Publ. Math. Debrecen
43 / 1–2 (1993), 1–8

Weak automorphisms of the permutation groups S_n

By MAREK ZABKA (Gliwice)

0. The notion of weak automorphisms was studied in [3] and [6]. Let G be a group and let us denote by $A^{(n)}$ the class of all n-ary words in G, i.e. the set of all functions $f : G^n \to G$ of the form

$$f(x_1, x_2, \dots, x_n) = x_{i_1}^{m_1} \cdot x_{i_2}^{m_2} \cdot \dots \cdot x_{i_l}^{m_l}, \tag{1}$$

where $m_1, m_2, \dots, m_l \in Z$ (= integers), $i_1, i_2, \dots, i_l \in \{1, 2, \dots, n\}$, and $n = 1, 2, \dots$. We call a permutation τ of the set G a weak automorphism of the group G if the mapping $\tau^* : A^{(n)} \to A^{(n)}$ defined by the formula:

$$(\tau^* f)(x_1, x_2, \dots, x_n) = \tau f(\tau^{-1}(x_1), \tau^{-1}(x_2), \dots, \tau^{-1}(x_n)) \tag{2}$$

is a bijection, where $n = 1, 2, \dots, n$. We denote the set of all weak automorphisms by $\mathrm{Aut}^* G$. (cf. [1], [2])

Observe that e is the unique element of $A^{(0)}$ and therefore we have $\tau(e) = e$ for all $\tau \in \mathrm{Aut}^* G$ (cf. [2]).

The purpose of the paper is to prove the following Theorem

Theorem 0. *Each weak automorphism τ of the permutation group S_n is of the form $\tau(x) = \alpha(x)^m$, where α is an automorphism of the group S_n and m is a positive integer $< \exp S_n$, coprime to $n!$, and the representation is unique.*

1. In [1] the following proposition is shown:

Proposition 1.1. *For any group G, the group $\mathrm{Aut}\, G$ is a normal subgroup of $\mathrm{Aut}^* G$.*

Let us start with the simple consequence of the Proposition 1.1.

Lemma 1.1. *Let G be a group, $x, y \in G$ and $\tau \in \mathrm{Aut}^* G$. The following conditions are equivalent:*

a) *there exists an automorphism φ of G such that $\varphi(x) = y$;*
b) *there exists an automorphism ψ of G such that $\psi(\tau(x)) = \tau(y)$.*

Lemma 1.2. *Let H be a set of generators of a group G. If $\tau \in \mathrm{Aut}^* G$, $\beta \in \mathrm{Aut}\, G$ and $\tau(x) = x$ and $\beta(x) \in H$ for all $x \in H$, then $\tau \circ \beta = \beta \circ \tau$.*

Proof. By proposition 1.1 $\tau^{-1} \circ \beta^{-1} \circ \tau \circ \beta \in \mathrm{Aut}\, G$, and it is the identity on the generating set H, so it is the identity automorphism. □

For any word f of the form (1) we denote by $S^i(f)$ the sum of exponents of x_i.

Lemma 1.3. *If τ is an weak automorphism of a group G and f is a word of the form $f(x_1, \dots, x_n) = x_1 \dots x_n$, then $x = x^{S^i(\tau^* f)}$ for any element $x \in G$ and $i = 1, 2, \dots, n$.*

Proof. $x = \tau f(e, \dots, e, \tau^{-1}(x), e, \dots, e) = x^{S^i(\tau^* f)}$.

Theorem 1.1. *If τ is a weak automorphism of a group G then $\tau(x^n) = \tau(x)^n$ for all $n \in Z$.*

Proof. For $n = 0$ Theorem 1.1 means that $\tau(e) = e$.

Now we prove Theorem 1.1 for $n \geq 1$. Let $f(x_1, x_2, \dots, x_n) = x_1 \cdot x_2 \cdot \dots \cdot x_n$. From Lemma 1.3, we have:

$$\tau(x^n) = \tau^*(f(\tau(x), \dots, \tau(x)) = \tau(x)^{S^1(\tau^* f)} \dots \tau(x)^{S^n(\tau^* f)} = \tau(x)^n.$$

Applying Lemma 1.3 in the case $n = 2$ for the weak automorphism τ^{-1} we get:

$$x = x^{S^1((\tau^{-1})^* f)} = x^{S^2((\tau^{-1})^* f)}.$$

Hence

$$\tau(x) \cdot \tau(x^{-1}) = f(\tau(x), \tau(x^{-1})) = \tau(((\tau^{-1})^* f)(x, x^{-1})) = \tau(x x^{-1}) = e$$

and Theorem 1.1 follows. □

Corollary 1.1. *Each weak automorphism of any group preserves the order of its element.*

The following Lemma 1.4 is a generalization of Lemma 1.3.

Lemma 1.4. *If τ is a weak automorphism of a group G and f is of the form (1), then*

$$x^{S^i f} = x^{S^i(\tau^* f)}$$

for $i = 1, 2, \dots, n$ and $x \in G$.

Proof. It follows from Theorem 1.1. □

Lemma 1.5. *Let S be a subset of a group G with the property $x \in S$ implies $x^n \in S$ for all integers n. If $x, y \in S$ and $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$ are integers such that:*

$$x^{a_1+a_2+\ldots+a_k} = y^{b_1+b_2+\ldots+b_k} = e,$$

where $k = 1, 2, \dots,$ then:

$$x^{a_1} y^{b_1} \dots x^{a_k} y^{b_k} \in [S, S] = \mathrm{gp}\ \{s_1^{-1} s_2^{-1} s_1 s_2 : s_1, s_2 \in S\}.$$

Proof. This is obvious for $k = 1$.

Let us suppose that we have proved Lemma 1.5 for $k \leq t$. To complete the proof it is enough to notice that we have:

$$x^{a_1} \cdot y^{b_1} \dots x^{a_{t+1}} \cdot y^{b_{t+1}} =$$
$$= x^{a_1} y^{b_1} \dots x^{a_{t-1}} y^{b_{t-1}} x^{a_t + a_{t+1}} y^{b_t + b_{t+1}} \left[y^{b_t + b_{t+1}}, x^{a_{t+1}}\right] \left[x^{a_{t+1}}, y^{b_{t+1}}\right]. \ \square$$

Theorem 1.2. *Let S be a subset of a group G with the property $x \in S$ implies $x^n \in S$ for all $n = 1, 2, \dots$. Then $\tau([S, S]) = [\tau(S), \tau(S)]$ for every weak automorphism τ of the group G.*

Proof. At first we prove that $\tau([S, S]) \subset [\tau(S), \tau(S)]$. Let τ be a weak automorphism of a group G and $f(x_1, x_2) = [x_1, x_2]$. We know from Theorem 1.1 that $x \in \tau(S)$ implies $x^n \in \tau(S)$. Since τ is a weak automorphism, $(\tau^* f)(u, v) = u^{a_1} v^{b_1} \dots u^{a_k} v^{b_k}$ for some integers $a_1, \dots, a_k$, $b_1, \dots, b_k$. Hence, applying Lemma 1.4 and Lemma 1.5, we get $\tau([x, y]) = \tau f(x, y) = (\tau^* f)(\tau(x), \tau(y)) \in [\tau(S), \tau(S)]$.

To complete the proof of Theorem 1.2 it is enough to consider τ^{-1} instead of τ and $\tau(S)$ instead of S. $\square$

Corollary 1.2. *We have $[x, y] = e$ if and only if $[\tau(x), \tau(y)] = e$ for any weak automorphism τ of a group G, and $x, y \in G$.*

Theorem 1.3. *Suppose that τ is a weak automorphism of a group G and x, y are elements of G such that $[x, y] = e$. Then we have $[\tau(x), \tau(y)] = e$ and $\tau(xy) = \tau(x)\tau(y)$.*

Proof. Let $[x, y] = e$ and $f(x, y) = x \cdot y$. By Corollary 1.2, $[\tau(x), \tau(y)] = e$. Moreover, $\tau(xy) = \tau^* f(\tau(x), \tau(y)) = \tau(x)^{S^1(\tau^* f)} \cdot \tau(y)^{S^2(\tau^* f)} = \tau(x)\tau(y)$ according to Lemma 1.3, which completes the proof. $\square$

Corollary 1.3. *Every weak automorphism of an abelian group is in fact an automorphism.*

2. Theorem 2.1. *Let G be a group of finite exponent n.*

a) *The mapping $x \to x^k$ is a bijection iff $(k,n) = 1$.*
b) *The inverse of $x \to x^k$ is $x \to x^m$, where $k \cdot m \equiv 1 \bmod n$.*
c) *If $(k,n) = 1$ then $x \to x^k$ is a weak automorphism of G.*

Proof. a) and b): If $x \to x^k$ is a bijection then for every $x \in G$ we have $(|x|, k) = 1$. So, $(k,n) = 1$. Conversely, if $(k,n) = 1$ then there exists m such that $k \cdot m \equiv 1$ mod n. Therefore, the mapping $x \to x^k$ is a bijection, where $x \to x^m$ is the inverse mapping.

c) Let $\tau(x) = x^k$, where $(k,n) = 1$, and let f be a n-ary word of the form

$$f(x_1, x_2, \dots, x_n) = x_{i_1}^{m_1} \cdot x_{i_2}^{m_2} \cdot \ldots \cdot x_{i_l}^{m_l}.$$

Then $\tau^{-1}(x) = x^m$ and so:

$$(\tau^* f)(x_1, x_2, \dots, x_n) = \tau f(\tau^{-1}(x_1), \tau^{-1}(x_2), \dots, \tau^{-1}(x_n)) = \\ = \left(x_{i_1}^{mm_1} \cdot x_{i_2}^{mm_2} \cdot \ldots \cdot x_{i_l}^{mm_l}\right)^k.$$

Hence τ^* is a mapping $A^{(n)}$ into $A^{(n)}$. But $(\tau^{-1})^*$ is also a mapping $A^{(n)}$ into $A^{(n)}$ and $(\tau^{-1})^* \circ \tau^* = \mathrm{id}|_{A^{(n)}}$. Hence τ^* is a bijection of $A^{(n)}$ and therefore τ is weak automorphism of G. □

Theorem 2.2. *For any group of exponent n the set of all weak automorphisms of the form $x \to x^k$ is a subgroup of the center of* $\mathrm{Aut}^* G$ *isomorphic to the multiplicative group Z_n^* of the ring Z_n.*

Proof. It follows from Theorem 1.1 and Theorem 2.1. □

Theorem 2.3. *For any group G of exponent n the set of all weak automorphisms of the form $x \to \alpha(x)^k$, where $\alpha \in \mathrm{Aut}\, G$, is a normal subgroup of* $\mathrm{Aut}^* G$.

Proof. It is a simple consequence of Proposition 1.1, Theorem 2.1 and Theorem 2.2. □

The following Example shows that the set of all weak automorphisms of the form $x \to \alpha(x)^k$, where $\alpha \in \mathrm{Aut}\, G$, could be a proper normal subgroup of $\mathrm{Aut}^* G$.

Example 2.1. Let G be a group of the form:

$$G = \langle a, b \mid [[a,b],a] = [[a,b],b] = [a,b]^4 = 1 \rangle.$$

Each element $g \in G$ is of the form

$$g = a^p b^q [a,b]^r,$$

where $r = 0, 1, 2, 3$, and this form is unique. The exponent of the group G is infinite, so, if a weak automorphism τ is of the form $\tau = \alpha(x)^n$, then

$n = 1$ or $n = -1$. Hence, each weak automorphism of the form $\tau = \alpha(x)^n$ satisfies one of the two equations:

$$\tau(x \cdot y) = \tau(x) \cdot \tau(y) \quad \text{or} \quad \tau(x \cdot y) = \tau(y) \cdot \tau(x).$$

Let τ be defined by

$$\tau(a^p b^q [a, b]^r) = a^p b^q [a, b]^{pq+3r}.$$

It is easy to check that:

a) $\tau \circ \tau = \mathrm{id}$,
b) $\tau(x \cdot y) = \tau(x)\tau(y)[\tau(x), \tau(y)]$,
c) $\tau(x \cdot y) \neq \tau(x) \cdot \tau(y)$ and $\tau(x \cdot y) \neq \tau(y) \cdot \tau(x)$.

Hence, the function τ is a weak automorphism and it is not of the form $\alpha(x)^n$. $\square$

3. Now we show that any weak automorphism of the group S_n of all permutations on n letters is of the form $x \to \alpha(x)^k$, where $\alpha \in \operatorname{Aut} S_n$, $(k, |S_n|) = 1$.

Let $B_{k,n}, 1 \leq k \leq n/2$, denote the set of all compositions of k disjoint transpositions in the group S_n.

Lemma 3.1. *Let τ be a weak automorphism of a group S_n, which satisfies the condition $\tau(B_{1,n}) = B_{1,n}$. If $\tau((i, j)) = (p, q)$ and $\tau((i, k)) = (p, r)$ then $\tau((j, k)) = (q, r)$.*

Proof. Let us put $f(x, y) = x \cdot y \cdot x$. For $x = (i, j)$ and $y = (i, k)$ we have $\tau((j, k)) = \tau(x \cdot y \cdot x) = (\tau^* f)(\tau(x), \tau(y)) = (\tau^* f)((p, r), (p, q))$, which is a permutation on three letters p, q, r. It follows from our hypothesis that $\tau((j, k))$ is a transposition. But τ is a bijection and so $\tau((j, k)) = (p, q)$. $\square$

Lemma 3.2. *If τ is a weak automorphism of the permutation group S_n, which satisfies the condition $\tau(B_{1,n}) = B_{1,n}$, then there exists an inner automorphism α of S_n such that $\tau(x) = \alpha(x)$ for each transposition x.*

Proof. Theorem 1.3 gives $[\tau((1, 2)), \tau((2, 3))] \neq e$. Therefore there exists $\sigma(1), \sigma(2), \sigma(3)$ such that $\tau((1, 2)) = (\sigma(1), \sigma(2))$ and $\tau((2, 3)) = (\sigma(2), \sigma(3))$. The equality $\tau((1, 3)) = (\sigma(1), \sigma(2))$ follows from Lemma 3.1.

Let us suppose that σ is a function: $\{1, \ldots, k\} \to \{1, \ldots, n\}$ such that $\tau((i, j)) = (\sigma(i), \sigma(j))$, where $i, j = 1, 2, \ldots, k$, $k \geq 3$. Since τ is a bijection and $\tau((1, 2)) = (\sigma(1), \sigma(2))$ and $\tau((1, 3)) = (\sigma(1), \sigma(3))$, so $\tau((1, k+1)) = (\sigma(1), d)$, where d is not equal to $\sigma(1), \sigma(2), \ldots, \sigma(k)$. Let us put $\sigma(k+1) = d$. The inductive conclusion follows from Lemma 3.1. So we have constructed a permutation $\sigma \in S_n$ such that $\tau((i, j)) = (\sigma(i), \sigma(j))$ for $i, j = 1, 2, \ldots, n$. Hence we have $\tau|_{B_{1,n}} = \alpha|_{B_{1,n}}$, where $\alpha(x) = \sigma x \sigma^{-1}$ and Lemma 3.2 follows. $\square$

Lemma 3.3. *For every weak automorphism τ of S_n there exists an automorphism α of S_n such that $\alpha(x) = \tau(x)$ for all $x \in B_{1,n}$.*

Proof. Let $n \neq 6$. Then it follows from Lemma 1.1 that for any weak automorphism τ of S_n there exists k such that $\tau(B_{1,n}) = B_{k,n}$. From [4] we know that $|B_{1,n}| \neq |B_{k,n}|$ for $n \neq 6$ and $k \neq 1$. Hence $\tau(B_{1,n}) = B_{1,n}$ and the conclusion follows from Lemma 3.2.

Now let $n = 6$. As we know from [5] for each automorphism β of S_6 $\beta(B_{2,6}) = B_{2,6}$. We have $|B_{1,6} \cup B_{3,6}| = 30$ and $|B_{2,6}| = 45$ so from Lemma 1.1 we obtain that $\tau(B_{2,6}) = B_{2,6}$.

Moreover, we shall show that $\tau(B_{1,6}) = B_{1,6}$ or $\tau(B_{1,6}) = B_{3,6}$. Indeed, if $\tau(B_{1,6}) \neq B_{1,6}$ and $\tau(B_{1,6}) \neq B_{3,6}$ then let us consider transpositions (i,j) and (j,k) such that $\tau((i,j)) \in B_{1,6}$ and $\tau((j,k)) \in B_{3,6}$. From Theorem 1.3 we know that $[\tau((i,j)), \tau((j,k))] \neq e$ so $\tau((i,j))$ and $\tau((j,k))$ are of the form $\tau((i,j)) = (p,q)$ and $\tau((j,k)) = (p,s)(q,t)(u,w)$. Then $\tau((i,j,k)) = \tau((i,j)(j,k)) = (\tau^* f)(\tau((i,j)), \tau((j,k))) = (\tau^* f)((p,q),(p,s)(q,t)(u,w))$, where $f(x,y) = x \cdot y$. We know that $(\tau^* f)((p,q),(p,s)(q,t)(u,w))$ is of the form $\mu \circ (u,w)$, where the permutation μ fixes u and w. Therefore its order is not equal to the order of (i,j,k), which contradicts Corollary 1.1.

From [5] we also know that there exists an automorphism β of S_6 such that $\beta(B_{3,6}) = B_{1,6}$. Let β be an automorphism of S_6 such that $\beta(B_{3,6}) = B_{1,6}$ if $\tau(B_{1,6}) = B_{3,6}$ and $\beta = \mathrm{id}$ if not. Then the conclusion follows from Lemma 3.2 after applying it for $\beta \circ \tau$. $\square$

In the proof of Lemma 3.5 we use the following obvious number-theoretical Lemma 3.4:

Lemma 3.4. *If $m_1, m_2, \ldots, m_n$ are positive integers such that $m_{rt} \equiv m_r \bmod r$ for all $r \cdot t \leq n$, then there exists m such that $m \equiv m_k \bmod k$ for all $k \leq n$.*

Lemma 3.5. *If τ is a weak automorphism of S_n such that $\tau(x) = x$ for each transposition x, then there exists a positive integer m such that $\tau(y) = y^m$ for all $y \in S_n$.*

Proof. First, we prove that if x is a permutation on some letters $i_1, i_2, \ldots, i_k$ then $\tau(x)$ is a permutation on the same letters. Indeed, there exists transpositions $x_1, x_2, \ldots, x_m$ on letters $i_1, i_2, \ldots, i_k$ such that $x = x_1 \cdot x_2 \cdot \ldots \cdot x_m$. Let us put $f(x_1, x_2, \ldots, x_m) = x_1 \cdot x_2 \cdot \ldots \cdot x_m$. Since $\tau(x_i) = x_i$ for each transposition x_i, so we have $\tau(x) = \tau f(x_1, x_2, \ldots, x_m) = \tau^*(f)(\tau(x_1), \tau(x_2), \ldots, \tau(x_m)) = \tau^*(f)(x_1, x_2, \ldots, x_m)$.

Now we prove that if x is a cycle of the form $x = (i_1, i_2, \ldots, i_k)$, then $\tau(x)$ is also a cycle on the same letters. Indeed, suppose that $\tau(x)$ is not a cycle. Then $\tau(x) = y_1 \cdot y_2$ for some independent permutations. From Theorem 1.3 we know that $x = \tau^{-1}(y_1 \cdot y_2) = \tau^{-1}(y_1) \cdot \tau^{-1}(y_2)$

and of course $\tau^{-1}(y_1)$ and $\tau^{-1}(y_2)$ are independent, which contradicts the assumption that x is a cycle.

Now we prove that for each cycle x we have $\tau(x) = x^m$ for some m (dependent on x) not greater then length of x. Indeed, applying Lemma 1.2 for the set H of all transpositions of S_n, for $\beta(y) = xyx^{-1}$ and for $y = x$ we get $\tau(x)x = x\tau(xxx^{-1}) = x\tau(x)$. So $\tau(x) = x^m$, where m is a positive integer.

Further, let us consider two cycles x, y of length k. We have $\tau(x) = x^m$ and $\tau(y) = y^w$. There exists an inner automorphism β of S_n such that $\beta(x) = y$, therefore, using Lemma 1.2, we get $y^w = \tau\beta(x) = \beta\tau(x) = \beta(x)^m = y^m$; hence $m = w$. So, there exists positive integers $m_2, m_3, \ldots,$ m_n such that $\tau(x) = x^{m_k}$ for each cycle x of length k. Moreover, if x is a composition of some disjoint cycles of length k then also $\tau(x) = x^{m_k}$, because of Theorem 1.3.

Now let r, t be positive integers such that $r, r \cdot t \leq n$ and let x be a cycle of length $r \cdot t$. Then x^t is a composition of disjoint cycles of length r. So, using Theorem 1.1, we have $x^{m_r t} = \tau(x^t)\tau(x)^t = x^{m_{tr} t}$. Hence $m_{tr} \equiv m_r \bmod r$. Using Lemma 3.4 we get a positive integer m such that $m \equiv m_k \bmod k$. Hence $\tau(x) = x^m$ for each cycle x of S_n.

If x is a composition of disjoint cycles of S_n then using Theorem 1.3 we conclude that also $\tau(x) = x^m$. So Lemma 3.5 is proved. □

Now we will PROVE THEOREM 0 from the introduction, which is the main result of the paper.

PROOF. Let τ be a weak automorphism of the group S_n. As we know from Lemma 3.3, there exists an automorphism α of S_n such that $\alpha^{-1}\tau(x) = x$ for each transposition x of S_n. It follows from Lemma 3.5 that there exists a positive integer m such that $\alpha^{-1}\tau(x) = x^m$. Hence $\tau(x) = \alpha(x)^m$. Theorem 2.1 implies that m is coprime to $n!$. Since an automorphism β of S_n can not be of the form $\beta(x) = x^k$ for $k \neq 1$, therefore the representation $\tau(x) = \alpha(x)^m$, with $0 < m < \exp(S_n)$, is unique and the result follows. □

Corollary 3.1. *The group* $\mathrm{Aut}^* S_n$ *is the direct product of the group* $\mathrm{Aut}\, S_n$ *and the group* H *of weak automorphisms of the form* $x \to x^k$, *where* k *is coprime to* $n!$, *and* H *is isomorphic to the multiplication group* Z_m^* *of the ring* Z_m, *where* $m = \exp S_n$.

References

[1] J. DUDEK and E. PŁONKA, Weak automorphisms of linear spaces and of some other abstract algebras, *Coll. Math.* **XXII** (1971), 201–208.

[2] A. GOETZ, On weak isomorphisms and weak automorphisms of abstract algebras, *Coll. Math.* **XIV** (1966), 163–167.

[3] A. HULANICKI and ŚWIERCZKOWSKI, On group operations other then xy or yx, *Publ. Math.* Debrecen **9** (1962), 142–148.

[4] M. Kargapałow and Ju. Merzliakow, Osnowy tieori grupp, *Moskwa*, *Nauka*, 1982.
[5] D.W. Miller, On a Theorem of Hölder, *Amer. Math. Monthly* **65**, nr. 4 (1958), 252–254.
[6] A.P. Street, Subgroup – determining functions on groups, *Illinois J. Math.* **12** (1968), 99–120.

INSTITUTE OF MATHEMATICS
OF SILESIAN TECHNICAL UNIVERSITY
UL. ZWYCIĘSTWA 42
44–100 GLIWICE
POLAND

(Received May 30, 1989; revised March 24, 1992)