On polynomial transformations

by

W. NARKIEWICZ (Wroclaw)

1. We shall say that a subset $X$ of a field $R$ has property $(P)$ if every polynomial $P(x)$ with coefficients from $R$ such that $P(X) = X$ is linear. It is easy to see that any number field in which the "Irreduzibilitätssatz" of Hilbert is true has property $(P)$. Consequently, any algebraic extension of the field of rational numbers has property $(P)$ and any number field which is transcendental extension of some (its) infinite subfield also has this property. (E.g. see [1], [3]). On the other hand, it is trivial that no finite set has property $(P)$. The problem can be posed, having a fixed number set $Z$, to characterize the subsets of $Z$ with property $(P)$. In this paper we solve this problem in the case where $Z$ is an algebraic number field. (By an algebraic number field we always understand a finite algebraic extension of the field of rational numbers.) Indeed, we shall prove

**Theorem I.** A subset $X$ of an algebraic number field has property $(P)$ if and only if it is infinite.

We shall say that a set $Z$ has property $(P)$ hereditarily if every infinite subset of $Z$ has property $(P)$. Thus algebraic number fields have property $(P)$ hereditarily. It turns out that also every finitely generated transcendental extension of an algebraic number field has property $(P)$ hereditarily. This follows from

**Theorem II.** Let $K$ be a finitely generated transcendental extension of a field $R$. Then $K$ has hereditarily property $(P)$ if and only if $R$ has this property. (The "only if" parts of our theorems are of course trivial.)

2. For the proof of our theorems we need the following

**Lemma 1.** Suppose that $T(x)$ is a transformation of the set $X$ onto itself. Suppose that 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 $f(x) \geq C$ follows $f(T(x)) > f(x)$.

Acta Arithmetica VII
For every constant $M$ there exists a constant $(B(M))$ such that if $f(x) \leq M$ and $g(x) \geq B(M)$ follows $g(T(x)) \geq g(x)$. Then $X$ is finite.

Proof of the lemma. Let $z \in X$. There exists a $z_{0} \in X$ such that $T(z_0) = z_0 = z$. Similarly there exists a $z_{1} \in X$ such that $T(z_1) = z_1 = z_{0}$ and so on. We thus obtain a set $A = \{z_{0}, z_{1}, \ldots, z_{n}\}$. Evidently $x = \bigcup z_{i}$. If $f(z_{0}) \leq C$ but $f(z_{n+1}) > C$, then $f(z_{n+1}) > f(z_{0}) = f(T(z_{n}))$ and by (b), $f(z_{n+1}) < C$, which is a contradiction. We thus have

(1) $f(z_{0}) \leq C = f(z_{n+1}) < C$.

If $f(z_{0}) > C$ but $f(z_{n+1}) \geq f(z_{n})$, then by (b), $f(z_{n+1}) < C < f(z_{n})$, which is a contradiction. We thus have

(2) $f(z_{0}) > C = f(z_{n+1}) < f(z_{n})$.

From (1) and (2) immediately follows max $f(x) \leq \max_{n \geq 0} f(x) = M_{0}$. For $x \in A_{0}$ we infer from (1) that: $g(x) \geq B(M_{0})$ then $g(T(x)) \geq g(x)$. In the same way as (1) and (2) we obtain

(1') $g(z_{0}) \leq B(M_{0}) \geq g(z_{n+1}) \leq B(M_{0})$,

(2') $g(z_{0}) > B(M_{0}) \geq g(z_{n+1}) > g(z_{0})$,

and similarly we see that $g(x)$ is bounded in $A_{0}$. From (a) it follows that for every $z \in X$ the set $A_{0}$ is finite; thus the sequence $x_{n}$ is periodical. From (2) we infer that in every $A_{0}$ there exists an $x_{n}$ such that $f(z_{n}) \leq C$. From the periodicity of $(z_{0})$ and (1) we see that $f(z_{n}) \leq C$ and so $M_{0}$ does not depend on $z$. Consequently $g(x)$ is in $A_{0}$ bounded by a constant independent of $z$. Thus $f(x) + g(x)$ is bounded in $X$ and from (a) we infer that $X$ is finite.

As a simple corollary to this lemma we obtain the following

**Theorem III.** If $X$ is a set of complex numbers such that $X^{(a)}$ is infinite but $X^{(b)}$ is void (where $X^{(n)}$ denotes the $n$-th derived set of $X$ and $n$ is finite), then $X$ has property (P).

(P) If $P(X) = X$ and $P(x) \neq ax + b$, then we put $f(x) = f_{0}, g(x) = 1, B(M) = 2$ for all $M$, and $C = 1 + \sup_{|P(x)| < |a|} j$. The conditions of lemma 1 are obviously satisfied, and thus we find that $X$ is finite—a contradiction which proves the theorem. (It can be proved, moreover, that if $X$ satisfies the conditions of theorem III and $P(x)$ is a polynomial with property $P(X) = X$, then $P(x) = ax + b$ where $a$ is a real number.)

3. We now proceed to the proof of theorem 1.

Let $K$ be an algebraic number field of degree $m$. Let us fix an integral basis of $K$: $(a_{0})_{1}^{m-1}$. By $(a_{0})_{1}^{m-1}$ we shall denote the conjugate basis in conjugate fields of $K$. Every number of $K$ can be represented in exactly one way in the form $a = \sum_{i=1}^{m} p_{i} a_{i}$, where $p_{1}, \ldots, p_{m}, q$ are rational integers, $(p_{1}, \ldots, p_{m}, q) = 1$ and $q > 0$. Let us define $f(x) = g$ and $g(x) = \max_{|P(x)|}$ (For the facts from algebraic number theory used here and in the sequel, see e.g. [2].)

Suppose that $X$ is an infinite subset of $K$, and $P(x)$ is a polynomial such that $P(X) = X$. We have to prove that $P(x) = ax + b$. Suppose that $P(x) \neq ax + b$. We can write: $P(x) = \max_{|P(x)|} a_{0} x^{b}$ where $A$ is a natural number, and $a_{0}$ are integers in $K$. Moreover, $a_{0} \neq 0$ and $n \geq 2$. By $B_{i}$ we shall denote constants which depend only on $X, a_{0}, \ldots, a_{m}$ and $P(x)$. The remaining constants we shall denote by $M_{l}$.

**Lemma 2.** There exists a constant $B_{i}$ such that from the conditions:

(i) $a_{0}$—rational integer, $a_{i}$—integer in $K$, $u$ divides $a_{i} w_{i}^{m}$;

(ii) No integral rational divisor $f(\pm 1)$ of $u$ divides $x$ follows $|u| \leq B_{i}$.

Proof. We shall denote by $B_{i}$ the principal ideal in $K$ generated by $h$. Let $u = \prod_{i=1}^{m} \phi_{i}$ be the decomposition of $u$ into rational primes, and

\[
(x) = \prod_{i=1}^{m} \phi_{i}^{n} [x_{i} > 0] \quad \text{and} \quad (a_{i}) = \prod_{i=1}^{m} \phi_{i}^{n} [x_{i} > 0, e_{i} > 0]
\]

are the decompositions into prime ideals in $K$. Let

\[
B_{i} = \max{e_{i}, \ldots, \beta_{0}, e_{0}, \beta_{1}, \ldots, \beta_{0} + m}.
\]

$(P_{1})|u)$ thus $(P_{1})|u_{m}$, but $(P_{1})|u_{m}$, Suppose that $(P_{1})$ is not ramified in $K$, and thus $(P_{1}) = 1$. There exist an $l$, not dividing $(x)$. Such an $l$, divides $(a_{i})$. Since $(a_{i})$ has only a finite number of ideal divisors, we see that there can be only a finite number of such $l$, and a fortiori there is only a finite number of such $P_{1}$. Since there is only a finite number of ramified $(P_{1})$ in $K$, we have thus proved the existence of $B_{i}$ such that $|P_{1}| < B_{i}$.}
Suppose now that there exists a sequence of non-zero integers in $K$: $(x_j)$ such that

\[ \lim_{j \to \infty} \frac{g(a_n x_j^n)}{g(x_j)} = 0. \]

Let

\[ x_j = \sum_{k=1}^{\infty} \frac{x_j^k}{a_k}, \]

By considering, say, a subsequence of $(x_j)$ we can assume that

\[ g(x_j) = |x_j^k| \]

and that there exist limits

\[ \delta_k = \lim_{j \to \infty} \frac{x_j^k}{a_k^k} \quad (k = 1, \ldots, m). \]

From (3'), (4), and (5) we obtain

\[ \lim_{j \to \infty} \frac{T_k(x_j, \ldots, x_j)}{(a_k)^k} = 0 \quad (k = 1, \ldots, m); \]

consequently, for $k = 1, \ldots, m$, $T_k(\delta_1, \ldots, \delta_n) = 0$, whence for $r = 1, \ldots, m$,

\[ \sum_{k=1}^{\infty} T_k(\delta_1, \ldots, \delta_m) a_k^r = 0. \]

From (3') follows

\[ a_k^r \left( \sum_{k=1}^{\infty} b_k a_k^r \right)^n = 0 \quad (r = 1, \ldots, m), \]

and thus

\[ \sum_{k=1}^{\infty} b_k a_k^r = 0 \quad (r = 1, \ldots, m). \]

But $b_r = 1$, and we must have $\det(a_k^r) = 0$, but this is impossible. This contradiction proves the lemma.

**Lemma 4.** For the set $X$, the polynomial $P(x)$ and the function $f(x)$ defined as above, condition (b) of the lemma 1 holds.

**Proof.** Suppose that

\[ x = \sum_{k=1}^{\infty} p_k x_k; \quad (p_1, \ldots, p_m, q) = 1, \quad \bar{x} = g \bar{x}, \]

\[ P(x) = \frac{1}{Q} \sum_{k=1}^{\infty} P_k x_k = \frac{1}{Q} \sum_{k=1}^{\infty} P_k x_k, \quad (Q, P_1, \ldots, P_m) = 1. \]
Evidently $Q$ divides $A_0$. Let $\mu = A_0^q$. Then $\mu$ divides $P_b$ for $b = 1, \ldots, m$. Let $\nu = (\mu, q)$. Thus

$$
\sum_{b=1}^{m} P_{b,\sigma_b} = A_0^q P(x) = \sum_{k=0}^{\infty} a_k q^{q-k\nu} = a_0 \omega^n + Bq,
$$

where $R$ is an integer in $K$.

From $\nu | \mu | P_b$ follows $\nu | \sum_{b=1}^{m} P_{b,\sigma_b}$ and thus we have $\nu | a_0 \omega^n$. We have $(P_1, \ldots, P_n, q) = 1$, whence no integral rational divisor ($\neq \pm 1$) of $\nu$ divides $\omega$, and from lemma 2 we obtain $|\nu| \leq B_1$. Now since $\mu = a_0 \omega^n$, $q = d_0 \nu$, $(d_1, d_0) = 1$, and $d_0$ divides $A_0^{q-1}$, we have $|d_0| \leq A_0^{q-1}$ and we obtain $\mu \leq A_0^{q} \leq A_0^{\nu} = B_1$.

Now if $f(P(x)) = Q < f(x) = q$, then evidently $g \geq \frac{A_0^q}{\mu}$ and so

$$
f(x) < \left( \frac{1}{q^n} \right)^{1/q} \left( \frac{B_1}{\nu} \right)^{1/q}.
$$

The lemma is thus proved.

**Lemma 5.** For the set $X$, the polynomial $P(x)$ and the functions $f(x)$ and $g(x)$ defined as above, condition (c) of lemma 1 holds.

**Proof.** The following inequalities can easily be verified:

(a) $f(x+y) \leq f(x) f(y)$.
(b) $f(xy) \leq f(x) f(y)$.
(c) $g(x+y) \leq \max \{ f(x), f(y) \} \left( g(x)+g(y) \right)$.
(d) $g(xy) \leq \max_{i \leq k} (\frac{1}{M_i} g(x) g(y)) = B g(x) g(y)$ where $\frac{1}{M_i}$ are defined as in lemma 3.

(e) For natural $n$, $\frac{1}{n} g(x) \leq \frac{1}{n} g(y) \leq g(x)$.

Suppose that $f(x) \leq M$. Then from the above inequalities it follows that

$$
g\left( \frac{1}{d} \sum_{k=0}^{n-1} a_k x^k \right) \leq g\left( \sum_{k=0}^{n-1} a_k x^k \right) \leq M g(x)^{n-1}
$$

with a suitable $M_i(M)$. From lemma 3 and (e) we obtain

$$
g\left( \frac{1}{d} a_0 x^d \right) \geq \frac{1}{d} g(a_0 x^d) = \frac{1}{d} g(a_0 f(a_0 x^d)) \geq \frac{1}{d} g(a_0 (f(a_0 x^d))^{g})
\geq \frac{1}{d M} B g(x)^{g} \geq \frac{1}{d M} B g(x)^{g}.
$$

If, for an infinite sequence $(x_i)$ with $f(x_i) \leq M$,

$$
\lim_{i \to \infty} g\left( \frac{f(x_i)}{g(x_i)^g} \right) = 0
$$

then (as $g(x_i) \to \infty$) we have

$$
0 \leq \frac{g(1/a_0 x^d)}{g(x)^{g}} - \frac{g\left( x_0 - \sum_{k=0}^{n-1} a_k x^k \right)}{g(x)^{g}} \leq \frac{A M^n}{g(x)} \left( g\left( x_0 \right) + \sum_{k=0}^{n-1} a_k x^k \right) \to 0,
$$

which is an obvious contradiction. Thus there exists a constant $M > 0$ such that $g(P(x)) \geq M g(x)^{g}$, whence the inequality $g(P(x)) \leq g(x)$ can be true only for $g(x) \leq M^{-1/n} = M$. The lemma is thus proved.

**Theorem I.** Now follows from lemmas 1, 4 and 5 and the trivial observation that condition (a) of lemma 1 is also satisfied by our set $X$ and the functions $f(x)$ and $g(x)$.

4. Now we shall prove theorem II. It is sufficient to prove it in the case of a single transcendental extension of a field $K$. Suppose that $\theta$ is transcendental upon $K$ and $K = K(\theta)$. Evidently every element $x$ of $K$ can be represented in the form $x = P(\theta)$ where $P$ and $Q$ are polynomials with coefficients from $K$ and without common zeros. Suppose that $X$ is an infinite subset of $K$ and $W(t)$ is a polynomial of at least second degree with the property $W(X) = X$. Let us put for every $x \cdot X$:

$$
f(x) = \text{degree of } Q \quad \text{and} \quad g(x) = \text{degree of } P.
$$

We can write

$$
W(t) = 1 + \sum_{i=1}^{n} A_i(\theta) t^i,
$$

where $A_i$ and $A_0$ are polynomials with coefficients from $K$. At first we prove that condition (a) of lemma 1 holds. If $R$ is finite, then this is evident. Suppose that $R$ is infinite. We can always select an infinite sequence $(r_i)$ from $R$ such that $A(r_i) \neq 0$ and $A_0(r_i) \neq 0$ for all $i$. Let us define

$$
W_i(t) = \sum_{i=1}^{n} A_i(r_i) t^i \quad \text{for } i = 1, 2, \ldots
$$

and then we obtain

$$
W(t) = \sum_{i=1}^{n} W_i(t) A_i(\theta) \quad \text{and} \quad W_i(t) \to 0.
$$

Theorem I thus follows.
and
\[ E_i = \frac{P_i(x)}{Q(x)} \mid_{x=0} \quad \text{for } i=0, \ldots, n. \]

Then evidently \( E_i \subset \mathcal{R} \) and \( W(E_i) = E_i \), whence for every \( i \) the set \( E_i \) is finite. Condition (a) can now easily be verified, since for every \( c \) there exist only a finite number of rational functions with bounded degree of numerator and denominator which can take only a finite number of values at every point from an infinite set.

We now proceed to condition (b). Let
\[ W \left( \frac{P(\theta)}{Q(\theta)} \right) = \frac{p(\theta)}{q(\theta)} = \frac{1}{A(\theta)Q(\theta)} \sum_{k=0}^{n} A_k(\theta)P^k(\theta)Q^{n-k}(\theta). \]

Let
\[ \mu(t) = \left( A(t)Q^n(t), \sum_{k=0}^{n} A_k(t)P^k(t)Q^{n-k}(t) \right), \]
\[ v(t) = (\mu(t), Q(t)). \]

Then \( v(t)A_u(t)P^n(t) \); consequently
\[ v(t)A_u(t), \quad \mu(t) = d_j(t)v(t), \]
\[ Q(t) = d_j(t)v(t), \quad [d_j(t), d_i(t)] = 1 \]
and so
\[ d_j(t)v(t) = d_j(t)d_i(t)v(t), \quad [d_j(t), d_i(t)] = 1. \]

Thus
\[ \mu(t) = \left( A(t)Q^{n-1}(t) \right), \]
and we see that the degree of \( \mu(t) \) is bounded by a constant \( M_1 \), depending only on the polynomial \( W(t) \). Consequently we obtain
\[ f(W(x)) \geq nf(x) + \deg \mu(t) - M_1, \]
and thus \( f(W(x)) > f(x) \) for sufficiently great \( f(x) \). It remains to prove that condition (c) of lemma 1 is satisfied. Suppose \( f(x) < M \). Then
\[ g(W(x)) = \deg \left( \sum_{k=0}^{n} A_k(t)P^k(t)Q^{n-k}(t) \right) - \deg \mu(t) \]
\[ \geq \deg \left( \sum_{k=0}^{n} A_k(t)P^k(t)Q^{n-k}(t) \right) - M_1 \]
and evidently
\[ \deg \left( \sum_{k=0}^{n} A_k(t)P^k(t)Q^{n-k}(t) \right) \leq (n-1)\deg P(t) + n\deg Q(t) + \max_{a \in [0,1]} \deg A_i(t) \]
\[ \leq (n-1)\deg P(t) + M_1 \text{ with some constant } M_2. \]

But
\[ \deg A_n(t)P^n(t) = \deg A_n(t) + n\deg P(t) > (n-1)\deg P(t) + M_1 \]
for sufficiently great \( \deg P(t) \). Consequently, when \( g(x) \) is sufficiently great, we obtain \( g(W(x)) > g(x) \) and so condition (c) is also satisfied. From lemma 1 it now follows that \( X \) must be finite, and this contradiction with our assumptions proves our theorem.

References


Reçu par la Rédaction le 27. 3. 1961