pour tout \( q \) positif appartenant à \( I \), on a quand \( x \) tend vers \( +\infty \)
\[
\nu_q(x) - d_q x = \frac{x^{1/2} (\log \log x)^{q-1}}{(q-1)! (\log x)^q} \left( q \left( \frac{q-1}{\log \log x} \right) + O \left( \frac{q}{(\log \log x)^2} \right) \right)
\]
uniformément pour \( 1 \leq q \leq \log \log x \).

7. Généralisations.
7.1. Le théorème fondamental pourrait être généralisé en supposant \( f \) à valeurs entières pas forcément \( \geq 0 \).
La conclusion serait alors une formule semblable à (2) mais valable seulement pour \( |x| = 1 \), la fonction \( F \) et les fonctions \( A_1 \) étant définies sur la circonférence \( |x| = 1 \) et continues sur cette circonférence.
On pourrait encore en deduire un développement asymptotique de \( \nu_q(x) \) analogue à (34), valable cette fois pour \( q \) quelconque appartenant à \( Z \). On l’obtiendrait en partant de ce que
\[
\nu_q(x) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \left( \sum_{n \in \mathbb{Z}} e^{(\log x) n} \right) e^{-q \theta} d\theta.
\]

Les polynômes \( P_j \) seraient remplacés par des fonctions entières de type exponentiel \( F_j \) telles que, quand \( |x| \) tend vers \( +\infty \),
\[
F_j(x) = O(\|x|^{1/3}).
\]
Le
\[
O\left( x^{1/2} (\log \log x)^{q-1} (\log x)^{m-1} \right)
\]
serait remplacé par
\[
O\left( x^{1/3} (\log \log x)^{1/2} (\log x)^{m-1} \right).
\]

7.2. On pourrait aussi évaluer la somme
\[
\sum_{\text{n\ mod\ k}} g(n)
\]
et le nombre des \( n \leq x \) tels que \( n = l \text{ (mod} k) \) et \( f(n) = q \).

7.3. Enfin on pourrait ne plus supposer que l’on a \( f(p) = 0 \) et \( f(p^4) = 1 \) pour tout \( p \), mais que l’on a \( f(p) = 0 \) et \( f(p^3) = 0 \) ou \( 1 \) pour tout \( p \), l’ensemble des \( p \) pour lesquels \( f(p^q) = 1 \) étant un „bon ensemble” de densité positive, ce terme ayant la signification qui lui est attribuée dans \( \Delta \mathbb{S} \) (p. 139).
provided one uses a stronger form of Siegel's Theorem ([7], pp. 127, 135.) Accordingly one finds that the components in question have polynomial parametrizations in each of the following cases:

(i) \( P_1 \) and \( P_2 \) have relatively prime degrees;

(ii) \( B \) is contained in an integrally closed subring \( B \) of \( K \) with only a finite number of units, e.g., \( B = \mathbb{Z} \), the ring of integers of a complex quadratic field, or \( \mathbb{Z}[X_1, X_2, \ldots, X_n] \);

(iii) \( K = \mathbb{Q} \) the field of rational numbers and the greatest common divisor of the degrees of \( P_3 \) and \( P_4 \) is neither even nor a multiple of 3.

The sufficiency of the first two conditions follows from the above mentioned results of M. Fried whereas the third requires in addition some results on minimal separations of M. Fried and R. E. MacRae ([3], Th. 2.3, Th. 4.2) as well as the fact that the minimal separation of a quadratic over \( \mathbb{Q} \) is of degree 2, 3, 4, or 6 which can be verified directly using linear recurrences.

I would like to thank Prof. D. J. Lewis for extensive conversations on this problem as well as Prof. P. Eakin for an idea used in the proof of the proposition below and Prof. M. Fried for pointing out a serious error in the original version of this paper.

Whereas the proof of the previously mentioned result on algebraic number fields was based on the idea that polynomials of different degrees grow at different rates, the idea of the proof of Theorem 1 depends on a somewhat more delicate property, viz. If \( a_1, a_2, \ldots \) are elements of \( K \) which satisfy \( a_1^2 = a_2^2 \), then the \( a_i \) are roots of unity. The following result is the first step toward reducing to a point where this idea can be used.

**Theorem 2.** Let \( K \) be a field finitely generated over the rationals and \( A \) be a finitely generated subring of \( K \). Suppose \( S(X) - T(Y) = 0 \) is a curve whose every absolutely irreducible component is defined over \( K \) and let \( m > 0, n > 0 \) be the degrees of \( S, T \) respectively where \( m = m, n \), and set \( r = (m, n) \). Then any absolutely irreducible component \( V_1 \) of \( S(X) - T(Y) = 0 \) which admits a polynomial parametrization is of the form \( S_1(X) - \xi T_1(Y) = 0 \) where

(i) \( S_1 \) and \( T_1 \) are polynomials over \( K \) of degree \( m \) and \( n \) respectively.

(ii) There is a polynomial \( U \) in \( K[X] \) of degree \( r \) such that \( S(Z) = U(S_1(X)) \) and \( T(Z) = U(T_1(X)) \).

(iii) There are polynomials \( F_1 \) and \( G_1 \) in \( K[X] \) of degrees \( m \) and \( n \) respectively such that \( S_1(F_1(X)) = T_1(G_1(X)) \).

Further, if \( V_2 \) is any other absolutely irreducible component of \( S(X) - T(Y) = 0 \) with a polynomial parametrization, then \( V_2 \) is of the form \( S_1(X) - \xi T_1(Y) + b = 0 \) where \( \xi \) is an \( r \)-th root of unity, \( b \in K \), and \( U(\xi X - b) = U(X) \).

The degrees of \( S_1, T_1, F_1, G_1 \) are clearly \( m/r, n/r, n/r \), and \( m/r \) respectively. Now \( X = F_1(t), Y = G_1(t) \) also parametrize \( V_1 \) and \( S_1(F_1(t)) = T_1(G_1(t)) \) since \( h(t) = S_1(F_1(h(t))) = T_1(G_1(h(t))) \). Finally \( S_1(X) - T_1(Y) \) is absolutely irreducible by Ehrenfeucht's Theorem ([1]), and so \( U, F_1, G_1, S_1, T_1 \) satisfy the conditions of the theorem.

Suppose now that \( V_2 \) is another absolutely irreducible component of \( S(X) - T(Y) = 0 \) with a polynomial parametrization. As in the case of \( V_1 \), we can find \( U', F'_1, G'_1, S'_1, T' \). Now \( S'(X) = U'(S'_1(X)) \)

\[ U'(S'_1(X)) \text{ and }, \text{since } U \text{ and } U' 	ext{ are of the same degree, there is a linear polynomial } \lambda \text{ over } K \text{ with } U_1 = U'_1 \lambda_1^{r_1}, \text{ and } S_1 = l_1 \circ S'_1 ([4], p. 169). \]

Applying the same argument to \( T(X) \), we get a linear polynomial \( l_2 \) over \( K \) with \( l_2 \circ T_1 = T'_1 \). It follows that \( V_2 \) is the curve \( S_2(X) = l_2 \circ l_1 \circ T_1(Y) \). Further \( T(X) = U(T_1(X)) = U(l_1(l_2(T_1(X)))) \) implies \( U(X) = U(l_2(l_1(X))) \) and so the leading coefficient of \( l_2(l_1(X)) \) is an \( r \)-th root of unity. This completes the proof of Theorem 2.
We will need to know that we can obtain almost all of the points of \( V \), defined over \( K \) by taking values in \( K \) of the parameter \( t \). This is the content of the following proposition.

**Proposition.** If \( S_1(X) = T_1(Y) = 0 \) is an affine plane curve defined and parametrized over a field \( K \) by \( X = F_1(t) \) and \( Y = G_1(t) \) where \( F_1 \) and \( G_1 \) are polynomials having relatively prime degrees, and if \( P \) is any simple point over \( K \) of \( S_1(X) - T_1(Y) = 0 \), then \( P = (F_1(t_0), G_1(t_0)) \) for some \( t_0 \in K \).

**Proof.** Since \( K[F_1(t)] \cap K[G_1(t)] = K[S_1(F_1(t))] \) and the degrees of \( F_1 \) and \( G_1 \) are relatively prime, it follows by a result of Fried ([14], p. 189) that \( K[F_1(t), G_1(t)] = K[1] \). Now the coordinate ring of \( S_1(X) - T_1(Y) = 0 \) is \( K[F_1(t), G_1(t)] \), and so its integral closure is \( K[1] \). Suppose \( \mathfrak{O} \) is the prime ideal corresponding to a simple point \( P \) of \( S_1(X) - T_1(Y) = 0 \) which is defined over \( K \), and that \( \mathfrak{O} \) is the prime lying over it in \( K[1] \). Then \( K[F_1(t), G_1(t)]_{\mathfrak{O}} = K[1]_{\mathfrak{O}} \). Now \( P \) is parametrized by the value of \( t \) in \( K[1]/\mathfrak{O} K[1] \cong K[F_1(t), G_1(t)]_{\mathfrak{O}}/\mathfrak{O} K[F_1(t), G_1(t)]_{\mathfrak{O}} = K \).

which shows the result.

Note that, since \( S_1(X) - T_1(Y) = 0 \) has at most a finite number of singular points, replacing \( K \) with some finite algebraic extension field would allow us to make the same conclusion without the restriction that \( P \) is simple.

For the proof of Theorem 1, we will need several lemmas on Tchebychev polynomials. Recall that the \( n \)th Tchebychev polynomial is the unique polynomial with integer coefficients such that \( T_n(\cos \theta) = \cos n \theta \) for all \( \theta \). The roots of \( T_n \) are therefore \( \cos \frac{k\pi}{n} \) for \( k = 0, 1, \ldots, n-1 \) and \( n=1 \). Adding the expansions of \( \cos(n+1)\theta \) and of \( \cos(n-1)\theta \) gives the recursion formula:

\[
T_{n+1}(X) = 2XT_n(X) - T_{n-1}(X).
\]

From this, it is easy to see that \( T_n \) is a polynomial of degree \( n \) with

(i) leading coefficient \( 2^{n-1} \),

(ii) trace 0,

(iii) coefficient of \( X^{n-2} \) equal to \( -n2^{n-1} \), and

(iv) constant term equal to 0 for \( n \) odd and \( (-1)^{n/2} \) for \( n \) even.

**Lemma A.** If \( n \geq 2 \) and

\[ aT_n(bX + c) + d = T_n(X), \]

then \( a = 0 \) and \( ab^n = 1 \). If further \( n \geq 3 \), then \( b = \pm 1 \) and \( d = 0 \). If however \( n = 2 \), then \( d = a = 1 \).

**Proof.** Comparing coefficients using (i) and (ii) above gives \( ab^n = 1 \) and \( c = 0 \). If \( n \geq 3 \), comparing the coefficients of \( X^{n-1} \) gives \( ab^{n-1} = 1 \) and so \( b = \pm 1 \). Comparing constant terms gives \( aT_n(0) + d = T_n(0) \). If \( n \) is odd, (iv) gives \( d = 0 \). If \( n = 2 \), then \( T_n(0) = -1 \) and so \( d = a = 1 \). If \( n \) is even and \( n \geq 3 \), then \( ab^n = 1 \) implies \( a = 1 \) and so \( d = 0 \) as desired.

**Lemma B.** Suppose \( n \geq 2 \) and \( m \neq 1 \). If \( g \) is a polynomial with \( g(0) \neq 0 \) and \( t_1, t_2 \) are linear such that

\[ T_n(X) = t_1 g(X)^m \circ t_2, \]

then

(i) \( g(t_1(0))^m = \text{constant} \Rightarrow n = 2, t_1(0) = -1, t_2(0) = 0, \)

(ii) \( g(t_2(0))^m = \text{constant} \Rightarrow t_2(0) = \pm 1, m = 2, \)

**Proof.** If \( t_1(X) = aX + b \) and \( t_2(X) = cX + d \), we have

\[ T_n(X) = a(cX + d)^m g(cX + d)^m + b. \]

Differentiating gives:

\[ T'_n(X) = nacg(aX + d)^m - 1k \]

if \( g(aX + d)^m = k \) is a constant,

\[ T'_n(X) = acmg(aX + d)^m - 1g'(aX + d) \]

if \( r = 0 \) but \( g(aX + d)^m \) is not constant, and

\[ T'_n(X) = acg(aX + d)^{m-1}g'(aX + d) + m(aX + d)g'(aX + d) \]

otherwise. In the first case, \( n = 2 \) since \( T'_n(X) \) has only simple roots and the conclusion follows. In the other two cases, the same argument shows that \( m \leq 2 \) and \( r \leq 2 \). The roots of \( g(aX + d) \) are among the \( \cos \frac{k\pi}{n} \) for \( k = 1, 2, \ldots, n \). But \( T_n \left( \cos \frac{k\pi}{n} \right) = cK \left( \cos k\pi = (-1)^{k} \right. \). Hence \( k = \pm 1 \) by substitution, which completes the proof.

Let us say that two polynomials \( S \) and \( F \) are permutable if there are polynomials \( T \) and \( G \) with degree \( S = \text{degree} G \), degree \( T = \text{degree} F \), and \( S \circ F = T \circ G \). There are two obvious kinds of permuting, viz.

\[ X^m \circ X^n h(X^m) = X^n h(X)^m \circ X^m \]

and

\[ T_n \circ T_m = T_m \circ T_n. \]

Ritt's Theorem is a converse ([14], § 4).
THEOREM. Suppose $S$, $T$, $F$, and $G$ are non-constant polynomials of a field of characteristic zero such that

$$S(F(X)) = T(G(X))$$

and

$$m = \deg S = \deg G \leq \deg F = \deg T = n.$$ 

If $(m, n) = 1$, then there are linear polynomials $l_1, l_2, l_3, l_4$ over $1$ such that either

(i) $l_1 \circ S \circ l_2 = X^m \circ l_4$ and $l_2 \circ F \circ l_3 = X^n \circ l_4$, where $h$ is a polynomial over the algebraic closure $K$ of $K$ or

(ii) $l_1 \circ S \circ l_2 = T_n \circ l_4$ and $l_2 \circ T \circ l_3 = T_n \circ l_4$.

COROLLARY 1. If $0 < m < n$ are relatively prime, then the only curve of the form $S(X) = T(Y) = 0$ where $S = m$, degree $T = n$, and which have an infinity of points defined over a ring finitely generated over the integers $Z$, are those of the form

$$l_1 \circ X^m \circ l_2 = l_1 \circ X^n \circ l_2(Y)$$
or

$$l_1 \circ T \circ l_3 = l_1 \circ T \circ l_4(Y),$$

where $l_1$, $l_2$, and $l_3$ are linear.

Proof. This follows from Ritt's Theorem, or more simply from Fried ([23], Theorem 3).

COROLLARY 2. Let $l_1, l_2, l_3$ be linear and $1 < m < n$ be integers with $(m, n) = 1$. Suppose that each of the following curves admits infinitely many points defined over some fixed finitely generated ring:

(i) $X^m = l_1 \circ X^n \circ l_2(Y)$. Then $l_2(0) = 0$.

(ii) $X^m = l_1 \circ T_n \circ l_2(Y)$. Then $m = 2$ and this curve is of the form

$$T(x) = T_n \circ l_2(Y).$$

(iii) $T_m(X) = l_1 \circ T_n \circ l_2(Y)$. If $m \geq 3$, then $l_2(X) = \pm X$. If $m = 2$, then $l_1(X)$ is of the form $\pm X + c - 1$. So the curve is

$$T_m(X) = T_n \circ l_2(Y).$$

Proof. (i) If $l_2 \circ X^m = X^n \circ l_2$ where $s \geq 2$ and the $l_i$ are linear, then $l_1(0) = l_2(0) = 0$. So this case follows from Lemma B and the last corollary.

(ii) By the last corollary and Lemma B, $m \geq 3$ is impossible. Suppose $m = 2$. If the curve is of type (i) in Corollary 1, then there are linear polynomials $l_1(X) = ax + b$ and $l_2(X)$ such that $l_2(X)^2 = l_1(X)^2$. Where $b \leq 1$ for some polynomial $g$. The first equation implies $f = 0$. If $l_2(X) = ax + b$, then by the second equation and Lemma B, $X = l_2 \circ l_1(X)$ for some constant $c$. So $X = cax + cx + b$ or $a = \mp b$. Hence $t_1$ is of the form $l_1(X) = ax \pm a$. If the curve is of type (ii) however, and $l_1(X) = ax + b$, then Lemma A implies that there is a linear polynomial $X^2 + a$ such that $(ax + b)^2 = (ax + b) = (ax + b)^2$. Hence $a = 0$ and $b = \pm a$. So once again $l_1(X) = ax \pm a$. But now it is easy to see that the curve is of the desired form with $d = (\mp 2 a)^{1/2}$ and $l_2(Y) = \mp l_2(Y)$.

(iii) If $m \geq 3$, then Lemma B says that this curve must come from an infinite number of Tchebychev polynomials. But then the result follows from Lemma A. If $m = 2$, then (ii) says that we have a curve arising from a Tchebychev polynomial. Again Lemma A gives the form for $l_1$. This completes the proof of Corollary 2.

REDUCTION LEMMA. Let $m$ and $n$ be relatively prime integers both of which are at least 2, and let $K$ be a field of characteristic 0. Suppose $S_i(F(X) - \mp V_i(Y) = 0$ for $i = 1, 2, \ldots, s$ are curves with polynomial parametrizations such that $S_i$ and $V_i$ are polynomials of degree $m$ and $n$ respectively. If there is an infinite sequence $\{a_i\}$ of elements of $K$ such that for each $i$, there is a $j$ with $S_i(a_j = V_j(a_{i+1})$ and such that no element of $K$ occurs more than a finite number of times in the sequence, then for some $j$, $S_i(F(X) - \mp V_i(Y) = 0$ has an infinity of points of the form $(a_i, a_{i+1})$ and both $S_i$ and $V_j$ are of the form

$$l_1 \circ X^n \circ l_2 \text{ or } l_2 \circ T \circ l_3$$

where $l_1$ and $l_2$ are linear and $T_k$ is a Tchebychev polynomial.

Proof. By discarding some of the curves $S_i(X) - \mp V_i(Y) = 0$ and an initial segment of the $a_i$, one can assume that all the curves have an infinity of points of the form $(a_i, a_{i+1})$. Theorem 2 shows that $S_i(F(X) - \mp V_i(Y) = 0$ has a parametrization of the form $\text{form } F_i(t) = F(t)$ and $Y = G(t)$ where $F_i$ and $G_i$ are polynomials of degree $m$ and $n$ respectively. After discarding an initial segment of the sequence of $a_i$, one can assume by the proposition that for each $i$ there is a $\beta_i$ in $K$ and a $j(i)$ such that

$$F_{i(j(i)}(\beta_i) = a_i \text{ and } G_{i(j(i)}(\beta_i) = a_{i+1}.$$ 

Now

$$F_{i(j(i)}(\beta_i) = a_i \text{ and } G_{i(j(i)}(\beta_i) = a_{i+1}.$$ 

Further $S_j(F_i(t)) = V_j(G_i(t))$ and so $S_j$ and $V_j$ permute with polynomials of degree $m$ and $n$ respectively.

Taking a suitable set of curves $F_i(X) - G_j(Y) = 0$ and a final segment of the $\beta_i$, one can repeat the construction again. (Here one uses those $F_i(X) - G_j(Y) = 0$ which admit an infinite number of solutions of the form $(\beta_i, \beta_{i-1})$ and so the curve have polynomial parametrizations by Fried ([2], Th. 3 and its Corollary). After repeating the process $k$ times, one gets that some $S_i$ and some $V_j$ permute with polynomials of degree $m^k$ and $n^k$ respectively. By choosing $k$ large enough so $m^k, n^k$ are greater
than \( n \), \( m \) respectively, one sees by Corollary 1 that \( S_i \) and \( V_j \) are within linear change of variables either powers or Techebychev polynomials. If \( m > n \), then \( S_i(X) - V_j(Y) = 0 \) satisfies the conclusion of the lemma by Corollary 1. Similarly, if \( m < n \), then \( S_i(X) - V_j(Y) \) works. This completes the proof of the lemma.

Remark 1. In the above proof, it was shown that at each step, at least one of the curves \( F_i(X) - G_j(Y) = 0 \) arising from the parametrizations \( X = F_i(t) \) and \( Y = G_j(t) \) has an infinity of points defined over a finitely generated subring \( A \). This fact will be used below in the proof of Theorem 1.

Lemma C. If \( K_o \) is a finitely generated field extension of the rationals \( \mathbb{Q} \) and if \( S \) and \( T \) are non-constant polynomials of different degrees, then there are at most a finite number of finite sets \( E \subseteq K_o \) with \( S(E) = T(E) \).

Proof. In the case of algebraic number fields, this result occurs as Theorem 2 of [5]. One can reduce to this case by the same method as is used in the previously mentioned paper of D. J. Lewis [9]. To do this we need only make a few changes in his section 5. In Lemma 5, replace condition (i) with \( X^s = \text{union of finite sets } X_k \) such that \( E(X_k) = G(X_k) \).

In the proof of that lemma, omit the condition (II) on the point \( a \) and replace the \( G_{i,j,s,a} \) with

\[
G_{i,j,s,a} = \sum_{E \subseteq K_o} [X^s E] - [X^s E].
\]

Conclude that \( E \) is finite.

Lemma D. Let \( S \), \( T \in k[X] \) be polynomials with coefficients in a field \( k \) of characteristic \( 0 \) and \( V_n \) be the algebraic set defined by the equations: \( S(X_1) = T(X_1), S(X_2) = T(X_2), \ldots, S(X_{n-1}) = T(X_{n-1}), S(X_n) = T(X_1) \). Suppose that \( S \) and \( T \) are not both constants. Then \( V_n \) is of dimension 0 except possibly when \( S \) and \( T \) have the same degrees and the ratio of their leading coefficients is an \( n \)-th root of unity in \( k \).

Proof. By the Lefschetz principal, we are reduced to the case where \( k \) is a subfield of the field of complex numbers. First let us prove the

FACT. The only bounded algebraic sets \( V \) of \( C^n \) are those of dimension zero.

Proof. It suffices to consider the case where \( V \) is irreducible of dimension, say \( r > 0 \). Let \( C[V] = C[x_1, x_2, \ldots, x_n] \) be the coordinate ring of \( V \). By the Noether normalization theorem, there are linear combinations \( y_i = (i = 1, 2, \ldots, r) \) of the \( x_i \) with complex coefficients such that \( C[y_1, y_2, \ldots, y_r] \) is a polynomial ring in \( r \) variables, and \( C[V] \) is integral over \( C[y_1, y_2, \ldots, y_r] \). The points of \( V \) are the finite specializations in \( C^n \) of \( (x_1, x_2, \ldots, x_n) \) over \( C \). Suppose the set of these is bounded. Then the set of finite specializations in \( C^n \) of \( (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r) \) over \( C \) is also bounded, say by \( M > 0 \). But \((y_1, y_2, \ldots, y_r) \rightarrow (M+1, 0, \ldots, 0)\)

can be extended to a finite specialization of \((x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r)\) by the lying over theorem which is a contradiction.

Now to prove the proposition, we may suppose

\[
S(X) = X^s + F(X), \quad T(X) = aX^t + G(X)
\]

where \( a \neq 0 \), degree \( F < s \), degree \( G < t \), and \( s, t > 0 \). If \( V_n \) is not of dimension 0, then by the fact, it is unbounded. Suppose for example that it is unbounded in the first coordinate, and choose points \( P_j = (x_{j,1}, x_{j,2}, \ldots, x_{j,n}) \) in \( V_n \) with \( |x_{j,i}| \rightarrow \infty \) as \( j \rightarrow \infty \). Now since \( S(a_{j,i}) = T(a_{j,i}), |a_{j,i}| \rightarrow \infty \) as \( j \rightarrow \infty \).

Similarly \( |a_{j,i}| \rightarrow \infty \) as \( j \rightarrow \infty \) for \( i = 1, 2, \ldots, n \). By deleting a finite number of the \( P_j \), we may suppose that \( x_{j,1}, x_{j,2}, \ldots, x_{j,n} \neq 0 \) for all \( j \). Multiplying the equations for \( V_n \) together and dividing by \( (X_1X_2 \ldots X_n)^i \) gives

\[
\prod_{i=1}^n \frac{a_{j,i} + F(x_{j,i})}{x_{j,i}} = \prod_{i=1}^n \left( a + G(x_{j,i}) \right).
\]

The right hand member approaches \( a^n \neq 0 \) as \( j \rightarrow \infty \). But then \( s = t \) and \( a^n = 1 \) which shows the result.

Proof of Theorem 1. Suppose \( S(E) \subseteq T(E) \) where \( S \) and \( T \) are of different degrees and \( E \) is an infinite subset of a field \( K \) which satisfies the hypothesis of Theorem 1. First note that there are but a finite number of finite sets \( F \subseteq K \) such that \( S(F) = T(F) \). This follows by Lemma D and Lemma C applied to the algebraic closure \( \bar{K} \) in \( K \) of the field generated over \( K \) by the coefficients of \( S \) and \( T \).

The sequences \( \{a_{i} \mid i \geq 0 \} \subseteq E \) such that \( T(a_i) = S(a_{i-1}) \) for \( i > 0 \) clearly cover \( E \). If the \( a_{i} \) is of finite cardinality for each such sequence, then for every \( a_j \in E \) there is a finite sequence \( a_0, a_1, a_2, \ldots, a_n \) where \( a_j \in E \), \( S(a_{i-1}) = T(a_i) \) for \( 0 < i < n \), \( a_n = a_j \) for some \( n \), and \( a_0, a_1, \ldots, a_{n-1} \) are distinct. Clearly \( F(a_0) = (a_{i+1}, a_{i+1}, \ldots, a_n) \) is a finite set satisfying \( S(F(a_0)) = T(F(a_0)) \). Since there are but a finite number of such sets, some \( F = F(a_0) \) for an infinity of \( a_j \in E \). On the other hand, for any \( b \) there are but a finite number of solutions of \( S(X) = T(b) \). It is therefore possible to construct by induction, using the sequences \( \{a_{i} \} \) for which \( F = F(a_0) \), new sequence of distinct elements \( \beta_0, \beta_1, \ldots, \) such that \( S(\beta_{i+1}) = T(\beta_i) \) for all \( i \geq 0 \).

If, however, at least one of the sequences \( \{a_{i} \} \) had infinite cardinality, then by deleting segments of the form \( a_{r}, a_{r+1}, \ldots, a_{s} \), where \( a_r = a_{r+1} \), one can assume that all the \( a_{i} \) are distinct. Up to switching the roles of \( S \) and \( T \), it has been shown that there is an infinite sequence \( \{a_{i} \} \) of distinct elements of \( E \) such that \( S(a_{i}) = T(a_{i+1}) \) for \( i \geq 0 \). From
now on we assume $E = \{a_i\}$. $E$ is contained in a subring of $K$ finitely generated over $\mathbb{Z}$ ([10], p. 132).

In order to complete the proof, it suffices by Theorem 2 and Fried and MacRae ([4], Theorem 3.5) to show that the degree $m$ of $S$ is a multiple of the degree $n$ of $T$ or vice versa. Suppose therefore that such is not the case. Let $r = n/m$, $s = m/n$, and $t = n/r$. By Theorem 2, the components of $S(X) - T(Y) = 0$ which admit polynomial parametrizations are of the form $S_t(X) - V_t(Y) = 0$, where $S_t$ and $V_t$ are of degree $s$ and $t$ respectively. By discarding an initial segment of the sequence $a_i$, one can suppose that for each $i$, $a_{s(i)}$ lies on at least one of the $S_t(X) - V_t(Y) = 0$. The Reduction Lemma now shows that at least one of these components, say $S_t(X) = V_t(Y)$ has $S_t$ and $V_t$, either a power of a Chebyshev polynomial (up to linear change of variables). Now considering each of these several cases, it will be shown that $S(X) - T(Y) = 0$ must have a very special form.

Case 1. Suppose $S_t(X) - V_t(Y) = 0$ is of the form

$X^{s_i}l_i(X) = l_i(Y)l_t(Y)$

where the $l_i$ are linear. By part (i) of Corollary 2, this can be rewritten as $X^{s_i}l_i(X) = Y^{s_i}l_i(Y)$ with $l_i$ linear. Further, by replacing the $a_i$ with $a_{s(i)} = Y^{s_i}l_i(Y)$, we are reduced to $S(X) = T(Y)$ which is $X = l(X)l_t(Y)$ where $l_t$ is an even root of unity. These are parametrized by $X = Y^t$, $S_t(X) = Y^{s-i}l_t(Y)$, $S_t(Y) = Y^{s-i}l_t(Y)$, $S_t(Y) = Y^{s-i}l_t(Y)$, $S_t(X) = Y^{s-i}l_t(Y)$, $S_t(Y) = Y^{s-i}l_t(Y)$, $S_t(X) = Y^{s-i}l_t(Y)$, $S_t(Y) = Y^{s-i}l_t(Y)$. By Remark 1 after the Reduction Lemma, at least one of the curves $X^{s-i}l_i(X) = Y^{s-i}l_i(Y)$ has an infinity of points over $A$. By Corollary 2, $l_t^{-1}(0) = l_t(0) = 0$. Let $l_t(X) = cX$ and choose a $c$ with $d^{s-i} = c^i$. Except for components with only a finite number of points of the form $(a_i, a_{s-i})$, $S(X) - T(Y) = 0$ is of the form $X^{s-i} = c^iY^{s-i}$. By replacing the $a_i$ with $a_{s-i}$, we are reduced to the case of $X^{s-i} = Y^{s-i} = 0$.

Case 2. Suppose $S_t(X) - V_t(Y) = 0$ is of the form

$T_i(X) = T_t(X)$

and that $s, t \geqslant 3$. As in Case 1, we can reduce to the case where $l_t(X) = X$ by replacing the $a_i$ with $a_{s(i)}$. By Corollary 2 and Theorem 2, the only other possible component of $S(X) - T(Y) = 0$ containing an infinity of points of the form $(a_i, a_{s-i})$ is $S_t(X) = T_t(Y)$. If not, by Remark 1, at least one of the $T_i(X) = \pm l_t^{-1}(T_i(Y))$ has an infinity of points over $A$. By Corollary 2, $T_i^{-1}(X) = T_i(0)$, $T_i^{-1}(Y) = T_i(0)$. Therefore, with the exception of components containing at most a finite number of points of the form $(a_i, a_{s-i})$, $S(X) - T(Y) = 0$ is $S_t(X) = T_t(Y)$.

Case 3. Suppose $S_t(X) = V_t(Y)$ is of the form

$T_t(X) = T_t(Y)$

where $t \geqslant 3$ is odd. As before, we may suppose $l_t(X) = X$. Remark 1 shows that for some linear $l_t$, both $T_t(X) = T_t(l_t(Y))$ which is a component of $S(X) = T(Y) = 0$ and $T_t^{-1}(T_t(X)) = T_t(Y)$ have an infinite number of points defined over $A$. By Corollary 2, this last curve looks like $T_t(eX) = \pm T_t(Y)$. This is parametrized by $X = e^{-1}T_t(Z)$ and $Y = T_t(Z)$. Again we may assume $T_t(X) = e^{-1}T_t(Y)$ has an infinity of points defined over $A$. By Corollary 2, $e^{-1} = \pm 1$. Hence $S(X) - T(Y) = 0$ is $T_t(X) = \pm T_t(Y)$ up to components with only a finite number of points of the form $(a_i, a_{s-i})$.

Corollary 2 shows that, except for the cases that we get by switching the roles of $s$ and $t$ in the three previous cases, that we have exhausted all possibilities of $s, t > 1$. If $s$ or $t$ is 1, then there is nothing to prove. Hence in all cases, we have reduced $S(X) - T(Y) = 0$ to a form where the next lemma applies and gives a contradiction.

LEMMA E. Let $S_t, T_t, T_s, \ldots, T_t$, be polynomials such that the set of curves $S_t(X) - T_t(Y) = 0$ is the same as the set of curves $X = T_t(Z), Y = S_t(Y)$. Suppose every component of the curve $S(X) - T(Y) = 0$ which has an infinity of points of the form $(a_i, a_{s-i})$ is among the curves $S_t(X) - T_t(Y) = 0$. If degree $S_t > 1$, then $E$ is a finite set.

Proof. The set $E$ can contain at most a finite number of points $(a_i, a_{s-i})$ which are not contained in the $S_t(X) - T_t(Y) = 0$. Choose a $k_i$ such that for $i > k_i$, $(a_i, a_{s-i})$ is not one of these bad points and renumber the $a_i$ for $i \leqslant k_i$ by $a_{s-i}$. By replacing $A$ with the integral closure of an appropriate finite extension, we can assume via the proposition that, for $i > 0$, the $(a_i, a_{s-i})$ are of the form $a_{s-i} = T_{(i)}(a_i), a_{s-i} = S_{(i)}(a_i)$ the $a_{s-i}$. Without making further extension of $A$, we can find $a_{s-i} \in A$ with $a_{s-i} = T_{(i)}(a_i), a_{s-i} = S_{(i)}(a_i)$. By induction, there are $a_{s-i} \in A$ for $i > k$ with $a_{s-i} = S_{(i)}(a_{s-i})$. The same equation can be used to inductively define the $a_{s-i}$ for $k$ negative. The set $F$ of all the $a_{s-i}$ satisfies $S_{(i)}(F) = F$. By [12] or the one-dimensional case of the theorem of D. J. Lewis [9], $F$ and $a_{s-i}$ is finite. This completes the proof of the lemma and of Theorem 1.

We conclude with the following example.

EXAMPLE. The proof of the theorem divided naturally into two parts.

The first part treated the sets $\{a_i\}$ where $P_i(a_i) = P_i(a_{s-i})$ for all $i$, and the second part was concerned with the number of finite sets $F$ which satisfy $P_i(F) = P_i(F)$. In general, it is possible that all sets of the first type be finite, but that there be an infinity of sets of the second type, for example, let $K = \mathbb{Q}(\zeta_p)$ where $\zeta_p$ is a primitive $p$th root of unity for
every prime \( p \) and let \( P_1, P_2 \) be polynomials with \( \deg P_1, \deg P_2 = 1 \). If \( p_1, p_2, \ldots, p_k \) are the first \( k \) primes, and if \( n < p_k \), then there is no proper extension of \( Q(\zeta_{p_1}, \zeta_{p_2}, \ldots, \zeta_{p_k}) \) contained in \( K \) of degree \( \leq n \). So by choosing \( n \) bigger than the degrees of \( P_1 \) and \( P_2 \) and \( k \) large enough so that \( k > n \) and the coefficients of the \( P_1 \) and \( P_2 \) are in \( Q(\zeta_{p_1}, \ldots, \zeta_{p_k}) \) we are assured that the sets of the form \( \{a_i\} \) are contained in \( Q(\zeta_{p_1}, \ldots, \zeta_{p_k}) \) and are hence finite. Nevertheless, if \( P_1(X) = X^n \) and \( P_2(Y) = Y^n \), then taking \( p \) to be any prime relatively prime to \( n \) and \( n \), we have \( P_1(E_p) = E_p = P_2(E_p) \) where \( E_p = (\zeta_{p_1}, k = 1, 2, \ldots, p) \). So there are infinitely many sets of the second type. The same phenomenon occurs for \( P_1, P_2 \) of the same degree when \( K = Q(\{0\}) \).

References


UNIVERSITY OF KENTUCKY
Lexington, Kentucky

Received on 30. 4. 1972 (374)