# 10 A Theorem of Mahler

The next result is due to Mahler and generalizes an earlier result (Theorem 14) we established.

**Theorem 28.** *Let*

$$f(z) = \sum_{j=0}^{\infty} z^{2^j}.$$

*If $\alpha$ is an algebraic number with $0 < |\alpha| < 1$, then $f(\alpha)$ is transcendental.*

*Proof.* Assume $f(\alpha)$ is algebraic. Let $K = \mathbb{Q}(\alpha, f(\alpha))$. Observe that every element of $K$ is a root of a polynomial with integer coefficients of degree $\le D$ where $D$ is the product of the degrees of the minimal polynomials of $\alpha$ and the minimal polynomial of $f(\alpha)$ (the specific value of $D$, however, is not important). Let $r$ be a positive integer to be specified later; we will want $r$ large compared to $D$. We show that there are polynomials $P_0(z), \dots, P_r(z)$ with degrees at most $r$ and with rational integer coefficients for which

$$E_r(z) = \sum_{j=0}^{r} P_j(z) f(z)^j = \sum_{j=0}^{\infty} B_j z^j$$

is not identically 0 but $B_j = 0$ for all $j \le r^2$. Observe that obtaining $B_j = 0$ for all $j \le r^2$ corresponds to solving $r^2+1$ homogeneous equations in $(r+1)^2$ unknowns, the unknowns being the coefficients of $P_0(z), \dots, P_r(z)$. A non-trivial solution to these $r^2+1$ homogeneous equations exists, and this solution will correspond to obtaining $P_j(x)$ with coefficients in $\mathbb{Q}$. We can multiply through by an appropriate positive integer to obtain solutions which are rational integers and, hence, $P_j(x)$ with rational integer coefficients. We recall from the proof of Theorem 14 that for any $s \ge 1$ and any $t \ge 1$, there are non-zero terms $z^m$ in $f(z)^s$ such that (i) the coefficient of $z^{m+j}$ in $f(z)^s$ is 0 for $0 < |j| \le t$ and (ii) for $0 \le u < s$, the coefficient of $z^{m+j}$ in $f(z)^u$ is 0 for $|j| \le t$. This easily implies that since $P_0(z), \dots, P_r(z)$ as constructed above are not all identically 0, $E_r(z)$ is not identically 0. This completes the argument for the existence of $P_0(z), \dots, P_r(z)$ with the desired properties indicated above.

Note that $f(z)$ converges for $|z| < 1$ and is, in fact, analytic in the disk $\{z : |z| < 1\}$. Hence, the same holds true of $E_r(z)$, and we can conclude that for all but finitely many $j \ge 0$, $|B_j| \le 2^j$. Therefore, if $B_j \ne 0$ and $j$ is sufficiently large (possibly depending on $r$ but not $k$), then $\log |B_j| \le j$. It follows that if $B_j \ne 0$ and $k$ is sufficiently large compared to $r$, then

$$\log \left| B_j \alpha^{2^k j} \right| \le -c_1 2^k j \tag{15}$$

for some constant $c_1$, where $c_1$ and other constants $c_j$ to follow are positive and independent of $r$ and $k$ but possibly depend on $\alpha$. Henceforth, we view $k$ as being large compared to $r$ so that, in particular, the above follows. There is an alternative way to bound $|B_j|$. From Lemma 1 for the proof of Theorem 14, we know that the coefficients of $f(z)^j$ are each non-negative and $\le j^{2j}$. Using our previous convention that if $g(z) = \sum_{j=0}^{r} b_j z^j$, then $|g|(z) = \sum_{j=0}^{r} |b_j| z^j$, we see that

$$|B_j| \le C(r) = r^{2r} \sum_{i=0}^{r} |P_i|(1).$$

Note that this bound on $|B_j|$ is independent of $\alpha$ and $k$, and (15) easily follows for $B_j \neq 0$.

Let $m = \min\{j : B_j \neq 0\}$. Then by the definition of $P_j(z)$, $m > r^2$. Also, since the coefficients of $P_j(z)$ are integers, we get that $B_m$ also satisfies $|B_m| \geq 1$. Thus, since $|\alpha| < 1$ and $k$ is large (depending on $\alpha$ and $r$)

$$\Big| \sum_{j=m+1}^{\infty} B_j \alpha^{2^k j} \Big| \leq r^{2r} \bigg( \sum_{i=0}^{r} |P_i|(1) \bigg) \sum_{j=m+1}^{\infty} |\alpha|^{2^k j}$$

$$\leq 2r^{2r} \bigg( \sum_{i=0}^{r} |P_i|(1) \bigg) |\alpha|^{2^k(m+1)} \leq (1/2)|\alpha|^{2^k m} \leq (1/2)\big|B_m \alpha^{2^k m}\big|.$$

This implies that

$$E_r\big(\alpha^{2^k}\big) \neq 0$$

since the term $B_m \alpha^{2^k m}$ in $E_r\big(\alpha^{2^k}\big)$ is greater in absolute value than the contribution of the remaining terms. Note that similar to the above, we obtain

$$\Big|E_r\big(\alpha^{2^k}\big)\Big| = \Big| \sum_{j=m}^{\infty} B_j \alpha^{2^k j} \Big| \leq r^{2r} \bigg( \sum_{i=0}^{r} |P_i|(1) \bigg) \sum_{j=m}^{\infty} |\alpha|^{2^k j} \leq 2r^{2r} \bigg( \sum_{i=0}^{r} |P_i|(1) \bigg) |\alpha|^{2^k m}.$$

Thus,

$$\log \Big|E_r\big(\alpha^{2^k}\big)\Big| \leq -c_2 2^k m < -c_2 2^k r^2. \tag{16}$$

Now, observe that for $|z| < 1$ and any positive integer $k$,

$$f\big(z^{2^k}\big) = f(z) - \sum_{i=0}^{k-1} z^{2^i}.$$

Therefore,

$$E_r\big(\alpha^{2^k}\big) = \sum_{j=0}^{r} P_j\big(\alpha^{2^k}\big) \bigg( f(\alpha) - \sum_{i=0}^{k-1} \alpha^{2^i} \bigg)^j. \tag{17}$$

Observe that the right-hand side is a polynomial in $\alpha$ and $f(\alpha)$ of degree $\leq 2^{k+1}r$ in $\alpha$ and of degree $\leq r$ in $f(\alpha)$ and which consists of coefficients which are algebraic integers in $K$.

For $\beta \in K$, we define $d = \text{den}(\beta)$ to be the least positive integer for which $d\beta$ is an algebraic integer, and we refer to $d$ as the denominator of $\beta$. If $\beta_1, \ldots, \beta_s$ denote the conjugates of $\beta$, we define (and this varies from a similar definition used previously in these notes)

$$||\beta|| = \max\{\max_{1 \leq j \leq s} |\beta_j|, \text{den}(\beta)\}.$$

We use the above information to bound $\log ||E_r\big(\alpha^{2^k}\big)||$. By our comments concerning the right-hand side of (17), we note that

$$\text{den}\Big(E_r\big(\alpha^{2^k}\big)\Big) \leq \text{den}(\alpha)^{2^{k+1}r} \times \text{den}(f(\alpha))^r.$$

Thus,

$$\log \text{den}\Big(E_r\big(\alpha^{2^k}\big)\Big) \le c_3 2^{k+1} r.$$

For any conjugate $\alpha'$ of $\alpha$ and any conjugate $\beta'$ of $f(\alpha)$, we have

$$\begin{aligned}\left|\sum_{j=0}^{r} P_j\big((\alpha')^{2^k}\big)\left(\beta' - \sum_{i=0}^{k-1}(\alpha')^{2^i}\right)^j\right| &\le \sum_{j=0}^{r} |P_j|\big(|\alpha'|^{2^k}\big)\left(|\beta'| + \sum_{i=0}^{k-1}|\alpha'|^{2^i}\right)^j \\ &\le c_4\Bigg(\sum_{j=0}^{r}|P_j|(1)\Bigg)(k+1)^r(|\alpha'|+1)^{2^{k+1}r}(|\beta'|+1)^r.\end{aligned}$$

It follows that each conjugate of $E_r\big(\alpha^{2^k}\big)$ is such that the logarithm of its absolute value is $\le c_5 2^{k+1} r$. We deduce that

$$\log \Big|\Big|E_r\big(\alpha^{2^k}\big)\Big|\Big| \le c_6 2^{k+1} r. \tag{18}$$

Suppose $\beta$ is any algebraic number with minimal polynomial of degree $s$ and with denominator $d$. Let $\beta_1, \dots, \beta_s$ denote the conjugates of $\beta$. Then $d\beta_j$ is an algebraic integer for each $j$ and $\prod_{j=1}^{s}(d\beta_j) \ge 1$. Hence,

$$(2s-1)\log||\beta|| + \log|\beta| \ge \sum_{j=1}^{s}\log d + \sum_{j=1}^{s}\log|\beta_j| \ge 0$$

which easily implies that

$$\log|\beta| \ge -2s\log||\beta||.$$

We consider $\beta = E_r\big(\alpha^{2^k}\big)$. We take $r > 4Dc_6/c_2$ (and $k$ sufficiently large compared to $r$). Then (16) and (18) imply that

$$\begin{aligned}\log\Big|E_r\big(\alpha^{2^k}\big)\Big| &< -c_2 2^k r^2 = c_6 2^{k+1} r\left(\frac{-c_2 r}{2c_6}\right) \\ &\le \frac{-c_2 r}{2c_6}\log\Big|\Big|E_r\big(\alpha^{2^k}\big)\Big|\Big| < -2D\log\Big|\Big|E_r\big(\alpha^{2^k}\big)\Big|\Big|.\end{aligned}$$

Since $E_r\big(\alpha^{2^k}\big)$ is in $K$ and, therefore, has minimal polynomial of degree $\le D$, we obtain a contradiction, completing the proof. $\square$