DISCRIMINANTS AND THE MONOID OF QUADRATIC RINGS

JOHN VOIGHT

Abstract. We consider the natural monoid structure on the set of quadratic rings over an arbitrary base scheme and characterize this monoid in terms of discriminants.

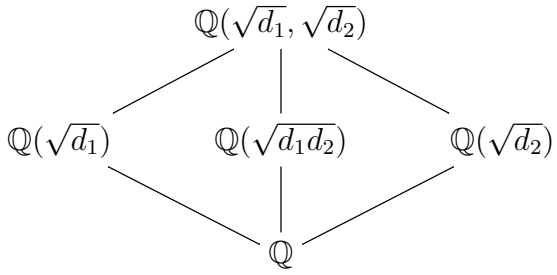
Quadratic field extensions K of $\mathbb{Q}$ are characterized by their discriminants. Indeed, there is a bijection

$$\left\{\begin{array}{c}\text{Separable quadratic}\\ \text{algebras over } \mathbb{Q}\\ \text{up to isomorphism}\end{array}\right\} \xrightarrow{\sim} \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$$
$$\mathbb{Q}[\sqrt{d}] = \mathbb{Q}[x]/(x^2-d) \mapsto d\mathbb{Q}^{\times 2}$$

where a separable quadratic algebra over $\mathbb{Q}$ is either a quadratic field extension or the algebra $\mathbb{Q}[\sqrt{1}] \simeq \mathbb{Q} \times \mathbb{Q}$ of discriminant 1. In particular, the set of isomorphism classes of separable quadratic extensions of $\mathbb{Q}$ can be given the structure of an elementary abelian 2-group, with identity element the class of $\mathbb{Q} \times \mathbb{Q}$: we have simply

$$\mathbb{Q}[\sqrt{d_1}] * \mathbb{Q}[\sqrt{d_2}] = \mathbb{Q}[\sqrt{d_1 d_2}]$$

up to isomorphism. If $d_1, d_2, d_1d_2 \in \mathbb{Q}^\times \setminus \mathbb{Q}^{\times 2}$ then $\mathbb{Q}(\sqrt{d_1d_2})$ sits as the third quadratic subfield of the compositum $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$:



Indeed, if σ_1 is the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d_1})/\mathbb{Q})$, then there is a unique extension of σ_1 to $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ leaving $\mathbb{Q}(\sqrt{d_2})$ fixed, similarly with σ_2, and $\mathbb{Q}(\sqrt{d_1d_2})$ is the fixed field of the composition $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

This characterization of quadratic extensions works over any base field F with $\mathrm{char}\, F \neq 2$ and is summarized concisely in the Kummer theory isomorphism

$$H^1(\mathrm{Gal}(\overline{F}/F), \{\pm 1\}) = \mathrm{Hom}(\mathrm{Gal}(\overline{F}/F), \{\pm 1\}) \simeq F^\times/F^{\times 2}.$$

On the other hand, over a field F with $\mathrm{char}\, F = 2$, all separable quadratic extensions have trivial discriminant and instead they are classified by the (additive) Artin-Schreier group

$$F/\wp(F) \quad \text{where} \quad \wp(F) = \{r + r^2 : r \in F\}$$

Date: April 16, 2016.

with the class of $a \in F$ in correspondence with the isomorphism class of the extension $F[x]/(x^2 - x + a)$. By similar considerations as above, we again find a natural structure of an elementary abelian 2-group on the set of isomorphism classes of separable quadratic extensions of F.

One can extend this correspondence between quadratic extensions and discriminants integrally, as follows. Let R be a commutative ring. An *R-algebra* is a ring B 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 via this embedding. A *free quadratic* R-algebra (also called a *free quadratic ring* over R) is an R-algebra S (associative with 1) that is free of rank 2 as an R-module. Let S be a free quadratic R-algebra. Then $S/R \simeq \wedge^2 S \simeq R$ is projective, so there is an R-basis $1, x$ for S; we find that $x^2 = tx - n$ for some $t, n \in R$ and that S is commutative. The map $\sigma : S \to S$ induced by $x \mapsto t - x$ is the unique *standard involution* on S, an R-linear (anti-)automorphism such that $y\sigma(y) \in R$ for all $y \in S$. The class of the *discriminant* of S

$$d = d(S) = (x - \sigma(x))^2 = t^2 - 4n$$

in $R/R^{\times 2}$ is independent of the choice of basis $1, x$. A discriminant d satisfies the congruence $d \equiv t^2 \pmod{4R}$, so for example if $R = \mathbb{Z}$ then $d \equiv 0, 1 \pmod 4$.

Now suppose that R is an integrally closed domain of characteristic not 2. Then there is a bijection

$$\left\{ \begin{array}{c} \text{Free quadratic rings over } R \\ \text{up to isomorphism} \end{array} \right\} \xrightarrow{\sim} \{d \in R : d \text{ is a square in } R/4R\}/R^{\times 2}$$
$$S \mapsto d(S)$$

For example, over $R = \mathbb{Z}$, the free quadratic ring $S(d)$ over $\mathbb{Z}$ of discriminant $d \in \mathbb{Z} = \mathbb{Z}/\mathbb{Z}^{\times 2}$ with $d \equiv 0, 1 \pmod 4$ is given by

$$S(d) = \begin{cases} \mathbb{Z}[x]/(x^2) \hookrightarrow \mathbb{Q}[x]/(x^2), & \text{if } d = 0; \\ \mathbb{Z}[x]/(x^2 - \sqrt{d}x) \hookrightarrow \mathbb{Q} \times \mathbb{Q}, & \text{if } d \neq 0 \text{ is a square;} \\ \mathbb{Z}[(d + \sqrt{d})/2] \hookrightarrow \mathbb{Q}(\sqrt{d}), & \text{otherwise.} \end{cases}$$

The set of discriminants under multiplication has the structure of a *commutative monoid*, a nonempty set equipped with a commutative, binary operation and identity element. Hence so does the set of isomorphism classes of free quadratic R-algebras, an operation we denote by $*$: the identity element is the class of $R \times R \simeq R[x]/(x^2 - x)$. The class of the ring $R[x]/(x^2)$ with discriminant 0 is called an *absorbing element*.

More generally, a *quadratic* R-algebra or *quadratic ring over* R is an R-algebra S which is locally free of rank 2 as an R-module. By definition, a quadratic ring over R localized at any prime (or maximal) ideal of R is a free quadratic R-algebra. Being true locally, a quadratic R-algebra S is commutative and has a unique standard involution.

There is a natural description of quadratic R-algebras as a stack quotient, as follows. A free quadratic R-algebra equipped with a basis $1, x$ has multiplication table uniquely determined by $t, n \in R$ and has no automorphisms, so the functor which associates to a commutative ring R the set of free quadratic R-algebras with basis (up to isomorphism) is represented by two-dimensional affine space $\mathbb{A}^2$ (over $\mathbb{Z}$). The change of basis for a free quadratic R-algebra is of the form $x \mapsto u(x + r)$ with $u \in R^\times$ and $r \in R$, mapping

$$(t, n) \mapsto (u(t + 2r), u^2(n + tr + r^2)).$$

Therefore, we have a map from the set of free quadratic R-algebras with basis to the quotient of $\mathbb{A}^2(R)$ by $G(R) = (\mathbb{G}_m \rtimes \mathbb{G}_a)(R)$ with the above action. Working over $\operatorname{Spec}\mathbb{Z}$, the group scheme G is naturally a subgroup scheme of GL_2, but it does not act linearly on $\mathbb{A}^2$, and the Artin stack $[\mathbb{A}^2/G]$ has dimension zero over $\operatorname{Spec}\mathbb{Z}$! Nevertheless, the set $[\mathbb{A}^2/G](R)$ is in bijection with the set of quadratic R-algebras up to isomorphism.

Recall that a commutative R-algebra S is *separable* if S is (faithfully) projective as an $S \otimes_R S$-module via the map $x \otimes y \mapsto xy$. A free quadratic R-algebra S is separable if and only if $d(S) \in R^\times$; so, for example, the only separable (free) R-algebra over $\mathbb{Z}$ is the ring $\mathbb{Z} \times \mathbb{Z}$ of discriminant 1, an impoverishment indeed! A separable quadratic R-algebra S is étale over R, and R is equal to the fixed subring of the standard involution of S over R. (In many contexts, one then says that S is Galois over R with Galois group $\mathbb{Z}/2\mathbb{Z}$, though authors differ on precise terminology. See Lenstra [13] for one approach to Galois theory for schemes.) If S, T are separable free quadratic R-algebras where R is a Dedekind domain of characteristic not 2, having standard involutions σ, τ, respectively, then the monoid product $S * T$ defined above (by transporting the monoid structure on the set of discriminants) is the fixed subring of $S \otimes_R T$ by $\sigma \otimes \tau$, in analogy with the case of fields.

The characterization of free quadratic R-algebras by their discriminants is an example of the parametrization of algebraic structures, corresponding to the Lie group A_1 in the language of Bhargava [2] (perhaps indexed by A_0 in the schema of Knus–Ojanguren–Parimala–Tignol [12, §15]).

Results in this direction go back to Gauss's composition law for binary quadratic forms and have been extended in recent years by Bhargava [4], Wood [21], and others. Indeed, several authors have considered the case of quadratic R-algebras, including Kanzaki [9] and Small [18]. In this article, we consider a very general instance of this monoidal correspondence between quadratic R-algebras and discriminants over an arbitrary base scheme.

Let X be a scheme. A *quadratic $\mathscr{O}_X$-algebra* is a coherent sheaf $\mathscr{S}$ of $\mathscr{O}_X$-algebras which is locally free of rank 2 as a sheaf of $\mathscr{O}_X$-modules. Equivalently, a quadratic $\mathscr{O}_X$-algebra is specified by a finite locally free morphism of schemes $\phi : Y \to X$ of degree 2 (sometimes called a *double cover*): the sheaf $\phi_*\mathscr{O}_Y$ is a sheaf of $\mathscr{O}_X$-algebras that is locally free of rank 2. If $f : X \to Z$ is a morphism of schemes, and $\mathscr{S}$ is a quadratic $\mathscr{O}_Z$-algebra, then the pullback $f^*\mathscr{S}$ is a quadratic $\mathscr{O}_X$-algebra. Let $\mathrm{Quad}(X)$ denote the set of isomorphism classes of quadratic $\mathscr{O}_X$-algebras, and for an invertible $\mathscr{O}_X$-module $\mathscr{L}$ let $\mathrm{Quad}(X; \mathscr{L}) \subseteq \mathrm{Quad}(X)$ be the subset of those algebras $\mathscr{S}$ such that there exists an isomorphism $\bigwedge^2 \mathscr{S} \simeq \mathscr{L}$ of $\mathscr{O}_X$-modules.

Our first result provides an axiomatic description of the monoid structure on the set $\mathrm{Quad}(X)$ (Theorem 3.27).

Theorem A. *There is a unique system of binary operations*

$$*_X : \mathrm{Quad}(X) \times \mathrm{Quad}(X) \to \mathrm{Quad}(X),$$

one for each scheme X, such that:

(i) $\mathrm{Quad}(X)$ *is a commutative monoid under $*_X$, with identity element the isomorphism class of $\mathscr{O}_X \times \mathscr{O}_X$;*

(ii) *The association* $X \mapsto (\mathrm{Quad}(X), *_X)$ *from schemes to commutative monoids is functorial in* X*: for each morphism* $f : X \to Z$ *of schemes, the diagram*

$$\begin{array}{ccc} \mathrm{Quad}(Z) \times \mathrm{Quad}(Z) & \xrightarrow{*_Z} & \mathrm{Quad}(Z) \\ \downarrow & & \downarrow{\scriptstyle f^*} \\ \mathrm{Quad}(X) \times \mathrm{Quad}(X) & \xrightarrow{*_X} & \mathrm{Quad}(X) \end{array}$$

is commutative; and

(iii) *If* $X = \operatorname{Spec} R$ *and* S, T *are separable quadratic* R*-algebras with standard involutions* σ, τ*, then* $S *_{\operatorname{Spec} R} T$ *is the fixed subring of* $S \otimes_R T$ *under* $\sigma \otimes \tau$*.*

The binary operation is defined locally (Construction 3.14): if $X = \operatorname{Spec} R$, and $S = R \oplus Rx$ and $T = R \oplus Ry$ are free quadratic R-algebras with $x^2 = tx - n$ and $y^2 = sy - m$ then we define the free quadratic R-algebra

$$S * T = R \oplus Rw$$

where

$$w^2 = (st)w - (mt^2 + ns^2 - 4nm).$$

This explicit description (in the free case over an affine base) is given by Hahn [8, Exercises 14–20, pp. 42–43].

A general investigation of the monoid structure on quadratic algebras goes back at least to Loos [14]. Loos gives via a universal construction a tensor product on the larger category of unital quadratic forms (quadratic forms representing 1); this category is equivalent to the category of quadratic algebras for forms on a finitely generated, projective module of rank 2 [14, Proposition 1.6] as long as one takes morphisms as isomorphisms in the category [15, §1.4]. (See also Loos [15, §6.1] for further treatment.) The existence of the monoid structure was also established in an unpublished letter of Deligne [6] by a different method: he associates to every R-algebra its discriminant algebra (a quadratic algebra) and extends the natural operation of addition of $\mathbb{Z}/2\mathbb{Z}$-torsors from the étale case to the general case by geometric arguments. Our proof of Theorem A above carries the same feel as these results, but it is accomplished in a more direct fashion and gives a characterization (in particular, uniqueness).

Recently, there has been renewed interest in the construction of discriminant algebras (sending an R-algebra A of rank n to a quadratic R-algebra) by Loos [15], Rost [17], and more recently by Biesel and Gioia [3]. Indeed, Biesel and Gioia [3, Section 8] describe the monoid operation in Theorem A over an affine base in the context of discriminant algebras. We hope that our theorem will have some application in this context.

Our second result characterizes quadratic algebras in terms of discriminants. A *discriminant* (over X) is a pair $(d, \mathscr{L})$ such that $\mathscr{L}$ is an invertible $\mathscr{O}_X$-module and $d \in (\mathscr{L}^\vee)^{\otimes 2}(X)$ is a global section which is a *square modulo* 4: there exists a global section $\overline{t} \in \mathscr{L}^\vee(X)/2\mathscr{L}^\vee(X) = \mathscr{L}^\vee \otimes \mathscr{O}_X/2\mathscr{O}_X$ such that $\overline{t} \otimes \overline{t} = \overline{d} \in (\mathscr{L}^\vee)^{\otimes 2}(X)/4(\mathscr{L}^\vee)^{\otimes 2}(X)$. We can of course also think of $d \in (\mathscr{L}^\vee)^{\otimes 2}(X)$ as an $\mathscr{O}_X$-module homomorphism $d : \mathscr{L}^{\otimes 2} \to \mathscr{O}_X$; but such a global section is also equivalently given by a quadratic form $D : \mathscr{L} \to \mathscr{O}_X$ (see section 2).

An isomorphism of discriminants $(d, \mathscr{L})$, $(d', \mathscr{L}')$ is an isomorphism $f : \mathscr{L} \xrightarrow{\sim} \mathscr{L}'$ such that $(f^\vee)^{\otimes 2}(d') = d$. For example, if $X = \operatorname{Spec} R$ for R a commutative ring and $\mathscr{L} = \mathscr{O}_X = \widetilde{R}$,

then as above a discriminant is specified by an element $d \in R$ such that $d \equiv t^2 \pmod{4R}$ for some $t \in R$ (noting that only $t \in R/2R$ matters), and two discriminants d, d' are isomorphic if and only if there exists $u \in R^\times$ such that $u^2 d' = d$. Thinking of a discriminant as a quadratic form $D : \mathscr{L} \to \mathscr{O}_X$, its image generates a locally principal ideal sheaf $\mathscr{I} \subseteq \mathscr{O}_X$, and the set of discriminants with given locally free image $\mathscr{I} \subseteq \mathscr{O}_X$, if nonempty, is a principal homogeneous space for the group $\mathscr{O}_X^\times / \mathscr{O}_X^{\times 2}$. Let $\mathrm{Disc}(X)$ denote the set of isomorphism classes of discriminants and $\mathrm{Disc}(X; \mathscr{L}) \subseteq \mathrm{Disc}(X)$ the subset with underlying line bundle $\mathscr{L}$. Then the tensor product

$$(d, \mathscr{L}) * (d', \mathscr{L}') = (d \otimes d', \mathscr{L} \otimes \mathscr{L}')$$

gives $\mathrm{Disc}(X)$ and $\mathrm{Disc}(X; \mathscr{O}_X)$ the structure of a commutative monoid with identity element the class of $(1, \mathscr{O}_X)$.

A quadratic $\mathscr{O}_X$-algebra $\mathscr{S}$ has a discriminant $\mathrm{disc}(\mathscr{S}) = (d(\mathscr{S}), \bigwedge^2 \mathscr{S})$, defined by

$$\begin{aligned} &d(\mathscr{S}) : (\textstyle\bigwedge^2 \mathscr{S})^{\otimes 2} \to \mathscr{O}_X \\ &(x \wedge y) \otimes (z \wedge w) \mapsto (x\sigma(y) - \sigma(x)y)(z\sigma(w) - \sigma(z)w) \end{aligned}$$

where σ is the unique standard involution on $\mathscr{S}$. Although a priori the codomain of $d(\mathscr{S})$ is $\mathscr{S}$, in fact its image lies in $\mathscr{O}_X$: if $X = \operatorname{Spec} R$ and $\mathscr{S} = \operatorname{Spec} S$ and S is free with basis $1, x$, then $(\bigwedge^2 S)^{\otimes 2}$ is freely generated by $(1 \wedge x) \otimes (1 \wedge x)$ and

$$1 \wedge x \otimes 1 \wedge x \mapsto (x - \sigma(x))^2 \in R.$$

We have a natural forgetful map $\mathrm{Disc}(X) \to \mathrm{Pic}(X)$ where $(d, \mathscr{L})$ maps to the isomorphism class of $\mathscr{L}$.

We say a sequence $A \xrightarrow{f} B \xrightarrow{g} C$ of commutative monoids is *exact* if f is injective, g is surjective, and for all $z, w \in B$, we have

$$g(z) = g(w) \text{ if and only if there exists } x, y \in A \text{ such that } xz = yw;$$

equivalently, the sequence is exact if and only if f is injective and g induces an isomorphism of monoids $B/f(A) \simeq C$. (For a review of monoids, see Section 1.)

We now describe the monoid $\mathrm{Quad}(X)$. We begin with the statement that the forgetful map is compatible with the discriminant map, as follows.

Theorem B. *Let X be a scheme. Then the diagram of commutative monoids*

$$\begin{array}{ccccc} \mathrm{Quad}(X; \mathscr{O}_X) & \longrightarrow & \mathrm{Quad}(X) & \xrightarrow{\wedge^2} & \mathrm{Pic}(X) \\ \downarrow{\scriptstyle \mathrm{disc}} & & \downarrow{\scriptstyle \mathrm{disc}} & & \| \\ \mathrm{Disc}(X; \mathscr{O}_X) & \longrightarrow & \mathrm{Disc}(X) & \longrightarrow & \mathrm{Pic}(X) \end{array}$$

is functorial and commutative with exact rows and Zariski locally surjective columns.

By "Zariski locally surjective columns", we mean that there is an (affine) open cover of X where (under pullback) the columns are surjective. (Considering the corresponding sheaves over X, we also obtain a surjective map of sheaves; see Theorem 3.28.)

We now turn to describe the morphism $\mathrm{Quad}(X; \mathscr{O}_X) \to \mathrm{Disc}(X; \mathscr{O}_X)$. For this purpose, we work locally and assume $X = \operatorname{Spec} R$ for a commutative ring R; we abbreviate $\mathrm{Quad}(\operatorname{Spec} R) = \mathrm{Quad}(R)$ and $\mathrm{Quad}(\operatorname{Spec} R; \mathscr{O}_{\operatorname{Spec} R}) = \mathrm{Quad}(R; R)$ and similarly with discriminants.

We would like to able to fit the surjective map $\mathrm{Quad}(R) \xrightarrow{\mathrm{disc}} \mathrm{Disc}(R)$ of monoids into an exact sequence by identifying its kernel, but unfortunately the fibers of this map vary over the codomain. Instead, we will describe the action of a subgroup of $\mathrm{Quad}(R)$ on the fibers of the map disc: this is a natural generalization, as the fibers of a group homomorphism are principal homogeneous spaces for the kernel K and are noncanonically isomorphic as a K-set to K with the regular representation.

Recalling the case of quadratic extensions of a field F with $\mathrm{char}\, F = 2$, for a commutative ring R we define the *Artin-Schreier group* $\mathrm{AS}(R)$ to be the additive quotient

$$\mathrm{AS}(R) = \frac{R[4]}{\wp(R)[4]} \quad \text{where} \quad \wp(R)[4] = \{n = r + r^2 \in R : r \in R\} \cap R[4]$$

and $R[4] = \{a \in R : 4a = 0\}$. We have a map $i : \mathrm{AS}(R) \to \mathrm{Quad}(R; R) \hookrightarrow \mathrm{Quad}(R)$ sending the class of $n \in \mathrm{AS}(R)$ to the isomorphism class of the algebra $S = R[x]/(x^2 - x + n)$. The group $\mathrm{AS}(R)$ is an elementary abelian 2-group since $2R[4] \subseteq \wp(R)$.

Our next main result is as follows (Theorem 4.3).

Theorem C. *The fibers of the map* $\mathrm{disc} : \mathrm{Quad}(R) \to \mathrm{Disc}(R)$ *have a unique action of the group* $\mathrm{AS}(R)$ *compatible with the inclusion of monoids* $\mathrm{AS}(R) \hookrightarrow \mathrm{Quad}(R)$*. Moreover, the kernel of this action on the fiber* $\mathrm{disc}^{-1}(dR^{\times 2})$ *contains* $\mathrm{ann}_R(d)[4]$*.*

Roughly speaking, Theorems B and C together say that "a quadratic algebra is determined by its Steinitz class and its discriminant, locally up to an Artin-Schreier extension". These theorems could be rephrased in terms of the Grothendieck group; however, due to the existence of an absorbing element, the group $K_0(\mathrm{Quad}(X))$ is trivial for all schemes X.

The article is organized as follows. In section 1, we briefly review the relevant notions from monoid theory. In section 2, we consider the monoid of discriminants; in section 3 we define the monoid of quadratic R-algebras and prove Theorems A and B. In section 4 we prove Theorem C.

The author would like to thank Asher Auel, Manjul Bhargava, James Borger, and Melanie Wood for helpful suggestions. The author is also indebted to the anonymous referee and Owen Biesel for very detailed and helpful comments and corrections. The author was supported by an NSF CAREER Award (DMS-1151047).

1. Monoids

To begin, we review standard terminology for monoids. A reference for the material in this section is Bergman [1, Chapter 3]; more generally, see Burris–Sankappanavar [5] and McKenzie–McNulty–Taylor [16].

A *semigroup* is a nonempty set A equipped with an associative binary operation

$$* : A \times A \to A.$$

A *monoid* is a semigroup with identity element 1 for $*$ (necessarily unique). Any semigroup without 1 can be augmented to a monoid. Natural examples of monoids abound: the natural numbers $\mathbb{N} = \mathbb{Z}_{\geq 0}$ under addition, a ring R under its multiplication, and the set of endomorphisms of an algebraic object (such as a variety) under composition. A *group* is a monoid equipped with an inverse map $^{-1} : A \to A$.

Let A be a semigroup. We say A is *commutative* if $xy = yx$ for all $x, y \in A$. An *absorbing element* of A is an element $0 \in A$ such that $0x = x0 = 0$ for all $x \in A$; a monoid has at

most one absorbing element. Multiplicative notation for A will be in general more natural for us; however, we will occasionally write A additively with operation $+$, in which case the identity element will be denoted 0 and to avoid confusion A will have no absorbing element. An element $x \in A$ is (left) *cancellative* if $xy = xz$ implies $y = z$ for all $y, z \in A$.

A *homomorphism* of semigroups is a map $f : A \to B$ such that $f(xy) = f(x)f(y)$ for all $x, y \in A$, and a homomorphism of monoids is a homomorphism of semigroups such that $f(1_A) = 1_B$.

Let $f : A \to B$ be a homomorphism of monoids. Unlike groups, the kernel $\ker f = \{x \in A : f(x) = 1\}$ of a monoid homomorphism does not determine the structure of the image of f; instead, we define the *kernel congruence* of f by

$$K_f = \{(x, y) : f(x) = f(y)\} \subseteq A \times A.$$

The set K_f defines a *congruence* on A, an equivalence relation compatible with the operation on A, i.e., if $(x, y), (z, w) \in K_f$ then $(xz, yw) \in K_f$. Conversely, given a congruence K on a monoid A, the set operation $[x] \cdot [y] = [x \cdot y]$ on equivalence classes $[x], [y] \in A/K$ is well-defined and the quotient map $A \to A/K$ via $x \mapsto [x]$ is a surjective homomorphism of monoids with kernel K; any homomorphism $f : A \to B$ with $K_f \supseteq K$ factors through $A \to A/K$.

The image $f(A) = \{f(x) : x \in A\}$ is a submonoid of B, but if A, B are noncommutative, then not every submonoid is eligible to be the kernel of a homomorphism (just as not every subgroup is normal). As we will be interested only in commutative monoids, and this assumption simplifies the presentation, suppose from now on that A, B are commutative. Then the set

$$I_f = \{(z, w) : f(x)z = f(y)w \text{ for some } x, y \in A\} \subseteq B \times B,$$

is a congruence called the *image congruence*. (Without the hypothesis of commutativity, I_f is a relation that is reflexive and symmetric, but not necessarily transitive nor a congruence; if A, B are possibly nonabelian groups, then I_f is transitive and is a congruence if and only if $f(A)$ is a normal subgroup of B.) Note that if $0 \in f(A)$ then $I_f = B \times B$. We write $B/f(A) = B/I_f$.

A sequence

$$A \xrightarrow{f} B \xrightarrow{g} C \tag{1.1}$$

is *exact* if f is injective, g is surjective, and $K_g = I_f$, i.e.

$$g(z) = g(w) \text{ if and only if there exists } x, y \in A \text{ such that } xz = yw;$$

equivalently, (1.1) is exact if f is injective and g induces an isomorphism $B/f(A) = B/I_f \xrightarrow{\sim} C$. A sequence of groups (1.1) is exact as a sequence of groups if and only if it is exact as a sequence of monoids.

Remark 1.2. We will not make use of long exact sequences of monoids here nor write the customary 0 or 1 at the ends of our short exact sequences. Indeed, the straightforward extension of the notion from groups to monoids using the definitions above (kernel congruence equals image congruence) has a defect: the sequence

$$\mathbb{N} \xrightarrow{f} \mathbb{Z} \xrightarrow{j} 0$$

of monoids under addition has $I_f = \mathbb{Z} \times \mathbb{Z} = K_j$ even though f is not surjective. (The map f is, however, an epimorphism in the category of monoids.)

We will also make use of sheaves of monoids over a scheme X. A sequence $\mathscr{A} \xrightarrow{f} \mathscr{B} \xrightarrow{g} \mathscr{C}$ of sheaves of monoids is *exact* if the sheaf associated to the presheaf $U \mapsto \mathscr{B}(U)/f(\mathscr{A}(U))$ is isomorphic to $\mathscr{C}$, or equivalently if the induced sequence $\mathscr{A}_x \xrightarrow{f_x} \mathscr{B}_x \xrightarrow{g_x} \mathscr{C}_x$ of monoid stalks is exact for all $x \in X$.

Like the formation of the integers from the natural numbers, one can construct the Grothendieck group $K_0(A)$ of a commutative monoid A, with the universal property that for any monoid homomorphism $A \to G$ with G an abelian group, there exists a unique group homomorphism $K_0(A) \to G$ such that the diagram

$$\begin{array}{ccc} A & \longrightarrow & G \\ \downarrow & \overset{\exists!}{\nearrow} & \\ K_0(A) & & \end{array}$$

commutes. The group $K_0(A)$ is constructed as $A \times A$ under the equivalence relation $(x, x') \sim (y, y')$ if there exists $z \in A$ such that $xy'z = x'yz$. Note that if A has an absorbing element 0 then $K_0(A) = \{0\}$. The set of cancellative elements A_{canc} is the largest submonoid of A which can be embedded in a group, and the smallest such containing group is the Grothendieck group $K_0(A_{\text{canc}})$.

2. Discriminants

In this section, we define discriminants for quadratic rings over general schemes (Definition 2.11); for a discussion of discriminant modules overlapping the one presented here, see Knus [11, §III.3] and Loos [14, §1.2]. We also relate semi-nondegenerate quadratic forms on line bundles by their images (Lemma 2.8) and factor the monoid of discriminants over the Picard group (Proposition 2.18).

Let X be a scheme. A *quadratic form* over X is a pair $(\mathscr{M}, Q)$ where $\mathscr{M}$ is a locally free $\mathscr{O}_X$-module of finite rank and $Q : \mathscr{M} \to \mathscr{O}_X$ is a *quadratic map*, i.e., for all open sets $U \subseteq X$, we have

(i) $Q(rx) = r^2 Q(x)$ for all $r \in \mathscr{O}_X(U)$ and $x \in \mathscr{M}(U)$; and
(ii) The map $T : \mathscr{M}(U) \times \mathscr{M}(U) \to \mathscr{O}_X(U)$ defined by

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

is $\mathscr{O}_X(U)$-bilinear; we call T the *associated bilinear form*.

An *isometry* between quadratic forms $Q : \mathscr{M} \to \mathscr{O}_X$ and $Q' : \mathscr{M}' \to \mathscr{O}_X$ is an $\mathscr{O}_X$-module isomorphism $f : \mathscr{M} \xrightarrow{\sim} \mathscr{M}'$ such that $Q' \circ f = Q$. A *similarity* between quadratic forms Q, Q' is a commutative square:

$$\begin{array}{ccc} \mathscr{M} & \xrightarrow{Q} & \mathscr{O}_X \\ \wr \downarrow f & & g \downarrow \wr \\ \mathscr{M}' & \xrightarrow{Q'} & \mathscr{O}_X \end{array}$$

and so an isometry is just a similarity with $g = \mathrm{id}$.

A quadratic form $(\mathscr{M}, Q)$ is also equivalently specified by $\mathscr{M}$ and an $\mathscr{O}_X$-module homomorphism $Q : \operatorname{Sym}_2 \mathscr{M} \to \mathscr{O}_X$, or a global section

$$Q \in \operatorname{Hom}(\operatorname{Sym}_2 \mathscr{M}, \mathscr{O}_X) = (\operatorname{Sym}_2 \mathscr{M})^\vee(X) \simeq \operatorname{Sym}^2(\mathscr{M}^\vee)(X).$$

(Here, $\operatorname{Sym}^2 \mathscr{M}$ denotes the second symmetric power of $\mathscr{M}$ and $\operatorname{Sym}_2 \mathscr{M}$ the submodule of symmetric second tensors of $\mathscr{M}$.)

A quadratic form $Q : \mathscr{M} \to \mathscr{O}_X$ with associated bilinear form $T : \mathscr{M} \times \mathscr{M} \to \mathscr{O}_X$ induces a homomorphism of $\mathscr{O}_X$-modules $\mathscr{M} \to \mathscr{M}^\vee$ defined by

$$\begin{aligned} \mathscr{M}(U) &\to \mathscr{M}^\vee(U) \\ y &\mapsto (x \mapsto T(x, y)) \end{aligned}$$

Following Knus [11, (I.3.2)], we say $Q : \mathscr{M} \to \mathscr{O}_X$ is *nondegenerate* if the associated map $\mathscr{M} \to \mathscr{M}^\vee$ is injective and *nonsingular* (or *regular*) if the associated map $\mathscr{M} \to \mathscr{M}^\vee$ is an isomorphism; these properties hold for Q if and only if they hold on an affine open cover. On an open set $U = \operatorname{Spec} R$ where $\mathscr{M}(U) = M$ is free of rank n, we define the *discriminant* of Q as $\operatorname{disc}(Q) = \det(T) \in R/R^{\times 2}$, the determinant of the bilinear form T with respect to a basis of $M \simeq R^n$; then Q is nondegenerate if and only if $\operatorname{disc}(Q)$ is a nonzerodivisor and nonsingular if and only if $\operatorname{disc}(Q)$ is a unit in R. When further n is odd, we define the *half-discriminant* (see e.g. Knus [11, (IV.3.1.3)]) by a universal formula, and we say that Q is *semi-nondegenerate* (resp. *semi-nonsingular* or *semi-regular*) if the half-discriminant is a nonzerodivisor (resp. a unit), and we extend these notions globally to a quadratic form $Q : \mathscr{M} \to \mathscr{O}_X$ if they hold on an affine open cover.

Now let $\mathscr{L}$ be an invertible $\mathscr{O}_X$-module (i.e., locally free of rank 1). A quadratic form on $\mathscr{L}$, the case of our primary concern, is a quadratic map $Q : \mathscr{L} \to \mathscr{O}_X$, but it is given equivalently by a global section $q \in \operatorname{Sym}^2(\mathscr{L}^\vee)(X) \simeq (\mathscr{L}^\vee)^{\otimes 2}(X)$. Because will use this identification frequently, we make it explicit. The identification is defined locally on X, so suppose $X = \operatorname{Spec} R$ and L is a free module of rank 1 over R. Then $\operatorname{Sym}^2(L^\vee) \simeq (L^\vee)^{\otimes 2} \simeq (L^{\otimes 2})^\vee$. Suppose $q \in \operatorname{Sym}^2(L^\vee)$, so $q : L \otimes L \to R$ is an R-module homomorphism. Let $L = Re$ for some $e \in L$ and define the quadratic map $Q : L \to R$ by $Q(re) = r^2 q(e \otimes e)$; this definition is independent of the choice of e. Conversely, if $Q : L \to R$ is a quadratic map, then again letting $L = Re$ we define the R-module homomorphism $q : L \otimes L \to R$ by $q(e \otimes e) = Q(e)$.

Remark 2.1. One must remember the domain $\mathscr{L}$ in this identification. Indeed, if $i : \mathscr{T}^{\otimes 2} \simeq \mathscr{O}_X$ is an isomorphism of $\mathscr{O}_X$-modules, so that $\mathscr{T} \in \operatorname{Pic}(X)[2]$, then i defines a quadratic form $I : \mathscr{T} \to \mathscr{O}_X$, called a *neutral form*, giving rise to an isomorphism

$$(\mathscr{L}^\vee)^{\otimes 2} \xrightarrow{\sim} ((\mathscr{L} \otimes \mathscr{T})^\vee)^{\otimes 2}.$$

The notions of *(semi-)nondegenerate* and *(semi-)nonsingular* can be made quite explicit for quadratic forms of rank 1. These conditions are local, so let $Q : L \to R$ be a quadratic form with $L = Re$. Then Q is uniquely specified by the element $Q(e) = a \in R$, and the associated bilinear form is specified by $T(e, e) = 2a$, with $2a = \det(Q) \in R/R^{\times 2}$ as a different choice of basis $e' = ue$ gives $Q(e') = u^2 Q(e) = au^2$ with $u \in R^\times$. We find that Q is nondegenerate if and only if $2a$ is a nonzerodivisor and regular if $2a \in R^\times$, and Q is semi-nondegenerate if a is a nonzerodivisor and semi-nonsingular if a is a unit.

Remark 2.2. The slightly unpleasant term *semi-nondegenerate* is not standard in the literature, but we believe it is clarifying to use in this situation. It is common to use the term *nondegenerate* instead, but we do not do this here to avoid potential confusion.

Given two quadratic forms $Q : \mathscr{L} \to \mathscr{O}_X$ and $Q' : \mathscr{L}' \to \mathscr{O}_X$, corresponding to $q \in (\mathscr{L}^\vee)^{\otimes 2}(X)$ and $q' \in (\mathscr{L}'^\vee)^{\otimes 2}(X)$, from the element

$$q \otimes q' \in ((\mathscr{L}^\vee)^{\otimes 2} \otimes (\mathscr{L}'^\vee)^{\otimes 2})(X) \simeq ((\mathscr{L} \otimes \mathscr{L}')^\vee)^{\otimes 2}(X)$$

we define the corresponding tensor product $Q \otimes Q' : \mathscr{L} \otimes \mathscr{L}' \to \mathscr{O}_X$: following the identification above, over $X = \operatorname{Spec} R$ where $L = Re$ and $L' = Re'$, then $L \otimes L' = R(e \otimes e')$ and $(Q \otimes Q')(e \otimes e') = Q(e)Q(e')$. The tensor product gives the set of similarity classes of quadratic forms of rank 1 over X the structure of a commutative monoid.

Remark 2.3. The definition of the tensor product of quadratic forms is more subtle in general for forms of arbitrary rank; here we find the correct notion because we can think of rank 1 quadratic forms as rank 1 symmetric bilinear forms.

Definition 2.4. Let $Q : \mathscr{L} \to \mathscr{O}_X$ be a (rank 1) quadratic form. We say Q is *cancellative* if it is cancellative in the monoidal sense, as $q \in (\mathscr{L}^\vee)^{\otimes 2}(X)$: if $q' \in ((\mathscr{L}')^\vee)^{\otimes 2}$ and $q'' \in ((\mathscr{L}'')^\vee)^{\otimes 2}(X)$ have $q \otimes q'$ similar to $q \otimes q''$, then q' is similar to q''.

We say Q is *locally cancellative* if for all $x \in X$ there exists an affine open neighborhood $U \ni x$ such that $Q|_U$ is cancellative.

Proposition 2.5. *A (rank 1) quadratic form $Q : \mathscr{L} \to \mathscr{O}_X$ is locally cancellative if and only if Q is semi-nondegenerate.*

Moreover, a locally cancellative rank 1 quadratic form Q over X is cancellative. If X is affine then Q is cancellative if and only if it is locally cancellative.

Proof. Both properties are local, so it suffices to check this over a ring $X = \operatorname{Spec} R$ such that the quadratic forms involved are free. To a quadratic form $Q : L = Re \to R$, we have $Q(e) = a \in R$. If Q', Q'' are similarly other rank 1 quadratic forms with $Q(e') = a' \in R$ and $Q(e'') = a'' \in R$, then $(Q \otimes Q')(e \otimes e') = aa'$ and $(Q \otimes Q'')(e \otimes e'') = aa''$. We have $Q' \sim Q''$ if and only if there exists $u \in R^\times$ such that $a' = ua''$.

Thus, if Q is semi-nondegenerate, then a is a nonzerodivisor, so $Q \otimes Q' \sim Q \otimes Q''$ implies $aa' = uaa''$ implies $a' = ua''$ implies $Q' \sim Q''$, so Q is locally cancellative. Conversely, if Q is locally cancellative and a is a zero divisor, with $aa' = 0$ and $a' \neq 0$, then taking $Q'(e') = a'$ and $Q''(e'') = 0$ we have $Q \otimes Q' \sim Q \otimes Q''$ so $Q' \sim Q''$ and thus there exists $u \in R^\times$ such that $a' = u(0) = 0$, a contradiction.

Now for the second statement. Let $Q : \mathscr{L} \to \mathscr{O}_X$ be locally cancellative. By the previous paragraph, Q is semi-nondegenerate. Suppose that $Q \otimes Q' \sim Q \otimes Q''$ for rank 1 quadratic forms Q', Q''; we will show that $Q' \sim Q''$. Cancelling in $\operatorname{Pic}(X)$, we may assume without loss of generality that $\mathscr{L}' = \mathscr{L}''$. Let $U = \operatorname{Spec} R$ be an affine open subset of X in which all of $\mathscr{L}|_U = L = Re$ is free and similarly $L' = Re' = L'' = Re''$. Let $a = Q(e)$ and similarly $a' = Q'(e')$ and $a'' = Q''(e'')$, so as in the previous paragraph we are given (a unique) $u \in R^\times$ such that $aa' = uaa''$. Since Q is locally cancellative, we have $a' = ua''$, and this defines a similarity $Q' \sim Q''$. Repeating this on an open cover, the elements u glue to give an element $g \in \mathscr{O}_X(X)^\times$, and so together with the identity map on $\mathscr{L}' = \mathscr{L}''$ we therefore have a similarity $Q' \sim Q''$.

The converse in the final statement follows immediately by taking $U = X$ if X is affine. $\square$

The following corollary is then immediate.

Corollary 2.6. *The subset of locally cancellative quadratic forms over X is a submonoid of the monoid of rank 1 quadratic forms over X.*

Remark 2.7. The global notion of cancellative is not as robust as one may like. Kleiman [10] gives an example of a scheme X and a global section $t \in \mathscr{O}_X(X)$ that is a nonzerodivisor such that it becomes a zerodivisor in an affine open $t|_U \in \mathscr{O}_X(U)$.

The similarity class of a locally cancellative quadratic form is determined by its image ("effective Cartier divisors on a scheme are the same as invertible sheaves with a choice of regular global section" [19, Tag 01X0]), as follows.

Lemma 2.8. *There is a (functorial) isomorphism of commutative monoids*

$$\left\{\begin{array}{c}\text{Similarity classes of rank 1}\\ \text{locally cancellative quadratic forms}\\ Q : \mathscr{L} \to \mathscr{O}_X\\ \text{modulo neutral forms}\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{Locally free ideal}\\ \text{sheaves } \mathscr{I} \subseteq \mathscr{O}_X\\ \text{such that } [\mathscr{I}] \in 2\operatorname{Pic}(X)\end{array}\right\}$$

where the similarity class of a quadratic form $Q : \mathscr{L} \to \mathscr{O}_X$ maps to the ideal $\mathscr{I}$ of $\mathscr{O}_X$ generated by the values $Q(\mathscr{L})$.

Ideal sheaves are a monoid under multiplication, so the "monoid" part of Lemma 2.8 says that the tensor product $Q \otimes Q'$ of two quadratic forms Q, Q' maps to the product $\mathscr{I}\mathscr{I}'$ of their associated ideal sheaves $\mathscr{I}, \mathscr{I}'$.

Proof. First, we show the map is well defined, which we may do locally. Let $Q : L \to R$ be a rank 1 locally cancellative quadratic form; then L is free so we may write $L = Re$ and then $Q(L) = Q(e)R$. By Proposition 2.5, we know that $Q(e)$ is a nonzerodivisor, and this is independent of the choice of e (up to a unit of R). If $Q' : L' \to R$ is similar to Q, then there exist R-linear isomorphisms $f : L \to L'$ and $g : R \to R$ such that $Q'(f(x)) = g(Q(x))$ for all $x \in L$. Letting $e' = f(e)$ we have $L' = Re'$. The map g must be of the form $g(a) = ua$ for some $u \in R^\times$, so $Q'(L') = Q'(f(L)) = uQ(L) = uQ(e)R = Q(e)R$, and so the image is a well-defined principal ideal.

Now let $Q : \mathscr{L} \to \mathscr{O}_X$ be a locally cancellative quadratic form of rank 1, corresponding to the global section $q \in (\mathscr{L}^{\otimes 2})^\vee(X)$. We claim that $q : \mathscr{L}^{\otimes 2} \to \mathscr{O}_X$ is an isomorphism onto its image $\mathscr{I} = Q(\mathscr{L}) = q(\mathscr{L}^{\otimes 2})$. If $U = \operatorname{Spec} R$ is an affine open set where $\mathscr{L}|_U = Re$, then $q(L^{\otimes 2}) = q(e \otimes e)R$; if further U is such that q is cancellative over U, we have that $q(e \otimes e)$ is a nonzerodivisor, so q is injective on U (and $q(L)$ is free). By hypothesis, such affine open sets U cover X, so we have $[\mathscr{I}] = [\mathscr{L}^{\otimes 2}] \in \operatorname{Pic}(X)$.

Next, let $q : \mathscr{L} \to \mathscr{O}_X$ and $q' : \mathscr{L}' \to \mathscr{O}_X$ be locally cancellative quadratic forms such that $q(\mathscr{L}) = q'(\mathscr{L}') = \mathscr{I}$. Since $[\mathscr{I}] = [\mathscr{L}^{\otimes 2}] = [(\mathscr{L}')^{\otimes 2}]$, tensoring q' by a neutral form we may assume that $f : \mathscr{L} \xrightarrow{\sim} \mathscr{L}'$. Then on any affine open set $U = \operatorname{Spec} R \subseteq X$, where $\mathscr{L}|_U = Re$ and $\mathscr{L}'|_U = Re'$, we have $q(L) = q(e)R = q'(e')R$. Therefore, there exists $u \in R$ such that $q(e) = uq'(e')$ and $u' \in R$ such that $q'(e') = u'q(e)$. Thus $q(e)(1 - uu') = 0$. On an affine open set U where q is cancellative, we have $uu' = 1$, so $u \in R^\times$. Moreover, the element u is unique, since if $q(e) = uq'(e') = vq'(e')$ then $(u - v)q'(e') = 0$ so since q' is cancellative, we have $u = v$. Repeating this argument on an open cover where both $\mathscr{L}$ and $\mathscr{L}'$ are free, there exists (a unique) $u \in \mathscr{O}_X(X)^\times$ giving rise to an isomorphism $\mathscr{O}_X \xrightarrow{\sim} \mathscr{O}_X$ such that $q'f = uq$, so that q, q' are similar.

Finally, the map is surjective. We are given that there exists an invertible bundle $\mathscr{L}$ such that $\mathscr{L}^{\otimes 2} \simeq \mathscr{I}$. The embedding $\mathscr{L}^{\otimes 2} \simeq \mathscr{I} \hookrightarrow \mathscr{O}_X$ then defines a locally cancellative quadratic form $Q : \mathscr{L} \to \mathscr{O}_X$ with values $Q(\mathscr{L}) = \mathscr{I}$, as can be readily checked locally. □

Remark 2.9. A (locally) cancellative rank 1 quadratic form might not pull back to a (locally) cancellative form under an arbitrary morphism of schemes.

To work with discriminants, we will work modulo 2 and 4 as follows. The multiplication by 4 map on $\mathscr{O}_X$ gives a closed immersion

$$X_{[4]} = X \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{Z}/4\mathbb{Z} \hookrightarrow X$$

and the pullback $\mathscr{L}_{[4]} = \mathscr{L} \otimes \mathscr{O}_X/4\mathscr{O}_X$ is an invertible $\mathscr{O}_{X_{[4]}}$-module, equipped with a map ${}_{[4]} : \mathscr{L} \to \mathscr{L}_{[4]}$. We can also further work modulo 2, obtaining $\mathscr{L}_{[2]}$.

Let R be a commutative ring. Then squaring gives a well-defined map of sets

$$\begin{aligned} \operatorname{sq} &: R/2R \to R/4R \\ \operatorname{sq}(t + 2R) &= t^2 + 4R \end{aligned} \tag{2.10}$$

The map sq is functorial in R and canonically defined, so we can sheafify: if $\mathscr{L}$ is an invertible $\mathscr{O}_X$-module, there is a unique map

$$\operatorname{sq} : \mathscr{L}_{[2]} \to (\mathscr{L}_{[4]})^{\otimes 2}$$

locally defined by (2.10). Explicitly, for an affine open $U = \operatorname{Spec} R$ of X where $\mathscr{L}(U) = L = Re$, we may write $\mathscr{L}_{[2]}(U) = (R/2R)e$ and $\mathscr{L}_{[4]}^{\otimes 2}(U) = (R/4R)(e \otimes e)$, and

$$\operatorname{sq}((t + 2R)e) = \operatorname{sq}(t + 2R)(e \otimes e)$$

is well-defined (independent of the choice of e).

Definition 2.11. A *discriminant* over X is a pair $(d, \mathscr{L})$ where $\mathscr{L}$ is an invertible $\mathscr{O}_X$-module and $d \in (\mathscr{L}^\vee)^{\otimes 2}(X)$ such that there exists $t \in \mathscr{L}_{[2]}^\vee(X)$ with

$$\operatorname{sq}(t) = d_{[4]} \in (\mathscr{L}_{[4]}^\vee)^{\otimes 2}(X). \tag{2.12}$$

If 2 is invertible on X, then $X_{[4]}$ is the empty scheme and the square condition (2.12) is vacuously satisfied.

Definition 2.13. An *isomorphism* between discriminants $(d, \mathscr{L})$ and $(d', \mathscr{L}')$ is an isomorphism $f : \mathscr{L} \xrightarrow{\sim} \mathscr{L}'$ such that $(f^\vee)^{\otimes 2} : (\mathscr{L}'^\vee)^{\otimes 2} \to (\mathscr{L}^\vee)^{\otimes 2}$ has $(f^\vee)^{\otimes 2}(d') = d$.

Equivalently, an isomorphism between discriminants is an isometry (not a similarity!) between the corresponding quadratic forms.

In what follows, we will often abbreviate d for a discriminant $(d, \mathscr{L})$, and refer to $\mathscr{L}$ as the underlying invertible sheaf.

Let $\operatorname{Disc}(X)$ denote the set of discriminants over X up to isomorphism. For an invertible sheaf $\mathscr{L}$ on X, let $\operatorname{Disc}(X; \mathscr{L}) \subseteq \operatorname{Disc}(X)$ denote the subset of isomorphism classes of discriminants d whose underlying invertible sheaf is (isomorphic to) $\mathscr{L}$. Define $\mathbf{Disc}(X)$ to be the sheaf associated to the presheaf $U \mapsto \operatorname{Disc}(U)$.

Lemma 2.14. $\operatorname{Disc}(X)$ *has the structure of commutative monoid under tensor product, with identity element represented by the class of* $(1, \mathscr{O}_X)$. *Moreover,* $\operatorname{Disc}(X; \mathscr{O}_X)$ *is a submonoid of* $\operatorname{Disc}(X)$ *with absorbing element* $(0, \mathscr{O}_X)$.

Proof. The binary operation of tensor product on quadratic forms restricts to a binary operation on discriminants: if $(d, \mathscr{L})$ and $(d', \mathscr{L}')$ are discriminants, with $t \in \mathscr{L}_{[2]}^{\vee}(X)$ satisfying $\mathrm{sq}(t) = d_{[4]} \in (\mathscr{L}_{[4]}^{\vee})^{\otimes 2}(X)$ and similarly for $(d', \mathscr{L}')$, then

$$\mathrm{sq}(t \otimes t') = d_{[4]} \otimes d'_{[4]} = (d \otimes d')_{[4]} \in ((\mathscr{L}_{[4]}^{\vee})^{\otimes 2} \otimes ((\mathscr{L}'_{[4]})^{\vee})^{\otimes 2})(X) \simeq ((\mathscr{L} \otimes \mathscr{L}')_{[4]}^{\vee})^{\otimes 2}(X).$$

This definition is independent of the choice of a representative discriminant in an isomorphism class, so we obtain a binary operation on $\mathrm{Disc}(X)$. This operation is associative and commutative and $(1, \mathscr{O}_X)$ is an identity by definition of the tensor product. The subset $\mathrm{Disc}(X; \mathscr{O}_X)$ is closed under tensor product, and $(0, \mathscr{O}_X)$ is visibly an absorbing element. □

Lemma 2.15. *There is a functorial monoid isomorphism*

$$\{d \in \mathscr{O}_X(X) : d \text{ is a square modulo } 4\mathscr{O}_X(X)\}/\mathscr{O}_X(X)^{\times 2} \xrightarrow{\sim} \mathrm{Disc}(X; \mathscr{O}_X). \tag{2.16}$$

Proof. The explicit identification as monoid homomorphism between elements

$$d \in \mathscr{O}_X(X) \simeq (\mathscr{O}_X^{\vee})^{\otimes 2}(X)$$

and discriminants as quadratic forms is explained in the beginning of section 2, with the discriminant condition passing through on both sides.

Suppose that f is an isomorphism between discriminants d, d'. Let $U = \operatorname{Spec} R \subseteq X$ be an affine open subset. Then $d|_U : R \to R$ is a quadratic map with $d(r) = r^2 d(1)$ for all $r \in R$. The restriction $f|_U : \mathscr{O}_X(U) = R \to R$ is an isomorphism and so is identified with a unique element $u \in R^{\times}$, and so in R we have $d'|_U(f|_U(1)) = d'|_U(u) = u^2 d'|_U(1) = d|_U(1)$; by gluing, there exists a (unique) global section $u \in \mathscr{O}_X(X)^{\times}$ such that $d = u^2 d'$. □

Example 2.17. If $X = \operatorname{Spec} R$ where R is a PID or local ring, then by Lemma 2.15, $\mathrm{Disc}(R) = \mathrm{Disc}(R; R)$ is canonically identified with

$$\{d \in R : d \text{ is a square in } R/4R\}/R^{\times 2}.$$

So for $R = \mathbb{Z}$, since $\mathbb{Z}^{\times 2} = \{1\}$ we recover the usual set of discriminants as those integers $d \equiv 0, 1 \pmod 4$.

To a discriminant $(d, \mathscr{L})$, we can forget the quadratic map d and consider only the isomorphism class of the $\mathscr{O}_X$-module $\mathscr{L}$: this gives a map

$$p : \mathrm{Disc}(X) \to \mathrm{Pic}(X).$$

Proposition 2.18. *The sequence*

$$\mathrm{Disc}(X; \mathscr{O}_X) \to \mathrm{Disc}(X) \xrightarrow{p} \mathrm{Pic}(X)$$

of commutative monoids is exact.

Proof. The map $p : \mathrm{Disc}(X) \to \mathrm{Pic}(X)$ is surjective because an invertible module $\mathscr{L}$ has the zero quadratic form $d = 0$, which is a discriminant taking $t = 0$. (One can hardly do better in general, since it may be the case that $\mathscr{L}(X) = \{0\}$ has no nonzero global sections.)

Let $i : \mathrm{Disc}(X; \mathscr{O}_X) \hookrightarrow \mathrm{Disc}(X)$ be the inclusion map. We show that $I_i = K_p$. The inclusion $I_i \subseteq K_p$ is easy, so we show the reverse inclusion. Let d, d' be discriminants and suppose $([d], [d']) \in K_p$; then the underlying invertible sheaves of d, d' are isomorphic, so we may assume without loss of generality that $d, d' \in (\mathscr{L}^{\vee})^{\otimes 2}(X)$. To show $([d], [d']) \in I_i$, we need to show that there exist $\delta, \delta' \in \mathrm{Disc}(X; \mathscr{O}_X)$ such that $\delta \otimes d' = \delta' \otimes d$. For this purpose, we may take $\delta = \delta' = 0$. More generally, we could take any $\delta \in (d : d') = \{\delta \in \mathscr{O}_X(X) : \delta d' \in \langle d \rangle\} \subseteq \mathscr{O}_X(X)$. □

3. Quadratic algebras

In this section, we give a monoid structure on the set of isomorphism classes of quadratic algebras. We begin by discussing the algebras over commutative rings, then work over a general base scheme. For more on quadratic rings and standard involutions, see Knus [11, Chapter I, §1.3] and Voight [20, §1–2].

Let R be a commutative ring. An *R-algebra* is an associative ring B 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 this image in B. In particular, B is necessarily faithful as an R-module. A homomorphism of R-algebras is required to preserve 1.

Definition 3.1. A *quadratic* R-algebra (or *quadratic ring* over R) is an R-algebra S that is finite locally free of rank 2 as an R-module.

By *finite locally free* we mean that there is a cover of $\operatorname{Spec} R$ by standard open sets $D(f_i)$ with $i \in I$ such that the localization M_{f_i} is a free R_{f_i}-module for all $i \in I$. There are a number of other equivalent formulations of this condition [19, Tag 00NV], including that M is finitely presented an R-flat, that M is finite projective, and that M is finitely presented and for all primes $\mathfrak{p} \in \operatorname{Spec}(R)$ that the localization $M_{\mathfrak{p}}$ is free.

Let S be a quadratic R-algebra. Then S is commutative, and there is a unique *standard involution* on S, an R-linear homomorphism $\sigma : S \to S^{\mathrm{op}} = S$ such that $\sigma(\sigma(x)) = x$ and $x\sigma(x) \in R$ for all $x \in S$ [20, Lemma 2.9]. Consequently, we have a linear map $\mathrm{trd} : S \to R$ defined by $\mathrm{trd}(x) = x + \sigma(x)$ and a multiplicative map $\mathrm{nrd} : S \to R$ by $\mathrm{nrd}(x) = x\sigma(x) = \sigma(x)x$ with the property that $x^2 - \mathrm{trd}(x)x + \mathrm{nrd}(x) = 0$ for all $x \in S$.

Lemma 3.2. *If S is free as an R-module, then there is a basis $1, x$ for S as an R-module.*

Proof. Let x_1, x_2 be a basis for S; then there exists $a_1, a_2 \in R$ such that $1 = a_1x_1 + a_2x_2$. Let $x_1^2 = b_1x_1 + b_2x_2$ and $x_1x_2 = c_1x_1 + c_2x_2$ with $b_1, b_2, c_1, c_2 \in R$. Then

$$x_1 = x_1 \cdot 1 = a_1x_1^2 + a_2x_1x_2 = (a_1b_1 + a_2c_1)x_1 + (a_1b_2 + a_2c_2)x_2.$$

Thus $a_1b_1 + a_2c_1 = 1$. Let $x = -c_1x_1 + b_1x_2$. Then

$$\det \begin{pmatrix} a_1 & a_2 \\ -c_1 & b_1 \end{pmatrix} = a_1b_1 + a_2c_1 = 1 \quad \text{and} \quad \begin{pmatrix} a_1 & a_2 \\ -c_1 & b_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ x \end{pmatrix}$$

so $1, x$ is a basis for S as an R-module. □

Remark 3.3. Lemma 3.2 does not generally extend to R-algebras of higher rank. On the one hand, if S is a finite locally free we always have $S \simeq R \oplus S/R$ as R-modules [20, Lemma 1.3]; on the other hand, if S is free this need not imply that S/R is free. (However, S/R is still locally free, so for the purposes of making local arguments, you can refine an open cover to one over which S/R is in fact free to then find a basis containing 1.)

If S is free over R with basis $1, x$, then the multiplication table is determined by the multiplication $x^2 = tx - n$: consequently, we have a bijection

$$\left\{ \begin{array}{c} \text{Free quadratic } R\text{-algebras} \\ S \text{ over } R \text{ equipped} \\ \text{with a basis } 1, x \end{array} \right\} \xrightarrow{\sim} R^2 \tag{3.4}$$

$$S \mapsto (\mathrm{trd}(x), \mathrm{nrd}(x)) = (x + \overline{x}, x\overline{x}) = (t, n).$$

A change of basis for a free quadratic R-algebra is of the form $x \mapsto u(x+r)$ with $u \in R^\times$ and $a \in R$, mapping

$$(t, n) \mapsto (u(t+2r), u^2(n+tr+r^2)). \tag{3.5}$$

We have identified $R \subseteq S$ as a subring; the quotient S/R is locally free of rank 1. Therefore, we have a canonical identification

$$\begin{aligned} S/R &\xrightarrow{\sim} \bigwedge^2 S \\ x + R &\mapsto 1 \wedge x. \end{aligned} \tag{3.6}$$

Lemma 3.7. *Let S be a quadratic R-algebra. Then the map*

$$\begin{aligned} d : (\bigwedge^2 S)^{\otimes 2} &\to R \\ (x \wedge y) \otimes (z \wedge w) &\mapsto (x\sigma(y) - \sigma(x)y)(z\sigma(w) - \sigma(z)w). \end{aligned} \tag{3.8}$$

is a discriminant.

We have

$$\begin{aligned} d((1 \wedge x)^{\otimes 2}) &= (x - \sigma(x))^2 = (2x - \operatorname{trd}(x))^2 \\ &= 4x^2 - 4x \operatorname{trd}(x) + \operatorname{trd}(x)^2 = \operatorname{trd}(x)^2 - 4 \operatorname{nrd}(x) \end{aligned} \tag{3.9}$$

in the lemma, as one might expect. We accordingly call the quadratic map $d = d(S)$ in Lemma 3.7 the *discriminant* of S.

Proof. We define the map

$$\begin{aligned} t : \bigwedge^2 (S/2S) &\to R/2R \\ t(1 \wedge x) &= \operatorname{trd}(x) \end{aligned}$$

via the identification (3.6). The map t is well-defined since $\operatorname{trd}(x+r) = \operatorname{trd}(x) + 2r \equiv \operatorname{trd}(x) \pmod{2R}$. We then verify that

$$\operatorname{sq}(t)((1 \wedge x)^{\otimes 2}) = t(1 \wedge x)^2 = \operatorname{trd}(x)^2 \equiv \operatorname{trd}(x)^2 - 4 \operatorname{nrd}(x) = d((1 \wedge x)^{\otimes 2}) \pmod{4R}$$

by (3.9). □

Recall that a commutative R-algebra B is *separable* if B is projective as a $B \otimes_R B$-module via the map $x \otimes y \mapsto xy$. If $B \simeq R[x]/(f(x))$ with $f(x) \in R[x]$, then B is separable if and only if the ideal generated by $f(x)$ and its derivative $f'(x)$ is the unit ideal.

Lemma 3.10. *A quadratic R-algebra S is separable if and only if its discriminant d is an isomorphism.*

Proof. The map $d : (\bigwedge^2 S)^{\otimes 2} \to R$ is an isomorphism if and only if it is locally an isomorphism, so we reduce to the case where $S = R[x]/(x^2 - tx + n) = R[x]/(f(x))$. Then by (3.9), d is an isomorphism if and only if $\operatorname{trd}(x)^2 - 4 \operatorname{nrd}(x) \in R^\times$ if and only if S is separable [11, Chapter I, (7.3.4)]. □

Corollary 3.11. *If S is a separable quadratic R-algebra, then $\bigwedge^2 S \in \operatorname{Pic}(R)[2]$.*

Now let X be a scheme.

Definition 3.12. A *quadratic $\mathscr{O}_X$-algebra* is a sheaf $\mathscr{S}$ of $\mathscr{O}_X$-algebras that is locally free of rank 2 as a sheaf of $\mathscr{O}_X$-modules: there is a basis of open sets U of X such that $\mathscr{S}(U)$ is free of rank 2 as an $\mathscr{O}_X(U)$-module.

Equivalently, a quadratic $\mathscr{O}_X$-algebra is given by a *double cover* $\phi : Y \to X$, a finite locally free morphism of schemes of degree 2: the sheaf $\phi_* \mathscr{O}_Y$ is a sheaf of $\mathscr{O}_X$-algebras that is locally free of rank 2. By uniqueness of the standard involution, we obtain a *standard involution* on $\mathscr{S}$, a standard involution on $\mathscr{S}(U)$ for all open sets U (covering each by affine open sets where $\mathscr{S}$ is free), and in particular maps trd and nrd on $\mathscr{S}$.

Analogous to Lemma 3.7, we have the following result.

Proposition 3.13. *Let $\mathscr{S}$ be a quadratic $\mathscr{O}_X$-algebra. Then there exists a unique discriminant $d : (\bigwedge^2 \mathscr{S})^{\otimes 2} \to \mathscr{O}_X$ that coincides locally with the one defined by* (3.8).

Proof. Let $\mathscr{L} = \bigwedge^2 \mathscr{S}$. We must exhibit $t \in \mathscr{L}^\vee_{[2]}(X)$ such that $\mathrm{sq}(t) = d_{[4]} \in (\mathscr{L}^\vee_{[4]})^{\otimes 2}(X)$, where $_{[4]}$ denotes working modulo 4, as in the previous section. We adapt the argument in Lemma 3.7 to a global setting. First working locally, let $U = \operatorname{Spec} R \subseteq X$ be an open set where $\mathscr{S}(U) = S$ and $\mathscr{L}(U) = L = \bigwedge^2 S$. Since $\mathrm{trd}(x + r) = \mathrm{trd}(x) + 2r$ for $r \in R$ and $x \in S$, the map

$$\begin{aligned} t : \textstyle\bigwedge^2 (S/2S) \simeq L/2L &\to R/2R \\ x \wedge y &\mapsto \mathrm{trd}(x + y) \end{aligned}$$

is well-defined (since $t(x \wedge x) = \mathrm{trd}(2x) = 0$) and R-linear. This map does not depend on any choices, so repeating this on an open cover, we obtain an element $t \in \mathscr{L}^\vee_{[2]}(X)$.

Now we verify that $\mathrm{sq}(t) = d_{[4]} \in (\mathscr{L}^\vee_{[4]})^{\otimes 2}(X)$. We may do so on an open cover, where $\mathscr{S}$ is free, so let $S = R \oplus Rx$, and $\bigwedge^2 S = L = R(1 \wedge x)^{\otimes 2}$. Then

$$d((1 \wedge x)^{\otimes 2}) = \mathrm{trd}(x)^2 - 4\,\mathrm{nrd}(x) \equiv \mathrm{trd}(x)^2 \pmod{4R}.$$

On the other hand, by definition we have

$$\mathrm{sq}(t)((1 \wedge x)^{\otimes 2}) \equiv t(1 \wedge x)^2 = \mathrm{trd}(1 + x)^2 = (2 + \mathrm{trd}(x))^2 \equiv \mathrm{trd}(x)^2 \pmod{4R}.$$

The result follows. □

A quadratic $\mathscr{O}_X$-algebra $\mathscr{S}$ is separable if and only if d induces an isomorphism of $\mathscr{O}_X$-modules $(\bigwedge^2 \mathscr{S})^{\otimes 2} \xrightarrow{\sim} \mathscr{O}_X$, as this is true on any affine open set.

Let $\mathrm{Quad}(X)$ denote the set of isomorphism classes of quadratic $\mathscr{O}_X$-algebras, and for an invertible $\mathscr{O}_X$-module $\mathscr{L}$ let $\mathrm{Quad}(X; \mathscr{L}) \subseteq \mathrm{Quad}(X)$ be the subset of those algebras $\mathscr{S}$ such that there exists an isomorphism $\bigwedge^2 \mathscr{S} \simeq \mathscr{L}$ of $\mathscr{O}_X$-modules. Similarly, define $\mathbf{Quad}(X)$ to be the sheaf associated to the presheaf $U \mapsto \mathrm{Quad}(U)$.

We now give $\mathrm{Quad}(X)$ the structure of a commutative monoid.

Construction 3.14. *Let $X = \operatorname{Spec} R$ and let $S = R \oplus Rx$ and $T = R \oplus Ry$ be free quadratic R-algebras with choice of basis. Let $x^2 = tx - n$ and $y^2 = sy - m$ so*

$$t = \mathrm{trd}(x), n = \mathrm{nrd}(x), s = \mathrm{trd}(y), m = \mathrm{nrd}(y) \quad \text{with } t, n, s, m \in R.$$

Then we define the free quadratic R-algebra

$$S * T = R \oplus Rw$$

where

$$w^2 = (st)w - (mt^2 + ns^2 - 4nm). \tag{3.15}$$

Construction 3.14 has been known for some time, e.g., it is given by Hahn [8, Exercises 14–20, pp. 42–43]. (See the introduction for further context and references.)

Lemma 3.16. *Construction* 3.14 *is functorial with respect to the base ring R. The operation $*$ gives the set of free quadratic R-algebras with basis the structure of commutative monoid with identity element $R \times R = R[x]/(x^2 - x)$ and absorbing element $R[x]/(x^2)$.*

Proof. Functoriality is clear, and $S * T = T * S$ for all free quadratic R-algebras S, T by the symmetry of the construction. It is routine to check associativity. To check that $E = R \times R$ is the identity element for $*$ we simply substitute $s = 1, m = 0$ to obtain $S * E = S$; a similar check works for the absorbing element. □

Remark 3.17. Construction 3.14 generalizes the Kummer map, presented in the introduction. Indeed, suppose that R is a PID or local ring and $2 \in R^\times$. Then by completing the square, any quadratic R-algebra S is of the form $S = R[x]/(x^2 - n) = R[\sqrt{n}]$ where $n = d(S)/4$. So if $S = R[\sqrt{n}]$ and $T = R[\sqrt{m}]$, then

$$S * T = R[x]/(x^2 - 4nm) \simeq R[\sqrt{nm}].$$

At the same time, Construction 3.14 generalizes Artin-Schreier extensions of fields. Suppose that $R = k$ is a field of characteristic 2. Then every separable extension of k can be written in the form $k[x]/(x^2 - x + n)$, and

$$k[x]/(x^2 - x + n) * k[x]/(x^2 - x + m) = k[x]/(x^2 - x + (m + n)).$$

Since $4 = 0$, the discriminant of every such algebra has class 1 in $R/R^{\times 2}$.

In the above construction, if S, T are separable over R, so that they are (étale) Galois [13] extensions of R (with the standard involutions σ, τ respectively as the nontrivial R-algebra automorphisms), then the algebra $S * T$ is the subalgebra of $S \otimes_R T$ fixed by the product of the involutions $\sigma \otimes \tau$ acting on $S \otimes_R T$ [18, Proposition 1].

In all cases, a direct calculation shows that Equation 3.15 is satisfied by the element

$$w = x \otimes y + \sigma(x) \otimes \tau(y) \in S \otimes_R T;$$

this will figure in the proof of Theorem 3.27. However, there is no reason why the R-algebra generated by w need be free of rank 2 over R; for example, if R has characteristic 2 and $\sigma(x) = x$, $\tau(y) = y$, then $w = 0$. Thus, Construction 3.14 can be thought of as a formal way to create a fixed subalgebra of $S \otimes_R T$ under the involution given by the product of standard involutions.

Lemma 3.18. *Construction* 3.14 *is functorial with respect to isomorphisms: if*

$$\phi : S = R \oplus Rx \xrightarrow{\sim} S' = R \oplus Rx'$$
$$\psi : T = R \oplus Ry \xrightarrow{\sim} T' = R \oplus Ry'$$

are R-algebra isomorphisms of quadratic R-algebras, then there is a canonical isomorphism

$$\phi * \psi : S * T \xrightarrow{\sim} S' * T'.$$

Proof. There exist unique $u, v \in R^\times$ and $r, q \in R$ such that $\phi(x) = ux' + r$ and $\psi(y) = vy' + q$. Because ϕ is an R-algebra homomorphism, both $\phi(x)$ and x satisfy the same unique monic quadratic polynomial, and from

$$(ux' + r)^2 = t(ux' + r) - n$$

we conclude that

$$(x')^2 = u^{-1}(t-2r)x' - u^{-2}(n-tr-r^2) = t'x - n'$$

so $t = ut'+2r$ and $n = u^2n'+tr+r^2$. Similarly, we obtain $s = vs'+2q$ and $m = v^2m'+sq+q^2$. We claim then that the map

$$\begin{aligned} \phi * \psi : S * T &\xrightarrow{\sim} S' * T' \\ (\phi * \psi)(w) &= (uv)w' + (qt + rs - 2qr) \end{aligned}$$

is an isomorphism; for this we simply verify that

$$((uv)w' + (qt + rs - 2qr))^2 = st((uv)w' + (qt + rs - 2qr)) - (mt^2 + ns^2 - 4nm)$$

and the result follows. □

Lemma 3.19. *Let $\mathscr{S}, \mathscr{T}$ be quadratic $\mathscr{O}_X$-algebras. Then there is a unique quadratic $\mathscr{O}_X$-algebra $\mathscr{S} * \mathscr{T}$ up to $\mathscr{O}_X$-algebra isomorphism with the property that on any affine open set $U \subseteq X$ such that $S = \mathscr{S}(U)$ and $T = \mathscr{T}(U)$ are free, we have*

$$(\mathscr{S} * \mathscr{T})(U) \simeq S * T$$

as in Construction 3.14.

Proof. This lemma is a standard application of gluing; we give the argument for completeness. Let $\{U_i = \operatorname{Spec} R_i\}$ be an affine open cover of X on which

$$\mathscr{S}(U_i) = S_i = R_i \oplus R_i x_i \text{ and } \mathscr{T}(U_i) = T_i = R_i \oplus R_i y_i$$

are free. We define $(\mathscr{S} * \mathscr{T})(U_i) = S_i * T_i = R_i \oplus R_i w_i$ according to Construction 3.14. We glue these according to the isomorphisms on $\mathscr{S}$ and $\mathscr{T}$ using Lemma 3.18, as follows. We have $U_i \cap U_j = U_j \cap U_i = \bigcup_k U_{ijk}$ covered by open sets $U_{ijk} = \operatorname{Spec} R_{ik} \simeq \operatorname{Spec} R_{jk}$ distinguished in U_i and U_j. Because $\mathscr{S}$ is a sheaf, we have compatible isomorphisms

$$\phi_{ijk} : R_{ik} \oplus R_{ik}x_i = \mathscr{S}(\operatorname{Spec} R_{ik}) \simeq \mathscr{S}(\operatorname{Spec} R_{jk}) = R_{jk} \oplus R_{jk}x_j$$

for each such open set. Similarly, we obtain compatible isomorphisms ψ_{ijk} for $\mathscr{T}$ over the same open cover. By Lemma 3.18, we obtain compatible isomorphisms

$$\phi_{ijk} * \psi_{ijk} : (\mathscr{S} * \mathscr{T})(\operatorname{Spec} R_{ik}) \simeq (\mathscr{S} * \mathscr{T})(\operatorname{Spec} R_{jk})$$

and can thereby glue on X to obtain a quadratic $\mathscr{O}_X$-algebra, unique up to $\mathscr{O}_X$-algebra isomorphism. □

Corollary 3.20. *Construction* 3.14 *gives* $\operatorname{Quad}(X)$ *the structure of a commutative monoid, functorial in X, with identity element the isomorphism class of $\mathscr{O}_X \times \mathscr{O}_X$.*

Proof. Lemma 3.19 shows that Construction 3.14 extends to X and is well defined on the set of isomorphism classes $\operatorname{Quad}(X)$ of quadratic $\mathscr{O}_X$-algebras. To check that we obtain a functorial commutative monoid, it is enough to show this when X is affine, and this follows from Lemmas 3.16 and 3.18. □

Lemma 3.21. *If $\mathscr{S}$ is a separable quadratic $\mathscr{O}_X$-algebra, then $\mathscr{S} * \mathscr{S} \simeq \mathscr{O}_X \times \mathscr{O}_X$.*

Proof. By gluing, it is enough to show this on an affine cover. Suppose $S = R[x]/(x^2 - tx + n)$ has discriminant $d = t^2 - 4n$. Then by definition, we have

$$S * S = R[w]/(w^2 - t^2 w + 2n(t^2 - 2n));$$

with the substitution $w \leftarrow w - 2n$, we find that $S * S \simeq R[w]/(w^2 - dw)$. Since $d \in R^\times$, the replacement $w \leftarrow wd^{-1}$ yields an isomorphism $S * S \simeq R \times R$. □

Remark 3.22. Given our description of the monoid product in the separable case, it follows that the submonoid of separable quadratic algebras is isomorphic to the group of isomorphism classes of étale quadratic covers $\check{\mathrm{H}}^1_{\text{ét}}(X, \mathbb{Z}/2\mathbb{Z})$, a group killed by 2: for more, see Knus [11, §III.4].

Lemma 3.23. *If $\mathscr{S}, \mathscr{T} \in \mathrm{Quad}(X)$ then*

$$d(\mathscr{S} * \mathscr{T}) = d(\mathscr{S})d(\mathscr{T}) \in \mathrm{Disc}(X)$$

and

$$\bigwedge^2(\mathscr{S} * \mathscr{T}) \simeq \bigwedge^2 \mathscr{S} \otimes \bigwedge^2 \mathscr{T}.$$

Proof. If $S = \mathscr{S}(U)$ and $T = \mathscr{T}(U)$ are as in Construction 3.14, then

$$\begin{aligned} d(S * T)((1 \wedge (x \otimes y))^{\otimes 2}) &= (st)^2 - 4(mt^2 + ns^2 - 4nm) = (t^2 - 4n)(s^2 - 4m) \\ &= d(S)((1 \wedge x)^{\otimes 2})d(T)((1 \wedge y)^{\otimes 2}) \end{aligned} \tag{3.24}$$

The first statement then follows. For the second, again on affine open sets we have the isomorphism

$$\begin{aligned} \textstyle\bigwedge^2 S \otimes_R \bigwedge^2 T &\to \bigwedge^2(S * T) \\ (1 \wedge x) \otimes (1 \wedge y) &\mapsto 1 \wedge w, \end{aligned} \tag{3.25}$$

which glues to give the desired isomorphism globally. □

Lemma 3.26. *The discriminant maps*

$$\mathrm{disc} : \mathbf{Quad}(X) \to \mathbf{Disc}(X) \text{ and } \mathrm{disc} : \mathbf{Quad}(X; \mathscr{O}_X) \to \mathbf{Disc}(X; \mathscr{O}_X)$$

are surjective homomorphisms of sheaves of commutative monoids.

Proof. The fact that these maps are homomorphisms of sheaves of monoids follows locally from Lemma 3.23. We show these maps are surjective locally, and for that we may assume $X = \operatorname{Spec} R$ and $L = Re$. We refer to Lemma 2.15 and Example 2.17: given any $d \in R$ such that $d = t^2 - 4n$ with $t, n \in R$, we have the quadratic ring $R[x]/(x^2 - tx + n)$ of discriminant d. □

We are now ready to prove Theorem A.

Theorem 3.27. *Construction* 3.14 *is the unique system of binary operations*

$$* = *_X : \mathrm{Quad}(X) \times \mathrm{Quad}(X) \to \mathrm{Quad}(X),$$

one for each scheme X, such that:

(i) $\mathrm{Quad}(X)$ *is a commutative monoid under $*$, with identity element the class of $\mathscr{O}_X \times \mathscr{O}_X$;*

(ii) *For each morphism $f : X \to Y$ of schemes, the diagram*

$$\begin{array}{ccc} \mathrm{Quad}(Y) \times \mathrm{Quad}(Y) & \xrightarrow{*_Y} & \mathrm{Quad}(Y) \\ \downarrow & & \downarrow{\scriptstyle f^*} \\ \mathrm{Quad}(X) \times \mathrm{Quad}(X) & \xrightarrow{*_X} & \mathrm{Quad}(X) \end{array}$$

is commutative; and

(iii) *If $X = \operatorname{Spec} R$ and S, T are separable quadratic R-algebras with standard involutions σ, τ, then $S * T$ is the fixed subring of $S \otimes_R T$ under $\sigma \otimes \tau$.*

Proof. By (3.4), the universal free quadratic algebra with basis is the algebra

$$S_{\mathrm{univ}} = R_{\mathrm{univ}}[x]/(x^2 - tx + n)$$

where $R_{\mathrm{univ}} = \mathbb{Z}[t, n]$ is the polynomial ring in two variables over $\mathbb{Z}$: in other words, for any commutative ring R and free quadratic R-algebra S with basis, there is a unique map $f : R_{\mathrm{univ}} \to R$ such that $S = f^* S_{\mathrm{univ}} = S_{\mathrm{univ}} \otimes_{f, R_{\mathrm{univ}}} R$. By (ii), then, following this argument on an affine open cover, we see that the monoid structure on $\mathrm{Quad}(\operatorname{Spec} R_{\mathrm{univ}})$ determines the monoid structure for all schemes X.

Dispensing with subscripts, consider $S = R[x]/(x^2 - tx + n)$ and $T = R[y]/(y^2 - sy + m)$ where $R = \mathbb{Z}[t, n, s, m]$; we show there is a unique way to define $S * T$.

To begin, we claim that $S * T$ is free over R. As R-modules, we can write $S * T = R \oplus Iz$ where $I \subseteq F = \mathrm{Frac}(R)$ is a projective R-submodule of F and the class $[I] \in \mathrm{Pic}(R)$ well-defined. But $\mathrm{Pic}(\mathbb{Z}[t, n, s, m]) \simeq \mathrm{Pic}(\mathbb{Z}) = \{0\}$ ($\mathbb{Z}$ is *seminormal* [7]), so $I \simeq R$.

Now let

$$D = (t^2 - 4n)(s^2 - 4m).$$

Then $S[1/D]$ and $T[1/D]$ are separable over $R[1/D]$, with involutions $\sigma(x) = t - x$ and $\tau(y) = s - y$. By (iii), the product $S[1/D] * T[1/D]$ is the subring of $S[1/D] \otimes_{R[1/D]} T[1/D]$ generated by

$$z = x \otimes y + \sigma(x) \otimes \tau(y) = 2(x \otimes y) - s(x \otimes 1) - t(1 \otimes y).$$

Then

$$\begin{aligned} z^2 &= x^2 \otimes y^2 + 2nm + \sigma(x)^2 \otimes \tau(y)^2 \\ &= (tx - n) \otimes (sy - m) + 2nm + (t\sigma(x) - n) \otimes (s\tau(y) - m) \\ &= ts(x \otimes y + \sigma(x) \otimes \tau(y)) - mt((x + \sigma(x)) \otimes 1) - ns(1 \otimes (y + \tau(y))) + 4nm \\ &= (st)z - (mt^2 + ns^2 - 4nm). \end{aligned}$$

In particular, $S[1/D] * T[1/D] \simeq R[1/D] \oplus R[1/D]z$.

By (ii), $(S * T)[1/D] \simeq S[1/D] * T[1/D]$, and we have $S * T \subseteq (S * T)[1/D]$. Since R is a UFD and $S * T$ is free over R, it is generated as an R-algebra by an element of the form $(az + b)/D^k$ for some $a, b \in R$ and $k \in \mathbb{Z}_{\geq 0}$. But by (3.24), $d((S * T)[1/D]) = D$, so $d(S * T) = (a/D^k)^2 D \in R$, thus $a/D^k \in R$. Since $\mathrm{trd}((az + b)/D^k) = (ast + 2b)/D^k \in R$, we conclude that $2b/D^k \in R$; since D is not divisible by 2, by Gauss's lemma we have $b/D^k \in R$, so without loss of generality we may take $b = 0$ and suppose that $S * T$ is generated by az

for some $a \in R$. Since $R^\times = \{\pm 1\}$ and $(S * T)[1/D]$ is generated by z, we must have $a = D^k$ for some $k \in \mathbb{Z}_{\geq 0}$. Finally, we consider

$$\frac{\mathbb{Z}[x]}{(x^2 - tx + n)} * \frac{\mathbb{Z}[y]}{(y^2 - y)} = \frac{\mathbb{Z}[z]}{(z^2 - D^k tz + D^{2k} n)}$$

over $\mathbb{Z}[t, n]$. The algebra on the right has discriminant $D^{2k}(t^2 - 4n)$, but by (i), it must be isomorphic to the algebra on the left of discriminant $(t^2 - 4n)$, so we must have $D^{2k} = 1$, so $k = 0$. Therefore $S * T = R \oplus Rz$. □

Having given the monoid structure, we conclude this section by proving Theorem B.

Theorem 3.28. *Let X be a scheme. Then the following diagram of commutative monoids is functorial and commutative with exact rows and surjective columns:*

$$\begin{array}{ccccc} \mathbf{Quad}(X; \mathscr{O}_X) & \longrightarrow & \mathbf{Quad}(X) & \xrightarrow{\wedge^2} & \mathbf{Pic}(X) \\ \downarrow{\scriptstyle \text{disc}} & & \downarrow{\scriptstyle \text{disc}} & & \| \\ \mathbf{Disc}(X; \mathscr{O}_X) & \longrightarrow & \mathbf{Disc}(X) & \longrightarrow & \mathrm{Pic}(X) \end{array}$$

Proof. The exactness of the bottom row follows from Proposition 2.18. The exactness of the top row and commutativity of the diagram follows by the same (trivial) argument. Surjectivity follows from Lemma 3.26. □

4. Proof of Theorem C

In this section, we prove Theorem C and conclude with some final discussion.

Let R be a commutative ring and let $R[4] = \{a \in R : 4a = 0\}$. Let

$$\wp(R) = \{r + r^2 : r \in R\}.$$

and let $\wp(R)[4] = \wp(R) \cap R[4]$. Note that $4(r + r^2) = 0$ if and only if $(1 + 2r)^2 = 1$, so we have equivalently

$$\wp(R)[4] = \{r + r^2 : r \in R \text{ and } (1 + 2r)^2 = 1\}.$$

Lemma 4.1. *$\wp(R)[4]$ is a subgroup of $R[4]$ under addition.*

Proof. We have $0 = 0 + 0^2 \in \wp(R)[4]$. If $n = r + r^2 \in \wp(R)[4]$ and $m = s + s^2 \in \wp(R)[4]$ then

$$(r + s + 2rs) + (r + s + 2rs)^2 = (r + r^2) + (s + s^2) + 4(r + r^2)(s + s^2) = n + m$$

and $4(n + m) = 0$, so $n + m \in \wp(R)[4]$. Finally, if $n \in \wp(R)[4]$ then $-n = 3n \in \wp(R)[4]$ by the preceding sentence. □

We define the *Artin-Schreier group* $\mathrm{AS}(R)$ to be the quotient

$$\mathrm{AS}(R) = \frac{R[4]}{\wp(R)[4]}.$$

Since $2R[4] \subseteq \wp(R)[4]$, the group $\mathrm{AS}(R)$ is an elementary abelian 2-group.

We define a map $i : \mathrm{AS}(R) \to \mathrm{Quad}(R; R)$ sending the class of $n \in \mathrm{AS}(R)$ to the isomorphism class of the algebra $S = R[x]/(x^2 - x + n)$.

Proposition 4.2. *The map $i : \mathrm{AS}(R) \to \mathrm{Quad}(R, R)$ is a (well-defined) injective map of commutative monoids.*

Proof. Let $S = i(n) = R[x]/(x^2-x+n)$ and $T = i(m) = R[y]/(y^2-y+m)$ with $n, m \in \mathrm{AS}(R)$. Then $S \simeq T$ if and only if $y = u(x+r)$ for some $u \in R^\times$ and $r \in R$, which by (3.5) holds if and only if $u(1+2r) = 1$ and $u^2(n+r+r^2) = m$; these are further equivalent to $1+2r \in R^\times$ and

$$n + r + r^2 = m(1+2r)^2 = (1+4r+4r^2)m.$$

But $4m = 0$ so $n + r + r^2 = m$ and since $4n = 0$ we have $4(r + r^2) = 0$. Thus $S \simeq T$ if and only if $(1+2r)^2 = 1$ and $n + r + r^2 = m$, as desired. It follows from Construction 3.14 that $S * T = R[w]/(w^2 - w + (n+m))$, since $4nm = 0$, and $i(0) = R[w]/(w^2 - w)$ is the identity, so i is a homomorphism of monoids. □

We now prove Theorem C, and recall $\mathrm{Quad}(R; R)$ is the set of isomorphism classes of free quadratic R-algebras.

Theorem 4.3. *Let R be a commutative ring and let $d \in R$ be a discriminant. Then the fiber $\mathrm{disc}^{-1}(d)$ of the map*

$$\mathrm{disc} : \mathrm{Quad}(R; R) \to \mathrm{Disc}(R; R)$$

above d has a unique action of the group $\mathrm{AS}(R)/\operatorname{ann}_R(d)[4]$ compatible with the inclusion of monoids $\mathrm{AS}(R) \hookrightarrow \mathrm{Quad}(R; R)$.

Proof. A (free) quadratic R-algebra with basis $1, x$ such that $(x - \sigma(x))^2 = d$ is of the form $S = R[x]/(x^2 - tx + n)$ with $t^2 - 4n = d$. Let $m \in R[4]$. Then by Construction 3.14 we have

$$S * (R[y]/(y^2 - y + m)) = (R[y]/(y^2 - y + m)) * S = R[w]/(w^2 - tw + dm + n)$$

since $4m = 0$ so $dm = (t^2 - 4n)m = t^2 m$. Thus we have an action of $R[4]$ on the set of these quadratic R-algebras with basis and a free action of $R[4]/\operatorname{ann}_R(d)[4]$. Two quadratic R-algebras S and S' are in the same orbit if and only if $t' = t$ and $n' = dm + n$ for some $m \in R[4]$ if and only if $t' = t$ and $n' - n \in dR[4]$; therefore, the orbits are indexed noncanonically by the set

$$\{t \in R : t^2 \equiv d \pmod{4R}\} \times R[4]/dR[4].$$

We now descend to isomorphism classes: by Proposition (4.2), the monoid multiplication $*$ is well-defined on isomorphism classes, giving the unique action of $\mathrm{AS}(R)/\operatorname{ann}_R(d)[4]$ on the fiber over d. □

Under favorable hypotheses, the action of $\mathrm{AS}(R)$ is free, and so we make the following definition.

Definition 4.4. An element $t \in R$ is *sec* (*square even cancellative*) if:

(i) t is a nonzerodivisor, and
(ii) $r^2, 2r \in tR$ implies $r \in tR$ for all $r \in R$.

A quadratic R-algebra S is *sec* if $\mathrm{disc}(S)$ is a nonzerodivisor and there a basis $1, x$ for S such that $\mathrm{trd}(x)$ is sec. A quadratic $\mathscr{O}_X$-algebra $\mathscr{S}$ is *sec* if $\mathscr{S}$ is sec on an affine open cover of X.

Proposition 4.5. *Let R be a commutative ring. Then the action of $\mathrm{AS}(R)$ on the set of sec quadratic R-algebras of discriminant d is free.*

Proof. We continue as in the proof of Theorem 4.3. Let $m \in R[4]$ and let S be a sec quadratic R-algebras with discriminant d. Let $1, x$ be a basis for $S = R[x]/(x^2 - tx + n)$ such that $t = \mathrm{trd}(x)$ is sec. To show the action is free, suppose that

$$S * (R[y]/(y^2 - y + m)) = R[w]/(w^2 - tw + dm + n) \simeq S; \tag{4.6}$$

we show that $m \in \wp(R)$. Equation (4.6) holds if and only if there exist $u \in R^\times$ and $r \in R$ such that $t = u(t + 2r)$ and $dm + n = u^2(n + tr + r^2)$. Consequently, $u^2 d = d$. Since S is sec, d is a nonzerodivisor, so $u^2 - 1 = 0$, and thus $t^2 m = dm = tr + r^2$ so $r^2 = (tm - r)t$. We also have $2r = (1 - u)t$, so since t is sec and $r^2, 2r \in tR$, we conclude that $r \in tR$. Let $r = at$ with $a \in R$. Then substituting, we have $t^2(a^2 + a - m) = r^2 + tr - t^2 m = 0$. Since t is a nonzerodivisor, we conclude that $a^2 + a - m = 0$, so $m \in \wp(R)$ as claimed. □

References

[1] George Bergman, *An invitation to general algebra and universal constructions*, `http://math.berkeley.edu/~gbergman/245/`.

[2] Manjul Bhargava, *Gauss composition and generalizations*, ANTS 2002, Claus Fieker and David Kohel, eds., 2002, 1–8.

[3] Owen Biesel and Alberto Gioia, *A new discriminant algebra construction*, 2015, `arXiv:1503.05318v1`.

[4] Manjul Bhargava, *Higher composition laws and applications*, Proceedings of the ICM: Madrid, 2006, 271–294.

[5] Stanley N. Burris and H.P. Sankappanavar, *A course in universal algebra: millenenium edition*, `http://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html`.

[6] Pierre Deligne, *Letter to Rost and Bhargava*, 2 March 2005.

[7] Robert Gilmer and Raymond C. Heitmann, *On* $\mathrm{Pic}(R[X])$ *for R seminormal*, J. Pure. Appl. Algebra **16** (1980), 251–257.

[8] Alexander J. Hahn, *Quadratic algebras, Clifford algebras, and arithmetic Witt groups*, Springer–Verlag, New York, 1994.

[9] Teruo Kanzaki, *On the quadratic extensions and the extended Witt ring of a commutative ring*, Nagoya Math. J. **49** (1973), 127–141.

[10] Steven L. Kleiman, *Misconceptions about* K_X, L'Enseignment Math. **25** (1979), 203–206.

[11] Max-Albert Knus, *Quadratic and Hermitian forms over rings*, Grundlehren der Mathematischen Wissenschaften, vol. 294, Springer-Verlag, Berlin, 1991.

[12] 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, 1998.

[13] Hendrik W. Lenstra, *Galois theory for schemes*, 2008.

[14] Ottmar Loos, *Tensor products and discriminants of unital quadratic forms over commutative rings*, Mh. Math. **122** (1996), 45–98.

[15] Ottmar Loos, *Discriminant algebras of finite rank algebras and quadratic trace modules*, Math. Z. **257** (2007), 467–523.

[16] Ralph N. McKenzie, George F. McNulty, and Walter F. Taylor, *Algebras, lattices, varieties*, vol. 1, Wadsworth & Brooks/Cole, Monterey, California, 1987.

[17] Markus Rost, *The discriminant algebra of a cubic algebra*, `http://www.math.uni-bielefeld.de/~rost/data/cub-disc.pdf`, 2002.

[18] Charles Small, *The group of quadratic extensions*, J. Pure Applied Algebra **2** (1972), 83–105.

[19] The Stacks Project Authors, *Stacks project*, `http://stacks.math.columbia.edu`, 2015.

[20] John Voight, *Rings of low rank with a standard involution*, Ill. J. Math. **55** (2011), no. 3, 1135–1154.

[21] Melanie Wood, *Gauss composition over an arbitrary base*, Adv. Math. **226** (2011), no. 2, 1756–1771.

Department of Mathematics and Statistics, University of Vermont, 16 Colchester Ave, Burlington, VT 05401, USA; Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: jvoight@gmail.com