

Hiroyuki Ishibashi

Involutions and semiinvolutions

Czechoslovak Mathematical Journal, Vol. 56 (2006), No. 2, 533–541

Persistent URL: <http://dml.cz/dmlcz/128084>

Terms of use:

© Institute of Mathematics AS CR, 2006

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

INVOLUTIONS AND SEMIINVOLUTIONS

HIROYUKI ISHIBASHI, Sakado

(Received September 26, 2003)

Abstract. We define a linear map called a semiinvolution as a generalization of an involution, and show that any nilpotent linear endomorphism is a product of an involution and a semiinvolution. We also give a new proof for Djocović's theorem on a product of two involutions.

Keywords: classical groups, vector spaces and linear maps, involutions, factorization of a linear map into a product of simple ones

MSC 2000: 15A04, 15A23, 15A33

1. INTRODUCTION

Let V be an n -dimensional vector space over a field k of any characteristic. The k -algebra of k -linear endomorphisms of V is denoted by $\text{End}_k V$, and the unit group of $\text{End}_k V$ is $\text{Aut}_k V$. An element $\xi \in \text{Aut}_k V$ is called an involution if $\xi^2 = 1$, and two elements $\eta, \eta' \in \text{End}_k V$ are said to be similar if $\eta' = \varrho\eta\varrho^{-1}$ for some $\varrho \in \text{Aut}_k V$. An element $\sigma \in \text{End}_k V$ is nilpotent if $\sigma^n = 0$ for some integer $n \geq 1$.

Suppose that V is a direct sum of two subspaces, say, $V = L \oplus M$. Then we shall call a linear map $\sigma = 0_L \oplus \varrho \in \text{End}_k V$ a semiinvolution if $0_L \in \text{End}_k L$ is the zero map on L and $\varrho \in \text{Aut}_k M$ is an involution on M . In case that L is spanned by a subset $S \subseteq V$, we may write 0_S for 0_L . Also 1_L or $1_S \in \text{Aut}_k L$ denotes the identity map on L .

Let H be a subspace of V having a basis $Z = \{x_1, x_2, \dots, x_m, y_m, \dots, y_2, y_1\}$ of an even number of elements. Then an involution $\Delta_Z \in \text{Aut}_k H$ is defined by

$$x_1 \rightleftarrows y_1, x_2 \rightleftarrows y_2, \dots, x_m \rightleftarrows y_m.$$

We shall call Δ_Z the transpose of Z or H . Our purpose is to prove the following two theorems, Theorems A and B.

Theorem A. For $\sigma \in \text{End}_k V$, the following (a) and (b) are equivalent:

- (a) σ is nilpotent.
 (b) $\sigma = \theta\tau$ for an involution $\tau = 1_{Z_1} \oplus \Delta_{Z_2}$ and a semiinvolution $\theta = 0_{Z'_0} \oplus 1_{Z'_1} \oplus \Delta_{Z'_2}$, where $\{Z_1, Z_2\}$ and $\{Z'_0, Z'_1, Z'_2\}$ are two bases for V which satisfy the following condition (C):
 (C) Z_1 and Z_2 are expressed as

$$Z_1 = \{x_{10}, x_{20}, \dots, x_{r0}\},$$

$$Z_2 = \{X_{r+s}, \dots, X_{r+1}, X_r, \dots, X_2, X_1, Y_1, Y_2, \dots, Y_r, Y_{r+1}, \dots, Y_{r+s}\}$$

for $X_i = \{x_{im_i}, \dots, x_{i2}, x_{i1}\}$, $Y_i = \{y_{i1}, y_{i2}, \dots, y_{im_i}\}$ and $1 \leq i \leq r+s$, and for which Z'_0, Z'_1, Z'_2 are expressed as

- (i) $Z'_0 = \{x_{im_i} : 1 \leq i \leq r+s\}$,
 i.e., the first elements of X_{r+s}, \dots, X_2, X_1 ,
 (ii) $Z'_1 = \{y_{i1} : r+1 \leq i \leq r+s\}$,
 i.e., the first elements of $Y_{r+1}, Y_{r+2}, \dots, Y_{r+s}$,

and

- (iii) $Z'_2 = \{X'_{r+s}, \dots, X'_{r+1}, X'_r, \dots, X'_2, X'_1, Y'_1, Y'_2, \dots, Y'_r, Y'_{r+1}, \dots, Y'_{r+s}\}$

for

$$X'_i = \begin{cases} \{x_{i(m_i-1)}, \dots, x_{i1}, x_{i0}\} & \text{if } 1 \leq i \leq r, \\ \{x_{i(m_i-1)}, \dots, x_{i1}\} & \text{if } r+1 \leq i \leq r+s, \end{cases}$$

and

$$Y'_i = \begin{cases} \{y_{i1}, y_{i2}, \dots, y_{im_i}\} & \text{if } 1 \leq i \leq r, \\ \{y_{i2}, y_{i3}, \dots, y_{im_i}\} & \text{if } r+1 \leq i \leq r+s. \end{cases}$$

Remark 1. Write $n_i = 2m_i + 1$ for $1 \leq i \leq r$ and $n_i = 2m_i$ for $r+1 \leq i \leq r+s$. By a rearrangement of $\{m_i\}$ we may assume that $n_1 \geq n_2 \geq \dots \geq n_t$ for $t = r+s$. Then, by the definition of τ_i and θ_i in the proof for Theorem A, we shall see that $\{n_i\}$ are the invariants of σ . Thus, the involution τ and the semiinvolution θ in Theorem A are unique for σ up to similarity. Further, as we see in Theorem A, the relationship between τ and θ is given by the condition (C), more precisely τ determines θ .

where

$$\sigma_i = \sigma|_{V_i} \in \text{End}_k V_i$$

(see for example Herstein [5, Theorem 6.5.1]).

By the above result, for $1 \leq i \leq t$, if we define $\tau_i, \theta_i \in \text{End}_k V_i$ by

$$(1) \quad \tau_i: v_{ij} \rightarrow v_{i(n_i-j+1)} \quad \text{for } 1 \leq j \leq n_i,$$

and

$$(2) \quad \theta_i = v_{i1} \rightarrow 0 \quad \text{and} \quad v_{ij} \rightarrow v_{i(n_i-j+2)} \quad \text{for } 2 \leq j \leq n_i,$$

we have

$$(3) \quad \sigma_i = \theta_i \tau_i \quad \text{for } 1 \leq i \leq t,$$

and so

$$(4) \quad \sigma = \theta_1 \tau_1 \oplus \theta_2 \tau_2 \oplus \dots \oplus \theta_t \tau_t = (\theta_1 \oplus \theta_2 \oplus \dots \oplus \theta_t)(\tau_1 \oplus \tau_2 \oplus \dots \oplus \tau_t).$$

To construct an involution τ and a semiinvolution θ as in the theorem, we will rearrange the basis elements $\{v_{ij}\}$ for V . To do so we will renumber the suffixes of the subspaces $\{V_1, V_2, \dots, V_t\}$ so that their dimensions $\{n_1, n_2, \dots, n_r\}$ are all odd numbers with $n_1 \geq n_2 \geq \dots \geq n_r$, and $\{n_{r+1}, n_{r+2}, \dots, n_{r+s}\}$ are all even with $n_{r+1} \geq n_{r+2} \geq \dots \geq n_{r+s}$ and $t = r + s$. Moreover, we rewrite the basis elements in $S_i = \{v_{i1}, v_{i2}, \dots, v_{in_i}\}$ for V_i as

$$(5) \quad S_i = \begin{cases} \{x_{im_i}, \dots, x_{i2}, x_{i1}, x_{i0}, y_{i1}, y_{i2}, \dots, y_{im_i}\} & \text{for } 1 \leq i \leq r, \\ \{x_{im_i}, \dots, x_{i2}, x_{i1}, y_{i1}, y_{i2}, \dots, y_{im_i}\} & \text{for } r+1 \leq i \leq r+s, \end{cases}$$

where $n_i = 2m_i + 1$ for $1 \leq i \leq r$, and $2m_i$ for $r+1 \leq i \leq r+s$.

This is equivalent to saying that for $1 \leq i \leq r+s$, setting

$$X_i = \{x_{im_i}, \dots, x_{i2}, x_{i1}\} \quad \text{and} \quad Y_i = \{y_{i1}, y_{i2}, \dots, y_{im_i}\},$$

we then have

$$S_i = \{X_i, x_{i0}, Y_i\} \quad \text{for } 1 \leq i \leq r, \quad \text{and} \quad S_i = \{X_i, Y_i\} \quad \text{for } r+1 \leq i \leq r+s.$$

Hence, if we define

$$\begin{aligned} Z_1 &= \{x_{10}, x_{20}, \dots, x_{r0}\}, \\ Z_2 &= \{X_{r+s}, \dots, X_{r+1}, X_r, \dots, X_1, Y_1, \dots, Y_r, Y_{r+1}, \dots, Y_{r+s}\}, \end{aligned}$$

and

$$\tau = 1_{Z_1} \oplus \Delta_{Z_2},$$

then by (1) we find that

$$(7) \quad \tau = \tau_1 \oplus \tau_2 \oplus \dots \oplus \tau_t.$$

Similarly, setting

$$X'_i = \{x_{i(m_i-1)}, \dots, x_{i0}\}, \quad Y'_i = \{y_{i1}, \dots, y_{im_i}\} \quad \text{for } 1 \leq i \leq r,$$

and

$$X'_i = \{x_{i(m_i-1)}, \dots, x_{i1}\}, \quad Y'_i = \{y_{i2}, \dots, y_{im_i}\} \quad \text{for } r+1 \leq i \leq r+s,$$

we get

$$S_i = \{x_{im_i}, X'_i, Y'_i\} \quad \text{for } 1 \leq i \leq r, \quad \text{and} \quad \{x_{im_i}, X'_i, y_{i1}, Y'_i\} \quad \text{for } r+1 \leq i \leq r+s.$$

Therefore, if we define

$$\begin{aligned} Z'_0 &= \{x_{1m_1}, x_{2m_2}, \dots, x_{(r+s)m_{(r+s)}}\}, \\ Z'_1 &= \{y_{(r+1)1}, y_{(r+2)1}, \dots, y_{(r+s)1}\}, \\ Z'_2 &= \{X'_{r+s}, \dots, X'_{r+1}, X'_r, \dots, X'_1, Y'_1, \dots, Y'_r, Y'_{r+1}, \dots, Y'_{r+s}\}, \end{aligned}$$

and

$$(8) \quad \theta = 0_{Z'_0} \oplus 1_{Z'_1} \oplus \Delta_{Z'_2},$$

we have

$$(9) \quad \theta = \theta_1 \oplus \theta_2 \oplus \dots \oplus \theta_t.$$

This shows that $\sigma = \theta\tau$ by (4), which gives us (b).

3. PROOF OF THEOREM B

If $\sigma = \tau\theta$ with $\tau^2 = \theta^2 = 1$, then $\sigma^{-1} = \theta\tau = \theta\tau\theta\theta^{-1} = \theta\sigma\theta^{-1}$ is similar to σ . So, all what we have to do is to show the converse.

Let $k[x]$ be the polynomial ring in x over k . Then, since the correspondence

$$\pi_\sigma: k[x] \longrightarrow \text{End}_k V$$

defined by $\pi_\sigma(f(x))(v) = f(\sigma)(v)$ for $v \in V$ and $f(x) \in k[x]$ is a ring homomorphism, if we define $f(x)v = f(\sigma)(v)$, V is endowed a module structure over the principal ideal domain $k[x]$. In particular, since $\dim V < \infty$, V is a finitely generated torsion $k[x]$ -module. Therefore by [10, XIV, Theorem 2.1, p. 557] there is a finite number of monic polynomials $f_1(x), f_2(x), \dots, f_n(x)$ in $k[x]$ such that

$$V \simeq k[x]/(f_1(x)) \oplus \dots \oplus k[x]/(f_n(x)) \quad \text{with} \quad f_1 \mid \dots \mid f_n$$

as $k[x]$ -modules. Further the sequence of ideals $(f_1), \dots, (f_n)$ is an invariant for V and π_σ , which is called the system of invariants.

Since $k[x]/(f_i(x)) = k[x](1 + (f_i(x)))$ is a cyclic $k[x]$ -submodule generated by one element $1 + (f_i(x))$, if we write

$$(1) \quad f_i(x) = a_{i0} + a_{i1}x + \dots + a_{i(m_i-1)}x^{m_i-1} + x^{m_i}, \quad a_{ij} \in k,$$

for $i = 1, 2, \dots, n$, we will find n elements $v_1, v_2, \dots, v_n \in V$ which satisfy for $i = 1, 2, \dots, n$,

- (i) $V = V_1 \oplus V_2 \oplus \dots \oplus V_n$ where $V_i = kv_i \oplus k\sigma v_i \oplus \dots \oplus k\sigma^{m_i-1}v_i \simeq k[x]/(f_i(x))$,
- (ii) $\sigma = \sigma_1 \oplus \sigma_2 \oplus \dots \oplus \sigma_n$, $\sigma_i = \sigma|_{V_i}$, and
- (iii) $f_i(x)$ is the minimal polynomial of σ_i .

Here we note that $\sigma_i \in \text{Aut}_k V_i$, or equivalently $a_{i0} \neq 0$, since $\sigma \in \text{Aut}_k V$. This implies that for $i = 1, 2, \dots, n$

$$V_i = (\sigma_i^{-1})^{m_i-1}V_i = kv_i \oplus k\sigma_i^{-1}v_i \oplus \dots \oplus k(\sigma_i^{-1})^{m_i-1}v_i, \\ \sigma^{-1} = \sigma_1^{-1} \oplus \sigma_2^{-1} \oplus \dots \oplus \sigma_n^{-1}$$

and

$$(2) \quad g_i(x) = a_{i0}^{-1}x^{m_i}f_i(x^{-1}) \\ = a_{i0}^{-1} + a_{i0}^{-1}a_{i(m_i-1)}x + \dots + a_{i0}^{-1}a_{i1}x^{m_i-1} + x^{m_i}$$

is the minimal polynomial of σ_i^{-1} . Accordingly if we give V another $k[x]$ -module structure by a ring homomorphism

$$\pi_{\sigma^{-1}}: k[x] \longrightarrow \text{End}_k V \quad \text{defined by} \quad \pi_{\sigma^{-1}}(f(x))(v) = f(\sigma^{-1})(v)$$

and write it V' for V , we have

$$V' \simeq k[x]/(g_1(x)) \oplus \dots \oplus k[x]/(g_n(x)) \quad \text{with} \quad g_1 \mid \dots \mid g_n.$$

As for $g_i \mid g_{i+1}$, since $f_i \mid f_{i+1}$, if we set $f_{i+1} = f_i h_i$ with $m_i = \dim f_i$ and $r_i = \dim h_i$, we get $g_{i+1}(x) = g_i(x)q_i(x)$ for $q_i(x) = h_i(0)^{-1}x_i^{r_i}h_i(x^{-1}) \in k[x]$. Hence $g_1 \mid \dots \mid g_n$.

On the other hand, since σ and σ^{-1} are similar, we have $\sigma^{-1} = \varrho\sigma\varrho^{-1}$ for some $\varrho \in \text{Aut}_k V$. Hence $\varrho\pi_\sigma(f(x))(v) = \varrho f(\sigma)(v) = \pi_{\sigma^{-1}}(f(x))\varrho(v)$, since $\sigma^{-1}\varrho = \varrho\sigma$. This shows that ϱ is a $k[x]$ -module isomorphism of V to V' . Therefore the uniqueness of the system of invariants gives us $(f_i) = (g_i)$ and so $f_i = g_i$, since they are monic. Thus (1), (2) imply that

$$(3) \quad a_{i0} = a_{i0}^{-1}, \quad a_{ij} = a_{i0}^{-1}a_{i(m_i-j)} \quad \text{for } j = 1, 2, \dots, m_i - 1.$$

Now for $i = 1, 2, \dots, n$, we define $\tau_i, \theta_i \in \text{Aut}_k V_i$ by

$$\begin{aligned} \tau_i: \sigma_i^j v_i &\longrightarrow \sigma_i^{m_i-j-1} v_i & \text{for } 0 \leq j \leq m_i - 1, \\ \theta_i: \sigma_i^j v_i &\longrightarrow \sigma_i^{m_i-j} v_i & \text{for } 0 \leq j \leq m_i - 1. \end{aligned}$$

Then, for $i = 1, 2, \dots, n$, we have

$$\sigma_i = \theta_i \tau_i \quad \text{and} \quad \tau_i^2 = 1 \text{ on } V_i, \quad \text{and} \quad \theta_i^2 = 1 \text{ on } \{\sigma_i v_i, \dots, \sigma_i^{m_i-1} v_i\}.$$

However, using (3), an easy calculation gives us $\theta_i^2 v_i = v_i$ and so $\theta_i^2 = 1$ on V_i .

Thus, setting

$$\tau = \bigoplus_{i=1}^n \tau_i \quad \text{and} \quad \theta = \bigoplus_{i=1}^n \theta_i,$$

we obtain $\sigma = \tau\theta$ and $\tau^2 = \theta^2 = 1$, which completes the proof of Theorem B.

References

- [1] *D. Ž. Djocović*: Product of two involutions. Arch. Math. XVIII (1967), 582–584. [Zbl 0153.35502](#)
- [2] *E. W. Ellers, H. Ishibashi*: Bireflectionality of the orthogonal group over a valuation domain. J. Algebra 149 (1992), 322–325. [Zbl 0779.20028](#)
- [3] *W. H. Gustafson, P. R. Halmos, and H. Radjavi*: Products of involutions. Linear Algebra Appl. 13 (1976), 157–162. [Zbl 0325.15009](#)
- [4] *A. J. Hahn, O. T. O’Meara*: The Classical Groups and K-Theory. Springer-Verlag, Berlin-Tokyo, 1989. [Zbl 0683.20033](#)
- [5] *R. Henstock*: The General Theory of Integration. Clarendon Press, Oxford, 1991. [Zbl 0745.26006](#)
- [6] *I. N. Herstein*: Topics in Algebra (2nd ed.). John Wiley and Sons, New York, 1964. [Zbl 0122.01301](#)
- [7] *H. Ishibashi*: Decomposition of isometries of $U_n(V)$ over finite fields into simple isometries. Czechoslovak Math. J. 31 (1981), 301–305. [Zbl 0464.20032](#)
- [8] *H. Ishibashi*: Involuntary expressions for elements in $GL_n(Z)$ and $SL_n(Z)$. Linear Algebra Appl. 219 (1995), 165–177. [Zbl 0823.20048](#)
- [9] *H. Ishibashi*: Groups generated by symplectic transvections over local rings. J. Algebra 218 (1999), 26–80. [Zbl 0984.20031](#)
- [10] *T. J. Laffey*: Products of matrices. In: Generators and Relations in Groups and Geometries. Proc. NATO ASI (C) (A. Barlotti et al., eds.). Kluwer Academic, Dordrecht-London, 1991, pp. 95–123. [Zbl 0729.15012](#)
- [11] *S. Lang*: Algebra (3rd ed.). Addison Wesley, Tokyo, 1993. [Zbl 0848.13001](#)
- [12] *A. R. Sourour*: A factorization theorem for matrices. Linear Multilinear Alg. 19 (1986), 141–147. [Zbl 0591.15008](#)
- [13] *B. Zheng*: Decomposition of matrices into commutators of involutions. Linear Algebra Appl. 347 (2002), 1–7. [Zbl 1004.20026](#)

Author’s address: H. Ishibashi, Department of Mathematics, Josai University, Sakado, Saitama 350-02, Japan, e-mail: hishi@math.josai.ac.jp.