COMPOSITIO MATHEMATICA

A. G. FADELL
K. D. MAGILL, JR.

Automorphisms of semigroups of polynomials

Compositio Mathematica, tome 21, nº 3 (1969), p. 233-239
<http://www.numdam.org/item?id=CM_1969__21_3_233_0>

COMPOSITIO MATHEMATICA, Vol. 21, Fasc. 3, 1969, pag. 233-239
Wolters-Noordhoff Publishing
Printed in the Netherlands

Automorphisms of semigroups of polynomials

by

A. G. Fadell and K. D. Magill, Jr.

1. Introduction

Let A be a ring and let $\mathscr{P}(A)$ denote the semigroup, under composition, of all polynomial functions on A. The question to which we address ourselves is this, "Is every automorphism of $\mathscr{P}(A)$ inner?". It is well known that every function mapping a finite field A into itself can be represented by a polynomial with coefficients in A. Consequently, $\mathscr{P}(A)$ in this case is simply the semigroup, under composition, of all selfmaps of A and it has been known for some time that every automorphism of this semigroup is inner. In fact, I. Schreier [2] proved this result as early as 1936.

The case is not resolved quite so easily for infinite fields. In the first place, either situation can occur. That is, there exist infinite fields A in which all automorphisms of $\mathscr{P}(A)$ are inner and there also exist infinite fields A with the property that not all automorphisms of $\mathscr{P}(A)$ are inner. In particular, not every automorphism of $\mathscr{P}(C)$ (C denotes the field of complex numbers) is inner. It is shown that the mapping which takes the polynomial defined by $a_0z^n+a_1z^{n-1}+\ldots+a_n$ into the polynomial defined by $\bar{a}_0z^n+\bar{a}_1z^{n-1}+\ldots+\bar{a}_n$ ($\bar{a}$ is the conjugate of a) is an automorphism which is not inner. The main result of this paper shows that every automorphism of $\mathscr{P}(R)$ is inner where R is the field of real numbers (actually, something more is shown). As a corollary, we obtain the fact that the automorphism group of $\mathscr{P}(R)$ is isomorphic to the group of all ordered pairs (a, b) of real numbers where $a \neq 0$ and multiplication is defined by

$$(a, b)(c, d) = (ac, ad+b).$$

2.

For any element a of the ring A, we let $\langle a\rangle$ denote the constant polynomial function defined by $\langle a\rangle(b) = a$ for all $b \in A$. Note that

for any $P \in \mathscr{P}(A)$, $\langle a \rangle \circ P = \langle a \rangle$. Furthermore, if Q has the property that $Q \circ P = Q$ for all $P \in \mathscr{P}(A)$ (i.e., Q is a left zero of $\mathscr{P}(A)$), then for any $a, b \in A$,

$$Q(a) = Q \circ \langle a \rangle(b) = Q(b).$$

This implies that $Q = \langle Q(a) \rangle$ and we have verified the following

PROPOSITION 1. *An element $Q \in \mathscr{P}(A)$ is a left zero of $\mathscr{P}(A)$ if and only if $Q = \langle a \rangle$ for some $a \in A$.*

Now suppose φ is an automorphism of $\mathscr{P}(A)$. Then φ must map $\{\langle a \rangle : a \in A\}$ bijectively onto itself and it follows that for each element $a \in A$, there exists a unique $b \in A$ such that $\varphi\langle a \rangle = \langle b \rangle$. We define a bijection h from A onto A by $h(a) = b$ and we note that φ and h are related by

$$\varphi\langle a \rangle = \langle h(a) \rangle.$$

Then for any $P \in \mathscr{P}(A)$ and any $a \in A$, we have

$$\begin{aligned}(h \circ P \circ h^{-1})(a) &= \langle h(P(h^{-1}(a))) \rangle(a) \\ &= \varphi\langle P(h^{-1}(a)) \rangle(a) = \varphi(P \circ \langle h^{-1}(a) \rangle)(a) \\ &= (\varphi(P) \circ \varphi\langle h^{-1}(a) \rangle)(a) = (\varphi(P) \circ \langle a \rangle)(a) = \varphi(P)(a).\end{aligned}$$

That is, $\varphi(P) = h \circ P \circ h^{-1}$ for each $P \in \mathscr{P}(A)$. It follows easily that h is unique, for suppose some function k also has the property that $\varphi(P) = k \circ P \circ k^{-1}$ for each $P \in \mathscr{P}(A)$. Then for any $a \in A$,

$$\langle h(a) \rangle = \varphi\langle a \rangle = \langle k(a) \rangle$$

which implies $h(a) = k(a)$. This proves

PROPOSITION 2. *Let A be any ring and let φ be an automorphism of $\mathscr{P}(A)$. Then there exists a unique bijection h from A onto A such that $\varphi(P) = h \circ P \circ h^{-1}$ for each $P \in \mathscr{P}(A)$.*

For an arbitrary semigroup S, we define an endomorphism φ to be inner if there exist elements a and b in S such that $\varphi(x) = axb$ for each $x \in S$. M. L. Vitanza has shown in [3] Theorem 1 that every inner epimorphism is in fact an automorphism and if such an automorphism φ exists then S must contain an identity and a and b are inverses of each other.

Now let us recall that $\mathscr{P}(C)$ denotes the semigroup of polynomials over the complex field. We mentioned in the introduction that the mapping φ which sends the polynomial P defined by

$$P(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_n$$

into the polynomial $\bar{P}$ defined by

$$\bar{P}(z) = \bar{a}_0 z^n + \bar{a}_1 z^{n-1} + \ldots + \bar{a}_n$$

is an automorphism which is not inner. The fact that φ is an automorphism follows from the observation that

$$\varphi(P) = h \circ P \circ h^{-1}$$

for each $P \in \mathscr{P}(C)$ where h is defined by $h(z) = \bar{z}$. Now if φ were an inner automorphism, then there would exist a polynomial Q such that

$$\varphi(P) = Q \circ P \circ Q^{-1}$$

for each $P \in \mathscr{P}(C)$. But by Proposition 2, the function Q is uniquely determined by φ and one obtains the contradiction that h is a polynomial. Consequently, we see that $\mathscr{P}(C)$ has automorphisms which are not inner.

The next result, which is the main result of the paper, shows that each epimorphism of $\mathscr{P}(R)$, the semigroup of polynomials over the real field, is inner.

THEOREM 3. *For each epimorphism φ of $\mathscr{P}(R)$, there exists a unique linear polynomial Q such that $\varphi(P) = Q \circ P \circ Q^{-1}$ for each $P \in \mathscr{P}(R)$.*

PROOF. Let φ be an epimorphism of $\mathscr{P}(R)$. The first thing we do is to show that there exists a surjection h of R and a function k mapping R into R such that

$$\varphi(P) = h \circ P \circ k \tag{3.1}$$

for all $P \in \mathscr{P}(R)$. As in the proof of proposition 2, we note that for any $a \in R$, $\varphi\langle a\rangle$ is a left zero of $\mathscr{P}(R)$ and consequently $\varphi\langle a\rangle = \langle b\rangle$ for some $b \in R$. We define $h(a) = b$ and note that

$$\varphi\langle a\rangle = \langle h(a)\rangle \tag{3.2}$$

for each $a \in R$.

On the other hand, each $\langle a\rangle$ is in the image of $\mathscr{P}(R)$ under φ, i.e., $\varphi(P) = \langle a\rangle$ for some $P \in \mathscr{P}(R)$. In fact, $\varphi\langle b\rangle = \langle a\rangle$ for some $b \in R$. To see this, choose any $c \in R$, let $b = P(c)$ and note that

$$\begin{aligned}\varphi\langle b\rangle &= \varphi\langle P(c)\rangle = \varphi(P \circ \langle c\rangle) \\ &= \varphi(P) \circ \varphi(c) = \langle a\rangle \circ \varphi\langle c\rangle = \langle a\rangle.\end{aligned}$$

We choose any $b \in R$ such that $\varphi\langle b\rangle = \langle a\rangle$ and we define a mapping k from R into R by $k(a) = b$. Note that

$$\varphi\langle k(a)\rangle = \langle a\rangle \tag{3.3}$$

for each $a \in R$. Now let P be an arbitrary polynomial over R. Then using both (3.2) and (3.3) we have

$$\begin{aligned}(h \circ P \circ k)(a) &= \langle h(P(k(a)))\rangle(a) \\ &= \varphi\langle P(k(a))\rangle(a) = \varphi(P \circ \langle k(a)\rangle)(a) \\ &= (\varphi(P) \circ \varphi\langle k(a)\rangle)(a) = (\varphi(P) \circ \langle a\rangle)(a) = \varphi(P)(a)\end{aligned}$$

for each $a \in R$. Hence, (3.1) is valid.

Now let I denote the identity of $\mathscr{P}(R)$, i.e., I is the polynomial defined by $I(x) = x$. Then φ must leave I fixed and from (3.1) we see that

$$h \circ k = I. \tag{3.4}$$

Suppose, however, that $k \circ h \neq I$. Then there exists a real number a such that $k(h(a)) \neq a$. Now the assumption that the image of R under h is one point leads to the contradiction that the image of φ is one point. Thus, there exist points $b, c \in R$ such that $h(b) \neq h(c)$. Choose any polynomial P such that

$$P(k(h(a))) = b \tag{3.5}$$

and

$$P(a) = c. \tag{3.6}$$

Then we have

$$\begin{aligned}(\varphi(P) \circ \varphi\langle a\rangle)(a) &= (h \circ P \circ k \circ h \circ \langle a\rangle \circ k)(a) \\ &= h(b) \neq h(c) = h(P(a)) \\ &= (h \circ P \circ \langle a\rangle \circ k)(a) = \varphi(P \circ \langle a\rangle)(a).\end{aligned}$$

But this is a contradiction since $\varphi(P \circ \langle a\rangle) = \varphi(P) \circ \varphi\langle a\rangle$ and we must conclude that $k \circ h = I$. This, together with (3.4) implies that h is a bijection and that $k = h^{-1}$. Thus, in place of (3.1), we are now able to write

$$\varphi(P) = h \circ P \circ h^{-1} \tag{3.7}$$

for each $P \in \mathscr{P}(R)$. Furthermore, it follows that φ is actually an automorphism.

Now let r be any real number and define

$$\begin{aligned}A_r &= \{x \in R : x \leqq r\} \\ B_r &= \{x \in R : x \geqq r\}.\end{aligned}$$

For each A_r, there exists a polynomial P such that $P[R] = A_r$.

For example, one may take P to be the polynomial defined by $P(x) = -x^2+r$. Then,

$$h[A_r] = h[P[R]]$$
$$= h[P[h^{-1}[R]]] = \varphi(P)[R].$$

That is, $h[A_r]$ is the range of some polynomial. Thus, $h[A_r]$ is either all of R or it is a set of the form A_v or B_w. The same statement holds for $h[B_r]$. Consequently, the bijection h takes subbasic closed subsets of R into subbasic closed subsets. The same statement holds for h^{-1} and we conclude that h is a homeomorphism. But this implies that h is strictly monotonic and is therefore differentiable almost everywhere. We will show that, in fact, h is differentiable at any real number a. Let b be any point at which h is differentiable, let $c = h(b)$ and define a polynomial P_a and a function t by

$$P_a(x) = -x+a+b$$
$$t(x) = h(-x+b)-c.$$

Note that t is a homeomorphism and that $t(0) = 0$. Consequently, $t(x) \to 0$ when $x \to 0$. Now let $\varphi(P_a) = Q_a$. Then by (3.7), $Q_a = h \circ P_a \circ h^{-1}$ and one can show that

$$\frac{h(a+x)-h(a)}{x} = -\frac{Q_a(c+t(x))-Q_a(c)}{t(x)} \cdot \frac{h(b+(-x))-h(b)}{(-x)}.$$

It follows from this that h is indeed differentiable at a and moreover, that

$$h'(a) = -Q_a'(c)\, h'(b). \tag{3.8}$$

Now the function Q_a certainly depends upon the function P_a which, in turn, depends upon the point a. Because of this, it may appear on the surface that h' is not constant. It turns out, however, that $h'(a)$ is, in fact, equal to $h'(b)$ for all $a \in R$. To verify this, one first shows that an element $P \in \mathscr{P}(R)$ has the properties that $P \neq I$ (the identity) and $P \circ P = I$ if and only if P is of the form $P(x) = -x+v$ for some real number v. Now P_a is of this form and since (as we observed earlier) φ is automorphism, $Q_a = \varphi(P_a)$ is of this form. Therefore $Q_a'(c) = -1$ for each Q_a and we see that h' is constant. Therefore, h must be a linear polynomial. One shows the uniqueness of h just as in the proof of proposition 2.

COROLLARY 4. *The automorphism group of $P(R)$ is isomorphic to the group of all ordered pairs (a, b) of real numbers where $a \neq 0$ and multiplication is defined by $(a, b)(c, d) = (ac, ad+b)$.*

PROOF. Let $\mathscr{A}$ denote the automorphism group of $\mathscr{P}(R)$ and let $\mathscr{G}$ denote the group of ordered pairs of real numbers mentioned in the statement of the corollary. Then for each automorphism φ there exists a unique linear polynomial $L_{a,b}$ (defined by $L_{a,b}(x) = ax+b$) such that

$$\varphi(P) = L_{a,b} \circ P \circ L_{a,b}^{-1}$$

for each $P \in \mathscr{P}(R)$. We define a mapping Φ from $\mathscr{A}$ into $\mathscr{G}$ by

$$\Phi(\varphi) = (a, b).$$

One easily checks that Φ is surjective. Let $\Phi(\varphi_1) = (a, b)$, $\Phi(\varphi_2) = (c, d)$. Then for every $P \in \mathscr{P}(R)$,

$$\varphi_1(P) = L_{a,b} \circ P \circ L_{a,b}^{-1}$$

and

$$\varphi_2(P) = L_{c,d} \circ P \circ L_{c,d}^{-1}.$$

Then

$$\begin{aligned}(\varphi_1 \circ \varphi_2)(P) &= \varphi_1(L_{c,d} \circ P \circ L_{c,d}^{-1}) \\ &= (L_{a,b} \circ L_{c,d}) \circ P \circ (L_{a,b} \circ L_{c,d})^{-1} \\ &= L_{ac,\,ad+b} \circ P \circ L_{ac,\,ad+b}^{-1}.\end{aligned}$$

Therefore, $\Phi(\varphi_1 \circ \varphi_2) = (ac, ad+b)$. But

$$(ac, ad+b) = (a, b)(c, d) = \Phi(\varphi_1)\,\Phi(\varphi_2).$$

Thus, Φ is an epimorphism. To show that Φ is injective, suppose $\Phi(\varphi)$ is the identity. Then $\Phi(\varphi) = (1, 0)$ which implies

$$\varphi(P) = L_{1,0} \circ P \circ L_{1,0}^{-1} = P$$

for each $P \in \mathscr{P}(R)$. Thus φ is the identity automorphism. This proves that the kernel of Φ is the identity and hence that Φ is an isomorphism.

We conclude by mentioning that it would be interesting to have a characterization of those infinite fields A with the property that every automorphism of $\mathscr{P}(A)$ is inner.

REFERENCES

A. H. CLIFFORD and G. B. PRESTON

[1] The algebraic theory of semigroups, Mathematical Surveys, No. 1, Amer. Math. Soc. 1961.

I. SCHREIER

[2] Über Abbildungen einer abstrakten Menge auf ihre Teilmengen, Fund. Math. 28 (1936), 261—264.

M. L. VITANZA
[3] Mappings of semigroups associated with ordered pairs, Amer. Math. Monthly 73 (1966) 1078—1082.

(Oblatum 26–3–68)

State University of New York
at Buffalo