НАУЧНОЕ ИЗДАНИЕ МГТУ ИМ. Н. Э. БАУМАНА

НАУКА и ОБРАЗОВАНИЕ

Эл № ФС77 - 48211. Государственная регистрация №0421200025. ISSN 1994-0408

электронный научно-технический журнал

Автоморфизмы полугрупп-степеней циклических групп простого порядка

11, ноябрь 2012

DOI: 10.7463/1112.0495704

Степанов Д. А.

УДК 512.53

Россия, МГТУ им. Н.Э. Баумана

dstepanov@bmstu.ru

Полугруппой-степенью некоторой группы называется множество всех непустых подмножеств данной группы с естественной операцией умножения, индуцированной операцией группы. В статье описаны автоморфизмы полугруппы-степени циклической группы простого порядка. Показано, что для всех простых чисел за исключением 3 и 5 все автоморфизмы полугруппы-степени индуцированы автоморфизмами исходной группы.

Список литературы

1. Mazorchuk V.S. All automorphisms of $FP^+(S_n)$ are inner // Semigroup Forum. 2000. V. 60, no. 3. P. 486–490.
2. Артамонов В.А., Салий В.Н., Скорняков Л.А. и др. Общая алгебра. В 2 т. Т. 2 / под ред. Л.А. Скорнякова. М.: Наука, 1991. 480 с. (Справочная математическая библиотека).

SCIENTIFIC PERIODICAL OF THE BAUMAN MSTU

SCIENCE and EDUCATION

EL № FS77 - 48211. №0421200025. ISSN 1994-0408

electronic scientific and technical journal

Automorphisms of global semigroups of cyclic groups of prime order

11, November 2012

DOI: 10.7463/1112.0495704

Stepanov D. A.

Russia, Bauman Moscow State Technical University

dstepanov@bmstu.ru

1. Introduction

We use terminology from [2] throughout. The *global semigroup* or the *semigroup-power* of a semigroup S is the set $\mathcal{P}^+(S)$ of all nonempty subsets of S with a natural associative operation $AB = \{ab \mid a \in A,\ b \in B\}$. In the general case, the description of the group of automorphisms of $\mathcal{P}^+(S)$ is not known. In the present work we solve this problem in a particular case when S is a cyclic group C_p of prime order p.

Let G be a group. An element A from $\mathcal{P}^+(G)$ is called a *k-element*, if A as a subset of G consists of k elements. We distinguish two subgroups in the group $\operatorname{Aut}\mathcal{P}^+(G)$ of all automorphisms of the global semigroup:

a) the group of induced automorphisms $\operatorname{Ind}\mathcal{P}^+(G)$. Each automorphism φ of the group G extends naturally to an automorphism $\bar{\varphi}$ of the semigroup $\mathcal{P}^+(G)$: $\bar{\varphi}(A) = \{\varphi(a) \mid a \in A\}$. The group $\operatorname{Ind}\mathcal{P}^+(G)$ consists of all automorphisms of $\mathcal{P}^+(G)$ that are induced in this way by the automorphisms of G;

b) the group of proper automorphisms $\operatorname{Own}\mathcal{P}^+(G)$. We say that an automorphism of $\mathcal{P}^+(G)$ is *proper*, if it fixes all the 1-elements of $\mathcal{P}^+(G)$.

Proposition 1. If G is a group, then

$$\operatorname{Aut}\mathcal{P}^+(G) \simeq \operatorname{Own}\mathcal{P}^+(G) \rtimes \operatorname{Ind}\mathcal{P}^+(G)$$

(semidirect product with $\operatorname{Own}\mathcal{P}^+(G)$ normal).

◄ Let φ be an automorphism of $\mathcal{P}^+(G)$. Its restriction onto 1-elements gives an automorphism of the group G. Consider the induced automorphism $\overline{\varphi|_G}$ of $\mathcal{P}^+(G)$ and also the proper automorphism $\psi = \varphi \circ (\overline{\varphi|_G})^{-1}$. We have $\varphi = \psi \circ \overline{\varphi|_G}$, thus $\operatorname{Aut}\mathcal{P}^+(G) = \operatorname{Own}\mathcal{P}^+(G) \inf \mathcal{P}^+(G)$. Also $\operatorname{Own}\mathcal{P}^+(G) \cap \operatorname{Ind}\mathcal{P}^+(G) = \{e\}$, $\operatorname{Own}\mathcal{P}^+(G) \lhd \operatorname{Aut}\mathcal{P}^+(G)$. ►

2. Auxiliary lemmas

Let e be the unit, and a a generator of the group C_p. In the sequel the words *set*, *subset* mean a subset of C_p, i. e. an element of $\mathcal{P}^+(C_p)$. The class of the Green's relation (all Green's relations on $\mathcal{P}^+(C_p)$ coincide, since $\mathcal{P}^+(C_p)$ is commutative) that contains a subset $\{g_1, \ldots, g_k\}$ will be denoted $[\{g_1, \ldots, g_k\}]$. Throughout this section we assume $p \geqslant 5$.

Lemma 1.

(a) $\forall A \in \mathcal{P}^+(C_p)$, $A \neq C_p$, $\forall g, h \in C_p$, $gA = hA \Leftrightarrow g = h$;

(b) if $2 \leqslant |A| < p$, $2 \leqslant |B| < p$, then $|AB| > |B|$;

(c) $B \in [A] \Leftrightarrow B = gA$, $g \in C_p$;

(d) for $A \neq C_p$ the class $[A]$ has p elements: A, aA, $\ldots$, $a^{p-1}A$; the class $[C_p]$ has only one element C_p, which is zero of $\mathcal{P}^+(C_p)$;

(e) there are $(p-1)/2$ Green's classes of 2-elements: $[\{e, a\}]$, $[\{e, a^2\}]$, $\ldots$, $[\{e, a^{(p-1)/2}\}]$;

(f) $\forall A \in \mathcal{P}^+(C_p)$, $A \neq C_p$, $\forall g \in C_p$ one has: $g(C_p \setminus A) = C_p \setminus gA$.

◄ Let us prove (c) and (e).

(c). $B \in [A]$ means that there exist D_1, $D_2 \in \mathcal{P}^+(C_p)$ such that $A = D_1B$, $B = D_2A$, or $A = D_1D_2A$. If $A \neq C_p$, then by (b) we have $|D_1D_2| = 1$, $|D_2| = 1$, that is $D_2 = \{g\}$, $g \in C_p$. If $A = C_p$, the statement does not need a proof.

(e). In view of (d) it remains only to prove that the classes listed in (e) are different. Suppose that $[\{e, a^k\}] = [\{e, a^l\}]$, $k \neq l$, $1 \leqslant k, l \leqslant (p-1)/2$. Then it follows from (c) that

$$\{e, a^k\} = a^m\{e, a^l\} = \{a^m, a^{m+l}\}$$

for some m, $0 \leqslant m \leqslant p-1$. But $k \neq l$, thus $m \neq 0$, $a^m \neq e$. Then it must be $a^{l+m} = e$, $l+m = p$, $m = k$. But this implies $l = p - k \geqslant (p+1)/2 > (p-1)/2$, which is a contradiction. ►

Note that the degree of nilpotency of each 2-element equals $p-1$. It follows from Lemma 1, 2, that for $|A| \geqslant 3$ the degree of nilpotency is not greater than $p-2$; 1-elements are not nilpotent. Therefore any automorphism maps the 2-elements to 2-elements.

In this section we speak only about proper automorphisms of $\mathcal{P}^+(C_p)$, so the word *proper* will usually be omitted.

Lemma 2. Let φ be a proper automorphism of $\mathcal{P}^+(C_p)$. If for any 2-element A it holds that $\varphi(A) \in [A]$, then for all 2-elements $\varphi(A) = A$. That is, if every class of 2-elements is invariant under the automorphism φ, then φ acts on 2-elements identically.

◄ Let $\varphi(\{e, a\}) = g\{e, a\}$. Take arbitrary k, $2 \leqslant k \leqslant (p-1)/2$, and let $\varphi(\{e, a^k\}) = h\{e, a^k\}$, $g, h \in C_p$. We have:

$$\varphi(\{e, a\}^{p-2}) = g^{p-2}\{e, a\}^{p-2} = g^{p-2}(C_p \setminus \{a^{-1}\}),$$

$$\varphi(\{e, a^k\}^{p-2}) = h^{p-2}(C_p \setminus \{a^{-k}\}).$$

But $C_p \setminus \{a^{-k}\} = a^{1-k}(C_p \setminus \{a^{-1}\})$, thus

$$\varphi(\{e, a^k\}^{p-2}) = h^{p-2}\{e, a^k\}^{p-2} = \varphi(a^{1-k}\{e, a\}^{p-2}) = g^{p-2}\{e, a^k\}^{p-2}.$$

It follows that $g^{p-2} = h^{p-2}$, $g = h$. Thus if A is a 2-element, then $\varphi(A) = gA$, in particular $\varphi(\{e, a^2\}) = g\{e, a^2\}$. Then

$$\varphi(\{e, a\}^3) = g^3\{e, a\}^3 = g^3\{e, a, a^2, a^3\},$$

but $\{e, a, a^2, a^3\} = \{e, a\}\{e, a^2\}$, that gives

$$\varphi(\{e, a\}^3) = \varphi(\{e, a\}\{e, a^2\}) = g^2\{e, a\}^3.$$

This is possible only for $g^3 = g^2$, that is for $g = e$. Therefore $\varphi(A) = A$ for every 2-element A. ►

Lemma 3. Let φ be a proper automorphism of $\mathcal{P}^+(C_p)$. If for some 2-element $\{g_1, g_2\}$ $\varphi(\{g_1, g_2\}) \in [\{g_1, g_2\}]$, then φ acts on all 2 elements identically.

◄ Without loss of generality we may assume that the class $[\{e, a\}]$ is invariant (we can take a different generator of C_p if necessary). So, let $\varphi(\{e, a\}) = g\{e, a\}$ for some $g \in C_p$.

Let us take arbitrary k, $2 \leqslant k \leqslant (p-1)/2$, and show that the class $[\{e, a^k\}]$ is also invariant under φ. Suppose that $\varphi(\{e, a^k\}) = h\{e, a^m\}$, $h \in C_p$, $2 \leqslant m \leqslant (p-1)/2$. We have:

$$\{e, a\}^{k-1}\{e, a^k\} = \{e, a, a^2, \ldots, a^{2k-1}\} = \{e, a\}^{2k-1} \neq C_p,$$

because $2k - 1 \leqslant p - 2$. Applying the automorphism φ to this relation we get

$$g^{k-1}h\{e, a\}^{k-1}\{e, a^m\} = g^{2k-1}\{e, a, \ldots, a^{2k-1}\},$$

or

$$g^k h^{-1}\{e, a, \ldots, a^{2k-1}\} = \{e, a, \ldots, a^{k-1}, a^m, \ldots, a^{m+k-1}\}.$$

This is possible only if $m = k$ or if $m = p-k$. We agreed to choose $m \leqslant (p-1)/2$, $k \leqslant (p-1)/2$, hence $m = k$, $\varphi(\{e, a^k\}) = h\{e, a^k\}$, i. e., φ does not move the class $[\{e, a^k\}]$. Now our lemma follows from Lemma 2. ►

We can conclude that an automorphism is either identity on 2-elements, or moves all the 2-elements.

Lemma 4. Each proper automorphism of $\mathcal{P}^+(C_p)$ acts identically on $(p-1)$-elements.

◄ If an automorphism acts identically on 2-elements, it acts also identically on $p - 1$ elements, since $\{e, a\}^{p-2} = \{e, a, \ldots, a^{p-2}\} = C_p \setminus \{a^{-1}\}$.

If an automorphism φ is not identity on 2-elements, consider one of the cycles of the permutation induced by φ on the classes of 2-elements:

$$\varphi(\{e, a^{k_1}\}) = g_1\{e, a^{k_2}\},\ \ldots,\ \varphi(\{e, a^{k_n}\}) = g_n\{e, a^{k_1}\},$$

$g_i \in C_p$, $1 \leqslant i \leqslant n$. $p-1$-elements constitute one class of the Green's relation on $\mathcal{P}^+(C_p)$; every 2-element in degree $p-2$ lies in this class, in particular

$$\{e, a^{k_1}\}^{p-2} = C_p \setminus \{a^{-k_1}\}, \quad \ldots, \quad \{e, a^{k_n}\}^{p-2} = C_p \setminus \{a^{-k_n}\}.$$

Thus (Lemma 1, 5) the following relations hold:

$$a^{k_1-k_2}\{e, a^{k_1}\}^{p-2} = \{e, a^{k_2}\}^{p-2}, \quad \ldots, \quad a^{k_{n-1}-k_n}\{e, a^{k_{n-1}}\}^{p-2} = \{e, a^{k_n}\}^{p-2}.$$

Applying to these relations the automorphism φ, we get

$$\begin{array}{l} g_1^{p-2}a^{k_1-k_2}\{e, a^{k_2}\}^{p-2} = g_2^{p-2}\{e, a^{k_3}\}^{p-2} = g_2^{p-2}a^{k_2-k_3}\{e, a^{k_2}\}^{p-2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_{n-1}^{p-2}a^{k_{n-1}-k_n}\{e, a^{k_n}\}^{p-2} = g_n^{p-2}\{e, a^{k_1}\}^{p-2} = g_n^{p-2}a^{k_n-k_1}\{e, a^{k_n}\}^{p-2}, \end{array}$$

from where we get

$$g_1^{p-2}a^{k_1-k_2} = g_2^{p-2}a^{k_2-k_3}, \quad \ldots, \quad g_{n-1}^{p-2}a^{k_{n-1}-k_n} = g_n^{p-2}a^{k_n-k_1}.$$

On the other hand, we have

$$\varphi^n(\{e, a^{k_1}\}) = \varphi^{n-1}(g_1\{e, a^{k_2}\}) = g_1 \ldots g_n\{e, a^{k_1}\},$$

that is the automorphism φ^n leaves invariant the class $[\{e, a^{k_1}\}]$. But then Lemma 3 implies that φ^n fixes all the 2-elements, that is $g_1 \ldots g_n = e$. Hence the elements $g_1, \ldots, g_n$ of C_p satisfy the system

$$\begin{cases} g_1^{p-2}a^{k_1-k_2} = g_2^{k_2-k_3}a^{k_2-k_3}, \\ \ldots\ldots\ldots\ldots\ldots \\ g_{n-1}^{p-2}a^{k_{n-1}-k_n} = g_n^{p-2}a^{k_n-k_1}, \\ g_1g_2\ldots g_n = e. \end{cases}$$

Let us express $g_2^{p-2}, \ldots, g_n^{p-2}$ through g_1^{p-2}:

$$\begin{array}{l} g_2^{p-2} = a^{k_1-2k_2+k_3}g_1^{p-2}, \\ g_3^{p-2} = a^{k_1-k_2-k_3+k_4}g_1^{p-2}, \\ \ldots\ldots\ldots\ldots\ldots \\ g_{n-1}^{p-2} = a^{k_1-k_2-k_{n-1}+k_n}g_1^{p-2}, \\ g_n^{p-2} = a^{2k_1-k_2-k_n}g_1^{p-2}g_1^{p-2}. \end{array}$$

Exponentiate the last equation of the system to the degree $p-2$ and substitute for $g_2^{p-2}, \ldots, g_n^{p-2}$ their expressions through g_1^{p-2}. We obtain $g_1^{n(p-2)}a^{n(k_1-k_2)} = e$. Since $n < p$, $g_1^{p-2}a^{k_1-k_2} = e$, $g_1^{p-2} = a^{k_2-k_1}$. It follows that

$$\varphi(\{e, a_1^k\}^{p-2} = a^{k_2-k_1}(C_p \setminus \{a^{-k_2}\}) = C_p \setminus \{a^{-k_1}\} = \{e, a^{k_1}\}^{p-2}.$$

This means that the set $\{e, a^{k_1}\}$ is fixed by φ. In the same way one proves that all the other 2-elements are fixed by φ. ►

Lemma 5. Assume that $p \geqslant 7$. Then each proper automorphism of $\mathcal{P}^+(C_p)$ leaves invariant all the 2-elements.

◀ Let $\varphi(\{e,a\}) = g\{e,a^k\}$, $g \in C_p$, $2 \leqslant k \leqslant (p-2)/2$. From the relation

$$\{e,a\}\{e,a,a^3\} = \{e,a,a^2,a^3,a^4\} = \{e,a\}^4$$

we get

$$g^4\{e,a^k\}^4 = g\{e,a^k\}\varphi(\{e,a,a^3\}). \tag{1}$$

First note that $|\varphi(\{e,a,a^3\})| = 3$. Indeed, since $|\{e,a^k\}^4| = 5$, it must be $3 \leqslant |\varphi(\{e,a,a^3\}) \leqslant 4$. But from $|\varphi(\{e,a,a^3\})| = 4$ and (1) it follows that

$$|\varphi(\{e,a,a^3\}) \cap a^k\varphi(\{e,a,a^3\})| = 3,$$

which is possible only if $\varphi(\{e,a,a^3\}) \in [\{e,a^k\}^3]$. But this class is the image of the class $[\{e,a\}^3] \neq [\{e,a,a^3\}]$. Thus, if we denote $g^{-3}\varphi(\{e,a,a^3\}) = \{a^x,a^y,a^z\}$, where $0 \leqslant x,y,z \leqslant p-1$, then (1) takes the form

$$\{a^x,a^y,a^z\}\{e,a^k\} = \{e,a^k,a^{2k},a^{3k},a^{4k}\},$$

or

$$\{a^x,a^y,a^z,a^{x+k},a^{y+k},a^{z+k}\} = \{e,a^k,a^{2k},a^{3k},a^{4k}\}.$$

Since the set on the right has 5 elements, one of the following congruences must hold:

$$\begin{aligned} &x \equiv (y+k), \quad x \equiv (z+k), \quad y \equiv (x+k) (\operatorname{mod} p), \\ &y \equiv (z+k), \quad z \equiv (x+k), \quad z \equiv (y+k) (\operatorname{mod} p). \end{aligned}$$

Let us suppose that $z \equiv (x+k) (\operatorname{mod} p)$ holds. Then we have

$$\{a^x,a^y,a^{x+k},a^{y+k},a^{x+2k}\} = \{e,a^k,a^{2k},a^{3k},a^{4k}\}.$$

Considering 5 cases 1) $a^x = e$, $x = 0$, 2) $a^y = e$, $y = 0$, 3) $a^{x+k} = e$, $x \equiv -k (\operatorname{mod} p)$, 4) $a^{y+k} = e$, $y + k \equiv -k (\operatorname{mod} p)$, 5) $a^{x+2k} = e$, $x \equiv -2k (\operatorname{mod} p)$, one checks that only

1) $[\{e,a,a^3\}] \xrightarrow{\varphi} [\{e,a^k,a^{3k}\}]$, or
2) $[\{e,a,a^3\}] \xrightarrow{\varphi} [\{e,a^{2k},a^{3k}\}]$

are possible. The argument below depends on the residue of p modulo 3, so we have to consider 4 cases.

But for the beginning let us prove 2 relations. Let $\varphi(\{e,a,a^3\}) = g\{e,a^k,a^{3k}\}$, $\varphi(\{e,a\}) = h\{e,a^k\}$, $g,h \in C_p$. First, applying to the relation

$$\{e,a\}\{e,a,a^3\} = \{e,a\}^4 \neq C_p$$

the automorphism φ, we get

$$g = h^3. \tag{2}$$

Also, $\{e,a\}^{p-2} = C_p \setminus \{a^{-1}\}$, thus $C_p \setminus \{a^{-1}\} \xrightarrow{\varphi} h^{p-2}\,(C_p \setminus \{a^{-1}\})$. But by Lemma 4 $C_p \setminus \{a^{-1}\} \xrightarrow{\varphi} C_p \setminus \{a^{-1}\}$, therefore $h^{p-2}a^{-k} = a^{-1}$,

$$h^{p-2} = a^{k-1}. \tag{3}$$

Relations (2) and (3) hold also when $\varphi(\{e,a,a^3\}) = g\{e,a^{2k},a^{3k}\}$ and can be proved in the same way.

I. Let $p = 3l+1$, $\{e,a,a^3\}^l = \{e,a,\ldots,a^{3l-2},a^{3l}\} = C_p \setminus \{a^{3l-1}\}$. Consider the case 1):

$$\{e,a,a^3\} \xrightarrow{\varphi} g\{e,a^k,a^{3k}\}, \quad \varphi(\{e,a\}) = h\{e,a^k\}, \quad g,h \in C_p, \quad 1 \leqslant k \leqslant (p-1)/2.$$

We have (2)

$$C_p \setminus \{a^{p-2}\} = C_p \setminus \{a^{3l-1}\} = \{e,a,a^3\}^l \xrightarrow{\varphi} g^l(C_p \setminus \{a^{3l-1}\}) = h^{p-1}(C_p \setminus \{a^{(p-2)k}\}).$$

Lemma 4 implies that

$$h^{p-1}a^{(p-2)k} = a^{p-2}, \quad h^{-1} = a^{(p-2)(k-1)}, \quad h = a^{(p-2)(k-1)}.$$

Then, by (3), $(p-2)^2(k-1) \equiv (k-1)(\mathrm{mod}\, p)$. If $2 \leqslant k \leqslant (p-1)/2$, $k-1$ is coprime to p, thus $(p-2)^2 \equiv 1(\mathrm{mod}\, p)$, but this may hold only for $p=3$, whereas we have $p \geqslant 7$. Hence $k=1$, $h=e$, $\varphi(\{e,a\}) = \{e,a\}$, and by Lemma 3 all the 2-elements are invariant.

Consider the case 2):

$$\{e,a,a^3\} \xrightarrow{\varphi} g\{e,a^{2k},a^{3k}\}, \quad \{e,a\} \xrightarrow{\varphi} h\{e,a^k\}.$$

We have $C_p \setminus \{a^{p-2}\} = \{e,a,a^3\}^l \xrightarrow{\varphi} h^{3l}\{e,a^{2k},a^{3k}\}^l = h^{p-1}(C_p \setminus \{a^k\})$, and by Lemma 4, $h^{-1}a^k = a^{p-2}$, $h = a^{k+2}$. Now by relation (3) $a^{(p-2)(k+2)} = a^{k-1}$, $a^{-2k-4+1-k} = e$, $-3(k+1) \equiv 0(\mathrm{mod}\, p)$. Under our restrictions on k the last congruence does not hold, thus variant 2) is impossible.

II. $p = 3l+2$. Then $\{e,a,a^3\}^l = C_p \setminus \{a^{p-3},a^{p-1}\}$, $\{e,a^2\}\{e,a,a^3\}^l = C_p \setminus \{a^{p-1}\}$.

If $[\{e,a\}] \xrightarrow{\varphi} [\{e,a^k\}]$, then $[\{e,a\}] \xrightarrow{\varphi} [\{e,a^k\}]$ (this follows from the relation $\{e,a\}\{e,a^2\} = \{e,a\}^3$). If $\{e,a^2\} \xrightarrow{\varphi} f\{e,a^{2k}\}$, then $\{e,a^2\}^{p-2} = C_p \setminus \{a^{-2}\} \xrightarrow{\varphi} f^{p-2}(C_p \setminus \{a^{-2k}\})$, and by Lemma 4, $f^{p-2}a^{-2k} = a^{-2}$,

$$f^{p-2} = a^{2(k-1)}. \tag{4}$$

Consider case 1): $\{e,a,a^3\} \xrightarrow{\varphi} h^3\{e,a^k,a^{3k}\}$. Then

$$C_p \setminus \{a^{-1}\} = \{e,a^2\}\{e,a,a^3\}^l \xrightarrow{\varphi} f\{e,a^{2k}\}h^{3l}(C_p \setminus \{a^{(p-3)k},a^{(p-1)k}\}) = fh^{p-2}(C_p \setminus \{a^{-k}\}).$$

By Lemma 4, $fh^{p-2} = a^{k-1}$, then by (3) $f = e$, and from (4) we get $k=1$. It follows from Lemma 3 all the 2-elements are invariant.

Now consider case 2): $\{e,a,a^3\} \xrightarrow{\varphi} h^3\{e,a^{2k},a^{3k}\}$. We have:

$$\{e,a^{2k},a^{3k}\}^l = C_p \setminus \{a^k,a^{-k}\}, \quad \{e,a^{2k}\}\{e,a^{2k},a^{3k}\}^l = C_p \setminus \{a^k\}.$$

Thus $C_p \setminus \{a^{-1}\} = \{e, a^2\}\{e, a, a^3\}^l \xrightarrow{\varphi} fh^{p-2}(C_p \setminus \{a^k\})$. By Lemma 4 and (3), $fa^{k-1}a^k = a^{-1}$, $f = a^{-2k}$. Then from (2) we get

$$(-2k(p-2)) \equiv 2(k-1)(\operatorname{mod} p),$$

or $k + 1 \equiv 0(\operatorname{mod} p)$, which does not hold under our restrictions on k. Hence variant 2) is impossible. In both possible cases the 2-elements are invariant. ►

Corollary 1. Elements of the subsemigroup S generated by 1- and 2-elements are invariant under each proper automorphism of the semigroup $\mathcal{P}^+(C_p)$.

3. The main result

Theorem 1. a. $\operatorname{Aut}\mathcal{P}^+(C_2) \simeq \{e\}$; $\operatorname{Aut}\mathcal{P}^+(C_3) \simeq C_3 \rtimes C_2$; $\operatorname{Aut}\mathcal{P}^+(C_5) \simeq C_2 \times C_4$. In the second case the only nontrivial element of C_2 acts nontrivially on C_3; in the third the product is direct.

b. If $p \geqslant 7$, then all the automorphisms of the semigroup $\mathcal{P}^+(C_p)$ are induced by the automorphisms of the group C_p, i. e.,

$$\operatorname{Aut}\mathcal{P}^+(C_p) \simeq \operatorname{Aut}(C_p) \simeq C_{p-1}.$$

◄ **a** is proved via a direct calculation. For the proof of **b** we use the technique of [1]. Suppose that there exist a proper automorphism φ of $\mathcal{P}^+(C_p)$ and elements $A, B \in \mathcal{P}^+(C_p)$, $A \neq B$, such that $\varphi(A) = B$. In the case $|A| \leqslant p-1$ or $|A| = 1$ we immediately get a contradiction with the invariance of the elements of S, so assume that $1 < |A| < p-1$. Also assume that $B \nsubseteq A$. Then there is $a \in B$, $a \notin A$, and also there is $b \in C_p$, $b \notin A$, $b \neq a$. Take $D_1 = \{e, ab^{-1}\}$ and consider D_1A, D_1B. We have $a \notin D_1A$, $a \in D_1B$, that is $D_1A \neq D_1B$, $D_1B \nsubseteq D_1A$, $|A| < |D_1A| \leqslant p-1$. Continue this process until $|D_1 \dots D_nA| = p-1$, i. e. $D_1 \dots D_nA \in S$. Each D_i is a 2-element, thus $D = D_1 \dots D_n \in S$. Moreover, $a \notin DA$, but $a \in DB$, thus $DA \neq DB$. But then $\varphi(DA) = D\varphi(A) = DB$, which contradicts invariance of the elements of S. This contradiction proves the theorem. ►

The present work was done in 1999, when the author was a student at Kiev Shevchenko University, Ukraine. The author thanks to his advisor of that time Alexander Grigor'evich Ganushkin. The importance of his help appears even more evident with the years that have passed.

The work was partially supported by the Russian Grant for Leading Scientific Schools, grant no. 5139.2012.1, and RFBR, grant no. 11-01-00336-a.

References

1. Mazorchuk V. S. All automorphisms of $FP^+(S_n)$ are inner // Semigroup Forum. 2000. Vol. 60, no. 3. P. 486–490.
2. Artamonov V.A., Salii V.N., Skorniakov L.A., et al. *Obshchaia algebra. V 2 t. T. 2* [General algebra. In 2 vols. Vol. 2]. Moscow, Nauka, 1991. 480 p. (*Spravochnaia matematicheskaia biblioteka* [Reference mathematical library]).