ACTA ARITHMETICA
XXXII (1977)

Abelian binomials, power residues and exponential congruences*

by

A. Schinzel (Warszawa)

In memory of Marceli Stark

This paper supplements the results of [6] concerning power residues and extends those pertaining to exponential congruences. We begin however with the study of binomials. G. Darbi [1] and E. Bessel-Hagen (cf. [10], p. 302) have found all binomials $x^n - a$ normal over the rational field Q. (Their argument extends to fields K such that a primitive nth root of unity ζ_n is of degree $\varphi(n)$ over K.) We shall do the same for an arbitrary field and n equal to a prime power. In fact, we shall prove

Theorem 1. *Let K be a field, p a prime different from the characteristic of K. A binomial $x^{p^\nu} - a$ is the product of factors normal over K if and only if at least one of the following conditions is satisfied for a suitable integer λ and a suitable $\gamma \in K$:*

(i) $a^{p^{\min(\omega,\nu)}} = \gamma^{p^\nu}$;

(ii) $p = 2,\ \omega = 1,\ \nu \leqslant \tau,\ a = -\gamma^2$;

(iii) $p = 2,\ \omega = 1,\ \nu = \tau+1,\ a = -\gamma^2,\ \sqrt{-(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)} \in K$;

(iv) $p = 2,\ \omega = 1,\ \nu = \tau+1,\ a = -(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{2^\lambda}\gamma^{2^{\lambda+1}},\ 1 \leqslant \lambda \leqslant \tau-2$;

(v) $p = 2,\ \omega = 1,\ \nu \geqslant \tau+2,\ a = -(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{2^{\nu-2}}\gamma^{2^{\nu-1}}$.

Here ω is the greatest integer such that $\zeta_{p^\omega} \in K$ if there are only finitely many of them, $\omega = \infty$ otherwise; τ is the greatest integer such that $\zeta_{2^\tau}+\zeta_{2^\tau}^{-1} \in K$ if there are only finitely many of them, $\tau = \infty$ otherwise.

If the binomial in question is irreducible (iv) *implies* $\tau \geqslant 3$, $\sqrt{-(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)} \notin K$, $\lambda = 1$; (v) *implies* $\tau = 2$.

Theorem 2. *Let n be a positive integer not divisible by the characteristic of K. A binomial $x^n - a$ has over K an abelian Galois group if and only if $a^{w_n} = \gamma^n$, where $\gamma \in K$ and w_n is the number of n-th roots of unity contained in K. When a binomial satisfying this condition is irreducible then its group*

* Written within the Research Program I.1.

is cyclic if $n \not\equiv 0 \bmod 4$ *or* $\zeta_4 \in K$ *and the product of cyclic groups of order* 2 *and* $n/2$ *otherwise.*

From Theorem 2 and a result of Hasse [2] concerning the case $n = p^\nu$ we shall deduce

THEOREM 3. *Let* n *be a positive integer not divisible by the characterictic of* K. *If*

$$\alpha = \vartheta^n, \quad \vartheta \in K(\zeta_n)$$

then

$$\alpha^\sigma = \gamma^n, \quad \gamma \in K,$$

where

(vi) $\sigma = \left(w_n, \text{ l.c.m.}_{\substack{q \mid n \\ q \text{ prime or } q=4}} [K(\zeta_q) : K]\right)$.

Moreover if for a certain m *prime to* n

(vii) $$\begin{cases} \text{either } \zeta_{(4,n)} \in K \text{ and } nm \equiv 0 \bmod w_n \text{l.c.m.}_{\substack{q \mid n \\ q \text{ prime}}} [K(\zeta_q) : K] \\ \text{or } \zeta_{(4,n)} \notin K, \ \tau < \infty \text{ and } nm \equiv 0 \bmod 2^\tau w_n \text{l.c.m.}_{\substack{q \mid n \\ q \text{ prime}}} [K(\zeta_q) : K] \end{cases}$$

then

$$\alpha = \gamma^{n/\sigma}, \quad \gamma \in K.$$

Next we shall assume that K is an algebraic number field and prove the following extension of Kummer's theorem (see [3], Satz 152) on power residues.

THEOREM 4. *Let* K *be an algebraic number field,* w *the number of roots of unity contained in* K, σ *given by* (vi). *If* $\alpha_1, \ldots, \alpha_k \in K$ *are such that*

(viii) $\alpha_1^{\sigma x_1} \ldots \alpha_k^{\sigma x_k} = \gamma^n$, $\gamma \in K$ *implies* $x_1 \equiv x_2 \ldots \equiv x_k \equiv 0 \bmod n/\sigma$

then for any integers $c_1, \ldots, c_k \equiv 0 \bmod \sigma$ *there exist infinitely many prime ideals* $\mathfrak{p}$ *of* $K(\zeta_n)$ *such that*

$$\left(\frac{\alpha_i}{\mathfrak{p}}\right)_n = \zeta_n^{c_i}.$$

If $\alpha_1, \ldots, \alpha_k$ *satisfy the stronger condition that*

(ix) $\zeta_w^{x_0} \alpha_1^{x_1} \ldots \alpha_k^{x_k} = \gamma^{n/\sigma}$ *implies* $x_1 \equiv x_2 \equiv \ldots \equiv x_k \equiv 0 \bmod n/\sigma$

and n *satisfies the condition* (vii) *of Theorem* 3 *then for any integers* $c_1, \ldots, c_k \equiv 0 \bmod \sigma$ *and any* c_0 *there exist infinitely many prime ideals* $\mathfrak{p}$ *of* $K(\zeta_n)$ *such that*

$$\left(\frac{\zeta_w}{\mathfrak{p}}\right)_n = \zeta_{(w,n)}^{c_0}, \quad \left(\frac{\alpha_i}{\mathfrak{p}}\right)_n = \zeta_n^{c_i}.$$

If $n = p^\nu$, p prime and $p > 2$ or $\nu = 1$ or $w \equiv 0 \bmod 4$ then the assertion holds without any restriction on c_i. Thus, for $n = p$, $\nu = 1$ we obtain Čebotarev's refinement [9] of Kummer's theorem. For $K = Q$ and n arbitrary a more precise result has been obtained by Mills [5].

We shall use Theorem 4 to prove two theorems on exponential congruences.

THEOREM 5. *Let* $f(x)$ *be a polynomial of degree* g *over* K, $\alpha_1, \ldots, \alpha_k \in K^*$. *If the congruence*

$$f(\alpha_1^{x_1} \ldots \alpha_k^{x_k}) \equiv 0 \bmod \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ *of* K *then the equation* $f(\alpha_1^{x_1} \ldots \alpha_k^{x_k}) = 0$ *is soluble in rational numbers* $x_1, \ldots, x_k$ *with the least common denominator not exceeding* $\max\{1, g-1\}$.

This is a generalization of Theorem 2 of [6] and the examples which we give further show that it is essentially best possible.

COROLLARY. *Let a sequence* u_n *of rational integers satisfy the recurrence relation* $u_{n+1} = au_n + bu_{n-1}$, *where* $a^2 + 4b \neq 0$. *If the congruence* $u_n \equiv c \bmod p$ *is soluble for almost all primes* p *and either* $b = 0, -1$ *or* $b = 1$, $a \neq d^3 + 3d$ (d *integer*), *then* $c = u_m$ *for an integer* m.

Here as in Theorem 5 almost all means all except a set of density zero.

It is conjectured that the Corollary holds for all recurring series of the second order satisfying $a^2 + 4b \neq 0$.

THEOREM 6. *Let* α_{hij}, β_{hi} *be non-zero elements of* K, D *a positive integer. If the system of congruences*

$$\prod_{h=1}^{g_i} \left(\prod_{j=1}^{k} \alpha_{hij}^{x_j} - \beta_{hi} \right) \equiv 0 \bmod \mathfrak{m} \qquad (i = 1, 2, \ldots, l)$$

is soluble for all moduli prime to D *then the corresponding system of equations is soluble in integers.*

This is a generalization of Theorem 3 of [6]. According to Skolem's conjecture Theorem 6 with $D = 1$ remains valid if

$$\prod_{h=1}^{g_i} \left(\prod_{j=1}^{k} \alpha_{hij}^{x_j} - \beta_{hi} \right)$$

is replaced by

$$\sum_{h=1}^{g_i} \beta_{hi} \prod_{j=1}^{k} \alpha_{hij}^{x_j},$$

but that we cannot prove.

LEMMA 1. *If p is a prime different from the characteristic of K, $\zeta_p \in K$, $\xi^{p^\mu} \in K^*$, $\eta^{p^\nu} \in K^*\langle\xi\rangle$ and $\eta \in K(\xi)$ then either $\eta \in K^*\langle\xi\rangle$ or $p = 2$, $\zeta_4 \notin K$ and $\zeta_4 \in K^*\langle\xi\rangle$. $K^*\langle\xi\rangle$ is the multiplicative group generated by K^* and ξ.*

Proof. For $p > 2$ this is an easy consequence of a theorem of Kneser [4] since however for $p = 2$ we have to go through Kneser's proof all over again, we can cover at once the general case. The proof is by induction with respect to μ and ν. If $\mu = 0$ or $\nu = 0$ the lemma is obvious. Assume it is true for $\mu = m-1$ and all ν. We prove it first for $\mu = m$, $\nu = 1$.

Suppose that $\xi \in K(\xi^p)$. Then using the inductive assumption with $\xi_1 = \xi^p$, $\eta_1 = \xi$, $\nu_1 = 1$ we get either $\xi \in K\langle\xi^p\rangle$ or $p = 2$, $\zeta_4 \notin K$ and $\zeta_4 \in K\langle\xi^2\rangle$. The former possibility gives $\xi \in K$, the latter $\zeta_4 \in K\langle\xi\rangle$, thus is this case lemma holds.

Suppose now that $\xi \notin K(\xi^p)$. Then also $\xi\zeta_p \notin K(\xi^p)$, ξ satisfies over $K(\xi^p)$ the irreducible equation $x^p - \xi^p = 0$ and denoting by N the norm from $K(\xi)$ to $K(\xi^p)$ we have

$$N\xi = (-1)^{p-1}\xi^p.$$

On the other hand, $\eta^p \in K^*\langle\xi\rangle$, hence $\eta^p = a\xi^{pk+q}$, where $0 \leqslant q < p$, $a \in K$. Consider first the case $q > 0$. Taking norms of both sides we get

$$\left((-1)^{p-1}\xi^p\right)^q = (N\eta)^p a^{-p}\xi^{-p^2k}.$$

For $p > 2$ it follows that $\xi^p \in K(\xi^p)^p$ and $\xi \in K(\xi)^p$ which has been excluded. For $p = 2$ we get

$$-\xi^2 = (N\eta)^2 a^{-2}\xi^{-4k}, \qquad \zeta_4\xi \in K(\xi^2), \qquad \eta^2 = \pm\zeta_4 N(\eta)$$

hence $\zeta_4 \in K(\xi)$, $\zeta_4 \notin K(\xi)^2$. Writing $\eta = g + \zeta_4 h$ with $g, h \in K(\xi^2)$ we obtain $g^2 = h^2$, $\eta = (1 \pm \zeta_4)g$. Hence $g^4 = -\eta^4/4 \in K\langle\xi^2\rangle$ and by the inductive assumption with $\xi_1 = \xi^2$, $\eta_1 = g$, $\nu_1 = 2$ we infer that $g \in K\langle\xi^2\rangle$, $\zeta_4 = \pm\frac{1}{2}\eta^2 g^{-2} \in K\langle\xi\rangle$.

Consider now the case $q = 0$. Let S be an automorphism of the normal closure of $K(\xi)$ over $K(\xi^p)$ such that $S\xi = \xi\zeta_p$. From $q = 0$ we infer that $\eta^p \in K^*(\xi^p)$, $S\eta^p = \eta^p$, $S\eta = \zeta_p^r\eta$. It follows that $S(\eta\xi^{-r}) = \eta\xi^{-r}$, $\eta\xi^{-r} \in K(\xi^p)$. Since $\eta^p\xi^{-rp} \in K\langle\xi^p\rangle$, we apply the inductive assumption with $\xi_1 = \xi^p$, $\eta_1 = \eta\xi^{-r}$, $\nu = 1$ and obtain that $\eta\xi^{-r} \in K\langle\xi^p\rangle$ or $p = 2$, $\zeta_4 \in K\langle\xi^2\rangle$. The former possibility gives $\eta \in K\langle\xi\rangle$ and the proof for $\mu = m$, $\nu = 1$ is complete. Assume now that $n \geqslant 2$, the lemma holds for $\mu = m$, $\nu < n$ and that $\eta^{2^n} \in K\langle\xi\rangle$. Using the inductive assumption with $\eta_1 = \eta^2$, $\nu = n-1$, we get $\eta^2 \in K\langle\xi\rangle$ or $\zeta_4 \in K\langle\xi\rangle$. In the former case we use the inductive assumption with $\nu_1 = 1$ and obtain $\eta \in K\langle\xi\rangle$, which completes the inductive proof.

LEMMA 2. *Let K be a field of characteristic different from 2. If $\vartheta \in K(\zeta_4)$, $\vartheta^{2^\nu} \in K$ then at least one of the following four conditions is satisfied for a suitable $\gamma \in K$*

$$\vartheta^{2^\nu} = \gamma^{2^\nu}; \tag{1}$$

$$\nu < \tau, \qquad \vartheta^{2^\nu} = -\gamma^{2^\nu}; \tag{2}$$

$$\nu = \tau, \qquad \vartheta^{2^\nu} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\tau-1}}\gamma^{2^\nu}; \tag{3}$$

$$\nu > \tau, \qquad \vartheta^{2^\nu} = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\nu-1}}\gamma^{2^\nu}. \tag{4}$$

Proof. This is a special case, $n = 2^\nu$ of Lemma 7 of [6]. Let us remark that the conditions (3) and (4) do not depend upon the choice of ζ_{2^τ}. Indeed, for any odd j

$$(\zeta_{2^{\tau+1}}^j + \zeta_{2^{\tau+1}}^{-j})(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1})^{-1} \in K,$$

hence

$$(\zeta_{2^{\tau+1}}^j + \zeta_{2^{\tau+1}}^{-j} + 2)^{2^{\nu-1}}(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1})^{-2^{\nu-1}} \in K^{2^\nu}.$$

(The same remark applies to the general case.)

LEMMA 3. *Let τ_1 be the greatest integer such that $\zeta_{2^{\tau_1}} \in K(\zeta_4)$, if there are only finitely many of them, $\tau_1 = \infty$ otherwise. Then*

$$\tau_1 = \begin{cases} \tau+1 & \text{if } \tau < \infty \text{ and } \sqrt{-(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)} \in K, \\ \tau & \text{otherwise.} \end{cases}$$

Proof. We have for all $\sigma \geqslant 2$

$$2\zeta_{2^\sigma} = (\zeta_{2^\sigma} + \zeta_{2^\sigma}^{-1}) + \zeta_4(\zeta_{2^\sigma}^{1-2^{\sigma-2}} + \zeta_{2^\sigma}^{-1+2^{\sigma-2}})$$

which implies $\tau_1 \geqslant \tau$. If we had $\tau < \infty$ and $\zeta_{2^{\tau+2}} \in K(\zeta_4)$ it would follow by Lemma 2 that

$$-1 = \zeta_{2^{\tau+2}}^{2^{\tau+1}} = \gamma^{2^{\tau+1}} \quad \text{or} \quad (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^\tau}\gamma^{2^{\tau+1}}, \qquad \gamma \in K,$$

hence $\zeta_4 \in K$ and $\zeta_{2^{\tau+2}} \in K$, $\zeta_{2^{\tau+2}} + \zeta_{2^{\tau+2}}^{-1} \in K$ contrary to the definition of τ. This proves $\tau_1 < \tau + 2$.

If $\zeta_{2^{\tau+1}} \in K(\zeta_4)$, then $\zeta_4 \notin K$ and ζ_{2^τ} is conjugate over K to $\zeta_{2^\tau}^{-1}$. Hence $\zeta_4\zeta_{2^{\tau+1}}$ is conjugate over K either to $\zeta_4\zeta_{2^{\tau+1}}^{-1}$ or to $-\zeta_4\zeta_{2^{\tau+1}}^{-1}$. However the latter possibility gives $\zeta_{2^{\tau+1}}^{1+2^{\tau-1}} + \zeta_{2^{\tau+1}}^{-1-2^{\tau-1}} \in K$ contrary to the definition of τ. Thus the former possibility holds and $\zeta_4\zeta_{2^{\tau+1}} + \zeta_4\zeta_{2^{\tau+1}}^{-1} \in K$, $\sqrt{-(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)} \in K$. Conversely if $\sqrt{-(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)} \in K$ then

$$\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1} \in K(\zeta_4) \quad \text{and} \quad \zeta_{2^{\tau+1}} = \frac{\zeta_{2^\tau} + 1}{\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}} \in K(\zeta_4).$$

This proves the lemma.

LEMMA 4. *If* $\xi^{p^\mu} = \beta \in K$, $\zeta_{p^\mu} \in K(\xi)$ *and either* $p > 2$, $\zeta_p \in K$ *or* $p = 2$, $\zeta_4 \in K$ *then*

$$\beta = \zeta_{p^\varkappa}^j \gamma^{p^{\mu-\varkappa}}, \quad 0 \leqslant \varkappa \leqslant \min(\mu, \omega), \quad (j, p) = 1, \quad \gamma \in K.$$

Proof. By Lemma 1 we have in any case

$$\zeta_{p^\mu} \in K^*\langle\xi\rangle,$$

$$\zeta_{p^\mu} = \delta\xi^i, \quad \delta \in K, \quad 1 \leqslant i \leqslant p^\mu. \tag{5}$$

Let

$$i = p^\varkappa h, \quad (h, p) = 1, \quad hj \equiv 1 \bmod p^{\mu-\varkappa}.$$

Raising both sides of (5) to the power $p^{\mu-\varkappa}j$ we get

$$\zeta_{p^\varkappa}^j = \delta^{p^{\mu-\varkappa}} \beta^{hj},$$

hence $\varkappa \leqslant \omega$ and the lemma holds with $\gamma = \beta^{(1-hj)p^{\varkappa-\mu}}\delta^{-1}$.

Proof of Theorem 1. Necessity. Assume that $x^{p^\nu} - a$ is the product of normal factors. Let μ be the least nonnegative integer such that

$$a = \beta^{p^{\nu-\mu}}, \quad \beta \in K.$$

If $\mu = 0$ then theorem holds with $\gamma = \beta^{\min(\nu,\omega)}$. If $\mu > 0$ then

$$\beta \neq \zeta_{p^{\nu-\mu}}^j \delta^p, \quad \delta \in K. \tag{6}$$

Hence if $p > 2$ or $p = 2$, $\zeta_4 \in K$ then $x^{p^\mu} - \beta$ is irreducible and by the assumption normal. Denoting any of its zeros by ξ we get

$$\zeta_{p^\mu} \in K(\xi), \quad \zeta_p \in K(\xi) \tag{7}$$

and since $[K(\xi) : K] = p^\mu$, $[K(\zeta_p) : K] \mid p-1$ it follows that $\zeta_p \in K$. By Lemma 4 we have

$$\beta = \zeta_{p^\varkappa}^j \gamma^{p^{\mu-\varkappa}}; \quad 0 \leqslant \varkappa \leqslant \min(\mu, \omega) \tag{8}$$

and $a^{p^\varkappa} = \gamma^{p^\nu}$, which proves (i).

Assume now that $p = 2$, $\zeta_4 \notin K$. Then either $x^{2^\mu} - \beta$ is irreducible or $\mu \geqslant 2$, $\beta = -4\delta^4$, $\delta \in K$. In the former case we get again (7) for any zero ξ of $x^{2^\mu} - \beta$, in the latter case let ϱ be the least nonnegative integer such that

$$(1+\zeta_4)\delta = \eta^{2^{\mu-2-\varrho}}, \quad \eta \in K(\zeta_4).$$

The binomial $x^{2^\varrho} - \eta$ is irreducible in $K(\zeta_4)$, hence

$$f(x) = N_{K(\zeta_4)/K}(x^{2^\varrho} - \eta)$$

is irreducible in K. $f(x)$ is a factor of

$$N_{K(\zeta_4)/K}(x^{2^{\mu-2}} - \eta^{2^{\mu-2-\varrho}}) = x^{2^\mu} + 2\delta x^{2^{\mu-2}} + 2\delta^2 \mid x^{2^\mu} + 4\delta^4,$$

hence it is normal. Let ξ be a zero of $x^{2^\varrho} - \eta$, ξ' a zero of $x^{2^\varrho} - \eta'$, where η' is conjugate to η over K. We have

$$\frac{\xi'}{\xi} \in K(\xi), \tag{9}$$

on the other hand

$$\left(\frac{\xi'}{\xi}\right)^{2^{\mu-\varrho}} = \left(\frac{\eta'}{\eta}\right)^{2^{\mu-2-\varrho}} = \frac{(1-\zeta_4)\delta}{(1+\zeta_4)\delta} = -\zeta_4,$$

hence $\frac{\xi'}{\xi} = \zeta_{2^\mu}^j$, $(j, 2) = 1$ and from (9) we get again (7). Using now Lemma 1 we get $\zeta_4 \in K^*\langle\xi\rangle$. Hence

$$\zeta_4 = \delta\xi^i, \quad \delta \in K, \tag{10}$$

$$2 = [K^*\langle\zeta_4\rangle : K^*] = [K^*\langle\xi^i\rangle : K^*] = 2^{\mu-\operatorname{ord}_2 i}, \quad i = 2^{\mu-1}j, \ (j, 2) = 1$$

and on squaring both sides of (10) we get

$$-1 = \delta^2\beta^j, \quad \beta = -\gamma^2.$$

It follows from (6) that $\mu = \nu$

$$a = \beta = -\gamma^2. \tag{11}$$

On the other hand, applying Lemma 4 to the field $K(\zeta_4)$ we get

$$a = \zeta_{2^\sigma}\vartheta^{2^{\nu-\sigma}}, \quad 0 \leqslant \sigma \leqslant \min(\nu, \tau_1), \quad \vartheta \in K(\zeta_4).$$

If $\nu \leqslant \tau_1$ we have by (11) and Lemma 3 (ii) or (iii). If $\nu > \tau_1$ then since $\zeta_4 \notin K$ by (11) and Lemma 2 $\sigma = 0$ is impossible. We get

$$a^{2^{\sigma-1}} = -\vartheta^{2^{\nu-1}}$$

and by Lemma 2 either

$$a^{2^{\sigma-1}} = -\gamma^{2^{\nu-1}}, \quad \gamma \in K \tag{12}$$

or

$$\nu - 1 = \tau = \tau_1, \quad a^{2^{\sigma-1}} = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{\tau-1}\gamma^{2^\tau} \tag{13}$$

or

$$\nu - 1 > \tau, \quad a^{2^{\sigma-1}} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{\nu-2}\gamma^{2^{\nu-1}}. \tag{14}$$

Since $\zeta_4 \notin K$, (12) and (14) imply $\sigma = 1$ and then we get (i) or (v) respectively. Finally (13) in view of (11) implies $\sigma > 1$

$$a = \pm(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\tau-\sigma}}\gamma^{2^{\tau-\sigma+1}},$$

again by (11) and Lemma 3, $\sigma < \tau$ and the upper sign is excluded. This gives (iv).

Sufficiency. To prove the sufficiency of (i) we proceed by induction with respect to ν. The case $\nu \leqslant \omega$ is trivial. If $\nu > \omega$ (i) gives

$$\alpha = \zeta_{p^\varkappa} \gamma^{p^{\nu-\omega}}, \quad 0 \leqslant \varkappa \leqslant \omega. \tag{15}$$

If $\varkappa < \omega$ we have

$$x^{p^\nu} - \alpha = \prod_{j=0}^{p-1} (x^{p^{\nu-1}} - \zeta_p^j \zeta_{p^{\varkappa+1}} \gamma^{p^{\nu-\omega-1}}).$$

Each of the factors on the right hand side is by the inductive assumption the product of normal factors, hence the same holds for $x^{p^\nu} - \alpha$. If $\varkappa = \omega = 0$ we have

$$x^{p^\nu} - \alpha = \alpha \prod_{\mu=0}^{\nu} X_{p^\mu}\left(\frac{x}{\gamma}\right),$$

where $X_n(x)$ is the nth cyclotomic polynomial. Every zero of $X_n\left(\frac{x}{\gamma}\right)$ generates over K all the other zeros, hence the desired result.

Finally if $\varkappa = \omega > 0$ let ξ denote as in the sequel any zero of $x^{p^\nu} - \alpha$.

We have by (15)

$$(\xi^{p^\omega} \gamma^{-1})^{p^{\nu-\omega}} = \zeta_{p^\omega}$$

hence

$$\zeta_{p^\nu} = (\xi^{p^\omega} \gamma^{-1})^j.$$

If (ii) or (iii) holds then

$$\zeta_4 = \pm \xi^{2^{\nu-1}} \gamma^{-1}.$$

Since by Lemma 3, $\nu \leqslant \tau_1$ and by definition $\zeta_{2^{\tau_1}} \in K(\zeta_4)$, it follows that

$$\zeta_{2^\nu} \in K(\xi).$$

If (iv) holds then

$$\xi^{2^{\tau-\lambda}} = \zeta_{2^{\lambda+2}}^j \gamma (\zeta_{2^{\tau+1}} + \zeta_{2^\tau}^{-1} + 1), \quad (j, 2) = 1$$

thus

$$\xi^{2^{\tau-\lambda}} \zeta_{2^{\tau+1}} \in K(\zeta_{2^\tau}), \quad \zeta_4 \in K(\xi^{2^\tau}).$$

Since by Lemma 3, $K(\zeta_{2^\tau}) = K(\zeta_4)$ it follows that

$$\xi^{2^{\tau-\lambda}} \zeta_{2^{\tau+1}} \in K(\xi^{2^\tau})$$

and

$$\zeta_{2^{\tau+1}} \in K(\xi).$$

If (v) holds then

$$\xi^2 = \zeta_{2^\nu}^j (\zeta_{2^{\tau+1}} + \zeta_{2^\tau}^{-1} + 1) \gamma, \quad (j, 2) = 1,$$

thus $\xi^2 \in K(\zeta_{2^\nu})$. We shall show that ξ^2 has as many distinct conjugates over K as ζ_{2^ν}. Indeed, if S is an automorphism of $K(\zeta_{2^\nu})$ over K then

$$S(\zeta_{2^{\tau+1}} + \zeta_{2^\tau}^{-1} + 1) = \pm (\zeta_{2^{\tau+1}} + \zeta_{2^\tau}^{-1} + 1).$$

Hence $S\xi^2 = \xi^2$ implies $S\zeta_{2^\nu}^j = \zeta_{2^\nu}^j$, $S\zeta_{2^\nu} = \zeta_{2^\nu}$ or

$$S\zeta_{2^\nu}^j = -\zeta_{2^\nu}^j, \quad S(\zeta_{2^{\tau+1}} + \zeta_{2^\tau}^{-1} + 1) = -(\zeta_{2^{\tau+1}} + \zeta_{2^\tau}^{-1} + 1).$$

The latter case is however impossible since $S\zeta_{2^{\tau+1}} = (S\zeta_{2^\nu})^{2^{\nu-\tau-1}}$. It follows that

$$\zeta_{2^\nu} \in K(\xi^2).$$

If the binomial $x^{p^\nu} - \alpha$ is irreducible then for $p = 2$, $\nu \geqslant 2$ we have $\alpha \neq -4\gamma^4$, hence for $\tau \geqslant 3$, $\alpha \neq -\gamma^4$, $\gamma \in K$. Thus (iv) implies $\tau \geqslant 3$, $\sqrt{-(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)} \notin K$, $\lambda = 1$; (v) implies $\tau = 2$.

Remark. Note that in case (i) if $\varkappa = \omega$ and in cases (ii)–(v) every root of $x^{p^\nu} - \alpha$ generates all the other.

LEMMA 5. *If a binomial $x^{p^\nu} - \alpha$ satisfies condition* (i) *then its Galois group G over K is abelian. If it is irreducible then G is cyclic unless $p = 2$, $\nu \geqslant 2$, $\omega = 1$, in which case G is of type $(2, 2^{\nu-1})$.*

If λ is the least nonnegative integer such that

$$\alpha = \zeta_{p^\varkappa} \gamma^{p^{\nu-\lambda}}, \quad 0 \leqslant \varkappa \leqslant \lambda \leqslant \omega, \quad \gamma \in K$$

then the Galois group of each irreducible factor of $x^{p^\nu} - \alpha$ contains an element of order p^λ and besides an element of order

$$p^{\nu-\omega+\varkappa} \quad \text{if} \quad \langle p, \omega \rangle \neq \langle 2, 1 \rangle \text{ and } \varkappa > \max\{0, \omega - \nu + \lambda\},$$

$$p^{\nu-\tau+1} \quad \text{if} \quad \langle p, \omega \rangle = \langle 2, 1 \rangle \text{ and } \varkappa = \lambda = 1 > \tau - \nu + 1.$$

Proof. We start by proving that an irreducible binomial satisfying (i) has a cyclic group G unless $p = 2$, $\nu \geqslant 2$, $\omega = 1$. Since it is irreducible we have either $\nu - \lambda = 0$ or $\varkappa = \omega = \lambda$. In the former case $\nu \leqslant \omega$; if ξ is any zero of $x^{p^\nu} - \alpha$ and S the substitution $\xi \to \zeta_{p^\nu} \xi$ we have $S^j(\xi) = \zeta_{p^\nu}^j \xi$ hence G is cyclic, generated by S. In the latter case let ξ be any zero of $x^{p^\nu} - \alpha$ satisfying

$$\xi^{p^\omega} = \zeta_{p^\nu} \gamma$$

and consider the substitution S: $\xi \to \zeta_{p^\nu} \xi$. We have

$$S(\zeta_{p^\nu}) = \zeta_{p^\nu}^{p^\omega + 1}, \quad S^j(\xi) = \zeta_{p^\nu}^{\sum_{i=0}^{j-1} (p^\omega+1)^i} \xi.$$

The order of S is the least j such that

$$\sum_{i=0}^{j-1} (p^\omega + 1)^i = \frac{(p^\omega+1)^j - 1}{p^\omega} \equiv 0 \bmod p^\nu. \tag{16}$$

However if $p>2$, $a\equiv 1 \bmod p$ or $p=2$, $a\equiv 1 \bmod 4$ we have

$$\operatorname{ord}_p(a^j-1)=\operatorname{ord}_p j+\operatorname{ord}_p(a-1) \tag{17}$$

(see [6], p. 401, formula (8)). Hence if $p>2$ or $p=2$, $\omega\geqslant 2$ (16) implies

$$\operatorname{ord}_p j\geqslant \nu$$

and S is of order p^ν. The same is clearly true for $p^\nu=2$.

The remaining assertions of the lemma are trivial for $\lambda=0$. If $\lambda>0$ we consider first the case $p>2$ or $p=2$, $\omega\geqslant 2$. If $\varkappa>\max\{0,\ \omega-\nu+\lambda\}$ we have the factorization

$$w^{p^\nu}-\alpha=\prod_{j=0}^{p^{\omega-\varkappa}-1}\left(w^{p^{\nu-\omega+\varkappa}}-\zeta_{p^\omega}^{j}\zeta_{p^\omega}\gamma^{p^{\nu-\lambda-\omega+\varkappa}}\right)$$

and the factors are irreducible since $\zeta_{p^{\omega+1}}\notin K$. By the fact already established the Galois groups are cyclic of order $p^{\nu-\omega+\varkappa}$ and since $\nu-\omega+\varkappa>\lambda$ contain also an element of order p^λ.

If $\varkappa\leqslant\omega-\nu+\lambda$ then

$$\alpha=\gamma_1^{p^{\nu-\lambda}},\qquad \gamma_1=\zeta_{p^{\varkappa+\nu-\lambda}}\gamma\in K.$$

We have the factorization

$$w^{p^\nu}-\alpha=\prod_{j=0}^{p^{\nu-\lambda}-1}\left(w^{p^\lambda}-\zeta_{p^{\nu-\lambda}}^{j}\gamma_1\right)$$

and the factors are irreducible, since $\zeta_{p^{\nu-\lambda}}^{j}\gamma_1=\gamma_2^{p}$, $\gamma_2\in K$ would imply

$$\alpha^{p^{\lambda-1}}=\gamma_2^{p^\nu}$$

contrary to the choice of λ. The Galois groups are cyclic of order p^λ.

If $\varkappa=0>\omega-\nu+\lambda$ we have the factorization

$$w^{p^\nu}-\alpha=\prod_{j=0}^{p^\omega-1}\left(w^{p^\lambda}-\zeta_{p^\omega}^{j}\gamma\right)\prod_{\mu=\lambda+1}^{\nu-\omega}\prod_{\substack{j=0\\(j,p)=1}}^{p^\omega-1}\left(w^{p^\mu}-\zeta_{p^\omega}^{j}\gamma^{p^{\mu-\lambda}}\right).$$

The factors of the first product are irreducible for the same reason as before, the other factors are irreducible since $\zeta_{p^{\omega+1}}\notin K$. The Galois groups are cyclic of order p^μ $(\lambda\leqslant\mu\leqslant\nu-\omega)$.

Consider now the case $p=2$, $\omega=\lambda=1$. Let τ_1 have the meaning of Lemma 3.

If $\varkappa=1>\tau-\nu+1$ we have $\nu\geqslant\tau+1\geqslant\tau_1$ and the factorization

$$w^{2^\nu}-\alpha=\prod_{\substack{j=1\\ j=1 \bmod 4}}^{2^{\tau_1}-1}N_{K(\zeta_4)/K}\left(w^{2^{\nu-\tau_1+1}}-\zeta_{2^{\tau_1}}^{j}\gamma^{2^{\nu-\tau_1}}\right).$$

If $f_j(w)=w^{2^{\nu-\tau_1+1}}-\zeta_{2^{\tau_1}}^{j}\gamma^{2^{\nu-\tau_1}}$ were reducible in $K(\zeta_4)$ then since $\zeta_{2^{\tau_1+1}}\notin K(\zeta_4)$ we would have $\nu=\tau_1=\tau+1$ and

$$\zeta_{2^{\tau_1}}^{j}\gamma=\vartheta^2,\qquad \vartheta\in K(\zeta_4),$$

whence $-\gamma^{2^\tau}=\vartheta^{2^{\tau+1}}$ contrary to Lemma 2. Thus $f_j(w)$ is irreducible in $K(\zeta_4)$ and $N_{K(\zeta_4)/K}f_j(w)=f_j(w)f_j'(w)$ is irreducible in K.

In order to determine the Galois group of f_jf_j' it is necessary to distinguish between the cases $\tau_1=\tau+1$ and $\tau_1=\tau$.

Let ξ be a zero of $f_j(w)$ satisfying

$$\xi^2=\zeta_{2^\tau}^{j}\gamma. \tag{18}$$

If $\tau_1=\tau+1$ then $-\zeta_{2^{\tau_1}}^{-j}$ is conjugate over K to $\zeta_{2^{\tau_1}}^{j}$ hence $\zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi$ is a zero of $f_j'(w)$. Let S be the substitution

$$\xi\to\zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi.$$

We have by (18)

$$S(\zeta_{2^\nu}^{j})=\zeta_{2^\nu}^{-j(1+2^\tau)}$$

hence

$$S^r(\xi)=\zeta_{2^\nu}^{-j(1+2^{\tau-1})\sum_{i=0}^{r-1}(-1-2^\tau)^i}\xi.$$

The order of S is the least r such that

$$-j(1+2^{\tau-1})\sum_{i=0}^{r-1}(-1-2^\tau)^i=-j\frac{(-1-2^\tau)^r-1}{2}\equiv 0 \bmod 2^\nu.$$

Clearly r must be even and since by (17)

$$\operatorname{ord}_2\left((1+2^\tau)^r-1\right)=\operatorname{ord}_2\nu+\tau$$

we get $r\equiv 0 \bmod 2^{\nu-\tau+1}$. The order of S is thus equal to the degree of f_jf_j' and since the latter polynomial is normal its group is cyclic of order $2^{\nu-\tau+1}$.

If $\tau_1=\tau$ then $\zeta_{2^{\tau_1}}^{-j}$ is conjugate over K to $\zeta_{2^{\tau_1}}^{j}$ hence $\zeta_{2^\nu}^{-j}\xi$ is a zero of $f_j'(w)$. Let S be the substitution $\xi\to\zeta_{2^\nu}^{-j}\xi$ and T the substitution $\xi\to\zeta_{2^{\nu-\tau+1}}^{j}\xi$. We have by (18)

$$S(\zeta_{2^\nu}^{j})=\zeta_{2^\nu}^{-j},\qquad S^2(\xi)=\xi;$$

$$T(\zeta_{2^\nu}^{j})=\zeta_{2^\nu}^{j(1+2^\tau)},\qquad T^r(\xi)=\zeta_{2^{\nu-\tau+1}}^{j\sum_{i=0}^{r-1}(1+2^\tau)^i}\xi.$$

Using (17) we infer that T is of order $2^{\nu-\tau+1}$, moreover $S\neq T^r$ since $-j\not\equiv 0 \bmod 2^{\tau-1}$. However

$$ST(\xi)=S(\zeta_{2^{\nu-\tau+1}}^{j})S(\xi)=\zeta_{2^{\nu-\tau+1}}^{-j}\zeta_{2^\nu}^{-j}\xi=\zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi,$$

$$TS(\xi)=T(\zeta_{2^\nu}^{-j})T(\xi)=\zeta_{2^\nu}^{-j(1+2^\tau)}\zeta_{2^{\nu-\tau+1}}^{j}\xi=\zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi,$$

thus $ST(\xi) = TS(\xi)$ and the group of $f_j f_j'$ being of order $2^{\nu-\tau+2}$ must be abelian of type $(2, 2^{\nu-\tau+1})$.

In particular if $x^{2^\nu} - a$ is irreducible we have $\tau_1 = \tau = 2$ and the group is abelian of type $(2, 2^{\nu-1})$.

Consider now the case $\varkappa = 1 \leqslant \tau - \nu + 1$. We have the factorization

$$x^{2^\nu} - a = \prod_{\substack{j=1 \\ j \equiv 1 \bmod 4}}^{2^\nu - 1} N_{K(\zeta_4)/K}(x^2 - \zeta_{2^\nu}^j \gamma).$$

The factors that are not irreducible are products of two quadratic factors and hence satisfy the condition of the lemma. The irreducible factors have groups abelian of type $(2, 2)$ generated by the substitutions $(\xi \to -\xi)$ and $(\xi \to \zeta_{2^\nu}^{-j}\xi)$, where ξ is a zero of $x^2 - \zeta_{2^\nu}^j \gamma$.

In particular this applies to the case of an irreducible binomial $x^4 + \gamma^2$.

It remains to consider the case $\varkappa = 0$. Then the assertions of the lemma follow by induction with respect to ν. They are true for $\nu = 1$. For $\nu > 1$ we have the factorization

$$x^{2^\nu} - \gamma^{2^{\nu-1}} = (x^{2^{\nu-1}} - \gamma^{2^{\nu-2}})(x^{2^{\nu-1}} + \gamma^{2^{\nu-2}}).$$

The first factor on the right hand side has an abelian Galois group and all its irreducible factors are of even degree by the inductive assumption, the second factor has this property by the already considered case $\varkappa = 1$ of the lemma.

Proof of Theorem 2. Necessity. Assume that the splitting field of $x^n - a$ is abelian over K. Then also the splitting field of $x^{p^\nu} - a$ is abelian over K for any $p^\nu \mid n$ and since every subgroup of an abelian group is normal $x^{p^\nu} - a$ is the product of normal factors. Thus we have one of the conditions (i)–(v) listed in Theorem 1. We shall show that under our assumption (ii)–(v) lead to (i). Consider first (ii), (iii) or (iv).

Let μ be the least nonnegative integer such that

$$a = -\gamma_1^{2^{\nu-\mu}}, \qquad \gamma_1 \in K.$$

Clearly $\mu < \nu$. If $\mu \leqslant 1$ we have (i). If $\mu > 1$ then by Lemma 3

$$\zeta_{2^{\nu-\mu+2}} \in K(\zeta_4). \tag{19}$$

$x^{2^\nu} - a$ has in $K(\zeta_4)$ the factor

$$f(x) = x^{2^\mu} - \zeta_{2^{\nu-\mu+1}}\gamma.$$

Now

$$\zeta_{2^{\nu-\mu+1}}\gamma \neq \vartheta^2, \qquad \vartheta \in K(\zeta_4),$$

since otherwise, by (19) $\gamma_1 = \vartheta_1^2$, $\vartheta_1 \in K(\zeta_4)$ and by Lemma 2

$$\gamma_1 = \pm\gamma_2^2, \qquad \gamma_2 \in K; \qquad a = -\gamma_2^{2^{\nu-\mu+1}}$$

contrary to the choice of μ. Thus $f(x)$ is irreducible in $K(\zeta_4)$ and $N_{K(\zeta_4)/K} f(x) = f(x)f'(x)$ is irreducible in K. By the assumption the latter polynomial is normal over K. Let ξ be any zero of $f(x)$

$$\xi_1 = \zeta_{2^\nu}^{-1}\xi, \qquad \xi_2 = \zeta_{2^\nu}^{-1-2^{\nu-\mu}}\xi.$$

ξ_1, ξ_2 are zeros of $f'(x)$. Let S_i be the automorphism of the Galois group of ff' over K such that

$$S_i\xi = \xi_i \qquad (i = 1, 2).$$

We have $S_i\zeta_{2^{\nu-\mu+1}} = \zeta_{2^{\nu-\mu+1}}^{-1}$ hence $S_i\zeta_{2^\nu} = \varepsilon_i\zeta_{2^\nu}^{-1}$ $(\varepsilon_i = \pm 1)$. It follows that

$$S_1S_2\xi = S_1\xi_2 = S_1(\zeta_{2^\nu}^{-1-2^{\nu-\mu}})S_1\xi = \varepsilon_1\zeta_{2^\mu}\xi,$$
$$S_2S_1\xi = S_2\xi_1 = S_2(\zeta_{2^\nu}^{-1})S_2\xi = \varepsilon_2\zeta_{2^\mu}^{-1}\xi.$$

By Lemma 3 we have $\varepsilon_1 = \varepsilon_2$ unless $\nu = \tau + 1$ and $\sqrt{-(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1} + 2)} \notin K$. In the latter case by (iv) $\mu = \nu - \lambda \geqslant 3$, thus $S_1S_2\xi \neq S_2S_1\xi$ and the group in question is not abelian.

Consider now the case (v). If $\sqrt{-(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)} \in K$ then we get (i). If $\sqrt{-(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)} \notin K$ then by Lemma 3

$$\zeta_{2^{\tau+1}} \notin K(\zeta_4). \tag{20}$$

$x^{2^\nu} - a$ has in $K(\zeta_4)$ the factor

$$f(x) = x^{2^{\nu-\tau+1}} - \zeta_{2^\tau}(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\nu-\tau-1}}\gamma^{2^{\nu-\tau}}.$$

By (20) and the inequality $\nu \geqslant \tau + 2$, $f(x)$ is irreducible in $K(\zeta_4)$. Hence $N_{K(\zeta_4)/K} f(x) = f(x)f'(x)$ is irreducible in K and by the assumption normal.

Let ξ be a zero of $f(x)$ satisfying

$$\xi^2 = \zeta_{2^\nu}(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1})\gamma \tag{21}$$

and let

$$\xi_1 = \zeta_{2^\nu}^{-1}\xi, \qquad \xi_2 = \zeta_{2^\nu}^{-1-2^{\tau-1}}\xi.$$

ξ_1 and ξ_2 are zeros of $f'(x)$. Let S_i $(i = 1, 2)$ be the automorphism of the Galois group of ff' over K such that

$$S_i\xi = \xi_i \qquad (i = 1, 2).$$

We have for a suitable $\varepsilon_i = \pm 1$

$$S_i(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}) = \varepsilon_i(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1});$$

then by (21)

$$S_1\zeta_{2^\nu} = \varepsilon_1\zeta_{2^\nu}^{-1}, \qquad S_2\zeta_{2^\nu} = \varepsilon_2\zeta_{2^\nu}^{-1-2^\tau} \tag{22}$$

hence

$$S_1(\zeta_{2^{\tau+1}}+\zeta_{2^{\tau+1}}^{-1}) = (\varepsilon_1\zeta_{2^\nu}^{-1})^{2^{\nu-\tau-1}}+(\varepsilon_1\zeta_{2^\nu})^{2^{\nu-\tau-1}} = \zeta_{2^{\tau+1}}+\zeta_{2^{\tau+1}}^{-1},$$

$$S_2(\zeta_{2^{\tau+1}}+\zeta_{2^{\tau+1}}^{-1}) = (\varepsilon_2\zeta_{2^\nu}^{-1-2^\tau})^{2^{\nu-\tau-1}}+(\varepsilon_2\zeta_{2^\nu}^{1+2^\tau})^{2^{\nu-\tau-1}} = -\zeta_{2^{\tau+1}}-\zeta_{2^{\tau+1}}^{-1}.$$

Thus $\varepsilon_1 = 1$, $\varepsilon_2 = -1$ and (22) implies

$$S_1S_2\xi = S_1\xi_2 = S_1(\zeta_{2^\nu}^{-1-2^{\tau-1}})S_1\xi = \zeta_{2^{\nu-\tau+1}}\xi,$$

$$S_2S_1\xi = S_2\xi_1 = S_2(\zeta_{2^\nu}^{-1})S_2\xi = -\zeta_{2^{\nu-\tau+1}}\xi.$$

Hence $S_1S_2\xi \neq S_2S_1\xi$ and the group in question is not abelian. Therefore, if $n = \prod_{i=1}^{k} p_i^{\nu_i}$ is the canonical factorization of n we get for each $i \leqslant k$

$$a^{w^i} = \gamma_i^{p_i^{\nu_i}}, \qquad \gamma_i \in K,$$

where we have put for abbreviation $w^i = w_{p_i^{\nu_i}}$. It follows that

$$a^{\frac{nw_n}{p_i^{\nu_i}}} = \gamma_i^{\frac{nw_n}{w^i}}.$$

If now

$$\frac{1}{n} = \sum_{i=1}^{k}\frac{r_i}{p_i^{\nu_i}} \tag{23}$$

we obtain

$$a^{w_n} = \Big(\prod_{i=1}^{k}\gamma_i^{r_i\frac{w_n}{w^i}}\Big)^n$$

and the proof is complete.

Sufficiency. Assume that

$$a^{w_n} = \gamma^n, \qquad \gamma \in K,$$

and let again $n = \prod_{i=1}^{k} p_i^{\nu_i}$, $w^i = w_{p_i^{\nu_i}}$.

Since $\left(\frac{w_n}{w^i}, p_i^{\nu_i}\right) = 1$ we have

$$a^{w^i} = \gamma_i^{p_i^{\nu_i}}. \tag{24}$$

Thus a satisfies the assumptions of Lemma 5 for all p_i and by that lemma the Galois groups over K of all binomials

$$x^{p_i^{\nu_i}} - a \qquad (1 \leqslant i \leqslant k) \tag{25}$$

are abelian. If ξ is any zero of $x^n - a$ then $\xi^{\frac{n}{p_i^{\nu_i}}}$ is a zero of (25) and defining r_i by (23) we get

$$\xi = \prod_{i=1}^{k}(\xi^{\frac{n}{p_i^{\nu_i}}})^{r_i}.$$

Hence the splitting field of $x^n - a$ as the composite of the splitting fields of (25) is abelian.

Moreover if $x^n - a$ is irreducible then also the binomials (25) are irreducible and their groups are cyclic of order $p_i^{\nu_i}$ unless $p_i^{\nu_i} \equiv 0 \bmod 4$ and $\zeta_4 \notin K$ in which case the group of (25) has a cyclic factor of order 2^{ν_i-1}. Since the direct product of cyclic groups of orders prime in pairs is again cyclic we get all assertions of the theorem.

Lemma 6 (Hasse). *If $a = \eta^{p^\nu}$, $\eta \in K(\zeta_{p^\nu})$ then at least one of the following conditions is satisfied for a suitable $\gamma \in K$*

$$a = \gamma^{p^\nu}; \tag{26}$$

$$p = 2,\ \omega = 1,\ 1 < \nu < \tau,\ a = -\gamma^{2^\nu};$$

$$p = 2,\ \omega = 1,\ \nu = \tau,\ a = -(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{2^{\tau-1}}\gamma^{2^\tau};$$

$$p = 2,\ \omega = 1,\ \nu > \tau,\ a = (\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{2^{\nu-1}}\gamma^{2^\nu},$$

where ω and τ have the meaning of Theorem 1.

Proof which we give is based on the previous results and therefore much shorter than the original Hasse's proof ([2]).

Since all the subextensions of $K(\zeta_{p^\nu})$ are normal over K the binomial $x^{p^\nu} - a$ satisfies the conditions of Theorem 1. Hence we have either (26) or $\omega \geqslant 1$. In the latter case Lemma 1 applies with $\xi = \zeta_{p^\nu}$, and we get either

$$\eta \in K\langle\zeta_{p^\nu}\rangle; \qquad \eta = \gamma\zeta_{p^\nu}, \qquad \gamma \in K \tag{27}$$

or $p = 2$, $\zeta_4 \notin K$. (27) gives at once (26). To settle the case $p = 2$ we apply the already proved case of our lemma for the field $K(\zeta_4)$ and get

$$a = \vartheta^{2^\nu}, \qquad \vartheta \in K(\zeta_4).$$

Now Lemma 6 follows immediately from Lemma 2.

Proof of Theorem 3. We start by estimating for each $p^\nu \| n$ the greatest exponent μ_p such that p^{μ_p} divides the order of an element in $\mathrm{Gal}(K(\zeta_{np^{-\nu}})/K)$. Since $K(\zeta_{np^{-\nu}})$ is the composite of $K(\zeta_{q^s})$, where $q \neq p$ is a prime and $q^s \| n$, we have

$$\mu_p \leqslant \max_{\substack{q^s \| n \\ q \neq p}} \mathrm{ord}_p[K(\zeta_{q^s}) : K].$$

Let r be the largest integer such that $\zeta_{q^r} \in K(\zeta_q)$. Then for $q^s > 2$

$$[K(\zeta_{q^s}) : K] = \begin{cases} q^{\max(0,s-r)}[K(\zeta_q) : K] & \text{if} \quad (q,r) \neq (2,1), \\ 2^{\max(0,s-r_1)}[K(\zeta_4) : K] & \text{if} \quad (q,r) = (2,1). \end{cases}$$

This gives

$$\mu_p \leqslant \max_{\substack{q \mid n \\ q \text{ prime}}} \operatorname{ord}_p [K(\zeta_q) : K]. \tag{28}$$

(Actually we have here the equality.)

Assume now that

$$a = \vartheta^n, \quad \vartheta \in K(\zeta_n). \tag{29}$$

Then for each $p^\nu \| n$, the binomial $x^{p^\nu} - a$ is abelian over K and by Theorem 2

$$a = \zeta_{p^\varkappa} \gamma_p^{p^{\nu-\lambda}}; \quad \varkappa \leqslant \lambda \leqslant \min(\nu, \omega), \tag{30}$$

where ω has the meaning of Theorem 1.

Suppose first $p^\nu \not\equiv 0 \bmod 4$ or $\zeta_4 \in K$. Then by Lemma 6 it follows from (29) that

$$a = \vartheta_1^{p^\nu}, \quad \vartheta_1 \in K(\zeta_{np^{-\nu}}). \tag{31}$$

By Lemma 5 $\operatorname{Gal}\big(K(\vartheta_1)/K\big)$ contains an element of order p^λ hence $\operatorname{Gal}\big(K(\zeta_{np^{-\nu}})/K\big)$ contains such an element and by (28) we have

$$\lambda \leqslant \mu_p \leqslant \max_{\substack{q \mid n \\ q \text{ prime}}} \operatorname{ord}_p [K(\zeta_q) : K].$$

By (30) we have also

$$\lambda \leqslant \operatorname{ord}_p w_n \tag{32}$$

hence $\lambda \leqslant \operatorname{ord}_p \sigma$.

The same inequality follows directly from (32) if $p^\nu \equiv 0 \bmod 4$, $\zeta_4 \notin K$. Thus for each p we have

$$a^\sigma = \delta_p^{p^\nu}, \quad \delta_p \in K,$$

whence by the standard argument (see proof of Theorem 2)

$$a^\sigma = \gamma^n, \quad \gamma \in K.$$

Assume now in addition to (29) that for a certain m prime to n

$$\begin{cases} \text{either } \zeta_{(4,n)} \in K \text{ and } nm \equiv 0 \bmod w_n \text{l.c.m.}_{\substack{q \mid n \\ q \text{ prime}}} [K(\zeta_q) : K] \\ \text{or } \zeta_{(4,n)} \notin K \text{ and } nm \equiv 0 \bmod 2^\tau w_n \text{l.c.m.}_{\substack{q \mid n \\ q \text{ prime}}} [K(\zeta_q) : K] \end{cases} \tag{33}$$

and consider again (30) for any $p^\nu \| n$.

If $\nu \leqslant \omega$ then from (30) we get immediately

$$a = \delta_p^{p^{\nu-\lambda}}, \quad \delta_p \in K. \tag{34}$$

If $\nu > \omega$ and either $p \geqslant 2$ or $\zeta_4 \in K$ we get from (28) and (33),

$$\nu \geqslant \omega + \mu_p, \tag{35}$$

hence in particular

$$\omega - \nu + \lambda \leqslant -\mu_p + \operatorname{ord}_p \sigma \leqslant 0.$$

Thus if (30) holds with $\varkappa > 0$ we get by Lemma 5 and (31)

$$\nu - \omega + 1 \leqslant \mu_p,$$

which contradicts (35). If $\nu > \omega = 1$ and $p = 2$ we get from (33)

$$\nu \geqslant \tau + 1 + \mu_2 > \tau. \tag{36}$$

Let τ_2 be the greatest integer such that

$$\zeta_{2^{\tau_2}} + \zeta_{2^{\tau_2}}^{-1} \in K(\zeta_{n2^{-\nu}}).$$

Since $K(\zeta_{2^{\tau_2}} + \zeta_{2^{\tau_2}}^{-1})$ is over K cyclic of degree $2^{\tau_2 - \tau}$ we have

$$\tau_2 - \tau \leqslant \mu_2$$

and by (36)

$$\nu \geqslant \tau_2 + 1.$$

Hence by (29) and Lemma 6

$$a = \vartheta_1^{2^{\nu-1}}, \quad \vartheta_1 \in K(\zeta_{n2^{-\nu}}).$$

Thus if (30) holds with $\varkappa > 0$ we get by Lemma 5

$$\nu - \tau \leqslant \mu_2$$

contrary to (36). Therefore (34) holds in any case and by the standard argument

$$a = \gamma^{n/\sigma}, \quad \gamma \in K.$$

Remark. If $(w_n, n/w_n) = 1$ the number σ occurring in Theorem 3 is the least integer with the required property. Indeed by the definition of σ there exists a character $\chi \bmod n$ belonging to exponent σ on the group $G = \operatorname{Gal}\big(K(\zeta_n)/K\big)$.

Let $\tau(\chi, \zeta_n)$ be the corresponding Gauss sum. Clearly $\tau(\chi) \in K(\zeta_n)$. Suppose that $\tau(\chi)^{n\varrho} = \gamma^n$, $\gamma \in K$. Then $\tau(\chi)^\varrho = \zeta_n^a \gamma$, $\gamma \in K$ and applying an automorphism

$$\zeta_n \to \zeta_n^j \tag{*}$$

from G we get $\overline{\chi}(j)^\varrho = \zeta_n^{a(j-1)}$. It follows that

$$\zeta_n^{a(j^2-1)} = \overline{\chi}(j^2)^\varrho = \overline{\chi}(j)^{2\varrho} = \zeta_n^{2a(j-1)}; \quad \zeta_n^{a(j-1)^2} = 1,$$

$a(j-1)^2 \equiv 0 \bmod n$ and since this holds for all automorphisms $(*)$ from G $aw_n^2 \equiv 0 \bmod n$. Since $(w_n, n/w_n) = 1$ we get

$$a \equiv 0 \bmod \frac{n}{w_n}, \quad a(j-1) \equiv 0 \bmod n \quad \text{and} \quad \overline{\chi}(j)^\varrho = 1$$

contrary to the choice of χ.

LEMMA 7. *Under the assumption* (viii) *of Theorem 4 the group*

$$G_0 = \mathrm{Gal}\big(K(\zeta_n, \sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_k})/K(\zeta_n)\big)$$

contains the substitution

$$\sqrt[n]{\alpha_i} \to \zeta_n^{c_i}\sqrt[n]{\alpha_i} \quad (1 \leqslant i \leqslant k)$$

under the assumptions (vii) *and* (ix) *the group*

$$G_1 = \mathrm{Gal}\big(K(\zeta_n, \sqrt[n]{\zeta_w}, \sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_k})/K(\zeta)_n\big)$$

contains the substitution

$$\sqrt[n]{\zeta_w} \to \zeta_{(w,n)}^{c_0}\sqrt[n]{\zeta_w}, \quad \sqrt[n]{\alpha_i} \to \zeta_n^{c_i}\sqrt[n]{\alpha_i} \quad (1 \leqslant i \leqslant k)$$

for any c_0 *and any* $c_i \equiv 0 \bmod \sigma$ $(1 \leqslant i \leqslant k)$.

Proof. Let us denote any value of $\sqrt[n]{\alpha_i}$ by ξ_i $(1 \leqslant i \leqslant k)$ and of $\sqrt[n]{\zeta_w}$ by ξ_0. To prove the first part of the lemma it is clearly sufficient to prove that G_0 contains each of the substitutions $(1 \leqslant i \leqslant k)$

$$\xi_j \to \xi_j \quad (1 \leqslant j \leqslant k, j \neq i), \quad \xi_i \to \zeta_n^\sigma \xi_i. \tag{37}$$

If (37) were not contained in G_0, we would have

$$d_i = \mathrm{Gal}\big(K(\zeta_n, \xi_1, \ldots, \xi_k)/K(\zeta_n, \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_k) \not\equiv 0 \bmod \frac{n}{\sigma}. \tag{38}$$

Now by Kneser's theorem

$$d_i = [K(\zeta_n)\langle \xi_1, \ldots, \xi_k\rangle : K(\zeta_n)\langle \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_k\rangle]$$

hence d_i is the least exponent such that

$$\xi_i^{d_i} = \vartheta \in K\langle \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_k\rangle. \tag{39}$$

By raising (39) to nth power we get that

$$\alpha_i^{d_i} = \vartheta^n \alpha_1^{x_1} \ldots \alpha_{i-1}^{x_{i-1}} \alpha_{i+1}^{x_{i+1}} \ldots \alpha_k^{x_k}$$

$\vartheta^n \in K$, and by Theorem 3 $\vartheta^{n\sigma} = \gamma^n$; $\gamma \in K$,

$$\alpha_1^{-\sigma x_1} \ldots \alpha_i^{d_i\sigma} \ldots \alpha_k^{-\sigma x_k} = \gamma^n.$$

By the assumption $d_i\sigma \equiv 0 \bmod n$, contrary to (38).

To prove the second part of the lemma we have similarly to prove that G_1 contains each of the substitutions $(1 \leqslant i \leqslant k)$

$$\xi_0 \to \zeta_{(n,w)}\xi_0, \quad \xi_j \to \xi_j \quad (1 \leqslant j \leqslant k);$$

$$\xi_0 \to \xi_0, \quad \xi_j \to \xi_j \quad (1 \leqslant j \leqslant k, j \neq i), \quad \xi_i \to \zeta_n^\sigma \xi_i.$$

This reduces to proving that the least exponents e_i $(0 \leqslant i \leqslant k)$ such that

$$\xi_i^{e_i} \in K(\zeta_n)\langle \xi_0, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_k\rangle \tag{40}$$

atisfy $e_0 \equiv 0 \bmod (n, w)$, $e_i \equiv 0 \bmod n/\sigma$. Now (40) implies for $i = 0$

$$\zeta_w^{c_0} = \vartheta^n \alpha_1^{x_1} \ldots \alpha_k^{x_k}, \quad \vartheta \in K(\zeta_n);$$

$$\zeta_w^{c_0} \alpha_1^{-x_1} \ldots \alpha_k^{-x_k} = \gamma^{n/\sigma}, \quad \gamma \in K; \quad x_i \equiv 0 \bmod n/\sigma;$$

$$\zeta_w^{c_0} = \gamma^{n/\sigma} \alpha_1^{y_1 n/\sigma} \ldots \alpha_k^{y_k n/\sigma} = \gamma_1^{n/\sigma}.$$

γ_1 must be a root of unity contained in K; $\gamma_1 = \zeta_w^j$ and so we get $e_0 \equiv 0 \bmod (w, n/\sigma)$. However by the condition (vii) $n/\sigma \equiv 0 \bmod (w, n)$ and thus $c_0 \equiv 0 \bmod (w, n)$.

For $i > 0$, (40) implies

$$\alpha_i^{e_i} = \vartheta^n \zeta_w^{x_0} \alpha_1^{x_1} \ldots \alpha_{i-1}^{x_{i-1}} \alpha_{i+1}^{x_{i+1}} \ldots \alpha_k^{x_k}, \quad \vartheta \in K(\zeta_n);$$

$$\zeta_w^{-x_0} \alpha_1^{-x_1} \ldots \alpha_i^{e_i} \ldots \alpha_k^{-x_k} = \gamma^{n/\sigma}, \quad \gamma \in K; \quad e_i \equiv 0 \bmod n/\sigma.$$

Proof of Theorem 4. We use Čebotarev's density theorem and get the existence of infinitely many prime ideals $\mathfrak{P}$ of $L_0 = K(\zeta_n, \xi_1, \ldots, \xi_k)$ or $L_1 = K(\zeta_n, \xi_0, \ldots, \xi_k)$ dividing $\mathfrak{p}$ in $K(\zeta_n)$ such that for all $\eta \in L_0$ or L_1 respectively

$$\eta^{N\mathfrak{p}} \equiv S\eta \bmod \mathfrak{P},$$

where S is the automorphism described in Lemma 7, $\xi_0^n = \zeta_w$, $\xi_i^n = \alpha_i$. Setting $\eta = \xi_i$ we get

$$\xi_i^{N\mathfrak{p}} \equiv \xi_i \zeta_n^{c_i} \bmod \mathfrak{P} \quad (i > 0),$$

$$\xi_0^{N\mathfrak{p}} \equiv \xi_0 \zeta_{(w,n)}^{c_0} \bmod \mathfrak{P},$$

consequently

$$\alpha_i^{\frac{N\mathfrak{p}-1}{n}} \equiv \zeta_n^{c_i} \bmod \mathfrak{P},$$

$$\zeta_w^{\frac{N\mathfrak{p}-1}{n}} \equiv \zeta_{(w,n)}^{c_0} \bmod \mathfrak{P}$$

and the same mod$\mathfrak{p}$. One has only to remark that $N\mathfrak{p} \equiv 1 \bmod n$.

Remark. If $(w_n, n/w_n) = 1$ the number σ occurring in the first part of Theorem 4 is the least integer with the required property. This follows

from the Remark after Theorem 3 on taking $k=1$, $\alpha=\tau(\chi)^\sigma$. If $(w_n, n/w_n)>1$ σ needs not be best possible. In particular, if $\zeta_4\notin K$, $n\not\equiv 0 \bmod 2^{r+1}$ σ can be replaced by $(w_n,\ \text{l.c.m.}_{q\mid n,\,q\text{prime}}\ [K(\zeta_q):K])$.

LEMMA 8. *If every integral vector $[t_0, t_1, \dots, t_r]$ satisfies at least one of the congruences*

$$\sum_{s=0}^{r} a_{hs}t_s \equiv 0 \bmod m \qquad (1\leqslant h\leqslant g) \tag{41}$$

then for at least one h we have

$$a_{h0}\equiv 0 \bmod (a_{h1}, \dots, a_{hr}, m)$$

and

$$\frac{m}{(a_{h1}, \dots, a_{hr}, m)} \leqslant \max(g-1, 1). \tag{42}$$

Proof. Let us choose in $\{1, 2, \dots, g\}$ a minimal subset M with the property that every integral vector $[1, t_1, \dots, t_r]$ satisfies at least one congruence (41) with $h\in M$.

Put $d_h=(a_{h1}, \dots, a_{hr}, m)$. For $h\in M$ we have $a_{h0}\equiv 0 \bmod d_h$, since otherwise the congruence

$$a_{h0}+\sum_{j=1}^{r} a_{hs}t_s \equiv 0 \bmod m \tag{43}$$

would not be satisfied by any $[t_1, \dots, t_r]$.

Hence, by a theorem of Frobenius the congruence (43) has $d_h m^{r-1}$ solutions $\bmod m$. If for a certain $h\in M$ we have $m/d_h<g$ (42) follows. If for all $h\in M$, $m/d_h\geqslant g$ then either

$$\sum_{h\in M}\frac{d_h}{m}<1$$

or $|M|=g$ and $d_h=m/g$ $(1\leqslant h\leqslant g)$. The former case is impossible since then the alternative of congruences (43) for $h\in M$ would have $m^r\sum d_h/m<m^r$ solution $\bmod m$, contrary to the choice of M. In the latter case, we consider the system of congruences

$$\sum_{s=1}^{r} a_{hs}t_s \equiv 0 \bmod m$$

obtained from (41) by the substitution $t_0=0$. Since every integral vector $[t_1, \dots, t_r]$ satisfies at least one of these congruences and $\sum_{h=1}^{g} d_h/m=1$, every vector must satisfy exactly one congruence. However, vector $[0, \dots, 0]$ satisfies them all. This is a contradiction unless $g=1$, $m=d_1$.

LEMMA 9. *In any number field K there exists a multiplicative basis, i.e. such a sequence $\pi_1, \pi_2, \dots$ that any non-zero element of K is represented uniquely as $\zeta\prod_{s=1}^{t}\pi_s^{x_s}$, where x_s are rational integers and ζ is a root of unity contained in K.*

Proof, see Skolem [8].

Proof of Theorem 5. Let $\beta_1, \dots, \beta_g$ be the zeros of f_i. We assume without loss of generality that $\beta_i\neq 0$ and put $K_1=K(\beta_1, \dots, \beta_g)$. Let in K_1

$$\alpha_j=\zeta_w^{a_{j0}}\prod_{s=1}^{t}\pi_s^{a_{js}} \qquad (1\leqslant j\leqslant k),$$

$$\beta_h=\zeta_w^{b_{h0}}\prod_{s=1}^{t}\pi_s^{b_{hs}} \qquad (1\leqslant h\leqslant g),$$

where w is the number of roots of unity contained in K_1 and π_s are elements of the multiplicative basis described in Lemma 9. Let $\boldsymbol{A}=[a_{js}]_{\substack{j\leqslant k\\ 1\leqslant s\leqslant t}}$ and let $\boldsymbol{P}$ and $\boldsymbol{Q}$ be unimodular matrices such that

$$\boldsymbol{PAQ}=\begin{bmatrix} e_1 & & & & \\ & e_2 & & & \\ & & \ddots & & \\ & & & e_r & \\ & & & & \ddots \end{bmatrix},$$

where all the elements outside the principal diagonal are zero, on the diagonal precisely $e_1, \dots, e_r$ are non-zero and $e_i\mid e_{i+1}$. Let

$$\boldsymbol{P}\begin{bmatrix} a_{10}\\ \vdots\\ a_{k0}\end{bmatrix}=\begin{bmatrix} c_1\\ \vdots\\ c_k\end{bmatrix}, \qquad [b_{h1}, \dots, b_{ht}]\boldsymbol{Q}=[d_{h1}, d_{h2}, \dots, d_{ht}].$$

We choose integers $\eta_{r+1}, \dots, \eta_t$ divisible by w so that for all $h\leqslant g$

$$\sum_{s=r+1}^{t} d_{hs}\eta_s=0 \quad \text{implies} \quad d_{hs}=0 \qquad (r<s\leqslant t)$$

and set

$$m=\max_{1\leqslant h\leqslant g}\Big|\sum_{s=r+1}^{t} d_{hs}\eta_s\Big|+1.$$

Further we set

$$n=2^\tau w m e_r\ \text{l.c.m.}_{\substack{q\leqslant m+e_r\\ q\,\text{prime}}}(q-1), \qquad \eta_s=(w, c_{r+1}, \dots, c_t)\frac{n}{e_s w}t_s+c_s\frac{n'}{e_s w}t_0,$$

$$(1\leqslant s\leqslant r$$

where τ is the relevant parameter of the field K_1,

$$\varepsilon_0 = -t_0, \qquad \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_t \end{bmatrix} = \boldsymbol{Q} \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_t \end{bmatrix}.$$

By Theorem 4 there exist infinitely many prime ideals $\mathfrak{p}$ of $K_1(\zeta_n)$ such that

$$\left(\frac{\zeta_w}{\mathfrak{p}}\right)_n = \zeta_w^{\varepsilon_0}, \qquad \left(\frac{\pi_s}{\mathfrak{p}}\right)_n = \zeta_n^{s_s} \qquad (1 \leqslant s \leqslant t).$$

The congruence

$$f(\alpha_1^{x_1} \dots \alpha_k^{x_k}) \equiv 0 \bmod \mathfrak{p}$$

gives for a suitable $h \leqslant g$

$$\left(\frac{\alpha_1^{x_1} \dots \alpha_k^{x_k}}{\mathfrak{p}}\right)_n = \left(\frac{\beta_h}{\mathfrak{p}}\right)_n$$

hence

$$\sum_{j=1}^{k} x_j \left(\frac{n}{w} a_{j0} \varepsilon_0 + \sum_{s=1}^{t} a_{js} \varepsilon_s\right) \equiv \frac{n}{w} b_{h0} \varepsilon_0 + \sum_{s=1}^{t} b_{hs} \varepsilon_s \bmod n.$$

Setting $[y_1, \dots, y_k] = [x_1, \dots, x_k]\boldsymbol{P}^{-1}$ we get

$$\sum_{j=1}^{k} y_j \left(\frac{n}{w} c_j \varepsilon_0 + e_j \eta_j\right) \equiv \frac{n}{w} b_{h0} \varepsilon_0 + \sum_{s=1}^{t} d_{hs} \eta_s \bmod n,$$

hence

$$\frac{n}{w}\left(\sum_{j=1}^{r} y_j (w, c_{r+1}, \dots, c_k) t_j - \sum_{j=r+1}^{k} y_j c_j t_0\right)$$

$$\equiv -\frac{n}{w} b_{h0} t_0 + \frac{n}{w} \sum_{s=1}^{r} d_{hs} \left(\frac{(w, c_{r+1}, \dots, c_k)}{e_s} + \frac{c_s}{e_s} t_0\right) + \sum_{s=r+1}^{t} d_{hs} \eta_s \bmod n.$$

It follows that

$$\sum_{s=r+1}^{t} d_{hs} \eta_s \equiv 0 \bmod m, \qquad \sum_{s=r+1}^{t} d_{hs} \eta_s = 0$$

and by the choice of $\eta_{r+1}, \dots, \eta_s$: $d_{hs} = 0$ $(r < s \leqslant t)$.

Hence all integer vectors $[t_1, \dots, t_r]$ satisfy at least one congruence

$$\sum_{s=1}^{r} \frac{n d_{hs}}{w e_s} (w, c_{r+1}, \dots, c_k) t_s + t_0 \left(\sum_{s=1}^{r} \frac{n c_s d_{hs}}{w e_s} - \frac{n}{w} b_{h0}\right) \bmod \frac{n}{w} (w, c_{r+1}, \dots, c_k),$$

where $d_{hs} = 0$ $(r < s \leqslant t)$.

It follows by Lemma 8 that for a certain h

$$(44) \quad q = \frac{n/w}{\left(\frac{n}{w}, \underset{1 \leqslant s \leqslant r}{\text{g.c.d.}} \frac{n}{w} \frac{d_{hs}}{e_s}\right)} \leqslant \max(g-1, 1), \qquad d_{hs} = 0 \qquad (r < s \leqslant t)$$

and

$$(45) \quad \sum_{s=1}^{r} \frac{n}{w} \frac{c_s d_{hs}}{e_s} - \frac{n}{w} b_{h0} \equiv 0 \bmod \frac{n}{wq} (w, c_{r+1}, \dots, c_k).$$

For h satisfying (44) we have

$$\frac{d_{hs}}{e_s} = \frac{p_s}{q}, \qquad p_s \text{ integer} \qquad (1 \leqslant s \leqslant r)$$

and by (45) there exist integers $u_1, \dots, u_k$ such that

$$(46) \quad \sum_{s=1}^{r} \frac{n}{w} \frac{c_s d_{hs}}{e_s} - \frac{n}{w} b_{h0} + \sum_{j=1}^{r} n \frac{d_{hs}}{e_s} u_s + \sum_{s=r+1}^{k} \frac{n}{wq} c_s u_s = 0.$$

Let us fix any values of $\log \pi_s$ $(1 \leqslant s \leqslant t)$ and set $\log \zeta_w = \frac{2\pi i}{w}$. α_j^x is a many valued function and $\prod_{j=1}^{k} \alpha_j^{x_j}$ can take any value

$$V = \exp\left[\frac{2\pi i}{w} \sum_{j=1}^{k} a_{j0} x_j + \sum_{s=1}^{t} \log \pi_s \sum_{j=1}^{k} a_{js} x_j + 2\pi i \sum_{j=1}^{k} v_j x_j\right],$$

where $[v_1, \dots, v_k]$ is an integral vector. Taking

$$[v_1, \dots, v_k] = [u_1, \dots, u_r, 0, \dots, 0](\boldsymbol{P}^{-1})^T,$$

$$[x_1, \dots, x_k] = \left[\frac{d_{h1}}{e_1}, \dots, \frac{d_{hr}}{e_r}, \frac{u_{r+1}}{q}, \dots, \frac{u_k}{q}\right]\boldsymbol{P}$$

we get

$$V = \exp\left[\frac{2\pi i}{w}\left(\sum_{j=1}^{r} \frac{d_{hj}}{e_j} c_j + \sum_{j=r+1}^{k} \frac{u_j}{q} c_j\right) + \sum_{s=1}^{t} b_{hs} \log \pi_s + 2\pi i \sum_{j=1}^{r} \frac{d_{hj}}{e_j} u_j\right].$$

By (46) $V = \beta_h$, hence $f(V) = 0$.

Remark. Theorem 5 is essentially best possible, as the following example shows:

$$f(t) = (t - \beta_1) \prod_{j=0}^{q-1} (t - \beta_1^j \beta_2),$$

where q is a prime and β_1, β_2 are integers of K multiplicatively independent.

The congruence

$$f(\alpha_1^{x_1}\alpha_2^{x_2}) \equiv 0 \bmod \mathfrak{p}, \quad \text{where} \quad \alpha_1 = \beta_1^q,\ \alpha_2 = \beta_2^q$$

is soluble for every prime ideal $\mathfrak{p}$. Indeed, let γ be a primitive root mod$\mathfrak{p}$.

If $\operatorname{ord}_q \operatorname{ind}_\gamma \beta_1 > \operatorname{ord}_q \operatorname{ind}_\gamma \beta_2$ then the equation

$$qx_1 \operatorname{ind}_\gamma \beta_1 + qx_2 \operatorname{ind}_\gamma \beta_2 = \operatorname{ind}_\gamma \beta_1$$

is soluble and so is the congruence

$$\alpha_1^{x_1}\alpha_2^{x_2} \equiv \beta_1 \bmod \mathfrak{p}.$$

If on the other hand, $\operatorname{ord}_q \operatorname{ind}_\gamma \beta_1 \leqslant \operatorname{ord}_q \operatorname{ind}_\gamma \beta_2$ then there is a $j < q$ such that

$$\operatorname{ord}_q(j \operatorname{ind}_\gamma \beta_1 + \operatorname{ind}_\gamma \beta_2) > \operatorname{ord}_q \operatorname{ind}_\gamma \beta_1.$$

This implies the solubility of the equation

$$qx_1 \operatorname{ind}_\gamma \beta_1 + qx_2 \operatorname{ind}_\gamma \beta_2 = j \operatorname{ind}_\gamma \beta_1 + \operatorname{ind}_\gamma \beta_2$$

and of the congruence

$$\alpha_1^{x_1}\alpha_2^{x_2} \equiv \beta_1^j \beta_2 \bmod \mathfrak{p}.$$

The solubility of $f(\alpha_1^{x_1}, \alpha_2^{x_2}) \equiv 0 \bmod \mathfrak{p}$ if $\mathfrak{p} \mid \alpha_1\alpha_2$ is trivial. On the other hand, the equation $f(\alpha_1^{x_1}\alpha_2^{x_2}) = 0$ has only the solutions $(x_1, x_2) = \left(\frac{1}{q}, 0\right)$, $\left(\frac{j}{q}, \frac{1}{q}\right)$ $(0 \leqslant j < q)$.

For $\beta_1 = \zeta_q$, β_2 different from a root of unity we get an example with $k = 1$.

Let us note further that Theorem 5 does not extend to all exponential congruences even in one variable, e.g. the congruence

$$(\alpha^x + \alpha)\left((-\alpha)^x - \alpha\right) \equiv 0 \bmod \mathfrak{p}$$

is soluble for all prime ideals $\mathfrak{p}$, but the corresponding equation has no rational solutions if α is not a root of unity.

Proof of the Corollary. For $b = 0$ it suffices to put in Theorem 5

$$f(t) = u_1 t - c, \quad k = 1, \quad \alpha_1 = \alpha.$$

For $b = -1$, we have $t^2 - at - b = (t-\alpha)(t-\alpha^{-1})$ with $\alpha \neq \pm 1$ since $a^2 - 4 \neq 0$. It is well known that $u_n = \lambda_1 \alpha^n + \lambda_2 \alpha^{-n}$ and it suffices to put in Theorem 5

$$f(t) = \lambda_1 t^2 - ct + \lambda_2, \quad k = 1, \quad \alpha_1 = \alpha.$$

For $b = 1$ we have $t^2 - at - b = (t-\alpha)(t+\alpha^{-1})$ with $\alpha \neq \pm 1$ since $a \neq 0$. Now $u_n = \lambda_1 \alpha^n + \lambda_2(-\alpha)^{-n}$, where λ_1, λ_2 are conjugate in the field $Q(\alpha)$. If $c = 0$, we set in Theorem 5

$$f(t) = \lambda_1 t + \lambda_2, \quad k = 1, \quad \alpha_1 = -\alpha^2.$$

If $c \neq 0$, we set

$$f(t) = (\lambda_1 t^2 - ct + \lambda_2)(\lambda_1 t^2 - ct - \lambda_2), \quad k = 1, \quad \alpha_1 = \alpha,$$

where α is chosen negative (one of the numbers α, $-\alpha^{-1}$ is always negative). We infer that the equation $f(\alpha^x) = 0$ has a solution $x = m/q$, where $(m, q) = 1$, $q \leqslant 3$. If $q = 1$ and

$$\lambda_1 \alpha^{2m} - c\alpha^m + (-1)^m \lambda_2 = 0$$

we get $c = u_m$. If $q = 1$ and

$$\lambda_1 \alpha^{2m} - c\alpha^m - (-1)^m \lambda_2 = 0 \tag{47}$$

we get a contradiction. Indeed, since

$$\lambda_1 \alpha^{2m} - u_m \alpha^m + (-1)^m \lambda_2 = 0$$

we obtain

$$2\lambda_1 \alpha^{2m} - (c + u_m)\alpha^m = 0, \quad \lambda_1 = \tfrac{1}{2}(c + u_m)\alpha^{-m},\ \lambda_2 = \tfrac{1}{2}(c + u_m)(-\alpha)^{-m}$$

and from (47) $c = 0$.

$q = 2$ is impossible since then both numbers $\lambda_1 \alpha^{2x} - c\alpha^x \pm \lambda_2$ have a non-zero imaginary part.

Finally $q = 3$ is impossible for the following reason. If $\alpha \neq \beta^3$, $\beta \in Q(\alpha)$ then $\alpha^{m/3}$ is of degree 3 over $Q(\alpha)$ and cannot satisfy the equation $\lambda_1 t^2 - ct \pm \lambda_2 \equiv 0$ for any choice of sign. If $\alpha = \beta^3$, $\beta \in Q(\alpha)$ then β satisfies an equation $t^2 - dt - 1 = 0$, d integer, and we get $a = \operatorname{Tr}\beta^3 = d^3 + 3d$, contrary to the assumption.

Lemma 10. *If every integral vector $[t_1, \ldots, t_k]$ satisfies at least one congruence of the set S:*

$$a_{h0} + \sum_{j=1}^{k} a_{hj} t_j \equiv 0 \bmod m \quad (1 \leqslant h \leqslant g) \tag{48}$$

and no proper subset of S has the same property then for all h, j

$$M(g)\, a_{hj} \equiv 0 \bmod m,$$

where

$$M(g) = \prod_{\substack{p \leqslant g \\ p \text{ prime}}} p^{\left[\frac{g-1}{p-1}\right]}.$$

Proof. Let $d_h = (a_{h1}, a_{h2}, \ldots, a_{hk}, m)$. If $d_h \nmid a_{h0}$ the congruence

$$\sum_{j=1}^{k} a_{hj} t_j + a_{h0} \equiv 0 \bmod m$$

is never satisfied contrary to the minimal property of S. Hence for all h

$$a_{h0} \equiv 0 \bmod d_h \tag{49}$$

and the congruences (48) take the form

$$\sum_{j=1}^{k} \frac{a_{hj}}{d_h} t_j + \frac{a_{h0}}{d_h} \equiv 0 \bmod \frac{m}{d_h} \quad (1 \leqslant h \leqslant g). \tag{50}$$

For a given prime p let n_r be the number of indices $h \leqslant g$ such that $p^r \| \frac{m}{d_h}$ and let s be the largest r with $n_r \neq 0$. We have

$$\frac{n_r}{p} + \frac{n_{r+1}}{p^2} + \ldots + \frac{n_s}{p^{s-r+1}} \geqslant 1 \quad (1 \leqslant r \leqslant s). \tag{51}$$

In order to prove this assume that for a certain $r \leqslant s$

$$\frac{n_r}{p} + \frac{n_{r+1}}{p^2} + \ldots + \frac{n_s}{p^{s-r+1}} < 1. \tag{52}$$

The congruences (48) with $p^r \nmid \frac{m}{d_h}$ form a proper subset of the set S and by the assumption there is a vector $\boldsymbol{t}^0$ which does not satisfy any of them.

On the other hand, a congruence (50) with $p^q \| \frac{m}{d_h}$ $(q \geqslant r)$ is in virtue of Frobenius's theorem (used in proof of Lemma 8) satisfied by at most

$$\left(\frac{a_{h1}}{d_h}, \ldots, \frac{a_{hk}}{d_h}, p^{q-r+1}\right) p^{(q-r+1)(k-1)} = p^{(q-r+1)(k-1)}$$

integral vectors $\boldsymbol{t} \bmod p^q$ satisfying

$$\boldsymbol{t} \equiv \boldsymbol{t}^0 \bmod p^{r-1}. \tag{53}$$

The alternative of all congruences in question is satisfied by at most $\sum_{q=r}^{s} \frac{n_q}{p^{q-r+1}} p^{(s-r+1)k}$ integral vectors $\boldsymbol{t} \bmod p^s$ satisfying (53). Since the number of all integral vectors $\boldsymbol{t} \bmod p^s$ satisfying (53) is $p^{(s-r+1)k}$ (52) implies the existence of a vector $\boldsymbol{t}_1 \equiv \boldsymbol{t}_0 \bmod p^{r-1}$ which satisfies no congruence (50) and consequently no congruence (48) with $p^r \mid \frac{m}{d_h}$. By the Chinese remainder theorem there exists a vector $\boldsymbol{t}$ such that

$$\boldsymbol{t} \equiv \boldsymbol{t}_0 \bmod \text{l.c.m.}_{p^r \nmid m/d_h} \frac{m}{d_h},$$

$$\boldsymbol{t} \equiv \boldsymbol{t}_1 \bmod p^s.$$

This vector satisfies no congruence (48). The obtained contradiction proves (51).

Consider the lower bound of the function $n_1 + n_2 + \ldots + n_s = f(n_1, \ldots, n_s)$ under the condition (51), where now $n_1, \ldots, n_s$ are non-negative real numbers. Since $f(n_1, n_2, \ldots, n_s) \geqslant \max_{1 \leqslant r \leqslant s} n_r$ the lower bound is attained.

Let $(n_1^{(0)}, \ldots, n_s^{(0)})$ be a point in which it is attained. We shall show by induction with respect to $s-r$

$$n_r^{(0)} = p-1 \quad (1 \leqslant r < s), \quad n_s^{(0)} = p. \tag{54}$$

Indeed (51) for $r = s$ gives $n_s^{(0)} \geqslant p$. If $n_s^{(0)} > p$, we set $n_r^{(1)} = n_r^{(0)}$ for $r < s-1$, $n_{s-1}^{(1)} = n_{s-1}^{(0)} + \frac{1}{p}(n_s^{(0)} - p)$, $n_s^{(1)} = p$, verify (51) and find $f(n_1^{(1)}, \ldots, n_s^{(1)}) < f(n_1^{(0)}, \ldots, n_s^{(0)})$ which is impossible. Assume now that (54) holds for $s-r < s-q$, i.e. $r > q$. The condition (51) for $r = q$ gives

$$\frac{n_q^{(0)}}{p} \geqslant 1 - \sum_{q=r+1}^{s-1} \frac{p-1}{p^{q-r+1}} - \frac{p}{p^{s-r+1}} \frac{p-1}{p}; \quad n_q^{(0)} \geqslant p-1.$$

If $n_q^{(0)} > p-1$, we set

$$n_r^{(1)} = n_r^{(0)} \quad \text{for} \quad r \neq q-1, q;$$

$$n_{q-1}^{(1)} = n_{q-1}^{(0)} + \frac{1}{p}(n_q^{(0)} - p + 1), \quad n_q^{(1)} = p-1,$$

verify (51) and find again

$$f(n_1^{(1)}, \ldots, n_s^{(1)}) < f(n_1^{(0)}, \ldots, n_s^{(0)}),$$

which is impossible.

Since $n_1^{(0)} + \ldots + n_s^{(0)} \leqslant g$ it follows from (54) that

$$s(p-1) + 1 \leqslant g, \quad s \leqslant \left[\frac{g-1}{p-1}\right]$$

and thus for all $h \leqslant g$, $\frac{m}{d_h} \mid M(g)$.

This together with (49) gives the lemma.

LEMMA 11. *If every integral vector $[t_1, \ldots, t_r]$ satisfies at least one of the congruences*

$$a_{h0} + \sum_{s=1}^{r} a_{hs} t_s \equiv 0 \bmod m \tag{55}$$

$(1 \leqslant h \leqslant g)$ then for at least one h

$$a_{h0} \equiv 0 \bmod m \quad \text{and} \quad M(g) a_{hs} \equiv 0 \bmod m \quad (1 \leqslant s \leqslant r), \tag{56}$$

where $M(g)$ has the meaning of Lemma 10.

Proof. Choose in $\{1, 2, \ldots, g\}$ a minimal subset M with the property that every integral vector satisfies at least one congruence (55) with $h \in M$. To the set of these congruences Lemma 10 applies. The congruence satisfied by the vector $[0, 0, \ldots, 0]$ satisfies also the conditions (56).

Remark. $M(g)$ is the least number with the property formulated in Lemmata 10 and 11, as the following example shows already in dimension one: $m = p^{\left[\frac{g-1}{p-1}\right]}$ (p prime), $a_{11} = 1$, $a_{10} = 0$ and for $h = (p-1)q + r + 1$, $1 \leqslant r \leqslant p-1$, $2 \leqslant h \leqslant g$, $a_{h1} = p^q$, $a_{h0} = \dfrac{m}{p} r$.

For $k = 1$ Lemma 10 is contained in a stronger result of S. Znám, however his proof does not extend to $k > 1$.

Lemma 12. *Let H, I be two finite sets and let M_{hi} ($h \in H$, $i \in I$) be inhomogeneous linear forms with integral coefficients. If for every positive integer m and a suitable $h \in H$ the system of congruences*

$$M_{hi}(x) \equiv 0 \bmod m \qquad (i \in I) \tag{57}$$

is soluble then for a suitable $h \in H$ the system of equations

$$M_{hi}(x) = 0 \qquad (i \in I) \tag{58}$$

is soluble in integers.

Proof. Suppose that no system (58) is soluble in integers. Then by Lemma 9 of [6] for each $h \in H$ there exists an m_h such that the system (57) is insoluble for $m = m_h$. Taking $m = \prod_{h \in H} m_h$ we infer that the system (57) is insoluble for any $h \in H$ contrary to the assumption.

Proof of Theorem 6. Let us set

$$\alpha_{hij} = \zeta_w^{a_{hij0}} \prod_{s=1}^{r} \pi_s^{a_{hijs}}, \qquad \beta_{hi} = \zeta_w^{b_{hi0}} \prod_{s=1}^{r} \pi_s^{b_{his}}, \tag{59}$$

where w is the number of roots of unity contained in K and π_s are elements of the multiplicative basis described in Lemma 9. Consider the linear forms

$$\begin{aligned} L_{hi0} &= wx_0 + \sum_{j=1}^{k} a_{hij0} x_j - b_{hi0}, \\ L_{his} &= \sum_{j=1}^{k} a_{hijs} x_j - b_{his} \qquad (1 \leqslant s \leqslant r) \end{aligned} \tag{60}$$

and let H be the set of all vectors $\boldsymbol{h} = [h_1, h_2, \ldots, h_l]$ with $1 \leqslant h_i \leqslant g_i$ ($1 \leqslant i \leqslant l$), I be the set of all vectors $\boldsymbol{i} = [i, s]$ with $1 \leqslant i \leqslant l$, $0 \leqslant s \leqslant r$.

For any $\boldsymbol{h} \in H$, $\boldsymbol{i} = [i, s] \in I$ we put

$$M_{\boldsymbol{hi}} = L_{h_i i s}. \tag{61}$$

We assert that for any positive integer m there exists an $\boldsymbol{h} \in H$ such that the system of congruences

$$M_{\boldsymbol{hi}}(x_0, x_1, \ldots, x_k) \equiv 0 \bmod m \qquad (\boldsymbol{i} \in I) \tag{62}$$

is soluble.

Let us take $n = 2^{\tau} w M(\max g_i)\, m \underset{\substack{q \leqslant m + \max g_i \\ q \text{ prime}}}{\text{l.c.m.}} (q-1)$, where τ is the relevant parameter of K.

By Theorem 4 for any choice of $t_1, \ldots, t_r \bmod n/w$ there exists a prime ideal $\mathfrak{p}$ of $K(\zeta_n)$ prime to D such that

$$\left(\frac{\zeta_w}{\mathfrak{p}}\right)_n = \zeta_w, \qquad \left(\frac{\pi_r}{\mathfrak{p}}\right)_n = \zeta_n^{w t_s} \qquad (1 \leqslant s \leqslant r).$$

Let $\mathfrak{m}$ be the product of all these prime ideals $\mathfrak{p}$.

The solubility of the system of congruences

$$\prod_{h=1}^{g_i} \left(\prod_{j=1}^{k} \alpha_{hij}^{x_j} - \beta_{hi} \right) \equiv 0 \bmod \mathfrak{m} \qquad (i = 1, \ldots, l) \tag{63}$$

implies that for any vector $[t_1, \ldots, t_r]$ and any $i \leqslant l$ there is an $h \leqslant g_i$ such that

$$\prod_{j=1}^{k} \alpha_{hij}^{x_j} \equiv \beta_{hi} \bmod \mathfrak{p}, \qquad \prod_{j=1}^{k} \left(\frac{\alpha_{hij}}{\mathfrak{p}}\right)_n^{x_j} = \left(\frac{\beta_{hi}}{\mathfrak{p}}\right)_n$$

for some $\mathfrak{p}$ satisfying (63). This implies by (59) that

$$\sum_{j=1}^{k} \left(\frac{n}{w} a_{hij0} + \sum_{s=1}^{r} w t_s a_{hijs} \right) x_j \equiv \frac{n}{w} b_{hi0} + \sum_{s=1}^{r} w t_s b_{his} \bmod n,$$

whence

$$\frac{n}{w} \left(\sum_{j=1}^{k} a_{hij0} x_j - b_{hi0} \right) + w \sum_{s=1}^{r} t_s \left(\sum_{j=1}^{k} a_{hijs} x_j - b_{his} \right) \equiv 0 \bmod n.$$

Using now Lemma 11 we get that for any $i \leqslant l$ and a certain $h_i \leqslant g_i$

$$\sum_{j=1}^{k} a_{h_i ij0} x_j - b_{h_i i0} \equiv 0 \bmod w,$$

$$\sum_{j=1}^{k} a_{h_i ijs} x_j - b_{h_i ir} \equiv \bmod m \qquad (1 \leqslant s \leqslant r).$$

In virtue of (60) and (61) this is equivalent for a suitable x_0 to the system

(62) in which $\boldsymbol{h} = [h_1, \ldots, h_l]$. Therefore, by Lemma 12 there exists a vector $\boldsymbol{h}^0 = [h_1^0, \ldots, h_l^0]$ such that the system of equations

$$M_{\boldsymbol{h}^0 i}(x_0, x_1, \ldots, x_k) = 0 \quad (i \in I)$$

is soluble in integers. Denoting a solution by $[x_0^0, x_1^0, \ldots, x_k^0]$ we get from (60) and (61) for all $i \leqslant l$

$$wx_0^0 + \sum_{j=1}^{k} a_{h_i^0 ij0} x_j^0 - b_{h_i^0 i0} = 0,$$

$$\sum_{j=1}^{k} a_{h_i^0 ijs} x_j^0 - b_{h_i^0 is} = 0 \quad (1 \leqslant s \leqslant r)$$

hence by (59)

$$\prod_{h=1}^{g_i} \Big(\prod_{j=1}^{h} \alpha_{hij}^{x_j^0} - \beta_{hi} \Big) = 0 \quad (1 \leqslant i \leqslant l).$$

References

[1] G. Darbi, *Sulla reducibilità delle equazioni algebriche*, Annali Mat. Pura Appl. 4 (1925), pp. 185–208.

[2] H. Hasse, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*, J. Reine Angew. Math. 188 (1950), pp. 40–64.

[3] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*, Ges. Abhandlungen, Band I, Reprint New York, 1965.

[4] M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. 26 (1975), pp. 307–308.

[5] W. H. Mills, *Characters with preassigned values*, Canad. J. Math. 15 (1963), pp. 169–171.

[6] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. 27 (1975), pp. 397–420.

[7] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Vid. akad. Avh. Oslo I, 1937, nr 12.

[8] — *On the existence of a multiplicative basis for an arbitrary algebraic field*, Norske Vid. Selsk. Forh. (Trondheim) 20 (1947), nr 2.

[9] N. G. Tschebotarëw (Čebotarev), *Über einen Satz von Hilbert*, Vestnik Ukr. Akad. Nauk, 1923, pp. 3–7.

[10] N. Tschebotarëw, H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Groningen-Djakarta 1950.

[11] S. Znám, *On properties of systems of arithmetic sequences*, Acta Arith. 26 (1975), pp. 279–283.

Correction to [6]

p. 401: insert after formula (8):

$$\text{provided } p_i > 2,\ a \equiv 1 \bmod p_i \text{ or } p_i = 2,\ a \equiv 1 \bmod 4.$$

Received on 15. 10. 1975 (772)

ACTA ARITHMETICA
XXXII (1977)

Diophantine approximation in power series fields*

by

WOLFGANG M. SCHMIDT (Boulder, Colo.)

Dedicated to Professor Theodor Schneider on his 65th birthday

1. Introduction

1.1. The setting. Let K be the field of formal series

$$a = a_k X^k + a_{k-1} X^{k-1} + \ldots \tag{1}$$

with an arbitrary integer k and with coefficients in a given field F of characteristic zero. The rational functions in X with coefficients in F form a subfield $K_0 = F(X)$ of K, and the polynomials form a subring $S = F[X]$. In K we have the non-archimedean valuation with

$$|a| = 2^k$$

if the leading coefficient in (1) is $a_k \neq 0$. If f is a polynomial, then

$$|f| = 2^{\deg f}.$$

Many results on "ordinary" diophantine approximation, i.e. approximation of reals by rationals, carry over to approximation of elements of K by rational functions, i.e. by elements of K_0.

For example, Dirichlet's Theorem holds: *If $\alpha \in K$ does not lie in K_0, then there are infinitely many rational functions $f/g = f(X)/g(X)$ in K_0 with*

$$|\alpha - (f/g)| \leqslant |g|^{-2}.$$

Also Liouville's Theorem holds: *If $\alpha \in K$ is algebraic over K_0 of degree $s > 1$, then for every rational function f/g, we have*

$$|\alpha - (f/g)| > c_1(\alpha) |g|^{-s}, \tag{2}$$

with a constant $c_1(\alpha) > 0$. Now just as in ordinary diophantine approxi-

* Written with partial support from NSF-MPS75-08233.