Canad. J. Math. Vol. **61** (2), 2009 pp. 264–281

On $\mathbb{Z}$-Modules of Algebraic Integers

J. P. Bell and K. G. Hare

Abstract. Let q be an algebraic integer of degree $d \geq 2$. Consider the rank of the multiplicative subgroup of $\mathbb{C}^*$ generated by the conjugates of q. We say q is of *full rank* if either the rank is $d-1$ and q has norm ± 1, or the rank is d. In this paper we study some properties of $\mathbb{Z}[q]$ where q is an algebraic integer of full rank. The special cases of when q is a Pisot number and when q is a Pisot-cyclotomic number are also studied. There are four main results.

(1) If q is an algebraic integer of full rank and n is a fixed positive integer, then there are only finitely many m such that $\operatorname{disc}\left(\mathbb{Z}[q^m]\right) = \operatorname{disc}\left(\mathbb{Z}[q^n]\right)$.
(2) If q and r are algebraic integers of degree d of full rank and $\mathbb{Z}[q^n] = \mathbb{Z}[r^n]$ for infinitely many n, then either $q = \omega r'$ or $q = \operatorname{Norm}(r)^{2/d}\omega/r'$, where r' is some conjugate of r and ω is some root of unity.
(3) Let r be an algebraic integer of degree at most 3. Then there are at most 40 Pisot numbers q such that $\mathbb{Z}[q] = \mathbb{Z}[r]$.
(4) There are only finitely many Pisot-cyclotomic numbers of any fixed order.

1 Introduction

In this paper we study some properties of $\mathbb{Z}[q]$, where q is an algebraic integer of full rank. As well, we study the special cases of Pisot numbers and Pisot-cyclotomic numbers. We begin by recalling the definition of full rank.

Definition Let q be an algebraic integer of degree $d \geq 2$. Consider the rank of the multiplicative subgroup of $\mathbb{C}^*$ generated by the conjugates of q. We say q is of *full rank* if either the rank is $d-1$ and q has norm ± 1, or the rank is d.

It is worth observing that if the multiplicative subgroup of $\mathbb{C}^*$ generated by the conjugates of q has rank d, then q cannot have norm ± 1. As we later show, an important class of full rank algebraic integers is given by the collection of Pisot numbers.

Definition A *Pisot number* is a real algebraic integer greater than 1, all of whose conjugates are of modulus strictly less than 1.

Our first result is the following theorem.

Theorem 1.1 *For a given algebraic integer q of full rank and a fixed positive integer n, there are only finitely many m for which* $\operatorname{disc}\left(\mathbb{Z}[q^m]\right) = \operatorname{disc}\left(\mathbb{Z}[q^n]\right)$. *Hence there are only finitely many m such that $\mathbb{Z}[q^m] = \mathbb{Z}[q^n]$.*

Received by the editors July 17, 2006.
Research of K. G. Hare was supported in part by NSERC of Canada and the Seggie Brown Fellowship, University of Edinburgh.
AMS subject classification: Primary: 11R04; secondary: 11R06.
Keywords: algebraic integers, Pisot numbers, full rank, discriminant.

From this we obtain the following corollary.

Corollary 1.2 *Let q be an algebraic integer of full rank. Then the absolute value of the discriminant of q^n tends to infinity as $n \to \infty$.*

We next consider under which conditions on two algebraic integers q and r we can have $\mathbb{Z}[q^n] = \mathbb{Z}[r^n]$ for infinitely many n.

Theorem 1.3 *Let q and r be full rank algebraic integers of degree d. If $\mathbb{Z}[q^n] = \mathbb{Z}[r^n]$ for infinitely many n, then either $q = \omega r'$ for some conjugate r' of r and some root of unity ω, or $q = \mathrm{Norm}(r)^{2/d}\omega/r'$ for some conjugate r' of r and some root of unity ω.*

Relating this theorem to Pisot numbers gives the following result.

Corollary 1.4 *Let q and r be Pisot numbers. Suppose that $\mathbb{Z}[q^n] = \mathbb{Z}[r^n]$ for infinitely many n. Then $q = r$.*

For Pisot numbers q and r of small degree we can in fact obtain upper bounds on the number of n for which $\mathbb{Z}[q^n] = \mathbb{Z}[r^n]$.

Theorem 1.5 *Let r be an algebraic integer of degree at most 3. Then there are at most 40 Pisot numbers q such that $\mathbb{Z}[q] = \mathbb{Z}[r]$.*

It should be mentioned that in practice no example has been found of an algebraic integer r of degree 3 for which there are more than 7 Pisot numbers q satisfying $\mathbb{Z}[q] = \mathbb{Z}[r]$.

An important application of Theorem 1.5 is the determination of Pisot-cyclotomic numbers.

Definition A *Pisot-cyclotomic number* of order n is a Pisot number q such that $\mathbb{Z}[q] = \mathbb{Z}[\beta_n]$, where $\beta_n = 2\cos\left(\frac{2\pi}{n}\right)$.

Pisot-cyclotomic numbers have applications to the study of quasicrystals and quasilattices [3, 4]. Methods to find Pisot-cyclotomic numbers of higher orders require solutions to homogeneous Diophantine problems in several variables and are the obvious extension to Theorem 1.5. This is discussed further in [1].

The last result of this paper implies that there are only finitely many Pisot-cyclotomic numbers of order n for any fixed n. In fact, a stronger result is given.

Theorem 1.6 *Let r be a Pisot number with the property that all of its conjugates lie in the extension $\mathbb{Q}(r)$. Then there are only finitely many Pisot numbers q with the property that $\mathbb{Z}[q] = \mathbb{Z}[r]$.*

Corollary 1.7 *There are only finitely many Pisot-cyclotomic numbers of any fixed order.*

Theorem 1.1 is proved in Section 4. Theorem 1.3, along with some interesting results concerning unitary matrices, is shown in Section 5. Section 6 gives a proof of Theorem 1.5. Section 7 gives of proof of Theorem 1.6 using the Schmidt Subspace Theorem. Section 8 lists some possible future work and some open problems in this area.

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

2 Background on the Discriminant

Throughout this paper we use the discriminant of an algebraic integer in our considerations. Given an algebraic integer q with conjugates $q = q_0, q_1, \ldots, q_{d-1}$, we define the *discriminant* of q to be

$$\operatorname{disc}(q) := \prod_{0 \le i < j < d} (q_i - q_j)^2 = \left(\det\left(q_{i-1}^{j-1} \right)_{i,j=1}^{d} \right)^2.$$

The following theorem is a famous result which shows the utility of discriminants.

Theorem 2.1 *Let q and r be algebraic integers. If $\mathbb{Z}[q] = \mathbb{Z}[r]$, then $\operatorname{disc}(q) = \operatorname{disc}(r)$. Conversely, if q and r are algebraic integers of the same degree with $\operatorname{disc}(q) = \operatorname{disc}(r)$ and $\mathbb{Z}[q] \subset \mathbb{Z}[r]$, then $\mathbb{Z}[q] = \mathbb{Z}[r]$.*

Proof cf. Marcus [6, Theorem 11 and exercise 27 on page 45]. ∎

From the first part of the Theorem, we observe that we can define $\operatorname{disc}(\mathbb{Z}[q]) = \operatorname{disc}(q)$ where q is any algebraic integer that generates the ring.

3 Algebraic Integers of Full Rank

In this section we prove some important facts about algebraic integers of full rank.

Proposition 3.1 *Every Pisot number is of full rank.*

Proof Let q be a Pisot number and let $q = q_0, \ldots, q_{d-1}$ denote its conjugates. Let m denote the norm of q. Suppose that

$$q_0^{a_0} \cdots q_{d-1}^{a_{d-1}} = 1. \tag{3.1}$$

Let $j = \max\{-a_i \mid 0 \le i < d\}$. Then $j + a_i \ge 0$ for $0 \le i < d$ and there exists some k such that $j + a_k = 0$. Then multiplying both sides of equation (3.1) by $(q_0 \cdots q_{d-1})^j$ we get

$$q_0^{j+a_0} \cdots q_{d-1}^{j+a_{d-1}} = m^j. \tag{3.2}$$

Now since the Galois group of $\mathbb{Q}(q_0, \ldots, q_{d-1})/\mathbb{Q}$ acts transitively on the conjugates of q, there is an automorphism σ which sends q_k to $q = q_0$. Applying σ to both sides of equation (3.2), we see that there exist nonnegative integers $b_1, \ldots, b_{d-1}$ such that $q_1^{b_1} \cdots q_{d-1}^{b_{d-1}} = m^j$. Since q is a Pisot number, $|q_1|, \ldots, |q_{d-1}| < 1$. Since $|m| \ge 1$, we see that $b_1 = b_2 = \cdots = b_{d-1} = 0$ and $|m| = 1$. Thus if the norm of q is not ± 1, then the multiplicative group generated by the conjugates of q has rank d. If the norm is equal to ± 1, then the only relations in the multiplicative group are of the form $(q_0 \cdots q_{d-1})^j = 1$. Hence the multiplicative group has rank $d - 1$. Thus q has full rank. ∎

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

Proposition 3.2 *Let q be an algebraic integer of full rank having conjugates $q = q_0, q_1, \ldots, q_{d-1}$. Suppose for some integers $a_0, \ldots, a_{d-1}$ satisfying either*

- *at least one of the a_i is 0; or*
- *the a_i sum to 0,*

that $\prod_i q_i^{a_i}$ is a root of unity. Then all the a_i are 0.

Proof By replacing each a_i by ma_i for some appropriate m, we may assume that the root of unity is in fact 1. If the norm of q is not ± 1, then since the multiplicative group generated by $q = q_0, \ldots, q_{d-1}$ has rank d, we conclude that $a_0 = \cdots = a_{d-1} = 0$.

Thus we may assume that q has norm ± 1. Let G denote the multiplicative group generated by $q_0, \ldots, q_{d-1}$. Then we have a surjection $\mathbb{Z}^d \to G$. By assumption, the kernel of this map is a subgroup of rank 1. Since it is finitely generated and torsion free the kernel is isomorphic to $\mathbb{Z}$. Notice that $q_0^2 \cdots q_{d-1}^2 = 1$ and so by the above remarks if $q_0^{a_0} \cdots q_{d-1}^{a_{d-1}} = 1$, then $a_0 = a_1 = \cdots = a_{d-1}$. Thus if $a_i = 0$ for some i or $a_0 + \cdots + a_{d-1} = 0$, we must have that all the a_i are 0. ∎

It should be noted that Proposition 3.2 is true if we replace algebraic integers with algebraic numbers. This generality was not needed for this paper.

4 Proof of Theorem 1.1.

Throughout the rest of the paper, we take S_m to be the set of permutations of $\{0, 1, \ldots, m-1\}$.

An important result we use is the so-called Skolem–Mahler–Lech theorem. See, for example, Lech [5].

Theorem 4.1 **(Skolem–Mahler–Lech)** *Suppose that a rational function over a field of characteristic 0 whose series expansion $\sum_{i=0}^{\infty} c_i z^i$ has infinitely many $c_i = 0$. Then there exist integers a, b with $0 \leq b < a$ such that $c_{am+b} = 0$ for all m sufficiently large.*

Corollary 4.2 *Suppose that a rational function over a field of characteristic 0 whose series expansion $f(z) := \sum_{i=0}^{\infty} c_i z^i$ has infinitely many $c_i = C$ for some constant C. Then there exist integers a, b with $0 \leq b < a$ such that $c_{am+b} = C$ for all m sufficiently large.*

Proof Consider $g(z) = f(z) - \frac{C}{1-z}$. ∎

Lemma 4.3 *Let q be an algebraic integer with conjugates $q = q_0, \ldots, q_{d-1}$ and let A_n denote the $d \times d$ matrix whose (i, j) entry is $q_{i-1}^{(j-1)n}$. Then for $0 \leq b < a$, the power series $\sum_{n=1}^{\infty} \det(A_{an+b}) z^n$ is a rational function whose poles are of the form $\prod_{i=0}^{d-1} q_i^{-a\sigma(i)}$ with $\sigma \in S_d$.*

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

Proof Using the Vandermonde formula for $\det(A_n)$, we see

$$\begin{aligned} F(z) &:= \sum_{n=0}^{\infty} \det(A_{an+b}) z^n \\ &= \sum_{\sigma \in S_d} \sum_{n=0}^{\infty} \operatorname{sgn}(\sigma) (q_0^{\sigma(0)} \cdots q_{d-1}^{\sigma(d-1)})^{an+b} z^n \\ &= \sum_{\sigma \in S_d} \operatorname{sgn}(\sigma) (q_0^{\sigma(0)} \cdots q_{d-1}^{\sigma(d-1)})^{b} \sum_{n=0}^{\infty} (q_0^{\sigma(0)} \cdots q_{d-1}^{\sigma(d-1)})^{an} z^n \\ &= \sum_{\sigma \in S_d} \operatorname{sgn}(\sigma) (q_0^{\sigma(0)} \cdots q_{d-1}^{\sigma(d-1)})^{b} \left(\frac{1}{1 - q_0^{a\sigma(0)} \cdots q_{d-1}^{a\sigma(d-1)} z} \right). \end{aligned}$$

Hence $F(z)$ is a rational function whose poles are of the form $\prod_i q_i^{-a\sigma(i)}$ with $\sigma \in S_d$. ∎

Again, Lemma 4.3 is valid with algebraic integers replaced with algebraic numbers, but this generality was not needed for this paper.

Proof of Theorem 1.1 Let $q = q_0, q_1, \ldots, q_{d-1}$ denote the conjugates of q and let A_n denote the $d \times d$ matrix whose (i, j)-th entry is $q_{i-1}^{n(j-1)}$. We note that $q_i^n \neq q_j^n$ for distinct conjugates q_i and q_j of q since q has full rank. Hence

$$\det(A_n)^2 = \operatorname{disc}(\mathbb{Z}[q^n])$$

Suppose there is an infinite subset $\mathcal{S}$ of $\mathbb{N}$ such that $\operatorname{disc}(\mathbb{Z}[q^n])$ is constant for $n \in \mathcal{S}$. By Theorem 2.1, there is some constant C such that $\det(A_n) = C$ for infinitely many $n \in \mathcal{S}$. Let

$$F(z) := \sum_{n=0}^{\infty} \det(A_n) z^n.$$

Then by Lemma 4.3, $F(z)$ is a rational function. Now suppose that $\det(A_n)$ is equal to C for infinitely many n. By Theorem 4.1, there exist a, b such that $\det(A_{am+b}) = C$ for all m sufficiently large. Hence

$$G(z) := \sum_{m=0}^{\infty} \det(A_{am+b}) z^m = P(z) + C/(1 - z),$$

for some polynomial $P(z)$. By Lemma 4.3, $G(z)$ is a rational function whose poles are of the form $\prod_i q_i^{-a\sigma(i)}$ with $\sigma \in S_d$. Since $\sigma(i) = 0$ for some i and q has full rank, we see that none of the poles are roots of unity by Proposition 3.2. Consequently, for a given integer k there are at most finitely many n for which $\operatorname{disc}(\mathbb{Z}[q^n]) = k$. ∎

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

5 Proof of Theorem 1.3

Throughout this section q and r are algebraic integers of full rank, and degree d. We shall also use $q = q_0, \dots, q_{d-1}$ and $r = r_0, \dots, r_{d-1}$ to denote the conjugates of q and r respectively. For convenience, we take S_d to be the group of permutations of $\{0, 1 \dots, d-1\}$. We define

$$X(\sigma) = \prod_{j=0}^{d-1} q_j^{\sigma(j)} \qquad \text{and} \qquad Y(\sigma) = \prod_{j=0}^{d-1} r_j^{\sigma(j)}$$

and we define

$$v(\sigma) := (\sigma(0), \dots, \sigma(d-1)) \in \mathbb{Q}^{1\times d}.$$

Finally, we let $\mathcal{P}_d = \{v(\sigma) \mid \sigma \in S_d\}$.

Lemma 5.1 *The $\mathbb{Q}$-vector space spanned by $\mathcal{P}_d$ is $\mathbb{Q}^{1\times d}$; moreover, a basis is given by $\{v(\mathrm{id})\} \cup \{v((i, i+1)) \mid 0 \le i \le d-2\}$.*

Proof We claim that

$$\mathcal{S} = \{v((i, i+1)) - v(\mathrm{id}) \mid 0 \le i \le d-2\}$$

is linearly independent. To see this, suppose that

$$\sum_{i=0}^{d-2} c_i \big(v((i, i+1)) - v(\mathrm{id})\big) = (0, 0, \dots, 0).$$

Then for $0 \le j \le d-1$ we have

$$\sum_{i=0}^{d-2} c_i(\delta_{j,i} - \delta_{j,i+1}) = 0.$$

Taking $j = 0$, we see that $c_0 = 0$. We also have $c_j - c_{j-1} = 0$ for $1 \le j \le d-2$ and so $c_0 = \cdots = c_{d-2} = 0$. Thus $\mathcal{S}$ is linearly independent. Notice that the sum of the entries of each element of $\mathcal{S}$ is equal to 0 and hence $v(\mathrm{id})$ cannot possibly be in the span of $\mathcal{S}$. It follows that

$$\{v((i, i+1)) \mid 0 \le i \le d-2\} \cup \{v(\mathrm{id})\}$$

is a basis for $\mathbb{Q}^{1\times d}$. ∎

Lemma 5.2 *Suppose that for every $\sigma \in S_d$ there is some $\tau \in S_d$ such that $X(\sigma) = Y(\tau)$. Then there is a $d \times d$ matrix E with rational entries such that whenever $X(\sigma) = Y(\tau)$, we have $v(\tau) = v(\sigma)E$; moreover the row sums of E are all equal to* 1.

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

Proof Take a basis $\{\nu(\sigma_0), \ldots, \nu(\sigma_{d-1})\}$ for the $\mathbb{Q}$-vector space spanned by $\mathcal{P}_d$. Then we can find $\tau_0, \ldots, \tau_{d-1}$ such that $X(\sigma_i) = Y(\tau_i)$ for $0 \leq i < d$. Since $\{\nu(\sigma_i) \mid 0 \leq i < d\}$ is a basis, there is a unique matrix E such that $\nu(\tau_i) = \nu(\sigma_i)E$ for $0 \leq i < d$. Let $\sigma \in S_d$. Then there exist integers $a_0, \ldots, a_{d-1}$ and $b \neq 0$ such that

$$b\nu(\sigma) = a_0\nu(\sigma_0) + \cdots + a_{d-1}\nu(\sigma_{d-1}). \tag{5.1}$$

Right-multiplying both sides of equation (5.1) by the vector $(1, 1, \ldots, 1)^{\mathrm{T}}$, we see that

$$b\binom{d}{2} = (a_0 + \cdots + a_{d-1})\binom{d}{2}.$$

Right-multiplying both sides of equation (5.1) by E, we see

$$b\nu(\sigma)E = a_0\nu(\tau_0) + \cdots + a_{d-1}\nu(\tau_{d-1}).$$

Write $b\nu(\sigma)E = (c_0, \ldots, c_{d-1})$. Then

$$c_0 + \cdots + c_{d-1} = (a_0 + \cdots + a_{d-1})\binom{d}{2} = b\binom{d}{2}.$$

Now

$$\prod_{i=0}^{d-1} r_i^{c_i} = \prod_{i=0}^{d-1} Y(\tau_i)^{a_i} = \prod_{i=0}^{d-1} X(\sigma_i)^{a_i} = X(\sigma)^b.$$

By assumption there is some τ such that $X(\sigma) = Y(\tau)$, and so

$$\prod_{i=0}^{d-1} r_i^{c_i} = \prod_{i=0}^{d-1} r_i^{b\tau(i)}.$$

Equivalently,

$$\prod_{i=0}^{d-1} r_i^{c_i - b\tau(i)} = 1.$$

Notice that

$$\sum_{i=0}^{d-1} \Big(c_i - b\tau(i)\Big) = \sum_{i=0}^{d-1} c_i - b\binom{d}{2} = 0.$$

Thus, $c_i = b\tau(i)$ for all i by Proposition 3.2, and so we see that $\nu(\tau) = \nu(\sigma)E$ for each $\sigma \in S_d$.

To show that the row sums of E are all equal to 1, we use our basis of row vectors. Using the fact that $\nu(\tau) = \nu(\sigma)E$, we see

$$\begin{bmatrix} \nu(\sigma_0) \\ \vdots \\ \nu(\sigma_{d-1}) \end{bmatrix} \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} c\nu(\tau_0) \\ \vdots \\ \nu(\tau_{d-1}) \end{bmatrix} E \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}$$

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

Furthermore, we have

$$\begin{bmatrix} v(\sigma_0) \\ \vdots \\ v(\sigma_{d-1}) \end{bmatrix} \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} v(\tau_0) \\ \vdots \\ v(\tau_{d-1}) \end{bmatrix} \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} = \binom{d}{2} \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}.$$

From this we get

$$\begin{bmatrix} v(\tau_0) \\ \vdots \\ v(\tau_{d-1}) \end{bmatrix} \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} v(\tau_0) \\ \vdots \\ v(\tau_{d-1}) \end{bmatrix} E \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}$$

Since q and r are of full rank, we see that $\{v(\tau_i) \mid 0 \leq i \leq d-1\}$ is a basis for $\mathbb{Q}^{d\times 1}$. Hence the matrix whose i-th row is $v(\tau_i)$ is invertible and so we see

$$\begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix} = E \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{bmatrix}$$

from which the result follows. ■

We are now almost ready to prove our key structure result for matrices which send $\mathcal{P}_n$ to itself. We need a few simple lemmas before we can continue.

Lemma 5.3 *Let d be a positive integer and let $\sigma \in S_d$. Then $\langle v(\mathrm{id}), v(\sigma)\rangle = \langle v(\mathrm{id}), v(\mathrm{id})\rangle - 1$ if and only if $\sigma = (i, i+1)$ for some i with $0 \leq i \leq d-2$.*

Proof When $\sigma = (i, i+1)$, it is easy to verify that $\langle v(\mathrm{id}), v(\sigma)\rangle = \langle v(\mathrm{id}), v(\mathrm{id})\rangle - 1$. We prove the other direction by induction. The claim is clearly true when $d = 1$. Suppose that the claim is true when $d = m$ and consider the case $d = m+1$. If $\sigma(m) = m$, then by the inductive hypothesis we have $\sigma = (i, i+1)$ for some $i < m-1$. Thus we may assume that $\sigma(m) = j < m$. Also, there is some $k < m$ with $\sigma(k) = m$. Let $S = 1^2 + \cdots + m^2$. Then

$$\begin{aligned} S - 1 &= \langle v(\mathrm{id}), v(\sigma)\rangle \\ &= \langle (0, 1, \ldots, m), (\sigma(0), \ldots, \sigma(m))\rangle \\ &= km + mj + \sum\nolimits_{i\neq k,m} i\sigma(i) \\ &\leq km + mj + \sum\nolimits_{i\neq k,m} \frac{i^2 + \sigma(i)^2}{2} \\ &= km + mj - k^2/2 - j^2/2 - m^2 + S \\ &= -(m-k)^2/2 - (m-j)^2/2 + S. \end{aligned}$$

Hence $(m-k)^2 + (m-j)^2 \leq 2$. Since $j, k < m$ are integers we must have equality and $k = j = m-1$. Thus $\sigma(m) = m-1$ and $\sigma(m-1) = m$. Thus σ restricted to

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

$\{0, 1, \ldots, m-2\}$ is a permutation of this set. Using the Cauchy–Schwarz inequality we see

$$\begin{aligned}\langle \nu(\mathrm{id}), \nu(\sigma)\rangle &= \langle (0, 1, \ldots, m-2), (\sigma(0), \ldots, \sigma(m-2))\rangle + 2(m-1)m \\ &\leq \left(0^2 + 1^2 + \cdots + (m-2)^2\right) + 2(m-1)m = S - 1.\end{aligned}$$

By assumption, $\langle \nu(\mathrm{id}), \nu(\sigma)\rangle = S-1$ and so we must have an equality in the Cauchy–Schwarz inequality. Hence $\sigma(i) = i$ for $i < m-1$ and σ is just the transposition $(m-1, m)$. This proves the lemma. ∎

Lemma 5.4 *Let E be an orthogonal $d \times d$ matrix with the property that $\mathcal{P}_d E = \mathcal{P}_d$ and $\nu(\mathrm{id})E = \nu(\mathrm{id})$. Then either E is the identity matrix, or $E = \frac{2}{d}J - U$, where U is the permutation matrix whose (i, j) entry is $\delta_{i+j,d+1}$ and J is the matrix of all 1's.*

Proof First observe that if $E = \frac{2}{d}J - U$ then

$$EE^{\mathrm{T}} = \left(\frac{2}{d}J - U\right)\left(\frac{2}{d}J - U^{-1}\right) = \frac{4}{d^2}J^2 - \frac{2}{d}JU^{-1} - \frac{2}{d}UJ + I = I,$$

and so E is unitary. Furthermore,

$$\begin{aligned}\nu(\sigma)E &= \frac{2}{d}\nu(\sigma)J - \nu(\sigma)U \\ &= (d-1, d-1, \ldots, d-1) - (\sigma(d-1), \ldots, \sigma(0)) \\ &= (d-1-\sigma(d-1), d-1-\sigma(d-2), \ldots, d-1-\sigma(0)) \\ &= \nu(\tau)\end{aligned} \tag{5.2}$$

for some permutation τ. Thus $E = \frac{2}{d}J - U$ satisfies the conditions of the lemma.

We now look at which matrices satisfy the conditions of the statement of the lemma.

$$\begin{aligned}\langle \nu(\mathrm{id}), \nu(\mathrm{id})\rangle - 1 &= \langle \nu(\mathrm{id}), \nu((i, i+1))\rangle = \langle \nu(\mathrm{id})E, \nu((i, i+1))E\rangle \\ &= \langle \nu(\mathrm{id}), \nu((i, i+1))E\rangle.\end{aligned}$$

Thus, $\nu((i, i+1))E = \nu((j, j+1))$ for some j by Lemma 5.3. Let τ be a permutation of $\{0, 1, \ldots, d-2\}$ such that $\nu((i, i+1))E = \nu((\tau(i), \tau(i)+1))$.

Let e_i denote the row vector which has a 1 in the i-th position and zeros everywhere else. Then $\nu((i, i+1)) - \nu(\mathrm{id}) = e_{i+1} - e_{i+2}$. Consequently,

$$\langle \nu((i, i+1)) - \nu(\mathrm{id}), \nu((j, j+1)) - \nu(\mathrm{id})\rangle = 0 \quad \text{if and only if} \quad |i-j| \geq 2.$$

Since E is unitary and $\nu(\mathrm{id})E = \nu(\mathrm{id})$, we see that

$$\begin{aligned}&\langle \nu((i, i+1)) - \nu(\mathrm{id}), \nu((j, j+1)) - \nu(\mathrm{id})\rangle \\ &\quad = \langle \nu((i, i+1))E - \nu(\mathrm{id})E, \nu((j, j+1))E - \nu(\mathrm{id})E\rangle \\ &\quad = \langle \nu(\tau(i), \tau(i)+1) - \nu(\mathrm{id}), \nu(\tau(j), \tau(j)+1) - \nu(\mathrm{id})\rangle.\end{aligned}$$

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

It is then clear that $|\tau(i)-\tau(j)| \geq 2$ if and only if $|i-j| \geq 2$. Hence $|\tau(i)-\tau(j)| \leq 1$ if and only if $|i-j| \leq 1$. Moreover, since τ is a permutation, if $i \neq j$, then $\tau(i) \neq \tau(j)$, and so $|i-j| = 1$ if and only if $|\tau(i)-\tau(j)| = 1$ for $0 \leq i, j \leq d-2$.

Notice that 0 and $d-2$ are the only values of $i \leq d-2$ such that there is exactly one j between 0 and $d-2$ with $|i-j| = 1$. Thus $\tau(0) \in \{0, d-2\}$. There are now two cases. Suppose that $\tau(0) = 0$ and that $\tau(i) \neq i$ for some i. Pick $i_0 > 0$ minimal with $\tau(i_0) \neq i_0$. Then

$$1 = |\tau(i_0) - \tau(i_0-1)| = |\tau(i_0) - (i_0-1)|.$$

Hence $\tau(i_0) \in \{i_0-2, i_0\}$. If $i_0 - 2 \geq 1$, then $\tau(i_0-2) = i_0-2$ and so $\tau(i_0) = i_0$; if $i_0 - 2 < 1$, then $\tau(i_0)$ cannot equal i_0-2 and hence must be i_0, a contradiction. It follows that if $\tau(0) = 0$ then τ is the identity. A similar argument shows that if $\tau(0) = d-2$, then $\tau(i) = d-2-i$ for $0 \leq i \leq d-2$.

If τ is the identity, then $\nu((i,i+1))E = \nu((i,i+1))$ for all applicable i and $\nu(\mathrm{id})E = \nu(\mathrm{id})$ and hence by Lemma 5.1, E is the identity matrix, and so the claim is true in this case.

If τ is not the identity, then $\nu((i,i+1))E = \nu((d-i-2, d-i-1))$ for all applicable i and $\nu(\mathrm{id})E = \nu(\mathrm{id})$. Above, we saw that $X = \frac{2}{d}J - U$ satisfies:

- $\mathcal{P}_d X = \mathcal{P}_d$;
- X is orthogonal; and
- $\nu((i,i+1))X = \nu(d-i-2, d-i-1))$ for all applicable i and $\nu(\mathrm{id})X = \nu(\mathrm{id})$.

Thus we see that in this case $E = \frac{2}{d}J - U$. The result follows. ∎

Proposition 5.5 *Let $G = \{Y \in \mathrm{GL}_d(\mathbb{C}) \mid \mathcal{P}_d Y = \mathcal{P}_d\}$. Then $G \cong \mathbb{Z}/2\mathbb{Z} \times S_d$, where S_d corresponds to the group of permutation matrices and $\mathbb{Z}/2\mathbb{Z}$ corresponds to the group $\{\mathbf{I}_d, \frac{2}{d}J - \mathbf{I}_d\}$, where J is the matrix of all 1's.*

Proof Clearly G is a finite group and the set of permutation matrices is a subgroup of G. Since G is a finite linear group, there is an invertible matrix M such that MYM^{-1} is unitary for all $Y \in G$. In particular MPM^{-1} is unitary for all permutation matrices P. Hence if P is a permutation matrix,

$$\mathbf{I}_d = (MPM^{-1})(MPM^{-1})^* = (MPM^{-1})((M^{-1})^* P^* M^*.$$

Letting $X = M^{-1}(M^{-1})^*$, we see that $PXP^* = X$; moreover, since P is unitary, we have $XP = PX$ for all permutation matrices P. The permutation matrices arise from a representation of S_d which is a direct sum of two irreducible representations. It follows that the set of X which commute with all permutation matrices is a 2 dimensional $\mathbb{C}$-vector space. Since both $\mathbf{I}_d$ and J commute with every permutation matrix, we see that these two matrices span the vector space of matrices which commute with every permutation matrix. Hence $X = \alpha\mathbf{I}_d + \beta J$. Since X is invertible and J is not, we see that α is nonzero. Let $Y \in G$. Observe that for each $\sigma \in S_d$, there exists $\tau \in S_d$ such that $\nu(\sigma)Y = \nu(\tau)$. Let y_i denote the sum of the i^{th} row of Y. Then multiplication by $(1, 1, \ldots, 1)^{\mathrm{T}}$ gives

$$\nu(\sigma) \cdot (y_1, \ldots, y_d) = \binom{d}{2}.$$

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

In particular, $\nu(\sigma) \cdot (y_1 - 1, \ldots, y_d - 1) = 0$ for all $\sigma \in S_d$. Since the vectors $\nu(\sigma)$ span $\mathbb{Q}^d$, we see that the row sums of Y must all be equal to 1. We have

$$\mathbf{I}_d = (MYM^{-1})((M^{-1})^* Y^* M^*),$$

and hence $YXY^* = X$. Equivalently, $Y(\alpha \mathbf{I}_d + \beta J)Y^* = \alpha \mathbf{I}_d + \beta J$. Since Y has row sums equal to 1 and Y^* has column sums equal to 1, we see that $YJY^* = J$, and so we conclude that $\alpha YY^* = \alpha \mathbf{I}_d$. Since $\alpha \neq 0$, we see that Y is unitary. Thus G is a unitary group.

Let Y be in G. Then there is some permutation matrix P such that $\nu(\mathrm{id})YP = \nu(\mathrm{id})$. By Lemma 5.4, YP is either the identity or $YP = \frac{2}{d}J - U$, where U and J are as in the statement of Lemma 5.4. Notice that in the second case $YPU = \frac{2}{d}J - \mathbf{I}_d$. Since P and U are permutation matrices, we conclude that G is indeed the product of the group of permutation matrices and the group $\{\mathbf{I}_d, \frac{2}{d}J - \mathbf{I}_d\}$. Since J commutes with the collection of permutation matrices, we obtain the direct product decomposition for G given in the statement of the proposition. ∎

Proof of Theorem 1.3 Let $\mathcal{S} = \{n \mid \mathbb{Z}[q^n] = \mathbb{Z}[r^n]\}$. From Theorem 2.1, we have $\mathrm{disc}(\mathbb{Z}[q^n]) = \mathrm{disc}(\mathbb{Z}[r^n])$ for all $n \in \mathcal{S}$.

Let A_n denote the $d \times d$ matrix whose (i, j)-th entry is $q_{i-1}^{n(j-1)}$ and let B_n be the $d \times d$ matrix whose (i, j)-th entry is $r_{i-1}^{n(j-1)}$. Then $\det(A_n)^2 = \mathrm{disc}(\mathbb{Z}[q^n])$ and $\det(B_n)^2 = \mathrm{disc}(\mathbb{Z}[r^n])$. Hence $\det(A_n) = \pm \det(B_n)$ for all $n \in \mathcal{S}$. We have $F(x) := \sum_{i=0}^{\infty} \det(A_i)x^i$ and $G(x) := \sum_{i=0}^{\infty} \det(B_i)x^i$ are rational power series whose coefficients agree (up to sign) on some infinite set. By Theorem 4.1, they must agree (up to sign) on some arithmetic progression. Hence there exist $a, b > 0$ and $\epsilon \in \{-1, 1\}$ such that $\det(A_{am+b}) = \epsilon \det(B_{am+b})$ for all m sufficiently large.

Now

$$\sum_{m=0}^{\infty} \det(A_{am+b})x^m = \epsilon \sum_{m=0}^{\infty} \det(B_{am+b})x^m$$

are rational functions. Hence they must have exactly the same poles. Let $a_\sigma = \prod_{j=0}^{d-1} q_j^{-a\sigma(j)}$. By Proposition 3.2 and Lemma 4.3, the a_σ are distinct and each must be a pole for each of these power series; *i.e.,* there can be no cancellation. Similarly, $b_\sigma = \prod_{j=0}^{d-1} r_j^{-a\sigma(j)}$ has the property that b_σ is a pole of

$$\sum \det(B_{am+b})x^m = \epsilon \sum \det(A_{am+b})x^m$$

for all $\sigma \in S_d$. Since the two power series in the line above are the same up to sign we have that for each permutation σ there is some permutation τ such that $X(\sigma) := \prod_i q_i^{a\sigma(i)}$ is equal to $Y(\tau) := \prod_i r_i^{a\tau(i)}$. Moreover, the correspondence $\sigma \mapsto \tau$ is a set-bijection of S_d. By Lemma 5.2, there exists some matrix E such that

$$\big(\sigma(0), \ldots, \sigma(d-1)\big)\, E = \big(\tau(0), \ldots, \tau(d-1)\big)$$

for all pairs (σ, τ) such that $X(\sigma) = Y(\tau)$. By relabeling the conjugates of r so that $X(\mathrm{id})$ corresponds to $Y(\mathrm{id})$, we may assume by Proposition 5.5 that E is either the identity or the matrix $\frac{2}{d}J - U$, where U is the permutation matrix whose (i, j) entry is $\delta_{i+j,d+1}$. Thus we are left with two cases.

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

Case I. $E = \frac{2}{d}J - U$.

In this case, we have $v((i, i+1))E = v((d-2-i, d-1-i))$ by equation (5.2). Hence

$$(v((i, i+1)) - v(\mathrm{id}))E = v((d-2-i, d-1-i)) - v(\mathrm{id}).$$

Equivalently, for each $i < d-1$, $q_i/q_{i+1} = r_{d-2-i}/r_{d-1-i} = r'_i/r'_{i+1}$, where $r'_i = r^{-1}_{d-1-i}$. Thus $q_0/q_j = r'_0/r'_j$ for $0 \leq j \leq d-1$. Take $s = q_0/r'_0 = q_0 r_{d-1}$. Then $sr'_j = q_j$ for all j. Notice that

$$s^m((r'_0)^m + \cdots + (r'_{d-1})^m) = (q_0^m + \cdots + q_{d-1}^m).$$

Since $(r'_0)^m + \cdots + (r'_{d-1})^m$ is a symmetric function of the r_i, it is rational; moreover, it is nonzero for infinitely many m. Similarly, $q_0^m + \cdots + q_{d-1}^m$ is rational for all m. It follows that s^m is rational for some m. Since it is an algebraic integer, we conclude that it is an integer. Hence there are integers m, N with $m > 0$ such that $q^m r_{d-1}^m = N$. Taking norms of both sides of this equation, we see that $N^d = \mathrm{Norm}(q)^m \mathrm{Norm}(r)^m$. The fact that $X(\mathrm{id}) = Y(\mathrm{id})$ gives that q and r have the same norm up to sign. Thus $q = \mathrm{Norm}(r)^{2/d}\omega/r'$ for some conjugate r' of r and some root of unity ω. This completes the proof in this case.

Case II. E is the identity matrix.

Assume that E is the identity matrix. Then since $v((i, i+1)) - v(\mathrm{id}) = e_{i+1} - e_{i+2}$ is fixed by E, we see that $q_i^a/q_{i+1}^a = r_i^a/r_{i+1}^a$ for all i. Let $z = q_0^a/r_0^a$. Then $q_i^a/r_i^a = z$ for all i. Since $v(\mathrm{id})$ is fixed by E, we have

$$z^{\binom{d}{2}} \prod_i r_i^{ai} = \prod (z r_i)^{ai} = \prod_i q_i^{ai} = \prod_i r_i^{ai}.$$

Hence $z^{\binom{d}{2}} = 1$ and so q_0/r_0 is a root of unity. It follows that $q = \omega r'$ for some root of unity ω and some conjugate r' of r.

In either case we have that $q = \omega r'$ for some conjugate r' of r and some root of unity ω. This completes the proof. ∎

Proof of Corollary 1.4 By Theorem 1.3, we see that there are two cases to consider.

Case I. $q = \omega r'$ for some conjugate r' of r and some root of unity ω.

In this case $|q| = |r'|$. Since all conjugates of r are less than 1, we deduce that $r' = r$. Thus $q = \omega r$. Since q and r are both positive real numbers, we see that $\omega = 1$ and hence $q = r$.

Case II. $q = \mathrm{Norm}(r)^{2/d}\omega/r'$ for some conjugate r' of r and some root of unity ω.

We see that if $\deg(q) = 2$, then $\mathrm{Norm}(r)^{2/d}\omega/r' = \omega r''$ where r'' is the conjugate of r'. Thus, for degree 2, it suffices to consider Case I only. So assume that $\deg(r) \geq 3$.

Let $q = q_0, \ldots, q_{d-1}$ denote the conjugates of q and let $r_0, r_1, \ldots, r_{d-1}$ denote the conjugates of r. By relabeling if necessary, we may assume that $q_i = \mathrm{Norm}(r)^{2/d}\omega_i/r_i$, where ω_i is a root of unity. Since $d \geq 3$, we can pick $j > 0$ such that $r_j \neq r$. Then $|q_j| = |\mathrm{Norm}(r)|^{2/d}/|r_j|$. But this gives an immediate contradiction since $|q_j|, |r_j| < 1$ and $|\mathrm{Norm}(r)| \geq 1$. ∎

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

We note that both possibilities given in the conclusion of Theorem 1.3 can occur. We give the following example to show this.

Example. Let q be a full rank algebraic integer of norm ± 1. Then

$$\mathbb{Z}[q^n] = \mathbb{Z}[1/q^n] = \mathbb{Z}[(-q)^n]$$

for all integers $n \neq 0$.

Proof This follows from the fact that q^n has norm ± 1. ∎

6 Pisot Numbers of Small Degree

Here we prove our finiteness results for Pisot numbers of degree at most 3.

Proof of Theorem 1.5 First suppose that $\deg(r) = 2$ and let r' denote the conjugate of r. Let q be a Pisot number with $\mathbb{Z}[q] = \mathbb{Z}[r]$ and let q' denote the conjugate of q. Then we can write $q = br + a$. Now $\operatorname{disc}(q) = b^2 \operatorname{disc}(r)$ and hence $b = \pm 1$. Thus either $q = a+r$ or $q = a-r$. If $q = a+r$, then $q' = a+r'$ and hence $|a+r'| < 1$. There are at most two integers a which satisfy this inequality and so there are at most two Pisot numbers q of the form $a + r$. If, on the other hand, $q = a - r$, then $q' = a - r'$ and so $|a - r'| < 1$. Again, we see that there are at most two integers a which give rise to a Pisot number q of the form $a - r$. Hence there are at most four Pisot numbers q such that $\mathbb{Z}[r] = \mathbb{Z}[q]$.

Next suppose that $\deg(r) = 3$ and let $r = r_0, r_1, r_2$ denote the conjugates of r. Let q be a Pisot number with $\mathbb{Z}[q] = \mathbb{Z}[r]$. Write $q = a + br + cr^2$. Then the conjugates of q are given by $a + br_i + cr_i^2$ for $i = 0, 1, 2$. Hence

$$\begin{aligned}\operatorname{disc}(q) &= \prod_{0\le i<j\le 2} (b(r_i - r_j) + c(r_i^2 - r_j^2))^2 \\ &= \prod_{0\le i<j\le 2} (r_i - r_j)^2 (b + c(r_i + r_j))^2 \\ &= \operatorname{disc}(r)(b + c(r_0 + r_1))^2 (b + c(r_0 + r_2))^2 (b + c(r_1 + r_2))^2.\end{aligned}$$

Since $\operatorname{disc}(q) = \operatorname{disc}(r)$, we deduce that

$$(b + c(r_0 + r_1))^2 (b + c(r_0 + r_2))^2 (b + c(r_1 + r_2))^2 = 1.$$

Consider the polynomial in indeterminates x and y

$$P(x, y) := (x + y(r_0 + r_1))(x + y(r_0 + r_2))(x + y(r_1 + r_2)). \tag{6.1}$$

Since P is a symmetric function of r_0, r_1, r_2, it is a homogeneous polynomial in x and y of degree 3 with integer coefficients. By the remarks above, we have $P(b, c) = \pm 1$. The polynomial $P(x, y)$ can factor into at most three irreducible polynomials in $\mathbb{Q}[x, y]$.

If $P(x, y)$ is not irreducible in $\mathbb{Q}[x, y]$, then it has at least one linear factor with rational coefficients. From equation (6.1) we then see that $r_i + r_j$ must be rational for

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

some $i \neq j$. But $r_0 + r_1 + r_2$ is also rational and hence r_k is rational for some k. But this contradicts the fact that r has degree 3, and so $P(x, y)$ must be irreducible.

Hence the equation $P(x, y) = \pm 1$ is a Thue equation. It is known that in the case of Thue equations, there are only a finite number of integer solutions to $P(x, y) = \pm 1$ [8]. Moreover, for cubic Thue equations, there are at most 20 integer solutions to $P(x, y) = \pm 1$ [2]. Thus there are at most 20 integer points (b, c) which satisfy $P(b, c) = \pm 1$. We claim that for particular b and c there are at most two a such that $q = a + br + cr^2$ is a Pisot number. The reason for this is that the conjugates of q must be less than 1; that is,

$$|a + br_1 + cr_1^2| < 1 \qquad \text{and} \qquad |a + br_2 + cr_2^2| < 1.$$

Let $\alpha = br_1 + cr_1^2$ and let $\beta = br_2 + cr_2^2$. Then there are at most two values of a such that $|a + \alpha| < 1$ and so there are at most two values of a giving solutions to both equations. Since there are at most 20 values of (b, c) which give rise to Pisot numbers, there are at most 40 Pisot numbers q such that $\mathbb{Z}[r] = \mathbb{Z}[q]$. ∎

In general, there are finitely many integer solutions (x, y) to a Thue equation $P(x, y) = \pm k$.

7 Pisot-Cyclotomic Numbers

In this section we prove that there are only finitely many Pisot-cyclotomic numbers of any fixed order. In fact we prove a stronger result. For this we use the Schmidt Subspace Theorem [7, Chapter VI].

Theorem 7.1 **(Schmidt Subspace Theorem)** *Let C be a positive constant and let $\varepsilon > 0$. If $L_1, \ldots, L_n$ are n independent linear homogeneous functions of $\mathbf{x} = (x_1, \ldots, x_n)$ with algebraic integer coefficients, then the set of points $\mathbf{x} \in \mathbb{Z}^n$ such that*

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < C||\mathbf{x}||^{-\varepsilon}$$

is finite.

We start with a Lemma.

Lemma 7.2 *Let $r_0, \ldots, r_{d-1}$ be distinct nonzero complex numbers. Then the $d - 1$ linear homogeneous forms*

$$L_i(\mathbf{x}) = (r_i - r_0)x_1 + (r_i^2 - r_0^2)x_2 + \cdots + (r_i^{d-1} - r_0^{d-1})x_{d-1}, \qquad 1 \leq i \leq d - 1,$$

are linearly independent over $\mathbb{C}$.

Proof Let $H_0(\mathbf{x}) = r_0x_1 + r_0^2x_2 + \cdots + r_0^{d-1}x_{d-1}$ and for $1 \leq i \leq d-1$, define $H_i(\mathbf{x}) = H_0(\mathbf{x}) + L_i(\mathbf{x})$. It is sufficient to show that $H_1, \ldots, H_{d-1}$ are linearly independent

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

over $\mathbb{C}$. Suppose that some linear combination of them is zero, say $\sum w_i H_i(\mathbf{x}) = 0$. Then we can express this as a vector equation

$$\mathbf{w}^T V \mathbf{x} = [w_0 r_0, \cdots, w_{d-1} r_{d-1}] \begin{bmatrix} 1 & r_0 & \cdots & r_0^{d-1} \\ 1 & r_1 & \cdots & r_1^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & r_{d-1} & \cdots & r_{d-1}^{d-1} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{d-1} \end{bmatrix} = \mathbf{0},$$

where V is a Vandermonde matrix and $\mathbf{w}$ is a nonzero column vector. Since this equation holds for all column vectors $\mathbf{x}$, we conclude that $\mathbf{w}^T V = 0$, contradicting the fact that V is invertible. The result follows. ∎

Lemma 7.3 *Let r and q be a Pisot numbers of degree d such that there exist integers $c_0, \ldots, c_{d-1}$ with the property that $q = c_0 + c_1 r + \cdots + c_{d-1} r^{d-1}$. Then there exist positive constants C_1 and C_2, dependent only on r (and hence independent of q) such that*

$$C_1 q < \sqrt{c_0^2 + \cdots + c_{d-1}^2} < C_2 q.$$

Proof To get the lower bound we use the Cauchy-Schwarz inequality, noting that

$$|q| = (c_0, \ldots, c_{d-1}) \cdot (1, r, \ldots, r^{d-1}) \leq \sqrt{c_0^2 + \cdots + c_{d-1}^2} \sqrt{1^2 + r^2 + \cdots + r^{2d-2}}.$$

Let $\mathbf{c} = [c_0, \ldots, c_{d-1}]^{\mathrm{T}}$. The upper bound relies on the fact that q and r are Pisot. Let $q = q_0, q_1, \ldots, q_{d-1}$ denote the conjugates of q and let $\mathbf{q} = [q_0, q_1, \ldots, q_{d-1}]^{\mathrm{T}}$. Then there is a Vandermonde matrix V whose entries are powers of conjugates of r such that

$$\mathbf{q} = \begin{bmatrix} q_0 \\ q_1 \\ \vdots \\ q_{d-1} \end{bmatrix} = \begin{bmatrix} 1 & r_0 & r_0^2 & \cdots & r_0^{d-1} \\ 1 & r_1 & r_1^2 & \cdots & r_1^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & r_{d-1} & r_{d-1}^2 & \cdots & r_{d-1}^{d-1} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{bmatrix} = V\mathbf{c}.$$

Thus $\|\mathbf{c}\| \leq \|V^{-1}\| \cdot \|\mathbf{q}\|$. Note that $\|V^{-1}\|$ depends only on r and since q is Pisot we have

$$\|\mathbf{q}\| \leq \sqrt{q^2 + |q_1|^2 + \cdots + |q_{d-1}|^2} \leq \sqrt{q^2 + q^2 + \cdots + q^2} \leq q\sqrt{d}.$$

Taking $C_2 = \|V^{-1}\|\sqrt{d}$ completes the proof. ∎

Proof of Theorem 1.6 We can, without loss of generality, assume that r is a Pisot number. For take r' a Pisot number such that $\mathbb{Z}[r] = \mathbb{Z}[r']$. If no such r' exists then there are no (hence finitely many) Pisot numbers q such that $\mathbb{Z}[r] = \mathbb{Z}[q]$. If such an r' exists, $\mathbb{Z}[q] = \mathbb{Z}[r]$ if and only if $\mathbb{Z}[q] = \mathbb{Z}[r']$.

Let q be a Pisot number satisfying $\mathbb{Z}[q] = \mathbb{Z}[r]$. Let $q = q_0, \ldots, q_{d-1}$ denote the conjugates of q, and similarly $r = r_0, \ldots, r_{d-1}$ denote the conjugates of r. Then there exists an integer polynomial $P(x) = c_0 + \cdots + c_{d-1} x^{d-1}$ of degree at most $d-1$ such that for some labeling $r_0, r_1, \ldots, r_{d-1}$ we have

$$q_i = P(r_i) = c_0 + c_1 r_i + \cdots + c_{d-1} r_i^{d-1} \tag{7.1}$$

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

and $q_0, r_0 > 1$. Further, we have

$$\operatorname{disc}(r) = \operatorname{disc}(q) = \prod_{i<j}(q_i - q_j)^2$$

is fixed, for all q. Using equation (7.1), we see that

$$q_i - q_j = P_{i,j} := c_1(r_i - r_j) + \cdots + c_{d-1}(r_i^{d-1} - r_j^{d-1}).$$

Consider the $d(d-1)$ linear homogeneous polynomials

$$L_{i,j}(\mathbf{x}) := (r_i - r_j)x_1 + \cdots + (r_i^{d-1} - r_j^{d-1})x_{d-1} \qquad 1 \le i, j \le d, i \ne j$$

and let $\mathbf{c} = (c_1, \ldots, c_{d-1})$. Notice that

$$\begin{aligned} q_i - q_j = P(r_i) - P(r_j) &= c_0 + c_1 r_i + \cdots + c_{d-1} r_i^{d-1} - (c_0 + c_1 r_j + \cdots + c_{d-1} r_j^{d-1}) \\ &= c_1(r_i - r_j) + \cdots + c_{d-1}(r_i^{d-1} - r_j^{d-1}) = L_{i,j}(\mathbf{c}). \end{aligned}$$

Then $|\operatorname{disc}(q)| = \prod_{i<j} |L_{i,j}(\mathbf{c})|^2$. For $0 \le i \le d-1$, define

$$Q_i(\mathbf{x}) = \prod_{j \le d-1, j \ne 0, i} L_{i,j}(\mathbf{x}).$$

Then

$$|\operatorname{disc}(q)| = |Q_1(\mathbf{c}) \cdots Q_{d-1}(\mathbf{c})(q_0 - q_2)^2 \cdots (q_0 - q_d)^2|.$$

By assumption $q_1, \ldots, q_{d-1}$ are in the unit disc, and so we have

$$|(q_0 - q_2)^2 \cdots (q_0 - q_{d-1})^2| > (q-1)^{2d-2}.$$

From this we see that $|Q_1(\mathbf{c}) \cdots Q_{d-1}(\mathbf{c})|(q-1)^{2d-2} < |\text{disc(q)}|$ and thus $|Q_i(\mathbf{c})| < (q-1)^{-2}|\text{disc(q)}|^{1/(d-1)}$ for some i. We are almost ready to apply the subspace theorem to the polynomials $L_{i,0}, \ldots, L_{i,d-1}$ (with $L_{i,i}$ omitted). Observe that these homogeneous linear forms are linearly independent over $\mathbb{C}$ by Lemma 7.2. Next observe that if $\mathbf{x} \in \mathbb{Z}^d$, then

$$|L_{i,0}(\mathbf{x}) \cdots L_{i,d-1}(\mathbf{x})| = |Q_i(\mathbf{x})|\,|L_{i,0}(\mathbf{x})|.$$

We have

$$\begin{aligned} |L_{i,0}(\mathbf{x})| &= |(r_i - r_0)x_1 + \cdots + (r_i^{d-1} - r_0^{d-1})x_{d-1}| \\ &\le \|[r_i - r_0, \ldots, r_i^{d-1} - r_0^{d-1}]\| \cdot \|[x_1, x_2, \ldots, x_{d-1}]\| \\ &\le \|[r+1, \ldots, r^{d-1} + 1]\| \cdot \|\mathbf{x}\| \\ &\le \|[r^{d-1} + 1, \ldots, r^{d-1} + 1]\| \cdot \|\mathbf{x}\| \\ &\le \sqrt{d-1} \cdot |r^{d-1} + 1| \cdot \|\mathbf{x}\|. \end{aligned}$$

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

Let $0 < \varepsilon < 1$. By Schmidt's subspace theorem, for any positive C, there are only finitely many $\mathbf{x} \in \mathbb{Z}^{d-1}$ such that $|L_{i,0}(\mathbf{x}) \cdots L_{i,d-1}(\mathbf{x})| < C\|\mathbf{x}\|^{-\varepsilon}$. Consequently, there are only finitely many integer points $\mathbf{x}$ such that $|Q_i(\mathbf{x})| < \|\mathbf{x}\|^{-1-\varepsilon}$, since for each such point $\mathbf{x}$, we have

$$\begin{aligned}|L_{i,0}(\mathbf{x}) \cdots L_{i,d-1}(\mathbf{x})| &= |Q_i(\mathbf{x})|\,|L_{i,0}(\mathbf{x})| < \|\mathbf{x}\|^{-1-\varepsilon}\sqrt{d-1} \cdot |r^{d-1}+1| \cdot \|\mathbf{x}\| \\ &= C\|\mathbf{x}\|^{-\varepsilon},\end{aligned}$$

for some constant C.

By Lemma 7.3, there exist positive constants C_0 and C_1 which depend only on r such that $C_0 q \leq \|\mathbf{c}\| \leq C_1 q$.

Thus there are only finitely many Pisot numbers q (with corresponding integer vectors $\mathbf{c}$) such that

$$\|Q_i(\mathbf{c})\| < \|\mathbf{c}\|^{-1-\varepsilon} \leq (C_0 q)^{-1-\varepsilon} \leq C_0^{-1-\varepsilon} \cdot q^{-1-\varepsilon} \leq C_2 \cdot q^{-1-\varepsilon},$$

(here $C_2 = C_0^{-1-\varepsilon}$). Suppose that there are infinitely many Pisot numbers q with $\mathbb{Z}[q] = \mathbb{Z}[r]$. Then we have just shown that $|Q_i(\mathbf{c})| \geq C_2 q^{-1-\varepsilon}$ for infinitely many such q. But we know $|Q_i(\mathbf{c})| < (q-1)^{-2}|\operatorname{disc}(q)|^{1/(d-1)} = (q-1)^{-2}\operatorname{disc}(r)^{1/(d-1)}$, and so we have $C_2 q^{-1-\varepsilon} < (q-1)^{-2}|\operatorname{disc}(q)|^{1/(d-1)}$ for infinitely many Pisot numbers q with $\mathbb{Z}[q] = \mathbb{Z}[r]$. Equivalently,

$$\frac{(q-1)^2}{q^{1+\varepsilon}} < \frac{\operatorname{disc}(r)^{1/(d-1)}}{C_3}$$

for infinitely many Pisot numbers q with $\mathbb{Z}[q] = \mathbb{Z}[r]$. But we see then that there is a computable upper bound for q, as $\frac{(q-1)^2}{q^{1+\varepsilon}} \to +\infty$ as $q \to +\infty$. But Pisot numbers in a number field are discrete, and so we obtain a contradiction. The result now follows. ∎

8 Conclusions, Open Questions, and Conjectures

A number of finiteness results are shown in this paper. Unfortunately, Theorem 1.5 only provides a bound for the number of Pisot numbers for degrees 2 and 3. In addition, these bounds are probably not best possible. Theorem 1.6 proves that there are a finite number of Pisot numbers q such that $\mathbb{Z}[q] = \mathbb{Z}[r]$, given some nice restrictions on r. Unfortunately, no upper bounds are given on the number of Pisot numbers q of this form. We therefore state the following open problems.

(1) Improve the bounds given in the statement of Theorem 1.5.
(2) Improve Theorem 1.6 to give bounds for the number of Pisot numbers q such that $\mathbb{Z}[q] = \mathbb{Z}[r]$ in terms of r.
(3) Extend the results of Theorem 1.6 to say something about the case where the conjugates of r do not all lie in $\mathbb{Q}[r]$, or give an example to show that the finiteness property does not hold.

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press

References

[1] J. P. Bell and K. G. Hare, *A classification of (some) Pisot-cyclotomic numbers.* J. Number Theory **115**(2005), no. 2, 215–229.
[2] M. A. Bennett, *On the representation of unity by binary cubic forms.* Trans. Amer. Math. Soc. **353**(2001), no. 4, 1507–1534 (electronic).
[3] Č. Burdík, Ch. Frougny, J. P. Gazeau, and R. Krejcar, *Beta-integers as natural counting systems for quasicrystals.* J. Phys. A **31**(1998), no. 30, 6449–6472.
[4] J.-P. Gazeau, *Pisot-cyclotomic integers for quasilattices.* In: The mathematics of long-range aperiodic order, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. 487, Kluwer Academic Publishing, Dordrecht, 1997, pp. 175–198.
[5] C. Lech, *A note on recurring series.* Ark. Mat. **2**(1953), 417–421.
[6] D. A. Marcus, *Number fields.* Universitext, Springer-Verlag, New York, 1977.
[7] W. M. Schmidt, *Diophantine approximation.* Lecture Notes in Mathematics 785, Springer, Berlin, 1980.
[8] V. G. Sprindžuk, *Classical Diophantine equations.* Lecture Notes in Mathematics 1559, Springer-Verlag, Berlin, 1993.

Department of Mathematics, Simon Fraser University, Burnaby, BC V5A 1S6
e-mail: jpb@math.sfu.ca

Department of Pure Mathematics, University of Waterloo, Waterloo, ON N2L 3G1
e-mail: kghare@math.uwaterloo.ca

https://doi.org/10.4153/CJM-2009-013-9 Published online by Cambridge University Press