[7] Yu. V. Linnik, *On the least prime in an arithmetic progression* I, Mat. Sb. N. S. 15 (57) (1944), pp. 139-178.

[8] K. Prachar, *Primzahlverteilung*, Berlin, 1957.

[9] K. A. Rodosskiĭ (К. А. Родосский), *О наименьшем простом числе в арифметической прогресии* (in Russian), Mat. Sb. N. S. 34 (76) (1954), pp. 331-356.

[10] A. Selberg, *On an elementary method in the theory of primes*, Norske Videnskabers Selskab Forhandlinger XIX, N 18 (1946), pp. 64-67.

[11] P. Turán, *On a density theorem of Yu. V. Linnik*, Publications of the Mathem. Institute of the Hungarian Academy of Sci. VI A (1961), pp. 165-179.

[12] H. Weber, *Lehrbuch der Algebra* II, Braunschweig, 1899.

Reçu par la Rédaction le 25. 2. 1961

ACTA ARITHMETICA
VII (1962)

On polynomial transformations

by

W. Narkiewicz (Wrocław)

1. We shall say that 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 $f(x) \geqslant C$ follows $f(T(x)) > f(x)$,*

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

Then X is finite.

Proof of the lemma. Let $z \in X$. There exists a $z_1 \in X$ such that $T(z_1) = z_0 = z$. Similarly there exists a $z_2 \in X$ such that $T(z_2) = z_1$ and so on. We thus obtain a set $A_z = \{z_k\}_{k=0}^{\infty}$.

Evidently $X = \bigcup_{z \in X} A_z$. If $f(z_k) \leqslant C$ but $f(z_{k+1}) > C$, then $f(z_{k+1}) > f(z_k) = f(T(z_{k+1}))$ and by (b), $f(z_{k+1}) < C$, which is a contradiction. We thus have

$$f(z_k) \leqslant C \Rightarrow f(z_{k+1}) \leqslant C\,. \tag{1}$$

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

$$f(z_k) > C \Rightarrow f(z_{k+1}) < f(z_k)\,. \tag{2}$$

From (1) and (2) immediately follows $\max_{x \in A_z} f(x) \leqslant \max(f(z), C) = M_z$. For $x \in A_z$ we infer from (c) that: if $g(x) \geqslant B(M_z)$ then $g(T(x)) > g(x)$. In the same way as (1) and (2) we obtain

$$g(z_k) \leqslant B(M_z) \Rightarrow g(z_{k+1}) \leqslant B(M_z)\,, \tag{1'}$$

$$g(z_k) > B(M_z) \Rightarrow g(z_{k+1}) < g(z_k)\,, \tag{2'}$$

and similarly we see that $g(x)$ is bounded in A_z. From (a) it follows that for every $z \in X$ the set A_z is finite; thus the sequence $\{z_k\}$ is periodical. From (2) we infer that in every A_z there exists an x_z such that $f(x_z) \leqslant C$. From the periodicity of $\{z_k\}$ and (1) we see that $\max_{x \in A_z} f(x) \leqslant C$ and so M_z does not depend of z. Consequently $g(x)$ is in A_z 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 $X^{(n)}$ is infinite but $X^{(n+1)}$ is void (where $X^{(n)}$ denotes the n-th derived set of X and n is finite), then X has property* (P).

(In particular every infinite set without limit points has property (P).)

Proof. It is sufficient to prove this theorem for $n = 0$ only, because if $P(X) = X$ then $P(X') = X'$. In this case X has no limit points, and we can write $X = \{x_k\}_{k=1}^{\infty}$ so that for $i < j$, $|x_i| \leqslant |x_j|$. If there exists a polynomial $P(x)$ such that $P(X) = X$ and $P(x) \neq ax + b$, then we put $f(x_j) = j$, $g(x_j) = 1$, $B(M) = 2$ for all M, and $C = 1 + \sup_{|P(x_j)| \leqslant |x_j|} j$. 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 $P(x) = e^{ia}x + b$ where a is a real number.)

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

Let K be an algebraic number field of degree m. Let us fix an integral basis of K: $\{\omega_i\}_{i=1}^{m}$. By $\{\omega_i^{(\nu)}\}_{i=1}^{m}$ $(1 \leqslant \nu \leqslant m)$ 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 $x = \frac{1}{q}\sum_{k=1}^{m} p_k\omega_k$, where $p_1, \ldots, p_m, q$ are rational integers, $(p_1, \ldots, p_m, q) = 1$ and $q > 0$. Let us define $f(x) = q$ and $g(x) = \max_{1 \leqslant i \leqslant m} |p_i|$. (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: $P(x) = \frac{1}{\Delta}\sum_{k=0}^{n} a_k x^k$ where Δ is a natural number, and a_k are integers in K. Moreover, $a_n \neq 0$ and $n \geqslant 2$. By B_i we shall denote constants which depend only on K, $\omega_1, \ldots, \omega_m$, and $P(x)$. The remaining constants we shall denote by M_i.

LEMMA 2. *There exists a constant B_1 such that from the conditions:*

(i) *u—rational integer, x—integer in K, u divides $a_n x^n$;*

(ii) *No integral rational divisor ($\neq \pm 1$) of u divides x*

follows $|u| \leqslant B_1$.

Proof. We shall denote by (h) the principal ideal in K generated by h. Let $u = \prod_{i=1}^{s} P_i^{a_i} \langle a_i > 0\rangle$ be the decomposition of u into rational primes, and

$$(x) = \prod_{i=1}^{r_1} \mathfrak{p}_i^{\delta_i} \quad \langle \delta_i > 0\rangle\,, \qquad (a_n) = \prod_{i=1}^{r_1} \mathfrak{p}_i^{\beta_i} \prod_{i=1}^{r_2} \mathfrak{q}_i^{\varepsilon_i} \quad \langle \beta_i \geqslant 0\,,\ \varepsilon_i > 0\rangle$$

are the decompositions into prime ideals in K. Let

$$B_3 = \max(\varepsilon_1, \ldots, \varepsilon_{r_2}, \beta_1, \ldots, \beta_{r_1}) + n\,.$$

$(P_i) | (u)$ thus $(P_i) | (a_n x^n)$, but $(P_i) \nmid (x)$. Suppose that (P_i) is not ramified in K, and thus $(P_i) = \mathfrak{i}_1 \ldots \mathfrak{i}_t$. There exist an $\mathfrak{i}_r$ not dividing (x). Such an $\mathfrak{i}_r$ divides (a_n). Since (a_n) has only a finite number of ideal divisors, we see that there can be only a finite number of such $\mathfrak{i}_r$, and *a fortiori* there is only a finite number of such P_i. Since there is only a finite number of ramified (P_i) in K, we have thus proved the existence of B_2 such that $|P_i| \leqslant B_2$.

Let

$$(P_i) = \prod_{j=1}^{\tau_1} \mathfrak{p}_j^{\lambda_j^i} \prod_{j=1}^{\tau_2} \mathfrak{q}_j^{\mu_j^i}$$

be the decomposition of (P_i) into prime ideals in K. $(P_i)^{a_i} | (a_n x^n)$ thus $a_i\lambda_j^i \leqslant n\delta_j + \beta_j$ and $a_i\mu_j^i \leqslant \varepsilon_j$. $(P_i) \nmid (x)$, whence (i) there exists a $\mu_j^i \neq 0$ and in this case $a_i \leqslant \varepsilon_i/\mu_j^i \leqslant \varepsilon_j \leqslant B_3$ or (ii) $\mu_j^i = 0$ for all j and there exists a λ_j^i such that $\lambda_j^i > \delta_j$ and now

$$n\delta_j + \beta_j \geqslant a_i\delta_j; \qquad a_i \leqslant n + \frac{\beta_j}{\delta_j} \leqslant n + \beta_j \leqslant B_3 .$$

By putting $B_1 = B_2^{B_3\pi(B_2)}$ we obtain the assertion of the lemma.

LEMMA 3. *If we write*

$$B_4 = \inf_{\substack{x \neq 0 \\ x \text{ integer in } K}} \frac{g(a_n x^n)}{[g(x)]^n},$$

then $B_4 \neq 0$.

Proof. Let

$$a_n^{(\nu)} = \sum_{k=1}^{m} a_k \omega_k^{(\nu)} \qquad (1 \leqslant \nu \leqslant m) .$$

Then for every complex $\lambda_1, \ldots, \lambda_m$ and $1 \leqslant \nu \leqslant m$ the following identity holds:

$$(3) \qquad a_n^{(\nu)} \Big(\sum_{k=1}^{m} \lambda_k \omega_k^{(\nu)} \Big)^n$$

$$= \sum_{e=1}^{m} \omega_e^{(\nu)} \sum_{j=1}^{m} \sum_{k=1}^{m} a_k \overline{\Gamma}_e^{(j,k)} \sum_{\Sigma i_t = n} \frac{n!}{i_1! \ldots i_m!} \lambda_1^{i_1} \ldots \lambda_m^{i_m} \Gamma_j^{(i_1 \ldots i_m)} ,$$

where the coefficients $\Gamma_j^{(i_1 \ldots i_m)}$ are defined by

$$\sum_{j=1}^{m} \Gamma_j^{(i_1 \ldots i_m)} \omega_j^{(\nu)} = \prod_{j=1}^{m} (\omega_j^{(\nu)})^{i_j}$$

and $\overline{\Gamma}_e^{(j,k)}$ by

$$\sum_{e=1}^{m} \overline{\Gamma}_e^{(j,k)} \omega_e^{(\nu)} = \omega_j^{(\nu)} \omega_k^{(\nu)} .$$

These coefficients do not depend on the choice of ν (see [2], Satz 55).

The proof of (3) is immediate by application of Newton's formula. For simplicity we shall write (3) in the form

$$(3') \qquad a_n^{(\nu)} \Big(\sum_{k=1}^{m} \lambda_k \omega_k^{(\nu)} \Big)^n = \sum_{k=1}^{m} T_k(\lambda_1, \ldots, \lambda_m) \omega_k^{(\nu)} .$$

Obviously $T_k(\lambda_1, \ldots, \lambda_m)$ are homogeneous forms of degree n in m variables.

Suppose now that there exists a sequence of non-zero integers in K: $\{x_j\}$ such that

$$(4) \qquad \lim_{j \to \infty} \frac{g(a_n x_j^n)}{[g(x_j)]^n} = 0 .$$

Let

$$x_j = \sum_{k=1}^{m} \xi_k^{(j)} \omega_k .$$

By considering, say, a subsequence of $\{x_j\}$ we can assume that

$$(5) \qquad g(x_j) = |\xi_{k_0}^{(j)}|$$

and that there exist limits

$$\delta_k = \lim_{j \to \infty} \frac{\xi_k^{(j)}}{\xi_{k_0}^{(j)}} \qquad (k = 1, \ldots, m) .$$

From (3′), (4), and (5) we obtain

$$\lim_{j \to \infty} \frac{T_k(\xi_1^{(j)}, \ldots, \xi_m^{(j)})}{(\xi_{k_0}^{(j)})^n} = 0 \qquad (k = 1, \ldots, m);$$

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

$$\sum_{k=1}^{m} T_k(\delta_1, \ldots, \delta_m) \omega_k^{(\nu)} = 0 .$$

From (3′) follows

$$a_n^{(\nu)} \Big(\sum_{k=1}^{m} \delta_k \omega_k^{(\nu)} \Big)^n = 0 \qquad (\nu = 1, \ldots, m) ,$$

and thus

$$\sum_{k=1}^{m} \delta_k \omega_k^{(\nu)} = 0 \qquad (\nu = 1, \ldots, m) .$$

But $\delta_{k_0} = 1$, and we must have $\det|\omega_k^{(\nu)}| = 0$, 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

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

$$P(x) = \frac{1}{Q} \sum_{k=1}^{m} P_k \omega_k = \frac{1}{\Delta q^n} \sum_{k=1}^{m} \overline{P}_k \omega_k , \qquad (Q, P_1, \ldots, P_m) = 1 .$$

Evidently Q divides Δq^n. Let $\mu = \Delta q^n Q^{-1}$. Then μ divides $\overline{P}_k$ for $k = 1, \ldots, m$. Let $\nu = (\mu, q)$. Thus

$$\sum_{k=1}^{m} \overline{P}_k \omega_k = \Delta q^n P(x) = \sum_{k=0}^{n} a_k q^{n-k} \overline{x}^k = a_n \overline{x}^n + Rq\,,$$

where R is an integer in K.

From $\nu | \mu | \overline{P}_k$ follows $\nu \Big| \sum_{k=1}^{m} \overline{P}_k \omega_k$ and thus we have $\nu | a_n \overline{x}_n$. We have $(p_1, \ldots, p_m, q) = 1$, whence no integral rational divisor ($\neq \pm 1$) of ν divides $\overline{x}$, and from lemma 2 we obtain $|\nu| \leqslant B_1$. Now since $\mu = d_1 \nu$, $q = d_2 \nu$, $(d_1, d_2) = 1$, and d_1 divides $\Delta \nu^{n-1}$, we have $|d_1| \leqslant \Delta \nu^{n-1}$ and we obtain $\mu \leqslant \Delta \nu^n \leqslant \Delta B_1^n = B_5$.

Now if $f(P(x)) = Q \leqslant f(x) = q$, then evidently $q \geqslant \dfrac{\Delta q^n}{\mu}$ and so

$$f(x) \leqslant \left(\frac{\mu}{\Delta}\right)^{1/(n-1)} \leqslant \left(\frac{B_5}{\Delta}\right)^{1/(n-1)}.$$

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) $f(x+y) \leqslant f(x) f(y)$.

(b) $f(xy) \leqslant f(x) f(y)$.

(c) $g(x+y) \leqslant \{\max(f(x), f(y))\}\,\{g(x) + g(y)\}$.

(d) $g(xy) \leqslant m^2 \max\limits_{i,j,k} |\overline{\Gamma}_k^{(i,j)}| g(x) g(y) = B_6 g(x) g(y)$ where $\overline{\Gamma}_k^{(i,j)}$ are defined as in lemma 3.

(e) For natural u, $\dfrac{1}{u} g(x) \leqslant g\left(\dfrac{x}{u}\right) \leqslant g(x)$.

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

$$g\left(\frac{1}{\Delta} \sum_{k=0}^{n-1} a_k x^k\right) \leqslant g\left(\sum_{k=0}^{n-1} a_k x^k\right) \leqslant M_1 g(x)^{n-1}$$

with a suitable $M_1(M)$. From lemma 3 and (e) we obtain

$$g\left(\frac{1}{\Delta} a_n x^n\right) \geqslant \frac{1}{\Delta} g(a_n x^n) = \frac{1}{\Delta} g\left(a_n \frac{[x \cdot f(x)]^n}{f(x)^n}\right) \geqslant \frac{1}{\Delta f(x)^n} g\left(a_n [x f(x)]^n\right)$$
$$\geqslant \frac{1}{\Delta M^n} B_4 [g(x f(x))]^n \geqslant \frac{1}{\Delta M^n} B_4 g(x)^n.$$

If, for an infinite sequence $\{x_i\}$ with $f(x_i) \leqslant M$,

$$\lim_{i\to\infty} \frac{g\big(P(x_i)\big)}{\big(g(x_i)\big)^n} = 0$$

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

$$0 < \frac{B_4}{M^n} \leqslant \Delta \frac{g\left(\frac{1}{\Delta} a_n x_i^n\right)}{[g(x_i)]^n} = \Delta \frac{g\left(P(x_i) - \sum\limits_{k=0}^{n-1} \frac{a_k}{\Delta} x_i^k\right)}{[g(x_i)]^n}$$
$$\leqslant \frac{\Delta^2 M^n}{[g(x_i)]^n} \left[g\big(P(x_i)\big) + g\left(\sum_{k=0}^{n-1} \frac{a_k}{\Delta} x_i^k\right)\right] \to 0\,,$$

which is an obvious contradiction. Thus there exists a constant $M_2 > 0$ such that $g\big(P(x)\big) \geqslant M_2 g(x)^n$, whence the inequality $g\big(P(x)\big) \leqslant g(x)$ can be true only for $g(x) \leqslant M_2^{-1/(n-1)} = M_3$. 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 R. Suppose that ϑ is transcendental upon R and $K = R(\vartheta)$. Evidently every element x of K can be represented in the form $x = \dfrac{P(\vartheta)}{Q(\vartheta)}$ where P and Q are polynomials with coefficients from R 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 $x \in X$: $f(x) =$ degree of Q and $g(x) =$ degree of P. We can write

$$W(t) = \frac{1}{\Delta(\vartheta)} \sum_{k=0}^{n} A_k(\vartheta) t^k\,,$$

where Δ and the A_k are polynomials with coefficients from R. 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 $\Delta(r_i) \neq 0$ and $A_n(r_i) \neq 0$ for all i. Let us define

$$W_i(t) = \frac{1}{\Delta(r_i)} \sum_{k=0}^{n} A_k(r_i) t^k \quad \text{for} \quad i = 1, 2, \ldots$$

and

$$E_i = \left\{\frac{P(r_i)}{Q(r_i)}\right\}_{\frac{P(\vartheta)}{Q(\vartheta)}\in X;\, Q(r_i)\neq 0}.$$

Then evidently $E_i \subset R$ and $W_i(E_i) = E_i$, 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

$$W\left(\frac{P(\vartheta)}{Q(\vartheta)}\right) = \frac{p(\vartheta)}{q(\vartheta)} = \frac{1}{\Delta(\vartheta)Q^n(\vartheta)}\sum_{k=0}^{n} A_k(\vartheta)P^k(\vartheta)Q^{n-k}(\vartheta).$$

Let

$$\mu(t) = \left(\Delta(t)Q^n(t), \sum_{k=0}^{n} A_k(t)P^k(t)Q^{n-k}(t)\right),$$

$$\nu(t) = \left(\mu(t), Q(t)\right).$$

Then $\nu(t)|A_n(t)P^n(t)$; consequently

$$\nu(t)|A_n(t), \quad \mu(t) = d_1(t)\nu(t),$$
$$Q(t) = d_2(t)\nu(t), \quad \left(d_1(t), d_2(t)\right) = 1$$

and so

$$d_1(t)\nu(t)|\Delta(t)d_2^n(t)\nu^n(t), \qquad d_1(t)|\Delta(t)\nu^n(t);$$

thus

$$\mu(t)|\Delta(t)A_n^{n+1}(t),$$

and we see that the degree of $\mu(t)$ is bounded by a constant M_1 dependent only on the polynomial $W(t)$. Consequently we obtain

$$f\left(W(x)\right) \geqslant nf(x) + \deg\Delta(t) - M_1,$$

and thus $f\left(W(x)\right) > f(x)$ for sufficiently great $f(x)$. It remains to prove that condition (c) of lemma 1 is satisfied. Suppose $f(x) \leqslant M$. Then

$$g\left(W(x)\right) = \deg\left(\sum_{k=0}^{n} A_k(t)P^k(t)Q^{n-k}(t)\right) - \deg\mu(t)$$
$$\geqslant \deg\left(\sum_{k=0}^{n} A_k(t)P^k(t)Q^{n-k}(t)\right) - M_1$$

and evidently

$$\deg\left(\sum_{k=0}^{n-1} A_k(t)P^k(t)Q^{n-k}(t)\right) \leqslant (n-1)\deg P(t) + n\deg Q(t) + \max_{0\leqslant j\leqslant n-1}\deg A_j(t)$$
$$\leqslant (n-1)\deg P(t) + M_2 \text{ with some constant } M_2.$$

But

$$\deg A_n(t)P^n(t) = \deg A_n(t) + n\deg P(t) > (n-1)\deg P(t) + M_2$$

for sufficiently great $\deg P(t)$. Consequently, when $g(x)$ is sufficiently great, we obtain $g\left(W(x)\right) > g(x)$ 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

[1] W. Franz, *Untersuchungen zum Hilbertschen Irreduzibilitätssatz*, Math. Zeitschr. 33 (1931), pp. 275-293.

[2] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923.

[3] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, Journal für die reine u. angew. Mathematik 110 (1892), pp. 104-129; Werke II, Berlin 1933, pp. 264-286.

Reçu par la Rédaction le 27. 3. 1961