ACTA ARITHMETICA
VIII (1962)

On polynomial transformations II

by

W. Narkiewicz (Wrocław)

1. We say that a subset X of a field K has property (P) if and only if every polynomial $P(t)$ with coefficients from K such that $P(X) = X$ is linear. We say that X has property (P_H) (i.e. property (P) hereditarily) if every infinite subset of X has property (P). It has been proved in [1] that the algebraic number fields have property (P_H) and, moreover, that this property is preserved by any pure transcendental, finitely generated extension of a field having this property. In this paper we prove:

THEOREM I. *If every finite algebraic extension of a number field has property* (P_H), *then every field of algebraic functions in any number of variables over K has property* (P_H).

THEOREM II. *If the field K has property* (P_H), *then every pure transcendental extension of K has this property also.*

From theorem I and from theorem I of [1] it follows that every field finitely generated over the rationals has property (P_H).

2. Proof of theorem I.

FUNDAMENTAL LEMMA (see [1], lemma 1). *Suppose Tx is a transformation of the set X onto itself. Suppose there exist two functions $f(x)$ and $g(x)$ defined on X, with values in the set of natural numbers, subject to the 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 $g(x) \geqslant B(M)$ follows $g(Tx) > g(x)$.*

Then X is finite.

Now let K be a number field such that every finite algebraic extension of K has property (P_H), and let R be a field of algebraic functions over K. Without restriction in generality we can assume that R is a normal extension of K and, moreover, that R is an algebraic functions field in one variable, since every algebraic functions field in a finite number of variables over a number field can be imbedded in the field of complex numbers, and the case when R is a field of algebraic functions in an infinite number of variables can be easily reduced to the finite case by theorem II proved below.

Let $\omega_1(x), \ldots, \omega_m(x)$ be an integral basis of R. The conjugate bases will be denoted by $\omega_1^{(r)}(x), \ldots, \omega_m^{(r)}(x)$ $(r = 1, \ldots, m)$. The elements of R can be treated as functions of the complex variable, defined in a strip $S = \{\sigma + it\colon \sigma \geqslant \sigma_0, |t| \leqslant t_0\}$ which is chosen in such a manner that no function $\omega_k^{(r)}$ has a singularity in S and the coefficients $\gamma_j^{(k)}(x)$ in the equalities $\omega_k'(x) = \sum_{j=1}^{m} \gamma_j^{(k)}(x)\omega_k(x)$ have no poles in S $(k = 1, \ldots, m)$.

Every element of R can be represented in the form:

$$\xi(x) = \frac{1}{Q(x)}\big(P_1(x)\omega_1(x) + \ldots + P_m(x)\omega_m(x)\big),$$

where $P_1, \ldots, P_m, Q$ are polynomials over K and $(P_1, \ldots, P_m, Q) = 1$. Let us define $f(\xi) = $ degree of Q, $g(\xi) = \max_k$ degree P_k. These functions are uniquely determined when the basis is fixed. The integral elements of R are characterized by $f(\xi) = 0$.

Let $W(t)$ be a polynomial with coefficients from R, of degree $n \geqslant 2$, and let X be a subset of R such that $W(X) = X$. We shall write $W(t)$ in the form

$$W(t) = \frac{1}{\Delta(x)} \sum_{j=0}^{n} A_j(x) t^j,$$

where $\Delta(x)$ is a polynomial and $f\big(A_j(x)\big) = 0$ for $j = 0, \ldots, n$.

Lemma 1. *For every c the equation $f(\xi) + g(\xi) = c$ has in X at most a finite number of solutions.*

Proof. Let $\{r_i\}$ be a sequence of numbers from $K \cap S$ satisfying the condition:

$$\Delta(r_i) A_n(r_i) \neq 0 \quad \text{for} \quad i = 1, 2, \ldots$$

Since the points r_i lie in S, they are regular points for the functions $\omega_j(x)$ (treated as functions of a complex variable) and so there exist finite limits:

$$\lim_{x \to r_i} \omega_j(x).$$

Now we prove that if $\xi(x) \in R$, then $\lim_{x \to r_i} |\xi(x)| = \infty$ or

$$\lim_{x \to r_i} \xi(x) \in K\big(\omega_1(r_i), \ldots, \omega_m(r_i)\big).$$

Indeed, suppose that in a neighbourhood of r_i the function $\xi(x)$ is bounded. If $Q(r_i) \neq 0$ then

$$\lim_{x \to r_i} \xi(x) = \frac{1}{Q(r_i)} \sum_{k=1}^{m} P_k(r_i)\omega_k(r_i) \in K\big(\omega_1(r_i), \ldots, \omega_m(r_i)\big).$$

If $Q(r_i) = Q'(r_i) = \ldots = Q^{(s-1)}(r_i) = 0$, but $Q^{(s)}(r_i) \neq 0$, then

$$\lim_{x \to r_i} \xi(x) = \frac{1}{Q^{(s)}(r_i)} \lim_{x \to r_i} \frac{d^s}{dx^s}\Big[\sum_{k=1}^{m} P_k(x)\omega_k(x)\Big].$$

From the definition of S it follows that the functions $d^s\omega_k/dx^s$ have no poles in S; consequently

$$\frac{d^s}{dx^s}\Big(\sum_{k=1}^{m} P_k(x)\,\omega_k(x)\Big)\Big|_{x=r_i} \in K\big(\omega_1(r_i), \ldots, \omega_m(r_i)\big)$$

and

$$\lim_{x \to r_i} \xi(x) \in K\big(\omega_1(r_i), \ldots, \omega_m(r_i)\big).$$

Let us define

$$W_i(t) = \frac{1}{\Delta(r_i)} \sum_{j=0}^{n} A_j(r_i) t^j, \qquad X_i = \{\lim_{x \to r_i} \xi(x)\colon\ \xi \in X,\ \lim_{x \to r_i} |\xi(x)| \neq \infty\}.$$

The foregoing argument shows that $X_i \subset K\big(\omega_1(r_i), \ldots, \omega_m(r_i)\big)$. Moreover, the polynomials $W_i(t)$ have the degree $n \geqslant 2$, and their coefficients belong to $K\big(\omega_1(r_i), \ldots, \omega_m(r_i)\big)$. Now we prove that $W_i(X_i) = X_i$. Let $\xi \in X_i$. Hence there exists $\Xi(x) \in X$ such that $\lim_{x \to r_i} \Xi(x) = \xi$; thus, since $W(X) = X$, there exists $U(x) \in X$ such that $W\big(U(x)\big) = \Xi(x)$, i.e.:

$$\Xi(x) = \frac{1}{\Delta(x)} \sum_{j=0}^{n} A_j(x) U^j(x)$$

and we obtain

$$|\Xi(x)| \geqslant \left|\frac{A_n(x)U^n(x)}{\Delta(x)}\right| - \left|\frac{1}{\Delta(x)} \sum_{j=0}^{n-1} A_j(x) U^j(x)\right|.$$

In a neighbourhood of r_i we have

$$\left|\frac{1}{\Delta(x)} \sum_{j=0}^{n-1} A_j(x) U^j(x)\right| \leqslant B|U(x)|^{n-1}$$

and, since $A_n(r_i) \neq 0$,

$$\left|\frac{1}{\Delta(x)} A_n(x) U^n(x)\right| \geqslant B_1 |U(x)|^n.$$

Now if $\lim_{x\to r_i}|U(x)| = \infty$, then

$$\left|\frac{\Xi(x)}{U^{n-1}(x)}\right| \geqslant B_1|u(x)| - B \to \infty \quad \text{as} \quad x \to r_i,$$

but this is impossible, since from $n \geqslant 2$ we infer that

$$\left|\frac{\Xi(x)}{U^{n-1}(x)}\right| \leqslant \frac{B_2|\xi|}{|U(x)|^{n-1}} \to 0 \quad \text{as} \quad x \to r_i.$$

Thus there exists a finite limit $u = \lim_{x\to r_i} U(x)$, $u \in X$, and obviously $W_i(u) = \xi$, whence $X_i \subset W_i(X_i)$. On the other hand, if $U(x) \in X$, $W(U(x)) = \Xi(x)$ and $\lim_{x\to r_i} U(x) = u \neq \infty$, then $\lim_{x\to r_i}\Xi(x) = W_i(u) \neq \infty$; consequently $W_i(u) \in X_i$ and so $X_i \supset W_i(X_i)$, which together with the inclusion formerly established gives $W_i(X_i) = X_i$.

Now let us remark that the field $K(\omega_1(r_i), \ldots, \omega_m(r_i))$ is for $r_i \in K$ a finite algebraic extension of K, and so this field possesses property (P_H); consequently the sets X_i must be finite. Since the sequence r_i is infinite, one infers without difficulty that there can be only a finite number of elements ξ in X such that $f(\xi) + g(\xi)$ is equal to a fixed c.

We have thus proved that our set X, the polynomial $W(t)$ and the functions $f(\xi)$, $g(\xi)$ defined as above satisfy condition (a) of our fundamental lemma. Now we are going to prove that the remaining two conditions are also satisfied.

LEMMA 2. *Let L be a principal ideal domain and L' its integral closure in a finite algebraic, normal, separable extension $\mathcal{K}'$ of the quotient field $\mathcal{K}$ of L. Then, for every fixed b in L' and every natural number n, there can be only a finite number of a in L such that, with some c in L', a divides bc^n in L' but no non-unit divisor of a in L divides c.*

The proof of this lemma in the case where L is the ring of rational integers was given in [1] (lemma 2). The proof in the general case is almost literally the same. One need only remark that L' is a Dedekind domain (see [3], p. 281) and that in L there is only a finite number of prime-ideals which ramify in L' (see [3], p. 303).

COROLLARY. *Let $A(x)$ be a fixed integral algebraic function from R, and let n be a positive integer. There exist only a finite number of polynomials $U(x)$ with coefficients from K such that for a certain integral algebraic function $V(x)$ from R, the quotient $A(x)V^n(x)/U(x)$ is integral in R and simultaneously for no non-constant polynomial $\Phi(x)$ over K dividing $U(x)$ the quotient $V(x)/\Phi(x)$ is integral in R.*

For the proof one should observe that the ring of polynomials over a field is a principal ideal domain.

LEMMA 3. *Let $A(x)$ be an integral algebraic function from R ($A(x) \not\equiv 0$), and let n be a positive integer. Then*

$$\psi(A) = \inf_{f(\xi)=0} \{g(A\xi^n) - ng(\xi)\} \neq -\infty.$$

Proof. Let $A(x) = A_1(x)\omega_1(x) + \ldots + A_m(x)\omega_m(x)$, where A_j are polynomials over K. For every m functions $f_1(x), \ldots, f_m(x)$ defined in S the following identity holds:

$$\Big(\sum_{k=1}^{m} A_k(x)\omega_k^{(r)}(x)\Big)\Big(\sum_{k=1}^{m} f_k(x)\omega_k^{(r)}(x)\Big)^n = \sum_{k=1}^{m} T_k(f_1, \ldots, f_m)\,\omega_k^{(r)}(x) \qquad (r = 1, \ldots, m),$$

where T_k are homogeneous forms of n-th degree of m variables, with coefficients which depend only on A and n and are polynomials over K. Suppose that

$$g(A\xi_j^n) - ng(\xi_j) \to -\infty, \qquad \xi_j(x) = \sum_{k=1}^{m} P_k^{(j)}(x)\,\omega_k(x).$$

We can assume that $g(\xi_j) =$ degree of $P_{k_0}^{(j)}$, $j = 1, 2, \ldots$, and that

$$g(A\xi_j^n) - ng(\xi_j) \leqslant -j, \qquad j = 1, 2, \ldots$$

Let us define, for $x \in S$, $s(x) = \max_{k,r}|\omega_k^{(r)}(x)|$. Evidently

$$\text{degree of } T_k(P_1^{(j)}, \ldots, P_m^{(j)}) \leqslant \text{degree } [P_{k_0}^{(j)}]^n - j,$$

whence for $|x|$ sufficiently large (say, for $|x| \geqslant x_0(j)$)

$$\left|\frac{T_k(P_1^{(j)}(x), \ldots, P_m^{(j)}(x))}{[P_{k_0}^{(j)}(x)]^n}\right| \leqslant \frac{B(j)}{|x|^j}$$

and

$$\left|T_k\left(\frac{P_1^{(j)}(x)}{P_{k_0}^{(j)}(x)}, \ldots, \frac{P_m^{(j)}(x)}{P_{k_0}^{(j)}(x)}\right)\right| \leqslant \frac{B(j)}{|x|^j}.$$

By multiplication by $\omega_k^{(r)}(x)$ and addition, we obtain

$$\left|\sum_{k=1}^{m} T_k\left(\frac{P_1^{(j)}(x)}{P_{k_0}^{(j)}(x)}, \ldots, \frac{P_m^{(j)}(x)}{P_{k_0}^{(j)}(x)}\right)\omega_k^{(r)}(x)\right| \leqslant B(j)\frac{s(x)}{|x|^j} \qquad (r = 1, \ldots, m),$$

whence

$$\left|\Big(\sum_{k=1}^{m} B_k(x)\,\omega_k^{(r)}(x)\Big)\Big(\sum_{k=1}^{m} \frac{P_k^{(j)}(x)}{P_{k_0}^{(j)}(x)}\,\omega_k^{(r)}(x)\Big)^n\right| \leqslant B(j)\frac{s(x)}{|x|^j},$$

which gives

$$\left|\sum_{k=1}^{m} \frac{P_k^{(j)}(x)}{P_{k_0}^{(j)}(x)}\,\omega_k^{(r)}(x)\right| = O\left(\frac{s^{1/n}(x)}{x^{j/n}}\right) \qquad (j = 1, 2, \ldots;\ r = 1, \ldots, m).$$

(Here and below the constents in O depend on j but not on x.)

The function $s(x)$ cannot tend to infinity more rapidly than every polynomial. Suppose thus that $s(x) = o(x^{\mu})$ when $x \in S$ and x tends to infinity. Let

$$H_r^{(j)}(x) = \sum_{k=1}^{m} \frac{P_k^{(j)}(x)}{P_{k_0}^{(j)}(x)} \omega_k^{(r)}(x).$$

Then

$$H_r^{(j)}(x) = o(x^{(\mu-j)/n});$$

but $P_{k_0}/P_{k_0} = 1$, whence, if we denote by $d(x)$ the discriminant of the field R,

$$1 = \frac{1}{\sqrt{d(x)}} \begin{vmatrix} \omega_1^{(1)}(x), \ldots, H_1^{(j)}(x), \ldots, \omega_m^{(1)}(x) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \omega_1^{(m)}(x), \ldots, H_m^{(j)}(x), \ldots, \omega_m^{(m)}(x) \end{vmatrix} = O\Big(\sum |H_r^{(j)}(x)|\, s^{m-1}(x)\Big),$$

and consequently

$$1 = o(x^{\mu(m-1)+(\mu-j)/n}),$$

which is impossible for j sufficiently large. The contradiction obtained proves the lemma.

LEMMA 4. *There exists a constant C such that from $f(\xi) \geqslant C$ follows $f(W(\xi)) > f(\xi)$ for ξ in X.*

The proof of this lemma is analogous to the proof of lemma 4 in [1] but for completeness we give it in full.

Let

$$\xi(x) = \frac{1}{q(x)} \sum_{k=1}^{m} p_k(x)\omega_k(x), \qquad (p_1(x), \ldots, p_m(x), q(x)) = 1,$$

$$\bar{\xi}(x) = q(x)\xi(x),$$

$$W(\xi(x)) = \frac{1}{Q(x)} \sum_{k=1}^{m} P_k(x)\omega_k(x) = \frac{1}{\Delta(x) q^n(x)} \sum_{k=1}^{m} \bar{P}_k(x)\omega_k(x),$$

$$(P_1(x), \ldots, P_m(x), Q(x)) = 1,$$

($\Delta(x)$ and $A_n(x)$ used below have the same meaning as in lemma 1). Evidently $Q(x)$ divides $\Delta(x)q^n(x)$. Let us put $\mu(x) = \Delta(x)q^n(x)Q^{-1}(x)$ and $\nu(x) = (\mu(x), q(x))$. Observe now that

$$\sum_{k=1}^{m} P_k(x)\omega_k(x) = A_n(x)\bar{\xi}^n(x) + R(x)q(x),$$

where $R(x)$ is an integral algebraic function from K.

From $\nu(x) | \mu(x) | \bar{P}_k(x)$ follows $\nu(x) \Big| \sum_{k=1}^{m} \bar{P}_k(x)\omega_k(x)$, and thus we have $\nu(x) | A_n(x)\bar{\xi}^n(x)$. The application of the corollary to lemma 2 shows us that the degree of the polynomial $\nu(x)$ is bounded by a constant B depending only on $A_n(x)$ and n. Now since $\mu(x) = d_1(x)\nu(x)$, $q(x) = d_2(x)\nu(x)$ (d_1, d_2 relatively prime), $d_1(x)$ divides $\Delta(x)\nu^{n-1}(x)$ and consequently the degree of $\mu(x)$ is bounded by $nB +$ degree of Δ.

If $f(W(\xi)) \leqslant f(\xi)$ then evidently the degree of q is at least equal to degree of Δ + degree of $q^n(x)$ − degree of $\mu(x)$ and so the degree of $q(x)$ is at most equal to $nB/(n-1)$, which proves the lemma.

LEMMA 5. *For every constant M there exists a constant $B(M)$ such that from $f(\xi) \leqslant M$ and $g(\xi) \geqslant B(M)$ follows $g(W(\xi)) > g(\xi)$, for $\xi \in X$.*

Proof. The following inequalities result directly from the definitions of the functions $f(\xi)$ and $g(\xi)$:

$$f(a+b) \leqslant f(a) + f(b), \qquad f(ab) \leqslant f(a) + f(b),$$
$$g(a+b) \leqslant \max\{f(a), f(b)\} + \max\{g(a), g(b)\},$$
$$g(ab) \leqslant B' + g(a) + g(b) \quad \text{with a suitable } B'.$$

If Q is a polynomial, then

$$g(a) - \text{degree } Q \leqslant g(a/Q) \leqslant g(a).$$

Suppose $f(\xi) \leqslant M$. Then

$$(1) \qquad g\Big(\frac{1}{\Delta(x)} \sum_{j=0}^{n-1} A_j(x)\xi^j(x)\Big) \leqslant g\Big(\sum_{j=0}^{n-1} A_j(x)\xi^j(x)\Big) \leqslant (n-1)g(\xi) + M_1$$

with a suitable $M_1(M)$. Let $\xi = \bar{\xi}/Q$, where $\deg Q = f(\xi)$, and $f(\bar{\xi}) = 0$. Then

$$g\Big(\frac{1}{\Delta} A_n \xi^n\Big) \geqslant g(A_n\xi^n) - \deg\Delta = g(A_n\bar{\xi}^n/Q^n) - \deg\Delta$$
$$\geqslant g(A_n\bar{\xi}^n) - nf(\xi) - \deg\Delta \geqslant g(A_n\bar{\xi}^n) = nM - \deg\Delta$$
$$\geqslant ng(\bar{\xi}) + \Psi(B, n) - nM - \deg\Delta \geqslant ng(\xi) + \Psi(B, n) - nM - \deg\Delta.$$

If for a sequence $\{\xi_i\}$, with $f(\xi_i) \leqslant M$,

$$(2) \qquad \lim_{i\to\infty} [g(W(\xi_i)) - ng(\xi_i)] = -\infty,$$

then (since in view of lemma 1, $g(\xi_i)$ tends to infinity) we have

$$\Psi(B, n) \leqslant g\Big(\frac{1}{\Delta} A_n \xi_i^n\Big) - ng(\xi_i) + nM + \deg\Delta$$
$$= \deg\Delta + nM + g\Big(W(\xi_i) - \sum_{j=0}^{n-1} \frac{A_j}{\Delta}\xi_i^j\Big) - ng(\xi_i)$$
$$\leqslant \deg\Delta + nM + M_2 + \max\Big[g(W(\xi_i)), g\Big(\sum_{j=0}^{n-1} \frac{A_j}{\Delta}\xi_i^j\Big)\Big] - ng(\xi_i) \to -\infty$$

in view of (1) and (2), which is incompatible with lemma 3. Thus

$$g\big(W(\xi_i)\big) \geqslant ng(\xi_i) - M_3$$

with some M_3, whence the inequality $g\big(W(\xi_i)\big) \leqslant g(\xi_i)$ cannot be true for sufficiently large $g(\xi_i)$. The lemma is thus proved.

To prove the theorem it suffices now to observe that, in view of lemmas 4 and 5, conditions (b) and (c) of the fundamental lemma are satisfied, and lemma 1 ensures condition (a), whence the application of this lemma shows us that the set X is finite, which is what was to be proved.

3. Proof of theorem II.

LEMMA 6 (see [2], p. 188). *Let $\mathcal{L} = \mathcal{K}(\vartheta)$ be a simple transcendental extension of a field $\mathcal{K}$. Let us define for $\xi = A(\vartheta)/B(\vartheta) \in \mathcal{L}$, $\big((A(t), B(t)) = 1\big)$, $F(\xi) = \max(\text{degree } A, \text{degree } B)$. If $P(t)$ is a polynomial of degree m with coefficients from $\mathcal{K}$, then $F\big(P(\xi)\big) = mF(\xi)$.*

Now let $K = R(\{\vartheta_a\}_{a\in A})$ be a pure transcendental extension of a field R which possesses property ($\mathrm{P_H}$). Let Q be a polynomial with coefficients from K, of degree $n \geqslant 2$, and let X be a subset of K for which $Q(X) = X$. Since (see theorem II in [1]) every pure transcendental extension of R obtained by adjoining a finite set of elements has property ($\mathrm{P_H}$), we can assume that the coefficients of the polynomial Q belong to R, for otherwise we could obtain this by adjoining to R all the indeterminates which occur in the coefficients of Q.

Let us now remark that, if $\mathcal{L}$ is a simple transcendental extension of a field $\mathcal{K}$, then, from $X \subset \mathcal{L}$, $X\setminus\mathcal{K}$ being non-void, and $\bar{Q}(X) = X$, where $\bar{Q}$ is a polynomial over $\mathcal{K}$, it follows that $\bar{Q}$ is linear. Indeed, let $a \in X\setminus\mathcal{K}$ be such that $\min\limits_{\xi\in X\setminus\mathcal{K}} F(\xi) = F(a) \neq 0$, and let $\bar{Q}(\beta) = a$. Then from lemma 6 follows $nF(\beta) = F(a)$, whence $F(\beta) \neq 0$, i.e. $\beta \in X\setminus\mathcal{K}$ and so $F(\beta) \geqslant F(a) = nF(\beta)$, which can occur only if $n = 1$.

Now, if $X \subset R$, then the set is finite by the assumption. If there exists $\xi \in X\setminus R$ which, for example, has the form

$$\xi = \frac{A(\vartheta_{i_1}, \ldots, \vartheta_{i_s})}{B(\vartheta_{i_1}, \ldots, \vartheta_{i_s})},$$

then let $K = \mathcal{K}(\vartheta_{i_1})$ where $\mathcal{K} = R(\{\vartheta_a\}_{a\in A,\, a\neq i_1})$. Since $X\setminus\mathcal{K}$ is non-void, then from the preceding remark we infer that $n = 1$, contrary to our assumption. The theorem is thus proved.

It is worth remarking that, if a field K has property ($\mathrm{P_H}$) and X is a subset of K such that with a suitable non-linear polynomial $P(t)$, $P(X) \supset X$, then X must be finite. Indeed, let Y be the smallest set

containing X and closed under the mapping $x \to P(x)$. If X is infinite, then the coefficients of $P(t)$ belong to K, and so Y is contained in K. Moreover $P(Y) = Y$, and so Y is finite, which is impossible.

References

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

[2] E. Steinitz, *Algebraische Theorie der Körper*, Journal f. d. reine u. angew. Mathematik 137 (1910), pp. 167-309.

[3] O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Princeton 1959.

KATEDRA MATEMATYKI POLITECHNIKI WROCŁAWSKIEJ
DEPARTMENT OF MATHEMATICS, TECHNICAL UNIVERSITY OF WROCŁAW

Reçu par la Rédaction le 6. 3. 1962