ON LATTICES GENERATED BY ALGEBRAIC CONJUGATES OF PRIME DEGREE

LENNY FUKSHANSKY AND EVELYNE KNIGHT

Abstract. We consider Euclidean lattices spanned by images of algebraic conjugates of an algebraic number under Minkowski embedding, investigating their rank, properties of their automorphism groups and sets of minimal vectors. We are especially interested in situations when the resulting lattice is well-rounded. We show that this happens for large Pisot numbers of prime degree, demonstrating infinite families of such lattices. We also fully classify well-rounded lattices from algebraic conjugates in the 2-dimensional case and present various examples in the 3-dimensional case. Finally, we derive a determinant formula for the resulting lattice in the case when the minimal polynomial of an algebraic number has its Galois group of a particular type.

1. Introduction

Algebraic constructions of Euclidean lattices received a great deal of attention in lattice theory over the past years. Perhaps the most commonly studied construction is that of *ideal lattices* from algebraic number fields, thoroughly described by E. Bayer-Fluckiger (see, e.g., [5]): a Euclidean lattice is obtained from an ideal in the ring of integers of a number field in question via an application of Minkowski embedding. The actively studied properties of lattices arising from such constructions include number and configurations of minimal vectors, as well as the size and structure of the automorphism group. The underlying algebraic structure allows for simpler description and informs the geometric properties of the resulting lattices. A great deal of attention in the recent years was specifically devoted to the *well-rounded* ideal lattices, i.e. ideal lattices containing full linearly independent sets of minimal vectors (see, e.g., [17], [16], [6], [9], [25], [19], [20], [1]). Applications of well-rounded ideal lattices to coding theory and cryptography were considered, for instance, in [22], [8] and [18].

A different construction of algebraic well-rounded lattices from cyclic number fields of odd prime degree has been proposed in [3] and [2]: instead of applying Minkowski embedding to an ideal (as in the construction of ideal lattices), the authors considered $\mathbb{Z}$-modules in the ring of integers spanned by the images of an algebraic integer under the action of the cyclic Galois group. In the present paper, we want to generalize this construction, viewing it from a somewhat different angle.

Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be an irreducible polynomial of degree $n \geq 2$ and let

$$\alpha_1, \alpha_2, \ldots, \alpha_n$$

2020 *Mathematics Subject Classification.* Primary: 11H06, 11R04, 11R06, 11R32.

Key words and phrases. well-rounded lattices, Pisot polynomials, algebraic conjugates.

be roots of $f(x)$. Let K be its splitting field and G its Galois group over $\mathbb{Q}$. Then

$$d := [K : \mathbb{Q}] = |G| \leq n!.$$

Write $G = \{\sigma_1, \dots, \sigma_d\}$, then for each $1 \leq i \leq n$ and $1 \leq j \leq d$, $\sigma_j(\alpha_i) = \alpha_{i_j}$ for some corresponding $1 \leq i_j \leq n$. Further,

$$-a_{n-1} = \alpha_1 + \cdots + \alpha_n \in \mathbb{Z}. \tag{1}$$

Define

$$\mathcal{M}_f = \operatorname{span}_{\mathbb{Z}} \{\alpha_1, \dots, \alpha_n\} \subset K,$$

so $\mathcal{M}_f$ is a $\mathbb{Z}$-module of rank $\leq n$ generated by all the conjugates of α. Notice that $\mathcal{M}_f$ is closed under the action of G, since automorphisms of the Galois extension $K/\mathbb{Q}$ simply permute the roots of an irreducible polynomial.

We can identify elements of G with the embeddings of K into $\mathbb{C}$, where r_1 of them are real and $2r_2$ are complex, coming in conjugate pairs, i.e., $d = r_1 + 2r_2$. The Minkowski embedding

$$\Sigma_K = (\sigma_1, \dots, \sigma_d) : K \hookrightarrow \mathbb{C}^d$$

takes K into the space $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$, which can be viewed as a subspace of

$$\left\{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \bar{y}_j \ \forall \ 1 \leq j \leq r_2\right\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \subset \mathbb{C}^d,$$

where in the last containment each copy of $\mathbb{R}$ is identified with the real part of the corresponding copy of $\mathbb{C}$. For each $\alpha \in K$, we write $\boldsymbol{\alpha}$ for its image $\Sigma_K(\alpha)$ in $K_{\mathbb{R}}$. Then $K_{\mathbb{R}}$ is a d-dimensional Euclidean space with the symmetric bilinear form induced by the trace form on K:

$$\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle := \operatorname{Tr}_K(\alpha\bar{\beta}) \in \mathbb{R},$$

for every $\alpha, \beta \in K$, where Tr_K is the number field trace on K. The Euclidean norm $\|\boldsymbol{\alpha}\|$ on $K_{\mathbb{R}}$ is given by $\sqrt{\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle}$ and the angle θ between $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ is given by

$$\theta = \cos^{-1}\left(\frac{\langle \boldsymbol{\alpha}, \boldsymbol{\beta} \rangle}{\|\boldsymbol{\alpha}\| \|\boldsymbol{\beta}\|}\right).$$

Define $L_f := \Sigma_K(\mathcal{M}_f)$, which is a Euclidean lattice in $K_{\mathbb{R}}$. Then

$$L_f = \operatorname{span}_{\mathbb{Z}} \{\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_n\}.$$

More generally, we will use boldface letters to denote vectors in L_f that are images of the corresponding algebraic numbers in $\mathcal{M}_f$ under the Minkowski embedding Σ_K. We write $\operatorname{Aut}(L_f)$ for the automorphism group of the lattice L_f, i.e., the group of isometries of the trace-induced bilinear form $\langle\ ,\ \rangle$ preserving L_f. Our first simple observation concerns this automorphism group.

Proposition 1.1. *The group G is a subgroup of* $\operatorname{Aut}(L_f)$.

We prove this proposition in Section 2. Notice that it guarantees that our construction L_f produces lattices with relatively large automorphism groups; indeed, a generic lattice has only two automorphisms: $\boldsymbol{x} \mapsto \pm\boldsymbol{x}$. In fact, unlike our construction L_f, ideal lattices are not necessarily closed under the action of the Galois group. We also define the *minimal norm* of L_f to be

$$|L_f| = \min\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L_f \setminus \{\boldsymbol{0}\}\}$$

and the *set of minimal vectors* of L_f to be

$$S(L_f) = \{\boldsymbol{x} \in L_f : \|\boldsymbol{x}\| = |L_f|\}.$$

With this notation, we can now state the following theorem.

Theorem 1.2. *Suppose n is prime. Then:*

(1) *The lattice L_f has rank n if $a_{n-1} \neq 0$ and rank $n-1$ if $a_{n-1} = 0$.*
(2) *If $|L_f| < \sqrt{d}|a_{n-1}|$, then the cardinality of $S(L_f)$ is divisible by n.*

A lattice L_f is called *well-rounded* (WR) if $S(L_f)$ contains at least n linearly independent vectors, i.e., if

$$\operatorname{span}_{\mathbb{R}} L_f = \operatorname{span}_{\mathbb{R}} S(L_f).$$

Corollary 1.3. *Let $n = d$ be prime, $|L_f| < \sqrt{n}|a_{n-1}|$ and let*

$$\boldsymbol{\beta} = \sum_{k=1}^{n} c_k \boldsymbol{\alpha}_k \in S(L_f).$$

If $\sum_{k=1}^{n} c_k \neq 0$ then L_f is WR.

We can give a more explicit criterion for well-roundedness in the three-dimensional case.

Corollary 1.4. *Let $n = d = 3$ and assume that $|L_f| < \sqrt{3}|a_2|$. Then:*

(1) *If $\sum_{i<j} \alpha_i \alpha_j < \frac{1}{2} \sum_{i \leq 3} \alpha_i^2$, then the lattice L_f is WR.*
(2) *If $\left|\sum_{i<j} \alpha_i \alpha_j\right| < \frac{1}{3} \sum_{i \leq 3} \alpha_i^2$, then $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3 \in S(L_f)$.*

We prove Theorem 1.2 and Corollaries 1.3 and 1.4 in Section 2. Our main tool is a result of Dubickas [11] on the degree of integer linear forms in algebraic conjugates. We separately consider the two-dimensional situation in Section 3, where the results can be made very explicit. In particular, we fully classify planar lattices of the form L_f in Theorem 3.2.

To state our main result, we need some additional notation. Let $\mathcal{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be an ordered basis for a lattice L in $\operatorname{span}_{\mathbb{R}} L$, and define a sequence of angles $\theta_1, \ldots, \theta_{n-1}$ as follows: each θ_i is the angle between $\boldsymbol{b}_{i+1}$ and the subspace

$$\operatorname{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i\}.$$

Then each $\theta_i \in [0, \pi/2]$ and we say that $\mathcal{B}$ is a *weakly nearly orthogonal* basis if $\theta_i \geq \pi/3$ for each $1 \leq i \leq n-1$. A basis $\mathcal{B}$ is called *nearly orthogonal* if every ordering of it is weakly nearly orthogonal. If L has such a basis, we say that L is a nearly orthogonal lattice. Nearly orthogonal lattices were introduced in [4], where they were applied to the problem of image compression. Nearly orthogonal lattices that are also well-rounded have been studied in [15].

The class of generic well-rounded (GWR) lattices was introduced in [18]: a WR lattice L of rank n is called *generic WR* if $|S(L)| = 2n$, i.e., if L contains the minimal possible number of minimal vectors for a WR lattice. GWR lattices are important for their application in coding theory and cryptography since they allow for simultaneous maximization of the packing density and minimization of the kissing number. In [18] and [10], the authors showed a particular construction of a family of GWR lattices. Our construction produces a new family of algebraic lattices, which are both, GWR and nearly orthogonal.

Theorem 1.5. *Let $n \geq 3$ be prime. There exist infinitely many polynomials $f(x) \in \mathbb{Z}[x]$ of degree n so that L_f is a GWR nearly orthogonal lattice of rank n in $K_{\mathbb{R}}$,*

where K is the splitting field of $f(x)$; further, L_f contains a basis consisting of minimal vectors. For example, we can take $f(x) = x^n + a_{n-1}x^{n-1} + a_0$, where

$$|a_0| > \frac{8(n-1)n!}{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)}$$

and $|a_{n-1}| > |a_0| + 1$ are integers.

We prove Theorem 1.5 in Section 4. Our main tools, in addition to Dubickas's result, are Strong Approximation Theorem, Perron's irreducibility criterion for Pisot polynomials and a theorem of Fukshansky and Kogan on coherence of nearly orthogonal well-rounded lattices. More generally, we show that the lattice constructions we seek are often yielded by sets of algebraic conjugates of large Pisot numbers, thus making a connection to the well-studied Pisot polynomials, a special class of which is described in the statement of our Theorem 1.5. We demonstrate some examples of cubic Pisot and non-Pisot polynomials giving rise to WR lattices in Section 5. Finally, in Section 6 we compute the determinant of the lattice L_f in situations when the Galois group of $f(x)$ is either cyclic of order $n = \deg(f)$, the full symmetric group S_n, or the alternating group A_n. We are now ready to proceed.

2. Automorphisms and minimal vectors

First, we prove Proposition 1.1, which is very similar to Lemma 6.1 of [14].

Proof of Proposition 1.1. The embeddings of K are precisely the elements of G, and for every $\tau \in G$ and $\alpha, \beta \in \mathcal{M}_f$, $\tau(\alpha), \tau(\beta) \in \mathcal{M}_f$ and

$$\begin{aligned} \langle \tau(\alpha), \tau(\beta) \rangle &= \mathrm{Tr}_K(\tau(\alpha\bar{\beta})) = \sum_{\sigma \in G} \sigma\tau(\alpha\bar{\beta}) \\ &= \sum_{\sigma \in G} \sigma(\alpha\bar{\beta}) = \mathrm{Tr}_K(\alpha\bar{\beta}) = \langle \alpha, \beta \rangle , \end{aligned}$$

since right-multiplication by τ simply permutes elements of G. Therefore G is a subgroup of $\mathrm{Aut}(L_f)$. □

Next, we assume that n is prime and prove Theorem 1.2. Our main tool is the following result of Dubickas, which we state specifically over $\mathbb{Q}$.

Theorem 2.1 ([11], Theorem 1)**.** *Let n be prime and $c_1, \dots, c_n \in \mathbb{Q}$. Then*

$$\beta = c_1\alpha_1 + \cdots + c_n\alpha_n \in \mathbb{Q}$$

if and only if $c_1 = \cdots = c_n$. If this is not the case, then $\deg(\beta)$ is divisible by n.

Proof of Theorem 1.2. First, suppose that $a_{n-1} \neq 0$. Notice that in the case $c_1 = \cdots = c_n$,

$$c_1\alpha_1 + \cdots + c_n\alpha_n = -c_1 a_{n-1} \neq 0,$$

unless $c_1 = 0$. By Theorem 2.1, if c_k's are not all equal, then this linear combination cannot be 0, since $0 \in \mathbb{Q}$. This implies that $\alpha_1, \dots, \alpha_n$ are $\mathbb{Q}$-linearly independent and $\mathcal{M}_f$ is a free $\mathbb{Z}$-module of rank n; hence, L_f is a Euclidean lattice of rank n.

On the other hand, suppose that $a_{n-1} = 0$. Again, by Theorem 2.1, the elements $\alpha_1, \dots, \alpha_n$ can satisfy only one linear relation of the form

$$c_1\alpha_1 + \cdots + c_n\alpha_n = 0,$$

the one with all coefficients equal. Therefore $\alpha_n = -\sum_{k=1}^{n-1} \alpha_k$ and $\alpha_1, \ldots, \alpha_{n-1}$ are $\mathbb{Q}$-linearly independent. Thus, $\mathcal{M}_f$ is a free $\mathbb{Z}$-module of rank $n-1$; hence, L_f is a Euclidean lattice of rank $n-1$.

Now, let $\beta \in \mathcal{M}_f$, then

$$\beta = \sum_{k=1}^{n} c_k \alpha_k, \tag{2}$$

for some $c_1, \ldots, c_n \in \mathbb{Z}$ and its conjugates are of the form

$$\beta_j = \sigma_j(\beta) = \sum_{k=1}^{n} c_k \sigma_j(\alpha_k) \in \mathcal{M}_f, \tag{3}$$

for all $1 \leq j \leq d$. In general, β may have degree less than d (and even less than n), in which case some of these β_j's may be equal to each other. In particular, if $c_1 = \cdots = c_n$, then $\beta = -c_1 a_{n-1} \in \mathbb{Q}$ and and hence $\beta_j = \sigma_j(\beta) = \beta$ for every $1 \leq j \leq n$, since σ_j's fix $\mathbb{Q}$. Thus

$$|\Sigma_K(\beta)| = \sqrt{d}|c_1||a_{n-1}|.$$

Taking $c_1 = 1$, we see that L_f contains a vector of norm $\sqrt{d}|a_{n-1}|$.

Suppose that $|L_f| < \sqrt{d}|a_{n-1}|$. Then there must exist a $\beta \in M_f$ as in (2) so that not all c_k's are equal and $|\Sigma_K(\beta)| = |L_f|$. Then, by Theorem 2.1, this β has degree divisible by n, and thus at least the number of distinct conjugates is divisible by n. All of these conjugates give rise to minimal vectors in L_f via the Minkowski embedding, so the cardinality of $S(L_f)$ is divisible by n. □

Proof of Corollary 1.3. Suppose $n = d$ is prime and $|L_f| < \sqrt{d}|a_{n-1}|$. Let $\boldsymbol{\beta} \in S(L_f)$ and let $\beta \in \mathcal{M}_f$ be such that $\boldsymbol{\beta} = \Sigma_K(\beta)$. Then β has degree divisible by n, by the same argument as in the proof of Theorem 1.2 above. Since $[K : \mathbb{Q}] = n$ and $\beta \in K$, we must have $\deg(\beta) = n$. Let $\beta = \beta_1, \beta_2, \ldots, \beta_n$ be its conjugates. Theorem 2.1 implies again that if

$$b_1\beta_1 + \ldots b_n\beta_n = 0,$$

then $b_1 = \cdots = b_n$. Assume that $\beta_1, \ldots, \beta_n$ are linearly dependent, then we must have

$$\beta_1 + \cdots + \beta_n = 0.$$

Writing β as in (2) and using (3), we obtain a relation

$$\begin{aligned} 0 &= \sum_{k=1}^{n} c_k\sigma_1(\alpha_k) + \cdots + \sum_{k=1}^{n} c_k\sigma_n(\alpha_k) = \sum_{k=1}^{n} c_k \left(\sigma_1(\alpha_k) + \cdots + \sigma_n(\alpha_k)\right) \\ &= \sum_{k=1}^{n} c_k \operatorname{Tr}_K(\alpha_k) = -a_{n-1} \sum_{k=1}^{n} c_k. \end{aligned}$$

Since $a_{n-1} \neq 0$, this means that $\sum_{k=1}^{n} c_k = 0$. Hence, if we assume that $\sum_{k=1}^{n} c_k \neq 0$, then $\boldsymbol{\beta}_1, \ldots, \boldsymbol{\beta}_n$ are linearly independent and L_f is WR. □

Remark 2.1. For the converse of Corollary 1.3, suppose L_f is WR. Then every minimal vector is of the form $\boldsymbol{\beta}$ for some $\beta \in \mathcal{M}_f$ of degree n. Indeed, since n is prime $\deg(\beta) = 1$ or n. Assume $\deg(\beta) = 1$ so $\beta \in \mathbb{Q}$, then by Theorem 2.1 we must have $c_1 = \cdots = c_n$, and so β is an integer multiple of $\beta' = \sum_{i=1}^{n} \alpha_i$. However,

we assumed that $|L_f| < \sqrt{d}|a_{n-1}| = \|\boldsymbol{\beta}'\| \leq \|\boldsymbol{\beta}\|$, a contradiction. Thus every minimal vector is of degree n.

Proof of Corollary 1.4. First notice that the assumption $n = d = 3$ implies that all three algebraic conjugates $\alpha_1, \alpha_2, \alpha_3$ are real. By Corollary 1.3, it suffices to show that if $\beta = \sum_{k=1}^3 c_k \alpha_k \in \mathcal{M}_f$ such that $\sum_{k=1}^3 c_k = 0$ then $\boldsymbol{\beta} \notin S(L_f)$. For any such β, the vector $\boldsymbol{\beta}$ is of the form

$$\boldsymbol{\beta} = \begin{pmatrix} c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 \\ c_1\alpha_3 + c_2\alpha_1 + c_3\alpha_2 \\ c_1\alpha_2 + c_2\alpha_3 + c_3\alpha_1, \end{pmatrix},$$

and $\|\boldsymbol{\beta}\|^2$ is equal to

$$(c_1^2 + c_2^2 + c_3^2)(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + 2(c_1c_2 + c_2c_3 + c_1c_3)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3). \tag{4}$$

Let $A = \sum_{i=1}^3 \alpha_i^2$ and $B = \sum_{i<j} \alpha_i\alpha_j$. Taking $c_1 = 1$ and $c_2 = c_3 = 0$, we obtain a vector $\boldsymbol{\alpha}_1 \in L_f$ with $\|\boldsymbol{\alpha}_1\|^2 = A$. On the other hand, if we assume that $\sum_{i=1}^3 c_i = 0$, (4) simplifies to

$$\|\boldsymbol{\beta}\|^2 = 2(c_1^2 + c_2^2 + c_1c_2)(A - B). \tag{5}$$

Suppose now that $B = \sum_{i<j} \alpha_i\alpha_j < \frac{1}{2}\sum_{i=1}^3 \alpha_i^2 = A/2$, then $2(A - B) > A$, and since $c_1^2 + c_2^2 + c_1c_2 \geq 1$, we have

$$\|\boldsymbol{\beta}\|^2 > A = \|\boldsymbol{\alpha}_1\|^2.$$

Thus $\boldsymbol{\beta} \notin S(L_f)$, and so L_f is WR by Corollary 1.3.

For the second statement of the corollary, let A, B be as above and assume that $|B| < A/3$. We first show that any $\beta = \sum_{i=1}^3 c_i\alpha_i$ with at most one $c_i = 0$ satisfies $\|\boldsymbol{\beta}\| > \|\boldsymbol{\alpha}_1\|$. We can assume without loss of generality that $c_3 = 0$, so equation (4) simplifies to

$$\|\boldsymbol{\beta}\|^2 = (c_1^2 + c_2^2)\sum_{i=1}^3 \alpha_i^2 + 2(c_1c_2)\sum_{i<j} \alpha_i\alpha_j. \tag{6}$$

Since $c_1, c_2 \in \mathbb{Z}$ and are both nonzero, let $r = c_2/c_1 \in \mathbb{Q}$ where we suppose $|r| \geq 1$ without loss of generality. Then we can rewrite (6) as

$$\|\boldsymbol{\beta}\|^2 = c_1^2\left((1 + r^2)A + 2rB\right) \geq c_1^2\left((1 + r^2)A - 2|r||B|\right) \geq 2|r|c_1^2(A - |B|), \tag{7}$$

since $1 + r^2 \geq 2|r|$. Additionally, $2|r|c_1^2 = 2|c_1c_2| \geq 2$, and since $|B| < A/3$, we $2(A - |B|) > 4A/3$, so $\|\boldsymbol{\beta}\|^2 > 4A/3 > \|\boldsymbol{\alpha}_1\|^2$.

Next, suppose $\beta = \sum_{i=1}^3 c_i\alpha_i$ with $c_i \neq 0$ for all i. We can assume without loss of generality that $|c_1| \leq |c_2| \leq |c_3|$, so there exists $r, s \in \mathbb{Q}$ with absolute value ≥ 1 such that $c_2 = rc_1$ and $c_3 = sc_1$. With this substitution, (4) becomes

$$\|\boldsymbol{\beta}\|^2 = c_1^2(1 + r^2 + s^2)A + 2c_1^2(r + s + rs)B \tag{8}$$

If at least one of r and s is ≤ 0, then $1 + r^2 + s^2 \geq 2|r + s + rs|$, and so the same argument as above holds. If, on the other hand, both $r, s > 0$, then we still have $1 + r^2 + s^2 \geq |r + s + rs|$, and (8) gives

$$\|\boldsymbol{\beta}\|^2 \geq c_1^2(|r + s + rs|)(A - 2|B|) \geq 3(A - 2|B|) > A = \|\boldsymbol{\alpha}_1\|^2. \tag{9}$$

Putting these observations together, we see that $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \boldsymbol{\alpha}_3$ must be minimal vectors. This completes the proof. □

Inequalities similar to Corollary 1.4 guaranteeing that $\boldsymbol{\alpha}_i$'s are minimal vectors in L_f can potentially be worked out in higher dimensions too, although the arguments become increasingly complicated with the growing dimension. These inequalities are essentially a special case (with the lattices of the special form L_f) of the more general Tammela inequalities [26] (see also Section 2/2 of [24]), which have been worked out in dimensions ≤ 7.

Remark 2.2. Our main tool in this section is Theorem 2.1, which applies only in the case when n is prime. What if n is not prime: are there some conditions to ensure that the conjugates $\alpha_1, \ldots, \alpha_n$ are linearly independent? In general, this is difficult, however there are a couple other observations we can mention. First, if $a_{n-1} \neq 0$ and $\sum_{i=1}^{n} c_i \alpha_i \neq 0$ for any $c_1, \ldots, c_n$ satisfying $\sum_{i=1}^{n} c_i \neq 0$, then $\alpha_1, \ldots, \alpha_n$ are linearly independent, and so L_f has rank n: this is guaranteed by Lemma 2.4 of [12]. Additionally, suppose $n = 2p$ for a prime number p and α_1 is a *Salem number* of degree n (a real algebraic number > 1 with all of its conjugates having absolute value no greater than 1 so that at least one of them has absolute value exactly 1) so that $a_{n-1} \neq 0$, then $\alpha_1, \ldots, \alpha_n$ are again linearly independent, so L_f has rank n: this is guaranteed by Corollary 1.2 of [13].

3. Two-dimensional situation

We start with a useful lemma about minimal norm of a 2-dimensional lattice.

Lemma 3.1. *Let L be a Euclidean lattice of rank 2 with a basis $\boldsymbol{x}, \boldsymbol{y}$. Then*

$$|L| = \min\left\{\|a\boldsymbol{x} + b\boldsymbol{y}\| : a, b \in \{0, 1, -1\}\right\}.$$

Proof. Let θ be the angle between $\boldsymbol{x}$ and $\boldsymbol{y}$. By Lemma 2.1 of [15], if $\theta \in [\pi/3, 2\pi/3]$, then $|L| = \min\{\|\boldsymbol{x}\|, \|\boldsymbol{y}\|\}$. Assume that this is not the case and let $\min\{\|\boldsymbol{x}\|, \|\boldsymbol{y}\|\} = \|\boldsymbol{x}\|$. Then it is easy to check that the angle between $\boldsymbol{x}$ and one of $\pm\boldsymbol{x} \pm \boldsymbol{y}$ satisfies this condition. Since

$$L = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}, \boldsymbol{y}\} = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{x}, \pm\boldsymbol{x} \pm \boldsymbol{y}\}$$

for any choice of $\pm$ signs, the result follows, again by Lemma 2.1 of [15]. □

Let $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ be an irreducible quadratic polynomial with discriminant $D = a_1^2 - 4a_2a_0$, then its roots are

$$\alpha_1 = \frac{-a_1 + \sqrt{D}}{2a_2},\ \alpha_2 = \frac{-a_1 - \sqrt{D}}{2a_2},$$

and the Galois group consists of the identity map σ_1 and the map $\sigma_2 : \sqrt{D} \mapsto -\sqrt{D}$. Consider the lattice $L_f = C_f\mathbb{Z}^2$, where

$$C_f = \begin{pmatrix} \frac{-a_1+\sqrt{D}}{2a_2} & \frac{-a_1-\sqrt{D}}{2a_2} \\ \frac{-a_1-\sqrt{D}}{2a_2} & \frac{-a_1+\sqrt{D}}{2a_2} \end{pmatrix},$$

i.e., $L_f = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2\}$. If $a_1 = 0$, then L_f has rank 1, hence assume $a_1 \neq 0$. Define

$$\beta = \alpha_1 - \alpha_2 = \sqrt{D},\ \gamma = \alpha_1 + \alpha_2 = -a_1 = \operatorname{Tr}_K(\alpha_1),$$

then $\boldsymbol{\beta} = \boldsymbol{\alpha}_1 - \boldsymbol{\alpha}_2 = \begin{pmatrix} \sqrt{D} \\ -\sqrt{D} \end{pmatrix} \in L_f$, $\boldsymbol{\gamma} = \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 = \begin{pmatrix} -a_1 \\ -a_1 \end{pmatrix} \in L_f$. Notice that

$$\|\boldsymbol{\beta}\| = \sqrt{2|D|}, \ \|\boldsymbol{\gamma}\| = \sqrt{2}|a_1|,$$

whereas $\|\boldsymbol{\alpha}_1\| = \|\boldsymbol{\alpha}_2\| = \frac{\sqrt{a_1^2+|D|}}{\sqrt{2}|a_2|}$. Then, by Lemma 3.1,

$$|L_f| = \min\{\|\boldsymbol{\alpha}_1\|, \|\boldsymbol{\beta}|, \|\boldsymbol{\gamma}\|\},$$

since $\|\boldsymbol{\alpha}_1\| = \|\boldsymbol{\alpha}_2\|$.

If $|L_f| = \|\boldsymbol{\gamma}\|$, then $S(L_f) = \{\pm\boldsymbol{\gamma}\}$. Assume then that $|L_f| < \|\boldsymbol{\gamma}\|$, so the conditions of Corollary 1.3 are satisfied. If $|L_f| = \|\boldsymbol{\beta}\|$, then $S(L_f) = \{\pm\boldsymbol{\beta}\}$. Otherwise, $S(L_f) = \{\pm\boldsymbol{\alpha}_1, \pm\boldsymbol{\alpha}_2\}$ and L_f is WR, as guaranteed by Corollary 1.3. All three of these situations are possible. Let us consider some examples.

First, take $f_1(x) = x^2 + x - 2$, then $D = 7$ and

$$L_{f_1} = \begin{pmatrix} \frac{-1+\sqrt{7}}{2} & \frac{-1-\sqrt{7}}{2} \\ \frac{-1-\sqrt{7}}{2} & \frac{-1+\sqrt{7}}{2} \end{pmatrix} \mathbb{Z}^2$$

with $|L_{f_1}| = \|\boldsymbol{\gamma}\| = \sqrt{2}$.

Next, consider $f_2(x) = x^2 + 5x + 5$, then $D = 5$ and

$$L_{f_2} = \begin{pmatrix} \frac{-5+\sqrt{5}}{2} & \frac{-5-\sqrt{5}}{2} \\ \frac{-5-\sqrt{5}}{2} & \frac{-5+\sqrt{5}}{2} \end{pmatrix} \mathbb{Z}^2$$

with $|L_{f_2}| = \|\boldsymbol{\beta}\| = \sqrt{10}$.

Finally, let $f_3(x) = x^2 - 2x - 1$, then $D = 8$ and

$$L_{f_3} = \begin{pmatrix} 1+\sqrt{2} & 1-\sqrt{2} \\ 1-\sqrt{2} & 1+\sqrt{2} \end{pmatrix} \mathbb{Z}^2$$

with $|L_{f_3}| = \|\boldsymbol{\alpha}_1\| = \sqrt{6}$. Thus, L_{f_3} is WR.

More generally, we have the following criterion for planar lattices.

Theorem 3.2. *Given an irreducible quadratic polynomial $f(x) = a_2x^2+a_1x+a_0 \in \mathbb{Z}[x]$ with discriminant $D = a_1^2 - 4a_0a_2$, the corresponding algebraic lattice*

$$L_f = \begin{pmatrix} \frac{-a_1+\sqrt{D}}{2a_2} & \frac{-a_1-\sqrt{D}}{2a_2} \\ \frac{-a_1-\sqrt{D}}{2a_2} & \frac{-a_1+\sqrt{D}}{2a_2} \end{pmatrix} \mathbb{Z}^2$$

is well-rounded if and only if $a_1^2 \geq 2\max\{3a_0a_2, -a_0a_2\}$. If this is the case,

$$S(L_f) = \left\{ \pm \begin{pmatrix} \frac{-a_1+\sqrt{D}}{2a_2} \\ \frac{-a_1-\sqrt{D}}{2a_2} \end{pmatrix}, \pm \begin{pmatrix} \frac{-a_1-\sqrt{D}}{2a_2} \\ \frac{-a_1+\sqrt{D}}{2a_2} \end{pmatrix} \right\}$$

and $\mathrm{Aut}(L_f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with one of the isomorphic copies of $\mathbb{Z}/2\mathbb{Z}$ coming from the Galois action and the other from the $\pm$ signs.

Proof. Let $\alpha_1 = \frac{-a_1+\sqrt{D}}{2a_2}$, $\alpha_2 = \frac{-a_1-\sqrt{D}}{2a_2}$. By Lemma 2.1 of [15], $\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2$ are minimal vectors if and only if the angle the angle θ between them is in the interval $[\pi/3, 2\pi/3]$. A simple calculation shows that

$$\cos\theta = \frac{a_1^2 - |D|}{a_1^2 + |D|}.$$

Hence, we want

$$-1/2 \leq \frac{a_1^2 - |D|}{a_1^2 + |D|} \leq 1/2,$$

meaning that $|D|/3 \leq a_1^2 \leq 3|D|$. Solving these inequalities, we obtain the condition

$$a_1^2 \geq \max\{6a_0a_2, -2a_0a_2\}.$$

Assume this is the case, so the lattice L_f is WR. Let $x_1, x_2 \in \mathbb{Z}$ so $\mathcal{H}_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 \in L_f$. In addition to the identity map, the automorphisms of L_f are given by $\tau_1 : x_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 \mapsto -x_1\boldsymbol{\alpha}_1 - x_2\boldsymbol{\alpha}_2$, the sign change, $\tau_2 : x_1\boldsymbol{\alpha}_1 + x_2\boldsymbol{\alpha}_2 \mapsto x_1\boldsymbol{\alpha}_2 + x_2\boldsymbol{\alpha}_1$, the Galois action, and their composition $\tau_2\tau_2$. These are all elements of order 2 commuting with each other. Hence $\mathrm{Aut}(L_f) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □

4. Pisot lattices

In this section we demonstrate explicit constructions of well-rounded lattices of the form L_f and prove Theorem 1.5. Let K be a number field of degree $d \geq 2$ and $M(K) = M_\infty(K) \cup M_0(K)$ set of places of K, where $M_\infty(K)$ stands for the set of archimedean places and $M_0(K)$ for the set of non-archimedean places. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of K and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be the complex embeddings coming in conjugate pairs, so that $\sigma_{r_1+r_2+j} = \bar{\sigma}_{r_2+j}$ for each $1 \leq j \leq r_2$. Then $d = r_1 + 2r_2$. We can write $M_\infty(K) = \{v_1, \ldots, v_{r_1}, u_1, \ldots, u_{r_2}\}$ and choose representative absolute values as

$$|\alpha|_{v_i} = |\sigma_i(\alpha)|, \ |\alpha|_{u_j} = |\sigma_{r_1+j}(\alpha)|,$$

for each $\alpha \in K$, $1 \leq i \leq r_1$, $1 \leq j \leq r_2$, where $|\ |$ stands for the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$, respectively. We choose the non-archimedean absolute values to extend the corresponding p-adic absolute values on $\mathbb{Q}$. For each place $w \in M(K)$, let $d_w = [K_w : \mathbb{Q}_w]$ be the local degree at w, then for each place $u \in M(\mathbb{Q})$,

$$\sum_{v \in M(K), v|u} d_v = d, \tag{10}$$

and the product formula reads as

$$\prod_{w \in M(K)} |a|_w^{d_w} = 1. \tag{11}$$

From here on, assume that K has at least two archimedean places. Fix an archimedean place $w \in M_\infty(K)$ corresponding to some embedding σ_k and let $\varepsilon > 0$. Then, by Strong Approximation Theorem, there exists $\alpha \in K$ such that

$$|\alpha|_v \leq \varepsilon \ \forall\ v \in M_\infty(K) \setminus \{w\}, \ |\alpha|_v \leq 1 \ \forall\ v \in M_0(K). \tag{12}$$

Notice that the condition $|\alpha|_v \leq 1 \ \forall\ v \in M_0(K)$ is equivalent to $\alpha \in \mathcal{O}_K$. Combining (10), (11) and (12), we obtain

$$|\alpha|_w^{d_w} \geq \frac{1}{\varepsilon^{d-d_w}}. \tag{13}$$

We want to remark that what we are using here is a limited version of Strong Approximation Theorem, which essentially follows from Minkowski's Linear Forms Theorem. For a real number $T \geq 1$, define

$$S_{K,w}(T) = \{\alpha \in \mathcal{O}_K : |\alpha|_v \leq 1 \ \forall\ v \in M_\infty(K) \setminus \{w\}, \ |\alpha|_w \geq T\}. \tag{14}$$

Then (13) implies that $S_{K,w}(T)$ is an infinite set. Indeed, suppose there were only finitely many such α, then let

$$T_0 = \max\{|\alpha|_w : |\alpha|_w \geq T\}.$$

Take $\varepsilon < T_0^{-\frac{d_w}{d-d_w}}$ and take α satisfying (13), then $|\alpha|_w^{d_w} > T_0$, a contradiction.

From here on, let the number field K as above be Galois over $\mathbb{Q}$ of degree $d \geq 3$ and let $3 \leq n \leq d$. Define

$$T_{d,n} = \frac{8d(n-1)}{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)}, \tag{15}$$

and let $\alpha \in S_{K,w}(T_{d,n})$ be of degree n. Let $f_\alpha(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α and let $\alpha_1, \dots, \alpha_n \in \mathcal{O}_K$ be its algebraic conjugates ordered so that $\alpha_k = \sigma_k(\alpha)$. Thus

$$|\alpha|_w = |\alpha_1| \geq T_{d,n},\ |\alpha_2|, \dots, |\alpha_n| \leq 1, \tag{16}$$

where $|\ |$ is the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$. Let $1 \leq m \leq n$ be such that $\alpha_1, \dots, \alpha_m$ are linearly independent over $\mathbb{Q}$. Then $\mathcal{M}_\alpha := \mathrm{span}_{\mathbb{Z}}\{\alpha_1, \dots, \alpha_m\} \subset \mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank m and hence $L_\alpha := \Sigma_K(\mathcal{M}_\alpha) \subset K_{\mathbb{R}}$ is a lattice of rank m.

Proposition 4.1. *For α satisfying* (16)*, the lattice L_α is nearly orthogonal and generic well-rounded. Further, it contains a basis consisting of minimal vectors.*

Proof. For each $1 \leq i \leq m$, the vector $\boldsymbol{\alpha}_i$ has d coordinates, precisely d/n of which are equal to α_1. Further, if $i \neq j$, then $\boldsymbol{\alpha}_i$ and $\boldsymbol{\alpha}_j$ cannot have α_1 in the same coordinate. For the product of two coordinates equal to, say, α_k and α_k, we have $|\alpha_k\alpha_l| \leq 1$, if $k, l \neq 1$; if $k = 1$ and $l \neq 1$, then $|\alpha_k\alpha_l| \leq |\alpha_1|$. This means that

$$|\langle \boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j \rangle| \leq \frac{d}{n}|\alpha_1| + \left(d - \frac{d}{n}\right),$$

whereas $\|\boldsymbol{\alpha}_i\| = \|\boldsymbol{\alpha}_j\| \geq |\alpha_1|$. Putting these observations together, we see that the *coherence* of the pair of vectors $\boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j$, defined as the absolute value of the cosine of the angle between them is given by

$$\frac{|\langle \boldsymbol{\alpha}_i, \boldsymbol{\alpha}_j \rangle|}{\|\boldsymbol{\alpha}_i\|\|\boldsymbol{\alpha}_j\|} \leq \frac{d}{|\alpha_1|} \leq \frac{d}{T_n} = \frac{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)}{8(n-1)} \tag{17}$$

$$\leq \frac{\sqrt{(m-2)^2 + 16(m-1)} - (m-2)}{8(m-1)}. \tag{18}$$

The conclusion now follows by Theorem 1.6 of [15]: while this theorem is stated for a full-rank lattice in $\mathbb{R}^d$, the argument applies verbatim to our situation of L_α being a full-rank lattice in the m-dimensional subspace $\mathrm{span}_{\mathbb{R}} L_\alpha$ of $\mathbb{R}^d$. □

Let us now give explicit examples of lattices as in Proposition 4.1, proving Theorem 1.5. First recall that a *Pisot number* is a real algebraic integer α greater than 1 all of whose algebraic conjugates have modulus strictly smaller than 1. Let F be a real algebraic extension of $\mathbb{Q}$ of degree n. Then F contains infinitely many Pisot numbers of degree n (see Theorem 5.2.2 of [7]). This in particular implies that there are infinitely many Pisot numbers $\alpha \in F$ such that $|\alpha| > T$ for any T. Indeed, if this was not true, then the set

$$\{\alpha \in \mathcal{O}_F : \max_{1 \leq i \leq n} |\sigma_i(\alpha)| \leq T\}$$

would have to be infinite, meaning that the set of points of the lattices $\Sigma_F(\mathcal{O}_F)$ inside of the cube $\{\boldsymbol{x} \in F_{\mathbb{R}} : \max_{1\leq i\leq n} |x_i| \leq T\}$ is infinite. However, the intersection of a discrete set and a compact set has to be finite.

The minimal polynomial of a Pisot number is called a *Pisot polynomial*. Let $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k \in \mathbb{Z}[x]$ be such that

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|. \tag{19}$$

Then Perron's irreducibility criterion [23] guarantees that $f(x)$ is a Pisot polynomial.

Proof of Theorem 1.5. Let the notation be as in the statement of the theorem. Then $d = [K : \mathbb{Q}] \leq n!$ and $f(x)$ is a Pisot polynomial, by (19). Let $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ be the roots of $f(x)$ with α_1 being the corresponding Pisot number. Then

$$|\alpha_1| \geq \prod_{i=1}^{n} |\alpha_i| = |a_0| > T_{d,n},$$

where $T_{d,n}$ is as in (15). Then $L_f = L_{\alpha_1}$ and so it is nearly orthogonal and GWR, by Proposition 4.1. Since $a_{n-1} \neq 0$, Theorem 1.2 implies that L_f has rank n. □

Remark 4.1. Notice, in fact, that Theorem 1.6 of [15] can be applied more generally than just to Pisot polynomials. Indeed, if the maximal coherence of the collection of vectors $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n$ is bounded from above as in (17), then these vectors still form a minimal basis for the corresponding lattice L_f. Consider, for instance, the case $n = d = 3$: then (17) gives the bound of 0.2965..., which is a bit weaker than the bound of $1/3$ coming from part (2) of Corollary 1.4. On the other hand, the bound of (17) works for any n and tends to $1/n$ as $n \to \infty$.

5. Cubic examples

In this section, we provide some explicit examples of WR lattices coming from irreducible cubic polynomials of the form

$$f(x) = x^3 + ax^2 + bx + c \tag{20}$$

The table below provides examples of Pisot polynomials of the form (20).

a, b, c	Galois Group
$\pm 42, 0, \mp 24$	$\mathbb{Z}/3\mathbb{Z}$
$-2, -1, 1$	$\mathbb{Z}/3\mathbb{Z}$
$32, 0, -28$	S_3
$49, 0, 47$	S_3
$-47, 0, 28$	S_3

All of these polynomials satisfy the conditions of Theorem 1.5, thus the corresponding lattices L_f are WR. The Galois group of the polynomial is $\mathbb{Z}/3\mathbb{Z}$ if and only if the discriminant of the polynomial is a square.

Remark 5.1. For our irreducible cubic as above to have Galois group $\mathbb{Z}/3\mathbb{Z}$, it is necessary for $ab < 0$. Indeed, the above polynomial has discriminant $-4a^3b - 27b^2$, and for all roots to be real we require

$$-4a^3b > 27b^2 \geq 0,$$

thus $-4a^3b \geq 0$, so $ab < 0$.

Next, we demonstrate some examples of non-Pisot cubic polynomials of the form (20) with Galois group $\mathbb{Z}/3\mathbb{Z}$.

a, b, c	Roots
$3, -6, 1$	$2.53209, 1.3473, -0.879385$
$5, 6, 1$	$-0.198062, -3.24698, -1.55496$
$-1, -2, 1$	$1.80194, -1.24698, 0.445042$
$-3, 0, 3$	$2.53209, 1.3473, -0.879385$

The fact all of these polynomials have Galois group $\mathbb{Z}/3\mathbb{Z}$ follows from the observation that they have square discriminants, thus we can use Corollary 1.3. In other words, if we show $|L_f| < \sqrt{3}|a_{n-1}|$ and $\sum_{i<j} \alpha_i\alpha_j < \frac{1}{2}\sum_{i=1}^3 \alpha_i^2$, then the lattice is WR by Corollary 1.4. Let us go through the first case as an illustrative example. We have $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 21 < 3\,\mathrm{Tr}(\alpha)^2 = 27$, thus $|L_f| < \sqrt{3}|a_{n-1}|$. Next, $\sum_{i<j} \alpha_i\alpha_j = -6 < 21/2$, so L_f satisfies Corollary 1.4.

6. Determinant

In this section, we obtain determinant formulas for some specific lattices of the form L_f. The first observation is that for a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree n with cyclic Galois group $\mathbb{Z}/n\mathbb{Z}$,

$$\det(L_f) = \prod_{j=1}^{n-1} g(\zeta_n^j),$$

where $g(x) := \alpha + \sigma_1(\alpha)x + \sigma_2(\alpha)x^2 + \cdots + \sigma_{n-1}(\beta)x^{n-1}$ and $\zeta_n = e^{2pi/n}$ is n-th primitive root of unity; this is simply the determinant of the corresponding circulant basis matrix (see, e.g., [21]). We also provide formulas for the determinant in the cases when the Galois group of $f(x)$ is the full symmetric group S_n or the alternating group A_n. We start with two preliminary lemmas.

Lemma 6.1. *Let $f(x)$ be of degree n with roots $\alpha_1, \ldots, \alpha_n$ and Galois group S_n. Let $C_f = (\boldsymbol{\alpha}_1 \ldots \boldsymbol{\alpha}_n)$ be the corresponding $n! \times n$ basis matrix for L_f, then ij-th entry of the Gram matrix $C_f^\top C_f$ is*

$$c_{ij} = \begin{cases} (n-1)!A & i = j \\ 2(n-2)!B & i \neq j, \end{cases}$$

where $A = \sum_{i \leq n} \alpha_i^2$ and $B = \sum_{i<j} \alpha_i\alpha_j$.

Proof. Let $d = n!$ and $\sigma_1, \ldots, \sigma_d$ be the embeddings of K, the splitting field of $f(x)$. Then

$$C_f = \begin{pmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_1(\alpha_n) \\ \vdots & \ldots & \vdots \\ \sigma_d(\alpha_1) & \ldots & \sigma_d(\alpha_n) \end{pmatrix},$$

and so the ij-th entry of this matrix is

$$c_{ij} = \sum_{k \leq d} \sigma_k(\alpha_i\alpha_j).$$

If $i = j$, we have $c_{ii} = (d/n)\sum_{k\leq n}\alpha_k^2$. Consider $i \neq j$. Since $\alpha_i\alpha_j = \alpha_j\alpha_i$, assume that $i < j$, and thus, there are $\frac{n(n-1)}{2}$ possibilities for $\alpha_i\alpha_j$, $i < j \leq n$. Each of these will appear an equal number of times, and since we are summing over $d = n!$ embeddings, each pair appears $n!/\left(\frac{n(n-1)}{2}\right) = 2(n-2)!$ times. □

Lemma 6.2. *Let $f(x)$ be of degree n with roots $\alpha_1, \ldots, \alpha_n$ and Galois group A_n. With the same notation as Lemma 6.1, we have*

$$c_{ij} = \begin{cases} (n-1)!A & i = j \\ (n-2)!B & i \neq j, \end{cases}$$

where $A = \sum_{i\leq n}\alpha_i^2$ and $B = \sum_{i<j}\alpha_i\alpha_j$.

Proof. The argument is the same as in the proof of Lemma 6.1, keeping in mind that $|A_n| = \frac{1}{2}|S_n|$. Also note that A_n contains all even permutations, thus all even products of disjoint two-cycles. □

Remark 6.1. Notice that the argument in the proofs of Lemmas 6.1 and 6.2 above uses the fact that we sum over all possible combinations of $\alpha_i\alpha_j, i < j \leq n$. This means that the Galois group of $f(x)$ must contain all even products of disjoint 2-cycles, so that we can simultaneously send α_i to α_ℓ and α_j to α_m for any $m \neq \ell$. Any subgroup of S_n with this property must contain A_n, thus our argument only works when the Galois group of $f(x)$ is A_n or S_n.

Proposition 6.3. *Let $f(x)$ be of degree n with roots $\alpha_1, \ldots, \alpha_n$ and let $A = \sum_{i\leq n}\alpha_i^2$ and $B = \sum_{i<j}\alpha_i\alpha_j$, as above. If the Galois group of $f(x)$ is S_n, then*

$$\det(L_f) = \left\{((n-2)!)^n(n-1)(A+2B)\left((n-1)A-2B\right)^{n-1}\right\}^{1/2}.$$

If the Galois group of $f(x)$ is A_n, then

$$\det(L_f) = \left\{((n-2)!)^n(n-1)(A+B)\left((n-1)A-B\right)^{n-1}\right\}^{1/2},$$

Proof. Using the notation of Lemmas 6.1 and 6.2, observe that in the case of the symmetric group,

$$\det(L_f) = \sqrt{\det(C_f^\top C_f)} = \left\{(n-2)!^n \det\begin{pmatrix} (n-1)A & \ldots & 2B \\ \vdots & \ddots & \vdots \\ 2B & \ldots & (n-1)A \end{pmatrix}\right\}^{1/2}.$$

Notice that

$$\begin{pmatrix} (n-1)A & \ldots & 2B \\ \vdots & \ddots & \vdots \\ 2B & \ldots & (n-1)A \end{pmatrix} = ((n-1)A-2B)I_n + 2BJ_n,$$

where J_n the all 1's matrix. The matrix $2BJ_n$ has eigenvalues $2nB$ with multiplicity 1 and 0 with multiplicity $n-1$. Adding $((n-1)A-2B)I_n$ shifts the eigenvalues by the same amount, so eigenvalues are $(n-1)A-2B$ with multiplicity $n-1$ and $(n-1)A-2B+2nB = (n-1)(A+2B)$ with multiplicity 1. Then the determinant is obtained by taking the product of these eigenvalues. The argument is the same when the Galois group is A_n with the entries in the matrix above being B instead of $2B$. □

References

[1] C. Alves, J. E. Strapasson and de Araujo, Robson R. On well-rounded lattices and lower bounds for the minimum norm of ideal lattices. *Arch. Math. (Basel)*, 124(2):121–130, 2025.

[2] R. R. de Araujo, A. de Andrade, T. da Nóbrega Neto and J. Bastos. Constructions of well-rounded algebraic lattices over odd prime degree cyclic number fields. *Commun. Math.*, 33(1), Paper No. 6, 18 pp., 2025.

[3] R. R. de Araujo and S. I. R. Costa. Well-rounded algebraic lattices in odd prime dimension. *Arch. Math. (Basel)*, 112(2):139–148, 2019.

[4] R. Baraniuk, S. Dash, and R. Neelamani. On nearly orthogonal lattice bases. *SIAM J. Discrete Math*, 21(1):199–219, 2007.

[5] E. Bayer-Fluckiger. Ideal lattices. *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, 168–184, Cambridge Univ. Press, Cambridge, 2002.

[6] S. C. Batson. The linear transformation that relates the canonical and coefficient embeddings of ideals in cyclotomic integer rings. *Int. J. Number Theory*, 13(9):2277–2297, 2017.

[7] M. J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, J. P. Schreiber. Pisot and Salem numbers. With a preface by David W. Boyd. *Birkhäuser Verlag, Basel,*, xiv+291 pp., 1992

[8] M. T. Damir, A. Karilla, L. Amoros, O. W. Gnilke, D. Karpuk and C. Hollanti. Well-rounded lattices: towards optimal coset codes for Gaussian and fading wiretap channels. *IEEE Trans. Inform. Theory*, 67(6, part 2):3645–3663, 2021.

[9] M. T. Damir and D. Karpuk. Well-rounded twists of ideal lattices from real quadratic fields. *J. Number Theory*, 196:168–196, 2019.

[10] M. T. Damir and G. Mantilla-Soler. Bases of minimal vectors in tame lattices. *Acta Arith.*, 205:265–285, 2022.

[11] A. Dubickas. On the degree of a linear form in conjugates of an algebraic number. *Illinois J. Math.*, 46(2):571–585, 2002.

[12] A. Dubickas and J. Jankauskas. Simple linear relations between conjugate algebraic numbers of low degree. *J. Ramanujan Math. Soc.*, 30(2):219–235, 2015.

[13] A. Dubickas and J. Jankauskas. Linear relations with conjugates of a Salem number. *J. Théor. Nombres Bordeaux*, 32(1):179–191, 2020.

[14] L. Fukshansky and D. Kogan. Cyclic and well-rounded lattices. *Mosc. J. Comb. Number Theory*, 11(1):79–96, 2022.

[15] L. Fukshansky and D. Kogan. On the geometry of nearly orthogonal lattices. *Linear Algebra Appl.*, 629:112–137, 2021.

[16] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun and S. Whitehead. On well-rounded ideal lattices II. *Int. J. Number Theory*, 9(1):139–154, 2013.

[17] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, 8(1):189–206, 2012.

[18] C. Hollanti, G. Mantilla-Soler and N. Miller. Dense generic well-rounded lattices. *SIAM J. Appl. Algebra Geom.*, 9(1):154–185, 2025.

[19] N. H. Le, D. T. Tran and H. T. N. Tran. Well-rounded twists of ideal lattices from imaginary quadratic fields. *J. Algebra Appl.*, 21(7), Paper No. 2250133, 21 pp., 2022.

[20] N. H. Le, D. T. Tran and H. T. N. Tran. Well-rounded ideal lattices of cyclic cubic and quartic fields. *Commun. Math.*, 31(2):209–250., 2023.

[21] D. H. Lehmer. Some properties of circulants. *J. Number Theory*, 5:43–54., 1973.

[22] D. Micciancio and J. Sorrell. Simpler statistically sender private oblivious transfer from ideals of cyclotomic integers. *Advances in cryptology–ASIACRYPT 2020. Part II*, 381–407, Lecture Notes in Comput. Sci., 12492, Springer, Cham, 2020.

[23] O. Perron. Neue Kriterien für die Irreduzibilität algebraischer Gleichungen. *J. Reine Angew. Math.*, 132:288–307, 1907.

[24] A. Schürmann. Computational geometry of positive definite quadratic forms. Polyhedral reduction theories, algorithms, and applications. *University Lecture Series, 48*, American Mathematical Society, Providence, RI, 2009.

[25] A. Srinivasan. A complete classification of well-rounded real quadratic ideal lattices. *J. Number Theory*, 207:349–355, 2020.

[26] P. Tammela. On the reduction theory of positive quadratic forms. *Soviet Math. Dokl.*, 14:651–655, 1973.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711
Email address: lenny@cmc.edu

Department of Mathematics, Pomona College, 610 N. College Ave, Claremont, CA 91711, USA
Email address: eski2022@mymail.pomona.edu