ACTA ARITHMETICA
XI (1965)

On polynomial transformations in several variables

by

W. Narkiewicz (Wrocław)*

1. In [1] and [2] it has been proved that a transformation defined by a nonlinear polynomial in one variable acting in a finitely generated extension of rationals cannot have infinite invariant sets. Now we consider the case of several variables and prove the following

Theorem. *Let K be an algebraic number field. Let $F_1(x_1, \ldots, x_N), \ldots, F_N(x_1, \ldots, x_N)$ be nonlinear polynomials with coefficients in K such that their leading forms have no nontrivial common zero in Z^N, where Z is the field of complex numbers. Then the transformation T:*

$$(x_1, \ldots, x_N) \to \big(F_1(x_1, \ldots, x_N), \ldots, F_N(x_1, \ldots, x_N)\big)$$

has no infinite invariant sets in K^N.

A special case ($N = 2$, and all F_i are forms of a degree at least 3) of that theorem has been proved in [3].

One can ask whether all assumptions are essential. It is trivial that for every system of N forms $G_1(x_1, \ldots, x_N), \ldots, G_N(x_1, \ldots, x_N)$ over K which have a nontrivial common zero (and thus have an infinite number of them) one can find polynomials $F_1, \ldots, F_N$ having $G_1, \ldots, G_N$ as their leading forms and such that the transformation defined by them has an infinite invariant set in a suitable extension of K. Indeed, the polynomials $F_i = G_i + x_i$ $(i = 1, \ldots, N)$ and the set $\{(a_1, \ldots, a_N)\colon G_i(a_1, \ldots \ldots, a_N) = 0, i = 1, \ldots, N\}$ are suitable.

However, if one is concerned with forms only, it seems that the conditions can be relaxed. It has been proved in [4] that if $N = 2$ and K is a quadratic extension of rationals with a negative discriminant, then the theorem remains true for pairs of forms $F_1(x, y), F_2(x, y)$ which have a common factor $F_0(x, y)$ such that F_1/F_0 and F_2/F_0 have no nontrivial zero in common if we impose some restriction on the degree of F_0. The method is based on the fact that the norm in such a field is positive-definite, but it seems that the result will hold for arbitrary fields.

* During the preparation of this paper the author held a British Council Scholarship at the University College, London.

The second possible weakening of our assumptions is to replace the condition "F_i are polynomials" by the condition "F_i are rational functions". In this direction only the case of rational functions in one variable over the rationals has been settled, and it has been proved that only homographies $(ax+b)/(cx+d)$ can have infinite invariant sets (see [5]), but it is very probable that the same result will hold for other algebraic number fields.

Another open question is whether one can replace the condition "G_i have no nontrivial common zero in Z^N" by the condition "G_i have no nontrivial common zero in K^N".

Finally, consider polynomials $F_i(x_1, \ldots, x_N)$ $(i = 1, \ldots, N)$ over K such that the transformation defined by them has an infinite invariant set in L^N, where L is an algebraic extension of K. Is it true that it must have an infinite invariant set in K^N?

The original proof of the theorem was based on another choice of function $f(x)$ occurring in Lemma 5, and was valid only for polynomials of sufficiently great degrees, satisfying some additional restrictions. The author is grateful to Dr. J. W. S. Cassels for his observation that the replacement of our function $f(x)$ by another simplifies the proof of Lemma 5, which is then valid in full generality.

2. The proof of the theorem is based on the following

LEMMA 1. (See [1], Lemma 1). *Let T be a transformation of a set X onto itself. Suppose there exist functions $f(x)$, $g(x)$ defined on X, with values in the set of natural numbers, subject to the following conditions:*

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

(ii) *There exists a constant C such that $f(x) \geqslant C$ implies $f(Tx) > f(x)$,*

(iii) *To every constant M there corresponds a constant $B(M)$ such that $f(x) \leqslant M$ and $g(x) \geqslant B(M)$ imply $g(Tx) > g(x)$.*

Then the set X must be finite.

LEMMA 2. *Suppose the theorem is true in the case where all polynomials $F_i(x_1, \ldots, x_N)$ are homogeneous. Then it is true in the general case also.*

Proof. Suppose that the polynomials $F_i(x_1, \ldots, x_N)$ $(i = 1, 2, \ldots, N)$ satisfy the assumptions of our theorem. We can write them in the form

$$F_i(x_1, \ldots, x_N) = \sum_{j=0}^{n_i} G_j^{(i)}(x_1, \ldots, x_N) \qquad (i = 1, \ldots, N),$$

where $G_j^{(i)}$ are forms of degree j, and n_i is the degree of F_i.

Let us now introduce the auxiliary forms

$$H_i(x_1, \ldots, x_{N+1}) = \sum_{j=0}^{n_i} x_{N+1}^j G_{n_i-j}^{(j)}(x_1, \ldots, x_N) \qquad (i = 1, \ldots, N),$$
$$H_{N+1}(x_1, \ldots, x_{N+1}) = x_{N+1}^2.$$

If for some complex $a_1, \ldots, a_{N+1}$, $H_i(a_1, \ldots, a_{N+1}) = 0$ for $i = 1, \ldots, N+1$, then $a_{N+1} = 0$ and $G_{n_i}^{(i)}(a_1, \ldots, a_{N+1}) = 0$ for $i = 1, \ldots, N$, which implies $a_1 = \ldots = a_N = 0$. Consequently the transformation T' defined by the forms H_i has no infinite invariant sets in K^{N+1}. If a set $X \subset K^N$ is invariant under the transformation T defined by the F_i's then the set $Y = \{(y_1, \ldots, y_N, 1)\colon (y_1, \ldots, y_N) \epsilon X\}$ is invariant under T'; hence it is finite and the finiteness of X follows.

LEMMA 3. *If $W_i(x_1, \ldots, x_N)$ $(i = 1, \ldots, N)$ are forms over K with no nontrivial common zero in Z^N, then there exist forms $V_j^{(i)}(x_1, \ldots, x_N)$ with coefficients integral in K, nonnegative exponents $a_1, \ldots, a_N$ and constants $C_i \neq 0$ integral in K such that*

$$\sum_{j=1}^{N} V_j^{(i)}(x_1, \ldots, x_N) W_j(x_1, \ldots, x_N) = C_i x_i^{a_i} \qquad (i = 1, \ldots, N).$$

The lemma is an easy consequence of a special case of Hilbert's Nullstellensatz (cf. [6], vol. II, p. 5).

LEMMA 4. *Suppose $a_1, \ldots, a_N$ are integers in K and $b_1, \ldots, b_N$ are natural numbers. Then there exists a constant A depending on $a_1, \ldots, a_N$, $b_1, \ldots, b_N$ only and such that if M is a rational integer which for some $z_1, \ldots, z_N$ integral in K divides $a_i z_i^{b_i}$ $(i = 1, \ldots, N)$ but no rational integral $\neq \pm 1$ divisor of M divides all the numbers $z_1, \ldots, z_N$, then $|M| \leqslant A$.*

Proof. Suppose M has the following factorization into primes: $M = \pm \prod_{i=1}^{t} p_i^{c_i}$. Let $P_k = \{p\colon p$ divides M, p does not divide $z_k\}$, and let $M_k = \prod_{p_i \epsilon P_k} p_i^{c_i}$. Observe now that M_k divides $a_k z^{b_k}$, but no rational integral $\neq \pm 1$ divisor of M_k divides z_k. By Lemma 2 of [1] it follows that $M_k \leqslant A_k$ with some constant A_k and, since obviously $|M| \leqslant \prod_{k=1}^{N} M_k$, the lemma follows.

3. Henceforth we assume that the transformation considered is defined by forms. We can do this in view of Lemma 2. Let us fix an integral basis $\omega_1, \ldots, \omega_m$ of K. Then every element ξ of K^N has a unique representation in the form

$$\xi = \left(\frac{p_1^{(1)}\omega_1 + \ldots + p_m^{(1)}\omega_m}{q}, \ldots, \frac{p_1^{(N)}\omega_1 + \ldots + p_m^{(N)}\omega_m}{q}\right), \tag{1}$$

where $p_1^{(1)}, \ldots, p_m^{(N)}$, q are rational integers, q is positive and

$$(p_1^{(1)}, \ldots, p_m^{(N)}, q) = 1. \tag{2}$$

It follows that the functions $f(\xi) = q$, $g(\xi) = \max_{i,j}\{|p_j^{(i)}|\}$ are well-defined. Obviously they satisfy the condition (i) of Lemma 1.

Let $F_i(x_1, \dots, x_N)$ $(i = 1, \dots, N)$ be nonlinear forms over K without a nontrivial common zero in Z^N, and let T be the transformation defined by them in K^N. Let D be the least positive rational integer such that the forms $F_i^* = DF_i$ have coefficients integral in K.

LEMMA 5. *There exists a constant C depending on the forms $F_1, \dots, F_N$ and the field K and such that $f(\xi) \geqslant C$ implies $f(T\xi) > f(\xi)$.*

Proof. If ξ has the form (1), then

$$(3)\qquad T(\xi) = \{F_1^*(P_1, \dots, P_N)/Dq^{n_1}, \dots, F_N^*(P_1, \dots, P_N)/Dq^{n_N}\}$$
$$= \{q^{R-n_1}F_1^*(P_1, \dots, P_N)/Dq^R, \dots, q^{R-n_N}F_N^*(P_1, \dots, P_N)/Dq^R\},$$

where n_i is the degree of F_i $(i = 1, \dots, N)$, $R = \max(n_1, \dots, n_N)$ and $P_i = p_1^{(i)}\omega_1 + \dots + p_m^{(i)}\omega_m$.

It follows that $f(T\xi) \geqslant q^R/\mu$, where μ is the greatest natural divisor of q^R that divides the numbers $q^{R-n_i}F_i^*(P_1, \dots, P_N)$ for all $i = 1, \dots, N$. If $r = \min(n_1, \dots, n_N)$, then μ must divide $q^{R-r}F_i^*(P_1, \dots, P_N)$ $(i = 1, \dots, N)$; hence if ν is the greatest natural divisor of q^R that divides the numbers $F_i^*(P_1, \dots, P_N)$ for all $i = 1, \dots, N$, then $\mu \leqslant q^{R-r}\nu$.

We shall prove that $\nu \ll 1$, and that will be sufficient for the proof of our lemma, since then $\mu \ll q^{R-r}$ and so $f(T\xi) \gg q^R \geqslant q^2 = f(\xi)^2$; hence the inequality $f(T\xi) \leqslant f(\xi)$ can hold only for $f(\xi) \ll 1$.

From Lemma 3 follows the existence of forms $V_j^{(i)}$ with coefficients integral in K, nonnegative rational integers $a_1, \dots, a_N$ and constants C_i integral in K such that

$$(4)\qquad \sum_{j=1}^{N} V_j^{(i)}(x_1, \dots, x_N)F_j^*(x_1, \dots, x_N) = C_i x_i^{a_i} \qquad (i = 1, \dots, N).$$

By putting $x_i = P_i$ we infer that ν must divide $C_iP_i^{a_i}$ for $i = 1, \dots, N$. If a certain natural divisor of ν divides all the numbers $P_1, \dots, P_N$, then, since it divides q^R, it must be equal to 1 by (2). Now it follows from Lemma 4 that $\nu \ll 1$, and so the lemma is proved.

LEMMA 6. *For every fixed M it follows from $f(\xi) \leqslant M$ that $g(T\xi) \gg g(\xi)^r$.*

Proof. Suppose that for a sequence $\{\xi_k\}$ in K^N we have $f(\xi) \leqslant M$ and

$$(5)\qquad \lim_{k\to\infty} \frac{g(T\xi_k)}{g(\xi_k)^r} = 0.$$

We can freely assume, choosing if necessary a subsequence, that $g(\xi_k) = |p_{j_0}^{(i_0)}|$ for $k = 1, 2, \dots$ with i_0, j_0 independent of k and that there exist limits

$$\lim_{k\to\infty} \frac{p_j^{(i)}}{p_{j_0}^{(i_0)}} = \vartheta_j^{(i)}.$$

(Here $p_j^{(i)}$ are actually functions of k, but for simplicity we shall not indicate this explicitly).

Let $\omega_1^{(\nu)}, \dots, \omega_m^{(\nu)}$ $(\nu = 1, \dots, m)$ be conjugates of $\omega_1, \dots, \omega_m$. For arbitrary complex $t_j^{(i)}$ $(i = 1, \dots, N;\ j = 1, \dots, m)$ the following identities hold:

$$(6)\qquad F_i^*(t_1^{(1)}\omega_1^{(\nu)} + \dots + t_m^{(1)}\omega_m^{(\nu)}, \dots, t_1^{(N)}\omega_1^{(\nu)} + \dots + t_m^{(N)}\omega_m^{(\nu)})$$
$$= \sum_{j=1}^{m} \Phi_j^{(i)}(t_1^{(1)}, \dots, t_m^{(N)})\,\omega_m^{(\nu)},$$

where $\Phi_k^{(i)}$ are forms of degree n_i in mN variables, with rational integral coefficients, independent of the choice of ν.

From (3) follows

$$g(T\xi_k) \gg \max_{i,j} |\Phi_j^{(i)}(p_1^{(1)}, \dots, p_m^{(N)})|.$$

Now (5) implies

$$\lim_{k\to\infty} \frac{\Phi_j^{(i)}(p_1^{(1)}, \dots, p_m^{(N)})}{(p_{j_0}^{(i_0)})^r} = 0$$

and *a fortiori*

$$\lim_{k\to\infty} \frac{\Phi_j^{(i)}(p_1^{(1)}, \dots, p_m^{(N)})}{(p_{j_0}^{(i_0)})^{n_i}} = 0;$$

hence

$$\Phi_j^{(i)}(\vartheta_1^{(1)}, \dots, \vartheta_m^{(N)}) = 0$$

for $i = 1, \dots, N$; $j = 1, \dots, m$.

Now by (6) we get

$$F_i^*(\vartheta_1^{(1)}\omega_1^{(\nu)} + \dots + \vartheta_m^{(1)}\omega_m^{(\nu)}, \dots, \vartheta_1^{(N)}\omega_1^{(\nu)} + \dots + \vartheta_m^{(N)}\omega_m^{(\nu)}) = 0$$

for $i = 1, \dots, N$, $\nu = 1, \dots, n$, and it follows that

$$\vartheta_1^{(i)}\omega_1^{(\nu)} + \dots + \vartheta_m^{(i)}\omega_m^{(\nu)} = 0$$

for $i = 1, \dots, N$, $\nu = 1, \dots, m$, and in particular

$$\vartheta_1^{(i_0)}\omega_1^{(\nu)} + \dots + \vartheta_m^{(i_0)}\omega_m^{(\nu)} = 0$$

for $\nu = 1, \dots, m$.

Since $\vartheta_{j_0}^{(i_0)} = 1 \neq 0$ it follows that

$$\operatorname{Det} \|\omega_j^{(\nu)}\|_{j,\nu=1}^{m} = 0,$$

which is clearly impossible. The contradiction obtained proves the lemma.

Since $r > 1$, it follows that the inequality $g(T\xi) \leqslant g(\xi)$ under the assumption $f(\xi) \leqslant M$ implies $g(\xi) \ll 1$.

If we now have a set X such that $T(X) = X$, we can, in view of the Lemmas 5 and 6, apply Lemma 1 to get the finiteness of X. The theorem is thus proved.

References

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

[2] — *On polynomial transformations II*, Acta Arith. 8 (1962), pp. 11 - 19.

[3] — *On transformations by polynomials in two variables*, Colloq. Math. 12 (1964), pp. 53 - 58.

[4] — *On transformations by polynomials in two variables II*, Colloq. Math. 13 (1964), pp. 101-106.

[5] — *Remark on rational transformations*, Colloq. Math. 10 (1963), pp .139 - 142.

[6] B. L. van der Waerden, *Moderne Algebra*, Berlin-Göttingen-Heidelberg.

INSTITUTE OF MATHEMATICS OF THE POLISH ACADEMY OF SCIENCES
INSTITUTE OF MATHEMATICS, WROCLAW UNIVERSITY
UNIVERSITY COLLEGE, LONDON

Reçu par la Rédaction le 8. 9. 1964

ACTA ARITHMETICA
XI (1965)

Grenzkreisgruppen und kettenbruchartige Algorithmen

von

M. Eichler (Basel)

§ 1. Einleitung. Eine reelle Zahl ϱ läßt sich auf mannigfache Weise in einen Kettenbruch

$$\varrho = m_0+1/m_1+\ldots+1/m_{i-1}+\varrho_i^{-1} \tag{1}$$

mit ganzen rationalen m_i entwickeln. U. a. gibt es genau einen *regelmäßigen* Kettenbruch mit

$$0 \leqslant \varrho_i - m_i < 1. \tag{2}$$

Will man speziell einen gekürzten Bruch $\varrho = a/c$ in einen Kettenbruch entwickeln, so kann man auch wie folgt verfahren. Man bestimmt ganze rationale b, d so, daß $ad-bc = 1$ ist und stellt die Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

ein Element der elliptischen Modulgruppe Γ, durch die beiden Erzeugenden

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

in der Weise

$$A = T^{n_0}JT^{n_1}J\ldots T^{n_l}J \tag{3}$$

dar. Dann ist

$$\frac{a}{c} = \begin{cases} n_0-1/n_1+\ldots+(-1)^l/n_l & \text{für} \quad n_l \neq 0, \\ n_0-1/n_1+\ldots+(-1)^{l-2}/n_{l-2} & \text{für} \quad n_l = 0. \end{cases} \tag{4}$$

Die Kettenbrüche (1) und (4) stimmen überein, wenn

$$-n_1, n_2, \ldots, (-1)^{l-1}n_{l-1} > 0, \quad (-1)^l n_l \geqslant 0 \tag{5}$$

ist. Durch (5) ist die Darstellung (3) von A eindeutig festgelegt.

Sei F ein Fundamentalbereich von Γ. Dann ist unter der Voraussetzung (3) und $n_0 < 0$

$$F,\ T^{-1}(F), \ldots,\ T^{n_0}(F),\ T^{n_0}J(F), \ldots, A(F)$$