JOURNAL OF
PURE AND
APPLIED ALGEBRA

ELSEVIER Journal of Pure and Applied Algebra 120 (1997) 255–280

# A stable range for quadratic forms over commutative rings

Dennis R. Estes, Robert M. Guralnick *[,1]

*Department of Mathematics, University of Southern California, Los Angeles, CA, 90089-1113, USA*

Communicated by C.A. Weibel; received 16 April 1995; revised 17 January 1996

**Abstract**

A commutative ring $A$ has quadratic stable range 1 ($\mathrm{qsr}(A) = 1$) if each primitive binary quadratic form over $A$ represents a unit. It is shown that $\mathrm{qsr}(A) = 1$ implies that every primitive quadratic form over $A$ represents a unit, $A$ has stable range 1 and finitely generated constant rank projectives over $A$ are free. A classification of quadratic forms is provided over Bezout domains with characteristic other than 2, quadratic stable range 1, and a strong approximation property for a certain subset of their maximum spectrum. These domains include rings of holomorphic functions on connected noncompact Riemann surfaces. Examples of localizations of rings of algebraic integers are provided to show that the classical concept of stable range does not behave well in either direction under finite integral extensions and that $\mathrm{qsr}(A) = 1$ does not descend from such extensions. © 1997 Elsevier Science B.V.

*1991 Math. Subj. Class.:* Primary 15A63; secondary 11E12, 46E25

## 1. Introduction

Let $A$ be a commutative ring with 1. Recall that $A$ has stable range 1 (and we write $\mathrm{sr}(A) = 1$) if whenever $aA + bA = A$, then the polynomial $a + bx$ represents a unit. A polynomial over $A$ (in any number of variables) is called primitive if 1 is in the ideal generated by its coefficients. It is an easy exercise to show that $\mathrm{sr}(A) = 1$ if and only if the product of any 2 primitive linear forms represents a unit.

We consider herein a slightly stronger *quadratic* stable range property: $\mathrm{qsr}(A) = 1$ if every primitive binary quadratic form over $A$ represents a unit. We prove in Theorem 2.3 that $\mathrm{qsr}(A) = 1$ implies that every primitive quadratic form over $A$ represents a

* Corresponding author. E-mail: guralnick@math.usc.edu.

[1] Partially supported by NSF.



*PII* S0022-4049(96)00040-0

unit. The proof of this is somewhat more involved than the analogous result for stable range. We also prove that the condition $\mathrm{qsr}(A) = 1$ forces every constant rank finitely generated projective module to be free (Theorem 2.4). We consider forms over such $A$; particularly for $A$ a Bezout domain (an integral domain for which finitely generated ideals are principal).

In Section 6, we show that this property does not descend under integral extensions. We also show that the stable range property is not preserved in either direction under integral extensions (we give examples of principal ideal domains, $R$ and $S$, with $S$ module finite over $R$ such that either $1 = \mathrm{sr}(R) \neq \mathrm{sr}(S)$ or $1 = \mathrm{sr}(S) \neq \mathrm{sr}(R)$). We also show that certain natural localizations of rings of algebraic integers satisfy these conditions.

Our motivation for studying the quadratic stable range problem was our investigation of quadratic forms over the ring of holomorphic functions on a connected noncompact Riemann surface $\Omega$. These rings have quadratic stable range 1. They do not however satisfy the stronger condition that every primitive quadratic polynomial represents a unit (see [3, Example 5.5]; the polynomial $x(x-z)$ does not represent a unit when $\Omega$ is the complex plane) or that every primitive cubic form represents a unit. In [10], rings for which primitive quadratic polynomials represent units were studied (under the assumption that 2 is invertible). In particular, they consider unimodular quadratic forms and their orthogonal groups.

In fact, we introduce a class of rings which satisfy a very strong approximation property (this class includes principal ideal domains with stable range one, the ring of holomorphic functions on a connected noncompact Riemann surface and the ring of analytic functions on the real line). We investigate quadratic forms over these rings.

In order to avoid introducing unnecessary notation here, we state our main results for rings of holomorphic functions.

Let $\Omega$ be a connected noncompact Riemann surface (i.e. a one dimensional Stein manifold). Let $H = H(\Omega)$ denote the ring of holomorphic functions on $\Omega$. Let $M = M(\Omega)$ denote its quotient field of meromorphic functions. In [6,7], a local-global principle was proved for module finite algebras over $H$; it was shown that two finitely presented modules which are locally isomorphic are isomorphic. In this note, we consider the analogous problem for quadratic modules over $H$. Our main result is:

**Theorem A.** *Let $\Omega$ be a connected noncompact Riemann surface. Let $H$ denote the ring of holomorphic functions on $\Omega$ and $q(x_1,\dots,x_d)$ be a quadratic form over $H$. Then $q$ is equivalent to a form $h = \sum_{i=1}^{r} a_i x_i^2$ with $a_i \neq 0$ for $i \leq r$, and $a_i | a_{i+1}$ for $i < r$. Moreover, the equivalence class of $q$ is uniquely determined by $r$, $a_iH, 1 \leq i \leq r$, and the square class of $a_1 \cdots a_r$ in $M^\times$, where $M$ is the field of meromorphic functions on $\Omega$.*

If $z \in \Omega$, let $H_z$ denote the ring of germs of analytic functions around $z$ (it would cause no harm to use the completion of the local ring at $z$).

**Corollary B.** *Let $q_i, i = 1,2$ be quadratic forms over $H$ in $d$ variables. The following are equivalent*:

(a) *$q_1$ and $q_2$ are equivalent over $H$*;

(b) *$q_1$ and $q_2$ are equivalent over $M$ and $H_z$ for each $z \in \Omega$.*

The previous result asserts that the genus of a quadratic form consists of a single equivalence class.

We can translate this to a result about symmetric matrices over $H$. Recall that two matrices $X$ and $Y$ over a ring are equivalent if $Y = UXV$ for invertible matrices $U$ and $V$. Two square matrices $X$ and $Y$ over a commutative ring are congruent if $Y = UXU^t$ for some invertible matrix $U$ ($U^t$ is the transpose of $U$). Let $S_n(A)$ denote the set of $n \times n$ symmetric matrices over $A$.

**Corollary C.** *Let $X \in S_n(H)$. Then $X$ is congruent to a diagonal matrix*

$$diag(x_1, \dots, x_r, 0, \dots, 0)$$

*where $x_i | x_{i+1}$ and $x_i \neq 0$ for $1 \leq i \leq r$ ($r$ may be 0). The congruence class of $X$ is uniquely determined by its rank, the square class of $x_1 \cdots x_r$ and the ideals $x_i H$.*

**Corollary D.** *Let $X, Y \in S_n(H)$. Then $X$ and $Y$ are congruent if and only if they are equivalent over $H$ and are congruent over $M$.*

**Corollary E.** *Let $X, Y \in S_n(H)$. Then $X$ and $Y$ are congruent if and only if they are congruent over $M$ and equivalent over $H_z$ for each $z \in \Omega$.*

We also compute precisely what values a quadratic form represents. Since $H$ is Bezout, it suffices to consider primitive forms.

If $T$ is any ring, let $T^\times$ denote the group of units of $T$.

**Theorem F.** *Let $q$ be a primitive quadratic form over $H$. Assume $q$ is equivalent to $\sum_{i=1}^r a_i x_i^2$ with $a_i | a_{i+1}$ and $a_r \neq 0$. Let $D(q)$ denote the values represented by $q$.*

(a) *If $r = 1$, then $D(q) = a_1 H^2$.*

(b) *If $r > 1$, then $D(q) \supseteq H^\times$ and*

$$D(q) = \{f \in H : f \equiv g^2 \pmod{a_2 H}\}.$$

*In particular, $D(q)$ is a multiplicatively closed set depending only upon $a_2 H$.*

The proofs depend on some algebraic properties of $H$ (we consider a class of rings which include certain principal ideal domains as well as the ring of holomorphic functions). As we remarked earlier, we prove the following result which may be of independent interest.

**Theorem G.** *Let $A$ be a commutative ring. If every primitive homogeneous polynomial of degree 2 in two variables represents a unit, then every primitive homogeneous polynomial of degree 2 represents a unit.*

The paper is organized as follows. In Section 2, we prove Theorem G and deduce various consequences of the property that every primitive binary quadratic form represent a unit. In particular, we prove that finitely generated projective modules of constant rank are free and that any two invertible skew symmetric matrices of the same size are congruent.

In Section 3, we discuss primitive binary quadratic forms. We prove a result which lets us identify rings having quadratic stable range 1.

In Section 4, we consider a class of Bezout domains having quadratic stable range 1. We prove that quadratic forms over such domains satisfy a local-global principle and under suitable hypotheses find canonical forms for quadratic forms.

In Section 5, we discuss rings of holomorphic functions.

In the final section, we consider certain localizations of rings of algebraic integers and discuss when they have stable range 1 and/or quadratic stable range 1. Examples showing that these properties are not invariant under module finite integral extension are constructed using these rings.

## 2. Primitive quadratic polynomials

Let $A$ denote a commutative ring (with 1). We consider the following quadratic stable range property for $A$:

$\mathrm{qsr}(A) = 1$: Every primitive binary quadratic form over $A$ represents a unit.

**Remarks.** (1) If $A$ is local, then $\mathrm{qsr}(A) = 1$. (see [3] for examples of other such rings which have the stronger property that every primitive polynomial represents a unit.)

(2) $\mathrm{qsr}(A) = 1$ is preserved under direct product and homomorphic images.

(3) One could define $\mathrm{qsr}(A) = d$ for any positive integer $d$ if all primitive quadratic forms in $d + 1$ variables represent units. Theorem 2.3 below shows however that $\mathrm{qsr}(A) = d$ for any positive integer $d$ is equivalent to $\mathrm{qsr}(A) = 1$. This is due in part to our definition allowing degenerate forms; in particular, any form in $d$ variables can be viewed as a (degenerate) form in $d' > d$ variables.

(4) An alternative definition arises by considering only nondegenerate quadratic forms in $d$ variables: $f$ is nondegenerate if the corresponding bilinear form $(x, y) = f(x + y) - f(x) - f(y)$ is nondegenerate; i.e., $(x, y) = 0\, \forall y \in A^d$ implies $x = 0$. Thus, we could say that $\mathrm{qsr}^*(A) = d$ if every nondegenerate primitive quadratic form in $d + 1$ variables represents units. Since our primary interest in this article is the case $\mathrm{qsr}(A) = 1$, we will not pursue the concept $\mathrm{qsr}^*(A) = d$ here except to provide in Section 6 an example that shows $\mathrm{qsr}^*(A) = d > 1$ does not imply $\mathrm{qsr}(A) = 1$.

Recall that a ring $T$ is said to have 1 in the stable range if whenever $T = aT + bT$, then $a + bt$ is a unit in $T$ for some $t \in T$. We write $\mathrm{sr}(T) = 1$ if this holds and refer the reader to [4] for properties of rings with 1 in the stable range.

**Lemma 2.1.** *If $A$ satisfies $\mathrm{qsr}(A) = 1$, then $\mathrm{sr}(A) = 1$.*

**Proof.** Assume $a$ and $b$ are relatively prime. Consider $q(x,y) = x(ax+by)$. Then $q(u,v) \in A^\times$ for some $u,v \in A$. Thus, $u \in A^\times$ and so $a + bvu^{-1} \in A^\times$. $\square$

**Lemma 2.2.** *The property that primitive binary quadratic forms over $A$ in $d$ variables represent units is inherited by homomorphic images of $A$.*

**Proof.** If $d = 1$, there is nothing to prove. So assume $d \geq 2$. Let $T = A/I, I$ a proper ideal of $A$. Suppose $f(x_1,\dots,x_d)$ is a primitive quadratic form over $T$. Let $F$ be any lift of $f$ to a form over $A$. Since the coefficients of $F$ and some element in $i \in I$ constitute a unimodular vector and $A$ has stable range 1 by Lemma 2.1, we can adjust the coefficients by adding multiples of $i$ to assume that $F$ is primitive. Since $F$ then represents a unit, $f$ does as well. $\square$

We now prove Theorem G by induction on the number of variables.

**Theorem 2.3.** *Let $A$ be a commutative ring. If every primitive quadratic form over $A$ in $d$ variables represents a unit for some $d > 1$, then every primitive quadratic form over $A$ represents a unit* ($\mathrm{qsr}(A) = 1$).

**Proof.** We need only prove by induction that each primitive form in $d+1$ variables represents a unit provided that each primitive form in $d$ variables has this property, $d > 1$.

Let $q$ denote a primitive quadratic form over $A$ in the $d+1$ variables $x_1,\dots,x_{d+1}$. We view $q$ as a function on $L = A^{(d+1)}$. Let $e_1,\dots,e_{d+1}$ denote the standard basis for $L$.

Write $q = q_0 + x_{d+1}\ell$, where $q_0$ is a function of $x_1,\dots,x_d$ and $\ell = \sum_{i=1}^{d+1} a_i x_i$. Let $I$ be the ideal of $A$ generated by the $a_i$.

Set $T = A/I$. Then $q_0$ is primitive over $T$. By Lemma 2.2, $q_0(u_1,\dots,u_{d-1}) = a$ is relatively prime to $I$ for some $u_i \in A$. Since $A$ has stable range one, so does $T$ (see [4] or alternatively apply Lemmas 2.1 and 2.2). Therefore $GL_{d-1}(T)$ is transitive on unimodular vectors. So by a linear change of variables in the $x_i, 1 \leq i < d$, we may assume that the coefficient $b$ of $x_1^2$ is relatively prime to $I$. Note that this does not affect $x_d$ and does not change the ideal $I$ (but will change the $a_i$ – which we still denote by $a_i$).

Thus, $A = bA + \sum a_i A$. Since $A$ has stable range 1, there exist $v \in A$ with

$$(b, a_2 + v_1 a_1, a_3, \dots, a_{d+1})$$

unimodular. The change of variables $x_1 \to x_1 + v_1 x_2$ replaces $a_2$ with $a_2 + va_1$ while $b, a_3, \dots, a_{d+1}$ remain unchanged, and we can therefore assume that $b, a_2, \dots, a_{d+1}$ are relatively prime. Now set $x_1 = 0$, obtaining a subform $q'$ in $d$ variables which is primitive modulo $b$. Lemma 2.2 implies that there is a $w$ such that $q(w) = c$ is relatively prime to $b$. Now consider $q''(x,y) = q(xw + yv)$. This is a quadratic form in two variables. Since $q''(1,0) = a$ and $q''(0,1) = b$, it is primitive and so represents a unit. Thus, $q$ does as well. $\square$

It is perhaps worth mentioning a more intuitive approach to the previous result. We sketch the proof under the assumption that $2 \in A^{\times}$. We can then consider the bilinear form on $L = A^{(d)}$ induced by $q$. We write $(v,w)$ for the symmetric inner product corresponding to $q$. Let $I$ be the ideal $(e_d, L)$. By induction, we can assume as above that $q(e_1) = b = (e_1, e_1)$ is prime to $I$. We can find $v \in L$ with $(v, e_d) = a$ relatively prime to $b$. Then $q$ restricted to the span of $v$ and $e_d$ is primitive modulo $bA$ (since some inner product is prime to $A$ – this is where we are using 2 is invertible). Thus, $q(w) = c$ is relatively prime to $b$ for some $w$ in the span of $v$ and $e_d$. Thus, $q$ restricted to the span of $e_1$ and $w$ is primitive and the result follows.

We close this section by deriving various consequences of the property that every primitive binary quadratic form represents a unit.

**Theorem 2.4.** *Let $A$ be a commutative ring. If every primitive binary quadratic form over $A$ represents a unit, then every finitely generated projective $A$-module of constant rank is free. In particular,* $\operatorname{Pic}(A) = 1$.

**Proof.** Assume that every primitive binary quadratic form over $A$ represents a unit. By Theorem 2.3, every primitive quadratic form represents a unit.

Let $X$ be a finitely generated $A$-module of constant rank $r > 0$. We prove the result by induction on $r$. If $r = 0$, there is nothing to prove. Let $Y = \operatorname{Hom}_A(X,A) = X^*$. A local argument shows that the ideal $\{f(x)\colon f \in X^*, x \in X\} = A$ (since locally $X$ is a nonzero free module). Thus, there are $a_i \in X$ and $f_i \in Y$ so that $1 = \sum_{i=1}^{d} f_i(a_i)$. Define

$$q(x_1,\dots,x_d,y_1,\dots,y_d) = \left(\sum y_i f_i\right)\left(\sum x_i a_i\right) = \sum_{i,j} f_i(a_j) x_i y_j.$$

Thus $q$ is a primitive quadratic form in $2d$ variables. Suppose $q(r_1,\dots,s_d) = u$ is a unit in $A$. Set $F = \sum s_i f_i \in Y$. Thus, $F$ is a surjection from $X$ to $A$. Hence $X \cong A \oplus X_1$. By induction, $X_1$ is free and the result follows. □

**Corollary 2.5.** *Let $A$ be a commutative ring and $I$ a proper ideal of $A$. If every primitive binary quadratic form over $A$ represents a unit, then every finitely generated projective $A/I$-module of constant rank is free. In particular,* $\operatorname{Pic}(A/I) = 1$.

**Proof.** The property that every primitive binary form represents a unit is inherited by homomorphic images (Lemma 2.2). Now apply the previous result. □

We note that alternating forms over such rings are quite easy to understand. Indeed, one can get by with a weaker assumption (see [8]).

A symplectic lattice over a commutative ring $A$ is a pair $(L,B)$ where $L$ is a finitely generated projective $A$-module of constant rank and $B$ is an alternating linear form on $L$ (i.e $B(x,x) = 0$). The lattice is said to be primitive if the ideal generated by the values $B(x,y)$ is $A$. Let $J(a)$ denote the rank 2 symplectic lattice with $L$ free with basis $e_1, e_2$ and $(e_1, e_2) = a$.

Suppose that every primitive binary quadratic form over $A$ represents a unit and that $(L,B)$ is a primitive symplectic lattice. Then we can view $B$ as a quadratic form on $L \oplus L$. Thus, $B(u,v)$ is a unit for some $u,v \in L$. By scaling $u$, we may assume that $B(u,v) = 1$. Let $L_1$ denote the submodule spanned by $u$ and $v$. Note that this is free and so is isometric to $J(1)$. Thus, $L \cong J(1) \perp L_2$. If $L$ is unimodular (i.e., the natural map induced by $B$ from $L$ to $L^*$ is an isomorphism), then $L_2$ is also primitive and we can continue. If $A$ is a Bezout domain, then $L_2$ is a scalar multiple of a primitive symplectic lattice. Thus we obtain:

**Corollary 2.6.** *Let $A$ be a commutative ring such that every primitive binary quadratic form represents a unit. Let $(L,B)$ be a symplectic lattice over $A$ of rank $d$. Let $R(L)$ denote the radical of $L$.*

(a) *$L \cong J(1) \perp L_1$ for some lattice $L_1$;*

(b) *If the lattice is unimodular, then $d$ is even and it is isometric to $d/2$ orthogonal copies of $J(1)$;*

(c) *If $A$ is a Bezout domain, then*

$$L \cong J(a_1) \perp \ldots \perp J(a_r) \perp R(L),$$

*with $a_i \neq 0$ and $a_i | a_{i+1}$ for $i < r$. Moreover, the class of the lattice is uniquely determined by $r$, the ideals $a_iA$ and the rank of $L$.*

**Proof.** The uniqueness of the decomposition in (c) follows by considering the elementary divisors for the matrix $(B(u_i,u_j))$, $u_1,\ldots,u_n$ a basis for $L$. Details are left to the reader. □

The previous results can also be stated in terms of congruence classes of skew symmetric matrices.

## 3. Binary quadratic forms

Let $A$ be a commutative ring. A quadratic lattice over $A$ is a pair $(L,q)$ where $L$ is a projective module over $A$ of constant rank and $q$ is a quadratic form on $L$. We say $(L,q)$ has rank $d$ if $L$ has rank $d$.

$(L,q)$ is called primitive if $q(L)$ is contained in no proper ideal of $A$. This agrees with our earlier definition if $L$ is a free module and $q$ is a polynomial.

We say $T$ is a quadratic $A$-algebra if $T$ is a commutative $A$-algebra, is a projective rank 2 $A$ module and $A$ is a summand of $T$ as an $A$-module.

The next result will allow us to identify rings satisfying the condition that every primitive binary quadratic form represents a unit.

**Theorem 3.1.** *Let $A$ be a commutative ring. The following are equivalent:*

(a) *Every primitive quadratic lattice $(L,q)$ of rank 2 over $A$ represents a unit;*

(b) *Every primitive quadratic lattice* $(L,q)$ *over* $A$ *represents a unit*;

(c) *Every binary primitive quadratic form over* $A$ *represents a unit*;

(d) $\mathrm{sr}(A)=1$, $\mathrm{Pic}(A)=1$ *and* $\mathrm{Pic}(T)=1$ *for every quadratic algebra* $T$ *over* $A$; *and*

(e) $\mathrm{Pic}(T)=1$ *for every quadratic algebra* $T$ *over* $A$.

**Proof.** First assume (c) holds. It follows by Section 2 that every constant rank projective $A$-module is free and that every primitive quadratic form represents a unit. Thus, (c) implies (b). Clearly (b) implies (a). Obviously (a) implies (c). So we have shown that the first three conditions are equivalent.

Clearly (d) implies (e).

Now assume (a) holds. Again, by the previous section, we know that $\mathrm{Pic}(A)=1$ and $\mathrm{sr}(A)=1$. Let $T$ be any quadratic algebra over $A$. Let $I\in\mathrm{Pic}(T)$. Then, $I$ is a free rank 2 $A$-module. For each $a\in I$, we obtain a map $L(a)$ from $I$ to $I\otimes_T I$ by multiplication by $a$ (i.e., $L(a)(b)=a\otimes b$). Let $D(a)$ denote the determinant of $L(a)$ (this makes sense since $I\otimes_T I$ is also a free rank 2 $A$-module). Then $(I,D)$ is a primitive quadratic lattice of rank 2 on $A$ (the primitivity follows since $I$ is locally free as a $T$-module). Thus, $D(a)$ is unit for some $a\in I$. It follows easily that $I=aT$ (use a local argument). Thus (a) implies (d).

The only remaining step is to show that (e) implies (c). Each primitive binary quadratic form $f$ over $A$ determines a quadratic lattice $L=L(f)=(A\oplus A,F)$ where $F(xe_1+ye_2)=f(x,y), e_1,e_2$ a basis for $L$. The Clifford algebra $C(L)$ for $L$ over $A$ has basis $1,e_1,e_2,e_1e_2$ where $e_i^2=-F(e_1), e_1e_2=-e_2e_1+(e_1,e_2)$ where $(e_1,e_2)=F(e_1+e_2)-F(e_1)-F(e_2)$. Now $L$ is a $T=C^+(L)=A+e_1e_2A$ module. Note that if $v\in L, F(v)\in A^\times$ then $L=vT$ since $T=v^{-1}(vT)\subset vL\subset T$. A local argument now shows that $L\in\mathrm{Pic}(T)$. Thus $L=vT$ for some $v\in L$. Since $L$ is primitive, it follows that $F(v)\in A^\times$ completing the proof. $\square$

One may ask whether $\mathrm{qsr}(A)=1$ is invariant under integral extensions (or perhaps more reasonably under quadratic integral extensions). The next result gives some evidence for believing this.

**Corollary 3.2.** *Let* $A$ *be a commutative ring with* $\mathrm{qsr}(A)=1$. *Let* $T$ *be any quadratic algebra over* $A$. *Then* $\mathrm{sr}(T)=1$ *and* $\mathrm{Pic}(T)=1$.

**Proof.** The fact that $\mathrm{Pic}(T)=1$ follows from Theorem 3.1. By definition, $T=A\oplus A\theta$ for some $\theta\in T$. Let $b\in T$ and consider the $A$-subalgebra $S=A\oplus Ab\theta$. Note that $bT\subseteq S\subseteq T$. By the Mayer–Vietoris sequence (cf. [2]), we have the following exact sequence:

$$(S/bT)^\times\times T^\times\to(T/bT)^\times\to\mathrm{Pic}(S).$$

Since $\mathrm{Pic}(S)=1$, it follows that the first map is surjective. Since $S/bT=A/bA$, the image of $(S/bT)^\times$ is the image of $A^\times\subseteq T^\times$. Thus, the natural map from $T^\times$ to $(T/bT)^\times$ is surjective. $\square$

In certain cases, the condition about all quadratic algebras can be relaxed to considering Picard groups of maximal orders.

**Corollary 3.3.** *Let $A$ be an integrally closed integral domain with quotient field $K$ and* $\mathrm{sr}(A) = 1, \mathrm{Pic}(A) = 1$. *Assume that for any quadratic extension of $K$, the integral closure $T$ of $A$ is a quadratic algebra over $A$ and satisfies* $\mathrm{Pic}(T) = 1$ *and* $\mathrm{sr}(T) = 1$. *If* $\mathrm{Pic}(A/bA) = 1$ *for every element $b \in A$, then every primitive quadratic form over $A$ represents a unit.*

**Proof.** Let $S$ be any quadratic $A$-algebra. By Theorem 3.1, it suffices to show that $\mathrm{Pic}(S) = 1$. Set $Q = S \otimes_A K$. Then $Q$ is a 2-dimensional $K$-algebra. If the nilradical $N$ of $Q$ is nonzero, then $Q/N = K$ and so $S/(S \cap N) \cong A$ has trivial Picard group, whence $S$ does.

So we may assume that $Q$ is semisimple. Let $T$ be the integral closure of $A$ in $Q$. Since $T$ is a quadratic algebra and $\mathrm{Pic}(A) = 1$, $T = A \oplus A\theta$ for some $\theta \in T$. Thus $S = A \oplus Ab\theta$ for some $b \in A$. The Mayer–Vietoris sequence gives:

$$(S/bT)^{\times} \times T^{\times} \to (T/bT)^{\times} \to \mathrm{Pic}(S) \to \mathrm{Pic}(T) \times \mathrm{Pic}(S/bT).$$

Using the facts that $\mathrm{sr}(T) = 1$, $\mathrm{Pic}(T) = 1$ and that $\mathrm{Pic}(S/bT) = \mathrm{Pic}(A/bA) = 1$, we see that $\mathrm{Pic}(S) = 1$. The result follows by Theorem 3.1. □

We close this section with the following trivial observation:

**Proposition 3.4.** *Let $A$ be a commutative ring with* $\mathrm{qsr}(A) = 1$. *Assume* $2 \in A^{\times}$.

(a) *Any unimodular quadratic form is diagonalizable.*

(b) *If $A$ is a Bezout domain, then every quadratic form is equivalent to one of the form $\sum_{i=1}^{r} a_i x_i^2$ where $a_i A \supseteq a_{i+1} A$ for $i = 1, \ldots, r-1$.*

**Proof.** Induct on the number of variables. □

## 4. Very strong approximation and quadratic forms

We will assume throughout this section that the fields/domains considered have characteristic other than 2 (some of the initial results are however valid in characteristic 2).

Let $k$ be a field. A *spot* $\omega$ on $k$ is an equivalence class of a valuation on $k$ (our valuations are assumed to be nontrivial and to have rank 1; i.e., map into the nonnegative real numbers). A *finite spot* contains a non-archimedean valuation. The finite spot is discrete if it contains a discrete valuation and is then called a *p-adic spot*. Let $| \ |_\omega$ denote a valuation in the spot $\omega$ on $k$. A subset $X$ of a set $\Omega$ of finite spots on $k$ is called a principal closed set if $\exists x \in k^{\times}$ such that $X = \{\omega \in \Omega \,|\, |x|_\omega \neq 1\} := V(x)$. $\Omega$ satisfies *strong approximation* if each principal closed subset $X$ has the property that for given values $x_\omega \in k$ and positive real numbers $\varepsilon_\omega$, $\omega \in X$, $\exists x \in k$ such that

(i) $|x - x_\omega|_\omega \le \varepsilon_\omega \, \forall\, \omega \in X$ and

(ii) $|x|_\omega \le 1 \, \forall\, \omega \in \Omega - X$.

$\Omega$ satisfies *very strong approximation* (VSA) if (ii) is replaced by

(ii)′ $|x|_\omega = 1 \, \forall\, \omega \in \Omega - X$.

It is well known that the $p$-adic spots $\Omega(A)$ defined on the quotient field of a Dedekind domain $A$ by the maximal ideals of $A$ satisfy strong approximation. It is not difficult to see that if $A$ is Dedekind then $\Omega(A)$ satisfies (VSA) if and only if $A$ is a principal ideal domain and $\mathrm{sr}(A) = 1$ (see below). Another example is given by taking a finite set $\Omega$ of finite spots on $k$. Here, (VSA) is just weak approximation which holds for any finite number of valuations.

Now let $\Omega$ be a set of finite spots on the field $k$. For $\omega \in \Omega$, let $A_\omega = \{x \in k \mid |x|_\omega \le 1\}$ and $m_\omega = \{x \in k \mid |x|_\omega < 1\}$ denote the valuation ring and maximal ideal corresponding to $\omega$. Since $\omega$ has rank 1, $m_\omega$ is the unique nonzero prime ideal of $A_\omega$. A spot $\omega$ divides $x \in k$ if $|x|_\omega < 1$; i.e., $x \in m_\omega$. $A = A(\Omega) := \bigcap_{\omega\in\Omega} A_\omega$ is the ring associated to $\Omega$ and $M_\omega := m_\omega \cap A$. Note that $A$ induces a Zariski topology on $\Omega$: $X \subset \Omega$ is closed if $\exists I \subset A$ such that $X = V(I) := \{\omega \in \Omega \mid I \subset m_\omega\}$. Note also that if $\Omega$ satisfies (VSA) then points are closed in this topology. For if $x \in m_\omega$ is nonzero then we can select $y \in k$ sufficiently approximating $x$ at $\omega$, 1 at $\lambda \in V(x) - \{\omega\}$ and $|y|_\lambda = 1$ elsewhere in $\Omega$. Then $y \in A$ and $\{\omega\} = V(y)$. If $\omega$ is discrete then $x$ can be selected to generate $m_\omega$, and it follows that $M_\omega$ is principal generated by $y$. More generally:

**Proposition 4.0.** *If a set $\Omega$ of finite spots on $k$ satisfies* (VSA) *and $X \subsetneq \Omega$ then the following are equivalent*:

(1) *$X$ is closed,*

(2) *$X$ is discrete,*

(3) *$X$ is a principal closed set.*

**Proof.** For $x \in k^\times, V(x) = S \cup T$, $S = \{\omega \in \Omega \mid |x|_\omega < 1\}, T = \{\omega \in \Omega \mid |x|_\omega > 1$. Select $y \in k$ such that $|y - x|_\omega < 1$, $\omega \in S$, $|y - x^{-1}|_\omega < 1$, $\omega \in T$ and $|y|_\omega = 1, \omega \in \Omega - (S \cup T)$. Thus, $y \in A$ and $V(y) = V(x)$. Therefore, (3) implies (1).

Now let $X = V(I) \neq \Omega, I \subset A$. Pick $i (\neq 0) \in I$ and select $j \in k$ such that $|i - j|_\omega < 1, \omega \in X, |i - 1|_\omega = 1, \omega \in V(i) - X$, and $|i|_\omega = 1, \omega \in \Omega - V(i)$. Hence, $j \in A$ and $V(j) = X$ so (1) implies (3).

Let $X$ be a discrete set. Since points are closed, we can assume for the purposes of (2) implies (1) that $|X| > 1$. Then $\forall \omega \in X$, $\exists a_\omega \in A$ such that $\omega \notin V(a_\omega)$ but $(X - \{\omega\}) \subset V(a_\omega)$. Pick $b_\omega \in k$ so that $|b_\lambda - a_\lambda|_\lambda < 1, \lambda \in V(a_\omega) \cap X$, $|b_\lambda - 1|_\lambda = 1, \lambda \in V(a) - X$ and $|b_\omega|_\lambda = 1, \lambda \in \Omega - V(a_\omega)$. Thus, $X - \{\omega\} = V(b_\omega)$. It follows that $X$ is the union of two closed sets, hence (2) implies (1).

It remains to show that (3) implies (2). Here, we just select $y \in k$ so that $y$ sufficiently approximates 1 at a fixed $\omega \in V(a)$, 0 elsewhere in $V(a)$, and $|y|_\lambda = 1$ off $V(a)$. Then $\Omega - V(y)$ is an open set containing $\omega$ but no other element in $V(a)$. $\square$

The assumption $X \neq \Omega$ in the above proposition is only used in the implication (1) implies (3). Indeed, $\Omega$ is discrete if and only if $\bigcap_{\omega\in\Omega} M_\omega \neq \{0\}$.

**Proposition 4.1.** *If $\Omega$ is a set of finite spots on $k$ and satisfies* (VSA), *$A = A(\Omega) := \bigcap_{\omega\in\Omega} A_\omega$, and $M_\omega = A \cap m_\omega$, then*

*(1) $k$ is the field of quotients of $A$,*

*(2) $A$ is a Bezout domain and* $\mathrm{sr}(A) = 1$,

*(3) $M_\omega$ is maximal and $A_{M_\omega} = A_\omega$,*

*(4) for $a(\neq 0) \in A, A/aA \cong \prod_{\omega\in\Omega} A_\omega/aA_\omega$,*

*(5) if $X \subset \Omega$ is a principal closed set and $\{e_\omega\}_{\omega\in X}$ a set of positive integers, then $\bigcap_{\omega\in X} m_\omega^{e_\omega} \neq \{0\}$, and*

*(6) $\Omega$ is the set of all finite spots on $k$ centered on maximal ideals of $A$ which are radicals of nonzero principal ideals.*

**Proof.** For (1), let $t \in k^\times$ and select $x \in k$ so that $|x - t^{-1}|_\omega < |t^{-1}|_\omega \forall\, \omega$ such that $|t|_\omega > 1$, $|x - t|_\omega < 1 \,\forall\, \omega$ such that $|t|_\omega < 1$ and $|x|_\omega = 1$ elsewhere. Thus, $x \in A - \{0\}$ and $xt \in A$. Consequently, $A$ has $k$ as its field of quotients.

For (2), it suffices to show that if $a,b \in A$ then $(a + bx)A = aA + bA$ for some $x \in A$. We can assume that $a,b$ are neither zero nor units. For each $\omega | ab \,\exists\, d_\omega \in A_\omega$ such that $aA_\omega + bA_\omega = d_\omega A_\omega$. If we select $d \in A$ such that $|d - d_\omega|_\omega < |d_\omega|_\omega$ for $w|ab$ and $|d| = 1$ elsewhere then $dA = aA + bA$. We can now assume that $a,b$ are relatively prime. Since $\mathrm{sr}(A_\omega) = 1$, $a \equiv u_\omega \bmod bA_\omega, u_\omega \in A_\omega^\times, \forall\, \omega | b$. Now use (VSA) to select a unit $u \in A^\times$ so that $|u - u_\omega| < |b|_\omega \forall\, \omega | b$. Then $a \equiv u \bmod bA$; i.e., $(a,b)$ is a stable pair.

For (3), if $t \in A - M_\omega$ then since $\{\omega\}$ is a principal closed set, we can select $x \in A$ such that $|x - t^{-1}|_\omega < 1$ and $|x|_\gamma = 1 \,\forall\, \gamma \in \Omega - \{\omega\}$. Then $x \in A$ and it follows that $xt \equiv 1 \bmod M_\omega$. Thus, $M_\omega$ is maximal.

Clearly, $A_{M_\omega} \subset A_\omega$. For the reverse implication, let $a/b \in A_\omega$. Since $A$ is Bezout, we can assume that $a,b$ are relatively prime. It follows therefore that $b$ is a unit in $A_\omega$ hence $b \notin M_\omega$.

For (4), there is a homomorphism $\pi : A \to \prod_{\omega\in\Omega} A_\omega/aA_\omega$ given by restricting the product of the projections $A_\omega \to A_\omega/aA_\omega$ to $A$. Since $|\,|_\omega$ is nonarchimedian, if $r,s \in A_\omega$ are sufficiently close then $rA_\omega = sA_\omega$. Thus, (VSA) implies that $\pi$ is onto. Clearly, $aA \subset \ker\pi$. If $g \in \ker\pi$ then $g/a \in A_\omega \forall\, \omega \in \Omega$. Therefore, $g/a \in A$.

Note that (5) follows easily by approximating a nonzero $a_\omega \in m_\omega^{e_\omega}, \omega \in X$.

For (6), assume that $R$ is a valuation ring in $k$ with maximal ideal $m$. Assume also that $m \cap A = M$ is a maximal ideal and $M = \sqrt{aA}$. The isomorphism (4) implies that $aA_\omega \neq A_\omega$ for some $\omega \in \Omega$. Thus $a \in m_\omega \cap A = M_\omega$ and $M = M_\omega$ follows. Since $A_\omega = A_M \subset R$ and $m$ contracts to $MA_M = m_\omega, R = A_\omega$. The converse was proved prior to Proposition 4.0 in verifying the observation that points in $\Omega$ are closed. $\square$

There is also a converse to Proposition 4.1. Let $\Omega(A)$ denote the set of finite spots $\omega$ of $k$ such that $A \subset A_\omega$. Note that since $A_\omega \subset k$, the field of quotients of $A$, $M_\omega =$

$A \cap m_\omega$ is a nonzero prime ideal in $A$. In the event $A$ is a Bezout domain, $A_\omega$ is the valuation ring $A_{M_\omega}$. Let $\Omega_p(A)$ denote the subset of $\Omega(A)$ of those spots centered on maximal ideals of $A$ which are radicals of principal ideals; i.e., for $A$ Bezout, $A_{M_\omega}$ is a rank 1 valuation ring (equivalently, $M_\omega$ has height 1), $M_\omega$ is maximal, and $M_\omega = \sqrt{aA}$.

**Proposition 4.2.** *Let $\Omega \subseteq \Omega(A)$. If the Bezout domain $A$ satisfies $\pi : A/aA \to \prod_{\omega\in\Omega} A_\omega/aA_\omega$ is an isomorphism $\forall a(\neq 0) \in A$, $\mathrm{sr}(A) = 1$, and $\bigcap_{\omega\in X} m_\omega^{e_\omega} \neq \{0\}$ for any principal closed $X \subset \Omega$ and any set $\{e_\omega\}_{\omega\in X}$ of positive integers, then $\Omega$ satisfies* (VSA), *$A = A(\Omega)$ and $\Omega = \Omega_p(A)$.*

**Proof.** Let $X$ be a principal closed subset of $\Omega$, $\{a_\omega\}_{\omega\in X} \subset k$, the field of quotients of $A$, and let $\{\varepsilon_\omega\}_{\omega\in X}$ be a set of positive real numbers. We can assume the $a_\omega \in A_\omega$ as follows. The last hypothesis of the proposition implies the existence of $p(\neq 0) \in A$ such that $pa_\omega \in A_\omega \,\forall\, \omega \in X$. If we select $b \in k$ so that $|b - pa_\omega|_\omega < |p|_\omega \varepsilon_\omega, \omega \in X, |b - p|_\omega < |p|_\omega, \omega \in V(p) - X$, and $|b|_\omega = 1$ otherwise in $\Omega$ then $b/p$ is the desired approximation of the $a_\omega$. Assume now that $a_\omega \in A_\omega$. The hypothesis implies that we can select $y \in A$ so that $|y|_\omega < \min\{\varepsilon_\omega, 1\} \,\forall\, \omega \in X$. We can assume that $X = V(y)$ by setting $a_\gamma = 1 = \varepsilon_\gamma$ at any $\gamma \in \Omega$ dividing $y$ but not in $X$. Now using that $\pi$ is onto, we find $a \in A$ such that $a \equiv a_\omega \bmod yA_\omega \,\forall\, \omega \in X$; or equivalently, $|a - a_\omega|_\omega \leq |y|_\omega < \varepsilon_\omega$. Moreover, we can replace $a$ with $a + ty$ for any $t \in A$ and since $\mathrm{sr}(A) = 1$ and $A$ is Bezout, $t$ can be selected so that $a + ty$ generates $aA + yA$. Since $a + ty$ is a unit at any spot in $\Omega - X, a' = a + ty$ is the desired approximation.

Given $x \in \bigcap_{\omega\in\Omega} A_\omega$, set $x = a/b$ with $a, b \in A$ relatively prime. Then $bA_\omega = A_\omega \,\forall\, \omega \in \Omega$. Since $\pi$ is an isomorphism, it follows that $bA = A$. Thus, $x \in A$ and $A = \bigcap_{\omega\in\Omega} A_\omega$ follows. The final conclusion is a consequence of Proposition 4.1(6). □

A Bezout domain $A$ which satisfies the hypothesis of the proposition with respect to a set $\Omega \subset \Omega(A)$ will be termed a Bezout domain satisfying (VSA). Necessarily, $\Omega = \Omega_p(A)$. The Bezout domains of special interest in this article satisfy Proposition 4.2 with respect to a set of $p$-adic spots. In this event, $\Omega_p(A)$ contains only the discrete spots: those defined by the valuation rings $A_M$ where $M$ is a height 1 principal maximal ideal in $A$.

We now show how to determine whether a Bezout domain satisfying (VSA) with respect to a discrete set of spots also has quadratic stable range 1.

**Proposition 4.3.** *Let $A$ be a Bezout domain satisfying* (VSA) *with respect to a set of* $p$-adic *spots. Let $k$ be the quotient field of $A$. If for each quadratic field extension* $K/k$, $\mathrm{Pic}(B) = 1$ *and* $\mathrm{sr}(B) = 1$ *for $B$ the integral closure of $A$ in $K$, then* $\mathrm{qsr}(A) = 1$.

**Proof.** Since $A$ satisfies (VSA), $\mathrm{Pic}(A/I) = 1$ for every nonzero principal ideal $I$ of $A$ (since it is the direct product of local Artinian principal ideal rings and therefore has quadratic stable range 1). We apply Corollary 3.3. We only need to show that the integral closure $T$ of $A$ in a quadratic field extension $K$ of $k$ is a free $A$-module. Choose $\theta \in T$ such that $K = k[\theta]$. Since $K/k$ is separable, $S := A[\theta] \supseteq bT$ for some nonzero $b \in A$ (e.g., $b = \mathrm{dis}(\theta)$). Since $A_\omega$ is a principal ideal domain for $\omega \in \Omega$, $T_\omega$ has a $A_\omega$ basis $1, c_\omega + d_\omega\theta$. We can choose approximations $c, d \in k$ with $d$ a unit outside $V(b)$ such that $T_\omega = A_\omega + A_\omega(c + d\theta)$. Since $1, c + d\theta$ is a $k$ basis for $K$ and $A = \bigcap A_\omega$, $T = A + (c + d\theta)A$. $\square$

We denote by $(V, q)$ an $n$-dimensional nonsingular quadratic $k$-space with corresponding bilinear form $2(u, v) = q(u + v) - q(u) - q(v)$, $k$ the field of quotients of $A$. $\| \|_\omega$ will denote an extension of $| |_\omega$ to $V$, $\omega \in \Omega_1(A)$. The orthogonal group of $(V, q)$ is denoted by $O(V)$ and the special orthogonal group by $O^+(V) = O(V) \cap SL_n(k)$. The elements in $O^+(V)$ are called rotations. The map $\tau_u(x) = x - \frac{2(x,u)}{(u,u)}u$ defines an element in $O(V)$ called a symmetry.

Let $L$ denote a quadratic $A$-lattice having rank $n$; i.e., $L$ is projective, finitely generated $A$-submodule of a nonsingular quadratic space $V$ over $k$ and $Lk$ is $n$-dimensional over $k$. $N(L)$ is the fractional $A$ ideal generated by $\{q(v) | v \in L\}$. $L$ is primitive if $N(L) = A$. $O(L) = \{\sigma \in O(V) | \sigma(L) = L\}, O^+(L) = O(L) \cap O^+(V)$.

If $L$ is a free $n$-dimensional $A$-submodule of $V$ with $v_1, \ldots, v_n$ a basis then $q(x_1v_1 + \ldots + x_nv_n) = ag(x_1, \ldots, x_n)$ where $aA = N(L)$ and $g(x_1, \ldots, x_n)$ is a primitive quadratic form over $A$. The form $ag$ will be called a quadratic form associated to $L$. Conversely, given a quadratic form $f = f(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij}x_ix_j$, $V(f) = k^n = \bigoplus_1^n k$, and $e_1, \ldots, e_n$ a basis for $k^n$, we view $V(f)$ as a quadratic space with quadratic norm $q_f(\sum x_ie_i) = f(x_1, \ldots, x_n)$ and bilinear form defined by $(e_i, e_i) = a_{ii}, (e_i, e_j) = \frac{1}{2}a_{ij}$. Let $L(f) = Ae_1 + \cdots + Ae_n$. Evidently, $f, g$ are equivalent if and only if there is an isometry $\sigma : V(f) \to V(g)$ such that $\sigma(L(f)) = L(g)$.

Thus, if finitely generated projective lattices over $A$ are free then the concept of quadratic forms and quadratic lattices are interchangeable. We will use the more convenient of the two in what follows.

For quadratic forms $f, g$ over $A$ and a set $\Omega \subset \Omega(A)$, we say that $f$ and $g$ are in the same $\Omega$-genus if $f$ and $g$ are equivalent over $k$ and over $A_\omega \forall \omega \in \Omega$. The transition to lattices is obtained as follows: since $f, g$ are equivalent over $k$, $V(f)$ and $V(g)$ are isometric. By replacing $L(f)$ by its image in $V(g)$ under this isometry, we can assume that $L(f), L(g)$ are lattices on the same space $W = L(g)$ and the question of whether $f, g$ are equivalent reduces to whether there is an isometry $\sigma \in O(W)$ such that $\sigma(L(f)) = L(g)$. Thus, for an $A$-lattice $L$ we set $V(L) = Lk$, $Cls(L) = \{\sigma(L) | \sigma \in O(V(L))\}$ and the $\Omega$-genus, $\mathrm{gen}_\Omega(L)$, is the set of all $A$-lattices $K$ in $V(L)$ such that $\forall \omega \in \Omega$, $\exists \sigma_\omega \in O(V(L))$ for which $\sigma_\omega(L_\omega) = K_\omega$ where $LA_\omega = L_\omega$. Let $k_\omega$ denote the completion of $k$ with respect to a p-adic spot $\omega$ and $\hat{A}_\omega$ (resp. $\hat{L}_\omega$) the closure of $A$ (resp. $L$) in $k_\omega$ ($V_\omega = V \otimes_k K_\omega$). The weak approximation theorem for rotations (see e.g., [11, Theorem 101.7]) and Nakayama's lemma imply that $L_\omega \cong K_\omega \Leftrightarrow \hat{L}_\omega \cong \hat{K}_\omega$.

**Proposition 4.4.** *If $A$ is a Bezout domain and* $\mathrm{qsr}(A) = 1$, *then $O(L)$ contains a symmetry for any quadratic $A$-lattice $L$ of finite rank.*

**Proof.** Let $ag(x_1,\dots,x_n)$ be a quadratic form associated to $L$, $aA = N(L)$. Since $g$ is primitive, $g$ represents a unit, hence $\exists v \in L$ such that $q(v)$ generates $N(L)$. Consequently, $\tau_v \in O(L)$. □

The proposition implies that the class of $L$ (defined as the orbit under $O(V)$) coincides with the proper class of $L$ (the orbit under $O^+(V)$).

**Lemma 4.5.** *Let $A$ be a Bezout domain satisfying* $\mathrm{qsr}(A) = 1$ *and* (VSA), *and let $L$ denote a rank $n$ primitive quadratic $A$-lattice. If $X$ is a discrete subset of $\Omega = \Omega_p(A)$, $\{v_\omega\}_{\omega\in X}$ a subset of $L$, and $\{\varepsilon_\omega\}_{\omega\in X}$ a set of positive real numbers then $\exists v \in L$ such that $\|v - v_\omega\|_\omega < \varepsilon_\omega \,\forall\, \omega \in X$ and $|q(v)|_\omega = 1 \;\forall\, \omega \in \Omega - X$.*

**Proof.** Here $\|\ \|$ denotes any extension of $|\ |_\omega$ to $V(L)$. Fix a basis $B$ for $L$. As previously, we can pick $a \neq 0 \in A$ such that $|a|_\omega < \varepsilon_\omega \max\{\|v\|, v \in B\} \,\forall\, \omega \in X$ and $|a|_\omega = 1 \,\forall\, \omega \in \Omega - X$. Now apply very strong approximation to the coefficients of the $v_\omega$ with respect to a fixed basis for $L$, to select $v \in L$ such that $v \equiv v_\omega \bmod aL_\omega \,\forall\, \omega \in X$. We can assume that $A$ is not a field and therefore that $k$ is not finite. Hence we can replace $v$ with $v+az$ for some $z \in L$ so that $q(v) \neq 0$. Use very strong approximation to select $b \neq 0 \in A$ such that $|b|_\omega < \min\{|q(v)|_\omega, |a|_\omega\} \,\forall\, \omega \in X$ and $|b|_\omega = 1, \omega \in \Omega - X$. Now consider the lattice $K = Av + bL$. The Bezout and $\mathrm{qsr}(A) = 1$ assumptions imply that $\exists u \in K$ such that $q(u)A = N(K)$. Set $u = tv + bz$, $t \in A$, $z \in L$. Note that $q(u) = t^2q(v) + 2bt(v,z) + b^2q(z)$ and $|q(v)|_\omega \leq |q(u)|_\omega$. Therefore the principle of domination implies that $|t|_\omega = 1 \;\forall\, \omega \in X$. Hence $t, b$ are relatively prime (a generator for $tA + bA$ is not in any $M_\omega$ and is therefore a unit by Proposition 4.1(4)). Since $\mathrm{sr}(A) = 1$, we can replace $t$ with $t + bd$, $z$ with $z - dv$ and assume $t$ is a unit and therefore assume $t = 1$. Since $N(K) \supset b^2A$, it follows that $|q(u)|_\omega = 1 \,\forall\; \omega \in \Omega - X$. □

**Theorem 4.6** (Very strong approximation of rotations). *Let $A$ be a Bezout domain which satisfies* $\mathrm{qsr}(A) = 1$ *and* (VSA), *and let $L$ denote a rank $n$ primitive quadratic $A$-lattice. If $X$ is a discrete subset of $\Omega = \Omega_p(A)$, $\{\sigma_\omega\}_{\omega\in X}$ a subset of $O^+(V)$, and $\{\varepsilon_\omega\}_{\omega\in X}$ a set of positive real numbers then $\exists \sigma \in O^+(V)$ such that $\|\sigma - \sigma_\omega\|_\omega < \varepsilon_\omega \,\forall\, \omega \in X$ and $\sigma \in O^+(LA_\omega) \,\forall\, \omega \in \Omega - X$.*

**Proof.** The argument is essentially the same as the standard proof of the weak approximation theorem for rotations (see e.g., [11, Theorem 101.7]); express the rotations as a product of symmetries and use the approximation result in the previous lemma to approximate the vectors defining the symmetries. We leave the details to the reader. □

**Corollary 4.7.** *If a Bezout domain $A$ satisfies* (VSA) *and* $\mathrm{qsr}(A) = 1$, *then the class and $\Omega_p(A)$-genus of any quadratic form over $A$ coincide.*

**Proof.** The above discussion reduces the proof to that of showing that if $L, K$ are two quadratic $A$-lattices in a quadratic $k$-space $V = Lk = Kk$ and if at each spot $\omega \in \Omega = \Omega_p(A)$ there is an isometry $\sigma_\omega \in O(V)$ such that $\sigma(L_\omega) = K_\omega$, then there is an isometry $\sigma \in O(V)$ such that $\sigma(L) = K$. Since $L, K$ are finitely generated and $Lk = Kk = V$, $\exists a (\neq 0) \in A$ such that $aL \subset K, aK \subset L$. Thus, $L_\omega = K_\omega \forall \omega \notin V(a)$. Let $\{\sigma_\omega\}_{\omega \in V(a)} \subset O(V)$ satisfy $\sigma_\omega(L_\omega) = K_\omega$. Since $O(L)$ contains a symmetry from the proposition above, we can assume that the $\sigma_\omega$ are rotations. Now apply the very strong approximation theorem for rotations with the $\varepsilon_\omega$ sufficiently small to insure that the approximating rotation $\sigma$ satisfies $\sigma(L_\omega) = \sigma_\omega(L_\omega) \forall \omega \in V(a)$ (existence of such $\varepsilon$ follows from Nakayama's lemma). Thus, $\sigma(L_\omega) = K_\omega \forall \omega \in \Omega$ and $\sigma(L) = K$ follows by looking at the coefficients of $A$-bases for $L, K$. □

**Theorem 4.8.** *Let $A$ be a Bezout domain that satisfies* (VSA) *and let $X$ be a discrete subset of $\Omega = \Omega_p(A)$. Let $V$ be a finite dimensional quadratic space over $k$, the field of quotients of $A$, and let $L(\omega), \omega \in \Omega$, be $A_\omega$-lattices in $V$ such that $L(\omega)k = V$ and $M_\omega = L(\omega)$, $\forall \omega \notin X$, for some fixed $A$-lattice $M$ in $V$. Then there exists an $A$-lattice $L$ in $V$ such that $L_\omega = L(\omega) \forall \omega \in \Omega$.*

**Proof.** Let $v_1, \ldots, v_n$ denote an $A$ basis for $M$. Since $A$ is Bezout, $L(\omega)$ has basis $d_{1\omega}v_1, \ldots, d_{n\omega}v_n$ for some $d_{i\omega} \in k$. If we now choose $d_i$ sufficiently approximating the $d_{i\omega}$ on $X$ and units off $X$ then $L = \sum d_i v_i A$ is the desired lattice. □

**Corollary 4.9.** *Let $A$ be a Bezout domain that satisfies* (VSA) *and* $\operatorname{qsr}(A) = 1$ *and assume that $f, g$ are quadratic forms over $A$. If the $\Omega_p(A)$-genus of $f$ represents $g$, then $f$ represents $g$.*

**Proof.** We can assume that $L(g) \subset L(f)k = V(f) = V$ and that $\forall \omega \in \Omega_p(A) \exists \sigma_\omega \in O^+(V)$ such that $\sigma_\omega(L(f)_\omega) \supset L(g)_\omega$. Also, $\exists a (\neq 0)$ such that $aL(g) \subset L(f)$. Let $L$ be the $A$-lattice on $V$ such that $L_\omega = L(f)_\omega \forall \omega$ not dividing $a$ and $L_\omega = \sigma_\omega(L(f)_\omega) \forall \omega \in V(a)$. Thus, $L$ is in the $\Omega_p(A)$-genus of $L(f)$ and $L \supset L(g)$. The result now follows from the previous corollary. □

**Corollary 4.10.** *Let $A$ be a Bezout domain that satisfies* (VSA) *and* $\operatorname{qsr}(A) = 1$. *If $f \perp g \cong f \perp h$, then $g \cong h$.*

**Proof.** Cancellation holds locally (cf. [1, Corollary 4.3]) and thus globally by the theorem. □

If $f$ is a quadratic form over $A$, $F = \frac{1}{2}(\partial^2 f/\partial x_i \partial x_j)$ is the matrix of $f$ and $\det(F)(A^\times)^2 := \det(f)$ is the determinant of $F$. We assume for convenience that the forms in the remainder of this section have nonzero determinant. Our goal is to classify forms over those rings which satisfy $\operatorname{qsr}(A) = 1$ and (VSA). The classification of quadratic forms over complete discrete rank 1 valuation rings having residue class fields of characteristic 2 is quite a difficult problem (see e.g., [11]), and we will avoid this difficulty in this article by confining our attention to domains in which 2 is invertible.

**Lemma 4.11.** *If $A$ is a Bezout domain that satisfies* (VSA) *with respect to a set of p-adic spots,* $\operatorname{qsr}(A) = 1$, *and* $2 \in A^\times$ *and $f$ is a unimodular quadratic form over $A$, then $f$ represents over $A$ exactly those values represented by $f$ over $k$, the field of quotients of $A$.*

**Proof.** Let $f(x_1/d, \dots, x_n/d) = a$, $x_i, d \in A$, $a \in A - \{0\}$. Then $f(x_1, \dots, x_n) = ad^2$ and we can assume that $x_1, \dots, x_n, d$ are relatively prime. We can also assume that $x_1, \dots, x_n$ are relatively prime by removing a square factor of $a$. By previous results, we need only show that $a$ is represented over $A_\omega$ for each $\omega \in \Omega_p(A)$. Again by weak approximation, we can work instead over $\hat{A}_\omega$ the completion of $A_\omega$. If $|d|_\omega = 1$, then there is nothing to prove. If $\omega | d$ then one of $x_i, 1 \leq i \leq r$, is a unit in $\hat{A}_\omega$. It now follows by Hensel's lemma that $f$ has a nontrivial representation of zero and since $f$ is unimodular, it follows that $f$ is split by a hyperbolic plane $xy$. In this event, $f$ is universal. □

**Theorem 4.12.** *If $A$ is a Bezout domain that that satisfies* (VSA) *with respect to a set of p-adic spots,* $\operatorname{qsr}(A) = 1$, *and* $2 \in A^\times$ *then two unimodular quadratic forms $f, g$ over $A$ are equivalent over $A$ if and only if they are equivalent over $k$, the field of quotients of $A$.*

**Proof.** The proof is by induction on the number of variables. Now $\operatorname{qsr}(A) = 1$ implies that $f$ represents a unit $u$ and the previous lemma implies that $g$ also represents $u$. Now $f, g$ are equivalent to $ux^2 \perp f_1, ux^2 \perp g_1$, respectively. By Witt's theorem, $f_1, g_1$ are equivalent over $k$ and since both are unimodular, the result follows. □

If $A$ is Bezout, satisfies $\operatorname{qsr}(A) = 1$ and $2 \in A^\times$, then each quadratic form $f$ over $A$ is equivalent to a diagonal form $g = \sum_1^n a_i x_i^2$ where $a_i | a_{i+1}$, $i = 1, \dots, n-1$. This follows easily by induction: first factor out a generator for the coefficients of $f$ leaving a primitive form. The primitive form represents a unit by $\operatorname{qsr}(A) = 1$ and a change of variables will place the unit as the coefficient of $x_1^2$. Now complete squares. Clearly, $n$ and $\det(f)$ are also class invariants. Moreover, the invariant factor theorem implies that the ideals $a_i A$ are class invariants. We will call $n, \det(f)$, and the $a_i A$ the Jordan invariants of $f$. In general, the Jordan invariants do not classify even over fields (e.g., the form $ax^2 + ady^2$ need not be equivalent to $x^2 + dy^2$). However, it follows easily by induction that if the necessary condition that $ux^2 + udy^2$ is equivalent to $h = x^2 + dy^2$ holds for all $u \in A^\times, d \in A$ is satisfied then the listed invariants do classify. The equivalence of the latter two forms is just the condition that $h$ represent all units in $A$. However, it suffices to assume only that all such $h$ represent all units of $A$ over $k$ as the following theorem shows.

**Theorem 4.13.** *Let $A$ be a Bezout domain satisfying* $\mathrm{qsr}(A) = 1$, (VSA) *with respect to a set of p-adic spots and* $2 \in A^\times$, *and let $k$ be its field of quotients. If each binary quadratic form* $h = x^2 + dy^2, d \in A$, *represents over $k$ all units in $A$, then the Jordan invariants of a quadratic form classify.*

**Proof.** It suffices to show that $h$ represents all units of $A$ over $A_\omega$, $\omega$ a $p$-adic spot on $k$. Let $M_\omega = mA$. For any unit $u \in A^\times, x^2 + my^2 = uz^2$ has solutions $x, y, z \in A$ which are relatively prime. Since $m$ cannot divide $z$, it follows that $u$ is a square modulo $m$. By weak approximation of rotations we can pass to the completion of $\hat{A}_\omega$. By Hensel's lemma, $u \in A^\times$ is a square in $\hat{A}_\omega$ and is therefore represented by all forms $x^2 + dy^2$, $d \in A$. □

Note from the proof of Theorem 4.13 the additional conclusion that $A/mA$ is quadratically closed for each maximal ideal $mA$ corresponding to a $p$-adic spot on $A$.

If $\mathrm{Br}(k)$ contains no elements of order 2, then every nondegenerate binary quadratic form over $k$ is universal. This implies the condition about representation of binary forms over $k$ in the previous result (this is equivalent to assuming that there are no nontrivial quaternion algebras). With this assumption, we can determine precisely the set $D(f)$ of values represented by $f$.

If $A$ satisfies (VSA) with respect to a set $\Omega$ of $p$-adic spots, then we say $a \in A$ is squarefree if $a \notin m_\omega^2$ for each $\omega \in \Omega$. Note that every nonzero element can be factored as a square times a squarefree element.

**Corollary 4.14.** *Let $A$ be a Bezout domain satisfying* $\mathrm{qsr}(A) = 1$, (VSA) *with respect to a set of p-adic spots and* $2 \in A^\times$, *and let $k$ be its field of quotients. Assume that $Br(k)$ has no elements of order 2. Suppose $f$ is a primitive quadratic form of rank $r > 1$ with Jordan invariants $a_iA$, $1 \le i \le r$ (Note $a_1A = A$). Then $D(f)$ is the multiplicatively closed set consisting of the elements of $A$ which are squares modulo $a_2A$. In particular, if $a_2$ is squarefree, then $f$ is universal.*

**Proof.** Clearly, $D(f)$ is contained in the set of squares modulo $a_2A$. Let $a \in A$ be a square modulo $a_2$. By Corollary 4.9, it suffices to prove this locally. We may also assume that $f = x^2 + a_2y^2$. Clearly, $D(f)$ is then a multiplicatively closed set.

So we may assume that $A$ is a discrete valuation ring. First note that $D(f)$ contains $A^\times$ (by the proof of the previous result). Clearly, it contains all squares. Let $c$ be a generator for the maximal ideal.

By modifying $x$, we can assume that $c^2$ does not divide both $a, a_2$. We can assume that $c|a$ and since $a$ is a square modulo $a_2$, either $a_2$ is a unit or $a_2$ is exactly divisible by $c$. If $a_2$ is a unit then $a$ is represented as is shown in Lemma 4.11. There remains only to show in the remaining event that $x^2 + a_2y^2$ is universal. This however is clear since $a_2$ and all units are represented. □

All our conditions are satisfied by the ring of holomorphic functions on a noncompact Riemann surface (see the next section).

## 5. Rings of holomorphic functions

Let $\Omega$ be a connected open Riemann surface. Let $H = H(\Omega)$ denote the ring of holomorphic functions on $\Omega$. Since $\Omega$ is connected, $H$ is a domain. We recall some properties of $H$, and in particular show that we can apply the results of the previous section. Let $M = M(\Omega)$ denote the quotient field of meromorphic functions on $\Omega$. If $x \in \Omega$ and $f \in H$, we let $v_x(f)$ denote the order of the zero of $f$ at $x$. We can identify $\Omega$ with a set of $p$-adic spots on $M$.

We first show that $H$ satisfies (VSA) with respect to $\Omega$.

**Theorem 5.1.** *$H$ satisfies the following properties*:
(i) *$H$ is Bezout*;
(ii) $\mathrm{sr}(H) = 1$;
(iii) *$H$ satisfies* (VSA) *with respect to $\Omega$.*

**Proof.** The first two properties are well known. See [5] or [7]. The proof of (iii) is a minor variation of [5, 26.7].

Let $h \in H$ with the divisor of $h$ being $\sum_{i=1}^{\infty} n_i x_i$. Let $X = \{x_1, x_2, \ldots\}$. Let $U_0 = \Omega - X$. Suppose we are given complex numbers $a_{ij}$, $0 \le j \le n_i$. Choose neighborhoods $U_i$ of $x_i$ such that $U_i \cap X = \{x_i\}$, and functions $f_i \in H(U_i)$ such that $f_i^{(j)}(x_i) = a_{ij}$ for $0 \le j \le n_i$. Set $f_0 = 0$. Let $g_i = f_i/h$. Then $g_i - g_j \in H(U_i \cap U_j)$ for all $i, j$. By Mittag–Leffler (cf. [5, 26.3]), there exists a meromorphic function $g$ on $\Omega$ such that $g - g_i$ is holomorphic on each $U_i$. Set $f = gh$. Then on each $U_i$, $f = g_i h + (g - g_i)h$. Hence the first $n_i$ derivatives of $f$ and $f_i$ agree at each $x_i$.

Let $A_i$ denote the localization of $A$ at the maximal ideal corresponding to $x_i$. The above discussion shows that the natural map $A \to \prod_{i=1}^{\infty} A_i/hA_i$ is a surjection. Clearly, the kernel is generated by $h$. Thus Proposition 4.2 applies. $\square$

We also prove (using Theorem 5.1 and the fact that the integral closure of $H$ in a finite dimensional extension of $H$ has the same properties [7]) that if $T$ is any integral extension of $H$, then $\mathrm{Pic}(T) = 1$. In particular, it follows from Theorem 3.1 that:

**Corollary 5.2.** $\mathrm{qsr}(H) = 1$.

Let $\mathrm{Br}(F)$ denote the Brauer group of field $F$. In [6], we also show that:

**Theorem 5.3.** $\mathrm{Br}(M) = 1$.

Serre had suggested an alternate proof by showing that the group cohomology and the analytic cohomology coincided by a spectral sequence argument. The compact version of Theorem 5.3 is a classical result of Tsen. Indeed, Tsen proved that in the compact case, the field of rational functions is a $C_1$ field (i.e. any homogeneous form of degree $d$ in $n > d$ variables has a nontrivial zero). As far as we know this is still open in the noncompact case.

**Corollary 5.4.** *Let $K$ be a finite dimensional field extension of $M$. Let $S$ be the integral closure of $H$ in $K$. Then $N(S^\times) = H^\times$, where $N$ is the norm map from $K$ to $M$.*

**Proof.** Without loss of generality, we may assume that $K$ is Galois over $M$ with Galois group $G$. Let $\Omega'$ be the surface corresponding to $K$. Then $S = H(\Omega')$. We first note that $K^\times$ is cohomologically trivial as a $G$-module (since every finite extension of $M$ has trivial Brauer group, see [12, p. 161]).

Consider the sequence

$$1 \to S^\times \to K^\times \to \prod_{z\in\Omega'} \mathbb{Z},$$

where the map on right is defined by $f \mapsto \prod_{z\in\Omega'} v_z(f)$. By Theorem 5.1, the image of this map is the direct limit of $A(\Gamma) := \prod_{z\in\Gamma} \mathbb{Z}$, where $\Gamma$ runs over all discrete subsets of $\Omega'$. Now $G$ acts on the right hand group by permuting the points of $\Omega'$ and so on $A(\Gamma)$ where $\Gamma$ is any $G$-invariant discrete subset. If $\Gamma$ is $G$-invariant, then $A(\Gamma)$ is a direct product of permutation lattices. Thus, $\hat{H}^{-1}(G, A(\Gamma)) = 0$ (by Shapiro's Lemma). It follows from the long exact sequence for cohomology that $\hat{H}^0(G, S^\times) = \hat{H}^0(G, K^\times)$ is trivial. In particular, the norm map is surjective. $\square$

In particular, the results in the previous section apply and so the results stated in the introduction have been proved.

We mention one other example. Let $X$ be the real line. Let $A_1$ be the ring of real analytic functions on $X$ and $A_2$ the ring of complex valued analytic functions on $X$. Let $M_i$ denote the quotient field of $A_i$. By using the results on $H(\Omega)$ (and noting that any analytic function on $X$ has an extension to some neighborhood of $X$ in the complex plane), one can prove that:

**Proposition 5.5.** *$A_1$ and $A_2$ are Bezout, have stable range* 1 *and satisfy* (VSA) *with respect to $X$. Moreover,* $\mathrm{Br}(M_1)$ *is an uncountable group of exponent* 2 *and* $\mathrm{Br}(M_2) = 1$.

**Proof.** The facts that $A_i$ is Bezout and has stable range one are well known and follow easily from the corresponding results in the holomorphic case.

We sketch the proof for the Brauer group assertions. First consider $A_2$. Let $K$ be a finite dimensional field Galois extension of $M_2$. Let $G$ denote its Galois group. Then $K$ is generated by some element $\theta$ which we take to be in $A_2$. Let $m(x)$ denote its minimal polynomial. Choose some neighborhood $U$ of $X$ in $\mathbb{C}$ such that each coefficient of $m(x)$ has an analytic continuation to $U$. Then we can consider the corresponding field extension $L$ of $M(U)$. By shrinking $U$ if necessary, we may assume that $G$ is also the Galois group of $L/M(U)$. If $\phi \in Z^2(G, K^\times)$, then (shrinking $U$ further if necessary), we can extend it to an element of $Z^2(G, L^\times)$. Since $H^2(G, L^\times) = 0$, $\phi \in B^2(G, L^\times)$ and so by restriction is in $B^2(G, K^\times)$. Thus, $\mathrm{Br}(M_2) = 1$.

Note that $M_2/M_1$ is Galois of degree 2. Let $J$ denote its Galois group. Since $\mathrm{Br}(M_2)$ is trivial, $\mathrm{Br}(M_1) = H^2(J, M_2^\times)$. If $f \in M_1$ is a norm from $M_2$, then $f$ is a square in $M_1$. (By multiplying by a square in $A_1$, we may assume that $f$ is a norm from $A_2$; in particular, $f$ takes on only nonnegative values. By considering its power series expansion, it follows that the multiplicity of $f$ at any point is even. Thus, we may assume that $f$ is a unit and takes only on positive values; whence it is a square.) Thus $\mathrm{Br}(M_1) \cong M_1^\times/N(M_2^\times) = M_1^\times/(M_1^\times)^2$. Since there are uncountably many square classes in $M_1$ (for example, the functions $x - a, a \in X$, are in different square classes), this group is uncountable. □

We now consider an example.

**Example 5.6.** Let $X$ be a compact Riemann surface of genus $g$. Let $\Omega = X - B$ where $|B| = m + 1$. Then $|H^\times/(H^\times)^2| = 2^{m+2g}$ and there are $2^{m+2g}$ inequivalent quadratic unimodular forms over $H$ for each rank.

**Proof.** The square classes of units are in bijection with the unramified coverings of $\Omega$ of degree at most 2. These can be extended to degree 2 coverings of $X$ with branch points contained in $B$. The fundamental group $G$ of $\Omega$ is generated by elements

$$d_0, \dots, d_m, e_1, f_1, \dots, e_g, f_g$$

subject to the one relation $d_0 \cdots d_m[e_1, f_1] \cdots [e_g, f_g] = 1$. It follows therefore that $G/[G, G]G^2$ has order $2^{m+2g}$, whence the number of branched coverings of $X$ of degree at most 2 with branched points contained in $B$ is $2^{m+2g}$. (Implicit in this argument is Riemann's Existence Theorem which asserts that any topological covering can be given the structure of an analytic covering.) □

In particular, if $\Omega = \mathbb{C}$, then any unimodular quadratic form is equivalent to the sum of squares form.

If $\Omega = \mathbb{C} - B$ where $B$ is an infinite set with no finite limit points , then there will be infinitely many square classes in $H^\times$.

One can use these results to easily describe the Witt rings of $H$ and $M$. We leave this to the reader.

There is a cohomological interpretation of Theorem A. Let $q$ be a quadratic form in $d$ variables over $H$. Let $\mathcal{O}(q, H)$ denote the sheaf of orthogonal groups of $q$ over $H$ and $\mathcal{O}(q, M)$ the sheaf of orthogonal groups over $M$.

Let $S$ be the symmetric $n \times n$ matrix representing $q$ with respect to the standard basis. For convenience, we assume that $d(S) = \det(S) \neq 0$ (the discussion below is valid with obvious modification as long as $q \neq 0$). Let $\mathscr{U} = (U_i)_{i \in I}$ be an open covering of $\Omega$. Let $F \in Z^1(\Omega, \mathcal{O}(q, H))$. Since $H^1(\Omega, GL_n) = 0$ ([5, 30.5]), it follows that there exist $G_i \in GL_n(H(U_i))$ with $F_{ij} = G_i G_j^{-1}$ representing $F$.

Let $T_i = U_i S U_i^t \in S_n(H(U_i))$. By construction, $T_i = T_j$ on $U_i \cap U_j$. Thus, we have defined a global $T \in S_n(H)$ and $T$ is locally congruent to $S$. If the family $G_i$ is replaced by an equivalent one, then the $T$ constructed will be globally equivalent to the original $T$.

By Corollary E, the congruence class of $T$ (over either $H$ or $M$), depends only on the square class of $d(T)$. Since $S$ and $T$ are locally congruent, it follows that $d(T)/d(S) \in H^\times$. Thus, the map $[F] \mapsto (d(T)/d(S))(H^\times/H^\times)^2$ is well defined. If $[F_1]$ and $[F_2]$ have the same image, then the corresponding symmetric matrices will be globally equivalent by Corollary E. Thus, this map is injective. Since locally every unit of $H$ is a square, the map is surjective. Thus, we have shown:

**Corollary 5.7.** *There is a natural identification of $H^1(\Omega, \mathcal{O}(q,H))$ and $H^\times/(H^\times)^2$ The natural map $H^1(\Omega, \mathcal{O}(q,H)) \to H^1(\Omega, \mathcal{O}(q,M))$ is injective.*

A minor variation on the discussion above shows that $H^1(\Omega, \mathcal{O}(q,M))$ may be identified with the square classes of $M^\times$ which are locally trivial (i.e. the multiplicities of the poles and zeroes are all even).

The same argument as above, using Corollary 2.6, shows that:

**Proposition 5.8.** $H^1(\Omega, \mathrm{Sp}(B,H)) = 0$, *where* $\mathrm{Sp}(B,H)$ *is the sheaf of symplectic groups associated to the alternating form B.*

Similarly, the local–global result in [6] can be interpreted as:

**Proposition 5.9.** *Let $A$ be an $H$-subalgebra of $M_n(H)$. Let $\mathscr{C}^\times$ be the sheaf associated to the units of the centralizer of $A$ in $M_n(H)$. Then $H^1(\Omega, \mathscr{C}^\times) = 0$.*

One can give cohomological interpretations of the results in the previous section in an analogous manner.

## 6. Integral extensions and number theoretic examples

We now consider how some of the properties we have been considering behave under finite integral extensions. If one considers the property that all primitive polynomials represent units (or equivalently all homogeneous primitive polynomials), then it was shown in [3] that any integral extension has the same property. (This property is not invariant under localizing at a multiplicatively closed set [6, Example 2.8] and the same example shows that the stable range 1 condition is not invariant under localization.) See [3] for various examples of commutative rings satisfying variations of these properties.

Suppose $\mathrm{sr}(A) = 1$. It was asked in [6] whether this property is invariant under finite integral extensions. We show that if $T/A$ is integral, then $\mathrm{sr}(A) = 1$ does not imply that $\mathrm{sr}(T) = 1$ even for $A$ a principal ideal domain.

**Example 6.1.** Let $S$ be the multiplicatively closed subset of $\mathbb{Z}$ generated by $-1$ and all primes $p \equiv 5 \pmod{12}$. Set $A = S^{-1}\mathbb{Z}$ and $T = A[\omega]$, where $\omega$ is a primitive 6th root of unity.

(a) $A$ is a principal ideal domain with $\mathrm{sr}(A) = 1$.

(b) $T$ is a principal ideal domain and one is not in the stable range of $T$.

**Proof.** Clearly $A$ is a principal ideal domain. $\mathrm{sr}(A) = 1$ by [4, 7.4]. Since $\mathbb{Z}[\omega]$ is a principal ideal domain, so is $T$. So we only need show that one is not in the stable range of $T$.

Note that every prime $p$ in $S$ remains prime in $\mathbb{Z}[\omega]$. Since $T = S^{-1}\mathbb{Z}[\omega]$, $T^\times = \langle S, \omega\rangle = \langle S, \omega^2\rangle$.

Consider $\mathbb{Z}/13\mathbb{Z} = A/13A \subset T/13T$. Since 13 splits in $T$, $(T/13T)^\times$ has order 144. Let $\pi$ be the natural map from $T$ to $T/13T$. Clearly $|\pi(S)| = 12$ (since $\pi(S) \subset A/13A$). Therefore, $|\pi(T^\times)| \le 36 < |(T/13T)^\times|$. Thus, $\pi$ is not a surjection from $T^\times$ to $(T/13T)^\times$. In particular, one is not in the stable range. $\square$

Note that the previous example also shows that stable range one and trivial Picard group do not imply that primitive binary quadratic polynomials represent units (see Theorem 3.1).

Example 6.5 below shows that if $S$ and $T$ are commutative rings with $T$ module finite over $S$ then $\mathrm{sr}(T) = 1$ does not imply $\mathrm{sr}(S) = 1$. Thus $\mathrm{sr}(T) = 1$ does not in general extend or descend with respect to pairs of commutative rings $S, T$ with $T$ an $S$-module of finite type.

Let $X$ denote a set of prime integers. By a set of *almost all primes* from $X$ we mean a subset $Y$ such that $X - Y$ has Dirichlet density 0 (see e.g., [9, p. 167] for a discussion of Dirichlet density). We let $\mathscr{R}_c = \mathscr{I}(c)/P_c$ denote the ray class defined by a cycle $c$ for a number field $k$ with ring of integers $\mathcal{O}$ (see e.g., [9]). Thus, $\mathscr{I}(c)$ is the set of fractional $\mathcal{O}$ ideals prime to $c$ and $P_c$ the set of principal fractional ideals generated by elements of the type $\alpha \in k$ satisfying $\alpha \equiv 1 \bmod^* c$. The following lemma is standard. We sketch the proof for completeness.

**Lemma 6.2.** *Let $\mathscr{A} = \bigoplus_1^n K_i$, $K_i$ a number field with ring of integers $\mathcal{O}_i$. If $T$ is a $\mathbb{Z}$-suborder of the ring $\mathcal{O} = \bigoplus \mathcal{O}_i$ and $T\mathbb{Q} = \mathscr{A}$ then there are cycles $c_i$ for $K_i, i = 1, \ldots, n$, such that* $\mathrm{Pic}(T)$ *is a homomophic image of $\prod \mathscr{R}_{c_i}$.*

**Proof.** Since $[\mathcal{O} : T]$ is finite, there is a positive integer $n$ such that $n\mathcal{O} \subset T$. Let $c_i$ denote the cycle defined on $K_i$ by $n$; i.e., the primes $P$ dividing $n$ with multiplicity their exponent in the prime factorization of $n$. Clearly, $\mathscr{I}(c) \cong \prod \mathscr{I}_i(c)$ where $\mathscr{I}(c)$ denotes the set of invertible $\mathcal{O}$ ideals prime to $c$. There is an epimorphism $\sigma : I(c) \to \mathrm{Pic}(T)$ defined by $\sigma(J) = J^*$ where $J_P^* = J_P$ at primes $P$ not dividing $c$ and $J_P^* = T_P$ for $P$ dividing $c$. The proof is completed by showing that $\prod P_{c_i}$ is in the kernel of this map. If however, $J \in P_{c_i}$ with $J = \alpha\mathcal{O}_i, \alpha \equiv 1 \bmod^* c_i$ then a local check shows that the image of $J$ in $\mathrm{Pic}(\mathcal{O})$ maps to $\alpha T$. $\square$

**Theorem 6.3.** *Let $K$ be a number field with ring of integers $\mathcal{O} = \mathcal{O}_K$ and let $S$ denote the multiplicative system generated by almost all primes from the set of primes $p \in \mathbb{Z}$ such that $p$ is the norm of a degree* 1 *prime ideal of $K/\mathbb{Q}$. Then* $\mathrm{qsr}(S^{-1}\mathcal{O}) = 1$.

**Proof.** It suffices by Theorem 3.1 to show that $\mathrm{Pic}(S^{-1}T) = 1$ for any quadratic $S^{-1}\mathcal{O}$-algebra. Since $\mathrm{Pic}(S^{-1}T)$ is isomorphic to the ideal class group of $S^{-1}T$ and the latter is a homomorphic image of the ideal class group of $T$, it suffices to show the ideal class group of $T$ is generated by the degree 1 prime ideals having norms in $S$. Lemma 6.2 allows us to replace the ideal class group of $T$ with a ray class group. The proof now follows from the density theorem for ray classes; i.e., each ray class contains a set of degree 1 prime ideals of positive Dirichlet density [9, p. 166]. □

Actually, one can prove more than required in the previous theorem; e.g., that $\mathrm{Pic}(R) = 1$ for any commutative ring $R$ integral over $S^{-1}\mathcal{O}$.

**Theorem 6.4.** *Let $K \neq \mathbb{Q}$ be an abelian extension of $\mathbb{Q}$ having conductor $\mathscr{F}$. Let $S$ denote the multiplicative system generated by all but finitely many $\{N(P)$: $P$ a degree 1 unramified prime ideal of $K\}$. If $[K:\mathbb{Q}] > 2$ or $K$ is a real quadratic extension of $\mathbb{Q}$ then $\mathrm{sr}(S^{-1}\mathbb{Z}) \neq 1$. If $K$ is a complex quadratic extension of $\mathbb{Q}$ then $\mathrm{sr}(S^{-1}\mathbb{Z}) = 1$.*

**Proof.** The Artin map $(J, K/\mathbb{Q})$ provides an isomorphism between $I(\mathscr{F})/\mathscr{P}_{\mathscr{F}}\mathscr{A}_{\mathscr{F}}$ and the Galois group $G = G_{K/\mathbb{Q}}$, $I(\mathscr{F})$ the set of fractional ideals of $K$ prime to $\mathscr{F}$, $\mathscr{A}_{\mathscr{F}}$ the image under the norm map of $I(\mathscr{F})$ and $P_{\mathscr{F}}$ the set of principal ideals generated by elements $e \equiv 1 \bmod \mathscr{F}$ (see e.g., [9, Chap. X]). Let $f$ denote the finite part of $\mathscr{F}$. If $[K:\mathbb{Q}] > 2$, we can pick a prime $p$ prime to $\mathscr{F}$ belonging to $g \in G, g \neq ((1-f)\mathbb{Z}, K/\mathbb{Q})^{-1}, 1$. Note that $((1-f)\mathbb{Z}, K/\mathbb{Q})^{-1} = ((1-2f)\mathbb{Z}, K/\mathbb{Q})$ since $(1-f)(1-2f)$ is positive and of the form $1+fj$. We claim that the pair $(p, f)$ is not stable in $S^{-1}\mathbb{Z}$. For if $p \equiv u \bmod f(S^{-1}\mathbb{Z})$ with $u \in (S^{-1}\mathbb{Z})^{\times}$ then $ps \equiv \pm s' \bmod f\mathbb{Z}$ for some $s, s' \in S$. Set $ps = \pm s'(1+fw), w \in \bigcap_{p|f} \mathbb{Z}_p$. Then, $g = ((1+fw)\mathbb{Z}, K/\mathbb{Q})$. The latter quantity is 1 if $1+fw > 0$ since then $1+fw \in P_{\mathscr{F}}$. Thus, $1+fw < 0$. However, then $(1+fw)(1-2f) = 1+ft > 0$ and $g = ((1-f)\mathbb{Z}, K/\mathbb{Q})^{-1}$, a contradiction.

In the event $K$ is totally real, $((1-f)\mathbb{Z}, K/\mathbb{Q}) = 1$ and the proof follows as above with $g \neq 1$.

Now assume that $K$ is a complex quadratic extension of $\mathbb{Q}$. We first show that $((1-f)\mathbb{Z}, K/\mathbb{Q}) \neq 1$. Assume otherwise that $(1-f)\mathbb{Z} = (1+fw)N(J), J \in I(\mathscr{F}), w \in \bigcap_{p|f} \mathbb{Z}_p$. Since all units are norms at unramified spots, the last equation implies that $x = \frac{1-f}{1+fw}$ is a norm at all unramified spots. Also, $x$ is a norm at the finite ramified spots (see e.g., [9, pp. 146–147]). By the product formula for the Hilbert symbol, $x$ is a norm at the archimedian spot. But $x < 0$ and since the archimedean spot ramifies, norms at this spot are positive, a contradiction. For the proof that $\mathrm{sr}(S^{-1}\mathbb{Z}) = 1$, it suffices by [4, 7.4] to show that for $u \in \mathbb{Z}$ prime to $f, \exists s \in S$ such that $u \equiv \pm s \bmod f$. Now one of $u\mathbb{Z}, u(1-f)\mathbb{Z}$ has trivial value under the Artin map. By the density theorem, we can pick a prime ideal $s\mathbb{Z}$ in the ray class (defined by $\mathscr{F}$) for this ideal. The proof now follows. □

Verification of the following example is a routine application of the previous two theorems.

**Example 6.5.** Let $p$ be a prime with $p \equiv 1 \bmod 4$ and $K = \mathbb{Q}(\sqrt{p})$. Let $S$ denote the set of primes which are nonzero squares modulo $p$. Then $\mathrm{sr}(S^{-1}\mathbb{Z}) \neq 1$ and $\mathrm{qsr}(S^{-1}\mathcal{O}_K) = 1$.

In view of Example 6.5 neither $\mathrm{sr}(T) = 1$ nor $\mathrm{qsr}(T) = 1$ for a ring $T$ descends to rings over which $T$ is module finite. Whether $\mathrm{qsr}(A) = 1$ extends to module finite extensions is still open.

**Question 6.6** Let $A$ and $T$ be commutative rings with $T$ integral over $A$. If every primitive quadratic form over $A$ represents a unit, is the same true for $T$?

Corollary 3.2 provides some evidence that the previous question could have an affirmative answer.

The next example shows that we can construct overrings $A$ of $\mathbb{Z}$ in $\mathbb{Q}$ which satisfy $\mathrm{qsr}(A) = 1$ (and in particular have stable range one) by inverting a set of primes of density zero. It is easy to see inverting a finite set of primes can never achieve this property.

**Example 6.7.** There exists a set $S$ prime integers such that $S$ has Dirichlet density zero and every primitive binary quadratic form over $A := S^{-1}\mathbb{Z}$ represents a unit.

**Proof.** Let $q_1, q_2, \ldots$ be a complete set of representatives of equivalence classes of rank 2 primitive binary quadratic forms over $\mathbb{Z}$. If $q_n$ is anisotropic then a classical result of Dirichlet implies that $q_n$ represents infinitely many primes, hence there exists a prime $p_n > n^2$ such that $q_n$ represents $p_n$. If $q_n$ is isotropic then $q_n$ is equivalent to a form $x(ax+by)$ with $a, b$ relatively prime and Dirichlet's theorem on primes in an arithmetic progression implies that $q_n$ represents a prime $p_n > n^2$. Let $S = \{p_n \colon n = 1, 2, \ldots\}$. Clearly, this set has density zero (since the sum of the reciprocals converges), and every primitive form over $A$ represents a unit (since such a form is a unit multiple of a primitive form over $\mathbb{Z}$, and rank 1 primitive binary quadratic forms over $\mathbb{Z}$ are equivalent to $\pm x^2$). $\square$

The following example shows that it is possible for primitive nondegenerate quadratic forms in $d > 2$ variables to represent units without primitive binary forms always representing units. That is, if we define $\mathrm{qsr}^*(A) = d$ when primitive nondegenerate quadrate forms in $d+1$ variables represent units then $\mathrm{qsr}{*}(A) = d > 1$ need not imply $\mathrm{qsr}(A) = 1$.

**Example 6.8.** Let $q$ be an odd prime, $r$ a nonquadratic residue modulo $q$, $S$ the multiplicative system in $\mathbb{Z}$ generated by -1 and all primes having residue $r$ modulo $q$, and set $A = S^{-1}\mathbb{Z}$. If $S$ does not contain all units modulo $q$ (e.g., $q = 13$, $r = 5$), then $\mathrm{qsr}{*}(A) \neq 1$ and $\mathrm{qsr}{*}(A) = d \ \forall d > 1$.

**Proof.** In order to show $\mathrm{qsr}(A) \neq 1$, we have only to show that $\mathrm{sr}(A) \neq 1$; i.e., the units of $A$ do not map onto the units of $A/qA$. Now $A^{\times} = SS^{-1}$ which by hypothesis does not map onto $(A/aA)^{\times} = (\mathbb{Z}/q\mathbb{Z})^{\times}$.

$A$ is a principal ideal domain with the set of $p$-adic spots $\Omega$ defined by the primes $p$ generating maximal ideals in $A$; i.e., all $p$-adic spots defined by primes $p \notin S$. Let $f$ denote a nondegenerate primitive quadratic form over $A$ in 3 or more variables. We will first will show that the $\Omega$-genus of $f$ represents elements in $S$ and by weak approximation need only show that there is an element in $S$ represented over $\mathbb{Z}_p$ for each $p \in \Omega$ and over the reals. Since representation by the genus implies representation by a form in the genus (see e.g., [11, 102:5]), the proof will follow if we next show that the $\Omega$-genus of $f$ and the class of $f$ over $A$ coincide. If $f$ is any nondegenerate primitive quadratic form in 3 or more variables over $A$ then $f$ is isotropic over the completion of $\mathbb{Q}$ at some prime in $S$. Thus $\Omega$ is an indefinite set of spots, and Eichler's theorem implies that the $\Omega$-spinor genus coincides with the class of $f$ over $A$ (see e.g., [11, 104:5]). Hence the proof will be concluded if we show that the $\Omega$-genus and $\Omega$-spinor genus of $f$ coincide.

*Representation by the $\Omega$-genus of $f$*: By multiplying $f$ with a suitable unit in $A$, we can assume that $f$ is a primitive form over $\mathbb{Z}$ which is not negative definite. We can therefore insure representation at the real spot by only considering positive values $s \in S$. Moreover, any such $s$ is represented at all odd primes at which $f$ is unimodular (since rank-$f \geq 3$ and $f$ unimodular imply that $f$ is isotropic at nondyadic spots). Let $T$ denote the spots at which $f$ is not unimodular along with the dyadic spot and let $u_p$ denote a unit represented by $f$ at each $p$-adic spot in $T$. We can assume that $u_p \in \mathbb{Z}$ by multiplying by square of units. If $q \in T$, then $u_q x^2$ splits $f$ and $f$ therefore represents all units $w_q$ such that $w_q u_q$ is a square. Thus, $f$ represents elements of $S$ at $q$: $f$ represents all $q$-adic squares in $S$ in the event $u_q$ is a square and all $rs$ such that $s \in S$ is a $q$-adic square in the event $u_q$ is not a square. Now use the Chinese remainder theorem and Dirichlet's theorem to select two primes $x, y$ such that $xu_p, y_p$ are squares of units at each prime $q \neq p \in T$ and $x \equiv y \equiv r \bmod q$. Thus, $x, xy$ are represented by $f$ at all $q \neq p \in T$ and either $x$ or $xy$ is represented by $f$ at $q$.

*$\Omega$-genus $f$ = $\Omega$-spinor genus $f$*: We can replace $f$ with its corresponding lattice $L = L_f$ on the quadratic space $V = V_f$ associated with $f$. Let $K$ be a lattice in the $\Omega$-genus of $L$ and choose $\sigma_p \in O(V_p)$ such that $\sigma_p(L_p) = K_p, p \in \Omega$. We can assume that $\sigma_p$ is the identity for all but finitely many $p$. The image of the spinor norm map on the quadratic space $V$ contains $\{e(\mathbb{Q}^\times)^2 | e \in \mathbb{Q}, e > 0\}$ [11, 101:8]. Thus, by replacing $K$ with $\sigma(K)$ and $\sigma_p$ with $\sigma\sigma_p$, we can assume that the spinor norm of each $\sigma_p$ is $u_p({\mathbb{Q}_p}^\times)^2$ with $u_p$ a unit. As previously, select two primes $x, y$ so that $xu_p, y$ are squares at each $p \in T - \{q\}$ and $x \equiv y \equiv r \bmod q$. Now select isometries $\tau, \tau'$ with respective spinor norms $x(\mathbb{Q}^\times)^2, y(\mathbb{Q}^\times)^2$. Since the spinor norm groups for the isometries of $L_p$ contain all units modulo squares at each $p \notin T$ [11, 92:5], it follows that there are local isometries $\lambda_p$ having spinor norm 1 and such that $\tau(K_p) = \lambda_p(L_p) \forall p \in \Omega$ or $\tau'\tau(K_p) = \lambda_p(L_p) \forall p \in \Omega$. Thus $K$ and $L$ are in the same $\Omega$-spinor genus. □

It would be of interest to determine whether some natural infinite integral extensions of $\mathbb{Z}$ have the property that every primitive binary quadratic form represents a unit.

If $A$ is the ring of all algebraic integers, then Skolem had already observed that every primitive polynomial represents a unit (cf., [3]). This was extended to the ring of all real algebraic integers in [3].

We close by mentioning some open cases.

If $A$ is the ring of all totally real algebraic integers, then it is known that $\mathrm{sr}(A) = 1$ (cf., [13]). It follows from class field theory that $A$ is Bezout. So the only condition to verify is that $\mathrm{Pic}(T) = 1$ for any quadratic extension $T$.

If $A$ is the ring all algebraic integers in the solvable closure of $\mathbb{Q}$, then $A$ has no nontrivial quadratic extensions. It is easy to see that $A$ is Bezout (either use class field theory or an elementary argument about domains closed under $n$th roots). Thus, one only needs to determine whether $\mathrm{sr}(A) = 1$.

## References

[1] R. Baeza, Quadratic Forms Over Semilocal Rings, Lecture Notes in Mathematics, Vol. 655 (Springer, New York, 1978).
[2] H. Bass, Algebraic K-theory, Math. Lecture Note Series (Benjamin, New York, 1968).
[3] D. Estes and R. Guralnick, Module equivalences: local to global when primitive polynomials represent units, J. Algebra 77 (1982) 138–157.
[4] D. Estes and J. Ohm, Stable range in commutative rings, J. Algebra 7 (1967) 343–362.
[5] O. Forster, Lectures on Riemann Surfaces (Springer, New York, 1981).
[6] R. Guralnick, Matrices and representations of rings of analytic functions and other one dimensional rings, Visiting Scholars Lectures, Mathematics Series 15 (1986–87) Texas Tech. University, 15–35.
[7] R. Guralnick, Similarity of holomorphic matrices, Linear Algebra Appl. 99 (1988) 85–96.
[8] B. Kirkwood and B. McDonald, The symplectic group over a ring with one in its stable range, Pacific J. Math. 92 (1981) 111–125.
[9] S. Lang, Algebraic Number Theory (Springer, New York, 1970).
[10] B. McDonald and B. Hershberger, The orthogonal group over a full ring, J. Algebra 51 (1978) 536–549.
[11] O.T. O'Meara, Introduction to Quadratic Forms (Springer, New York, 1963).
[12] J.-P. Serre, Local Fields (Springer, New York, 1979).
[13] W. Van der Kallen, The $K_2$ of rings with many units, Ann. Sci. École Norm. Sup 4 (1977) 473–515.