On the Measure of Algebraic Independence of Certain Values of Elliptic Functions

ROBERT TUBBS*

Department of Mathematics, The Claremont Colleges, Pitzer College, Claremont, California 91711

Communicated by W. Schmidt

Received July 5, 1983, revised March 19, 1984

We provide a measure for the algebraic independence of some special values of the Weierstrass elliptic function with complex multiplication and algebraic invariants. Specifically, suppose \( \wp(z) \) is such an elliptic function, \( u \) is a nontorsion algebraic point for \( \wp(z) \), and \( \beta \) is an algebraic number which is cubic over the field of multiplications of \( \wp(z) \). We then give the following result: For every \( \varepsilon > 0 \) there exists a positive real number \( \varepsilon > 0 \) such that for any nonzero integral polynomial \( P(X, Y) \), with \( t(P) = \deg P + \log \text{height } P > t(\varepsilon) \), \( \log |P(\wp(\beta u), \wp(\beta^2 u))| > -\exp(t(P)^{4 + \varepsilon}). \)

I. INTRODUCTION

In transcendental number theory there are, at least, two central yet intertwined themes. The first of these involves investigations into the arithmetic nature of particular values, e.g., a demonstration that some classical constant is transcendental or that several special values of a classical function are algebraically independent. The second theme considers the diophantine, or approximation, properties of these values. This involves providing a quantitative measure for the transcendence of a particular value, or for the algebraic independence of several values. In this paper we provide a quantitative result on the algebraic independence of some special values of elliptic functions with complex multiplication and algebraic invariants.

In 1949, Gelfond [7] showed that for \( \alpha, \beta \) algebraic, with \( \alpha \neq 0, 1 \) and \( \beta \) cubic, the numbers \( \alpha^\beta \) and \( \alpha^{\beta^2} \) are algebraically independent. A quantitative version of this result was given in the following year by Gelfond and Feldman [9]. To state their result we recall that if \( P \) is a polynomial in one

* Current address: Department of Mathematics, R.L.M. 8-100, University of Texas, Austin, Texas 78712.
or several variables the \textit{height} of $P$ ($\text{Ht}(P)$) is defined to be the maximum absolute value of its coefficients. We also use the notation $\text{deg}(P)$ to denote the maximum partial degree of $P$. In this notation Gelfond and Feldman proved:

For every $\varepsilon > 0$ there exists a real number $T(\varepsilon) > 0$ such that for every nonzero polynomial $P(X, Y)$ over $\mathbb{Z}$ with

$$T(P) = \text{deg} P + \log(\text{Ht}(P))$$

satisfying $T(P) > T(\varepsilon)$, we have the lower bound

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

Several authors have improved the lower bound given in (1), notably, Brownawell [2], who derived a lower bound of the form $-\exp(\text{deg}(P)^3 T(P)^{1+\varepsilon})$ as a special case of a more general result, and, Chudnovsky [5], who derived the lower bound $-\exp(T(P)^{2+\varepsilon})$.

In 1980, Masser and Wüstholz [13] provided a partial elliptic analogue to Gelfond's original result. They showed, among other things, that if $\varphi(z)$ is a Weierstrass elliptic function with algebraic invariants and complex multiplication a suitable version of Gelfond's independence result can be given. Specifically, if $u$ is a complex number such that $\varphi(u)$ is defined and algebraic, and if $\beta$ is an algebraic number which is cubic over the field of multiplications of $\varphi(z)$, then $\varphi(\beta^2 u)$ and $\varphi(\beta^2 u)$ are defined and are algebraically independent. Their proof depended on an estimate for the number of zeros of a particular meromorphic function, which they established through an application of commutative algebra. This approach was initiated by Nesterenko [16], developed in a fruitful manner by Brownawell and Masser [4], and then extended by Masser and Wüstholz in their papers [13–15].

The main result of this paper is the following quantitative version of Masser and Wüstholz's result.

\textbf{Theorem.} Let $\varphi(z)$ denote a Weierstrass elliptic function with complex multiplication and algebraic invariants. Suppose that $u$ is a nontorsion algebraic point for $\varphi(z)$ and that $\beta$ is cubic over the field of multiplications of $\varphi(z)$. Then for every $\varepsilon > 0$ there exists a real number $T(\varepsilon) > 0$ such that for every nonzero integral polynomial $P(X, Y)$ with $T(P) > T(\varepsilon)$ we have

$$\log |P(\varphi(\beta u), \varphi(\beta^2 u))| > -\exp(T(P)^{4+\varepsilon}).$$

Finally, I would like to thank David Masser and the referee for their helpful comments on an earlier version of this paper, and Dale Brownawell for our many enlightening conversations on this and other topics.
II. Preliminaries

Our basic objects of study are values of elliptic functions with complex multiplication and algebraic invariants. Central among these functions is the Weierstrass elliptic function \( \wp(z) \), which is doubly periodic with the lattice of periods \( \Omega = \omega_1 \mathbb{Z} + \omega_2 \mathbb{Z} \). \( \wp(z) \) is said to have complex multiplication if \( \tau = \omega_1/\omega_2 \) is imaginary quadratic. In that case the complex numbers \( m \) such that \( m\Omega \subseteq \Omega \) form an order \( \mathcal{O} \) in the ring of integers of \( \mathbb{Q}(\tau) \). As such \( \mathcal{O} = \mathbb{Z} + \mu \mathbb{Z} \) for some multiplication \( \mu \). For any nonnegative real number \( S \), we define a subset of \( \mathcal{O} \) by

\[
\mathcal{O}(S) = \{ \sigma \in \mathcal{O} \mid \sigma = s_1 + s_2 \mu \text{ with } |s_i| \leq S \text{ for } i = 1, 2 \}.
\]

We also let \( K_\tau = \mathbb{Q}(\tau) \). \( K_\tau \) is called the field of multiplications for \( \wp(z) \).

Throughout this paper we will assume not only that the invariants of \( \wp(z) \), \( g_2 \) and \( g_3 \), are algebraic, but that \( g_2/4 \), \( g_3/4 \) are algebraic integers. With this assumption we lose no generality thanks to the homogeneity properties relating the functions \( \wp(\lambda z : \lambda \Omega) \) and \( \wp(z : \Omega) \), and the relationship between their invariants \( \lambda^{2k} g_k(\lambda \Omega) = g_k(\Omega) \) for \( k = 2, 3 \).

Further, to avoid complications with lattice points, we work with the normalized elliptic function \( p(z) = \wp(z + (\omega_1/2)) \), which is analytic at \( z \in \Omega \).

We prove the theorem with \( \wp(z) \) replaced by \( p(z) \), which will imply our stated result since the addition formula for \( \wp(z) \) yields

\[
p(z) = \frac{e_1 \wp(z) + (e_1^3 + e_2 e_3)}{\wp(z) - e_1},
\]

where \( e_1 = \wp(\omega_1/2) \), \( e_2 = \wp(\omega_2/2) \), and \( e_3 = \wp((\omega_1 + \omega_2)/2) \) are algebraic.

Our proof depends on information regarding the diophantine nature of each of the values \( u, \beta u, \) and \( \beta^2 u \), as well as \( p(z) \) evaluated at these points. The most basic of these is a transcendence measure for \( p(\beta u) \). We have derived such a measure for a larger class of values and record this measure as our first lemma. The constant \( C_0 \) appearing in this lemma and the later constants \( C_1, C_2, \ldots \), are all positive and depend effectively on \( u, \beta, \) and \( p(z) \).

**Lemma 1.** Suppose that \( p(z) \) is the normalized elliptic function as above with complex multiplication and algebraic invariants, and that \( u \) is a nontorsion algebraic point for \( p(z) \). Then for any algebraic number \( \beta \notin K_\tau \) there exists a positive constant \( C_0 \) such that for any nonzero integral polynomial \( P(X) \) with \( d = \deg P \) and \( T = T(P) \),

\[
|P(p(\beta u))| > \exp(-C_0 d^2 T^2 (\log T)^4).
\]
**Proof.** See [17].

**Remark.** The proof of Lemma 1 also provides a lower bound on the modulus of a certain class of polynomials with coefficients in $L = K_{u}(g_{2}, g_{3}, p(u), p'(u), e_{1}, e_{2}, e_{3})$ when evaluated at $p(\beta u)$. For a polynomial $P$ in one or several variables with coefficients $a_{0}, \ldots, a_{d}$ in $L$ we define the $L$-height of $P$, $ht(P)$, by

$$ht(P) = \sum_{v} \log \max \{1, |a_{i}|_{v}\},$$

where the sum is over all normalized valuations $v$ of $L$. Then if $P(X)$ is nonconstant, monic, and irreducible over $L$ with coefficients in $L$, the proof of Lemma 1 offers the lower bound:

$$\log |P(p(\beta u))| \geq -C_{1} d^{2} t^{2} (\log t)^{4},$$

where $d = \deg(P)$ and $t = t(P) = d + ht(P)$.

We also need diophantine information on the nature of the elliptic logarithms of algebraic points on an elliptic curve with complex multiplication. This information is provided by the following elliptic analogue to Baker's lower bound on a linear form in the logarithms of algebraic numbers. Work in this direction due to Masser [12] would have sufficed, however, the result we give follows from the work of Coates and Lang [6].

**Lemma 2.** Let $E$ be an elliptic curve with complex multiplication and exponential map $p(z)$. Suppose $\beta_{1}, \ldots, \beta_{n}$ are algebraic numbers and $u_{1}, \ldots, u_{n}$ are algebraic points for $p(z)$. Put $A = \beta_{1} u_{1} + \cdots + \beta_{n} u_{n}$ and assume $A \neq 0$. Then for each $\lambda > 8n + 6$ there exists a positive constant $c$ (depending on $u_{1}, \ldots, u_{n}$, the degrees of $\beta_{1}, \ldots, \beta_{n}$, and $A$) such that $|A| > c \exp(-(\log H)^{2})$, where $H = \max_{1 \leq i \leq n} ht(\beta_{i})$.

**Proof.** See theorem, p. 129, [6].

In this paper we use the following immediate consequence of Lemma 2.

**Lemma 3.** Suppose $\beta$ is cubic over $K_{u}$, $u$ is a nontorsion algebraic point for $p(z)$ and $\sigma_{1}, \sigma_{2}, \sigma_{3}$ are multiplications contained in $\mathcal{O}(S)$. Then there exists a positive constant $C_{2}$ such that

$$||(\sigma_{1} + \sigma_{2} \beta + \sigma_{3} \beta^{2})u|| > C_{2} \exp(-(\log S)^{23}),$$

where $|| \cdot ||$ denotes the distance to the nearest lattice point.

In this paper we prove the theorem stated in Section I by showing that
there exists $t(\varepsilon) > 0$ such that for every polynomial $Q(X, Y)$ irreducible over $L$ with coefficients in $L$ and $t(Q) > t(\varepsilon)$ the lower bound

$$\log |Q(p(\beta u), p(\beta^2 u))| > -\exp(t(Q)^{4+\varepsilon})$$

holds. It then follows that there exists a constant $c(\varepsilon) \geq 1$, depending on $u, \beta, \rho(z)$, and $\varepsilon$, with

$$\log |Q(p(\beta u), p(\beta^2 u))| > -c(\varepsilon) \exp(t(Q)^{4+\varepsilon})$$

for every polynomial $Q$ irreducible over $L$.

From this we deduce the general case. For $Q(X, Y)$ with integral coefficients we have a factorization $Q(X, Y) = \prod_{i=1}^k Q_i(X, Y)$ into polynomials $Q_i$ which are irreducible over $L$. By the theory of polynomial heights $\sum_{i=1}^k t(Q_i)^{4+\varepsilon} \leq C T(Q)^{4+\varepsilon}$, where $C$ is positive and depends only on $L$. Thus

$$\log |Q(p(\beta u), p(\beta^2 u))| \geq \sum_{i=1}^k \log |Q_i(p(\beta u), p(\beta^2 u))|$$

$$\geq -C_3 c(\varepsilon) \exp(T(Q)^{4+\varepsilon}) \geq -\exp(T(Q)^{4+\varepsilon}),$$

provided $T(Q)$ is sufficiently large, which is equivalent to the statement of the theorem.

As is typical in transcendence theory we begin by assuming the contrary of our theorem. That is, we assume that there exists an $\varepsilon > 0$ such that for any choice of $t(\varepsilon) > 0$ there exists a nonzero polynomial $Q(X, Y)$ irreducible over $L$ with coefficients in $L$, and $t(Q) \geq t(\varepsilon)$ satisfying

$$\log |Q(p(\beta u), p(\beta^2 u))| \leq -\exp(t(Q)^{4+\varepsilon}). \quad (3)$$

The assumption $(3)$ allows us to derive the following lemma which guarantees the existence of a good approximation to $\beta^2 u$ satisfying additional approximation properties. In this lemma, as in the remainder of this paper, $d = \deg(Q)$ and $t = t(Q)$.

**Lemma 4.** With $u$ and $\beta$ as above, if $(3)$ holds then there exists a complex number $\theta$ satisfying:

(i) $Q(p(\beta u), p(\theta)) = 0,$

(ii) $\log \max\{|p(\beta^2 u) - p(\theta)|, |p'(\beta^2 u) - p'(\theta)|\} < -\exp(t^{4+(\varepsilon/2)})$,

(iii) $\log \|\beta^2 u - \theta\| < -\exp(t^{4+(\varepsilon/2)})$,

(iv) $u, \beta u, \text{and } \theta$ are $K(\varepsilon)$-linearly independent.

provided $t(\varepsilon)$ is large enough.
Proof. \( Q(p(\beta u), Y) \) factors over the algebraic closure of \( L(p(\beta u)) \) in \( \mathbb{C} \) as

\[
Q(p(\beta u), Y) = g(p(\beta u)) \prod_{i=1}^{e} (Y - r_i),
\]

where \( g(X) \) is a nonzero polynomial over \( L \) with \( \deg(g) \leq d \) and \( \text{ht}(g) \leq t \). We apply the remark following Lemma 1 to obtain a lower bound on \( |g(p(\beta u))| \) by factoring \( g(X) \) as

\[
g(X) = a \prod_{i=1}^{k} g_i(X)
\]

with \( a \in L \) satisfying \( \log |a| \leq t \); each polynomial \( g_i(x) \) is nonconstant, monic, and irreducible over \( L \) with coefficients in \( L \). If we let \( d_i = \deg(g_i) \) and \( t_i = t(g_i) \) we then have

\[
\log |g_i(p(\beta u))| \geq -C_1 d_i^2 t_i^2 (\log t_i)^4.
\]

From the usual estimates for the degrees and heights of polynomials we deduce:

\[
\log |g(p(\beta u))| \geq -C_1 \sum_{i=1}^{k} d_i^2 t_i^2 (\log t_i)^4 + \log |a| \geq -C_4 d^2 t^2 (\log t)^4.
\]

This estimate along with our assumption (3) implies that \( e > 0 \); and, combining this estimate, (3), and the factorization of \( Q(p(\beta u), Y) \) we deduce that

\[
\min_{1 \leq i \leq e} \log |p(\beta^2 u) - r_i| \leq -\exp(t^4 + (9/10)e).
\]

Let \( r \) denote the value \( r_i \) which gives this minimum, and choose \( \alpha \) in a fundamental parallelogram of \( \varphi \) such that \( p(\alpha) = r \).

It then follows that for \( t(e) \) large enough

\[
\log |\varphi(\beta^2 u) - \varphi(\alpha)| \leq -\exp(t^4 + (8/10)e).
\]

Then the sigma expansion

\[
\varphi(\beta^2 u) - \varphi(\alpha) = -\frac{\sigma(\beta^2 u + \alpha) \sigma(\beta^2 u - \alpha)}{\sigma^2(\beta^2 u) \sigma^2(\alpha)},
\]

together with the product representation for the sigma function yields:

\[
\log \min \{ \|\beta^2 u + \alpha\|, \|\beta^2 u - \alpha\| \} \leq -\exp(t^4 + (7/10)e).
\]
Given this estimate choose \( \theta = \alpha \) or \( \theta = -\alpha \), whichever is closest to \( \beta^2 u \) modulo the lattice of periods. With this choice of \( \theta \) (i), (ii), and (iii) hold.

Let \( \theta' = \theta + \omega_1 \); \( \theta' \) also satisfies (i), (ii), and (iii). Additionally, one of \( \theta \) or \( \theta' \) satisfies (iv). If not, then there exist \( \sigma_1, \sigma_2, \sigma_3 \) (resp. \( \sigma'_1, \sigma'_2, \sigma'_3 \)) in \( K_\tau \), not all zero, with

\[
\sigma_1 u + \sigma_2 \beta u + \sigma_3 \theta = 0 \quad \text{(resp. } \sigma'_1 u + \sigma'_2 \beta u + \sigma'_3 \theta = -\sigma'_3 \omega_1)\).
\]

Since \( u \) is nonzero \( \sigma_3 \neq 0 \) and \( \sigma'_3 \neq 0 \). Therefore we use the two linear forms to eliminate \( \theta \) and obtain a \( K_\tau \)-linear dependence between \( u, \beta u \), and \( \omega_1 \). However, \( \omega_1 / u \) is transcendental, thus such a dependence is impossible. Hence one of \( \theta \) or \( \theta' \) satisfies all of the conclusions of the lemma; and, without ambiguity we denote this number by \( \theta \).

We now make one further reduction in that we assume that the minimal polynomial of \( \beta \) over \( \mathbb{C} \) has leading coefficient 1. One can show that we lose no generality under this assumption if we let \( n \) denote the \( K_\tau \)-denominator of \( \beta \) and consider the polynomial expressions which hold identically between the functions \( p(z) \) and \( p(nz) \), and between the functions \( p(z) \) and \( p(n^2 z) \). Elementary elimination theory then shows that a measure for the algebraic independence of \( p(n \beta u) \) and \( p(n^2 \beta^2 u) \) implies a similar measure for the algebraic independence of \( p(\beta u) \) and \( p(\beta^2 u) \). We omit these details.

The last result of this section is a multiplicity estimate for homogeneous polynomials evaluated on a finite subset of a finitely generated subgroup of a group variety. This lemma, along with several related results, was announced by Masser and Wüstholz in [14]. Before stating their result we describe the basic set up.

We let \( \sigma(z) \) denote the Weierstrass sigma function and put

\[
h(z) = \sigma^3 \left( z + \frac{\omega_1}{2} \right), \quad f(z) = h(z) p(z), \quad g(z) = h(z) p'(z).
\]

The projective coordinates

\[
(h(z), f(z), g(z))
\]

then parametrize an elliptic curve \( E \) in \( \mathbb{P}_2 \). The product of \( n \) such elliptic curves

\[
G = E^n
\]

is a group variety contained in \( (\mathbb{P}_2)^n \).

The Segre mapping gives an embedding of \( G \) into \( \mathbb{P}_N \) with \( N = 3^n - 1 \). We give this embedding explicitly. If

\[
(\xi_{0i}, \xi_{1i}, \xi_{2i}) \quad (1 \leq i \leq n)
\]
are the projective coordinates of a point in \((\mathbb{P}_2)^n\), then the Segre mapping
\[
\Psi: (\mathbb{P}_2)^n \to \mathbb{P}_N
\]  
(5)
takes this point to the point in \(\mathbb{P}_N\) with projective coordinates
\[
\Psi_0, \Psi_1, \ldots, \Psi_N,
\]
where each \(\Psi_j\) is a product \(t_1 \times \cdots \times t_n\), with each \(t_i \in \{\xi_{0i}, \xi_{1i}, \xi_{2i}\}\).

Similarly, we have a correspondence between polynomials in elliptic functions and homogeneous polynomials. Let
\[
X_{0i}, X_{1i}, X_{2i} \quad (1 \leq i \leq n)
\]
denote the variables of the \(i\)th copy of \(E\); and let
\[
X_0, X_1, \ldots, X_N
\]
denote the homogeneous variables of \(\mathbb{P}_N\). For any polynomial in several elliptic functions of total degree at most \(D\)
\[
P(p(z_1), p'(z_1), \ldots, p(z_n), p'(z_n)),
\]
we consider the associated homogeneous polynomial
\[
X_{01}^p X_{02}^p \cdots X_{0n}^p \frac{X_{11}}{X_{01}} \frac{X_{21}}{X_{01}} \frac{X_{12}}{X_{02}} \frac{X_{22}}{X_{02}} \cdots \frac{X_{1n}}{X_{0n}} \frac{X_{2n}}{X_{0n}}.
\]  
(6)

With the Segre embedding (5) defined as above, the polynomial (6) can be expressed as a homogeneous polynomial of degree \(D\) in the homogeneous variables \(X_0, X_1, \ldots, X_N\).

Hence when a homogeneous polynomial in the projective coordinates of \(\mathbb{P}_N\), coming from a polynomial (6), is evaluated at a point in \(\mathbb{P}_N\) with \(\prod_{i=1}^{n} \xi_{0i} \neq 0\), then we can return to evaluation at a point in \((\mathbb{P}_2)^n\). We come back to this translation in Section IV.

Suppose \(\Gamma\) is a finitely generated subgroup of \(G\) with rank \(l\). For each integer \(r, 1 \leq r \leq n\), following [14] we define an integer \(p_r\) as follows. Let \(p_r\) equal the minimum corank (in \(\Gamma\)) of any subgroup of \(\Gamma\) which is contained in an algebraic subgroup of \(G\) of codimension \(r\). In the case where \(G\) has no algebraic subgroups of codimension \(r\), we let \(p_r = l\). These integers appear as exponents in Lemma 5.

If \(\Gamma\) has generators \(h_1, \ldots, h_l\), for any nonnegative integer \(S\) we define a subset of \(\Gamma\) by
\[
\Gamma(S) = \{ n_1 h_1 + \cdots + n_l h_l : 0 \leq n_i \leq S \}
\]  
(7)
We will define the order of vanishing of a homogeneous polynomial \( P(X_0, ..., X_N) \) at a point of \( I(S) \).

Let \( z_1, ..., z_n \) denote coordinates of \( T(G) \), the tangent space of \( G \) at its identity element. Then the exponential map

\[
\exp_G : T(G) \rightarrow \mathcal{P}(G) \subseteq \mathbb{P}_N
\]

is given by holomorphic functions

\[
f_0(z_1, ..., z_n), ..., f_N(z_1, ..., z_n).
\]  

These functions can be given explicitly in terms of the projective coordinates (4) of the copies of \( E \) and the Segre mapping (5), just as the projective variables \( X_0, ..., X_N \) were given in terms of the variables \( X_{0i}, X_{1i}, X_{2i} \) for \( 1 \leq i \leq n \).

Let

\[
\phi : \mathbb{C} \rightarrow G
\]

be a one-parameter subgroup of \( G \); and identify the tangent space of \( \phi(\mathbb{C}) \) at the identity element of \( G \) with \( \mathbb{C} \).

Then there exists an injective linear map

\[
L : \mathbb{C} \rightarrow T(G)
\]

such that \( \phi \) factors through \( T(G) \)

\[
\phi = \exp_G \circ L.
\]

For a homogeneous polynomial \( P(X_0, X_1, ..., X_N) \) we now define the order of vanishing of \( P \) at a point in \( G \), along \( \phi \). For \( g \in G \) such that there exists \( z \in T(G) \) with \( \exp_G(z) = g \) and \( f_0(z) \neq 0 \), we consider the function:

\[
\chi(\zeta) = P \left( 1, \frac{f_1}{f_0}(z + L(\zeta)), ..., \frac{f_N}{f_0}(z + L(\zeta)) \right).
\]

Then the order of vanishing of \( P \) at \( g \) along \( \phi \) is defined as:

\[
\text{ord}_g P = \begin{cases} 
\infty, & \text{if } \chi(\zeta) \equiv 0; \\
\max \left\{ T : \left( \frac{d}{d\zeta} \right)^T \chi(0) = 0, \text{ for all } t < T \right\}, & \text{otherwise.}
\end{cases}
\]

In this setting Masser and Wüstholz have established the following multiplicity estimate.
LEMMA 5. There exists a constant $C_G$ depending only on $G$ with the following property. Suppose that for some real $S > 0$, $f_0(\exp^{-1}(y)) \neq 0$ for any $y \in \Gamma(S)$ and that for some $T \geq 1$ there exists a homogeneous polynomial $P$ of degree at most $D$ which vanishes to order at least $T$ at every point in $\Gamma(S)$. Then if

$$T \left( \frac{S}{n} \right)^{n_r} \geq C_G D^r \quad (1 \leq r \leq n)$$

and

$$\left( \frac{S}{n} \right)^{n_r} \geq C_G D^{r-1} \quad (1 \leq r < n)$$

it follows that $P$ vanishes on all of $\gamma + \phi(C)$ for some $\gamma \in \Gamma$.

Proof. See [19]. For a preliminary announcement see Theorem A, p. 514, [14].

We apply Lemma 5 in Section IV.

III. THE AUXILIARY POLYNOMIALS

In this section we consider a family of meromorphic functions with prescribed zeros of at least a certain multiplicity. Each function is a polynomial, with estimates for its degree and height, composed with elliptic functions. Furthermore, these functions take on values in the algebraic closure of $L(p(\beta u), p(\beta^2 u))$ in $\mathbb{C}$ which have a small modulus, measured in terms of the degree and $L$-height of the polynomial. These small values are examined following the reduction of the transcendence basis through the substitution of $0$ for $\beta^2 u$.

Our family of meromorphic functions is parametrized by the integers in a certain interval. To describe this interval, we define the integers $D_0 = \lfloor \exp(t^4 + 6/4) \rfloor$ and $D_1 = \lfloor \exp(t^4 + 6/3) \rfloor$, where, as before, $t = t(Q)$ with $Q$ being the polynomial in (3). We take $c$ to be a large constant and for each integer $D$, with $D_0 \leq D \leq D_1$, we define parameters $S$ and $K$ by

$$S = \lfloor D^{1/4}(\log D)^{1/8} \rfloor \quad \text{and} \quad K = \lfloor c^{-1}D^{3/2}(\log D)^{-3/4} \rfloor. \quad (10)$$

These parameters, and the relationship between them and our assumption that (3) holds, play a central role in our proof.

We return to the situation of $\beta$ cubic over $K$, and $u$ a nontorsion algebraic point for $p(z)$. The set of points at which we prescribe the zeros of our meromorphic function is defined as a subset of the set $\Gamma^u$:

$$\Gamma^u = \{ \sigma_1 u + \sigma_2 \beta u + \sigma_3 \beta^2 u \mid \sigma_i \in \mathbb{C}, i = 1, 2, 3 \}. \quad (11)$$
To be precise, we consider the subset of $\Gamma^u, \Gamma^u(S)$, defined by

$$\Gamma^u(S) = \{ \sigma_1 u + \sigma_2 \beta u + \sigma_3 \beta^2 u \mid \sigma_i \in \mathcal{O}(S), i = 1, 2, 3 \}. \quad (12)$$

We remark that there exists a constant $C_5$ such that for $\gamma \in \Gamma^u(S)$ there exist multiplications $\sigma_{j,l} \in \mathcal{O}(C_5 S)$ ($1 \leq j \leq 3, 1 \leq l \leq 3$) with

$$\beta^{l-1} \gamma = \sigma_{j,1} u + \sigma_{j,2} \beta u + \sigma_{j,3} \beta^2 u \quad (1 \leq j \leq 3).$$

(The multiplications $\sigma_{j,l}$ are determined by the action of multiplication by $\beta^{l-1}$ on the elements of $\Gamma^u$.) With this in mind we can now give the following lemma.

**Lemma 6.** Suppose $D, S, and K$ are as above. Then there exists a nonzero polynomial

$$P(x_1, x_2, x_3) = \sum_{i} a_i (p(\beta u), p(\beta^2 u), x_{i_1}^1 x_{i_2}^2 x_{i_3}^3) \quad (13)$$

(where the sum is over all $i = (i_1, i_2, i_3)$ with each $i_j$ satisfying $0 \leq i_j \leq D$) with $a_i \in \mathcal{O} \{ x_2, x_3 \}$, without a nonconstant common factor, with $t(a_i) \leq C_6 DS^2$, such that the function

$$\Phi(z) = P(p(z), p(\beta z), p(\beta^2 z)) \quad (14)$$

satisfies

$$\Phi^{(k)}(\gamma) = 0 \quad \text{for all } \gamma \in \Gamma^u(S) \text{ and all } k, 0 \leq k \leq K.$$

**Proof.** The construction of auxiliary functions is standard and therefore we include only an outline of the construction of $P$. The procedure we follow is to construct a system of equations, with unknowns $a_i$, which mimic the condition that $\Phi^{(k)}(\gamma) = 0$ for $\gamma \in \Gamma^u(S)$ and $0 \leq k \leq K$. Throughout this proof all implied constants are positive and depend at most on $\gamma(z)$, $u$, and $\beta$.

For each $\gamma \in \Gamma^u(S)$ we use the multiplications $\sigma_{j,l} \in \mathcal{O}(C_5 S)$ as above to define the function

$$\Phi_{\gamma}(z) = \sum_{i} a_i \prod_{j=1}^{3} p_{j}^{b_{j}} \left( \sum_{l=1}^{3} \sigma_{j,l} \beta^{l-1} z \right)$$

which satisfies $\Phi_{\gamma}(u) = \Phi(\gamma)$. By applying the addition formulae for $p(z)$ we can express each expression $p(\sum_{l=1}^{3} \sigma_{j,l} \beta^{l-1} z)$ as a rational function in $p(\sigma_{j,l} \beta^{l-1} z)$ and $p'(\sigma_{j,l} \beta^{l-1} z)$, with a denominator which does not vanish
at $z = u$. Multiplying by these denominators to the appropriate powers yields functions

$$\Theta_j(z) = \sum_i a_i P_i(\ldots, p(\sigma_i \beta^{l-1} z), p'(\sigma_i \beta^{l-1} z), \ldots), j = 1, 2, 3, l = 1, 2, 3,$$

where $\Theta_j(u) = 0$ if and only if $\Phi(\gamma) = 0$. The polynomials $P_i$ have coefficients in $\mathbb{Z} [g_3/4, g_5/4]$, and $t(P_i) \ll D$.

By the Anderson–Baker–Coates lemma (e.g., [18, Lemma 6.2.3, p. 6.63]) for each $k$, $0 \leqslant k \leqslant K$, there are polynomials $G^k_{ij}(x_1, \ldots, x_6)$ such that the polynomial $Q^k_{ij}(x_1, \ldots, x_6) = \sum_i G^k_{ij}(x_1, \ldots, x_6)$ vanishes at $x_r = p(\beta^{l-1} u)$, $x_{r+3} = p'(\beta^{l-1} u)$, for $l = 1, 2, 3$, if and only if $\Phi^{(k)}(\gamma) = 0$. We also know that $t(G^k_{ij}) \ll D S^2$, $G^k_{ij}$ is linear in $x_4, x_5, x_6$, and that the coefficients of each $G^k_{ij}$ lie in $\mathcal{O}[g_3/4, g_5/4]$.

By the Thue–Siegel lemma we solve the system of equations (formally)

$$Q^k_{ij}(p(u), x_2, x_3, p'(u), x_5, x_6) = 0$$

and obtain a solution $a_i \in \mathcal{O}_L[x_2, x_3]$ with $t(a_i) \ll D S^2$. By [8, Lemma 2, p. 135], we may assume that the polynomials $a_i$ have no nonconstant common factor. Evaluation of each $a_i$ at $x_r = p(\beta^{l-1} u)$ for $l = 2, 3$ yields the desired function.

Furthermore, $|\Phi^{(k)}(\gamma)|$, for each $\gamma \in \Gamma^u(S)$, can be majorized for $k$ over a slightly larger interval. Specifically, Cauchy's integral formula and Schwarz's Lemma applied to the function

$$Q^k(\gamma) = \sum_i h(p(\beta^{l-1} z)) D \cdot Q^k(\gamma)$$

on circles of radii $r = C_7 S$ and $R = C_7 S^2$, yields

$$\log |Q^{(k)}(\gamma)| \leqslant -C_8 D^3 \log D,$$

for all $\gamma \in \Gamma^u(S)$ and $0 \leqslant k \leqslant C_6 3^2 K$, provided that we take $t(\varepsilon)$ large enough.

The lower bound in Lemma 3 together with the estimate for the sigma function of [12, Lemma 7.1, p. 78] and the usual estimate for the binomial coefficients implies

$$\log |\Phi^{(k)}(\gamma)| < -C_9 D^3 \log D \quad \text{for} \quad \gamma \in \Gamma^u(S) \quad \text{and} \quad 0 \leqslant k \leqslant C_6 3^2 K. \quad (15)$$

We retain the notation of Lemma 6 for our affine variables $x_1, \ldots, x_6$. Our goal is to use the estimate (15) and Lemma 5 (in the proper setting) to obtain a nonzero polynomial $P_D \in \mathcal{O}_L[p(u), p'(u)][x_2, x_3, x_5, x_6]$ with $t(P_D) \ll D S^2$; and, letting $\xi = (p(\beta u), p(\theta), p'(\beta u), p'(\theta))$, which satisfies
$P_D(\xi) \neq 0$ and $\log |P_D(\xi)| \ll -D^3 \log D$, where the implied constants depend at most on $u, \beta$, and $p(z)$.

As a first step towards reaching our goal, we associate with the auxiliary polynomial $P(x_1, x_2, x_3)$, (13), the polynomial $\tilde{P}$ which is obtained from $P$ by substituting $\theta$ for $\beta^2u$ in each coefficient $a_i$ of $P$. In Lemma 6 we have taken the coefficients $a_i$ without any common factors, therefore $\tilde{P}$ is not identically zero. We let $\Phi(\gamma)$ denote the function (14) associated with $\tilde{P}$. Further, we let $\Phi^{(k)}(\gamma)^*$ denote the value obtained by evaluation of $\Phi^{(k)}(\gamma)$ at $z = \gamma$ followed by substitution of $\theta$ for $\beta^2u$ in each argument of the function. Our aim is to show that one of the values $\Phi^{(k)}(\gamma)^*$ is nonzero with $\gamma$ and $k$ as in (15), and to estimate its modulus.

However, we must first show that each expression $\Phi^{(k)}(\gamma)^*$ is finite with $\gamma$ and $k$ as in (15). To prove this, we use the following lemma which is a simple consequence of Lemma 3 and our choice of $\theta$.

**Lemma 7.** Choose $D$ in the interval $[D_0, D_1]$, with $D_0$ and $D_1$ as above; and fix any positive real number $\kappa$. For $t(\varepsilon)$ large enough, if $\sigma_i \in \mathbb{C}(\kappa S)$, for $i = 1, 2, 3$, are not all zero, then

$$\sigma_1 u + \sigma_2 \beta u + \sigma_3 \theta \notin \Omega.$$

**Proof.** If there were such an expression in $\Omega$, then apply Lemma 3 to obtain an inequality,

$$C_2 \exp(- (\log \kappa S)^{23}) \leqslant |\sigma_1 u + \sigma_2 \beta u + \sigma_3 \beta^2 u| \leqslant |\sigma_3| \|\beta^2 u - \theta\|.$$

Recalling our choice of $\theta$ and that $t > t(\varepsilon)$ we deduce

$$C_{10} (\log \kappa S)^{23} \geqslant \exp(t(\varepsilon)^4 + (\varepsilon/2)),$$

which cannot hold provided $t(\varepsilon)$ is large enough.

Following the substitution $\beta^2u \to \theta$, each of the arguments of $\varphi$ in $\Phi^{(k)}(\gamma)^*$ becomes an expression of the form $\sigma_i u + \sigma_2 \beta u + \sigma_3 \theta + (\omega_i/2)$, with each $\sigma_i$ in $\mathcal{O}(C_5 S)$. Then if $t(\varepsilon)$ is taken to be large enough, none of the substituted values will lie in the period lattice, and $\Phi^{(k)}(\gamma)^*$ is defined.

If $\Phi^{(k)}(\gamma)^*$ is nonzero, then an application of the addition and multiplication formulae for $p(z)$ allows us to express this value as

$$\Phi^{(k)}(\gamma)^* = \frac{Q_1(p(\theta), p'(\theta))}{Q_2(p(\theta), p'(\theta))},$$

where $Q_1$ and $Q_2$ are nonzero and relatively prime polynomials. Further, for $i = 1, 2$, $t(Q_i) < C_{11} D^{2/3} (\log D)^{1/4}$, $Q_i$ is at most linear in $p'(\theta)$, and each
coefficient of $Q_i$ is a polynomial expression in $\mathcal{O}_L[p(u), p'(u), p(\beta u), p'(\beta u)]$ with degree $+L$-height at most $C_{12} D^{3/2}(\log D)^{1/4}$, which is at most linear in $p'(u)$ and $p'(\beta u)$.

If

$$\log |Q_2(p(\theta), p'(\theta))| < -\frac{1}{3} C_9 D^3 \log D$$

(17)

then $Q_2$ plays the role of $p_D$ as above and we proceed to Section V.2.

If, on the other hand, (17) does not hold for $Q_2$, we show that a similar estimate holds for $Q_1$, possibly with a different constant. This deduction depends on a majorization of $|\Phi^{(k)}(\gamma)^*|$, which we obtain by considering the inequality

$$|\Phi^{(k)}(\gamma) - \Phi^{(k)}(\gamma)^*| \leq \left| \frac{|\Phi^{(k)}(\gamma)| + 1}{|Q_2(p(\theta), p'(\theta))|} \right| \cdot A,$$

where

$$A = \max_{i=1,2} \{ |Q_i(p(\theta), p'(\theta))| - Q_i(p(\beta^2 u), p'(\beta^2 u)) | \}.$$

Here we have used the fact that $\Phi^{(k)}(\gamma)$ equals the rational expression in (16) with $\theta$ replaced by $\beta^2 u$.

By our choice of $\theta$ and the information we have regarding $Q_1$ and $Q_2$ we deduce the estimate $\log |A| < -\frac{1}{3} \exp(t^4 + (t/2))$, provided $t(\varepsilon)$ is large enough. This leads to the estimate

$$\log |\Phi^{(k)}(\gamma)^*| < -C_{13} D^3 \log D.$$ (18)

Given the nature of the polynomial $Q_2$, we have

$$\log |Q_2(p(\theta), p'(\theta))| < C_{14} D^{3/2}(\log D)^{1/2}.$$ (19)

Then combining (16), (18), and (19) we obtain

$$\log |Q_1(p(\theta), p'(\theta))| < -C_{15} D^3 \log D.$$
1. The Nonzero Value

To apply Lemma 5 we examine the values of the meromorphic function $\Phi(z)$ on $\Gamma^\omega(S)$ as the values of a homogeneous polynomial evaluated on a finite subset of a finitely generated subgroup of $G$. Here we take

$$G = E^3,$$

where each elliptic curve $E$ is given by the projective coordinates (4); and $G$ is embedded into $\mathbb{P}_{26}$ by the Segre mapping (5).

Assuming that $\beta^3 = a\beta^2 + b\beta + c$ ($a, b, c \in \mathbb{C}$) we begin with the elements

$$
\begin{align*}
    &h_1 = (u, \beta u, \beta^2 u), \\
    &h_2 = (\beta u, \beta^2 u, cu + b\beta u + a\beta^2 u), \\
    &h_3 = (\beta^2 u, cu + b\beta u + a\beta^2 u, acu + (ab + c)\beta u + (a^2 + b)\beta^3 u),
\end{align*}
$$

of $T(G)$. These are defined such that for $\gamma = \sigma_1 u + \sigma_2 \beta u + \sigma_3 \beta^2 u$ in $\Gamma^\omega$ and an auxiliary polynomial $P$ in $\mathbb{C}[X_0, \ldots, X_{26}]$, the homogeneous version (6) of $P$ in the variables $X_0, \ldots, X_{26}$ evaluated at $\exp_G(\sigma_1 h_1 + \sigma_2 h_2 + \sigma_3 h_3)$ equals the value $Q(\gamma)$, where $Q(z)$ is the associated function of $P$ as in (14).

To introduce the $\theta$ substitution, for $i = 1, 2, 3$, let $h_i^\theta$ denote $h_i$ with $\theta$ substituted for $\beta^2 u$ throughout. We then have that $\Phi(\gamma)^\theta$ equals $P$ evaluated at $\exp_G(\sigma_1 h_1^\theta + \sigma_2 h_2^\theta + \sigma_3 h_3^\theta)$. Define the subgroup $\Gamma$ of $G$ by

$$\Gamma = \mathfrak{C} \exp_G(h_1^\theta) + \mathfrak{C} \exp_G(h_2^\theta) + \mathfrak{C} \exp_G(h_3^\theta).$$

To apply Lemma 5 with the subgroup $\Gamma$ of $G$ as above, we need to calculate the exponents $p_i$ for $r = 1, 2, 3$. This calculation is given in

**Lemma 8.** With $G$ and $\Gamma$ as above, we have the estimates $p_1 > 2$ and $p_2 - p_3 = 6$.

**Proof.** We first show that the $\mathbb{Z}$-rank of $\Gamma$ is 6. For $g = \sigma_1 \exp_G(h_1^\theta) + \sigma_2 \exp_G(h_2^\theta) + \sigma_3 \exp_G(h_3^\theta)$ in $\Gamma$, the matrix expressing the $T(G)$-components of $g$ in terms of $u, \beta u, \text{ and } \theta$ has determinant

$$\text{Norm}_{\mathcal{K}(\mathbb{F}_t)}(\sigma_1 + \sigma_2 \beta + \sigma_3 \beta^2).$$

This determinant is non-zero unless $\sigma_1 = \sigma_2 = \sigma_3 = 0$. Hence the $\mathbb{Z}$-rank of $\Gamma$ is 6.

Let $\pi_i$ denote the projection from $G$ to its $i$th factor. Suppose $\Gamma$ contains a subgroup of corank less than 6 which is contained in an algebraic sub-
group $H$ of $G$ of codimension 3 (resp. 2). Then by [14, Lemma 11, p. 512],

$F(H) = \{ (t_1, t_2, t_3) \in \mathcal{O}^3 : t_1 \pi_1(h) + t_2 \pi_2(h) + t_3 \pi_3(h) = 0 \text{ for all } h \in H \}$,

is an $\mathcal{O}$-module with rank at least 3 (resp. 2).

Choose two $\mathcal{O}$-linearly independent elements $t_1$ and $t_2$ of $F(H)$, and choose $g = \sigma_1 \exp_G(h_1^*) + \sigma_2 \exp_G(h_2^*) + \sigma_3 \exp_G(h_3^*)$, $\sigma_1$, $\sigma_2$, $\sigma_3$ not all zero, in the subgroup of $\Gamma$ which is contained in $H$. Then we obtain two relations $t_1(g) = 0$ and $t_2(g) = 0$, which yield two forms

$\sigma_{11}u + \sigma_{12}u + \sigma_{13} = \Omega$ and $\sigma_{21}u + \sigma_{22} + \sigma_{23} = \Omega$. (20)

The matrix expressing $(\sigma_{11}, \sigma_{12}, \sigma_{13})$ in terms of the coordinates of $t_1 \in \mathcal{O}^3$ has determinant equal to the norm above, which is nonzero by our choice of $g$. Therefore $(\sigma_{11}, \sigma_{12}, \sigma_{13})$ and $(\sigma_{21}, \sigma_{22}, \sigma_{23})$ are $\mathcal{O}$-linearly independent. Hence, we can eliminate $\theta$ from the forms (20) and obtain a nontrivial $\mathbb{K}_L$-linear dependence between $u$, $\beta u$, and some period $\omega \in \Omega$. This is impossible since $\omega/\mu$ is transcendental.

Therefore, we have shown that $p_3 = 6$ (resp. $p_2 = 6$).

If $p_1 \leq 2$ then $\Gamma$ contains a subgroup of $\mathbb{Z}$-rank at least 4 which is annihilated by some nonzero $t = (t_1, t_2, t_3) \in \mathcal{O}^3$. If we take

$g_j = \sigma^{(j)}_1 \exp_G(h_1^*) + \sigma^{(j)}_2 \exp_G(h_2^*) + \sigma^{(j)}_3 \exp_G(h_3^*)$

for $j = 1, 2$, with $g_1$ and $g_2$ $\mathcal{O}$-linearly independent, then we obtain two relations $t(g_1) = 0$ and $t(g_2) = 0$, which implies the existence of two expressions as in (20). The matrix expressing $(\sigma_{11}, \sigma_{12}, \sigma_{13})$ in terms of $(\sigma^{(1)}_1, \sigma^{(1)}_2, \sigma^{(1)}_3)$ (resp. $(\sigma_{21}, \sigma_{22}, \sigma_{23})$ in terms of $(\sigma^{(2)}_1, \sigma^{(2)}_2, \sigma^{(2)}_3)$) has determinant

$N_{\mathbb{K}_L/\mathbb{K}_L}(t_1 + \beta t_2 + \beta^2 t_3) \neq 0$.

Therefore, we may eliminate $\theta$ from the expressions (20). As before, this leads to a contradiction. Therefore $p_1 > 2$.

We now define the one-parameter subgroup $\phi : \mathbb{C} \to G$ by

$\phi(z) = (h(z), f(z), g(z), h(\beta z), f(\beta z), g(\beta z), h(\beta^2 z), f(\beta^2 z), g(\beta^2 z))$; (21)

$\phi(\mathbb{C})$ is Zariski dense in $G$. If not then $H = \overline{\phi(\mathbb{C})}$ (the Zariski closure) is a proper algebraic subgroup of $G$, and therefore $F(H) \neq 0$. Then there exists a nontrivial $(t_1, t_2, t_3) \in \mathcal{O}^3$ with

$t_1 z + t_2 \beta z + t_3 \beta^2 z \in \Omega$

for all $z$. For $z$ sufficiently small this is impossible, since $\Omega$ is discrete. Therefore $\overline{\phi(\mathbb{C})} = G$. 

We are now in a position to apply Lemma 5 to obtain the necessary nonzero value. We observe that the homogeneous version of our substituted auxiliary polynomial $\overline{P}_h$ does not vanish on $\gamma + \phi(\zeta)$ for any $\gamma$ in $\Gamma$. Since $\phi(\zeta)$ is dense in $G$ then so is $\gamma + \phi(\zeta)$; therefore, if $\overline{P}_h$ vanishes on $\gamma + \phi(\zeta)$ then it vanishes on all of $G$. Dehomogenizing, we obtain

$$\sum_i a_i(p(\beta u), p(\theta)) p(z_1)^i p(z_2)^j p(z_3)^k = 0$$

identically in $z_1, z_2, z_3$, which is clearly impossible.

If we specify $f_0(z)$ in (8) as $f_0(z) = h(z_1) \cdots h(z_n)$ then Lemma 7 implies that for $\gamma \in \Gamma(S)$ we have $f_0(\exp^{-1}(\gamma)) \neq 0$. Let $T$ be a lower bound for the order of vanishing of $\overline{P}_h$ at each point of $\Gamma(S)$; then, Lemma 5 together with Lemma 8 implies that

$$T < C_6^{-3} K.$$

Hence for some $\gamma_0 \in \Gamma(S)$ and some $k_0$, $0 \leq k_0 \leq C_6^{-3} K$, the function $\chi(\zeta)$, defined in (9), satisfies

$$\left( \frac{d^k}{d\zeta^k} \right) \chi(0) \neq 0. \quad (22)$$

Yet if we view (22) explicitly we have the following. If $\exp_G(z_1, z_2, z_3) = \gamma_0$ then $\chi(\zeta)$ can be written as

$$\chi(\zeta) = \overline{P}(p(z_1 + \zeta), p(z_2 + \beta \zeta), p(z_3 + \beta^2 \zeta),$$

here we have translated back from $P_{26}$ to affine coordinates, thanks to Lemma 7.

Choose $\gamma_1 \in \Gamma^u(S)$ such that $\exp_G(\gamma_1, \beta \gamma_1, \beta^2 \gamma_1)$ goes to $\gamma_0$ following the substitution of $\theta$ for $\beta^2 u$. We then have

$$\overline{P}^{(10)}(\gamma_1) \neq 0.$$

2. The Last Stage

Repeating the above argument for each choice of the parameter $D$, $D_0 \leq D \leq D_1$, we have constructed a family of nonzero polynomials $P_D$ with coefficients in $\mathcal{O}_z[p(u), p'(u)]$, where $P_D(\xi) \neq 0$, $\xi = (p(\beta u), p(\theta), p'(\beta u), p'(\theta))$; and

(i) $\log |P_D(\xi)| \leq -C_{16} D^3 \log D \quad (23)$

(ii) $\deg_x P_D \leq C_{17} D^{3/2}(\log D)^{1/4}$ for $l = 2, 3,$

(iii) $\deg_x P_D \leq 1$ for $l = 5, 6.$ \quad (24)

$$\log \text{ht}(P_D) \leq C_{18} D^{3/2}(\log D)^{1/4}.$$
We now use $P_D$ to produce a nonzero polynomial $R_D(X) \in \mathbb{Z}[X]$ satisfying

\begin{align*}
(i) & \quad \log |R_D(p(\beta u))| \leq -D^3 \log D, \\
(ii) & \quad \deg R_D \leq \epsilon D^{3/2}(\log D)^{1/4}, \\
(iii) & \quad \log \text{ht}(R_D) \leq \epsilon D^{3/2}(\log D)^{1/4}.
\end{align*}

where $d = \deg Q$ and $t = t(Q)$ for $Q$ satisfying (3).

The variables $x_5$ and $x_6$ are eliminated successively. Since $P_D$ is at most linear in $x_6$ we consider the polynomial $P^1_{D,6} = P_D(x_2, x_3, x_5, -x_6)$ and put

\[ P_D^1 = \begin{cases} P_D + P_{D,6} & \text{if } P_{D,6}(\xi) = 0 \\ P_D \cdot P_{D,6} & \text{otherwise.} \end{cases} \]

In either case $P_D^1$ is a polynomial which does not involve $x_6$ and takes on a small nonzero value at $\xi$. Further, since $P_{D,6}$ satisfies the estimate (19) and $P_D$ satisfies (23) we have

\[ \log |P_D^1(\xi)| \leq -C_{19} D^3 \log D \quad \text{and} \quad t(P_D^1) \leq C_{20} D^{3/2}(\log D)^{1/4}. \]

Similarly we eliminate $x_5$ to obtain a polynomial $P_D^2(x_2, x_3)$ with $P_D^2(\xi) \neq 0$ which satisfies

\[ \log |P_D^2(\xi)| \leq -C_{21} D^3 \log D \quad \text{and} \quad t(P_D^2) \leq C_{22} D^{3/2}(\log D)^{1/4}. \]

It is clear from (3) that if we view $Q$ as $Q(x_2, x_3)$ then $Q$ must involve $x_3$, for otherwise our assumption (3) violates the conclusion of Lemma 1. With this in mind we define a new polynomial $r(x_2)$ by

\[ r(x_2) = \begin{cases} \text{Res}_{x_3}(P_D^2(x_2, x_3), Q(x_2, x_3)) & \text{if } P_D^2 \text{ involves } x_3 \\ P_D^2 & \text{otherwise;} \end{cases} \]

$r(x_2)$ is a nonzero polynomial, since $Q$ is irreducible over $L$ and does not divide $P_D^2$. Further $r(p(\beta u)) \neq 0$ and we have the estimates

\begin{align*}
(i) & \quad \log |r(p(\beta u))| \leq -C_{23} D^3 \log D, \\
(ii) & \quad \deg(r) \leq C_{24} D^{3/2}(\log D)^{1/4}, \log \text{ht}(r) \leq C_{25} D^{3/2}(\log D)^{1/4}. 
\end{align*}

Taking the relative norm from $L(p(\beta u))$ to $\mathbb{Q}(p(\beta u))$ and multiplying by the denominator of $p(u)$ to the appropriate power we obtain $R_D(X) \in \mathbb{Z}[X]$ satisfying the estimates stated in (25), here we have replaced the subscripted variable $x_2$ by $X$. 


By [8, Lemma VI, p. 147], $R_D(X)$ has a factor which is a power, $t_D$, of an irreducible polynomial $Q_D(X) \in \mathbb{Z}[X]$ with

(i) \[ \deg Q_D^{t_D} \leq C_{26} d D^{3/2}(\log D)^{1/4} \]

(ii) \[ \log \text{ht}(Q_D^{t_D}) \leq C_{27} t D^{3/2}(\log D)^{1/4} \]

(iii) \[ \log |Q_D^{t_D}(p(\beta u))| \leq -C_{28} D^3 \log D. \]

Following the structure of proof utilized by Brownawell in [2] we begin by showing that the underlying polynomial $Q_D(X)$ is the same for each $D$ over our interval. In fact this is elementary. Fix a choice of $D$, with $D_0 \leq D < D_1$, and let $N = \text{Res}_X(Q_D^{t_D}(X), Q_D^{t_D+1}(X))$. Then $N$ is an integer with $\log |N| \leq -D^3 \log D$, therefore, $N = 0$.

By the elementary properties of the resultant of two polynomials, we conclude that $Q_D^{t_D}$ and $Q_D^{t_D+1}$ have a common factor; and, since each $Q_D$ is irreducible, $Q_D = Q_D^{t_D+1}$ for all choices of $D$. For simplicity, call this irreducible polynomial $q(X)$.

We next estimate $|q(p(\beta u))|$ by comparing the information available first by viewing $q(X)$ as $Q_D^{t_D}(X)$, and then by viewing $q(X)$ as $Q_D^{t_D+1}(X)$. The idea here is that the degree and height are best estimated through the former perspective, and $|q(p(\beta u))|$ is best estimated through the latter.

From (26) we obtain the bounds

\[ \deg q \leq \frac{1}{t_{D_0}} C_{29} d D_0^{3/2}(\log D_0)^{1/4}, \]

\[ \log \text{ht}(q) \leq \frac{1}{t_{D_0}} C_{30} t D_0^{3/2}(\log D_0)^{1/4}. \]

and

\[ \log |q(p(\beta u))| \leq -\frac{1}{t_{D_1}} C_{31} D_1^3(\log D_1). \]

We also have the easy estimates on the exponents: $1 \leq t_D \leq C_{26} d D^{3/2}(\log D)^{1/4}$.

The estimate for $t_{D_0}$ together with (27) and Lemma 1 offers the lower bound

\[ \log |q(p(\beta u))| > -C_6 t^4 D_0^6(\log D_0)^5. \]

However, (28) implies that

\[ \log |q(p(\beta u))| \leq -C_{32} D_1^{3/2}(\log D_1)^{1/2}. \]
These estimates for $|q(p(\beta u))|$ yield the inequality
\[ C_{32} t^2 + (e/6) \exp\left(\frac{1}{2} t^4 + (e/3)\right) < C_0 t^{24 + (5/4) e} \exp(6t^4 + (e/4)), \]
which cannot hold for $t(e)$ large enough (since $t \geq t(e)$). Hence (3) cannot hold and our proof is complete.

REFERENCES