STICKELBERGER'S DISCRIMINANT THEOREM FOR ALGEBRAS

ASHER AUEL, OWEN BIESEL, AND JOHN VOIGHT

Abstract. Stickelberger proved that the discriminant of a number field is congruent to 0 or 1 modulo 4. We generalize this to an arbitrary (not necessarily commutative) ring of finite rank over $\mathbb{Z}$ using techniques from linear algebra. Our proof relies on elementary matrix identities.

1. Introduction

The *discriminant* arises naturally in many situations in mathematics, often as a measure of size or arithmetic complexity. In perhaps its simplest form, we learn that a quadratic equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbb{R}$ has a real root if and only if its discriminant $d := b^2 - 4ac$ is nonnegative. In algebraic number theory, the discriminant of a number field measures ramification of primes [Mar18, Chapters 2–3]; in the theory of differential equations, the discriminant measures the extent to which singular solutions exist.

In this note, we pursue discriminants in the context of rings and with a view toward arithmetic.

Motivation. As motivation, we consider a very simple case: let $d \in \mathbb{Z}$ be a nonsquare and consider the quadratic ring

$$\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}. \tag{1.1}$$

This ring has a natural notion of trace given by

$$\mathrm{Tr}(a + b\sqrt{d}) = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a \in \mathbb{Z}.$$

Of course $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \mathbb{Z}\sqrt{d} \simeq \mathbb{Z}^2$ as abelian groups, and multiplication in $\mathbb{Z}[\sqrt{d}]$ can be written out as

$$(a + b\sqrt{d})(a' + b'\sqrt{d}) = (aa' + bb'd) + (ab' + a'b)\sqrt{d} \tag{1.2}$$

for $a, b, a', b' \in \mathbb{Z}$. The multiplication law (1.2) in $\mathbb{Z}[\sqrt{d}]$ can be given without an embedding into $\mathbb{C}$: on the free abelian group $\mathbb{Z}^2$ with basis $1, e$, there is a unique ring structure satisfying $e^2 = d$. Indeed, by the distributive law, it is enough to remember the products of basis elements, with only the product $e \cdot e$ needing to be specified. Finally, we can recover the discriminant from the *traces* of these products, taking the determinant:

$$\det \begin{pmatrix} \mathrm{Tr}(1 \cdot 1) & \mathrm{Tr}(1 \cdot e) \\ \mathrm{Tr}(e \cdot 1) & \mathrm{Tr}(e \cdot e) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d. \tag{1.3}$$

This calculation agrees with the more familiar notion, since $\sqrt{d}$ is a root of the equation $x^2 - d = 0$ which has discriminant $4d$. In a similar manner, we can define a ring structure for e satisfying $e^2 + be + c = 0$, and we find the discriminant $b^2 - 4c$.

Date: August 20, 2022.

This approach works more generally. Let K be a number field (a finite extension of $\mathbb{Q}$), and let $\mathbb{Z}_K$ be its ring of integers, the subset of K of elements that satisfy a monic polynomial with integer coefficients [Mar18, Chapter 1]. For example, we might take $K = \mathbb{Q}(\sqrt{-1})$, in which case $\mathbb{Z}_K = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Then one can define the discriminant of $\mathbb{Z}_K$ in a similar manner: if $\alpha_1, \dots, \alpha_n$ is an integral basis for $\mathbb{Z}_K$, and $\mathrm{Tr}\colon K \to \mathbb{Q}$ the trace, then we form the $n \times n$-matrix

$$B := (\mathrm{Tr}(\alpha_i \alpha_j))_{i,j=1}^n \in \mathrm{M}_n(\mathbb{Z}) \tag{1.4}$$

and define the discriminant

$$\operatorname{disc} \mathbb{Z}_K := \det B.$$

(See Remark 4.4 for an equivalent definition in the context of Minkowski's *geometry of numbers*.) The matrix B can be interpreted in linear algebraic terms: the bilinear form

$$\begin{aligned} \mathrm{Tr}\colon K \times K &\to \mathbb{Q} \\ (\alpha, \beta) &\mapsto \mathrm{Tr}(\alpha\beta) \end{aligned} \tag{1.5}$$

is symmetric (and nondegenerate), and the matrix B is the *Gram matrix* of this bilinear form in the basis $\alpha_1, \dots, \alpha_n$.

Visibly, for quadratic rings we have $b^2 - 4c \equiv b^2 \equiv 0, 1 \pmod 4$. In fact, this congruence generalizes to all rings of integers, the starting point of our investigation.

Theorem 1.6 (Stickelberger)**.** *We have* $\operatorname{disc} \mathbb{Z}_K \equiv 0, 1 \pmod 4$.

This theorem is called *Stickelberger's discriminant theorem*, among other names. While never stated explicitly in Stickelberger's work [Sti98], this statement can be deduced from the main results. The modern simple proof given by Schur [Sch29] is typically provided as an exercise in an algebraic number theory class (see e.g. Marcus [Mar18, Chapter 2, Exercise 22] or Neukirch [Neu99, Section I.2, Exercise 7]). For further discussion, see Remark 4.4; and for more on this history, see Cox [Cox]. (There is a different, much deeper, theorem of Stickelberger in algebraic number theory that describes the Galois module structure of class groups of cyclotomic fields. For more on this theorem, see Washington [Was82, Chapter 6].) Various generalizations of this congruence have also been made [Mar89, Ber76, Bae81, Har12, BG16].

Generalization. With the motivation to study discriminants as measuring the bilinear form coming from the trace of multiplication, we are now ready to generalize. A ring of rank $n \in \mathbb{Z}_{\geq 1}$ is a ring (with 1), not necessarily commutative, whose underlying additive group is isomorphic to $\mathbb{Z}^n$. Concretely, in a $\mathbb{Z}$-basis $e_1, e_2, \dots, e_n$ for $A \simeq \mathbb{Z}^n$, multiplication is defined by

$$e_i e_k = \sum_{j=1}^n c_{ijk} e_j \tag{1.7}$$

for $i, k = 1, \dots, n$, with $c_{ijk} \in \mathbb{Z}$ (with multiplication extended to A using the distributive law). The n^3 coefficients $(c_{ijk})_{i,j,k=1}^n$ form what is called a multiplication table for A.

Commutative rings of rank n, including rings of integers in number fields, are of considerable interest. For an overview, see Bhargava [Bha06]. However, we do not restrict our work here to the commutative case. Already, the ring $\mathrm{M}_n(\mathbb{Z})$ of $n \times n$-matrices with entries in $\mathbb{Z}$ is a ring of rank n^2, noncommutative for $n \geq 2$.

Other noncommutative examples of rings of rank n abound. Even before J.J. Sylvester coined the term "matrix" in 1848, Sir William Rowan Hamilton had discovered in 1843 the noncommutative algebra of quaternions

$$\mathbb{H} := \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

famously inscribing the equations

$$i^2 = j^2 = k^2 = ijk = -1$$

into the Broom Bridge in Dublin. Fifty years later, Hurwitz [Hur1896] considered the subring of (integral) Hurwitz quaternions

$$\mathcal{O} := \left\{ t + xi + yj + zk \in \mathbb{H} : \begin{array}{c} t, x, y, z \in \frac{1}{2}\mathbb{Z} \text{ and} \\ 2t, 2x, 2y, 2z \in \mathbb{Z} \text{ of the same parity} \end{array} \right\}. \tag{1.8}$$

A $\mathbb{Z}$-basis for $\mathcal{O}$ is given by $1, i, j, \omega$ where $\omega := (-1 + i + j + k)/2$ satisfies the identity $\omega^2 + \omega + 1 = 0$. The ring $\mathcal{O}$ is a noncommutative ring of rank 4; it may be thought of as a noncommutative analogue of the ring of integers of a quadratic field. (For further reading, see Voight [Voi21].)

In fact, *every* ring A of rank n is a subring of $\mathrm{M}_n(\mathbb{Z})$. Explicitly, the coefficients of the multiplication table (1.7) provide a map

$$\begin{aligned} \lambda \colon A &\to \mathrm{M}_n(\mathbb{Z}) \\ e_i &\mapsto (c_{ijk})_{j,k=1,\dots,n} \end{aligned} \tag{1.9}$$

(extended $\mathbb{Z}$-linearly) which defines an injective ring homomorphism. Analogously to the above, we then define the discriminant of A by

$$\mathrm{disc}(A) := \det(B) \tag{1.10}$$

where $B = (b_{ij})_{i,j} \in \mathrm{M}_n(\mathbb{Z})$ is the matrix obtained by taking the trace of pairwise products of basis elements

$$b_{ij} := \mathrm{Tr}(\lambda(e_i e_j)). \tag{1.11}$$

The discriminant $\mathrm{disc}(A)$ does not depend on the basis (see Lemma 2.8).

Example 1.12. Computed using the basis of matrix units, we have $\mathrm{disc}(\mathrm{M}_n(\mathbb{Z})) = (-1)^{n(n-1)/2} n^{n^2}$.

Example 1.13. For the Hurwitz quaternions $\mathcal{O}$ in the basis $1, i, j, \omega$, we have for example

$$\lambda(i) = \begin{pmatrix} 0 & -1 & 1 & 0 \\ 1 & 0 & -1 & -1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 2 & 1 \end{pmatrix}$$

since $ij = k = 1 - i - j + 2\omega$ and $i\omega = -i - j + \omega$. Multiplying matrices and taking traces yields

$$B = \begin{pmatrix} 4 & 0 & 0 & -2 \\ 0 & -4 & 0 & -2 \\ 0 & 0 & -4 & -2 \\ -2 & -2 & -2 & -2 \end{pmatrix}$$

and we find that $\mathrm{disc}(A) = \det(B) = -64$.

Main result. Our main result is a generalization of Stickelberger's theorem to an arbitrary rank n ring.

Theorem 1.14. *If A is a ring of rank n, then* $\operatorname{disc}(A) \equiv 0, 1 \pmod 4$.

We prove this theorem using purely linear algebra techniques (as Theorem 3.1), giving a new proof of Stickelberger's theorem even in the case of the ring of integers of a number field. Moreover, our proof introduces a new invariant of a ring of rank n equipped with a basis β containing 1. We call it the discriminant pfaffian $\operatorname{discpf}(A, \beta) \in \mathbb{Z}$ (see §4), and it satisfies

$$\operatorname{disc}(A) \equiv \operatorname{discpf}(A, \beta)^2 \pmod 4.$$

For a quadratic ring $A := \mathbb{Z}[x]/(x^2 - bx + c)$ we have $\operatorname{discpf}(A, (1, e)) = b$. And in general our discriminant pfaffian extracts a square root of the "square part" of the discriminant modulo 4. The name is motivated by the analogy with the classical pfaffian, the square root of the determinant of a skew-symmetric matrix.

Example 1.15. Let A be a ring of rank 3, with basis $(1, e_2, e_3)$. Let $B = (b_{ij})_{i,j}$. Then $\operatorname{discpf}(A, \beta) = b_{12}b_{13} + b_{23} = \operatorname{Tr}(\lambda(e_2)) \operatorname{Tr}(\lambda(e_3)) + \operatorname{Tr}(\lambda(e_2e_3))$.

Organization. This paper is organized as follows. In Section 2 we set up background and notation. In Section 3 we prove our main result, and then in Section 4 we describe the discriminant pfaffian.

Acknowledgments. The authors would like to thank Darij Grinberg for posing the question [Gri17], for helpful correspondence, and for feedback. The authors are also grateful to the reviewers for their comments. Auel was supported by a Simons Foundation Collaboration Grant (712097), a National Science Foundation Grant (2200845), and a Walter and Constance Burke Research Award. Voight was supported by a Simons Collaboration Grant (550029).

2. Notation

We begin by setting notation, building upon and detailing what was presented in the introduction. Throughout this paper, by a ring we mean a (not necessarily commutative) ring with multiplicative identity 1.

Definition 2.1. Let $n \in \mathbb{Z}_{\geq 1}$. A ring of rank n is a ring that is isomorphic to $\mathbb{Z}^n$ as a $\mathbb{Z}$-module (equivalently, as an abelian group).

Definition 2.2. Let A be a ring of rank n. A basis for A is an ordered n-tuple $\beta = (e_1, \dots, e_n)$ of elements of A that generate A as a $\mathbb{Z}$-module. The multiplication table for A in a basis β is the tuple $(c_{ijk})_{i,j,k}$ of n^3 coefficients $c_{ijk} \in \mathbb{Z}$ defined by

$$e_i e_k = \sum_{j=1}^{n} c_{ijk} e_j. \tag{2.3}$$

A framed ring (A, β) of rank n is a ring A of rank n equipped with a basis β.

Let (A, β) be a framed ring of rank n with $\beta = (e_1, \dots, e_n)$.

Definition 2.4. The matrix of $a \in A$ is $\lambda_\beta(a) = (a_{ij})_{i,j} \in \mathrm{M}_n(\mathbb{Z})$ where

$$ae_j = \sum_{i=1}^{n} a_{ij} e_i.$$

The following lemma follows from a direct verification.

Lemma 2.5. *The matrix map*

$$\lambda_\beta \colon A \hookrightarrow \mathrm{M}_n(\mathbb{Z})$$

defines an injective ring homomorphism, and the map

$$\begin{aligned} t_\beta \colon A \times A &\to \mathbb{Z} \\ (a, b) &\mapsto \mathrm{Tr}(\lambda_\beta(ab)) \end{aligned} \tag{2.6}$$

defines a symmetric, bilinear pairing on A.

The matrix (or "left multiplication") map λ_β is called the left regular representation of A. Indeed, on basis elements we have $\lambda_\beta(e_i)$ defined by the entries of the multiplication table as in (1.9). We call the map t_β the trace pairing on A.

Definition 2.7. The Gram matrix of (A, β) is the (symmetric) matrix $B = B(A, \beta)$ defined by

$$(t_\beta(e_i, e_j))_{i,j=1,\dots,n} = \begin{pmatrix} t_\beta(e_1, e_1) & t_\beta(e_1, e_2) & \dots & t_\beta(e_1, e_n) \\ t_\beta(e_2, e_1) & t_\beta(e_2, e_2) & \dots & t_\beta(e_2, e_n) \\ \vdots & \vdots & \ddots & \vdots \\ t_\beta(e_n, e_1) & t_\beta(e_n, e_2) & \dots & t_\beta(e_n, e_n) \end{pmatrix}.$$

Thus the Gram matrix of (A, β) is defined to be the classical Gram matrix of the trace form t_β. The discriminant of A (with respect to β) is

$$\mathrm{disc}(A, \beta) := \det(B).$$

Lemma 2.8. *The trace pairing $t = t_\beta$ and the discriminant* $\mathrm{disc}(A) = \mathrm{disc}(A, \beta)$ *are well-defined, independent of the choice of basis β.*

Proof. Let $Q = [\mathrm{id}]_\beta^{\beta'} \in \mathrm{GL}_n(\mathbb{Z})$ be a change of basis from β to β'. Then $\lambda_{\beta'}(a) = Q\lambda_\beta(a)Q^{-1}$ so $\mathrm{Tr}(\lambda_{\beta'}(a)) = \mathrm{Tr}(\lambda_\beta(a))$ for all $a \in A$, hence t is independent of the choice of basis. Correspondingly, we have $B(A, \beta') = Q^{\mathsf{T}} B(A, \beta) Q$, hence

$$\det(B(A, \beta')) = \det(Q)^2 \det(B(A, \beta)) = \det(B(A, \beta)) \tag{2.9}$$

since $\det(Q) \in \{\pm 1\}$. □

Remark 2.10. Strictly speaking, our definition of discriminant depends on the choice of representation λ. One could also consider the right regular representation or indeed any faithful matrix representation of A. Although these need not give the same answers, the proof below shows that they all satisfy a discriminant congruence.

It will turn out to be crucial to our arguments in the next section to have 1 as the first element of a basis.

Definition 2.11. A unital basis for A is a basis $\beta = (e_1, \dots, e_n)$ with $e_1 = 1$, and a unitally framed ring of rank n (A, β) is a ring A of rank n equipped with a unital basis β.

Proposition 2.12. *Every ring of rank n has a unital basis.*

Proof. Let A be a ring of rank n and let $\beta = (e_1, \dots, e_n)$ be a (not necessarily unital) basis for A. Then $1 = a_1 e_1 + \cdots + a_n e_n$ with $a_1, \dots, a_n \in \mathbb{Z}$.

We first claim that $\gcd(a_1, \dots, a_n) = 1$. Indeed, using the multiplication table, we have

$$e_1 = e_1 \cdot 1 = \sum_{k=1}^{n} a_k e_1 e_k = \sum_{k=1}^{n} a_k \left(\sum_{j=1}^{n} c_{1jk} e_j \right) = \sum_{j=1}^{n} \left(\sum_{k=1}^{n} a_k c_{1jk} \right) e_j. \tag{2.13}$$

Since β is a basis, by the coefficient of e_1 we have $1 = \sum_{k=1}^{n} a_k c_{11k}$. We conclude that $\gcd(a_1, \dots, a_n) = 1$.

Consider the row vector $a := (a_1, \dots, a_n)$. We claim that there exists (invertible) $Q \in \mathrm{GL}_n(\mathbb{Z})$ such that $aQ = (1, 0, \dots, 0)$. Although the proof of this claim can be found in many places, we give an argument here in order to be self-contained. We proceed by induction. The base case $n = 1$ is immediate. In general, by the extended Euclidean algorithm (Bézout relation), there exist $x_{n-1}, x_n \in \mathbb{Z}$ such that $a_{n-1}x_{n-1} + a_n x_n = g := \gcd(a_{n-1}, a_n)$. Let

$$P := \begin{pmatrix} x_{n-1} & -a_n/g \\ x_n & a_{n-1}/g \end{pmatrix};$$

then $\det(P) = 1$ so $P \in \mathrm{SL}_2(\mathbb{Z})$, and the block matrix $\begin{pmatrix} I & 0 \\ 0 & P \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z})$ has

$$(a_1, \dots, a_{n-1}, a_n) \begin{pmatrix} I & 0 \\ 0 & P \end{pmatrix} = (a_1, \dots, a_{n-2}, g, 0) \tag{2.14}$$

still with $\gcd(a_1, \dots, g) = \gcd(a_1, \dots, a_{n-1}, a_n) = 1$. Therefore by induction, there exists $Q \in \mathrm{GL}_{n-1}(\mathbb{Z})$ such that $(a_1, \dots, g)Q = (1, 0, \dots, 0)$, so multiplying (2.14) by $\begin{pmatrix} Q & 0 \\ 0 & 1 \end{pmatrix}$ gives the result.

From the claim, we have $aQ = (1, 0, \dots, 0)$ and so the first row of the inverse $Q^{-1} \in \mathrm{GL}_n(\mathbb{Z})$ is indeed $(a_1, \dots, a_n)$. Now consider the change of basis of A provided by Q^{-1}: write $Q^{-1} = (q_{ij})_{i,j=1}^{n}$ and let $f_i := \sum_{j=1}^{n} q_{ij} e_j$ for $i = 1, \dots, n$. Then $f_1 = 1$, and so the elements f_i form a unital basis for A, as desired. □

The next lemma, which follows an observation by Darij Grinberg, is proved by direct computation.

Lemma 2.15. *The product $\mathbb{Z} \times A$ is a ring of rank $n + 1$ with basis*

$$\beta' = ((1, e_1), (0, e_1), \dots, (0, e_n));$$

β' is unital if β is unital; and $\mathrm{disc}(\mathbb{Z} \times A, \beta') = \mathrm{disc}(A, \beta)$.

3. Stickelberger's discriminant theorem

In this section, we prove our main theorem, restated here for convenience.

Theorem 3.1. *Let A be a ring of rank n. Then* $\mathrm{disc}(A) \equiv 0, 1 \pmod 4$.

The outline of the proof is as follows. First, we study the properties of the Gram matrix of A, noting it has a certain property relating the first row and column to the diagonal; we call such Gram matrices *tracelike*, and we prove the congruence more generally for tracelike

matrices. Second, we transform the symmetric matrix to one with even diagonal; from there, we *expand by the adjugate* to establish the congruence.

Tracelike Gram matrices. As a first step, consider the following well-known lemma. We give a quick proof, to provide motivation and for completeness.

Lemma 3.2. *We have* $\mathrm{Tr}(M^2) \equiv \mathrm{Tr}(M)^2 \pmod 2$ *for all* $M \in \mathrm{M}_n(\mathbb{Z})$.

Proof. Let $M = (m_{ij})_{i,j=1}^n$. Then

$$\mathrm{Tr}(M)^2 = \left(\sum_{i=1}^n m_{ii}\right)^2 = \sum_{i=1}^n m_{ii}^2 + 2\sum_{1\le i<j\le n} m_{ii}m_{jj},$$

whereas

$$\begin{aligned}\mathrm{Tr}(M^2) = \mathrm{Tr}\left(\sum_{j=1}^n m_{ij}m_{jk}\right)_{i,k=1}^n &= \sum_{i=1}^n\sum_{j=1}^n m_{ij}m_{ji} \\ &= \sum_{i=1}^n m_{ii}^2 + 2\sum_{1\le i<j\le n} m_{ij}m_{ji}.\end{aligned}$$

So modulo 2, both sums are congruent to $\sum_{i=1}^n m_{ii}^2$. □

In particular, Lemma 3.2 applies to the entries of the Gram matrices considered in the previous section (Definition 2.7).

Corollary 3.3. *Let A be a ring of rank n, let $\beta = (e_1, \dots, e_n)$ be a unital basis for A, and let $B(A,\beta) = (b_{ij})_{i,j}$ be the Gram matrix of (A,β). Then $b_{11} = n$ and $b_{ii} \equiv b_{1i}^2 \pmod 2$ for $i = 2, \dots, n$.*

Proof. Since β is a unital basis we have $e_1 = 1$ so for all $i = 1, \dots, n$ we have

$$b_{1i} = t(e_1, e_i) = \mathrm{Tr}(\lambda_\beta(e_i)). \tag{3.4}$$

Taking $i = 1$ in (3.4) we get $b_{11} = \mathrm{Tr}(I) = n$, where $I \in \mathrm{M}_n(\mathbb{Z})$ is the identity matrix. For $i = 2, \dots, n$, applying Lemma 3.2 and (3.4) gives

$$b_{ii} = \mathrm{Tr}(\lambda_\beta(e_i)^2) \equiv \mathrm{Tr}(\lambda_\beta(e_i))^2 = b_{1i}^2 \pmod 2.$$ □

Corollary 3.3 isolates the key property that implies our desired congruence. Accordingly, we make the following definition.

Definition 3.5. A symmetric matrix $B = (b_{ij})_{i,j} \in \mathrm{M}_n(\mathbb{Z})$ is tracelike if $b_{11} = n$ and $b_{ii} \equiv b_{1i}^2 \pmod 2$ for all $i = 2, \dots, n$.

The Gram matrix $B(A,\beta)$ of any framed ring (A,β) of rank n is a tracelike matrix by Corollary 3.3.

Question 3.6. Is every tracelike matrix the Gram matrix of an algebra in a unital basis?

Symmetrizing. We now proceed to study determinants of tracelike matrices. Our proof consists first of a row reduction step to obtain a symmetric matrix with even diagonal; then we prove such matrices satisfy the desired congruence. From now on, let $B = (b_{ij})_{i,j} \in \mathrm{M}_n(\mathbb{Z})$ be a tracelike matrix.

Lemma 3.7. *Let $B = (b_{ij})_{i,j} \in \mathrm{M}_n(\mathbb{Z})$ be a tracelike matrix. Suppose that $4 \mid n$, and for $i = 2, \dots, n$ let $c_i \in \mathbb{Z}$ be such that $b_{ii} = b_{1i}^2 + 2c_i$. Let*

$$C := \begin{pmatrix} n & b_{12} & b_{13} & \dots & b_{1n} \\ b_{12} & 2c_2 & b_{23} - b_{12}b_{13} & \dots & b_{2n} - b_{12}b_{1n} \\ b_{13} & b_{23} - b_{12}b_{13} & 2c_3 & \dots & b_{3n} - b_{13}b_{1n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{1n} & b_{2n} - b_{12}b_{1n} & b_{3n} - b_{13}b_{1n} & \dots & 2c_n \end{pmatrix} \in \mathrm{M}_n(\mathbb{Z}).$$

Then C is a symmetric matrix with diagonal entries in $2\mathbb{Z}$ and $\det(B) \equiv \det(C) \pmod 4$.

Proof. We begin with

$$B = \begin{pmatrix} n & b_{12} & b_{13} & \dots & b_{1n} \\ b_{12} & b_{12}^2 + 2c_2 & b_{23} & \dots & b_{2n} \\ b_{13} & b_{23} & b_{13}^2 + 2c_3 & \dots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{1n} & b_{2n} & b_{3n} & \dots & b_{1n}^2 + 2c_n \end{pmatrix}.$$

Subtracting b_{12} times the first row from the second, and b_{13} times the first row from the third, and so on, we preserve the determinant:

$$\det(B) = \det \begin{pmatrix} n & b_{12} & b_{13} & \dots & b_{1n} \\ (1-n)b_{12} & 2c_2 & b_{23} - b_{12}b_{13} & \dots & b_{2n} - b_{12}b_{1n} \\ (1-n)b_{13} & b_{23} - b_{12}b_{13} & 2c_3 & \dots & b_{3n} - b_{13}b_{1n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (1-n)b_{1n} & b_{2n} - b_{12}b_{1n} & b_{3n} - b_{13}b_{1n} & \dots & 2c_n \end{pmatrix}.$$

The result now follows since $4 \mid n$ so $1 - n \equiv 1 \pmod 4$. □

Expanding by adjugate. Recall that the adjugate of $A \in \mathrm{M}_n(\mathbb{Z})$ is the transpose of the matrix of the cofactors of A, defined by

$$\operatorname{adj}(A) := \left((-1)^{i+j} \det(A'_{ji})\right)_{i,j=1}^{n}, \tag{3.8}$$

where $A'_{ij} \in \mathrm{M}_{n-1}(\mathbb{Z})$ is the submatrix of A obtained by removing the ith row and jth column. We have

$$A \operatorname{adj}(A) = \operatorname{adj}(A)A = \det(A)I \tag{3.9}$$

as well as $\operatorname{adj}(A^{\mathsf{T}}) = \operatorname{adj}(A)^{\mathsf{T}}$ and $\operatorname{adj}(cA) = c^{n-1} \operatorname{adj}(A)$ for $c \in \mathbb{Z}$.

Proposition 3.10. *Let $M, Q \in \mathrm{M}_n(\mathbb{Z})$. Then*

$$\det(M + 2Q) \equiv \det(M) + 2 \operatorname{Tr}(\operatorname{adj}(M)Q) \pmod 4.$$

Proof. Write $M = (m_{ij})_{i,j=1}^n$ and $Q = (q_{ij})_{i,j=1}^n$. We begin with the expansion

$$\det(M + 2Q) = \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) \prod_{i=1}^n (m_{i\sigma(i)} + 2q_{i\sigma(i)}) \tag{3.11}$$

where S_n is the symmetric group of degree n. Expanding out the right-hand side modulo 4, for each $\sigma \in S_n$ we have

$$\prod_{i=1}^n (m_{i\sigma(i)} + 2q_{i\sigma(i)}) \equiv \prod_{i=1}^n m_{i\sigma(i)} + 2 \sum_{j=1}^n q_{j\sigma(j)} \prod_{\substack{i=1 \\ i \neq j}}^n m_{i\sigma(i)} \pmod 4. \tag{3.12}$$

Combining (3.11)–(3.12) and interchanging summations gives

$$\det(M + 2Q) \equiv \sum_{\sigma \in S_n} (\operatorname{sgn} \sigma) \prod_{i=1}^n m_{i\sigma(i)} + 2 \sum_{j=1}^n \sum_{\sigma \in S_n} q_{j\sigma(j)} \prod_{\substack{i=1 \\ i \neq j}}^n m_{i\sigma(i)} \pmod 4, \tag{3.13}$$

ignoring signs as we work with an even integer modulo 4. The first term is of course $\det(M)$. For the second sum, for all j, k we have

$$\det(M'_{jk}) = \pm \sum_{\substack{\sigma \in S_n \\ \sigma(j) = k}} (\operatorname{sgn} \sigma) \prod_{\substack{i=1 \\ i \neq j}}^n m_{i\sigma(i)}. \tag{3.14}$$

Reorganizing the sum, working modulo 2 so we may ignore signs, we obtain

$$\begin{aligned} \sum_{j=1}^n \sum_{\sigma \in S_n} q_{j\sigma(j)} \prod_{\substack{i=1 \\ i \neq j}}^n m_{i\sigma(i)} &\equiv \sum_{j=1}^n \sum_{k=1}^n \sum_{\substack{\sigma \in S_n \\ \sigma(j) = k}} q_{jk} \prod_{\substack{i=1 \\ i \neq j}}^n m_{i\sigma(i)} \equiv \sum_{j=1}^n \sum_{k=1}^n q_{jk} \det(M'_{jk}) \\ &\equiv \sum_{j=1}^n \sum_{k=1}^n q_{jk} \operatorname{adj}(M)_{kj} \equiv \operatorname{Tr}(Q \operatorname{adj}(M)) \pmod 2. \end{aligned} \tag{3.15}$$

Plugging (3.15) into (3.13) then gives the result. □

Second proof of Proposition 3.10. We extend our scope to real matrices and show that the identity holds when M is invertible, and then for all matrices. Let $M, Q \in \mathrm{M}_n(\mathbb{R})$.

First, using an indeterminate x we have

$$\det(M + xQ) = c_0(M, Q) + c_1(M, Q)x + \cdots + c_n(M, Q)x^n \in \mathbb{R}[x].$$

For example, plugging in $x = 0$ gives $c_0(M, Q) = \det(M)$ for all M, Q. Moreover, $\det(I - xQ)$ is the reverse characteristic polynomial of Q, so $c_1(I, Q) = -\operatorname{Tr}(Q)$. We define the map

$$\begin{aligned} \mathrm{M}_n(\mathbb{R}) \times \mathrm{M}_n(\mathbb{R}) &\to \mathbb{R} \\ (M, Q) &\mapsto c_1(M, Q). \end{aligned} \tag{3.16}$$

Next, if $M \in \mathrm{GL}_n(\mathbb{R})$ is invertible, we have

$$\begin{aligned} \det(M + xQ) &= \det(M) \det(I + xM^{-1}Q) \\ &= \det(M)(1 - \operatorname{Tr}(M^{-1}Q)x + h_{M,Q}(x)) \\ &= \det(M) - \operatorname{Tr}(\operatorname{adj}(M)Q)x + \det(M)x^2 h_{M,Q}(x) \end{aligned} \tag{3.17}$$

for some $h_{M,Q}(x) \in \mathbb{R}[x]$, using (3.9) which gives $\operatorname{adj}(M) = \det(M)M^{-1}$. Thus $c_1(M,Q) = -\operatorname{Tr}(\operatorname{adj}(M)Q)$ for the set of matrices $M \in \mathrm{GL}_n(\mathbb{R})$ which are dense with respect to the usual topology on $\mathrm{M}_n(\mathbb{R}) \simeq \mathbb{R}^{n^2}$.

Finally, the function $c_1(M,Q)$ is a polynomial in the entries of M, Q (as M, Q range over $\mathrm{M}_n(\mathbb{R})$) so continuous in these entries; the same is true for $-\operatorname{Tr}(\operatorname{adj}(M)Q)$. We just showed these functions are equal whenever $\det(M) \neq 0$, so in fact they must equal for all M, Q. Restricting back to $M, Q \in \mathrm{M}_n(\mathbb{Z})$, we have

$$\begin{aligned}\det(M + xQ) = \det(M) - \operatorname{Tr}(\operatorname{adj}(M)Q)x \\ + c_2(M,Q)x^2 + \cdots + c_n(M,Q)x^n \in \mathbb{Z}[x],\end{aligned} \tag{3.18}$$

the resulting polynomial visibly having integer coefficients. Plugging in $x = 2$ into (3.18) then gives the result. □

Remark 3.19. Many linear algebra statements can be proven in the same manner as the second proof, using the method of *universal polynomials*, where the entries of the matrices are left as indeterminates. If instead of a congruence, once wishes to prove an equality, then it is enough to do so over the field $\mathbb{Q}(x_{ij})_{i,j}$, where now the determinant is a nonzero polynomial, so invertible. For example, the Cayley–Hamilton theorem may be proven this way.

Determinants of even symmetric matrices. We are now ready for the second key step in the proof. We will use the fact that the determinant of every skew-symmetric matrix A has a canonical square root called its pfaffian $\operatorname{pf}(A)$; see, for example, Stembridge [Ste90, Proposition 2.2].

Proposition 3.20. *Let $C \in \mathrm{M}_n(\mathbb{Z})$ be a symmetric matrix with diagonal entries in $2\mathbb{Z}$. Suppose $4 \mid n$, and let U be the matrix obtained from the upper-triangular part of C and half its diagonal. Then $C = U + U^{\mathsf{T}}$ and*

$$\det(C) \equiv \det(U - U^{\mathsf{T}}) = \operatorname{pf}(U - U^{\mathsf{T}})^2 \equiv 0, 1 \pmod 4.$$

For this proposition, we need a lemma.

Lemma 3.21. *Let $M \in \mathrm{M}_n(\mathbb{Z})$ with $2 \mid n$. Then*

$$2\operatorname{Tr}(\operatorname{adj}(M - M^{\mathsf{T}})M^{\mathsf{T}}) = -n\det(M - M^{\mathsf{T}}).$$

Proof. Let $r := \operatorname{Tr}(\operatorname{adj}(M - M^{\mathsf{T}})M^{\mathsf{T}})$. Taking the transpose and recalling the properties of the adjugate,

$$\begin{aligned}r &= \operatorname{Tr}(M(\operatorname{adj}(M - M^{\mathsf{T}}))^{\mathsf{T}}) = \operatorname{Tr}(M\operatorname{adj}(M^{\mathsf{T}} - M)) \\ &= \operatorname{Tr}(M(-1)^{n-1}\operatorname{adj}(M - M^{\mathsf{T}})) = -\operatorname{Tr}(\operatorname{adj}(M - M^{\mathsf{T}})M).\end{aligned} \tag{3.22}$$

Adding back r, by linearity of trace we have

$$\begin{aligned}2r &= \operatorname{Tr}(\operatorname{adj}(M - M^{\mathsf{T}})M^{\mathsf{T}}) - \operatorname{Tr}(\operatorname{adj}(M - M^{\mathsf{T}})M) \\ &= \operatorname{Tr}(\operatorname{adj}(M - M^{\mathsf{T}})(M^{\mathsf{T}} - M)) = \operatorname{Tr}(-\det(M - M^{\mathsf{T}})I) \\ &= -n\det(M - M^{\mathsf{T}})\end{aligned}$$

proving the claim. □

Proof of Proposition 3.20. We have $C = U + U^{\mathsf{T}} = (U - U^{\mathsf{T}}) + 2U^{\mathsf{T}}$. By Proposition 3.10, we have

$$\det(C) \equiv \det(U - U^{\mathsf{T}}) + 2\operatorname{Tr}(\operatorname{adj}(U - U^{\mathsf{T}})U^{\mathsf{T}}) \pmod 4. \tag{3.23}$$

Since $U - U^{\mathsf{T}}$ is a skew-symmetric matrix, we have

$$\det(U - U^{\mathsf{T}}) = \operatorname{pf}(U - U^{\mathsf{T}})^2 \equiv 0, 1 \pmod 4.$$

By Lemma 3.21 we have

$$2\operatorname{Tr}(\operatorname{adj}(U - U^{\mathsf{T}})U^{\mathsf{T}}) \equiv 0 \pmod 4 \tag{3.24}$$

and the result follows. □

Remark 3.25. The hypothesis $4 \mid n$ in Proposition 3.20 is necessary. Indeed, for $n = 1$ we could take $\det\begin{pmatrix}2\end{pmatrix} = 2$, for $n = 2$ we could take $\det\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = -1$, and for $n = 3$ we could take the block matrix obtained from these two.

Proof conclusion. With these ingredients in hand, we now prove our main theorem.

Proof of Theorem 3.1. Let A be a ring of rank n. Replacing A by $A \times \mathbb{Z}^r$ if necessary, by Lemma 2.15 we may suppose without loss of generality that $4 \mid n$. By Proposition 2.12, A has a unital basis β, so by Corollary 3.3, the Gram matrix $B = B(A, \beta)$ is tracelike. Then by Lemma 3.7, there exists a symmetric matrix C with even diagonal such that $\det(B) \equiv \det(C) \pmod 4$. Putting these together and applying Proposition 3.20:

$$\operatorname{disc}(A) = \det(B) \equiv \det(C) \equiv 0, 1 \pmod 4$$

as desired. □

Generalizations. The proof of our main result used just techniques from linear algebra. Accordingly, it immediately generalizes to a wider context, allowing an arbitrary commutative base ring.

Let R be a commutative ring (with 1). An R-algebra is a ring A (with 1), not necessarily commutative, equipped with a ring homomorphism $R \to A$ whose image lies in the center of A. For the R-algebras considered in this section, we will suppose that the map $R \hookrightarrow A$ is injective, so that we may identify R with its image $R1 \subseteq A$. An R-algebra A is free of rank n if $A \simeq R^n$ as R-modules, i.e., A has an R-basis $\beta = (e_1, \dots, e_n)$.

The rest of the definitions and results in Section 2 generalize, with only two adjustments. First, in contrast to Lemma 2.8, we only obtain a well-defined discriminant $\operatorname{disc} A \in R/R^{\times 2}$, the set of elements of R up to squares of units in R, as $\det(\mathrm{GL}_n(R)) = R^\times$. Second, in contrast to Proposition 2.12, we do not know whether unital bases exist for an arbitrary free R-algebra. However, we may always reduce to working with a unitally framed algebra by invoking the following, which is a direct generalization of Lemma 2.15.

Lemma 3.26. *If (A, β) is a framed R-algebra of rank n with $\beta = (e_1, \dots, e_n)$, then $A' := R \times A$ has a unital framing*

$$\beta' = ((1, 1), (0, e_1), \dots, (0, e_n)). \tag{3.27}$$

Furthermore, we have $\operatorname{disc}(R \times A, \beta') = \operatorname{disc}(A, \beta)$ *in* $R/R^{\times 2}$.

With these in mind, the same proof gives the following theorem.

Theorem 3.28. *Let R be a commutative ring and let A be a free R-algebra of rank n. Then*

$$\operatorname{disc}(A, \beta) \equiv \operatorname{discpf}(A', \beta')^2 \pmod 4$$

where $A' = R \times A$ and β' is as in (3.27).

Remark 3.29. We can also go a bit farther, arguing *locally*. An R-module M is said to have some property (Zariski-)locally if there exist $r_1, \dots, r_m \in R$ generating the unit ideal R such that the localization $M[r_i^{-1}]$ has that property as an $R[r_i^{-1}]$-module for all $i = 1, \dots, m$. In particular, we can speak of an R-module M being locally free of rank n. The same arguments then show that if R is a commutative ring and A is an R-algebra that is locally free of rank n as an R-module, then $\operatorname{disc}(A)$ is locally a square modulo 4.

4. Discriminant pfaffian

In this section, we refine the result of the previous section by giving an explicit, combinatorial expression for our "square root modulo 4" obtained from pfaffians.

To begin, recall that a perfect matching P on a set J is a partition of J into subsets of cardinality 2.

Definition 4.1. Let $B = (b_{ij})_{i,j} \in \mathrm{M}_n(\mathbb{Z})$ be tracelike. Define the discriminant pfaffian of B by

$$\operatorname{discpf}(B) := \sum_{\substack{J \subseteq \{2,\dots,n\} \\ \#J \text{ even}}} \sum_{\substack{\text{perfect} \\ \text{matchings} \\ P \text{ on } J}} \left(\prod_{\{i,j\} \in P} b_{ij} \right) \left(\prod_{k \in \{2,\dots,n\} \smallsetminus J} b_{1k} \right).$$

(If $P = \emptyset$, by convention the empty product is defined to be 1.)

If (A, β) is a unitally framed ring of rank n, define its discriminant pfaffian by

$$\operatorname{discpf}(A, \beta) = \operatorname{discpf}(B(A, \beta)).$$

The value of $\operatorname{discpf}(B)$ for the first few values of n are as follows:

n	$\operatorname{discpf}(B)$
1	1
2	b_{12}
3	$b_{12}b_{13} + b_{23}$
4	$b_{12}b_{13}b_{14} + b_{23}b_{14} + b_{24}b_{13} + b_{34}b_{12}$

In general the number of terms in $\operatorname{discpf}(A, \beta)$ is given by the number of involutions on a set of $n-1$ letters [OEIS, Sequence A000085].

Theorem 4.2. *Let $B \in \mathrm{M}_n(\mathbb{Z})$ be tracelike. Then* $\det(B) \equiv \operatorname{discpf}(B)^2 \pmod 4$.

Example 4.3. For example, if $n = 2$ we have

$$B = \begin{pmatrix} 2 & b_{12} \\ b_{12} & b_{12}^2 + 2c_2 \end{pmatrix}$$

for some $c_2 \in \mathbb{Z}$, so

$$\det B = 2b_{12}^2 + 4c_2 - b_{12}^2 \equiv b_{12}^2 = \operatorname{discpf}(B)^2 \pmod 4.$$

Before proceeding with the proof, we motivate the discriminant pfaffian using the modern proof of Stickelberger's theorem.

Remark 4.4. Let K be a number field with ring of integers $\mathbb{Z}_K$ and integral basis $\alpha_1, \dots, \alpha_n$. Letting $\sigma_1, \dots, \sigma_n \colon K \hookrightarrow \mathbb{C}$ be the distinct embeddings of K into $\mathbb{C}$, we consider the $n \times n$ matrix of complex numbers $E := (\sigma_i(\alpha_j))_{i,j}$. Then $B = E^{\mathsf{T}}E$ (see Marcus [Mar18, Theorem 6]) and so $\operatorname{disc} \mathbb{Z}_K = \det(B) = \det(E)^2$. (The definition in (1.4) has the virtue that it expresses the discriminant as the determinant of a matrix of integers.)

Letting P and N be the sum of terms in the expansion of $\det(E)$ involving even and odd permutations, respectively, the standard proof of Stickelberger's discriminant theorem is to write

$$\operatorname{disc} \mathbb{Z}_K = \det(\sigma_i(\alpha_j))_{i,j}^2 = (P-N)^2 = (P+N)^2 - 4PN; \tag{4.5}$$

by construction, the elements $P+N, PN$ are algebraic integers, and by Galois theory they belong to $\mathbb{Q}$, hence $P+N, PN \in \mathbb{Z}$ and the result follows. With this in mind, a natural square root of the discriminant modulo 4 is $P+N$, which is equal to the *permanent* of the matrix E. This permanent agrees with the discriminant pfaffian modulo 2 by Theorem 4.2.

Proof of Theorem 4.2. We first consider the case that $4 \mid n$. Combining Lemma 3.7 and Proposition 3.20, we have

$$\det(B) \equiv \operatorname{pf}(U - U^{\mathsf{T}})^2 \pmod 4 \tag{4.6}$$

where

$$U - U^{\mathsf{T}} = \begin{pmatrix} 0 & b_{12} & b_{13} & \dots & b_{1n} \\ -b_{12} & 0 & b_{23} - b_{12}b_{13} & \dots & b_{2n} - b_{12}b_{1n} \\ -b_{13} & -(b_{23} - b_{12}b_{13}) & 0 & \dots & b_{3n} - b_{13}b_{1n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -b_{1n} & -(b_{2n} - b_{12}b_{2n}) & -(b_{3n} - b_{13}b_{1n}) & \dots & 0 \end{pmatrix}. \tag{4.7}$$

Since $x \equiv y \pmod 2$ implies $x^2 \equiv y^2 \pmod 4$ for all $x, y \in \mathbb{Z}$, it suffices to show that

$$\operatorname{discpf}(B) \equiv \operatorname{pf}(U - U^{\mathsf{T}}) \equiv \operatorname{pf}(U + U^{\mathsf{T}}) \pmod 2. \tag{4.8}$$

In particular, we can ignore signs throughout.

To prove (4.8), we write $U - U^{\mathsf{T}} \equiv B' + B'' \pmod 2$ where

$$B' := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & b_{23} & \dots & b_{2n} \\ 0 & b_{23} & 0 & \dots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & b_{2n} & b_{3n} & \dots & 0 \end{pmatrix}$$

$$B'' := \begin{pmatrix} 0 & b_{12} & b_{13} & \dots & b_{1n} \\ b_{12} & 0 & b_{12}b_{13} & \dots & b_{12}b_{1n} \\ b_{13} & b_{12}b_{13} & 0 & \dots & b_{13}b_{1n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{1n} & b_{12}b_{2n} & b_{13}b_{1n} & \dots & 0 \end{pmatrix}.$$

By Stembridge [Ste90, Lemma 4.2(a)],

$$\operatorname{pf}(B' + B'') \equiv \sum_{\substack{J \subseteq \{1,\dots,n\} \\ \#J \text{ even}}} \operatorname{pf}(B'_J) \operatorname{pf}(B''_{J^c}) \pmod 2$$

where B'_J is the submatrix of B' obtained by keeping only the entries in rows and columns indexed by elements of J, and B''_{J^c} is similarly the matrix of entries in B'' whose row and column indices are *not* in J.

To evaluate $\mathrm{pf}(B'_J)$ modulo 2, note first that if $1 \in J$, then B'_J contains a row of zeros, so its determinant (and therefore its pfaffian) vanishes. Otherwise, the ijth entry of B' is just b_{ij} for $i > j$, so by the usual pfaffian formula in terms of perfect matchings (see the definition in [Ste90, p. 102]), we have

$$\mathrm{pf}(B'_J) \equiv \sum_{P \text{ on } J} \prod_{\{i,j\} \in P} b_{ij} \pmod 2, \tag{4.9}$$

the sum over perfect matchings P on J. Meanwhile, given a subset $J \subseteq \{2, \dots, n\}$, each perfect matching on J^c contributes the same product to $\mathrm{pf}(B''_{J^c})$, namely $\prod_{k \in \{2,\dots,n\} \setminus J} b_{1k}$. Since there is an odd number of perfect matchings on any even-cardinality set, modulo 2 we have $\mathrm{pf}(B'_{J^c}) \equiv \prod_{k \in \{2,\dots,n\} \setminus J} b_{1k} \pmod 2$. Now we just put this altogether:

$$\begin{aligned} \mathrm{pf}(U - U^{\mathsf{T}}) \equiv \mathrm{pf}(B' + B'') &\equiv \sum_{\substack{J \subseteq \{1,\dots,n\} \\ \#J \text{ even}}} \mathrm{pf}(B'_J)\,\mathrm{pf}(B''_{J^c}) \\ &\equiv \sum_{\substack{J \subseteq \{2,\dots,n\} \\ \#J \text{ even}}} \sum_{P \text{ on } J} \left(\prod_{\{i,j\} \in P} b_{ij} \right) \left(\prod_{k \in \{2,\dots,n\} \setminus J} b_{1k} \right) \\ &\equiv \mathrm{discpf}(A, \beta) \pmod 2. \end{aligned} \tag{4.10}$$

Having proven it for all n such that $4 \mid n$, we finish by a reverse induction, showing that if statement holds for $n \in \mathbb{Z}_{\geq 2}$ then it holds for $n - 1$. Since every positive integer n is less than or equal to a multiple of 4, this will prove the theorem. Let $B_{n-1} \in \mathrm{M}_{n-1}(\mathbb{Z})$ be tracelike. Let $B_n = \begin{pmatrix} B_{n-1} & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{M}_n(\mathbb{Z})$ be the block matrix formed from B_{n-1} and $\begin{pmatrix} 1 \end{pmatrix}$. Then $\det(B_n) = \det(B_{n-1})$. If we add the last row to the first row, then add the last column to the first column, we obtain

$$B'_n := \begin{pmatrix} B'_{n-1} & v^{\mathsf{T}} \\ v & 1 \end{pmatrix} \tag{4.11}$$

where $v = (1, 0, \dots, 0)$ and B'_{n-1} is the matrix obtained from B_{n-1} by adding 1 to b_{11}. Now B'_n is tracelike! By the inductive hypothesis, we have

$$\det(B_{n-1}) = \det(B'_n) \equiv \mathrm{discpf}(B'_n)^2 \pmod 4. \tag{4.12}$$

Now the discriminant pfaffian $\mathrm{discpf}(B'_n)$ is obtained from substituting $b_{1n} = 1$ and $b_{in} = 0$ for $i = 2, \dots, n-1$. To evaluate, we look at Definition 4.1. For every term with $n \in J$, any perfect matching P on J has $\{i, n\}$ in P with $i \in \{2, \dots, n-1\}$ and therefore such a term vanishes. On the other hand, every term with $n \notin J$ corresponds to $J \subseteq \{2, \dots, n-1\}$ with final term $\prod_{k \in \{2,\dots,n-1\} \setminus J} b_{1k}$ since $b_{1n} = 1$. □

References

[Bae81] Ricardo Baeza, *Discriminants of polynomials and of quadratic forms*, J. Algebra **72** (1981), no. 1, 17–28. 2

[Bha06] Manjul Bhargava, *Higher composition laws and applications*, International Congress of Mathematicians. Vol. II, Eur. Math. Soc., Zürich, 2006, 271–294. 2

[Ber76] E.R. Berlekamp, *An analog to the discriminant over fields of characteristic two*, J. Algebra **38** (1976), no. 2, 315–317. 2

[Bou98] Nicolas Bourbaki, *Eléments de mathématique. Algèbre commutative. Chapitres 1 à 4*, vol. 1, Springer, 1998.

[BG16] Owen Biesel and Alberto Gioia, *A new discriminant algebra construction*, Documenta Math. **21** (2016), 1051–1088. 2

[Cox] David A. Cox, *Stickelberger and the eigenvalue theorem*, preprint, 2020, `arXiv:2007.12573`. 2

[Gri17] Darij Grinberg (https://mathoverflow.net/users/2530/darij-grinberg), Is the discriminant of a free (as a module) R-algebra always congruent to a square modulo 4?, URL (version: 2017-04-13): https://mathoverflow.net/q/257889. 4

[Har12] Daniel Harrer, *Parametrization of cubic rings*, Diplomarbeit, Universität München, 2012. 2

[Hur1896] Adolf Hurwitz, *Über die Zahlentheorie der Quaternionen*, Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, 1896, 314–340. 3

[Lam06] T. Y. Lam, *Serre's problem on projective modules*, Springer Mono. Math., Springer–Verlag, Berlin, 2006.

[Mar18] Daniel A. Marcus, *Number fields*, 2nd ed., Universitext, Springer Nature, Cham, 2018. 1, 2, 13

[Mar90] Marvin Marcus, *Determinants of sums*, Coll. Math. J. **21** (1990), no. 2, 130–135.

[Mar89] Jacques Martinet, *Les discriminants quadratiques et la congruence de Stickelberger*, J. Théorie Nombres Bordeaux **1** (1989), no. 1, 197–204. 2

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Springer, Berlin, 1999. 2

[Sch29] I. Schur, *Elementarer Beweis eines Satzes von L. Stickelberger*, Math. Z. **29** (1929), no. 1, 464–465. 2

[OEIS] N. J. A. Sloane, editor, *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org, 2021, Sequence A000085 12

[Ste90] John R. Stembridge, *Nonintersecting paths, Pfaffians, and plane partitions*, Adv. Math. **83** (1990), no. 1, 96–131. MR 1069389 10, 13, 14

[Sti98] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlk örper*, Verhandlungen des ersten internationalen Mathematiker-Kongresses, Zürich 1897 (Teubner, Leipzig) (F. Rudio, ed.), 1898, p. 182–193. 2

[Voi21] John Voight, *Quaternion algebras*, Grad. Texts in Math., vol. 288, Springer, Cham, 2021. 3

[Was82] Lawrence C. Washington, *Introduction to cyclotomic fields*, Grad. Texts. in Math., vol. 83, Springer, New York, 1982. 2

Department of Mathematics, Dartmouth College, Kemeny Hall, Hanover, NH 03755, USA
Email address: asher.auel@dartmouth.edu

Department of Mathematics and Statistics, Carleton College, Center for Mathematics and Computing, Northfield, MN 55057, USA
Email address: owenbiesel@gmail.com

Department of Mathematics, Dartmouth College, Kemeny Hall, Hanover, NH 03755, USA
Email address: jvoight@gmail.com