

Indecomposable integral quadratic forms over global function fields

by

LARRY J. GERSTEIN (Santa Barbara, CA)

A *global field* is an algebraic number field or an algebraic function field in one variable over a finite constant field. We will assume throughout that all fields have characteristic not 2. The *Hasse domains* of global fields include the rings of algebraic integers and their analogues in function fields. (A more precise definition will be given below.) Here is the situation with which we will be concerned: F is a global field, \mathfrak{o} is a Hasse domain of that field, V is a regular quadratic space of dimension n over F , and L is an \mathfrak{o} -lattice on V . (That is, L is a finitely generated \mathfrak{o} -module spanning V .)

Must L have a nontrivial orthogonal decomposition if n is sufficiently large? If the space V is *definite* the answer is a resounding “no.” For example, for every positive integer n the root lattice A_n is an indecomposable positive definite \mathbb{Z} -lattice of rank n . Similarly, the root lattice D_n is indecomposable for each $n \geq 3$. (See [C–S, Chapter 4] or [M–H, Appendix 5] for a description of these and other families of lattices.) Kitaoka [K] has shown that whenever an indecomposable definite \mathbb{Z} -lattice is extended (via tensor product) to a lattice over the ring of integers of a totally real algebraic number field, the result is again indecomposable. So there are indecomposable lattices of every rank in the definite case over number fields.

The notions of definiteness and indefiniteness extend to the arbitrary global context: Given a Hasse domain \mathfrak{o} of a global field F , a quadratic F -space V and the \mathfrak{o} -lattices on it are said to be *definite* if $V_{\mathfrak{p}}$ is anisotropic for every “infinite” spot (place) \mathfrak{p} on F ; that is, for every spot not corresponding to a prime ideal of \mathfrak{o} . The space V and its lattices are *indefinite* otherwise. O’Meara [O’M2, Theorem 3.1] showed that indecomposable \mathfrak{o} -lattices exist on any definite quadratic space over a global field. In particular, if \mathfrak{o} is a Hasse domain of a function field, then there exist indecomposable \mathfrak{o} -lattices of every rank $n \leq 4$.

What about the indefinite case? Watson [W, Chapter 7, §4] showed that every indefinite \mathbb{Z} -lattice of rank ≥ 12 has an orthogonal splitting, and in a subsequent unpublished note he showed 12 to be best possible; that is, there exists an indecomposable indefinite \mathbb{Z} -lattice of rank 11. In [G1] I extended Watson's result to arbitrary Hasse domains, showing that for every Hasse domain \mathfrak{o} there is a positive integer $n_{\mathfrak{o}}$ such that every indefinite \mathfrak{o} -lattice of rank $\geq n_{\mathfrak{o}}$ splits. I went on to show that there is no $n_{\mathfrak{o}}$ that works simultaneously for all Hasse domains; specifically, for the rings of algebraic integers of all algebraic number fields. However, in the same paper I showed that $n_{\mathfrak{o}} = 7$ always works in the global function field setting, and further that an orthogonal splitting will occur (again, in the function field case) whenever $n \geq 5$ if any of the following three conditions hold:

- (i) -1 is a square in F ;
- (ii) \mathfrak{o} is a principal ideal domain;
- (iii) there is an infinite spot \mathfrak{q} at which -1 is not a square.

In [G3] I showed (via a scaling argument) that $n \geq 5$ forces splitting whenever the class number of \mathfrak{o} is odd, a weakening of condition (ii) above.

It is natural to ask whether the "universal splitting number" 7 for global function fields is the best possible, and in this paper we answer this question in the affirmative by giving a construction for an indecomposable lattice of rank 6 over an appropriate Hasse domain of any rational function field in which -1 is not a square.

The classification up to isometry of lattices on quadratic spaces over global fields is understood only in very special cases. For instance, if L is a unimodular $k[x]$ -lattice on a quadratic space over the rational function field $k(x)$, then it can be shown that L has an orthogonal basis; and from this it follows that the classification of unimodular $k[x]$ -lattices reduces to the classification of quadratic spaces over k (see [G2, Theorem 3.1], [L, §VI.3], or [S, §6.3]); but the problem of classifying nonunimodular $k[x]$ -lattices is still wide open. And even the unimodular case remains to be settled over other Hasse domains. Achieving an understanding of orthogonal decomposition may turn out to be fruitful in advancing the classification theory, and this is an underlying motivation of this work.

DEFINITION. Let F be a global field. A *Hasse domain* of F is a Dedekind domain obtained by intersecting the valuation rings associated with almost all the discrete spots on F . That is, if S is such a set of spots, the associated Hasse domain is the ring

$$\mathfrak{o} = \mathfrak{o}(S) = \{\alpha \in F \mid \text{ord}_{\mathfrak{p}} \alpha \geq 0 \text{ for all } \mathfrak{p} \in S\}.$$

EXAMPLES. (i) The ring of integers of an algebraic number field F is the Hasse domain associated with the set S consisting of *all* the discrete spots

on F . (ii) If F is a global function field, with k its finite field of constants, then every Hasse domain of F can be realized as the integral closure in F of the polynomial ring $k[x]$ for a suitable choice of $x \in F$. (See Rosen [R, Prop. 7]; in fact Rosen does not require that the constant field k be finite.)

Our notation and terminology will generally be that of [O'M1]. From now on F will denote a global *function* field with finite constant field k ; thus k is algebraically closed in F , and F is a finite extension of $k(x)$ for some element x transcendental over k . We use $\Omega = \Omega_F$ for the set of non-trivial spots on F . And for each $\mathfrak{p} \in \Omega$ we use $|\cdot|_{\mathfrak{p}}$ for the normalized valuation on F at \mathfrak{p} (or on the completion $F_{\mathfrak{p}}$ of F at \mathfrak{p}); thus if $\alpha \neq 0$ then

$$|\alpha|_{\mathfrak{p}} = \left(\frac{1}{N_{\mathfrak{p}}} \right)^{\text{ord}_{\mathfrak{p}} \alpha}$$

where $N_{\mathfrak{p}}$ is the cardinality of the residue class field at \mathfrak{p} . Every completion $F_{\mathfrak{p}}$ is a nondyadic local field. For each discrete $\mathfrak{p} \in \Omega$ the residue class field $F(\mathfrak{p})$ (or $F_{\mathfrak{p}}(\mathfrak{p})$) is a finite extension of k . By the *degree* of \mathfrak{p} , denoted $\text{deg } \mathfrak{p}$, we mean the degree $[F(\mathfrak{p}) : k]$. Finally, if K is a field, then K^* denotes its multiplicative group of nonzero elements, and \dot{K}^2 its subgroup of nonzero squares.

We remark that in the literature the Hasse domain $\mathfrak{o}(S)$ is sometimes referred to as the ring of *S-integers*. Some authors use S for what is here the complementary set $\Omega - S$.

LEMMA (Local Square Theorem). *If $|\alpha|_{\mathfrak{p}} < 1$ then $1 + \alpha \in \dot{F}_{\mathfrak{p}}^2$.*

PROOF. See [O'M1, Theorem 63:1].

THEOREM. *Let k be a finite field in which -1 is not a square, and let $F = k(x)$. Let $q = x^2 + 1$, let \mathfrak{q} be the q -adic spot on F , and let $S = \Omega - \{\mathfrak{q}\}$. Then there exists an indecomposable $\mathfrak{o}(S)$ -lattice of rank 6 on a suitable quadratic F -space.*

PROOF. We first claim that there exist spots $\mathfrak{p}_1, \mathfrak{p}_2 \in S$ of odd degree such that $x^2 + 1 \in \dot{F}_{\mathfrak{p}_1}^2$ and $x^2 + 1 \notin \dot{F}_{\mathfrak{p}_2}^2$. In fact we can take \mathfrak{p}_1 to be the x -adic spot, for then since x is prime at \mathfrak{p}_1 the statement $x^2 + 1 \in \dot{F}_{\mathfrak{p}_1}^2$ is immediate from the local square theorem. Now suppose $\beta \in k$, and let \mathfrak{p} be the $(x + \beta)$ -adic spot on F . Then $F_{\mathfrak{p}}(\mathfrak{p}) = k$, and hence an element of k is square in $F_{\mathfrak{p}}$ if and only if it is square in k ; from this observation and the equation

$$x^2 + 1 = (\beta^2 + 1) \left(1 + \frac{x - \beta}{\beta^2 + 1} (x + \beta) \right),$$

the local square theorem gives

$$x^2 + 1 \begin{cases} \in \dot{F}_{\mathfrak{p}}^2 & \text{if } \beta^2 + 1 \in \dot{k}^2, \\ \notin \dot{F}_{\mathfrak{p}}^2 & \text{if } \beta^2 + 1 \notin \dot{k}^2. \end{cases}$$

As in [O'M1, 62:1] we now argue that since the sets \dot{k}^2 and $\dot{k}^2 + 1$ have the same cardinality, and 1 is in the former but not the latter, there is an element $\beta \in \dot{k}$ such that $\beta^2 + 1 \notin \dot{k}^2$; and $\beta^2 + 1 \neq 0$ by hypothesis. With β such an element of k , let \mathfrak{p}_2 be the $(x + \beta)$ -adic spot on F .

Having fixed \mathfrak{p}_1 and \mathfrak{p}_2 , let \mathfrak{p}_3 be any other spot in S of odd degree. At each of these spots \mathfrak{p}_i fix a prime element π_i . Let $U_{\mathfrak{q}}$ be a 6-dimensional quadratic $F_{\mathfrak{q}}$ -space with $dU_{\mathfrak{q}} = 1$ and $S_{\mathfrak{q}}U_{\mathfrak{q}} = -1$. There is a 6-dimensional quadratic F -space V satisfying

$$V_{\mathfrak{p}} \cong \begin{cases} \langle \pi_i, \dots, \pi_i \rangle & \text{if } \mathfrak{p} = \mathfrak{p}_i, \ i = 1, 2, 3, \\ \langle 1, \dots, 1 \rangle & \text{if } \mathfrak{p} \in S - \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}, \\ U_{\mathfrak{q}} & \text{if } \mathfrak{p} = \mathfrak{q}. \end{cases}$$

Such an F -space V exists by Theorem 72:1 of [O'M1]—a theorem that holds over arbitrary global fields, though it is stated only for number fields.

There is an $\mathfrak{o}(S)$ -lattice L on V satisfying

$$L_{\mathfrak{p}} \cong \begin{cases} \langle \pi_i, \pi_i^3, \pi_i^5, \pi_i^7, \pi_i^9, \pi_i^{11} \rangle & \text{when } \mathfrak{p} = \mathfrak{p}_i, \ i = 1, 2, 3, \\ \langle 1, \dots, 1 \rangle & \text{for all } \mathfrak{p} \in S - \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}. \end{cases}$$

To see this, first note that each local space $V_{\mathfrak{p}}$ supports an $\mathfrak{o}_{\mathfrak{p}}$ -lattice $J_{(\mathfrak{p})}$ with the given local structure. Any given lattice K on V is unimodular at almost all \mathfrak{p} and hence satisfies $K_{\mathfrak{p}} \cong J_{(\mathfrak{p})}$ at almost all \mathfrak{p} . Then it follows from [O'M1, 81:14] that there is a lattice L on V with the stated local structure at all $\mathfrak{p} \in S$. We claim that L is indecomposable.

The argument will be in three stages, and crucial to everything is the classification of lattices over the ring of integers of a nondyadic local field: such a lattice is an orthogonal sum of modular components—the *Jordan* components. The ranks and discriminants of those components constitute a complete set of invariants for the lattice up to isometry. (See [O'M1, Theorem 92:2] for the details.) The Jordan components for the three localized lattices $L_{\mathfrak{p}_i}$ in our present situation are of the form $\langle \pi_i^j \rangle$, with j odd.

(I) We first show that L has no orthogonal splitting $L = L_1 \perp L_2$ in which rank L_1 is odd. Suppose to the contrary that there *is* such a splitting. Let $\alpha = d(FL_1)$. Then, from the uniqueness properties of Jordan splittings, $\text{ord}_{\mathfrak{p}_i} \alpha$ is odd, for $i = 1, 2, 3$; while $\text{ord}_{\mathfrak{p}} \alpha$ is even for all $\mathfrak{p} \in S - \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$, since $L_{\mathfrak{p}}$ is unimodular when $\mathfrak{p} \in S - \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$. Then we have

$$\begin{aligned}
 1 &= \prod_{\mathfrak{p} \in \Omega} |\alpha|_{\mathfrak{p}} = \prod_{\mathfrak{p} \in \Omega} \left(\frac{1}{N\mathfrak{p}} \right)^{\text{ord}_{\mathfrak{p}} \alpha} = \prod_{\mathfrak{p} \in \Omega} \left(\frac{1}{\#k} \right)^{(\deg \mathfrak{p}) \text{ord}_{\mathfrak{p}} \alpha} \\
 &= \left(\frac{1}{\#k} \right)^{\sum_{\mathfrak{p} \in \Omega} (\deg \mathfrak{p}) \text{ord}_{\mathfrak{p}} \alpha}
 \end{aligned}$$

by the product formula for global fields, and therefore $\sum_{\mathfrak{p} \in \Omega} (\deg \mathfrak{p}) \text{ord}_{\mathfrak{p}} \alpha = 0$. But $\deg \mathfrak{q} = 2$, and hence $\sum_{i=1}^3 (\deg \mathfrak{p}_i) \text{ord}_{\mathfrak{p}_i} \alpha \equiv 0 \pmod{2}$, a contradiction.

(II) Next we claim that L has no orthogonal splitting $L = L_1 \perp L_2$ in which $\text{rank } L_1 = 2$ and $d(FL_1) = 1$. Suppose there is such a splitting. For all $\mathfrak{p} \in S - \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$ the lattice $L_{\mathfrak{p}}$ is unimodular; so, from the triviality of the Hilbert symbol on the units of nondyadic local fields, the Hasse symbol equation $S_{\mathfrak{p}}(FL_1) = 1$ holds at these spots. On the other hand, for $i = 1, 2, 3$ we have

$$S_{\mathfrak{p}_i}(FL_1) = S_{\mathfrak{p}_i}(\langle \pi_i, \pi_i \rangle) = \left(\frac{\pi_i, -1}{\mathfrak{p}_i} \right) = -1.$$

Here the final equality holds because

$$[F(\mathfrak{p}_i) : k] \equiv 1 \pmod{2} \Rightarrow -1 \notin F(\mathfrak{p}_i)^2 \Rightarrow -1 \notin \dot{F}_{\mathfrak{p}_i}^2.$$

Thus $\prod_{\mathfrak{p} \in S} S_{\mathfrak{p}}(FL_1) = -1$. On the other hand, since $[F(\mathfrak{q}) : k] \equiv 0 \pmod{2}$ it follows that $-1 \in \dot{F}_{\mathfrak{q}}^2$; therefore $F_{\mathfrak{q}}L_1$ is a hyperbolic plane, and so $S_{\mathfrak{q}}(FL_1) = 1$. This contradicts the fact that every quadratic F -space U satisfies $\prod_{\mathfrak{p} \in \Omega} S_{\mathfrak{p}}U = 1$.

(III) Finally, we show that L has no orthogonal splitting $L = L_1 \perp L_2$ in which $\text{rank } L_1 = 2$. Suppose there is such a splitting. Let $\alpha = d(FL_1)$. Then $\text{ord}_{\mathfrak{p}} \alpha \equiv 0 \pmod{2}$ for all $\mathfrak{p} \in S$. In particular, we can suppose $\text{ord}_{\mathfrak{p}} \alpha = 0$ for all prime polynomials $p \neq q$; so $\alpha = \varepsilon(x^2 + 1)^\lambda$, with $\varepsilon \in k$ and $\lambda \in \{0, 1\}$.

From the uniqueness properties of the given Jordan splitting of $L_{\mathfrak{p}_1}$, it follows that $d(F_{\mathfrak{p}_1}L_1) = 1$. And $x^2 + 1 \in \dot{F}_{\mathfrak{p}_1}^2$ from our choice of \mathfrak{p}_1 . Therefore we must have $\varepsilon \in k \cap \dot{F}_{\mathfrak{p}_1}^2$. But $\deg \mathfrak{p}_1$ is odd, so in fact $\varepsilon \in k^2$. Thus $\alpha = (x^2 + 1)^\lambda$. If $\lambda = 1$ this would contradict the fact that $d(F_{\mathfrak{p}_2}L_1) = 1$ (again from uniqueness properties of Jordan splittings), since $x^2 + 1 \notin \dot{F}_{\mathfrak{p}_2}^2$. Therefore we must have $\lambda = 0$, that is, $d(FL_1) = 1$. But this contradicts part (II). ■

REMARKS. (1) The indecomposability of the lattice L in the above theorem is a consequence of the local structure of L at all $\mathfrak{p} \in S$. Therefore every lattice in the *genus* of L is indecomposable. More generally, if the genus of any lattice K of rank $n \geq 5$ over a Hasse domain contains a decomposable lattice then so does the spinor genus of K , and hence in the indefinite case K itself is decomposable. (See [G1, Theorem 2].) Therefore, in the function

field setting, when $n \geq 5$ every genus consists completely of indecomposable lattices or completely of decomposable lattices. (Indefiniteness, indeed isotropy, is automatic over function fields when $n \geq 5$.)

(2) From O'Meara's work discussed in the introduction, we know that there exist indecomposable lattices of rank 4 over any Hasse domain of a function field; and our theorem gives an indecomposable lattice of rank 6 over a Hasse domain of any rational function field in which -1 is not a square. It remains to be seen whether there exists an indecomposable of rank 5 over a suitable function field Hasse domain.

(3) It was seen in [G3] that for a set S of primes on F with $\Omega - S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$, the ideal class group $C(S) = I(S)/P(S)$ of $\mathfrak{o}(S)$ is a finite cyclic group of order $\gcd(\deg \mathfrak{p}_1, \dots, \deg \mathfrak{p}_s)$; and if $\mathfrak{p}_0 \in S$ is any prime of degree 1 then its ideal class generates $C(S)$. The Hasse domains in our theorem are of the form

$$\mathfrak{o}(S) = \mathfrak{o}(\Omega - \mathfrak{q}) = \left\{ \frac{f(x)}{(x^2 + 1)^m} \mid f(x) \in k[x], \deg f \leq 2m \right\}$$

and have class number 2. Let \mathfrak{p}_0 be the x -adic prime ideal in $\mathfrak{o}(S)$; so

$$\text{ord}_{\mathfrak{p}} \mathfrak{p}_0 = \begin{cases} 1 & \text{if } \mathfrak{p} = \mathfrak{p}_0, \\ 0 & \text{if } \mathfrak{p} \in S - \{\mathfrak{p}_0\}. \end{cases}$$

Then \mathfrak{p}_0 is not principal, and hence its ideal class generates $C(S)$, and

$$\mathfrak{p}_0^2 = \left(\frac{x^2}{x^2 + 1} \right).$$

(4) Question: Does there exist an indecomposable lattice of rank 6 over some Hasse domain of *every* global function field F in which -1 is not a square?

References

- [C-S] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, 1988.
- [G1] L. J. Gerstein, *Splitting quadratic forms over integers of global fields*, Amer. J. Math. 91 (1969), 106–134.
- [G2] —, *Unimodular quadratic forms over global function fields*, J. Number Theory 11 (1979), 529–541.
- [G3] —, *A note on splitting quadratic forms*, *ibid.* 29 (1988), 231–233.
- [K] Y. Kitaoka, *Scalar extension of quadratic lattices*, Nagoya Math. J. 66 (1977), 139–149.
- [L] T.-Y. Lam, *Serre's Conjecture*, Lecture Notes in Math. 635, Springer, 1978.
- [M-H] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Springer, 1973.
- [O'M1] O. T. O'Meara, *Introduction to Quadratic Forms*, Springer, 1963 (reprinted in 2000).

- [O'M2] O. T. O'Meara, *The construction of indecomposable positive definite quadratic forms*, J. Reine Angew. Math. 276 (1975), 99–123.
- [R] M. Rosen, *S-units and S-class groups in algebraic function fields*, J. Algebra 26 (1973), 98–108.
- [S] W. Scharlau, *Quadratic and Hermitian Forms*, Springer, 1985.
- [W] G. L. Watson, *Integral Quadratic Forms*, Cambridge Univ. Press, 1960.

Department of Mathematics
University of California
Santa Barbara, CA 93106-3080, U.S.A.
E-mail: gerstein@math.ucsb.edu

*Received on 30.9.1999
and in revised form 4.4.2000*

(3718)