Séminaire Delange-Pisot-Poitou.
Théorie des nombres

W. Dale Brownawell

Pairs of polynomials small at a number to certain algebraic powers

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 17, n° 1 (1975-1976), exp. n° 11, p. 1-12
<http://www.numdam.org/item?id=SDPP_1975-1976__17_1_A11_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
17e année, 1975/76, n° 11, 12 p.

15 décembre 1975

PAIRS OF POLYNOMIALS SMALL AT A NUMBER TO CERTAIN ALGEBRAIC POWERS

by W. Dale BROWNAWELL (*)

In 1949, A. O. GEL'FOND [6] proved that when α is algebraic, $\alpha \neq 0$, $\log \alpha \neq 0$, and β is a cubic irrational, then α^β and α^{β^2} are algebraically independent. Almost immediately thereafter GEL'FOND and N. I. FEL'DMAN [7] were able to show that for fixed $\varepsilon > 0$, when $P[x , y] \in \mathbb{Z}[x , y]$ is non-zero with

$$\deg_x P + \deg_y P + \log \text{height } P = t \geqslant t_0(\alpha , \beta , \varepsilon) ,$$

then

$$\log |P(\alpha^\beta , \alpha^{\beta^2})| \geqslant - \exp(t^{4+\varepsilon}) .$$

For this, they used Gel'fond's transcendence measure [6] for α^β.

In 1974, G.V. ČUDNOVSKIJ [5] significantly extended the method of GEL'FOND and FEL'DMAN to show that in certain specific sets of numbers at least three are algebraically independent. Using some of these ideas, M. WALDSCHMIDT and the author [3] recently showed that if α is only very well approximated by algebraic numbers in an appropriate sense, then α^β and α^{β^2} are still algebraically independent.

Later the author [2] remarked that when α itself is not algebraic, then these ideas suffice to show that α, α^β and α^{β^2} are algebraically independent when α is well approximated by algebraic numbers.

1. Statement of results and preliminary comments.

THEOREM 1. - Let $\alpha , \beta \in \mathbb{C}$, $\alpha \neq 0$, $\log \alpha \neq 0$ with β cubic irrational. Then there is a constant C, depending only on β and $\log \alpha$, such that for relatively prime polynomials $R(x , y)$, $S(x , z) \in \mathbb{Z}[x , y , z]$ the following inequality holds :

$$\log \max \{ |R(a_0 , a_1)| , |S(a_0 , a_2)| \} \geqslant - \exp (C d^{11/2} d_1^2 \log h) ,$$

where

$$d = (\deg_y R) , (\deg_z S) > 0 ,$$

$$d_1 = \deg_x R + \deg_x S > 0 ,$$

$$\log h = d_1 + \log \text{ht } R + \log \text{ht } S ,$$

(*) Research supported in part by the National Science Foundation.

and a_0 , a_1 , a_2 *is an arbitrary permutation of* α , α^β , α^{β^2} .

As usual, height, abreviated ht, denotes the maximum absolute value of the coefficients of a polynomial.

When d or d_1 is zero, one of the variables x , y or z does not actually occur. Then a direct argument using a very recent result of M. MIGNOTTE and M. WALDSCHMIDT [8] applies (see remark 3 below). The result of MIGNOTTE and WALDSCHMIDT has the following corollary :

THEOREM. – *Let* $a \in \underset{\sim}{C}$, $a \neq 0$, $\log a \neq 0$, *and* b *be algebraic irrational. Then for any non-zero* $P(x), Q(x) \in \underset{\sim}{Z}[x]$ *with*

$$\deg P + \deg Q + \log \operatorname{ht} P + \log \operatorname{ht} Q = t \geqslant t_0 ,$$

we have

$$\log \max\{ |P(a)| , |Q(a^b)| \} \geqslant - t^{11} .$$

As a consequence of theorem 1, one can deduce a non-trivial lower bound for arbitrary relatively prime polynomials at $(\alpha , \alpha^\beta , \alpha^{\beta^2})$ in which x , y and z actually occur. Theorem 1 deals with the case that at most one variable occurs in both R and S .

THEOREM 2. – *Let* α , β , a_0 , a_1 , a_2 *be as above. There is a positive constant* B , *depending only on* β *and* $\log \alpha$, *such that for any relatively prime polynomials* $R(x , y)$, $S(x , y , z) \in \underset{\sim}{Z}[x , y , z]$, *we have*

$$\log \max\{ |R(a_0 , a_1)| , |S(a_0 , a_1 , a_2)| \} \geqslant - \exp(B\, d^{11/2}\, d_1^2 \log h) ,$$

where

$$d = (\deg_y R)^2 (\deg_z S) > 0 ,$$

$$d_1 = \deg_x R \deg_y S + \deg_y R \deg_x S ,$$

$$\log h = d_1 + \deg_y R \log \operatorname{ht} S + \deg_y S \log \operatorname{ht} R ,$$

and

$$\deg_y S > 0 , \quad \deg_x R + \deg_x S > 0 .$$

After a permutation of a_0 , a_1 , a_2 if necessary, it is clear that theorems 1 and 2 cover any case where R and S have at most two variables in common and a direct argument from the result of MIGNOTTE and WALDSCHMIDT is impossible. The remaining cases are covered by the following result :

THEOREM 3. – *Let* α , β , a_0 , a_1 , a_2 *be as above. There is a positive constant* $\mathfrak{a}$, *depending only on* β *and* $\log \alpha$, *such that for any relatively prime polynomials* $R(x , y , z)$, $S(x , y , z) \in \underset{\sim}{Z}[x , y , z]$, *each involving* x , y *and* z , *we have*

$$\log \max\{|R(a_0, a_1, a_2)|, |S(a_0, a_1, a_2)|\} \geq \exp - \mathfrak{X} d^{11/2} d_1^2 \log h) ,$$

<u>where</u>

$$d = \{(\deg_y R)(\deg_z S) + (\deg_z R)(\deg_y S)\}^2 ,$$

$$d_1 = \deg_x R(\deg_y S + \deg_z S) + \deg_x S(\deg_y R + \deg_z R) ,$$

$$\log h = d_1 + (\deg_y R + \deg_z R)\log \operatorname{ht} S + (\deg_y S + \deg_z S)\log \operatorname{ht} R .$$

The spirit of the theorem is thus that any two polynomials which are both small at $(\alpha, \alpha^\beta, \alpha^{\beta^2})$ must have a non-constant common factor. The title was chosen to reflect this way of expressing the results.

The results in this report represent the third stage in the investigations beginning with the joint work with WALDSCHMIDT. Since we do not assume α to be algebraic, we have no transcendence measure for α^β, as did GEL'FOND and FEL'DMAN. Instead we use the above consequence of the result of MIGNOTTE and WALDSCHMIDT [8] which gives a lower bound on simultaneous approximations to a, b, a^b ($a \neq 0$, $\log a \neq 0$, $b \notin \mathbb{Q}$) by algebraic numbers. The results in this direction by T. SCHNEIDER [10], A.A. ŠMELEV [9] or P. BUNDSCHUH [4] would have sufficed, except that they concerned only approximation by algebraic numbers of bounded degree. There are many such results on the simultaneous approximation of certain numbers by algebraic numbers or, equivalently on the simultaneous smallness of polynomials over $\mathbb{Z}$ in each of the given numbers. However the results above seem to be the first which give lower bounds on the simultaneous smallness of two relatively prime polynomials in three quantities.

<u>Preliminary remarks.</u>

1° In view of lemma 3, we can assume that R and S are irreducible.

2° It is immediate from lemma 5 that two small relatively prime polynomials can not involve just one of the a_0, a_1, a_2.

3° In fact, two relatively prime polynomials which do not involve all three variables between them can be treated directly by the result of MIGNOTTE and WALDSCHMIDT : Say R and S involve only a_0 and a_1. Then using an argument on resultants to alternately eliminate the variables occuring in both R and S, we obtain non-zero polynomials $P(a_0) \in \mathbb{Z}[a_0]$, $Q(a_1) \in \mathbb{Z}[a_1]$ with

$$\deg P , \deg Q \leq d_2 = (1 + \deg_x R)(1 + \deg_y S) + (1 + \deg_x S)(1 + \deg_y R)$$

$$\log \operatorname{ht} P \leq h_1 = (1 + \deg_y R)(1 + \log \operatorname{ht} S) + (1 + \deg_y S)(1 + \log \operatorname{ht} R)$$

$$\log \operatorname{ht} Q \leq h_2 = (1 + \deg_x R)(1 + \log \operatorname{ht} S) + (1 + \deg_x S)(1 + \log \operatorname{ht} R) ,$$

and

$$|P(a_0)| \leq (1 + e + |a_0|)^{d_2} e^{h_1} \max\{|R(a_0, a_1)|, |S(a_0, a_1)|\} ,$$

$$|Q(a_1)| \leq (1 + e + |a_1|)^{d_2} e^{h_2} \max\{|R(a_0, a_1)|, |S(a_0, a_1)|\} ,$$

as in [1] (p. 6-7, 10-11).

4° For similar reasons, we may assume that <u>there is a constant</u> $\varepsilon > 0$, <u>depending only on</u> β <u>and</u> $\log \alpha$ <u>such that when</u> $B[a_0] \in \mathbb{Z}[a_0]$ <u>is non-zero with</u>

$$\deg B \leqslant (\deg R + \deg S)$$

$$\log \mathrm{ht}\, B \leqslant (\log \mathrm{ht}\, R + \log \mathrm{ht}\, S + \deg R + \deg S) \quad ,$$

<u>then</u>

$$\log |B(a_0)| > -\varepsilon(\deg R + \deg S + \log \mathrm{ht}\, R + \log \mathrm{ht}\, S)^{22} .$$

Otherwise we could take the resultant of $B(x)$ and R (or S) with respect to x ([1] p. 6-7, 10-11) to obtain a small non-zero polynomial in a_1 (or a_2), which together with $B(a_0)$ would contradict the result of MIGNOTTE and WALDSCHMIDT.

5° One uses similar arguments with resultants to deduce theorem 2 from theorem 1 by eliminating y between R and S . The resultant plays the role of S in theorem 1. For theorem 3, one eliminates both z and y , alternately. The first resultant plays the role of R and the second that of S in theorem 1.

<u>Notation</u>. - The gothic lower case letters $\mathfrak{l}$, $\mathfrak{m}$, $\mathfrak{n}$ will denote triples of integers given by corresponding Greek letters, and absolute value signs will denote the sup norm. E. g. $\mathfrak{l} = (\lambda_0 , \lambda_1 , \lambda_2) \in \mathbb{Z}^{(3)}$ and $|\mathfrak{l}| = \max_{i=0,1,2} |\lambda_i|$. The coordinates of $\mathfrak{l}$ and $\mathfrak{n}$ will be non-negative. In addition, we set $\mathfrak{b} = (1 , \beta , \beta^2)$, $\mathfrak{l}.\mathfrak{b} = \lambda_0 + \lambda_1 \beta + \lambda_2 \beta^2$ and similarly for $\mathfrak{n}.\mathfrak{b}$..

The letters c_1 , c_2 , c_3 , ... will denote positive constants depending only on β and $\log \alpha$.

2. Auxiliary lemmas .

LEMMA 1. - <u>Let</u>

$$P(x , y) = P_0(x)y^n + P_1(x)y^{n-1} + \ldots + P_n(x) \in \mathbb{Z}[x , y]$$

<u>and</u> $P(x , \xi) = 0$. <u>Then for every positive integer</u> $r \geqslant n$, <u>we can write</u>

$$(P_0(x)\xi)^r = P_{r,0}(x)\xi^{n-1} + \ldots + P_{r,n-1}(x)$$

<u>with each</u> $P_{r,j}(x) \in \mathbb{Z}[x]$ <u>satisfying</u>

(i) $\deg P_{r,j}(x) \leqslant (r + 1 - n)\deg_x P(x , y)$

(ii) $\text{height } P_{r,j} \leqslant (1 + (1 + \deg_x P)\text{height } P)^{r+1-n}$
$\leqslant (e^{\deg_x P}\, \mathrm{ht}\, P)^{r+1-n}$.

The lemma clearly holds for $r = n$ and follows for $r > n$ by a straight-forward induction.

LEMMA 2. - <u>Let</u> R <u>and</u> S <u>be positive integers,</u> $2R < S$, <u>and let</u> $a_{ij} \in \mathbb{Z}[x]$,

$1 \leq i \leq R$, $1 \leq j \leq S$, satisfy

$$\deg a_{ij} \leq d , \quad \text{height } a_{ij} \leq A \text{ where } A \geq 1 .$$

Then there exist polynomials $f_1 , \dots , f_S \in \mathbb{Z}[x]$, not all zero, satisfying

$$\deg f_j \leq d , \quad \text{height } f_j \leq ((1 + d^2)SA)^{2R/(S-2R)}$$

and

$$\sum_{j=1}^{S} a_{ij} f_j = 0 , \quad 1 \leq i \leq R .$$

For a proof, see [1], lemma 5.2.

LEMMA 3. – <u>Suppose</u> $P(x , y) , Q(x , y) \in \mathbb{C}[x , y]$. <u>Then</u>

$$(\text{height } PQ)\, e^{\deg_x PQ + \deg_y PQ} \geq (\text{height } P)(\text{height } Q) .$$

For a proof, see [6], lemma 2, p. 135, or [11], lemma 3, p. 149, where a particularly clear exposition of the fundamental one variable result is given.

LEMMA 4. – <u>Suppose</u> $F(z) = \sum_{|n|<N} A_n e^{(n.b)z}$ <u>and</u>

$$b_0 = \min_{0<|n|<N} (1 , |n.b| \min(1 , |\log \alpha|))$$

$$b = \max_{|n|<N} (1 , |n.b| \max(1 , |\log \alpha|))$$

$$E = \max_{\substack{|n|<L\leq N \\ 0\leq p<P}} |F^{(p)}((n.b)\log \alpha)| .$$

<u>If</u> $PL^3 \geq 2N^3 + 13 b^2$, <u>then</u>

$$\max |A_n| \leq L^3((N^3)!)^{1/2} e^{7b^2} (2bb_0)^{-N^3} (72b/b_0 L^{3/2})^{PL^3} E .$$

For a proof, see [12].

LEMMA 5. – <u>Let</u> $f(x) , g(x) \in \mathbb{Z}[x]$ <u>have heights</u> $|f| , |g|$ <u>and degrees</u> m , n , <u>respectively</u>. <u>Then</u> $f(x)$ <u>and</u> $g(x)$ <u>have a common non-constant divisor in</u> $\mathbb{Z}[x]$ <u>if, and only if, for some</u> $\omega \in \mathbb{C}$,

$$\max\{ |f(\omega)| , |g(\omega)|\} |f|^n |g|^m (m + n)^{m+n} < 1 .$$

For a proof, see [6], lemma V, p. 145–146.

LEMMA 6. – <u>Suppose</u> $\omega \in \mathbb{C}$ <u>and</u> $P(x) \in \mathbb{Z}[x]$ <u>satisfy</u> $|P(\omega)| < e^{-\lambda d(h+d)}$ <u>where</u> $\lambda \geq 3$, $d \geq \deg P$, $e^h \geq \text{height } P$. <u>Then there is a factor</u> $Q(x)$ <u>of</u> $P(x)$ <u>which is a power of an irreducible polynomial in</u> $\mathbb{Z}[x]$ <u>such that</u>

$$\log |Q(\omega)| < - (\lambda - 1) d(h + d) .$$

For a proof, see [6], lemma VI, p. 147.

LEMMA 7. – <u>Suppose</u> $\omega \in \mathbb{C}$ <u>is transcendental and</u> $\xi \in \mathbb{C}$ <u>satisfies a monic poly-</u>

<u>nomial</u> f <u>of degree</u> $\leqslant d$ <u>which has coefficients in</u> $\underset{\sim}{Z}[\omega]$ <u>of degree</u> $\leqslant \delta$, <u>and height</u> $\leqslant e^{\chi}$. <u>Let</u> λ_1 , λ_2 <u>be real numbers satisfying</u>

$$\lambda_1 > \lambda_2 > 6 + 2 \log(d + 1) + 2 \log(|\omega| + 1) .$$

If

$$- \lambda_1 \delta(\delta + \chi) \leqslant \log|\xi| \leqslant - \lambda_2 \delta(\delta + \chi) ,$$

<u>then there exist an irreducible polynomial</u> $P(\omega) \in \underset{\sim}{Z}[\omega]$ <u>and an integer</u> $s \geqslant 1$ <u>such that</u> P^s <u>divides the constant term of</u> f <u>and that</u>

$$-3d\lambda_1 , \delta(\delta + \chi) \leqslant \log|P(\omega)| \leqslant - \frac{\lambda_2}{6s} \delta(\delta + \chi) .$$

For a proof, see [3], lemma 6, where a little less is claimed.

LEMMA 8 (Newton's Identities). - <u>If</u> $\alpha_1 , \dots , \alpha_n$ <u>are the roots of</u>

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n \quad \text{and} \quad S_k = \alpha_1^k + \dots + \alpha_n^k , \quad 1 \leqslant k \leqslant n ,$$

<u>then</u> for $1 \leqslant k \leqslant n$,

$$S_k + a_1 S_{k-1} + \dots + a_{k-1} S_1 + k a_k = 0 .$$

3. Proof of theorem 1.

This proof has much in common with those of [2] and [3]. When the details are the same, we shall indicate briefly the basic idea and refer to [3]. For definiteness, we shall prove the case $a_0 = \alpha$, $a_1 = \alpha^{\beta}$, $a_2 = \alpha^{\beta^2}$ below. The other cases are essentially the same.

STEP 0 = <u>Setting the stage</u>. - We assume for the sake of argument that the assertion of the theorem fails for C and $d^{11/2} d_1^2 \log h$ sufficiently large, depending on β , $\log \alpha$, (by tracing through the proof, one can state explicitly what one is requiring). We take

$b \in N$ such that $b\beta$ is an algebraic integer,

$B_1 \in \underset{\sim}{Z}[\alpha]$ to be the leading coefficient of $R(\alpha , y)$ with respect to y ,

$B_2 \in \underset{\sim}{Z}[\alpha]$ to be the leading coefficient of $S(\alpha , z)$ with respect to z ,

ξ_1 to be a root of $R(\alpha , y)$ closest to α^{β} , and

ξ_2 to be a root of $S(\alpha , z)$ closest to α^{β^2} .

As in the proof of lemma 3.11 of [1], p. 12, one has that

$$|\alpha^{\beta} - \xi_1| \leqslant 2^{\deg_y R} |R(\alpha , \alpha^{\beta})| / |R_2(\alpha , \alpha^{\beta})|$$
$$|\alpha^{\beta^2} - \xi_2| \leqslant 2^{\deg_z S} |S(\alpha , \alpha^{\beta^2})| / |S_3(\alpha , \alpha^{\beta^2})| ,$$

where the subscript 2 (or 3) denotes partial differentiation with respect to y (or z). Applying the lower bound, we have for polynomials in α to the resultant of R and R_2 with respect to y (and S and S_3 with respect to z) we have that

(1) $$\log|\alpha^\beta - \xi_1| \,,\ \log|\alpha^{\beta^2} - \xi_2| \leqslant - \exp((C-1)d^{11/2}\, d_1^2 \log h) \,.$$

Moreover

(2) $$\log|B_1| \,,\ \log|B_2| \geqslant - \varepsilon(\deg R + \deg S + \log \mathrm{ht}\, R + \log \mathrm{ht}\, S)^{22} \,.$$

Let

$$N_0 = [\exp(Cd^{11/2}\ d_1^2 \,,\ \log h/7)] \,, \qquad N_1 = [N_0^2 \log N_0] \,.$$

It is easy to verify that when $d^{11/2}\, d_1^2 \log h$ is large enough,

$$N_1^3 \log N_1 < \exp(13Cd^{11/2}\ d_1^2 \log h/14) \,.$$

For $N_0 \leqslant N \leqslant N_1$, we define

$$L_N = [N^{1/2}(\log N/d \log h)^{1/4}]$$
$$P_N = [N^{3/2}(\log h/\log N)^{3/4}/12d^{1/4}]$$
$$H_N = [N^{3/2}(\log N)^{1/4}\ (\log h)^{3/4}/d^{1/4}] \,.$$

Note that

$$NL_N \log h + P_N \log N < 2H_N \,.$$

STEP 1. – We show that <u>there exist</u> $\varphi(n) \in \underset{\sim}{Z}[\alpha]$, $|n| < N$, <u>not all zero and even without a common divisor in</u> $\underset{\sim}{Z}[\alpha]$ <u>satisfying</u>

$$\log(\text{height } \varphi(n)) \leqslant c_1 H_N \,,$$
$$\text{degree } \varphi(n) \leqslant c_2\, d_1\, NL_N$$

<u>such that the function</u>

$$F_N(z) = \sum_{|n|<N} \varphi(n) \exp((n.b)z)$$

<u>satisfies</u>

$$\log|F_N(z)|_{|z|=N^{4/3}} \leqslant - c_3\, N^3 \log N/d \,.$$

(A) Consider for $|l| < L$, $0 \leq p < P_N$ the expressions

$$b^{2P_N}(B_1 B_2)^{C_5 NL_N}(\alpha\xi_1 \xi_2)^{C_4 NL_N} \sum_{|n|<N} \varphi(n)(n.b)^p\, \alpha^{\mu_0}\, \xi_1^{\mu_1}\, \xi_2^{\mu_2}$$

where $\mu_0 , \mu_1 , \mu_2 \in \underset{\sim}{Z}$ satisfy

$$b^2(n.b)(l.b) = \mu_0 + \mu_1\, \beta + \mu_2\, \beta^2 \,.$$

(Multiplying by $(\alpha\xi_1 \xi_2)^{C_4 NL_N}$ with C_4 large enough ensures that the powers of α , ξ_1 , and ξ_2 appearing are non-negative.) Since $B_1 \xi_1$ and $B_2 \xi_2$ are integral over $\underset{\sim}{Z}[\alpha]$, we use lemma 1 to rewrite the above expressions as

$$\Phi_{p,I} = \sum_n \varphi(n)(\pi_0 + \pi_1 \beta + \pi_2 \beta^2) \sum P_{k_1,k_2}(\alpha)(B_1 \xi_1)^{k_1} (B_2 \xi_2)^{k_2}$$

where (k_1, k_2) runs over all pairs with $0 \leq k_1 < \deg_y R$, $0 \leq k_2 < \deg_z S$ and where $\pi_i \in \underset{\sim}{Z}$ with $\log|\pi_i| \leq c_6 P_N \log N$ and where $P_{k_1,k_2}(\alpha) \in \underset{\sim}{Z}[\alpha]$ with

$$\deg P_{k_1,k_2} \leq c_7 NL_N(\deg_x R + \deg_x S) = c_7 d_1 NL_N$$

$$\log \text{ht } P_{k_1,k_2} \leq c_8 NL_N (d_1 + \log \text{ht } R + \log \text{ht } S) = c_8 NL_N \log h .$$

We plan to choose the $\varphi(n) \in \underset{\sim}{Z}[\alpha]$ so that the coefficient of each $(B_1 \xi_1)^{k_1}$ $(B_2 \xi_2)^{k_2}$ vanishes for $0 \leq p < P_N$, $|I| < L_N$. That gives us $3dP_N L_N^3$ equations. But the number of unknowns $\varphi(n)$ is N^3 . Since

$$3dP_N L_N^3 < N^3/4 ,$$

we may apply lemma 2 to obtain a non-trivial solution with $\varphi_0(n) \in \underset{\sim}{Z}[\alpha]$ satisfying

$$\deg \varphi_0(n) < c_7 d_1 NL_N$$

$$\log \text{ht } \varphi_0(n) \leq c_9 P_N \log N + c_8 NL_N \log h \leq c_{10} H_N .$$

After dividing each $\varphi_0(n)$ by the greatest common divisor of all the $\varphi_0(n)$, lemma 3 assures us that the quotients $\varphi(n)$ which remain satisfy

$$\deg \varphi(n) \leq c_2' d_1 NL_N$$

$$\log \text{ht } \varphi(n) \leq c_1 H_N$$

as desired.

(B) For $0 \leq p < P_N$ and $|I| < L_N$, we have

$$|\Phi_{p,I} - b^{2P_N}(B_1 B_2)^{c_5 NL_N} (\alpha \xi_1 \xi_2)^{c_4 NL_N} F_N^{(p)}((I\cdot b)b^2 \log \alpha)|$$
$$\leq c_{11}^{P_N+NL_N} \sum_n |\varphi(n)|\,|b^2(n\cdot b)|^p\, |\alpha|^{\nu_0}\, |(B_1 \alpha^{\beta})^{\nu_1} (B_2 \alpha^{\beta^2})^{\nu_2} - (B_1 \xi_1)^{\nu_1} (B_2 \xi_2)^{\nu_2}| .$$

$$|(B_1 \alpha^{\beta})^{\nu_1} (B_2 \alpha^{\beta^2})^{\nu_2} - (B_1 \xi_1)^{\nu_1} (B_2 \xi_2)^{\nu_2}|$$
$$\leq |B_1^{\nu_1} B_2^{\nu_2}|\,(|\alpha^{\beta\nu_1}|\,|\alpha^{\beta^2\nu_2} - \xi_2^{\nu_2}| + |\xi_2^{\nu_2}|\,|\alpha^{\beta\nu_1} - \xi_1^{\nu_1}|) \tag{3}$$

and

$$H_N + P_N \log N + d_1 NL_N < 2H_{N_1} + c_{11} H_{N_1} \log N_1 ,$$

we have, by (1) and (2), that

$$\log|F_N^{(p)}(b^2(I\cdot b) \log \alpha)| \leq -\exp(13\, C\, d^{11/2} d_1^2 \log h/14) < -(N_1^3 \log N_1)^2 .$$

(C) To establish the claim, we use Hermite's interpolation formula on the circles about the origin of radii $N^{4/3}$ and $N^{5/3}$:

$$F_N(z) = \frac{1}{2\pi i}\int_{|\zeta|=N^{5/3}} \frac{F_N(\zeta)}{\zeta - z} \prod_I \left(\frac{z - b^2(I\cdot b)\ \log \alpha}{\zeta - b^2(I\cdot b)\ \log \alpha}\right)^{P_N} d\zeta$$

$$- \frac{1}{2\pi i}\sum_{I,p} \frac{F_N^{(p)}(b^2(I\cdot b)\ \log \alpha)}{p!} \int_{|\zeta - b^2(I\cdot b)\log\alpha| = b_2} \frac{(\zeta - b^2(I\cdot b)\ \log \alpha)^p}{\zeta - z} \prod_{I'} \left(\frac{z - b^2(I\cdot b)\ \log \alpha}{\zeta - b^2(I\cdot b)\ \log \alpha}\right)^{P_N} d\zeta$$

where the indices I , I' run over all possibilities with coordinates between 0 and $L_N - 1$, and where

$$2b_2 = b^2(\log \alpha)\ \min_{I \neq I'} |I\cdot b - I'\cdot b| .$$

For the details, see [3], step 1.

STEP 2. - We now note that <u>there is an integer</u> $r_N \in \underset{\sim}{N}$, $1 \leq r_N^4 \leq c_{12}\ d$, <u>such that for some</u> $p_0 \in \underset{\sim}{N}$, $P_N \leq p_0 < r_N P_N$ <u>and</u> $|I_0| < r_N L_N$, <u>we have</u>

$$- c_{13}\ N^3 \log N \leq \log |F_N^{(p_0)}(b^2(I_0\cdot b)\ \log \alpha)| \leq - c_{14}\ r_N^4\ N^3 \log N/d .$$

Otherwise by lemmas 4, 6 and 5, the $\varphi(n)$ must have a common factor in $\underset{\sim}{Z}[\alpha]$. For the details, see [3], step 2. In fact, by (3) and easy upper bounds on $|B_1|$ and $|B_2|$, we see that

$$- c_{15}\ N^3 \log N \leq \log |\Phi_{p_0,I_0}| \leq - c_{16}\ r_N^4\ N^3 \log N/d ,$$

where, when we write Φ_{p_0,I_0} as

$$\Phi_{p_0,I_0} = \sum_{i,j,k} (b\beta)^i\ (B_1\ \xi_1)^j\ (B_2\ \xi_2)^k\ P_{i,j,k}(\alpha) \tag{4}$$

with $0 \leq i \leq 2$, $0 \leq j \leq \deg_y R$, $0 \leq k \leq \deg_z S$, $P_{ijk} \in \underset{\sim}{Z}[\alpha]$, we have

$$\deg P_{ijk} \leq c_{17}\ d_1\ r_N\ NL_N$$

$$\log \mathrm{ht}\ P_{ijk} \leq c_{18}\ r_N\ H_N .$$

STEP 3. - We know that Φ_{p_0,I_0} is integral over $\underset{\sim}{Z}[\alpha]$ of degree at most $3d$. To apply lemma 7, we must find appropriate upper bounds on the degree and height of the coefficients of a monic polynomial for Φ_{p_0,I_0} over $\underset{\sim}{Z}[\alpha]$. Surprizingly, it seems more convenient to use Newton's formulae for this purpose than to take a more direct approach.

The coefficient of $(B_1\ y)^{\deg_y R - j}$ in $(B_1\ y)^{\deg_y R-1}\ R$ (of $(B_2\ z)^{\deg_z S-k}$ in $(B_2\ z)^{\deg_z S-1}\ S$) has degree in x at most

$$(j + 1)\ \deg_x R \qquad ((k + 1)\ \deg_x S)$$

and height at most

$$(1 + \deg_x R)^j\ (\mathrm{ht}\ R)^{j+1} \qquad ((1 + \deg_x S)^k\ (\mathrm{ht}\ S)^{k+1}) ,$$

as one sees by keeping in mind that for polynomials f_1, f_2 in one variable

(5) $$\mathrm{ht}\, f_1 f_2 \leq (1 + \min\{\deg f_1, \deg f_2\})(\mathrm{ht}\, f_1)(\mathrm{ht}\, f_2) .$$

Let s_{1j} (s_{2k}) denote the sum of the j-th (k-th) powers of the conjugates of $B_1 \xi_1$ $(B_2 \xi_2)$ over $\underset{\sim}{Q}(\alpha)$. Then $s_{1j}, s_{2k} \in \underset{\sim}{Z}[\alpha]$. Lemma 8 and (5) allow us to show by induction that for $1 \leq j \leq \deg_y R$, $1 \leq k \leq \deg_z S$, we have

$$\deg s_{1j} \leq 2j \deg_x R , \qquad \deg_{2k} \leq 2k \deg_x S ,$$

$$\mathrm{ht}\, s_{1j} \leq 2^{j-1} (j!)^2 (1 + \deg_x R)^{2j} (\mathrm{ht}\, R)^{2j} ,$$

$$\mathrm{ht}\, s_{2k} \leq 2^{k-1} (k!)^2 (1 + \deg_x S)^{2k} (\mathrm{ht}\, S)^{2k} .$$

Let $\mathbb{s}_\ell \in \underset{\sim}{Z}[\alpha]$ denote the sum of the ℓ-th powers of the $\Phi^{\sigma}_{p_0, I_0}$, the 3d expressions obtained by replacing $B_1 \xi_1$, $B_2 \xi_2$ and $b\beta$ in Φ_{p_0, I_0} by their conjugates. We consider the powers $\ell \leq 3d$ of Φ_{p_0, I_0}. They may be expressed as in (4), but now the coefficient $Q_{ijk}(\alpha)$ of $(b\beta)^i (B_1 \xi_1)^j (B_2 \xi_2)^k$ has

$$\text{degree} \leq c_{19}\, \ell d_1\, r_N\, NL_N ,$$

$$\log \text{height} \leq c_{20}\, \ell r_N H_N .$$

Thus we see that, for $s_0, s_1, s_2 \in \underset{\sim}{Z}$, dependent only on β,

$$\mathbb{s}_\ell = \textstyle\sum_{i,j,k} s_i\, s_{1j}\, s_{2k}\, Q_{ijk}(\alpha) .$$

Hence

$$\deg \mathbb{s}_\ell \leq 2 \deg_y R \deg_x R + 2 \deg_z S \deg_x S + c_{19}\, \ell d_1\, r_N\, NL_N \leq c_{21} \ell d_1\, r_N\, NL_N ,$$

$$\begin{aligned} \log \mathrm{Ht}\, \mathbb{s}_\ell \leq\ & 2[(\deg_y R) \log(1 + \deg_x R)] \\ & + c_{22}[(\deg_y R) \log(1 + \deg_y R) + (\deg_z S) \log(1 + \deg_z S)] \\ & + 2[\deg_y R \log(1 + \deg_x R) + (\deg_z S) \log(1 + \deg_x S)] \\ & + 2[\deg_y R(\log \mathrm{ht}\, S) + (\deg_z S) \log \mathrm{ht}\, R] \\ \leq\ & c_{23}\, \ell r_N H_N . \end{aligned}$$

Applying Newton's identities inductively and recalling (5), we conclude that the coefficient of $U^{3d-\ell}$ in $\prod(U - \Phi^{\sigma}_{p_0, I_0})$ has

$$\text{degree} \leq c_{21}\, \ell d_1\, r_N\, NL_N \leq 3c_{21}\, dd_1\, r_N\, NL_N ,$$

$$\log \text{height} \leq c_{24}\, \ell r_N H_N .$$

Since $d_1 d^2 (r_N NL_N)(r_N H_N) < r_N^4 N^3 \log N/d$, with the ratio arbitrarily large (depending on our choice of C) we can apply lemma 7 to conclude that <u>there is a</u>

polynomial $T_N(\alpha) \in \mathbb{Z}[\alpha]$ which is a power $s_N \geq 1$ of an irreducible polynomial $U_N(\alpha) \in \mathbb{Z}[\alpha]$ with

$$\deg T_N(\alpha) \leq c_{25}\, dd_1\, r_N\, NL_N \,,$$
$$\log \operatorname{ht} T_N(\alpha) \leq c_{26}\, d\, r_N\, H_N \,,$$

and

$$- c_{27}\, dN^3 \log N \leq \log |U_N(\alpha)| \leq - c_{28} \frac{r_N^4 N^3 \log N}{ds_N} .$$

Note that, according to lemma 6 ,

$$\deg U_N \leq c_{25}\, dd_1\, r_N\, NL_N / s_N$$

and

$$\log \operatorname{ht} U_N \leq c_{29}\, dr_N\, H_N / s_N .$$

STEP 4. - We apply lemma 5 to U_N and U_{N+1} , $N_0 \leq N < N_1$. Since $(C/14)\, d^{11/2}\, d_1^2 \log h < \log N_0$ and since r_N/s_N , $r_{N+1}/s_{N+1} \leq c_{12}\, d^{1/4}$, we see that, for large C ,

$$\begin{aligned} & c_{30}\, d^2\, d_1 (r_N/s_N)(r_{N+1}/s_{N+1})\, N^3 (\log N)^{\frac{1}{2}} (\log h)^{\frac{1}{2}}/d^{\frac{1}{2}} \\ & \leq c_{30}\, d^{11/4}\, d_1 \min\{r_N/s_N , r_{N+1}/s_{N+1}\} N^3 (\log N)^{\frac{1}{2}} (\log h)^{\frac{1}{2}}/d \\ & \leq c_{30} (14/C)^{\frac{1}{2}}\, N^3 \log N (\min\{r_N/s_N , r_{N+1}/s_{N+1}\})/d \\ & < c_{28}\, N^3 \log N (\min\{r_N/s_N , r_{N+1}/s_{N+1}\})/d , \end{aligned}$$

as required to show that $U_N = U_{N+1}$, $N_0 \leq N < N_1$.

STEP 5. - We now derive the final contradiction by showing that $U_{N_0} \neq U_{N_1}$. Otherwise $T_{N_1} = U_{N_0}^{s_{N_1}}$.

Hence

$$\log |T_{N_1}(\alpha)| = s_{N_1} \log |U_{N_0}(\alpha)| \geq - c_{25}\, dd_1\, r_{N_1}\, N_1\, L_{N_1} \times c_{27}\, dN_0^3 \log N_0 .$$

But in step 3 we saw that

$$\log |T_{N_1}(\alpha)| \leq - c_{28}\, r_{N_1}^4\, N_1^3 \log N_1/d .$$

It is a straight-forward calculation to show that these two inequalities cannot both hold under our definition of N_0 and N_1 .

BIBLIOGRAPHY

[1] BROWNAWELL (W. D.). — Gel'fond's method for algebraic independence, Trans. Amer. math. Soc., t. 210, 1975, p. 1-26.