

RINGS OF LOW RANK WITH A STANDARD INVOLUTION AND QUATERNION RINGS

JOHN VOIGHT

ABSTRACT. We consider the problem of classifying (possibly noncommutative) R -algebras of low rank over an arbitrary base ring R . We first classify algebras by their degree, and we relate the class of algebras of degree 2 to algebras with a standard involution. We then investigate a class of exceptional rings of degree 2 which occur in every rank $n \geq 1$ and show that they essentially characterize all algebras of degree 2 and rank 3. Finally, we subdivide the class of algebras of rank 4 and degree 2 between exceptional rings and quaternion rings, those algebras defined by an even Clifford algebra construction.

CONTENTS

1. Degree	4
2. Involutions	8
3. Commutative algebras with a standard involution and exceptional rings	12
4. Algebras of rank 3	14
5. Ternary quadratic modules and Clifford algebras	17
6. The canonical exterior form	20
7. Characterizing quaternion rings	22
8. An equivalence of categories	25
References	31

Let R be a commutative Noetherian ring (with 1) which is connected, so that R has only $0, 1$ as idempotents (or equivalently that $\text{Spec } R$ is connected). Let B be an algebra over R , an associative ring with 1 equipped with an embedding $R \hookrightarrow B$ of rings (mapping $1 \in R$ to $1 \in B$) whose image lies in the center of B ; we identify R with its image in B . Assume further that B is a finitely generated, projective R -module.

The problem of classifying algebras B of low rank has an extensive history. The identification of quadratic rings over \mathbb{Z} by their discriminants is classical and goes back as far as Gauss. Commutative rings of rank at most 5 over $R = \mathbb{Z}$ have been classified by Bhargava [3] building work of many others, including Delone and Faddeev [8] and Gan, Gross, and Savin [9]; this beautiful work has rekindled interest in the subject and has already seen many applications. Progress on generalizing these results to arbitrary commutative base rings R (or even arbitrary base schemes) has been made by Wood [27]. A natural question in this vein is to consider noncommutative algebras of low rank, and in this article we treat algebras of rank at most 4.

Date: July 16, 2009.

The category of R -algebras (with morphisms given by isomorphisms) has a natural decomposition by degree. The *degree* of an R -algebra B , denoted $\deg_R(B)$, is the smallest positive integer n such that every $x \in B$ satisfies a monic polynomial of degree n . Any *quadratic algebra* B , i.e. an algebra of rank $\text{rk}(B) = 2$, is necessarily commutative (see Lemma 2.9) and has degree 2. Moreover, a quadratic algebra has a unique R -linear (anti-)involution $\bar{} : B \rightarrow B$ such that $x\bar{x} \in R$ for all $x \in B$, which we call a *standard involution*.

The situation is much more complicated in higher rank. In particular, the degree of B does not behave well with respect to base extension (Example 1.20). We define the *geometric degree* of B to be the maximum of $\deg_S(B \otimes_R S)$ with $R \rightarrow S$ a homomorphism of (commutative) rings. Our first main result is as follows (Corollary 2.17).

Theorem A. *Let B be an R -algebra and suppose there exists $a \in R$ such that $a(a - 1)$ is a nonzerodivisor. Then the following are equivalent.*

- (i) B has degree 2;
- (ii) B has geometric degree 2;
- (iii) $B \neq R$ has a standard involution.

Note that if 2 is a nonzerodivisor in R then we can take $a = -1$ in the above theorem.

In view of Theorem A, it is natural then to consider the class of R -algebras B equipped with a standard involution (which is then necessarily unique (Corollary 2.11)). For such an algebra B , we define the *reduced trace* by $\text{trd} : B \rightarrow R$ by $x \mapsto x + \bar{x}$ and the *reduced norm* by $\text{nrd} : B \rightarrow R$ by $x \mapsto x\bar{x}$. Then every element $x \in B$ satisfies the polynomial $\mu(x; T) = T^2 - \text{trd}(x)T + \text{nrd}(x)$.

Commutative algebras with a standard involution can be easily characterized: for example, if 2 is a nonzerodivisor in R and B is a commutative R -algebra with a standard involution, then either B is a quadratic algebra or B is a quotient of an algebra of the form $R[x_1, \dots, x_n]/(x_1, \dots, x_n)^2$ (more generally, see Proposition 3.1).

There is a natural class of noncommutative algebras equipped with a standard involution which occur in every rank $n \geq 1$, defined as follows. Let M be a projective R -module of rank $n - 1$ and let $t : M \rightarrow R$ be an R -linear map. Then we give the R -module $B = R \oplus M$ the structure of an R -algebra by defining the multiplication rule $xy = t(x)y$ for $x, y \in M$. The map $x \mapsto \bar{x} = t(x) - x$ is a standard involution on B . An *exceptional ring* is an R -algebra B with the property that there is a left ideal $M \subset B$ such that $B = R \oplus M$ and the map $M \rightarrow \text{Hom}_R(M, B)$ given by left multiplication factors through a linear map $t : M \rightarrow R$.

We prove (Proposition 4.8) by a direct calculation that an R -algebra B of rank 3 has a standard involution if and only if it is an exceptional ring.

Thus we are led to investigate the case of algebras of rank 4. When $R = F$ is a field, the distinguished class of central simple algebras of rank 4 is known as the class of *quaternion algebras* over F . Generalizations of the notion of quaternion algebra to other base rings R have been considered by Kanzaki [15], Hahn [11], Knus [18], and many others. Recently, Gross and Lucianovic [10] have pursued these generalizations further. A *free quaternion ring* B over a PID or local ring R is an R -algebra of rank 4 with a standard involution such that the characteristic polynomial $\chi(x; T)$ of left multiplication by x on B is equal to $\mu(x; T)^2 = (T^2 - \text{trd}(x)T + \text{nrd}(x))^2$. They prove the following proposition.

Proposition ([10, Proposition 4.1]). *Let R be a PID or local ring. Then there is a bijection between twisted isometry classes of ternary quadratic forms over R and isomorphism classes of free quaternion rings over R .*

In this correspondence, one associates to a ternary quadratic form q the even Clifford algebra $C^0(q)$. In this article, we generalize this result and treat an arbitrary commutative base ring R .

A *ternary quadratic module* is a triple (M, I, q) where M, I are projective R -modules of ranks 3, 1, respectively, and $q : M \rightarrow I$ is a quadratic map (see §4 for definitions). Given a ternary quadratic module (M, I, q) , one can associate the even Clifford algebra $C^0(M, I, q)$, which is an R -algebra of rank 4 with standard involution. Conversely, to an R -algebra B of rank 4 with a standard involution, we associate the quadratic map

$$\phi_B : \bigwedge^2(B/R) \rightarrow \bigwedge^4 B$$

with the property that

$$\phi_B(x \wedge y) = 1 \wedge x \wedge y \wedge xy$$

for all $x, y \in B$. We call ϕ_B the *canonical exterior form*. This form can be found in a footnote of Gross and Lucianovic [10] and is inspired by the case of commutative quartic rings, investigated by Bhargava [5].

Theorem B. *Let B be an R -algebra of rank 4 with a standard involution. Then the following are equivalent.*

- (i) *There exists a ternary quadratic module (M, I, q) such that $B \cong C^0(M, I, q)$;*
- (ii) *For all $x \in B$, the characteristic polynomial of left multiplication by x on B is equal to $\mu(x; T)^2$;*
- (iii) *For all $x \in B$, the trace of left multiplication by x on B is equal to $2 \operatorname{trd}(x)$;*
- (iv) *For all primes \mathfrak{p} of R , the localization of the canonical exterior form*

$$\phi_{B, \mathfrak{p}} : \bigwedge^2(B_{\mathfrak{p}}/R_{\mathfrak{p}}) \rightarrow \bigwedge^4 B_{\mathfrak{p}}$$

at \mathfrak{p} is zero if and only if $B_{\mathfrak{p}}$ is commutative.

Moreover, there exists a decomposition $\operatorname{Spec} R = \operatorname{Spec} R_Q \cup \operatorname{Spec} R_E$ such that the restriction B_{R_Q} of B to R_Q satisfies the above (equivalent) conditions and B_{R_E} is an exceptional ring.

An algebra B that satisfies any one of the equivalent conditions in Theorem B is called a *quaternion ring* over R .

To conclude, we note that although by definition the association $(M, I, q) \mapsto C^0(M, I, q)$ yields all isomorphism classes of quaternion rings, it does not yield a bijection over a general commutative ring R . However, we may recover a bijection by rigidifying the situation as follows. A *parity factorization* of an invertible R -module N is an R -module isomorphism

$$p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} N$$

where P, Q are invertible R -modules. Our last main result is the following (Theorem 8.13).

Theorem C. *There is a bijection*

$$\left\{ \begin{array}{l} \text{Isometry classes of ternary} \\ \text{quadratic modules } (M, I, q) \\ \text{over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Isomorphism classes of quaternion} \\ \text{rings } B \text{ over } R \text{ equipped with a parity} \\ \text{factorization } p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} \bigwedge^4 B \end{array} \right\}$$

which is functorial in the base ring R . In this bijection, the isometry class of a quadratic module (M, I, q) maps to the isomorphism class of the quaternion ring $C^0(M, I, q)$ equipped with the parity factorization

$$(\wedge^3 M \otimes (I^\vee)^{\otimes 2})^{\otimes 2} \otimes I \xrightarrow{\sim} \wedge^4 C^0(M, I, q).$$

Theorem C compares to work of Balaji [2], who takes a more categorical perspective.

This article is organized as follows. We begin (§1) with some preliminary notions and define the degree of an algebra. We then explore the relationship between algebras of degree 2 and those with a standard involution and then prove Theorem A (§2). Next, we investigate the class of commutative algebras with a standard involution and define exceptional rings (§3). We then classify algebras of rank 3, relating them to certain endomorphism rings of flags (§4). Turning to rings of rank 4, we review ternary quadratic modules and Clifford algebras (§5) and define the canonical exterior form. Relating this work to that of Gross and Lucianovic, we prove Theorem B (§7). Finally we prove the equivalence in Theorem C (§8).

The author would like to thank Asher Auel, Manjul Bhargava, Noam Elkies, Jon Hanke, Hendrik Lenstra, and Raman Parimala for their suggestions and comments which helped to shape this research. We are particularly indebted to Melanie Wood who made many helpful remarks and corrections. This project was partially supported by the National Security Agency under Grant Number H98230-09-1-0037.

1. DEGREE

In this section, we discuss the notion of the degree of an algebra, generalizing the notion from that over a field. We refer the reader to Scharlau [25, §8.11] for an alternative approach.

Throughout this article, let R be a commutative, connected Noetherian ring and let B be an algebra over R , which as in the introduction is defined to be an associative ring with 1 equipped with an embedding $R \hookrightarrow B$ of rings. We assume further that B is finitely generated, projective R -module. For a prime \mathfrak{p} of R , we denote by $R_{\mathfrak{p}}$ the completion of R at \mathfrak{p} ; we abbreviate $B_{\mathfrak{p}} = B \otimes_R R_{\mathfrak{p}}$ and for $x \in B$ we write $x_{\mathfrak{p}} = x \otimes 1 \in B_{\mathfrak{p}}$.

Remark 1.1. There is no loss of generality in working with connected rings, since for an arbitrary ring R one has a statement for each of the connected components of $\text{Spec } R$. Furthermore, one may work with non-Noetherian rings by the process of Noetherian reduction, by finding a Noetherian subring $R_0 \subset R$ and an R_0 -algebra B_0 such that $B_0 \otimes_{R_0} R \cong B$.

Remark 1.2. For the questions we consider herein, we work (affinely) with algebras over base rings. If desired, one could without difficulty extend our results to an arbitrary Noetherian (separated) base scheme by the usual patching arguments.

We begin with a preliminary lemma.

Lemma 1.3. *R is a direct summand of B .*

Proof. For every prime ideal \mathfrak{p} of R , there exists a basis for the algebra $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$ over the field $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ which includes 1, and by Nakayama's lemma this lifts to a basis for $B_{\mathfrak{p}}$. In particular, the quotient B/R is locally free and finitely generated of constant rank (since B is finitely generated over R , and R is connected) hence projective, which implies that B/R and hence R is a direct summand of B . \square

Every element $x \in B$ satisfies a monic polynomial with coefficients in R by the (generalized) Cayley-Hamilton theorem; indeed, by the “determinant trick”, this polynomial has degree bounded by the minimal number of generators for B as an R -module [21, Theorem IV.17] (see also the determinant-trace polynomial [21, Section V.E]). In fact, one can extend the notion of characteristic polynomial directly as follows.

Lemma 1.4. *For every $x \in B$, there exists a unique monic polynomial $\chi(x; T) \in R[T]$ of degree $n = \text{rk}(B)$ with the property that for every prime \mathfrak{p} of R , the characteristic polynomial of left multiplication by x on $B_{\mathfrak{p}}$ is equal to $\chi(x; T)_{\mathfrak{p}} \in R_{\mathfrak{p}}[T]$. Moreover, we have $\chi(x; x) = 0$.*

Proof. Let $x \in B$. Since B is projective, for each prime \mathfrak{p} of R we have that $B_{\mathfrak{p}}$ is free over $R_{\mathfrak{p}}$ of rank n . By the determinant trick, we see that $x_{\mathfrak{p}} \in R_{\mathfrak{p}}$ satisfies the characteristic polynomial $\chi_{\mathfrak{p}}(x; T) \in R_{\mathfrak{p}}[T]$ of left multiplication by $x_{\mathfrak{p}}$ on $B_{\mathfrak{p}}$, where $\chi_{\mathfrak{p}}(x; T)$ is monic of degree n . Therefore by standard patching arguments [12, Proposition II.2.2], there exists a unique monic polynomial $\chi(x; T) \in R[T]$ such that $\chi(x; T)_{\mathfrak{p}} = \chi_{\mathfrak{p}}(x; T)$. Finally, since $\chi(x; x)_{\mathfrak{p}} = 0 \in R_{\mathfrak{p}}$ for all primes \mathfrak{p} , we have that $\chi(x; x) = 0 \in R$. \square

Definition 1.5. *The degree of $x \in B$, denoted $\deg_R(x)$ (or simply $\deg(x)$ if the base ring R is clear from context), is the smallest positive integer $n \in \mathbb{Z}_{>0}$ such that x satisfies a monic polynomial of degree n with coefficients in R .*

By Lemma 1.4, we have $\deg_R(x) \leq \text{rk } B$ for all $x \in B$. Note that $\deg_R(x) = 1$ if and only if $x \in R$.

For $x \in B$, denote by $R[x]$ the (commutative) R -subalgebra of B generated by x , i.e., $R[x] = \bigcup_{d=0}^{\infty} Rx^d \subset B$.

Lemma 1.6. *Let $x \in B$. Then the following are equivalent:*

- (i) $R[x]$ is free;
- (ii) $R[x]$ is projective;
- (iii) x satisfies a unique monic polynomial of minimal degree $\deg_R(x)$ with coefficients in R ;
- (iv) The ideal $\{f(T) \in R[T] : f(x) = 0\} \subset R[t]$ is principal and generated by a monic polynomial.

If any one of these holds, then $\deg_R(x) = \text{rk}_R R[x]$.

Proof. The lemma is clear if $x \in R$, so we may assume $x \notin R$ or equivalently $\deg_R(x) > 1$.

The statement (i) \Rightarrow (ii) is trivial. To prove (ii) \Rightarrow (i), suppose that $R[x]$ is projective. Let \mathfrak{p} be a prime ideal of R and let $k = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$ be the residue field of $R_{\mathfrak{p}}$. Then $R[x] \otimes_R k = k[x]$ has a k -basis $1, x, \dots, x^{d-1}$ for some $d \in \mathbb{Z}_{>1}$. By Nakayama’s lemma, $1, \dots, x^{d-1}$ is a $R_{\mathfrak{p}}$ -basis for $R_{\mathfrak{p}}[x]$. Since R is connected, the value of $d = \text{rk } R_{\mathfrak{p}}[x]$ does not depend on the prime ideal \mathfrak{p} . It follows that the surjective map $\bigoplus_{i=0}^{d-1} Re_i \rightarrow R[x]$ by $e_i \mapsto x^i$ is an isomorphism since it is so locally, and hence $R[x]$ is free.

To prove that (iii) \Leftrightarrow (i), we note that if $f(T) \in R[T]$ is the unique monic polynomial of degree $d = \deg_R(x) \geq 2$ with $f(x) = 0$, then $1, x, \dots, x^{d-1}$ is an R -basis for $R[x]$ —indeed, if $a_{d-1}x^{d-1} + \dots + a_0 = 0$ with $a_i \in R$ then $g(T) = f(T) + a_{d-1}T^{d-1} + \dots + a_0$ has $g(x) = 0$ so $f(T) = g(T)$ and $a_0 = \dots = a_{d-1} = 0$, and the converse follows similarly.

The equivalence (iii) \Leftrightarrow (iv) follows similarly. \square

Corollary 1.7. *Suppose that $\deg_R(x) = 2$. Then $R[x]$ is projective if and only if $ax \notin R$ for all $a \neq 0 \in R$ if and only if $1, x$ belong to basis for $B_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ for all primes \mathfrak{p} of R .*

Example 1.8. Let p be prime and let $B = \mathbb{Z}/p^2\mathbb{Z}[\epsilon]/(\epsilon^2)$ with $R = \mathbb{Z}/p^2\mathbb{Z}$. Then $R[\epsilon] = B$ is projective, but the element $x = p\epsilon$ satisfies $x^2 = 0$ as well as $px = 0$, so $R[x]$ is not projective.

If $R \rightarrow S$ is a ring homomorphism and $x \in B$, then we abbreviate $\deg_S(x)$ for $\deg_S(x \otimes 1)$ with $x \otimes 1 \in B \otimes_R S = B_S$.

Lemma 1.9. *For any $x \in B$, the map*

$$\begin{aligned} \text{Spec } R &\rightarrow \mathbb{Z} \\ \mathfrak{p} &\mapsto \deg_{R_{\mathfrak{p}}}(x) = \deg_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(x) \end{aligned}$$

is lower semicontinuous, i.e., for all primes $\mathfrak{q} \supset \mathfrak{p}$ we have $\deg_{R_{\mathfrak{q}}}(x) \geq \deg_{R_{\mathfrak{p}}}(x)$.

Proof. Let $n = \deg_R(x)$, and for each integer $0 \leq m \leq n$, let \mathfrak{a}_m be the ideal of R consisting of all leading coefficients of polynomials $f(T) \in R[T]$ such that $f(x) = 0$ with $\deg(f) \leq i$. Clearly we have $\mathfrak{a}_0 = (0) \subset \mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_n = R$. It follows that $\deg_{R_{\mathfrak{p}}}(x_{\mathfrak{p}}) = n$ if and only if $\mathfrak{p} \supset \mathfrak{a}_{n-1}$, and more generally that $\deg_{R_{\mathfrak{p}}}(x_{\mathfrak{p}}) = m$ if and only if $\mathfrak{a}_{m+1} \not\supset \mathfrak{p} \supset \mathfrak{a}_m$, and consequently the map is lower semicontinuous.

The equality $\deg_{R_{\mathfrak{p}}}(x) = \deg_{R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}}(x)$ follows from this analysis, since no leading coefficient which is not a unit in $R_{\mathfrak{p}}$ becomes a unit in $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. \square

Corollary 1.10. *For any $x \in B$ with $\deg_R(x) = n$, the set of primes $\mathfrak{p} \in \text{Spec } R$ where $\deg_{R_{\mathfrak{p}}}(x) = n$ is closed and nonempty. Moreover, we have $\deg_R(x) \geq \deg_{R_{\mathfrak{p}}}(x)$ for all primes \mathfrak{p} .*

Remark 1.11. Note that if $R[x]$ is projective, Lemma 1.9 is immediate since then in fact $\deg_{R_{\mathfrak{p}}}(x_{\mathfrak{p}}) = \text{rk}(R[x]_{\mathfrak{p}})$ is constant.

Definition 1.12. *The degree of B , denoted $\deg_R(B)$ (or simply $\deg(B)$, when no confusion can result), is the smallest positive integer $n \in \mathbb{Z}_{>0}$ such that every element of B has degree at most n .*

Example 1.13. B has degree 1 as an R -algebra if and only if $B = R$.

If B is free of rank n , then B has degree at most n but not necessarily degree n , even if B is commutative: for example, the algebra $R[x, y, z]/(x, y, z)^2$ has rank 4 but has degree 2 and $R[x, y]/(x^3, xy, y^2)$ has rank 4 but degree 3.

Example 1.14. If K is a separable field extension of F with $\dim_F K = n$, then K has degree n as a F -algebra (in the above sense) by the primitive element theorem.

More generally, if F is a field and B is a commutative étale algebra with $\#F \geq \dim_F(B) = n$, then $\deg_F(B) = n$. Indeed, we can write $B \cong \prod_i K_i$ as a product of separable field extensions K_i/F , and so if $a_i \in K_i$ are primitive elements with different characteristic polynomials (equivalently, minimal polynomials), which is possible under the hypothesis that $\#K_i \geq \#F \geq n$, then the element $(a_i)_i \in \prod_i K_i \cong B$ has minimal polynomial of degree n .

Example 1.15. If B is a central simple algebra over a field F , then $\deg(B)^2 = \dim_F(B)$. More generally, if B is a semisimple algebra over F , then the degree of B agrees with the usual definition [19] given in terms of the Wedderburn-Artin theorem.

Definition 1.16. B has constant degree $n \in \mathbb{Z}_{>0}$ if $\deg_{R_{\mathfrak{p}}}(B_{\mathfrak{p}}) = n$ for all prime ideals \mathfrak{p} of R .

Example 1.17. If R is a domain then any R -algebra B has constant degree. Indeed, for any prime \mathfrak{p} of R we have $\deg_R(B) \geq \deg_F(B)$ where F denotes the quotient field of R , but on the other hand if $\deg_F(x/d) = n = \deg_F(B)$ for $x \in B$ and $d \in R$, then we must have $\deg_R(x) = n$.

Lemma 1.18. If B has constant degree $n = \text{rk}_R(B)$, then B is commutative.

Proof. We know that B is commutative if and only if $B_{\mathfrak{m}}$ is commutative for all maximal ideals \mathfrak{m} of B , since then the commutator $[B, B]$ is locally trivial and hence trivial. So we may suppose that R is a local ring with maximal ideal \mathfrak{m} . By hypothesis, we have $\deg_R(B) = n = \text{rk}_R(B)$, so there exists an element $x \in B$ with $\deg_R(x) = n$. By Nakayama's lemma, we find that $\deg_k(x) = n$, where $k = R/\mathfrak{m}$ is the residue field of R ; so the powers of x form a basis for B_k , hence also of B , and it follows that B is commutative, as claimed. \square

Example 1.19. Lemma 1.18 is false without the hypothesis that the algebra is of constant degree, as in Example 4.6.

Unfortunately, $\deg_R(B)$ is not invariant under base extension, as the following example illustrates.

Example 1.20. Let p be prime, let $R = \mathbb{F}_p$, and let $B = \prod_{i=1}^n \mathbb{F}_p$ with $n \geq p$. Then every element $x \in B$ satisfies $x^p = x$, so $\deg_R(B) \leq p$. On the other hand, the element $x = (0, 1, 2, \dots, p-1, 0, \dots, 0)$ has degree p since the elements $1, x, \dots, x^{p-2}$ are linearly independent over \mathbb{F}_p (consider the corresponding Vandermonde matrix), hence $\deg_R(B) = p$. On the other hand, $\deg_{\overline{\mathbb{F}_p}}(B \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}) = n$ by Example 1.14.

Definition 1.21. The geometric degree of B , denoted $\text{gdeg}_R(B)$ (or simply $\text{gdeg}(B)$), is the maximum of $\deg_S(B \otimes_R S)$ for all maps $R \rightarrow S$ with S a (connected, Noetherian, commutative) ring.

Remark 1.22. In Definition 1.21, we may equivalently restrict the maximum to rings S which are algebraically closed fields: indeed, if $\text{gdeg}(B) = \deg_S(B \otimes_R S)$ with $\deg_S(x \otimes s) = \deg_S(B \otimes_R S) = n$ then by Lemma 1.9 there exists a maximal ideal $\mathfrak{m} \subset S$ such that $\deg_{S_{\mathfrak{m}}}(x \otimes s) = \deg_k(x \otimes s) = n$ where $k = S_{\mathfrak{m}}/\mathfrak{m}S_{\mathfrak{m}}$, and then $\deg_{\overline{k}}(x \otimes s) = n$ as well, where \overline{k} is the algebraic closure of k .

For $m \in \mathbb{Z}_{>0}$, we denote by $R[a_1, \dots, a_m] = R[a]$ the polynomial ring in n variables over R .

Lemma 1.23. Suppose that B is generated by x_1, \dots, x_m , and define

$$\xi = a_1x_1 + \dots + a_mx_m = \sum_{i=1}^m a_ix_i \in B \otimes_R R[a].$$

Then $\text{gdeg}_R(B) = \deg_{R[a]}(\xi) < \infty$.

Proof. Let S be an R -algebra. Then since x_1, \dots, x_m generate $B \otimes_R S$ as an S -algebra, by specialization we see that $\deg_S(B \otimes_R S) \leq \deg_{R[a]}(\xi)$, so $\text{gdeg}(B) \leq \deg_{R[a]}(\xi)$. But

$$\deg_{R[a]}(\xi) \leq \deg_{R[a]}(B_{R[a]}) \leq \text{gdeg}(B)$$

by definition, so equality holds. \square

We conclude with two results which characterize the geometric degree.

Lemma 1.24. *If S is a flat R -algebra, then $\text{gdeg}_R(B) = \text{gdeg}_S(B \otimes_R S)$.*

Proof. For ξ as in Lemma 1.23, we have $\text{gdeg}_R(B) = \text{deg}_{R[a]}(\xi) = \text{rk}_{R[a]} R[a][\xi]$; since S is flat over R we have that $S[a]$ is flat over $R[a]$ and $\text{rk}_{R[a]} R[a][\xi] = \text{rk}_{S[a]} S[a][\xi] = \text{deg}_{S[a]}(\xi) = \text{deg}_S(B \otimes_R S)$, as claimed. \square

Lemma 1.25. *We have $\text{gdeg}_R(B) = \max_{\mathfrak{p} \in \text{Spec } R} \text{gdeg}_{R_{\mathfrak{p}}}(B_{\mathfrak{p}})$.*

Proof. We have by definition $\text{gdeg}_R(B) \geq \text{gdeg}_{R_{\mathfrak{p}}}(B_{\mathfrak{p}})$ for all primes \mathfrak{p} . Conversely, let S be a ring such that $\text{gdeg}_R(B) = \text{deg}_S(B \otimes S) = n$, and let $x \in B \otimes S$ have $\text{deg}_S(x) = n$. Then by Lemma 1.9, there exists a prime $\mathfrak{q} \subset S$ such that $\text{deg}_{S_{\mathfrak{q}}}(x) = n$. If \mathfrak{q} lies over $\mathfrak{p} \in \text{Spec } R$, then it follows that $\text{gdeg}_{R_{\mathfrak{p}}}(B_{\mathfrak{p}}) = n = \text{gdeg}_R(B)$. The result follows. \square

2. INVOLUTIONS

In this section, we discuss the notion of a standard involution on an R -algebra, and we compare this to the notion of degree and geometric degree from the previous section.

Definition 2.1. *An involution (of the first kind) $\bar{} : B \rightarrow B$ is an R -linear map which satisfies:*

- (i) $\bar{\bar{x}} = x$,
- (ii) $\bar{}$ is an anti-automorphism, i.e., $\overline{xy} = \bar{y}\bar{x}$ for all $x, y \in B$, and
- (iii) $\overline{\bar{x}} = x$ for all $x \in B$.

If B^{op} denotes the opposite algebra of B , then one can equivalently define an involution to be an R -algebra isomorphism $B \rightarrow B^{\text{op}}$ such that the underlying R -linear map has order at most 2.

Definition 2.2. *An involution $\bar{}$ is standard if $x\bar{x} \in R$ for all $x \in B$.*

Example 2.3. The usual adjoint map $M_k(R) \rightarrow M_k(R)$ defined by $A \mapsto A^\dagger$ (with $AA^\dagger = A^\dagger A = \det(A)I$) is R -linear if and only if $k = 2$, since it restricts to the map $r \mapsto r^{k-1}$ on R ; if $k = 2$, then it is in fact a standard involution. In particular, we warn the reader that many authors consider involutions which are not R -linear—although this more general class is certainly of interest (see e.g. Knus and Merkurjev [17]), we will not consider them here.

Example 2.4. To verify that an involution $\bar{} : B \rightarrow B$ is standard, it is not enough to check that $x\bar{x} \in R$ for x in a set of generators for B as an R -module. The Clifford algebra gives a variety of such examples; see Remark 5.4.

Remark 2.5. Note that if $\bar{}$ is a standard involution, so that $x\bar{x} \in R$ for all $x \in B$, then

$$(x + 1)(\overline{x + 1}) = (x + 1)(\bar{x} + 1) = x\bar{x} + x + \bar{x} + 1 \in R$$

and hence $x + \bar{x} \in R$ for all $x \in B$ as well.

Example 2.6. A standard involution is *trivial* if it is the identity map. The R -algebra $B = R$ has a trivial standard involution as does the commutative algebra $B = R[\epsilon]/(\epsilon^2)$ for R any commutative ring of characteristic 2.

B has a trivial standard involution if and only if B is commutative and $x^2 \in R$ for all $x \in B$. If the identity map is a standard involution on B , then either $B = R$ or 2 is a zerodivisor in R . Indeed, for any $x \in B$ we have $(x+1)^2 \in R$, so $2x \in R$ for all $x \in B$; if 2 is a nonzerodivisor in R , then $x/1 \in R[1/2]$ so $\text{rk } B[1/2] = \text{rk } B = 1$ so $B = R$.

Let $\bar{} : B \rightarrow B$ be a standard involution on B . Then we define the *reduced trace* $\text{trd} : B \rightarrow R$ by $\text{trd}(x) = x + \bar{x}$ and the *reduced norm* $\text{nrd} : B \rightarrow R$ by $\text{nrd}(x) = \bar{x}x$ for $x \in B$. Since

$$(2.7) \quad x^2 - (x + \bar{x})x + \bar{x}x = 0$$

identically we have $x^2 - \text{trd}(x)x + \text{nrd}(x) = 0$ for all $x \in B$. Therefore any R -algebra B with a standard involution has $\deg_R(B) \leq 2$. In particular, for $x, y \in B$ we have

$$(x + y)^2 - \text{trd}(x + y)(x + y) + \text{nrd}(x + y) = 0$$

so

$$(2.8) \quad xy + yx = \text{trd}(y)x + \text{trd}(x)y + \text{nrd}(x + y) - \text{nrd}(x) - \text{nrd}(y).$$

An R -algebra S is *quadratic* if S has rank 2. The following lemma is well-known [16, I.1.3.6]; we give a proof for completeness.

Lemma 2.9. *Let S be a quadratic R -algebra. Then S is commutative, we have $\deg_R(S) = \text{gdeg}_R(S) = 2$, and there is a unique standard involution on S .*

Proof. First, suppose that S is free. Then by Lemma 1.3, we can write $S = R \oplus Rx = R[x]$ for some $x \in S$ and so in particular S is commutative. By Lemma 1.6, the element x satisfies a unique polynomial $x^2 - tx + n = 0$ with $t, n \in R$, so $\deg_R(x) = \deg_R(B) = 2$. We define $\bar{} : R[x] \rightarrow R$ by $\bar{x} = t - x$, and we extend the map $\bar{}$ by R -linearity to a standard involution on S . If $\bar{} : S \rightarrow S$ is any standard involution then identically equation (2.7) holds; by uniqueness, we have $t = x + \bar{x}$ and $n = x\bar{x} = \bar{x}x$, and the involution $\bar{x} = t - x$ is unique.

We now use a standard localization and patching argument to finish the proof. For any prime ideal \mathfrak{p} of R , the $R_{\mathfrak{p}}$ -algebra $S_{\mathfrak{p}}$ is free. It then follows that S is commutative, since the map R -linear map $S \times S \rightarrow S$ by $(x, y) \mapsto xy - yx$ is zero at every localization, hence identically zero. Further, for each prime \mathfrak{p} , there exists $f \in R \setminus \mathfrak{p}$ such that S_f is free over R_f . Since $\text{Spec } R$ is quasi-compact, it is covered by finitely many such $\text{Spec } R_f$, and the uniqueness of the involution defined on each S_f implies that they agree on intersections and thereby yield a (unique) involution on S .

To conclude, we must show that $\text{gdeg}_R(S) = 2$. But any base extension of S has rank at most 2 so has degree at most 2, and the result follows. \square

Remark 2.10. It follows from Lemma 2.9 that in fact $\text{nrd}(x) = \bar{x}x = x\bar{x}$.

By covering any R -algebra B with a standard involution by quadratic algebras, we have the following corollary.

Corollary 2.11. *If B has a standard involution, then this involution is unique.*

Proof. By localizing at all primes of R , we may assume without loss of generality that B is free over R . Choose a basis for B over R . For any element x of this basis, from Corollary 1.7 we conclude that $S = R[x]$ is free, hence projective; by Example 2.6 (if $S = R$) or Lemma 2.9, we conclude that S has a unique standard involution. By R -linearity, we see that B itself has a unique standard involution. \square

For the rest of this section, we relate the (geometric) degree of B to the existence of a standard involution. We have already seen that if B has a standard involution, then it has degree at most 2. The converse is not true, as the following example (see also Example 1.20) illustrates.

Example 2.12. Let $R = \mathbb{F}_2$ and let B be a Boolean ring of rank at least 3 over \mathbb{F}_2 . Then B has degree 2, since every element $x \in B$ satisfies $x^2 = x$. The unique standard involution on any subalgebra $R[x]$ with $x \in B \setminus R$ is the map $x \mapsto \bar{x} = x + 1$, but this map is not R -linear, since

$$\overline{x+y} = 1 + (x+y) \neq \bar{x} + \bar{y} = 1 + x + 1 + y = x + y$$

for any $x, y \in B$ such that $1, x, y$ are linearly independent over \mathbb{F}_2 . It is moreover not an involution, since if $x \neq y \in B \setminus R$ satisfy $xy \notin R$, then

$$\overline{xy} = 1 + xy \neq \bar{y}\bar{x} = (1+y)(1+x) = 1 + x + y + xy.$$

We see from Example 2.12 that the condition of R -linearity is essential. We are led to the following key lemma.

Lemma 2.13. *Suppose that B has an R -linear map $\bar{} : B \rightarrow B$ with $\bar{1} = 1$ such that $x\bar{x} \in R$ for all $x \in B$. Then $\bar{}$ is a standard involution on B .*

Proof. We must prove that $\bar{}$ is an anti-involution, i.e., $\overline{xy} = \bar{y}\bar{x}$ for all $x, y \in B$. We can check that this equality holds over all localizations, so we may assume that B is free over R . Since $\bar{}$ is R -linear, we may assume $x, y \in B \setminus R$ are part of an R -basis for B which includes 1. Write $xy = a + bx + cy + z$ with z linearly independent of $1, x, y$. Replacing x by $x - c + 1$ (again using R -linearity), we may assume without loss of generality that $c = 1$. It follows that $1, xy$ belongs to a basis for B , so by Corollary 1.7 we have $R[xy]$ free over R .

Now notice that

$$(xy)(\bar{y}\bar{x}) = x(y\bar{y})\bar{x} = (x\bar{x})(y\bar{y}) = (\bar{y}y)(\bar{x}x) = (\bar{y}\bar{x})(xy) \in R$$

and also (using R -linearity one last time)

$$xy + \bar{y}\bar{x} = (x + \bar{y})(\overline{x + \bar{y}}) - x\bar{x} - y\bar{y} \in R.$$

But then

$$(xy)^2 - (xy + \bar{y}\bar{x})xy + (\bar{y}\bar{x})(xy) = 0$$

as well as

$$(xy)^2 - (xy + \overline{xy})xy + \overline{xy}(xy) = 0$$

and so by the uniqueness in Lemma 1.6 we conclude that $\overline{xy} = \bar{y}\bar{x}$. \square

With this lemma in hand, we prove the following central result.

Proposition 2.14. *B has a standard involution if and only if $\text{gdeg}_R(B) \leq 2$.*

Proof. First, suppose that B is free with basis x_1, \dots, x_m . We refer to Lemma 1.23; consider the element $\xi = a_1x_1 + \dots + a_mx_m \in B_{R[a]}$, with $R[a] = R[a_1, \dots, a_m]$ a polynomial ring.

The total degree map on $R[a]$ defines a grading of $R[a]$. We have a natural induced grading on $B_{R[a]}$ as an $R[a]$ -module, taking coefficients in the basis x_1, \dots, x_m . Since the coefficients of multiplication in $B_{R[a]}$ are elements of R and so have degree 0, we see that this grading respects multiplication in B . In this grading, the element ξ has degree 1.

Suppose that $\text{gdeg}_R(B) \leq 2$. The proposition is true if $B = R$, so we may assume $\text{gdeg}_R(B) = 2$. Then $\text{deg}_{R[a]}(\xi) = 2$, so there exist polynomials $t(a), n(a) \in R[a]$ such that

$$\xi^2 - t(a)\xi + n(a) = 0.$$

This equality must hold in each degree, so looking in degree 2 we may assume that $t(a)$ has degree 1 (and $n(a)$ has degree 2). By specialization, it follows that $t(a)$ induces an R -linear map $\bar{} : B \rightarrow B$ by $x \mapsto t(x) - x$ with the property that $x\bar{x} = n(x) \in R$ for all $x \in B$. This map is then a standard involution by Lemma 2.13.

Conversely, suppose that B has a standard involution. Define the maps (of sets) $t, n : B \rightarrow R$ by $\text{trd}(x) = x + \bar{x}$ and $\text{nrd}(x) = x\bar{x}$ for $x \in B$, so that $x^2 - \text{trd}(x)x + \text{nrd}(x) = 0$ for all $x \in B$. Define

$$t(a) = \sum_{i=1}^n \text{trd}(x_i)a_i \in R[a]$$

and

$$n(a) = \sum_{i=1}^n \text{nrd}(x_i)a_i^2 + \sum_{1 \leq i < j \leq n} (\text{nrd}(x_i + x_j) - \text{nrd}(x_i) - \text{nrd}(x_j))a_i a_j \in R[a].$$

Then $t(a)$ has degree 1 and $n(a)$ has degree 2. Now consider the element

$$(2.15) \quad \xi^2 - t(a)\xi + n(a) = \sum_{k=1}^n c_k(a)x_k \in B_{R[a]}.$$

Each polynomial $c_k(a) \in R[a]$ in (2.15) has degree 2. If we let e_i be the coordinate point $(0, \dots, 0, 1, 0, \dots, 0)$ with 1 in the i th place for $i = 1, \dots, m$, then by construction $c_k(e_i) = c_k(e_i + e_j) = 0$ for all i, j , and therefore $c_k(a) = 0$ identically. Therefore $\text{deg}_{R[a]}(\xi) = 2$ and $\text{gdeg}_R(B) = 2$, as claimed.

Now let B be an arbitrary R -algebra. If $\text{gdeg}_R(B) \leq 2$, then by localization and uniqueness (Corollary 2.11) the result follows from the case where B is free. Conversely, if B has a standard involution, we conclude that $\text{gdeg}_R(B_{\mathfrak{p}}) \leq 2$ for all primes $\mathfrak{p} \in B$. The result then follows from Lemma 1.25. \square

We conclude this section by relating the existence of a standard involution to degree (not geometric degree).

Proposition 2.16. *Suppose that $\text{deg}_R(B) = 2$ and suppose that there exists $a \in R$ such that $a(a - 1)$ is a nonzerodivisor. Then there is a standard involution on B .*

Proof. Again by localization and uniqueness, we may suppose that B is free with basis x_1, \dots, x_m with $x_1 = 1$. Thus for each i , the algebra $S_i = R[x_i]$ is free and by Lemma 2.9 there is a unique standard involution on S_i . This involution extends by R -linearity to a map $\bar{} : B \rightarrow B$, which (for the moment) is just an R -linear map whose restriction to each S_i is a standard involution. For $x \in B$, we define $t(x) = x + \bar{x}$ and $n(x) = x\bar{x}$.

We need to show that in fact $n(x) \in R$ for all $x \in B$, for then $\bar{}$ is a standard involution by Lemma 2.13. Let $x, y \in B$ satisfy $n(x), n(y) \in R$. Since

$$\begin{aligned} n(x + y) &= (x + y)\overline{(x + y)} = x\bar{x} + y\bar{y} + x\bar{y} + y\bar{x} \\ &= n(x) + n(y) + t(y)x + t(x)y - (xy + yx) \end{aligned}$$

we have $n(x+y) \in R$ if and only if $xy + yx - t(y)x + t(x)y \in R$, or equivalently if

$$(x+y)^2 - t(x+y)(x+y) \in R.$$

By this criterion, it is clear that $n(x+y) \in R$ if and only if $n(ax+by) \in R$ for all $a, b \in R$. So it is enough to prove that $n(x+y) \in R$ when $1, x, y$ is part of a basis for B with $n(x), n(y) \in R$.

Let $a \in R$. By Lemma 1.7, since $x+ay$ is contained in a basis for B we have that $R[x+ay]$ is free over R . Letting $a = 1$, we have that $R[x+y]$ is free so $x+y$ satisfies a unique polynomial of degree 2 over R , hence there exists a unique $u \in R$ such that $(x+y)^2 - u(x+y) \in R$. From the above, $n(x+y) \in R$ if and only if $u = t(x+y)$.

We have

$$(x+ay)^2 = x^2 + a(xy+yx) + a^2y^2 = a(xy+yx) + t(x)x + a^2t(y)y \in B/R$$

and since

$$xy+yx = (x+y)^2 - x^2 - y^2 = u(x+y) - t(x)x - t(y)y \in B/R$$

we have

$$(x+ay)^2 = (au - at(x) + t(x))x + (au - at(y) + a^2t(y))y \in B/R.$$

But $\deg_R(B) = 2$, so $(x+ay)^2$ is an R -linear combination of $1, x+ay$. But this can only happen if

$$a(au - at(x) + t(x)) = (au - at(y) + a^2t(y))$$

which becomes simply

$$a(a-1)(u - t(x) - t(y)) = 0.$$

So, if $a(a-1)$ is a nonzerodivisor, then we have $u = t(x) + t(y) = t(x+y)$, as desired. \square

We finish then by proving Theorem A.

Corollary 2.17. *Suppose that there exists $a \in R$ such that $a(a-1)$ is a nonzerodivisor. Then the following are equivalent:*

- (i) $\deg_R(B) = 2$;
- (ii) $\text{gdeg}_R(B) = 2$;
- (iii) $B \neq R$ and B has a standard involution.

Proof. Combine Proposition 2.14 with Proposition 2.16 and the trivial implication (ii) \Rightarrow (i). \square

3. COMMUTATIVE ALGEBRAS WITH A STANDARD INVOLUTION AND EXCEPTIONAL RINGS

In this section, we investigate two classes of algebras with a standard involution: commutative algebras and exceptional rings.

Proposition 3.1. *Let $J = \text{ann}_R(2) = \{x \in R : 2x = 0\}$ and let B be a commutative R -algebra. Then B has a standard involution if and only if either $\text{rk } B \leq 2$ or B is generated by elements x_1, \dots, x_n that satisfy $x_i^2 \in J$ for all i and $x_i x_j \in JB$ for all $i \neq j$.*

Consequently, if a commutative R -algebra B with $\text{rk } B > 2$ has a standard involution, then the involution is trivial.

Proof. Let B be a commutative R -algebra with a standard involution and assume that $\text{rk } B > 2$.

First, suppose that $2 = 0 \in R$. Let $1, x, y \in B$ be R -linearly independent. Then by (2.8) we have

$$0 = 2xy = xy + yx = \text{trd}(x)y + \text{trd}(y)x + \text{nrd}(x+y) - \text{nrd}(x) - \text{nrd}(y).$$

Therefore $\text{trd}(x) = \text{trd}(y) = 0$.

Now let R be any commutative ring. For any $x \in B$ such that $1, x$ is R -linearly independent, there exists $y \in B$ such that $1, x, y$ is R -linearly independent. By the preceding paragraph, by considering the image of x in the $R/2R$ -algebra $B/2B$ we conclude that $\text{trd}(x) = 2u \in 2R$. Replacing x by $x - u$, we conclude that we may write $B = R \oplus B_0$ where $B_0 = \{x \in B : \text{trd}(x) = 0\}$.

Again by (2.8), for any $x, y \in B_0$ such that $1, x, y$ are R -linearly independent, we have

$$2xy = n = \text{nrd}(x+y) - \text{nrd}(x) - \text{nrd}(y) \in R.$$

But then

$$x(2xy) = 2x^2y = -2\text{nrd}(x)y = nx,$$

and this is a contradiction unless $n = 2\text{nrd}(x) = 0$. Thus $2xy = 0$ and hence $xy \in JB$, and $x^2 = a$ with $a = -\text{nrd}(x) \in J$.

The conversely is easily verified, equipping B with the trivial standard involution. \square

Corollary 3.2. *If 2 is a nonzerodivisor in R and $\text{rk } B > 2$ then B has a standard involution if and only if B is a quotient of the algebra*

$$R[x_1, \dots, x_n]/(x_1, \dots, x_n)^2.$$

If $2 = 0 \in R$ and $\text{rk } B > 2$ then B has a standard involution if and only if B is a quotient of the algebra

$$R[x_1, \dots, x_n]/(x_1^2 - a_1, \dots, x_n^2 - a_n)$$

with $a_i \in R$.

We now investigate the class of exceptional rings, first defined in the introduction. Let M be a projective R -module M of rank $n - 1$ and let $t : M \rightarrow R$ be an R -linear map. Then we define the R -algebra $B = R \oplus M$ by the rule $xy = t(x)y$ for $x, y \in M$. This algebra is indeed associative because

$$(xy)z = (t(x)y)z = t(x)yz = x(yz)$$

for all $x, y, z \in M$. The map $\bar{} : M \rightarrow M$ by $x \mapsto t(x) - x$ is an R -linear map, and since $x^2 = t(x)x$ we have $x\bar{x} = 0 \in R$ for all $x \in M$. We conclude by Lemma 2.13 that $\bar{}$ defines a standard involution on B .

Definition 3.3. *An R -algebra B of rank n is an exceptional ring if there is a left ideal $M \subset B$ such that $B = R \oplus M$ and the map $M \rightarrow \text{Hom}_R(M, B)$ given by left multiplication factors through a linear map $t : M \rightarrow R$.*

It follows from the preceding paragraph that an exceptional ring has a standard involution. Since a standard involution is necessarily unique (Corollary 2.11), if $B = R \oplus M$ is exceptional, corresponding to $t : M \rightarrow R$, then we automatically have $t = \text{trd}$. If $R \rightarrow S$ is any ring homomorphism and B is an exceptional ring over R then $B \otimes_R S$ is an exceptional ring over S .

Remark 3.4. There is an equivalence of categories between the category of exceptional rings of rank n , with morphisms isomorphisms, and the category of R -linear maps $t : M \rightarrow R$, where a morphism between $t : M \rightarrow R$ and $t' : M' \rightarrow R$ is simply a map $f : M \rightarrow M'$ such that $t' \circ f = t$.

Lemma 3.5. *An R -algebra B is exceptional if and only if the set*

$$(3.6) \quad M = \{y \in B : xy \in Ry \text{ for all } x \in B\}.$$

is an R -module such that $B = R \oplus M$.

Proof. Suppose that M is nonzero and closed under addition. Note automatically that M is then a two-sided ideal of B . Let $x \in B$ and let $y, z \in M$ be R -linearly independent. Then $xy = ty$ and $xz = uz$ for some $t, u \in R$. But $x(y + z) = ty + uz \in R(y + z)$ so $t = u$. Therefore, we have a well-defined function $t : B \rightarrow R$ such that $xy = t(x)y$ for all $x \in B$ and $y \in M$. But then if $B = R \oplus M$, we have that B is exceptional by definition. \square

Corollary 3.7. *If B is an exceptional ring, then the splitting $B = R \oplus M$ is unique.*

Proof. The left ideal M in Definition 3.3 is uniquely characterized by (3.6). \square

Example 3.8. If B is quadratic, then B is an exceptional ring if and only if $B \cong R \times R$. We will show in the next section that every if $\text{rk } B = 3$ then B is exceptional.

Lemma 3.9. *An R -algebra B is exceptional if and only if $B_{\mathfrak{p}}$ is exceptional for all primes \mathfrak{p} of R .*

Proof. If B is exceptional then obviously $B_{\mathfrak{p}}$ is exceptional for all primes \mathfrak{p} . Conversely, consider the set M as in (3.6). By localization, we have that $B_{\mathfrak{p}} = R_{\mathfrak{p}} \oplus M_{\mathfrak{p}}$ is exceptional, and it follows that $B = R \oplus M$ is exceptional as well. \square

Exceptional rings can be distinguished by a comparison of minimal and characteristic polynomials. For an element $x \in B$, let $\mu(x; T) = T^2 - \text{trd}(x)T + \text{nrd}(x)$ and let $\chi_L(x; T)$ (resp. $\chi_R(x; T)$) be the characteristic polynomial of left (resp. right) multiplication as in Lemma 1.4. Recall from Section 1 that if $x \notin R$, then $\mu(x; T)$ is the polynomial which realizes $\deg_R(x) = 2$, i.e., it is the monic polynomial of smallest degree with coefficients in R which is satisfied by x . Let $\text{Tr}(x)$ denote the trace of left multiplication by x .

Lemma 3.10. *Let $B = R \oplus M$ be an exceptional ring. Then for all $x \in M$, we have $\mu(x; T) = T(T - \text{trd}(x))$ and*

$$\chi_L(x; T) = T(T - \text{trd}(x))^{n-1} = \mu(x; T)(T - \text{trd}(x))^{n-2}$$

so $\text{Tr}(x) = (n - 1) \text{trd}(x)$ and

$$\chi_R(x; T) = T^{n-1}(T - \text{trd}(x)).$$

Proof. This statement follows from a direct calculation. \square

4. ALGEBRAS OF RANK 3

We saw in Section 2 that an algebra of rank 2 is necessarily commutative, has (geometric and constant) degree 2, and has a (unique) standard involution. Quadratic R -algebras are classified by their discriminants, and this is a subject that has seen a great deal of study (see Knus [16]). In this section, we consider the next case, algebras of rank 3.

First, suppose that B is a free R -algebra of rank 3. We follow Gross and Lucianovic [10, §2] (see also Bhargava [4]). They prove that if B is commutative and R is a PID or a local ring, then B has an R -basis $1, i, j$ such that

$$(C) \quad \begin{aligned} i^2 &= -ac + bi - aj \\ j^2 &= -bd + di - cj \\ ij &= -ad \end{aligned}$$

with $a, b, c, d \in R$. But upon further examination, we see that their proof works for free R -algebras B over an arbitrary commutative ring R and that their calculations remain valid even when B is noncommutative, since they use only the associative laws. If we write

$$ji = r + si + tj$$

with $r, s, t \in R$, then the algebra (C) is associative if and only if

$$(4.1) \quad as = dt = 0 \quad \text{and} \quad r + ad = -bs = ct.$$

For example, B is commutative if and only if $r = -ad$ and $s = t = 0$.

We now consider the classification of such algebras B by degree. We assume that B has constant degree (otherwise see Example 4.6). If $\deg_R(B) = 3$, then B is commutative by Lemma 1.18. So we are left to consider the case $\deg_R(B) = 2$. Then the coefficients of j, i in i^2, j^2 , respectively, must vanish, so $a = d = 0$ in the laws (C), and we have $r = -bs = ct$ in (4.1). After the equivalences of Theorem A, it is natural to consider the case where further B has a standard involution. Then

$$0 = -ad = \bar{i}\bar{j} = \bar{j}\bar{i} = (-c - j)(b - i) = -bc + ci - bj + ji$$

so $ji = bc - ci + bj$ and $r = bc, s = -c, t = b$. Now replacing i by $\bar{i} = b - i$, and letting $u = b$ and $v = -c$ we obtain the equivalent multiplication rules

$$(NC) \quad \begin{aligned} i^2 &= ui & ij &= uj \\ j^2 &= vj & ji &= vi. \end{aligned}$$

Following Gross and Lucianovic, we call such a basis $1, i, j$ a *good basis*. Note that by definition an algebra with multiplication rules (NC) is exceptional, with $M = Ri \oplus Rj$. We have therefore proven that every free R -algebra B of rank 3 with a standard involution is an exceptional ring.

We have shown that there is a bijection between pairs $(u, v) \in R^2$ and free R -algebras of rank 3 with a standard involution equipped with a good basis. The natural action of $GL_2(R)$ on a good basis, defined by

$$(4.2) \quad \begin{pmatrix} i \\ j \end{pmatrix} \mapsto \begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix}$$

takes one good basis to another, and the induced action on R^2 is simply $(u, v) \mapsto (\alpha u + \beta v, \gamma u + \delta v)$. Therefore the set of good bases of B is a principal homogeneous space for the action of $GL_2(R)$, and we have proved the following.

Proposition 4.3. *Let N be a free module of rank 2. Then there is a bijection between the set of orbits of $GL(N)$ acting on N and the set of isomorphism classes of free R -algebras of rank 3 with a standard involution.*

Example 4.4. The map $R^2 \rightarrow R$ with $e_1, e_2 \mapsto u, v$ corresponds to the algebra (NC) . In particular, the zero map $R^2 \rightarrow R$ corresponds to the commutative algebra $R[i, j]/(i, j)^2$.

Remark 4.5. The universal element $\xi = x + yi + zj$ of the algebra B defined by the multiplication rules (NC) for $u, v \in R$ satisfies the polynomial

$$\xi^2 - (2x + uy + vz)\xi + (x^2 + uxy + vxz) = 0$$

hence $\text{gdeg}_R(B) = 2$ and this verifies (in another way) that any such algebra indeed has a standard involution.

The only algebra which is both of type (C) and (NC) is the algebra with $u = v = 0$ (or $a = b = c = d = 0$), i.e., the commutative algebra $R[i, j]/(i, j)^2$.

Example 4.6. We pause to exhibit in an explicit example the irregular behavior of an algebra which is not of constant degree. Roughly speaking, we can glue together an algebra of degree 2 and an algebra of degree 3 along a degenerate algebra of degree 3.

Let k be a field and let $R = k[a, b]/(ab)$, so that $\text{Spec } R$ is the variety of intersecting coordinate lines in the (affine) plane. Consider the free R -algebra B with basis $1, i, j$ and with multiplication defined by

$$\begin{aligned} i^2 &= bi - aj & ij &= -a^2 \\ j^2 &= ai - bj & ji &= b^2 - a^2 - bi + bj. \end{aligned}$$

We note that B indeed has degree 3, since for example $i^3 = b^2i + a^3$ is the monic polynomial of smallest degree satisfied by i .

We have $R_{(b)} \cong k(a)$ with $B_{(b)}$ isomorphic to the algebra above with $b = 0$; this algebra is commutative of rank 3, with $ij = ji = -a^2$ (and $i^2 = -aj$ and $j^2 = ai$). On the other hand, we have $R_{(a)} \cong k(b)$ with $B_{(a)}$ subject to $ij = 0 \neq b^2 - bi + bj = ji$ and $i^2 = bi, j^2 = -bj$, so $B_{(b)}$ is a noncommutative algebra of rank 3 and degree 2.

Now consider a (projective, not necessarily free) R -algebra B of rank 3 with a standard involution.

Lemma 4.7. *There exists a unique splitting $B = R \oplus M$ with M projective of rank 2 such that for all primes \mathfrak{p} of R and any basis i, j of $M_{\mathfrak{p}}$, the elements $1, i, j$ are a good basis for $B_{\mathfrak{p}}$.*

Proof. Let M be the union of all subsets $\{i, j\} \subset B$ such that i, j satisfy multiplication rules as in (NC) . We claim that $B = R \oplus M$ is the desired splitting. It suffices to show this locally, and for any prime \mathfrak{p} , the module $M_{\mathfrak{p}}$ contains all good bases for $B_{\mathfrak{p}}$ by the calculations above, and the result follows. \square

Let $B = R \oplus M$ as in Lemma 4.7. Consider the map

$$M \rightarrow \text{End}_R(M).$$

According to the multiplication laws (NC) , this map is well-defined and factors as $M \rightarrow R \subset \text{End}_R(M)$ through scalar multiplication, since it does so locally. It follows by definition that B is an exceptional ring, and that the splitting $B = R \oplus M$ agrees with that in Lemma 3.7.

Proposition 4.8. *Every R -algebra B of rank 3 with a standard involution is an exceptional ring. There is an equivalence of categories between the category of R -algebras B of rank 3*

with a standard involution and the category of R -linear maps $t : M \rightarrow R$ with M projective of rank 3.

Corollary 4.9. *There is a bijection between the set of isomorphism classes of R -algebras of rank 3 with a standard involution and isomorphism classes of R -linear maps $t : M \rightarrow R$ with M projective of rank 3.*

We conclude this section with the following observation. Consider now the *right* multiplication map $M \rightarrow \text{End}_R(M)$. When $M = R^2$ is free as in (NC) with basis i, j , we have under this map that

$$i \mapsto \begin{pmatrix} u & 0 \\ v & 0 \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & u \\ 0 & v \end{pmatrix}.$$

If $\text{ann}_R(u, v) = (0)$, then this map is injective. Note that $(u, v) = t(R^2) \subset R$, and $\text{ann}(u, v) = (0)$ if and only if $B_{\mathfrak{p}}$ is noncommutative for every prime ideal \mathfrak{p} , in which case we say B is *noncommutative everywhere locally*. We compute directly that element $k = vi - uj$ satisfies $k^2 = 0$, and hence is contained in the Jacobson radical of B . Indeed, we have $ki = kj = 0$, and of course $ik = uk$ and $jk = vk$. In any change of good basis as in (4.2), we find that $k' = (\alpha\delta - \beta\gamma)k$ with $\alpha\delta - \beta\gamma \in R^*$, so the R -module (or even two-sided ideal) generated by k is independent of the choice of good basis, and so we denote it $J(B)$. Note that $J(B)$ is free if and only if $\text{ann}_R(u, v) = (0)$.

More generally, suppose that $t : M \rightarrow R$ has $\text{ann}_R t(M) = (0)$, or equivalently that B is noncommutative everywhere locally. Then the right multiplication map is injective since it is so locally, and so the right multiplication map yields an injection $B \hookrightarrow \text{End}_R(M)$. By the above calculation, we see that two-sided ideals $J(B_{\mathfrak{p}})$ for each prime \mathfrak{p} patch together to give a well-defined two-sided ideal $J(B)$ of B which is projective of rank 1, and the image of B in $\text{End}_R(M)$ annihilates this rank 1 submodule. Conversely, given a flag $I \subset J$, we associate the subalgebra $B = R \oplus M$ where $M \subset \text{End}_R(I \subset J)$ (acting on the right) consists of elements which annihilate I . We obtain the following proposition.

Proposition 4.10. *There is a bijection between the set of isomorphism classes of R -algebras of rank 3 with a standard involution which are noncommutative everywhere locally and flags $I \subset J$ such that I, J are projective of ranks 1, 2.*

Example 4.11. If $M = R^2 \rightarrow R$ is the map $e_1 \mapsto 1$ and $e_2 \mapsto 0$, then the above correspondence realizes the associated algebra B as isomorphic to the upper-triangular matrices in $M_2(R)$.

5. TERNARY QUADRATIC MODULES AND CLIFFORD ALGEBRAS

Before proceeding to algebras of rank 4, we introduce ternary quadratic modules and the construction of the Clifford algebra which will be relevant to classification.

Let M, N be projective (finitely generated) R -modules. A *quadratic map* is a map $q : M \rightarrow N$ satisfying:

- (i) $q(rx) = r^2q(x)$ for all $r \in R$ and $x \in M$; and
- (ii) The map $T : M \times M \rightarrow N$ defined by

$$T(x, y) = q(x + y) - q(x) - q(y)$$

is R -bilinear.

Condition (ii) is equivalent to

$$(5.1) \quad q(x + y + z) = q(x + y) + q(x + z) + q(y + z) - q(x) - q(y) - q(z)$$

for all $x, y, z \in M$. A quadratic map $q : M \rightarrow N$ is equivalently a section of $\text{Sym}^2 M^\vee \otimes N$; see e.g. Wood [27, Chapter 2] for further discussion.

A *quadratic module* over R is a triple (M, I, q) where M, I are projective R -modules with $\text{rk}(I) = 1$ and $q : M \rightarrow I$ is a quadratic map. An *isometry* between quadratic modules (M, I, q) and (M', I', q') is a pair of R -module isomorphisms $f : M \xrightarrow{\sim} M'$ and $g : I \xrightarrow{\sim} I'$ such that $q'(f(x)) = g(q(x))$ for all $x \in M$, i.e., such that the diagram

$$\begin{array}{ccc} M & \longrightarrow & I \\ \wr \downarrow f & & \wr \downarrow g \\ M' & \longrightarrow & I' \end{array}$$

commutes. When $I = R$, we abbreviate (M, I, q) by simply (M, q) .

We now construct the Clifford algebra associated to a quadratic module, following Bichsel and Knus [6, §3]. Let (M, I, q) be a quadratic module over R . Write $I^{-1} = I^\vee = \text{Hom}(I, R)$ denote the dual of the invertible R -module I , and abbreviate $I^0 = R$ and $I^n = \underbrace{I \otimes \cdots \otimes I}_d$

for $d \in \mathbb{Z}_{\geq 1}$. The R -module

$$L[I] = \bigoplus_{d \in \mathbb{Z}} I^{\otimes d}$$

with multiplication given by the tensor product and the canonical isomorphism

$$\begin{aligned} I \otimes I^{-1} &\xrightarrow{\sim} R \\ x \otimes f &\mapsto f(x) \end{aligned}$$

has the structure of a (commutative) R -algebra. We call $L[I]$ the *Rees algebra* of I .

Let

$$T(M) = \bigoplus_{d=0}^{\infty} M^{\otimes d}$$

be the tensor algebra of M . Let $J(q)$ denote the two-sided ideal of $T(M) \otimes L[I]$ generated by elements

$$(5.2) \quad x \otimes x \otimes 1 - 1 \otimes q(x)$$

for $x \in M$. (For a detailed treatment of the Clifford algebra when $N = R$ see also Knus [16, Chapter IV].) The algebra $T(M)$ has a natural $\mathbb{Z}_{\geq 0}$ -grading (with $\delta(x) = 1$ for $x \in M$); doubling the natural grading on $L[I]$, so that $\delta(a) = 2$ for $a \in I$, we find that $J(q)$ has a \mathbb{Z} -grading. Thus, the algebra

$$C(M, I, q) = (T(M) \otimes L[I]) / J(q)$$

is also \mathbb{Z} -graded; we call $C(M, I, q)$ the *Clifford algebra* of (M, I, q) .

Let $C^0(M, I, q)$ denote the R -subalgebra of $C(M, I, q)$ consisting of elements in degree 0; we call $C^0(M, I, q)$ the *even Clifford algebra* of (M, I, q) . The R -algebra $C^0(M, I, q)$ has rank 2^{n-1} where $n = \text{rk } M$ [6, Proposition 3.5]. Indeed, if I is free over R , generated by a , then we have a natural isomorphism

$$C^0(M, I, q) \cong C^0(M, R, a^\vee \circ q)$$

where $a^\vee \in I^\vee = \text{Hom}(I, R)$ is the dual element to a . If further M is free over R with basis e_1, \dots, e_n , then $C^0(M, I, q)$ is a free R -algebra generated by $e_{i_1} \otimes e_{i_2} \otimes \dots \otimes e_{i_{2m}} \otimes (f^\vee)^m$ with $1 \leq i_1 < i_2 < \dots < i_{2m} \leq n$. We abbreviate $C^0(M, R, q)$ by simply $C^0(M, q)$.

We write $e_1 e_2 \dots e_d$ for the image of $e_1 \otimes e_2 \otimes \dots \otimes e_d \otimes 1$ in $C(M, I, q)$, for $e_i \in M$. A standard computation gives

$$(5.3) \quad xy + yx = T(x, y) \in C(M, I, q)$$

for all $x, y \in M$.

The *reversal map* defined by

$$x = e_1 e_2 \dots e_d \mapsto \bar{x} = e_d \dots e_2 e_1$$

is an involution on $C(M, I, q)$ which restricts to an involution on $C^0(M, I, q)$.

Remark 5.4. The reversal map $\bar{} : C(M, I, q) \rightarrow C(M, I, q)$ has the property that $x\bar{x} \in R$ for all pure tensors $x = e_1 e_2 \dots e_d$, so in particular for all $x \in M$; however, it does not always define a standard involution. It is easy to see that the reversal map defines a standard involution whenever $\text{rk}(M) \leq 2$.

More generally, for any $x, y, z \in M$, applying (5.3) we have

$$\begin{aligned} (x + yz)(\overline{x + yz}) &= (x + yz)(x + zy) = q(x) + yzx + xzy + q(y)q(z) \\ &= q(x) + q(y)q(z) - T(x, y)z + T(x, z)y + T(y, z)x. \end{aligned}$$

Suppose that $\bar{} : C(M, I, q) \rightarrow C(M, I, q)$ is a standard involution and $\text{rk}(M) \geq 3$. If x, y, z are R -linearly independent, then we must have $T(x, y) = T(x, z) = T(y, z) = 0$. Moreover, the fact that $(x + 1)(x + 1) = q(x) + 1 + 2x$ for all $x \in M$ implies that $2 = 0 \in R$. We conclude then that $2 = 0 \in R$ and the reversal map is the identity map (and $C(M, I, q)$ is commutative), and indeed under these assumptions the reversal map gives a standard involution. (Compare this to Proposition 3.1.)

Now let (M, I, q) be a ternary quadratic module, so that M has rank 3. Then by the above, the even Clifford algebra $C^0(M, I, q)$ is an R -algebra of rank 4. Explicitly, we have

$$(5.5) \quad C^0(M, I, q) \cong \frac{R \oplus (M \otimes M \otimes I^\vee)}{J^0(q)}$$

where $J^0(q)$ is the R -module generated by elements of the form

$$x \otimes x \otimes f - 1 \otimes f(q(x))$$

for $x \in M$ and $f \in I^\vee$. A standard calculation (similar to Remark 5.4, or see below) shows that the reversal map defines a standard involution on $C^0(M, I, q)$. The association $(M, I, q) \rightarrow C^0(M, I, q)$ is functorial with respect to isometries of quadratic modules and so we refer to it as the *Clifford functor*.

Example 5.6. Given the free module $M = R^3 = Re_1 \oplus Re_2 \oplus Re_3$ equipped with the quadratic form $q : M \rightarrow R$ by

$$(5.7) \quad q(xe_1 + ye_2 + ze_3) = q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy,$$

with $a, b, c, u, v, w \in R$, we compute directly that the Clifford algebra of M is given by

$$C^0(M, q) = R \oplus Re_2 e_3 \oplus Re_3 e_1 \oplus Re_1 e_2$$

and the map

$$(5.8) \quad \begin{aligned} B &\xrightarrow{\sim} C^0(M, I, q) \\ i, j, k &\mapsto e_2 e_3, e_3 e_1, e_1 e_2 \end{aligned}$$

gives an isomorphism to the algebra B where the following multiplication laws hold.

$$(Q) \quad \begin{array}{lll} i^2 = ui - bc & jk = a\bar{i} & kj = -vw + ai + wj + vk \\ j^2 = vj - ac & ki = b\bar{j} & ik = -uw + wi + bj + uk \\ k^2 = wk - ab & ij = c\bar{k} & ji = -uv + vi + uj + ck \end{array}$$

(One can recover the multiplication rule for kj, ik, ji given that for jk, ki, ij by applying the standard involution.) This construction has been attributed to Eichler and appears in Brzezinski [7] in the case $R = \mathbb{Z}$.

Such a free quaternion ring is commutative if and only if either $B \cong R[i, j, k]/(i, j, k)^2$ or

$$B \cong R[i, j, k]/(i^2 + bc, j^2 + ac, k^2 + ab, jk + ai, ki + bj, ij + ck)$$

with $a, b, c \in R$ satisfying $2a = 2b = 2c = 0$. (See also Section 3.)

Definition 5.9. A quaternion ring over R is an R -algebra B such that $B \cong C^0(M, I, q)$ with (M, I, q) a ternary quadratic module over R .

In the remainder of this paper, we investigate the class of quaternion rings. We note that if $R \rightarrow S$ is any ring homomorphism and B is a quaternion ring, then $B_S = B \otimes_R S$ is also a quaternion ring.

6. THE CANONICAL EXTERIOR FORM

We have seen in the previous section how via the Clifford functor to associate an R -algebra of rank 4 with a standard involution to a ternary quadratic module. In this section, we show how to do the converse; we will show in Section 9 that, up to a rigidification, this furnishes an inverse to the Clifford functor on its image. Throughout this section, let B be an R -algebra of rank 4 with a standard involution.

Following Bhargava [5] (who considered the case of commutative rings of rank 4) and a footnote of Gross and Lucianovic [10, Footnote 2], we define the following quadratic map.

Lemma 6.1. *There exists a unique quadratic map*

$$\phi_B : \bigwedge^2(B/R) \rightarrow \bigwedge^4 B$$

with the property that

$$\phi_B(x \wedge y) = 1 \wedge x \wedge y \wedge xy$$

for all $x, y \in B$.

Proof. We first define the map on sets $\varphi : B \times B \rightarrow \bigwedge^4 B$ by $(x, y) \mapsto 1 \wedge x \wedge y \wedge xy$, where $B \times B$ denotes the Cartesian product. This map descends to a map from $B/R \times B/R$. We have $\varphi(ax, y) = \varphi(x, ay)$ for all $x, y \in B$ and $a \in R$. Furthermore, we have $\varphi(x, x) = 0$ for all $x \in B$ and by (2.8) we have

$$(6.2) \quad \varphi(y, x) = 1 \wedge y \wedge x \wedge yx = -1 \wedge x \wedge y \wedge (-xy) = \varphi(x, y) = \varphi(x, -y)$$

for all $x, y \in B$. Finally, the map φ when restricted to each variable x, y separately yields a quadratic map $B/R \rightarrow \bigwedge^4 B$.

We now prove the existence of the map $\phi = \phi_B$ when B is free. Let $i, j, k \in B$ form a basis for B/R . Then $i \wedge j, j \wedge k, k \wedge i$ is a basis for $\bigwedge^2(B/R)$. It follows from (5.1) that to define a quadratic map $q : M \rightarrow N$ on a free module M is equivalent to choosing elements $q(x), q(x+y) \in N$ for x, y in any basis for M . We thereby define

$$(6.3) \quad \begin{aligned} \phi : \bigwedge^2(B/R) &\rightarrow \bigwedge^4 B \\ \phi(i \wedge j) &= \varphi(i, j) \\ \phi(i \wedge j + j \wedge k) &= \varphi(i - k, j) = \varphi(j, k - i) \end{aligned}$$

together with the cyclic permutations of (6.3). By construction, the map ϕ is quadratic.

Now we need to show that in fact $\phi(x \wedge y) = \varphi(x, y)$ for all $x, y \in B$. By definition and (6.2), we have that this is true if $x, y \in \{i, j, k\}$. For any $y \in \{i, j, k\}$, consider the maps

$$\begin{aligned} \varphi_y, \phi_y : B/R &\rightarrow \bigwedge^4 B \\ x &\mapsto \varphi(x \wedge y), \phi(x \wedge y) \end{aligned}$$

restricted to the first variable. Note that each of these maps are quadratic and they agree on the values $i, j, k, i - k, j - i, k - j$, so they are equal. The same argument on the other variable, where now we may restrict φ, ϕ with any $x \in B$, gives the result.

To conclude, for any R -algebra B there exists a finite cover of standard open sets $\{\text{Spec } R_f\}_f$ of $\text{Spec } R$ with $f \in R$ such that each localization B_f is free. By the above constructions, we have a map on each B_f and by uniqueness these maps agree on overlaps, so by gluing we obtain a unique map ϕ . \square

Remark 6.4. Note that we used in (6.3) in the proof of Lemma 6.1 that B has rank 4; indeed, if $\text{rk}(B) > 4$, there will be many ways to define the map ϕ .

We call the map $\phi_B : \bigwedge^2(B/R) \rightarrow \bigwedge^4 B$ in Lemma 6.1 the *canonical exterior form* of B .

Example 6.5. Let B be a free quaternion ring with basis i, j, k and multiplication laws as in (Q) in Example 5.6. We compute the canonical exterior form

$$\phi = \phi_B : \bigwedge^2(B/R) \rightarrow \bigwedge^4 B$$

directly. We have isomorphisms $\bigwedge^4 B \rightarrow R$ by $1 \wedge i \wedge j \wedge k \mapsto -1$ and

$$\bigwedge^2(B/R) \xrightarrow{\sim} R(j \wedge k) \oplus R(k \wedge i) \oplus R(i \wedge j) = Re_1 \oplus Re_2 \oplus Re_3.$$

With these identifications, the canonical exterior form $\phi : R^3 \rightarrow R$ has

$$\phi(e_1) = \phi(j \wedge k) = 1 \wedge j \wedge k \wedge jk = 1 \wedge j \wedge k \wedge (-ai) \mapsto a$$

and

$$\begin{aligned} \phi(e_1 + e_2) - \phi(e_1) - \phi(e_2) &= \phi(k \wedge (i - j)) - \phi(j \wedge k) - \phi(k \wedge i) \\ &= -1 \wedge k \wedge j \wedge ki - 1 \wedge k \wedge i \wedge kj = -w(1 \wedge k \wedge i \wedge j) \mapsto w. \end{aligned}$$

In this way, we see directly that $\phi(x(j \wedge k) + y(k \wedge i) + z(i \wedge j)) = q(xe_1 + ye_2 + ze_3)$ is identically the same form as in (5.7).

Example 6.6. Suppose that R is a Dedekind domain with field of fractions F . Then we can write

$$(6.7) \quad B = R \oplus \mathfrak{a}i \oplus \mathfrak{b}j \oplus \mathfrak{c}k$$

with $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subset F$ fractional R -ideals and $i, j, k \in B$. By the same reasoning as in the free case, we may assume that $1, i, j, k$ satisfy the multiplication rules (Q) , and then we say that the decomposition (6.7) is a *good pseudobasis*, and the canonical exterior form of B is, analogously as in Example 6.5, given by

$$\phi_B : \mathfrak{b}ce_1 \oplus \mathfrak{a}ce_2 \oplus \mathfrak{a}be_3 \rightarrow \mathfrak{a}bc$$

under the identification $\bigwedge^4 B \xrightarrow{\sim} \mathfrak{a}bc$ induced by $1 \wedge i \wedge j \wedge k \mapsto -1$; here, $\phi_B(xe_1 + ye_2 + ze_3)$ is given as in (5.7) but now with x, y, z in their respective coefficient ideals.

Example 6.8. Let B be a free exceptional ring $B = R \oplus M$ where M has basis i, j, k . Then by definition we have the following multiplication laws in B :

$$(E) \quad \begin{array}{lll} i^2 = ui & jk = vk & kj = wj \\ j^2 = vj & ki = wi & ik = uk \\ k^2 = wk & ij = uj & ji = vi. \end{array}$$

We then compute as in the previous example that the canonical form ϕ_B is identically zero.

Note that such an exceptional ring is commutative if and only if $B \cong R[i, j, k]/(i, j, k)^2$, in which case B is also a quaternion ring (Q) . In particular, the only free R -algebra which is both a quaternion ring and a exceptional ring is the (commutative) algebra $B \cong R[i, j, k]/(i, j, k)^2$.

Remark 6.9. From the above example, we see directly that a bijection between the set of orbits of $GL(R^3)$ on R^3 and the set of isomorphism classes of free exceptional rings of rank 4, where we associate to the triple $(u, v, w) \in R^3$ the algebra with multiplication laws as in (E) . This also follows from Remark 3.4.

Lucianovic [20, Proposition 1.8.1] instead associates to $(u, v, w) \in R^3$ the skew-symmetric matrix $M = \begin{pmatrix} 0 & w & -v \\ -w & 0 & u \\ v & -u & 0 \end{pmatrix}$, and $g \in GL_3(R)$ acts on M by $M \mapsto (\det g)({}^t g)^{-1} M g^{-1}$.

This more complicated (but essentially equivalent) association gives a bijection to the set of orbits of $GL(N)$ on $\bigwedge^2 N^\vee \otimes \bigwedge^3 N$.

Using the canonical exterior form, we can distinguish exceptional algebras in the class of algebras of rank 4 with a standard involution as follows.

7. CHARACTERIZING QUATERNION RINGS

In this section, we compare quaternion rings and exceptional rings of rank 4 and prove Theorem B. Throughout, we let B denote an R -algebra of rank 4 with a standard involution.

To begin, suppose that B is free over R . We will compute the ‘universal’ such free algebra, following Gross and Lucianovic [10] as follows. A basis $1, i, j, k$ for B is *good* if the coefficient of j (resp. k, i) in jk (resp. ki, ij) is zero. One can add suitable elements of R to any basis to turn it into a good basis.

Proposition 7.1. *If B is free R -algebra of rank 4 with a standard involution with good basis $1, i, j, k$, then*

$$(U) \quad \begin{aligned} i^2 &= ui - bc & jk &= a\bar{i} + v'k \\ j^2 &= vj - ac & ki &= b\bar{j} + w'i \\ k^2 &= wk - ab & ij &= c\bar{k} + u'j \end{aligned}$$

with $a, b, c, u, v, w, u', v', w' \in R$ which satisfy

$$(7.2) \quad \begin{pmatrix} a \\ b \\ c \end{pmatrix} \begin{pmatrix} u' & v' & w' \end{pmatrix} = 0 \quad \text{and} \quad \begin{pmatrix} u' - u \\ v' - v \\ w' - w \end{pmatrix} \begin{pmatrix} u' & v' & w' \end{pmatrix} = 0.$$

Conversely, any algebra defined by laws (U) subject to (7.2) is an algebra of rank 4 with standard involution equipped with the good basis $1, i, j, k$.

Proof. The result follows by an explicit calculation, considering the consequences of the associative laws $j(k\bar{k}) = (jk)\bar{k}$ and $(ij)k = i(jk)$, and the others one obtains by symmetry. For details, see Lucianovic [20, Proposition 1.6.2]. \square

We recall from Example 6.8 that the only R -algebra which is both a free quaternion ring and a free exceptional ring is the (commutative) algebra $B \cong R[i, j, k]/(i, j, k)^2$.

Lemma 7.3 ([20, Proposition 1.6.2]). *Let B be an algebra of rank 4 with a standard involution over R . If R is a domain, then either B is a quaternion ring or B is an exceptional ring.*

Proof. It is enough to check these conditions locally, so we may assume that B is free over R with multiplication laws (U). The conditions (7.2) over a domain yield either a quaternion ring (Q) or an exceptional ring (E). \square

Continuing to follow Gross and Lucianovic, we characterize quaternion rings as follows. Recall for $x \in B$ that $\chi_L(x; T)$ (resp. $\chi_R(x; T)$) denotes the characteristic polynomial of left (resp. right) multiplication by x , $\text{Tr}_L(x)$ (resp. $\text{Tr}_R(x)$) denotes the trace of left (resp. right) multiplication by x , and we let $\mu(x; T) = T^2 - \text{trd}(x)T + \text{nrd}(x)$.

Proposition 7.4. *Let B be an R -algebra of rank 4 with a standard involution. Then the following are equivalent:*

- (i) B is a quaternion ring;
- (ii_L) $\chi_L(x; T) = \mu(x; T)^2$ for all $x \in B$;
- (ii_R) $\chi_R(x; T) = \mu(x; T)^2$ for all $x \in B$;
- (iii_L) $2 \text{trd}(x) = \text{Tr}_L(x)$ for all $x \in B$;
- (iii_R) $2 \text{trd}(x) = \text{Tr}_R(x)$ for all $x \in B$;

If 2 is a nonzerodivisor in R , then these are further equivalent to

- (iv) $\chi_L(x; T) = \chi_R(x; T)$ for all $x \in B$.

Proof. These statements follow from a direct calculation. It is enough to check these conditions at each localization, so we may assume that B is free over R . Then the algebra B has multiplication laws as in (U). Let $\xi = xi + yj + zk \in B \otimes_R R[x, y, z]$. Then we compute that

$$\mu(\xi; T) = T^2 - (ux + vy + wz)T + n(x, y, z)$$

where

$$-n(x, y, z) = bcx^2 + (uv - cw)xy + (uw - bv)xz + acy^2 + (vw - au)yz + abz^2.$$

We also compute that

$$\chi_L(\xi; T) = \mu(\xi; T)(\mu(\xi; T) - (\alpha + \beta + \gamma)T),$$

and

$$\chi_R(\xi; T) = \mu(\xi; T)(\mu(\xi; T) + (\alpha + \beta + \gamma)T).$$

The equivalences now follow easily. \square

Corollary 7.5. *If $R \rightarrow S$ is flat, then B is a quaternion ring if and only if B_S is a quaternion ring.*

Proof. If S is flat over R then the map $B \rightarrow B_S$ is injective, and the first result follows by checking condition (ii) in Proposition 7.4 over B_S . \square

Proposition 7.6. *Let B be an R -algebra of rank 4 with a standard involution. Then B is an exceptional ring if and only if the canonical exterior form ϕ_B of B is identically zero.*

Proof. One direction is proved in Example 6.8. Conversely, suppose that the canonical exterior form ϕ_B is zero. By localizing and Lemma 3.9, we may assume that B is free over R with multiplication laws (U) . Applying the standard involution, we have

$$(u - i)(w - k) = \bar{i}\bar{k} = \overline{ki} = bj + w'\bar{i} = bj + w'(u - i)$$

so

$$ik = u(w' - w) - (w' - w)i + bj + uk.$$

and similarly we have the products ji and kj .

We again identify $\bigwedge^4 B \xrightarrow{\sim} R$ by $1 \wedge i \wedge j \wedge k \mapsto -1$. We compute that $1 \wedge i \wedge j \wedge ij = c = 0$ and by symmetry $a = b = 0$. Similarly, we have

$$\phi(i \wedge (j - k)) = -1 \wedge i \wedge k \wedge ij - 1 \wedge i \wedge j \wedge ik = -u' + u = 0.$$

Thus $u' = u$, and by symmetry $v' = v$ and $w' = w$. It follows then that $B = R \oplus M$ is an exceptional ring with $M = Ri \oplus Rj \oplus Rk$ (see also Lemma 3.5). \square

Corollary 7.7. *The set of primes \mathfrak{p} such that $B_{\mathfrak{p}}$ is a quaternion (resp. exceptional) ring is closed in $\text{Spec } R$.*

Given an algebra of rank 4 over R with standard involution, there exists a decomposition $\text{Spec } R = \text{Spec } R_Q \cup \text{Spec } R_E$ such that the restriction B_{R_Q} of B to R_Q is a quaternion ring and B_{R_E} is an exceptional ring.

Proof. The statement for quaternion rings follows by noting that the conditions in Proposition 7.4 are preserved under specialization. The statement for exceptional rings follows similarly from 7.6.

The final statement follows from the fact that at each closed point $\text{Spec } k \rightarrow \text{Spec } R$ corresponding to a field gives a ring B_k which is either a quaternion ring or an exceptional ring by Lemma 7.3. Taking the Zariski closure, we obtain the result. \square

Remark 7.8. It is indeed possible for the set in Corollary 7.7 to be a proper subset of $\text{Spec } R$: an explicit example can be constructed in the same way as in Example 4.6.

Also note that if $\text{Spec } R_{QE} = \text{Spec } R_Q \cap \text{Spec } R_E$, then $B_{R_{QE}}$ is everywhere locally isomorphic to $R_{\mathfrak{p}}[i, j, k]/(i, j, k)^2$ for \mathfrak{p} a prime of R_{QE} .

We now put the pieces together and prove Theorem B.

Proof of Theorem B. We combine Proposition 7.4, Corollary 7.7, and Proposition 7.6, recalling that the only free algebra which is both a quaternion ring and an exceptional ring is commutative. \square

8. AN EQUIVALENCE OF CATEGORIES

In this final section, we prove Theorem C, which generalizes the following equivalence of Gross and Lucianovic.

Proposition 8.1 (Gross-Lucianovic). *Let N be a free module of rank 3. Then there is a bijection between the set of orbits $GL(N)$ on $\text{Sym}^2(N^\vee) \otimes \bigwedge^3 N$ and the set of isomorphism classes of free quaternion rings over R .*

This bijection has several nice properties. First, it is discriminant-preserving. We define the (half-)discriminant of a quadratic form $q(x, y, z)$ as in (5.7) by

$$(8.2) \quad D(q) = 4abc + uvw - au^2 - bv^2 - cw^2.$$

On the other hand, we define the (reduced) discriminant $D(B)$ of an algebra B of rank 4 with standard involution to be the ideal of R generated by all values

$$(8.3) \quad \{x, y, z\} = \text{trd}([x, y]\bar{z})$$

where $x, y, z \in B$ and $[,]$ denotes the commutator. If $1, i, j, k$ is a good basis for B , a direct calculation verifies that already

$$\{i, j, k\} = -D(q)$$

so the map preserves discriminants (as signs are ignored). In particular, every such exceptional ring B with good basis i, j, k has $\{i, j, k\} = 0$ so that $D(B) = 0$; hence if one restricts to R -algebras B with $D(B) \neq 0$ one will never see an exceptional ring, and it is perhaps for this reason that they fail to appear in more classical treatments.

We warn the reader that although the equivalence in Proposition 8.1 is functorial with respect to isometries and isomorphisms, respectively, it is not always functorial with respect to other morphisms, even inclusions.

Example 8.4. Consider the sum of squares form $q(x, y, z) = x^2 + y^2 + z^2$ over $R = \mathbb{Z}$. The associated quaternion ring B is generated over \mathbb{Z} by the elements i, j, k subject to $i^2 = j^2 = k^2 = -1$ and $ijk = -1$ and has discriminant 4. The ring B is an order inside the quaternion algebra of discriminant 2 over \mathbb{Q} which gives rise to the Hamiltonian ring over \mathbb{R} , and B is contained in the maximal order B_{\max} (of discriminant 2) obtained by adjoining the element $(1 + i + j + k)/2$ to B . Indeed, the ring B_{\max} is obtained from the Clifford algebra associated to the form $q_{\max}(x, y, z) = x^2 + y^2 + z^2 + yz + xz + yz$ of discriminant 2. However, the lattice associated to the form q is maximal in \mathbb{Q}^3 , so there is no inclusion of quadratic modules which gives rise to the inclusion $B \hookrightarrow B_{\max}$ of these two quaternion orders. Of course, if we consider the correspondence over \mathbb{Q} (or even $\mathbb{Z}[1/2]$) then the inclusion becomes an isomorphism, which shows that the lattice associated to each of the quadratic forms q and q_{\max} are contained in the same quadratic space over \mathbb{Q} , and the change of basis from one to the other is defined over $GL_3(\mathbb{Q})$ (but not $GL_3(\mathbb{Z})$).

Remark 8.5. There is an alternative association between forms and algebras which we call the *trace zero method* and describe for the sake of comparison (see also Lucianovic [20, Remark, pp. 28–29]). Let B be a free R -algebra of rank 4 with a standard involution and let $B^0 = \{x \in B : \text{trd}(x) = 0\}$ be the elements of reduced trace zero in B . Then $(B^0, \text{nrd}|_{B^0})$ is a ternary quadratic module.

Starting with a quadratic form (R^3, q) , considering the free quaternion algebra $B = C^0(R^3, q)$ with good basis as in (5.8), then the trace zero module (B^0, nrd) has basis $jk - kj, ki - ik, ij - ji$ and we compute that

$$\text{nrd}(x(jk - kj) + y(ki - ik) + z(ij - ji)) = D(q)q(x, y, z).$$

In particular, if $D(q) = D(B) \in R^*$, in which case q is said to be *semiregular*, we can instead associate to B the quadratic module $(B^0, D(B)^{-1} \text{nrd})$ to give an honest bijection. One can use this together with localization to prove a result for an arbitrary quadratic module (M, q) , as exhibited by Knus [18, §V.3]. This strategy works very well, for example, in the classical case where R is a field. When the discriminant of (M, q) is principal and R is a domain, one can similarly adjust the maps to obtain a bijection [7]. However, in general it is not clear how to generalize this method to quadratic forms which are not semiregular.

It is perhaps tempting to think that we will simply find a functorial bijection between isomtery classes of ternary quadratic modules over R and isomorphism classes of quaternion rings over R ; however, we notice one obstruction which does not appear in the free case.

Let (M, I, q) be a ternary quadratic module. Recall the definition of the even Clifford algebra $C^0(M, I, q)$ from Section 5. We find that as an R -module, we have

$$(8.6) \quad C^0(M, I, q)/R \cong \bigwedge^2 M \otimes I^\vee.$$

To analyze this isomorphism, we first note the following lemma.

Lemma 8.7. *Let M be a projective R -module of rank 3. Then there are isomorphisms*

$$(8.8) \quad \bigwedge^3(\bigwedge^2 M) \xrightarrow{\sim} (\bigwedge^3 M)^{\otimes 2}$$

and

$$(8.9) \quad \bigwedge^2(\bigwedge^2 M) \xrightarrow{\sim} M \otimes \bigwedge^3 M.$$

Proof. We exhibit first the isomorphism (8.8). We define the map

$$\begin{aligned} s : M^{\otimes 6} &\rightarrow (\bigwedge^3 M)^{\otimes 2} \\ x \otimes x' \otimes y \otimes y' \otimes z \otimes z' &\mapsto (x \wedge x' \wedge y') \otimes (y \wedge z \wedge z') \\ &\quad - (x \wedge x' \wedge y) \otimes (y' \wedge z \wedge z') \end{aligned}$$

with $x, x', y, y', z, z' \in M$.

It is easy to see that s descends to $(\bigwedge^2 M)^{\otimes 3}$; we show that s in fact descends to $\bigwedge^3(\bigwedge^2 M)$. We observe that

$$s(x \wedge x' \otimes y \wedge y' \otimes z \wedge z') = 0$$

whenever $x = y$ and $x' = y'$ (with similar statements for x, z and y, z). To finish, we show that

$$(8.10) \quad s((x \wedge x') \otimes (y \wedge y') \otimes (z \wedge z')) = -s((y \wedge y') \otimes (x \wedge x') \otimes (z \wedge z')).$$

To prove (8.10) we may do so locally and hence assume that M is free with basis e_1, e_2, e_3 ; by linearity, it is enough to note that

$$\begin{aligned} s((e_1 \wedge e_2) \otimes (e_2 \wedge e_3) \otimes (e_3 \wedge e_1)) &= (e_1 \wedge e_2 \wedge e_3) \otimes (e_2 \wedge e_3 \wedge e_1) \\ &= (e_2 \wedge e_3 \wedge e_1) \otimes (e_2 \wedge e_3 \wedge e_1) \\ &= -s((e_2 \wedge e_3) \otimes (e_1 \wedge e_2) \otimes (e_3 \wedge e_1)). \end{aligned}$$

It follows then also that s is an isomorphism, since it maps the generator

$$(e_1 \wedge e_2) \wedge (e_2 \wedge e_3) \wedge (e_3 \wedge e_1) \in \bigwedge^3(\bigwedge^2 M)$$

to the generator $(e_1 \wedge e_2 \wedge e_3) \otimes (e_2 \wedge e_3 \wedge e_1) \in (\bigwedge^3 M)^{\otimes 2}$.

The second isomorphism (8.9) arises from the map

$$(8.11) \quad \begin{aligned} M^{\otimes 4} &\rightarrow M \otimes \bigwedge^3 M \\ x \otimes x' \otimes y \otimes y' &\mapsto x' \otimes (x \wedge y \wedge y') - x \otimes (x' \wedge y \wedge y') \end{aligned}$$

and can be proved in a similar way. □

By (8.8) and (8.6), we find that

$$(8.12) \quad \bigwedge^4 C^0(M, I, q) \cong \bigwedge^3(C^0(M, I, q)/R) \cong \bigwedge^3(\bigwedge^2 M \otimes I^\vee) \cong (\bigwedge^3 M)^{\otimes 2} \otimes (I^\vee)^{\otimes 3}.$$

(Compare this with work of Kable et al. [13], who considers the Steinitz class of a central simple algebra over a number field, and the work of Peters [23] who works over a Dedekind domain.)

Cognizant of (8.12), we make the following definition. Let N be an invertible R -module. A *parity factorization* of N is an R -module isomorphism

$$p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} N$$

where P, Q are invertible R -modules. Note that N always has the *trivial* parity factorization $R^{\otimes 2} \otimes N \xrightarrow{\sim} N$. An isomorphism between two parity factorizations $p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} N$ and $p' : P'^{\otimes 2} \otimes Q' \xrightarrow{\sim} N'$ is given by isomorphism $P \xrightarrow{\sim} P', Q \xrightarrow{\sim} Q', N \xrightarrow{\sim} N'$ which commute with p, p' .

We are now ready for the main result in these sections.

Theorem 8.13. *There is a bijection*

$$\left\{ \begin{array}{l} \text{Isometry classes of ternary} \\ \text{quadratic modules } (M, I, q) \\ \text{over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Isomorphism classes of quaternion} \\ \text{rings } B \text{ over } R \text{ equipped with a parity} \\ \text{factorization } p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} \bigwedge^4 B \end{array} \right\}$$

which is functorial in the base ring R . In this bijection, the isometry class of a quadratic module (M, I, q) maps to the isomorphism class of the quaternion ring $C^0(M, I, q)$ equipped with the parity factorization

$$(8.14) \quad (\bigwedge^3 M \otimes (I^\vee)^{\otimes 2})^{\otimes 2} \otimes I \xrightarrow{\sim} \bigwedge^4 C^0(M, I, q).$$

Proof. Given a ternary quadratic (M, I, q) , we associate to it the even Clifford algebra $B = C^0(M, I, q)$ with (8.14) which is indeed a parity factorization, as in (8.12). The algebra B is a quaternion ring by definition.

In the other direction, we use the canonical exterior form $\phi_B : \Lambda^2(B/R) \rightarrow \Lambda^4 B$ as defined in (6.1). Let B be a quaternion ring with parity factorization $p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} \Lambda^4 B$. Then by dualizing, the map p gives an isomorphism

$$p^* : (P^\vee)^{\otimes 2} \xrightarrow{\sim} (\Lambda^4 B)^\vee \otimes Q.$$

Note that p^* defines a quadratic map $P^\vee \rightarrow (\Lambda^4 B)^\vee \otimes Q$ by $x \mapsto p^*(x \otimes x)$. We associate then to the pair (B, p) the ternary quadratic module associated to the quadratic map

$$(8.15) \quad \phi_B \otimes p^* : \Lambda^2(B/R) \otimes P^\vee \rightarrow \Lambda^4 B \otimes ((\Lambda^4 B)^\vee \otimes Q) \xrightarrow{\sim} Q.$$

We need to show that these associations are indeed adjoint to each other. First, given the algebra $C^0(M, I, q)$ with parity factorization p as in (8.14), we have by the above association the ternary quadratic module

$$(8.16) \quad \phi \otimes p^* : \Lambda^2(C^0(M, I, q)/R) \otimes (\Lambda^3 M)^\vee \otimes I^{\otimes 2} \rightarrow I.$$

From (8.6) and (8.9) we obtain

$$\Lambda^2(C^0(M, I, q)/R) \cong \Lambda^2(\Lambda^2 M \otimes I^\vee) \cong \Lambda^2(\Lambda^2 M) \otimes (I^\vee)^{\otimes 2} \cong M \otimes \Lambda^3 M \otimes (I^\vee)^{\otimes 2}$$

hence the ternary quadratic module $\phi \otimes p^*$ (8.16) has domain canonically isomorphic to

$$(M \otimes \Lambda^3 M \otimes (I^\vee)^{\otimes 2}) \otimes (\Lambda^3 M)^\vee \otimes I^{\otimes 2} \cong M$$

and so yields a quadratic map $\phi \otimes p^* : M \rightarrow I$.

To show that q is isometric to $\phi \otimes p^*$ we may do so locally, and therefore assume that M, I are free so that $q : R^3 \rightarrow R$ is given as in (5.7). Then the Clifford algebra $B = C^0(R^3, q)$ is a quaternion ring defined by the multiplication rules (Q). By Example 6.5, we indeed have an isometry between ϕ_B and q , as desired.

The other direction is proved similarly. Beginning with an R -algebra B with a parity factorization $p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} \Lambda^4 B$, we associate the quadratic map $\phi_B \otimes p^*$ as in (8.15); to this, we associate the Clifford algebra $C^0(\Lambda^2(B/R) \otimes P^\vee, Q, \phi_B \otimes p^*)$, which we abbreviate simply $C^0(B)$, with parity factorization

$$(8.17) \quad \Lambda^4 C^0(B) \xrightarrow{\sim} (\Lambda^3(\Lambda^2(B/R) \otimes P^\vee) \otimes (Q^\vee)^{\otimes 2})^{\otimes 2} \otimes Q.$$

From (8.8) we obtain the canonical isomorphism

$$\begin{aligned} \Lambda^3(\Lambda^2(B/R) \otimes P^\vee) &\cong \Lambda^3(\Lambda^2(B/R)) \otimes (P^\vee)^{\otimes 3} \\ &\cong (\Lambda^3(B/R))^{\otimes 2} \otimes (P^\vee)^{\otimes 3} \cong (\Lambda^4 B)^{\otimes 2} \otimes (P^\vee)^{\otimes 3}. \end{aligned}$$

But now applying the original parity factorization $p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} \Lambda^4 B$, we obtain

$$(\Lambda^4 B)^{\otimes 2} \otimes (P^\vee)^{\otimes 3} \cong (P^{\otimes 2} \otimes Q)^{\otimes 2} \otimes (P^\vee)^{\otimes 3} \cong P$$

so putting these together, the parity factorization (8.17) becomes simply

$$\Lambda^4 C^0(B) \cong P^{\otimes 2} \otimes Q.$$

Similarly, putting together (8.6), (8.9), and the dual isomorphism p^\vee to p , we have

$$\begin{aligned}
(8.18) \quad C^0(B)/R &= C^0(\wedge^2(B/R) \otimes P^\vee, Q, \phi_B \otimes p^*)/R \\
&\cong \wedge^2(\wedge^2(B/R) \otimes P^\vee) \otimes Q^\vee \\
&\cong \wedge^2(\wedge^2(B/R)) \otimes (P^\vee)^{\otimes 2} \otimes Q^\vee \\
&\cong B/R \otimes \wedge^3(B/R) \otimes (\wedge^4 B)^\vee \cong B/R.
\end{aligned}$$

We now show that there is a unique isomorphism $C^0(B) \xrightarrow{\sim} B$ of R -algebras which lifts the map in (8.18). It suffices to show this locally, since the map is well-defined up to addition of scalars) and hence we may assume that B is free with good basis $1, i, j, k$ (and that $P, Q \cong R$ are trivial). But then with this basis it follows that the map (5.8) is the already the unique map which identifies $C^0(B) \cong B$, and the result follows.

In this way, we have exhibited an equivalence of categories between the category of isometry classes of ternary quadratic modules (with morphisms isometries) and the category of quaternion rings B over R equipped with a parity factorization p (with morphisms isomorphisms). It follows that the set of equivalence classes under isometry and isomorphisms are in functorial bijection. \square

We note that Theorem 8.13 reduces to the bijection of Gross-Lucianovic (Proposition 8.1) when B is free. Compare this result with work of Balaji [2].

If one wishes only to understand isomorphism classes of quaternion rings, one can consider the functor which forgets the parity factorization. In this way, certain ternary quadratic modules will be identified. Following Balaji, we define a *twisted discriminant module* to be a quadratic module (P, Q, d) where P, Q are invertible R -modules, or equivalently an R -linear map $d : P \otimes P \rightarrow Q$. A *twisted isometry* between two quadratic modules (M, I, q) and (M', I', q') is an isometry between $(M \otimes P, I \otimes Q, q \otimes d)$ and (M', I', q') for some twisted discriminant module (P, Q, d) .

Corollary 8.19. *There is a functorial bijection*

$$\left\{ \begin{array}{l} \text{Twisted isometry classes of} \\ \text{ternary quadratic modules} \\ (M, I, q) \text{ over } R \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{Isomorphism classes of} \\ \text{quaternion rings } B \text{ over } R \end{array} \right\}.$$

Proof. Given a quaternion ring B over R , from the trivial parity factorization we obtain the ternary quadratic module $\phi_B : \wedge^2(B/R) \rightarrow \wedge^4 B$. By (8.16), we see that the choice of an (isomorphism class of) parity factorization $p : P^{\otimes 2} \otimes Q \xrightarrow{\sim} \wedge^4 B$ corresponds to twisting ϕ_B by $(P^\vee, (\wedge^4 B)^\vee \otimes Q, p^*)$, and the result follows. \square

The bijection of Theorem 8.13 is also discriminant-preserving as in the free case, when the proper definitions are made. We define the (*half-*)*discriminant* $D(M, I, q)$ of a quadratic module (M, I, q) to be ideal of R generated by $D(q|_N)$ for all free (ternary) submodules $N \subset M$. Then in this correspondence we have since $D(M, I, q)_\mathfrak{p} = D(C^0(M, I, q))_\mathfrak{p}$ since the bijection preserves discriminants in the local (free) case.

Remark 8.20. An R -algebra B is *Azumaya* if B is central and R -*simple* (or *ideal*, as in Rao [24]), that is to say every two-sided ideal I of B is of the form $\mathfrak{a}B$ with $\mathfrak{a} = I \cap R$, or equivalently that any R -algebra homomorphism $B \rightarrow B'$ is either the zero map or injective. Equivalently, B is Azumaya if and only if $B/\mathfrak{m}B$ is a central simple algebra over the field R/\mathfrak{m}

for all maximal ideals \mathfrak{m} of R , or if the map $B^e = B \otimes_R B^o \rightarrow \text{End}_R B$ by $x \otimes y \mapsto (z \mapsto xzy)$ is an isomorphism, where B^o is the opposite algebra. (For a proof of these equivalences, see Auslander-Goldman [1] or Milne [22, §IV.1].)

Suppose that B is an R -algebra of rank 4 with a standard involution. Then if B is Azumaya then in particular B is a quaternion ring. A quaternion ring is Azumaya if and only if $D(B) = R$, or equivalently if the twisted isometry class of ternary quadratic modules associated to B is semiregular (i.e. $D(M, I, q) = R$).

We conclude this paper with some comments on writing quaternion rings as crossed products using the correspondence of Theorem C, and we compare our definition of quaternion ring to that of Kanzaki [14, 15].

Let S be a quadratic R -algebra, let J be an invertible S -module, and let $b : J \times J \rightarrow S$ be a Hermitian form on J , an S -bilinear form which satisfies $\overline{b(x, y)} = b(y, x)$ for all $x, y \in J$, where $\overline{}$ is the standard involution on S . With this data, we define the R -algebra $\left(\frac{S, J, b}{R}\right) = S \oplus J$ with the multiplication rules $xy = b(x, y)$ for $x, y \in J$ and $xu = \overline{u}x$ for $u \in S$ and $x \in J$. In particular, we note that $x^2 = b(x, x) \in R$ for all $x \in J$. One can verify in a straightforward way that $\left(\frac{S, J, b}{R}\right)$ is indeed an (associative) R -algebra equipped with a standard involution given by $x \mapsto -x$ on J .

Remark 8.21. If $B = S \oplus J$ is an R -algebra of rank 4 with a standard involution such that S is a quadratic R -algebra and J is a projective S -module of rank 1, then it is not necessarily true that $J^2 \subset S$ as in the example above. Indeed, the free R -algebra $B = R \oplus Ri \oplus Rj \oplus Rij$ with $S = R \oplus Ri$ and $J = Sj = Rj \oplus Rij$ subject to $i^2 = i$, $j^2 = j$, and $ij + ji = i + j$ has $j^2 = j(ij) = j \notin S$.

Since J is projective over S and hence over R , there exists $u \in S$ and $x \in I$ such that x, ux are R -linearly independent. It follows that $\phi(u \wedge x) = 1 \wedge u \wedge x \wedge ux \neq 0$, and making this argument locally we conclude by Proposition 7.6 that $B = \left(\frac{S, J, b}{R}\right)$ is nowhere locally isomorphic to an exceptional ring, and in particular B is a quaternion ring. A quaternion ring B which is of the form $B \cong \left(\frac{S, J, b}{R}\right)$ is called a *crossed product*.

Proposition 8.22. *A quaternion ring B is a crossed product if and only if it corresponds in the bijection of Theorem C to a ternary quadratic module (M, I, q) with the property that M is an orthogonal direct sum $M = Q \oplus N$ where Q, N are of ranks 1, 2.*

Proof. We first compute the canonical exterior form ϕ corresponding to a crossed product $B = \left(\frac{S, J, b}{R}\right)$. We find that the domain of ϕ is

$$\wedge^2(B/R) \cong \wedge^2(S/R \oplus J) \cong (S/R \otimes_R J) \oplus \wedge^2 J$$

and we claim that in fact the summands $S/R \otimes_R J$ and $\wedge^2 J$ are orthogonal under ϕ . It is enough to prove this locally, in which case we can write $S = R \oplus Ri$ and $J = (R \oplus Ri)j = Rj \oplus Rk$ with $i, j \in B$ and $k = ij$. Then $i \wedge j, k \wedge i, j \wedge k$ is a basis for $\wedge^2(B/R)$, and we

compute that

$$\phi(j \wedge (k - i)) - \phi(i \wedge j) - \phi(j \wedge k) = 1 \wedge j \wedge k \wedge ij - 1 \wedge j \wedge i \wedge jk = 0$$

so that $i \wedge j$ is orthogonal to $k \wedge i$, and similarly that $i \wedge j$ is orthogonal to $j \wedge k$.

Conversely, suppose that the ternary quadratic module (M, I, q) has $M = Q \oplus N$ an orthogonal direct sum. From the expression (5.5) we compute that that

$$C^0(M, I, q) \cong \frac{R \oplus (N \otimes N \otimes I^\vee)}{J^0(q|_N)} \oplus (N \otimes Q) = S \oplus J$$

as R -modules, where $J^0(q|_N)$ is the R -module generated by elements of the form

$$x \otimes x \otimes f - 1 \otimes f(q(x))$$

for $x \in N$ and $f \in I^\vee$. To verify that J is an S -module and that the multiplication map on I gives a Hermitian form $b : I \times I \rightarrow S$, it suffices to prove this locally, whence we may assume that $N = Re_1 \oplus Re_2$ and $J = Re_3$ as in Example 5.6, so that

$$q(xe_1 + ye_2 + ze_3) = q(x, y, z) = ax^2 + by^2 + cz^2 + uyz + vxz + wxy.$$

Then in the above we have $1, k$ a basis for S and i, j a basis for J . By orthogonality, we have $u = v = 0$, so the multiplication laws (Q) read

$$\begin{array}{lll} i^2 = -bc & jk = a\bar{i} & kj = ai + wj \\ j^2 = -ac & ki = b\bar{j} & ik = wi + bj \\ k^2 = wk - ab & ij = c\bar{k} & ji = ck. \end{array}$$

The result follows. □

REFERENCES

- [1] Maurice Auslander and Oscar Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.
- [2] Venkata Balaji Thiruvallur Eesanaipaadi *Line-bundle-valued ternary quadratic forms over schemes*, J. Pure Appl. Algebra **208** (2007), 237–259.
- [3] Manjul Bhargava, *Higher composition laws and applications*, International Congress of Mathematicians, Vol. II, Eur. Math. Soc., Zürich, 2006, 271–294.
- [4] Manjul Bhargava, *Higher composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886.
- [5] Manjul Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2) **159** (2004), no. 3, 1329–1360.
- [6] W. Bichsel and M.-A. Knus, *Quadratic forms with values in line bundles*, Recent advances in real algebraic geometry and quadratic forms (Berkeley, CA, 1990/1991; San Francisco, CA, 1991), Contemp. Math., vol. 155, Amer. Math. Soc., Providence, 1994, 293–306.
- [7] J. Brzeziński, *A characterization of Gorenstein orders in quaternion algebras*, Math. Scand. **50** (1982), no. 1, 19–24.
- [8] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Amer. Math. Soc., Providence, R.I., 1964.
- [9] W.T. Gan, B.H. Gross, and G. Savin, *Fourier coefficients of modular forms on G_2* , Duke Math. J. **115** (2002), no. 1, 105169.
- [10] Benedict H. Gross and Mark W. Lucianovic, *On cubic rings and quaternion rings*, J. Number Theory **129** (2008), no. 6, 1468–1478.
- [11] Alexander J. Hahn, *Quadratic algebras, Clifford algebras, and arithmetic Witt groups*, Universitext, Springer-Verlag, New York, 1994.

- [12] Robin Hartshorne, *Algebraic geometry*, Graduate texts in mathematics, vol. 52, Springer-Verlag, New York, 1977.
- [13] Anthony C. Kable, Heather Russell, and Nilabh Sanat, *Steinitz classes of central simple algebras*, Acta Arith. **125** (2006), no. 4, 393–406.
- [14] Teruo Kanzaki, *On non-commutative quadratic extensions of a commutative ring*, Osaka J. Math. **10** (1973), 597–605.
- [15] Teruo Kanzaki, *Note on quaternion algebras over a commutative ring*, Osaka J. Math. **13** (1976), no. 3, 503–512.
- [16] Max-Albert Knus, *Quadratic forms, Clifford algebras and spinors*, Seminários de Matemática, 1, Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Ciência da Computação, Campinas, 1988.
- [17] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998.
- [18] Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin, 1991.
- [19] T.Y. Lam, *A first course in noncommutative rings*, 2nd ed., Graduate texts in mathematics, vol. 131, American Math. Soc., Providence, 2001.
- [20] M. Lucianovic, *Quaternion rings, ternary quadratic forms, and Fourier coefficients of modular forms on $PGSp_6$* , Ph.D. Thesis, Harvard University, 2003.
- [21] Bernard McDonald, *Linear algebra over commutative rings*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 87, Marcel Dekker, New York, 1984.
- [22] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, 1980.
- [23] M. Peters, *Ternäre und quaternäre quadratische Formen und Quaternionenalgebren*, Acta Arith. **15** (1969), 329–365.
- [24] M. L. Ranga Rao, *Azumaya, semisimple and ideal algebras*, Bull. Amer. Math. Soc. **78** (1972), 588–592.
- [25] Winfried Scharlau, *Quadratic and Hermitian forms*, Springer-Verlag, Berlin, 1985.
- [26] Marie-France Vignéras, *Arithmétique des algèbres de quaternions*, Lecture notes in mathematics, vol. 800, Springer, Berlin, 1980.
- [27] Melanie Wood, *Moduli spaces for rings and ideals*, Ph.D. dissertation, Princeton, 2009.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF VERMONT, 16 COLCHESTER AVE,
 BURLINGTON, VT 05401, USA
E-mail address: jvoight@gmail.com