Relative negligibility of linear automorphisms

Hamza Ahmad ¹, Mowaffaq Hajja a,*,2

a Department of Mathematics, Yarmouk University, Irbid, Jordan

Received 4 September 2007
Available online 12 May 2008
Communicated by Efim Zelmanov

Abstract

Let $U$ and $V$ be finite-dimensional vector spaces over a field $k$, $\alpha \in GL(U)$, $\beta \in GL(V)$ and $I$ be the identity transformation on $V$. Denote by $\alpha \ast \beta$ and $\alpha \ast I$ the induced linear automorphisms on $U \oplus V$; $\alpha \ast \beta$ and $\alpha \ast I$ can also be regarded as $k$-automorphisms on the function field $k(U \oplus V)$. It is elementary to check whether $\alpha \ast \beta$ and $\alpha \ast I$ are conjugate within $GL(U \oplus V)$ by examining their rational canonical forms. In this paper we shall give necessary and sufficient conditions for $\alpha \ast \beta$ and $\alpha \ast I$ to be conjugate within $\text{Aut}_k(k(U \oplus V))$. For this characterization, we introduce the concept of the generalized order. Through this invariant we also settle the question of when two different polynomials are minimal polynomials of the same linear automorphism of a rational function field.

© 2008 Elsevier Inc. All rights reserved.

Keywords: Linear automorphisms; Generalized order; Relative negligibility

1. Introduction

Let $K = k(x_1, \ldots, x_n)$ be the field of rational functions in $n$ indeterminates over a field $k$. Such a field is said to be a rational extension of $k$, and the set $\{x_1, \ldots, x_n\}$, as well as any other set of $n$ elements that generate $K$, is called a base of $K$ (over $k$). It is clear that a $k$-automorphism

* Corresponding author.
E-mail addresses: hyahmad@svsu.edu (H. Ahmad), mhajja@yu.edu.jo, mowhajja@yahoo.com (M. Hajja).

1 It is a pity that Dr. Ahmad did not live to see a work that he was so proud of accomplishing see light. Hamza passed away on February 11, 2007 at the age of 39 after struggling with cancer for several years. The death of such a talented mathematician at such an early age is a great loss to the mathematical community.

2 The second named author is supported by a research grant from Yarmouk University.

0021-8693/$ – see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jalgebra.2008.02.039
of $K$ is completely determined by how it acts on a base of $K$. When $n = 1$, this action is necessarily projective linear, by Lüroth’s Theorem. When $n = 2$ and $k$ is algebraically closed of characteristic 0, a set of nice-looking generators of the group $\text{Aut}_k(K)$ of $k$-automorphisms of $K$ is given in [14, Chapter 5, p. 17]. When $n \geq 3$, no such set of generators is known and the problem of finding such generators is a long standing open problem in transcendental field theory. However, certain types of actions of elements of $\text{Aut}_k(K)$ have been extensively studied. Notable among these are those $k$-automorphisms that stabilize the $k$-submodule $kx_1 + \cdots + kx_n$ of $K$ for some base $\{x_1, \ldots, x_n\}$ of $K$. For lack of a better term, such automorphisms are called linear automorphisms.

Note that the set of linear automorphisms on $K$ does not have any algebraic structure since the composition of linear automorphisms is not necessarily linear, linearity being base-dependent. Note also that a linear action may be preserved under a certain non-linear change of base, and thus a linear automorphism is not expected to have a unique minimal polynomial. A simple example is obtained by taking $\alpha$ to be the $k$-automorphism of $k(x, y)$ defined by $\alpha(x) = -x$ and $\alpha(y) = -y$, where $\text{char}(k) \neq 2$, and considering the two bases $\{x, y\}$ and $\{x, xy\}$. One sees that $\alpha$ has both $T + 1$ and $T^2 - 1$ as minimal polynomials. This unpleasant situation of not having a unique minimal polynomial is compensated by the intriguing fact that a linear automorphism is completely determined by any of its minimal polynomials [11, Theorem 3]. Thus if $f(T) \in k[T]$ is a minimal polynomial for two linear $k$-automorphisms of $K$, then these automorphisms are conjugate in the group $\text{Aut}_k(K)$.

The fact that a linear automorphism does not determine a unique minimal polynomial raises the very natural question regarding what the different minimal polynomials of the same linear automorphism have in common. It is obvious that if a linear automorphism $\alpha$ has a finite order, then any two minimal polynomials $f$ and $g$ of $\alpha$ must have the same order, where the order of $f$ is understood to be the smallest $n$ for which $f(T)$ divides $T^n - 1$. The converse is also true: If two polynomials have the same finite order, then they can be realized as minimal polynomials of the same linear automorphism [6, Theorem 1.5(ii)]. This prompts the following analogous question regarding polynomials of infinite order.

**Question 1.** What are the conditions on $f(T), g(T) \in k[T]$ that are necessary and sufficient for $f$ and $g$ to be minimal polynomials of the same linear automorphism?

A complete and satisfactory answer to Question 1 is given in Theorem 6.6 in terms of what we have chosen to call the generalized order of $f$. This is a pair $(R(f), \omega(f))$, where $R(f)$ is the multiplicative group generated by the zeros of $f$ in some algebraic closure $\bar{k}$ of $k$, and where $\omega(f)$ is a non-negative integer that depends on the maximum multiplicity among the zeros of $f$ in $\bar{k}$. With this term introduced, we prove that $f$ and $g$ can serve as minimal polynomials for the same linear automorphism if and only if they have the same generalized order, i.e., if $R(g) = R(f)$ and $\omega(g) = \omega(f)$. In fact, this comes as a consequence of a fairly stronger result regarding negligibility properties of linear automorphisms that we now describe.

Let $K$ and $L$ be rational extensions of $k$, and let $\alpha$ and $\beta$ be $k$-automorphisms of $K$ and $L$, respectively. The free compositum of $K$ and $L$ over $k$ will be denoted by $K \ast L$. Thus $K \ast L$ is the field of quotients of the tensor product $K \otimes_k L$. The natural extension of $\alpha \otimes_k \beta$ to a $k$-automorphism on $K \ast L$ will be denoted by $\alpha \ast \beta$. We will say that $\beta$ is negligible relative to $\alpha$ if $\alpha \ast \beta$ and $\alpha \ast I$ are conjugate in $\text{Aut}_k(K \ast L)$, where $I$ is the identity automorphism on $L$.

The notion of negligibility was introduced in [6], and several negligibility theorems, together with applications to rationality problems can be found in [1,7,11,12], and [2]. In particular, it
follows from [8] and [9] that if \( f \) and \( g \) are minimal polynomials of the linear \( k \)-automorphisms \( \alpha \) and \( \beta \), respectively, then \( \beta \) is negligible relative to \( \alpha \) in the two cases when \( g \) divides \( f \) and when order(\( g \)) divides order(\( f \)). Since neither of these two conditions implies the other, it follows that neither of them can be necessary for \( \beta \) to be negligible relative to \( \alpha \). This gives even more impetus to the following very natural question.

**Question 2.** If \( \alpha \) and \( \beta \) are linear \( k \)-automorphisms having \( f \) and \( g \) as minimal polynomials, respectively, then what conditions on \( f \) and \( g \) are necessary and sufficient for \( \beta \) to be negligible relative to \( \alpha \)?

We give a complete answer to this question in Theorem 6.5. We prove that \( \beta \) is negligible relative to \( \alpha \) if and only if the generalized order of \( g \) divides that of \( f \), in the sense that \( R(g) \subseteq R(f) \) and \( \omega(g) \leq \omega(f) \). This is the main theorem of this article.

The paper is organized as follows: After introducing the terminology and preliminary facts in Section 2, we give in Section 3 a refined description of a linear automorphism of a rational function field in terms of (any of) its minimal polynomial(s). Sections 4 and 5 establish necessary conditions for a linear automorphism \( \beta \) to be negligible relative to a linear automorphism \( \alpha \), and introduce the ingredients of the generalized order, namely the inseparability \( \omega(\alpha) \) and the group \( R(\alpha) \). The last section completes our main theorems by establishing sufficiency of the conditions for negligibility.

2. Terminology, notation, and preliminaries

Throughout, \( k \) will denote an arbitrary field. We fix an algebraic closure \( \bar{k} \) of \( k \), and we assume that all algebraic extensions of \( k \) are in \( \bar{k} \).

The set of all rational (= purely transcendental) extensions of \( k \) of finite transcendence degree over \( k \) is denoted by \( \mathbb{E}(k) \). A transcendence basis \( B \) of \( K \in \mathbb{E}(k) \) for which \( k(B) = K \) will be called a base of \( K \). The group of all \( k \)-automorphisms of \( K \) will be denoted by \( \text{Aut}_k(K) \) (or simply \( \text{Aut}(K) \)). The identity automorphism of \( K \) is denoted by \( I_K \) or by \( I_n \), where \( n \) is the transcendence degree of \( K \) over \( k \). Thus \( I_0 \) stands for the identity automorphism of \( k \). Where no confusion should arise, \( I \) stands for “\( I_n \) for some \( n \)”.

For \( i = 1, 2 \), let \( K_i \in \mathbb{E}(k) \) and let \( s_i \) be a \( k \)-automorphism of \( K_i \). We denote by \( K_1 \otimes K_2 \) the free compositum of \( K_1 \) and \( K_2 \) over \( k \), or equivalently, the quotient field of the tensor product \( K_1 \otimes_k K_2 \). We denote by \( \alpha_1 \otimes_k \alpha_2 \) the natural extension of \( \alpha_1 \otimes_k \alpha_2 \) to \( K_1 \otimes K_2 \). We say that \( \alpha_1 \) and \( \alpha_2 \) are equivalent, and we write \( \alpha_1 \cong \alpha_2 \), if there exists a \( k \)-isomorphism \( \sigma : K_1 \rightarrow K_2 \) such that \( \sigma^{-1} \alpha_2 \sigma = \alpha_1 \).

A \( k \)-automorphism \( \alpha \) of \( K \in \mathbb{E}(k) \) is said to be affine if it stabilizes the \( k \)-submodule \( k \oplus kx \) of \( K \) for some base \( x = \{x_1, \ldots, x_n\} \) of \( K \), i.e., if

\[
\alpha(x) = Ax + B
\]

where \( A \in GL_n(k) \), \( B \) a column vector in \( k^n \), and \( x = [x_1, \ldots, x_n]^T \). When \( \alpha \) stabilizes the \( k \)-submodule \( kx_1 \oplus kx_2 \oplus \cdots \oplus kx_n \), i.e., when \( B = 0 \), the automorphism \( \alpha \) is called linear. Equivalently, a linear automorphism is obtained by extending an automorphism \( \alpha \) of a finite-dimensional \( k \)-module \( V \) in the natural way to a \( k \)-automorphism of the symmetric \( k \)-algebra \( k[V] \) and then again to its quotient field \( k(V) \), which is nothing but the rational extension of \( k \) whose transcendence degree is the dimension of \( V \). (In fact, if \( x \) is a basis of \( V \), then a basis of the dual \( V^* \) of \( V \) would serve as a base of \( k(V) \).)
The simplest linear automorphisms are those companion to a (uni-variable) polynomial: If \( f(T) \in k[T] \) is of degree \( d \) and \( f(0) \neq 0 \), then the automorphism companion to \( f \) is the automorphism \( s \) defined on the \( d \)-dimensional \( k \)-module \( V^* = kx_0 \oplus kx_2 \oplus \cdots \oplus kx_{d-1} \) by

\[
s(x_i) = x_{i+1} \quad \text{for } 0 \leq i \leq d - 2, \quad \text{and} \quad f(s)x_0 = 0.
\]

We denote this \( k \)-automorphism by \([f]\), and we denote its extension to \( k(V) \) by \( \langle f \rangle \). We also denote the \( k \)-automorphism defined on \( k \oplus V \) by \( s(x_i) = x_{i+1} \quad \text{for } 0 \leq i \leq d - 2, \quad \text{and} \quad f(s)x_0 = c, \quad c \in k, \) by \([f, c]\), and its extension to \( k(V) \) by \( \langle f, c \rangle \). Thus \( \langle f \rangle = \langle f, 0 \rangle \) . It is worth mentioning that in previous articles, the automorphism \( \langle f \rangle \) (respectively \( \langle f, c \rangle \) ) was denoted by \( \sigma \langle f \rangle \) (respectively \( \sigma \langle f, c \rangle \) ), and was called the cyclic linear (respectively affine) automorphism associated with \( f \) (respectively with \( f \) and \( c \) ). We also remark that the delimiters \( \langle \rangle \) are also used to mean “the group generated by,” but no ambiguity will arise.

The theory of rational canonical forms in linear algebra dictates that every automorphism of a finite-dimensional \( k \)-module \( V \) is uniquely of the form

\[
[g_1] \oplus [g_2] \oplus \cdots \oplus [g_m],
\]

where \( g_i \) divides \( g_{i+1} \) for \( 1 \leq i \leq m - 1 \). Consequently, every linear \( k \)-automorphism of \( K \in \mathbb{E}(k) \) is of the form

\[
\langle g_1 \rangle * \langle g_2 \rangle * \cdots * \langle g_m \rangle,
\]

where \( g_i \) divides \( g_{i+1} \) for \( 1 \leq i \leq m - 1 \). In view of Theorem 2.1 below, which we record for ease of reference, (1) can be further refined to take the form \( I * \langle g_m \rangle \). This, together with a yet another refinement, are recorded in Theorems 2.2 and 2.3. Note that Theorem 2.2 follows from Theorem 2.1. However, we record it for ease of reference.

**Theorem 2.1.** (See [11, Theorem 3].) Let \( f(T), g(T) \in k[T] \) be monic polynomials. If \( g(T) \) divides \( f(T) \), then \( \langle f(T) \rangle * \langle g(T) \rangle \simeq \langle f(T) \rangle * I \).

**Theorem 2.2.** (See [10, Theorem 4.6].) Let \( \alpha \) be a linear \( k \)-automorphism of a rational function field with minimal polynomial \( f(T) \). Then

\[
\alpha \simeq \langle f(T) \rangle * I.
\]

**Theorem 2.3.** (See [9, Theorem 4].) Let \( \alpha \) be a linear \( k \)-automorphism of a rational function field with minimal polynomial \( f(T) = \prod_{i=1}^{n} (f_i(T))^{n_i} \) where the \( f_i(T) \) ’s are distinct and irreducible, and the inseparability degree of \( f_i \) is \( q_i \). Then

\[
\alpha \simeq \langle \sqrt{f(T)} \rangle * \langle (T - 1)^{\mu(f)} \rangle * I,
\]

where

\[
\sqrt{f(T)} = \prod_{i=1}^{n} f_i(T) \quad \text{and} \quad \mu(f) = \max\{ (n_i - 1)q_i : 1 \leq i \leq n \}.
\]

(4)
A further and useful refinement of the above will be established in Theorem 3.6 in the next section.

One of the powerful tools that was used in proving the theorems above and that we shall frequently use in this article is the following generalization of Hilbert’s Theorem 90. This is a restatement of the cohomological facts $H^1(G, GL_n(L)) = 0$ and $H^1(G, Aff_n(L)) = 0$, and has appeared in many variations in the literature. See [3,4,13], [8, Theorem 3] and [12, Theorem 1].

Theorem 2.4. (See [12, Theorem 1].) Let $G$ be a finite group acting on the rational function field $L(x_1, \ldots, x_m)$ of $m$ variables over a field $L$. Suppose that

1. for any $\sigma \in G$, $\sigma(L) \subseteq L$,
2. the restriction of the actions of $G$ to $L$ is faithful,
3. for any $\sigma \in G$,

$$
\begin{pmatrix}
\sigma(x_1) \\
\sigma(x_2) \\
\vdots \\
\sigma(x_m)
\end{pmatrix} = A(\sigma) 
\begin{pmatrix}
x_1 \\
x_2 \\
\vdots \\
x_m
\end{pmatrix} + B(\sigma)
$$

where $A(\sigma) \in GL_m(L)$ and $B(\sigma)$ is an $m \times 1$ matrix over $L$.

Then there exist $(\alpha_{ij})_{1 \leq i, j \leq m} \in GL_m(L)$ and $\beta_j \in L$, $1 \leq j \leq m$, such that, if $z_j := \sum_{i=1}^{m} \alpha_{ij} x_i + \beta_j$, we have $L(x_1, \ldots, x_m) = L(z_1, \ldots, z_m)$ and $\sigma(z_i) = z_i$ for any $\sigma \in G$, any $1 \leq i \leq m$.

The affine automorphism $S_r = \langle (T - 1)^r, 1 \rangle$ that occurred in Theorem 2.3 will be encountered often in the sequel. For the convenience of the reader, we point out that $S_r$, a $k$-automorphism of $k(x_1, \ldots, x_r)$, can be defined by $S_r(x_i) = x_i + x_{i+1}$ for $1 \leq i < r$, and $S_r(x_r) = x_r + 1$. When $r = 0$, $S_r$ stands for $I_0$, the identity automorphism of $k$. The useful fact that when $r$ is a power of the characteristic of $k$, $(T - 1)^r = T^r - 1$ will be used freely in this article. We restate some properties of $S_r$ that are quite handy in simplifying linear automorphisms.

Lemma 2.5. (See [8, Lemma 1].) Let $d$ be a non-negative integer, and let $S_d$ denote the affine automorphism $\langle (T - 1)^d, 1 \rangle$.

1. If $\text{char}(k) = 0$ and $d \geq 1$, then $S_d \cong S_1 \ast I$.
2. If $m \geq d$, then $S_m \ast S_d \cong S_m \ast I$.
3. If $\text{char}(k) = p > 0$ and $d$ is not a power of $p$, then $S_d$ is equivalent to the linear automorphism $\langle (T - 1)^d \rangle$.
4. The linear automorphism $\langle (T - 1)^{d+1} \rangle$ is equivalent to $S_d \ast I$.

Note that [8, Lemma 1] states that (iv) holds under the assumptions that $\text{char}(k) = p > 0$ and that $d$ is a power of $p$. However, its simple proof does not use these assumptions.

We also find it convenient to introduce the following symbol.
Definition 2.6. For any non-negative integer $n$, we set

$$[n] = [n]_k := \begin{cases} \frac{p^l}{p} & \text{if } \text{char}(k) = p > 0 \text{ and } p^l \leq n < p^{l+1}, \\ 1 & \text{if } \text{char}(k) = 0 \text{ and } n \geq 1, \\ 0 & \text{if } n = 0. \end{cases}$$

Non-negative integers $q$ with $[q] = q$ will play a special role. Observe that

$$q = [q] \quad \text{if and only if} \quad q = \begin{cases} 0 \text{ or } 1 & \text{if } \text{char}(k) = 0, \\ 0 \text{ or a } p \text{-power} & \text{if } \text{char}(k) = p > 0. \end{cases} \quad (5)$$

Finally, we make the convention that all polynomials $f(T) \in k[T]$ in this paper are monic with $f(0) \neq 0$, for in the case $f(0) = 0$, $\langle f \rangle$ and $\langle f, c \rangle$ would not define automorphisms. When we write the factorization of a polynomial $f(T) \in k[T]$ in the form

$$f(T) = \prod_{i=1}^{n} (f_i(T))^{n_i},$$

we tacitly assume that the $f_i$’s are distinct and irreducible and that $n_i \geq 1$.

3. A refined description of linear automorphisms

In this section we improve on Theorem 2.3 by providing a refined description of a linear automorphism based on its minimal polynomial. This refinement is the content of Theorem 3.6 below.

Proposition 3.1. Let $S_r$ denote the affine automorphism $\langle (T - 1)^r, 1 \rangle$.

(i) For any non-negative integer $d$, $S_d \cong S_{\lfloor d \rfloor} \ast I$.
(ii) If $\text{char}(k) = p$ and $q$ is a $p$-power, then $S_d^q \cong S_1 \ast I_{q-1}$ and $S_d^{pq} = I_q$.

Proof. (i) Suppose $d > \lfloor d \rfloor$. If $\text{char}(k) = 0$, then $\lfloor d \rfloor = 1$ and our statement coincides with Lemma 2.5(i). If $\text{char}(k) = p > 0$, then $d$ is not a power of $p$; hence by Lemma 2.5(iii) and (iv), $\langle (T - 1)^d, 1 \rangle \cong \langle (T - 1)^{d-1}, 1 \rangle \ast I$. If $d - 1 = \lfloor d \rfloor$, we are done. Otherwise, we repeat as above until we reach $\lfloor d \rfloor$.

For (ii), set $\sigma := S_q$. Since $q$ is a power of $\text{char}(k)$, we have $\sigma = \langle (T^q - 1), 1 \rangle$. Hence $\sigma$ is an automorphism of $K \in E(k)$ of dimension $q$, and $K$ has a base $\{x_1, x_2 := \sigma(x_1), \ldots, x_q = \sigma^{q-1}(x_1)\}$, with $\sigma^q(x_1) = x_1 + 1$, and therefore $\sigma^q(x_i) = x_i + 1$ for $i = 1, \ldots, q$. That is, on $k(x_i), \sigma^q \cong S_1$. Therefore, on $K = k(x_1, \ldots, x_q), \sigma^q \cong S_1 \ast \cdots \ast S_1 \cong S_1 \ast I$ (by Lemma 2.5(ii)), as desired. The second assertion now follows because $S_1^p = I$. \qed

Lemma 3.2. Let $\text{char}(k) = p > 0$ and $f(T)$ be an irreducible $k$-polynomial of inseparability degree $q > 1$. If $r < q$, then $\langle f(T) \rangle \ast \langle (T - 1)^r, 1 \rangle \cong \langle f(T) \rangle \ast I_r$. 

Proof. Write $f(T) = g(T^q)$, where $g(T) \in k[T]$ is irreducible and separable, and let $n = \deg g(T)$. Let $s_1 = (f)$, $s_2 = ((T - 1)^r, 1)$, and set $s = s_1 \ast s_2$. Then $s$ is the $k$-automorphism on $K \in \mathbb{E}(k)$, where $K$ has a base $x \cup y$ of the form

$$x = \{s^j(x) : 0 \leq j \leq nq - 1\} \quad \text{and} \quad y = \{s^j(y) : 0 \leq j \leq r - 1\},$$

with $f(s)(x) = 0$ and $(s - 1)^r(y) = 1$.

Let $L$ be the splitting field of $g(T)$ over $k$, and let $\Gamma = \text{Gal}(L/k)$ be its Galois group. Let $g(T) = (T - a_1) \cdots (T - a_n)$ be the factorization of $g$ over $L$. Every $\gamma \in \Gamma$ permutes the set $\{a_1, \ldots, a_n\}$. By letting $s$ act trivially on $L$, we extend $s$ to an $L$-automorphism of $L(x \cup y)$. We also extend the action of $\Gamma$ to $L(x \cup y)$ by letting it act trivially on $x \cup y$.

For $1 \leq i \leq n$, set

$$f_i(T) = \frac{f(T)}{Tq - a_i}, \quad X_i = f_i(s)(x), \quad \text{and} \quad z_i = \frac{s(x_i)}{X_i}.$$

Then $\{s^j(X_i) : i = 1, \ldots, n; \ j = 0, \ldots, q - 1\}$ is a base of $L(x)$ over $L$ and $s^q(X_i) = a_iX_i$. Thus, the set $z = \{s^j(z_i) : i = 1, \ldots, n; \ j = 1, \ldots, q - 1\}$ consists of $L$-linearly independent elements on which $\Gamma$ acts by permutation, and where the action of $s$ on $z$ is that of a finite group (of order $q$).

Let $L_1 = L(z)$ and set $G = \{\gamma s^j : \gamma \in \Gamma, \ j = 0, \ldots, q - 1\}$. Then $G$ acts (as a finite group) faithfully on $L_1$. Also $y$ is a set of indeterminates over $L_1$ such that $G$ acts on $L_1(y)$. Thus, by Theorem 2.4, one finds a base $Y = \{Y_0, \ldots, Y_{r-1}\}$ such that $L_1(y) = L_1(Y)$, and each $Y_i$ is fixed by $G$ (i.e., $Y_i$ is fixed by $s$ and $\Gamma$). Since $\Gamma = \text{Gal}(L(x, y)/k(x, y))$, we conclude that $Y \subseteq k(x, y)$. We also have

$$k(x, y) = L(x, y)\Gamma = L_1(x, y)\Gamma = L_1(x, Y)\Gamma = L(x, Y)\Gamma = k(x, Y).$$

The action of $s$ on the $k$-base $x \cup Y$ implies that $s \equiv (f(T)) \ast I$. \hfill \Box

Corollary 3.3. Let $f(T) \in k[T]$ be of inseparability degree $q$. Let $\alpha$ be a linear automorphism with minimal polynomial $f(T)$. For $m$ with $[m] < q$,

$$\alpha \ast \langle(T - 1)^m, 1\rangle \equiv \langle f(T) \rangle \ast I.$$

Proof. By part (i) of Proposition 3.1, we may assume that $m = [m]$. If $m = 0$, there is nothing to prove. If $m > 0$, then $q > [m] \geq 1$; hence $\text{char}(k) = p > 0$. Let $f(T) = (f_1(T))^m \cdots (f_r(T))^m$ be the factorization of $f$ over $k$, where the inseparability degree of $f_i$ is $q_i$. Then $q = \text{Max}\{q_1, \ldots, q_r\}$. By Theorem 2.3, $\langle f \rangle \equiv \langle \sqrt{f} \rangle \ast \langle(T - 1)^m, 1\rangle \ast I$. From linear algebra, $\langle \sqrt{f} \rangle \equiv \langle f_1 \rangle \ast \cdots \ast \langle f_r \rangle$. Since $q = q_i$ for some $i$, by Lemma 3.2, we can use $\langle f_i \rangle$ to neglect $\langle(T - 1)^m, 1\rangle$. \hfill \Box

Definition 3.4. Let $f(T) \in k[T]$, and let $f(T) = (f_1(T))^m \cdots (f_r(T))^m$ be the factorization of $f$ over $k$, where the $f_i$'s are distinct and irreducible, and the inseparability degree of $f_i$ is $q_i$. Let $q = \text{Max}\{q_1, \ldots, q_r\}$. We define $\omega_1(f) = \omega_1(f, k)$, $\omega_2(f) = \omega_2(f, k)$ and $\omega(f) = \omega(f, k)$ as follows:
\[ \omega_1(f) = \text{Max}\{ [(n_i - 1)q_i]: 1 \leq i \leq r \}, \]
\[ \omega_2(f) = \text{Max}\{ [q_i - 1]: 1 \leq i \leq r \} = [q - 1], \]
\[ \omega(f) = \text{Max}\{ \omega_1(f), \omega_2(f) \}. \]

Note that over any algebraically closed field \( \Omega \),
\[ f(T) = \prod_{i=1}^{r} \prod_{j=1}^{r_i} (T - c_{ij})^{q_i n_j}. \]

Hence \( \omega(f, \Omega) = \text{Max}\{ [n_i q_i - 1]: 1 \leq i \leq r \} \).

When \( q_i = 1 \) for all \( i \), we have \( \omega_2(f, k) = 0 \) and \( \text{Max}\{ [n_i - 1]: 1 \leq i \leq r \} = \omega(f, k) = \omega(f, k)\). In particular when \( \text{char}(k) = p > 0 \), then \( q_i = p^{a_i} \). When \( n_i = 1 \), \( q_i - 1 = n_i q_i - 1 \) and \( q_i(n_i - 1) = 0 \). When \( n_i > 1 \), let \( p^{b_i} < n_i < p^{b_i+1} \). Clearly, \( q_i < p^{a_i+b_i} \), \( (n_i - 1)q_i < n_i q_i - 1 < p^{a_i+b_i}+1 \) and \( q_i - 1 < [n_i - 1]q_i = [n_i q_i - 1] \). Therefore, \( \omega(f, k) = \text{Max}\{ \omega_1(f), \omega_2(f) \} = \text{Max}\{ [n_i q_i - 1]: 1 \leq i \leq r \} = \omega(f, \Omega) \).

Since any two fields over which \( f \) is defined can be embedded in an algebraically closed field, the above paragraph implies the following.

**Proposition 3.5.** \( \omega(f, k) = \text{Max}\{ [n_i q_i - 1]: 1 \leq i \leq r \} \) and does not depend on the ground field.

The following is a more refined version of Theorem 2.3. Note that the radical \( \sqrt{f} \), as defined in Eq. (4), depends on the ground field \( k \).

**Theorem 3.6.** Let \( k \) be a field and let \( f(T) \in k[T] \) of inseparability degree \( q \). Let \( \alpha \) be a linear automorphism with minimal polynomial \( f(T) \).

(i) \( \alpha \cong (\sqrt{f(T)}) \ast ((T - 1)^{\omega_1(f,k)}, 1) \ast I \).

(ii) If \( \omega_1(f) \leq \omega_2(f) \), then \( \alpha \cong (\sqrt{f(T)}) \ast I \).

(iii) If \( k \) is algebraically closed, then \( \alpha \cong (\sqrt{f(T)}) \ast ((T - 1)^{\omega(f)}, 1) \).

**Proof.** Let \( f(T) = (f_1(T))^{n_1} \cdots (f_r(T))^{n_r} \) be the factorization of \( f \) over \( k \), where the \( f_i \)'s are distinct and irreducible. Suppose that the inseparability degree of \( f_i \) is \( q_i \). Then \( q = \text{Max}\{q_1, \ldots, q_r\} \) is the inseparability degree of \( f \). Let \( \mu(f) = \text{Max}\{(n_i - 1)q_i: 1 \leq i \leq r\} \). By definition, \( \omega_1(f) = [\mu(f)] \). Using Theorem 2.3 and Proposition 3.1 we have,
\[\alpha \cong (\sqrt{f}) \ast ((T - 1)^{\mu(f)}, 1) \ast I \cong (\sqrt{f}) \ast ((T - 1)^{\omega_1(f)}, 1) \ast I.\]

This proves part (i).

Now suppose that \( \omega_1(f) \leq \omega_2(f) \). Since \( \omega_2(f) = [q - 1] < q \) and \( q \) is the inseparability of \( \sqrt{f} \), it follows by Corollary 3.3 that \( (\sqrt{f}) \ast ((T - 1)^{\omega_1(f)}, 1) \cong (\sqrt{f}) \ast I \). So (ii) follows.

Finally, when \( k \) is algebraically closed, \( q_i = 1 \) for all \( i \), and therefore \( \omega_1 = \omega \). Hence, (iii) follows from (i). \( \square \)
4. Inseparability of linear automorphisms

In this section, we establish a part of our main theorem 6.5. In the previous section we have defined the function $\omega(f)$ for a polynomial $f(T) \in k[T]$. In this section (Corollary 4.4), we will show that if two polynomials $f$ and $g$ are minimal polynomials of a linear automorphism $\alpha$, then $\omega(f)$ and $\omega(g)$ must be equal. We will refer to common value as the inseparability degree of $\alpha$, and will write it as $\omega(\alpha)$.

Lemma 4.1. Let $\sigma$ be the $k$-automorphism of $K \in \mathbb{E}(k)$ defined by

$$\sigma = (T - a_1) \cdots (T - a_n),$$

where $a_1, \ldots, a_n \in k^*$. Then $K$ does not contain any element $z$ such that $\sigma(z) = z + 1$.

Proof. $K$ has base $x = \{x_i: 1 \leq i \leq n\}$ such that $\sigma(x_i) = a_ix_i$. Let $z \in K = k(x)$ be such that $\sigma(z) = z + 1$. We will reach a contradiction.

Write $z$ as $z = f/g$, where $f$ and $g$ are relatively prime elements in the polynomial ring $k[x]$. From $\sigma(f/g) = 1 + f/g$, it follows that $g\sigma(f) = (f + g)\sigma(g)$. Since $\sigma$ acts as a $k$-automorphism on $k[x]$, and since $g$ and $f + g$ are relatively prime, it follows that $g$ divides $\sigma(g)$. Since $\sigma$ preserves degrees, we have $\sigma(g) = cg$ for some $c \in k^*$. Therefore we also have $\sigma(f) = c(f + g)$. Hence

$$g = c^{-1}(\sigma(f) - cf).$$

Write $f$ as $f = \sum b_M M$, where $M$ runs over a finite set $S$ of monomials in the $x_i$’s, and where the $b_M$’s are non-zero. Clearly $\sigma(M)/M \in k^*$ for all such monomials, say $\sigma(M)/M = c_M$. From Eq. (6), it follows that $g = \sum b_M c^{-1}(c_M - c)M$. From $\sigma(g) = cg$, it follows that

$$\sum b_M c^{-1}(c_M - c)c_MM = \sum b_M (c_M - c)M.$$ 

Therefore $c_M = c$ for all $M \in S$, resulting in the contradiction $g = 0$. □

Corollary 4.2. Let $\sigma$ be the $k$-automorphism of $K \in \mathbb{E}(k)$ defined by

$$\sigma = (T - a_1) \cdots (T - a_n) \ast \{(T - 1)^Q, 1\}$$

where $a_1, \ldots, a_n \in k^*$, and let $q = |q| \geq 1$. Then there exists $z \in K$ such that $\sigma^q(z) = z + 1$ if and only if $q \leq |Q|$.

Proof. By Proposition 3.1(i), we may assume that $[Q] = Q$. Suppose that $q \leq Q$. If char($k$) = 0, then $q = Q = 1$, and there is nothing to prove. So let char($k$) = $p > 0$. Then $q$ and $Q$ are powers of $p$. By Proposition 3.1(ii), $\sigma^Q \cong (T - a_1^Q) \ast \cdots \ast (T - a_n^Q) \ast ((T - 1), 1)$, hence $(\sigma - 1)^Q(x) = 1$ for some $x \in K$. Let $z = (\sigma - 1)^Q(x)$. Then $(\sigma - 1)^Q(z) = (\sigma - 1)^Q(x) = 1$; hence $\sigma^q(z) = z + 1$, as desired.

Conversely, let $q > Q = |Q|$. We shall prove that there does not exist $z \in K$ such that $\sigma^q(z) = z + 1$. If $Q = 0$, then we are done by the previous lemma. Otherwise, $q = |q| > Q = |Q| \geq 1$. In particular, char($k$) = $p > 0$. By Proposition 3.1(ii), $\sigma^q \cong (T - a_1^Q) \ast \cdots \ast (T - a_n^Q) \ast I$. By
the previous lemma, there does not exist \( z \in K \) such that \( \sigma^q(z) = z + 1 \). This completes the proof. \( \square \)

**Theorem 4.3.** Let \( \alpha \) be a linear \( k \)-automorphism of \( K \in \mathbb{E}(k) \), with a minimal polynomial \( f(T) \in k[T] \). Let \( m \) be a non-negative integer. Then

\[
\alpha \ast \langle (T - 1)^m, 1 \rangle \cong \alpha \ast I \quad \text{if and only if} \quad \lfloor m \rfloor \leq \omega(f).
\]

**Proof.** Let \( S_r \) denote \( \langle (T - 1)^r, 1 \rangle \). By Proposition 3.1(i), we may assume that \( \lfloor m \rfloor = m \). For the “if part,” suppose first that \( \lfloor m \rfloor \leq \omega_2(f) \). Then \( \lfloor m \rfloor \) is less than the inseparability degree of \( f \), and we are done by Corollary 3.3. Now suppose that \( m = \lfloor m \rfloor \leq \omega_1(f) \). By Lemma 2.5(ii), \( S_{\omega_1(f)} \ast S_m \cong S_{\omega_1(f)} \ast I \). Hence, by Theorem 3.6(i), we get

\[
\alpha \ast S_m \cong \langle \sqrt{f(T)} \rangle \ast S_{\omega_1(f)} \ast S_m \ast I \cong \langle \sqrt{f(T)} \rangle \ast S_{\omega_1(f)} \ast I \cong \alpha \ast I.
\]

This concludes the “if part” of the assertion.

Conversely, let \( \sigma_1 = \alpha \ast S_m \) and \( \sigma_2 = \alpha \ast I \). Let \( \bar{k} \) be the algebraic closure of \( k \). Over \( \bar{k} \), \( \sqrt{f(T)} \) is a product of distinct linear factors. Hence it follows by Theorem 3.6(iii) that \( \alpha \cong \bar{k} \langle T - c_1 \rangle \ast \cdots \ast \langle T - c_n \rangle \ast S_{\omega(f)} \ast I \), and therefore, by Lemma 2.5(ii), \( \sigma_1 \cong \bar{k} \langle T - c_1 \rangle \ast \cdots \ast \langle T - c_n \rangle \ast S_{\omega(f)} \ast I \), where \( Q = \text{Max}[\lfloor m \rfloor, \omega(f)] \). In particular, by Corollary 4.2, we can find an element \( z \) in the underlying field such that \( \sigma_1^Q(z) = z + 1 \). Now if, \( \sigma_1 \cong \sigma_2 \), then (over \( \bar{k} \)) we can find an element \( z' \) in the underlying field such that \( \sigma_2^Q(z') = z' + 1 \). Since \( \sigma_2 = \alpha \ast I \cong \bar{k} \langle T - c_1 \rangle \ast \cdots \ast \langle T - c_n \rangle \ast S_{\omega(f)} \ast I \), it follows by Corollary 4.2 that \( \text{Max}[\lfloor m \rfloor, \omega(f)] = Q \leq \omega(f) \). \( \square \)

In light of the previous theorem, it follows that \( \omega(f) \) is completely determined by the automorphism \( \alpha \). We record this.

**Corollary 4.4.** Let \( f(T) \) and \( g(T) \in k[T] \) be two minimal polynomials of a linear \( k \)-automorphism \( \alpha \). Then \( \omega(f) = \omega(g) \).

**Definition 4.5 (The Inseparability Degree of \( \alpha \)).** For any \( k \)-linear automorphism \( \alpha \) of a rational function field, we define the inseparability degree of \( \alpha \), written \( \omega(\alpha) \), to be \( \omega(f) \) for any minimal polynomial \( f \) of \( \alpha \). The well definition of \( \omega(\alpha) \) is guaranteed by the previous corollary.

**5. The group \( R(\alpha) \)**

For the remainder of the paper, for \( h(T) \in k[T] \), we let \( R(h) \) denote the multiplicative group generated by the roots of \( h \) (in some fixed algebraic closure of \( k \)).

In this section we will prove the following theorem, which establishes necessary conditions for relative negligibility.

**Theorem 5.1.** Let \( \alpha_1 \) and \( \alpha_2 \), respectively, be linear \( k \)-automorphisms of \( K_1 \) and \( K_2 \in \mathbb{E}(k) \) with minimal polynomials \( f \) and \( g \), respectively. Suppose that \( \alpha_1 \ast \alpha_2 \cong \alpha_1 \ast I \). Then \( R(g) \subseteq R(f) \) and \( \omega(g) \leq \omega(f) \).
Lemma 5.2. Let \( \sigma \) be the \( k \)-automorphism of \( K \in \mathbb{E}(k) \) defined by

\[
\sigma = \langle T - a_1 \rangle \ast \cdots \ast \langle T - a_n \rangle \ast \langle (T - 1)^Q, 1 \rangle,
\]

where \( a_1, \ldots, a_n \in k^* \), and let \( A = \langle a_1, \ldots, a_n \rangle \) be the multiplicative subgroup of \( \bar{k}^* \) generated by \( a_1, \ldots, a_n \). Let \( c \in k^* \). Then there exists \( z \in K \) such that \( \sigma(z) = cz \) if and only if \( c \in A \).

Proof. It is clear that there exist \( x_1, \ldots, x_n \in K \) such that \( \sigma(x_i) = a_i x_i \). If \( c \in A \), then \( c \) is of the form \( a_1^{e_1} \cdots a_n^{e_n} \), where \( e_j \in \mathbb{Z} \). Letting \( z = x_1^{e_1} \cdots x_n^{e_n} \), it is easily seen that \( \sigma(z) = cz \).

Conversely, suppose that there exists \( z \in K \) such that \( \sigma(z) = cz \). We shall show that \( c \in A \).

By Proposition 3.1(i), we may assume that \( |Q| = Q \). We start with the case \( Q = 0 \). In this case, \( K \) has a base \( \mathbf{x} = \{x_1, \ldots, x_n\} \) with \( \sigma(x_i) = a_i x_i \).

Let \( f \in k[\mathbf{x}] \) be such that \( \sigma(f)/f = c \in k^* \). Then \( f \) is of the form \( f = \sum b_M M \), where \( M \) runs over a finite set \( S \) of monomials in the \( x_i \)'s. Clearly, \( c_M := \sigma(M)/M \in A \). From \( \sigma(f) = cf \), it follows that \( c_M = c \) for all \( M \in S \), and therefore \( c \in A \), as desired.

Next, let \( h \in k(\mathbf{x}) \) be such that \( \sigma(h)/h \in k^* \), and write \( h = f/g \), where \( f \) and \( g \) are relatively prime elements of \( k[\mathbf{x}] \). Since \( \sigma \) restricts to a \( k \)-automorphism of \( k[\mathbf{x}] \), it follows that \( \sigma(f) \) and \( \sigma(g) \) are relatively prime elements in \( k[\mathbf{x}] \). Then it follows from \( \sigma(f/g) = c(f/g) \) that \( \sigma(g) = dg \) and \( \sigma(f) = cdg \), where \( d \in k^* \), because \( \sigma \) preserves degrees. Thus \( \sigma(f)/f \) and \( \sigma(g)/g \) belong to \( k^* \) and hence to \( A \), from the previous paragraph. Hence \( c \in A \). This completes the proof of the case \( Q = 0 \).

Next we consider the case \( Q = 1 \) and \( \text{char}(k) = 0 \). In this case, \( K \) has a base \( \mathbf{x} \cup \{y\} \) where \( \mathbf{x} = \{x_1, \ldots, x_n\} \) and where \( \sigma(x_i) = a_i x_i \) and \( \sigma(y) = y + 1 \). Note that \( \sigma \) acts as a \( k \)-automorphism on each of the polynomial rings \( k[y], k[\mathbf{x}] \) and \( k[y, \mathbf{x}] \).

If \( f \in k[\mathbf{x}] \) is such that \( \sigma(f)/f = c \in k^* \), then it follows as in the proof of the case \( Q = 0 \) that \( c \in A \).

If \( f \in k[y] \) is such that \( \sigma(f)/f = c \in k^* \), then \( f(y + 1) = cf(y) \). Thus if \( f \) has a zero \( r \) (in \( \bar{k} \)), then \( r + 1 \) would be a zero of \( f \) for all \( t \in \mathbb{Z} \), and we would obtain the contradiction that \( f \) has infinitely many zeros. Thus the only elements \( f \) in \( k[y] \) with \( \sigma(f)/f \in k^* \) are the constants \( k^* \).

If \( f \in k[y, \mathbf{x}] \) is such that \( \sigma(f)/f = c \in k^* \), then \( f \) can be written uniquely in the form \( \sum f_M M \), where \( f_M \in k[y] \) and where \( M \) runs over a finite set \( S \) of monomials in the \( x_i \)'s. From \( \sigma(f) = cf \) and from the uniqueness of representation, it follows that \( cf_M = c_M \sigma(f_M) \) for all \( M \in S \). From the previous paragraph, it follows that \( f_M \in k^* \) and that \( c_M = c \) for all \( M \in S \). Since \( c_M \in A \) for all \( M \in S \), it follows that \( c \in A \).

Finally, if \( h \in k(y, \mathbf{x}) \) is such that \( \sigma(h)/h = c \in k^* \), then by writing \( h = f/g \) where \( f, g \in k[y, \mathbf{x}] \) are relatively prime and arguing as before, we conclude that \( \sigma(f)/f \) and \( \sigma(g)/g \) (and hence \( \sigma(h)/h \)) are in \( A \), as desired. This completes the proof of the case \( Q = 1 \) and \( \text{char}(k) = 0 \).

It remains to deal with the case \( \text{char}(k) = p > 0 \) and \( Q \) is a power of \( p \). In this case, let \( r > Q \) be another power of \( p \). Then \( \sigma^r = \langle T - a_1^r \rangle \ast \cdots \ast \langle T - a_n^r \rangle \ast I \), and \( \sigma^r(f) = c^r f \). Applying the case \( Q = 0 \) to \( \sigma^r \), we conclude that \( c^r \in \langle a_1^r, \ldots, a_n^r \rangle \). Since \( r \) is power of \( p \), this is equivalent to saying that \( c \in \langle a_1, \ldots, a_n \rangle = A \), as desired. \( \square \)

Corollary 5.3. Let \( \alpha_1 \) and \( \alpha_2 \), respectively, be linear \( k \)-automorphisms of \( K_1 \) and \( K_2 \in \mathbb{E}(k) \) with minimal polynomials \( f(T) \) and \( g(T) \), respectively. If \( \alpha_1 \ast I \cong \alpha_2 \ast I \), then \( R(g) = R(f) \) and \( \omega(f) = \omega(g) \).
Proof. If $\alpha_1 \cong \alpha_2$ over $k$, then it is so over any extension of $k$. Thus we may assume that $k$ is algebraically closed and therefore each of $\sqrt{f}$ and $\sqrt{g}$ is a product of distinct linear factors. By Theorem 3.6(iii), we have

$$\alpha_1 = (T - a_1) \cdots (T - a_N) \ast \{(T - 1)^\omega(f), 1\}, \quad \text{and}$$

$$\alpha_2 = (T - b_1) \cdots (T - b_n) \ast \{(T - 1)^\omega(g), 1\},$$

with $R(f) = \langle a_1, \ldots, a_N \rangle$ and $R(g) = \langle b_1, \ldots, b_n \rangle$. Thus, $K_1$ contains elements $z_i$ with $\sigma_1(z_i) = a_i z_i$. If $\alpha_1 \cong \alpha_2$, then $K_2$ contains elements $Z_i$ with $\sigma_2(Z_i) = a_i Z_i$. By Lemma 5.2, $a_i \in \langle b_1, \ldots, b_n \rangle = R(g)$; hence $R(f) \subseteq R(g)$. By symmetry, we conclude $R(f) = R(g)$. The equality of $\omega$’s follows by Corollary 4.4. \hfill \Box

Definition 5.4 (The group $R(\alpha)$). For any $k$-linear automorphism $\alpha$ of $K \in \mathbb{E}(k)$, the group $R(\alpha)$ is defined to be $R(f)$ for any minimal polynomial $f$ of $\alpha$. This is well defined by the previous corollary.

Proof of Theorem 5.1. Let $\sigma_1 = \alpha_1 \ast \alpha_2$ and $\sigma_2 = \alpha_1 \ast I$. These are automorphisms of $K = K_1 \ast K_2 \in \mathbb{E}(k)$. If $\sigma_1 \cong \sigma_2$ over $k$, then so is the case over any extension of $k$. Thus we may assume that $k$ is algebraically closed. Over such a field, each of $\sqrt{f}$ and $\sqrt{g}$ is a product of distinct linear factors. Let $\beta_1 = \langle \sqrt{f} \rangle$ and $\beta_2 = \langle \sqrt{g} \rangle$. Then

$$\beta_1 = (T - a_1) \cdots (T - a_N), \quad \text{and}$$

$$\beta_2 = (T - b_1) \cdots (T - b_n),$$

with $R(f) = \langle a_1, \ldots, a_N \rangle$ and $R(g) = \langle b_1, \ldots, b_n \rangle$. Thus, by Theorem 3.6(iii) (and Lemma 2.5(ii)),

$$\sigma_2 \cong \beta_1 \ast \{(T - 1)^\omega(f), 1\} \ast I, \quad \text{and}$$

$$\sigma_1 \cong \beta_1 \ast \beta_2 \ast \{(T - 1)^Q, 1\} \ast I, \quad \text{with } Q := \text{Max}\{\omega(f), \omega(g)\}.$$

In particular, $K$ contains elements $z_i$ with $\sigma_1(z_i) = b_i z_i$. If $\sigma_1 \cong \sigma_2$, then $K$ contains elements $Z_i$ with $\sigma_2(Z_i) = b_i Z_i$. Since $\sigma_2 \cong \{(T - a_1) \cdots (T - a_N) \ast \{(T - 1)^\omega(f), 1\} \ast I, \text{Lemma 5.2 implies that } b_i \in \langle a_1, \ldots, a_N \rangle = R(f)$, hence $R(g) \subseteq R(f)$.

Also, it is clear that $K$ contains an element $z$ with $\sigma_1^Q(z) = z + 1$; hence $\sigma_1 \cong \sigma_2$ implies that $K$ contains an element $Z$ with $\sigma_2^Q(Z) = Z + 1$. By Corollary 4.2, we have $Q \leq \omega(f)$. Since $Q = \text{Max}\{\omega(f), \omega(g)\}$, we have $\omega(g) \leq \omega(f)$, as desired. \hfill \Box

6. Negligibility and the generalized order

In this section we establish our main theorem (Theorem 6.5) on negligibility by showing that the converse of Theorem 5.1 holds. We start with a simple fact from Galois theory. Its proof is included for the sake of completeness.

Proposition 6.1. Let $f(T)$ and $F(T)$ be polynomials in $k[T]$ of inseparability degrees $q$ and $Q$, respectively. If $R(f) \subseteq R(F)$, then $q \leq Q$. 
Proof. Let \( \Omega \) be the splitting field of \( F(T) \) over \( k \) and let \( L \) be the separable closure of \( k \) in \( \Omega \). Then \( Q \) is the smallest positive integer for which \( \Omega^Q \subseteq L \). Now let \( \Omega_1 \) be the splitting field of \( f \) over \( k \) and let \( L_1 \) be the separable closure of \( L_1 \) in \( \Omega_1 \). Since \( R(f) \subseteq R(F) \), it follows that \( \Omega_1 \subseteq \Omega \), and \( L_1 = L \cap \Omega_1 \). In particular, \( \Omega^Q_1 \subseteq \Omega^Q \subseteq L \), and hence \( \Omega^Q_1 \subseteq L \cap \Omega_1 = L_1 \). But \( q \) is the smallest positive integer that satisfies \( \Omega^q \subseteq L_1 \), hence \( q \leq Q \), as desired. \( \square \)

Recall that \( \alpha_2 \) is said to be negligible with respect to \( \alpha_1 \) if \( \alpha_1 * \alpha_2 \cong \alpha_1 * I \).

Lemma 6.2. Let \( f(T), g(T) \in k[T] \) be square-free. If \( R(g) \) is a subgroup of \( R(f) \), then \( \langle g \rangle \) is negligible with respect to \( \langle f \rangle \).

Proof. We may assume that \( g \) is irreducible. In fact, if the lemma is true under this assumption, and if \( g = g_1 \cdots g_r \) is the factorization of \( g \) into distinct irreducible polynomials, then noting that \( R(g_i) \subseteq R(g) \) and that \( \langle g \rangle \cong \langle g_1 \rangle * \cdots * \langle g_r \rangle \), one applies the lemma to each \( \langle g_i \rangle \) to get the desired result.

We may also assume that no proper factor \( f_1 \) of \( f \) has the property that \( R(g) \subseteq R(f_1) \). Otherwise, noting that \( \langle f \rangle \cong \langle f_1 \rangle * \langle f/f_1 \rangle \), one applies the lemma to \( f_1 \).

Let \( Q \) and \( q \) be the inseparability degrees of \( f \) and \( g \), respectively. By the previous proposition, \( q \leq Q \). Let \( s_1 = \langle f \rangle \) and \( s_2 = \langle g \rangle \). Then \( s_1 \) and \( s_2 \) are, respectively, \( k \)-automorphisms of \( K_1 \) and \( K_2 \in \mathbb{E}(k) \) such that there exist \( X_0 \in K_1 \) and \( Y_0 \in K_2 \) with \( f(s_1)(X_0) = 0 = g(s_2)(Y_0) \) and so that the sets

\[
X = \{s_1^j(X_0) : j = 0, \ldots, \deg(f) - 1\} \quad \text{and} \quad Y = \{s_2^j(Y_0) : j = 0, \ldots, \deg(g) - 1\}
\]

are bases of \( K_1/k \) and \( K_2/k \), respectively. Let \( \sigma = s_1 * s_2 \) and \( K = K_1 * K_2 = k(X \cup Y) \).

Let \( \Omega \) be the splitting field of \( f \) over \( k \). Let \( L \) be the maximal Galois extension in \( \Omega/k \), and let \( \Gamma = \text{Gal}(L/k) \) be the Galois group of \( L/k \). Since any separable polynomial whose roots are in \( \Omega \) must also split over \( L \), it follows that

\[
f(T) = \prod_{i=1}^{n}(T^{q_i} - a_i) \quad \text{and} \quad g(T) = \prod_{i=1}^{m}(T - b_i)^{q}
\]

\((a_i, b_j \in L)\) where \( q_1, \ldots, q_n \) are the inseparability degrees of the irreducible factors (over \( k \)) of \( f \) (hence \( Q = \text{Max}(q_1, \ldots, q_n) \)). The roots of \( f \) (respectively, \( g \)) in \( \Omega \) are \( \{\alpha_1, \ldots, \alpha_n\} \) (respectively, \( \{\beta_1, \ldots, \beta_m\} \) where

\[
a_i = \alpha_i^{q_i} \quad \text{and} \quad b_j = \beta_j^q. \quad (7)
\]

Note that \( \Gamma \) permutes the elements of the sets \( A := \{a_1, \ldots, a_n\} \) and \( B := \{b_1, \ldots, b_m\} \), with \( \Gamma \) acting transitively on \( B \) since \( g \) is irreducible over \( k \). So \( \gamma \in \Gamma \) induces permutations \( \gamma_1 \) and \( \gamma_2 \) on \( \{1, \ldots, n\} \) and \( \{1, \ldots, m\} \), respectively, defined by

\[
\gamma_1(i) = j \quad \text{if and only if} \quad \gamma(a_i) = a_j, \quad \text{and} \quad \gamma_2(i) = j \quad \text{if and only if} \quad \gamma(b_i) = b_j.
\]
For any $\gamma \in \Gamma$, $a_i$ and $\gamma(a_i)$ are roots of the same irreducible factor (over $k$) of $f$, and therefore

$$q_{\gamma(i)} = q_i.$$  \hfill (8)

By letting $\sigma$ act trivially on $L$, we extend $\sigma$ to an $L$-automorphism of $L(X \cup Y)$. We also let $\Gamma$ act on $L(X \cup Y)$ by fixing every element of $X \cup Y$. For $i = 1, \ldots, n$ and $j = 1, \ldots, m$, let $f_i(T) = f(T)/(T^{q_i} - a_i)$ and $g_j(T) = g(T)/(T^{q_j} - b_j)$, and set $x_i = f_i(s_1)(X_0)$ and $y_j = g_j(s_1)(Y_0)$. Let $x = \{\sigma^j(x_i): i = 1, \ldots, n; j = 0, \ldots, q_i - 1\}$, and $y = \{\sigma^j(y_i): i = 1, \ldots, m; j = 1, \ldots, q - 1\}$. Then $x \cup y$ is a base $L(X \cup Y)$, $L(X) = L(x)$, and $L(Y) = L(y)$. Note that

$$\sigma^{q_i}(x_i) = a_ix_i \quad \text{and} \quad \sigma^{q_j}(y_i) = b_jy_i,$$

and, for any $\gamma \in \Gamma$,

$$\gamma(x_i) = x_{\gamma(i)} \quad \text{and} \quad \gamma(y_i) = y_{\gamma^2(i)}.$$

Let

$$d = Q/q \quad \text{and} \quad d_i = Q/q_i.$$  \hfill (10)

Since, by hypothesis, $\beta_t \in \langle \alpha_1, \ldots, \alpha_n \rangle$, we have

$$b^d_t = \beta^{q^d}_t = \beta^{q^d}_t \in \langle \alpha^Q_1, \ldots, \alpha^Q_n \rangle = \langle (\alpha^{q^d}_1)^{d_1}, \ldots, (\alpha^{q^d}_n)^{d_n} \rangle = \langle a_1^{d_1}, \ldots, a_n^{d_n} \rangle.$$  

Therefore, we can fix $e = (e_1, \ldots, e_n) \in \mathbb{Z}^n$ such that $b^d_t = \prod_{i=1}^n a_i^{d_i e_i}$. Observe that $e_i \neq 0$ for some $i$ with $q_i = Q$. Otherwise, $\beta_1$ (hence all the other zeros of $g$ since $g$ is irreducible) would belong to $R(f/h)$, where $h$ is the product of factors of $f$ having inseparability degree $Q$, contradicting the assumption made in the second paragraph of the proof. After re-indexing the $a_i$’s (if needed) we may assume that

$$e_1 \neq 0 \quad \text{and} \quad Q = q_1 \geq q_2 \geq \cdots \geq q_n.$$  \hfill (11)

Let $\xi_i = \{\sigma^{i^{-1}}(x_{\gamma(i)}): \gamma \in \Gamma\}, i = 1, \ldots, Q$. Note that the $\xi_i$’s are disjoint subsets of $x$, hence their elements are algebraically independent over $L$.

For $\gamma \in \Gamma$, let $\delta = \gamma^{-1}$, and define $\gamma(e) := (e_{\delta_1(1)}, \ldots, e_{\delta_1(n)})$. Set $\Lambda = \Lambda(e) := \{\gamma(e): \gamma \in \Gamma\}$. Note that

$$\prod_{i=1}^n (a_i^{d_i})^{e_{\gamma(i)}} = ((a_{\gamma_1(1)})^{d_1})^{e_1} \cdots ((a_{\gamma_1(n)})^{d_n})^{e_n}$$

$$= (a_1^{d_1})^{e_1} \cdots (a_n^{d_n})^{e_n}$$

since, by (8), $d_{\gamma_1(i)} = d_i$.

$$= \gamma(a_1^{d_1} \cdots a_n^{d_n})$$

$$= \gamma(b^d_t) = b^d_{\gamma(t)}.$$  \hfill (12)
Now define the sets $R_t$, $t = 1, \ldots, m$, as

$$R_t = \left\{ (\epsilon_1, \ldots, \epsilon_n) \in \Lambda : \prod_{i=1}^{n} a_i^{d_i \epsilon_i} = b_t^d \right\}.$$  \hfill (13)

By Eq. (12), $\gamma(e) \in R_{\gamma(1)}$, and since the action of $\Gamma$ on $B$ is transitive, $R_t$ is non-empty for all $t = 1, \ldots, m$. It can be readily verified that if $\gamma \in \Gamma$ and if $\delta = \gamma^{-1}$, then

$$(\epsilon_1, \ldots, \epsilon_n) \in R_t \quad \text{if and only if} \quad (\epsilon_{\delta(1)}, \ldots, \epsilon_{\delta(n)}) \in R_{\gamma(1)}.$$  \hfill (14)

Now let

$$M_t = \left\{ \prod_{i=1}^{n} x_i^{\epsilon_i} : (\epsilon_1, \ldots, \epsilon_n) \in R_t \right\} \quad \text{and} \quad z_t = \sum_{M \in M_t} M.$$  \hfill (15)

(Here we note the similarity of our construction to that in [5, Lemma 1].) It follows from (9) and (10) that $\sigma^Q(x_i) = a_i^{d_i} x_i$, and it follows from (13) that $\sigma^Q(M) = b_t^d M$ for all $M \in M_t$. Hence $\sigma^Q(z_t) = b_t^d z_t$. In other words, $z_t$ is annihilated by $\sigma^Q - b_t^d$. Since the $z_t$’s are sums of distinct monomials in the indeterminates in $x$, the set $\{z_1, \ldots, z_m\}$ is linearly independent over $L$. Therefore, $\{\sigma^j(z_1), \ldots, \sigma^j(z_m)\}$ is linearly independent for any $j$. By (11) and (14), each monomial $M \in M_t$ contains a factor from the indeterminates in $\xi$, and therefore, for $j = 1, \ldots, Q$, $\sigma^{j-1}(M)$ contains a factor from the indeterminates in $\xi_j$. Therefore we conclude that for a fixed $t$, $\{z_t, \sigma(z_t), \ldots, \sigma^{Q-1}(z_t)\}$ consists of algebraically independent elements. In particular, for any $H(T) \subseteq L[T]$ of degree less than $Q$, $H(\sigma)(z_t) \neq 0$, thus showing that $\sigma^Q - b_t^d$ is the minimal polynomial that annihilates $z_t$.

From $Q = qd$, it follows that $\sigma^Q - b_t^d = (\sigma^q - b_t)^d$. Let $Z_t = (\sigma^q - b_t)^{d-1}(z_t)$. Then $Z_t \neq 0$ and $(\sigma^q - b_t)(Z_t) = 0$, i.e., $\sigma^q(Z_t) = b_t Z_t$. Also, it follows from (14) that $M \in M_t$ if and only if $\gamma(M) \in M_{\gamma(1)}$. Therefore, $\gamma(z_t) = z_{\gamma(1)}$ and $\gamma(Z_t) = Z_{\gamma(1)}$ for all $\gamma \in \Gamma$. Thus the actions of $\sigma$ and $\Gamma$ on $\mathbf{z} = \{\sigma^j(Z_j) : j = 1, \ldots, m, i = 0, \ldots, q - 1\}$ and on $\mathbf{y}$ are identical.

Let $w_t = y_t / Z_t$, and let

$$\mathbf{w} = \{\sigma^j(w_j) : j = 1, \ldots, m, i = 0, \ldots, q - 1\}.$$  

Then $L(\mathbf{x} \cup \mathbf{y}) = L(\mathbf{x} \cup \mathbf{w})$ and the action of $\sigma$ on $L(\mathbf{w})$ is nothing but $(T^q - 1)$. Also, $\Gamma$ acts on $\mathbf{w}$ by permutation. By Theorem 2.4, we can find a base $\mathbf{W}$ of $L(\mathbf{w})$ consisting of $\Gamma$-fixed elements on which the action of $\sigma$ is $(T^q - 1)$. From $L(\mathbf{x}, \mathbf{y}) = L(\mathbf{x}, \mathbf{W})$, it follows by Galois descent that $k(\mathbf{x}, \mathbf{y}) = k(\mathbf{x}, \mathbf{W})$ and therefore $\langle f \rangle \ast \langle g \rangle \cong \langle f \rangle \ast \langle T^q - 1 \rangle$. By (iv) of Lemma 2.5, $\langle T^q - 1 \rangle \cong \langle (T - 1)^q, 1 \rangle \ast I$, and since the inseparability degree of $f$ is $Q \geq q$, it follows from Theorem 3.2 that $\langle f \rangle \ast \langle g \rangle \cong \langle f \rangle \ast I$, as desired. \hfill \Box

**Theorem 6.3.** Let $\alpha$ and $\beta$ be $k$-linear automorphisms of $K_1$ and $K_2 \subseteq E(k)$, respectively with $R(\beta) \subseteq R(\alpha)$ and $\omega(\beta) \leq \omega(\alpha)$. Then $\beta$ is negligible with respect to $\alpha$. 


Proof. Let \( f(T) \) and \( g(T) \in k[T] \) be minimal polynomials of \( \alpha \) and \( \beta \), respectively. Then by Definitions 4.5 and 5.4, \( R(g) = R(\beta) \subseteq R(\alpha) = R(f) \) and \( \omega(g) = \omega(\beta) \leq \omega(\alpha) = \omega(f) \). By Theorem 3.6(i),

\[ \alpha \cong \langle \sqrt{f} \rangle \star (T - 1)^{\omega_1(f)}, 1, \quad \text{and} \quad \beta \cong \langle \sqrt{g} \rangle \star (T - 1)^{\omega_1(g)}, 1. \]

Since \( \sqrt{f} \) and \( \sqrt{g} \) are square-free and since \( R(\sqrt{g}) = R(g) \subseteq R(f) = R(\sqrt{f}) \), it follows from Lemma 6.2 that \( \langle \sqrt{g} \rangle \) is negligible with respect to \( \langle \sqrt{f} \rangle \). Since \( \omega(g) \leq \omega(f) \), it follows that (i) \( \omega_1(g) \leq \omega_1(f) \) or \( \omega_1(g) \leq \omega_2(f) \). In the first case, \( \langle (T - 1)^{\omega_1(g)}, 1 \rangle \) is negligible with respect to \( \langle (T - 1)^{\omega_1(f)}, 1 \rangle \), by Theorem 2.5(ii). In the second case, \( \langle (T - 1)^{\omega_2(g)}, 1 \rangle \) is negligible with respect to \( \langle \sqrt{f} \rangle \), by Corollary 3.3. This completes the proof. \( \square \)

In view of Theorems 5.1 and 6.3, it is tempting to define the generalized order and divisibility among generalized orders as follows.

Definition 6.4. Let \( \alpha \) and \( \beta \) be \( k \)-linear automorphisms of rational function fields.

(1) The generalized order of \( \alpha \) is defined as \( \text{Ord}(\alpha) = (R(\alpha), \omega(\alpha)) \).
(2) We will say that \( \text{Ord}(\beta) \) divides \( \text{Ord}(\alpha) \) if and only if \( R(\beta) \subseteq R(\alpha) \) and \( \omega(\beta) \leq \omega(\alpha) \).

The combination of Theorems 5.1 and 6.3 gives an answer for Question 1 of the introduction as follows.

Theorem 6.5. Let \( \alpha \) and \( \beta \) be \( k \)-linear automorphisms of rational function fields. Then \( \beta \) is negligible relative to \( \alpha \) if and only if \( \text{Ord}(g) \) divides \( \text{Ord}(f) \).

The answer to Question 1 of the introduction now comes as an immediate consequence.

Theorem 6.6. Let \( f(T), g(T) \in k[T] \) be polynomials of degree \( m \) and \( n \) respectively and suppose \( f(0)g(0) \neq 0 \). Then the following are equivalent:

(i) There exists a linear \( k \)-automorphism \( \sigma \) on some \( K \in E(k) \) so that both \( f(T) \) and \( g(T) \) are minimum polynomials of \( \sigma \).
(ii) \( \langle f \rangle \star I_n \cong \langle g \rangle \star I_m \).
(iii) \( \text{Ord}(\langle f \rangle) = \text{Ord}(\langle g \rangle) \).

Proof. We show first that (ii) and (iii) are equivalent. If \( \text{Ord}(\langle f \rangle) = \text{Ord}(\langle g \rangle) \), then by Theorem 6.5, \( \langle f \rangle \) and \( \langle g \rangle \) are negligible relative to one another. Hence

\[ \langle f \rangle \star I_m \cong \langle f \rangle \star \langle g \rangle \cong \langle g \rangle \star I_n. \]

Thus (iii) implies (ii). Conversely, (ii) implies (iii) by Corollary 5.3. Thus (ii) and (iii) are equivalent.

We next note that (i) implies (ii) by Theorem 2.2.

Thus it remains to show that (ii) and (iii) imply (i). So suppose that (ii) and (iii) hold. If \( m \geq 2 \) and \( n \geq 2 \), let \( \sigma_1 = \langle f \rangle \star \langle f \rangle \star \cdots \star \langle f \rangle \) (\( n \) copies) and \( \sigma_2 = \langle g \rangle \star \langle g \rangle \star \cdots \star \langle g \rangle \) (\( m \) copies). Then \( \sigma_1 \) and \( \sigma_2 \) are equivalent and have \( f \) and \( g \), respectively, as their minimal polynomials.
If $n = 1$, let $\sigma_1 = \langle f \rangle * \langle f \rangle$ and $\sigma_2 = \langle g \rangle * \langle g \rangle * \cdots * \langle g \rangle$ ($2m$ copies). Then again $\sigma_1$ and $\sigma_2$ are equivalent with the desired minimal polynomials. Similarly for $m = 1$. Thus (ii) and (iii) imply (i), as desired.

This completes the proof. □

The relation between the generalized order of $\langle f(T) \rangle$ and its ordinary order (when this order is finite) is summarized in the following theorem whose proof is immediate. Note that every finite subgroup of $\bar{k}^*$ is cyclic and that no different finite subgroups can have the same order. The order of such a group is relatively prime to $p$ if $\text{char}(k) = p > 0$. Note also that if $\text{char}(k) = p > 0$ and $s = p^r$, then the order of $\langle (T - 1)^r, 1 \rangle = p^{r+1}$ (cf. Proposition 3.1(ii)).

**Theorem 6.7.** Let $f(T) \in k[T]$ and let $\sigma = \langle f(T) \rangle$.

(i) If $\text{char}(k) = 0$, then $\sigma$ has a finite order $m$ if and only if $R(f)$ has order $m$ and $\omega(f) = 0$.

(ii) If $\text{char}(k) = p > 0$, then $\sigma$ has a finite order $m = np^r$ with $\gcd(n, p) = 1$ if and only if $R(f)$ has order $n$ and $\omega(f) = p^{r-1}$.

We end this paper by remarking that condition (ii) of Theorem 6.6 cannot be replaced by either of the stronger conditions

$$\langle f \rangle \cong \langle g \rangle$$

and

$$\langle f \rangle \cong \langle g \rangle * I.$$ (16)

In fact, it is easy to see that if $u, v \in k^*$, then $\langle T - u \rangle$ and $\langle T - v \rangle$ are equivalent if and only if $u = v$ or $u = 1/v$ [8, Lemma 7, p. 1544]. Taking $u$ and $v$ (in the field $\mathbb{C}$ of complex numbers, say) to be distinct primitive $n$th roots of unity with $u \neq 1/v$, and letting $\alpha = \langle T - u \rangle$ and $\beta = \langle T - v \rangle$, we see that $\text{Ord}(\alpha) = \text{Ord}(\beta)$, and that neither of the conditions in (16) holds.

**Acknowledgments**

We would like to thank Prof. Ming-chang Kang (National Taiwan University) for correspondence and fruitful discussions regarding both the content and the exposition of this paper, and also for pointing out Ref. [5]. We would also like to thank the referee who, beside providing several valuable suggestions, is responsible for the present proof of Theorem 6.6.

**References**