9. *The Number of Embeddings of Integral Quadratic Forms. II**)

By Rick MIRANDA**) and David R. MORRISON***)

(Communicated by Kunihiko KODAIRA, M. J. A., Jan. 13, 1986)

This is a continuation of our previous note [5], to which we refer the reader for definitions and notation.

1. Introduction. Let $\phi : M \to L$ be a primitive embedding from a nondegenerate integral quadratic form M into an indefinite unimodular integral quadratic form L. In [5] we showed that the number of equivalence classes of primitive embeddings from M into L coincides with a certain invariant $e(N)$ of the orthogonal complement N of M in L. (We also proved a similar statement for (α, β)-equivalence classes and the invariant $e_{\alpha\beta}(N)$.) In this note, we give an effective procedure for calculating these invariants $e(N)$ and $e_{\alpha\beta}(N)$ when N is indefinite with rank at least three. This extends some work of Nikulin [6], who gave sufficient conditions for $e(N)$ to be 1 (under the same hypotheses on N). The proofs, together with some applications to algebraic geometry, will be given elsewhere.

2. The structure of finite quadratic forms. A *finite quadratic form* is a finite abelian group G together with a map $q : G \to \boldsymbol{Q}/\boldsymbol{Z}$ such that the induced map $b : G \times G \to \boldsymbol{Q}/\boldsymbol{Z}$ defined by $b(x, y) = q(x+y) - q(x) - q(y)$ is $\boldsymbol{Z}$-bilinear, and such that $q(nx) = n^2 q(x)$ for all $n \in \boldsymbol{Z}$ and $x \in G$. G is called *nondegenerate* if the adjoint map $\mathrm{Ad}\, b : G \to \mathrm{Hom}(G, \boldsymbol{Q}/\boldsymbol{Z})$ of the associated bilinear form b is injective.

We recall from Wall [8] and Durfee [2] the basic structure of a nondegenerate finite quadratic form G, using the notation of Brieskorn [1]. The Sylow decomposition $G = \oplus_p G_p$ is an orthogonal direct sum decomposition with respect to the form q; moreover, each Sylow subgroup G_p admits an orthogonal direct sum decomposition into groups of ranks one and two of the following types:

(i) If $p \neq 2$ and $\varepsilon = \pm 1$, $w^{\varepsilon}_{p,k}$ denotes $\boldsymbol{Z}/p^k\boldsymbol{Z}$ with a generator x such that the quadratic map is given by $q(x) = p^{-k}u \pmod{\boldsymbol{Z}}$ for some $u \in \boldsymbol{Z}$ with $(u, p) = 1$ and $\left(\frac{2u}{p}\right) = \varepsilon$, where $\left(\frac{\ }{\ }\right)$ is the Legendre symbol.

(ii) If $\varepsilon \in (\boldsymbol{Z}/8\boldsymbol{Z})^{\times}$, $w^{\varepsilon}_{2,k}$ denotes $\boldsymbol{Z}/2^k\boldsymbol{Z}$ with a generator x such that $q(x) = 2^{-k-1}u \pmod{\boldsymbol{Z}}$ for some $u \in \boldsymbol{Z}$ with $u \equiv \varepsilon \pmod 8$.

---

*) Research partially supported by the National Science Foundation and the Japan Society for the Promotion of Science.

**) Department of Mathematics, Colorado State University.

***) Research Institute for Mathematical Sciences, Kyoto University and Department of Mathematics, Princeton University.

(iii) u_k (or v_k) denotes $\boldsymbol{Z}/2^k\boldsymbol{Z}\times\boldsymbol{Z}/2^k\boldsymbol{Z}$ with a basis x, y such that $q(x)=q(y)=0$ and $q(x+y)=2^{-k} \pmod{\boldsymbol{Z}}$ (or $q(x)=q(y)=q(x+y)=2^{-k} \pmod{\boldsymbol{Z}}$).

Note that when $p\neq 2$, this implies that G_p can be diagonalized (it is a direct sum of the rank one groups $w^{\varepsilon}_{p,k}$).

When $p=2$, there are in general many ways of decomposing G_2 into an orthogonal direct sum of groups of ranks one and two. The following proposition singles out a special kind of decomposition which will be useful later.

Proposition. *A nondegenerate finite quadratic form on a 2-group G_2 has an orthogonal direct sum decomposition*

$$G_2\cong\bigoplus_{k\geq 1}(u_k^{n(k)}\oplus v_k^{m(k)}\oplus w(k))$$

such that $m(k)\leq 1$, rank $(w(k))\leq 2$, *and $w(k)$ is a sum of forms of type $w^{\varepsilon}_{2,k}$.*

The proof, which we omit, is entirely analogous to that of a lemma of Miranda [4].

A fundamental invariant of a nondegenerate finite quadratic form on a p-group G_p is the discriminant disc (G_p) introduced by Nikulin [6]. This is an element of the group $\boldsymbol{Z}_p/(\boldsymbol{Z}_p^{\times})^2$ of p-adic integers modulo squares of units; it is always defined when $p\neq 2$, and is defined for $p=2$ if and only if $w(1)=0$ for a decomposition of G_2 as in the proposition.

We recall the definition of the discriminant for the forms of ranks one and two:

(i) If $p\neq 2$, disc $(w^{\varepsilon}_{p,k})=p^k u$, where $u\in\boldsymbol{Z}_p$ with $(u, p)=1$ and $\left(\frac{u}{p}\right)=\varepsilon$.

(ii) If $k\geq 2$, disc $(w^{\varepsilon}_{2,k})=2^k u$, where $u\in\boldsymbol{Z}_2$ with $u\equiv\varepsilon \pmod 8$.

(iii) disc $(u_k)=2^{2k}$, disc $(v_k)=3\cdot 2^{2k}$.

The discriminant multiplies under direct sum, so the above data is sufficient to compute disc (G_p) from any decomposition of G_p into forms of ranks one and two.

3. The computation of $e(N)$ and $e_{\alpha\beta}(N)$. Let N be a nondegenerate integral quadratic form, let $G_N=\mathrm{Coker}\,(\mathrm{Ad}\, b: N\rightarrow \mathrm{Hom}\,(N, \boldsymbol{Z}))$ be the discriminant-form of N, which is a nondegenerate finite quadratic form, and let G_{N_p} be the p-Sylow subgroup of G. For each prime number p, we will define two invariants of N and p, which can be effectively computed once N and G_N are known. These invariants are a natural number $e_p(N)$ and a subgroup $\tilde{\Sigma}(N_p)$ of $\{+, -\}\times\{+, -\}$. We describe $\tilde{\Sigma}(N_p)$ by giving its order $f_p(N)$, and, in case the order is 2, by specifying the nontrivial element, which we call the *type*.

Definition. Let N be a nondegenerate integral quadratic form and p a prime number. Let $l(G_{N_p})$ denote the minimum number of generators of G_{N_p}, and let disc (N) denote the discriminant of N, which is the determinant of the matrix of the bilinear form b of N in any basis.

(i) If $p\neq 2$, let $\Delta=\mathrm{disc}\,(N)/\mathrm{disc}\,(G_{N_p})$. Then $e_p=e_p(N)$, $f_p=f_p(N)$, and the type of $\tilde{\Sigma}(N_p)$ (when $f_p(N)=2$) are defined by Table I.

Table I

rank $(N)-l(G_{N_p})$	$p \bmod 4$	$\left(\frac{2\Delta}{p}\right)$	e_p	f_p	type
≥ 2			1	4	
1	1	1	2	4	
		-1	2	2	$(+, -)$
	3	1	2	2	$(-, +)$
		-1	2	2	$(-, -)$
0	1		4	2	$(+, -)$
	3		4	1	

(ii) If $p=2$, choose a decomposition of G_{N_2} as in Proposition, let $s(k)=n(k)+m(k)$ for $k\geq 1$, and let $s(0)=(1/2)(\text{rank}(N)-l(G_{N_2}))$. If $s(0)=s(1)=0$ and $w(1)$ has rank 1, let

$$G'\cong\bigoplus_{k\geq 2}(u_k^{n(k)}\oplus v_k^{m(k)}\oplus w(k))$$

and define $\Delta=\text{disc}(N)/2\,\text{disc}(G')$. Then $e_2=e_2(N)$, $f_2=f_2(N)$ and the type of $\tilde{\Sigma}(N_2)$ (when $f_2(N)=2$) are defined by Table II.

Theorem. *Let N be a nondegenerate integral quadratic form which is indefinite and has rank at least 3. Let $e_p(N)$ and $\tilde{\Sigma}(N_p)$ be as defined above, and let $\tilde{\Sigma}(N)=\bigcap_p \tilde{\Sigma}(N_p)$. Then*

(i) $e_{++}(N)=\prod_p e_p(N)$. *(All but finitely many of the terms in this product are 1).*

(ii) *If $\tilde{\Sigma}(N)=\{+,-\}\times\{+,-\}$ then $e(N)=e_{\alpha\beta}(N)=e_{++}(N)$ for all $\alpha,\beta\in\{+,-\}$.*

(iii) *If $\tilde{\Sigma}(N)=\{(+,+),(\alpha,\beta)\}$ for some $(\alpha,\beta)\neq(+,+)$, then $e_{\alpha\beta}(N)=e_{++}(N)$, while $e(N)=e_{\gamma\delta}(N)=(1/2)e_{++}(N)$ for $(\gamma,\delta)\neq(\alpha,\beta),(+,+)$.*

(iv) *If $\tilde{\Sigma}(N)=\{(+,+)\}$, then $e(N)=(1/4)e_{++}(N)$ and*

$$e_{+-}(N)=e_{-+}(N)=e_{--}(N)=(1/2)e_{++}(N).$$

The proof will be given elsewhere. The main tools used in the proof are Kneser's strong approximation theorem for the spin group [3], and a refinement of the factorization theorem for local integral isometries due to O'Meara and Pollak [7].

References

[1] E. Brieskorn: Die Milnorgitter der exzeptionellen unimodularen Singularitäten. Bonner Math. Schr., vol. 150 (1983).

[2] A. H. Durfee: Bilinear and quadratic forms on torsion modules. Advances in Math., **25**, 133–164 (1977).

[3] M. Kneser: Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen. Arch. Math. (Basel), **7**, 323–332 (1956).

[4] R. Miranda: Nondegenerate symmetric bilinear forms on finite abelian 2-groups. Trans. Amer. Math. Soc., **284**, 535–542 (1984).

Table II

<table>
<tr><th>$s(0)$</th><th>$w(1)$</th><th>$s(1)$</th><th>$w(2)$</th><th>$s(2)$</th><th>$w(3)$</th><th>ε, η mod 4</th><th>Δ mod 8</th><th>e_2</th><th>f_2</th><th>type</th></tr>
<tr><td>>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>4</td><td rowspan="4"></td></tr>
<tr><td rowspan="24">0</td><td rowspan="5">$w^{\varepsilon}_{2,1}\oplus w^{\eta}_{2,1}$</td><td>$>0$</td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>4</td></tr>
<tr><td rowspan="4">0</td><td>$rk>0$</td><td></td><td></td><td></td><td></td><td>1</td><td>4</td></tr>
<tr><td rowspan="3">0</td><td rowspan="3"></td><td rowspan="3"></td><td>$\varepsilon\equiv-\eta$</td><td></td><td>1</td><td>4</td></tr>
<tr><td>$\varepsilon\equiv\eta\equiv1$</td><td></td><td>2</td><td>2</td><td>(−, +)</td></tr>
<tr><td>$\varepsilon\equiv\eta\equiv-1$</td><td></td><td>2</td><td>2</td><td>(−, −)</td></tr>
<tr><td rowspan="15">$w^{\varepsilon}_{2,1}$</td><td>>0</td><td></td><td></td><td></td><td></td><td></td><td>1</td><td>4</td><td rowspan="4"></td></tr>
<tr><td rowspan="14">0</td><td>$rk=2$</td><td></td><td></td><td></td><td></td><td>1</td><td>4</td></tr>
<tr><td rowspan="6">$w^{\eta}_{2,2}$</td><td>>0</td><td></td><td></td><td></td><td>1</td><td>4</td></tr>
<tr><td rowspan="5">0</td><td>$rk>0$</td><td></td><td></td><td>1</td><td>4</td></tr>
<tr><td rowspan="4">0</td><td rowspan="2">$\varepsilon\equiv\eta$</td><td>1, 3</td><td>2</td><td>2</td><td>(−, +)</td></tr>
<tr><td>5, 7</td><td>2</td><td>2</td><td>(−, −)</td></tr>
<tr><td rowspan="2">$\varepsilon\equiv-\eta$</td><td>3, 5</td><td>2</td><td>2</td><td>(+, −)</td></tr>
<tr><td>1, 7</td><td>2</td><td>4</td><td></td></tr>
<tr><td rowspan="7">0</td><td rowspan="2">>0</td><td rowspan="2"></td><td>$\varepsilon\equiv1$</td><td></td><td>2</td><td>2</td><td>(−, +)</td></tr>
<tr><td>$\varepsilon\equiv-1$</td><td></td><td>2</td><td>2</td><td>(−, −)</td></tr>
<tr><td rowspan="5">0</td><td rowspan="2">$rk>0$</td><td>$\varepsilon\equiv1$</td><td></td><td>2</td><td>2</td><td>(−, +)</td></tr>
<tr><td>$\varepsilon\equiv-1$</td><td></td><td>2</td><td>2</td><td>(−, −)</td></tr>
<tr><td rowspan="3">0</td><td rowspan="3"></td><td>1</td><td>4</td><td>2</td><td>(−, +)</td></tr>
<tr><td>7</td><td>4</td><td>2</td><td>(−, −)</td></tr>
<tr><td>3, 5</td><td>4</td><td>1</td><td></td></tr>
<tr><td rowspan="4">0</td><td>>0</td><td></td><td></td><td></td><td></td><td></td><td>2</td><td>2</td><td>(+, −)</td></tr>
<tr><td rowspan="3">0</td><td>$rk=2$</td><td></td><td></td><td></td><td></td><td>4</td><td>1</td><td rowspan="3"></td></tr>
<tr><td rowspan="2">$rk\leq1$</td><td>>0</td><td></td><td></td><td></td><td>4</td><td>1</td></tr>
<tr><td>0</td><td></td><td></td><td></td><td>8</td><td>1</td></tr>
</table>

[5] R. Miranda and D. R. Morrison: The number of embeddings of integral quadratic forms. I. Proc. Japan Acad., **61**A, 317–320 (1985).

[6] V. V. Nikulin: Integral symmetric bilinear forms and some of their applications. Izv. Akad. Nauk SSSR, **43**, 111–177 (1979); Math. USSR Izvestija, **14**, 103–167 (1980).

[7] O. T. O'Meara and B. Pollak: Generation of local integral orthogonal groups. Math. Z., **87**, 385–400 (1965).

[8] C. T. C. Wall: Quadratic forms on finite groups, and related topics. Topology, **2**, 281–298 (1963).