COLLOQUIUM MATHEMATICUM

VOL. XII 1964 FASC. 1

ON TRANSFORMATIONS BY POLYNOMIALS IN TWO VARIABLES

BY

W. NARKIEWICZ (WROCŁAW)

1. In [1] and [2] we were concerned with invariant sets of polynomial transformations in one variable in various fields. For a class of fields (including all finitely generated extensions of the rationals) it was proved that if the polynomial is non-linear, then the invariant sets must be finite. Analogous question for rational transformations (which are not homographies) was answered in the same way for the field of rational numbers (see [3]). One can consider invariant sets of transformations defined by n polynomials in n variables acting in K^n — the set of all n-tuples of elements of a field K — and ask under what assumptions they must be finite. If we do not impose some additional conditions upon the polynomials, then already in the rational plane one can give examples of polynomial transformations which are non-linear and have infinite invariant sets. As an example one can take the transformation $(x, y) \to (x^2-y^2+x, x^2-y^2+y)$, which transforms the set with equal first and second coordinates onto itself. Even transformations defined by homogeneous polynomials can have infinite invariant sets as has the transformation $(x, y) \to (x^2-xy, xy-y^2)$, namely the set $\{(a, a-1) \mid a\text{-rational}\}$. In this paper, we consider the case of $n = 2$ and prove the following

THEOREM. *Let K be a finite algebraic extension of the field R of rational numbers. Let $F_1(x, y)$ and $F_2(x, y)$ be homogeneous polynomials with coefficients from K, of degrees m_1, m_2 respectively. Suppose $F_1(x, y)$ and $F_2(x, y)$ are without a common non-trivial factor and m_1, m_2 are greater than 2. Then the transformation T defined in K^2 by $(x, y) \to \big(F_1(x, y), F_2(x, y)\big)$ has no infinite invariant sets.*

Remark. The same holds if one supposes $m_1 = m_2 = 2$.

The question can be posed whether the same holds for $n \geqslant 3$ (**P 458**). This seems very plausible, but our method of proof does not work in the general case. One can also ask whether the assumption

$m_1, m_2 \geqslant 3$ or $m_1 = m_2 = 2$ is essential (**P 459**). It is not difficult to show that if our theorem holds for $n = 3$ with some restriction on the degrees of the corresponding forms, say $m_1, m_2, m_3 \geqslant A$, then it holds also for $n = 2$ with the single restriction $m_1, m_2 \geqslant 2$.

Now we prove that the Remark above follows from the Theorem. Consider the iterated transformation $T^2 = T(T)$. If $T(X) = X$, then also $T^2(X) = X$. As $m_1, m_2 = 2$, thus T^2 is defined by a pair of polynomials, say $G_1(x, y)$, $G_2(x, y)$, which are obviously homogeneous, and it remains to prove that their degrees are both greater than two, and that they have not any common, non-trivial factor. (It is evident that this procedure fails if $m_1 \neq m_2$, as then the polynomials need not be homogeneous).

LEMMA 1. *Suppose that $A(x, y)$ and $B(x, y)$ are homogeneous polynomials with coefficients from a field K, without any common non-trivial factor. Then there exist homogeneous forms $f_i(x, y)$, $i = 1, \ldots, 4$, with coefficients from K and natural numbers $a_1, \ldots, a_6$ such that*

$$x^{a_1}f_1(x, y)A(x, y) + x^{a_2}f_2(x, y)B(x, y) = x^{a_3},$$

$$y^{a_4}f_3(x, y)A(x, y) + y^{a_5}f_4(x, y)B(x, y) = y^{a_6}.$$

For the proof, consider the polynomials $A(x, 1)$ and $B(x, 1)$, and remark that they have no non-trivial common factor. Hence we can find polynomials $f(x)$, $g(x)$ with degrees n_1, n_2 respectively such that $A(x, 1)f(x) + B(x, 1)g(x) = 1$. Define now $f_1(x, y) = y^{n_1}f(x/y)$ and $f_2(x, y) = y^{n_2}g(x/y)$. The second equality follows immediately. The first follows similarly by considering the polynomials $A(1, y)$ and $B(1, y)$.

By substituting $A(x, y) = F_1(x, y)$, $B(x, y) = F_2(x, y)$ in Lemma 1 and then $x = F_1(u, v)$, $y = F_2(u, v)$ we infer that the forms $G_1(x, y)$ and $G_2(x, y)$ cannot have a non-trivial common factor. Remark finally that all terms in $G_i(x, y)$ are of degree 4 and evidently $G_i(x, y)$ cannot vanish identically. We proved thus that the Remark follows from the Theorem.

2. We shall need two lemmas proved in [1].

LEMMA 2 (see [1], lemma 1). *Suppose T is a transformation of a set X onto itself. Suppose there exist two functions f and g defined in X with values in the set of natural numbers, subject to the following conditions:*

(a) *For every constant c the equation $f(x) + g(x) = c$ has only a finite number of solutions.*

(b) *There exists a constant C such that from $f(x) \geqslant C$ it follows $f(Tx) > f(x)$.*

(c) *For every M there exists a constant $B(M)$ such that from $f(x) \leqslant M$ and $g(x) \geqslant B(M)$ it follows $g(Tx) > g(x)$.*

Then the set X is finite.

LEMMA 3 (see [1], lemma 2). *Let K be a finite, algebraic extension of the rationals, let a be a fixed integer in K and let m be a fixed natural number. Then there exists only a finite number of rational integers u such that with a suitable integral b in K, a divides $b^m a$, but no integral rational divisor $(\neq \pm 1)$ of u divides b.*

Now to the proof of the Theorem. We denote by K_0 the ring of integers in K, and by $\omega_1, \ldots, \omega_r$ a fixed integral basis in K, so that every $a \in K$ can be represented in the form

$$a = \frac{1}{q} \sum_{i=1}^{r} p_i \omega_i,$$

where $p_1, \ldots, p_r$ are rational integers, $(p_1, \ldots, p_r) = 1$, and q is a natural number.

Let

$$F_i(x, y) = \frac{1}{\Delta_i} \sum_{j=0}^{m_i} a_j^{(i)} x^j y^{m_i - j} = \frac{1}{\Delta_i} G_i(x, y)$$

(where $a_j^{(i)} \in K_0$, Δ_i are rational integers). Let

$$\xi = \left(\frac{1}{q_1} \sum_{k=1}^{r} p_k^{(1)} \omega_k, \frac{1}{q_2} \sum_{k=1}^{r} p_k^{(2)} \omega_k \right) \tag{1}$$

and denote by ϱ the greatest common divisor of the q_i-s. Finally, let

$$Q_i = q_i / \varrho \quad \text{and} \quad y_i = \sum_{k=1}^{r} p_k^{(i)} \omega_k \quad (i = 1, 2).$$

Suppose now that the transformation T has an invariant set X.

To apply lemma 2, we define the functions $f(x)$ and $g(x)$ as follows: $f(\xi) = \max\limits_i q_i$, $g(\xi) = \max\limits_{i,k} |p_k^{(i)}|$ for ξ of the form (1). The condition (a) of lemma 2 is obviously satisfied.

LEMMA 4. *Condition* (b) *of lemma 2 is satisfied by the set X, the transformation T and the functions $f(x)$, $g(x)$ defined above.*

Proof of the lemma. Let $\eta = T(\xi)$. Then evidently

$$\eta = \left(\frac{G_1(y_1 Q_2, y_2 Q_1)}{\Delta_1 \varrho^{m_1} Q_1^{m_1} Q_2^{m_1}}, \frac{G_2(y_1 Q_2, y_2 Q_1)}{\Delta_2 \varrho^{m_2} Q_1^{m_2} Q_2^{m_2}} \right)$$

and $f(\eta) = \max\{\Delta_1(\varrho Q_1 Q_2)^{m_1}/\mu_1,\ \Delta_2(\varrho Q_1 Q_2)^{m_2}/\mu_2\}$, where μ_i is the greatest rational integral divisor of $\Delta_i \varrho^{m_i} Q_1^{m_i} Q_2^{m_i}$ which divides $G_i(y_1 Q_2, y_2 Q_1)$.

Write $Q^* = \max(Q_1, Q_2)$, $Q_* = \min(Q_1, Q_2)$, $N = \min(m_1, m_2)$, and suppose $f(\eta) \leqslant f(\xi)$. Then

$$\mu_i \geqslant \Delta_i(\varrho Q^*)^{m_i - 1} Q_*^{m_i}. \tag{2}$$

Let $\nu = (\mu_1, \mu_2)$. We have

$$\mu_1 \mu_2 \mid \nu \cdot \Delta_1 \cdot \Delta_2 (\varrho Q_1 Q_2)^{\max(m_1, m_2)}.$$

Thus by (2)

$$\nu \geqslant \varrho^{N-2}(Q^*)^{N-2} Q_*^N \geqslant \varrho Q^* = f(\xi) \quad \text{as} \quad N \geqslant 3. \tag{3}$$

By applying lemma 1 to the forms $G_1(x, y)$, $G_2(x, y)$ we infer, after multiplying by suitable constants C_1, C_2, that for some forms f_1, f_2, g_1, g_2 with coefficients from K_0, and some exponents $a_0, a_1, a_2, b_0, b_1, b_2$ we have

$$f_1(x, y) G_1(x, y) x^{a_1} + f_2(x, y) G_2(x, y) x^{a_2} = C_1 x^{a_0},$$

$$g_1(x, y) G_1(x, y) y^{b_1} + g_2(x, y) G_2(x, y) y^{b_2} = C_2 y^{b_0}.$$

By putting here $x = y_1 Q_2$, $y = y_2 Q_1$ we see that ν divides $C_1(y_1 Q_2)^{a_0}$ and $C_2(y_2 Q_1)^{b_0}$.

Obviously, one can write $\nu = A_0 A_1 A_2 A_3$, where $A_0 \mid \Delta_1$, $A_1 \mid Q_1^{m_1}$, $A_2 \mid Q_2^{m_1}$, $A_3 \mid \varrho^{m_1}$. Now, $(A_1, Q_2) = 1$ and so no rational integral divisor $(\neq \pm 1)$ of A_1 divides $y_1 Q_2$. Hence A_1 can assume values only from a finite set (by lemma 3). Similar argument applies to A_2 and A_3. It follows that ν is bounded by a constant C depending on the transformation T only and we see by (3) that from $f(T(\xi)) \leqslant f(\xi)$ follows $f(\xi) \leqslant C$, which proves the lemma.

LEMMA 5. *Condition* (c) *of lemma* 2 *is satisfied by the set* X, *the transformation* T *and the functions* $f(x)$ *and* $g(x)$.

Proof. Suppose that

$$\lim_{j \to \infty} g(T(\xi_j)) / g(\xi_j)^{\max(m_1, m_2)} = 0 \tag{4}$$

for an infinite sequence $\{\xi_j\}$ with $f(\xi_j) \leqslant M$. Let

$$\xi_j = \left(\frac{1}{q_1^{(j)}} \sum_{k=1}^{r} p_{k,j}^{(1)} \omega_k,\ \frac{1}{q_2^{(j)}} \sum_{k=1}^{r} p_{k,j}^{(2)} \omega_k \right) = \left(\frac{1}{q_1^{(j)}} y_1^{(j)},\ \frac{1}{q_2^{(j)}} y_2^{(j)} \right).$$

Then evidently

$$g(T(\xi_j)) \geqslant \frac{1}{B_1} \max\{G_1(y_1^{(j)} q_2^{(j)}, y_2^{(j)} q_1^{(j)}),\ G_2(y_1^{(j)} q_2^{(j)}, y_2^{(j)} q_1^{(j)})\} \tag{5}$$

with some constant $B_1(M)$.

Without any restriction we can suppose, by considering a subsequence if necessary, that $g(\xi_j) = |p^{(t)}_{k_0,j}|$ with fixed t and k, and, moreover, that there exist

$$\delta^{(s)}_k = \lim_{j\to\infty} \frac{p^{(s)}_{k,j}}{p^{(t)}_{k_0,j}} \quad (s = 1, 2;\ k = 1, \ldots, r)$$

and that $q^{(j)}_1, q^{(j)}_2$ do not depend on j. Then, for $k = 1, 2$,

$$G_k(y^{(j)}_1 q_2, y^{(j)}_2 q_1) = \sum_{i=1}^{r} \hat{G}^{(k)}_i \omega_i, \tag{6}$$

where $\hat{G}^{(1)}_i, \hat{G}^{(2)}_i$ $(i = 1, 2, \ldots, r)$ are homogeneous forms with rational integral coefficients in $2r$ variables $p^{(1)}_1, \ldots, p^{(r)}_2$, of degrees m_1 and m_2 respectively. From (4) and (5) it follows that

$$\lim_{j\to\infty} \frac{\hat{G}^{(k)}_j(p^{(1)}_{1,j}, \ldots, p^{(r)}_{2,j})}{|p^{(t)}_{k_0,j}|^{m_k}} = 0 \quad (k = 1, 2).$$

Thus we obtain

$$\hat{G}^{(k)}_j(\delta^{(1)}_1, \ldots, \delta^{(r)}_1, \delta^{(1)}_2, \ldots, \delta^{(r)}_2) = 0.$$

As (6) is an identity in $p^{(k)}_i$, we have

$$G_i(q_2 \sum_{k=1}^{r} \delta^{(k)}_1 \omega^{(\nu)}_k, q_1 \sum_{k=1}^{r} \delta^{(k)}_2 \omega^{(\nu)}_k) = 0 \quad \text{for} \quad i = 1, 2,$$

where $\omega^{(\nu)}_k$ $(\nu = 1, 2, \ldots, r)$ are conjugates of ω_k in K. From the last equality and from the fact that G_1 and G_2 have no common factor it follows that

$$\sum_{k=1}^{r} \delta^{(k)}_1 \omega^{(\nu)}_k = \sum_{k=1}^{r} \delta^{(k)}_2 \omega^{(\nu)}_k = 0$$

for $\nu = 1, 2, \ldots, r$. But $\delta^{(t)}_{k_0} = 1$, hence $\det \|\omega^{(\nu)}_k\| = 0$, which is clearly impossible. Thus (4) is impossible and so

$$g\big(T(\xi_j)\big) \geqslant B_2 g(\xi_j)^{\max(m_1,m_2)} \geqslant B_2 g(\xi_j)^3$$

for some positive constant B_2. Consequently, $g\big(T(\xi)\big) \leqslant g(\xi)$ implies $g(\xi) \leqslant B_2^{-1/2}$, which proves the lemma.

Now the Theorem follows directly by lemma 2.

One can remark that theorem I in [1] is a consequence of the theorem proved above. Indeed, suppose that $P(t)$ is a polynomial with coefficients from K, of degree at least two, and $X \subset K$ is such that $P(X) = X$. Consider the transformation T of K_2 defined by $(x, y) \to \big(y^m P(x/y), y^3\big)$,

if the degree m of $P(t)$ is at least 3, and by $(x, y) \to (y^2 P(x/y), y^2)$, if $m = 2$. Then the set $Y = \{(a, 1) \mid a \in X\} \subset K_2$ is invariant under T and, consequently, it must be finite. This implies the finiteness of X too.

REFERENCES

[1] W. Narkiewicz, *On polynomial transformations*, Acta Arithmetica 7 (1962), p. 241-249.

[2] — *On polynomial transformations, II*, ibidem 8 (1962), p. 11-19.

[3] — *Remark on rational transformations*, Colloquium Mathematicum 9 (1962), p. 135-138.

MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCES
MATHEMATICAL INSTITUTE OF THE WROCŁAW UNIVERSITY

Reçu par la Rédaction le 6. 6. 1963