A final remark: Gauss' theory of binary quadratic forms led to two major developments: the theory of number fields on the one hand, and the theory of quadratic forms in more than two variables on the other. The arithmetic of forms of higher degree over $\mathbf{Z}$ seems to have been largely neglected. In modern times Shintani revived interest in the arithmetic of cubic forms by introducing a family of Dirichlet series that depend on class numbers of cubic forms, and have good analytic properties (analytic continuation and functional equations). This work has been reinterpreted in the language of adèles by Wright [16]. For a general introduction to arithmetic problems concerning forms of higher degree, see [9].

We would like to thank J. Hurrelbrink and S. Weintraub for helpful discussions concerning this work.

CONTENTS

2. BINARY QUADRATIC MAPPINGS

We shall assume throughout this section that the ground ring R is an integral domain of characteristic not 2. The fraction field of R will be denoted by K.

A *binary quadratic form* is a pair (M, q) such that M is a projective R-module of rank two and $q: M \to R$ is a mapping such that $q(a\mathbf{x}) = a^2 q(\mathbf{x})$, $a \in R$, $\mathbf{x} \in M$, and such that $b(\mathbf{x}, \mathbf{y}) := q(\mathbf{x} + \mathbf{y}) - q(\mathbf{x}) - q(\mathbf{x})$ is R-bilinear. The form q is said to be *primitive* if the ideal generated by $q(M)$ is R. A morphism $(M, q) \to (M', q')$ is an R-linear mapping $f: M \to M'$ such that $q = q' \circ f$. If $M = R^2$ is the free module, we will often omit reference to M.

Let C be a quadratic R-algebra in the sense of [11], that is, an R-algebra, which as an R-module is projective of rank two, and such that $R1 \subset C$ is a direct factor of C as R-modules. Locally over $\operatorname{Spec} R$, such an algebra C is isomorphic with an algebra of the form

$$R[t]/(t^2 + bt + c), \qquad (b, c \in R).$$

Let $n\colon C \to R$ and $t\colon C \to R$ be the norm and the trace maps of C. It is easy to see that C possesses a unique nontrivial R-automorphism $x \mapsto \bar{x}$ satisfying $t(x) = x + \bar{x}$ and $n(x) = x\bar{x}$.

When $R = \mathbf{Z}$, for each nonzero integer $D \equiv 0$ or $1 \pmod 4$, we shall denote by C_D the unique quadratic $\mathbf{Z}$-algebra of discriminant D.

The notion of a *form of type* C was introduced by Kneser [11] and will play an important role in this paper.

DEFINITION 2.1. Let M be a projective C-module of rank 1. We say that a quadratic form $q\colon M \to R$ is *of type* C if it satisfies

$$q(c\mathbf{x}) = n(c)q(\mathbf{x}) \tag{8}$$

for all $\mathbf{x} \in M$, $c \in C$. A C-morphism $(M, q) \to (M', q')$ is a C-linear mapping $f\colon M \to M'$ such that $q = q' \circ f$.

Recall that the Clifford algebra $C(M, q)$ is the quotient of the tensor algebra $T_R(M)$ by the ideal generated by $\mathbf{x}\otimes\mathbf{x} - q(\mathbf{x})1$ for all $\mathbf{x} \in M$. The *even Clifford algebra*, $C^+(M, q)$, is the subalgebra generated by tensors of even degree, and is easily seen to be a quadratic R-algebra. Also, M is identified with the odd part of the Clifford algebra (i.e., generated by tensors of odd degree), and the map $C^+(M, q) \times M \to M$ induced by multiplication in $C(M, q)$ makes M into a $C^+(M, q)$-module. The formation of the Clifford algebra commutes with localization on $\operatorname{Spec} R$.

In the special case when $M = R^2$ we can describe $C^+(M, q)$ explicitly: Let $\{e_1, e_2\}$ be a basis of R^2 relative to which $q = ax_1^2 + bx_1x_2 + cx_2^2$. Then $e_1^2 = a$, $e_2^2 = c$, $e_1e_2 + e_2e_1 = b$ in the Clifford algebra of q. Thus if $\omega = -e_1e_2$ we have

$$C^+(q) = R[\omega] = R[x]/(x^2 + bx + ac).$$

PROPOSITION 2.2 ([11, Proposition 1]).

1. *Let (M,q) be a primitive quadratic form and $C = C^+(M,q)$ its even Clifford algebra. Then M becomes a projective C-module of rank one, and (M,q) is a quadratic form of type C.*

2. *Let C be a quadratic R-algebra and (M,q) be a nonzero quadratic form of type C. Then there exists a unique homomorphism of R-algebras*

$$\phi\colon C^+(M,q) \to C$$

satisfying $\phi(u)\mathbf{x} = u\mathbf{x}$ for $u \in C^+(M,q)$ and $\mathbf{x} \in M$. Furthermore, ϕ is an isomorphism if and only if q is primitive.

If q is a binary form over $\mathbf{Z}$ of discriminant D, then $C^+(M,q)$ is the unique quadratic algebra C_D over $\mathbf{Z}$ of discriminant D. If moreover q is primitive, then q is of type C_D. Thus all the primitive forms of discriminant D are of type C_D.

Kneser showed [11, Theorem 3] that the set $G(C)$ of primitive binary forms of type C modulo C-isomorphism forms a group for composition, which generalizes Gauss' theory for binary quadratic forms over $\mathbf{Z}$. The group law on $G(C)$ is explicitly given as follows: The composition of (M,q) and (M',q') is the form $(M \otimes_C M', q'')$, where $q''(\mathbf{x} \otimes \mathbf{y}) = q(\mathbf{x})q'(\mathbf{y})$. The neutral element is clearly (C,n).

The relation between C-isomorphism and R-isomorphism of quadratic forms is explained by the following proposition. Recall that an algebra over a field is *étale* if it is a product of separable extension fields of that field.

PROPOSITION 2.3. *Let C be a quadratic R-algebra, and suppose that $C \otimes K$ is an étale K-algebra. Let (M,q) and (M',q') be nonzero quadratic forms of type C. Then every R-isomorphism $f\colon (M,q) \to (M',q')$ is either C-linear or C-sesquilinear.*

Proof. By extending scalars to K, it will suffice to prove our proposition for the case when $R = K$. The map f will induce an isomorphism of the even Clifford algebras $C^+(M,q) \to C^+(M',q')$. These algebras are canonically isomorphic with C by Proposition 2.2, and hence f induces an automorphism f_* of the K-algebra C satisfying $f(c\mathbf{x}) = f_*(c)f(\mathbf{x})$. By hypothesis C is an étale algebra over K, so its only K-automorphisms are the identity and the canonical conjugation. Thus $f_*(c)$ is either c or $\bar{c}$ for all $c \in C$, which completes the proof. □

Note that the proposition is false if $C \otimes K$ is not étale, as can be easily seen by taking $C = R[t]/(t^2)$ with the norm form.

Let (M, q) be a nonzero binary quadratic form over R. Suppose that it is of type C, and let $C_1^\times$ be the subgroup of the units of C with $n(c) = 1$. Then we obtain a natural homomorphism (l_c = multiplication by c in M):

$$\begin{aligned} C_1^\times &\longrightarrow \mathbf{SO}(M, q) \\ c &\longmapsto l_c \end{aligned} \tag{9}$$

where $\mathbf{SO}(M, q) \subset \mathrm{Aut}_R(M)$ is the subgroup of R-automorphisms fixing q and having determinant 1.

COROLLARY 2.4. *With the above hypotheses, and assuming that $C \otimes K$ is an étale K-algebra, the map (9) is an isomorphism.*

Proof. Since M is projective of rank one over C, the map $c \to l_c$ is an isomorphism $C \simeq \mathrm{End}_C(M)$; thus it is enough to show that the elements of $\mathbf{SO}(M, q)$ are C-linear.

Let $f \in \mathbf{SO}(M, q)$. It is sufficient to show the C-linearity of f locally; so we may assume $M = C$ and $q = an$ with $a \in C^\times$.

The canonical conjugation σ of C preserves q and has determinant -1. Suppose now that f is C-sesquilinear. Then $f\sigma$ is C-linear, i.e. $f\sigma = l_c$ for some $c \in C^\times$ which must satisfy $n(c) = \det(l_c) = 1$, since l_c preserves q. Thus $\det(f) = -1$, contrary to our hypothesis. Hence, by Proposition 2.3, the map f must be C-linear. □

To define an analogue of Eisenstein's determining form (2) for general rings, we shall need the more general notion of binary quadratic mapping.

A *binary quadratic mapping* over R is a triple (M, q, N) where M is a projective R-module of rank two, N is a projective R-module of rank one and $q: M \to N$ is a map such that $q(a\mathbf{x}) = a^2 q(\mathbf{x})$ and $b(\mathbf{x}, \mathbf{y}) = q(\mathbf{x} + \mathbf{y}) - q(\mathbf{x}) - q(\mathbf{y})$ is R-bilinear.

A morphism $(M, q, N) \to (M', q', N')$ is a pair (f, g) of R-linear maps

$$f: M \to M' \qquad \text{and} \qquad g: N \to N'$$

such that $q'f = gq$. We say that (M, q, N) is *primitive* if $Rq(M) = N$. If N is free over R, then choosing a basis $\mathbf{n}$ of N we can write $q(\mathbf{x}) = Q(\mathbf{x})\mathbf{n}$. Then (M, Q) is a quadratic form in the previous sense. Note however that in this case (M, q, N) is isomorphic to (M', q', N') as quadratic mappings if and only if there exists a unit $u \in R^\times$ such that $(M, Q) \simeq (M', uQ')$ as quadratic forms.

Hence we can think of a quadratic mapping over R as defining a family of quadratic forms up to similarity equivalence, locally on a covering of $\operatorname{Spec} R$, and glued together in an obvious sense.

In the case $R = \mathbf{Z}$ every projective module is free, so that a quadratic mapping in this case is the same thing as a quadratic form, but up to similarity equivalence as above. This differs therefore from the usual theory, based on $\mathbf{SL}_2(\mathbf{Z})$-equivalence, but this difference is easily accounted for (see the discussion for PIDs in Section 5).

Let C be a quadratic algebra and assume that M is a projective C-module of rank 1. A quadratic mapping (M, q, N) is of *type* C if q satisfies the identity (8).

In order to have an analogue of Proposition 2.2 we need a definition of the even Clifford algebra in the context of quadratic mappings. The (total) Clifford algebra of a quadratic mapping (as opposed to a quadratic form) cannot be defined. The reason is that the Clifford algebra is not a functor for similarities of quadratic forms. As Kneser observed, the *even* Clifford algebra is a functor for similarities of quadratic forms. We can define directly the even Clifford algebra for quadratic mappings as follows:

DEFINITION 2.5. Let (M, q, N) be a quadratic mapping. The *even Clifford algebra* $C^+(M, q, N)$ is the quotient of the tensor algebra

$$T_R(N^* \otimes M \otimes M),$$

where $N^* = \operatorname{Hom}_R(N, R)$, by the ideal generated by

$$(10) \qquad \begin{cases} \lambda \otimes \mathbf{x} \otimes \mathbf{x} - \lambda(q(\mathbf{x})) \\ (\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \otimes (\mu \otimes \mathbf{y} \otimes \mathbf{z}) - \lambda(q(\mathbf{y}))\ \mu \otimes \mathbf{x} \otimes \mathbf{z} \end{cases}$$

$(\lambda, \mu \in N^*,\ \mathbf{x}, \mathbf{y}, \mathbf{z} \in M)$.

One verifies easily that the above definition depends only on the isomorphism class of (M, q, N). For a similar construction, see [10, Ch. II, Section 8]. Note that the second defining relation can also be written as

$$(\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \otimes (\mu \otimes \mathbf{y} \otimes \mathbf{z}) - \mu(q(\mathbf{y}))\ \lambda \otimes \mathbf{x} \otimes \mathbf{z}.$$

This is because $\lambda(u)\mu(v) = \lambda(v)\mu(u)$ on N since the difference is an alternating bilinear form, which must vanish since N has rank 1. We also need to define a $C^+(M, q, N)$-module structure on M; this is not completely obvious since the total Clifford algebra is no longer available. We begin with a lemma:

LEMMA 2.6. *Let Q be a quadratic form on M and let B be the associated bilinear form. Then*

$$B(\mathbf{x},\mathbf{y})\mathbf{z} - B(\mathbf{z},\mathbf{x})\mathbf{y} + B(\mathbf{y},\mathbf{z})\mathbf{x} \equiv 0 \pmod{2M}$$

for all $\mathbf{x},\mathbf{y},\mathbf{z} \in M$.

Proof. Let C be the Clifford algebra of Q. The expression

$$\sum_{\sigma} \operatorname{sign}(\sigma)\mathbf{x}_{\sigma 1}\mathbf{x}_{\sigma 2}\mathbf{x}_{\sigma 3}\,, \tag{11}$$

where σ runs over all permutations of $\{1,2,3\}$, defines an alternating R-trilinear map $M^3 \to C$. Since M has rank 2 over R, we have $\wedge^3 M = 0$; thus the expression (11) is identically zero. The lemma follows from the identity $\mathbf{x}_i\mathbf{x}_j + \mathbf{x}_j\mathbf{x}_i = B(\mathbf{x}_i,\mathbf{x}_j)$ in the Clifford algebra. □

We can now define a $C^+(M,q,N)$-module structure on M as follows:

$$(\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \cdot \mathbf{z} = \tfrac{1}{2}[\lambda(b(\mathbf{x},\mathbf{y}))\mathbf{z} - \lambda(b(\mathbf{z},\mathbf{x}))\mathbf{y} + \lambda(b(\mathbf{y},\mathbf{z}))\mathbf{x}]\,. \tag{12}$$

Note that dividing by 2 in (12) makes sense in M by virtue of Lemma 2.6 applied to $Q = \lambda \circ q$, $B = \lambda \circ b$, and the fact that R is an integral domain of characteristic not 2. To see that this is a well-defined module we need:

LEMMA 2.7. *The definition* (12) *is compatible with the defining relations* (10) *for* $C^+(M,q,N)$.

Proof. This is straightforward for the first relation. For the second relation of (10), we can, without loss of generality, extend scalars from R to its fraction field K. We prove that the second relation vanishes when applied to an element $\mathbf{w} \in M$. If the vectors $\mathbf{z}$ and $\mathbf{y}$ are linearly dependent, say $\mathbf{z} = a\mathbf{y}$ for $a \in K$, then the second relation is a consequence of the first, so we may assume that $\mathbf{z}$ and $\mathbf{y}$ are linearly independent. In this case it is enough to consider the subcases (a) $\mathbf{w} = \mathbf{y}$, (b) $\mathbf{w} = \mathbf{z}$, since now $\mathbf{y}$, $\mathbf{z}$ forms a basis of M. The case (b) is easily seen by direct computation of both sides. In case (a), applying $(\lambda \otimes \mathbf{x} \otimes \mathbf{y}) \otimes (\mu \otimes \mathbf{y} \otimes \mathbf{z})$ to $\mathbf{y}$, we get

$$\tfrac{1}{4}\big(2\mu(b(\mathbf{y},\mathbf{z}))\,\lambda(b(\mathbf{y},\mathbf{y}))\,\mathbf{x} - \mu(b(\mathbf{y},\mathbf{y}))\,\lambda(b(\mathbf{x},\mathbf{y}))\,\mathbf{z} + \mu(b(\mathbf{y},\mathbf{y}))\,\lambda(b(\mathbf{z},\mathbf{x}))\,\mathbf{y} - \mu(b(\mathbf{y},\mathbf{y}))\,\lambda(b(\mathbf{y},\mathbf{z}))\,\mathbf{x}\big)\,.$$

In the last three terms in this formula, we may exchange λ and μ, using the identity $\lambda(u)\mu(v) = \lambda(v)\mu(u)$. The expression then reduces to

$$\tfrac{1}{2}\lambda(q(\mathbf{y}))\big(\mu(b(\mathbf{x},\mathbf{z}))\,\mathbf{y} - \mu(b(\mathbf{y},\mathbf{x}))\,\mathbf{z} + \mu(b(\mathbf{z},\mathbf{y}))\,\mathbf{x}\big)$$

which is exactly the proposed identity. □

It is important to note that in the case of a quadratic form, as opposed to a quadratic mapping, (12) really defines the usual module structure given by multiplication in the Clifford algebra of the form. Namely, the expression in (12) equals $\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z}$ in that algebra. We leave this verification to the reader (hint: use (11) and the fact that $\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z} = \mathbf{z} \otimes \mathbf{y} \otimes \mathbf{x}$ in the Clifford algebra of a binary quadratic form).

Locally on $\mathrm{Spec}(R)$, where both M and N are free, the choice of trivializations of these modules reduces a quadratic mapping to a quadratic form well-defined up to scalar multiples by a local unit. The even Clifford algebra as we have defined it is isomorphic on this open set to the Clifford algebra of this quadratic form, and the module structure as we have defined it coincides with the module structure given by multiplication in the Clifford algebra of the locally defined form. In fact, we can define the even Clifford algebra and the module structure by taking these locally defined objects and gluing them together, which provides an alternative construction.

Here is the analogue of Proposition 2.2 for quadratic mappings:

PROPOSITION 2.8.

1. *If* (M, q, N) *is primitive, then* M *is a projective* $C = C^+(M, q, N)$*-module of rank one and* q *is of type* C.

2. *Let* (M, q, N) *be a nonzero quadratic mapping of type* C, *and let* $C^+(M, q, N)$ *be its even Clifford algebra. Then there exists a unique homomorphism of* R*-algebras* $\phi\colon C^+(M, q, N) \to C$ *satisfying* $\phi(u)\mathbf{x} = u\mathbf{x}$ *for* $u \in C^+(M, q, N)$ *and* $\mathbf{x} \in M$. *Furthermore,* ϕ *is an isomorphism if and only if* q *is primitive.*

We shall omit the proof, since it is essentially rephrasing the proof given in [11, Proposition 1].

REMARK 2.9. Proposition 2.3 also holds for quadratic mappings. This can be easily seen by extending the scalars to K.

M. Kneser [11, Section 6] shows that the set $H(C)$ of isomorphism classes of primitive binary quadratic mappings (M, q, N) of type C forms a group for composition, the neutral element being (C, n, R). Note that the equivalence relation here is C-equivalence: an isomorphism is a pair (f, g) as before, but with f a C-linear isomorphism. He also showed that $H(C)$ is isomorphic to the group $\mathrm{Pic}(C)$ via the canonical map $(M, q, N) \mapsto M$.

We compare the group $G(C)$ of C-isomorphism classes of primitive quadratic forms of type C and the group $H(C)$ above by means of the canonical group homomorphism $G(C) \to H(C)$ induced by the correspondence $(M,q) \mapsto (M,q,R)$. M. Kneser (*op. cit.*) showed that this map fits into an exact sequence

$$0 \longrightarrow R^\times/n(C^\times) \longrightarrow G(C) \longrightarrow H(C) \xrightarrow{n} \operatorname{Pic}(R). \tag{13}$$

In the classical case of a quadratic $\mathbf{Z}$-algebra C of discriminant D, the sequence (13) was essentially known to Dedekind. Since $\operatorname{Pic}(\mathbf{Z}) = 0$ and $\mathbf{Z}^\times = \{\pm 1\}$, the sequence (13) shows that the group $G(C)$ is the narrow class group of C if $D > 0$, and it is $\{\pm 1\}\times$ the class group of C if $D < 0$ (the sign corresponding to positive and negative definite forms). In either case, it differs from the ideal class group $\operatorname{Pic}(C)$ at most by a cyclic factor of order 2.

It is worth noticing that the exact sequence above has a natural interpretation in flat cohomology. Let $\pi\colon \operatorname{Spec} C \to \operatorname{Spec} R$ be the natural morphism. Let $\mathcal{G} = \operatorname{Aut}_C(C,n)$ and $\mathcal{H} = \operatorname{Aut}_C(C,n,R)$ as group schemes over $\operatorname{Spec} R$. One sees immediately that $\mathcal{H} = \pi_*\mathbf{G}_m$, where $\mathbf{G}_m$ is the multiplicative group scheme, and that $\mathcal{G}$ is the kernel of the norm map $n\colon \pi_*\mathbf{G}_m \to \mathbf{G}_m$. From the short exact sequence of group schemes over $\operatorname{Spec} R$

$$0 \longrightarrow \mathcal{G} \longrightarrow \mathcal{H} \longrightarrow \mathbf{G}_m \longrightarrow 0,$$

we obtain the long exact sequence (see [14, Chap. III, §4])

$$0 \to R^\times/n(C^\times) \to H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{G}) \to H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{H}) \xrightarrow{n} H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathbf{G}_m),$$

where the flat topology is understood. The group $G(C)$ [respectively $H(C)$] can be identified with $H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{G})$ [respectively $H^1_{\mathrm{fl}}(\operatorname{Spec} R, \mathcal{H})$] by interpreting quadratic forms [respectively quadratic mappings] as torsors for $\mathcal{G}$ [respectively $\mathcal{H}$] in the flat topology.

Note that there is a natural isomorphism

$$H^1_{\mathrm{fl}}(\operatorname{Spec} R, \pi_*\mathbf{G}_m) = H^1_{\mathrm{fl}}(\operatorname{Spec} C, \mathbf{G}_m),$$

so we also have $H(C) = \operatorname{Pic}(C)$ (compare [11, Proposition 2]).