Table des matières du tome XI, fascicule 1

La revue est consacrée à toutes les branches de l'arithmétique et de la théorie des nombres, ainsi qu'aux fonctions ayant de l'importance dans ces domaines.

Prière d'adresser les textes dactylographiés à l'un des redacteurs de la revue ou bien à la Rédaction de

ACTA ARITHMETICA

Warszawa 1 (Pologne) ul. Śniadeckich 8.

La même adresse est valable pour toute correspondance concernant l'échange de Acta Arithmetica.

Les volumes IV et suivants de ACTA ARITHMETICA sont à obtenir chez

Ars Polona, Warszawa 5 (Pologne), Krakowskie Przedmieście 7.

Prix de ce fascicule 3.00 $.

Les volumes I-III (reédits) sont à obtenir chez

Johnson Reprint Corp., 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XI (1965)

On the reducibility of polynomials and in particular of trinomials

by

A. Schinzel (Warszawa)

§ 1. In the course of this paper *reducibility* means reducibility over the rational field Q unless stated to the contrary. Constants are considered neither reducible nor irreducible. A factorization of a polynomial into a product of a constant and of coprime powers of irreducible polynomials is called its *standard form*. For a given polynomial $f(x)$, $Kf(x)$ denotes the factor of $f(x)$ of the greatest possible degree, whose no root is 0 or a root of unity and whose leading coefficient is equal to the leading coefficient of $f(x)$. Clearly

$$Kf(x) = \frac{f(x)}{\left(f(x), x^d \prod_{\varphi(\delta)\leqslant d} (x^\delta - 1)^d\right)},$$

where d is the degree of $f(x)$. The paper has emerged from the efforts to solve the following problem formulated in [4]:

Do there exist integers $a, b \neq 0$ such that for infinitely many rational r one can find integers m, n satisfying

(i) $m/n = r$,

(ii) $K(x^n + ax^m + b)$ *is reducible*?

The negative answer to this problem follows at once from Theorem 3 below; however, more general results are obtained. To state them I use the following notation:

If $\Phi(x_1, \ldots, x_k)$ is a rational function of the form $\sum_{i=0}^{I} a_i \prod_{j=1}^{k} x_j^{a_{i,j}}$, where $a_i \neq 0$, $a_{i,j}$ are integers and the systems $\langle a_{i,1}, \ldots, a_{i,k}\rangle$ are all different for $i \leqslant I$, then

$$J\Phi(x_1, \ldots, x_k) = \Phi(x_1, \ldots, x_k) \prod_{j=1}^{k} x_j^{-\min_i a_{i,j}}.$$

It is clear that $J\Phi(x_1, \ldots, x_k)$ is a polynomial and that the operation J as well as K is distributive with respect to multiplication. I prove

THEOREM 1. *For every irreducible polynomial $F(x)$ not dividing $x^\delta - x$ $(\delta > 1)$ and every positive integer n there exists an integer v satisfying the following conditions*:

(i) $0 < v \leqslant C(F)$;

(ii) $n = vu$, *u integer*;

(iii) *if* $F(x^v) = F_1(x)F_2(x)\dots F_r(x)$ *is a standard form of* $F(x^v)$, *then*

$$F(x^n) = F_1(x^u)F_2(x^u)\dots F_r(x^u)$$

is a standard form of $F(x^n)$.

$C(F)$ is an effectively computable constant independent of n.

THEOREM 2. *For every irreducible polynomial $F(y, z)$ satisfying $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$ and for every pair of positive integers n, m there exists an integral non-singular matrix*

$$\begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the following conditions:

(i) $0 \leqslant \nu_i \leqslant C_1(F)$, $0 \leqslant \mu_i \leqslant C_1(F)$ $(i = 1, 2)$;

(ii) $n = \nu_1 u + \nu_2 v$, $m = \mu_1 u + \mu_2 v$, *u, v integers* $\geqslant 0$;

(iii) *if*

$$JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2}) = \operatorname{const} F_1(x^u, x^v)^{e_1}F_2(x^u, x^v)^{e_2}\dots F_r(x^u, x^v)^{e_r}$$

is a standard form of $JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2})$, *then either*

$$KF(x^n, x^m) = \operatorname{const} KF_1(x^u, x^v)^{e_1}KF_2(x^u, x^v)^{e_2}\dots KF_r(x^u, x^v)^{e_r}$$

is a standard form of $KF(x^n, x^m)$ *or*

$$\max\{n, m\} \leqslant C_0(F)(n, m).$$

$C_0(F)$ and $C_1(F)$ are effectively computable constants independent of n, m.

For every polynomial $F(x)$ to which Theorem 1 applies the number of irreducible factors of $F(x^n)$ remains bounded as n tends to infinity. On the other hand, if $F(x)$ is any cyclotomic polynomial $X_k(x)$ and $(n, k) = 1$, then

$$F(x^n) = X_k(x^n) = \prod_{d|n} X_{kd}(x);$$

thus the number of irreducible factors of $F(x^n)$ can be arbitrarily large. Therefore, the condition in Theorem 1 that $F(x)$ does not divide $x^\delta - x$ is necessary. On the other hand, it seems that the condition in Theorem 2: $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$, is too strong and could be replaced by the

condition that $F(y, z)$ does not divide $yzJ(y^{\delta_1}z^{\delta_2} - 1)$ for any integers δ_1, δ_2 not both zero. Moreover, the following conjecture seems to me plausible.

CONJECTURE. *Let $F(y_1, \dots, y_k)$ be an irreducible polynomial which does not divide $y_1\dots y_k J(y_1^{\delta_1}y_2^{\delta_2}\dots y_k^{\delta_k} - 1)$ for any integers $\delta_1, \dots, \delta_k$ not all zero.*

For every system of k positive integers $n_1, \dots, n_k$ there exists an integral non-singular matrix $[\nu_{i,j}]$ $(1 \leqslant i \leqslant k, 1 \leqslant j \leqslant k)$ satisfying the following conditions:

(i) $0 \leqslant \nu_{i,j} \leqslant C_1(F)$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant k)$;

(ii) $n_i = \sum_{j=1}^{k} \nu_{i,j}u_j$ $(1 \leqslant i \leqslant k)$, *$u_j$ integers* $\geqslant 0$ $(1 \leqslant j \leqslant k)$;

(iii) *if*

$$JF\Big(\prod_{j=1}^{k} y_j^{\nu_{1,j}}, \prod_{j=1}^{k} y_j^{\nu_{2,j}}, \dots, \prod_{j=1}^{k} y_j^{\nu_{k,j}}\Big) = \operatorname{const} F_1(y_1, \dots, y_k)^{e_1}\dots F_r(y_1, \dots, y_k)^{e_r}$$

is a standard form of $JF\big(\prod_{j=1}^{k} y_j^{\nu_{1,j}}, \prod_{j=1}^{k} y_j^{\nu_{2,j}}, \dots, \prod_{j=1}^{k} y_j^{\nu_{k,j}}\big)$, *then either*

$$KF(x^{n_1}, \dots, x^{n_k}) = \operatorname{const} KF_1(x^{u_1}, \dots, x^{u_k})^{e_1}\dots KF_r(x^{u_1}, \dots, x^{u_k})^{e_r}$$

is a standard form of $KF(x^{n_1}, \dots, x^{n_k})$ *or*

$$a_1n_1 + \dots + a_kn_k = 0,$$

where a_i are integers not all zero and $|a_i| \leqslant C_0(F)$ $(1 \leqslant i \leqslant k)$.

$C_0(F)$ and $C_1(F)$ are constants independent of $n_1, \dots, n_k$.

The method of proof in Theorem 1 permits us to obtain an analogous result for reducibility in an arbitrary algebraic number field. The method of proof in Theorem 2 is valid only for totally real number fields and their quadratic extensions (in the latter case the condition $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$ should be replaced by $JF(y, z) \neq \pm\overline{JF(y^{-1}, z^{-1})}$). I do not know, however, any algebraic number field in which the Conjecture could be disproved.

The following theorem can easily be inferred from Theorems 1 and 2.

THEOREM 3. *For any given non-zero integers a, b, c there exist two effectively computable constants A (a, b, c) and B (a, b, c) such that if $n > m > 0$ and $K(ax^n + bx^m + c)$ is reducible, then*

(i) $n/(n, m) \leqslant A(a, b, c)$,

(ii) *there exists integers ν and μ such that $m/\mu = n/\nu$ is integral, $0 < \mu < \nu \leqslant B(a, b, c)$ and if*

$$K(ax^\nu + bx^\mu + c) = \operatorname{const} F_1^{e_1}(x)\dots F_r^{e_r}(x)$$

is a standard form of $K(ax^\nu+bx^\mu+c)$, *then*

$$K(ax^n+bx^m+c) = \text{const}\,F_1^{c_1}(x^{n/\nu})\dots F_r^{c_r}(x^{n/\nu})$$

is a standard form of $K(ax^n+bx^m+c)$.

In order to complete the investigation of trinomials I also prove

THEOREM 4. *If* a, b, c *are integers* $\neq 0$, $0<m<n$, $d=(m,n)$, $m=dm_1$, $n=dn_1$, ε, η *denote* ± 1, *then*

$$\frac{ax^n+bx^m+c}{K(ax^n+bx^m+c)}$$

$$= \begin{cases} x^{2d}+\varepsilon^{m_1}(\varepsilon^{n_1}\eta^{m_1})x^d+1, & \text{if } c=\varepsilon a=\eta b,\ n_1+m_1\equiv 0 \pmod 3,\ \varepsilon^{m_1}=\eta^{n_1}, \\ \left(x^d-(-\varepsilon)^{m_1}\varepsilon\eta\right)^2, & \text{if } c=\varepsilon a+\eta b,\ (-\varepsilon)^{m_1}=(-\eta)^{n_1},\ an\varepsilon+bm\eta=0, \\ x^d-(-\varepsilon)^{m_1}\varepsilon\eta, & \text{if } c=\varepsilon a+\eta b,\ (-\varepsilon)^{m_1}=(-\eta)^{n_1},\ an\varepsilon+bm\eta\neq 0, \\ 1 & \text{otherwise.} \end{cases}$$

Theorems 3 and 4 generalize the results of papers [1], [3] and [2], in which the case $|a|=|c|=1$ has been considered. The results of those papers could be expressed in the present language in the form $A(1,\pm 1,\pm 1)=0$, $A(1,\pm 2,\pm 1)=B(1,\pm 2,\pm 1)=7$, $A(1,\pm p,\pm 1)\leqslant 4^{p^2}$ (p prime >2), respectively. The ideas of papers [1] and [2] are fundamental for the proof of Theorem 2. The Conjecture formulated above would give a result similar to Theorem 3 but concerning $(k+1)$-nomials.

As a second application of Theorem 2 I prove

THEOREM 5. *Let* $f(x)\neq \pm 1$ *be a polynomial such that* $f(0)\neq 0$. *There exist two constants* $D_0(f)$ *and* $D_1(f)\neq 0$ *such that if* $n>D_0(f)$ *and* $(n, D_1(f))=1$, *then* $K(x^n+f(x))$ *is irreducible.*

It seems natural to ask whether the irreducibility of $K(x^n+f(x))$ cannot be replaced in Theorem 5 by the irreducibility of $x^n+f(x)$ provided $f(1)\neq -1$. The example

$$f_0(x)=\frac{1}{12}(3x^9+8x^8+6x^7+9x^6+8x^4+3x^3+6x+5)$$

shows that it is impossible. In fact, $f_0(1)\neq -1$ and $x^n+f_0(x)$ has for every n a factor in common with $x^{12}-1$. I do not know whether a similar phenomenon can occur for polynomials with integral coefficients.

§ 2. LEMMA 1. *Let* Ω *be an algebraic number field, and* α *an element of* Ω *which is not* 0 *or a root of unity.*

There exist only finitely many integers e *such that* $\alpha=w\beta^e$, *where* w *is a root of unity,* $\beta\in\Omega$. *The greatest of them,* $e(\alpha,\Omega)$, *satisfies the following relations*:

(1) $$e(\alpha,\Omega)\leqslant(\exp 2N^2)\log\left(NH(\alpha)\right),$$

where N *is the degree of* Ω *and* $H(\alpha)$ *is the height of the irreducible primitive polynomial of* α,

(2) $$e(\alpha^n,\Omega)=ne(\alpha,\Omega)\quad (n=1,2,\dots).$$

Proof. We note first that if $\gamma\in\Omega$ is an algebraic integer and $\gamma^{(i)}$ $(i=1,\dots,n)$ are all its conjugates, then

(3) $$\frac{1}{N}\max_{1\leqslant i\leqslant N}|\gamma^{(i)}|\leqslant H(\gamma)\leqslant(1+\max_{1\leqslant i\leqslant N}|\gamma^{(i)}|)^N.$$

This obvious inequality implies the following one:

(4) $$\max_{1\leqslant i\leqslant N}|\beta^{(i)}|>\exp\exp(-2N^2),$$

which holds for all integers $\beta\in\Omega$ which are not 0 or roots of unity. Indeed, assuming the contrary we would clearly have $N>1$ and for all $k\leqslant\exp 2N^2$

$$\max_{1\leqslant i\leqslant N}|(\beta^k)^{(i)}|\leqslant\exp 1.$$

Hence, by (3) applied to $\gamma=\beta^k$,

$$H(\beta^k)\leqslant(1+\exp 1)^N\quad(1\leqslant k\leqslant\exp 2N^2).$$

Now there are no more integers of degree $\leqslant N$ and height $\leqslant H$ than $N(2H+1)^N$; thus there are no more integers of degree $\leqslant N$ and height $\leqslant(1+\exp 1)^N$ than

$$N\left(2(1+\exp 1)^N+1\right)^N<3^N(1+\exp 1)^{N^2}<\exp 2N^2\quad(N>1).$$

It follows that among the numbers β^k $(1\leqslant k\leqslant\exp 2N^2)$ at least two are equal, whence β is a root of unity. The contradiction obtained proves (4).

Now we show that the equality

(5) $$\alpha=w\beta^e,$$

where w is a root of unity, $\beta\in\Omega$, $e\geqslant 1$, implies

(6) $$e\leqslant(\exp 2N^2)\log\left(NH(\alpha)\right).$$

This will prove the existence of $e(\alpha,\Omega)$ and inequality (1).

Let α be a zero of a primitive irreducible polynomial

$$a_0x^m+\dots+a_m,$$

where $m\mid N$, a_i rational integers, $a_0>0$, $H(\alpha)=\max_{0\leqslant i\leqslant m}|a_i|$.

If $a_0 = 1$, α is an integer, and by (5), β is also an integer which is neither 0 nor a root of unity. It follows from (5) that

$$\log(\max_{1\leqslant i\leqslant N}|\alpha^{(i)}|) = e\log(\max_{1\leqslant i\leqslant N}|\beta^{(i)}|),$$

and hence by (3) applied to $\gamma = \alpha$ and by (4)

$$\log\big(NH(\alpha)\big) \geqslant e\exp(-2N^2),$$

which gives (6).

If $a_0 > 1$, $a_0\alpha$ is an integer but α is not. Therefore, there exists a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^\lambda \parallel a_0$, $\mathfrak{p}^\mu \parallel a_0\alpha$ and $\mu < \lambda$. Let $\mathfrak{p}^\nu \parallel a_0\beta$. If follows from (5) that $(\lambda-\mu) = (\lambda-\nu)e$, and since $\lambda-\mu > 0$ we get $\lambda-\nu > 0$ and $e \leqslant \lambda-\mu \leqslant \lambda$. On the other hand, $(\operatorname{norm}\mathfrak{p})^\lambda \mid a_0^N$, hence

$$2^\lambda \leqslant a_0^N \leqslant H(\alpha)^N.$$

This gives

$$e \leqslant \lambda \leqslant \frac{N}{\log 2}\log H(\alpha) < (\exp 2N^2)\log\big(NH(\alpha)\big),$$

i. e. again (6).

In order to prove (2) we put $e(\alpha, \Omega) = e$, $e(\alpha^n, \Omega) = f$, $(n, f) = d$ and assume

$$\alpha = w_1\beta^e, \qquad \alpha^n = w_2\gamma^f, \tag{7}$$

where w_1, w_2 are roots of unity, $\beta, \gamma \in \Omega$. Clearly $\alpha^n = w_1^n\beta^{ne}$, whence $f \geqslant ne$.

On the other hand, there exist integers p, q such that $pn - qf = d$ and it follows from (7) that

$$\big(\alpha(\alpha^q\gamma^{-p})^{f/d}\big)^d = \alpha^{d+qf}\gamma^{-pf} = \alpha^{pn}(w_2\alpha^{-n})^p = w_2^p;$$

thus $\alpha(\alpha^q\gamma^{-p})^{f/d}$ is a root of unity, say w_3. We get

$$\alpha = w_3(\alpha^{-q}\gamma^p)^{f/d}$$

and, by the definition of e, $e \geqslant f/d \geqslant f/n \geqslant e$. This gives $f = ne$ and completes the proof.

LEMMA 2. *Let Ω be an algebraic number field and α an element of Ω which is not 0 or a root of unity. For every positive integer n we put*

$$\nu = \nu(\alpha, \Omega, n) = \big(n, 2^{e(\alpha,\Omega)-1}e(\alpha, \Omega)!\big).$$

If $g(x)$ is a monic polynomial irreducible over Ω and $g(x) \mid x^n - \alpha$, then $g(x) = G(x^{n/\nu})$, where $G(x)$ is a polynomial over Ω.

Proof. We proceed by induction with respect to $e(\alpha, \Omega)$. If $e(\alpha, \Omega) = 1$, then neither $\alpha = \beta^p$, $p > 1$ nor $\alpha = -4\beta^4$, $\beta \in \Omega$; thus, in view of a theorem of Capelli (for the proof and references see [5], p. 288-294),

$x^n - \alpha$ is irreducible in Ω and $g(x) = x^n - \alpha$. The lemma holds with $G(x) = x - \alpha$. Assume that the lemma is true for all Ω' and α' with $e(\alpha', \Omega') < m$ $(m > 1)$ and let $e(\alpha, \Omega) = m$, $g(x) \mid x^n - \alpha$.

If $x^n - \alpha$ is irreducible, then the lemma is trivially true with $G(x) = x^n - \alpha$. If it is reducible, then by the theorem of Capelli

(A) $\alpha = \beta^p$, where $p \mid n$, p prime > 1, $\beta \in \Omega$,

or

(B) $\alpha = -4\beta^4$, where $4 \mid n$, $\beta \in \Omega$.

We consider these cases successively, using the following notation: ζ_q is a primitive qth root of unity, $\Omega_q = \Omega(\zeta_q)$, d_q is the degree of Ω_q over Ω, $N_{\Omega_q/\Omega}$ is the norm of elements of Ω_q or polynomials over Ω_q relative to Ω.

(A) We have here

$$g(x) \mid x^n - \beta^p = (x^{n/p} - \beta)\prod_{r=1}^{p-1}(x^{n/p} - \zeta_p^r\beta). \tag{8}$$

If $g(x) \mid x^{n/p} - \beta$ our inductive assumption applies directly, since by (A) and Lemma 1

$$m = e(\alpha, \Omega) = pe(\beta, \Omega) > e(\beta, \Omega). \tag{9}$$

Putting $\nu_0 = \nu(\beta, \Omega, n/p)$ we have

$$\nu_0 \mid \big(n/p, 2^{m-2}(m-1)!\big), \qquad g(x) = G_0(x^{n/p\nu_0}),$$

$G_0(x) \in \Omega[x]$ and it is sufficient to take $G(x) = G_0(x^{\nu/p\nu_0})$.

If $g(x) \nmid x^{n/p} - \beta$, let $h(x)$ be a monic factor of $g(x)$ irreducible over Ω_p. By (8)

$$h(x) \mid g(x) \mid \prod_{r=1}^{p-1}(x^{n/p} - \zeta_p^r\beta);$$

thus for some positive $r < p$

$$h(x) \mid x^{n/p} - \zeta_p^r\beta. \tag{10}$$

Let $h^{(1)}(x) = h(x), \ldots, h^{(d_p)}(x)$ be all the conjugates of $h(x)$ relative to Ω. It follows from (10) that

$$\big(h^{(i)}(x), h^{(j)}(x)\big) \mid \beta(\zeta_p^{(i)r} - \zeta_p^{(j)r}) \qquad (1 \leqslant i \leqslant j \leqslant d_p);$$

thus $h^{(i)}(x)$ $(i = 1, 2, \ldots, d_p)$ are relatively prime in pairs.

Since $h^{(i)}(x) \mid g(x)$, it follows that

$$g(x) = N_{\Omega_p/\Omega}\big(h(x)\big). \tag{11}$$

On the other hand, we have $e(\zeta_p^r\beta, \Omega_p) = e_1 < m$. Indeed, if

$$\zeta_p^r\beta = w\gamma^{e_1}, \quad w \text{ a root of unity}, \ \gamma \in \Omega_p,$$

then

$$\alpha = \beta^p = w^p\gamma^{pe_1} \quad \text{and} \quad \alpha^{d_p} = N_{\Omega_p/\Omega}(w^p)\big(N_{\Omega_p/\Omega}(\gamma)\big)^{pe_1}.$$

It follows by Lemma 1 that

$$d_p m = e(\alpha^{d_p}, \Omega) > pe_1$$

and, since $d_p \leqslant p-1$, $e_1 < m$.

Applying the inductive assumption to (10) and putting

$$\nu_1 = \nu(\zeta_p^r\beta, \Omega_p, n/p),$$

we get

$$(12) \qquad \nu_1 \mid \big(n/p, 2^{m-2}(m-1)!\big), \quad h(x) = H(x^{n/p\nu_1}), \quad H(x) \in \Omega_p[x].$$

Since $p \mid m$ by (9), we have $\nu_1 p \mid (n, 2^{m-1}m!) = \nu$ and it is sufficient to put

$$G(x) = N_{\Omega_p/\Omega}\big(H(x^{\nu/p\nu_1})\big).$$

Indeed, by (11) and (12)

$$g(x) = N_{\Omega_p/\Omega}\big(H(x^{n/p\nu_1})\big) = G(x^{n/\nu}).$$

(B) We have here

$$g(x) \mid x^n + 4\beta^4 = \prod_{\varepsilon\eta=\pm 1}\big(x^{n/4} - (\varepsilon+\eta\zeta_4)\beta\big).$$

Let $h(x)$ be a monic factor of $g(x)$ irreducible over Ω_4. There is a pair of integers ε, η such that $\varepsilon\eta = \pm 1$,

$$(13) \qquad h(x) \mid x^{n/4} - (\varepsilon+\eta\zeta_4)\beta.$$

It follows, like (11) from (10), that

$$(14) \qquad g(x) = N_{\Omega_4/\Omega}\big(h(x)\big).$$

On the other hand, $e\big((\varepsilon+\eta\zeta_4)\beta, \Omega_4\big) = e_2 < m$. Indeed, if

$$(\varepsilon+\eta\zeta_4)\beta = w\gamma^{e_2}, \quad w \text{ a root of unity}, \ \gamma \in \Omega_4,$$

then

$$\alpha = -4\beta^4 = w^4\gamma^{4e_2} \quad \text{and} \quad \alpha^{d_4} = N_{\Omega_4/\Omega}(w^4)\big(N_{\Omega_4/\Omega}(\gamma)\big)^{4e_2}.$$

It follows by Lemma 1 that

$$d_4 m = e(\alpha^{d_4}, \Omega) > 4e_2$$

and since $d_4 \leqslant 2$, $e_2 < m$.

Applying the inductive assumption to (13) and putting

$$\nu_2 = \nu(\varepsilon+\eta\zeta_4, \Omega_4, n/4)$$

we get

$$(15) \qquad \nu_2 \mid \big(n/4, 2^{m-2}(m-1)!\big), \quad h(x) = H(x^{n/4\nu_2}), \quad H(x) \in \Omega_4[x].$$

By Lemma 1 and (B) $m = e(\alpha, \Omega) = 2e(2\beta^2, \Omega)$. Thus $2 \mid m$ and by (15) $4\nu_2 \mid (n, 2^{m-1}m!) = \nu$. Now put

$$G(x) = N_{\Omega_4/\Omega}\big(H(x)^{\nu/4\nu_2}\big).$$

By (14) and (15)

$$g(x) = N_{\Omega_4/\Omega}\big(H(x)^{n/4\nu_2}\big) = G(x^{n/\nu}),$$

which completes the inductive proof.

Proof of Theorem 1. Put $C(F) = \exp\big((2N^2+\log\log NH)\times \times(\exp 2N^2)\log NH\big)$, where N is the degree of F and H its height. Let a_0 be the leading coefficient of F, α any of its zeros and $\Omega = Q(\alpha)$. For any given n, we put $\nu = \big(n, 2^{e(\alpha,\Omega)-1}\, e(\alpha, \Omega)!\big)$. Clearly $\nu \leqslant e(\alpha, \Omega)^{e(\alpha,\Omega)}$ and by Lemma 1, $\nu \leqslant C(F)$. Besides, $u = n/\nu$ is an integer; thus parts (i) and (ii) of Theorem 1 are proved. In order to prove (iii) assume that

$$(16) \qquad F(x^\nu) = F_1(x)\ldots F_r(x)$$

is a standard form of $F(x^\nu)$ (since $F(x)$ is irreducible, there are no multiple factors). Clearly $F_j(x^u)$ $(1 \leqslant j \leqslant r)$ are relatively prime in pairs and it remains to show that they are all irreducible. Let $f_j(x)$ be a monic irreducible factor of $F_j(x^u)$. Clearly

$$(17) \qquad f_j(x) \mid F(x^n).$$

We now use the following Lemma of Capelli (cf. [5], pp. 288-290): if

$$(18) \qquad x^n - a = \prod_{i=1}^{l} g_i(x)$$

is a decomposition of $x^n - a$ into monic factors irreducible over $Q(\alpha) = \Omega$ and $N_{\Omega/Q}$ denotes the norm relative to Q, then

$$(19) \qquad F(x^n) = a_0 \prod_{i=1}^{l} N_{\Omega/Q}\big(g_i(x)\big)$$

is the decomposition of $F(x^n)$ into monic factors irreducible over Q.

It follows from (17) and (19) that for some $i \leqslant l$

$$(20) \qquad f_j(x) = N_{\Omega/Q}\, g_i(x).$$

On the other hand, it follows from (18) and Lemma 2 that

$$g_i(x) = G_i(x^u), \tag{21}$$

where $G_i(x)$ is a polynomial over Ω.

By (20), (21) and the choice of $f_j(x)$

$$f_j(x) = N_{\Omega/Q} G_i(x^u) \mid F_j(x^u); \tag{22}$$

thus

$$N_{\Omega/Q}\, G_i(x) \mid F_j(x).$$

Since $F_j(x)$ is irreducible,

$$F_j(x) = \operatorname{const} N_{\Omega/Q}\, G_i(x);$$

thus by (22)

$$F_j(x^u) = \operatorname{const} f_j(x)$$

and by the choice of $f_j(x)$, $F_j(x^u)$ is irreducible. This completes the proof.

Corollary to Theorem 1. *For every polynomial $F(x)$ and every positive integer n there exists an integer v satisfying the following conditions:*

$$0 \leqslant v \leqslant C'(F); \tag{23}$$

$$n = vu, \quad u \text{ — an integer}; \tag{24}$$

if $KF(x^v) = \operatorname{const} F_1(x)^{e_1} F_2(x)^{e_2} \dots F_r(x)^{e_r}$ is a standard form of $KF(x^v)$, then

$$KF(x^n) = \operatorname{const} F_1(x^u)^{e_1} F_2(x^u)^{e_2} \dots F_r(x^u)^{e_r}$$

is a standard form of $KF(x^n)$.

Proof. Let $KF(x) = \operatorname{const} \Phi_1^{\varepsilon_1}(x) \Phi_2^{\varepsilon_2}(x) \dots \Phi_\varrho^{\varepsilon_\varrho}(x)$ be a standard form of $KF(x)$.

Since each polynomial $\Phi_i(x)$ $(1 \leqslant i \leqslant \varrho)$ satisfies the conditions of Theorem 1, there exists for each $i \leqslant \varrho$ a positive integer v_i satisfying the following conditions:

$0 < v_i \leqslant C(\Phi_i)$; $n = v_i u_i$, u_i — an integer;

if $\Phi_i(x^{v_i}) = \Phi_{i,1}(x) \Phi_{i,2}(x) \dots \Phi_{i,r_i}(x)$ is a standard form of $\Phi_i(x^{v_i})$, then

$$\Phi_i(x^n) = \Phi_{i,1}(x^{u_i}) \Phi_{i,2}(x^{u_i}) \dots \Phi_{i,r_i}(x^{u_i})$$

is a standard form of $\Phi_i(x^n)$.

We put

$$v = [v_1, \dots, v_\varrho], \qquad C'(F) = \Big(\max_{1 \leqslant i \leqslant \varrho} C(\Phi_i)\Big)!.$$

Conditions (23) and (24) are clearly satisfied. Since $v_i \mid v$ we have $u \mid u_i$ and the irreducibility of $\Phi_{i,j}(x^{u_i})$ implies the irreducibility of $\Phi_{i,j}(x^{u_i/u})$ $(1 \leqslant i \leqslant \varrho, 1 \leqslant j \leqslant r_i)$. Since polynomials $\Phi_{i,j}$ are relatively prime in pairs, it follows that

$$KF(x^v) = \operatorname{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{i,j}(x^{u_i/u})^{\varepsilon_i}$$

is a standard form of $KF(x^v)$ and

$$KF(x^n) = \operatorname{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{i,j}(x^{u_i})^{\varepsilon_i}$$

is a standard form of $KF(x^n)$. This completes the proof.

§ 3. Lemma 3. *For any two relatively prime polynomials $G(y, z)$, $H(y, z)$ there exist two constants $B_0(G, H) = B_0 \geqslant 1$ and $B_1(G, H)$ such that if n, m are positive integers, then*

$$\left(\frac{JG(x^n, x^m)}{KG(x^n, x^m)}, \frac{JH(x^n, x^m)}{KH(x^n, x^m)}\right) \Bigg| (x^{(n,m)B_0} - 1)^{B_0}, \tag{25}$$

$$\big(KG(x^n, x^m), KH(x^n, x^m)\big) = 1 \tag{26}$$

unless $\max\{n, m\} \leqslant B_1(G, H)(n, m)$.

Proof. Let $R(z)$ be the resultant of polynomials $G(y, z)$ and $H(y, z)$ with respect to y and $S(y)$ their resultant with respect to z, and $D = \max\{\text{degree } R, \text{degree } S\}$.

Let $e^{2\pi i r_1}, e^{2\pi i r_2}, \dots, e^{2\pi i r_k}$ be all the roots of unity which are zeros of R and $\varrho_1, \varrho_2, \dots, \varrho_k$ their respective multiplicities, and similarly let $e^{2\pi i s_1}, e^{2\pi i s_2}, \dots, e^{2\pi i s_l}$ be all the roots of unity which are zeros of S and $\sigma_1, \sigma_2, \dots, \sigma_l$ their respective multiplicities. Let d be the least common denominator of $1, r_1, \dots, r_k, s_1, \dots, s_l$. We put

$$B_0 = B_0(G, H) = d \max\{1, \max_{1 \leqslant i \leqslant k} \varrho_i, \max_{1 \leqslant j \leqslant l} \sigma_j\}, \qquad B_1(G, H) = DC'(R)C'(S),$$

where C' is a constant from the Corollary to Theorem 1. Clearly

$$\frac{JR(z)}{KR(z)} \Bigg| (z^{B_0} - 1)^{B_0}, \qquad \frac{JS(y)}{KS(y)} \Bigg| (y^{B_0} - 1)^{B_0},$$

whence

$$\frac{JR(x^m)}{KR(x^m)} \Bigg| (x^{mB_0} - 1)^{B_0}, \qquad \frac{JS(x^n)}{KS(x^n)} \Bigg| (x^{nB_0} - 1)^{B_0};$$

$$\left(\frac{JR(x^m)}{KR(x^m)}, \frac{JS(x^n)}{KS(x^n)}\right) \Bigg| (x^{(n,m)B_0} - 1)^{B_0}.$$

Since

$$\big(G(x^n, x^m), H(x^n, x^m)\big) \mid \big(R(x^m), S(x^n)\big), \tag{27}$$

(25) follows. In order to prove (26), assume that $f(x)$ is an irreducible polynomial such that

$$f(x) \mid \big(KG(x^n, x^m), KH(x^n, x^m)\big).$$

By (27)

$$f(x) \mid KR(x^m) \quad \text{and} \quad f(x) \mid KS(x^n).$$

Now by the Corollary to Theorem 1 there exist a $\mu \leqslant C'(R)$ and a polynomial $F_1(x)$ such that

$$f(x) = F_1(x^{m/\mu}) \quad \text{and} \quad F_1(x) \mid KR(x^\mu). \tag{28}$$

Similarly there exist a $\nu \leqslant C'(S)$ and a polynomial $F_2(x)$ such that

$$f(x) = F_2(x^{n/\nu}) \quad \text{and} \quad F_2(x) \mid KS(x^\nu). \tag{29}$$

Let d_1, d_2 be the degrees of F_1 and F_2 respectively. It follows from (28) and (29) that

$$d_1 \frac{m}{\mu} = d_2 \frac{n}{\nu}, \quad d_1 \leqslant D\mu, \quad d_2 \leqslant D\nu.$$

Hence $\max\{n, m\}/(n, m) \leqslant D\mu\nu \leqslant DC'(R)C'(S) = B_1(G, H)$, which completes the proof.

LEMMA 4. *Let k_i $(0 \leqslant i \leqslant l)$ be an increasing sequence of integers. Let $k_{j_1} - k_{i_1}, \ldots, k_{j_P} - k_{i_P}$ $(P \geqslant 0)$ be all the numbers besides $k_l - k_0$ which appear only once in the double sequence $k_j - k_i$ $(0 \leqslant i < j \leqslant l)$. Suppose that for each pair p, q, where $1 \leqslant p < q \leqslant P$*

$$c_{p,q}(k_l - k_0) + c'_{p,q}(k_{j_p} - k_{i_p}) + c''_{p,q}(k_{j_q} - k_{i_q}) = 0, \tag{30}$$

where $c_{p,q}$, $c'_{p,q}$, $c''_{p,q}$ are integers not all zero. Let $c = 1$ if $P < 2$ and $c = \max\limits_{1 \leqslant p < q \leqslant P} \max\{|c_{p,q}|, |c'_{p,q}|, |c''_{p,q}|\}$ if $P \geqslant 2$. Then there exist integers s, t, $\varkappa_i$, λ_i $(0 \leqslant i \leqslant l)$ such that

$$k_i - k_0 = s\varkappa_i + t\lambda_i \quad (0 \leqslant i \leqslant l),$$
$$|\varkappa_i| < (5c)^l, \quad |\lambda_i| < (5c)^l \quad (0 \leqslant i \leqslant l).$$

Proof. By the assumption, for each pair $\langle i, j\rangle$, where $0 \leqslant i < j \leqslant l$ and $\langle i, j\rangle \neq \langle 0, l\rangle, \langle i_1, j_1\rangle, \ldots, \langle i_P, j_P\rangle$ there exists a pair $\langle g_{i,j}, h_{i,j}\rangle \neq \langle i, j\rangle$ such that

$$k_j - k_i = k_{h_{i,j}} - k_{g_{i,j}}.$$

Let us consider the system of linear homogeneous equations

$$\begin{aligned} &x_0 = 0, \\ &x_j - x_i = x_{h_{i,j}} - x_{g_{i,j}}, \quad \langle i, j\rangle \neq \langle 0, l\rangle, \langle i_1, j_1\rangle, \ldots, \langle i_P, j_P\rangle, \\ &c_{p,q}x_l + c'_{p,q}(x_{j_p} - x_{i_p}) + c''_{p,q}(x_{j_q} - x_{i_q}) = 0, \quad 1 \leqslant p < q \leqslant P. \end{aligned} \tag{31}$$

$\mathfrak{k} = [0, k_1 - k_0, \ldots, k_l - k_0]$ is a solution of this system. Suppose that there are two other linearly independent solutions, $\mathfrak{a} = [a_0, a_1, \ldots, a_l]$ and $\mathfrak{b} = [b_0, b_1, \ldots, b_l]$. Performing linear transformations on the system $\mathfrak{k}$, $\mathfrak{a}$, $\mathfrak{b}$ we shall denote by $\mathfrak{a}^{(\nu)}$, $\mathfrak{b}^{(\nu)}$ the successive images of $\mathfrak{a}$ and $\mathfrak{b}$, and by $a_i^{(\nu)}$, $b_i^{(\nu)}$ the components of $\mathfrak{a}^{(\nu)}$, $\mathfrak{b}^{(\nu)}$ respectively.

Put

$$\mathfrak{a}' = \mathfrak{a} - \frac{a_l}{k_l - k_0}\mathfrak{k}, \qquad \mathfrak{b}' = \mathfrak{b} - \frac{b_l}{k_l - k_0}\mathfrak{k},$$

i' = the least i such that $a'_i = \min\limits_{0 \leqslant j \leqslant l} a'_j$ or $\max\limits_{0 \leqslant j \leqslant l} a'_j$,

j' = the greatest i such that $a'_i = \min\limits_{0 \leqslant j \leqslant l} a'_j + \max\limits_{0 \leqslant j \leqslant l} a'_j - a'_{i'}$ (the opposite extremum).

Clearly $j' > i'$. Since $\mathfrak{a}' \neq 0$ and $a'_0 = 0$, it follows from the definition of j' that $a'_{j'} \neq 0$.

Put

$$\mathfrak{b}'' = \mathfrak{b}' - \frac{b'_{j'}}{a'_{j'}}\mathfrak{a}',$$

i'' = the least i such that $b''_i = \min\limits_{0 \leqslant j \leqslant l} b''_j$ or $\max\limits_{0 \leqslant j \leqslant l} b''_j$,

j'' = the greatest i such that $b''_i = \min\limits_{0 \leqslant j \leqslant l} b''_i + \max\limits_{0 \leqslant j \leqslant l} b''_j - b''_{i''}$.

Clearly $j'' > i''$. $\mathfrak{a}'$ and $\mathfrak{b}''$ are solutions of the system (31) and satisfy the following conditions:

$$a'_{j'} \neq 0 = a'_{i'}, \tag{32}$$

(33) all a'_i are in the interval $\langle a'_{i'}, a'_{j'}\rangle$, $a'_i \neq a'_{i'}$ for $i < i'$, $a'_i \neq a'_{j'}$ for $i \leqslant i'$ and for $i > j'$.

$$b''_{j''} \neq 0 = b''_{j'} = b''_{i'}, \tag{34}$$

(35) all b''_i are in the interval $\langle b''_{i''}, b''_{j''}\rangle$, $b''_i \neq b''_{i''}$ for $i < i''$, $b''_i \neq b''_{j''}$ for $i \leqslant i''$ and for $i > j''$.

Now, (32) and (33) imply that $\langle i', j'\rangle$ is for some $p \leqslant P$ identical with $\langle i_p, j_p\rangle$. Indeed, by (32), $\langle i', j'\rangle \neq \langle 0, l\rangle$, whence we would have in the opposite case

$$a'_{j'} - a'_{i'} = a'_h - a'_g, \quad \text{where } \langle g, h\rangle = \langle g_{i',j'}, h_{i',j'}\rangle \neq \langle i', j'\rangle.$$

It follows from (33) that $a'_h = a'_{j'}$, $a'_g = a'_{i'}$, whence $g \geqslant i'$, $h \leqslant j'$.

On the other hand,

$$k_{j'} - k_{i'} = k_h - k_g$$

and since k_i are increasing, $g = i'$, $h = j'$, which gives a contradiction. Similarly, (34) and (35) imply that $\langle i'', j''\rangle$ is $\langle i_q, j_q\rangle$, where $1 \leqslant q \leqslant P$.

Moreover, by (34) $\langle i', j'\rangle \neq \langle i'', j''\rangle$. Thus $p \neq q$ and without loss of generality we may assume $p < q$. Putting for brevity $c'_{p,q} = c'$ and $c''_{p,q} = c''$, we get from (30), (32) and (34)

$$c_{p,q}(k_l - k_0) + c'(k_{j'} - k_{i'}) + c''(k_{j''} - k_{i''}) = 0, \tag{36}$$

$$c'(a'_{j'} - a'_{i'}) + c''(a'_{j''} - a'_{i''}) = 0, \tag{37}$$

$$c'(b''_{j'} - b''_{i'}) + c''(b''_{j''} - b''_{i''}) = 0. \tag{38}$$

Since $k_l > k_0$, it follows from (36) that $c' \neq 0$ or $c'' \neq 0$. Now in view of (33) and (37) $|c''| \geqslant |c'|$, and in view of (35) and (38) $|c'| \geqslant |c''|$. Hence $c' = \pm c'' \neq 0$. If $c' = -c''$, (35) and (38) imply that $b''_{j'} = b''_{j''}$, which contradicts (34). If $c' = c''$, (33) and (37) imply that $a'_{i''} = a'_{j'}$, $i'' > i'$. Similarly (35) and (38) imply that $b''_{i'} = b''_{j''}$, $i' > i''$. The contradiction obtained proves that system (31) has at most two linearly independent solutions. Therefore, the rank of the matrix M of system (31) is at least $l-1$. If this rank is l, solving the system by means of Cramer's formulae we get

$$x_i = x_\mu D_i/D \quad (0 \leqslant i \leqslant l,\ \mu \text{ fixed}),$$

where D and D_i are determinants of degree l and, as can easily be seen from the form of matrix M, the sum of absolute values of integers standing in any line of D_i does not exceed $5c$. Hence $|D_i| < (5c)^l$ and *a fortiori* $|D_i|/(D_0, \ldots, D_l) < (5c)^l$.

Since

$$\frac{(k_\mu - k_0)D_i}{D} = k_i - k_0 \quad (0 \leqslant i \leqslant l),$$

$(k_\mu - k_0)(D_0, \ldots, D_l)/D$ is an integer and the lemma holds with

$$s = (k_\mu - k_0)(D_0, \ldots, D_l)/D, \quad t = 0,$$
$$x_i = D_i/(D_0, \ldots, D_l), \quad \lambda_i = 0 \quad (0 \leqslant i \leqslant l).$$

If the rank of M is $l-1$, we get similarly

$$x_i = (x_\mu D'_i + x_\nu D''_i)/D \quad (0 \leqslant i \leqslant l,\ \mu, \nu \text{ fixed}),$$

where D, D'_i and D''_i are determinants of degree $l-1$,

$$|D'_i| < (5c)^{l-1}, \quad |D''_i| < (5c)^{l-1} \quad (0 \leqslant i \leqslant l). \tag{39}$$

Integral vectors $[x_\mu, x_\nu]$ such that all numbers $(x_\mu D'_i + x_\nu D''_i)/D$ $(0 \leqslant i \leqslant l)$ are integers form a module, say $\mathfrak{M}$. Clearly $[0, |D|] \in \mathfrak{M}$ and $[|D|, 0] \in \mathfrak{M}$. Let ξ_1 be the least positive integer such that for some η_1, $[\xi_1, \eta_1] \in \mathfrak{M}$ and let η_2 be the least positive integer such that $[0, \eta_2] \in \mathfrak{M}$. Clearly $[\xi_1, \eta_1]$ and $[0, \eta_2]$ form a basis for $\mathfrak{M}$ and without lost of generality we may assume $0 \leqslant \eta_1 < \eta_2$. On the other hand, $\eta_2 \leqslant |D|$ and $\xi_1 \leqslant |D|$.

Since k_i are integers, $[k_\mu - k_0, k_\nu - k_0] \in \mathfrak{M}$; thus there are integers s, t such that $k_\mu - k_0 = \xi_1 s, k_\nu - k_0 = \eta_1 s + \eta_2 t$.

Putting $\varkappa_i = (\xi_1 D'_i + \eta_1 D''_i)/D$, $\lambda_i = \eta_2 D''_i/D$, we get for $i \leqslant l$

$$k_i - k_0 = \varkappa_i s + \lambda_i t$$

and by (39)

$$|\varkappa_i| \leqslant \frac{\xi_1}{|D|}|D'_i| + \frac{|\eta_1|}{D}|D''_i| \leqslant 2(5c)^{l-1} < (5c)^l,$$

$$|\lambda_i| \leqslant \frac{\eta_2}{|D|}|D''_i| < (5c)^{l-1}.$$

This completes the proof.

Remark. For a given finite linear set, denote by ϱ the number of rationally independent distances and by ϱ_0 the number of rationally independent distances which appear only once. It follows from the lemma that if $\varrho_0 \leqslant 2$, then $\varrho \leqslant 2$. It can easily be found from remark 1 at the end of paper [2] that if $\varrho_0 = 1$ then $\varrho = 1$. The equality $\varrho = \varrho_0$ suggests itself, but I am unable to prove it.

Definition. For a given integral matrix A, $h(A)$ will denote the maximum of absolute values of the elements of A.

Lemma 5. *Let Γ be any given integral matrix 2×2. For arbitrary positive integers d, n, m there exists an integral matrix*

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the conditions:

$$0 \leqslant \nu_i \leqslant \big((2d^2)!\big)^2, \quad 0 \leqslant \mu_i \leqslant \big((2d^2)!\big)^2 \quad (i = 1, 2), \tag{40}$$

$$|M| > 0, \tag{41}$$

$$[n, m] = [u, v]M, \quad u, v \text{ integers} \geqslant 0, \tag{42}$$

and with the following property. If

$$[n, m]\Gamma = [s, t]\Delta, \tag{43}$$

where s, t are integers, Δ is an integral matrix,

$$|\Delta| \neq 0 \quad \text{and} \quad h(\Delta) \leqslant d, \tag{44}$$

then

$$M\Gamma = T\Delta \quad \text{and} \quad [s, t] = [u, v]T, \tag{45}$$

where T is an integral matrix and

$$h(T) \leqslant 4d\big((2d^2)!\big)^2 h(\Gamma). \tag{46}$$

Proof. Let S be the set of all integral matrices Δ satisfying (43) and (44). Integral vectors $[x, y]$ such that for all $\Delta \in S$ and suitable integers s_Δ, t_Δ, $[x, y]\Gamma = [s_\Delta, t_\Delta]\Delta$ form a module, say $\mathfrak{M}$. By (44) $2d^2 \geqslant |\Delta| \neq 0$, whence $|\Delta|$ divides $(2d^2)!$.

It follows that $[(2d^2)!, 0] \in \mathfrak{M}$ and $[0, (2d^2)!] \in \mathfrak{M}$. Let ξ_1 be the least positive integer such that, for some η_1, $[\xi_1, \eta_1] \in \mathfrak{M}$ and let η_2 be the least positive integer such that $[0, \eta_2] \in \mathfrak{M}$. Clearly $[\xi_1, \eta_1]$ and $[0, \eta_2]$ form a basis for $\mathfrak{M}$ and we may assume without loss of generality that $0 \leqslant \eta_1 < \eta_2$. Hence

$$0 < \xi_1 \leqslant (2d^2)!, \quad 0 \leqslant \eta_1 < \eta_2 \leqslant (2d^2)! . \tag{47}$$

Let

$$\frac{\eta_1}{\eta_2} = \frac{1}{|b_1|} - \frac{1}{|b_2|} - \ldots - \frac{1}{|b_r|}$$

be the expansion of $\frac{\eta_1}{\eta_2}$ into a continued fraction, where b_p are integers > 1 $(1 \leqslant p \leqslant r)$; if $\eta_1 = 0$ let $r = 0$. Put

$$A_{-1} = -1, \quad B_{-1} = 0; \quad A_0 = 0, \quad B_0 = 1;$$
$$A_{p+1} = b_p A_p - A_{p-1}, \quad B_{p+1} = b_p B_p - B_{p-1} \quad (0 \leqslant p < r).$$

It follows that the sequences A_p, B_p are increasing and for $p \leqslant r$

$$A_p B_{p-1} - B_p A_{p-1} = 1, \tag{48}$$

$$0 \leqslant A_p \leqslant \eta_1, \quad 0 < B_p \leqslant \eta_2, \tag{49}$$

$$A_p/B_p < A_r/B_r = \eta_1/\eta_2. \tag{50}$$

Since m, n are > 0, we have

$$\frac{\eta_1}{\eta_2} - \frac{m}{n} \cdot \frac{\xi_1}{\eta_2} < \frac{A_r}{B_r}.$$

Let q be the least non-negative integer which can be substitued for r in the last inequality. Assuming $A_{-1}/B_{-1} = -\infty$ we have therefore

$$\frac{A_{q-1}}{B_{q-1}} \leqslant \frac{\eta_1}{\eta_2} - \frac{m}{n} \cdot \frac{\xi_1}{\eta_2} < \frac{A_q}{B_q}. \tag{51}$$

Let us put

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix} = \begin{bmatrix} B_q & -A_q \\ B_{q-1} & -A_{q-1} \end{bmatrix} \begin{bmatrix} \xi_1 & \eta_1 \\ 0 & \eta_2 \end{bmatrix} = \begin{bmatrix} B_q \xi_1 & B_q \eta_1 - A_q \eta_2 \\ B_{q-1}\xi_1 & B_{q-1}\eta_1 - A_{q-1}\eta_2 \end{bmatrix}.$$

Inequalities (47), (49) and (50) imply (40). By (48)

$$|M| = \begin{vmatrix} \xi_1 & \eta_1 \\ 0 & \eta_2 \end{vmatrix} = \xi_1 \eta_2 > 0.$$

Moreover, the vectors $[\nu_1, \mu_1]$, $[\nu_2, \mu_2]$ form a basis for $\mathfrak{M}$. Since $[n, m] \in \mathfrak{M}$, there are integers u, v satisfying (42). We have

$$[u, v] = [n, m]M^{-1} = \frac{1}{\xi_1 \eta_2} [n, m] \begin{bmatrix} B_{q-1}\eta_1 - A_{q-1}\eta_2 & -B\eta_1 + A_q \eta_2 \\ -B_{q-1}\xi_1 & B_q \xi_1 \end{bmatrix}$$
$$= \frac{1}{\xi_1 \eta_2} [B_{q-1}(n\eta_1 - m\xi_1) - A_{q-1}\eta_2, A_q \eta_2 - B_q(n\eta_1 - m\xi_1)].$$

It follows from (51) that $u \geqslant 0$, $v \geqslant 0$. In order to prove the last statement of the lemma suppose that for some integral matrix Δ (43) and (44) hold. Thus $\Delta \in S$ and since $[\nu_i, \mu_i] \in \mathfrak{M}$ $(i = 1, 2)$ there are integers σ_i, τ_i such that $[\nu_i, \mu_i]\Gamma = [\sigma_i, \tau_i]\Delta$ $(i = 1, 2)$. Putting

$$T = \begin{bmatrix} \sigma_1 & \tau_1 \\ \sigma_2 & \tau_2 \end{bmatrix} \tag{52}$$

we get

$$M\Gamma = T\Delta.$$

On the other hand, (42) and (43) imply

$$[u, v]M\Gamma = [s, t]\Delta. \tag{53}$$

Since $|\Delta| \neq 0$ by (44), we get (45) from (52) and (53). Finally, by (52), (40) and (44)

$$h(T) = h(M\Gamma\Delta^{-1}) \leqslant 4h(M)h(\Gamma)h(\Delta) \leqslant 4d(|(2d^2)!|)^2 h(\Gamma).$$

This completes the proof.

Lemma 6. *Let $f(x)$ be an irreducible polynomial not dividing $x^\delta - x$ $(\delta > 1)$, α, β integers, $\alpha > 0$ or $\beta > 0$. For arbitrary positive integers n, m such that $an + \beta m > 0$ there exists an integral matrix*

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the conditions

$$0 \leqslant \nu_i \leqslant C(f, \alpha, \beta), \quad 0 \leqslant \mu_i \leqslant C(f, \alpha, \beta) \quad (i = 1, 2), \tag{54}$$

$$|M| > 0, \tag{55}$$

$$[n, m] = [u, v]M, \quad u, v \text{ integers} \geqslant 0, \tag{56}$$

$$a\nu_i + \beta\mu_i \geqslant 0 \quad (i = 1, 2), \tag{57}$$

and having the following property:

if $f(y^{\alpha\nu_1+\beta\mu_1}z^{\alpha\nu_2+\beta\mu_2}) = f_1(y,z)\dots f_r(y,z)$ *is a standard form of* $f(y^{\alpha\nu_1+\beta\mu_1}z^{\alpha\nu_2+\beta\mu_2})$, *then*

$$f(x^{\alpha n+\beta m}) = f_1(x^u, x^v)\dots f_r(x^u, x^v)$$

is a standard form of $f(x^{\alpha n+\beta m})$.

$C(f, \alpha, \beta)$ *is an effectively computable constant, independent of* n *and* m.

Proof. By Theorem 1, there exists a positive integer $\nu \leqslant C(f)$ such that $\alpha n+\beta m = vw$, w integer and having the following property: if

$$f(x^\nu) = f_1'(x)\dots f_{r'}'(x) \tag{58}$$

is a standard form of $f(x^\nu)$, then

$$f(x^{\alpha n+\beta m}) = f_1'(x^w)\dots f_{r'}'(x^w) \tag{59}$$

is a standard form of $f(x^{\alpha n+\beta m})$.

Now we distinguish two cases, $\alpha\beta \geqslant 0$ and $\alpha\beta < 0$.

If $\alpha\beta \geqslant 0$ we put in Lemma 5:

$$\Gamma = \begin{bmatrix} \alpha & \alpha \\ \beta & \beta \end{bmatrix}, \quad d = C(f).$$

Let

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

be an integral matrix whose existence for n, m is asserted in that lemma. It follows from (40) that

$$0 \leqslant \nu_i \leqslant \left(2\left(C^2(f)!\right)\right)^2, \quad 0 \leqslant \mu_i \leqslant \left(2\left(C^2(f)!\right)\right)^2 \quad (i = 1, 2); \tag{60}$$

thus (54) is satisfied with $C(f, \alpha, \beta) = \left(2\left(C^2(f)!\right)\right)^2$ and, in view of $\alpha \geqslant 0$, $\beta \geqslant 0$, (57) holds. Formulae (55) and (56) follow from (41) and (42). We apply the last statement of Lemma 5 with

$$[s, t] = [w, w], \quad \Delta = \begin{bmatrix} \nu & 0 \\ 0 & \nu \end{bmatrix}.$$

In virtue of that statement there exists an integral matrix T such that

$$\begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}\begin{bmatrix} \alpha & \alpha \\ \beta & \beta \end{bmatrix} = T\begin{bmatrix} \nu & 0 \\ 0 & \nu \end{bmatrix},$$

whence

$$\nu \mid a\nu_i+\beta\mu_i \quad (i = 1, 2). \tag{61}$$

If $\alpha\beta < 0$, we may assume without loss of generality $\alpha > 0$, $\beta < 0$. We put in Lemma 5:

$$\Gamma' = \begin{bmatrix} \nu & \nu \\ -\beta & -\beta \end{bmatrix}, \quad d' = \alpha, \quad n' = \frac{\alpha n+\beta m}{\nu}, \quad m' = m$$

(the "dash" is added to avoid a confusion in notation). In virtue of that lemma there exists an integral matrix

$$M' = \begin{bmatrix} \nu_1' & \mu_1' \\ \nu_2' & \mu_2' \end{bmatrix}$$

such that

$$0 \leqslant \nu_i' \leqslant \left((2\alpha^2)!\right)^2, \quad 0 \leqslant \mu_i' \leqslant \left((2\alpha^2)!\right)^2 \quad (i = 1, 2), \tag{62}$$

$$|M'| > 0, \tag{63}$$

$$[(\alpha n+\beta m)/\nu, m] = [u, v]M', \quad u, v \text{ integers} \geqslant 0. \tag{64}$$

We apply the last statement of Lemma 5 with

$$[s, t] = [w, w], \quad \Delta = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}.$$

In virtue of that statement there exists an integral matrix T such that

$$\begin{bmatrix} \nu_1' & \mu_1' \\ \nu_2' & \mu_2' \end{bmatrix}\begin{bmatrix} \nu & \nu \\ -\beta & -\beta \end{bmatrix} = T\begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix},$$

whence $\alpha \mid \nu\nu_i'-\beta\mu_i'$ $(i = 1, 2)$. We put

$$\nu_i = (\nu\nu_i'-\beta\mu_i')/\alpha, \quad \mu_i = \mu_i' \quad (i = 1, 2).$$

(62) implies (57) and the inequality

$$0 \leqslant \nu_i \leqslant \left((2\alpha^2)!\right)^2\left(C(f)+|\beta|\right), \quad 0 \leqslant \mu_i \leqslant \left((2\alpha^2)!\right)^2 \quad (i = 1, 2);$$

thus (54) is satisfied with $C(f, \alpha, \beta) = \left((2\alpha^2)!\right)^2\left(C(f)+|\beta|\right)$. Formulae (55) and (56) follow from (53) and (64); besides we have (61).

In order to prove the last property of the matrix M postulated in the lemma, we put

$$f_j'(y, z) = f_j'(y^{(\alpha\nu_1+\beta\mu_1)/\nu}z^{(\alpha\nu_2+\beta\mu_2)/\nu}) \quad (1 \leqslant j \leqslant r'). \tag{65}$$

By (56) $f_j'(x^u, x^v) = f_j'(x^w)$, whence by (59), $f_j'(x^u, x^v)$ is irreducible. We show that $f_j'(y, z)$ is not reducible.

Denote by δ the degree of $f_j'(x)$ and suppose that

$$f_j'(y, z) = g(y, z)h(y, z), \tag{66}$$

where g is of degree γ_1 in y, γ_2 in z; h is of degree χ_1 in y, χ_2 in z and $\gamma_1+\gamma_2 > 0$, $\chi_1+\chi_2 > 0$. By (65) we have

$$\delta(\alpha\nu_i+\beta\mu_i)/\nu = \gamma_i+\chi_i \quad (i = 1, 2).$$

On the other hand,

$$f_j'(x^w) = g(x^u, x^v)h(x^u, x^v).$$

The degree of $f_j'(x^w)$ equals

$$\delta(\alpha n+\beta m)/\nu = \delta u(\alpha\nu_1+\beta\mu_1)/\nu+\delta v(\alpha\nu_2+\beta\mu_2)/\nu = u(\gamma_1+\chi_1)+v(\gamma_2+\chi_2).$$

The degree of $g(x^u, x^v)h(x^u, x^v)$ can be equal to $u\gamma_1+u\chi_1+v\gamma_2+v\chi_2$ only if the degree of $g(x^u, x^v)$ equals $u\gamma_1+v\gamma_2$ and the degree of $h(x^u, x^v)$ equals $u\chi_1+v\chi_2$. Since $f_j'(x^w)$ is irreducible we get $u\gamma_1+v\gamma_2 = 0$ or $u\chi_1+v\chi_2 = 0$, whence $u = 0$ and $\gamma_2\chi_2 = 0$ or $v = 0$ and $\gamma_1\chi_1 = 0$ or $u = v = 0$. The last case is impossible by (56), and in view of symmetry it is enough to consider $u = 0$, $\gamma_2 = 0$. Thus $g(y, 0) = g(y, z)$ is not constant and, since $f_j'(0) \neq 0$, it follows from (65) and (66) that $\alpha\nu_2+\beta\mu_2 = 0$. This gives $\alpha n+\beta m = u(\alpha\nu_1+\beta\mu_1)+v(\alpha\nu_2+\beta\mu_2) = 0$. The contradiction obtained proves that no $f_j'(y, z)$ $(1 \leqslant j \leqslant r')$ is reducible. Since $f_j'(y, z)$ are also not constant, and by (58)

$$f(y^{\alpha\nu_1+\beta\mu_1}z^{\alpha\nu_2+\beta\mu_2}) = f_1'(y, z)\dots f_{r'}'(y, z),$$

it follows that the polynomials $f_j'(y, z)$ $(1 \leqslant j \leqslant r')$ and $f_j(y, z)$ $(1 \leqslant j \leqslant r)$, after a suitable permutation, differ only by constant factors. Since the polynomials $f_j'(x^u, x^v) = f_j'(x^w)$ $(1 \leqslant j \leqslant r')$ are irreducible and coprime, the same applies to $f_j(x^u, x^v)$ $(1 \leqslant j \leqslant r)$, which completes the proof.

§ 4. Proof of Theorem 2. It is clear that if $\Phi(x)$ is a polynomial, then $K\Phi(x) = KJ\Phi(x)$. We take this equality as a definition of $K\Phi(x)$, where $\Phi(x)$ is a rational function of the form $\sum_{i=0}^{I} a_i x^{\alpha_i}$ (a_i integers).

Now let

$$F(y, z) = \sum_{i=0}^{I} a_i y^{\alpha_i} z^{\beta_i},$$

where a_i are integers $\neq 0$ and the pairs $\langle\alpha_i, \beta_i\rangle$ $(0 \leqslant i \leqslant I)$ are all different (it is clearly sufficient to prove the theorem for polynomials with integral coefficients). Let ϱ be the rank of the matrix

$$\begin{bmatrix} \alpha_1-\alpha_0 & \alpha_2-\alpha_0 & \dots & \alpha_I-\alpha_0 \\ \beta_1-\beta_0 & \beta_2-\beta_0 & \dots & \beta_I-\beta_0 \end{bmatrix}.$$

We consider separately two cases, $\varrho = 1$ and $\varrho = 2$.

Case $\varrho = 1$. In this case there exist integers α, β and γ_i $(0 \leqslant i \leqslant I)$ such that $\alpha > 0$ or $\beta > 0$ and

$$\alpha_i-\alpha_0 = \alpha\gamma_i, \quad \beta_i-\beta_0 = \beta\gamma_i \quad (0 \leqslant i \leqslant I).$$

Put

$$f(x) = J\sum_{i=0}^{I} a_i x^{\gamma_i}.$$

Clearly

$$JF(y, z) = Jf(y^\alpha z^\beta). \tag{67}$$

Since $F(y, z)$ is irreducible and is different from ay, az, both $f(x)$ and $Jf(x^{-1}) = J\sum_{i=0}^{I} a_i x^{-\gamma_i}$ are irreducible. If we had for some $\delta > 1$, $f(x) \mid x^\delta - x$, this would imply $f(x) = \pm Jf(x^{-1})$, whence $JF(y, z) = \pm JF(y^{-1}, z^{-1})$, against the assumption. Thus both $f(x)$ and $Jf(x^{-1})$ satisfy the conditions of Lemma 6 and constants $C(f, \alpha, \beta)$, $C(Jf(x^{-1}), \alpha, \beta)$ are well defined. We put

$$C_0(F) = \max\{|\alpha|, |\beta|\}; \quad C_1(F) = \max\{C(f, \alpha, \beta), C(Jf(x^{-1}), \alpha, \beta)\}.$$

If $\alpha n+\beta m = 0$, we have $\max\{n, m\} \leqslant C_0(F)(n, m)$.

If $\alpha n+\beta m < 0$, we can replace in (67) f by $Jf(x^{-1})$, α by $-\alpha$, β by $-\beta$, which will not affect the inequality

$$C(f, \alpha, \beta) \leqslant C_1(F). \tag{68}$$

We may therefore assume without loss of generality that $\alpha n+\beta m > 0$ and (68) holds. Let

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

be an integral matrix, whose existence for n, m is asserted in Lemma 6. Since by (57) and (67)

$$JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2}) = f(y^{\alpha\nu_1+\beta\mu_1}z^{\alpha\nu_2+\beta\mu_2}),$$
$$KF(x^n, x^m) = f(x^{\alpha n+\beta m}),$$

Theorem 2 follows in this case ($\varrho = 1$) from Lemma 6 and (68).

Case $\varrho = 2$. We may assume without loss of generality that

$$\begin{vmatrix} \alpha_1-\alpha_0 & \alpha_2-\alpha_0 \\ \beta_1-\beta_0 & \beta_2-\beta_0 \end{vmatrix} \neq 0.$$

Let ξ be any irrational number. Clearly the numbers $(\alpha_1-\alpha_0)+\xi(\beta_1-\beta_0)$ and $(\alpha_2-\alpha_0)+\xi(\beta_2-\beta_0)$ are incommensurable; thus there are incommensurable distances in the set of points $\alpha_i+\xi\beta_i$ $(0 \leqslant i \leqslant I)$. By remark 1 at the end of paper [2] (cf. also the remark after Lemma 4) there are in this set two incommensurable distances which appear only once in the double sequence $\alpha_j-\alpha_i+\xi(\beta_j-\beta_i)$ $(0 \leqslant i < j \leqslant I)$. This means that there exist 4 non-negative integers i', i'', j', j'' such that $\langle \alpha_{j'}-\alpha_{i'}, \beta_{j'}-\beta_{i'} \rangle$ and $\langle \alpha_{j''}-\alpha_{i''}, \beta_{j''}-\beta_{i''} \rangle$ appear only once in the double sequence $\langle \alpha_j-\alpha_i, \beta_j-\beta_i \rangle$ $(0 \leqslant i < j \leqslant I)$ and

$$\begin{vmatrix} \alpha_{j'}-\alpha_{i'} & \alpha_{j''}-\alpha_{i''} \\ \beta_{j'}-\beta_{i'} & \beta_{j''}-\beta_{i''} \end{vmatrix} \neq 0.$$

We put in Lemma 5

$$\Gamma = \begin{bmatrix} \alpha_{j'}-\alpha_{i'} & \alpha_{j''}-\alpha_{i''} \\ \beta_{j'}-\beta_{i'} & \beta_{j''}-\beta_{i''} \end{bmatrix}, \quad d = 2(10N^2)^A, \tag{69}$$

where $N = \max\limits_{0 \leqslant i \leqslant I} \max\{\alpha_i, \beta_i\}$, $A = \sum\limits_{i=0}^{I} a_i^2$.

Let

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

be an integral non-singular matrix, whose existence for n, m is asserted in that lemma. Thus we have by (40) and (42)

$$0 \leqslant \nu_i \leqslant \left((8\cdot 10^{2A}N^{4A})!\right)^2, \quad 0 \leqslant \mu_i \leqslant \left((8\cdot 10^{2A}N^{4A})!\right)^2 \quad (i = 1, 2), \tag{70}$$

$$[n, m] = [u, v]M, \quad u, v \text{ integers} \geqslant 0. \tag{71}$$

We see that assertions (i) and (ii) of Theorem 2 are satisfied with $C_1(F) = \left((8\cdot 10^{2A}n^{4A})!\right)^2$.

Moreover, by (70) and (71)

$$\max\{n, m\} \leqslant 2C_1(F)\max\{u, v\}, \quad (n, m) \geqslant (u, v). \tag{72}$$

Let

$$JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2}) = \operatorname{const} F_1(y, z)^{e_1}F_2(y, z)^{e_2}\dots F_r(y, z)^{e_r} \tag{73}$$

be a standard form of $JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2})$. In order to prove (iii) we have to show that either

$$KF(x^n, x^m) = \operatorname{const} KF_1(x^u, x^v)^{e_1}KF_2(x^u, x^v)^{e_2}\dots KF_r(x^u, x^v)^{e_r}$$

is a standard form of $KF(x^n, x^m)$ or $\max\{n, m\} \leqslant C_0(F)(n, m)$, where $C_0(F)$ is a constant independent of n, m. In view of (70) it is sufficient to prove the same with $C_0(F)$ replaced by $C_0(F, M)$, a constant depending only on F and M.

In order to define $C_0(F, M)$ we notice that by the assumption $\left(JF(y, z), JF(y^{-1}, z^{-1})\right) = 1$ and by Lemma 3 there exist two constants, $B_{00} = B_0\left(JF(y, z), JF(y^{-1}, z^{-1})\right) \geqslant 1$ and $B_{01} = B_1\left(JF(y, z), JF(y^{-1}, z^{-1})\right)$, such that

$$\left(\frac{JF(x^n, x^m)}{KF(x^n, x^m)}, \frac{JF(x^{-n}, x^{-m})}{KF(x^{-n}, x^{-m})}\right) \Big| (x^{(n,m)B_{00}}-1)^{B_{00}} \tag{74}$$

and

$$\left(KF(x^n, x^m), KF(x^{-n}, x^{-m})\right) = 1 \tag{75}$$

unless

$$\max\{n, m\} \leqslant B_{01}(n, m).$$

Since for an arbitrary polynomial $f(x)$

$$Jf(x)/Kf(x) = Jf(x^{-1})/Kf(x^{-1}), \tag{76}$$

we get from (74)

$$\frac{JF(x^n, x^m)}{KF(x^n, x^m)} \Big| (x^{(n,m)B_{00}}-1)^{B_{00}}. \tag{77}$$

Let S_j $(1 \leqslant j \leqslant r)$ be the set of all the polynomials not divisible by $F_j(y, z)$ which are of the form $J\sum\limits_{i=0}^{l} c_i y^{\sigma_i}z^{\tau_i}$, where c_i are integers $\neq 0$, $\sum\limits_{i=0}^{l} c_i^2 = A$ and

$$\max\{|\sigma_i|, |\tau_i|\} \leqslant 16\cdot 10^{2A}N^{4A+1}C_1(F) \quad (0 \leqslant i \leqslant l).$$

Clearly the sets S_j $(1 \leqslant j \leqslant r)$ are finite and effectively computable. Moreover, for each $H \in S_j$ there exists by Lemma 3 a constant $B_1(F_j, H)$ such that

$$\left(KF_j(x^u, x^v), KH(x^u, x^v)\right) = 1 \tag{78}$$

unless

$$\max\{u, v\} \leqslant B_1(F_j, H)(u, v).$$

Finally for each pair $\langle i, j\rangle$, where $1 \leqslant i < j \leqslant r$ there exists by Lemma 3 a constant $B_1(F_i, F_j)$ such that

$$(79) \qquad \left(KF_i(x^u, x^v), KF_j(x^u, x^v)\right) = 1$$

unless

$$\max\{u, v\} \leqslant B_1(F_i, F_j)(u, v).$$

We put

$$C_0(F, M) = \max\{8NC_1^2(F)B_{00}^2, B_{01}, 2C_1(F)\times \\ \times \max_{1\leqslant j\leqslant r}\max_{H\in S_j} B_1(F_j, H), 2C_1(F)\max_{1\leqslant i<j\leqslant r} B_1(F_i, F_j)\}.$$

If for any pair $\langle i, j\rangle$ where $1 \leqslant i < j \leqslant r$, $\left(KF_i(x^u, x^v), KF_j(x^u, x^v)\right) \neq 1$ we have by (72) and (79)

$$\max\{n, m\}/(n, m) \leqslant 2C_1(F)B_1(F_i, F_j) \leqslant C_0(F, M).$$

It remains to prove that if any polynomial $KF_j(x^u, x^v)$ $(1 \leqslant j \leqslant r)$ is not irreducible, then $\max\{n, m\} \leqslant C_0(F, M)(n, m)$.

We shall do that in two steps assuming first that $KF_1(x^u, x^v)$ is constant and secondly that it is reducible (the treatment of $F_1(x^u, x^v)$ instead of $F_j(x^u, x^v)$ does not affect generality and simplifies a little the notation).

1. Assume that $KF_1(x^u, v^v)$ is constant. Let

$$(80) \qquad F_1(y, z) = \sum_{j=0}^{k} b_j y^{\gamma_j} z^{\delta_j} \qquad (b_j \neq 0,\ \langle\gamma_j, \delta_j\rangle \text{ all different})$$

and let ϱ_1 be the rank of the matrix

$$\begin{bmatrix} \gamma_1-\gamma_0 & \dots & \gamma_k-\gamma_0 \\ \delta_1-\delta_0 & \dots & \delta_k-\delta_0 \end{bmatrix}.$$

It follows from (70) and (73) that

$$(81) \qquad \begin{aligned} &0 \leqslant \gamma_j \leqslant N(\mu_1+\nu_1) \leqslant 2NC_1(F), \\ &0 \leqslant \delta_j \leqslant N(\mu_2+\nu_2) \leqslant 2NC_1(F) \end{aligned} \qquad (0 \leqslant j \leqslant k)$$

and $\varrho_1 = 1$ or 2. If $\varrho_1 = 1$, we have

$$(82) \qquad F_1(y, z) = Jf(y^\gamma z^\delta),$$

where f is a polynomial in one variable, γ, δ are integers (cf. p. 21 and by (81)

$$(83) \qquad 0 < \max\{|\gamma|, |\delta|\} \leqslant 2NC_1(F).$$

$KF_1(x^u, x^v) = \text{const}$ implies $Kf(x^{\gamma u+\delta v}) = \text{const}$; thus $\gamma u + \delta v = 0$ or $Kf(x) = \text{const}$. In the first case, by (83)

$$(84) \qquad \max\{u, v\} \leqslant 2NC_1(F)(u, v);$$

in the second case by (76) $Jf(x) = \pm Jf(x^{-1})$ and by (82)

$$Jf(y^\gamma z^\delta) = F_1(y, z) = \pm JF_1(y^{-1}, z^{-1}).$$

The last equality implies by (73)

$$Jf(y^\gamma z^\delta) \mid \left(JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2}), JF(y^{-\nu_1}z^{-\nu_2}, y^{-\mu_1}z^{-\mu_2})\right).$$

By a substitution $y = \eta^{\mu_2}\zeta^{-\nu_2}$, $z = \eta^{-\mu_1}\zeta^{\nu_1}$ we get

$$(85) \qquad Jf(\eta^{\gamma\mu_2-\delta\mu_1}\zeta^{-\gamma\nu_2+\delta\nu_1}) \mid \left(JF(\eta^{|M|}, \zeta^{|M|}), JF(\eta^{-|M|}, \zeta^{-|M|})\right).$$

However $\left(JF(y, z), JF(y^{-1}, z^{-1})\right) = 1$, and thus

$$\left(JF(\eta^{|M|}, \zeta^{|M|}), JF(\eta^{-|M|}, \zeta^{-|M|})\right) = 1$$

and (85) implies

$$Jf(\eta^{\gamma\mu_2-\delta\mu_1}\zeta^{-\gamma\nu_2+\delta\nu_1}) = \text{const}.$$

Since by (82) $Jf(x) \neq \text{const}$, we get

$$\begin{aligned} \gamma\mu_2 - \delta\mu_1 &= 0, \\ -\gamma\nu_2 + \delta\nu_1 &= 0. \end{aligned}$$

Since

$$\begin{vmatrix} \mu_2 & -\mu_1 \\ -\nu_2 & \nu_1 \end{vmatrix} = |M| \neq 0,$$

the last system of equations gives $\gamma = \delta = 0$, against (83). The contradiction obtained proves (84).

If $\varrho_1 = 2$ we may assume without loss of generality that

$$\begin{vmatrix} \gamma_1-\gamma_0 & \gamma_2-\gamma_0 \\ \delta_1-\delta_0 & \delta_2-\delta_0 \end{vmatrix} \neq 0.$$

On the other hand, by (73)

$$\frac{JF_1(x^u, x^v)}{KF_1(x^u, x^v)} \,\Big|\, \frac{JF(x^n, x^m)}{KF(x^n, x^m)}$$

and since $KF_1(x^u, x^v) = \text{const}$, we get from (77)

$$JF_1(x^u, x^v) \mid (x^{(n,m)B_{00}} - 1)^{B_{00}}.$$

It follows by (80) that either

(86) $u\gamma_i+v\delta_i = u\gamma_j+v\delta_j$ for $i=1$ or 2 and some $j \leqslant k$

or

(87) $|u(\gamma_i-\gamma_0)+v(\delta_i-\delta_0)| \leqslant B_{00}^2(n, m)$ $(i=1, 2)$.

(81) and (86) imply

(88) $$\max\{u, v\} \leqslant 2NC_1(F)(u, v),$$

(81) and (87) imply

(89) $$\max\{u, v\} \leqslant 4NC_1(F)B_{00}^2(n, m).$$

In view of (72) it follows from (84), (88) and (89) that

$$\max\{n, m\} \leqslant C_0(F, M)(n, m).$$

2. Assume that $KF_1(x^u, x^v)$ is reducible. Let $f(x)$ be its irreducible primitive factor. Since by (71) and (73) $KF_1(x^u, x^v) \mid F(x^n, x^m)$, we have

(90) $$F(x^n, x^m) = f(x)g(x),$$

where $g(x)$ is a polynomial with integral coefficients. It follows from (75) that

$$\big(KF_1(x^u, x^v), KF(x^{-n}, x^{-m})\big) = 1 \quad \text{unless} \quad \max\{n, m\} \leqslant B_{01}(n, m),$$

whence by (90)

(91) $$f(x) = \operatorname{const}\big(KF_1(x^u, x^v), K[f(x)g(x^{-1})]\big)$$

or

(92) $$\max\{n, m\} \leqslant B_{01}(n, m).$$

In order to calculate the right-hand side of (91) we put

(93) $$f(x)g(x^{-1}) = \sum_{i=0}^{l} c_i x^{k_i} \quad (c_i \text{ integers} \neq 0,\ k_0 < k_1 < \ldots < k_l)$$

and consider two expressions for $F(x^n, x^m)F(x^{-n}, x^{-m})$:

(94)
$$F(x^n, x^m)F(x^{-n}, x^{-m}) = \sum_{i=0}^{I} a_i^2 + \sum_{\substack{0\leqslant i,j\leqslant I\\ i\neq j}} a_i a_j x^{na_j+m\beta_j-(na_i+m\beta_i)},$$
$$[f(x)g(x^{-1})][f(x^{-1})g(x)] = \sum_{i=0}^{l} c_i^2 + \sum_{\substack{0\leqslant i,j\leqslant l\\ i\neq j}} c_i c_j x^{k_j-k_i}.$$

If for any pair $\langle i, j\rangle$:

(95) $$i \neq j \quad \text{and} \quad na_j+m\beta_j-(na_i+m\beta_i) = 0,$$

we get $n(a_j-a_i)+m(\beta_j-\beta_i) = 0$, whence

(96) $$\max\{n, m\} \leqslant N(n, m).$$

Similarly, if for any pair $\langle i, j\rangle$

(97) $\langle i, j\rangle \neq \langle i', j'\rangle$ and $na_j+m\beta_j-(na_i+m\beta_i)$
$$= na_{j'}+m\beta_{j'}-(na_{i'}+m\beta_{i'})$$

or

(98) $\langle i, j\rangle \neq \langle i'', j''\rangle$ and $na_j+m\beta_j-(na_i+m\beta_i)$
$$= na_{j''}+m\beta_{j''}-(na_{i''}+m\beta_{i''}),$$

we get by the choice of $\langle i', j'\rangle$, $\langle i'', j''\rangle$ (p. 22) a linear homogeneous equation on m and n with non-zero coefficients absolutely $\leqslant 2N$, whence

(99) $$\max\{n, m\} \leqslant 2N(n, m).$$

If no pair $\langle i, j\rangle$ satisfies (95), (97) or (98), it follows from (94) that

(100) $$\sum_{i=0}^{l} c_i^2 = \sum_{i=0}^{I} a_i^2 = A,$$

(101) the numbers $na_{j'}+m\beta_{j'}-(na_{i'}+m\beta_{i'})$ and $na_{j''}+m\beta_{j''}-(na_{i''}+m\beta_{i''})$ appear among the differences k_j-k_i $(0 \leqslant i \leqslant l,\ 0 \leqslant j \leqslant l)$,

(102) each number k_j-k_i which appears only once in the double sequence k_j-k_i $(0 \leqslant i < j \leqslant l)$ has a value $n\gamma+m\delta$, where $|\gamma| \leqslant N$, $|\delta| \leqslant N$.

Let $k_{j_1}-k_{i_1}, k_{j_2}-k_{i_2}, \ldots, k_{j_P}-k_{i_P}$ $(P \geqslant 0)$ be all the numbers mentioned in (102) besides k_l-k_0.

If $P \geqslant 2$, $1 \leqslant p < q \leqslant P$, it follows from

$$k_l-k_0 = \gamma_0 n+\delta_0 m,$$
$$k_{j_p}-k_{i_p} = \gamma_p n+\delta_p m,$$
$$k_{j_q}-k_{i_q} = \gamma_q n+\delta_q m,$$

$$\varrho_{p,q} = \text{rank of } \begin{bmatrix}\gamma_0 & \delta_0\\ \gamma_p & \delta_p\\ \gamma_q & \delta_q\end{bmatrix},$$

that

$$c_{p,q}(k_l-k_0)+c'_{p,q}(k_{j_p}-k_{i_p})+c''_{p,q}(k_{j_q}-k_{i_q}) = 0,$$

where

$$[c_{p,q}, c'_{p,q}, c''_{p,q}] = \begin{cases}\left[\begin{vmatrix}\gamma_p & \delta_p\\ \gamma_q & \delta_q\end{vmatrix}, \begin{vmatrix}\gamma_q & \delta_q\\ \gamma_0 & \delta_0\end{vmatrix}, \begin{vmatrix}\gamma_0 & \delta_0\\ \gamma_p & \delta_p\end{vmatrix}\right] & \text{if } \varrho_{p,q} = 2\\ [\gamma_p, -\gamma_0, 0] & \text{if } \varrho_{p,q} = 1 \text{ and } \gamma_0 \neq 0,\\ [\delta_p, -\delta_0, 0] & \text{if } \varrho_{p,q} = 1 \text{ and } \delta_0 \neq 0.\end{cases}$$

Clearly

$$0 < \max\{|c_{pq}|, |c'_{pq}|, |c''_{pq}|\} \leqslant 2N^2 \quad (1 \leqslant p < q \leqslant P).$$

Therefore, the assumptions of Lemma 4 are satisfied with $c \leqslant 2N^2$ and we get from that lemma

$$k_i - k_0 = s\varkappa_i + t\lambda_i \quad (0 \leqslant i \leqslant l), \tag{103}$$

where s, t, $\varkappa_i$, λ_i $(0 \leqslant i \leqslant l)$ are integers, $|\varkappa_i| \leqslant (10N^2)^l$, $|\lambda_i| \leqslant (10N^2)^l$.

Since by (93) and (100) $l < A$, we have

$$|\varkappa_i| < (10N^2)^A, \quad |\lambda_i| < (10N^2)^A \quad (0 \leqslant i \leqslant l). \tag{104}$$

Now by (101), (103) and (104)

$$\begin{aligned} na_{j'} + m\beta_{j'} - (na_{i'} + m\beta_{i'}) &= \varkappa' s + \lambda' t, \\ na_{j''} + m\beta_{j''} - (na_{i''} + m\beta_{i''}) &= \varkappa'' s + \lambda'' t, \end{aligned} \tag{105}$$

where $\varkappa'$, λ', $\varkappa''$, λ'' are integers and

$$0 < \max\{|\varkappa'|, |\lambda'|\} < 2(10N^2)^A, \quad 0 < \max\{|\varkappa''|, |\lambda''|\} < 2(10N^2)^A. \tag{106}$$

($\varkappa' = \lambda' = 0$ or $\varkappa'' = \lambda'' = 0$ would imply (96)).

We put

$$\Delta = \begin{bmatrix} \varkappa' & \varkappa'' \\ \lambda' & \lambda'' \end{bmatrix}.$$

It follows from (69), (105) and (106) that

$$[n, m]\Gamma = [s, t]\Delta \quad \text{and} \quad h(\Delta) < 2(10N^2)^A = d. \tag{107}$$

We distinguish two cases, $|\Delta| = 0$ and $|\Delta| \neq 0$.

If $|\Delta| = 0$, let

$$|\Gamma|\Delta\Gamma^{-1} = \begin{bmatrix} \xi_1 & \eta_1 \\ \xi_2 & \eta_2 \end{bmatrix}$$

(by the choice of Γ, Γ^{-1} exists). It follows from (106) that

$$0 < \max\{|\xi_1|, |\eta_1|\} \leqslant 2h(\Delta)h(\Gamma) < 4 \cdot 10^A N^{2A+1}. \tag{108}$$

On the other hand, since $\xi_1\eta_2 - \eta_1\xi_2 = 0$, we get from (107) $\xi_1 m - \eta_1 n = 0$, and thus by (108)

$$\max\{n, m\}/(n, m) < 4 \cdot 10^A N^{2A+1} < C_1(F). \tag{109}$$

If $|\Delta| \neq 0$, we can apply to (107) the last statement of Lemma 5. In virtue of that statement there exists an integral matrix T such that

$$[s, t] = [u, v]T \tag{110}$$

and

$$h(T) \leqslant 8 \cdot 10^A N^{2A+1}\big((8 \cdot 10^{2A} N^{4A})!\big)^2 = 8 \cdot 10^A N^{2A+1} C_1(F). \tag{111}$$

Put

$$T\begin{bmatrix} \varkappa_i \\ \lambda_i \end{bmatrix} = \begin{bmatrix} \sigma_i \\ \tau_i \end{bmatrix} \quad (0 \leqslant i \leqslant l), \tag{112}$$

$$H(y, z) = J\sum_{i=0}^{l} c_i y^{\sigma_i} z^{\tau_i}. \tag{113}$$

We have by (103) and (110)

$$k_i - k_0 = u\sigma_i + v\tau_i \quad (0 \leqslant i \leqslant l);$$

thus by (93), (113) and (91)

$$K\big(f(x)g(x^{-1})\big) = K\sum_{i=0}^{l} c_i x^{k_i - k_0} = KH(x^u, x^v),$$

$$f(x) = \text{const}\big(KF_1(x^u, x^v), KH(x^u, x^v)\big). \tag{114}$$

If we had $F_1 \mid H$, it would imply $KF_1(x^u, x^v) \mid KH(x^u, x^v)$, whence $KF_1(x^u, x^v) \mid f(x)$, against the choice of $f(x)$. Thus $(F_1, H) = 1$. On the other hand, by (104), (111) and (112)

$$\max\{|\sigma_i|, |\tau_i|\} \leqslant 16 \cdot 10^{2A} N^{4A+1} C_1(F) \quad (0 \leqslant i \leqslant l);$$

thus by (100), (113) and the choice of S_1 (p. 23), $H \in S_1$. It follows by (78) that

$$\big(KF_1(x^u, x^v), KH(x^u, x^v)\big) = 1$$

or

$$\max\{u, v\}/(u, v) \leqslant B_1(F_1, H) \leqslant \max_{H \in S_1} B_1(F_1, H). \tag{115}$$

A comparison with (114) shows that (115) holds. In view of (72) it follows from (92), (96), (99), (109) and (115) that

$$\max\{n, m\} \leqslant C_0(F, M)(n, m).$$

The proof is complete.

§ 5. Proof of Theorem 3. Put in Theorem 2 $F(y, z) = ay + bz + c$. Since $c \neq 0$ we have $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$; thus the assumptions of the theorem are satisfied and the constant $C_0(ay + bz + c)$ exists. Put

$$\begin{aligned} A(a, b, c) &= C_0(ay + bz + c), \\ B(a, b, c) &= A(a, b, c) \max_{(\alpha,\beta) \in S, \alpha > \beta} C'(ax^\alpha + bx^\beta + c), \end{aligned} \tag{116}$$

where C' is a constant from the Corollary to Theorem 1 and S consists of all pairs of relatively prime positive integers $\leqslant A(a, b, c)$.

Now, assume that n, m are positive integers, $n > m$ and $K(ax^n+bx^m+c)$ is reducible. Let

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

be an integral non-singular matrix whose existence for F, n, m is asserted in Theorem 2.

Without loss of generality we may assume that $|M| > 0$. It follows from part (iii) of Theorem 2 that if $K(ax^n+bx^m+c)$ is reducible then either $J(ay^{\nu_1}z^{\nu_2}+by^{\mu_1}z^{\mu_2}+c)$ is reducible or

$$n/(n, m) \leqslant C_0(F) = A(a, b, c). \tag{117}$$

We prove that the former eventuality is impossible. Suppose that

$$J(ay^{\nu_1}z^{\nu_2}+by^{\mu_1}z^{\mu_2}+c) = G_1(y, z)G_2(y, z), \tag{118}$$

where G_1, G_2 are polynomials. By a substitution $y = \eta^{\mu_2}\zeta^{-\nu_2}$, $z = \eta^{-\mu_1}\zeta^{\nu_1}$ we get

$$J(a\eta^{|M|}+b\zeta^{|M|}+c) = JG_1(\eta^{\mu_2}\zeta^{-\nu_2}, \eta^{-\mu_1}\zeta^{\nu_1})JG_2(\eta^{\mu_2}\zeta^{-\nu_2}, \eta^{-\mu_1}\zeta^{\nu_1}).$$

However,

$$J(a\eta^{|M|}+b\zeta^{|M|}+c) = a\eta^{|M|}+b\zeta^{|M|}+c = a\eta^{|M|}+D(\zeta)$$

is irreducible by the theorem of Capelli applied to the binomial $a|\eta|^M+D(\zeta)$ in the function field $Q(\zeta)$; in fact, $\pm D(\zeta)$ is not a power of any element of $Q(\zeta)$ with exponent > 1. It follows that

$$JG_i(\eta^{\mu_2}\zeta^{-\nu_2}, \eta^{-\mu_1}\zeta^{\nu_1}) = \text{const}, \quad i = 1 \text{ or } 2,$$

whence by a substitution $\eta = Y^{\nu_1}Z^{\nu_2}$, $\zeta = Y^{\mu_1}Z^{\mu_2}$

$$JG_i(Y^{|M|}, Z^{|M|}) = \text{const}, \quad i = 1 \text{ or } 2.$$

Since $|M| \neq 0$ and by (118) $G_i(0, 0) \neq 0$, we get $G_i(y, z) = \text{const}$ ($i = 1$ or 2). This shows that $J(ay^{\nu_1}z^{\nu_2}+by^{\mu_1}z^{\mu_2}+c)$ is irreducible and consequently (117) holds. Part (i) of Theorem 3 is thus proved.

In order to prove part (ii) we notice that by the Corollary to Theorem 1 there exists an integer δ satisfying the following conditions:

$$0 < \delta \leqslant C'(ax^{n/(n,m)}+bx^{m/(n,m)}+c); \quad (n, m) = \delta u, \ u \text{ integer}; \tag{119}$$

if

$$K(ax^{n\delta/(n,m)}+bx^{m\delta/(n,m)}+c) = \text{const}\,F_1(x)^{e_1}F_2(x)^{e_2}\dots F_r(x)^{e_r}$$

is a standard form of $K(ax^{n\delta/(n,m)}+bx^{m\delta/(n,m)}+c)$, then

$$K(ax^n+bx^m+c) = \text{const}\,F_1(x^u)^{e_1}F_2(x^u)^{e_2}\dots F_r(x^u)^{e_r}$$

is a standard form of $K(ax^n+bx^m+c)$. We put $\nu = n\delta/(n, m)$, $\mu = m\delta/(n, m)$.

Clearly $n/\nu = m/\mu$ is integral. Further by (117) and the definition of S: $\langle n/(n, m), m/(n, m)\rangle \in S$, and thus by (116) and (119)

$$\nu \leqslant A(a, b, c)\delta \leqslant B(a, b, c).$$

This completes the proof.

§ 6. Proof of Theorem 4. Put $(ax^n+bx^m+c)/K(ax^n+bx^m+c) = g(x)$. Clearly $g(x) \mid ax^n+bx^m+c$ and $g(x) \mid cx^n+bx^{n-m}+a$, whence

$$g(x) \mid (cx^n+a)(ax^n+bx^m+c)-bx^m(cx^n+bx^{n-m}+a) = ac\left(x^{2n}+\frac{a^2+c^2-b^2}{ac}x^n+1\right), \tag{120}$$

$$g(x) \mid (cx^m+b)(ax^n+bx^m+c)-ax^m(cx^n+bx^{n-m}+a) = bc\left(x^{2m}+\frac{b^2+c^2-a^2}{bc}x^m+1\right).$$

If $g(x) \neq 1$, it follows that

$$x^2+\frac{a^2+c^2-b^2}{ac}x+1 \neq K\left(x^2+\frac{a^2+c^2-b^2}{ac}x+1\right),$$

$$x^2+\frac{b^2+c^2-a^2}{bc}x+1 \neq K\left(x^2+\frac{b^2+c^2-a^2}{bc}x+1\right).$$

On the other hand, the only monic reciprocal quadratic polynomials which have roots of unity as zeros are x^2+1, $x^2\pm x+1$, $x^2\pm 2x+1$. It follows that $a^2+c^2-b^2 = \varepsilon rac$, $b^2+c^2-a^2 = \eta sbc$, where $|\varepsilon| = |\eta| = 1$; $r = 0, 1$ or 2; $s = 0, 1$ or 2. Hence

$$2c^2 = \varepsilon rac+\eta sbc, \quad 2a^2-2b^2 = \varepsilon rac-\eta sbc;$$

$$2c = \varepsilon ra+\eta sb; \quad 4a^2-4b^2 = (\varepsilon ra)^2-(\eta sb)^2,$$

and

$$a^2(4-(\varepsilon r)^2) = b^2(4-(\eta s)^2).$$

The last equality implies $(\varepsilon r)^2 = (\eta s)^2$, and thus $r = s$. Since $c \neq 0$, it is impossible that $s = r = 0$; thus two cases remain:

$$r = s = 1, \quad a^2 = b^2, \quad c = \varepsilon a = \eta b; \tag{121}$$

$$r = s = 2, \quad c = \varepsilon a+\eta b. \tag{122}$$

In the first case, by (120)

$$g(x) \mid x^{2n}+\varepsilon x^n+1,$$

and since all zeros of $x^{2n}+\varepsilon x^n+1$ are roots of unity

$$g(x) = (ax^n+bx^m+c, x^{2n}+\varepsilon x^n+1).$$

On the other hand, by (121)

$$c(x^{2n}+\varepsilon x^n+1)x^m = \eta(ax^n+bx^m+c)+c(x^{m+n}-\varepsilon\eta)(x^n+\varepsilon)$$

and since $(x^{2n}+\varepsilon x^n+1, x^n+\varepsilon) = 1$, it follows that

$$g(x) = (ax^n+bx^m+c, x^{2n}+\varepsilon x^n+1) = (x^{2n}+\varepsilon x^n+1, x^{m+n}-\varepsilon\eta).$$

In the second case, by (120)

$$g(x) \mid x^{2n}+2\varepsilon x^n+1 = (x^n+\varepsilon)^2,$$

and since all zeros of $x^n+\varepsilon$ are roots of unity,

$$g(x) = \left(ax^n+bx^m+c, (x^n+\varepsilon)^2\right).$$

On the other hand, by (122)

$$ax^n+bx^m+c = a(x^n+\varepsilon)+b(x^m+\eta),$$

and every multiple factor of ax^n+bx^m+c divides

$$nax^n+bmx^m = na(x^n+\varepsilon)+mb(x^m+\eta)-(an\varepsilon+bm\eta).$$

It follows that in the second case

$$g(x) = \begin{cases} (x^n+\varepsilon, x^m+\eta)^2 & \text{if} \quad an\varepsilon+bm\eta = 0, \\ (x^n+\varepsilon, x^m+\eta) & \text{if} \quad an\varepsilon+bm\eta \neq 0. \end{cases}$$

In order to complete the proof it remains to calculate

$$(x^{2n}+\varepsilon x^n+1, x^{m+n}-\varepsilon\eta) \quad \text{and} \quad (x^n+\varepsilon, x^m+\eta).$$

This is easily done by factorization in cyclotomic fields (cf. [1], p. 69).

§ 7. Proof of Theorem 5. Put in Theorem 2 $F(y,z) = y+f(z)$. Since $f(z) \neq \pm 1$ and $f(0) \neq 0$, $JF(y,z) \neq \pm JF(y^{-1}, z^{-1})$, and thus the assumptions of the theorem are satisfied and the constants $C_0(y+f(z))$, $C_1(y+f(z))$ exist. We put

$D_0(f) = \max\{C_0(y+f(z)), C_1(y+f(z))\}$,

$D_1(f)$ = the greatest common divisor of multiplicities of all the zeros of $f(z)$.

By Theorem 2 for every n there exists an integral matrix

$$\begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the following conditions

(123) $$0 \leqslant \nu_i \leqslant C_1(y+f(z)), \quad 0 \leqslant \mu_i \leqslant C_1(y+f(z)) \quad (i = 1, 2),$$

(124) $$n = \nu_1 u+\nu_2 v, \quad 1 = \mu_1 u+\mu_2 v, \ u, v \text{ integers} \geqslant 0;$$

(125) if $K(x^n+f(x))$ is reducible, then either $J(y^{\nu_1}z^{\nu_2}+f(y^{\mu_1}z^{\mu_2}))$ is reducible or

$$n = \max(n,1)/(n,1) \leqslant C_0(y+f(z)) \leqslant D_0(f).$$

It follows from (123) and (124) that $\mu_1 u = 0$, $\mu_2 v = 1$ or $\mu_1 u = 1$, $\mu_2 v = 0$. In view of symmetry it is enough to consider the first possibility. We then have $\mu_2 = v = 1$ and $u = 0$ or $\mu_1 = 0$. If $u = 0$, then

(126) $$n = \nu_2 \leqslant C_1(y+f(z)) \leqslant D_0(f).$$

If $\mu_1 = 0$, then

$$J(y^{\nu_1}z^{\nu_2}+f(y^{\mu_1}z^{\mu_2})) = y^{\nu_1}z^{\nu_2}+f(z).$$

By the theorem of Capelli applied to the binomial $y^{\nu_1}+z^{-\nu_2}f(z)$ in the function field $Q(z)$, $y^{\nu_1}z^{\nu_2}+f(z)$ is reducible only if $-z^{-\nu_2}f(z) = g(z)^p$ and $p \mid \nu_1$ or $z^{-\nu_2}f(z) = 4g(z)^4$ and $4 \mid \nu_1$, where $g(z)$ is a rational function and p is a prime. Since $f(0) \neq 0$, it follows that for some prime p

$$p \mid D_1(f), \quad p \mid \nu_1 \quad \text{and} \quad p \mid \nu_2.$$

By (124), this implies

(127) $$(n, D_1(f)) \neq 1.$$

Therefore, if $K(x^n+f(x))$ is reducible, at least one of the inequalities (125), (126) and (127) is satisfied. This completes the proof.

Note added in proof. 1. H. Zassenhaus and the writer have proved (cf. Michigan Math. Journ. 12 (1965)) the following improvement of inequality (4): $\max_{1 \leqslant i \leqslant N} |\beta^{(i)}| > 1+2^{-N-4}$. Hence inequality (1) can be improved as follows:

$$e(a, \Omega) \leqslant (2^{N+4}+1)\log(NH(a)).$$

2. E. G. Straus has proved the equality $\varrho = \varrho_0$ conjectured on p. 15. His general proof (to appear in the next issue of Acta Arith.) specialized to the case $\varrho_0 = 2$ would lead also to a simpler proof of Lemma 4 than that given in the present paper.

References

[1] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8 (1960), pp. 65-70.

[2] J. Mikusiński et A. Schinzel, *Sur la réductibilité de certains trinômes*, Acta Arith. 9 (1964), pp. 91-96.

[3] A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives des nombres irrationnels*, Colloq. Math. 9 (1962), pp. 291-296, *Correction*, ibid. 12 (1964), p. 289.

[4] A. Schinzel, *Some unsolved problems on polynomials*, Matematička Biblioteka 25 (1963), pp. 63-70.

[5] N. Tschebotaröw und H. Schwerdtfeger, *Grundzüge der Galoischen Theorie*, Groningen-Djakarta 1950.

Reçu par la Rédaction le 21. 2. 1964

ACTA ARITHMETICA
XI (1965)

Primes, polynomials and almost primes

by

R. J. Miech (Urbana, Ill.)

A set of almost primes is a set of integers each of which contains no more than a fixed number of prime factors. An integral valued polynomial $F(n)$ which is of degree h and which has k irreducible factors, for example, will generate a sequence of almost primes, the bound being approximately $(9h/5+k\log k)$, [3]. I propose to show that the sequence $\{F(p)\}$, where p is a prime, contains an infinite subsequence of almost primes. To be specific, I shall prove:

THEOREM. *Let $F(n)$ be an integral valued polynomial. Let K be any integer and let c be any integer which is relatively prime to K. Then there is a constant A which depends on the polynomial $F(n)$ such that there are an infinite number of primes p congruent to c modulo K for which $F(p)$ has at most A prime factors, multiple prime factors being counted multiply.*

The constant A of the conclusion of the theorem is not readily computable.

Several comments regarding assumptions and notational devices are in order. First of all, we shall assume without loss of generality that $F(n)$ has a non-zero constant term, for if n^L is the highest power of n dividing $F(n)$ we can apply our theorem to the polynomial $F(n)/n^L$ and replace A by $A+L$ to get the same general result. Secondly, we shall suppose that $F(n)$ has k distinct irreducible factors. Finally, the letter p will always denote a prime.

The Theorem will be proved by a main-term versus remainder-term type of argument. We shall actually prove that there is an integer H which is a multiple of K and a positive constant B which depends on the polynomial $F(n)$ and the integers H and c such that there are

$$Bx(\log x)^{-k-2}+O\big(x(\log x)^{-k-3}\big)$$

primes p congruent to c modulo H which do not exceed x for which $F(p)$ has at most A prime factors. We shall use Brun's method [1] to obtain the main term and then use of result of Renyi's [5] on the distribution of the zeros of the L-series to evaluate the error term. This paper is accordingly divided into three sections: the main term is developed in the first,