Furthermore $F[T]$ denotes the polynomial ring over a set T of independent, commuting variables with coefficients in F, and $F(T)$ is its function field. In particular we are interested in the fields

(2.2) $$F_0 = K(X) \subseteq F = K(X \cup Y) \subseteq \hat{F}.$$

If $h \in G$, then let

$$\text{(2.3)}\qquad \begin{aligned} &\text{(i)} && rh = r \text{ for all } r \in K.\\ &\text{(ii)} && x_{\alpha k g}h = x_{\alpha k(gh)} \text{ for all } \alpha kg \in \lambda \times \kappa \times G.\\ &\text{(iii)} && y_{fg}h = y_{f(gh)} \text{ for all } fg \in \lambda^{\omega} \times G. \end{aligned}$$

The map h on $K \cup X \cup Y$ is injective because G satisfies the law for right cancellation. Hence h induces a unique canonical endomorphism (injection) of F which can be extended (not uniquely) to an endomorphism of $\hat{F}$ because $\hat{F}$ is algebraically closed. This endomorphism on F will be denoted by h as well. Therefore we conclude

$$\text{(2.4)}\qquad G \subseteq \operatorname{End} F \quad \text{via (2.3).}$$

Observe that it is impossible, in general, to extend G to a submonoid of $\operatorname{End} \hat{F}$; e.g. consider $G = \mathbf{Z}/2\mathbf{Z}$. If $G \subseteq \operatorname{Aut} \hat{F}$, then $\hat{F}$ is a real closed field. Used facts on field theory can be found in [**39** and **40**]. Similar to [**5** or **2**, p. 451, (1.7)] we will work with supports, which here depend on X or Y.

If $f \in \hat{F}$, then f is algebraic over $K(X, Y)$; cf. (2.2). Hence there exist minimal and finite sets $[f]^x \subseteq X$ and $[f]^y \subseteq Y$ such that

$$\text{(2.5)}\qquad f \in K\widehat{([f]^x \cup [f]^y)} \subseteq \hat{F}.$$

We call $[f]^x$ the x-support and $[f]^y$ the y-support of f and $[f] = [f]^x \cup [f]^y$ is the support of f.

REMARK. Take the minimum polynomial of f over $K(X \cup Y)$ and collect the variables $x \in X$ used for coefficients of this polynomial. The resulting set will be $[f]^x$. Similarly define $[f]^y$.

We also introduce a norm which is related to supports in λ. Here we assume $\operatorname{cf}(\lambda) > \aleph_0$. The other case $\operatorname{cf}(\lambda) = \aleph_0$ is similar using notation from [**10**]. If $U \subseteq \lambda$, then $\|U\| = \sup U \in \lambda + 1$. Furthermore, if $f \in \hat{F}$, then $\|f\| = \sup\{\alpha \in \lambda\colon x_{\alpha k g} \in [f]^x \text{ or } \alpha \in \operatorname{Im} u_1, y_{ug} \in [f]^y \text{ for some } k, g, u\} = \|[f]\| \in \lambda$ and $y_u \in Y$ has support $\operatorname{Im}(u_1)$, hence $\|y_u\| = \|\operatorname{Im}(u_1)\| \in \lambda$. Similar to [**2**, p. 451] we will use the

DEFINITION 2.6. A canonical subfield P is a subfield of F_0 of the form

$$P = P_T = K(x_t\colon t \in T \times \kappa \times G)$$

for some subset $T \subseteq \lambda$ with $0 \neq |T| \leqslant \kappa$. Let $[P]^x = \{x_t\colon t \in T \times \kappa \times G\}$ denote the x-support of P. Let us agree on writing $P = P_T = P_{[P]}x$. In addition, call

$$P^* = K\Big([P]^x \cup \big\{ y_{fg}\colon fg \in \lambda^{\omega} \times G, \operatorname{Im}(f) \subseteq T, \|f\| < \|T\| \big\}\Big)$$

the *Y-closure* of P.

Observe that $G \subseteq \operatorname{End} P_T$. Similar to [**2**, p. 454] we now define a trap.

DEFINITION 2.7. A trap is a triple $\tau = (f, P, \phi)$ where

(1) $f \in \lambda^{\omega}$ is a branch.

(2) P is a canonical subfield of F_0 such that $\phi\colon \hat{P}^* \to \hat{F}$ is a field embedding with the following properties, for all $n \in \omega$,

(i) $[P]^x = \dot{\cup}_{n \in \omega} T_n$ with $f(n) \in T_n$,

(ii) $\sup T_n < \min T_{n+1}$ (using $<$ from the λ-component),

(iii) if $I_n = \bigcup_{k<n} I_k$ and $P_n = P_{I_n}$, then $\hat{P}_n^* \phi \subseteq \hat{P}_{n+1}^*$,

(3) $K(x_{001}) \subseteq P$ and $\|K(x_{001})\phi \cup K(x_{001})\| < \|P\|$.

From (2.7)(2) we have the immediate

OBSERVATION 2.8. If $\tau = (f, P, \phi)$ is a trap, then $\|\tau\| = \|f\| = \|P\| = \|\hat{P}\| \in \lambda$ has cofinality ω, and $\bigcup_{n\in\omega} \hat{P}_n^* \phi \subseteq \hat{P}^*$.

Similar to Dugas, Göbel [5] ("λ-big") or Göbel, Shelah [18], we will also need the notion of a "large trap".

DEFINITION 2.9. Let τ_α ($\alpha \in \lambda^*$) be a sequence of traps. Then we say that a trap $\tau_\alpha = (f, P, \phi)$, $\alpha \in \lambda^*$, is large (over λ^*), if there exists an ω-sequence $\tau_{m^*} = (f_{m^*}, P_{m^*}, \phi_{m^*})$ $(m^* \in \lambda^*)$ $(m \in \omega)$ of traps such that, for all $m \in \omega$,

(i) $\|\tau_{m^*}\| < \|\tau_{(m+1)^*}\|$ is strictly increasing, and $\|K(x_{001})\phi\| < \|\tau_0\|$,

(ii) $\|\{\tau_{m^*}: m \in \omega\}\| \leqslant \|\tau_\alpha\|$,

(iii) $[P_{m^*}] \subseteq [P]$ and $\phi_{m^*} = \phi \restriction \hat{P}_{m^*}^*$.

If τ_α is a large trap, we will write $\tau_\alpha = (\tau_{m^*})_{m\in\omega}$.

BLACK BOX 2.10. For some ordinal $\lambda^* > \lambda^{\aleph_0}$ (as ordinal) with $|\lambda^*| = \lambda^{\aleph_0}$ there exists a transfinite sequence $\tau_\alpha = (f_\alpha, P_\alpha, \phi_\alpha)$ $(\alpha < \lambda^*)$ of traps, such that, for $\alpha, \beta < \lambda^*$,

(i) if $\beta \leqslant \alpha$, then $\|P_\beta\| \leqslant \|P_\alpha\|$,

(ii) if $\beta \neq \alpha$, then $\operatorname{Im} f_\alpha \cap \operatorname{Im} f_\beta$ is finite,

(iii) if $\beta + \kappa^{\aleph_0} < \alpha$, then $[P_\beta]_1^x \times \kappa \cap \{(f_\alpha(n), e(n)): n \in \omega\}$ is finite for any function e: $\omega \to \kappa$. ($[\ ]_1$ denotes the first ($= \lambda$) index of an x-element.)

(iv) For any subset $X \subseteq \hat{F}$ with $|X| \leqslant \kappa$, and any $\phi \in \operatorname{End} \hat{F}$, there exists $\alpha \leqslant \lambda^*$ such that

(a) τ_α is a large trap with $\tau_\alpha = (\tau_{\alpha m})_{m\in\omega}$ and,

(b) τ_α catches X and ϕ, i.e.

$$X \subseteq \hat{P}_\alpha^* \quad \text{and} \quad \phi \restriction \hat{P}_\alpha^* = \phi_\alpha.$$

PROOF. If $\lambda^\kappa = \lambda^{\aleph_0}$ $(\kappa \geqslant \aleph_0)$ follow Corner, Göbel [2, pp. 476–478] or Dugas, Mader, Vinsonhaler [8, Proof of Theorem 2.6] where the tree ${}^{\omega>}\omega$ is replaced by a branch ω. In this case cf. $(\lambda) > \kappa \geqslant \aleph_0$. The proof for $\lambda \geqslant \kappa$ with cf. $\lambda > \aleph_0$ is similar and only the case cf. $\lambda = \omega$ needs some extra arguments due to S. Shelah [34]. A more direct proof is given in Franzen and Göbel [10].

3. The construction of a field $R = R(K, G)$. In Dugas and Göbel [5] and Corner and Göbel [2] we used divisibility chains in some completion in order to construct (pure sub-) modules with prescribed endomorphism rings. The crucial operation in fields is multiplication—addition is less important. Hence divisibility chains must be replaced by root chains, which is the basic algebraic concept of this paper.

Let us agree for the rest of this paper on the following

CONVENTION 3.0. The exponent z of an element of the fields under discussion denotes $z = 2$ if the characteristic of the fixed ground field K is not 2 and $z = 3$ if $\operatorname{char} K = 2$.

Recall from Dugas and Göbel [6] the following

DEFINITION 3.1. Let $K \subset P$ be any field extension and let z be a prime.

(a) An element $f \in P \setminus K$ is called z^*-high over K in P, if there exist $k_n \in K^* = K \setminus \{0\}$, $f_n \in P$ with $f_0 = f$ and $f_{n+1}^z = f_n k_n$ for all $n \in \omega$.

(b) We say that K is z-pure in P if $f \in R$, $f^z \in K$ imply $f \in K$.

Next we want to carry out

(3.2) *The construction of the field* $R = R(K, G)$. Recall (2.2) and choose a transfinite sequence $\tau_\alpha = (f_\alpha, P_\alpha, \phi_\alpha)$ $(\alpha \in \lambda^*)$ of traps satisfying the conclusion of the Black Box 2.10. Then we will construct our desired field R as the union of an ascending chain of subfields R_α of $\hat{F}$ with $\alpha < \lambda^*$.

Let $\mu \leqslant \lambda^*$ and assume that we have found two ascending chains of subsets $S_\alpha \subseteq \alpha$, and of subfields $R_\alpha \subseteq \hat{F}$ for all $\alpha < \mu$. The elements of S_α are called *strong ordinals*. We also assume that G acts on R_α extending the action of G on R_β for all $\beta < \alpha$. Moreover, we make the following requirements.

If $\mu = 0$, we assume nothing and put

$$(\mathrm{I}_0) \qquad R_0 = F_0 = K(X) \quad \text{and} \quad S_0 = \varnothing,$$

cf. (2.1), (2.2). Observe that G operates on R_0 via (2.3). If μ is a limit ordinal, take

$$(\mathrm{I}_\mu) \qquad \left.\begin{array}{l} R_\mu = \bigcup_{\alpha<\mu} R_\alpha \quad \text{and} \quad S_\mu = \bigcup_{\alpha<\mu} S_\alpha \\ \text{The } G\text{-action can be extended trivially} \end{array}\right\} \quad (\mu \text{ a limit}).$$

When $\mu = \alpha + 1$, a successor, we distinguish three cases.

THE STRONG CASE. Choose $S_{\alpha+1} = S_\alpha \cup \{\alpha\}$. Suppose that it is possible to choose "root chains" ${}_iy_{f_\alpha g}$ $(i \in \omega)$ in $\hat{P}_\alpha^*$ $(g \in G)$ and $R_{\alpha+1}$ in such a way that each of the following conditions is satisfied.

$$(\mathrm{I}_{\alpha+1}) \qquad R_{\alpha+1} = R_\alpha\big({}_iy_{f_\alpha g}\colon i \in \omega,\ g \in G\big).$$

(a) ${}_0y_{f_\alpha g} = y_{f_\alpha g}$,

(b) ${}_{i+1}y_{f_\alpha g}^{\bar{}} = {}_iy_{f_\alpha g} m_i^\alpha g$ with $m_i^\alpha \in \hat{P}_\alpha^* \cap R_\alpha$ such that for all $i \in \omega$,

(i) $m_i^\alpha = a_{\alpha i}(1 - x_{f_\alpha(i)e_\alpha(i)})$ $(i \in \omega)$ for some injection $e_\alpha\colon \omega \to \kappa$, $a_{\alpha i} \in \hat{P}_\alpha^* \cap R_\alpha$ with $\|\{a_{\alpha i}\colon i \in \omega\}\| < \|f_\alpha\|$, and if τ_α is a large trap with $\tau_\alpha = (f_{i^*}, P_{i^*}, \phi_{i^*})_{i \in \omega}$ $(i^* \in \lambda^*)$, then either (i) holds or

(ii) $m_i^\alpha = a_{\alpha i}(1 - x_{f_\alpha(i)e_\alpha(i)})(b_\alpha - y_{f_{i^*}})(1 - y_{f_{i^*}})$ for some injection $e_\alpha\colon \omega \to \kappa$, $a_{\alpha i}, b_\alpha \in \hat{P}_\alpha^* \cap R_\alpha$ with $\|\{a_{\alpha i}, b_\alpha\colon i \in \omega\}\| < \|\tau_{0^*}\|$.

(c) If $h \in G$, we define its action on $R_{\alpha+1}$ extending $h \restriction R_\alpha$. If ${}_iy_{f_\alpha g} \in R_{\alpha+1}$, then ${}_iy_{f_\alpha g}h = {}_iy_{f_\alpha gh}$ which is an injective map because G satisfies the law of right cancellations. Using $(\mathrm{I}_{\alpha+1})$(a), (b) then $h \restriction R_\alpha$ extends to an endomorphism of $R_{\alpha+1}$. Therefore G acts on $R_{\alpha+1}$ extending the action on each R_β for $\beta < \alpha$.

$(\mathrm{II}_{\alpha+1})$ If $\beta \in S_{\alpha+1}$ and ϕ'_β extends $\phi_\beta \restriction R_{\alpha+1}$, then there are numbers $i(\alpha, \beta) \in \omega$ with $i(\alpha, \alpha) = 0$ and ${}_iy_{f_\beta 1}\phi'_\beta \notin R_{\alpha+1}$ for all $i \geqslant i(\alpha, \beta)$.

If this strong case is possible, we make this choice and continue the construction at $\alpha + 2$. If not, we consider

THE WEAK CASE. In this case we choose $S_{\alpha+1} = S_\alpha$. Suppose that it is possible to choose "root chains" ${}_iy_{f_\alpha g}$ $(i \in \omega)$ in $\hat{P}_\alpha^*$ $(g \in G)$ such that $(\mathrm{I}_{\alpha+1})$ and $(\mathrm{II}_{\alpha+1})$ hold [but certainly ${}_0y_{f_\alpha 1}\phi'_\alpha \in R_{\alpha+1}$ for some extension $\phi'_\alpha \supset \phi_\alpha \restriction R_{\alpha+1}$]. Now we require less.

($\mathrm{III}_{\alpha+1}$) If ϕ'_α extends $\phi_\alpha \restriction R_{\alpha+1}$, then ${}_iy_{f_\alpha 1}\phi'_\alpha \notin R_\alpha$ for all $i \in \omega$. If we can make this choice, we will do so and call α a weak ordinal and continue the construction at $\alpha + 2$. If not, we consider

THE USELESS CASE. Choose $S_{\alpha+1} = S_\alpha$, $R_{\alpha+1} = R_\alpha$ and call α a useless ordinal. [We will show in §5 that this case does not exist: There are essentially no useless ordinals.]

In order to compute the inductive construction, we must show

(II_μ) for limit ordinals $\mu \leqslant \lambda^*$:

(II_μ) If $\beta \in S_\mu$, and ϕ'_β extends $\phi_\beta \restriction R_\mu$, then there are numbers $i(\mu,\beta) \in \omega$ with ${}_iy_{f_\beta 1}\phi'_\beta \notin R_\mu$ for all $i \geqslant i(\mu,\beta)$.

If (II_μ) does not hold, then ${}_iy_{f_\beta 1}\phi'_\beta \in R_\mu$ for infinitely many $i \in \omega$. Hence ${}_iy_{f_\beta 1}\phi'_\beta \in R_{\alpha_i}$ for some $\alpha_i < \mu$ and we may assume $\beta < \alpha_i$ without loss of generality. From (I_β)(b) we have $({}_{i+1}y_{f_\beta 1}\phi'_\beta)^z \in R_{\alpha_i}$. Since R_{α_i} is z-pure in R_μ, also ${}_{i+1}y_{f_\beta 1}\phi'_\beta \in R_{\alpha_i}$ and ${}_{i+k}y_{f_\beta 1}\phi'_\beta \in R_{\alpha_i}$ for all $k \geqslant 0$. This contradicts (II_{α_i}) because $\beta \in S_{\alpha_i}$. Now transfinite induction completes the construction. Finally we derive the desired field

$$R = R(K,G) = R_{\lambda^*} \quad \text{with } G \subseteq \operatorname{End} R.$$

The ordinals $< \lambda^*$ are divided into strong ordinals in $S = \bigcup_{\alpha<\lambda^*} S_\alpha$, weak ordinals, and useless ordinals. It will be convenient to simplify the notations. Let us agree on the following.

($\mathrm{IV}_{\alpha+1}$) We will write in ($\mathrm{I}_{\alpha+1}$).

(a) ${}_iy_{f_\alpha g} = {}_iy_{\alpha g}$, ${}_0y_{\alpha g} = y_{\alpha g}$ and ${}_iy_{\alpha 1} = {}_iy_\alpha$,

(b) $x_{f_\alpha(i)e_\alpha(i)g} = x_{\alpha eig}$ and $x_{\alpha eil} = x_{\alpha ei}$,

(c) $y_{f_i *} = y_{\alpha i}$ or simply $y_{\alpha i} = y_{i*}$.

Since $G \subseteq \operatorname{End} R$, we ask for other endomorphisms in R. What are the unavoidable endomorphisms? If $\operatorname{char}(K) = p$ ($= \operatorname{char} R$) is a prime, then the set

$$\operatorname{ex}(p^t)\colon R \to R(r \to r^{p^t}) \qquad (t \geqslant 0)$$

of Frobenius homomorphisms form a cyclic semisubgroup $\Phi_p = \Phi_p(R)$ ($\cong N^*$) of $(\operatorname{End} R)^*$ which is generated by $\operatorname{ex}(p)$.

Observe that the Frobenius group Φ_p corresponds to the ideal $\operatorname{Ines}(R)$ of unavoidable homomorphisms of a module R, cf. [**2**, §4].

If $p = 0$, then $\Phi_p = \{1\}$ is degenerated. In any case, it is clear from the G-action on R that $\Phi_p \cap G = 1$ and Φ_p is central. We derive

(3.3) $\qquad \Phi_p \times G \subseteq \operatorname{End} G$ is a semidirect product.

It remains to show equality. This is the main object of this paper, which we postpone to §5.

It will be convenient to define a special support $T(\ldots)$. If $\alpha \in \lambda^*$ and $\tau_\alpha = (f_\alpha, P_\alpha, \phi_\alpha)$, $g \in G$, we define a support of $f_{\alpha g}$ to be

$$T(f_{\alpha g}) = \bigcup_{i\in\omega} \left[{}_{i+1}y^z_{\alpha g i}y^{-1}_{\alpha g}\right]. \tag{3.4}$$

It follows from ($\mathrm{I}_{\alpha+1}$)(b) and ($\mathrm{IV}_{\alpha+1}$) that

$$\begin{aligned} &T(f_{\alpha g}) = T_0 \cup \{x_{\alpha eig}\colon i \in \omega\} \text{ where } T_0 \subseteq X \text{ and} \\ &\|T_0\| < \|f_\alpha\| = \|T(f_\alpha)\|. \end{aligned} \tag{3.5}$$

4. Algebraic tools: Simple field extensions. Observe that the construction (3.2) (I_α) gives rise to many z^*-high elements in R. In the following lemmas we will deal with such elements. This is the central algebraic part of this paper. Special cases are derived in Dugas and Göbel [**6**] as Lemma 2.2, Corollary 2.3.

LEMMA 4.1. *Let K be a field of characteristic $\neq 2$ and $P = K({}_i x\colon i \in \omega)$ where $x = {}_0x$ is transcendental over K and ${}_{n+1}x^2 = {}_n x k_n$ for some $k_n \in K$. If $u \in K({}_i x)$ is a square in P, then*

(a) *u is a square in $K({}_{i+1}x)$,*

(b) *if also $u = f/F$ with inhomogeneous polynomials $f, F \in K[{}_i x]$, then u is a square in $K({}_i x)$.*

PROOF. Observe that $K({}_i x) \subseteq K({}_{i+1}x)$ and $P = \bigcup_{i\in\omega} K({}_i x)$.

(a) Let $u = v^2$ with $v \in P$. Clearly we may assume $u \in P \setminus K$ and let $i \in \omega$ minimal with $u \in K({}_i x)$. Let $t \geqslant 0$ be minimal with $v \in K({}_{i+t}x)$. We want $t \in \{0,1\}$ and assume $t \geqslant 2$ for contradiction. Since $K({}_{i+t}x) = K({}_{i+t-1}x)({}_{i+t}x)$ with ${}_{i+t}x^2 = {}_{i+t-1}x k_{i+t-1}$, $K({}_{i+t}x)$ is a quadratic field extension over $K({}_{i+t-1}x)$. Therefore $v = a\,{}_{i+t}x + b$ with $a, b \in K({}^x_{i+t-1})$ and $a \neq 0$, because t is minimal. We derive

$$\begin{aligned} u = v^2 &= a^2\,{}_{i+t-1}x k_{i+t-1} + 2ab\,{}_{i+t}x + b^2 \\ &= \left(a^2\,{}_{i+t-1}x k_{i+t-1} + b^2\right) + 2ab\,{}_{i+t}x. \end{aligned}$$

Because $\operatorname{char} K \neq 2$, this implies $ab = 0$. Since $a \neq 0$, also $b = 0$ and $u = a^2\,{}_{i+t-1}x k_{i+t-1} \in K({}_i x)$.

Since $k_{i+t-1} \in K$, also $a^2\,{}_{i+t-1}x \in K({}_i x)$. On the other hand $a \in K({}_{i+t-1}x)$ which is a quadratic field extension of $K({}_{i+t-2}x)$ and we can write $a = c\,{}_{i+t-1}x + d$ for some $c, d \in K({}_{i+t-2}x)$. Therefore $(c^2\,{}_{i+t-2}x k_{i+t-2} + 2cd\,{}_{i+t-1}x + d^2)\,{}_{i+t-1}x \in K({}_i x)$ and $2cd\,{}_{i+t-2}x k_{i+t-2} \in K({}_{i+t-2}x)$. From $K({}_i x) \subseteq K({}_{i+t-2}x)$ we derive $(c^2\,{}_{i+t-2}x k_{i+t-2} + d^2)\;{}_{i+t-1}x \in K({}_{i+t-2}x)$. Since $c^2\,{}_{i+t-2}x k_{i+t-2} + d^2 \in K({}_{i+t-2}x)$, we have

$$c^2\,{}_{i+t-2}x k_{i+t-2} + d^2 = 0.$$

Therefore ${}_{i+t-2}x = ky^2$ for some $k \in K$, $y \in K({}_{i+t-2}x)$ which is impossible by an obvious degree argument. We conclude $t \leqslant 1$ and (a) holds.

(b) Let $u = f/F$ with $f, F \in K[{}_i x]$ inhomogeneous and relatively prime. If $u = v^2$, then $v = h/H$ and $h, H \in K[{}_{i+1}x]$ from (a). Without loss of generality we assume that h, H are relatively prime as well. Hence

$$u = \frac{f({}_i x)}{F({}_i x)} = \frac{h^2({}_{i+1}x)}{H^2({}_{i+1}x)},$$

and using ${}_{i+1}x^2 = {}_i x k_i$ we define $g, G \in K[{}_{i+1}x]$ by $G({}_{i+1}x) = F({}_{i+1}x^2 k_i^{-1})$ and $g({}_{i+1}x) = f({}_{i+1}x^2 k_i^{-1})$. Therefore

$$u = \frac{g\left({}_{i+1}x^2\right)}{G\left({}_{i+1}x^2\right)} = \frac{h^2({}_{i+1}x)}{H^2({}_{i+1}x)} = \frac{h^2(-{}_{i+1}x)}{H^2(-{}_{i+1}x)}.$$

If $e = h({}_{i+1}x)/h(-{}_{i+1}x)$, then $h^2({}_{i+1}x) = e^2h^2(-{}_{i+1}x)$ and $H^2({}_{i+1}x) = e^2H^2(-{}_{i+1}x)$. Since h, H are relatively prime, we have $e \in K$. Let $n \geqslant 0$ be the smallest integer with coefficient c_n of the polynomial h different from 0. From $h({}_{i+1}x) = eh(-{}_{i+1}x)$ and $e \in K$ we conclude $c_n({}_{i+1}x)^n = ec_n(-{}_{i+1}x)^n$. Therefore $e = (-1)^n$. We may write $h({}_{i+1}x) = ({}_{i+1}x)^n h'({}_{i+1}x)$ with h' inhomogeneous. Therefore ${}_{i+1}x^n h'({}_{i+1}x) = {}_{i+1}x^n h'(-{}_{i+1}x)$ and h' is even.

In the same way we can find $m \in \omega$ such that $H({}_{i+1}x) = ({}_{i+1}x)^m H'({}_{i+1}x^2)$. From $h({}_{i+1}x) = ({}_{i+1}x^n)h'({}_{i+1}x^2)$ and h, H relatively prime, we derive $n = 0$ or $m = 0$. By assumption h/H is inhomogeneous, which implies $n = m = 0$. This and ${}_{i+1}x^2 \in K({}_ix)$ show that $u = v^2 = (h'({}_{i+1}x^2)/H'({}_{i+1}x^2))^2$ is a square in $K({}_ix)$. □

In order to cover the case $\operatorname{char} K = 2$, we must derive a similar result in this case.

LEMMA 4.1*. *Let K be a field of characteristic 2. Then $P = K({}_ix\colon i \in \omega)$ denotes the extension of K, where $x = {}_0x$ is transcendental over K and ${}_{n+1}x^3 = {}_nx\, k_n$ for some $k_n \in K$. If $u \in K({}_ix)$ and $u = v^3$, then the following holds.*

(a) $v \in K({}_{i+1}x)$.

(b) *If also $u = g/G$ with inhomogeneous polynomials $g, G \in K[{}_ix]$, then $u \in K({}_ix)$.*

PROOF. Consider $K \subset \hat{K}$ and the Galois field $GF(4) \subseteq \hat{K}$ of 4 elements. Recall that $GF(4) = \{0, 1, e, f\}$ with equations

(i) $e^3 = f^3 = 1$, $e + f = 1$, $e = f^{-1}$.

We will also use the trivial equations

(ii) If $a, b, c \in K$, then $a^2 + b^2 = (a + b)^2$ and $(a + b + c)^3 = a^3 + a^2(b + c) + b^3 + b^2(a + c) + c^3 + c^2(a + b)$.

Let $u \in K({}_ix)$ and i be minimal. We may assume $u \notin K$, hence $i \geqslant 0$. Let t be minimal $\geqslant 0$ such that

(iii) $v \in K({}_{i+1}x)$,

and suppose $t \geqslant 2$ for contradiction. The element v can be expressed as $v = a_{i+t}x^2 + b_{i+t}x + c$ with coefficients $a, b, c \in K({}_{i+t-1}x)$. Since t is minimal, also

(iv) $ab \neq 0$.

An easy calculation, using (ii), shows

(v)

$$\begin{aligned} v^3 = {}&{}_{i+t}x^2\left(a^2b_{i+t-1}xk_{i+t-1} + b^2c + c^2a\right) \\ &+ {}_{i+t}x\left(a^2c_{i+t-1}xk_{i+t-1} + b^2a_{i+t-1}xk_{i+t-1} + c^2b\right) \\ &+ \left(a^3{}_{i+1-1}x^2k^2_{i+t-1} + b^3{}_{i+t-1}xk_{i+t-1} + c^3\right). \end{aligned}$$

Since $v^3 = u \in K({}_ix)$ and $t \geqslant 2$, we get from (v) and $\operatorname{char} K = 2$,

(vi)

$$a^2b_{i+t\ 1}x\,k_{i+t-1} = b^2c + c^2a, \quad \left(a^2c + b^2a\right)_{i+t-1}x\,k_{i+t-1} = c^2b.$$

Case 1. Suppose $a \neq 0 \neq b$, $c \neq 0$. Hence $c^2b \neq 0$ and also $a^2c + b^2a \neq 0$ by (vi). Equations (vi) lead to

$$c^2b/(a^2c + b^2a) = (b^2c + c^2a)/a^2b.$$

Using $\operatorname{char} K = 2$, we derive $a^2b^2c^2 = b^4ac + c^3a^3$, hence $b^4 + b^2ac + a^2c^2 = 0$. If $d = b^2$, we apply (i) and derive $d^2 + dac + a^2c^2 = (d - eac)(d - fac)$ in $\hat{K}$, recall $GF(4) \subseteq \hat{R}$. Without any restriction choose $(d =)\ eac = b^2$.

The first equation (vi) can be written

$$ {}_{i+t-1}xk_{i+t-1} = \frac{b^3}{a^3e(e+1)} = \left(\frac{b}{a}\right)^3. $$

Since $a, b \in K({}_{i+t-1}x)$, we can find polynomials $g, G \in K[{}_{i+t-1}x]$ such that

$$ {}_{i+t-1}xk_{i+t-1} = \left(\frac{g}{G}\right)^3; $$

hence ${}_{i+t-1}xk_{i+t-1}G^3 = g^3$. If deg denotes the degree of these polynomials, then $1 + 3 \cdot \deg(G) = 3\deg(g)$ which is impossible.

Therefore we are in

Case 2. $a \cdot b \cdot c = 0$.

Suppose $c = 0$, then $ab = 0$ from the first equation of (vi), which contradicts (iv). Therefore $c \neq 0$ and either $a = 0$ or $b = 0$ in this case. In case $a = 0$, also $b \neq 0$ by (iv). From the second equation (vi) we have $c^2b = 0$, hence $c = 0$ or $b = 0$ is a contradiction. If $b = 0$, then $a \neq 0$ by (iv) and $a^2c = 0$ from the second equation of (vi). Therefore $a = 0$ or $c = 0$ is a contradiction and (4.1*)(a) is shown.

(b) Let $u = g/G$ with $g, G \in K[{}_ix]$ inhomogeneous and relatively prime. If $u = v^3$, then $v = h/H$ with $h, H \in K[{}_{i+1}x]$ from (a). We may assume that h, H are relatively prime as well. Using ${}_{i+1}x^3 = {}_ixk_i$, we define $g', G' \in K[{}_{i+1}x]$ by $g'({}_{i+1}x) = G({}_{i+1}x^3k_i^{-1})$ and $G'({}_{i+1}x) = G({}_{i+1}x^3k_i^{-1})$. Hence $u = v^3$ can be written as

$$ u = \frac{g'({}_{i+1}x)}{G'({}_{i+1}x)} = \frac{g'(f_{i+1}x)}{G'(f_{i+1}x)} = \frac{h({}_{i+1}x)^3}{H({}_{i+1}x)^3} = \frac{h(f_{i+1}x)^3}{H(f_{i+1}x)^3} $$

where $f^3 = 1$ from (i).

If $d = h({}_{i+1}x)/h({}_{i+1}xf)$, then

$$ H({}_{i+1}x)^3 = d^3H({}_{i+1}xf)^3 \quad \text{and} \quad h({}_{i+1}x)^3 = d^3h({}_{i+1}xf)^3. $$

Since h, H are relatively prime, we have $d \in K$ and $df^n = 1$ for $h({}_{i+1}x) = ({}_{i+1}x)^n h'({}_{i+1}x)$ and h' inhomogeneous. Therefore $h'({}_{i+1}x) = h'({}_{i+1}xf)$ and h' depends on ${}_{i+1}x^3$ only. Since H, h are relatively prime, we have $m = n = 0$ and since ${}_{i+1}x^3 \in K({}_ix)$ also $u = (h'/H')^3$ with $h'/H' \in K({}_ix)$ as desired. □

Recall that $z = 2$ if $\operatorname{char} K \neq 2$ and $z = 3$ if $\operatorname{char} K = 2$.

RECOGNITION LEMMA 4.2. *Let K be a field and choose $X = \{{}_0x_g\colon g \in G\}$ a set of independent, commuting variables and root chains ${}_ix_g \in \widetilde{K(x)}$ $(i \in \omega)$ such that*

$$ {}_{i+1}x_g^z = {}_ix_gk_{ig} \quad \textit{for some } k_{ig} \in K. $$

The field $P = K({}_ix_g\colon i \in \omega;\ g \in G)$ has the following properties:

(a) *If $y \in P$ is z^*-high over K, then we can write $y = \prod_{j=1}^{r} {}_{j^*}x_{g_j}^{s(j)}k$ with r distinct elements $g_j \in G$, $k \in K$, $j^* \geqslant 0$, $s(j) \in \mathbf{Z}$ and $s(j) \notin z\mathbf{Z}$ if $j^* > 0$.*

(b) *If* $y = {}_0y \in P$ *and* ${}_{i+1}y^z = {}_iy f_i$ *for some* $f_i \in K$, *then we can find* $r \geqslant 1$, $b_i \in K$ $(i \in \omega)$, *and* $j_0 \geqslant 0$, $g_j \in G$, $s(j) \in \mathbf{Z} \setminus z\mathbf{Z}$ *for* $j \leqslant r$, *such that* $i_0 = \max_{j \leqslant r} j_0$ *and*

$$b_{i+1}^z = b_i \cdot f_i \prod_{j=1}^{r} k_{i-j_0 g_j}^{-s(j)} \quad \text{for all } i \geqslant i_0,$$

where ${}_iy = \prod_{j=1}^{r} {}_{i_j}x_{g_j}^{s(ij)} b_i$ *from* (a).

PROOF. By definition of the sequence ${}_ix_g$ we have

$$k_{ig}^{-1}\, {}_{i+1}x_g^z = {}_ix_g \in K\big({}_{i+1}x_g\colon\ g \in G\big)$$

and therefore $K({}_ix_g\colon\ g \in G) \subseteq K({}_{i+1}x_g\colon\ g \in G)$ is an ascending chain of fields such that $P = \bigcup_{i \in \omega} K({}_ix_g\colon\ g \in G)$. We will show (a) by induction.

(a) Since $y \in P \setminus K$, we find a minimal $i \in \omega$ such that $y \in K({}_ix_g\colon\ g \in G)$. By minimality there must be at least one $h \in G$ such that ${}_ix_h$ appears in the representation of y as a quotient of polynomials in $K[{}_ix_g\colon\ g \in G]$. Extracting the homogeneous part we may write

$$(*) \qquad y = \frac{f}{F}\, {}_ix_h^s$$

with $s \in \mathbf{Z}$ and relatively prime polynomials $f, F \in K[{}_ix_g\colon\ g \in G]$ which are inhomogeneous with respect to the variable ${}_ix_h$. If $K_h = K[{}_ix_g\colon\ g \in G \setminus \{h\}]$, then we claim

$$(**) \qquad f, F \in K_h.$$

Consider f, F as polynomials in ${}_ix_h$, i.e. $f, F \in K_h'[{}_ix_h]$ where K_h' is the quotient field of K_h. In this setting we have to show that f, F are constant. Since y is z^*-high over K, we find $k_t \in K$ $(t \in \omega)$ and relatively prime polynomials

$$f_t, F_t \in K\big[{}_nx_g\colon\ n \in \omega,\ g \in G\big]$$

with $y = (f_t/F_t)^{z'} \cdot k_t$.

Using $(*)$, we derive

$$fF_t^{z'}\, {}_ix_h^s = f_t^{z'} \cdot F \cdot k_t \quad \text{for all } t \in \omega.$$

From Lemmas 4.1(b) and (4.1*)(b), respectively, we see that $f_t, F_t \in K_h'[{}_ix_h]$. Let q be a prime divisor of $f \in K_h'[{}_ix_h]$. Then $q | f_t^{z'} F k_t$ and since f, F are relatively prime, also $q | f_t^{z'}$. Therefore $q | f_t$ and $q^{z'} | f F_t^{z'}\, {}_ix_h^s$. Since f_t, F_t are relatively prime, also $q^{z'} | f_i x_h^s$, and because f is inhomogeneous $q^{z'} | f$. However, $f \in K_h[{}_ix_h]$ has finite degree and $q \in K_h'[{}_ix_h]$ must be a constant, i.e. $q \in K_h'$. We conclude $f \in K_h$ and the same argument shows $F \in K_h$ and $(**)$. There are only finitely many elements ${}_ix_h$ involved in the representation of y at "level" $K[{}_ix_g\colon\ g \in G]$. Therefore the first half of (a) follows by induction. If $i > 0$ in $(*)$, then $s \notin z\mathbf{Z}$ by minimality of i and ${}_ix_h^z = {}_{i-1}x_h k_{i-1|h}$. Therefore $s(j) \notin z\mathbf{Z}$ if $j^* > 0$ in (a). Similarly elements ${}_{j^*}x_{g_j}^{s(j)}$ with the same g_j can be collected into one element, and (a) follows.

(b) Since ${}_iy$ is z^*-high, from (a) we have

$${}_iy = \prod_{j=1}^{r} {}_{i_j}x_{g_j}^{s(ij)} b_i$$

for some $b_i \in K$ and $s(ij) \not\equiv 0 \bmod z$ if $i_j > 0$. Using ${}_{i+1}y^z = {}_iyf_i$ and ${}_{i+1}x_g^z = {}_ix_gk_{ig}$ we compute, for $(i+1)_j > 0$,

$$
\begin{aligned}
{}_{i+1}y^z &= \left(\prod_{t\neq j} {}_{(i+1)_t}x_{g_t}^{s(i+1t)}b_{i+1}\cdot {}_{(i+1)_j}x_{g_j}^{s(i+1j)}\right)^z \\
&= \prod_{t\neq j} {}_{(i+1)_t}x_{g_t}^{zs(i+1t)}b_{i+1}^z\cdot {}_{(i+1)_j}x_{g_j}^{zs(i+1j)} \\
&= \prod_{t\neq j} {}_{(i+1)_t}x_{g_t}^{zs(i+1t)}b_{i+1}^z\cdot {}_{(i+1)_j-1}x_{g_j}^{s(i+1j)}k_{(i+1)_j-1g_j}^{s(i+1j)} \\
&= {}_iyf_i = \prod_{t=1}^{r} {}_{i_t}x_{g_t}^{s(it)}b_if_i.
\end{aligned}
$$

Therefore

$$
(*)\qquad \prod_{t\neq j} {}_{(i+1)_t}x_{g_t}^{zs(i+1t)}b_{i+1}^z\cdot k_{(i+1)_j-1g_j\,(i+1)_j-1}^{s(i+1j)}x_{g_j}^{s(i+1j)} = \prod_{t=1}^{r} {}_{i_t}x_{g_t}^{s(it)}b_if_i \quad \text{if } (i+1)_j > 0
$$

and

$$
(**)\qquad \prod_{t\neq j} {}_{(i+1)_t}x_{g_t}^{zs(i+1t)}b_{i+1}^z\cdot {}_0x_{g_j}^{zs(i+1j)} = \prod_{t=1}^{r} {}_{i_t}x_{g_t}^{s(it)}g_if_i \quad \text{if } (i+1)_j = 0.
$$

From $(*)$ and our representation of ${}_iy$ we derive

$(+)$ If $(i+1)_j > 0$, then $(i+1)_j - 1 = i_j$ and $s(i+1j) = s(ij)$.

From $(**)$ we have

$(++)$ If $(i+1)_j = 0$, then $i_j = 0$ and $zs(i+1j) = s(ij)$.

From $(+)$ and $(++)$ we see that it is impossible to have $i_j = 0$ for infinitely many $i \in \omega$. Hence

$(+++)$ there exists $j_0 \in \omega$ such that $i_j > 0$ for all $i > j_0$.

A trivial induction and $(+)$ imply $i_j = i - j_0$ for all $i \geqslant j_0$. Choose $s(j) = s(j_0, j) = s(i, j)$ which is independent of $i \geqslant j_0$ by $(+)$. Therefore (4.2)(b) follows immediately. □

We will also use the following well-known

OBSERVATION 4.3. If K is a field, $t \in \omega$ and $f(x) = 1 - x^{z^t} \in K[x]$, then $f(x)$ is z-power-free in $K[x]$.

REMARK. Compare the Abel-Capelli-Redei-Theorem in Schinzel [**30**, p. 91, Theorem 21] characterizing irreducible polynomials $x^n - a$.

PROOF. Let $f = \sum_{i<n} a_ix^i \in K[x]$ and $f' = \sum_{i<n} ia_i^{t-1}$ be its derivative. Then $(fg)' = f'g + g'f$ for any $f, g \in K[x]$. Suppose f is not z-power-free, then $f = q^zg$ for some $g, q \in K[x]$ with degree $\deg(q) \geqslant 1$. Then

$$
f' = (q^zg)' = (q^z)'g + g'qz = zq^{z-1}q'g + g'q^z = q\left(zq^{z-2}q'g + g'q^{z-1}\right).
$$

If $f' \neq 0$, then q is a common divisor of f and f'. On the other hand, if $f = 1 - x^{z^t}$, then $f' = z^t x^{z^t - 1}$ and (4.3) holds trivially for $t = 0$. Therefore $t \geqslant 1$ and $f' \neq 0$. In this case $f = 1 - x^{z^t}$ and $f' = z^t x^{z^t - 1}$ are relatively prime, a contradiction. Hence (4.3) holds.

LEMMA 4.4. *Let K be a field and P be the extension field $P = K({}_i x\colon i \in \omega)$ with ${}_{i+1}x^z = {}_i x k_i$ for some $k_i \in K^*$. If $t \in \mathbf{Z} \setminus z\mathbf{Z}$ and $1 \neq b \in K$, then*

$$f = \left(b - {}_i x^t\right)\left(1 - {}_i x^t\right)$$

is not a z-power in P.

PROOF. We distinguish two cases $t > 0$ and $t < 0$ and suppose $f = v^z$ in P for contradiction.

If $t > 0$, then $f = f({}_i x)$ is an inhomogeneous polynomial. From (4.1)(b) and (4.1*)(b), respectively, we find relatively prime polynomials $g({}_i x)$, $G({}_i x) \in K[{}_i x]$ such that $f = (g/G)^z$; hence

$$(*) \qquad G^z({}_i x)\left(b - {}_i x^t\right)\left(1 - {}_i x^t\right) = g^z({}_i x).$$

If q is a prime divisor of $(1 - {}_i x^t)$, then $q | g^z$ and $q^z | g^z$ as well. Hence

$$q^z | G^z\left(b - {}_i x^t\right)\left(1 - {}_i x^t\right)$$

and since g, G are relatively prime, $q^z | (b - {}_i x^t)(1 - {}_i x^t)$. Because $q | (1 - {}_i x^t)$ and $(b - {}_i x^t)$, $(1 - {}_i x^t)$ are relatively prime, also $q^z | (1 - {}_i x^t)$. Hence the degree $\deg(1 - {}_i x^t) = t$ must be a multiple of z which contradicts $t \in \mathbf{Z} \setminus z\mathbf{Z}$. If $t < 0$, then $(*)$ can be replaced by

$$(**) \qquad G^z({}_i x)\left(b - {}_i x^{-t}\right)\left(1 - {}_i x^{-t}\right) = \left(g({}_i x) \cdot {}_i x^{-t}\right)^z$$

which is again an equation in $K[{}_i x]$. The same argument leads to $-t \in z\mathbf{Z}$, which is a contradiction.

Using our notion (2.5) of supports, the convention (3.0) and (3.2), we have

LEMMA 4.5. *Let $R = R(K, G)$ be the field constructed in* (3.2). *If $\alpha k \in \lambda \times \kappa$, define*

$$X_{\alpha k} = \left\{x_{\alpha k g}\colon g \in G\right\}, \quad X_\alpha = \left\{x_{\alpha k g}\colon k \in \kappa,\ g \in G\right\}$$

and similarly

$$X^{\alpha k} = X \setminus X_{\alpha k}, \quad Y^{\alpha k} = \left\{y_{\nu g}\colon \nu \in \lambda^*,\ g \in G,\ k \notin [e_\nu] = \operatorname{Im} e_\nu,\ [y_\nu] \cap X_\alpha = \varnothing\right\}.$$

If $0 \neq a \in F_{\alpha k} = K(X^{\alpha k} \cup Y^{\alpha k})$ and $g \in G$, then $a(1 - x_{\alpha k g})$ is not a z^nth power in R.

PROOF. If $K_{\alpha k} = K(X^{\alpha k})$, then either $a \in K_{\alpha k}$ or $a \in F_{\alpha k} \setminus K_{\alpha k}$. In the first case, let $\nu(a) = 0$, and in the second case there is a $\nu = \nu(a) \in \lambda^*$, not a limit ordinal, such that $a \in R_\nu \setminus R_{\nu - 1}$. Suppose (4.5) does not hold and consider the least criminal $\nu(a)$ for some $a \in F_{\alpha k}^*$.

If $\nu(a) = 0$, then $a \in K_{\alpha k}^*$ and $a(1 - x_{\alpha k g}) = b^z$ $(b \in R)$ is a z-power in R for some $g \in G$. Clearly b must be in $K_{\alpha k}(x_{\alpha k g})$. Since $1 - x_{\alpha k g}$ is a polynomial of degree 1 in $K_{\alpha k}[x_{\alpha k g}]$, and $b = f/F$ with relatively prime polynomials $f, F \in K_\alpha[x_{\alpha k g}]$, we have an equation $aF^z(1 - x_{\alpha x g}) = f^z$ which is impossible by degrees.

Therefore $\nu = \nu(a) > 0$ and $y_\nu \in Y$. The element a can be expressed as $a = (f/F)_i y_{\nu g}^s$ for some $s \in \mathbf{Z}$, and inhomogeneous, relatively prime polynomials $f = f({}_i y_{\nu g})$, $F = F({}_i y_{\nu g})$; compare (3.2)(I_ν). Since $a(1 - x_{\alpha k g})$ is a z-power, $z \in \{2, 3\}$, we can apply (4.10(b) respectively (4.1*)(b) to find polynomials $h, H \in R_\nu[{}_i y_{\nu g}]$ with

$$a(1 - x_{\alpha k g}) = \frac{f}{F}\, {}_i y_{\nu g}^s (1 - x_{\alpha k g}) = \left(\frac{h}{H}\right)^z.$$

From (3.2), (I_ν)(b), we derive

$$(*) \qquad \frac{f}{F}(1 - x_{\alpha x g}) = \left(\frac{h'}{H'}\right)^z (m_i^\alpha g)^{-s}$$

for some new polynomials $h', H' \in R_\nu[{}_i y_{\nu g}]$.

Now we substitute ${}_i y_{\nu g} = 0$, and if $a' = (f(0)/F(0))(m_i^\alpha g)^s$ (f, F are inhomogeneous!), then the last equation (*) turns into

$$a'(1 - x_{\alpha x g}) = (h'(0)/H'(0))^z.$$

Since $\nu(a') < \nu(a) = \nu$ and $a' \in F_{\alpha k}$ as well, the last equation contradicts the minimality of ν. □

In order to prescribe not only automorphisms but also the endomorphism monoid of a field we need the following Lemma 4.6. Our original proof was based on algebraic geometry using the fact that $F(x, y) = f(x) + yg(x)$ as below defines an algebraic curve, cf. R. Hartshorne [**21**, p. 300, Proposition 2.2], W. Fulton [**16**, p. 63ff.]. Then we can argue with M. Deuring [**3**, p. 11, Theorem] counting prime divisors of extension fields which are ramified or inseparable. We conclude that E (below) is finite. However, we can also give a direct and simpler proof.

We would like to thank our colleagues J. Herzog and H. Stichtenoth for a very helpful discussion which lead to the earlier above indicated proof of (4.6).

LEMMA 4.6. *Let K be a field of characteristic $p \geqslant 0$, and z any integer > 1 such that p does not divide z. If $f, g \in K[x]$ are relatively prime and not both in K, then*

$$E = \{k \in K\colon f + kg = h^z \text{ for some } h = h_k \in K[x]\}$$

is a finite set.

PROOF. If f, g are relatively prime in $K[x]$, then $fa + gb = 1$ for some $a, b \in K[x]$ and f, g are also relatively prime over the algebraic closure of K. Passing to the algebraic closure of K, the set E might increase. Hence, we may assume

(i) K is algebraically closed.

If $f \in K$ is a constant, then $g \notin K$ by hypothesis. In this case, consider E' which is defined as E but permuting f and g. Then (i) and $k(g + k^{-1}f) = f + kg = h_k^z$ imply $0 \neq k \in E$ if and only if $k^{-1} \in E'$. Hence we may assume that

(ii) $f \notin K$ is not constant.

Moreover, we may assume that

(iii) $g \notin K$.

If $g \in K$, then E is certainly finite.

Let $n \geqslant 0$ be maximal with $q = p^n$ and $f, g \in K[x^q]$. Then $f + kg \in K[x^q]$ for any $k \in E$. Since $q = p^n$ is a Frobenius automorphism on K by (i), we find $F \in K[x]$ with $F^q = f + kg$ and let f^*, g^* and k^* be the preimages of f, g and k respectively. We derive $F^q = (f^* + k^* g^*)^q$. If t is a prime divisor of $h^z = f + kg = F^q$, then $t|F$ and $t^q|F^q = h^z$. If $h = t^m h^*$ and $(t, h^*) = 1$ are relatively prime, then $(F/t)^q = h^* t^{mz-q}$ and induction shows $mz = sq$ for some $s \in \mathbf{N}$. Since $q = p^n$ and $p \nmid z$, also $m^* = m/q \in \mathbf{N}$. We conclude $h = (t^{m^*})^q h^*$ and induction on the prime components shows $h = H^q$ for some $H \in K[x]$. We conclude $H^z = F = f^* + k^* g^*$. If E^* is as E using f^*, g^* instead, then we have found a bijection $k \to k^*$ between E and E^*. The polynomials f^*, g^* have the additional property that not both are in $K[x^p]$ by maximality of n. We may assume

(iv) $f \notin K[x^p]$ and $f + kg \notin K[x^p]$.

If f' denotes the derivative of f, then (iv) implies $f' \neq 0$ and $f' + kg' \neq 0$. We have to show $f + kg (k \in K)$ has only finitely many roots. Let y be a root of $f + kg = h^z = h_k^z$ for some $k \in K$. Then $h^z(y) = 0$ is a multiple root and y is a root of the polynomial $f' + k'g'$. If $D(x) = f'(x)g(x) - g'(x)f(x)$ is the determinant of this system, then $D(y) = 0$.

We now distinguish cases.

Case 1. If $D(x) = 0$ for all x, then $f'g = fg'$ and $f' \neq 0$ implies $g \mid fg'$. Since f, g are relatively prime, also $g \mid g'$ and g must be constant. This contradicts (iii).

Case 2. If Case 1 does not hold, then $D(x)$ is a polynomial $\neq 0$, which has only finitely many $x \in K$ with $D(x) = 0$. Since $D(y) = 0$, also $f'(y)g(y) = f(y)g'(y)$ and $(f + kg)(y) = 0$ implies $f'(y)g(y) = -kg(y)g'(y)$. If $g(y) = 0$, then $f(y) = 0$ and f, g are not relatively prime, which was excluded. Hence $g(y) \neq 0$ and from the last equation we have $k = -f(y) \cdot g(y)^{-1}$ for only finitely many $y \in K$ with $D(y) = 0$. Hence E must be finite.

5. The field $R(K, G)$ is G-rigid. In this section we want to show that $R = R(K, G)$ satisfies

THEOREM 5.0. End $R = \Phi_p \times G$.

Observe that the theorem and the corollary in §1 follow immediately from §3 and (5.0). If G is infinite and $r \in R \setminus K$, then $[r]$ is finite nonempty and we can find $g \in G$ such that $[r]g \not\subseteq [r]$. Hence $rg \neq r$ and $r \notin R^G$, the fix field of R under the action of G. Since $K \subseteq R^G$ by (2.3), we derive $K = R^G$.

In order to complete the proof, we consider a fixed homomorphism $\phi \in \operatorname{End} R$ and will derive $\phi \in \Phi_p \times G$ at the end of this section. Replacing K by an intermediate field $K' \subseteq R$ of size $\leqslant \kappa$ if necessary, we can find

$(*)$ infinitely many elements $w_n \in K$ with $w_n\phi \in K$ and $w_0 = 0$.

If $x \in X$, then $w\phi \in \widehat{K([x\phi])}$ for all $w \in X$ with $[w\phi] = [x\phi]$. Since $|\widehat{K([x\phi])}| \leqslant \kappa < \lambda = |X|$, by a puigeonhole argument we can find a subset $X' \subseteq X$ such that $|X'| = \lambda$ and $[x\phi] \neq [w\phi]$ for all $x \neq w \in X'$. Because ϕ is injective $[X'\phi]$ has λ many elements and $[X'\phi] = [X'\phi]^\chi \dot\cup [X'\phi]^\nu$ leads to two cases: Either $\|[X'\phi]^\chi| = \lambda$ or $\|[X'\phi]^\chi| < \lambda$, and in the second case we must have $\|[X'\phi]^\nu| = \lambda$.

If $[X'\phi]^X$ has λ many elements, then we recall $\kappa < \lambda$ and can choose sequences $x_i \in X'$ and $x_i' \in X$ $(i \in \omega)$ such that

$$\text{(5.1)} \quad \begin{aligned} &\text{(a) } x_i' \in [x_i\phi]^X \text{ of maximal norm with } x_i' \in \bigcup_{j=0}^{i-1} [x_j\phi], \\ &\text{(b) } x_i' = x_{\alpha_i\beta g_i} \text{ with } \alpha_i < \alpha_{i+1} \in \lambda,\ \beta \in \kappa,\ g_i \in G \ (i \in \omega) \end{aligned}$$

If $|[X'\phi]^Y| = \lambda$, similarly we can choose $x_i \in X'$ and ${}_{n_i}y_i \in R$ with

$$\text{(5.1)(a')} \qquad {}_{n_i}y_i \in [x_i\phi]^Y \quad \text{and} \quad y_i \notin \bigcup_{j<i} [x_j\phi].$$

In case (5.1)(a)(b) let $F^i = \widehat{K(X \setminus \{x_i'\}, Y)} \subseteq \hat{F}$ be the algebraic closure. We use $(*)$ and suppose, for some fixed i,

$$(x_i + w_n)\phi = c_n \text{ is a } z\text{-power in } F^i(x_i) \text{ for all } n \in \omega.$$

Then $c_n = f_n^z/g_n^z$ with $f_n, g_n \in F^i[x_i']$ relatively prime. Since $w_0 = 0$, we have $c_0 + w_n\phi = c_n$, hence $f_0^z/g_0^z + w_n\phi = f_n^z/g_n^z$ and $g_n^z(f_0^z + w_n\phi g_0^z) = f_n^z g_0^z$ follow.

An easy prime divisor argument shows $g_0^z = g_n^z e$ for some unit $e \in F^i$. The last equation turns into $f_0^z + (w_n\phi)g_0^z = f_n^z e$ and $f_0^z + (w_n\phi)g_0^z$ is a z-power in $F^i[x_i']$ for all $n \in \omega$. Since $w_n\phi \in K$ by $(*)$, we derive a contradiction from Lemma 4.6.

We have found a sequence $x_i + w_{n_i} = a_i$ such that (5.1)(a), (b) hold and

$$\text{(5.1)(c)} \qquad a_i\phi \text{ is not a } z\text{-power in } F^i(x_i') \text{ with } F^i = \widehat{K(X \setminus \{x_i'\}, Y)}.$$

A similar argument in case (5.1)(a') leads to a sequence $a_i = x_i + w_{n_i}$ such that (5.1)(a') holds and

$$\text{(5.1)(c')} \qquad a_i\phi \text{ is not a } z\text{-power in } F^i({}_{n_i}y_i) \text{ with } F^i = \widehat{K(X, Y \setminus \{y_i\})}.$$

We will fix this sequence $\{a_i : i \in \omega\} = A$.

By the Black Box (2.10) there exists an ordinal $\alpha \in \lambda^*$ such that the following conditions are satisfied.

$$\text{(5.1)(d)} \qquad A \subseteq P_\alpha \quad \text{and} \quad \phi \restriction \widehat{P_\alpha^*} = \phi_\alpha \restriction R$$

$$\text{(5.1)(e)} \qquad \begin{aligned} &\|A\|, \|A\phi\| < \|f_\alpha\| \quad \text{and} \\ &\|A\|, \|A\phi\| < \|f_{\alpha 0^*}\| \quad \text{if } \tau_\alpha \text{ is a large trap.} \end{aligned}$$

Now we want to show

LEMMA 5.2. *Any ordinal $\alpha \in \lambda^*$ which satisfies* (5.1) *is not useless.*

REMARK. We will find $a_i \in R_\alpha$ $(i \in \omega)$ with the following property of the weak case (§3).

$$(*) \qquad \begin{aligned} &\text{If the choice of } m_i^\alpha \text{ implies } (\mathrm{II}_{\alpha+1}) \text{ for } \beta \in S_\alpha \text{ then either} \\ &m_i^\alpha \text{ or the new choice } m_i^\alpha a_i \text{ in place of } m_i^\alpha \text{ implies } (\mathrm{III}_{\alpha+1}). \end{aligned}$$

PROOF. If α is useless, then any choice $m_i^\alpha \in R_\alpha$ and any ${}_i y_{\alpha g}$ as in $(\mathrm{I}_{\alpha+1})(\mathrm{IV}_{\alpha+1})$ will violate $(\mathrm{III}_{\alpha+1})$ or $(\mathrm{II}_{\alpha+1})$ for $S_{\alpha+1} = S_\alpha$. First we want to get hold of $(\mathrm{III}_{\alpha+1})$ only. Suppose that our first choice $m_i^\alpha \in R_\alpha$ and ${}_i y_{\alpha g}$ implies ${}_i y_\alpha \phi_\alpha' \in R_\alpha$ for some

extension $\phi'_\alpha\colon \widehat{P^*_\alpha}({}_i y_\alpha\colon i\in\omega)\to \widehat{P^*_\alpha}({}_i y_\alpha\colon i\in\omega)$ of $\phi_\alpha\restriction R$ and all $i\geqslant n$. Therefore

(a) $$({}_{i+1}y^z_\alpha)\phi'_\alpha = ({}_i y_\alpha)\phi'_\alpha(m^\alpha_i)\phi_\alpha,\qquad {}_i y_\alpha\phi'_\alpha\in R_\alpha.$$

Next we try $m^\alpha_i a_i$ with $a_i\in R_\alpha\cap \widehat{P^*_\alpha}$ from (5.1). To be definite, we deal with case (5.1)(a); the case (5.1)(a′) is similar. Let ${}_i y'_{\alpha g}$ $(i\in\omega,\ g\in G)$ be the new choice of elements defining

$$R'_{\alpha+1} = R_\alpha\big({}_i y'_{\alpha g}\colon i\in\omega,\ g\in G\big).$$

From $(\mathrm{I}_{\alpha+1})$ we have ${}_{i+1}y'^z_\alpha = {}_i y'_\alpha m^\alpha_i a_i$. Suppose we are unlucky again, hence there exists another extension ϕ''_α of $\phi_\alpha\restriction R$ with ${}_i y'_\alpha\phi''_\alpha\in R_\alpha$ for almost all $i\in\omega$, say for all $i\geqslant n$. We derive

(b) $$({}_{i+1}y'_\alpha)\phi''^z_\alpha = ({}_i y_\alpha)\phi''_\alpha\cdot(m^\alpha_i\phi_\alpha)(a_i\phi_\alpha)\quad\text{where } {}_i y'_\alpha\phi''_\alpha\in R_\alpha\ (i\geqslant n).$$

If $b_i = ({}_i y'_\alpha)\phi''_\alpha/({}_i y_\alpha)\phi'_\alpha$, dividing (b) and (a) leads to

$$b^z_{i+1} = b_i(a_i\phi_\alpha)\quad\text{and}\quad b_i\in R_\alpha\qquad\text{for all } i\geqslant n.$$

If $c_i = a_i\phi_\alpha$, then $b^z_{i+1} = b_i c_i$ and induction shows

(c) $$b^{z^j}_{n+j} = b_n\cdot\prod_{m=0}^{j-1} c^{z^m}_{n+m}.$$

Let $[b_n]^{<} = \{{}_{\gamma_i}y\colon i\leqslant t\}$ and $\gamma_1<\gamma_2<\cdots<\gamma_t$.

Since $\beta\in\kappa$ is fixed in (5.1)(b) and $e_{\gamma_t}\colon\omega\to\kappa$ is an injection, by (I_{γ_t}) there exists $n'\geqslant n$ such that $x'_{\alpha,\beta g_t}\notin\{x_{\gamma_t e_{\gamma_t}ji}\colon i\in\omega,\ j\leqslant t\}$ for all $i\geqslant n'$.

We distinguish three cases $\alpha = \|\{\alpha_i\colon i\geqslant n'\}\| > \|f_{\gamma_t}\|$, $\alpha<\|f_{\gamma_t}\|$ and $\alpha=\|f_{\gamma_t}\|$.

In the first case we find some $n''\geqslant n'$ with $\alpha_i>\|f_{\gamma_t}\|$ for all $i\geqslant n''$. We derive $b_n\in F^i$ with F^i defined in (5.1)(c). Similarly $c_j\in F^i$ for all $j<i$ from (5.1)(a). If $i = n+j-1$ then (c) implies that $c_i^{z^{j-1}}$ is z^jth power of an element in $F^i(x'_i)$; hence c_i is a z-power in $F^i(x'_i)$, which contradicts (5.1)(c).

In the second case $(\alpha<\|f_{\gamma_t}\|)$ we have $b_n\in R_{\gamma_t+1}\setminus R_{\gamma_t}$ and $c_i\in R_\beta$ for some $\beta<\gamma_t$ and almost all $i\in\omega$. Hence $c_i\in R_{\gamma_t}$ for all $i\geqslant n'$ and some n', and we may let $n' = n$. From $b^z_{i+1} = b_i c_i$ $(i\geqslant n)$ and Definition 3.1(a) we see that b_n is z^*-high in R_{γ_t+1} over R_{γ_t}. From Lemma 4.2(b) we find elements $d_i\in R_{\gamma_t+1}$ and M_i a product of elements $m^{\gamma_t}_i$ such that

(d) $$d^{z^j}_{n+j} = b_n M_j.$$

If $q_j = M_j\prod_{m=0}^{j-1} c^{-z^m}_{n+m}L$, then $1\neq q_j\in R_{\gamma_t}$ by supports of c_i and M_j; cf. (5.1)(e). Dividing (d) by (c) we have $q_j = (d_{n+j}/b_{n+j})^{z^j}$. By z-purity $q_j\neq 1$ is a z^j-power in R_{γ_t}. This contradicts the choice of q_j in R_{γ_t}.

Finally let $\alpha = \|f_{\gamma_t}\|$. Since $\|\{a_{\gamma_t i}\colon i\in\omega\}\|<\|f_\alpha\|$, there exists $n'\geqslant n$ such that $x'_i\notin\bigcup_{j\in\omega}[m^{\gamma_t}_j]$ for all $i\geqslant n'$ and the argument as in the first case leads to a contradiction.

From this contradiction we derive the following:

(i) There exists a sequence $a_{\alpha i}\in R_\alpha\cap\widehat{P^*_\alpha}$ with the following property. If m^α_i is chosen after (I_α) and $(\mathrm{III}_{\alpha+1})$ fails, then $m^\alpha_i a_{\alpha i}$ and appropriate ${}_i y_{\alpha g}$ will satisfy $(\mathrm{III}_{\alpha+1})$, i.e.

$${}_i y_{\alpha g}\phi'_\alpha\notin R_\alpha\quad\text{for all } i\in\omega\text{ and all extensions }\phi'_\alpha\supseteq\phi_\alpha\restriction R.$$

Next we want to take care of $(\mathrm{II}_{\alpha+1})$ for $S_{\alpha+1} = S_\alpha$, i.e.

(ii) There exist $m_i^\alpha \in R_\alpha \cap \widehat{P_\alpha^*}$ $(i \in \omega)$ and ${}_iy_{\alpha g} (i \in \omega,\ g \in G)$ such that for any $\beta \in S_\alpha$ and any extension $\phi'_\beta \supseteq \phi_\beta \restriction R_{\alpha+1}$ there are numbers $i(\alpha+1, \beta)$ such that

$$ {}_iy_\beta\phi'_\beta \notin R_{\alpha+1} = R_\alpha\big({}_iy_{\alpha g}\colon i \in \omega,\ g \in G\big) \quad \text{for all } i \geqslant i(\alpha+1, \beta). $$

First we concentrate on a *fixed* ordinal $\beta \in S_\alpha$ and consider $\phi'_\beta\colon \widehat{P_\beta^*}({}_iy_\beta\colon i \in \omega) \to \hat{F}$ some extension of $\phi_\beta \restriction R_\alpha$. Since β is strong, we have by the induction hypothesis

(iii) $$ {}_iy_\beta\phi'_\beta \notin R_\alpha \quad \text{for all } i \geqslant i(\alpha, \beta). $$

Choose the sequence $a_{\alpha i} \in R_\alpha$ by (i), choose any fixed increasing sequence $e_\alpha\colon \omega \to \kappa$ after $(\mathrm{I}_{\alpha+1})$ and pick a parameter b_α which will be corrected later. Hence m_i^α is determined by the Black Box (2.10) and we find ${}_iy_\alpha$ which satisfy $(\mathrm{I}_{\alpha+1})$ and $(\mathrm{III}_{\alpha+1})$. Suppose we are unlucky and there exists $i_0 \in \omega$ such that (ii) does not hold for some ϕ'_β; hence

$$ {}_iy_\beta\phi'_\beta \in R_{\alpha+1} = R_\alpha\big({}_iy_{\alpha g}\colon i \in \omega,\ g \in G\big) \quad \text{for all } i \geqslant i_0. $$

Clearly $m_i^\beta \in \widehat{P_\beta^*} \cap R_\beta$ by (I_β)(b) and also $m_i^\beta\phi'_\beta = m_i^\beta\phi_\beta \in R_\beta$. If ${}_iy_\beta\phi'_\beta \in R_\alpha$, from

$$ \big({}_{i+1}y_\beta^z \cdot {}_iy_\beta^{-1}\big)\phi'_\beta = m_i^\beta\phi_\beta \in R_\beta \subseteq R_\alpha $$

we derive $({}_{i+1}y_\beta\phi'_\beta)^z \in R_\alpha$. Since R_α is z-pure in R, also ${}_{i+1}y_\beta\phi'_\beta \in R_\alpha$.

Induction shows ${}_iy_\beta\phi'_\beta \in R_\alpha$ for almost all $i \in \omega$. This contradicts (iii) and we derive

(iv) $$ {}_iy_\beta\phi'_\beta \in R_{\alpha+1} \setminus R_\alpha \quad \text{for all } i \geqslant i_0, $$

which is z^*-high in $R_{\alpha+1}$ over R_α.

Hence we can apply Lemma 4.2(b) and find elements

(v) $$ r \geqslant 1, \quad b_i \in R_\alpha, \quad g_j \in G, \quad j_0 \geqslant 0, \quad s(j) \in \mathbf{Z} \setminus z\mathbf{Z} \quad \text{for } j \leqslant r $$

and if $i_1 = \max\{j_0, i_0, j \leqslant r\}$, then

(vi) $$ b_{i+1}^z = b_i\big(m_i^\beta\phi_\beta\big) \prod_{j=1}^{r} \big(m_{i-j_0g_j}^\alpha\big)^{-s(j)} \quad \text{for all } i \geqslant i_1. $$

We now distinguish cases, either $\beta + \kappa^{\aleph_0} \geqslant \alpha$ or $\beta + \kappa^{\aleph_0} < \alpha$. In the first case we want to trade ${}_iy_\alpha$ into a better element such that "β becomes strong at level $\alpha+1$", i.e. ${}_iy_\beta\phi'_\beta \notin R_{\alpha+1}$ for all extensions ϕ'_β of $\phi_\beta \restriction R_\alpha$. In the second case we will derive strongness at level $\alpha+1$ by our choice of the Black Box: In this case the branch at β is far away from α.

Case 1. Let $\beta < \alpha$ be such that $\beta + \kappa^{\aleph_0} \geqslant \alpha$. Let us choose another sequence $e'_\alpha\colon \omega \to \kappa$ with $\mathrm{Im}(e'_\alpha) \cap \mathrm{Im}(e_\alpha)$ finite. The elements $a_{\alpha i}$ remain the same such that (i) holds for ${}_iy'_\alpha$ and $m'_i\alpha$ as in (I_α) with the new elements. Therefore, from (I_α)(b) ${}_{i+1}y_\alpha'^z = {}_iy'_\alpha m_i'^\alpha$, and suppose that we are still unlucky for β. The same arguments lead to the elements

(v′) $$ r' \geqslant 1,\ b'_i \in R_\alpha,\ g'_j \in G,\ j'_0 \geqslant 0,\ s'(j) \in \mathbf{Z} \setminus z\mathbf{Z} \text{ for } j \leqslant r',\ i'_1 \in \omega, $$

such that for $i_2 = \max\{i_1, i_1', j_0' : j \leqslant r'\}$ the following holds:

(vi') $$b_{i+1}'^{z} = b_i'\left(m_i^{\beta}\phi_\beta\right)\prod_{j=1}^{r'}\left(m_{i-j_0'g_j'}'^{\alpha}\right)^{-s'(j)} \quad \text{for all } i \geqslant i_2.$$

If $B_i = b_i/b_i'$ $(i \geqslant i_2)$, then we derive from (vi) and (vi') the new equations

(vii) $$B_{i+1}^{z} = B_i\prod_{j=1}^{r}\left(m_{i-j_0g_j}^{\alpha}\right)^{-s(j)}\prod_{j=1}^{r'}\left(m_{i-j_0'g_j'}'^{\alpha}\right)^{s'(j)} \quad \text{for all } i \geqslant i_2.$$

We will show the existence of $i_3 \geqslant i_2$ such that

(viii)
(a) $x_{\alpha eig} \notin \left[B_{i_2}\right]^{x}$ [compare (2.5) and $(\mathrm{IV}_{\alpha+1})$(b)],
(b) $x_{\alpha eig} \notin T(f_\gamma)$ for all $y_{f_\gamma} \in \left[B_{i_2}\right]^{y}$ [compare (2.5), (3.5)],
(c) $x_{\alpha eig} \notin \bigcup_{j\in\omega}\left[m_i'^{\alpha}\right]^{x}$, for all $i \geqslant i_3$ and all $g \in G$.

Requirement (viii)(c) can be arranged because $\operatorname{Im}e_\alpha' \cap \operatorname{Im}e_\alpha$ is finite and $x_{\alpha eig} \in [y_{\alpha g}]^{x}$. There are only finitely many $\gamma_1, \ldots, \gamma_k < \lambda^*$ such that $[B_{i_2}]^{y} = \{y_{\gamma_1}, \ldots, y_{\gamma_k}\}$. Since $B_{i_2} \in R_\alpha$, also $\gamma_i < \alpha$. Therefore $\operatorname{Im}f_\alpha \cap \operatorname{Im}f_{\gamma_i}$ is finite by the Black Box 2.10(ii) and we can choose i_3 large enough such that (viii)(b) holds. Finally $B_{i_2} \in R_\alpha$ and $\|[B_{i_2}]^{x}\| < \|f_\alpha\|$, hence (viii)(a) can be arranged easily. Using the explicite form of m_i^{α} in (I_α)(b)(i) or (ii), respectively, an induction on (vii) leads to the equations

$$B_{i_2+m+1}^{z^{m+1}} = B_{i_2}\cdot H_m\prod_{j=1}^{m}\left(1 - x_{\alpha e(m-j_0)g_j}\right)^{z^j}.$$

By our last observation (viii), $[H_m]$ and $[B_{i_2}]$ do not contain $x_{\alpha e(m-j_*)g_j}$ for $m \geqslant i_3 + i_1$, $j \leqslant r$. If $F^j = F_{\alpha e(i_3+i_1-j_0)}$ as defined in Lemma 4.5, then the last remark is equivalent to saying that H_m and B_{i_2} are both elements in the field F^j. If $c_r = \sqrt[z^m]{B_{i_2}H_m}$, then $c_r \in F^r$ and the last equation turns into $c_r(1 - x_{\alpha e(i_3+i_1-r_0)g_r}) = B_{i_2+i_3+i_1+1}^{z}$ which is a z-power in $F_{\alpha e(i_3+i_1-r_0)}$. This contradicts Lemma 4.5, i.e. we cannot be unlucky twice at β.

Let e^ν $(\nu \in \kappa^{\aleph_0})$ be a set of pairwise almost disjoint maps $e^\nu\colon \omega \to \kappa$ (which certainly exist). If we cannot finish Case 1 with these e^ν $(\nu \in \kappa^{\aleph_0})$, then for each $\nu \in \kappa^{\aleph_0}$ there exists an ordinal $\beta(\nu)$ such that $\beta(\nu) < \alpha \leqslant \beta(\nu) + \kappa^{\aleph_0}$ where $\beta(\nu)$ is strong, but ${}_iy_{\beta(\nu)}\phi_\beta' \in R_{\alpha+1}^{\nu}$ for some $\phi_\beta' = \phi_{\beta(\nu)}'$ where

$$R_{\alpha+1}^{\nu} = R_\alpha\left({}_iy_{\alpha g}^{\nu} : i \in \omega,\ g \in G\right)$$

and ${}_iy_{\alpha g}^{\nu}$ is constructed as in (I_α) with the help of e^ν in place of e_α. Since $\beta(\nu)$ assumes fewer than $\kappa^{\aleph_0}$ values, there must be a β which is the image $\beta = \beta(\nu) = \beta(\nu')$ of two different $\nu \neq \nu' \in \kappa^{\aleph_0}$. Hence we are unlucky twice at this β, which was just ruled out. Therefore we can find $\nu \in \kappa^{\aleph_0}$ and $e_\alpha = e^\nu$ such that

(ix) ${}_iy_\beta\phi_\beta' \notin R_{\alpha+1}$ for all extensions $\phi_\beta' \supset \phi_\beta \restriction R_\alpha$, almost all $i \in \omega$ and all $\beta \in S_\alpha$ with $\beta + \kappa^{\aleph_0} \geqslant \alpha$.

Therefore we fix this e_α (and $a_{\alpha i}$) and consider the

Case 2. $\beta < \alpha$ such that $\beta + \kappa^{\aleph_0} < \alpha$.

We want to show

(x) If $\beta < \alpha$ is strong, then ${}_i y_\beta \phi'_\beta \notin R_{\alpha+1}$ for all extensions $\phi'_\beta \supseteq \phi_\beta \restriction R_\alpha$ and for almost all $i \in \omega$.

We fix such ordinal β and argue as in (viii) but using (vi). We can find $i_2 \geqslant i_1$ such that

(xi)
(a) $x_{\alpha e i g} \notin [b_{i_1}]^x$,
(b) $x_{\alpha e i g} \notin T(f_\gamma)$ for all $y_\gamma \in [b_{i_1}]^y$,
(c) $x_{\alpha e i g} \notin \bigcup_{j \in \omega} [m_j^\beta \phi_\beta]^x$.

In this case only (c) needs explanation. Recall $m_j^\beta \phi_\beta \in \widehat{P_\beta^*}$ and $\|m_j^\beta \phi_\beta\| < \|f_\beta\| \leqslant \|f_\alpha\|$ by the Black Box 2.10(i) and (2.7). From $\beta + \kappa^{\aleph_0} < \alpha$ and (2.10)(iii) we derive (xi)(c).

As in Case 1, an induction on (vi) leads to

(xii) $$b_{i_1+m+1}^{z^{m+1}} = b_{i_1} h_m \prod_{j=1}^{m} \left(1 - x_{\alpha e (m-j_0) g_j}\right)^{z^j}.$$

By observation (xi), $[h_m]^x$ and $[b_{i_1}]^x$ do not contain $x_{\alpha e(m-j_0)g_j}$ for $m \geqslant i_2 + i_1$, $j \leqslant r$.

$$\text{If } c_m = \sqrt[z^m]{b_{i_1} h_m}, \text{ then } c_m = \prod_{j=1}^{r} \left(1 - x_{\alpha e (m-j_0) g_j}\right) \text{ is a } z\text{-power.}$$

Again, Lemma 4.5 leads to a contradiction. We conclude (x) and (5.2) is shown. □

We have the immediate

COROLLARY 5.3. *An ordinal $\alpha < \lambda^*$ which satisfies* (5.1) *is strong or weak according as ${}_i y_\alpha \phi'_\alpha$ lies outside or in R for some extension $\phi'_\alpha \supseteq \phi_\alpha \restriction R$ and for almost all $i \in \omega$, respectively.*

LEMMA 5.4. *Let K be a field with endomorphism ϕ such that $a\phi \in \{a, a^{-1}\}$ for all $a \in K$. Then $\phi = \mathrm{id}$.*

PROOF. Since $\mathrm{Im}\phi \subseteq K$ is a subfield and $a\phi = a$, respectively $a\phi = a^{-1}$, we must have $a \in \mathrm{Im}\phi$ for all $a \in K$. Therefore $\mathrm{Im}\phi = K$ and ϕ is an automorphism.

Suppose that we found $a \in K$ such that $a\phi = a^{-1}$. Therefore $(1 + a)\phi = 1 + a^{-1} \in \{(1 + a), (1 + a)^{-1}\}$. If $1 + a^{-1} = 1 + a$, then $a^2 = 1$. If $(1 + a^{-1}) = (1 + a)^{-1}$, then $1 = (1 + a^{-1})(1 + a)$ and $a^2 + a + 1 = 0$. Hence $a^2 = 1$ or $a^2 + a + 1 = 0$ which leaves at most 4 possibilities for such elements a. Hence

$$[K : \mathrm{Fix}\, K] = r \text{ is finite and } |K \setminus \mathrm{Fix}\, K| \leqslant 3$$

for the field $\mathrm{Fix}\, K$ of all invariant elements of ϕ. We derive

$$(r - 1)|\mathrm{Fix}\, K| = |K \setminus \mathrm{Fix}\, K| \leqslant 3$$

and r must be 1 or 2. If $r = 1$, then $K = \mathrm{Fix}\, K$ and (5.4) follows. If $r = 2$, then $|\mathrm{Fix}\, K| = |K \setminus \mathrm{Fix}\, K| \leqslant 3$ and again $K = \mathrm{Fix}\, K$ implies (5.4). If $\mathrm{Char}(K) > 0$, we need a more general result.

Recall our notion $\mathrm{ex}(p^t) \in \Phi_p$ of Frobenius homomorphisms from §3.

LEMMA 5.5. *Let* $R = R(K,G)$ *be the field constructed in* (3.2). *If* $\phi \in \operatorname{End} R$ *such that the following holds*:

(*) *For all* $a \in R$ *there exist* $\varepsilon(a) \in \{1, -1\}$, $g(a) \in G$, $t(a) \in \mathbf{Z}$ *with* $a\phi = a^{\varepsilon(a)}g(a)\exp(p^{t(a)})$,

then $\phi \in G \times \Phi_p$.

PROOF. We want to find $t \in \mathbf{Z}$, $g \in G$ such that

(i) $$\phi \restriction X = g \cdot \exp(p^t) \restriction X.$$

If $x, y \in X$ are different, and $\varepsilon(x) = \varepsilon$, $t(x) = t$, $g(x) = g$ from (*), then we have to show

(ii) $$\varepsilon = \varepsilon(y), \quad t = t(y) \quad \text{and} \quad g = g(y).$$

From (*) we derive

(iii) $$x^{\varepsilon p^t g} + y^{\varepsilon(y)p^{t(y)}g(y)} = (x+y)^{\varepsilon(x+y)p^{t(x+y)}g(x+y)},$$

and we distinguish four cases. The first one leads to (ii) and the others lead to contradictions.

Case 1. Let $\varepsilon(x+y) = 1$ and $t' = t = t(x+y) \geqslant 0$.

From (iii) we have

$$(xg)^{\varepsilon p^t} + (yg(y))^{\varepsilon(y)p^{t(y)}} = (xg(x+y))^{p^{t'}} + (yg(x+y))^{p^{t'}}.$$

Recall the action of G on X; hence

$$(xg)^{tp^t} = (xg(x+y))^{p^{t'}}, \qquad (yg(y))^{\varepsilon(y)p^{t(y)}} = (yg(x+y))^{p^{t'}}$$

and $g = g(x+y)$, $g(x+y) = g(y)$, $\varepsilon p^t = p^{t'} = \varepsilon(y)^{pt(y)}$ by independence of the variables. Therefore $g = g(y)$ and $\varepsilon = \varepsilon(y)$, $t = t(y)$ and (ii) is shown in this case.

Case 2. Let $\varepsilon(x+y) = 1$ and $t(x+y) < 0$, hence $t' = -t(x+y) > 0$ and (iii) implies

$$xg(x+y) + yg(x+y) = (x+y)g(x+y) = \left[(x+y)^{\varepsilon(x+y)g(x+y)p^{-t'}}\right]^{p^{t'}}$$

$$= [(x+y)\phi]^{p^{t'}} = (x\phi)^{p^{t'}} + (y\phi)^{p^{t'}} = xg^{\varepsilon p^{t+t'}} + yg(y)^{\varepsilon(y)p^{t(y)+t'}}.$$

Hence $g = g(x+y) = g(y)$, $\varepsilon = \varepsilon(y) = 1$ and $t = -t' < 0$. Therefore $x\phi = xg^{p^t} \in R$ and since $t \leqslant -1$, also $(xg)^{p^{-1}} = \sqrt[p]{x} \in R$ which is impossible.

Case 3. Let $\varepsilon(x+y) = -1$ and $t' = t(x+y) > 0$.

Then we have from (iii),

(iv) $$(x+y)^{-g(x+y)p^{t'}} = (x+y)\phi = x\phi + y\phi = xg^{\varepsilon p^t} + yg(y)^{\varepsilon(y)p^{t(y)}}$$

and also

$$(x+y)^{g(x+y)p^{t'}}\left(xg^{\varepsilon p^t} + yg(y)^{\varepsilon(y)^{t(y)}}\right) = 1.$$

Substitute $y = 0$ to get

$$xg(x + y)^{p^{t'}} \cdot (xg)^{\varepsilon p^t} = 1,$$

hence

$$xg(x + y)^{p^{t'}} = xg^{-\varepsilon p^t}$$

and $g(x + y) = g$, $p^{t'} = -\varepsilon p^t$ and $\varepsilon = -1$, $t = t'$.

Similarly, substitute $x = 0$ to get $g(x + y) = g(y)$, $\varepsilon(y) = -1$, t'-$t(y)$. Together we have $g = g(x + y) = g(y)$, $t = t(y)$, $\varepsilon = \varepsilon(y) = -1$, and (iv) turns into

$$(x + y)^{-p^t} = x^{-p^t} + y^{-p^t}.$$

The last equation is equivalent to

$$x^{2p^t} + x^{p^t}y^{p^t} + y^{2p^t} = 0;$$

however, y is transcendental over $K(x)$, a contradiction.

Case 4. If $\varepsilon(x + y) = -1$, and $t(x + y) < 0$, then let $t' = -t(x + y) > 0$ and argue as in the last case for a contradiction.

Hence (i) follows, and finally we show

(v) $$\phi \restriction R = g \cdot \mathrm{ex}(p^t), \quad \text{i.e.} \quad a\phi = ag^{p^t} \quad \text{for all } a \in R.$$

Let $a \in R$ and choose any variable $x \in X$ algebraically independent from $ag(a)$ and $ag(xa)$ (which certainly exists). From (i) and (*) we have

$$\begin{aligned}(xg)^{p^t}(ag(a))^{\varepsilon(a)p^{t(a)}} &= (x\phi)(a\phi) = (xa)\phi = ((xa)g(xa))^{\varepsilon(xa)p^{t(xa)}} \\ &= (xg(xa))^{\varepsilon(xa)p^{t(xa)}} \cdot (ag(xa))^{\varepsilon(xa)p^{t(xa)}}\end{aligned}$$

and from our choice of x,

$$xg(xa)^{\varepsilon(xa)p^{t(xa)}} = (xg)^{p^t} \quad \text{and} \quad (ag(a))^{\varepsilon(a)p^{t(a)}} = (ag(xa))^{\varepsilon(xa)p^{t(xa)}}.$$

The first equation implies $g(xa) = g$, $\varepsilon(xa)s = 1$ and $t(xa) = t$. Hence

$$(ag(a))^{\varepsilon(a)p^{t(a)}} = (ag)^{p^t}$$

from the second equation, and (v) is shown. □

From (3.3) we have $\Phi_p \times G \subseteq \mathrm{End}\, R$. From (5.4) and (5.5) we have a

COROLLARY 5.6. *If* $\alpha \in \lambda^*$ *and* $v\phi_\alpha \in v\Phi_p \times G \cup v^{-1}\Phi_p \times G$ *for all* $v \in \widehat{P_\alpha^*} \cap R$, *then* $\phi_\alpha \restriction R \in \Phi_p \times G \restriction \widehat{P_\alpha^*}$.

Observe that it is easy for $p = 0$, to replace $v\phi_\alpha \in v\Phi_p \times G \cup v^{-1}\Phi_p \times G$ by $v\phi_\alpha \in \{v, v^{-1}\}$ in (5.6).

The following lemma is the major step in the proof of (5.0).

LEMMA 5.7. *Let* $\alpha \in \lambda^*$ *be such that* τ_α *is a large trap* $\tau_\alpha = (\tau_{i^*})_{i \in \omega}$. *If* $\phi_{0^*} \restriction R_\alpha$ *is not the restriction of a map in* $\Phi_p \times G$, *then* α *is a strong ordinal.*

PROOF. Since $\tau_\alpha = (f_\alpha, P_\alpha, \phi_\alpha)$ is a large trap, we have a sequence $\tau_\alpha = (\tau_{i^*})_{i\in\omega}$ of traps $\tau_{i^*} = (f_{i^*}, P_{i^*}, \phi_{i^*})$ $(i^* \in \lambda)$ satisfying (2.9). Suppose R_α has been constructed. From Lemma 5.2 we know at least that α is not a useless ordinal. Hence we can find ${}_iy_\alpha$ $(i \in \omega)$ with

(i) ${}_iy_\alpha\phi'_\alpha \notin R_\alpha$ for any map ϕ'_α extending $\phi = \phi_\alpha \restriction R_\alpha$ and all $i \in \omega$ and

(ii) $m_i^\alpha = a_{\alpha i}(1 - x_{\alpha ei})$, say $a_{\alpha i} = a_i$, $x_{\alpha ei} = z_i$ from (I_α). In fact, the remark after (5.2) holds as well. If ${}_iy_\alpha\phi' \notin R_{\alpha+1}$ for almost all $i \in \omega$, and each extension ϕ' of ϕ, then (5.7) holds. Hence we may assume

(iii) ${}_iy_\alpha\phi' \in R_{\alpha+1}$ for all $i \in \omega$, and some extension ϕ' of ϕ. Therefore

$$\big({}_{i+1}y_\alpha^z\,{}_iy_\alpha^{-1}\big)\phi' = m_i^\alpha\phi' = a_i(1 - z_i)\phi \in R_{\alpha+1} \quad \text{by } (\mathrm{I}_\alpha) \text{ and (ii)}.$$

Since $\|a_i(1 - z_i)\| < \|f_\alpha\|$, also

(iv) $a_i(1 - z_i)\phi \in R_\alpha$.

Using (i) and (iv), we see that ${}_iy_\alpha\phi'$ is z^*-high over R_α. From Lemma 4.2(b) we find $r \geqslant 1$, $b_i \in R_\alpha$, $j_0 \geqslant 0$, $g_j \in G$, $s(j) \in \mathbf{Z} \setminus z\mathbf{Z}$ $(j \leqslant r)$ such that for $i_0 = \max\{j_0, j \leqslant r\}$ the following holds

$$\text{(v)} \qquad b_{i+1}^z = b_i\big[a_i(1 - z_i)\big]\phi \cdot \prod_{j=1}^{r}\big[a_{i-j_0}(1 - z_{i-j_0})\big]g_j^{-s(j)} \quad \text{for all } i \geqslant i_0.$$

Now we want to find better elements ${}_iy'_\alpha$ $(i \in \omega)$ such that

$$\text{(vi)} \qquad {}_{i+1}y_\alpha'^z = {}_iy'_\alpha m_i'^\alpha \quad \text{and} \quad R'_{\alpha+1} = R_\alpha\big({}_iy'_{\alpha g}\colon i \in \omega,\ g \in G\big) \qquad [\text{see (3.2)}].$$

Our hypothesis that $\phi_{0^*} \restriction R$ is not the restriction of a map from $\Phi_p \times G$ will allow us to prove ${}_iy_\alpha\phi' \notin R'_{\alpha+1}$ for any extension $\phi' \supseteq \phi_\alpha$. From Corollary 5.6 and our hypothesis $\phi_\alpha \restriction P_{0^*}^* \cap R_\alpha = \phi_{0^*} \restriction R_\alpha \notin \Phi_p \times G$, we find in this case

$$(+) \qquad b \in \widehat{P_{0^*}^*} \cap R_\alpha \text{ that } b\phi \notin bg\Phi_p \cup b^{-1}g\Phi_p \text{ for all } g \in G.$$

We choose this element b and see that the element $m_i'^\alpha$ in (I_α)(b)(ii) hence ${}_iy'_\alpha$, is completely determined by a_i, z_i as in (ii), $y_i = y_{f_i}$, from the partial trap τ_{i^*} of the large trap τ_α.

Suppose that the new elements are not good enough to prove strongness of α, hence ${}_iy'_\alpha \in R'_{\alpha+1} \setminus R_\alpha$ for all $i \in \omega$. We now work for contradiction. Since $m_i'^\alpha = a_i(1 - z_i)(b - y_i)(1 - y_i)$, the same argument as for (v) leads to elements $r' \geqslant 1$, $b'_i \in R_\alpha$, $j'_0 \geqslant 0$, $g'_j \in G$, $s'(j) \in \mathbf{Z} \setminus z\mathbf{Z}$ $(j \leqslant r')$ such that for $i_2 = \max\{j'_0, i_1\colon j \leqslant r\}$ the following holds:

$$\text{(v')} \qquad b_{i+1}'^z = b'_i\big[a_i(1 - z_i)(b - y_i)(1 - y_i)\big]\phi \cdot \prod_{j=1}^{r'}\big[a_{i-j'_0}(1 - z_{i-j'_0})(1 - y_{i-j'_0})\big]g_j'^{-s'(j)} \quad \text{for all } i \geqslant i_2.$$

If $B_i = b'_i/b_i$, then (v) and (v') give rise to equations

$$\text{(viii)} \qquad B_{i+1} = B_i\big[(b - y_i)(1 - y_i)\big]\phi \prod_{j=1}^{r'}\big[(b - y_{i-j'_0})(1 - y_{i-j'_0})\big]g_j'^{-s'(j)} \cdot \prod_{j=1}^{r'}\big[a_{i-j'_0}(1 - z_{i-j'_0})\big]g_j'^{-s'(j)} \cdot \prod_{j=1}^{r}\big[a_{i-j_0}(1 - z_{i-j_0})\big]g_j^{s(j)}.$$

We want to simplify (viii) and derive first

(ix) $$r = r';\ j_0 = j_0',\ g_j = g_j',\ s(j) = s'(j) \quad \text{for all } j \leqslant r.$$

Let $j \leqslant r'$ be fixed and suppose $g_j' \notin \{g_1, \ldots, g_r\}$. Then we choose $i \in \omega$ large enough such that $z_{i-j_0'g_j'} = x_{\alpha e i - j_0' g_j'}$ occurs only in the x-supports of the elements $z_{i-j_0'}g_j'$ or B_i of the right-hand side of (viii). Collecting factors of (viii) into w_i, equations (viii) can be written as

(viii′) $$B_{i+1}^z = B_i \cdot w_i\big(1 - z_{i-j_0'}\big) g_j'^{-s'(j)} \quad \text{and} \quad z_{i-j_0'g_j} \notin [w_i].$$

Induction on (viii′) leads to

(∗) $$B_{i+m+1}^{z^{m+1}} = B_i H_m \big(1 - z_{i-j_0'+m}\big)^{-s'(j)z^m},$$

where $z_{i-j_0'+m} \notin [H_m]^*$. If m is large enough, also $z_{i-j_0'+m} \notin [B_i]^x$ and (∗) leads to a z-power

$$B_{i+m+1}^z = \big(B_i H_m\big)^{1/z^m}\big(1 - z_{i-j_0'+m}\big)^{-s'(j)} \text{ such that } s'(j) \notin z\mathbf{Z},$$

which contradicts Lemma 4.5. Therefore $g_j' \in \{g_1, \ldots, g_r\}$ and by induction, symmetry and new enumeration we conclude

$$r = r' \quad \text{and} \quad g_j = g_j' \qquad \text{for all } j \leqslant r.$$

Therefore (viii) turns into

(viii″)
$$\begin{cases} B_{i+1}^z = B_i\big[(b - y_i)(1 - y_i)\big]\phi \cdot \prod_{j=1}^{r}\big[(b - y_{i-j_0'})(1 - y_{i-j_0'})\big] g_j^{-s'(j)} \\ \qquad \cdot \dfrac{\big[a_{i-j_0}(1 - z_{i-j})\big] g_j^{s(j)}}{\big[a_{i-j_0'}(1 - z_{i-j_0'})\big] g_j^{s'(j)}}. \end{cases}$$

If $j \leqslant r$ is fixed and $j_0 \neq j_0'$, we may assume without loss of generality that $j_0' < j_0$, which implies

(xi) $$i - j_0 < i - j_0' \quad \text{for all } i.$$

As before, but using (xi) instead, we can choose i large enough such that $z_{i-j_0'g_j} = x_{\alpha e i - j_0' g_j}$ occurs only in the supports of elements $z_{i-j_0'}g_j$ or B_i of the right-hand side of (viii″). Again, (viii″) can be written as

$$B_{i+1}^z = B_i w_i \big(1 - z_{i-j_0'}\big) g_j^{-s'(j)}$$

for some w_i with $z_{i-j_0'}g_j \notin [w_i]^x$. As in case (x) we are lead to a contradiction, which shows $j_0 = j_0'$ for all $j \leqslant r$. Again, we can simplify (viii″) and we derive

(viii‴) $$B_{i+1}^z = B_i \prod_{j=1}^{r} T_{ij}\big(1 - z_{i-j_0}\big) g_j^{s(j)-s'(j)}$$

$$\text{where } T_{ij} = \frac{\big[(b - y_i)(1 - y_i)\big]\phi}{\big[(b - y_{i-j_0})(1 - y_{i-j_0})\big] g_j^{s'(j)}} g_j^{s(j)-s'(j)}.$$

If $j \leqslant r$ is fixed and $s(j) \neq s'(j)$, then let $s(j) - s'(j) = u \cdot z^n$ with $u \in \mathbf{Z} \setminus z\mathbf{Z}$. Observe that $\|T_{ij}\| < \|z_0\|$. Then we can choose i large enough such that $z_{i-j_0}g_j \notin [\prod_{j=1}^{r} T_{ij}]^x$. Induction on (viii‴) leads to the equation

$$B_{i+m+1}^{z^{m+1}} = B_i \cdot H_m \big(1 - z_{i-j_0+m-n}\big)^{z^m u}$$

such that, for m large enough, $z_{(i-j_0+m-n)g_j}$ is not in the support of B_i and H_m. Again, Lemma 4.5 will give a contradiction. Hence (ix) is settled and (viii‴) turns into the handsome equations

$$B_{i+1}^{z} = B_i Y_i \tag{xii}$$

with

$$Y_i = \frac{(b\phi - y_i\phi)(1 - y_i\phi)}{\prod_{j=1}^{r}(b - y_{i-j_0})g_j^{s(j)}(1 - y_{i-j_0})g_j^{s(j)}}. \tag{xiii}$$

Induction shows

$$B_{i+m+1}^{z^{m+1}} = B_i Z_m \quad \text{for } Z_m = \prod_{j=0}^{m} Y_{i+j}^{2^j}. \tag{xiv}$$

Let $[B_i]^{y} = \{y_{u_i}\colon u_i = (f_{\gamma_i}, g_i') \in \lambda^{\omega} \times G,\ i \leqslant e\}$ the y-support of B_i and choose $\gamma_1 < \cdots < \gamma_e$ in λ^*. Now we compare $\beta = \sup_{i\in\omega} y_i$ and $\|f_{\gamma_e}\|$. Call $u_e = u$, $\gamma_e = \gamma$, $g_e' = g'$ and consider

Case I. $\|f_\gamma\| > \beta$.

Certainly we can write $B_i = (f/F)_k y_u^t$ with relatively prime and inhomogeneous polynomials $f, F \in R^e[{}_k y_u]$, where $R^e = R_\gamma({}_i y_{\gamma g}\colon\ g \in G \setminus \{g'\},\ i \in \omega\}$. From Lemma 4.1 and (4.1*) we find inhomogeneous, relatively prime polynomials h_m, $H_m \in R^e[{}_k y_u]$ such that

$$\left(\frac{h_m}{H_m}{}_{k+m} y_u^t\right)^{z^m} = \frac{f}{F}\,{}_k y_u^t Z_m.$$

If $t = 0$, then substitute ${}_k y_u^t = 0$ and continue at the equations similar to (xvi).

Using definition (3.2)(III$_\gamma$)(b) of ${}_k y_u$, we have ${}_{i+1} y_u^z\, {}_i y_u^{-1} = m_i^\gamma g'$ and the last equation turns into

$$\left(\frac{h_m}{H_m}\right)^{z^m} = \frac{f}{F} Z_m \prod_{j=0}^{m-1} \left(m_{k+j}^\gamma g'\right)^{z^j}. \tag{xv}$$

Observe that ${}_k y_u$ appears only in the inhomogeneous polynomials h_m, H_m, f, F. Now we substitute ${}_k y_u = 0$ and obtain new z-power equations from (xv).

$$\left(\frac{h_m(0)}{H_m(0)}\right)^{z^m} = \frac{f(0)}{F(0)} Z_m \prod_{j=0}^{m-1} \left(m_{k+j}^\gamma g'\right)^{z^j}. \tag{xvi}$$

Finally use the (by now) standard support argument to kill (xvi): Since $x_{\gamma e(k+j)g'} \in [m_{k+j}^\gamma g']$ by (3.2)(III$_\gamma$)(c), (d), we can choose j large enough such that $x_{\gamma e(k+j)g'}$ does not appear in Z_m and $f(0)$, $F(0)$. Then Lemma 4.5 leads to a contradiction.

Case II. $\|f_\gamma\| = \beta$.

Since $\|m_k^{\gamma'}\| < \beta$, we can find $i_2 \geqslant i_1$ such that

$$y_i \notin \bigcup_{j\leqslant e} [m_k^{m_j}] \quad \text{for all } i \geqslant i_2.$$

Using the same substitution argument, we derive a contradiction from (4.5).

After finitely many steps we derive at the final

Case III. $\|f_\gamma\| < \beta$.

Observe that the substitution argument (xvi) might have changed the B_i but not Z_m. Without loss of generality we will work with the same equations as in (xiv).

By hypothesis, we can choose $q \geqslant i_2$ such that $\|y_i\| > \|f_\gamma\|$ for all $i \geqslant q$. Hence $B_{i_2} \in R_{q^*}$ and suppose $j_0 > 0$ for some fixed $j \leqslant r$ in (xiii). If

$$R^j = R_{q^*}\big({}_k y_{q^*} g\colon k \in \omega,\ g \in G \setminus \{g_j\}\big),$$

then (xiii) and (xiv) can be written as

$$B_{q+m+1}^{z^{m+1}} = A\big[(b - y_q)\phi(1 - y_q)\phi\big]^{z^m} \quad \text{with } A \in R^j.$$

Since $y_q\phi = y_q\phi_{q^*}$ is z^*-high in $R_{q^*}({}_i y_{qg}\colon i \in \omega,\ g \in G)$ over R_{q^*}, we find $k' \geqslant 1$, $h_{qj} \in G$, $u_q \in R_{q^*}$, $j_q^* \geqslant 0$, $t(q_j) \in \mathbf{Z} \setminus z\mathbf{Z}$ with

$$y_q\phi = \prod_{j=1}^{k'} {}_{j_q} y_q^{t(q_j)} h_{qj} u_q \tag{xvi}$$

from Lemma 4.2(a).

We will consider the case $g_j = h_{qi}$ for some $i \leqslant k'$. The case $g_j \notin \{h_{ki}\colon i \leqslant k'\}$ is similar but simpler. We may assume that $g_j = h_{qj}$ and substitute (xvi) into the last equation. Hence

$$B_{q+m+1}^{z^{m+1}} = A\big(b\phi - {}_{j^*} y_q g_j d\big)\big(1 - {}_{j^*} y_q g_j d\big) \quad \text{with } A, d \in R^j,\ j^* = j_q^*. \tag{xvii}$$

By Lemma 4.1, respectively (4.1*) the inhomogeneous polynomial

$$\big(b\phi - {}_{j^*} y_q g_j d\big)\big(1 - {}_{j^*} y_q g_j d\big) \in R^j[{}_{j^*} y_q g_j]$$

is a z-power in $R^j({}_i y_q g_j\colon i \in \omega)$, which contradicts Lemma 4.4. Therefore $j_0 = 0$ and $g_j = h_{qj}$ for all $j \leqslant r$. Together with (xvi) we can write (xiii) as

$$Y_i = \frac{\big(b\phi - \prod_{j=1}^r {}_{j^*} y_i^{t(ij)} g_j u_i\big)\big(1 - \prod_{j=1}^r {}_{j^*} y_i^{t(ij)} g_j u_i\big)}{\prod_{j=1}^r \big(bg_j - y_i g_j\big)^{s(j)} (1 - y_i g_i)^{s(j)}}. \tag{xiii'}$$

Now suppose $r > 1$ in (xiii'). We collect all other factors ($j \neq 1$) of (xiii') in

$$u = \prod_{j=2}^r {}_{j^*} y_i^{t(ij)} u_i \quad \text{and} \quad A = \prod_{j=2}^r \big(bg_j - y_i g_j\big)^{s(j)} (1 - y_i g_i)^{s(j)}.$$

Let $0 < s < z$ such that $s(1) \equiv s \bmod z$ and $1^* = w$, $g_1 = g$, $y = {}_w y_{ig}$, $t = t(i, 1)$.

Recall from the construction (3.2) that $R_{i^*+1} = R_{i^*}({}_n y_{ih}\colon n \in \omega,\ h \in G)$ and consider the subfield

$$S_{i^* g} = R_{i^*}\big({}_n y_{ih}\colon n \in \omega,\ h \in G \setminus \{g\}\big).$$

Since $y_i g = d \cdot {}_w y_{ig}^{z^n} = d y^{z^n}$ for some $d \in R_{i^*}$ from (3.2), equation (xiii') turns into an equation with coefficients $(u, A, \dots)$ in $S_{i^* g}$:

$$Y_i = \frac{\big(b\phi - y^t u\big)\big(1 - y^t u\big)}{A\big(bg - y^{z^n} d\big)^s \big(1 - y^{z^n} d\big)^s}$$

with $s \in \{1,2\}$ ($\operatorname{char} K \neq 2 \Rightarrow s = 1$) and $w = 0$ or $t \notin z\mathbf{Z}$. From (xii) we know that B_iY_i (with $B_i \in S_{i^*g}$) is a z-power in R_{i^*+1}. From (4.1) and (4.1*) we find relatively prime polynomials $h, H \in S_{i^*g}[y]$ with

$$\frac{B_i(b\phi - y^t u)(1 - y^t u)}{A(bg - y^{z^w}d)^s(1 - y^{z^w}d)^w} = \left(\frac{h}{H}\right)^z.$$

Therefore, since $s \in \{1,2\}$ and $s = 1$ if $\operatorname{char} K \neq 2$,

$$\text{(xx)} \qquad \begin{aligned} H^z(b\phi - y^t u)(1 - y^t u)B_i &= h^z(bg - y^{z^w}d^*)^s(1 - y^{z^w}d)^s A \\ &= h^z(bg^s - y^{sz^w}d)(1 - y^{sz^w}d^s)A \end{aligned}$$

The polynomials $(g - y^{z^w}d)^s$ and $(1 - y^{z^w}d)^s$ are z-power-free by (4.3). Since $b \neq 1$ by ( ), also $bg \neq 1$, and the polynomials are relatively prime as well. Arguing with prime divisors in some algebraic closure $\widehat{S_{i^*g}}[y]$, (xx) implies

$$(bg - y^{z^w}d)^s(1 - y^{z^w}d)^s \mid (b\phi - y^t u)(1 - y^t u).$$

Consider the case $\operatorname{char}(K) = p \nmid t$. Then also $(b\phi - y^t u)$ and $(1 - y^t u)$ are z-power-free and relatively prime by (+). Similarly

$$(b\phi - y^t u)(1 - y^t u) \mid (bg - y^{z^w}d)^s(1 - y^{z^w}d)^s.$$

Therefore the two products differ only by a unit in $S_{i^*g}[y]$. There exists $B \in S_{i^*g}$ such that

$$\text{(xxi)} \qquad (b^s g - y^{sz^w}d^s)(1 - y^{sz^w}d^s) = B(b\phi - y^t u)(1 - y^t u).$$

From the degree of the polynomials we conclude $2t = 2sz^w$, hence $t = sz^w$. If $w = 0$, then $t = s$. Suppose $w \neq 0$, then $t \notin z\mathbf{Z}$, hence $sz^w \notin z\mathbf{Z}$ and $w = 0$ is a contradiction. Since $w = 0$, $t = s$, we derive from (xxi)

$$(b^s g - y^s d^s)(1 - y^s d^s) = (b\phi - y^s u)(1 - y^s u).$$

Comparing roots of y^s, we find $\{(b^s g)d^{-s}, d^{-s}\} = \{b\phi u^{-1}, u^{-1}\}$, hence $\{b\phi, 1\} = \{(b^s g)d^{-s}u, d^{-s}u\}$. There are two possibilities. Either $d^{-s}u = 1$ and $b\phi = b^s g d^{-1}u = b^s g$ or $1 = b^s g d^{-s}u$ and $b\phi = d^{-s}u = b^{-s}g$. Because $s = 1$ or $s = \operatorname{char} K = 2$, the map is a Frobenius homomorphism and in any case $b\phi \in bg\Phi_p \cup b^{-1}g\Phi_p$ which contradicts (+). Therefore we consider the case $\operatorname{char}(K) = p \mid t$, say $t = p^n m$ with $n > 0$, and $0 \neq p \nmid m$. If $b' = (b\phi)^{p^n}$ and $u' = u^{p^n}$ in $\widehat{S_{i^*}}$, then (xx) turns into

$$H^z(b' - y^m u')^{p^n}(1 - y^m u')^{p^n} B_i = h^z(bg - y^{z^w}d)^s(1 - y^{z^w})^s A.$$

If $w \neq 0$, then $t \notin z\mathbf{Z}$ and the multiplicity of roots forces $n = 0$. Therefore $t = m$ and $p \nmid t$ was excluded in this case. Hence $w = 0$ and $d = 1$ by definition. The last equation equals

$$H^z(b' - y^m u')^{p^n}(1 - y^m u')^{p^n} B_i = h^z(bg - y)^s(1 - y)^s A.$$

Since $\operatorname{char}(K) = p \nmid m$ and $u' \neq 0$, $b' \neq 1$, the polynomials $(b' - y^m u')$ and $(1 - y^m u')$ are z-power-free by (4.3) and relatively prime. The last equation implies

$$(b' - y^m u')(1 - y^m u') \mid (bg - y)^s(1 - y)^s$$

and the degree forces $m = 1$.

Since $(bg - y)^s(1 - y)^s$ is z-power-free, we also have

$$(bg - y)^s(1 - y)^s \mid (b' - yu')^{p^n}(1 - yu')^{p^n}.$$

Hence $H^z \mid h^z$ and H is constant because H, h are relatively prime. Therefore $(b' - yu')^{p^n}(1 - yu')^{p^n}B_i/(bg - y)^s(1 - y)^s A$ is a z-power in $S_{i*}[y]$. Comparing roots, we find $\{bg, 1\} = \{b'u'^{-1}, u'^{-1}\}$, hence $\{bgu', u'\} = \{b', 1\}$.

Case I. $u' = 1$, $bgu' = b'$. By definition of b' we have $(b\phi)^{p^{-n}} = b' = bg$ and $b\phi = b^{p^n}g \in bg\Phi_p$.

Case II. $u' = b'$, $bgu' = 1$. By definition of b' we have $(b\phi)^{p^{-n}} = u' = b^{-1}g$ and $b\phi = (b^{-1})^{p^n}g \in b^{-1}g\Phi_p$. In any case $b\phi \in bg\Phi_p \cup b^{-1}g\Phi_p$ which contradicts (+). Therefore α must be strong.

Finally we want to prove (5.0). Because of (3.3) it remains to show $\operatorname{End} R \subseteq \Phi_p \times G$. Suppose $\phi \in \operatorname{End} R \setminus \Phi_p \times G$ and suppose we derived

(*) There exists $\alpha \in \lambda^*$ such that $\phi_\alpha \restriction R = \phi \restriction \widehat{P_\alpha^*}$ is not the restriction of a map in $\Phi_p \times G$.

By the Black Box we can find another $\beta \in \lambda^*$ with (*) for $\phi_\beta \restriction R$ and the hypothesis of (5.7). Hence β is a strong ordinal and ${}_iy_\beta\phi = {}_iy_\beta\phi'_\beta \notin R$. In particular, $\phi \notin \operatorname{End} R$, a contradiction. Therefore (5.0) follows as soon as (*) is proved.

Suppose $\phi_\alpha \restriction R = {}^\alpha\phi g^\alpha \restriction R$ with ${}^\alpha\phi$ induced by ${}^\alpha\phi \in \Phi_p$ and g^α induced by ${}^\alpha g \in G$ on $R \cap \widehat{P_\alpha^*}$. We want to show

(**) If $\alpha, \beta \in \lambda^*$, then ${}^\alpha\phi = {}^\beta\phi$ and ${}^\alpha g = {}^\beta g$.

Choose any $x_t \in \widehat{[P_\alpha]^x}$ and $x_{t'} \in [P_\beta]^x$. There exists $\gamma \in B$ such that $x_t, x_{t'} \in [P_\gamma]^x$ and $\phi_\gamma = \phi \restriction \widehat{(P_\gamma^* \cap R)}$ by the Black Box 2.10. Since $t, t' \in \lambda \times \kappa \times G$, let $t = (\delta, k, h)$ and $t' = (\delta', k', h')$. We derive $x_t\phi = x_t\phi_\alpha = x_t({}^\alpha\phi)(g^\alpha) = x_{\delta k h^\alpha g}{}^\alpha\phi$ and similarly $x_{t'}\phi = x_{\delta' k' h'^\beta g}{}^\beta\phi$ as well as

$$x_t\phi = x_t\phi_\gamma = x_{\delta k h^\gamma g}{}^\gamma\phi \quad \text{and} \quad x_{t'}\phi = x_{\delta' k' h'^r g}{}^\gamma\phi.$$

Using the law of right cancellation on G, we derive ${}^\alpha g = {}^\gamma g = {}^\beta g$ and ${}^\alpha\phi = {}^\gamma\phi = {}^\beta\phi$. From (**) we have $\phi \in \Phi_p \times G$, which contradicts our assumption on ϕ. □

References

1. N. Bourbaki, *Algebra*, Part 1, Addison-Wesley, Reading, Mass., 1974.
2. A. L. S. Corner and R. Göbel, *Prescribing endomorphism algebras—a unified treatment*, Proc. London Math. Soc. (3) **50** (1985), 447–479.
3. M. Deuring, *Lectures on the theory of algebraic functions of one variable*, Lecture Notes in Math., vol. 314, Springer-Verlag, Berlin and New York, 1973.
4. M. Dugas and R. Göbel, *Every cotorsion-free ring is an endomorphism ring*, Proc. London Math. Soc. (3) **45** (1982), 319–336.
5. _____, *Every cotorsion-free algebra is an endomorphism algebra*, Math. Z. **181** (1982), 451–470.
6. _____, *Field extensions in L,—A solution of C. U. Jensen's $25-problem*, (Proc. Oberwolfach, 1985), Abelian Group Theory (R. Göbel and E. A. Walker, eds.), Gordon and Breach, London, 1986.
7. _____, *Field extensions*, Notices Amer. Math. Soc. **32** (1985), 482.
8. M. Dugas, A. Mader and C. Vinsonhaler, *Large E-rings exist*, J. Algebra (to appear).
9. W. Feit and P. Fong, *Rational rigidity of $G_2(p)$ for any prime $p > 5$*, Proc. Rutgers Group Theory Year, 1983–1984, (M. Aschbacher, D. Gorenstein, R. Lyons, M. O'Nan, C. Sims and W. Feit, eds.), Cambridge Univ. Press, Cambridge, 1984, pp. 323–326.
10. B. Franzen and R. Göbel, *Prescribing endomorphism rings—the cotorsion-free case*, Pacific J. Math. (to appear).

11. E. Fried, *Automorphism group of integral domains fixing a given subring*, Algebra Universalis **7** (1977), 373–387.

12. _____, *A comment on automorphism groups of fields*, Studia Sci. Math. Hungar. **14** (1979), 315–317.

13. E. Fried and J. Kollar, *Automorphism groups of fields*, Colloq. Math. Soc. János Bolyai **29** (1977), 293–303.

14. _____, *Automorphism group of algebraic number fields*, Math. Z. **163** (1978), 121–123.

15. M. Fried, *A note on automorphism groups of algebraic number fields*, Proc. Amer. Math. Soc. **80** (1980), 386–388.

16. W. Fulton, *Algebraic curves*, Benjamin, New York, 1969.

17. W. D. Geyer, *Jede endliche Gruppe ist Automorphismengruppe einer endlichen Erweiterung $K|\mathbf{Q}$*, Arch. Math. **41** (1983), 139–142.

18. R. Göbel and S. Shelah, *Torsion-free modules*. II, Fund. Math. (to appear).

19. R. Göbel, *Wie weit sind Moduln vom Satz von Krull-Remak-Schmidt entfernt*? Jahresber. Deutsch. Math.-Verein. **88** (1986), 11–49.

20. J. De Groot, *Groups represented by homomorphism groups*, Math. Ann. **138** (1959), 80–102.

21. R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math., No. 52, Springer-Verlag, Berlin and New York, 1977.

22. D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math. **110** (1892), 104–129.

23. W. Kuyk, *The construction of fields with infinite cyclic automorphism group*, Canad. J. Math. **17** (1965), 665–668.

24. D. J. Madden and R. C. Valentini, *The group of automorphisms of algebraic function fields*, J. Reine Angew. Math. **343** (1983), 162–168.

25. B. H. Matzat, *Über das Umkehrproblem der Galoisschen Theorie*, Jahresber. Deutsch. Math.-Verein. (1986).

26. E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1918), 221–229.

27. P. Pröhle, *Does the Frobenius endomorphism always generate a direct summand in the endomorphism monoid of prime characteristic*, Bull. Austral. Math. Soc. **30** (1984), 335–356.

28. P. Pröhle, unpublished.

29. I. R. Safarevic, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR Ser. Math. **18** (1954), 525–578; Amer. Math. Soc. Transl. **4** (1956), 185–237.

30. A. Schinzel, *Selected topics on polynomials*, Univ. of Michigan Press, Ann Arbor, 1982.

31. S. Shelah, *Classification theory*, North-Holland, Amsterdam, 1978.

32. _____, *Existence of rigid-like families of abelian p-groups*, Model Theory and Algebra, Lecture Notes in Math., vol. 498, Springer-Verlag, Berlin and New York, 1975, pp. 384–402.

33. _____, *A combinatorial principle and endomorphism rings*. I, *On p-groups*, Israel J. Math. **49** (1984), 239–257.

34. _____, *A combinatorial theorem and endomorphism rings of abelian groups*. II, Abelian Groups and Modules (Proc. Udine conference), (R. Göbel, C. Metelli, A. Orsatti, and L. Salce, eds.), CISM, Courses and Lectures, vol. 287, Springer, Wien, 1984, pp. 37–86.

35. H. Stichtenoth, *Zur Realisierbarkeit endlicher Gruppen als Automorphismengruppen algebraischer Funktionenkörper*, Math. Z. **187** (1984), 221–225.

36. R. G. Swan, *Noether's problem in Galois theory*, pp. 21–40, Emmy Noether in Bryn Mawr (J. D. Sally and B. Srinivasan, eds.), Springer, New York, 1983, pp. 21–40.

37. J. G. Thompson, *Some finite groups of type G_2 which appear as Galois groups over Q*, J. Algebra (to appear).

38. _____, *Some finite groups which appear as Galois groups over* **Q**, J. Algebra (to appear).

39. D. J. Winter, *The structure of fields*, Graduate Texts in Math., No. 16, Springer-Verlag, Berlin and New York, 1974.

40. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Graduate Texts in Math., No. 28, Springer-Verlag, Berlin and New York, 1975.

Department of Mathematics, Baylor University, Waco, Texas 76798

Fachbereich 6, Mathematik, Universitat GHS Essen, D-4300 Essen 1, Federal Republic of Germany (Current addres of Rüdiger Göbel)

Current address (Manfred Dugas): Department of Mathematics, Baylor University, Waco, Texas 76798