

On the number of terms of a composite polynomial

by

UMBERTO ZANNIER (Pisa)

1. Introduction. From a certain viewpoint, the *number of terms* of a polynomial (here over a field k supposed throughout of characteristic 0) measures its complexity, and is thus sometimes a relevant quantity to consider.

In particular, one may ask how this complexity is affected by rational operations. For instance Schinzel has shown that, roughly speaking, *the square of a polynomial with “many” terms also has “many” terms*. Actually, he proved a similar statement for any fixed m th power and with explicit lower bounds on the number of terms (see [S, p. 187]).

Schinzel also conjectured that, more generally, if g is a fixed nonconstant polynomial, then the number of terms of $g(h(x))$ tends to infinity as the number of terms of $h(x)$ tends to infinity. This problem appears quite difficult and to my knowledge is so far unsolved (*).

In the present short paper we are concerned with a similar question, but letting the degree of $g(x)$ grow. We have the following

THEOREM 1. *Let $f \in k[x]$ have $l > 0$ nonconstant terms. Assume that $f = g(h(x))$, where $g, h \in k[x]$ and where $h(x)$ is not of the shape $ax^m + b$ for $a, b \in k$. Then*

$$\deg f + l - 1 \leq 2l(l - 1) \deg h.$$

We may rephrase a consequence of this result by saying that *a polynomial with few terms and large degree cannot have an inner noncyclic composition factor of small degree*.

In the special case when $g(x) = cx^m$ one can prove the sharper bound $\deg f \leq l \deg h$ provided h has at least one nonzero root; this follows directly from a result by Hajós which bounds by $t - 1$ the maximal multiplicity of a nonzero root of a polynomial with t terms. (Hajós’ result will be useful here, and is explicitly recalled below, together with a simple proof.)

2000 *Mathematics Subject Classification*: 10M05, 12E05, 12Y05.

(*) See the “Added in proof” on p. 166.

Note that the exclusion of the polynomials $h(x) = ax^m + b$ is relevant: in fact, if h has this shape, we can take $g(x) = g_1(x - b)$ where g_1 has a fixed number of terms and large degree to obtain a contradiction with the inequality of the theorem.

Similar, slightly weaker, results may be obtained for rational functions in place of polynomials, by a straightforward adaptation of the present methods ⁽¹⁾. For the sake of brevity we limit ourselves to a statement involving Laurent's polynomials, that is, polynomials in x, x^{-1} . We have:

THEOREM 2. *Let $f \in k[x, x^{-1}]$ have $l > 0$ nonconstant terms. Assume that $f = g(h(x))$, where $g \in k[x]$, $h \in k[x, x^{-1}]$ and where h is not of the shape $ax^m + a'x^{-m} + b$. Then*

$$\deg f \leq (2l - 1)(l - 1)(4(\deg h)^2 - 7 \deg h + 1).$$

The estimate here is weaker than in Theorem 1. Actually, our proof of Theorem 2 is simpler than the one for Theorem 1; the latter goes exactly in the same direction, but uses certain additional features which allow some improvements.

Again, the special shape in the statement must be taken into account: for instance, if $h(x) = x + x^{-1}$ and if we take $g(x) = T_n(x)$, the n th Chebyshev polynomial, then $f(x) = T_n(x + x^{-1}) = x^n + x^{-n}$ has only two terms.

These questions were motivated by work in progress with R. Dvornicich [DZ], concerning polynomial maps with infinitely many *preperiodic points* defined over a cyclotomic field. In such context, a relevant property of a polynomial $p \in k[x]$ is the existence of a Laurent polynomial q such that the number of terms in each of several iterates $p \circ \dots \circ p \circ q$ is bounded. It is a simple corollary of the above statements that this can happen only in very special cases; we have:

COROLLARY. *Let $p \in k[x]$ have degree ≥ 2 and let $q \in k[x, x^{-1}]$ be nonconstant. Then the number of nonconstant terms of $f(x) := p^{(r)}(q(x))$ is at least*

$$\frac{\sqrt{8}}{(\deg p)^2 \deg q} \sqrt{\deg f}$$

up to the following exceptions: there exist a polynomial $L(x)$ of degree 1 and an $\varepsilon = \pm 1$ such that $(L \circ p \circ L^{-1})(x)$ is either $(\varepsilon x)^d$ or $T_d(\varepsilon x)$ and $L(q(x)) = cx^m$ for a $c \in k^$ and an integer $m \neq 0$.*

By $p^{(r)}(x)$ we mean the r th iterate $p \circ \dots \circ p(x)$. (In [DZ] we used other special properties of the relevant polynomials to obtain the conclusion needed there, which would immediately follow also from this corollary.)

⁽¹⁾ In this case we may consider the maximum number of terms of the numerator and denominator.

As in the above theorems, it is readily checked that the special cases are indeed relevant, in the sense that they lead to a bounded number of terms in $p^{(r)}(q(x))$, as r grows.

As to inequalities going in the opposite direction, we thank A. Schinzel for the following general remark: *for every positive integer d there exist g and h such that $\deg g = d$ and $\deg f \geq l \deg h - 2$.* To check this, Schinzel takes $h(x) = x^2 + x$ and chooses g so that $g(h(x)) - x^{2d}$ is an odd polynomial, which can be done with $\deg g = d$.

Apart from this, we have no significant example, forgetting the exceptional cases appearing in the statements. However, we think that the estimates of the theorems and corollary are probably not best possible (which seems to be common in this type of questions). A question is for instance whether the quadratic term in l in the bounds may be replaced by a linear growth.

CONVENTION. Throughout the paper, k will be an algebraically closed field (which causes no loss of generality in our context) of zero characteristic.

2. Some lemmas

LEMMA 1 (Hajós lemma). *Let $f \in k[x]$ have l nonconstant terms and let $\beta \in k^*$. Then $\text{ord}_\beta(f(x) - f(0)) \leq l - 1$.*

A proof may be readily obtained as follows: suppose by contradiction that the order at β is $\geq l$, so the first l derivatives of $f(x) - f(0)$ vanish at β . Writing $f(x) = c_0 + c_1x^{m_1} + \dots + c_lx^{m_l}$, $0 < m_1 < \dots < m_l$, this gives an $l \times l$ linear system in c_1, \dots, c_l , whose determinant is easily reduced to a Vandermonde type and found to be nonzero. See [S, p. 187, Lemma 1].

COROLLARY (to Lemma 1). *Suppose that $f \in k[x]$ has l nonconstant terms and that $f(x) = f(\alpha x + \beta)$ for some $\alpha, \beta \in k^*$. Then $\deg f \leq \binom{l}{2}$.*

Proof. In this proof $f^{(m)}$ will denote the m th derivative (elsewhere the iterated composition). Again, write $f(x) = c_0 + c_1x^{m_1} + \dots + c_lx^{m_l}$, $0 < m_1 < \dots < m_l$. Observe that for $0 \leq r \leq l - 1$, we have $\text{ord}_0(f^{(m_r)}(x) - m_r!c_r) \geq m_{r+1} - m_r$. From the equation $f(x) = f(\alpha x + \beta)$ we deduce that $\text{ord}_\beta(f^{(m_r)}(x) - m_r!c_r\alpha^{-m_r}) \geq m_{r+1} - m_r$.

Applying Lemma 1 with $f^{(m_r)}$ in place of f and $m_r!c_r\alpha^{-m_r}$ in place of c_0 we obtain $m_{r+1} - m_r \leq l - r - 1$. Summing this inequality for $r = 0, \dots, l - 1$ we get $\deg f = m_l = \sum_{r=0}^{l-1} (m_{r+1} - m_r) \leq \sum_{r=0}^{l-1} (l - r - 1) = \binom{l}{2}$, as required. ■

LEMMA 2. *Suppose that $f \in k[x]$ has l nonconstant terms and that $f(x) = g(h(x))$, where $h(x)$ is not of the shape $ax^m + b$. Then we have $\text{ord}_0(f(x) - f(0)) \leq (l - 1)(\deg h - 1)$.*

Proof. Write $f(x)$ as in the Corollary and set

$$g(x) - c_0 = g_0(x - \varrho_1)^{e_1} \cdots (x - \varrho_r)^{e_r},$$

with $g_0 \in k^*$, pairwise distinct $\varrho_i \in k$ and positive integers e_i . Now, x^{m_1} divides $f(x) - c_0 = g_0 \prod_{i=1}^r (h(x) - \varrho_i)^{e_i}$; the factors in this product are pairwise coprime, hence x^{m_1} has to divide some factor $(h(x) - \varrho_j)^{e_j}$.

Since by assumption $h(x)$ is not of the form $ax^m + b$, $h(x) - \varrho_j$ has at least one nonzero root $\alpha \in k^*$. Hence, on the one hand $e_j(\deg h - 1) \geq m_1$, because the multiplicity of 0 as a root of $h(x) - \varrho_j$ is at most $\deg h - 1$; on the other hand, α is a root of $f(x) - c_0$, of multiplicity $\geq e_j$, hence $e_j \leq l - 1$ by Lemma 1. Combining these estimates we obtain the conclusion of the lemma. ■

In what follows we shall need some simple facts on certain function fields in one variable. The next lemma will take care of this; in it, $h(x)$ will again denote a polynomial of positive degree $\deg h$, but the assumption $h(x) \neq ax^m + b$ will not be needed now.

LEMMA 3. *Let $\lambda := h(x)$. There exists a conjugate y of x over $k(\lambda)$ with the following properties:*

- (i) *If $q \in k[x]$, then $q(x) = q(y)$ if and only if $q \in k[h(x)]$.*
- (ii) *Let $d := [k(x, y) : k(x)]$. Then $d \leq \deg h - 1$.*
- (iii) *The genus of the function field $K = k(x, y)$ (over k) is not greater than $(d - 1)(d - 2)/2$.*
- (iv) *There exist pairwise distinct places $\mathcal{P}_1, \dots, \mathcal{P}_d$ of K/k such that the divisor of poles of both x, y is $\mathcal{P}_1 + \cdots + \mathcal{P}_d$.*

Proof. Plainly, $k(x)$ is an extension of $k(\lambda)$ of degree $\deg h$. Let L be a Galois closure of $k(x)$ over $k(\lambda)$, with Galois group G , and let H be the subgroup corresponding to $k(x)$.

Observe first that the point at infinity of $k(\lambda)$ (i.e. the unique pole of λ) ramifies totally in $k(x)$; in fact, the Puiseux series for x at $\lambda = \infty$ are of the shape $x = a\theta\lambda^{1/\deg h} + b + c\theta^{-1}\lambda^{-1/\deg h} + \cdots$, where $b, c, \dots \in k$, $a \in k^*$ are independent of the branch and where θ runs over the $\deg h$ -th roots of unity.

In particular, G , as a permutation group on the $\deg h$ solutions of $h(X) = \lambda$, contains a $\deg h$ -cycle, i.e. a generator σ of the inertia group above $\lambda = \infty$. We set $y := \sigma(x)$. (More explicitly, note that if x is represented by the above series with $\theta = 1$, we may take y as the above series with θ a primitive $\deg h$ -th root of 1.)

Since the group generated by σ is transitive and since H is the stabilizer of x in G , it follows that H, σ generate G . Hence, if $q(x) = q(y)$ for a $q \in k(x)$, then $q(x)$ is left fixed by both H and σ , hence by G , i.e., $q(x) \in k(\lambda)$. If now q is a polynomial, then q is integral over $k[\lambda]$, hence must be a polynomial in λ , because $k[\lambda]$ is integrally closed. This proves part (i).

Note now that setting $H(X, Y) := (h(X) - h(Y))/(X - Y)$ we have $H(x, y) = 0$. Assertion (ii) follows since plainly $\deg_Y H \leq \deg H = \deg h - 1$.

Let $H_1 \in k[X, Y]$ be an irreducible polynomial with $H_1(x, y) = 0$. Then H_1 divides H , so the highest homogeneous part of it divides the highest one of H , which is a constant multiple of $(X^{\deg h} - Y^{\deg h})/(X - Y)$. This implies that $\deg H_1 = \deg_X H_1 = \deg_Y H_1 = d$. Now assertion (iii) is just the well-known upper bound $(d - 1)(d - 2)/2$ for the genus of a plane curve of degree $\leq d$.

Since the infinite place of $k(\lambda)$ is totally ramified in both $k(x)$ and $k(y)$, the infinite place of $k(x)$ is unramified in $k(x, y)$, and hence there are exactly d places above it. Since each of them is unramified, x has a simple pole at each of them, and no other poles. A symmetrical argument with x, y interchanged concludes the proof. ■

REMARK. Actually, (i) will not be strictly necessary for the rest, and y can be just any conjugate of x different from x .

M. Fried determined the precise conditions for the reducibility of the polynomial $H(X, Y)$ of the above proof. See [S, §1.5, Thm. 10].

LEMMA 4. *Let K/k be a function field in one variable, of genus g , and let $z_1, \dots, z_s \in K$ be not all constant and such that $1 + z_1 + \dots + z_s = 0$. Suppose also that no proper subsum of the left side vanishes. Then*

$$\max(\deg(z_i)) \leq \binom{s}{2} (\#S + 2g - 2),$$

where S is a set of points of K containing all zeros and poles of the z_i .

By $\deg(z)$ we mean $[K : k(z)]$; equivalently, this is the number of poles of z counted with multiplicity. This lemma is an immediate consequence of Corollary I of [BM] (as improved after Thm. B therein); we have just used the fact that the “ K -height” of the projective point $(1 : z_1 : \dots : z_s)$ is bounded below by the maximum degree. (See also [Z] for analogous statements.)

3. Proof of main results

Proof of Theorem 1. The polynomial $f(x)$ will be written as follows:

$$(1) \quad f(x) = c_0 + c_1 x^{m_1} + \dots + c_l x^{m_l},$$

where

$$(2) \quad c_i \in k, \quad c_1 \cdots c_l \neq 0, \quad 0 =: m_0 < m_1 < \dots < m_l := \deg f.$$

Suppose first that $h \in k(x^n)$ for some integer $n > 1$, so $h = q(x^n)$, $q \in k[x]$, and $f = \tilde{f}(x^n)$, where $\tilde{f}(x) = g(q(x))$. Since \tilde{f} has the same number of (nonconstant) terms as f , we may argue with $q(x)$ in place of $h(x)$. Note in fact that $q(x)$ cannot be of the shape $ax^m + b$, for otherwise

$h(x) = ax^{mn} + b$ would also be. If we assume the inequality to be proved for q in place of h and the same g , we find $(\deg f)/n + l - 1 \leq 2l(l - 1)(\deg h)/n$, whence $\deg f + n(l - 1) \leq 2l(l - 1) \deg h$, which implies the sought estimate and more.

Therefore, we may suppose that, for any $n > 1$, $h \notin k(x^n)$.

Secondly, suppose that h is decomposable, i.e. that $h(x) = p(q(x))$ for $p, q \in k[x]$ both of degree > 1 . Note that if $q(x) = ax^m + b$ then $m > 1$ and $h \in k(x^m)$, against the previous assumption. Hence q is not of the shape $ax^m + b$. We may now write $f(x) = r(q(x))$, where $r(x) = g(p(x))$. Again, if we assume the sought inequality for $q(x)$ in place of $h(x)$ and for $g(p(x))$ in place of $g(x)$, we obtain $\deg f + l - 1 \leq 2l(l - 1) \deg q$, which again implies the inequality we want to prove. Hence it will suffice to prove the theorem with g, h replaced by $g \circ p, q$ respectively.

Therefore, by iterating suitably this argument, we may assume from now on that h is indecomposable.

If $m_l \leq (l - 1)(\deg h - 1)$ the inequality in the conclusion of the theorem is true. Hence suppose that $m_l > (l - 1)(\deg h - 1)$.

In the rest of this proof we let $K = k(x, y)$ and we adopt the notation of Lemma 3. Since $f \in k(h(x))$ we have $f(x) - f(y) = 0$, where y is as in Lemma 3. In view of (1) this reads

$$(3) \quad c_1x^{m_1} - c_1y^{m_1} + \dots + c_lx^{m_l} - c_ly^{m_l} = 0.$$

We shall exploit (3) by means of Lemma 4. Before applying it, we deal with possible vanishing subsums of the left side of (3). We partition the terms on the left of (3) into minimal subsets with vanishing sum. (*A priori* this partition may be done in several ways; we can choose freely one of them.) Among such subsets we pick the one containing the term $c_lx^{m_l}$. We denote the corresponding terms by w_0, \dots, w_s agreeing that $w_s = c_lx^{m_l}$. We shall then obtain a relation $w_0 + \dots + w_s = 0$, without proper vanishing subsums, where $w_s = c_lx^{m_l}$ and where w_0, \dots, w_s are distinct terms on the left side of (3).

Also, we may write such a vanishing relation in the form

$$p(x) = q(y),$$

where p and q are nonzero polynomials obtained as certain nonempty subsums of terms $\pm w_j$ and where $\deg p = m_l$.

This equation says that $p(x)$ lies in the intersection $k(x) \cap k(y)$, which is a field intermediate between $k(\lambda)$ and $k(x)$ (we are using throughout the notation of Lemma 3 above). By the Lüroth Theorem (see [S]) this field is of the shape $k(r(x))$, where $r \in k(x)$ is such that $\lambda = h(x) = t(r(x))$ for some $t \in k(X)$. However, h is a polynomial, i.e. $\infty \in \mathbf{P}_1(k)$ has just the preimage ∞ under the map $P \mapsto h(P)$. Hence ∞ must have just one preimage, denoted

by Q , under the map $P \mapsto r(P)$. Then, replacing r by $L \circ r$ and t by $t \circ L^{-1}$, for a suitable $L \in \text{PSL}_2(k) = \text{Aut}(\mathbf{P}_1(k))$, we may assume that $Q = \infty$. This means however that r, t may be assumed to be polynomials, without changing their respective degrees. (This simple self-contained argument may be replaced by a quotation of [S, §1.2, Thm. 4].)

However, we are assuming that h is an indecomposable polynomial, so we must have either $\deg r = 1$ or $\deg t = 1$.

In the first case we must therefore have $k(x) \cap k(y) = k(x)$, i.e., $y = v(x) \in k(x)$. Since y is integral over $k[x]$ we deduce that $v \in k[x]$. By looking at the poles at \mathcal{P}_i we also deduce that $\deg v = 1$, namely $y = \alpha x + \beta$ for suitable $\alpha \in k^*, \beta \in k$. Since $h(x) = h(y)$ we have $h(x) = h(\alpha x + \beta)$ identically. If $\beta = 0$, α must be a root of unity, of exact order $n > 1$; this implies that $h \in k(x^n)$, which we are assuming not to be the case. Hence $\beta \neq 0$. By the Corollary to Lemma 1 we thus find $m_l \leq \binom{l}{2}$, which gives the sought result and more.

In the second case, $k(x) \cap k(y) = k(\lambda)$, so $p(x) \in k(h(x))$, which means that $p(x) = u(h(x))$ for some polynomial $u \in k[x]$. By Lemma 2 (applied with $p(x)$ in place of $f(x)$ and $u(x)$ in place of $g(x)$) we deduce that the minimum degree of a term of p is $\leq (l-1)(\deg h - 1)$. Let m_ℓ be this minimum degree (so in particular $\ell \neq l$); this amounts to assuming that $c_\ell x^{m_\ell}$ appears in $p(x)$ and that ℓ is minimal for this property. We may renumber the indices so that this term is w_0 .

Dividing the relation $w_0 + \dots + w_s = 0$ by $w_0 = c_\ell x^{m_\ell}$ and setting $z_j := w_j/w_0$ we find

$$(4) \quad 1 + z_1 + \dots + z_s = 0.$$

Note that $w_s \neq w_0$, hence there is at least one nonconstant term in the sum. We are then in a position to apply Lemma 4. We proceed to estimate the relevant quantities.

Note that z_s has a pole of order at least $m_l - m_\ell$ at each $\mathcal{P}_1, \dots, \mathcal{P}_d$. Hence $\deg(z_s) \geq d(m_l - m_\ell)$. Further, x, y have altogether the same d simple poles (Lemma 3(iv)) and therefore at most d distinct zeros each. We can then bound $\#S$ by $3d$ ⁽²⁾. Finally, the genus g is estimated by Lemma 2 as $\leq (d-1)(d-2)/2$.

Combining these estimates and using Lemma 4 we find

$$d(m_l - m_\ell) \leq \binom{s}{2} (3d + (d-1)(d-2) - 2) = \binom{s}{2} d^2.$$

Now, we have $s + 1 \leq 2l$, whence $m_l \leq m_\ell + (2l-1)(l-1)d$. Finally, recall that $m_\ell \leq (l-1)(\deg h - 1)$ and that $d \leq \deg h - 1$ by Lemma 3. All of this

⁽²⁾ Here a very slight improvement would be possible, taking into account that x, y may be proved to have some common zero.

gives

$$m_l \leq (l-1)(\deg h - 1) + (2l-1)(l-1)\deg h = 2l(l-1)\deg h - l + 1,$$

which proves Theorem 1. ■

Proof of Theorem 2. This proof is analogous, but simpler than the one for Theorem 1, and leads to a weaker result; the point is that the polynomial case has peculiar features which allow some improvements. (We do not know whether this could be done more generally.)

We write $f(x)$ in the form (1), but where now $m_1 < \dots < m_l$ are nonzero integers, not necessarily positive. By changing x into x^{-1} we may also assume that $m_l = \max(|m_j|)$; in particular, $\deg f = m_l$.

As in the opening step of the proof of Theorem 1, we reduce to the case when $h(x)$ does not lie in a field $k(x^n)$, no matter the integer $n > 1$. Clearly we may also suppose that $\deg h > 1$.

Similarly to the proof of Theorem 1, we let $y \neq x$ be a conjugate of x over $k(\lambda)$, where $h(x) = \lambda$, so $h(y) = h(x)$; we let $K = k(x, y)$.

If $y = cx$ for a $c \in k^*$, then $h(x) = h(cx)$, whence c is a root of unity and $h \in k(x^n)$ where $n > 1$ is the order of c , a case which we are excluding. The case $y = c/x$ may happen, but possibly for a single conjugate: if it happens for two conjugates y, y' then their ratio is constant and leads to an excluded case, as we have just shown. If there are no conjugates other than c/x , then $h(x)$ has degree 2 and then must be of the shape $ax + bx^{-1} + c'$, which we are again excluding.

Hence we may assume that y is neither of the form cx nor c/x .

Since $f = g(h(x))$ we also have $f(x) - f(y) = 0$. This last equation may be written as a sum of $2l$ terms, according to (1). As in the proof of Theorem 1 we partition the set of these terms into subsets with vanishing subsum. The subsum containing $c_l x^{m_l}$ will correspond to a relation $w_0 + \dots + w_s = 0$, where each w_j is a nonconstant term in $f(x)$ or in $-f(y)$, where $w_s = c_l x^{m_l}$ and where there are no proper vanishing subsums.

Dividing by w_0 we get a relation $1 + z_1 + \dots + z_s = 0$ without vanishing subsums, where $z_j = w_j/w_0$.

Suppose first that z_s is constant. Plainly, this can happen only if w_0 is of type $-c_j y^{m_j}$, and then x^{m_l}/y^{m_j} would be constant.

Now, $\deg(\lambda) = \deg(h)\deg(x) = \deg(h)\deg(y)$, so $\deg(x) = \deg(y)$ (viewing λ, x, y as elements of K). If $x^{m_l} = cy^{m_j}$ for a $c \in k^*$ then $|m_l|\deg(x) = |m_j|\deg(y)$, whence $|m_l| = |m_j|$. By our assumption that $|m_l| = \max(|m_i|)$, we can have either $m_j = m_l$ (and $j = l$) or $m_j = -m_l$ (and $m_j = m_1$).

In the first case we have $y = ax$ for an $a \in k^*$, which we are excluding.

If we have $m_j = m_1 = -m_l < 0$, then $y = b/x$ for a $b \in k^*$, which we are also excluding.

In conclusion, we may suppose that the term x^{m_l}/y^{m_j} is not constant.

Suppose first $m_j > 0$. If $\text{div}_0(y) \geq \text{div}_0(x)$ then the divisors are equal, because they have equal degree; similarly if $\text{div}_\infty(y) \geq \text{div}_\infty(x)$. Then, if both inequalities hold, x/y must be constant, which we are excluding. Hence at least one of the two inequalities does not hold, which implies that there is a point \mathcal{P} of K with $|\text{ord}_{\mathcal{P}}(x)| > |\text{ord}_{\mathcal{P}}(y)|$. Hence $|\text{ord}_{\mathcal{P}}(x^{m_l}/y^{m_j})| \geq |m_l|(|\text{ord}_{\mathcal{P}}(x)| - |\text{ord}_{\mathcal{P}}(y)|) \geq |m_l|$, which implies $\deg(x^{m_l}/y^{m_j}) \geq |m_l|$.

The same inequality holds if $m_j < 0$: we can simply repeat the argument just given, replacing y with y^{-1} and noting that xy cannot be constant.

Let now $d = [K : k(x)]$; we have $d \leq \deg h - 1$.

Suppose that $h(x)$ has a pole at $x = \infty$. Then a pole of x (resp. of y) must be a pole or a zero of y (resp. of x). Hence there are at most $3d$ places of K at which x or y has a zero or a pole. Similarly if $h(x)$ has a pole at $x = 0$.

Using Lemma 4 we then obtain

$$\deg f = m_l \leq \binom{s}{2} (3d + 2g - 2),$$

where g is the genus of K . This is estimated as $\leq (D - 1)(D - 2)/2$, where D is the degree of an irreducible equation $H(x, y) = 0$. Since $h(x) - h(y) = 0$, $H(X, Y)$ must be a divisor of the numerator of $(h(X) - h(Y))/(X - Y)$, which has degree $\leq 2 \deg h - 1$; hence $D \leq 2 \deg h - 1$. In conclusion we obtain

$$\deg f \leq \binom{2l - 1}{2} (4(\deg h)^2 - 7 \deg h + 1),$$

finishing the proof of Theorem 2. ■

Proof of Corollary to Theorem 2. Put $f(x) = p^{(r)}(q(x))$. We may suppose without loss of generality that $r \geq 2$.

We follow in part the normalization arguments from [DZ, Lemma 2], and we start to normalize $p(x)$ in the *Fatou normal form*.

Namely, let $L \in k[x]$ be a polynomial of degree 1 and set $p_1 := L \circ p \circ L^{-1}$, $q_1 := L \circ q$. We have $p_1^{(r)} \circ q_1 = L \circ p^{(r)} \circ q = L \circ f$.

Also, the number of nonconstant terms of $L \circ f$ is the same as that of f , and moreover if the conclusion is true for p_1, q_1 it is true for p, q . Therefore, we may work with p, q replaced by p_1, q_1 . Observe finally that by a suitable choice of L we may suppose that

$$(5) \quad p(x) = x^d + \alpha_2 x^{d-2} + \dots + \alpha_d$$

where $d := \deg p \geq 2$ and $\alpha_i \in k$.

Suppose first that one among $h_s(x) := p^{(s)}(q(x))$, $s = 0, 1, 2$, is not of the shape $ax^m + bx^{-m} + c$. Then we may apply Theorem 2 to $h_s(x)$ in place

of $h(x)$ and to $p^{(r-s)}(x)$ in place of $g(x)$. We obtain in the worst case

$$\deg f \leq (2l-1)(l-1)4(\deg p)^4(\deg q)^2,$$

whence

$$l \geq \frac{\sqrt{8}}{(\deg p)^2 \deg q} \sqrt{\deg f},$$

proving the inequality in the statement.

Hence we may assume that all $h_s(x)$, $s = 0, 1, 2$, are of the mentioned special shape, i.e.

$$h_s(x) = p^{(s)}(q(x)) = a_s x^{m_s} + b_s x^{-m_s} + c_s, \quad s = 0, 1, 2.$$

Putting $m := \deg q$, we have necessarily $m_s = md^s$.

Suppose first that $a_0 b_0 = 0$; then after replacing x with x^{-1} we may suppose $a_0 \neq 0$, $b_0 = 0$, whence $b_1 = b_2 = 0$ and $a_0 a_1 a_2 \neq 0$. Now, setting $L_s(x) = a_s x + c_s$, we have $q(x) = L_0(x^m)$, $p(L_0(x)) = L_1(x^d)$, $p(L_1(x)) = L_2(x^d)$.

If we take into account (5), the last two equations imply $c_0 = c_1 = 0$ (look at the second coefficient on both sides). Thus $p(a_0 x) = a_1 x^d$. In turn, (5) implies $p(x) = x^d$, as required.

Suppose now that $a_0 b_0 \neq 0$. Note that we may write x for x^m without affecting the content, which amounts to supposing $\deg q = 1$. Next, on setting $u := vx$ where $v^2 b_0 = a_0$, we have $q(x) = a(u + u^{-1}) + c_0$, where $a := b_0 v$.

From now on we write $z := u + u^{-1}$, so $q(x) = az + c_0$ and $h_s(x) = p^{(s)}(az + c_0)$.

This forces $p^{(s)}(az + c_0) = a^{d^s} T_{d^s}(z) + c_s$ for $s = 1, 2$, where T_m is the Chebyshev polynomial. Since the second coefficient of T_d is 0 (T_d has the same parity as d) we deduce from (5) that $c_0 = 0$.

The identity with $s = 1$ yields $p(az) = a^d T_d(z) + c_1$, which leads to $p^{(2)}(az) = p(a^d T_d(z) + c_1)$. The left side is $a^{d^2} T_{d^2}(z) + c_2$, by the use of the identity with $s = 2$. Hence, since $T_{d^2} = T_d \circ T_d$, we have $a^{d^2} T_d(z) + c_2 = p(a^d z + c_1)$. Comparing again the second coefficients we find $c_1 = 0$, whence $a^{d^2} T_d(z) + c_2 = p(a^d z) = a^d T_d(a^{d-1} z)$. But now Lemma 5, Ch. 1.4 of [S] implies $c_2 = 0$ and $a^{d-1} =: \varepsilon = \pm 1$.

From $p(az) = a^d T_d(z)$ we find $a^{-1} p(az) = \varepsilon T_d(z)$, and we have $q(z) = az$, proving finally what we want. ■

Added in proof (January 2007). In a recent preprint entitled “On composite lacunary polynomials and the proof of a conjecture of Schinzel” the present author has solved the problem mentioned in the Introduction, by proving that if $g(h(x))$ has boundedly many terms, then the same is true of $h(x)$.

References

- [BM] W. D. Brownawell and D. W. Masser, *Vanishing sums in function fields*, Math. Proc. Cambridge Philos. Soc. 100 (1986), 427–434.
- [DZ] R. Dvornicich and U. Zannier, *Cyclotomic Diophantine problems*, Duke Math. J., to appear.
- [S] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Cambridge Univ. Press, 2000.
- [Z] U. Zannier, *Some remarks on the S-unit equation in function fields*, Acta Arith. 64 (1993), 87–98.

Scuola Normale Superiore
Piazza dei Cavalieri, 7
56126 Pisa, Italy
E-mail: u.zannier@sns.it

Received on 2.7.2006
and in revised form on 3.12.2006

(5232)