pour tout ϱ positif appartenant à I, on a quand x tend vers $+\infty$

$$v_q(x)-d_qx=\frac{x^{1/2}(\log\log x)^{q-1}}{(q-1)!(\log x)^2}\left(A\left(\frac{q-1}{\log\log x}\right)+O\left(\frac{q}{(\log\log x)^2}\right)\right)$$

uniformément pour $1\leqslant q\leqslant \varrho\log\log x$.

7. Généralisations.

7.1. Le théorème fondamental pourrait être généralisé en supposant f à valeurs entières *pas forcément* $\geqslant 0$.

La conclusion serait alors une formule semblable à (2) mais valable seulement pour $|z|=1$, la fonction F et les fonctions A_j étant définies sur la circonférence $|z|=1$ et continues sur cette circonférence.

On pourrait encore en déduire un développement asymptotique de $v_q(x)$ analogue à (34), valable cette fois pour q quelconque appartenant à $\boldsymbol{Z}$. On l'obtiendrait en partant de ce que

$$v_q(x)=\frac{1}{2\pi}\int_{-\pi}^{+\pi}\left(\sum_{n\leqslant x}e^{i\theta f(n)}\right)e^{-qi\theta}\,d\theta.$$

Les polynomes P_j seraient remplacés par des fonctions entières de type exponentiel F_j telles que, quand $|X|$ tend vers $+\infty$,

$$F_j(X)=O(e^X|X|^{-1/2}).$$

Le

$$O\left(x^{1/2}\frac{(\log\log x)^{q-1}}{(\log x)^{m+2}}\right)$$

serait remplacé par

$$O\left(x^{1/2}\frac{(\log\log x)^{-1/2}}{(\log x)^{m+1}}\right).$$

7.2. On pourrait aussi évaluer la somme

$$\sum_{\substack{n\leqslant x\\ n\equiv l(\mathrm{mod}\,k)}}z^{f(n)}$$

et le nombre des $n\leqslant x$ tels que $n\equiv l(\mathrm{mod}\,k)$ et $f(n)=q$.

7.3. Enfin on pourrait ne plus supposer que l'on a $f(p)=0$ et $f(p^2)=1$ pour tout p, mais que l'on a $f(p)=0$ et $f(p^2)=0$ ou 1 pour tout p, l'ensemble des p pour lesquels $f(p^2)=1$ étant un „bon ensemble" de densité positive, ce terme ayant la signification qui lui est attribuée dans AS (p. 139).

Reçu le 22. 4. 1972 (270)

ACTA ARITHMETICA
XXIII (1973)

Image sets of polynomials

by

K. K. Kubota (Lexington, Ky.)

W. Narkiewicz has shown ([11], [12]) that if K is a purely transcendental extension of a number field, then the only polynomials $P\in K[X]$ which admit infinite invariant sets in K (i.e. subsets E of K with $P(E)=E$) are the linear ones. He conjectured [13] that more generally if P_1 and P_2 are two polynomials over K such that there is an infinite subset $E\subseteq K$ satisfying $P_1(E)=P_2(E)$, then P_1 and P_2 have the same degree. In [5], this conjecture was verified in the case of algebraic number fields under the additional assumption that the polynomial of lower degree is injective on E. This was generalized by D. J. Lewis [9] to the case of finitely generated fields K and also to morphisms over such fields of projective n-space into itself.

However, as noted in [5], the conjecture as stated is false. $P_1(X)=X^2+X+1$, $P_2(X)=P_1(F(X))$ where $F(X)=X^2-X+1$, and E the set consisting of 0, 1, $F(1), F(F(1)), \ldots$ was the counter-example given there. The main result of this paper states that under certain conditions this is the only possible kind of counter-example.

Theorem 1. *Let K be a field of characteristic zero such that the algebraic closure in K of any subfield finitely generated over the rationals $\boldsymbol{Q}$ is finitely generated. Suppose P_1 and P_2 are polynomials over K with degree $P_1<$ degree P_2. If there is an infinite subset E of K satisfying $P_1(E)\subseteq P_2(E)$ or $P_2(E)\subseteq P_1(E)$ and if every component of $P_1(X)-P_2(Y)=0$ containing an infinity of points of $E\times E$ has a polynomial parametrization, then $P_2(X)=P_1(F(X))$ for some polynomial F over K.*

The applicability of Theorem 1 depends on being able to verify that the components of $P_1(X)-P_2(Y)=0$ which admit an infinity of points of $E\times E$, have polynomial parametrizations. In the proof of Theorem 1, it is shown that E contains a set which in addition to satisfying the requirements of E also is contained in a subring A of K finitely generated over the integers. But then one can apply M. Fried's characterization ([2], Th. 3 and its corollary) of genus 0 curves with separated variables having infinitely many A-valued points. (The corollary holds for a ring like A

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

(iii) $K = \boldsymbol{Q}$ the field of rational numbers and the greatest common divisor of the degrees of P_1 and P_2 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 $\boldsymbol{Q}$ 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 $a_{i-1}^2 = a_i^3$, 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 $m \neq n$ 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 $S_1(X)-T_1(Y)=0$ where*

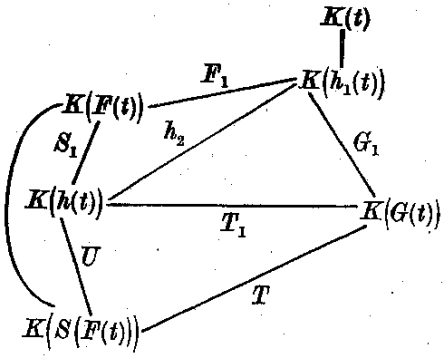
(i) *S_1 and T_1 are polynomials over K of degree m/r and n/r respectively.*

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

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

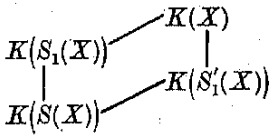
Further, if V_2 is any other absolutely irreducible component of $S(X)-T(Y)=0$ with a polynomial parametrization, then V_2 is of the form $S_1(X)-\zeta T_1(Y)+b=0$ where ζ is an r-th root of unity, $b \in K$, and $U(\zeta X-b) = U(X)$.

Proof. Let $X=F(t)$, $Y=G(t)$ be a polynomial parametrization of V_1. Since V_1 is a component of $S(X)-T(Y)=0$, we have $S(F(t)) = T(G(t))$. By a result of Fried ([4], pp. 168–169) and Ritt ([14]), there are two polynomials h, $U \in K[X]$ with degree $U=r$, $K(F(t)) \cap K(G(t)) = K(h(T))$, and $S(F(t)) = U(h(t)) = T(G(t))$. It follows that there are polynomials S_1 and T_1 over K with $h(t) = S_1(F(t)) = T_1(G(t))$. By the same theorem, there are polynomials h_1 and h_2 with degree $h_1 = (\deg F, \deg G)$, $h(t) = h_2(h_1(t))$, and $K(F(t), G(t)) = K(h_1(t))$. Thus, there are also polynomials F_1, G_1 over K with $F(t) = F_1(h_1(t))$ and $G(t) = G_1(h_1(t))$.



The degrees of S_1, T_1, F_1, and 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 $h(t) = S_1(F_1(h_1(t))) = T_1(G_1(h_1(t)))$. Finally $S_1(X) - T_1(Y)$ is absolutely irreducible by Ehrenfeucht's Theorem ([1]), and so U, F_1, G_1, S_1, and 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' and T_1'. Now $S(X) = U(S_1(X))$



$= U'(S_1'(X))$ and, since U and U' are of the same degree, there is a linear polynomial l_1 over K with $U_1 = U_1' \circ l_1^{-1}$ 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 $S_1(X) = l_1 \circ l_2 \circ T_1(Y)$. Further $T(X) = U(T_1(X)) = U(l_1(l_2(T_1(X))))$ implies $U(X) = U(l_1(l_2(X)))$ and so the leading coefficient of $l_1(l_2(X))$ is an rth 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_1 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 $K(F_1(t)) \cap K(G_1(t)) \supseteq K(S_1(F_1(t)))$ and the degrees of F_1 and G_1 are relatively prime, it follows by a result of Fried ([4], p. 169) that $K(F_1(t), G_1(t)) = K(t)$. 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 $K[t]$. Suppose $\mathscr{P}$ 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 $\mathscr{P}'$ is the prime lying over it in $K[t]$. Then $K[F_1(t), G_1(t)]_{\mathscr{P}} = K[t]_{\mathscr{P}'}$. Now P is parametrized by the value of t in

$$K[t]/\mathscr{P}'K[t] \cong K[F_1(t), G_1(t)]_{\mathscr{P}}/\mathscr{P}K[F_1(t), G_1(t)]_{\mathscr{P}} = K$$

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 Tchebychef polynomials. Recall that the nth Tchebychef polynomial is the unique polynomial with integer coefficients such that $T_n(\cos\theta) = \cos n\theta$ for all θ. The roots of T_n are therefore $\cos\frac{2k+1}{2n}\pi$ for $k = 0, 1, \ldots, n-1$ and differentiating shows the roots of $T_n'(X) = 0$ to be $\cos\frac{k\pi}{n}$ for $k = 1, 2, \ldots, n-1$. 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 $-n2^{n-3}$, and
(iv) constant term equal to 0 for n odd and $(-1)^{n/2}$ for n even.

LEMMA A. *If $n \geqslant 2$ and*

$$aT_n(bX+c)+d = T_n(X),$$

then $c=0$ and $ab^n=1$. If further $n \geqslant 3$, 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 $n \geqslant 3$, comparing the coefficients of X^{n-2} gives $ab^{n-2} = 1$ 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 $T_2(0) = -1$ and so $d = a-1$. If n is even and $\geqslant 3$, then $ab^n = 1$ implies $a=1$ and so $d=0$ as desired.

LEMMA B. *Suppose $n \geqslant 2$ and $m \neq 1$. If g is a polynomial with $g(0) \neq 0$ and l_1, l_2 are linear such that*

$$T_n(X) = l_1 \circ X^r g(X)^m \circ l_2,$$

then

(i) $g(l_2(X))^m = \text{constant} \Rightarrow n=2,\ l_1(0) = -1,\ l_2(0) = 0,$
(ii) $g(l_2(X))^m \neq \text{constant} \Rightarrow l_1(0) = \pm 1,\ m = 2.$

Proof. If $l_1(X) = aX+b$ and $l_2(X) = cX+d$, we have

$$T_n(X) = a(cX+d)^r g(cX+d)^m + b.$$

Differentiating gives:

$$T_n'(X) = rac(cX+d)^{r-1}k$$

if $g(cX+d)^m = k$ is a constant,

$$T_n'(X) = acmg(cX+d)^{m-1}g'(cX+d)$$

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

$$T_n'(X) = ac(cX+d)^{r-1}g(cX+d)^{m-1}\{rg(cX+d)+m(cX+d)g'(cX+d)\}$$

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 $m \leqslant 2$ and $r \leqslant 2$. The roots of $g(cX+d)$ are among the $\cos\frac{k\pi}{n}$ for $k = 1, 2, \ldots, n-1$. But $T_n\left(\cos\frac{k\pi}{n}\right) = \cos k\pi = (-1)^k$. Hence $b = \pm 1$ 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 = degree G, degree T = degree F, and $S \circ F = T \circ G$. There are two obvious kinds of permuting, viz.

$$X^m \circ X^s h(X^m) = X^s h(X)^m \circ X^m$$

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 ove a field of characteristic zero such that*

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

and

$$m = \text{degree } S = \text{degree } G \leqslant \text{degree } F = \text{degree } T = n.$$

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

(i) $l_1^{-1} \circ S \circ l_3 = X^m = l_4^{-1} \circ G \circ l_2$, $l_3^{-1} \circ F \circ l_2 = X^s h(X^m)$, *and* $l_1^{-1} \circ T \circ l = X^s h(X)^m$ *where h is a polynomial over the algebraic closure $\bar{K}$ of K o*

(ii) $l_1^{-1} \circ S \circ l_3 = T_m = l_4^{-1} \circ G \circ l_2$ *and* $l_1^{-1} \circ T \circ l_4 = T_n = l_3^{-1} \circ F \circ l_2$.

COROLLARY 1. *If $0 < m < n$ are relatively prime, then the only curve of the form $S(X) - T(Y) = 0$ where degree $S = m$, 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*

$$l_1 \circ X^m \circ l_2(X) = l_1 \circ Y^s h(Y)^m \circ l_3(Y)$$

or

$$l_1 \circ T_m \circ l_2(X) = l_1 \circ T_n \circ l_3(Y),$$

where l_1, l_2, and l_3 are linear.

Proof. This follows from Ritt's Theorem, or more simply from Fried ([2], Theorem 3).

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

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

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

$$T_2(dX) = T_n \circ l_3(Y).$$

(iii) $T_m(X) = l_1 \circ T_n \circ l_3(Y)$. *If $m \geqslant 3$, then* $l_1(X) = \pm X$. *If $m = 2$, then $l_1(X)$ is of the form $\pm cX + c - 1$. So the curve is*

$$T_2(\sqrt{c}X) = \pm T_n(Y).$$

Proof. (i) If $l_3 \circ X^s = X^s \circ l_4$ where $s \geqslant 2$ and the l_i are linear, then $l_4(0) = l_3(0) = 0$. So this case follows from Lemma B and the last corollary.

(ii) By the last corollary and Lemma B, $m \geqslant 3$ is impossible. Suppose $m = 2$. If the curve is of type (i) in Corollary 1, then there are linear polynomials $l_3(X) = cX + f$, $l_4(X)$, and $l_5(X)$ such that $l_3(X^2) = (l_4(X))^2$ and $l_3 \circ l_1 \circ T_n \circ l_2 = Y^r g(Y)^2 \circ l_5$ for some polynomial g. The first equation implies $f = 0$. If $l_1(X) = aX + b$, then by the second equation and Lemma B, $X = l_3 \circ l_1 \circ (cX \pm 1)$ for some constant c. So $X = eacX \pm ea + be$ or $a = \mp b$. Hence l_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 $cX + d$ such that $(\pm aX + b)^{-1} \circ X^2 = (2X^2 - 1) \circ (cX + d)$ or $X^2 = \pm 2a(cX + d)^2 \mp a + b$. Hence $d = 0$ 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 $d = (\mp 2a)^{-1/2}$ and $l_3(Y) = \mp l_2(Y)$.

(iii) If $m \geqslant 3$, then Lemma B says that this curve must come from permuted Tchebychef polynomials. But then the result follows from Lemma A. If $m = 2$, then (ii) says that we have a curve arising from permuted Tchebychef polynomials. 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 $S_i(X) - V_i(Y) = 0$ 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 $S_j(a_i) = V_j(a_{i+1})$ and such that no element of K occurs more than a finite number of times in the sequence, then for some j, $S_j(X) - V_j(Y) = 0$ has an infinity of points of the form (a_i, a_{i+1}) and both S_j and V_j are of the form*

$$l_1 \circ X^k \circ l_2 \quad \text{or} \quad l_1 \circ T_k \circ l_2$$

where l_1 and l_2 are linear and T_k is a Tchebychef polynomial.

Proof. By discarding some of the curves $S_i(X) - V_i(Y) = 0$ 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 $S_j(X) - V_j(Y) = 0$ has a parametrization of the form $X = F_j(t)$ and $Y = G_j(t)$ where F_j and G_j are polynomials of degree n and m 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 β_i in K and a $j(i)$ such that

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

Now

$$F_{j(i)}(\beta_i) = a_i = G_{j(i-1)}(\beta_{i-1}).$$

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

Taking a suitable set of curves $F_i(X) - G_j(Y) = 0$ and a final segment of the β_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 (β_i, β_{i-1}) and so the curves have polynomial parametrizations by Fried ([2], Th. 3 and its Corollary).) After repeating the process k times, one sees that some S_i and some V_j permute with polynomials of degree n^k and m^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 Tchebychef polynomials. If $m > n$, then $S_i(X) - V_i(Y) = 0$ satisfies the conclusion of the lemma by Corollary 1. Similarly, if $m < n$, then $S_j(X) - V_j(Y)$ 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 $F_j(X) - G_k(Y) = 0$ arising from the parametrizations $X = F_k(t)$ and $Y = G_k(t)$ 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_0 is a finitely generated field extension of the rationals $\boldsymbol{Q}$ and if S and T are non-constant polynomials of different degrees, then there are at most a finite number of finite sets $F \subseteq K_0$ with $S(F) = T(F)$.*

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 is a union of finite sets X_i such that $F(X_i) = G(X_i)$". In the proof of that lemma, omit the condition (II) on the point a and replace the $G_{i,j,\sigma,\tau}$ with

$$G_{i,j,\sigma,\tau} = N_{K/k(t)}[X_i^{(\sigma)} X_j^{(\tau)} - X_i^{(\tau)} X_j^{(\sigma)}].$$

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: $S(X_1) = T(X_2)$, $S(X_2) = T(X_3), \ldots, S(X_{n-1}) = T(X_n)$, $S(X_n) = T(X_1)$. 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 $\boldsymbol{C}^n$ are those of dimension zero.*

Proof. It suffices to consider the case where V is irreducible of dimension, say $r > 0$. Let $\boldsymbol{C}[V] = \boldsymbol{C}[x_1, x_2, \ldots, x_n]$ 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 $\boldsymbol{C}[y_1, y_2, \ldots, y_r]$ is a polynomial ring in r variables, and $\boldsymbol{C}[V]$ is integral over $\boldsymbol{C}[y_1, y_2, \ldots, y_r]$. The points of V are the finite specializations in $\boldsymbol{C}^n$ of $(x_1, x_2, \ldots, x_n)$ over $\boldsymbol{C}$. Suppose the set of these is bounded. Then the set of finite specializations in $\boldsymbol{C}^{n+r}$ of $(x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_r)$ over $\boldsymbol{C}$ is also bounded, say by $M > 0$. But $(y_1, y_2, \ldots, y_r) \to (M+1, 0, \ldots, 0)$ 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 $P_j = (x_{1j}, x_{2j}, \ldots, x_{nj})$ in V_n with $|x_{1j}| \to \infty$ as $j \to \infty$. Now since $S(x_{1j}) = T(x_{2j})$,

$$|x_{2j}| \to \infty \quad \text{as} \quad j \to \infty.$$

Similarly $|x_{ij}| \to \infty$ as $j \to \infty$ for $i = 3, 4, \ldots, n$. By deleting a finite number of the P_j, we may suppose that $x_{1j} x_{2j} \ldots x_{nj} \neq 0$ for all j. Multiplying the equations for V_n together and dividing by $(X_1 X_2 \ldots X_n)^t$ gives

$$\prod_{i=1}^{n} \frac{x_{ij}^s + F(x_{ij})}{x_{ij}^t} = \prod_{i=1}^{n} \left(a + \frac{G(x_{ij})}{x_{ij}^t}\right).$$

The right hand member approaches $a^n \neq 0$ as $j \to \infty$. 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 K_0 in K of the field generated over $\boldsymbol{Q}$ by the coefficients of S and T.

The sequences $\{a_i \mid i \geqslant 0\} \subseteq E$ 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 $a_0 \in E$ there is a finite sequence $a_0, a_1, \ldots, a_n$ where $a_i \in E$, $S(a_{i-1}) = T(a_i)$ for $0 < i \leqslant n$, $a_n = a_r$ for some $r < n$, and $a_1, \ldots, a_{n-1}$ are distinct. Clearly $F(a_0) = \{a_{r+1}, a_{r+2}, \ldots, a_n\}$ is a finite set satisfying $S(F(a_0)) = T(F(a_0))$. Since there are but a finite number of such sets, some $F_0 = F(a_0)$ for an infinity of $a_0 \in E$. 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 $\{a_0, \ldots, a_n\}$ for which $F_0 = F(a_0)$, a new sequence of distinct elements $\beta_0, \beta_1, \ldots$ such that $S(\beta_{i+1}) = T(\beta_i)$ for all $i \geqslant 0$.

If, however, at least one of the sequences $\{a_i \mid i \geqslant 0\}$ had infinite cardinality, then by deleting segments of the form $a_k, a_{k+1}, \ldots, a_r$ where $a_k = a_{r+1}$, 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 $i \geqslant 0$. From

now on we assume $E = \{a_i\}$. E is contained in a subring of K finitely generated over $\boldsymbol{Z}$ ([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 $r = (m, n)$, $s = m/r$, and $t = n/r$. By Theorem 2, the components of $S(X)-T(Y) = 0$ which admit polynomial parametrizations are of the form $S_i(X)-V_i(Y) = 0$ where S_i and V_i 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_i, a_{i+1}) lies on at least one of the $S_j(X)-V_j(Y) = 0$. The Reduction Lemma now shows that at least one of these components, say $S_1(X) = V_1(Y)$ has S_1 and V_1 either a power or a Tchebychef polynomial (up to linear change of variables). Now considering each of several possible cases, it will be shown that $S(X)-T(Y) = 0$ must have a very special form.

Case 1. Suppose $S_1(X)-V_1(Y) = 0$ is of the form

$$X^s \circ l_1(X) = l_2 \circ Y^t \circ l_3(Y)$$

where the l_i are linear. By part (i) of Corollary 2, this can be rewritten as $X^s \circ l_1(X) = Y^t \circ l_4(Y)$ with l_4 linear. Further, by replacing the a_i with $l_1(a_i)$, we are reduced to $X^s = Y^t \circ l_5(Y)$ where $l_5 = l_4 \circ l_1^{-1}$. By Corollary 2 and Theorem 2, the other components of $S(X)-T(Y) = 0$ containing an infinity of points of the form (a_i, a_{i+1}) are all of the form $X^s = \zeta^t Y^t \circ l_5(Y)$ where ζ is an nth root of unity. These are parametrized by $X = Z^t$, $Y = l_5^{-1} \circ \zeta^{-1} Z^s$. So, by Remark 1 after the Reduction Lemma, at least one of the curves $X^t = l_5^{-1} \circ \zeta^{-1} Y^s$ has an infinity of points over A. By Corollary 2, $l_5^{-1}(0) = l_5(0) = 0$. Let $l_5(X) = cX$ and choose a d with $d^{m-n} = c^{tr}$. Except for components with only a finite number of points of the form (a_i, a_{i+1}), $S(X)-T(Y) = 0$ is of the form $X^m = c^{rt} Y^n$. By replacing the a_i with da_i, we are reduced to the case of $X^m - Y^n = 0$.

Case 2. Suppose $S_1(X)-V_1(Y) = 0$ is of the form

$$T_s \circ l_1(X) = T_t \circ l_2(Y)$$

and that $s, t \geqslant 3$. As in case 1, we can reduce to the case where $l_1(X) = X$ by replacing the a_i with the $l_1(a_i)$. 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_{i+1}) is $T_s(X) = -T_t(l_2(Y))$. If, say t, is odd, these curves are parametrized by $X = T_t(X)$ and $Y = \pm l_2^{-1} \circ T_s(Z)$. So by Remark 1, at least one of the $T_t(X) = \pm l_2^{-1}(T_s(Y))$ has an infinity of points over A. By Corollary 2, $l_2^{-1} = l_2 = \pm X$. Therefore, with the exception of components containing at most a finite number of points of the form (a_i, a_{i+1}), $S(X)-T(Y) = 0$ is $T_s(X) = \pm T_t(Y)$.

Case 3. Suppose $S_1(X) = V_1(Y)$ is of the form

$$T_2 \circ l_1(X) = T_t \circ l_2(Y)$$

where $t \geqslant 3$ is odd. As before, we may suppose $l_1(X) = X$. Remark 1 shows that for some linear l_3, both a $T_2(X) = T_t(l_3(Y))$ which is a component of $S(X)-T(Y) = 0$ and $l_3^{-1}(T_2(X)) = T_t(Y)$ have an infinite number of points defined over A. By Corollary 2, this last curve looks like $T_2(cX) = \pm T_t(Y)$. This is parametrized by $X = c^{-1} T_t(Z)$ and $Y = T_2(Z)$. Again we may assume $\pm T_2(X) = c^{-1} T_t(Y)$ has an infinity of points defined over A. By Corollary 2, $c^{-1} = \pm 1$. Hence $S(X)-T(Y) = 0$ is $T_2(X) = \pm T_t(Y)$ up to components with only a finite number of points of the form (a_i, a_{i+1}).

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 $S_1, T_1, T_2, \ldots, T_r$ be polynomials such that the set of curves $S_1(X)-T_i(Y) = 0$ is the same as the set of curves $X = T_i(t)$, $Y = S_1(t)$. Suppose every component of the curve $S(X)-T(Y) = 0$ which has an infinity of points of the form (a_i, a_{i+1}) is among the curves $S_1(X)-T_i(Y) = 0$. If degree $S_1 > 1$, then E is a finite set.*

Proof. The set E can contain at most a finite number of points (a_i, a_{i-1}) which are not contained in the $S_1(X)-T_i(Y) = 0$. Choose a k_1 such that for $i > k_1$, (a_i, a_{i-1}) is not one of these bad points and renumber the a_i for $i \geqslant k_1$ by $a_{0j} = a_{j+k_1}$. By replacing A with the integral closure of an appropriate finite extension, we can assume via the proposition that, for $i > 0$, the $(a_{0i}, a_{0,i-1})$ are of the form $a_{0i} = T_{j(i)}(a_{1i})$, $a_{0,i-1} = S_1(a_{1i})$ where the $a_{1i} \in A$. Without making further extension of A, we can find $a_{2i} \in A$ with $a_{1i} = T_{k(i)}(a_{2i})$, $a_{1,i-1} = S_1(a_{2i})$. By induction, there are $a_{ki} \in A$ for $i > k$ with $a_{k,i-1} = S_1(a_{k+1,i})$. The same equation can be used to inductively define the a_{ki} for k negative. The set F of all the a_{ki} satisfies $S_1(F) = F$. By [12] or the one dimensional case of the theorem of D. J. Lewis [9], F and *a fortiori* E 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 $P_1(a_i) = P_2(a_{i-1})$ for all i, and the second part was concerned with the number of finite sets F which satisfy $P_1(F) = P_2(F)$. 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 $K = \boldsymbol{Q}(\{\zeta_p\})$ where ζ_p is a primitive pth 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 $\boldsymbol{Q}(\zeta_{p_1}, \zeta_{p_2}, \ldots, \zeta_{p_k})$ contained in K of degree $\leqslant n$. 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_i and a_1 are in $\boldsymbol{Q}(\zeta_{p_1}, \ldots, \zeta_{p_k})$, we are assured that the sets of the form $\{a_i\}$ are contained in $\boldsymbol{Q}(\zeta_{p_1}, \ldots, \zeta_{p_k})$ and are hence finite. Nevertheless, if $P_1(X) = X^m$ and $P_2(Y) = Y^m$, then taking p to be any prime relatively prime to m and n, we have $P_1(E_p) = E_p = P_2(E)$ where $E_p = \{\zeta_p^k \mid k = 1, 2, \ldots, p\}$. So there are infinitely many sets of the second type. The same phenomenon occurs for P_1, P_2 of the same degree when $K = \boldsymbol{Q}$ ([6]).

References

[1] A. Ehrenfeucht, *Kryterium absolutnej nierozkładalności wielomianów*, Prace Mat. 2 (1958), pp. 167–169.

[2] M. Fried, *On a theorem of Ritt and related diophantine problems*, to appear.

[3] M. D. Fried and R. E. MacRae, *On curves with separated variables*, Math. Ann. 180 (1969), pp. 220–226.

[4] — — *On the invariance of chains of fields*, Illinois J. Math. 13 (1969), pp. 165–171. The quoted results appeared earlier in Fried's thesis, *Value Sets of Polynomials*, Ann Arbor 1967.

[5] K. K. Kubota, *Note on a conjecture of W. Narkiewicz*, to appear in J. of Number Theory.

[6] — *Factors of polynomials under composition*, to appear in J. of Number Theory.

[7] S. Lang, *Diophantine Geometry*, New York 1962.

[8] — *Introduction to Algebraic Geometry*, New York 1958.

[9] D. J. Lewis, *Invariant sets of morphisms on projective and affine number spaces*, J. Algebra 20 (1972), pp. 419–434.

[10] M. Nagata, *Local Rings*, New York 1962.

[11] W. Narkiewicz, *On polynomial transformations*, Acta Arith. 7 (1962), pp. 241–249.

[12] — *On polynomial transformations II*, Acta Arith. 8 (1962), pp. 11–19.

[13] — *Problem 416*, Colloq. Math. 10 (1963), p. 187.

[14] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), pp. 51–66.

UNIVERSITY OF KENTUCKY
Lexington, Kentucky

Received on 26. 4. 1972 (274)

ACTA ARITHMETICA
XXIII (1973)

On the number of Abelian groups of a given order

by

B. R. Srinivasan (Bombay, India)

1. Introduction. Let $A(x)$ denote the number of essentially distinct Abelian groups of order not exceeding x. Then

$$A(x) = A_1 x + A_2 x^{1/2} + A_3 x^{1/3} + \Delta(x)$$

where

$$A_r = \prod_{\substack{\nu=1 \\ \nu \neq r}}^{\infty} \zeta\left(\frac{\nu}{r}\right) \qquad (r = 1, 2, 3)$$

and

$$\Delta(x) \ll x^{\theta} \log^{\theta'} x.$$

Results of the above type with the pairs

$$(\theta, \theta') = (\tfrac{1}{2}, 0),\ (\tfrac{1}{3}, 2),\ (\tfrac{3}{10}, \tfrac{9}{10}),\ (\tfrac{20}{69}, \tfrac{21}{23}),\ (\tfrac{2}{7}, \tfrac{6}{7}),\ (\tfrac{34}{123}, 0),\ (\tfrac{7}{27}, 2)$$

were proved by P. Erdös and G. Szekeres [1], D. G. Kendall and R. A. Rankin [2], H. E. Richert [3], W. Schwarz [4], and P. G. Schmidt [5], [6]. As an application of the theory of two dimensional exponent pairs I have developed elsewhere [9], I here show that

$$\Delta(x) \ll x^{105/407} \log^2 x. \tag{1}$$

Here the exponent $\frac{105}{407} = .257\ldots < \frac{7}{27} = .259\ldots$

Actually the method yields exponents smaller than $\frac{105}{407}$, but I shall avoid the computations that will be necessary to obtain the best possible exponent in this way.

2. Lemmas.

Lemma 1 (Lemma of partial summation). *Let $g(m, n)$ denote any numbers, real or complex, such that, if*

$$G(m, n) = \sum_{\substack{1 \leqslant \mu \leqslant m \\ 1 \leqslant \nu \leqslant n \\ (\mu, \nu) \in D}} g(\mu, \nu)$$