Tôhoku Math. Journ.
30 (1978), 525-535.

POLYNOMIAL INVARIANTS OF ISOMETRY GROUPS OF INDEFINITE QUADRATIC LATTICES

ROBERT V. MOODY

(Received March 8, 1977, revised August 2, 1977)

1. Introduction. There is a well known theorem of Chevalley [1] describing the ring of polynomial invariants of the Weyl group W of a complex simple Lie algebra $\mathfrak{g}$. Briefly the situation is this: Let the rank of $\mathfrak{g}$ be l and let Δ be the root system of $\mathfrak{g}$ with respect to some Cartan subalgebra. Then Δ spans an l dimensional real vector space $\boldsymbol{R}\Delta$ on which W acts as a finite linear group. By extension of the transpose action, W acts on the symmetric algebra $\mathscr{S}$ of the dual space $\boldsymbol{R}\Delta^*$. Chevalley's theorem says that the ring of W-invariant elements of $\mathscr{S}$ is generated by l algebraically independent homogeneous polynomials. The unique one of degree 2 is the quadratic form ψ on $\boldsymbol{R}\Delta$ which is due to the Killing form on $\mathfrak{g}$.

Initially we began to consider how the situation would change when Δ was an infinite root system defined by a non-singular symmetrizable Cartan matrix of non-finite type. The set-up is much the same, with ψ an indefinite quadratic form and W an infinite group acting in $\boldsymbol{R}\Delta$. The conclusions, however, are quite different, being of the form that ψ by itself generates the entire ring of invariants. Moreover it became clear that this type of result held in a considerably more general situation. If we recall that the integral span $\boldsymbol{Z}\Delta$ of Δ is a lattice in $\boldsymbol{R}\Delta$, then W is a subgroup of the group $O(\boldsymbol{Z}\Delta)$ of all isometries of $\boldsymbol{Z}\Delta$ with respect to ψ.

Suppose now that L is a lattice in a rational vector space V equipped with a non-degenerate indefinite quadratic form ψ. The type of result we obtain is that for all suitable subgroups G of the isometry group $O(L)$ of L, the ring of G-invariant polynomials on V is precisely $\boldsymbol{Q}[\psi]$. For example, this is true if $\dim V \geqq 3$ and G is any subgroup of finite index in $O(L)$ (Theorem 4.1). It is also true for a wide class of Weyl groups of infinite root systems, including all the hyperbolic root systems (Theorems 5.1 and 5.2) and we conjecture that it is in fact true for all Weyl groups arising from non-singular Cartan matrices of non-finite type.

At the center of the argument lies the celebrated theorem of Thue

This work has been assisted by the support of the National Research Council of Canada.

that if $f(x, y)$ is an irreducible integral binary form of degree $\geqq 3$ then for any $m \in \boldsymbol{Z}$ the Diophantine equation $f(x, y) = m$ has at most a finite number of solutions [4]. This explains why the results are statements about rational invariants, though it is clear this is not a restriction: that is, if K is any extension of $\boldsymbol{Q}$ and $V_K = K \otimes_Q V$ then any subgroup G of $O(L)$ is canonically a subgroup of isometries on V_K with respect to the canonical extension of ψ to V_K, and if the rational invariants of G on V are $\boldsymbol{Q}[\psi]$ then the ring of G-invariant polynomials on V_K is $K[\psi]$.

The main theorem from which everything else follows is Theorem 3.1. Its statement is full of the inductive hypotheses necessary to increase the dimension beyond 2 which is the domain of Thue's theorem. The essential content of sections 4 and 5, which are devoted to applying Theorem 3.1 to orthogonal and Weyl groups, is the establishment of suitable chains of subspaces satisfying these inductive hypotheses.

As usual it is my pleasure to thank Professor Stephen Berman for the valuable and pleasant conversations which contributed to this work.

2. Background and Notation. Let V be a finite-dimensional vector space over the rational numbers $\boldsymbol{Q}$. By a *lattice* in V we shall mean a free abelian subgroup L of $(V, +)$ whose rank is the dimension of V. If X is a subset of V, $[X]$ denotes its rational span. If $\psi: V \to \boldsymbol{Q}$ is a quadratic form on V we shall also denote by ψ the corresponding bilinear form (so that $\psi(v, w) = (\psi(v + w) - \psi(v) - \psi(w))/2$) and all the restrictions of ψ to various subsets of V. We say that the *signature* of ψ is (p, q, n) if there is an orthogonal basis $v_1, \cdots, v_l$ of $R \otimes_Q V$ such that $p + q + n = l$ and $\psi(v_i) = 1$ if $i \leqq p$, $\psi(v_i) = -1$ if $p < i \leqq p + q$ and $\psi(v_i) = 0$ if $i > p + q$. ψ is *indefinite* if $pq \neq 0$. If $e_1, \cdots, e_l$ is a base for L over $\boldsymbol{Z}$ then the *discriminant* of L is $\operatorname{disc} L = \det(\psi(e_i, e_j))$. For a subset X of V, $O(X)$ denotes the group of isometries g of V with respect to ψ for which $Xg = X$. Thus $O(V)$ is the entire orthogonal group. If L is a lattice in V then $O(L) \equiv \{g \in O(V) \mid Lg = L\} = \{g \in O(V) \mid Lg \subseteq L\}$ since $\det g = \pm 1$.

Let L be a lattice in V and set $\mathscr{S}(V)$ and $\mathscr{S}(L)$ to be the symmetric algebras of V and L over $\boldsymbol{Q}$ and $\boldsymbol{Z}$ respectively. Then $\mathscr{S}(V) = \boldsymbol{Q} \otimes_{\boldsymbol{Z}} \mathscr{S}(L)$. $f \in \mathscr{S}(L)$ is *primitive* if for all $m \in \boldsymbol{Z}$ with $m > 1$, $f \notin m\mathscr{S}(L)$. If $f \in \mathscr{S}(L)$ permits a factorization over $\mathscr{S}(V)$ then it permits one over $\mathscr{S}(L)$, and if $f = gh$ with $g, h \in \mathscr{S}(L)$ then f is primitive if and only if g and h are primitive.

With V and L as above, let V^* and L^* be the rational and $\boldsymbol{Z}$ dual spaces of V and L respectively. Then L^* is a lattice in V^*. Let $\mathscr{S} = \mathscr{S}(V^*)$ and $\mathscr{S}_L = \mathscr{S}(L^*)$ which we may view as $\boldsymbol{Q}$ and $\boldsymbol{Z}$ valued func-

tions on V and L respectively. $\mathscr{S}$ is the ring of *rational polynomial functions* on V. If $g \in \mathfrak{gl}(V)$ is any endomorphism of V, then its transpose on V^* permits an extension to an algebra homomorphism of $\mathscr{S}$. We use the symbol g throughout, though we will use right action on V and left action on $\mathscr{S}$. If g stabilizes L then g will stabilize $\mathscr{S}_L$. If G is a subgroup of $GL(V)$ then $f \in \mathscr{S}$ is a *G-invariant* if for all $g \in G$, $g \cdot f = f$. Let ψ be a quadratic form on V. Then ψ is an $O(V)$-invariant in $\mathscr{S}$. We say that a subgroup F of a group G is *cofinite* in G if the index $[G: F]$ of F in G is finite.

For background on infinite root systems and their Weyl groups one may refer to [2]. In order to establish the notation and context we will provide the barest outlines here.

Let (A_{ij}) be an $l \times l$ indecomposable symmetrizable Cartain matrix with symmetrizing matrix diag $\{\varepsilon_1, \cdots, \varepsilon_l\}$, where the $\varepsilon_i \in \boldsymbol{N}$. The root system Δ (which is said to have rank l) corresponding to (A_{ij}) lies in a free abelian group $\boldsymbol{Z}\Delta$ of rank l generated by l fundamental roots $\alpha_1, \cdots, \alpha_l$. The Weyl group W is the subgroup of $GL(\boldsymbol{Z}\Delta)$ generated by the involutions r_j $j = 1, \cdots, l$ defined through $\alpha_i r_j = \alpha_i - A_{ij}\alpha_j$ $i = 1, \cdots, l$. W acts as a group of isometries with respect to the bilinear form ψ defined by $\psi(\alpha_i, \alpha_j) = A_{ij}\varepsilon_j$. W and ψ naturally extend to actions on the rational space $\boldsymbol{Q} \otimes_{\boldsymbol{Z}} \boldsymbol{Z}\Delta$.

(A_{ij}) is of *finite type* if (A_{ij}) is the Cartan matrix of a finite dimensional semi-simple Lie algebra $\mathfrak{g}$ over $\boldsymbol{C}$. (A_{ij}) is *Euclidean* if it is singular and for all non-empty proper subsets S of $\{1, \cdots, l\}$ the submatrix $A_S = (A_{ij})_{i,j \in S}$ is of finite type. (A_{ij}) is *hyperbolic* if it is nonsingular and all the submatrices A_S are of finite or Euclidean type.

3. The Main Theorem. Let Y be a rational vector space of finite dimension m and let ψ be a quadratic form on Y. Let K be a lattice in Y and H a subgroup of the lattice-preserving elements of the orthogonal group of Y. The quadruple (Y, K, ψ, H) satisfies the hypotheses (H) if

(a) ψ is non-degenerate and indefinite;

(b) H is infinite and acts irreducibly on Y.

THEOREM 1. *Let (V, L, ψ, G) be a quadruple as above with* $\dim V = l \geqq 2$. *Suppose that there is a chain of quadruples (V_i, L_i, ψ_i, G_i) $i = l, l-1, \cdots, 2$ such that*

(i) $V_l = V \supset V_{l-1} \supset \cdots \supset V_2$, $\dim V_i = i$;

(ii) $\psi_l = \psi$ *and* $\psi_i = \psi|_{V_i}$, $L_l = L$ *and* $L_i \subseteqq L_{i+1} \cap V_i$, $G_l = G$ *and* G_i *is a subgroup of* $\{g \in G_{i+1} | L_i g \subseteq L_i\}$ *for* $i < l$;

(iii) *each quadruple (V_i, L_i, ψ_i, G_i) satisfies the hypotheses* (H).

Then for every subgroup F of finite index in G the complete ring of F-invariant polynomials on V is the ring $Q[\psi]$ generated by ψ.

We will precede the proof of this result with two partial results which do not involve the inductive hypotheses of the statement of the theorem. The second of these results is in fact the crux of the whole matter.

With the notation of the theorem, what we have to prove is that if $f \in \mathscr{S}$ and f is F-invariant, then $f \in \boldsymbol{Q}[\psi]$. Now it is clear that we only have to deal with homogeneous f and we may scale f to be primitive in $\mathscr{S}_L$. Write f as a product of irreducible factors each of which is primitive in $\mathscr{S}_L$ — say $f = p_1 \cdots p_r$. Then F must permute the set $\{\pm p_1, \cdots, \pm p_r\}$ and so the stabilizer of each p_i is a subgroup F_i which is cofinite in F, hence G. This shows that it is enough to establish that for F a cofinite subgroup of G and f an irreducible primitive homogeneous F-invariant polynomial of $\mathscr{S}_L$, $f \in Q[\psi]$.

THEOREM 2. *Let (V, L, ψ, G) be a quadruple satisfying* (H). *Then for F a cofinite subgroup of G there are no F-invariant homogeneous polynomials of degree* 1 *on V.*

PROOF. Let $f \in \mathscr{S}_L$ be an F-invariant homogeneous polynomial of degree 1. The hyperplane $X = \{v \in V \mid f(v) = 0\}$ is F-invariant and hence so is the line $X^\perp$. Since $[G: F] < \infty$, $(X^\perp)G$ is a finite set of lines $X_1, \cdots, X_s$ and it generates a G-invariant subspace of V, and hence V itself. Let F_0 be the subgroup of F fixing each of these lines ($[F: F_0] < \infty$), and let the notation be chosen so that $V = X_1 \oplus \cdots \oplus X_l$. Let $X_i = [x_i]$ and let $f(x_i) = a_i \in \boldsymbol{Q}$. Fix an i for which $a_i \neq 0$. The equation $f(x_i g) = f(x_i)$ together with $X_i g = X_i$ for all $g \in F_0$ implies x_i is fixed by F_0. Then $x_i G$ is a finite G-stable set spanning V, and so G is finite, contrary to hypothesis.

THEOREM 3. *Let (V, L, ψ, G) be a quadruple satisfying* (H) *and suppose* $\dim V = 2$. *Then for F any cofinite subgroup of G the ring of F-invariant polynomials on V is $\boldsymbol{Q}[\psi]$.*

PROOF. Let f be an irreducible F-invariant polynomial of degree 2 in $\mathscr{S}_L$ and let v_1, v_2 be a basis of V. Then for $x = x_1 v_1 + x_2 v_2$, $f(x) = Ax_1^2 + Bx_1x_2 + Cx_2^2$ and $\psi(x) = ax_1^2 + bx_1x_2 + cx_2^2$. The coefficient a is not 0 for otherwise ψ would be reducible and its linear factors would contradict Theorem 2. However $f - (A/a)\psi$ is F-invariant and reducible and so by Theorem 2 is 0. Thus $f \in \boldsymbol{Q}[\psi]$.

If f is irreducible of degree 3 or higher, then let $v \in L$, $v \neq 0$, and

let $f(v) = m \in \boldsymbol{Z}$. The set vG is infinite and hence so is vF. But for all $g \in F$ $f(vg) = (gf)(v) = f(v) = m$, contradicting Thue's theorem.

PROOF OF THEOREM 1. We may assume that $\dim V = l \geqq 3$. Let f be an irreducible homogeneous F-invariant polynomial of degree N. We use induction on l and N.

Using the subspace V_{l-1} of the hypotheses of the theorem, $V = V_{l-1} \perp [v]$. Let $e_1, \cdots, e_{l-1}$ be a basis for V_{l-1} and let the general point $x \in V$ be $\sum_{i=1}^{l-1} x_i e_i + zv$. Then $f(x) = \sum_{i=0}^{N} f_i(X) z^{N-i}$ where $f_i(X)$ is a polynomial of degree i in $x_1, \cdots, x_{l-1}$. Let $F_{l-1} = F \cap G_{l-1}$. Then $[G_{l-1}: F_{l-1}] < \infty$ and stabilizes V_{l-1} and hence $[v]$. Since $(v, v) \neq 0$, $vg = \pm v$ for all $g \in F_{l-1}$, and so the stabilizer of v in F_{l-1} is F'_{l-1} of index at most 2 in F_{l-1}. For $g \in F'_{l-1}$, $g \cdot f(x) = \sum gf_i(X) z^{N-i}$, implying $gf_i = f_i$ and so $f_i \in \boldsymbol{Q}[\psi_{l-1}]$ and is of even degree. Thus $f(X, z) = \sum_{j=0}^{[N/2]} a_j \psi_{l-1}^j(X) z^{N-2j}$, $a_j \in \boldsymbol{Q}$. If N is odd or $a_{[N/2]} = 0$, z is a factor and f is reducible. Thus $N = 2M$ and $a_M \neq 0$.

Now $\psi((X, z)) = \psi_{l-1}(X) + (v, v) z^2$. Consequently, $f(X, z) - a_M \psi((X, z))^M$ is F-invariant and has a factor of z^2 throughout. It then lies in $\boldsymbol{Q}[\psi]$ and this proves the theorem.

4. Orthogonal Groups of Lattices.

THEOREM 1. *Let V be a finite dimensional vector space over $\boldsymbol{Q}$, L a lattice in V, and ψ a non-degenerate indefinite quadratic form on V. If $\dim V \geqq 3$ or $\dim V = 2$ and $|\operatorname{disc} L|$ is not a rational square, then for all cofinite subgroups F of $O(L)$ the ring of F-invariant rational polynomial functions on V is precisely $\boldsymbol{Q}[\psi]$.*

To prove this it is sufficient to find a descending chain of quadruples as in Theorem 3.1 with $(V, L, \psi, O(L))$ at the top. We achieve this through the sequence of lemmas below. The essential feature is to show that $O(L)$ is rich enough, and it is the two dimensional case once again which lies at the bottom of the argument. Throughout, V is a finite dimensional rational space, L is a lattice in V, and ψ is a non-degenerate quadratic form on V.

LEMMA 1. *Let L^0 denote $\{x \in V | \text{for all } y \in L, \psi(x, y) \in \boldsymbol{Z}\}$. Then L^0 is a lattice in V and $(L^0)^0 = L$. If $\psi(L, L) \subseteqq \boldsymbol{Z}$ then $L^0 \supseteqq L$ and $[L^0: L]$ is finite.*

PROOF. If $\{x_1, \cdots, x_n\}$ is a base for L then the dual $\{x_1^0, \cdots, x_n^0\}$ defined by $\psi(x_i^0, x_j) = \delta_{ij}$ is a base for L^0.

LEMMA 2. *Let L', L be lattices in V with $L' \subseteqq L$ and $\psi(L, L) \subseteqq \boldsymbol{Z}$.*

Then $L'^0 \supseteq L \supseteq L'$, $O(L') = O(L'^0)$, *and the stabilizer of* L *in* $O(L')$ *is cofinite in* $O(L')$.

PROOF. For $g \in O(L')$, for $y \in L'^0$, and for all $x \in L'$, we have $\psi(x, yg) = \psi(xg^{-1}, y) \in \boldsymbol{Z}$, so $yg \in L'^0$. Thus $O(L') \subseteq O(L'^0)$. Similarly $O(L'^0) \subseteq O(L')$. It is clear that $L'^0 \supseteq L \supseteq L'$. Since $O(L')$ stabilizes L'^0 and L' it must permute the finite number of subgroups lying between them, and so the stabilizer of L in $O(L')$ is cofinite.

LEMMA 3. *Let* $L = \boldsymbol{Z}x + \boldsymbol{Z}y$ *be a lattice in* $V = \boldsymbol{Q}x \oplus \boldsymbol{Q}y$ *and suppose that* $\psi(x, x) = A$, $\psi(y, y) = -B$, $\psi(x, y) = 0$, *where* $A, B \in \boldsymbol{N}$ *and* AB *is not a square. Then* $O(L)$ *is infinite and contains a cyclic group* $\langle\sigma\rangle$ *such that for all* $k \in \boldsymbol{Z}$, $k \neq 0$, $x\sigma^k = c_k x + d_k y$, $y\sigma^k = c'_k x + d'_k y$, *where* $c_k, d_k, c'_k, d'_k \in \boldsymbol{Z}$ *and* $c_k d_k \neq 0$, $c'_k d'_k \neq 0$.

PROOF. The set $(B/A)\boldsymbol{Q}^{\times 2} \cap \boldsymbol{N}$ has a least element D. Let $D = Bk^2/Al^2$ where $k, l \in \boldsymbol{N}$, $(k, l) = 1$. Let $K = \boldsymbol{Z} + \boldsymbol{Z}\sqrt{D}$ and let $L_1 = \boldsymbol{Z}lx + \boldsymbol{Z}ky \subseteq L$. K is a quadratic lattice in $Q(\sqrt{D})$ with respect to the norm N of this field, and the mapping $\Phi: K \to L_1$ defined by $1 \mapsto lx$, $\sqrt{D} \mapsto ky$ is an isometry from (K, N) onto $(L_1, (Al^2)^{-1}\psi)$. It is well known that the group of units of the ring I of integers of $\boldsymbol{Q}(\sqrt{D})$ possesses an infinite cyclic subgroup and this is a group of isometries of the ring of integers treated as a quadratic lattice with respect to N. Since $2I \subset K \subset I$, the stabilizer of K in this cyclic group is cofinite and so again is infinite cyclic. From this we see that in turn (K, N), $(L_1, (Al^2)^{-1}\psi)$, (L_1, ψ) and (L, ψ) (last lemma) have isometries of infinite order.

The last statement is obvious since an isometry of V cannot stabilize $[x]$ or $[y]$ without being of finite order.

LEMMA 4. *Let* $a, b, c \in \boldsymbol{Z}$ *with* $abc \neq 0$. *Then there are arbitrarily large* $d \in \boldsymbol{N}$ *such that* $d^2a + b$ *and* c *lie in different square classes in* $\boldsymbol{Z}$.

PROOF. Suppose the lemma is false and that for all large d, $d^2a + b = (p(d)/q(d))^2 c$ where $p(d), q(d) \in \boldsymbol{N}$ and $(p(d), q(d)) = 1$. Then $q(d) \mid c$. Let P be the product of all the positive divisors of c. Then $P^2d^2a/c + P^2b/c = p(d)^2P^2/q(d)^2$. Let $a' = P^2a/c$, $b' = P^2b/c$, and $s(d) = p(d)P/q(d)$, all of which are integers. We have $d^2a' + b' = s(d)^2$ for all large d. Choose an odd prime p so that $p \nmid b'$ and a' is a quadratic residue modulo p [3, p. 55]. Then as d runs through $\boldsymbol{Z}$, $d^2a' + p\boldsymbol{Z}$ runs through the squares of $\boldsymbol{Z}/p\boldsymbol{Z}$, as does $(d^2a' + b') + p\boldsymbol{Z}$. Thus the squares of $\boldsymbol{Z}/p\boldsymbol{Z}$ are closed by addition of $b' + p\boldsymbol{Z}$, which is impossible since $p \nmid b'$.

LEMMA 5. *Let* U *be a subspace of* V *such that* ψ *is non-degenerate on* U. *Let* $\psi(L, L) \subseteq \boldsymbol{Z}$ *and let* L_U *be a lattice of* U *lying in* $L \cap U$.

Let G_U be a subgroup of $O(L_U)$. Then there is a cofinite subgroup G'_U of G_U which consists of restrictions of elements of $O(L)$ to L_U.

PROOF. Write $L' = L_U \perp (L_U^{\perp} \cap L)$. L' is a lattice in V and $L' \subseteqq L \subseteqq L'^0$. For $\sigma \in G_U$, let $\tilde{\sigma} = \sigma \perp 1$ be its extension an element of $O(L')$ according to the orthogonal splitting above. We know that $[O(L'): O(L') \cap O(L)]$ is finite and so the preimage S of $O(L') \cap O(L)$ in G_U under $\sim$ is a cofinite subgroup of G_U. This is the group we want.

LEMMA 6. *Let $U_1 \subset U_2 \subset \cdots \subset U_k = V$ be a chain of non-degenerate ψ subspaces of V and suppose $L_1 \subset L_2 \subset \cdots \subset L_k$ are lattices in these spaces. Suppose $\psi(L_k, L_k) \subseteqq \boldsymbol{Z}$. Let $\tau \in O(L_1)$ have infinite order. Then there is an $m \in \boldsymbol{N}$ such that for all $i = 1, 2, \cdots, k$, τ^m is the restriction to L_1 of an element of $O(L_i)$.*

PROOF. Use Lemma 5 $k - 1$ times.

LEMMA 7. *Let* $\dim V = l > 2$ *and let L be a lattice in V. Let ψ be a non-degenerate indefinite quadratic form on V such that $\psi(L, L) \subseteqq \boldsymbol{Z}$. Then there is a subspace U of V with* $\dim U = l - 1$ *such that ψ on U is non-degenerate and indefinite; and a lattice L_U of U such that $L_U \subseteqq L \cap U$ and if $l - 1 = 2$, $|\operatorname{disc} L_U|$ is not a square.*

PROOF. Let $\{v_1, \cdots, v_l\}$ be an orthogonal basis of V with $v_i \in L$ for each i. Let $\psi(v_i) = a_i \in \boldsymbol{Z}$ and choose the indexing so that $a_i > 0$ if $i \leqq m$ and $a_i < 0$ if $i > m$. By assumption $1 \leqq m < l$. Either $m > 1$ or $l - m > 1$. We may assume without loss of generality that $m > 1$. Then there is a $c \in \boldsymbol{N}$ such that $c^2 a_1 + a_2$ is not in the square class of $|a_l|$ and $c^2 a_1 + a_2 > 0$. The quadratic space $([cv_1 + v_2, v_l], \psi)$ is indefinite and contains $L_1 = \boldsymbol{Z}(cv_1 + v_2) + \boldsymbol{Z}v_l \subset L$ whose discriminant has absolute value $(c^2 a_1 + a_2)|a_l|$, which is not a square. Set $L_U = \boldsymbol{Z}(cv_1 + v_2) + \boldsymbol{Z}v_3 + \cdots + \boldsymbol{Z}v_l$.

LEMMA 8. *Let (U, ψ) be a non-degenerate indefinite quadratic space and L a lattice in U. Suppose that if* $\dim U = 2$ *then* $|\operatorname{disc} L|$ *is not a square. Let X be any subspace of U such that $X \neq (0), U$. Then there is an element of infinite order in $O(L)$ none of whose positive powers leave X-invariant.*

PROOF. If $\dim U = 2$ then U has no non-zero isotropic vectors. No isometry can stabilize a non-isotropic line in a plane without being of finite order. By Lemma 3 there is an isometry of U which has infinite order, and this will do.

If $\dim U > 2$ we consider two cases.

X is non-singular. Replacing X by $X^\perp$ if necessary, we may have $\dim X = m \geqq 2$. Let $\{u_1, \cdots, u_m\}$ be an orthogonal basis of X in $X \cap L$ and let $\{u_{m+1}, \cdots, u_l\}$ be an orthogonal basis for $X^\perp$ in $X^\perp \cap L$. Let $\psi(u_i) = a_i$. There is an $i \leqq m$ and a $j > m$ for which $a_i a_j < 0$, say $a_1 a_l < 0$. Choose $c \in \boldsymbol{N}$ so that $c^2 a_1 + a_2$ has the same sign as a_1 and $|(c^2 a_1 + a_2)a_l|$ is not a square. Then with $L_1 = \boldsymbol{Z}(c^2 a_1 + a_2) + \boldsymbol{Z}a_l$, $O(L_1)$ has an element σ of infinite order. Then after Lemma 5, for some $k \in \boldsymbol{N}$, σ^k is the restriction to L_1 of some element τ of $O(L)$. None of the powers of τ can leave $L_1 \cap X = \boldsymbol{Z}(c^2 a_1 + a_2)$ invariant.

X is singular. $X \cap X^\perp$ is non-trivial and evidently is invariant by any isometry leaving X invariant. Thus it suffices to assume that X is totally isotropic. Let $u \in X \cap L$ and choose $v \in L$ so that $\psi(v) = 0$ and $[u, v]$ is a hyperbolic plane. Let $\psi(u, v) = a$, which we can assume to be in $\boldsymbol{N}$. Let w be chosen in $[u, v]^\perp \cap L$ with $\psi(w) = b \neq 0$. Let $x = u + v$, $y = u - v$ and choose $c \in \boldsymbol{N}$ so that $2ac^2 + b$ is positive and in a different square class than $2a$. Let $L_1 = \boldsymbol{Z}(cx + w) + \boldsymbol{Z}y$ and $U_1 = [L_1]$. ψ is non-degenerate on U_1 and $|\operatorname{disc} L_1| = (2ac^2 + b)|-2a|$ which is not a square. Thus $O(L_1)$ contains an element τ of infinite order. Let $L_2 = \boldsymbol{Z}cx + \boldsymbol{Z}w + \boldsymbol{Z}y$ and $U_2 = [L_2]$. ψ is non-degenerate on U_2 and $U_2 \cap X = [u]$ since $\dim U_2 = 3$ and X is totally isotropic. By Lemma 6, for suitable $m \in \boldsymbol{N}$, τ^m is the restriction to U_1 of isometries in $O(L_2)$ and $O(L)$.

Now write $u = u_1 + u_2$ where $u_1 \in U_1$ and $u_2 \in U_2 \cap U_1^\perp$. Then if X were invariant by some power σ of τ^m, σ would leave invariant the lines $[u]$ and $[u_2]$ $(= U_2 \cap U_1^\perp)$ and so $[u_1]$. This is impossible by the same argument that began the proof of the lemma.

PROOF OF THEOREM 4.1. Using Lemma 7 we can construct a descending chain of subspaces $V_l = V \supset V_{l-1} \supset \cdots \supset V_2$ with $\dim V_i = i$ and lattices $L_l \supset L_{l-1} \supset \cdots \supset L_2$ in the V_i with $L_l = mL$ for some $m \in \boldsymbol{N}$, such that $\psi(L_i, L_i) \subseteqq \boldsymbol{Z}$ for each i, ψ is non-degenerate and indefinite on each L_i and $|\operatorname{disc} L_2|$ is not a square. Let $G_l = O(L_l) = O(L)$ and set

$$G_i = \{g \in G_{i+1} \mid (L_i)g \subseteqq L_i\} \quad \text{for} \quad i = l-1, l-2, \cdots, 2 .$$

Then using Lemmas 8 and 6 we see that for each i, G_i is infinite and acts irreducibly on V_i. The hypotheses of Theorem 3.1 now apply to the chain (V_i, L_i, ψ, G_i) thus proving our theorem.

REMARKS. The conclusions of this theorem are not true if ψ is definite or if $\dim V = 2$ and $|\operatorname{disc} L|$ is a square, even if we restrict ourselves to $O(L)$-invariants. For example if L is the lattice generated by

a root system of type B_l ($l \geqq 2$) then $O(L)$ is the corresponding Weyl group and Chevalley's theorem shows that there are l algebraically independent invariants. If $\dim V = 2$ and $|\operatorname{disc} L|$ is a square then L has two isotropic lines and $O(L)$ in an elementary 2-group of order 4. The ring of $O(L)$-invariants may be identified with the ring of symmetric polynomials whose homogeneous components have even degree, which is a polynomial ring in two variables.

5. Applications to Weyl Groups. The notation in this section is the same as that in [2]. All the basic results to which we refer are also to be found there.

THEOREM 1. *Let (A_{ij}) be an indecomposable symmetrizable $l \times l$ Cartan matrix whose associated quadratic form ψ is of signature $(l-1, 1, 0)$. Let Δ be the associated root system with a base $\alpha_1, \cdots, \alpha_l$ spanning the rational space $\boldsymbol{Q}\Delta$. Let W be the associated Weyl group with its natural action on $\boldsymbol{Q}\Delta$. Let F be a subgroup of finite index in W. Then the ring of F-invariant polynomial functions on $\boldsymbol{Q}\Delta$ is $\boldsymbol{Q}[\psi]$.*

The whole thing depends on the construction of a suitable chain of the sort hypothesized in Theorem 3.1. We carry this out by constructing symmetrizable indefinite root systems of decreasing rank.

Let Δ be a root system of rank l, with Weyl group W, and associated quadratic form ψ. Suppose that $\gamma_1, \cdots, \gamma_k \in \Delta_R$ with $\psi(\gamma_i, \gamma_j) \leqq 0$ for all $i \neq j$. Then the $k \times k$ matrix B defined by $B_{ij} = 2\psi(\gamma_i, \gamma_j)/\psi(\gamma_j, \gamma_j)$ is a Cartan matrix. If B is non-singular then the root system Δ_B defined by B is actually embedded in Δ with $\gamma_1, \cdots, \gamma_k$ playing the role of a base. Furthermore the embedding is isometric in the sense that the form on the rational span $\boldsymbol{Q}\Delta_B$ of Δ_B is precisely that induced on it from $\boldsymbol{Q}\Delta$ by restriction. The subgroup of W generated by $\{r_{\gamma_i} | i = 1, \cdots, k\}$ is isomorphic in the obvious way to the Weyl group W_B of Δ_B.

Now suppose that $k = l - 1$ and B is non-degenerate and indefinite. Let $\boldsymbol{Z}\Delta_B = \boldsymbol{Z}\gamma_1 + \cdots + \boldsymbol{Z}\gamma_k$ and let ψ_B be the quadratic form for Δ_B. Then the quadruple $(\boldsymbol{Q}\Delta_B, \boldsymbol{Z}\Delta_B, \psi_B, W_B)$ satisfies the hypotheses (H) (see Lemma 1 below). In addition $\boldsymbol{Z}\Delta_B \subseteqq \boldsymbol{Z}\Delta \cap \boldsymbol{Q}\Delta_B$, $\psi_B = \psi|_{\boldsymbol{Z}\Delta_B}$, and $W_B \subseteqq \{w \in W | (\boldsymbol{Z}\Delta_B)w \subseteqq \boldsymbol{Z}\Delta_B\}$, which is the requirement of Theorem 3.1. The Lemmas 2 and 3 show that if $l \geqq 3$ it is always possible to construct such a set $\{\gamma_1, \cdots, \gamma_{l-1}\}$.

LEMMA 1. *Let (A_{ij}) be any indecomposable symmetrizable Cartan matrix and let the notation be as in Theorem* 5.1. *Then W acts irreducibly on $\boldsymbol{Q}\Delta$.*

PROOF. Suppose $(0) \subset U \subset \boldsymbol{Q}\Delta$ were a W-invariant subspace of $\boldsymbol{Q}\Delta$.

Then for all $u \in U$ and base elements α_i we have $ur_i = u - 2(\psi(u, \alpha_i)/\psi(\alpha_i, \alpha_i))\alpha_i \in U$ and so either $\psi(u, \alpha_i) = 0$ or $\alpha_i \in U$. Thus each root α_i lies in U or in $U^\perp$ and since neither is $\boldsymbol{Q}\Delta$, neither contains the entire base. This contradicts the indecomposability of (A_{ij}) and proves the lemma.

REMARK. Let V be a real quadratic space with signature $(l-1, 1, 0)$. Then any subspace of V is of signature $(k-1, 1, 0)$, $(k, 0, 0)$ or $(k-1, 0, 1)$.

LEMMA 2. *Let (A_{ij}) be an indecomposable symmetrizable Cartan matrix of signature $(l-1, 1, 0)$. Then either there is an indecomposable subset of fundamental roots which is of type $(l-2, 1, 0)$ or (A_{ij}) is hyperbolic.*

PROOF. Suppose (A_{ij}) is not hyperbolic. Then there is a subset of $l-1$ base roots, at least one of whose indecomposable components is neither finite nor Euclidean. Let such a component be $\alpha_1, \cdots, \alpha_k$. Then by the remark above, it spans a space of signature $(k-1, 1, 0)$. Build $\alpha_1, \cdots, \alpha_k$ up step by step to an indecomposable system of rank $l-1$. At each step it remains indefinite and so the final result has signature $(l-2, 1, 0)$. This proves the lemma.

LEMMA 3. *Let (A_{ij}) be hyperbolic of rank $l > 2$. Then there is a subroot system of rank $l-1$ and signature $(l-2, 1, 0)$.*

PROOF. Suppose we can find a root $\beta \in \Delta_I^+$ and an $i \in \{1, \cdots, l\}$ such that

(1) $\psi(\beta, \beta) < 0$,

(2) the α_i-root string $\beta - k\alpha_i, \cdots, \beta, \cdots, \beta + m\alpha_i$ terminates in real roots.

Then let $\lambda = \beta - k\alpha_i$ and let S be a subset of $l-2$ elements of $\{1, \cdots, l\}$ such that $i \in S$ and $\{\alpha_j \mid j \in S\}$ is indecomposable. Let W_S be the Weyl group $\langle r_j \mid j \in S\rangle$. W_S is finite because (A_{ij}) is hyperbolic, and so λW_S has an element α_0 of least height with respect to $\alpha_1, \cdots, \alpha_l$. Then $\psi(\alpha_0, \alpha_j) \leqq 0$ for all $j \in S$ and $\{\alpha_0\} \cup \{\alpha_j \mid j \in S\}$ forms a base for a subsystem of roots of rank $l-1$. Indeed the system of roots so generated includes the elements of $\alpha_0 W_S$ and so λ, λr_i and hence β. This shows that it is indecomposable and indefinite.

We need to show that we can always find such a β. First suppose there is a Euclidean subset, say $\alpha_1, \cdots, \alpha_{l-1}$, of the fundamental roots (it is necessarily of rank $l-1$). Let ξ be the canonical null root. It involves all of $\alpha_1, \cdots, \alpha_{l-1}$ and so $\psi(\xi, \alpha_l) < 0$. Then for some real root

λ of the form $\alpha_i + n\xi$, $n \in \boldsymbol{N}$, $i < l$, we have $d \equiv 2\psi(\lambda, \alpha_l)/\psi(\alpha_l, \alpha_l) \leqq -(2l + 2)$. The α_l-string through λ is then of the form $\lambda, \lambda + \alpha_l, \cdots, \lambda - d\alpha_l$, and since there are at most 2 roots of any given length in a root string and at most l lengths for real roots, there must be a root β in the string which satisfies $\psi(\beta, \beta) < 0$. This is what we need. Now suppose there is no Euclidean subset of fundamental roots. Then choose $\beta \in \Delta_I^+$ of minimal height. There is an $i \in \{1, \cdots, l\}$ such that $\beta - \alpha_i \in \Delta_R^+$. The minimality assumption guarantees that $(\beta - \alpha_i)r_i = \beta + k\alpha_i$ with $k > 0$. In particular β is in the α_i-string through the real root $\beta - \alpha_i$. Finally $\psi(\beta, \beta) < 0$ for otherwise β is null and so writing $\beta = \sum c_j\alpha_j$, $\{\alpha_j \mid c_j \neq 0\}$ forms a Euclidean subset contrary to assumption. This completes the lemma.

This sequence of lemmas proves Theorem 5.1.

THEOREM 2. *Let (A_{ij}) be an indecomposable symmetrizable $l \times l$ Cartan matrix. Suppose (A_{ij}) is non-singular and not of finite type. For each non-empty subset S of $\{1, \cdots, l\}$ let $A_S = (A_{ij})_{i,j \in S}$. Suppose there is a chain of subsets $S_l = \{1, \cdots, l\} \supset S_{l-1} \supset \cdots \supset S_k$ such that*

(i) $|S_i| = i \quad i = k, \cdots, l$;

(ii) *each A_{S_i} is indecomposable and non-singular;*

(iii) *A_{S_k} has associated quadratic form of signature $(k - 1, 1, 0)$.*

Then in the notation of Theorem 3.1, *the ring of F-invariant polynomial functions on $\boldsymbol{Q}\Delta$ is $\boldsymbol{Q}[\psi]$.*

In particular such a chain exists if for each non-empty subset S of $\{1, \cdots, l\}$ for which A_S is indecomposable, either A_S is Euclidean or non-singular.

REFERENCES

[1] C. CHEVALLEY, Invariants of finite groups generated by reflections, Amer. J. Math., 77 (1955), 778-782.

[2] R. MOODY, Root systems of hyperbolic type, Advances in Math., (to appear).

[3] P. RIBENBOIM, Algebraic Numbers, Wiley-Interscience, New York, 1972.

[4] A. THUE, Über Annäherungswerte algebraischer Zahlen, J. Math., 135 (1909), 284-305.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF SASKATCHEWAN
SASKATOON, CANADA