# The values of Mahler measures

John D. Dixon  Artūras Dubickas

September 28, 2004

**Abstract**

We investigate the set $\mathcal{M}^*$ of numbers which occur as Mahler measures of integer polynomials and the subset $\mathcal{M}$ of Mahler measures of algebraic numbers (that is, of irreducible integer polynomials). We prove that every number $\alpha$ of degree $d$ in $\mathcal{M}^*$ is the Mahler measure of a separable integer polynomial of degree at most $\sum_{1\le r\le d/2}\binom{d}{r}$ with all its roots lying in the Galois closure $F$ of $\mathbb{Q}(\alpha)$, and every unit in $\mathcal{M}$ is the Mahler measure of a unit in $F$ of degree at most $\binom{d}{\lfloor d/2\rfloor}$ over $\mathbb{Q}$. We use this to show that some numbers considered earlier by D.W. Boyd are not Mahler measures. We also investigate the set of numbers which occur as Mahler measures of both reciprocal and nonreciprocal algebraic numbers. In particular, we describe all cubic units in this set and show that the smallest Pisot number is not the measure of a reciprocal number.

**2000 Mathematics Subject Classification:** 11R06, 11R32, 12D10.
**Keywords:** Mahler measure, Galois extension, reciprocal numbers, Pisot numbers.

## 1 Introduction

Let $f(X)$ be a nonzero complex polynomial. We shall define the *large* roots of $f(X)$ to be those roots with absolute value strictly greater than 1. The *Mahler measure* $M(f)$ of $f(X)$ is defined to be the absolute value of the product of the leading coefficient of $f(X)$ and all large roots of $f(X)$. It is a multiplicative measure (namely, $M(fg) = M(f)M(g)$) and has many interesting properties (for example, Mahler [15] showed that $M(f)$ is a geometric mean of the values of $f$ over the unit circle).

We shall be interested in the case where $f(X) \in \mathbb{Z}[X]$. In this case, the complex roots of $f(X)$ come in complex conjugate pairs and so $M(f)$ is (up to a plus or minus sign) equal to the product of the leading coefficient and the large roots of $f(X)$. In particular, $\alpha := M(f)$ is algebraic over $\mathbb{Q}$ and lies in the splitting field $F$ of $f(X)$ in $\mathbb{C}$. Following [3] we shall call such an algebraic number a *Mahler measure*. An important class of Mahler measures are those which arise from polynomials $f(X)$ which are irreducible over $\mathbb{Z}[X]$. If $\beta$ is algebraic over $\mathbb{Q}$ then its minimal polynomial over $\mathbb{Z}$ is a polynomial $f(X)$ irreducible over $\mathbb{Z}[X]$ determined up to a factor of $\pm 1$. Without ambiguity we can set $M(\beta) := M(f)$. We denote the set of all Mahler measures of algebraic numbers by $\mathcal{M}$ and the set of all Mahler measures $M(f)$ (where $f$ ranges over possibly reducible polynomials) by $\mathcal{M}^*$. Clearly, $\mathcal{M} \subseteq \mathcal{M}^*$. By the multiplicative property of Mahler measures, $\mathcal{M}^*$ is a monoid under multiplication generated by $\mathcal{M}$. As we shall see below (Theorem 10), $\mathcal{M}$ is not a monoid and so $\mathcal{M} \neq \mathcal{M}^*$.

A natural question is to ask how we can determine whether a particular algebraic number is a Mahler measure. A number of necessary conditions are known (see, for example, [3], [4], [5], [9] and Lemma 2 below). The numbers of degree at most 3 lying in $\mathcal{M}^*$ are characterized completely by Theorem 9. Although a characterization of Mahler measures of higher degrees seems difficult, the next result (together with Lemma 2(x)) shows that, in principle, this problem can be solved for any specified $\alpha$.

**Theorem 1** *Suppose that $\alpha$ is an algebraic number of degree $d$, and $F$ is the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. If $\alpha \in \mathcal{M}^*$ then $\alpha = M(f)$ for some separable polynomial $f(X) \in \mathbb{Z}[X]$ of degree at most $\sum_{1 \leq r \leq d/2} \binom{d}{r}$ whose roots lie in $F$. Moreover, if $\alpha \in \mathcal{M}$ is a unit then $\alpha = M(\beta)$ for some unit $\beta \in F$ of degree at most $\binom{d}{\lfloor d/2 \rfloor}$.*

Theorem 1 follows from Lemma 2(vii), Theorem 4 and Corollary 8 below. The second part of the theorem can be written in a stronger form: if $\alpha \in \mathcal{M}$, and its norm $N(\alpha)$ is not divisible by a $d$th power of an integer $> 1$, then $\alpha = M(\beta)$ for some $\beta \in F$ of degree at most $\binom{d}{\lfloor d/2 \rfloor}$. (Indeed, in this case Lemma 2(vii) shows that the leading and the constant coefficients of the minimal polynomial for $\beta$ are relatively prime.) However, we have not determined whether $\alpha := 3(3 + \sqrt{5})/2$ belongs to $\mathcal{M}$ (see [9]), although $\alpha = M(3(X^2 - 3X + 1)) \in \mathcal{M}^*$.

An important subclass of Mahler measures consists of measures $M(\beta)$

arising from *reciprocal* algebraic numbers; that is, where the minimal polynomial $f(X)$ of $\beta$ is reciprocal (both $\beta$ and $\beta^{-1}$ are roots). In general, a polynomial $f(X)$ of degree $n$ is called reciprocal if $f(X) = \pm X^n f(X^{-1})$. It has long been known (especially in connection with D.H. Lehmer's question [13] on whether there is a nonempty interval $(1, 1+\delta)$ free of values of $\mathcal{M}^*$) that Mahler measures arising from reciprocal algebraic numbers are of importance. For example, C.J. Smyth [18] showed that $\beta$ is reciprocal whenever $M(\beta) < \theta_0 = 1.32471\ldots$. Here $\theta_0$ is a root of $X^3 - X - 1$ and is the smallest Pisot number (see [17]). We denote by $\mathcal{R}$ the set of all $M(\beta)$ where $\beta$ is a reciprocal algebraic number, and denote by $\mathcal{N}$ the set of all $M(\beta)$ where $\beta$ is not reciprocal. Clearly, $\mathcal{R} \cup \mathcal{N} = \mathcal{M}$. It is possible for a Mahler measure to lie in both sets, so $\mathcal{R} \cap \mathcal{N}$ is nonempty. For example, the number $\alpha := 5 + 2\sqrt{6}$ is the unique large root of the reciprocal polynomial $X^2 - 10X + 1$ and so $\alpha \in \mathcal{R}$. On the other hand $\beta := 2 + \sqrt{2} + \sqrt{3} + \sqrt{6}$ has minimal polynomial $X^4 + 8X^3 + 2X^2 - 8X + 1$ and $M(\beta) = \alpha$ so we also have $\alpha \in \mathcal{N}$.

In the next section we summarize some earlier results on Mahler measures. In Section 3 we prove Theorem 1 and also some more precise results. Section 4 includes applications and examples. In Section 5 we investigate properties of the set $\mathcal{R} \cap \mathcal{N}$ and conclude by giving a general construction of reciprocal units whose Mahler measures are nonreciprocal.

# 2 Some known results on Mahler measures

We summarize some basic properties of Mahler measures.

**Lemma 2** *(i) Every $\alpha \in \mathcal{M}^*$ is a Perron number; that is, $\alpha$ is a real positive algebraic number $> 1$ such that every algebraic conjugate $\alpha'$ of $\alpha$ over $\mathbb{Q}$ with $\alpha' \neq \alpha$ satisfies $\alpha > |\alpha'|$. Moreover, if $\alpha \in \mathcal{M}^*$, then $|\alpha'| > \alpha^{-1}$ unless $\alpha' = \pm\alpha^{-1}$. Conversely, if $\alpha$ is a Perron number, then there is a positive integer $n$ such that $n\alpha \in \mathcal{M}$.*

*(ii) Suppose that $f(X)$ and $g(X)$ are nonzero polynomials such that $g(X) = \pm X^k f(\pm X^l)$ for some integers $k, l$ with $l \neq 0$. Then $M(f) = M(g)$. In particular, the Mahler measures of a polynomial and of its reciprocal polynomial are equal.*

*(iii) If $f(X) \in \mathbb{Z}[X]$ has leading coefficient $a_n$ and roots $\xi_1, \ldots, \xi_n$ (not necessarily distinct), then $a_n \xi_{i_1} \cdots \xi_{i_k}$ is an algebraic integer for any subset $\{i_1, \ldots, i_k\}$ of $\{1, \ldots, n\}$. In particular, every Mahler measure is an algebraic*

*integer.*

*(iv) Suppose that $\alpha, \beta$ and $\gamma$ are Perron numbers and $\alpha = \beta\gamma$. Then $\beta, \gamma \in \mathbb{Q}(\alpha)$. In particular, this holds for Mahler measures by (i).*

*(v) Let $f(X)$ and $g(X)$ be polynomials in $\mathbb{Z}[X]$ with $f(X)$ irreducible. Suppose that $K$ is a finite Galois extension of $\mathbb{Q}$ which contains the splitting field of $f(X)g(X)$, and that $\alpha := M(fg) = M(f)M(g)$. Then each automorphism $x \in \mathrm{Gal}(K/\mathbb{Q}(\alpha))$ maps the set of large roots of $f(X)$ onto itself.*

*(vi) Suppose that $\beta$ is an algebraic number of degree $n$ whose minimal polynomial over $\mathbb{Q}$ has $s$ large roots. If $M(\beta)$ has degree $d$, then $n$ divides $sd$.*

*(vii) Let $\alpha = M(\beta)$ for some algebraic number $\beta$ with minimal polynomial $f(X) = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$ where $a_n \neq 0$. If $\alpha$ is algebraic of degree $d \geq 2$, then $N(\alpha) = (\pm a_n)^d N(\beta)^r = \pm a_n^{d-r} a_0^r$ for some integer $r$ with $0 < r < d$. In particular, $\alpha$ is a unit if and only if $\beta$ is a unit.*

*(viii) If $f(X) = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$ with $a_n$ nonzero, then $M(f) \geq \max(|a_n|, |a_0|)$. In particular, any nonunit in $\mathcal{M}^*$ is at least 2.*

*(ix) Given any bound $B > 1$ and degree $d$, there are only finitely many Mahler measures $\alpha$ of degree $d$ with $\alpha \leq B$.*

*(x) Suppose that $\alpha \in \mathcal{M}^*$. Then, for each integer $n \geq 0$, there are only finitely many $f(X) \in \mathbb{Z}[X]$ of degree $n$ such that $M(f) = \alpha$.*

**Proof.** (i) See [1], [14], [4], [8] and [9].

(ii) This is well known. Its proof follows from the representation of the Mahler measure of a polynomial as an integral over the unit circle (see [15]).

(iii) This is a classical result which dates back to Dedekind and Kronecker (see [11, Part 0], or [12, p. 91]).

(iv) (See [14, Section 5].) Consider any finite Galois extension $K$ of $\mathbb{Q}(\alpha)$ containing $\beta$ and $\gamma$. If $\beta$, say, did not lie in $\mathbb{Q}(\alpha)$, then there would be a $\mathbb{Q}(\alpha)$-automorphism of $K$ which maps $\beta$ and $\gamma$, respectively, onto $\beta'$ and $\gamma'$ with $\beta \neq \beta'$ and $\alpha = \beta'\gamma'$. Since $\beta$ and $\gamma$ are Perron numbers, this gives the contradiction: $\alpha = |\beta'|\,|\gamma'| < \beta\gamma = \alpha$.

(v) Enumerate the roots $\xi_1, \ldots, \xi_n$ of $f(X)$ so that $\xi_1, \ldots, \xi_k$ are the large roots. Then $M(f) = \pm a_n \xi_1 \cdots \xi_k$ where $a_n$ is the leading coefficient of $f(X)$. Let $\xi_i \mapsto \xi_{i'}$ denote the permutation of the roots of $f(X)$ induced by $x$. Since $x$ fixes $M(f)$ by (iv), therefore $\xi_1 \cdots \xi_k = \xi_{1'} \cdots \xi_{k'}$, and this can only occur when $\xi_{1'}, \ldots, \xi_{k'}$ are the large roots of $f(X)$.

(vi) and (vii) See [4] and [9].

(viii) The first statement follows at once from (ii) and the definition of $M(f)$. As a consequence, if $\alpha \in \mathcal{M}$ is not a unit, then $\alpha = M(\beta)$ where $\beta$ is not a unit by (vii), and hence $\alpha \geq 2$. Any nonunit $\alpha \in \mathcal{M}^*$ is a product of elements of $\mathcal{M}$ at least one of which is nonunit.

(ix) Parts (i) and (iii) show that if $\alpha$ is a Mahler measure of degree $d$ and $1 < \alpha \leq B$ then $\alpha$ is a root of a monic integer polynomial whose coefficients are majorized by those of $(X + B)^d$. In particular, for each $d$ and $B$, there are only finitely many such Mahler measures.

(x) Suppose that $\alpha = M(f)$ where $f(X)$ has degree $n$. Then (viii) shows that the leading coefficient $f(X)$ is bounded in absolute value by $\alpha$ and similarly this is true for each root. Thus the coefficients of $f(X)$ are majorized by those of $\alpha(X + \alpha)^n$. There are only a finite number of integer polynomials with this property. ■

# 3 Basal polynomials

If $\alpha = M(f)$ for some $f(X) \in \mathbb{Z}[X]$, then we say that $f(X)$ *realizes* the Mahler measure $\alpha$. In general, there will be infinitely many polynomials which realize $\alpha$. Lemma 2(ii) shows that, if $\alpha$ is realized by a polynomial of degree $n$, then $\alpha$ is also realized by a polynomial of degree $n$ such that each of its irreducible factors has at most half its roots large. We call $f(X) \in \mathbb{Z}[X]$ a *basal* polynomial (for $\alpha$) when it is a polynomial of least degree such that $\alpha = M(f)$ and at most half the roots of each irreducible factor of $f(X)$ are large. If $\alpha \in \mathcal{M}$, then $f(X)$ is a *basal irreducible* polynomial for $\alpha$ if it is of least degree among the irreducible polynomials which realize $\alpha$ and at most half of its roots are large. (We often omit "for $\alpha$", because if a polynomial is basal then it is basal for only one number $\alpha$.) Evidently, if $f(X)$ is basal, then all of its irreducible factors are also basal. Each Mahler measure is realized by at least one basal polynomial, but it can be realized by more than one; for example, $f(X)$ and $f(-X)$ have the same measure and, for each positive integer $m \geq 3$, $M(mX - m') = m$ for each integer $m'$ satisfying $1 \leq |m'| \leq m$. We shall see that basal polynomials satisfy some very specific conditions.

Throughout the rest of the paper we shall use the following notation. For any finite set $\Lambda$ we shall use $\overline{\Lambda}$ to denote the product of the elements in $\Lambda$. If $F$ is a Galois extension of $\mathbb{Q}$, and $G := \mathrm{Gal}(F/\mathbb{Q})$, then G acts as a permutation group on $F$. We shall use standard notations: $\gamma^x$ will denote the

image of $\gamma \in F$ under $x \in G$, $\Gamma^x := \{\gamma^x \mid \gamma \in \Gamma\}$ for any subset $\Gamma \subseteq F$, $\gamma^H$ is the orbit of $\gamma$ under a subgroup $H$ of $G$, and $H_\gamma := \{x \in H \mid \gamma^x = \gamma\}$ and $H_{\{\Gamma\}} := \{x \in H \mid \Gamma^x = \Gamma\}$ are stabilizers of a point and a set. The "orbit-stabilizer lemma" states that $\left|\gamma^H\right| = |G : G_\gamma|$. (For general properties about permutation groups see [22] or [6].)

**Lemma 3** *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $n$ with leading coefficient $a_n$ and constant coefficient $a_0$. Let $F$ be a finite Galois extension of $\mathbb{Q}$ which contains the set $\Omega := \{\xi_1, \ldots, \xi_n\}$ of roots of $f(X)$ and let $G$ be the Galois group $\mathrm{Gal}(F/\mathbb{Q})$. Suppose that $\Sigma := \{\Delta_1, \ldots, \Delta_m\}$ is a system of blocks for the action of $G$ on $\Omega$ with the properties:*

*(a) for some $t$, $\Delta_1 \cup \ldots \cup \Delta_t$ is the set of all large roots of $f(X)$;*

*(b) the size $m$ of the block system is minimal with respect to condition (a).*

*Put $\delta_i := \bar{\Delta}_i$ for each $i$, and $g(X) := a_n \prod_{i=1}^m (X - \delta_i)$.*

*Then $g(X) \in \mathbb{Z}[X]$ has degree $m$ with leading coefficient $a_n$ and constant coefficient $a_0$ and $M(g) = M(f)$. Moreover, $g(X)$ is not a product of two polynomials of degrees $\geq 1$.*

**Proof.** Property (a) shows that $|\delta_i| > 1$ if and only if $\Delta_i$ consists of large roots. Define an equivalence relation on $\Sigma$ by $\Delta_i \sim \Delta_j \Leftrightarrow \delta_i = \delta_j$. This relation is invariant under the action of $G$ and so taking unions of $\Delta_i$ with the same value of $\delta_i$ gives another system of blocks for $G$. From the observation made at the beginning of this proof, this new system of blocks satisfies condition (a). Hence condition (b) shows that the relation $\sim$ must be equality. Therefore all of the $\delta_i$ are distinct.

Since $G$ acts transitively on $\Sigma$, it also acts transitively on $\{\delta_1, \ldots, \delta_m\}$. Thus $g(X)$ is a polynomial of degree $m$ over $\mathbb{Q}$ and is not a product of two polynomials of degree $\geq 1$. Lemma 2(iii) shows that every coefficient of $g(X)$ is an algebraic integer, and so $g(X) \in \mathbb{Z}[X]$ with leading coefficient $a_n$. The constant coefficient of $g(X)$ is $a_n \prod_j \delta_j = a_n \prod_i \xi_i = a_0$. Finally, from the property noted at the beginning of this proof we have $M(g) = M(f)$. ∎

**Theorem 4** *Let $E \subseteq \mathbb{C}$ be a finite Galois extension of $\mathbb{Q}$. Let $f(X) \in \mathbb{Z}[X]$ with $M(f) \in E$.*

*(i) If $f(X)$ is a basal polynomial, then all the roots of $f(X)$ lie in $E$;*

*(ii) If $f(X)$ is basal irreducible polynomial and the leading and constant coefficients of $f(X)$ are relatively prime (in particular, if $f(X)$ is monic), then all roots of $f(X)$ lie in $E$.*

**Remark** The point in (ii) is that $f(X)$ has least degree as an irreducible polynomial which realizes the given Mahler measure. It is conceivable that some reducible polynomial of smaller degree may have the same Mahler measure.

**Proof.** By Lemma 2(iv) and the fact that the Mahler measure is a multiplicative function, it is enough in (i) to consider the case where $f(X)$ is irreducible. Thus suppose that $f(X)$ is irreducible, let $F$ be the splitting field of $f(X)$ over $E$, and let $\Omega := \{\xi_1, \ldots, \xi_n\}$ be the set of roots of $f(X)$. Put $G := \mathrm{Gal}(F/\mathbb{Q})$ and $H := \mathrm{Gal}(F/E)$. Then $H$ is normal in $G$ because $E$ is a normal extension of $\mathbb{Q}$. Because $H$ is normal in $G$, the set of $H$-orbits on $\Omega$ is a system of blocks for $G$ (see, for example, [6, Theorem 1.6A]). Now applying Lemma 3 to $f(X)$ we see that in both cases (i) and (ii) we must have $m = n$ since $f(X)$ is basal (in case (ii) the primality condition ensures that $g(X)$ has no nontrivial factor of degree 0 and so is irreducible). Thus the $H$-orbits on $\Omega$ must have length 1. This implies that $H$ is trivial, and so $F = E$ as required. ■

**Open Problem** Does the conclusion of Theorem 4(ii) remain true if we drop the assumption that the leading and constant coefficients are relatively prime?

In connection with this problem, the following example shows that some care must be taken. The irreducible polynomial $f(X) := 2X^2 + X + 4$ has two large (complex) roots, say $\xi_1$ and $\xi_2$, and $M(f) = 2\xi_1\xi_2 = 4$. The construction in Lemma 3 with $m = 1$ gives the polynomial $g(X) = 2(X - 2)$ which is not irreducible. Of course, in this case $f(X)$ is not a basal irreducible polynomial.

Theorem 4 appears in a slightly different form in a short unpublished note by David Cantor which he kindly sent to the first named author. The remaining material in the note by Cantor considers the kind of problem dealt with in the theorem below, but in a less precise form. We are indebted to David Cantor for permission to include this material.

**Theorem 5** *Suppose $\alpha$ is a nonrational Mahler measure with minimal polynomial $g(X) \in \mathbb{Z}[X]$. Let $F$ be the splitting field of $g(X)$, $\Sigma := \{\alpha = \alpha_1, \ldots, \alpha_d\}$ be the set of roots of $g(X)$ in $F$, and $G := \mathrm{Gal}(F/\mathbb{Q})$. Suppose that $f(X)$ is a nonconstant irreducible factor in $\mathbb{Z}[X]$ of a basal polynomial for $\alpha$, or that $f(X)$ is a basal irreducible polynomial for $\alpha$ with the leading*

*coefficient and constant coefficient relatively prime. Put* $n := \deg f$. *Then, for each large root* $\xi$ *of* $f(X)$, *there exists a subset* $\Gamma \subseteq \Sigma$ *such that*

*(i)* $G_\xi = G_{\{\Gamma\}}$;

*(ii)* $\left|G : G_{\{\Gamma\}}\right| = n$;

*(iii)* $f(X)$ *has exactly* $n\,|\Gamma|\,/d$ *large roots.*

**Proof.** By Theorem 4 $f(X)$ splits into linear factors over $F$. Let $\Omega$ be the set of roots of $f(X)$, and $\Delta \subseteq \Omega$ be the set of large roots. Note that $\Delta \neq \emptyset$ by the hypotheses on $f(X)$, and that $G_\alpha \leq G_{\{\Delta\}}$ by Lemma 2(v).

Next define $U := \{u \in G \mid \xi \in \Delta^u\}$ and $\Gamma := \{\alpha^u \mid u \in U\}$. Note that, if $v \in G$, then $\alpha^v \in \Gamma$ implies $\alpha^v = \alpha^u$ for some $u \in U$, and hence $v \in G_\alpha u \subseteq G_{\{\Delta\}} u \subseteq U$ by the definition of $U$. Hence, for all $u \in G$,

$$\xi \in \Delta^u \;\Leftrightarrow\; u \in U \;\Leftrightarrow\; \alpha^u \in \Gamma.$$

Put $H := G_{\{\Delta\}}, K := G_\xi$ and $L := G_{\{\Gamma\}}$. Then it is clear that $HU = U = UL$, and $L \geq K$ because $\Gamma^K = (\alpha^U)^K = \alpha^U = \Gamma$.

We claim that in fact $L = K$. Since $f(X)$ is irreducible over $\mathbb{Q}$, $G$ acts transitively on $\Omega$. Now $\Lambda := \xi^L$ is a block of imprimitivity for $G$ on $\Omega$. Indeed, if $x \in G$ and $\Lambda \cap \Lambda^x \neq \emptyset$, then $\xi^L \cap \xi^{Lx} \neq \emptyset$; hence $x \in LKL \subseteq L$, and so $\Lambda = \Lambda^x$. Thus $\Omega$ is a union of disjoint blocks of the form $\Lambda^x$ $(x \in G)$. Moreover, $\Delta$ is a union of complete blocks since $\Delta = \{\xi^{u^{-1}} \mid u \in U\}$ by the transitivity of $G$ on $\Omega$, and $U^{-1} = LU^{-1}$ is a union of right cosets of $L$ from above. We can therefore apply Lemma 3 and the hypotheses on $f(X)$ to conclude that the blocks must have size 1. Thus $\xi^L = \{\xi\}$ and so $L \leq G_\xi = K$. Since we already saw that $K \leq L$, we conclude that $K = L$ as required.

This proves (i). Now (ii) follows because $n = |G : G_\xi|$ by the transitivity of $G$ on $\Omega$. Finally, the definition of $U$ shows that $|\Delta|\,|G_\xi| = |U| = |\Gamma|\,|G_\alpha|$ and so $n\,|\Gamma| = |G : G_\xi|\,|\Gamma| = |G : G_\alpha|\,|\Delta| = d\,|\Delta|$ proving (iii). ■

We shall denote the subset $\Gamma \subseteq \Sigma$ defined in the proof of Theorem 5 by $\Gamma(f, \xi)$. We can be more explicit about the dependence of this set on the choice of the large root $\xi$. Note that by definition $\alpha \in \Gamma(f, \xi')$ for each large root $\xi'$ of $f(X)$.

**Corollary 6** *Under the hypotheses of Theorem 5 suppose that* $\xi'$ *is also a large root of* $f(X)$. *Then there exists* $x \in G$ *such that* $\xi^x = \xi'$ *and* $\Gamma(f, \xi') = \Gamma(f, \xi)^x$. *Conversely, for each* $x \in G$ *such that* $\alpha \in \Gamma(f, \xi)^x$, $\xi^x$ *is a large root of* $f(X)$ *and* $\Gamma(f, \xi)^x = \Gamma(f, \xi^x)$.

**Proof.** Put $\Gamma := \Gamma(f,\xi)$ and $\Gamma' := \Gamma(f,\xi')$. With the notation of the proof of the theorem, since $\xi' \in \Delta$, there exists $x \in U$ such that $\xi' = \xi^x$ because of the transitivity of $G$ on $\Omega$. Now $\xi' \in \Delta^u \Rightarrow ux^{-1} \in U \Rightarrow \alpha^u \in \Gamma^x$ and so $\Gamma^x = \Gamma'$. Conversely, given $x \in G$ such that $\alpha \in \Gamma^x$, we have $\alpha^{x^{-1}} \in \Gamma \Rightarrow x^{-1} \in U \Rightarrow \xi^x \in \Delta$, and so $\xi^x$ is a large root. Moreover, $x \in U$ by the definition of $U$, so $\Gamma^x = \Gamma(f,\xi^x)$ from what we have just proved. ■

**Theorem 7** *Suppose that the Mahler measure $\alpha$ has the minimal polynomial $g(X)$ of degree $d$ over $\mathbb{Q}$. Let $\Sigma$ be the set of roots of $g(X)$, $F$ be the splitting field of $g(X)$, and $G := \mathrm{Gal}(F/\mathbb{Q})$. Let $f(X) = f_1(X)\dots f_m(X)$ be a basal polynomial for $\alpha$ where each $f_i(X)$ is irreducible over $\mathbb{Z}[X]$, or $f(X) = f_1(X)$ is a basal irreducible polynomial with the leading and constant coefficients relatively prime. Let $\Delta_i$ be the set of large roots of $f_i(X)$, and let $\Gamma_i := \Gamma(f_i,\xi_i)$ for some $\xi_i \in \Delta_i$. Then $|\Gamma_i| \le d/2$ for each $i$, and $\Gamma_i$ and $\Gamma_j$ lie in different $G$-orbits whenever $i \ne j$.*

**Proof.** By Theorem 5(iii) we have $|\Gamma_i| = |\Delta_i|\, d/(\deg f_i) \le d/2$ since the irreducible factors of a basal polynomial have at most half their roots large. This proves the first statement. In proving the second statement we can simplify notation; it is enough to show that $\Gamma_1$ and $\Gamma_2$ are not in the same $G$-orbit.

Suppose on the contrary that $\Gamma_1 = \Gamma_2^x$ for some $x \in G$. Then as in Theorem 5 we have $\xi_1 \in \Delta_1^u \Rightarrow \alpha^u \in \Gamma_1 = \Gamma_2^x \Rightarrow \alpha^{ux^{-1}} \in \Gamma_2 \Rightarrow \xi_2^x \in \Delta_2^u$. In particular, taking $u = 1$ we see that $\xi_2^x$ is a large root of $f_2(X)$. Theorem 5(i) also shows that $G_{\xi_1} = G_{\{\Gamma_1\}} = x^{-1}G_{\{\Gamma_2\}}x = x^{-1}G_{\xi_2}x$ because $\Gamma_1 = \Gamma_2$. Let $T$ be a set of right coset representatives for $G_{\xi_1}$ $(= x^{-1}G_{\xi_2}x)$ in $G$, and put $\eta_t = \xi_1^t\xi_2^{xt}$ $(t \in T)$. Let $c$ be the leading coefficient of $f_1(X)f_2(X)$. Then

$$h(X) := c\prod_{t\in T}(X - \eta_t)$$

is $G$-invariant, and so its coefficients are in $\mathbb{Q}$. Lemma 2(iii) shows that the coefficients of $h(X)$ are algebraic integers; hence $h(X) \in \mathbb{Z}[X]$. Since $\xi_1^t \in \Delta_1 \Rightarrow \alpha^{t^{-1}} \in \Gamma_1 = \Gamma_2^x \Rightarrow \xi_2^{xt} \in \Delta_2$, $\eta_t$ is a large root of $h(X)$ if and only if $\xi_1^t$ and $\xi_2^{xt}$ are both large. Thus $\xi_1^t$ (respectively, $\xi_2^{xt}$) runs over $\Delta_1$ (respectively, $\Delta_2$) as $t$ runs over $T$. Hence $M(h) = c\overline{\Delta}_1\overline{\Delta}_2 = M(f_1f_2)$. Since $\deg h = \deg f_1 = \deg f_2$, this contradicts the minimality of the choice of $f(X)$. Thus we conclude that $\Gamma_1$ and $\Gamma_2$ lie in different $G$-orbits as claimed. This proves the theorem. ■

**Corollary 8** *Let $\alpha$ be an algebraic integer of degree $d$. If $\alpha \in \mathcal{M}^*$ then every basal polynomial for $\alpha$ has distinct roots and its degree is at most $\sum_{1\le r\le d/2} \binom{d}{r}$. If $\alpha \in \mathcal{M}$ then every basal irreducible polynomial for $\alpha$ in which the leading and constant coefficients are relatively prime has degree at most $\binom{d}{\lfloor d/2\rfloor}$.*

**Proof.** We use the notation of the theorem. Every basal polynomial $f(X)$ has distinct roots because the irreducible factors of $f(X)$ are distinct. Theorem 5(ii) and the orbit-stabilizer lemma show that the degree of $f_i(X)$ is equal to the size of the orbit of $\Gamma_i$ under $G$. Because these orbits are disjoint for distinct $f_i(X)$, the sum of the degrees of the $f_i(X)$ for which $|\Gamma_i| = r$ is at most the number of $r$-subsets of $\Sigma$, namely $\binom{d}{r}$. Since this binomial coefficient is largest when $r = \lfloor d/2\rfloor$, the bounds on the degrees for both cases now follow. ■

# 4 Applications of the main results

We shall use the following notation. A polynomial $f(X)$ is said to be of *type* $(n, m)$ if it has degree $n$ and exactly $m$ large roots. Under the hypotheses of Theorem 5, $G$ acts transitively on the set $\Omega$ of roots of $f(X)$ and $\xi^x = \xi^y$ for $x, y \in G$ if and only if $x$ and $y$ lie in the same right coset of $G_\xi$ in $G$. Similarly, $\Gamma^x = \Gamma^y$ if and only if $x$ and $y$ lie in the same right coset of $G_{\{\Gamma\}}$. Since $G_\xi = G_{\{\Gamma\}}$ by Theorem 5(i), we can unambiguously label the roots $\xi^x$ of $f(X)$ by the sets $\Gamma^x$ in the orbit of $\Gamma$. Then the action of $G$ on $\Omega$ is described simply by its action on the subsets in the $G$-orbit of $\Gamma$. It is a little simpler to enumerate the roots $\Sigma = \{\alpha = \alpha_1, \ldots, \alpha_d\}$ and to denote the root $\xi^x$ by $\xi_{i_1\ldots i_r}$ when $\Gamma^x = \{\alpha_{i_1}, \ldots, \alpha_{i_r}\}$ (the order of the indices is disregarded). Then the permutation $\left(\begin{smallmatrix} 1 & 2 & \ldots & d \\ 1' & 2' & \ldots & d' \end{smallmatrix}\right)$ which describes the action of an element $y$ ($\alpha_i^y = \alpha_{i'}$ for $i = 1, \ldots, d$), can be applied directly to the indices of the roots in $\Omega$. If $\Delta$ is the set of large roots of $f(X)$, then Corollary 6 shows that $\xi^x \in \Delta$ if and only if $\alpha_1 = \alpha \in \Gamma^x$, so the large roots of $f(X)$ are those with indices containing 1.

**Example 1** Under the hypotheses of Theorem 7, assume we are in the "generic" case where $G$ is isomorphic to the full symmetric group $S_d$ (according to a classical theorem of van der Waerden this happens for "almost all" $g(X)$). If we fix an enumeration $\alpha = \alpha_1, \ldots, \alpha_d$ of $\Sigma$, then we can use ordinary permutation notation to denote the elements of $G$; a permutation

$x \in S_d$ acts on $F$ by mapping $\alpha_i$ into $\alpha_{i^x}$. Since $S_d$ has a single orbit of length $\binom{d}{r}$ on the set of $r$-subsets of $\{1,\ldots,d\}$, Theorems 5 and 7 show that in this case each irreducible factor of a basal polynomial for $\alpha$ has degree $\binom{d}{r}$ for some $r \le d/2$, and exactly $\binom{d}{r}r/d = \binom{d-1}{r-1}$ large roots; thus it has type $(\binom{d}{r}, \binom{d-1}{r-1})$. In this case no two irreducible factors can have the same degree.

**Example 2** The table below give the types of potential irreducible factors of a basal polynomial for an algebraic integer $\alpha$ of degree $d \le 5$ where $G$ is the Galois group of the minimal polynomial for $\alpha$. Using the notation of Theorem 7 the degrees $n$ are classified according to the size $r$ of $\Gamma$. The entries under $r$ are the types $(n,m)$ of irreducible polynomial factors where $n$ runs over the sizes of the orbits of $G$ on $r$-sets, and $m := |\Delta|$ is given by Theorem 5(iii).

| $d$ | $G$ | $r=1$ | $r=2$ |
|---|---|---|---|
| 2 | $S_2$ | $(2,1)$ | |
| 3 | $S_3, A_3$ | $(3,1)$ | |
| 4 | $S_4, A_4$ | $(4,1)$ | $(6,3)$ |
| | $\langle(1234),(13)\rangle, \langle(1234)\rangle$ | $(4,1)$ | $(4,2),(2,1)$ |
| | $\langle(12)(34),(13)(24)\rangle$ | $(4,1)$ | $(2,1),(2,1),(2,1)$ |
| 5 | $S_5, A_5, \langle(12345),(2354)\rangle$ | $(5,1)$ | $(10,4)$ |
| | $\langle(12345),(25)(34)\rangle, \langle(12345)\rangle$ | $(5,1)$ | $(5,2),(5,2)$ |

For example, for $d=4$ there are (up to permutation isomorphism) five different transitive groups. The third of these is the dihedral group $\langle(1234),(13)\rangle$ generated by the permutations (1234) and (13). It has one orbit of length 4 on the set of 1-subsets, and two orbits of lengths 4 and 2, respectively, on the set of 2-subsets. In this case the potential irreducible factors of a basal polynomial are of types $(4,1)$, $(4,2)$ or $(2,1)$.

The following theorem enables us to determine whether a given algebraic integer of degree $d$ is a Mahler measure realizable by an irreducible polynomial of type $(d,1)$. In particular, it gives necessary and sufficient conditions for an algebraic integer of degree $\le 3$ to be in $\mathcal{M}^*$. Note that for an irreducible polynomial of type $(2,1)$ or $(3,1)$ the large root is necessarily a Pisot number since no irreducible polynomial of degree $>1$ can have a single root on the unit circle.

**Theorem 9** *Let $\alpha > 1$ be a real root of the irreducible monic polynomial $g(X) := X^d + a_{d-1}X^{d-1} + \ldots + a_0 \in \mathbb{Z}[X]$. Then $\alpha = M(f)$ for some irreducible polynomial $f(X) \in \mathbb{Z}[X]$ of type $(d, 1)$ if and only if for some integer $c > 0$ we have $c^i \mid a_{d-i-1}$ $(i = 1, \ldots, d-1)$, the integers*

$$c, a_{d-1}, a_{d-2}/c, \ldots, a_0/c^{d-1}$$

*have no common factor $> 1$, and $\alpha/c$ is the only large root of $g(cX)$.*

**Proof.** First suppose that such an integer $c$ exists. Then the divisibility conditions show that $f(X) := g(cX)/c^{d-1} \in \mathbb{Z}[X]$ is irreducible and has leading coefficient $c$. Now the condition on $g(cX)$ shows that $f(X)$ has a single large root and $M(f) = c(\alpha/c) = \alpha$.

Conversely, suppose that $\alpha = M(f)$ where $f(X) \in \mathbb{Z}[X]$ has leading coefficient $c$ and a single large root $\xi$. Then $\alpha = \pm c\xi$. Replacing $f(X)$ by $f(-X)$ if necessary, we may assume that $\xi = \alpha/c$. Hence $\alpha$ is a root of $f(X/c)c^{d-1}$. Since the latter is monic with integer coefficients and is irreducible by hypothesis, therefore $g(X) = f(X/c)c^{d-1}$. Thus $\xi$ is the unique large root of $g(cX)$ and the divisibility conditions on the coefficients of $g(X)$ are easily verified. ■

**Example 3** A Mahler measure $\alpha$ of degree 2 or 3 is not necessarily the only large root of its minimal polynomial. For example, the minimal polynomial for $\alpha := \sqrt{13} + 1$ is $X^2 - 2X - 12$ which has two large roots. However $3 \mid 12$ and $\alpha/3$ *is* the unique large root of the polynomial $3X^2 - 2X - 4$, so $M(3X^2 - 2X - 4) = \alpha$.

**Example 4** Consider the generic case of $d = 4$ (so $G \cong S_4$) with $r = 2$. If $f(X)$ is a basal irreducible polynomial of degree 6 then the roots of $f(X)$ can denoted by $\xi_{ij}$ $(1 \le i < j \le 4)$. If $f(X)$ has leading coefficient $c$, then $\alpha = \alpha_1 = \pm c\xi_{12}\xi_{13}\xi_{14}$ and so, by applying Galois mappings, $\alpha_2 = \pm c\xi_{12}\xi_{23}\xi_{24}, \alpha_3 = \pm c\xi_{13}\xi_{23}\xi_{34}$ and $\alpha_4 = \pm c\xi_{14}\xi_{24}\xi_{34}$.

**Example 5** Consider the irreducible polynomial $g(X) := X^6 - X^4 - X^3 - X^2 + 1$. It has a unique large root $\theta_1 := 1.40126\ldots$, so $M(g) = \theta_1$. Maple shows that the Galois group over $\mathbb{Q}$ of the splitting field for $g(X)$ is isomorphic to $\langle (135)(246), (14)(25), (15)(24) \rangle$. This group has one orbit (of length 6) on 1-subsets, two orbits (of lengths 3 and 12) on 2-subsets, and three orbits (of lengths 4, 4 and 12) on 3-subsets. The orbit-stabilizer lemma and Theorem

5(ii) show that every irreducible factor of a basal polynomial for $\theta_1$ must have degree 6, 3, 12 or 4. Since $M(g) = \theta_1$, a basal polynomial for $\theta_1$ has degree at most 6. Thus, if $g(X)$ is not basal, then Theorem 5(iii) shows there exists a basal polynomial for $\theta_1$ of type $(3, 1)$ since $3 \cdot 2/6 = 1$ or $(4, 2)$ since $4 \cdot 3/6 = 2$. The former is impossible because $\theta_1$ has degree 6 and hence cannot be the root of a cubic, so consider the second possibility. A simple search shows that $f(X) := X^4 - X + 1$ has two large roots (a pair of complex conjugates) and $M(f) = \theta_1$.

The last example may seem somewhat surprising at first, because it shows that a basal polynomial for a Salem number of degree 6 is of smaller degree 4. However, it is easy to see that if we start with any totally complex non-reciprocal quartic unit $\beta$ whose Galois group is isomorphic to $S_4$ (as it was in the previous example where $\beta^4 - \beta + 1 = 0$) we always obtain a Salem number $\alpha = M(\beta)$ of degree 6.

We conclude this section with a theorem which answers a question raised in [9].

**Theorem 10** $\mathcal{M} \neq \mathcal{M}^*$. *Indeed, if $\alpha > 1$ and $\beta > 1$ are two quadratic units such that $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$, then $\alpha\beta \in \mathcal{M}^* \setminus \mathcal{M}$.*

**Proof.** The algebraic conjugates of $\alpha$ and $\beta$ are $\pm 1/\alpha$ and $\pm 1/\beta$, respectively, for some choice of signs. Hence $\alpha = M(\alpha)$ and $\beta = M(\beta)$, and so $\alpha\beta \in \mathcal{M}^*$. On the other hand, the condition $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\beta) = \mathbb{Q}$ implies that $\mathbb{Q}(\alpha, \beta)$ is a Galois extension of $\mathbb{Q}$ whose Galois group is the Klein 4-group.

Now suppose that $\alpha\beta \in \mathcal{M}$ contrary to what is claimed. As a product of units, $\alpha\beta$ is also a unit and so by Theorem 4(ii) a basal irreducible polynomial $f(X)$ which realizes $\alpha\beta$ splits into linear factors in $\mathbb{Q}(\alpha, \beta)$. By the table in Example 2, $f(X)$ is of type $(4, 1)$ or $(2, 1)$. The latter case is impossible, because $\alpha\beta$ is of degree 4. The algebraic conjugates of $\alpha\beta$ are $\alpha\beta$, $\pm\alpha/\beta$, $\pm\beta/\alpha$ and $\pm 1/\alpha\beta$ for suitable choice of signs, and exactly two of these have absolute value $> 1$. Thus the type $(4, 1)$ is also impossible. We have a contradiction and conclude $\alpha\beta \notin \mathcal{M}$ as required. ■

# 5 Reciprocal and nonreciprocal measures

Our main interest in the present section is to investigate the set $\mathcal{R} \cap \mathcal{N}$ of Mahler measures which are realizable both by reciprocal irreducible polyno-

mials and also by nonreciprocal irreducible polynomials. We begin with a theorem which relates to the reciprocal case. Clearly an irreducible reciprocal polynomial of degree $> 1$ is of even degree.

**Theorem 11** *Suppose that $\alpha > 1$ is a Mahler measure which is algebraic of degree $d$ over $\mathbb{Q}$. Let $F$ be the splitting field of the minimal polynomial of $\alpha$ over $\mathbb{Q}$, and put $G := \mathrm{Gal}(F/\mathbb{Q})$.*

*(i) If there is a basal polynomial $f(X)$ for $\alpha$ which is reciprocal, then each irreducible factor $h(X)$ of $f(X)$ is reciprocal and $\deg h \neq 1$.*

*(ii) If there is a basal polynomial $f(X)$ for $\alpha$ which is reciprocal and $G \cong S_d$ (the generic case), then $d$ is even and $f(X)$ is an irreducible polynomial of type $(n, n/2)$ times a constant where $n = \binom{d}{d/2}$.*

*(iii) In the generic case, if a reciprocal polynomial $f(X)$ is a basal polynomial for $\alpha$ then $f(X)$ has no root of absolute value 1.*

**Proof.** (i) Let $h(X) \in \mathbb{Z}[X]$ be an irreducible nonreciprocal factor of $f(X)$. Then its reciprocal is another irreducible factor of $f(X)$. Since they both have the same Mahler measure by Lemma 2(ii), in a factorization of $f(X)$ we can replace the polynomial reciprocal to $h(X)$ by $h(X)$ to get another basal polynomial for $\alpha$. But this latter polynomial is divisible by $h(X)^2$ which is contrary to Corollary 8. Finally, if $h(X)$ had degree 1 then $h(X)$ has the form $\pm X \pm 1$ which has Mahler measure 1 contradicting the hypothesis that $f(X)$ is basal.

(ii) Let $h(X) \in \mathbb{Z}[X]$ be a nonconstant irreducible factor of $f(X)$ and let $\Omega$ denote the set of roots of $h(X)$. Theorem 4 shows that $\Omega \subset F$. By (i) $h(X)$ is reciprocal and has degree $> 1$. Thus $G$ acts transitively and the sets $\{\xi, \xi^{-1}\}$ ($\xi \in \Omega$) form a system of blocks. Thus, with the notation of Theorem 5 with $h(X)$ in place of $f(X)$, $G_{\{\Gamma\}}$ ($= G_\xi$) is not a maximal subgroup of $G$. However, it is well known (and easily proved) that when $G$ is the full symmetric group on a set $\Sigma$ of size $d$ then $G_{\{\Gamma\}}$ is maximal in $G$ for $\Gamma \subseteq \Sigma$ except when $|\Gamma| = 0$, $d/2$ or $d$ (much more is proved, for example, in [6, Section 5.2]). Thus we conclude that $|\Gamma| = d/2$ and that $h(X)$ has $(\deg h)\,|\Gamma|\,/d = (\deg h)/2$ large roots by Theorem 7.

Hence we have shown that $d$ is even, and exactly half of the roots of every irreducible factor of $f(X)$ are large. Since $G \cong S_d$, Example 1 then shows that every nonconstant irreducible factor of $f(X)$ is of type $\left(\binom{d}{r}, \binom{d-1}{r-1}\right)$ with $\binom{d}{r} = 2\binom{d-1}{r-1}$. The latter condition implies that $r = d/2$. The same example shows that there can only be one irreducible factor of this type, so the claim

follows.

(iii) By (ii) $f(X)$ is of type $(n, n/2)$. Thus half the roots are large, and the other half are reciprocals of these. ■

**Example 6** The polynomial $g(X) := X^5 - X^2 - 1$ is given as an example in [4]. It has one real root $\alpha := 1.19385\ldots$, two complex roots of absolute value $1.08646\ldots$ and two of absolute value $0.84238\ldots$. Thus if $\alpha$ is a Mahler measure then it must be realized by a reciprocal polynomial by the theorem of Smyth quoted in the Introduction. The conditions of Lemma 2(i) do not rule out the possibility that $\alpha$ is a Mahler measure, and that possibility was left open in [4]. However, using Maple we find that the Galois group of the splitting field $F$ of $g(x)$ is isomorphic to $S_5$. Since $d = 5$ is odd, Theorem 11 shows that $\alpha$ cannot have a reciprocal basal polynomial, and so $\alpha$ is not a Mahler measure. A similar argument shows that *in the generic case* no algebraic integer $\alpha$ of odd degree with $1 < \alpha < \theta_0 = 1.32471\ldots$ can be a Mahler measure.

We now look at properties of elements of $\mathcal{R} \cap \mathcal{N}$. We begin with a simple method of constructing elements of this set.

**Theorem 12** *Let $\alpha$ be a unit whose minimal polynomial is reciprocal with no root on the unit circle. Then for infinitely many integers $m > 0$ we have $M(\alpha)^m \in \mathcal{R} \cap \mathcal{N}$.*

**Proof.** Let $f(X)$ of degree $n$ be the minimal polynomial for $\alpha$ over $\mathbb{Q}$, $\Omega := \{\alpha = \alpha_1, \ldots, \alpha_n\}$ be the roots of $f(X)$, and let $K$ be the splitting field. Choose a monic polynomial $g(X) \in \mathbb{Z}[X]$ of degree $p$ with the following properties: (a) $p$ is an odd prime not dividing $[K : \mathbb{Q}]$; (b) $g(0) = 1$ but $g(X)$ is not reciprocal; (c) $g(X) \bmod 2$ is irreducible over the field $\mathbb{F}_2$ of two elements; (d) for some prime $q$, $g(X) \bmod q$ is a product of an irreducible quadratic and $p - 2$ distinct linear factors over $\mathbb{F}_q$. Conditions (b)-(d) are easily satisfied using the Chinese remainder theorem. Let $\Gamma := \{\gamma_1, \ldots, \gamma_p\}$ be the roots of $g(X)$, $L$ be its splitting field and $E$ be the splitting field of $f(X)g(X)$.

First note that a theorem of Frobenius (see, for example, [21, Section 61]) shows that (c) and (d) imply that the Galois group $H := \mathrm{Gal}(L/\mathbb{Q})$ acting on $\Gamma$ contains an element which acts as a $p$-cycle and another which acts as a 2-cycle. Since $p$ is prime this implies that $H$ is isomorphic to the symmetric group on $\Gamma$. In particular, $g(X)$ is irreducible and condition (b) implies that

its roots are units and nonreciprocal. Since $K \cap L$ is a intersection of Galois extensions, it is also Galois and not equal to $L$ by (a). The only normal subgroups of $S_p$ are $1, S_p$ and the alternating group $A_p$ of index 2. Thus by Galois theory we see that $[K \cap L : \mathbb{Q}] = 1$ or 2. We claim that $\gamma_i \gamma_j^{\varepsilon} \notin K \cap L$ when $\varepsilon = \pm 1$, except in the case where $i = j$ and $\varepsilon = -1$. Indeed $\gamma_i^2 \notin K \cap L$ because $\mathbb{Q}(\gamma_i)$ has degree $p$ over $\mathbb{Q}$. Also since $H$ acts 2-transitively on $\Gamma$, the elements of the form $\gamma_i \gamma_j^{\varepsilon}$ (with $1 \le i < j \le p$) with fixed $\varepsilon = \pm 1$ are conjugates. Clearly there are at least $p - 1$ distinct elements of this form (and three if $p = 3$), so $\gamma_i \gamma_j^{\varepsilon} \notin K \cap L$.

Now with a suitable choice of the prime $p$ above, we can choose infinitely many integers $N > 0$ satisfying the following conditions: the numbers $\alpha_i^{Np}$ $(i = 1, \ldots, n)$ are distinct and

$$|\alpha_i|^N > \max(|\gamma_1|^{-1}, \ldots, |\gamma_p|^{-1}, |\gamma_1|, \ldots, |\gamma_p|)$$

if and only if $\alpha_i$ is a large root. The first condition is satisfied if we avoid choosing $Np$ as a multiple of $d$ whenever $\alpha_i/\alpha_j$ is a primitive $d$th root of 1 for some $d > 0$. The second condition is satisfied by all sufficiently large $N$ because we are assuming that $f(X)$ has no root on the unit circle. Note that the first condition implies that $\alpha^{Np}$ is a reciprocal unit of degree $n$, and so $M(\alpha)^{Np} = M(\alpha^{Np}) \in \mathcal{R}$.

Now let $G := \mathrm{Gal}(E/\mathbb{Q})$ and assume that $N$ satisfies the two conditions above. Since the stabilizers $G_{\alpha_i}$ and $G_{\gamma_j}$ have index $n$ and $p$, respectively, in $G$, and $p$ and $n$ are relatively prime by (a), therefore $\left|G : G_{\alpha_i} \cap G_{\gamma_j}\right| = np$. Thus $G$ acts transitively on the set $\Omega \times \Gamma$ of $np$ pairs and hence on the set

$$\Delta := \left\{\alpha_i^N \gamma_j \,|\, i = 1, \ldots, n \text{ and } j = 1, \ldots, p\right\}$$

On the other hand, the latter set consists of $np$ distinct elements because $\alpha_i^N \gamma_j = \alpha_k^N \gamma_l$ implies that $\gamma_j \gamma_l^{-1} \in K \cap L$, and then $j = l$ and $i = k$ because the $\alpha_i^N$ are distinct. Put $\beta := \alpha_1^N \gamma_1$, and note that $\beta$ is also a unit. Moreover $\beta$ is not reciprocal since $\alpha_1^N \gamma_1 \alpha_i^N \gamma_j \neq 1$ because $\gamma_1 \gamma_j \notin K \cap L$ from above. Hence $M(\beta) \in \mathcal{N}$. Since $\alpha$ is a unit and $f(X)$ has no root on the unit circle, exactly half the roots of $f(X)$ are large. Thus by the choice of $N$ we have $M(\beta) = M(\alpha)^{Np} \left(\prod_{j=1}^{p} |\gamma_i|\right)^{n/2} = M(\alpha)^{Np}$. This shows that $M(\alpha)^{Np} \in \mathcal{N}$ and completes the proof. ■

In particular, how small can the elements of $\mathcal{R} \cap \mathcal{N}$ be? Since all Mahler measures are algebraic integers, the smallest rational element is an integer.

Clearly $1 \notin \mathcal{N}$. On the other hand, $\mathcal{R} \cap \mathcal{N}$ contains every integer $m \geq 2$ since

$$M(m) = M((m + m' + i\sqrt{(3m + m')(m - m')})/2m) = m$$

where $m' < m$ is a positive integer such that the polynomial $mx^2 - (m + m')x + m$ is irreducible.

In general, in trying to find lower bounds for $\mathcal{R} \cap \mathcal{N}$, Lemma 2(viii) shows that it is enough to consider the units. Every quadratic unit is a root of polynomial of the form $X^2 - mX \pm 1$ ($m \in \mathbb{Z}$). It is now easy to verify that $(3 + \sqrt{5})/2$ is the smallest quadratic element in $\mathcal{R} \cap \mathcal{N}$ (it is the Mahler measure of itself and of the nonreciprocal number $\omega(1 + \sqrt{5})/2$ where $\omega$ is a primitive cube root of 1). We now look at the cubic units in $\mathcal{R} \cap \mathcal{N}$. Theorem 9 shows that we can restrict ourselves to Pisot numbers.

**Theorem 13** *Let $\beta$ be a cubic Pisot unit. Then $\beta \in \mathcal{R}$ if and only if $\beta = |\alpha|^2 > 1$ where $\alpha$ is a totally complex reciprocal unit of degree 6 and $\mathbb{Q}(\alpha)$ is normal over $\mathbb{Q}$. Moreover, such $\beta$ is not totally real.*

**Proof.** Let $\beta = \beta_1, \beta_2$ and $\beta_3$ be the roots of the minimal polynomial $g(X)$ of $\beta$ over $\mathbb{Q}$. If $\beta = |\alpha|^2$ where $\alpha$ has the form described, then the minimal polynomial $h(X)$ of $\alpha$ has roots $\alpha, \bar{\alpha}, \alpha^{-1}, \bar{\alpha}^{-1}, \gamma$ and $\gamma^{-1}$ for some $\gamma$ with $\bar{\gamma} = \gamma^{-1}$. Then $|\gamma| = 1$ and the only large roots of $h(X)$ are $\alpha$ and $\bar{\alpha}$. Because $\beta$ is a unit, $\alpha$ is also a unit, so the leading coefficient of $h(X)$ is 1. This shows that $\beta = |\alpha|^2 = M(\alpha)$ and $\beta \in \mathcal{R}$ as required.

Conversely, suppose that $\beta \in \mathcal{R}$, so $\beta = M(\xi)$ for some reciprocal $\xi$. Because $\beta$ is a unit, $\xi$ is also a unit by Lemma 2(vii). Suppose that the minimal polynomial $f(X)$ of $\xi$ over $\mathbb{Q}$ has degree $n$, $\Omega := \{\xi = \xi_1, \ldots, \xi_n\}$ is the set of its roots, and $K$ is its splitting field over $\mathbb{Q}$. Let $\Delta$ be the set of large roots of $f(X)$. Since $\xi$ is a unit, $\beta = \varepsilon\bar{\Delta}$ for some $\varepsilon = \pm 1$, and we can assume $|\Delta| \leq n/2$ by Lemma 2(ii).

If $\Delta_1 = \Delta, \Delta_2$ and $\Delta_3$ are the images of $\Delta$ under $G := \mathrm{Gal}(K/\mathbb{Q})$, then $\beta_2 := \varepsilon\bar{\Delta}_2$ and $\beta_3 := \varepsilon\bar{\Delta}_2$ are the conjugates of $\beta$. Since $G$ acts transitively on $\Omega$, each root of $f(X)$ appears in the same number $l$ of the sets $\Delta_1, \Delta_2$ and $\Delta_3$. Thus $nl = 3\,|\Delta|$. Since $|\Delta| \leq n/2$, we conclude that $l = 1$ and so the three sets form a partition of $\Omega$. Thus $\{\Delta_1, \Delta_2, \Delta_3\}$ is a system of blocks of imprimitivity for $G$ acting on $\Omega$. Put $\Delta_i^{-1} := \{\eta^{-1} \,|\, \eta \in \Delta_i\}$. Then $\left\{\Delta_1^{-1}, \Delta_2^{-1}, \Delta_3^{-1}\right\}$ is also a system of blocks because $f(X)$ is reciprocal. The partition given by the nonempty sets among $\Delta_{ij} := \Delta_i \cap \Delta_j^{-1}$ $(i, j = 1, 2, 3)$

is therefore also a system of blocks. Clearly $\Delta_{11} = \emptyset$ and so $\Delta_{ii} = \emptyset$ for all $i$ by transitivity of $G$. On the other hand, since $\beta$ is a Pisot number, $\beta_2$ and $\beta_3$ have absolute values $< 1$, and so $\Delta_{12}$ and $\Delta_{13}$ are nonempty. Thus transitivity shows that $\Delta_{ij} \neq \emptyset$ for all $i \neq j$, and so the system has six blocks each of size $n/6$ and these are permuted transitively by $G$.

Put $\alpha_{ij} := \bar{\Delta}_{ij}$ for $i \neq j$, and note that $\alpha_{ij} = \alpha_{ji}^{-1}$. We first show that the $\alpha_{ij}$ are distinct. Indeed, if this was not true, then by the transitivity of $G$ we would have $\alpha_{12} = \alpha_{ij}$ for some $(i, j) \neq (1, 2)$. Since $\Delta_1$ is the set of large roots, the only possibility is $\alpha_{12} = \alpha_{13}$. But then transitivity of $G$ on $\{\Delta_1, \Delta_2, \Delta_3\}$ shows that $\alpha_{23} = \alpha_{21} = \alpha_{12}^{-1} = \alpha_{13}^{-1} = \alpha_{31} = \alpha_{32}$. This implies $\beta_2 = \beta_3$ which is a contradiction. Thus the $\alpha_{ij}$ are distinct and $h(X) := \prod_{i \neq j}(X - \alpha_{ij})$ is an irreducible polynomial of degree 6. Since the $\xi_i$ are units, the same is true for the $\alpha_{ij}$, and so $h(X) \in \mathbb{Z}[X]$. Now $h(X)$ is a reciprocal polynomial ($\alpha_{ij}^{-1} = \alpha_{ji}$) and $|\alpha_{ij}| \leq 1$ for $i \neq 1$, so $\beta = \varepsilon\alpha_{12}\alpha_{13} = M(\alpha)$ where $\alpha := \alpha_{12}$.

Now observe that both $\Delta_{23}$ and $\Delta_{32}$ are disjoint from $\Delta_1 \cup \Delta_1^{-1}$, and so those sets consist of roots of absolute value 1. Thus $\alpha_{23} = \alpha_{32}^{-1} = \bar{\alpha}_{32}$ is not real (because $\alpha_{23} \neq \alpha_{32}$) and has absolute value 1. We claim that $\alpha_{12}$ is not real. Indeed, otherwise $\alpha_{21}, \alpha_{13}$ and $\alpha_{31}$ are all real. But then $\beta_1$ and $\beta_2$ are not real, and so must be complex conjugate roots of $g(X)$. But this implies $\alpha_{21} = \alpha_{31}$ contrary to the fact that the $\alpha_{ij}$ are distinct. Thus $\alpha = \alpha_{12}$ is not real and its complex conjugate must be the other large root $\alpha_{13}$. This shows that $\beta = \alpha\bar{\alpha}$ and all the roots of $h(X)$ are nonreal, and so the first claim of the lemma is proved. We also see that $\beta_2$ and $\beta_3$ are complex conjugates and so $\beta$ is not totally real.

Finally we show that $\mathbb{Q}(\alpha)$ is normal over $\mathbb{Q}$. Indeed, for each $x \in \mathrm{Gal}(K/\mathbb{Q}(\alpha))$ we have $\Delta_{12}^x = \Delta_{12}$ (because the $\alpha_{ij}$ are distinct) and so $\Delta_1 \cap \Delta_1^x$ and $\Delta_2 \cap \Delta_2^x$ are nonempty. Thus $x$ must fix the two blocks $\Delta_1$ and $\Delta_2$ (and hence also $\Delta_3$). Hence $x$ fixes $\beta_1, \beta_2$ and $\beta_3$, and so by Galois theory $\mathbb{Q}(\alpha)$ contains the splitting field $L$ of $g(X)$. On the other hand, since $g(X)$ has a pair of complex roots, $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Therefore a comparison of degrees shows that $\mathbb{Q}(\alpha) = L$ and therefore $\mathbb{Q}(\alpha)$ is normal over $\mathbb{Q}$. This completes the proof. ■

**Corollary 14** *The smallest cubic number in $\mathcal{R}$ is the root $\alpha = 1.83928\ldots$ of $X^3 - X^2 - X - 1$.*

**Proof.** By Lemma 2(viii) it is enough to consider units and so the theorem on Pisot units applies. In [2, p. 1373] Boyd lists the irreducible reciprocal

polynomials of degree 6 with Mahler measure less than 2. A simple computation with Maple shows that $X^6+X^5+2X^4+3X^3+2X^2+X+1$ is the only polynomial on the list which has a Galois group of order 6, and its Mahler measure is $\alpha$. ■

In particular, Corollary 14 implies that $\theta_0 \notin \mathcal{R}$ and thus answers a question raised in [3]. From the comments preceding Theorem 13 we see that $1.83928\ldots$ is the smallest element of degree at most 3 in $\mathcal{R} \cap \mathcal{N}$. The root $\theta_1 = 1.40126\ldots$ of $X^6 - X^4 - X^3 - X^2 + 1$ which occurs in Example 5 is a Salem number and the smallest element of $\mathcal{R} \cap \mathcal{N}$ known to us.

**Open Lehmer-type Problem** Is $\theta_1$ the smallest element in $\mathcal{R} \cap \mathcal{N}$?

Smyth's result quoted in the Introduction shows that $\inf \mathcal{N} = \theta_0 = 1.32471\ldots$. The theorem below gives a slightly better lower bound for $\inf(\mathcal{R} \cap \mathcal{N})$.

**Theorem 15** $\inf(\mathcal{R} \cap \mathcal{N}) \geq \theta_2 = 1.32497\ldots$ *where $\theta_2$ is the largest real root of $4X^8 - 5X^6 - 2X^4 - 5X^2 + 4$. (Note that $\theta_2 \notin \mathcal{R} \cap \mathcal{N}$ because it is not a Mahler measure by Lemma 2(vii).)*

**Proof.** The proof uses results of Smyth [18], [19], and a result of one of the authors [7] combined with the corollary above. Smyth's proof of the lower bound for $M(\alpha)$, where $\alpha$ is not reciprocal, is based on considering the quotient of the minimal polynomial of $\alpha$ and of its reciprocal. Expanding this quotient as a formal power series in $X$ we get the expression $1 + b_k X^k + b_l X^l + \ldots$. Assume first that $l \geq 2k$. In his thesis [19] Smyth showed then that either $M(\alpha) = \theta_0$ or $M(\alpha) > \theta_0 + 0.00029 > 1.325$. On the other hand, if $l < 2k$, then Theorem 1 of [7] implies that $M(\alpha)$ is greater than the largest real root $\theta_2 = 1.32497\ldots$ of $4X^8 - 5X^6 - 2X^4 - 5X^2 + 4$. Hence the interval $(\theta_0, \theta_2)$ contains no nonreciprocal measures. Since $\theta_0$ is a cubic Pisot number, the corollary above shows that $\theta_0 \notin \mathcal{R}$. Since $\mathcal{N}$ contains no elements smaller than $\theta_0$, we have $\inf(\mathcal{R} \cap \mathcal{N}) \geq \theta_2$. ■

**Example 7** (Compare with [3, Theorem 2].) The set $\mathcal{R} \cap \mathcal{N}$ contains units of every even degree. Indeed, suppose that $\zeta$ is a Pisot number with norm $N(\zeta) = 1$ and degree $2r > 2$, and let $f(X) \in \mathbb{Z}[X]$ be its minimal polynomial. Let $\zeta_1 = \zeta, \zeta_2, \ldots, \zeta_{2r}$ be the roots of $f(X)$ and suppose that we are in the generic case (the Galois group of the splitting field of $f(X)$ acts as the full symmetric group on the set of roots). It is known that in this case the

multiplicative relations between the roots are all consequences of the trivial relation $\zeta_1\zeta_2\dots\zeta_{2r}=1$ (see, for example, [20]). Put $m:=\binom{2r-2}{r-1}$. Then $\zeta^m$ has $2r$ distinct conjugates $\zeta_i^m$ $(i=1,\dots,2r)$ and is not reciprocal, so $\zeta^m=M(\zeta^m)\in\mathcal{N}$. On the other hand, because $f(X)$ is generic, $\alpha:=\zeta_1\zeta_2\dots\zeta_r$ has $\binom{2r}{r}$ conjugates $\zeta_{i_1}\zeta_{i_2}\dots\zeta_{i_r}$ $(1\le i_1<i_2<\ldots<i_r\le 2r)$. These include $\zeta_{r+1}\zeta_{r+2}\dots\zeta_{2r}=\alpha^{-1}$, and so $\alpha$ is reciprocal. Moreover, one of these conjugate has absolute value $>1$ if and only if $i_1=1$, so $M(\alpha)=\zeta^m$ and hence $\zeta^m$ is also in $\mathcal{R}$ .

It is also observed in [10] that the product of half conjugates of the smallest known Salem number $\sigma=1.17628\dots$ is a nonreciprocal number of degree 16. This number has 8 conjugates on the circle $|z|=\sigma$ and eight on $|z|=1/\sigma$, so $\sigma^8\in\mathcal{R}\cap\mathcal{N}$.

Another example can be constructed as follows. Take a cubic Pisot unit $\zeta$ with a nonreal conjugate $\zeta_2$ (so the Galois group of the field generated by the conjugates of $\zeta$ has order 6). Then $\zeta/\zeta_2$ is reciprocal and so $\zeta^3=M(\zeta^3)=M(\zeta/\zeta_2)\in\mathcal{R}\cap\mathcal{N}$.

All this is related to the fact, first discovered by Boyd [3], [5], that numbers in $\mathcal{R}$ are not necessarily reciprocal. One way to prove this is to construct reciprocal $\alpha$ with $M(\alpha)$ of odd degree. This can be accomplished as follows.

**Theorem 16** *Let $d\ge 2$. There is a reciprocal unit of degree $d$ whose Mahler measure is of odd degree (and so nonreciprocal) if and only if $d$ is even but not a power of 2.*

**Proof.** It is shown in [3] that, if $\gamma$ is a real but not totally real unit of odd degree $r$ with dihedral Galois group $D_r$ and $\gamma_2$ is a conjugate of $\gamma$, then $\gamma/\gamma_2$ is reciprocal, and $M(\gamma/\gamma_2)$ is of odd degree. Assume that $d$ is even but not a power of 2. Write $d=2^m r$ with odd $r>1$. Choose $\gamma$ as above and put $\alpha:=(\gamma/\gamma_2)^{1/2^{m-1}}$. Then $\alpha$ is a reciprocal unit of degree $2^{m-1}2r=d$ with Mahler measure $M(\alpha)=M(\gamma/\gamma_2)$ of odd degree.

We now show that there is a nonreciprocal unit $\alpha$ with minimal polynomial $f(X)$ of degree $2^m$ such that $M(\alpha)$ is of odd degree $d$. Indeed, since $\alpha$ is reciprocal, $M(\alpha)$ is not rational (see [8]), so the set $\Delta$ of large roots of $f(X)$ has size $<2^m$. However Lemma 2(vii) shows that $2^m$ divides $|\Delta|\,d$. Since $d$ is odd this is a contradiction. ∎

In [5] Boyd gives a method of constructing units in $\mathcal{R}$ which are not reciprocal. We can describe a general method of producing such units. Let

$\gamma$ be an arbitrary unit of degree $r$ with minimal polynomial $f(X) \in \mathbb{Z}[X]$ and let $\gamma = \gamma_1, \ldots, \gamma_r$ be the roots of $f(X)$. For simplicity we assume that $f(X)$ is generic. As we noted earlier, in this case every multiplicative relation between the roots is a consequence of the trivial relation $\gamma_1 \ldots \gamma_r = \varepsilon$ where $\varepsilon = N(\gamma) = \pm 1$. Now set $\beta := \gamma_1^{k_1} \ldots \gamma_r^{k_r}$ where the integers $k_1, \ldots, k_r$ are chosen so that for some permutation $k_{1'}, \ldots, k_{r'}$ we have $\beta^{-1} = \gamma_1^{k_{1'}} \ldots \gamma_r^{k_{r'}}$. Because $f(X)$ is generic, this means that $\beta^{-1}$ is conjugate to $\beta$ and so $\beta$ is reciprocal. Now $\alpha := M(\beta)$ has the form $\pm\gamma_1^{s_1} \ldots \gamma_r^{s_r}$ for some integers $s_1, \ldots, s_r$ which can be calculated from the $k_i$ when we have sufficient information about the sizes of the roots $\gamma_i$. For "most" choices of $k_1, \cdots, k_r$, $\alpha$ is not reciprocal. In specific cases (see the examples below) we can prove that $\alpha$ is not reciprocal using the fact that the only relations between the roots are the trivial ones.

Two methods involving Pisot units with norm 1 considered by Boyd in [5] essentially correspond to the cases where $r$ is even, and either $k_1 = k_2 = \cdots = k_{r/2} = 2$, $k_{r/2+1} = \cdots = k_d = 0$, or $k_1 = 2$, $k_2 = \cdots = k_{r-1} = 1$, $k_r = 0$. (In the latter case, the fact that the Galois group is the dihedral group $D_r$ and not $S_r$ makes no difference.) For a Pisot unit $\gamma$, Boyd [5] noted that $\beta$ is of degree $\binom{r}{\lfloor r/2 \rfloor}$, and $\alpha = M(\beta)$ is a power of $\gamma$ and so of degree $r$. His second example also gives a nonreciprocal number $\alpha \in \mathcal{R}$ which has smaller degree than $\beta$. One may get an impression that this is always the case. However, using the general scheme above we can construct examples where $\beta$ is reciprocal, $\alpha = M(\beta)$ is not reciprocal, and the ratio $\deg \alpha / \deg \beta$ is arbitrarily large. We also construct an example where $\beta$ and $\alpha$ have the same degree.

**Example 8** Consider the polynomial $f(X) := X^r - X - 1$ where $r \geq 3$ is odd. It is readily verified that this polynomial has one real root $\gamma > 1$ and $(r-1)/2$ pairs of complex conjugate roots. We shall enumerate these roots $\gamma_1 = \gamma, \gamma_2, \ldots, \gamma_r$ in order of decreasing absolute values. It is known that Galois group of $f(X)$ is the full symmetric group $S_r$ (see [16, p. 42]) and so, as we have noted before, every multiplicative relation between the roots is a consequence of the trivial relation $\gamma_1\gamma_2 \cdots \gamma_r = 1$. In particular, not more than two roots can have the same absolute value (else we would obtain a relation between these roots). Hence $|\gamma_i/\gamma_j| > 1$ if and only if either: $i = 1$ and $j > 1$; or $i = 2l$ or $2l+1$ (for some $l \geq 1$) and $j > 2l+1$. We now take $\beta := \gamma_1/\gamma_2$. It is then easy to show that

$$\alpha := M(\beta) = \gamma_1^{2r-3}(\gamma_2\gamma_3)^{2r-6}(\gamma_4\gamma_5)^{2r-10} \ldots (\gamma_{r-3}\gamma_{r-2})^4$$

using the relation above. Since $S_r$ is 2-transitive, $\beta$ has $r(r-1)$ algebraic conjugates, one of which is $\beta^{-1}$. Thus $\beta$ is reciprocal of degree $r(r-1)$. Similarly, since the only relations between the $\gamma_i$ are trivial, $\alpha$ has degree $r!/2^{(r-1)/2}$ but is not reciprocal. Thus $\alpha \in \mathcal{R}$ but is not reciprocal, and $\deg \alpha / \deg \beta$ is unbounded as $r \to \infty$. (Similarly, taking a unit $\gamma$ with Galois group $S_r$ whose all conjugates except for two smallest in absolute value are real we will get a reciprocal $\beta = \gamma_1/\gamma_2$ of degree $r(r-1)$ and nonreciprocal $\alpha = M(\beta)$ of degree $r!/2$ instead of $r!/2^{(r-1)/2}$.)

**Example 9** In particular, consider $f(X) := X^5 - X - 1$. It has one real root $\gamma_1 = 1.16730\ldots$, a complex pair $\gamma_2 = \bar{\gamma}_3 = 0.18123\ldots + i1.08395\ldots$ outside the unit circle, and a complex pair $\gamma_4 = \bar{\gamma}_5 = -0.76488\ldots + i0.35247\ldots$ inside the unit circle. Put $\beta := \gamma_1^2\gamma_2^2\gamma_3$. Using the fact that $f(X)$ is generic, it is readily checked that $\beta$ has $\binom{5}{1}\binom{4}{2} = 30$ conjugates and that one of these is $\beta^{-1} = \gamma_3\gamma_4^2\gamma_5^2$. We can verify that that 13 of these conjugates have absolute value $> 1$ and that

$$\alpha := M(\beta) = \gamma_1^{21}(\gamma_2\gamma_3)^{15}(\gamma_4\gamma_5)^8 = \gamma_1^{13}(\gamma_2\gamma_3)^7$$

Now a similar argument shows that $\alpha$ also has 30 conjugates but is not conjugate to its inverse. Thus $\alpha \in \mathcal{R}$ but is not reciprocal, and $\deg \alpha = \deg \beta = 30$.

**Acknowledgements.** We thank David Cantor for permission to include some of his unpublished work (Theorem 4). We also thank David Boyd who has encouraged us and supplied some of the references, and Chris Smyth who provided information about relevant results from his thesis.

The first author was partially supported by NSERC Grant A7171.

The second author thanks the Max-Planck-Institut für Mathematik, Bonn, where his initial work on this paper was carried out during his research stay in Autumn 2002. His research was partially supported by the Lithuanian State Science and Studies Foundation.

# References

[1] R.L. Adler and B. Marcus, Topological entropy and equivalence of dynamical systems, *Mem. Amer. Math. Soc.* **20** (1979), no. 219.

[2] D.W. Boyd, Reciprocal polynomials having small measure, *Math. Comp.* **35** (1980), 1361–1377.

[3] D.W. Boyd, Inverse problems for Mahler's measure, in "Diophantine Analysis" (J. Loxton and A. van der Poorten, eds.), *London Math. Soc. Lecture Notes*, **109**, Cambridge Univ. Press, Cambridge 1986, 147–158.

[4] D.W. Boyd, Perron units which are not Mahler measures, *Ergod. Theory and Dynamical Sys.* **6** (1986), 485–488.

[5] D.W. Boyd, Reciprocal algebraic integers whose Mahler measures are non-reciprocal, *Canad. Math. Bull.* **30** (1987), 3–8.

[6] J.D. Dixon and B. Mortimer, Permutation Groups, Springer-Verlag, New York, 1996.

[7] A. Dubickas, Algebraic conjugates outside the unit circle, in "New Trends in Probability and Statistics" Vol. 4: Analytic and Probabilistic Methods in Number Theory (A. Laurinčikas et al. eds.), Palanga, 1996, TEV Vilnius, VSP Utrecht, 1997, 11–21.

[8] A. Dubickas, Mahler measures close to an integer, *Canad. Math. Bull.* **45** (2002), 196–203.

[9] A. Dubickas, On numbers which are Mahler measures, *Monatsh. Math.* (to appear).

[10] A. Dubickas and C.J. Smyth, On the Remak height, the Mahler measure, and conjugate sets of algebraic numbers lying on two circles, *Proc. Edinburgh Math. Soc.* **44** (2001) 1–17.

[11] H.M. Edwards, Divisor Theory, Birkhauser, Boston, Mass., 1990.

[12] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Akad. Verlag. M.B.H., Leipzig, 1923 (reprinted, Chelsea, New York, 1948).

[13] D.H. Lehmer, Factorization of certain cyclotomic functions, *Ann. of Math.* (2) **34** (1933), 461–479.

[14] D.A. Lind, The entropies of topological Mahler shifts and a related class of algebraic integers, *Ergod. Theory and Dynamical Sys.* **4** (1984), 283–300.

[15] K. Mahler, On some inequalities for polynomials in several variables, *J. London Math. Soc.* **37** (1962) 341–344.

[16] J.-P. Serre, Topics in Galois theory, Jones and Bartlett, Boston, Mass., 1992.

[17] C.L. Siegel, Algebraic integers whose conjugates lie in the unit circle, *Duke Math. J.* **11** (1944), 597–602.

[18] C.J. Smyth, On the product of conjugates outside the unit circle of an algebraic integer, *Bull. London Math. Soc.* **3** (1971), 169–175.

[19] C.J. Smyth, Topics in the theory of numbers, Ph. D. Thesis, University of Cambridge, 1972.

[20] C.J. Smyth, Additive and multiplicative relations connecting conjugate algebraic numbers, *J. Number Theory* **23** (1986), 243–254.

[21] B.L. van der Waerden, Modern Algebra, Frederick Ungar Publ., New York, 1948.

[22] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.

John D. Dixon
School of Mathematics and Statistics
Carleton University
Ottawa ON K1S 5B6
Canada
email: jdixon@math.carleton.ca

Artūras Dubickas
Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius 2600, Lithuania
email: arturas.dubickas@maf.vu.lt