A NOTE ON LINEAR AUTOMORPHISMS OVER $\mathbf{R}$

MOWAFFAQ HAJJA

(Communicated by Louis J. Ratliff, Jr.)

Abstract. Let $K$ be a rational (= purely transcendental) extension of (the field) $k$, and let $s$ be a $k$-automorphism of $K$ of finite order. Let $s$ be linear in the sense that $K$ has a base $B$ (i.e., a transcendence basis $B$ with $K = k(B)$) for which the $k$-submodule $\Sigma(kb : b \in B)$ of $K$ generated by $B$ is stabilized by $s$. In [1, Question 6], it is asked whether $s$ is completely determined by its order (and $\text{tr. deg}_k(K)$) and it is proved that, when $k$ is the complex number field $\mathbf{C}$, then the answer to this question is affirmative iff $\text{tr. deg}_\mathbf{C}(K) > 1$ [1, Corollary 9, Question 6 and Lemma 7]. In this paper, we solve the problem for the field $\mathbf{R}$ of real numbers under the condition that $\text{tr. deg}_\mathbf{R}(K)$ is $\neq 2, 3$. For $\text{tr. deg}_\mathbf{R}(K) = 2$ or $3$, the problem remains open.

Definitions. Let $\mathbf{R}$ and $\mathbf{C} = \mathbf{R}(i)$ denote the real and complex number fields (with $i^2 = -1$), and let $\gamma$ be the generator of the Galois group $\text{Gal}(\mathbf{C}/\mathbf{R})$ of $\mathbf{C}$ over $\mathbf{R}$. For any rational extension $K$ of $\mathbf{R}$, let $\overline{K} = K(i)$, and let the same letter $\gamma$ stand for the generator of $\text{Gal}(\overline{K}/K)$. If $t \in \overline{K}$, then $t = t_1 + it_2$ for some $t_1, t_2 \in K$ and $\gamma(t)$ is the conjugate $t_1 - it_2$ of $t$. We denote $\gamma(t)$ by $\overline{t}$.

If $f(T) = \sum_{i=0}^{d} a_i T^i \in \mathbf{R}[T]$ is of degree $d$, with $a_0 \neq 0$, then $\sigma(f)$ is defined (as in [1]) to be the cyclic linear automorphism associated with $f$. Thus $s = \sigma(f)$ is the $\mathbf{R}$-automorphism defined on the rational function field $K = \mathbf{R}(X_1, X_2, \ldots, X_d)$ by

$$s(X_j) = X_{j+1}, \quad \text{for } 1 \leq j < d,$$

$$f(s)X_1 = 0.$$

If $K_1$ and $K_2$ are rational extensions of $\mathbf{R}$ with $\mathbf{R}$-automorphisms $s_1$ and $s_2$ (respectively), then $K_1 \ast K_2$ denotes the quotient field of the tensor product $K_1 \otimes_\mathbf{R} K_2$ and $s_1 \ast s_2$ denotes the $\mathbf{R}$-automorphism induced by $s_1 \otimes_\mathbf{R} s_2$ on $K_1 \ast K_2$. Thus if $B_1, B_2$ are bases of $K_1, K_2$ (respectively), then $K_1 \ast K_2$ is the rational extension of $\mathbf{R}$ having for a base the union of (independent copies of) $B_1$ and $B_2$. Also, we say that $s_1 \cong s_2$ iff $s_1 = s^{-1}s_2s$ for some $\mathbf{R}$-isomorphism $s : K_1 \to K_2$. The subfield of a rational extension $K$ of $\mathbf{R}$ fixed by an $\mathbf{R}$-automorphism $s$ of $K$ is denoted by $K^s$, and $s$ is said to be
rational if $K^+$ is (over $R$). The identity automorphism on $R(X_1, X_2, \ldots, X_n)$ is denoted by $I_n$. Thus $I_n = \sigma^{\sum_{j=1}^{n} \sigma(T - 1)}$. The letter $I$ stands for “$I_n$ for some $n$”. The order of $f(T) \in R[T]$ is understood to be the order of $\sigma(f)$. Thus the order of $f$ is the smallest $n \in N$ for which $f(T)$ divides $T^n - 1$ (or, equivalently, the least common multiple of the orders in $C$ of the roots of $f$ if $f$ has no multiple roots). It is clear that the only degree 1 polynomials in $R[T]$ of finite order are $T - 1$ and $T + 1$. The set of irreducible quadratics having finite order is denoted by $\Omega$. Also, the GCD of two integers $n$ and $m$ is denoted by $(n, m)$.

**Lemma 1.** If $Q_1, Q_2 \in \Omega$, then $\exists Q \in \Omega$ such that

$$\sigma(Q_1) \ast \sigma(Q_2) \cong \sigma(Q) \ast I.$$ 

**Proof.** Let $s = \sigma(Q_1) \ast \sigma(Q_2)$. Then $s$ is the $R$-automorphism defined on $K = R(x_1, y_1, x_2, y_2)$ by

$$s(x_1) = y_1, \quad s(x_2) = y_2,$$

$$Q_1(s)x_1 = Q_2(s)x_2 = 0.$$ 

Let $\bar{K} = C(x_1, y_1, x_2, y_2)$ and let the same letter $s$ denote the extension of $s$ to $\bar{K}$ obtained by letting $s$ act trivially on $C$. For $j = 1, 2$, let

$$Q_j(T) = (T - r_j)(T - \bar{r}_j)$$ 

be the factorization of $Q_j(T)$ in $C[T]$ and let

$$\xi_j = (s - \bar{r}_j)x_j = (y_j - \bar{r}_jx_j).$$

Then it is easy to see that

$$\bar{K} = C(\xi_1, \bar{\xi}_1, \xi_2, \bar{\xi}_2)$$

and that

$$s(\xi_j) = r_j\xi_j, \quad s(\bar{\xi}_j) = \bar{r}_j\bar{\xi}_j.$$ 

Let $G = \langle r_1, r_2 \rangle$ be the subgroup of $C^*$ generated by $r_1$ and $r_2$. Since $r_1$ and $r_2$ are of finite orders, then $G$ is finite and hence is cyclic. Let $r$ be a generator of $G$. If

$$r_1 = r_1^{n_1}, \quad r_2 = r_2^{n_2}$$

and if $(n_1, n_2) = d$, then

$$G = \langle r_1, r_2 \rangle \subseteq \langle r^d \rangle \subseteq \langle r \rangle = G$$

and therefore $r^d$ is a generator of $G$. Replacing $r$ by $r^d$ allows us to assume that $(n_1, n_2) = 1$. Let $\alpha_1, \alpha_2 \in Z$ be such that

$$\alpha_1n_1 + \alpha_2n_2 = 1,$$

and let

$$\eta_1 = \xi_1^{\alpha_1}\xi_2^{\alpha_2}, \quad \eta_2 = \xi_1^{-n_2}\xi_2^{n_1}.$$
Since \(\det\begin{bmatrix} -\eta_1 & \eta_2 \\ \eta_1 & -\eta_2 \end{bmatrix} = 1\), then it follows from [2, Lemma 0] that \(C(\xi_1, \xi_2) = C(\eta_1, \eta_2)\). It is also clear that
\[
s(\eta_1) = r\eta_1, \quad s(\eta_2) = \eta_2.
\]
Therefore \(\overline{K} = C(\xi_1, \xi_2, \xi_1, \xi_2) = C(\eta_1, \eta_2, \eta_1, \eta_2)\) and
\[
s(\eta_1) = r\eta_1, \quad s(\eta_1) = r\eta_1
\]
\[
s(\eta_2) = \eta_2, \quad s(\eta_2) = \eta_2.
\]
Let \(X_j = (\eta_j - \eta_j)/(r - \overline{r})\), \(Y_j = (\eta_j - \overline{\eta}_j)/(r - \overline{r})\). Then \(\overline{K} = C(X_1, Y_1, X_2, Y_2)\) and \(X_1, Y_1, X_2, Y_2\) are all fixed by \(\gamma\). From the linear disjointness of \(C\) and \(K\) [4; Exercise 1, p. 530], we conclude that
\[
K = R(X_1, Y_1, X_2, Y_2).
\]
It is now easy to check that the restrictions of \(s\) to \(R(X_1, Y_1)\) and \(R(X_2, Y_2)\) are nothing but \(\sigma(Q)\) and \(I\) (respectively), where \(Q = (T - r)(T - \overline{r})\). This proves the lemma. \(\Box\)

**Lemma 2.** If \(Q \in \Omega\), then \(\sigma(Q) * \sigma(T + 1) \cong \sigma(Q_1) * I\) for some \(Q_1 \in \Omega\).

**Proof.** Let \(s = \sigma(Q) * \sigma(T + 1)\). Then \(s\) is the \(R\)-automorphism on \(K = R(x, y, z)\) defined by
\[
s(x) = y, \quad Q(s)x = 0
\]
\[
s(z) = -z.
\]
If the order of \(\sigma(Q)\) is even, then the result follows from [1, Theorem 4] with \(Q_1 = Q\). Otherwise, note that \(K = R(xz, yz, z)\) and that the restriction of \(s\) to \(R(xz, -yz)\) is \(\sigma(Q_1)\) where \(Q_1\) is given by \(Q_1(T) = Q(-T)\). Therefore \(s \cong \sigma(Q_1) * \sigma(T + 1)\). Since the order of \(Q_1\) is even, then the result follows again from [1, Theorem 4]. \(\Box\)

**Lemma 3.** If \(Q \in \Omega\), then \(\sigma(Q)\) is rational.

**Proof.** Let \(s = \sigma(Q)\). Then \(s\) is the \(R\)-automorphism defined on \(K = R(x, y)\) by
\[
s(x) = y, \quad Q(s)x = 0.
\]
Let \(\overline{K} = C(x, y)\) and let \(s\) be extended to a \(C\)-automorphism of \(\overline{K}\) by letting it act trivially on \(C\). Let \(Q(T) = (T - r)(T - \overline{r})\) be the factorization of \(Q(T)\) in \(C[T]\) and let \(\xi = (s - \overline{r})x\). Then
\[
\overline{K} = C(\xi, \overline{\xi})
\]
and
\[
s(\xi) = r\xi, \quad s(\overline{\xi}) = r\overline{\xi}.
\]
Let \(A = \xi\overline{\xi}\) and \(B = \xi^n\), where \(n = \text{order}(s) = \text{order}(r)\). Then \(A\) and \(B\) are \(s\)-fixed and \([C(\xi, \overline{\xi}) : (A, B)] = \det\begin{bmatrix} n & 0 \\ 0 & 1 \end{bmatrix} = n = \text{order}(s)\). Hence \(\overline{K} = C(A, B)\). Also,
\[
\gamma(A) = A, \quad \gamma(B) = A^n/B.
\]
Let \( \beta = B/A^{[n/2]} \), where \([\ ]\) is the greatest integer function. Then \( \overline{K^s} = C(A, \beta) \), \( \gamma(A) = A \) and
\[
\gamma(\beta) = \begin{cases} 
1/\beta & \text{if } n \text{ is even} \\
A/\beta & \text{if } n \text{ is odd}.
\end{cases}
\]
If \( n \) is even, let \( X = A \) and \( Y = i(1 - \beta)/(1 + \beta) \), and if \( n \) is odd, let \( X = \beta + A/\beta \) and \( Y = i(\beta - A/\beta) \). Then \( \overline{K^s} = C(X, Y) \) and both \( X \) and \( Y \) are \( \gamma \)-fixed. By the linear disjointness of \( K \) and \( C \), we conclude that \( K^s = R(X, Y) \) and is hence rational. \( \square \)

**Lemma 4.** Let \( Q, Q_1 \in \Omega \) be of the same order. If \( n \geq 2 \), then
\[
\sigma(Q) * I_n \cong \sigma(Q_1) * I_n.
\]

**Proof.** Let
\[
Q(T) = (T - r)(T - \bar{r}), \quad Q_1(T) = (T - r_1)(T - \bar{r}_1)
\]
be the factorization of \( Q \) and \( Q_1 \) in \( \mathbb{C}[T] \). Since \( r \) and \( r_1 \) have the same order, \( m \), say, then \( r_1 = r^d \) for some \( d \in \mathbb{N} \) with \( (d, m) = 1 \). Let \( \delta, \mu \in \mathbb{Z} \) be such that
\[
\delta d + \mu m = 1.
\]
Let \( s = \sigma(Q) * I_2 \). Then \( s \) is the \( R \)-automorphism on \( R(X, Y, Z, W) \) defined by
\[
s(X) = Y, \quad Q(s)X = 0, \\
s(Z) = Z, \quad s(W) = W.
\]
Let \( \overline{K} = C(X, Y, Z, W) \), and let \( s \) be extended to \( \overline{K} \) by letting it act trivially on \( C \). Let
\[
\xi = (s - \bar{r})X, \quad \zeta = Z + iW.
\]
Then \( \overline{K} = C(\xi, \bar{\xi}, \zeta, \bar{\zeta}) \) and
\[
s(\xi) = r\xi, \quad s(\zeta) = \zeta.
\]
Let
\[
A = \xi^d \xi^\mu, \quad B = \xi^{-m} \xi^\delta.
\]
Since \( \det \begin{pmatrix} d & \mu \\ -m & \delta \end{pmatrix} = 1 \) (by \( \ast \)), then it follows [2, Lemma 0] that \( C(\xi, \zeta) = C(A, B) \) and hence \( \overline{K}(= C(\xi, \bar{\xi}, \zeta, \bar{\zeta})) = C(A, B, \bar{A}, \bar{B}) \). Also
\[
s(A) = r^d A = r_1 A, \quad s(B) = B.
\]
Finally let
\[
x = (A - \bar{A})/(r_1 - \bar{r}_1), \\
y = s(x) = (r_1 A - \bar{r}_1 \bar{A})/(r_1 - \bar{r}_1), \\
z = B + \bar{B}, \quad w = i(B - \bar{B}).
\]
Then $\overline{K} = \mathbb{C}(x, y, z, w)$ with $x, y, z, w$ all $\gamma$-fixed. So $K = \mathbb{R}(x, y, z, w)$. It is also easy to see that the restrictions of $s$ to $\mathbb{R}(x, y)$ and $\mathbb{R}(z, w)$ are $\sigma(Q_1)$ and $I_2$ (respectively). Therefore our lemma is proved for $n = 2$. The case $n \geq 2$ follows immediately. □

**Theorem 5.** Let $K$ be a rational extension of $\mathbb{R}$ having a finite transcendence degree $n$, and let $s$ be a linear $\mathbb{R}$-automorphism of $K$ of a finite order $d$. Then

(i) $s = I$ or $I \ast \sigma(T + 1)$ or $I \ast \sigma(Q)$ for some $Q \in \Omega$.
(ii) $s$ is rational.
(iii) If $n \geq 4$, then $s$ is completely determined by $d$ and $n$. The same holds for $n = 1$.

**Proof.** (i) Let $\mu(T) \in \mathbb{R}[T]$ be the minimal polynomial of $s$. Since $s$ has finite order, then $\mu(T)$ has no repeated factors and therefore the rational canonical form theorem allows us to assume that

$$s = I \ast \left[ \prod_{i=1}^{r} \sigma(F_i) \right],$$

where each $F_i$ is an irreducible factor of $\mu(T)$ other than $T - 1$. Since the irreducible polynomials in $\mathbb{R}[T]$ are of degree 1 or 2, then the $F_i$'s (being of finite order) are elements of $\Omega \cup \{T + 1\}$. Using Lemmas 1 and 2 repeatedly, we arrive at the conclusion of (i).

(ii) This follows from Lemma 3 and the trivial fact that $s = \sigma(T + 1)$ is rational (being nothing but the $\mathbb{R}$-automorphism on $\mathbb{R}(X)$ defined by $s(X) = -X$ and hence having $\mathbb{R}(X^2)$ as its fixed field).

(iii) If $\text{order}(s) = 1$ or 2 (which is the only possible case for $n = 1$), then $s = I \ast \sigma(T + 1)$ and there is nothing to prove. Otherwise $s = I_m \ast \sigma(Q)$ for some $Q \in \Omega$. Since $m = n - 2 \geq 4 - 2 = 2$, then the result follows from Lemma 4. □

**Remark 6.** A different proof of Theorem 5(ii) can be found in [5, §2].

**Remark 7.** It is open whether the conclusion of Lemma 4 (respectively, Theorem 5(iii)) holds for $n = 0, 1$ (respectively, for $n = 2, 3$). The situation for the field $\mathbb{C}$ of complex numbers is simpler. Thus if one replaces $\mathbb{R}$ by $\mathbb{C}$ in the hypothesis of Theorem 5, then one concludes from [1] that if $n > 1$ then $s$ is completely characterized by its order [1, Corollary 9] and that if $n = 1$ then the number of inequivalent linear automorphisms of any order $d$ is precisely $1 + [\varphi(d)/2]$, where $\varphi$ is the Euler phi-function [1; Question 6 and Lemma 7].

**Remark 8.** It is clear that one can replace $n$ in Lemma 4 by any cardinal. The same is true of Theorem 5 since the decomposition (***) in the proof of (i) follows from the fact that every algebraic automorphism is completely determined by its minimal polynomial (and $n$) [3].
REFERENCES


DEPARTMENT OF MATHEMATICS, KuWAIT University, P.O. BOX 5969 (SafAT), KuWAIT 13060