Acta Mathematica Universitatis Ostraviensis

Ladislav Skula

A note on involutory automorphisms of C and the use of algebraically independent numbers for the construction of diagonable matrices

Acta Mathematica Universitatis Ostraviensis, Vol. 12 (2004), No. 1, 49--60

Persistent URL: http://dml.cz/dmlcz/120604

Acta Mathematica Universitatis Ostraviensis 12 (2004) 49–60

A note on involutory automorphisms of C and the use of algebraically independent numbers for the construction of diagonable matrices

Ladislav Skula

Abstract. The involutory automorphisms of the complex field are investigated and classified into three families: Archimedian - "like real numbers", Archimedian - "like a proper subfield of real numbers" and non-Archimedian. It is shown that these families have the same cardinality equal to $\exp\exp\aleph_0$. By means of the involutory automorphisms and Lindemann's criterion on algebraically independent numbers a class of diagonable matrices is constructed.

1. Introduction

The involutory automorphisms of the complex field $\mathbf{C}$ play an important role in description of all involutions for matrices with complex entries ([Sk], Theorems 2.1 and 2.2). The main objective of this article is to investigate such automorphisms. These automorphisms (except the identity) are of two kinds — Archimedian or non-Archimedian. An involutory automorphism is *Archimedian* if its fixed field is Archimedian, hence this field is embedded into the real field. This embedding can be isomorphism onto but it can also happen that it is not surjective. In this case the fixed field of the involutory automorphism contains gaps. All these three types have the same cardinality equal to $\exp\exp\aleph_0$.

The last Section is devoted to application to the regular (diagonable) matrices. By means of an involutory automorphism of the complex field a family of regular matrices is constructed. In concrete cases this construction makes use of Theorem 5.1 garanteeing existence of an involutory automorphism of $\mathbf{C}$ extending a special mapping for complex numbers. Theorem 5.2 gives a rule for an involutory

Received: March 21, 2005.

1991 *Mathematics Subject Classification:* Primary 15A57; Secondary 11J85, 12D15, 12F20.

Key words and phrases: Involutory automorphism of the complex field, Archimedian (non-Archimedian) involutory automorphism, regular (diagonable) matrix, transcendence degree, algebraically independent numbers, Lindemann criterion on algebraically independent numbers, cyclotomic field.

Research was supported by the Grant Agency of the Czech Republic, No. 201/04/0381.

automorphism of $\mathbf{C}$ stating how to operate on elements from a cyclotomic field. The construction uses the criterion of Lindemann (Theorem 5.4) on algebraically independent numbers.

2. Notation and Fundamental Assertions

Throughout the whole paper we designate by

$\mathbf{C}$ the field of complex numbers,
$\mathbf{R}$ the field of real numbers,
$\mathbf{Q}$ the field of rational numbers,
$i_{\mathbf{C}}$ the identity mapping of $\mathbf{C}$,
σ the complex conjugation, hence $\sigma(\alpha) = \bar{\alpha}$ for $\alpha \in \mathbf{C}$,
$\{x_\iota : \iota \in I\}$ the set of any symbols where I is an index set (I can be empty) and it is supposed $x_{\iota_1} \neq x_{\iota_2}$ for $\iota_1, \iota_2 \in I$, $\iota_1 \neq \iota_2$,
$X = \{X_\iota : \iota \in I\}$ the set of indeterminates,
$k[X] = k[X_\iota]_{\iota \in I}$ the polynomial ring over the (commutative) field k with indeterminates $X = \{X_\iota : \iota \in I\}$,
$k(X) = k(X_\iota)_{\iota \in I}$ the field of rational forms over the field k.

We will use the common concepts and assertions of commutative algebra, particulary of the theory of field extensions and of (linearly) ordered fields ([Bb], [F], [N]). We will use the following known Theorems 2.1 - 2.4.

Theorem 2.1 *Let F be an isomorphism from a field k onto a field k' and let K, K' be algebraic closures of k, k', respectively. Then there exists an isomorphism F' from K onto K' such that the following diagram is commutative:*

$$\begin{array}{ccc} k & \xrightarrow{F} & k' \\ \downarrow & & \downarrow \\ K & \xrightarrow{F'} & K' \end{array}$$

In this article, the morphisms which are not denoted mean the inclusion mappings.

Theorem 2.2 *The transcendence degrees of $\mathbf{C}/\mathbf{Q}$ and $\mathbf{R}/\mathbf{Q}$ are equal and they equal* $\exp \aleph_0$.

An *ordered field* will be a linearly ordered field and a *maximal ordered field* will denote an ordered field K such that each algebraic extension of K which is ordered equals K.

Theorem 2.3 *Each ordered field possesses an algebraic extensionfield which is a maximal ordered field.*

Theorem 2.4 *(Euler-Lagrange). Let K be an ordered field. Then the following statements are equivalent:*
(a) The field $K(i)$ is algebraically closed.
(b) The field K is a maximal ordered field.

(c) Each positive element of K is a square root of an element from K and each polynomial of odd degree over K has at least one root in K.

Definition 2.1. An automorphism f of the field $\mathbf{C}$ is called *involutory* if $f^2 = i_{\mathbf{C}}$. The fixed field of $\{f\}$ will be denoted by $F(f)$, therefore

$$F(f) = \{\gamma \in \mathbf{C} : f(\gamma) = \gamma\}.$$

In the paper [Sk] Theorem 2.5 and 2.6 were proved (Proposition 3.1 and Theorem 3.1).

Theorem 2.5 *Let f be an involutory automorphism of the field $\mathbf{C}$, $f \neq i_{\mathbf{C}}$. Then*
(a) $f(i) = -i$,
(b) for each $\delta \in \mathbf{C}$ there exist unique numbers $\alpha, \beta \in F(f)$ such that

$$\delta = \alpha + i\beta,$$

(c) for these δ, α, β we have

$$f(\delta) = \alpha - i\beta.$$

Theorem 2.6 *For an involutory automorphism f of the field $\mathbf{C}$, $f \neq i_{\mathbf{C}}$, the field $F(f)$ is an ordered field with the positive cone $P = \{\varrho^2 : \varrho \in F(f)\}$. Hence, $F(f)$ is a maximal ordered field.*

For further purpose we will need the lemma.

Lemma 2.1 *Let K, L be subfields of $\mathbf{C}$, g an isomorphism of K onto L and $\pi = \sigma/_K, \varrho = \sigma/_L$ automorphisms of K, L, respectively. Suppose $i \in K \cap L$, $g(i) = i$ and $\sqrt{k} \in K$ for each $k \in K \cap \mathbf{R}$, $k > 0$.*
If $g \circ \pi = \varrho \circ g$, then $K = L$ and $g = i_K$ (the identity mapping of K).

Proof. Let $U = K \cap \mathbf{R}$, $V = L \cap \mathbf{R}$. For $r \in U$ we have $g(r) = a + ib$, where $a, b \in \mathbf{R}$, therefore $a - ib = (\varrho \circ g)(r) = (g \circ \pi)(r) = g(r) = a + ib$, which gives $b = 0$ and $g(r) \in \mathbf{R}$.

Denote by f the restriction of g on U, hence f is an isomorphism from U to V. For the same reason we get that the restriction of g^{-1} on V is an isomorphism from V to U, consequently f is surjective.

Let $u \in U$, $u > 0$. Then $\sqrt{u} \in U$, $f(\sqrt{u}) \in V$ and $f(u) = f(\sqrt{u})^2$, thus $f(u) > 0$, which follows that f preserves ordering. Therefore $U = V$ and f is the identity mapping of U.

For $k = a + ib \in K$, $a, b \in \mathbf{R}$ we have $a, b \in U$ (since $\sigma(k) = \bar{k} \in K$), hence $g(k) = g(a) + ig(b) = f(a) + if(b) = a + ib = k$.

The lemma is proved.

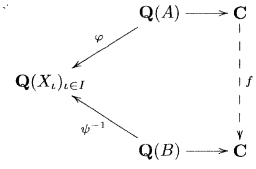
3. Isomorphisms from C into C

Construction 3.1. Let $A = \{a_\iota : \iota \in I\}$ be a transcendence base of the extension $\mathbf{C}/\mathbf{Q}$ and let $B = \{b_\iota : \iota \in I\}$ be an algebraically independent subset of $\mathbf{C}$ (over

$\mathbf{Q}$). Then there exist isomorphisms φ, ψ from the field $\mathbf{Q}(A)$, $\mathbf{Q}(B)$, respectively, onto the field $\mathbf{Q}(X_\iota)_{\iota\in I}$ such that

$$\varphi(x) = \psi(x) = x \quad \text{for each } x \in \mathbf{Q},$$
$$\varphi(a_\iota) = \psi(b_\iota) = X_\iota \quad \text{for each } \iota \in I.$$

According to Theorem 2.1 there exists an isomorphism f from $\mathbf{C}$ into $\mathbf{C}$ such that the following diagram is commutative.



The field $f(\mathbf{C})$ is an algebraic closure of $\mathbf{Q}(B)$. Obviously,

Proposition 3.1 *The above constructed isomorphism f is an automorphism of $\mathbf{C}$ if and only if B is a transcendence base of $\mathbf{C}/\mathbf{Q}$.*

Proposition 3.2 *Each isomorphism f from $\mathbf{C}$ into $\mathbf{C}$ can be constructed by means of Construction 3.1.*

Proof. Let f be an isomorphism from $\mathbf{C}$ into $\mathbf{C}$ and let $A = \{a_\iota : \iota \in I\}$ be a transcendence base of $\mathbf{C}/\mathbf{Q}$. The set $B = \{f(a_\iota) : \iota \in I\}$ is an algebraically independent subset of $\mathbf{C}$ (over $\mathbf{Q}$). If φ, ψ are isomorphisms from $\mathbf{Q}(A), \mathbf{Q}(B)$, respectively, onto $\mathbf{Q}(X_\iota)_{\iota\in I}$ described in Construction 3.1, then for $\alpha \in \mathbf{Q}(A)$ we have $\psi^{-1}\varphi(\alpha) = f(\alpha)$ and we are done.

Definition 3.1. We will call an isomorphism f from the field $\mathbf{C}$ into $\mathbf{C}$ a *$\varkappa$-isomorphism* if $\bar{\lambda} = \sigma(\lambda) \in f(\mathbf{C})$ for each $\lambda \in f(\mathbf{C})$. Hence *$f$ is a $\varkappa$-isomorphism if and only if* $f(\mathbf{C}) = \overline{f(\mathbf{C})} = \sigma f(\mathbf{C})$.

Proposition 3.3 *Suppose that f is an isomorphism from $\mathbf{C}$ into $\mathbf{C}$ constructed by means of Construction 3.1. Then the following statements are equivalent:*

(a) f is a $\varkappa$-isomorphism.

(b) If $\iota \in I$ and $\bar{b}_\iota \notin B$, then the set $B \cup \{\bar{b}_\iota\}$ is algebraically dependent (over $\mathbf{Q}$).

(c) For each $\iota \in I$, $\bar{b}_\iota$ is an algebraic element over $\mathbf{Q}(B)$.

Proof. It is easy to see that (b) and (c) are equivalent. Since $f(\mathbf{C})$ is an algebraic closure of $\mathbf{Q}(B)$, statement (c) follows from (a).

Suppose that (c) is true. Clearly, $\bar{\beta} \in f(\mathbf{C})$ for each $\beta \in \mathbf{Q}(B)$. Let $\lambda \in f(\mathbf{C})$. Since λ is an algebraic element over $\mathbf{Q}(B)$, there exist positive integers n, m, polynomials $g_i(X_1, \ldots, X_n) \in \mathbf{Q}[X_1, \ldots, X_n]$ for $0 \le i \le m$ ($X_1, \ldots, X_n$ are indeterminates) and elements $\beta_1, \ldots, \beta_n \in B$ such that

$$\sum_{i=0}^{m} g_i(\beta_1, \ldots, \beta_n)\lambda^i = 0 \quad \text{and} \quad g_m(\beta_1, \ldots, \beta_n) \neq 0.$$

Setting $\gamma_i = g_i(\bar{\beta}_1, \ldots, \bar{\beta}_n)$ for $0 \leq i \leq m$ we get $\gamma_i \in f(\mathbf{C})$, $\gamma_m \neq 0$ and $\sum_{i=0}^{m} \gamma_i \bar{\lambda}_i = 0$. The result follows by noting that $f(\mathbf{C})$ is an algebraic closure of $\mathbf{Q}(B)$.

Notation. We denote by $\mathcal{K}$, $\mathcal{L}$, $\mathcal{A}$ the systems of all $\varkappa$-isomorphisms which are not surjective, all isomorphisms from $\mathbf{C}$ into $\mathbf{C}$ which are not $\varkappa$-isomorphisms, all automorphisms of $\mathbf{C}$, respectively. If $\mathcal{B} \in \{\mathcal{K}, \mathcal{L}, \mathcal{A}\}$, let $\mathcal{B}^+ = \{g \in \mathcal{B} : g(i) = i\}$ and $\mathcal{B}^- = \{g \in \mathcal{B} : g(i) = -i\}$.

Theorem 3.1 *The sets* $\mathcal{K}$, $\mathcal{K}^+$, $\mathcal{K}^-$, $\mathcal{L}$, $\mathcal{L}^+$, $\mathcal{L}^-$, $\mathcal{A}$, $\mathcal{A}^+$, $\mathcal{A}^-$ *have the same cardinality equal to* $\exp\exp\aleph_0$.

Proof. I. Put $F(g) = g \circ \sigma$ for each $g \in \mathcal{B}^+$, where $\mathcal{B} \in \{\mathcal{K}, \mathcal{L}, \mathcal{A}\}$. It is easy to see that F is a bijection from $\mathcal{B}^+$ onto $\mathcal{B}^-$.

II. Let A, C be transcendence bases of the extensions $\mathbf{C}/\mathbf{Q}$, $\mathbf{R}/\mathbf{Q}$, respectively. By Theorem 2.2 $A = \{a_\iota : \iota \in I\}$ and there exists $B = \{b_\iota :\in I\} \subseteq C$ such that card $I = \exp\aleph_0$. We can suppose either (a) B is a transcendence base of $\mathbf{C}/\mathbf{Q}$ or (b) $B \neq C$. If f is the isomorphism from $\mathbf{C}$ into $\mathbf{C}$ constructed in the way of Construction 3.1, then $f \in \mathcal{K}$ in case (b) and $f \in \mathcal{A}$ in case (a) (by Propositions 3.1 and 3.3). Using the permutations of the set I we get

$$\text{card } \mathcal{K} = \text{card } \mathcal{A} = \exp\exp\aleph_0.$$

III. Choose two different elements c, d from C and put $\alpha = c + id$, $\beta = \bar{\alpha} = c - id$. Let $F(X, Y)$ be a polynomial in the indeterminates X, Y order $\mathbf{Q}$. Using the substitution $X = x + iy$, $Y = x - iy$ for other indeterminates x, y we get $F(X, Y) = \varphi(x, y) + i\psi(x, y)$, where $\varphi(x, y), \psi(x, y) \in \mathbf{Q}[x, y]$.

Assume $F(\alpha, \beta) = 0$. Then $\varphi(c, d) + i\psi(c, d) = 0$, which follows that $\varphi(x, y) = \psi(x, y) = 0$, therefore $F(X, Y) = 0$ and the numbers α, β are algebraically independent over $\mathbf{Q}$.

There exists a transcendence base E of $\mathbf{C}/\mathbf{Q}$ containing the elements α, β. Put $D = E - \{\beta\} = \{\delta_\iota : \iota \in I\}$. Let us construct the isomorphism f from $\mathbf{C}$ into $\mathbf{C}$ by means of Construction 3.1 using the set D instead of B. By Proposition 3.3 f is not a $\varkappa$-isomorphism, hence $f \in \mathcal{L}$. Again considering the cardinality of all permutations of the set I we get

$$\text{card } \mathcal{L} = \exp\exp\aleph_0.$$

The theorem is proved.

4. Involutory Automorphisms of $\mathbf{C}$

Definition 4.1. An involutory automorphism f of $\mathbf{C}$ is called *Archimedian* if $f \neq i_{\mathbf{C}}$ and the ordered field $F(f)$ is Archimedian, which is equivalent with the following condition:

there exists an embedding of the ordered field $F(f)$ *into the real field* $\mathbf{R}$.

([F], Chap. VIII. Theorem 1). In the opposite case and in case $f \neq i_{\mathbf{C}}$, f is called *non-Archimedian.*

Notation. If φ is a $\varkappa$-isomorphism from $\mathbf{C}$ into $\mathbf{C}$, we denote by $\sigma(\varphi)$ the complex conjugation from $\varphi(\mathbf{C})$ onto $\varphi(\mathbf{C})$. The $\varkappa$-isomorphism φ will be considered as a

map from $\mathbf{C}$ onto $\varphi(\mathbf{C})$ and the symbol φ^{-1} will denote the inverse map of φ from $\varphi(\mathbf{C})$ onto $\mathbf{C}$.

The following theorem gives a characterization of all Archimedian involutory automorphisms of $\mathbf{C}$.

Theorem 4.1 *The system of all Archimedian involutory automorphisms f of $\mathbf{C}$ is equal to the system of all f of the form $f = \varphi^{-1} \circ \sigma(\varphi) \circ \varphi$, where φ is a $\varkappa$-isomorphism from $\mathbf{C}$ into $\mathbf{C}$ such that $\varphi(i) = i$ (hence $\varphi \in \mathcal{K}^+ \cup \mathcal{A}^+$).*

The isomorphism $\varphi \in \mathcal{K}^+ \cup \mathcal{A}^+$ is uniquely defined by $f = \varphi^{-1} \circ \sigma(\varphi) \circ \varphi$. The embedding from $F(f)$ into $\mathbf{R}$ is given by restriction $\tilde{\varphi}$ of φ on $F(f)$.

$\tilde{\varphi}$ surjective if and only if φ is surjective, i.e., $\varphi \in \mathcal{A}^+$.

Proof. I. Let $\varphi \in \mathcal{K}^+ \cup \mathcal{A}^+$, $f = \varphi^{-1} \circ \sigma(\varphi) \circ \varphi$. Clearly, f is an involutory automorphism of $\mathbf{C}$ and since $f(i) = -i$, we have $f \neq i_{\mathbf{C}}$.

The field $F(f)$ satisfies the equalities:

$$F(f) = \{\omega \in \mathbf{C} : f(\omega)\} = \{\omega \in \mathbf{C} : \sigma(\varphi)(\varphi(\omega)) = \\ = \varphi(\omega)\} = \{\omega \in \mathbf{C} : \varphi(\omega) \in \mathbf{R}\}.$$

Clearly, the restriction $\tilde{\varphi}$ of φ on $F(f)$ is an embedding from $F(f)$ into $\mathbf{R}$ and $\tilde{\varphi}$ is surjective if and only if φ is surjective.

II. Let f be an Archimedian involutory automorphism of $\mathbf{C}$ and let ψ be an embedding of the ordered field $F(f)$ into $\mathbf{R}$.

Suppose $\omega \in \mathbf{C}$. By Theorem 2.5 there exist unique numbers $\alpha, \beta \in F(f)$ such that $\omega = \alpha + i\beta$ and $f(\omega) = \alpha - i\beta$. Put

$$\varphi(\omega) = \psi(\alpha) + i\psi(\beta).$$

Obviously, φ is an isomorphism from $\mathbf{C}$ into $\mathbf{C}$ such that $\varphi(i) = i$. If $\lambda \in \varphi(\mathbf{C})$, then there exists $\delta \in \mathbf{C}$ such that $\varphi(\delta) = \lambda$. Let $\alpha, \beta \in F(f)$, $\delta = \alpha + i\beta$. Setting $\delta' = \alpha - i\beta$, we get $\varphi(\delta') = \psi(\alpha) - i\psi(\beta) = \bar{\lambda}$, therefore φ is a $\varkappa$-isomorphism. It is easy to see that $f = \varphi^{-1} \circ \sigma(\varphi) \circ \varphi$.

III. Let $\varphi, \psi \in \mathcal{K}^+ \cup \mathcal{A}^+$ and let $\varphi^{-1} \circ \sigma(\varphi) \circ \varphi = \psi^{-1} \circ \sigma(\psi) \circ \psi$. Let $K = \varphi(\mathbf{C})$, $L = \psi(\mathbf{C})$, $\pi = \sigma(\varphi) : K \to K$, $\varrho = \sigma(\psi) : L \to L$, $g = \psi \circ \varphi^{-1} : K \to L$. Then according to Lemma 2.1 $\varphi = \psi$.

The theorem is proved.

Remark. In Theorem 4.1 we can replace the requirement $\varphi(i) = i$ by $\varphi(i) = -i$. The mapping $\varphi \to \sigma(\varphi) \circ \varphi$ is namely a bijection from the set of all $\varkappa$-isomorphisms φ of $\mathbf{C}$ into $\mathbf{C}$ with $\varphi(i) = i$ onto the set of all $\varkappa$-isomorphisms ψ of $\mathbf{C}$ into $\mathbf{C}$ with $\psi(i) = -i$.

Notation. Denote by $\mathcal{A}_1, \mathcal{A}_2$ the systems of all Archimedian involutory automorphisms f of $\mathbf{C}$ such that the fields $F(f)$ and $\mathbf{R}$ are isomorphic, the field $F(f)$ is isomorphically embedded into $\mathbf{R}$ but not onto (i.e., the ordered field $F(f)$ contains gaps), respectively.

Using Theorems 3.1 and 4.1 we get

Corollary 4.1 $\operatorname{card} \mathcal{A}_1 = \operatorname{card} \mathcal{A}_2 = \exp\exp \aleph_0$.

Construction 4.1. Let $A = \{a_\iota : \iota \in I\}$ be a transcendente base of the extension $\mathbf{C}/\mathbf{Q}$ and let the set I be linearly ordered: $I = (I, \leq)$. Let us order the polynomial ring $\mathbf{Q}[X] = \mathbf{Q}[X_\iota]_{\iota \in I}$ as follows:

The monomials in $\mathbf{Q}[X]$ are ordered lexicographically; i.e., for monomials

$$\alpha = \prod_{i=1}^{n} X_{\iota_i}^{k_i} \qquad \text{and} \qquad \beta = \prod_{i=1}^{n} X_{\iota_i}^{h_i}$$

(n is a positive integer, $k_1, \dots k_n$, $h_1, \dots, h_n$ are non-negative integers and $\iota_1 < \iota_2 < \cdots < \iota_n$ are elements from I) we have $\alpha \leq \beta$ if $\alpha = \beta$ or $k_m < h_m$, where m is the smallest positive integer $\mu \leq n$ with $k_\mu \neq h_\mu$.

Let $f, g \in \mathbf{Q}[X]$, $f = a_1\alpha_1 + \cdots + a_v\alpha_v$, $g = b_1\alpha_1 + - + b_v\alpha_v$, where v is a positive integer, $\alpha_1 < \alpha_2 < \cdots < \alpha_v$ are monomials in $\mathbf{Q}[X]$ and $a_1, \dots, a_v, b_1, \dots, b_v \in \mathbf{Q}$. Set $f \leq g$ if $f = g$ or $a_w < b_w$, where w is the largest integer $u \leq v$ with $a_u \neq b_u$.

Then $\leq$ is a linear ordering on $\mathbf{Q}[X]$ and $(\mathbf{Q}[X], \leq)$ is a linearly ordered ring. The linear ordering $\leq$ can be extended uniquely on $\mathbf{Q}(X)$ such that $(\mathbf{Q}(X), \leq)$ is an ordered field. The natural isomorphism $(X_\iota \to a_\iota)$ makes from $\mathbf{Q}(A)$ an ordered field $(\mathbf{Q}(A), \leq)$ which is not Archimedian since for each positive integer n and each $\iota \in I$ we have $n < a_\iota$.

According to Theorem 2.3 there exists an algebraic extensionfield $\mathbf{F}$ of $\mathbf{Q}(A)$ which is a maximal ordered field. We can suppose that $\mathbf{F}$ is a subfield of $\mathbf{C}$. Clearly, $\mathbf{F}$ is non-Archimedian. By the Euler-Lagrange theorem (Theorem 2.4) the field $\mathbf{F}(i)$ is algebraically closed. The situation is demonstrated on the diagram:

$$\mathbf{Q} \longrightarrow \mathbf{Q}(A) \longrightarrow \mathbf{F} \longrightarrow \mathbf{F}(i) \longrightarrow \mathbf{C}.$$

If $\alpha \in \mathbf{C} - \mathbf{F}(i)$, then α is transcendental over $\mathbf{F}(i)$, therefore α is transcendental over $\mathbf{Q}(A)$, which is a contradiction. It follows that $\mathbf{F}(i) = \mathbf{C}$.

Put $f(\omega) = \alpha - i\beta$ for $\omega \in \mathbf{C}$, $\omega = \alpha + i\beta$, $\alpha, \beta \in \mathbf{F}$. Therefore *$f$ is a non-Archimedian involutory automorphism of* $\mathbf{C}$ *and the fixed field $F(f)$ of $\{f\}$ equals* $\mathbf{F}$.

Theorem 4.2 *The cardinality of the system of all non-Archimedian involutory automorphisms of* $\mathbf{C}$ *is equal to* $\exp\exp\aleph_0$.

Proof. Consider the automorphism f from Construction 4.1. This automorphism depends on the linear ordering $\leq$ of I. If this ordering is changed, we get a different non-Archimedian involutory automorphism from f. According to Theorem 2.2 card $I = \exp\aleph_0$ and the result follows.

5. Application of algebraically independent numbers to a construction of diagonable matrices

For an application to matrix algebra we rise the following problem:

Problem *Assume that M, N are subsets of* $\mathbf{C}$ *and f is a bijection from M onto N. When can f be extended to an involutory automorphism of* $\mathbf{C}$*?*

We will give only some partial answers to this question, a complete solution is open. The following necessary conditions are obvious.

Proposition 5.1 *Let M, N be subsets of $\mathbf{C}$ and let f be an isomorphism from $\mathbf{C}$ into $\mathbf{C}$ such that $f(M) = N$.*

(a) *If $\alpha \in M$, then α is an algebraic number if and only if $f(\alpha)$ is an algebraic number. In this case α and $f(\alpha)$ possess the same minimal polynomial.*

(b) *A subset $T \subseteq M$ is algebraically independent if and only if $f(T)$ is algebraically independent.*

Lemma 5.1 *Suppose that U, V, W are mutually disjoin sets of real numbers and χ is a bijection from U onto V. If the set $U \cup V \cup W$ is algebraically independent, then the set*

$$\{\alpha + i\chi(\alpha) : \alpha \in U\} \cup \{\alpha - i\chi(\alpha) : \alpha \in U\} \cup W$$

is algebraically independent.

Proof. Assume that there exist positive integers n, m, different elements $\alpha_1, \ldots, \alpha_n \in U$, $\gamma_1, \ldots, \gamma_m \in W$ and a polynomial $F = F(X_1, \ldots, X_n, Y_1, \ldots, Y_n, Z_1, \ldots, Z_m)$ over $\mathbf{Q}$ such that

$$F(\varphi_1, \ldots, \varphi_n, \psi_1, \ldots, \psi_n, \gamma_1, \ldots, \gamma_m) = 0,$$

where $\varphi_j = \alpha_j + i\chi(\alpha_j)$ and $\psi_j = \alpha_j - i\chi(\alpha_j)$ for $1 \leq j \leq n$. Substituting for $X_j = U_j + iV_j$, $Y_j = U_j - iV_j$ $(1 \leq j \leq n)$ in F we get a polynomial $G = G(U_1, \ldots, U_n, V_1, \ldots, V_n, Z_1, \ldots, Z_m)$ over $\mathbf{Q}(i)$.

Since the set $U \cup V \cup W$ is algebraically independent and $G(\alpha_1, \ldots, \alpha_n, \chi(\alpha_1), \ldots, \chi(\alpha_n), \gamma_1, \ldots, \gamma_m) = 0$, we have $G = 0$, therefore $G(U_1, \ldots, U_n, V_1, \ldots, V_n, Z_1, \ldots, Z_m) = 0$ for all complex numbers $U_1, \ldots, U_n, V_1, \ldots, V_n, Z_1, \ldots, Z_m$. Consequently, $F = 0$ and we are done.

Theorem 5.1 *Let A, B, C be mutually disjoint subsets of $\mathbf{C}$ such that the set $A \cup B \cup C$ is algebraically independent, and let there exist a bijection χ from A onto B. Then there exists an involutory automorphism h of $\mathbf{C}$ such that*

$$\alpha \in A \implies h(\alpha) = \chi(\alpha),$$
$$\gamma \in C \implies h(\gamma) = \gamma.$$

Proof. Since the transcendence degree of $\mathbf{R}/\mathbf{Q}$ equals $\exp \aleph_0$ (Theorem 2.2), there exist mutually disjoint subsets U, V, W, Z of $\mathbf{R}$ such that $\operatorname{card} A = \operatorname{card} B = \operatorname{card} U = \operatorname{card} V$, $\operatorname{card} W = \operatorname{card} C$, $\operatorname{card} Z = \exp \aleph_0$ and the set $U \cup V \cup W \cup Z$ is algebraically independent. Let $\varphi : U \to V$, $\psi : A \to U$, $\omega : C \to W$ be bijections. According to Lemma 5.1 the set

$$N = \{\xi + i\varphi(\xi) : \xi \in U\} \cup \{\xi - i\varphi(\xi) : \xi \in U\} \cup W \cup Z$$

is algebraically independent and clearly $\operatorname{card} N = \exp \aleph_0$. There exists a subset $D \subseteq \mathbf{C} - A \cup B \cup C$ such that $M = A \cup B \cup C \cup D$ is a transcendence base of

$\mathbf{C}/\mathbf{Q}$ and there exists an injective mapping g from M into N with the following property:

$$\begin{aligned}
&\alpha \in A \implies g(\alpha) = \psi(\alpha) + i\varphi\psi(\alpha),\\
&b \in B \implies g(\beta) = \sigma g \chi^{-1}(\beta),\\
&\gamma \in C \implies g(\gamma) = \omega(\gamma),\\
&\delta \in D \implies g(\delta) \in Z.
\end{aligned}$$

Using Construction 3.1 ($M = A$, $g(M) = B$) we get a $\varkappa$-isomorphism f from $\mathbf{C}$ into $\mathbf{C}$ (by Proposition 3.3) with $f(\mu) = g(\mu)$ for each $\mu \in M$. Put $h = f^{-1} \circ \sigma(f) \circ f$. Then h is an involutory automorphism of $\mathbf{C}$. For $a \in A$ we have $h(\alpha) = f^{-1}(\psi(\alpha) - i\varphi\psi(\alpha))$ and $f\chi(\alpha) = g\chi(\alpha) = \sigma g \chi^{-1}\chi(\alpha) = \sigma g(\alpha) = \psi(\alpha) - i\varphi\psi(\alpha)$, hence $h(\alpha) = \chi(\alpha)$. For $\gamma \in C$ we get $h(\gamma) = (f^{-1}\sigma(f))g(\gamma) = f^{-1}\omega(\gamma) = f^{-1}g(\gamma) = \gamma$. The proof is complete.

For the further theorem we will need two lemmas.

Lemma 5.2 *Let $n \geq 2$ be an integer, $\xi = \cos\frac{\pi}{2^{n-1}} + i\sin\frac{\pi}{2^{n-1}}$ (a primitive 2^nth root of unity) and let f be an involutory automorphism of $\mathbf{C}$, $f \neq i_{\mathbf{C}}$. Then $f(\xi) = \bar{\xi} = \xi^{-1}$.*

Proof. We will use induction on n. If $n = 2$, then $\xi = i$ and by Theorem 2.5 (a) $f(\xi) = -i = \bar{\xi}$. Suppose that $n \geq 3$ and for $n-1$ the statement is true. By noting that $f(\xi)^2 = f(\xi^2) = \xi^{-2}$ we have $f(\xi) = \pm\xi^{-1}$. Suppose $f(\xi) = -\xi^{-1}$. According to Theorem 2.5 (b), (c), $\xi = \alpha + i\beta$, where $\alpha, \beta \in F(f)$ and $f(\xi) = \alpha - i\beta$. Consequently,

$$-1 = \xi f(\xi) = \alpha^2 + \beta^2 > 0,$$

which is a contradiction.

Lemma 5.3 *Let p be an odd prime, n a positive integer, $\xi = \cos\frac{2\pi}{p^n} + i\sin\frac{2\pi}{p^n}$ (a primitive p^nth root of unity) and let f be an involutory automorphism of $\mathbf{C}$, $f \neq i_{\mathbf{C}}$. Then $f(\xi) = \bar{\xi} = \xi^{-1}$.*

Proof. Since $\xi^{p^n} = 1$, there exists an integer x, $1 \leq x \leq p^n - 1$, $p \nmid x$ such that $f(\xi) = \xi^x$. Then $\xi = f^2(\xi) = \xi^{x^2}$, therefore $x^2 \equiv 1 \pmod{p^n}$ and $x = 1$ or $x = p^n - 1$.

Suppose $f(\xi) = \xi$. Then $\xi \in F(f)$ and $\xi < 0$ or $0 < \xi < 1$ or $1 < \xi$, which is a contradiction to $\xi^{p^n} = 1$. The result follows.

Definition 5.1. We call an algebraic number α *abelian* if the extension $K/\mathbf{Q}$ is abelian, where K is the splitting field of the minimal polynomial of α. (Remind that an extension $K/\mathbf{Q}$ is called abelian if $K/\mathbf{Q}$ is a Galois extension and the Galois group of $K/\mathbf{Q}$ is abelian.)

Theorem 5.2 *For any involutory automorphism f of $\mathbf{C}$, $f \neq i_{\mathbf{C}}$ and any abelian algebraic number α we have $f(\alpha) = \bar{\alpha}$.*

Proof. Let K be a subfield of $\mathbf{C}$ which is the splitting field of the minimal polynomial of α. Since the extension $K/\mathbf{Q}$ is abelian, there exists according to the Kronecker-Weber Theorem ([W], Chapter 14) an integer $m \geq 3$ such that the mth cyclotomic field $\mathbf{Q}(\xi)$ $\left(\xi = \cos\frac{2\pi}{m} + i\sin\frac{2\pi}{m}\right)$ contains K.

Let $m = p_1^{a_1} \dots p_k^{a_k}$ be the canonical decomposition of m. We can suppose that in case m being even, m is divisible by 4. For each $1 \leq j \leq k$ set

$$m_j = \frac{m}{p^{a_j}}, \ \eta_j = \xi^{m_j} = \cos\frac{2\pi}{p_j^{a_j}} + i\sin\frac{2\pi}{p_j^{a_j}}.$$

Since $\xi^m = 1$, there exists an integer x, $1 \leq x \leq m-1$ such that $f(\xi) = \xi^x$. Then for each $1 \leq j \leq k$ we have according to Lemmas 5.2 and 5.3

$$\xi^{-m_j} = \eta_j^{-1} = f(\eta_j) = \xi^{xm_j}$$

and therefore $xm_j \equiv -m_j \pmod{m}$. It follows that $x \equiv -1 \pmod{p_j^{a_j}}$ for each $1 \leq j \leq k$, hence $x \equiv -1 \pmod{m}$ and thus $x = m-1$. The result follows immediately by noting that

$$\alpha = \sum\nolimits_{(\nu,m)=1}^{=1} a_\nu \xi^\nu \qquad (a_\nu \in \mathbf{Q}).$$

Remark. Using the Kronecker-Weber Theorem we can easily show that *a complex number is abelian algebraic number if and only if it is contained in a cyclotomic field.*

Now we will consider the matrices with complex entries and we will use this theory for regular matrices ([Se], Chapter 11, Section 5 for matrices with real entries). Recall that a square matrix A of order n is called *regular* or *diagonable* if there exists a non-singular matrix U of order n such that $U^{-1}AU = D = \operatorname{diag}\{\lambda_1, \dots, \lambda_n\}$. Then $\lambda_1, \dots, \lambda_n$ are eigenvalues of A. It is well-known that *a square matrix is regular if and only if its Jordan normal form is a diagonal matrix* (Jordan blocks are square matrices of order 1).

Another characterization is formulated by means of the concept of regular eigenvalue. If A is a square matrix of order n and λ is an eigenvalue of A with multiplicity m, then λ is called a *regular eigenvalue of* A if rank of $A - \lambda I_n$ equals $n - m$. *The matrix A is regular if and only if each its eigenvalue is regular.*

The symmetric matrices (with real entries) are regular and the Hermitian matrices as well. Also the families of idempotent matrices and circulant matrices belong to the diagonable matrices ([Se], Chapter 12, Section 2; [D], Theorem 3.2.2). Also the square matrices with simple eigenvalues are regular. In the paper [Sk] another class of the regular matrices was described. Recall the basic notions:

Definition 5.2. Let f be an involutory automorphism of $\mathbf{C}$ and let $A = [a_{ij}]$ be a matrix of size $m \times n$. Put

$$A^f = [b_{kl}]_{1 \leq k \leq n, 1 \leq \ell \leq m},$$

where $b_{kl} = f(a_{\ell k})$ $(1 \leq k \leq n, 1 \leq \ell \leq m)$.

A matrix M is called *f-Hermitian* if $M^f = M$. Obviously, the f-Hermitian matrices are square matrices. A non-singular matrix U is said to be *f-unitary* if $U^{-1} = U^f$.

It was stated in ([Sk], Theorem 3.5):

Theorem 5.3 *Let f be an involutory automorphism of* $\mathbf{C}$, $f \neq i_{\mathbf{C}}$. *A square matrix H of order n is f-Hermitian if and only if there exists an f-unitary matrix U of order n such that*

$$H = U^f D U,$$

where D is a diagonal, f-Hermitian matrix of order n. Therefore, the *f-Hermitian matrices are regular.*

Using Theorems 5.1 and 5.2 we are able to construct some f-Hermitian matrices as follows. It is not difficult to determine some abelian algebraic numbers, e.g., $\sqrt{2}$, $i\sqrt[3]{3}$, $\xi = e^{\frac{2\pi i}{5}}$, etc. The application of Theorem 5.1 requests some criteria on algebraically independent numbers. One of the most beautiful criterion is due to *Lindemann* ([Sh], Chapter 2, §7):

Theorem 5.4 (Lindemann) *If $\xi_1, \ldots, \xi_k$ (k a positive integer) are algebraic numbers linearly independent over* $\mathbf{Q}$, *then the numbers*

$$e^{\xi_1}, \ldots, e^{\xi_k}$$

are algebraically independent.

The reader is referred to ([Sh], Chapter 3 or [Bu]) for other criteria on algebraically independent numbers.

Example. The numbers $\sqrt{7}$, $\sqrt[3]{5}$, $i\sqrt{2}$, $i\sqrt[5]{3}$ are linearly independent over $\mathbf{Q}$ and the numbers $e^{\frac{2\pi i}{7}}$, $\sqrt[4]{2}$, $\sqrt{7}$ are abelian algebraic numbers. Then according to Theorems 5.1, 5.2 and 5.4 there exists an involutory automorphism f of $\mathbf{C}$, $f \neq i_{\mathbf{C}}$ such that the matrix

$$M = \begin{bmatrix} e^{\sqrt[3]{5}} & e^{\frac{2\pi i}{7}} & e^{i\sqrt{2}} \\ e^{-\frac{2\pi i}{7}} & \sqrt[4]{2} & \sqrt{7} \\ e^{\sqrt{7}} & \sqrt{7} & e^{i\sqrt[5]{3}} \end{bmatrix}$$

is f-Hermitian and hence by Theorem 5.3 M is diagonable. Using MATLAB system we get

$$M = \begin{bmatrix} 5.5288 & 0.6235 + 0.7818i & 0.1559 + 0.9878i \\ 0.6235 - 0.7818i & 1.1892 & 2.6458 \\ 14.0940 & 2.6458 & 0.3194 + 0.9476i \end{bmatrix}$$

with simple eigenvalues $\lambda_1 = 7.4734 + 2.2135i$, $\lambda_2 = -1.5116 + 0.3697i$, $\lambda_3 = 1.0756 - 1.6356i$.

References

[Bb] N. Bourbaki, *Algèbre*, Chap. IV-VI, Paris, 1952.

[Bu] P. Bundschuh *A criterion for algebraic independence with some applications.* Osaka J. Math. 25 (1988), 849-858.

[D] B. J. Davis *Circulant Matrices.* New York, 1979.

[F] L. Fuchs *Partially Ordered Algebraic Systems.* Oxford-London-New York-Paris, 1963.

[N] W. K. Nicholson *Introduction to Abstract Algebra.* Boston, 1993.

[Se] S. R. Searle *Matrix Algebra Useful for Statistics.* New York, 1982.

[Sh] A. B. Shidlovskiy *Transcendentnye chisla.* Moskva, 1987 (Russian).

[Sk] L. Skula *Involutions for matrices and general inverses.* Linear Algebra and its Applications, 271(1998), 283-308.

[W] L. C. Washington *Introduction to Cyclotomic Fields.* Springer-Verlag, New York, Inc., 1982.

Author(s) Address(es):
Department of Applied Mathematics, Faculty of Science, Masaryk University,
662 95 Brno, Janáčkovo nám. 2a, Czech Republic

E-mail address: skula@math.muni.cz