RINGS OF LOW RANK WITH A STANDARD INVOLUTION

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.

Let R be a commutative ring (with 1). 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, faithfully projective R-module of constant rank.

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 [1], building on work of others; 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 [11]. 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 3.

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 with coefficients in R. Any *quadratic* algebra B, i.e. an algebra of rank 2, is necessarily commutative (see Lemma 2.9) and has degree 2. Moreover, a quadratic algebra has a unique R-linear (anti-)involution $\overline{} : B \to B$ such that $x\overline{x} \in R$ 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 $\deg_S(B \otimes_R$

Date: October 20, 2018.

1991 *Mathematics Subject Classification.* 16G30, 11E20, 16W10.

S) with $R \to S$ 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* $\operatorname{trd} : B \to R$ by $x \mapsto x + \overline{x}$ and the *reduced norm* by $\operatorname{nrd} : B \to R$ by $x \mapsto x\overline{x}$; then every element $x \in B$ satisfies the polynomial $\mu(x;T) = T^2 - \operatorname{trd}(x)T + \operatorname{nrd}(x)$.

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 faithfully projective R-module of rank $n-1$ and let $t : M \to R$ 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 $x \mapsto \overline{x} = t(x) - x$ 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 $M \to \operatorname{Hom}_R(M, B)$ given by left multiplication factors through a linear map $t : M \to R$.

Our second main result (Theorem 4.8) is as follows.

Theorem B. *An R-algebra B of rank 3 has a standard involution if and only if it is an exceptional ring.*

The results of this paper will be further used in an upcoming work [10] which investigates algebras of rank 4 with a standard involution, in an attempt to characterize quaternion rings over an arbitrary base ring.

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 and prove Theorem B (§4).

The author would like to thank Hendrik Lenstra for his suggestions and comments which helped to shape this research. We are particularly indebted to Melanie Wood who made many helpful remarks and suggestions. We would also like to thank David Speyer and the referee.

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 [9, §8.11] for an alternative approach.

Throughout this article, let R be a commutative 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, faithfully projective R-module. For a prime $\mathfrak{p}$ of R, we denote by $R_{\mathfrak{p}}$ the localization of R at $\mathfrak{p}$; we abbreviate $B_{\mathfrak{p}} = B \otimes_R R_{\mathfrak{p}}$ and for $x \in B$ we write $x_{\mathfrak{p}} = x \otimes 1 \in B_{\mathfrak{p}}$. Since B is (finitely generated and) faithfully projective, we have that $B_{\mathfrak{p}}$ is locally free of finite rank n, which we suppose throughout is independent of $\mathfrak{p}$ (automatic if R is connected), and we define the *rank* of B to be this common rank and denote $n = \mathrm{rk}_R(B)$. (An R-module M is faithfully projective if and only if M projective and faithfully flat; when R is noetherian and connected, M is faithfully projective if and only if M is projective.)

Remark 1.1. One may work with connected rings, since for an arbitrary ring R one has a statement for each of the connected components of $\operatorname{Spec} R$. 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 (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 hence projective, which implies that B/R and hence R is a direct summand of B. □

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 [8, Theorem IV.17] (see also the determinant-trace polynomial [8, 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 $n = \operatorname{rk}(B)$ 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 [4, Proposition II.2.2] (see also the proof of Proposition 2.9), 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 $\chi(x;x) = 0 \in R$. □

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 $\deg_R(x) \leq \operatorname{rk} B$ 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 as an R-module;*
(ii) *$R[x]$ is faithfully projective as an R-module;*
(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 $\deg_R(x) = \operatorname{rk}_R R[x]$.

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) ⇒ (ii) is trivial. To prove (ii) ⇒ (i), suppose that $R[x]$ is faithfully 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 $R[x]$ is faithfully projective, the value of $d = \operatorname{rk} R_{\mathfrak{p}}[x]$ does not depend on the prime ideal $\mathfrak{p}$. It follows that the surjective map $\bigoplus_{i=0}^{d-1} Re_i \to R[x]$ 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 $a_{d-1}x^{d-1} + \cdots + a_0 = 0$ with $a_i \in R$ then $g(T) = f(T) + a_{d-1}T^{d-1} + \cdots + a_0$ has $g(x) = 0$ so $f(T) = g(T)$ and $a_0 = \cdots = a_{d-1} = 0$, and the converse follows similarly.

The equivalence (iii) $\Leftrightarrow$ (iv) follows similarly. □

Corollary 1.7. *Suppose that* $\deg_R(x) = 2$*. Then* $R[x]$ *is faithfully projective if and only if* $ax \notin R$ *for all* $a \neq 0 \in R$*, and this holds if* $1, x$ *belongs to a basis for* B*.*

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

If $R \to S$ 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*

$$\begin{aligned} \operatorname{Spec} R &\to \mathbb{Z} \\ \mathfrak{p} &\mapsto \deg_{R_\mathfrak{p}}(x) \end{aligned}$$

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 $\mathfrak{a}_m \supsetneq \mathfrak{p} \supset \mathfrak{a}_{m-1}$, and consequently the map is lower semicontinuous. □

Corollary 1.10. *For any* $x \in B$ *with* $\deg_R(x) = n$*, the set of primes* $\mathfrak{p} \in \operatorname{Spec} R$ *where* $\deg_{R_\mathfrak{p}}(x) \geq n$ *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 faithfully projective, Lemma 1.9 is immediate since then in fact $\deg_{R_\mathfrak{p}}(x_\mathfrak{p}) = \operatorname{rk}(R[x]_\mathfrak{p})$ 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*.*

In other words, $\deg_R(B) = n$ if and only if n is the smallest positive integer such that every element of B satisfies a monic polynomial of degree n with coefficients in R.

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 [7] 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 $n = \operatorname{rk}_R(B)$, 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 $\deg_R(B) = n = \operatorname{rk}_R(B)$, 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. □

Example 1.19. Lemma 1.18 is false if merely B has degree $n = \operatorname{rk}_R(B)$ (but not 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* $\operatorname{gdeg}_R(B)$ *(or simply* $\operatorname{gdeg}(B)$*), is the maximum of* $\deg_S(B \otimes_R S)$ *for all maps $R \to S$ with S a (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 $\operatorname{gdeg}(B) = \deg_S(B \otimes_R S)$ 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 $x_1, \dots, x_m$ as an R-module, and define*

$$\xi = a_1 x_1 + \dots + a_m x_m = \sum_{i=1}^{m} a_i x_i \in B \otimes_R R[a].$$

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

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 $\deg_S(B \otimes_R S) \le \deg_{R[a]}(\xi)$, so $\operatorname{gdeg}(B) \le \deg_{R[a]}(\xi)$. But

$$\deg_{R[a]}(\xi) \le \deg_{R[a]}(B_{R[a]}) \le \operatorname{gdeg}(B)$$

by definition, so equality holds. □

We conclude with two results which characterize the geometric degree.

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

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

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

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

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) $\overline{} : B \to B$ *is an R-linear map which satisfies:*

(i) $\overline{1} = 1$,
(ii) $\overline{}$ *is an anti-automorphism, i.e.,* $\overline{xy} = \overline{y}\,\overline{x}$ *for all* $x, y \in B$, *and*
(iii) $\overline{\overline{x}} = x$ *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 $B \to B^{\mathrm{op}}$ such that the underlying R-linear map has order at most 2.

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

Example 2.3. The usual adjoint map $M_k(R) \to M_k(R)$ defined by $A \mapsto A^\dagger$ (with $AA^\dagger = A^\dagger A = \det(A)$) 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, Merkurjev, Rost, and Tignol [6]), we will not consider them here.

Example 2.4. To verify that an involution $\overline{} : B \to B$ is standard, it is not enough to check that $x\overline{x} \in R$ for x in a set of generators for B as an R-module. The Clifford algebra of a quadratic form in many variables gives a wealth of such examples, among others. See work of the author [10, Remark 1.9].

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

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

and hence $x + \overline{x} \in R$ for all $x \in B$ as well. Consequently, $(x+\overline{x})x = x(x+\overline{x})$ so $\overline{x}x = x\overline{x}$ for all $x \in B$.

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 $\operatorname{rk} B[1/2] = \operatorname{rk} B = 1$ so $B = R$.

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

$$x^2 - (x + \overline{x})x + \overline{x}x = 0 \tag{2.7}$$

identically we have $x^2 - \operatorname{trd}(x)x + \operatorname{nrd}(x) = 0$ 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

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

so

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

An R-algebra S is *quadratic* if S has rank 2. The following lemma is well-known [5, 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 $\deg_R(S) = \operatorname{gdeg}_R(S) = 2$, and there is a unique standard involution on S.*

Proof. First, suppose that S is free with basis $1, x$, so $S = R \oplus Rx = R[x]$ 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 $^{-} : R[x] \to R$ by $\overline{x} = t - x$, and we extend the map $^{-}$ by R-linearity to a standard involution on S. If $^{-} : S \to S$ is any standard involution then identically equation (2.7) holds; by uniqueness, we have $t = x + \overline{x}$ and $n = x\overline{x} = \overline{x}x$, and the involution $\overline{x} = t - x$ is unique.

We now use a standard localization and patching argument to finish the proof. By Lemma 1.3, we have $S \simeq R \oplus S/R$ with S/R locally free of rank 1, so there is an open cover $\operatorname{Spec} R = \bigcup_f \operatorname{Spec} R_f$ such that $S_f = S \otimes_R R_f$ is free with a basis containing 1 as in the previous paragraph. It follows that S is commutative, since the map R-linear map $S \times S \to S$ by $(x, y) \mapsto xy - yx$ is zero on the affine cover, hence identically zero; 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 $\operatorname{gdeg}_R(S) = 2$. But any base extension of S has rank at most 2 so has degree at most 2, and the result follows. □

Remark 2.10. It also follows from Lemma 2.9 that $\operatorname{nrd}(x) = \overline{x}x = x\overline{x}$.

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 faithfully 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 $x \mapsto \overline{x} = x + 1$, but this map is not R-linear, since

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

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

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

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 $^- : B \to B$ with $\overline{1} = 1$ such that $x\overline{x} \in R$ for all $x \in B$. Then $^-$ is a standard involution on B.*

Proof. We must prove that $^-$ is an anti-involution, i.e., $\overline{xy} = \overline{y}\,\overline{x}$ 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 $^-$ 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

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

and also (using R-linearity one last time)

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

But then

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

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 $\overline{xy} = \overline{y}\,\overline{x}$. □

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

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

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 $\operatorname{gdeg}_R(B) \leq 2$. The proposition is true if $B = R$, so we may assume $\operatorname{gdeg}_R(B) = 2$. Then $\deg_{R[a]}(\xi) = 2$, 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 $\overline{} : B \to B$ by $x \mapsto t(x) - x$ with the property that $x\overline{x} = n(x) \in R$ 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) $t, n : B \to R$ by $\operatorname{trd}(x) = x + \overline{x}$ and $\operatorname{nrd}(x) = x\overline{x}$ for $x \in B$, so that $x^2 - \operatorname{trd}(x)x + \operatorname{nrd}(x) = 0$ for all $x \in B$. Define

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

and

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

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

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

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 ith 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 $\deg_{R[a]}(\xi) = 2$ and $\operatorname{gdeg}_R(B) = 2$, as claimed.

Now let B be an arbitrary R-algebra. If $\operatorname{gdeg}_R(B) \leq 2$, 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 $\operatorname{gdeg}_R(B_{\mathfrak{p}}) \leq 2$ for all primes $\mathfrak{p} \in B$. The result then follows from Lemma 1.25. □

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

Proposition 2.16. *Suppose that* $\deg_R(B) = 2$ *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 $\overline{} : B \to B$, 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 $t(x) = x + \overline{x}$ and $n(x) = x\overline{x}$.

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

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

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

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

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. □

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) $\operatorname{gdeg}_R(B) = 2$*;*
(iii) $B \neq R$ *and* B *has a standard involution.*

Proof. Combine Proposition 2.14 with Proposition 2.16 and the trivial implication (ii) ⇒ (i). □

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.

First note that if B is a commutative R-algebra with a standard involution $\overline{} : B \to B$, then $\overline{}$ is in fact an R-algebra automorphism.

Proposition 3.1. *Let $J = \operatorname{ann}_R(2) = \{x \in R : 2x = 0\}$ and let B be a commutative R-algebra. Then B has a standard involution if and only if either* $\operatorname{rk} B \leq 2$ *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 $\operatorname{rk} B > 2$ has a standard involution, then the involution is trivial.

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

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

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

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

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 $\operatorname{trd}(x) = 2u \in 2R$. Replacing x by $x-u$, we conclude that we may write $B = R \oplus B_0$ where $B_0 = \{x \in B : \operatorname{trd}(x) = 0\}$.

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

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

But then

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

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

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

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

$$R[x_1, \dots, x_n]/(x_1, x_2, \dots, x_n)^2$$

for some $n \in \mathbb{Z}_{\geq 2}$.

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

$$R[x_1, \dots, x_n]/(x_1^2, x_2^2, \dots, x_n^2)$$

for some $n \in \mathbb{Z}_{\geq 2}$.

We now investigate the class of exceptional rings, first defined in the introduction. Let M be a faithfully projective R-module M of rank $n-1$ and let $t : M \to R$ 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 $x, y, z \in M$ (since $yz = t(y)z \in M$). The map $\overline{} : M \to M$ by $x \mapsto t(x) - x$ is an R-linear map, and since $x^2 = t(x)x$ we have $x\overline{x} = 0 \in R$ for all $x \in M$. We conclude by Lemma 2.13 that $\overline{}$ 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 $M \to \operatorname{Hom}_R(M, B)$ given by left multiplication factors through a linear map $t : M \to R$.*

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 $t : M \to R$, then we automatically have $t = \operatorname{trd}|_M$. If $R \to S$ is a ring homomorphism and B is an exceptional ring over R then $B \otimes_R S$ is an exceptional ring over S.

Example 3.4. Suppose B is a quadratic R-algebra. Then B is a free exceptional ring if and only if $B \cong R \times R$ or $B \cong R[x]/(x^2)$. Moreover, the splitting $B = R \oplus M$ (with $\operatorname{rk}_R(M) = 1$) is unique up to replacing M by its conjugate $\overline{M}$.

Lemma 3.5. *If B is an exceptional ring and* $\operatorname{rk}(B) > 2$, *then the splitting $B = R \oplus M$ is unique.*

Proof. Localizing, we may assume that B and M are free as R-modules. Suppose that $B = R \oplus M = R \oplus M'$ are splittings associated to linear maps $t : M \to R$ and $t' : M' \to R$. Let $x, y \in M$ be such that $1, x, y$ are R-linearly independent. Then $x = r + x'$ and $y = s + y'$ with $r, s \in R$ and $x', y' \in M'$. From $xy = t(x)y$ we have

$$(r + x')(s + y') = rs + sx' + (r + t'(x'))y' = t(x)(s + y') = t(x)s + t(x)y'.$$

Since $1, x', y'$ are R-linearly independent, we conclude from the coefficient of x' that $s = 0$ and hence $y = y' \in N$. Interchanging the roles of x and y we find $x = x' \in N$ as well. □

Remark 3.6. Consequently, there is an equivalence of categories between the category of exceptional rings of rank $n > 2$, with morphisms isomorphisms, and the category of R-linear maps $t : M \to R$ with M faithfully projective of rank $n - 1 > 1$, where a morphism between $t : M \to R$ and $t' : M' \to R$ is simply a map $f : M \to M'$ such that $t' \circ f = t$.

We will show in the next section that if $\operatorname{rk} B = 3$ and B has a standard involution then B is exceptional.

Lemma 3.7. *An R-algebra B with* $\operatorname{rk}(B) > 2$ *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, suppose $B_\mathfrak{p}$ is exceptional for all primes $\mathfrak{p}$ of R. By Lemma 3.5, we may write $B_\mathfrak{p} = R_\mathfrak{p} \oplus M_\mathfrak{p}$ uniquely for each prime $\mathfrak{p}$. Gluing, we have $B = R \oplus M$ where

$$M = \{x \in B : x_\mathfrak{p} \in M_\mathfrak{p} \text{ for all } \mathfrak{p}\}.$$

Similarly, by uniqueness the linear maps $t_\mathfrak{p} : M_\mathfrak{p} \to R_\mathfrak{p}$ glue to give a map $t : M \to R$ such that $xy = t(x)y$ for all $x, y \in M$. □

Remark 3.8. Lemma 3.7 is false when $\operatorname{rk}(B) = 2$, consequent to the fact that there exists a ring R and an element $a \in R$ such that a is a square in every localization $R_\mathfrak{p}$ but a itself is not a square: the algebra $B = R[x]/(x^2 - a)$ is then a counterexample.

Exceptional rings can be distinguished by a comparison of minimal and characteristic polynomials. For an element $x \in B$, let $\mu(x; T) = T^2 - \operatorname{trd}(x)T + \operatorname{nrd}(x)$ 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 $\operatorname{Tr}(x)$ denote the trace of left multiplication by x.

Lemma 3.9. *Let $B = R \oplus M$ be an exceptional ring. Then for all $x \in M$, we have $\mu(x;T) = T(T - \operatorname{trd}(x))$ and*

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

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

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

Proof. This statement follows from a direct calculation. □

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 [5]). 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 [3, §2] (see also Bhargava [2]). 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

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

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 if the algebra (C) is associative then

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

Moreover, B is associative and 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

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

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

$$(NC) \qquad \begin{array}{ll} i^2 = ui & ij = uj \\ j^2 = vj & ji = vi \end{array}$$

which are visibly associative. 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

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

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 $R^2 \to R$ with $e_1, e_2 \mapsto u, v$ corresponds to the algebra (NC). In particular, the zero map $R^2 \to R$ 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 $\mathrm{gdeg}_R(B) = 2$ 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 $\operatorname{Spec} R$ 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

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

We note that B indeed has degree 3, since for example $i^3 = b^2 i + a^3$ 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 (faithfully 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 faithfully 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. □

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

$$M \to \operatorname{End}_R(M).$$

According the multiplication laws (NC), this map is well-defined and factors as $M \to R \subset \operatorname{End}_R(M)$ 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 3.5.

Theorem 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 $t : M \to R$ with M faithfully projective of rank 2.*

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 $t : M \to R$ with M faithfully projective of rank 2.*

We conclude this section with the following observation. Consider now the *right* multiplication map $M \to \operatorname{End}_R(M)$. 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 $\operatorname{ann}_R(u,v) = (0)$, then this map is injective. Note that $(u,v) = t(R^2) \subset R$, and $\operatorname{ann}(u,v) = (0)$ 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 $\operatorname{ann}_R(u,v) = (0)$.

More generally, suppose that $t : M \to R$ has $\operatorname{ann}_R t(M) = (0)$, 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 $B \hookrightarrow \operatorname{End}_R(M)$. 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 faithfully projective of rank 1, and the image of B in $\operatorname{End}_R(M)$ annihilates this rank 1 submodule. Conversely, given a flag $I \subset J$, we associate the subalgebra $B = R \oplus M$ where $M \subset \operatorname{End}_R(I \subset J)$ (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 faithfully projective of ranks $1, 2$.*

Example 4.11. If $M = R^2 \to R$ 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 $M_2(R)$.

References

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

[2] Manjul Bhargava, *Higher composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2) **159** (2004), no. 2, 865–886.

[3] Benedict H. Gross and Mark W. Lucianovic, *On cubic rings and quaternion rings*, J. Number Theory **129** (2008), no. 6, 1468–1478.

[4] Robin Hartshorne, *Algebraic geometry*, Graduate texts in mathematics, vol. 52, Springer-Verlag, New York, 1977.

[5] Max-Albert Knus, *Quadratic forms, Clifford algebras and spinors*, Seminários de Matemática, 1, Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Ciência da Computaç ã o, Campinas, 1988.

[6] 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.

[7] T.Y. Lam, *A first course in noncommutative rings*, 2nd ed., Graduate texts in mathematics, vol. 131, American Math. Soc., Providence, 2001.

[8] Bernard McDonald, *Linear algebra over commutative rings*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 87, Marcel Dekker, New York, 1984.

[9] Winfried Scharlau, *Quadratic and Hermitian forms*, Springer-Verlag, Berlin, 1985.

[10] John Voight, *Characterizing quaternion rings over an arbitrary base*, J. Reine Angew. Math. **657** (2011), 113–134.

[11] 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