International Journal of Pure and Applied Mathematics
Volume 41 No. 4 2007, 499-504

FACTORIZATION OF ELEMENTS IN CLASSICAL GROUPS INTO A PRODUCT OF INVOLUTIONS

Hiroyuki Ishibashi
Department of Mathematics
Josai University
1-1 Keyakidai, Sakado, Saitama, 350-0295, JAPAN
e-mail: hishi@math.josai.ac.jp

Abstract: An element τ in an algebraic system is called an involution if $\tau^2 = 1$. Our interest is to factorize elements in various algebraic systems into a product of as small number of involutions as possible.

In this direction we present Djocović's two involution theorem for linear automorphisms, which he proved by using elementary divisors, whereas we will do it by using system of invariants of a finitely generated module over a principal ideal domain. As a result the proof will become rather simpler.

Also we shall introduce without proof some results on factorizations of elements in some classical groups into a product of involutions.

AMS Subject Classification: 15A04, 15A23, 15A33
Key Words: involution, structure theorem of modules over PID, factorization of linear maps and matrices

1. Introduction

We discuss products of involutions in classical groups. Let x be an element in a semigroup G. Then, x is called an involution if its order is two, i.e., $x \neq 1$ and $x^2 = 1$.

We can find many involutions in various algebraic system. In the following examples each x is an involution in each group G.

(1) $G = \mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$, the ring of rational integers and $x = -1$.

(2) $G = S_n$, the symmetric group of degree n and $x = (a\ b)$, a transposition.

Received: September 28, 2007

(3) $G = \mathrm{GL}_n(R)$, the general linear group of degree n over a ring R and

$$x = \begin{pmatrix} \varepsilon_1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon_n \end{pmatrix}$$

with $\varepsilon_i^2 = 1$ for $i = 1, 2, \cdots, n$.

(4) $G = \mathrm{Aut}_R(M)$ with $M = L \oplus N$, the automorphism group on a module M which is split into a direct sum of two submodule L, N over R, and

$$x = 1_L \oplus (-1)_N.$$

2. Theorems

The problem of factorizing an element into a product of involutions has been treated by many mathematicians and we have rich of results.

However, since our purpose is to introduce a proof for Theorem 2, we will quote just a few of them stated in the following theorems.

Theorem 1. *Let S_n be the symmetric group of degree n. Then any σ in S_n is a product of two involutions, that is, there are τ, θ in S_n such that*

$$\sigma = \theta\tau \quad \textit{with} \quad \theta^2 = \tau^2 = 1.$$

Proof. This is well known and the proof will be left to the reader. □

Theorem 2. *Let F be a field, M a vector space of dimension n over F, and $GL_n(M)$ the general linear group on M.*

Then, for any σ in $GL_n(M)$ the following are equivalent:

(a) $\sigma \sim \sigma^{-1}$.

(b) σ is a product of two involutions, i.e., there are θ, τ in $GL_n(M)$ such that

$$\sigma = \theta\tau \quad \textit{with} \quad \theta^2 = \tau^2 = 1.$$

Proof. See Djoković [1]. □

Theorem 3. *Let $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ be the ring of rational integers, M a free module of rank n over $\mathbb{Z}$, and $GL_n(M)$ the general linear group and $SL_n(M)$ the special linear group. Then:*

(a) if $\sigma \in GL_n(M)$, σ is a product of $3n + 9$ involutions in $GL_n(M)$ and

(b) if $\sigma \in SL_n(M)$, σ is a product of $3n+11$ involutions in $SL_n(M)$.

Proof. See Ishibashi [4]. □

Theorem 4. *Let F be a field, M a free module over F of rank n equiped a symmetric bilinear form $B : M \times M \longrightarrow F$, $GL_n(M)$ the general linear group and σ in $GL_n(M)$.*

Suppose that:

(i) char $F \neq 2$,

(ii) B is nondegenerate, i.e., $|B(v_i, v_j)| \neq 0$ for $\{v_i\}$ a basis for M,

and

(iii) M is anisotropic, i.e., $B(v, v) \neq 0$ for any $0 \neq v \in V$.

Then, σ is a product of two involutions.

Proof. See Wonnenburger [5]. □

Theorem 5. *Let R be a valuation domain, that is, an integral domain in which a divides b or b devides a for any a, b in R. Let M be a free module of rank n over R equiped a quadratic map $Q : M \longrightarrow R$, and $O_n(M)$ the orthogonal group.*

Suppose that $Q(u)$ is a unit for any $u \in M - \mathfrak{m}M$, where $\mathfrak{m}$ is the unique maximal ideal of R.

Then, σ is a product of two involutions.

Proof. See Ellers and Ishibashi [2]. □

3. Proof for Theorem 2 by Invariant Factors

Professor Djocović proved this theorem by using the uniqueness of the elementary divisors of σ, whereas we will do it by using the uniqueness of the invariant factors of σ. The reader can also consult the proof for Theorem B of Ishibashi [5].

(I) First we prove (b) to (a).

If $\sigma = \theta\tau$ with $\theta^2 = \tau^2 = 1$, then $\sigma^{-1} = \tau^{-1}\theta^{-1} = \tau\theta = \tau\theta\tau\tau^{-1} = \tau\sigma\tau^{-1}$ is similar to σ.

(II) Next we prove (a) to (b).

Let $F[x]$ be the polynomial ring in x over F. So, $F[x]$ is a principal ideal domain (PID).

Define an action φ^+ of $F[x]$ on M by substituting σ for x, that is

$$\varphi^+ : F[x] \looparrowright M \quad \text{by} \quad f(x)u = f(\sigma)u$$

for $f(x) \in F[x]$ and $u \in M$.

Then, φ^+ gives a F-module M a $F[x]$-module structure which we denote by M^+ for M. Clearly M^+ is finitely generated and torsion over PID as $F[x]$-module.

Thus, the structure theorem of a finitely generated torsion module over PID induces

$$M = M^+ \simeq M_1 \oplus M_2 \oplus \cdots \oplus M_r \ \text{ as } F[x]\text{-module},$$

where for $i = 1, 2, \cdots, r$

(i) $M_i \simeq \dfrac{F[x]}{(f_i(x))}$,

(ii) f_i is monic,

and

(iii) $f_1 | f_2 | \cdots | f_r$.

This guarantees for $i = 1, 2, \cdots, r$ the existence of $u_i \in M_i$ such that

(iv) $M_i = Fu_i \oplus F\sigma u_i \oplus \cdots \oplus F\sigma u_i^{n_i - 1}$ with $n_i = \deg f_i$,

and

(v) f_i is the minimal polynomial of $\sigma_i = \sigma|_{M_i}$.

Here, we write

$$f_i(x) = a_{i0} + a_{i1}x + \cdots + a_{i(n_i-1)}x^{n_i-1} + x^{n_i}, \quad a_{ij} \in F.$$

Then, by $\sigma \in \mathrm{Aut}_F M$ we have $\sigma_i \in \mathrm{Aut}_F M_i$, which implies that $a_{i0} \neq 0$ for $i = 1, 2, \cdots, r$.

Now, we define $\tau_i, \theta_i \in \mathrm{Aut}_F M_i$ for $i = 1, 2, \cdots, r$ by

$$\tau_i \ : \ \sigma_i^j u_i \longrightarrow \sigma_i^{n_i - j - 1} u_i \ \text{ for } \ 0 \leq j \leq n_i - 1,$$

$$\theta_i \ : \ \sigma_i^j u_i \longrightarrow \sigma_i^{n_i - j} u_i \ \text{ for } \ 0 \leq j \leq n_i - 1.$$

Then, for $i = 1, 2, \cdots, r$ we observe that

$$\sigma_i = \theta_i \tau_i, \ \ \tau_i^2 = 1 \ \text{ and } \ \theta_i^2 = 1 \ \text{ on } \ \{\sigma_i u_i, \sigma_i^2 u_i, \cdots, \sigma_i^{n_i - 1} u_i\}.$$

So, if we can show that $\theta_i^2 = 1$ on u_i for $i = 1, 2, \cdots, r$, we will obtain $\theta_i^2 = 1$ on M_i.

To show it we define another action φ^- of $F[x]$ on M by substituting σ^{-1} for x, that is,

$$\varphi^- \ : \ F[x] \curvearrowright M \ \text{ by } \ f(x)u = f(\sigma^{-1})u$$

for $f(x) \in F[x]$ and $u \in M$.

This endows M another $F[x]$-module structure, which we denote by M^- for M.

Our next purpose is to show that M^+ and M^- are isomorphic as $F[x]$-modules.

Recall that we are proving (b) to (a) of Theorem 2, and by (b) $\sigma \sim \sigma^{-1}$ we have

$$\sigma^{-1} = \rho\sigma\rho^{-1}, \quad \text{i.e.,} \quad \sigma^{-1}\rho = \rho\sigma$$

for some $\rho \in \mathrm{Aut}_F M$. This implies that

$$\sigma^{-j}\rho = \rho\sigma^j \quad \text{for} \quad j = 0, 1, 2, \cdots,$$

and so

$$\rho(f(x)u) = \rho(f(\sigma)u) = f(\sigma^{-1})\rho u.$$

From this, we find that $\rho \in \mathrm{Aut}_F M$ is not only a F-module isomorphism but also a $F[x]-$module isomorphism by

$$\rho \ : \ M^+ \to M^-.$$

Moreover we see that

$$g_i(x) = a_{i0}^{-1}x^{n_i}f_i(x^{-1}) = a_{i0}^{-1} + a_{i0}^{-1}a_{i(n_i-1)}x + \cdots + a_{i0}^{-1}a_{i1}x^{n_i-1} + x^{n_i}$$

is the minimal polynomial of σ_i^{-1} for $i = 1, 2, \cdots, r$. Therefore, again by the structure theorem we have a splitting

$$M = M^- = M_1 \oplus M_2 \oplus \cdots \oplus M_r$$

as $F[x]$-module, where

$$M_i = \frac{F[x]}{(g_i(x))} \quad \text{for} \quad i = 1, 2, \cdots, r.$$

It is straightforward that $g_1|g_2|\cdots|g_r$ by $f_1|f_2|\cdots|f_r$. Thus we have obtained two invariant factors, one is $\{f_1, f_2, \cdots, f_r\}$ for M^+, and the other is $\{g_1, g_2, \cdots, g_r\}$ for M^-. However, as we have already shown these two $F[x]$-modules are isomorphic by $\rho \ : \ M^+ \to M^-$. Therefore, the uniqueness of invariant factors gives us $(f_i) = (g_i)$ for $i = 1, 2, \cdots, r$. However, since $\{f_i, g_i\}$ are all monic, this implies that $f_i = g_i$ for $i = 1, 2, \cdots, r$. Comparing coefficients of f_i and g_i, we have

$$a_{i0} = a_{i0}^{-1}, \quad a_{ij} = a_{i0}^{-1}a_{i(n_i-1)}$$

for $i = 1, 2, \cdots, r$ and $j = 1, 2, \cdots, n_i - 1$.

Then, an easy calculation yields $\theta_i^2 u_i = u_i$ as was to be shown. Now define

$$\tau = \tau_1 \oplus \tau_2 \oplus \cdots \oplus \tau_r \quad \text{and} \quad \theta = \theta_1 \oplus \theta_2 \oplus \cdots \oplus \theta_r.$$

Then we get

$$\sigma = \theta\tau \quad \text{with} \quad \theta^2 = \tau^2 = 1,$$

which completes our proof.

References

[1] D.Ẑ. Djocović, Product of two involutions, *Arch. Math.*, **XVIII** (1967) 582-584.

[2] E.W. Ellers, H. Ishibashi, Bireflectionality of the orthogonal group over a valuation domain, *J. Algebra*, **149**, No. 2 (1992), 322-324.

[3] W.H. Gustafson, P.R. Halmos, H. Radjavi, Products of involutions, *Linear Algebra Appl.*, **13** (1976), 157-162.

[4] H. Ishibashi, Involutary expressions for elements in $GL_n(Z)$ and $SL_n(Z)$, *Linear Algebra Appl.*, **219** (1995), 165-177.

[5] H. Ishibashi, Involutions and semiinvolutions, *Czechoslovak Math. J.*, **56**, No. 131 (2006), 533-541.

[6] M.J. Wonenburger, A decomposition of orthogonal transformations, *Canad. Math. Bull.*, **7** (1964), 379-383.