# Algebraic Independence of Values of Elliptic Functions 

D. W. Masser ${ }^{1}$ and G. Wüstholz ${ }^{2}$

${ }^{1}$ Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1003, USA
${ }^{2}$ Max-Planck-Institut für Mathematik, Gottfried-Claren-Strasse 26, D-5300 Bonn 3, Federal Republic of Germany and Bergische Universität - Gesamthochschule, FB 7, Gauß-Strasse 20, D-5600 Wuppertal, Federal Republic of Germany

## 1. Introduction

In this article we give proofs of the theorems announced in [7] on the algebraic independence of values of elliptic functions. Let $\wp(z)$ be a Weierstrass elliptic function with algebraic invariants $g_{2}, g_{3}$. If $\wp(z)$ has complex multiplication we write $k$ for the associated quadratic field; otherwise, if $\wp(z)$ has no complex multiplication, then $k$ denotes the rational field $\mathbb{Q}$. For an integer $n \geqq 1$ let $u_{1}, \ldots, u_{n}$ be complex numbers linearly independent over $k$, and for an integer $m \geqq 1$ let $v_{1}, \ldots, v_{m}$ be complex numbers linearly independent over $\mathbb{Q}$. Our results are as follows.

Theorem 1. If $m n \geqq 2 m+4 n$ then at least two of the numbers

$$
\wp\left(u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

are defined and are algebraically independent over $\mathbb{Q}$.
Theorem 2. If $m n \geqq 2 m+2 n$ then at least two of the numbers

$$
u_{i}, \wp\left(u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

are defined and are algebraically independent over $\mathbb{Q}$.
Theorem 3. If $m n \geqq m+4 n$ then at least two of the numbers

$$
v_{j}, \wp\left(u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

are defined and are algebraically independent over $\mathbb{Q}$.
Theorem 4. If $m n>m+2 n$ then at least two of the numbers

$$
u_{i}, v_{j}, \wp\left(u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

are defined and are algebraically independent over $\mathbb{Q}$.
Theorem 5. Suppose that $m=4, n=2$ and that the numbers

$$
\wp\left(u_{1} v_{j}\right) \quad(1 \leqq j \leqq m)
$$

are defined and are algebraic over $\mathbb{Q}$. Then at least two of the numbers

$$
u_{i}, v_{j}, \wp \prec\left(u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

are defined and are algebraically independent over $\mathbb{Q}$.
Some numerically weaker results of the same form, but relating to more general functions, were obtained by the second author in [17]; for example, they imply our Theorem 2 with $m=16, n=3$ (instead of $m=6, n=3$ ). See also the related work [11, 12] of Smelev, and the earlier results [3] of Brownawell and Kubota on transcendence types.

We leave it to the reader to deduce the usual corollaries from our theorems by suitably specializing the $u$ 's and $v$ 's. But in the case of complex multiplication two of these are sufficiently interesting to be recorded here.
Corollary 1. Suppose $\wp(z)$ has complex multiplication over $k \neq \mathbb{Q}$. Then if $u$ is a complex number such that $\wp(u)$ is defined and is algebraic over $\mathbb{Q}$, and $\beta$ is cubic over $k$, the numbers $\wp(\beta u), \wp\left(\beta^{2} u\right)$ are defined and are algebraically independent over $\mathbb{Q}$.

Corollary 2. Suppose $\wp(z)$ has complex multiplication over $k \neq \mathbb{Q}$. Then at least one of the numbers $\wp(\wp(1))$, $\wp\left((\wp(1))^{2}\right)$ is defined and is transcendental over $\mathbb{Q}$.

Our results are the natural elliptic analogues of theorems of Gelfond [6], Brownawell [1, 2], Smelev [10], Tijdeman [14], Waldschmidt [15, 16], and Wallisser for the exponential function. In particular Corollary 1 may be compared with Gelfond's result on the algebraic independence of $\alpha^{\beta}, \chi^{\beta^{2}}$ for algebraic $\alpha \neq 0,1$ and cubic $\beta$. And Corollary 2 may be compared with the theorem of Brownawell and Waldschmidt to the effect that at least one of $e^{e}, e^{e^{2}}$ is transcendental.

An essential component in our proofs consists of some algebraic zero estimates for polynomials in elliptic functions. These replace the fundamental analytic estimates [13] of Tijdeman for the exponential case. They will be proved in Sect. 2 as a consequence of our recent work [9]. Then in Sect. 3 we prove Theorems 1, 3, and 4. Here we shall be comparatively brief in our exposition, since this part of the proof closely follows the exponential analogue, apart from the (by now routine) use of the trick known as the Baker-Coates argument. Then in Sect. 4 we prove Theorems 2 and 5 . Here we shall be even briefer, and we shall leave to the reader the detailed checking of the zero estimates required.

We end this introduction by deducing Corollaries 1 and 2. Choose $\tau$ such that $k=\mathbb{Q}(\tau) \neq \mathbb{Q}$. Corollary 1 can be proved in two ways. We put $m=6, n=3$. Then either we apply Theorem 2 with $u_{1}=1, u_{2}=\beta, u_{3}=\beta^{2}$ and

$$
v_{1}=u, \quad v_{2}=\beta u, \quad v_{3}=\beta^{2} u, \quad v_{4}=\tau u, \quad v_{5}=\tau \beta u, \quad v_{6}=\tau \beta^{2} u,
$$

or we apply Theorem 3 with $u_{1}=u, u_{2}=\beta u, u_{3}=\beta^{2} u$ and

$$
v_{1}=1, \quad v_{2}=\beta, \quad v_{3}=\beta^{2}, \quad v_{4}=\tau, \quad v_{5}=\tau \beta, \quad v_{6}=\tau \beta^{2} .
$$

For Corollary 2 we can apply Theorem 5 with $u_{1}=\wp(1), u_{2}=1$ and

$$
v_{1}=1, \quad v_{2}=\wp(1), \quad v_{3}=\tau, \quad v_{4}=\tau \wp(1),
$$

since it is well-known that $\wp(1)$ is not in $k$ (and is even transcendental).

## 2. A Zero Estimate

Let $\wp(z)$ and $k$ be defined as in Sect. 1, let $\mathscr{L}$ be the period lattice of $\wp(z)$, and let $\mathscr{L}_{0}=\mathscr{L} \otimes \mathbb{Q}$ be the set of all $x \omega$ for $x$ in $\mathbb{Q}$ and $\omega$ in $\mathscr{L}$. Then $\mathscr{L}_{0}$ is a vector space over $k$. For integers $m \geqq 1, n \geqq 1$ let $u_{1}, \ldots, u_{n}$ and $v_{1}, \ldots, v_{m}$ be complex numbers linearly independent over $k$ and $\mathbb{Q}$ respectively. Let $U$ be the vector space over $k$ generated by $u_{1}, \ldots, u_{n}$, and let $V$ be the vector space over $\mathbb{Q}$ generated by $v_{1}, \ldots, v_{m}$. We define integers $m_{r}=m_{r}(U, V)(1 \leqq r \leqq n)$ as follows. For an integer $r$ with $1 \leqq r \leqq n$ let $m_{r}$, be the maximum dimension over $\mathbb{Q}$ of any subspace $V^{\prime}$ of $V$ for which there exists a subspace $U^{\prime}$ of $U$, of dimension $r$ over $k$, such that $u^{\prime} v^{\prime}$ lies in $\mathscr{L}_{0}$ for all $u^{\prime}$ in $U^{\prime}$ and all $v^{\prime}$ in $V^{\prime}$. Finally let $z_{0}$ be a complex number such that for all $v$ in $V$ none of the numbers $z_{0}+u_{i} v(1 \leqq i \leqq n)$ lies in $\mathscr{L}$.

Proposition 1. There is a constant $c$ depending only on $m$ and $n$ with the following property. Let $S \geqq 0$ be a real number and let $D \geqq 1, L \geqq 1, T \geqq 1$ be integers satisfying

$$
\begin{equation*}
T S^{m} \geqq c L D^{n}, \quad S^{m} \geqq c L D^{n-2} \tag{1}
\end{equation*}
$$

and

$$
\begin{equation*}
T S^{m-m_{r}} \geqq c D^{r}, \quad S^{m-m_{r}} \geqq c D^{r-1} \quad(1 \leqq r \leqq n) \tag{2}
\end{equation*}
$$

Suppose $P=P\left(x_{0}, x_{1}, \ldots, x_{n}\right)$ is a polynomial, of degree at most $\operatorname{Lin} x_{0}$ and of degree at most $D$ in each of $x_{1}, \ldots, x_{n}$, such that the function

$$
\varphi(z)=P\left(z, \wp\left(z_{0}+u_{1} z\right), \ldots, \wp\left(z_{0}+u_{n} z\right)\right)
$$

satisfies

$$
\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)=\mathbf{0}
$$

for all integers $t, s_{1}, \ldots, s_{m}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{m} \leqq S .
$$

Then $P$ is identically zero.
Proof. This is a straightforward deduction from one of the main results of [9] for a product of $k$ group varieties. For the convenience of the reader we reproduce this result here in the case $k=2$, which happens to suffice for our applications.

Accordingly let $H$ and $K$ be commutative group varieties defined over the complex field $\mathbb{C}$ and embedded in projective spaces $\mathbb{P}_{M}$ and $\mathbb{P}_{N}$ for integers $M \geqq 1$ and $N \geqq 1$ respectively. Then $G=H \times K$ is embedded in $\mathbb{P}_{M} \times \mathbb{P}_{N}$, whose points can be described in the usual way in terms of biprojective coordinates $x_{0}, \ldots, x_{M}$ and $y_{0}, \ldots, y_{N}$. Since $G$ is a smooth variety, it has the natural structure of a complex manifold. Let $\Phi$ be an analytic map from $\mathbb{C}$ to $G$ that is a homomorphism of additive groups, and denote also by $\Phi$ the image $\Phi(\mathbb{C})$ in $G$. Assume $\Phi$ does not reduce to the origin of $G$.

For an element $g$ of $G$ and a bihomogeneous polynomial $P$ in $\mathbb{C}\left[X_{0}, \ldots, X_{M}, Y_{0}, \ldots, Y_{N}\right]$ we define the order of vanishing of $P$ at $g$ along $\Phi$ as follows. It is well-known that the map $T_{g}$ from $G$ to $G$ representing translation by $g$ is analytic. Hence the composition $\Psi(z)=T_{g}(\Phi(z))$ is an analytic map from $\mathbb{C}$ to $G$.

In particular, there exist functions

$$
\begin{equation*}
\xi_{0}(z), \ldots, \xi_{M}(z), \eta_{0}(z), \ldots, \eta_{N}(z), \tag{3}
\end{equation*}
$$

analytic near $z=0$, such that for all $z$ sufficiently small their values are biprojective coordinates of $\Psi(z)$. If now the function

$$
f(z)=P\left(\xi_{0}(z), \ldots, \xi_{M}(z), \eta_{0}(z), \ldots, \eta_{N}(z)\right)
$$

is identically zero we write $\operatorname{ord}_{g} P=\infty$, this symbol being subject to the usual conventions. Otherwise we define $\operatorname{ord}_{g} P$ as the order of zero of $f(z)$ at $z=0$. It is easily seen that this definition is independent of the choice of functions (3) that represent $\Psi(z)$.

Next we assume that $H$ and $K$ are disjoint in the sense described in [9]. Namely, we assume that every connected algebraic subgroup $C$ of $G$ has the form $C=A \times B$ for algebraic subgroups $A$ of $H$ and $B$ of $K$. Let $X$ be a finite subset of $G$ containing the origin. Suppose the dimensions of $H$ and $K$ are $p \geqq 1$ and $q \geqq 1$ respectively. For integers $r, s$ with

$$
0 \leqq r \leqq p, \quad 0 \leqq s \leqq q, \quad r+s \geqq 1
$$

we define quantities $Q_{r s}(X)$ as follows. Firstly, if either $H$ has no algebraic subgroups of codimension $r$ or $K$ has no algebraic subgroups of codimension $s$ we put

$$
Q_{r s}(X)=|X|
$$

the cardinality of $X$. Otherwise for each subgroup $C$ of $G$ write $|X / C|$ for the maximum number of elements of $X$ that are distinct modulo $C$. Then we put

$$
Q_{r s}(X)=\min _{C}|X / C|
$$

as $C$ runs over all connected algebraic subgroups of $G$ of the form $C=A \times B$ with $A$ a connected algebraic subgroup of $H$ of codimension $r$ and $B$ a connected algebraic subgroup of $K$ of codimension $s$. Finally for an integer $k \geqq 1$ let $X^{(k)}$ denote the set of all sums $x_{1}+\ldots+x_{k}$ for $x_{1}, \ldots, x_{k}$ in $X$.

Now the Main Theorem (disjoint version) of [9] states the existence of a constant $c^{\prime}$ depending only on $H$ and $K$ with the following property. Suppose for integers $L \geqq 1, \quad D \geqq 1$ and $T \geqq 1$ there is a polynomial $P^{\prime}$ in $\mathbb{C}\left[X_{0}, \ldots, X_{M}, Y_{0}, \ldots, Y_{N}\right]$, homogeneous of degree at most $L$ in $X_{0}, \ldots, X_{M}$ and homogeneous of degree at most $D$ in $Y_{0}, \ldots, Y_{N}$, that vanishes at each point of $X^{(p+q)}$ to order at least $T$ along $\Phi$. As in [9], we say that a group variety embedded in projective space is linear if its addition laws can be given by bilinear forms. Let $T_{0}$ be any integer with $T_{0} \leqq L$ if $H$ is not a linear group variety and $T_{0} \leqq D$ if $K$ is not a linear group variety. Suppose that

$$
\begin{equation*}
T Q_{r s}(X) \geqq c^{\prime} L^{r} D^{s} \quad(0 \leqq r \leqq p, 0 \leqq s \leqq q, r+s \geqq 1) \tag{4}
\end{equation*}
$$

and

$$
\begin{equation*}
T_{0} Q_{r s}(X) \geqq c^{\prime} L^{\prime} D^{s} \quad(0 \leqq r \leqq p, 0 \leqq s \leqq q, 1 \leqq r+s<p+q) \tag{5}
\end{equation*}
$$

Suppose further that either

$$
T_{0} Q_{p q}(X) \geqq c^{\prime} L^{p} D^{q}
$$

or

$$
\begin{equation*}
\left|X / G_{\text {tors }}\right|=|X| \tag{6}
\end{equation*}
$$

where $G_{\text {tors }}$ is the torsion part of $G$. Then $P^{\prime}$ vanishes on all of $g+\Phi$ for some $g$ in $G$.
We can now deduce our Proposition 1. Let $\sigma(z)$ be the Weierstrass sigma function associated with $\wp(z)$, and denote by $\psi(z)$ the point in $\mathbb{P}_{2}$ with projective coordinates

$$
\wp\left(z_{0}+z\right)\left(\sigma\left(z_{0}+z\right)\right)^{3}, \wp^{\prime}\left(z_{0}+z\right)\left(\sigma\left(z_{0}+z\right)\right)^{3},\left(\sigma\left(z_{0}+z\right)\right)^{3} .
$$

As in [8, p. 511] denote by $E$ the elliptic curve such that $\psi$ is a group homomorphism from $\mathbb{C}$ to $E$. Thus $E$ is embedded in $\mathbb{P}_{2}$, and $K=E^{n}$ can then be embedded in $\mathbb{P}_{N}$ by means of the standard Segre map $\lambda$ from $\mathbb{P}_{2}^{n}$ to $\mathbb{P}_{N}$, where $N=3^{n}-1$. Also the additive group $H=\mathbb{C}$ can be embedded in $\mathbb{P}_{1}$ as a linear group, and we put $G=H \times K$. From part (i) of Lemma 7 of [9] it is clear that $H$ and $E$ are disjoint, since the only relevant subquotients are $H$ and $E / F$ respectively, where $F$ is a finite subgroup of $E$. These cannot be isomorphic, as one is complete and the other is not. Hence by repeated use of part (ii) of Lemma 7 of [9] we see that $H$ and $K=E^{n}$ are also disjoint.

We define the map $\Phi$ from $\mathbb{C}$ to $G=H \times K$ by

$$
\Phi(z)=\left(z, \lambda\left(\psi\left(u_{1} z\right), \ldots, \psi\left(u_{n} z\right)\right)\right)
$$

and the points $g_{1}, \ldots, g_{m}$ of $G$ by

$$
g_{j}=\Phi\left(v_{j}\right) \quad(1 \leqq j \leqq m)
$$

Let $X$ be the set of all combinations $s_{1} g_{1}+\ldots+s_{m} g_{m}$ for integers $s_{1}, \ldots, s_{m}$ with

$$
0 \leqq s_{1}, \ldots, s_{m} \leqq S /(n+1)
$$

Thus any $g$ in $X^{(n+1)}$ has the form $g=s_{1} g_{1}+\ldots+s_{m} g_{m}$ for integers $s_{1}, \ldots, s_{m}$ with $0 \leqq s_{1}, \ldots, s_{m} \leqq S$. If $v=s_{1} v_{1}+\ldots+s_{m} v_{m}$ then $g=\Phi(v)$ and so the map $\Psi(z)$ $=T_{g}(\Phi(z))$ is given by

$$
\Psi(z)=\Phi(z+v)=\left(z+v, \lambda\left(\psi\left(u_{1}(z+v)\right), \ldots, \psi\left(u_{n}(z+v)\right)\right)\right) .
$$

Since by hypothesis the function

$$
\varphi(z+v)=P\left(z+v, \wp\left(z_{0}+u_{1}(z+v)\right), \ldots, \wp\left(z_{0}+u_{n}(z+v)\right)\right)
$$

has a zero of order at least $T$ at $z=0$, it follows without difficulty that the polynomial $P$ of Proposition 1 gives rise to a bihomogeneous polynomial $P^{\prime}$ vanishing on $X^{(n+1)}$ to order at least $T$ along $\Phi$. Because $H$ is a linear group variety, we may choose $T_{0}=D$. We now verify that the conditions (1), (2) imply the conditions (4)-(6). In fact (6) is clear at once, as $G_{\text {tors }}=0 \times K_{\text {tors }}$ and $v_{1}, \ldots, v_{m}$ are linearly independent over $\mathbb{Q}$. To verify (4) and (5) we have to estimate the quantities $Q_{r s}(X)$ from below.

To start with, we note that

$$
Q_{1 s}(X)=|X| \geqq(S /(n+1))^{m} \quad(0 \leqq s \leqq n),
$$

since the subgroup $C$ of $G$ now has the form $0 \times B$. Next, we claim that

$$
\begin{equation*}
Q_{0 s}(X) \geqq(S /(n+1))^{m-m_{s}} \quad(1 \leqq s \leqq n) . \tag{7}
\end{equation*}
$$

This is clear if $m_{s}=m$. So assume $m_{s}<m$. The subgroup $C$ of $G$ now has the form $H \times B$ for some algebraic subgroup $B$ of $K$ of codimension $s$. If $\mathcal{O}$ is the endomorphism ring of the lattice $\mathscr{L}$, it follows from Lemma 11 (p. 512) of [8] that we can find $s$ elements $\left(t_{i 1}, \ldots, t_{i n}\right)(1 \leqq i \leqq s)$ of $\mathcal{O}^{n}$, linearly independent over $k$, such that for any $\left(\psi\left(z_{1}\right), \ldots, \psi\left(z_{n}\right)\right)$ in $B$ we have

$$
\varphi\left(t_{i 1} z_{1}+\ldots+t_{i n} z_{n}\right)=0 \quad(1 \leqq i \leqq s) ;
$$

that is, $t_{i 1} z_{1}+\ldots+t_{i n} z_{n}$ lies in $\mathscr{L}(1 \leqq i \leqq s)$. Thus the elements

$$
u_{i}^{\prime}=t_{i 1} u_{1}+\ldots+t_{\text {in }} u_{n} \quad(1 \leqq i \leqq s)
$$

of $U$ generate a subspace $U^{\prime}$ of $U$ of dimension sover $k$. Let $V^{\prime}$ be the subspace of all $v^{\prime}$ in $V$ such that $u^{\prime} v^{\prime}$ lies in $\mathscr{L}_{0}$ for all $u^{\prime}$ in $U^{\prime}$. By the definition of $m_{s}$, the dimension of $V^{\prime}$ over $\mathbb{Q}$ is at most $m_{s}$. We may therefore find $l=m-m_{s}$ elements among $v_{1}, \ldots, v_{m}$ that are linearly independent over $\mathbb{Q}$ modulo $V^{\prime}$; and without loss of generality we can suppose these to be $v_{1}, \ldots, v_{1}$.

Now we observe that the elements of $X$ given by

$$
s_{1} g_{1}+\ldots+s_{l} g_{l} \quad\left(0 \leqq s_{1}, \ldots, s_{l} \leqq S /(n+1)\right)
$$

are distinct modulo $C=H \times B$. For if not, we could find integers $s_{1}^{\prime}, \ldots, s_{l}^{\prime}$, not all zero, such that $g^{\prime}=s_{1}^{\prime} g_{1}+\ldots+s_{l}^{\prime} g_{l}$ lies in $C$. Thus if $v^{\prime}=s_{1}^{\prime} v_{1}+\ldots+s_{l}^{\prime} v_{l}$ the element ( $\psi\left(u_{1} v^{\prime}\right), \ldots, \psi\left(u_{n} v^{\prime}\right)$ ) lies in $B$, and this would imply that $t_{i 1} u_{1} v^{\prime}+\ldots+t_{i n} u_{n} v^{\prime}$ lies in $\mathscr{L}(1 \leqq i \leqq s)$. Thus $u^{\prime} v^{\prime}$ lies in $\mathscr{L}$ for all $u^{\prime}$ in $U^{\prime}$. Hence $v^{\prime}$ lies in $V^{\prime}$; however, this contradicts the linear independence of $v_{1}, \ldots, v_{l}$ modulo $V^{\prime}$. It follows that $|X / C|$ $\geqq(S /(n+1))^{m-m_{s}}$, and then taking the minimum over all $C$ gives (7).

It is now easy to verify that if we define $c$ in terms of $c^{\prime \prime}$ by $c=\dot{c}^{\prime}(n+1)^{m}$ then the conditions (1), (2) imply (4), (5). Accordingly our bihomogeneous polynomial $P^{\prime}$ vanishes on $g+\Phi$ for some $g$ in $G$. To deduce that the original polynomial $P$ is identically zero it suffices to prove that $\Phi$ is Zariski-dense in $G$. But the Zariskiclosure is an algebraic subgroup of $G$; let $C$ be its connected component through the origin. By disjointness $C=A \times B$ for algebraic subgroups $A$ of $H$ and $B$ of $K$, and clearly from the form of $\Phi(z)$ we must have $A=H$. But also $B=K$, otherwise by Lemma 11 of [8] there would exist a non-zero ( $t_{1}, \ldots, t_{n}$ ) in $\mathcal{O}^{n}$ such that $t_{1} u_{1} z+\ldots+t_{n} u_{n} z$ lies in $\mathscr{L}$ for all complex $z$, which is obviously impossible as $t_{1} u_{1}+\ldots+t_{n} u_{n} \neq 0$. Thus $C=G$, and $\Phi$ is indeed Zariski-dense in $G$. This completes the proof of Proposition 1.

Actually the calculations of [9] show that $c^{\prime}$ can be taken as $4^{3^{n+1}}$. Hence Proposition 1 holds with $c=4^{3^{n+1}}(n+1)^{m}$.

To apply the proposition we need upper bounds for the numbers $m_{1}, \ldots, m_{n}$. We record these in the following simple lemma.

Lemma 1. We have $m_{1} \leqq 2$; also if $n \geqq 2$ then $m_{2} \leqq 1$; and if $n \geqq 3$ then $m_{r}=0$ whenever $\mathbf{3} \leqq r \leqq n$.

Proof. First suppose on the contrary that $m_{1} \geqq 3$. Then there exist elements $v_{1}^{\prime}, v_{2}^{\prime}, v_{3}^{\prime}$ of $V$, linearly independent over $\mathbb{Q}$, and a non-zero element $u_{1}^{\prime}$ of $U$, such that $u_{1}^{\prime} v_{1}^{\prime}, u_{1}^{\prime} v_{2}^{\prime}, u_{1}^{\prime} v_{3}^{\prime}$ all lie in $\mathscr{L}_{0}$. Since $\mathscr{L}_{0}$ is a vector space over $\mathbb{Q}$ of dimension 2,
there are rationals $x_{1}, x_{2}, x_{3}$, not all zero, such that

$$
0=x_{1} u_{1}^{\prime} v_{1}^{\prime}+x_{2} u_{1}^{\prime} v_{2}^{\prime}+x_{3} u_{1}^{\prime} v_{3}^{\prime}=u_{1}^{\prime}\left(x_{1} v_{1}^{\prime}+x_{2} v_{2}^{\prime}+x_{3} v_{3}^{\prime}\right) .
$$

This is clearly impossible under the hypotheses given, and hence indeed $m_{1} \leqq 2$.
Next suppose $n \geqq 2$ and $m_{2} \geqq 2$. Then there exist elements $v_{1}^{\prime}, v_{2}^{\prime}$ of $V$, linearly independent over $\mathbb{Q}$, and elements $u_{1}^{\prime}, u_{2}^{\prime}$ of $U$, linearly independent over $k$, such that $u_{1}^{\prime} v_{1}^{\prime}, u_{1}^{\prime} v_{2}^{\prime}, u_{2}^{\prime} v_{1}^{\prime}, u_{2}^{\prime} v_{2}^{\prime}$ all lie in $\mathscr{L}_{0}$. If $V^{\prime}$ is the vector space over $\mathbb{Q}$ generated by $v_{1}^{\prime}, v_{2}^{\prime}$, it follows that $\mathscr{L}_{0}=u_{1}^{\prime} V^{\prime}=u_{2}^{\prime} V^{\prime}$. Thus $u_{2}^{\prime} / u_{1}^{\prime}$ is an endomorphism of $\mathscr{L}_{0}$, so it must lie in $k$, which is not possible. Hence indeed $m_{2} \leqq 1$.

Finally suppose $n \geqq 3$ and $m_{r} \geqq 1$ for some $r$ with $3 \leqq r \leqq n$. Then there exists a non-zero $v_{1}^{\prime}$ of $V$, and elements $u_{1}^{\prime}, \ldots, u_{r}^{\prime}$ of $U$ linearly independent over $k$ such that $u_{1}^{\prime} v_{1}^{\prime}, \ldots, u_{r}^{\prime} v_{1}^{\prime}$ lie in $\mathscr{L}_{0}$. In particular $u_{1}^{\prime}, u_{2}^{\prime}, u_{3}^{\prime}$ are linearly independent over $\mathbb{Q}$, and now the argument of the first part applies mutatis mutandis. This completes the proof of Lemma 1.

It is clear that these upper bounds can be improved in the case $k \neq \mathbb{Q}$ of complex multiplication; in fact one then has $m_{1} \leqq 1$ and $m_{r}=0$ for $r \geqq 2$. But we will not need these improvements except for a very special case of Theorem 5.

## 3. Proof of Theorems $1,3,4$

We shall describe in turn the proofs of Theorems 1, 3, and 4. Now that Proposition 1 is available, no new principles are involved, and we can be relatively concise.

Suppose $\vartheta$ is transcendental over $\mathbb{Q}$. Then any non-zero $\lambda$ in $\mathbb{Z}[\vartheta]$ can be written uniquely as $P(\vartheta)$ for some non-zero polynomial $P(x)$ in $\mathbb{Z}[x]$. Recall that the (logarithmic) type of $\lambda$ is defined as $\max (d, \log H)$, where $d$ is the degree of $P$ and $H$ is the maximum of the absolute values of its coefficients. It is convenient also to define the type of the zero element as $-\infty$.

The first step in all the proofs is to find a complex number $z_{0}$ such that $\ell\left(z_{0}\right)$ is algebraic and such that for any integers $s_{1}, \ldots, s_{m}$ none of the numbers

$$
z_{0}+u_{i}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right) \quad(1 \leqq i \leqq n)
$$

lie in the period lattice $\mathscr{L}$ of $\wp(z)$. This is clearly possible.
Now assume Theorem 1 is false for some integers $m \geqq 1, n \geqq 1$ satisfying

$$
\begin{equation*}
m n \geqq 2 m+4 n \tag{8}
\end{equation*}
$$

It follows easily that the numbers

$$
g_{2}, g_{3}, \wp\left(z_{0}\right), \wp^{\prime}\left(z_{0}\right), \wp\left(z_{0}+u_{i} v_{j}\right), \wp^{\prime}\left(z_{0}+u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

lie in a field $K$ of transcendence degree at most 1 over $\mathbb{Q}$. We can therefore find complex numbers $\vartheta, \vartheta_{1}$ such that $K$ is contained in $\mathbb{Q}\left(\vartheta, \vartheta_{1}\right)$, where $\vartheta$ is transcendental over $\mathbb{Q}$, and $\vartheta_{1}$ is algebraic over $\mathbb{Q}(\vartheta)$. We fix a suitably large constant $C$ depending only on these quantities, and we choose any large integer $D$. We define

$$
S=C D^{n / m}, \quad S_{0}=C^{-2} S
$$

We use $c_{1}, c_{2}, \ldots$ for positive constants independent of $D$.

From Siegel's version of the Box Principle we can construct a non-zero polynomial $P\left(x_{1}, \ldots, x_{n}\right)$, of degree at most $D$ in each variable, with the following properties. Firstly, the coefficients of $P$ are elements of $\mathbb{Z}[\vartheta]$ with types at most $c_{1} D S_{0}^{2}$, and secondly, the function

$$
\varphi(z)=P\left(\wp\left(z_{0}+u_{1} z\right), \ldots, \wp\left(z_{0}+u_{n} z\right)\right)
$$

satisfies

$$
\varphi\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)=0
$$

for all integers $s_{1}, \ldots, s_{m}$ with

$$
0 \leqq s_{1}, \ldots, s_{m} \leqq S_{0}
$$

Next, by applying the maximum modulus principle on circles of radius $C S$ and $C D^{s} S$ for suitably small $\varepsilon>0$ we see that

$$
\log \left|\varphi\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)\right|<-c_{2} S_{0}^{m} \log D
$$

for all integers $s_{1}, \ldots, s_{m}$ with

$$
0 \leqq s_{1}, \ldots, s_{m} \leqq S
$$

We now apply Proposition 1 with $L=T=1$ to deduce that at least one of these numbers $\xi=\varphi\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)$ is non-zero. By Lemma 1, it suffices to check the conditions

$$
S^{m} \geqq c D^{n}, \quad S^{m-1} \geqq c D^{2}, \quad S^{m-2} \geqq c D .
$$

But these follow from the definition of $S$ and the inequality (8).
Finally, by clearing denominators and taking norms of $\xi$ in the usual way we end up with a non-zero element $\pi=\pi_{D}$ of $\mathbb{Z}[\vartheta]$, of type at most $c_{3} D S^{2}$, such that

$$
\log \left|\pi_{D}\right|<-c_{4} S_{0}^{m} \log D
$$

Since

$$
\left(D S^{2}\right)^{2} \leqq c_{5} D^{(2 m+4 n) / m}, \quad S_{0}^{m} \log D \geqq c_{6} D^{n} \log D,
$$

the inequality (8) shows that we can apply the well-known criterion of Gelfond to the sequence of elements $\pi_{D}$ to obtain a final contradiction. This proves Theorem 1. We note that the critical pairs $(m, n)$ satisfying $(8)$ are $(5,10),(6,6),(7,5)$, $(8,4)$, and $(12,3)$.

Next assume Theorem 3 is false for some integers $m \geqq 1, n \geqq 1$ satisfying

$$
\begin{equation*}
m n \geqq m+4 n . \tag{9}
\end{equation*}
$$

We note that this implies $m \geqq 5$. This time the numbers

$$
g_{2}, g_{3}, \wp\left(z_{0}\right), \wp^{\prime}\left(z_{0}\right), v_{j}, \wp\left(z_{0}+u_{i} v_{j}\right), \wp^{\prime}\left(z_{0}+u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

lie in a field $\mathbb{Q}\left(\vartheta, \vartheta_{1}\right)$ as before. For $C, D$ as above we define

$$
S=C D^{(n+1) /(m-2)}(\log D)^{-1 /(m-2)}, \quad S_{0}=C^{-2} S
$$

and

$$
L=\left[D^{(m+2 n) /(m-2)}(\log D)^{-m /(m-2)}\right] .
$$

We construct a non-zero polynomial $P\left(x_{0}, x_{1}, \ldots, x_{n}\right)$, of degree at most $L$ in $x_{0}$ and of degree at most $D$ in each of $x_{1}, \ldots, x_{n}$, whose coefficients are in $\mathbb{Z}[\vartheta]$ of types at most

$$
c_{1}\left(L \log D+D S_{0}^{2}\right) \leqq c_{2} D S^{2},
$$

such that the function

$$
\varphi(z)=P\left(z, \wp\left(z_{0}+u_{1} z\right), \ldots, \wp\left(z_{0}+u_{n} z\right)\right)
$$

satisfies

$$
\varphi\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)=0
$$

for all integers $s_{1}, \ldots, s_{m}$ with

$$
0 \leqq s_{1}, \ldots, s_{m} \leqq S_{0} .
$$

The maximum modulus principle on the circles of radius $C S$ and $C D^{2} S$ then gives

$$
\log \left|\varphi\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)\right|<-c_{3} S_{0}^{m} \log D
$$

for all integers $s_{1}, \ldots, s_{m}$ with

$$
0 \leqq s_{1}, \ldots, s_{m} \leqq S
$$

We apply Proposition 1 with $T=1$ to deduce that at least one of these numbers $\varphi\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)$ is non-zero. By Lemma 1 , it suffices to check the conditions

$$
S^{m} \geqq c L D^{n}, \quad S^{m-1} \geqq c D^{2}, \quad S^{m-2} \geqq c D .
$$

These follow from the definitions and the inequality (9).
So we get a non-zero element $\pi=\pi_{D}$ of $\mathbb{Z}[\vartheta]$, of type at most $c_{4} D S^{2}$, such that

$$
\log \left|\pi_{D}\right|<-c_{S} S_{0}^{m} \log D .
$$

Since

$$
\begin{gathered}
\left(D S^{2}\right)^{2} \leqq c_{6} D^{(2 m+4 n) /(m-2)}(\log D)^{-4 /(m-2)}, \\
S_{0}^{m} \log D \geqq c_{7} D^{(m n+m) /(m-2)}(\log D)^{-2 /(m-2)},
\end{gathered}
$$

we see again from (9) that Gelfond's criterion applies and gives our contradiction. This proves Theorem 3. The critical values of $(m, n)$ are $(5,5),(6,3)$, and $(8,2)$.

Finally assume Theorem 4 is false for some integers $m \geqq 1, n \geqq 1$ satisfying

$$
\begin{equation*}
m n>m+2 n . \tag{10}
\end{equation*}
$$

Then $m \geqq 3$, and the numbers

$$
g_{2}, g_{3}, \wp\left(z_{0}\right), \wp^{\prime}\left(z_{0}\right), u_{i}, v_{j}, \wp\left(z_{0}+u_{i} v_{j}\right), \wp^{\prime}\left(z_{0}+u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

lie in $\mathbb{Q}\left(\vartheta, \vartheta_{1}\right)$. We put

$$
\begin{equation*}
l=\min (m+2 n-1,2 m) \tag{11}
\end{equation*}
$$

and we define

$$
\begin{gathered}
S=C D^{n / m}, \quad S_{0}=C^{-2} S \\
L=T=\left[D^{l / m}\right] .
\end{gathered}
$$

We construct a non-zero polynomial $P\left(x_{0}, x_{1}, \ldots, x_{n}\right)$, of degree at most $L$ in $x_{0}$ and of degree at most $D$ in each of $x_{1}, \ldots, x_{n}$, whose coefficients are in $\mathbb{Z}[\vartheta]$ of types at most

$$
c_{1}\left(T \log D+L \log D+D S_{0}^{2}\right) \leqq c_{2} D S^{2}
$$

such that the function

$$
\varphi(z)=P\left(z, \wp\left(z_{0}+u_{1} z\right), \ldots, \wp\left(z_{0}+u_{n} z\right)\right)
$$

satisfies

$$
\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)=0
$$

for all integers $t, s_{1}, \ldots, s_{m}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{m} \leqq S_{0}
$$

We should emphasize here that in order to avoid quantities of order $T S_{0}^{2}$ appearing in the estimates for the types, the Baker-Coates trick should be used (see for example [4, p. 208]). The maximum modulus principle on circles of radius CS and $C D^{e} S$ then gives

$$
\log \left|\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)\right|<-c_{3} T S_{0}^{m} \log D
$$

for all integers $t, s_{1}, \ldots, s_{m}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{m} \leqq S .
$$

We apply Proposition 1 to deduce that at least one of these numbers $\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)$ is non-zero. By Lemma 1, it suffices to check the conditions

$$
T S^{m} \geqq c L D^{n}, \quad T S^{m-1} \geqq c D^{2}, \quad T S^{m-2} \geqq c D
$$

and

$$
\begin{equation*}
S^{m} \geqq c L D^{n-2}, \quad S^{m} \geqq c D^{n-1}, \quad S^{m-1} \geqq c D, \quad S^{m-2} \geqq c . \tag{12}
\end{equation*}
$$

Using (10) and (11), we easily verify all of these. Thus we obtain a non-zero element $\pi=\pi_{D}$ of $\mathbb{Z}[\vartheta]$, of type at most $c_{4} D S^{2}$, such that

$$
\log \left|\pi_{D}\right|<-c_{5} T S_{0}^{m} \log D .
$$

This time we have

$$
\left(D S^{2}\right)^{2} \leqq c_{6} D^{(2 m+4 n) / m}, \quad T S_{0}^{m} \log D \geqq c_{7} D^{(1+m n) / m} \log D,
$$

and it can be verified from (10) and (11) that

$$
l+m n \geqq 2 m+4 n
$$

provided $m \geqq 4$. Now the critical solutions of $(10)$ are given by $(m, n)=(3,4),(4,3)$, and (5,2). Hence we deduce Theorem 4 in all these cases except the first. It remains thus to consider $(m, n)=(3,4)$.

But if $k=\mathbb{Q}$ we see by interchanging the $u$ 's and $v$ 's that Theorem 4 with $(m, n)=(3,4)$ is equivalent to the same theorem with $(m, n)=(4,3)$, and is therefore also proved. Next suppose $k=\mathbb{Q}(\tau) \neq \mathbb{Q}$. Consider the vector space generated over
$k$ by $v_{1}, v_{2}, v_{3}$. This is also a vector space over $\mathbb{Q}$ whose dimension $d$ is even with $d \geqq 3$. Hence $d \geqq 4$, and without loss of generality we can assume that $v_{4}=\tau v_{1}$ together with $v_{1}, v_{2}, v_{3}$ are linearly independent over $\mathbb{Q}$. Now since $\wp\left(u_{i} v_{4}\right)$ is algebraic over $\mathbb{Q}\left(\wp\left(u_{i} v_{1}\right)\right)(1 \leqq i \leqq 4)$, we are in the situation of Theorem 4 with $(m, n)=(4,4)$. But such a result is covered by the case $(m, n)=(4,3)$ just established. This completes the proof of Theorem 4 in general.

## 4. Proof of Theorems 2,5

For Theorem 2 we shall need the following simpler version of Proposition 1 when the polynomial $P\left(x_{0}, x_{1}, \ldots, x_{n}\right)$ is independent of $x_{0}$. We keep the same notation for $u_{1}, \ldots, u_{n}, v_{1}, \ldots, v_{m}, z_{0}$ and the integers $m_{1}, \ldots, m_{n}$.
Proposition 2. There is a constant $c$ depending only on $m$ and $n$ with the following property. Let $S \geqq 0$ be a real number and let $D \geqq 1, T \geqq 1$ be integers satisfying

$$
T S^{m-m_{r}} \geqq c D^{r} \quad(1 \leqq r \leqq n)
$$

and (if $n \geqq 2$ )

$$
S^{m-m_{r}} \geqq c D^{r-1} \quad(1 \leqq r<n) .
$$

Suppose $P=P\left(x_{1}, \ldots, x_{n}\right)$ is a polynomial, of degree at most $D$ in each of $x_{1}, \ldots, x_{n}$, such that the function

$$
\varphi(z)=P\left(\wp\left(z_{0}+u_{1} z\right), \ldots, \not \wp\left(z_{0}+u_{n} z\right)\right)
$$

satisfies

$$
\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)=0
$$

for all integers $t, s_{1}, \ldots, s_{m}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{m} \leqq S .
$$

Then $P$ is identically zero.
Proof. This can be deduced from either Main Theorem of [9] just as we proved Proposition 1. But it is simpler to appeal directly to Theorem A (p. 514) of [8] (see [9, Sect. 8]), as there is then no need to check the condition (6) above. We leave the details to the reader.

Now assume Theorem 2 is false for some integers $m \geqq 1, n \geqq 1$ satisfying

$$
\begin{equation*}
m n \geqq 2 m+2 n . \tag{13}
\end{equation*}
$$

Then $m \geqq 3, n \geqq 3$, and, choosing $z_{0}$ as in Sect. 3, we see that the numbers

$$
g_{2}, g_{3}, \wp\left(z_{0}\right), \wp^{\prime}\left(z_{0}\right), u_{i}, \wp\left(z_{0}+u_{i} v_{j}\right), \wp^{\prime}\left(z_{0}+u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

lie in a field $\mathbb{Q}\left(\vartheta, \vartheta_{1}\right)$ as before. For $C, D$ as in Sect. 3 we define

$$
\begin{aligned}
& S=C D^{(n-1) /(m+2)}(\log D)^{1 /(m+2)}, \quad S_{0}=C^{-2} S \\
& T=\left[D^{(m+2 n) /(m+2)}(\log D)^{-m /(m+2)}\right] .
\end{aligned}
$$

Using the Baker-Coates argument, we construct a non-zero polynomial $P\left(x_{1}, \ldots, x_{n}\right)$, of degree at most $D$ in each variable, whose coefficients are in $\mathbb{Z}[\vartheta]$ of types at most

$$
c_{1}\left(T \log D+D S_{0}^{2}\right) \leqq c_{2} D S^{2},
$$

such that the function

$$
\varphi(z)=P\left(\wp\left(z_{0}+u_{1} z\right), \ldots, \wp\left(z_{0}+u_{n} z\right)\right)
$$

satisfies

$$
\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)=0
$$

for all integers $t, s_{1}, \ldots, s_{m}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{m} \leqq S_{0} .
$$

Next the maximum modulus principle on circles of radius $C S$ and $C D^{s} S$ gives

$$
\log \left|\varphi^{(t)}\left(S_{1} v_{1}+\ldots+s_{m} v_{m}\right)\right|<-c_{3} T S_{0}^{m} \log D
$$

for all integers $t, s_{1}, \ldots, s_{m}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{m} \leqq S .
$$

We apply Proposition 2 to deduce that at least one of these numbers $\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)$ is non-zero. By Lemma 1 , it suffices to check the conditions

$$
T S^{m} \geqq c D^{n}, \quad T S^{m-1} \geqq c D^{2}, \quad T S^{m-2} \geqq c D
$$

as well as

$$
\begin{equation*}
S^{m} \geqq c D^{n-2}, \quad S^{m-1} \geqq c D, \quad S^{m-2} \geqq c . \tag{14}
\end{equation*}
$$

Using (13) we easily verify all of these except the first of (14), which needs the additional inequality $m \geqq 2 n-4$. We therefore temporarily assume this. Then we obtain a non-zero element $\pi=\pi_{D}$ of $\mathbb{Z}[9]$, of type at most $c_{4} D S^{2}$, such that

$$
\log \left|\pi_{D}\right|<-c_{5} T S_{0}^{m} \log D .
$$

This time we have

$$
\begin{gathered}
\left(D S^{2}\right)^{2} \leqq c_{6} D^{(2 m+4 n) /(m+2)}(\log D)^{4 /(m+2)}, \\
T S_{0}^{m} \log D \geqq c_{7} D^{n} \log D,
\end{gathered}
$$

and so Gelfond's criterion applies using (13). Now the critical solutions of (13) are given by $(m, n)=(3,6),(4,4)$, and $(6,3)$. Since we have assumed $m \geqq 2 n-4$, we deduce Theorem 2 in all these cases except the first. But we can deal with the remaining case much as in the proof of Theorem 4. Namely, if $k=\mathbb{Q}$ we see on interchanging the $u$ 's and $v$ 's that Theorem 2 with $(m, n)=(3,6)$ is equivalent to Theorem 3 with ( $m, n$ ) $=(6,3)$, and is therefore also proved. If $k \neq \mathbb{Q}$ we can adjoin $v_{4}$ as before, and this puts us in the situation of Theorem 2 with $(m, n)=(4,6)$. But such a result is covered by the case $(m, n)=(4,4)$ of Theorem 2 just established. This completes the proof of Theorem 2 in general.

For Theorem 5 we shall need the following zero estimate, again in the notation of Sect. 2.

Proposition 3. There is a constant $c$ depending only on $m$ and $n$ with the following property. Let $S \geqq 0$ be a real number and let $D_{0}, \ldots, D_{n}, T \geqq 1$ be integers with

$$
D_{0} \geqq D_{1} \geqq \ldots \geqq D_{n} \geqq 1
$$

and satisfying

$$
\begin{aligned}
& T S^{m} \geqq c D_{0} D_{1} \ldots D_{n} \\
& T S^{m-m_{r}} \geqq c D_{0} \ldots D_{r-1}, \quad D_{n} S^{m-m_{r}} \geqq c D_{0} \ldots D_{r-1} \quad(1 \leqq r \leqq n) .
\end{aligned}
$$

Suppose $P=P\left(x_{0}, x_{1}, \ldots, x_{n}\right)$ is a polynomial, of degree at most $D_{r}$ in $x_{r}(0 \leqq r \leqq n)$, such that the function

$$
\varphi(z)=P\left(z, \wp\left(z_{0}+u_{1} z\right), \ldots, \wp\left(z_{0}+u_{n} z\right)\right)
$$

satisfies

$$
\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)=0
$$

for all integers $t, s_{1}, \ldots, s_{m}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{m} \leqq S .
$$

Then $P$ is identically zero.
Proof. This can be deduced from the Main Theorem (disjoint version) of [9] just as we proved Propositions 1 and 2, using disjointness only to observe that in the notation of [9] we have

$$
Q_{s}(X)=\min \left(Q_{0 s}(X), Q_{1, s-1}(X)\right) \quad(1 \leqq s \leqq n)
$$

and

$$
Q_{n+1}(X)=Q_{1 n}(X)
$$

for any finite subset $X$ of $\mathbb{C} \times E^{n}$. Alternatively we can appeal to Theorem ABC (p. 515) of [8]. We leave the details to the reader.

We shall also need the following special algebraic independence result for a Weierstrass elliptic function with algebraic invariants.

Lemma 2. Suppose $\wp(z)$ has no complex multiplication, let $\omega_{1}, \omega_{2}$ be periods of $\wp(z)$ linearly independent over $\mathbb{Q}$, and suppose $\chi_{1}, \chi_{2}, \chi_{3}$ are complex numbers with 1 , $\chi_{1}, \chi_{2}, \chi_{3}$ linearly independent over $\mathbb{Q}$. Then at least two of the numbers

$$
\omega_{1} / \omega_{2}, \wp\left(\omega_{i} \chi_{j}\right) \quad(i=1,2 ; j=1,2,3)
$$

are defined and are algebraically independent over $\mathbb{Q}$.
Proof. We only give a very rapid sketch, since the result could have been proved by classical methods without the aid of zero estimates on group varieties (see Theorem 4.2 (p. 314) of Chudnovsky [5] for a similar result). For $z_{0}, \vartheta, \vartheta_{1}, C, D$ as before define

$$
S=C D^{3 / 14}, \quad S_{0}=C^{-2} S, \quad T=\left[D^{19 / 14}\right]
$$

and construct a non-zero polynomial $P\left(x_{1}, x_{2}\right)$, of degree at most $D$ in each variable, whose coefficients are in $\mathbb{Z}[\vartheta]$ of types at most $c_{1} D S_{0}^{2} \leqq c_{1} D^{10 / 7}$, such that

$$
\varphi(z)=P\left(\wp\left(z_{0}+\omega_{1} z\right), \wp\left(z_{0}+\omega_{2} z\right)\right)
$$

satisfies

$$
\varphi^{(t)}\left(s_{1} \chi_{1}+s_{2} \chi_{2}+s_{3} \chi_{3}\right)=0
$$

for all integers $t, s_{1}, s_{2}, s_{3}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, s_{2}, s_{3} \leqq S_{0} .
$$

Put

$$
R=D^{13 / 14} ;
$$

then by periodicity we have

$$
\varphi^{(t)}\left(s_{1} \chi_{1}+s_{2} \chi_{2}+s_{3} \chi_{3}+s_{4}\right)=0
$$

for all integers $t, s_{1}, s_{2}, s_{3}, s_{4}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, s_{2}, s_{3} \leqq S_{0}, \quad 0 \leqq s_{4} \leqq R .
$$

The maximum modulus principle on circles of radius $C R$ and $C^{2} R$ yields

$$
\log \left|\varphi^{(t)}\left(s_{1} \chi_{1}+s_{2} \chi_{2}+s_{3} \chi_{3}\right)\right|<-c_{2} T S_{0}^{3} R
$$

for all integers $t, s_{1}, s_{2}, s_{3}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, s_{2}, s_{3} \leqq S .
$$

A routine application of Theorem A of [8] shows that at least one of these values is non-zero, and this gives rise to a non-zero $\pi_{D}$ in $\mathbb{Z}[9]$ with type at most $c_{3} D^{10 / 7}$ and

$$
\log \left|\pi_{D}\right|<-c_{4} T S_{0}^{3} R .
$$

Since $T S_{0}^{3} R \geqq c_{5} D^{41 / 14}$, Gelfond's criterion now supplies the contradiction which proves Lemma 2.

Alternatively we can avoid the appeal to [8] by using Theorem 1 (p. 200) of [4]. Denoting by $X$ the vector space generated over $\mathbb{Q}$ by $\chi_{1}, \chi_{2}, \chi_{3}$, the distinctness condition in this result applied to $\varphi\left(\left(z-z_{0}\right) / \omega_{1}\right)$ shows that there exists $\chi \neq 0$ in $X$ with $\omega_{1} \chi$ in $\mathscr{L}$. It is not possible to deduce a contradiction instantly; however, we observe that the content of Lemma 2 is not altered by replacing in its statement the periods $\omega_{1}, \omega_{2}$ by any two periods $\omega^{\prime}, \omega^{\prime \prime}$ linearly independent over $\mathbb{Q}$. In particular, taking $\omega_{j}^{\prime}=\omega_{1}+j \omega_{2}$ and suitable $\omega_{j}^{\prime \prime}(1 \leqq j \leqq 4)$, we see that there exists $\chi_{j}^{\prime} \neq 0$ in $X$ with

$$
\begin{equation*}
\omega_{j}^{\prime} x_{j}^{\prime}=a_{j} \omega_{1}+b_{j} \omega_{2} \tag{15}
\end{equation*}
$$

for rational $a_{j}, b_{j}(1 \leqq j \leqq 4)$. Since the dimension of $X$ is 3 , we can find rationals $x_{1}, x_{2}, x_{3}, x_{4}$, not all zero, with $\sum_{j=1}^{4} x_{j} \chi_{j}^{\prime}=0$. Hence $\tau=\omega_{1} / \omega_{2}$ satisfies the equation $R(\tau)=0$, where

$$
R(t)=\sum_{j=1}^{4} x_{j}\left(a_{j} t+b_{j}\right) /(t+j) .
$$

But because there is no complex multiplication we know from Schneider's theorem that $\tau$ is transcendental; hence $R(t)$ must be identically zero. It follows easily on considering the possible poles of $R(t)$ that we have $j a_{j}=b_{j}$ for some $j$ with $1 \leqq j \leqq 4$. In this case (15) shows that $\chi_{j}^{\prime} \neq 0$ is rational, which contradicts the linear independence over $\mathbb{Q}$ of $1, \chi_{1}, \chi_{2}, \chi_{3}$.

Now suppose Theorem 5 is false. By Lemma 1, the corresponding integer $m_{2}$ is either 0 or 1 . We assume for the moment that $m_{2}=0$. Choosing $z_{0}$ in the usual way, we find that

$$
g_{2}, g_{3}, \wp\left(z_{0}\right), \wp^{\prime}\left(z_{0}\right), u_{i}, v_{j}, \wp\left(z_{0}+u_{i} v_{j}\right), \wp^{\prime}\left(z_{0}+u_{i} v_{j}\right) \quad(1 \leqq i \leqq n, 1 \leqq j \leqq m)
$$

lie in $Q\left(\vartheta, \vartheta_{1}\right)$. For $C, D$ as before define

$$
\begin{gathered}
S=C D^{1 / 2}(\log D)^{3 / 16}, \quad S_{0}=C^{-2} S, \quad T=\left[D^{2}(\log D)^{-1 / 4}\right] \\
D_{0}=\left[D^{2}(\log D)^{-1 / 8}\right], \quad D_{1}=\left[D(\log D)^{5 / 8}\right], \quad D_{2}=D .
\end{gathered}
$$

We construct a non-zero polynomial $P\left(x_{0}, x_{1}, x_{2}\right)$, of degree at most $D_{r}$ in $x_{r}$ ( $r=0,1,2$ ), with coefficients in $\mathbb{Z}[\vartheta]$, such that the function

$$
\varphi(z)=P\left(z, \wp\left(z_{0}+u_{1} z\right), \wp\left(z_{0}+u_{2} z\right)\right)
$$

satisfies

$$
\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{4} v_{4}\right)=0
$$

for all integers $t, s_{1}, \ldots, s_{4}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{4} \leqq S_{0} .
$$

These coefficients are polynomials in $\vartheta$ with integer coefficients of logarithmic absolute values at most

$$
c_{1}\left(D_{0} \log D+T \log D+D_{1} S_{0}^{2}\right) \leqq c_{2} D^{2} \log D,
$$

but because the numbers $\wp\left(u_{1} v_{j}\right)(1 \leqq j \leqq 4)$ are algebraic by hypothesis, the degrees in $\vartheta$ are only at most

$$
c_{3}\left(D_{0}+T+D_{2} S_{0}^{2}\right) \leqq c_{4} D^{2}(\log D)^{3 / 8}
$$

The maximum modulus principle gives

$$
\log \left|\varphi^{(t)}\left(s_{1} v_{1}+\ldots+s_{4} v_{4}\right)\right|<-c_{5} T S_{0}^{4} \log D
$$

for all integers $t, s_{1}, \ldots, s_{4}$ with

$$
0 \leqq t<T, \quad 0 \leqq s_{1}, \ldots, s_{4} \leqq S .
$$

We use Proposition 3 to see that at least one of these values is non-zero. By Lemma 1 and our assumption $m_{2}=0$, it suffices to check the conditions

$$
\begin{array}{rrr}
T S^{4} \geqq c D_{0} D_{1} D_{2}, & T S^{2} \geqq c D_{0}, \\
D_{2} S^{4} \geqq c D_{0} D_{1}, & D_{2} S^{2} \geqq c D_{0} .
\end{array}
$$

So we end up with $\pi_{D} \neq 0$ in $\mathbb{Z}[\vartheta]$ satisfying

$$
\log \left|\pi_{D}\right|<-c_{6} T S_{0}^{4} \log D,
$$

and the coefficients of $\pi_{D}$ have logarithmic absolute values at most $c_{7} D^{2} \log D$, while its degree in $\vartheta$ is at most $c_{8} D^{2}(\log D)^{3 / 8}$. Since $T S_{0}^{4} \log D \geqq c_{9} D^{4}(\log D)^{3 / 2}$, the sharpened Gelfond criterion due to Brownawell [2] and Waldschmidt [16] yields the final contradiction. This proves Theorem 5 in the case $m_{2}=0$.

It remains to consider the case $m_{2}=1$. But then the remarks at the end of Sect. 2 show that $\delta(z)$ has no complex multiplication. Furthermore, we can without loss of generality assume that $u_{1} v_{4}=\omega_{1}, u_{2} v_{4}=\omega_{2}$ are periods of $\mathscr{L}$. Now Theorem 5 is a weak consequence of Lemma 2 applied to the ratios $\chi_{j}=v_{j} / v_{4}(1 \leqq j \leqq 3)$. This completes the proof of Theorem 5 in general.

Note added in proof. It has kindly been pointed out to us by R. Tubbs that the applications of the maximum modulus principle on pages $8 \mathbf{- 1 0}, 12,14$, and 15 may fail if the appropriate power of some

$$
\left(\sigma\left(z_{0}+u_{( }\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)\right)\right)^{2} \quad(1 \leqq i \leqq n)
$$

is too small. But in this case it is not too difficult to deduce that the same power of $\wp\left(z_{0}+u_{i}\left(s_{1} v_{1}+\ldots+s_{m} v_{m}\right)\right.$ is correspondingly large, and that a suitable denominator of this in $Q\left(\vartheta, \vartheta_{1}\right)$ will then yield the desired element $\pi_{D}$ for use in Gelfond's criterion.

## References

1. Brownawell, W.D.: The algebraic independence of certain values of the exponential function. K. norske Vidensk. Selsk. Skr. No. 23 (1972)
2. Brownawell, W.D.: The algebraic independence of certain numbers related by the exponential function. J. Number Theory 6, 22-31 (1974)
3. Brownawell, W.D., Kubota, K.K.: The algebraic independence of Weierstrass functions and some related numbers. Acta Arith. 33, 111-149 (1971)
4. Brownawell, W.D., Masser, D.W.: Multiplicity estimates for analytic functions I. J. reine angew. Math. 314, 200-216 (1980)
5. Chudnovsky, G.V.: Contributions to the theory of transcendental numbers. A.M.S. Surveys and Monographs, No. 19, 1984
6. Gelfond, A.O.: Transcendental and algebraic numbers. New York: Dover 1960
7. Masser, D.W., Wüstholz, G.: Algebraic independence properties of values of elliptic functions. Journées Arithmétiques 1980, London Math. Soc. Lecture Notes Vol. 56 (ed. J.V. Armitage), Cambridge 1982
8. Masser, D.W., Wüstholz, G.: Zero estimates on group varieties I. Invent. Math. 64, 489-516 (1981)
9. Masser, D.W., Wüstholz, G.: Zero estimates on group varieties II. Invent. Math. 80, 233-276 (1985)
10. Smelev, A.A.: On the method of A.O. Gelfond in the theory of transcendental numbers. Mat. Zametki 10, 415-426 (1971); Math. Notes 10, 672-678 (1971)
11. Smelev, A.A.: Algebraic independence of values of exponential and elliptic functions. Mat. Zametki 20, 195-202 (1976); Math. Notes 20, 669-673 (1976)
12. Smelev, A.A.: Algebraic independence of several numbers connected with exponential and elliptic functions. Ukr. Mat. Z. 33, 277-282 (1981); Ukr. Math. J. 33, 216-220 (1981)
13. Tijdeman, R.: On the number of zeroes of general exponential polynomials. Indagationes Math. 33, 1-7 (1971)
14. Tijdeman, R.: On the algebraic independence of certain numbers. Indagationes Math. 33, 146-162 (1971)
15. Waldschmidt, M.: Indépendance algébrique des valeurs de la fonction exponentielle. Bull. Soc. Math. Fr. 99, 285-304 (1971)
16. Waldschmidt, M.: Solution du huitième problème de Schneider. J. Number Theory 5, 191-202 (1973)
17. Wüstholz, G.: Algebraische Unabhängigkeit von Werten von Funktionen, die gewissen Differentialgleichungen genügen. J. reine angew. Math. 317, 102-119 (1980)
[^0]
[^0]:    Received January 22, 1985

