*Revista Colombiana de Matemáticas*
*Volúmen VII, 1973, págs. 53 - 66*

# A NOTE ON THE ARITHMETIC OF THE ORTHOGONAL GROUP

*by*

*Nelo D.* ALLAN

The purpose of this paper is to discuss the maximality as a discrete group of the group $G_Z$ of all rational integral matrices of the Real Special Orthogonal Group $G = SO(H)$ for all unimodular integral symmetric $n$ by $n$ matrices $H$ with signature $(p+r, p)$, $p > 1$.

We prove that $N(G_Z) = G_Z$, where $N(G_Z)$ denotes the normalizer of $G_Z$ in $G$ and that there is at most one maximal discrete subgroup of $G$ which contains $G_Z$. Moreover $G_Z$ is always maximal, with exception of the case where $r$ is an odd multiple of four and $H$ is odd. It is well known that if $\Gamma$ is a maximal discrete subgroup of $G$ then $N(\Gamma) = \Gamma$ ; the above exceptions give a negative answer to the question of whether the conditions $N(\Gamma) = \Gamma$ is enough to characterize maximality.

Essentially we present complete proofs for the results anounced in [3] ; also we use, and the material overlaps with, chapter III of [4] .

1. *Preliminaries.* We shall denote by $R$ the field of all real numbers, by $Q$ the field of all rational numbers and by $Z$ the ring of all rational integers. If

$a \in Q$, ord(a) will denote the order of $2$ in $a$. For any subring $S$ of $R$, $M_n(S)$ will denote the ring of all $n$ by $n$ matrices with entries in $S$, and $GL_n(S)$, the group of units of $M_n(S)$. The determinant of a matrix $g$ will be denoted by det(g); the $n$ by $n$ identity matrix will be denote by $E_n$, or simply $E$ whenever there is no danger of confusion, and $e_{ij}$, $1 \leq i, j \leq n$, denotes the matrix with $1$ in $(i,j)$-entry, zero otherwise. ${}^t g$ is the transpose matrix of the matrix $g$. Let $H$ be an integral unimodular symmetric matrix of signature $(p+r, p)$, $n = 2p+r$, i.e., $H \in M_n(Z)$, ${}^t H = H$, and $det(H) = \pm 1$. We say that two matrices $H$ and $H'$ are integrally equivalent, $H \approx H'$, if there exists an integral unimodular matrix $U$ such that $H' = {}^t UHU$. Let $V$ be an $n$-dimensional vector space over $R$ and $\{ \varepsilon_j \}$, $j = 1, \ldots, n$, be a fixed basis for $V$; we shall identify, as usual, a vector $x \in V$ with a column matrix; the bilinear form associated to $H$ shall be written as $f(x,y) = {}^t xHy$, and we set $f(x) = f(x,x)$ for all $x \in V$. We call $(V,f)$ a quadratic space. Let $L$ be the lattice of all points in $V$ whose coordinates are integers. If $H \approx H'$, then we can regard $U$ as a change of basis of $L$ and $H$ and $H'$ as the matrices associated to the same form $f$ in different basis. We say that $H$ is even if for all $x \in L$, $f(x)$ is even; otherwise we say that $H$ is odd. Let $A$ and $B$ be respectively $r$ by $r$ and $s$ by $s$ matrices, then we shall denote by $A \perp B$ the $r+s$ by $r+s$ matrix

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}. \quad \text{We write} \quad J(a) = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}, \quad J(0) = J \quad \text{and} \quad J_p = \begin{pmatrix} 0 & E_p \\ E_p & 0 \end{pmatrix}.$$

We recall the following two results from [1].

*LEMMA 1. Given* $m > 0$ *there exists a unimodular symmetric integral* $m$ *by* $m$ *matrix* $V$ *such that* $E_m \approx V$ *and* $V \equiv J_q \perp A \mod 2$, *where* $A = J(1)$ *or* *else* $E_1$, *according to whether* $m$ *is even* $(m-2=q)$ *or odd* $(q=m-1)$. *Moreover if* $m$ *is even and if we write* $V=(v_{ij})$, *then we can find such* $V$ *with* $v_{m-1\,m-1}=m$ *and* $V\equiv V'\perp J(1)$ *modulo* $2^a$ *where* $a=\mathrm{ord}(m)$

LEMMA 2. *(Meyer) Let* $H$ *be an unimodular symmetric integral matrix with signature* $(p+r,\ p)$, $p\neq 0$.

*(a) If* $H$ *is even, then either* $r>0$ *and* $H\approx J_p\perp\phi_r$, *where* $\phi_r$ *is positive definite, even and* $r$ *is a multiple of* 8, *or* $r=0$ *and* $H\approx J_p$

*(b) If* $H$ *is odd and* $r\neq 0$, *then* $H\approx J_p\perp V_1$ *where* $V_1$ *satisfies lemma 1.*

*(c) If* $H$ *is odd and* $r=0$, *then* $H\approx J_{p-1}\perp J(1)$.

2. *The enveloping algebra of* $G_Z$. Let $O(V)$ be the group of automorphisms of $(V,f)$, $G$ be the group of all rotations in $O(V)$, i.e., $G=O^+(V)$, and $G^o$ be the connected component of $G$. Let $G_Z$ be the group of units of $L$ in $G$, i.e., the group of all $g\in G$ such that $gL=L$; with respect to the basis $\{e_i\}$, $G=SO(H)=\{g\in GL_n(R)\mid {}^tgHg=H,\ \det(g)=1\}$, $G_Z=G\cap M_n(Z)$ and $G_Q = G\cap M_n(Q)$. We have $O(V)_Z\supset G^o_Z$. If $H\approx H'$, then $G$ is isomorphic to $G'=SO(H')$ under an isomorphism which sends $G_Z$ onto $G'_Z$ and $G_Q$ onto $G'_Q$. Hence the maximality or not of $G_Z$ is preserved. It follows from lemma 2 that we may assume $H=J_q\perp V$, $m=2q+s$ where $q$ is respectively $p,p$ or $p-1$ and $V$ is respectively $\phi_r$ (or $0$) $V_1$, or $J(1)$, according to whether we are in the case (a), (b), or (c). If $\Gamma$ is any subgroup of $O(V)_Q$, then we shall denote by $A(\Gamma,Z)$ the $Z$-algebra generated by the element of $\Gamma$ in $M_n(Q)$. Although if follows from the general theory that $A(\Gamma,Z)$ is an order, if $\Gamma$ is discrete, in our case the direct calculation will automatically prove this fact. Another trivial remark is that if $H=K\perp H'$ then $O(K)$, $SO(K)$, and $O(K)^o$ can be embedded

respectively, in $O(H)$, $SO(H)$ and $O(H)^o$, the mapping being $g \to g \perp E$ where $E$ is the identity of $O(H')$; also $O(K)$ can be embedded in $SO(H)$, but now the mapping is $g \to g \perp h$ where $h \in O(H')$ and $det(g) = det(h)$. The same is valid for the corresponding groups of integral matrices. In particular this applies to our case with $K = J_q$. Moreover we have an imbedding of $A(O(K)_Z, Z)$ into $A(SO(H)_Z, Z)$ which preserves addition and multiplication, namely $g \to g \perp 0$, where $0$ is the $n-m$ by $n-m$ zero matrix, and $K$ is $m$ by $m$.

*LEMMA 3. Let* $K = SO(J_q)^o$, $n = 2q$. *Then the order* $L = A(K_Z, Z)$ *is generated by* $g - E_n$, $g \in K_Z$, *and coincides with* $M_n(Z)$.

*Proof.* First of all $D = \{g \in O(J_q) \mid g = g(A,D) = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, A \in GL_q(R)\}$ is clearly isomorphic to $GL_q(R)$; let $T = \{g \in O(J_q) \mid g = g(B) = \begin{pmatrix} E & B \\ 0 & E \end{pmatrix}, {}^tB = -B\}$ and ${}^tT = \{{}^tg \mid g \in T\}$. Clearly $D, T,$ and ${}^tT$ are connected. Hence $D_Z, T_Z,$ and ${}^tT_Z$ are subgroups of $K_Z$. Now if we take $A = E + e_{ij}$, $i \neq j$, and $B = e_{jm} - e_{mj}$, $m \neq j$, we get that $(g(A,D) - E)(g(B) - E) = e_{iq+m} \in L$, and $(g(D,A) - E)({}^tg(B) - E) = e_{i+q\, m} \in L$. Hence after interchanging indices and taking products we get that $e_{ii}$ lies in this order for all $i = 1, \dots, n$. Now $e_{ii}g(A,D)e_{jj} = e_{ij} \in L$ and so does $e_{j+q\, i+q}$. Also $e_{i+q\, m}e_{mj} = e_{i+q\, j} \in L$ and similarly $e_{i\, j+q} \in L$. Therefore $e_{ij} \in L$ for all $i,j = 1, \dots, n$.

q.e.d.

We shall decompose the matrices $g \in M_n(R)$ in 9 blocks, $g = (a_{ij})$, $i,j = 1,2,3$, in such way that $a_{11}$ and $a_{22}$ are $q$ by $q$ matrices; we let $H = (h_{ij})$, and $H^{-1} = (h'_{ij})$, $i,j = 1, 2, 3$. From ${}^tgHg = H$ if and only if $g(H^{-1})({}^tg) = H^{-1}$, we get immediately :

*LEMMA 4.* $g \in O(H)$ *if and only if either*

$$\sum_{k,m=1}^{3} {}^{t}a_{mi} b_{mk} a_{kj} = b_{ij}$$

or

$$\sum_{k,m=1}^{3} a_{im} b'_{mk} {}^{t}a_{jk} = b'_{ij} .$$

We shall consider special elements in $G$; we shall denote by $S_u(R,T)=S'_u(R',T)$ (respectively $S_l(R,T)=S'_l(R',T)$) the matrix $g$ where $a_{jj}=E$ for all $j$, $a_{32}=R$, $a_{12}=T$, $a_{13}=-{}^{t}RV=R'$ and $a_{21}=a_{31}=0$ (respectively $a_{31}=R$, $a_{21}=-T$, $a_{23}=R'$, $a_{12}=a_{13}=a_{32}=0$). They are the so called Siegel-Eichler double transvections. By $S(R,T)$ we shall denote either $S_u$ or $S_l$. If we replace $g$ by $S(R,T)$ in lemma 4 we get immediately :

*LEMMA 5.* *$S(R,T) = S'(R',T) \in O(H)$ if and only if either ${}^{t}RVR = T+{}^{t}T$, or $-R'V^{-1}\,{}^{t}R' = T + {}^{t}T$.*

The following lemma yield trivial solutions of these eqnations.

*LEMMA 6.* *$S(R,T) \in G^{o}_{Z}$ in the following cases :*

*1. $R = 2e_{ij}$ and $T = 2v_{ii}e_{jj}$.*

*2. If $2 \mid v_{ii}$, $R = e_{ij}$ and $T = (1/2)v_{ii}\,e_{jj}$ where $i = 1,\dots,q$ and $j = 1,\dots,s$ ; where $V=(v_{ij})$.*

*COROLLARY.* *$S'(R',T) \in G^{o}_{Z}$ in the following cases :*

*1. $R' = 2e_{ij}$, $T = 2w_{jj}\,e_{ii}$*

*2. If $2 \mid w_{jj}$, $R' = e_{ij}$ and $T = (1/2)\,w_{jj}\,e_{ii}$ where $i = 1,\dots,q$, where $j = 1,\dots,s$ and $V^{-1} = (w_{ij})$.*

*LEMMA 7. Assume that $2|v_{ii}$ precisely when $i = 1,\dots, s-1$. Let $R$ and*

*$T$ be integral matrices such that ${}^tRVR = T + {}^tT + aV$. If $a = 0$, then the entries in the last row of $R$ are all divisible by 2. If $a = 1$, then then same is true with the exception of the last entry of the last row of $R$ which is not divisible by 2.*

*Proof.* Let $L'$ be the set of all $x \in Z^s$ such that ${}^txVx = 0$ modulo 2; $L'$ is a $Z$-module and modulo 2 we have ${}^txVx = x_s^2\, v_{ss}$, where $x_s$ is the last coordinate of $x$; hence $2 \mid x_s$ for all $x \in L'$. In the case where $a = 0$, if $y$ denotes any column of $R$, then ${}^tRVR = T + {}^tT$ implies that ${}^tyVy = 0$ modulo 2, i.e., $y \in L'$ and hence our assertion. The same argument applies to any column of $R$, in the case where $a = 1$, with the exception of the last one; for this last column ${}^tRVR = T + {}^tT + V$ implies ${}^tyVy \equiv v_{ss} \equiv 1$ modulo 2, hence the correspondent $y_s$ is such that $y_s^2 \equiv y_s^2\, v_{ss} \equiv 1$ modulo 2. Therefore $y_s$ is odd.

q.e.d.

COROLLARY 1. *Assume that $2 \mid w_{ii}$ precisely when $i \neq m$. Let $R'$ and $T$ be integral matrices such that $R'(V^{-1})({}^tR') = T + {}^tT + aV^{-1}$. Then the same statement holds if we replace last row of $R$ by $m$-th column of $R'$.*

COROLLARY 2. *Assume that $2 \mid v_{ii}, w_{jj}$ precisely when $i \neq s$, and $j \neq m$. Then all $g \in O(H)_Z$ have, with the exception of the diagonal entries, all the entries in the last row and $(2s+m)$-th column, divisible by 2.*

*Proof.* It suffices to observe that

$${}^ta_{3i}Va_{3i} = (-{}^ta_{1i}a_{2i}) + {}^t(-{}^ta_{1i}a_{2i}) + \delta_{i3}\, V$$

and a similar equation holds for $a_{i3}$, where $\delta_{i3} = 1$ or $0$ according to whether $i = 3$ or not.

q.e.d.

We are now ready to calculate the enveloping algebra $L$ of $G_Z$. We recall that $n = 2q + s = 2p + r$.

*LEMMA 8. If $H$ es even (case (a)), then $L = M_n(Z)$. In the case where $H$ is odd we have: If $r$ is odd, then $L$ is generated by $e_{ij}$, $2e_{in}$ for all $i,j = 1, \ldots, n$, and $i,j \neq n$. If $r$ is even (cases (b), and (c) with $s = 2$), then $L$ contains the order $L^*$ generated by all $e_{ij}, 2e_{i\,n-1}, 2e_{nj}, 2e_{n\,n-1}$ and $e_{nn} + e_{n-1\,n-1}$, $i,j = 1, \ldots, n$, $i \neq n$ and $j \neq n-1$, and is contained in the order $L^{**}$ generated by $L^*$ and $e_{nn}$.*

*Proof.* From the embedding of $A(O(J_q)_Z, Z)$ into $A(G_Z, Z)$ we get by lemma 3, that $e_{ij} \in L$ for all $i, j = 1, \ldots, q$. By lemma 5 and its corollary, $S(R,T)$, $S'(R',T) \in G_Z$ if $R = e_{ij}$ or $R' = e_{mk}$ provided $2 \mid v_{ii}$, $2 \mid w_{kk}$, $m, j = 1, \ldots, q$. Our objective now is, by considering the corresponding $S_l$ and $S_\mu$ to see that $e_{2q+i\,j}$ and $e_{m\,2q+k}$ all lie in $L$ for $j, m = 1, \ldots, 2q$ and cor sequently by taking products we see that $e_{2q+i\,2q+k} \in L$ for these values of $i$ and $k$. We let $g^*_\mu = (a_{ij})$, $\mu = 1, 2, 3$, be such that $a_{\mu\mu} = E$ and $\cdot a_{ij} = 0$ otherwise; clearly $g^*_\mu \in L$, $\mu = 1, 2$ and $g^*_3 = E - g^*_1 - g^*_2 \in L$ and this implies that $g^* (S(R, T) - E) = e_{2q+i\,j}$, and $(S'(R', T) - E)\, g^* = e_{m\,2q+k}$ both lie in $L$, as desired. Now we shall study case by case.

In the case where $V$ is even, $V^{-1}$ is also even $e_{ij} \in L$ for all $i,j = 1, \ldots, n$, i.e., $L = M_n(Z)$. In the case where $r$ is odd, then lemma 1 says that we can choose $V \equiv J_k \perp E_1$ modulo 2 hence the same is true for $V^{-1}$. Consequently $v_{ii}$, $w_{ii}$ are multiple of 2 precisely when $i \neq m$. Thus $e_{ij} \in L$ for all $i,j = 1, \ldots, m-1$, and hence $e_{nn} = E - \sum_{i \neq m} e_{ii} \in L$. Now by lemma 6, $2e_{in}$ and $2e_{nj}$ lie in $L$; the corollary 2 of lemma 7 with $s = r = m$

implies that the entries of the last row and column, which are non diagonal, of all matrices in $L$ are divisible by 2, and our assertion is verified in this case. In the case that $r$ is even by using lemma 6 and products we arrive to $2e_{nj}, 2e_{i\,n-1}$ and $4e_{n\,n-1}$ all lie in $L$ for all $j, i \neq n, n-1$, and a similar argument as above shows that they are generators of $L$ with the possible exception of $4e_{n\,n-1}$. As $e_{ii} \in L$ for all $i \neq n, n-1$, we get that $e_{nn} + e_{n-1\,n-1}$ lies in $L$. It remains to prove that $2e_{n\,n-1} \in L$. If $r = 0$ this follows from the fact that $\begin{pmatrix} 1 & 0 \\ -2 & -1 \end{pmatrix} \in O(J(1))_Z$. Let now $V = {}^tUU$ ; $g \in O(E_r)$ if and only if $U^{-1}gU \in O({}^tUU)$. If $g$ is either a permutation matrix or a diagonal matrix having $\pm 1$ as diagonal entries, then for all $x \in Z^r$, ${}^txg$ differs from ${}^tx$ either by few changes of sign or by a permutation of two coordinates of $x$. Now if ${}^tx$ is the s-th row of $U^{-1}$ and $y$ is the (s-1)-th column of $U$, the $(U^{-1}gU)_{s\,s-1} = {}^txgy$. As $y$ is primitive we may assume that its first entry, $y_1$ is odd, and since $x$ is also primitive we can find $g$ such that the first element of ${}^txg$ is not divisible by 2. Hence we may assume that its first entry $x_1$ is odd. If ${}^txy$ is not divisible by 4 we are done; otherwise we consider $g' = diagonal\{-1, 1, \ldots, 1\}$ and we get that ${}^txg'y = {}^txy - 2x_1y_1$ is not divisible by 4. Completing $U^{-1}gg'U$ to an element of $SO(H)_Z$ we get and element $g$ in $G_Z$ such that ord $(g_{n-1n}) = 2$. q.e.d.

*COROLLARY 1.* $L^* \subset A(O(H))_Z \subset L^{**}$. *The generators of* $A(G^o_Z, Z)$ *and* $L^*$ *are the same with possible exception of* $2e_{n\,n-1}$, *and* $e_{nn} + e_{n-1\,n-1}$.

*Proof.* Our assertions follows from the fact all the elements used in the above proof lie in $G^o$ with the exception of the one in the last paragraph.

*Remark.* We do not know whether $e_{nn}$ lies in $L$ or not.

*COROLLARY 2.* *If $H$ is even, or if $H$ is odd and $r$ is odd, then* $L = A(O(H)_Z, Z) = A(G^o{}_Z, Z)$.

*Proof.* For all the elements used in the proof of lemma, in this case belong $G^o{}_Z$.

*COROLLARY 3.* *If $p = 1$ and $r$ is even, then* $A(G^o{}_Z, Z) \subset A(O(H)_Z, Z) \subset L'$.

*Proof.* The reason our calculation does not go through in this case is that we were not able to prove that $e_{11}, e_{22} \epsilon L$. Of course if we add these element to $L$ all the argument remains valid.

3. *Main result.* Let $\overline{G}$ denote any of the three groups $O(H)$, $G'$ or $G^o$. We are now in the position of computing all maximal discrete groups containing $\overline{G}_Z$. Let $\Gamma \subset \overline{G}_Q$ be a discrete group containing $\overline{G}_Z$; the enveloping algebra $L(\Gamma) = A(\Gamma, Z)$ of $\Gamma$ contains $L$ and is such that $(H^{-1})({}^tL(\Gamma))H = L(\Gamma)$, because $g^{-1} = (H^{-1})({}^tg)H$. Consequently our problem is the calculation of all orders $L^*$ in $M_n(Q)$ which contains $L$ and are maximal among the orders having the property $(H^{-1})({}^tL^*)H = L^*$. In the case (a) $L = M_n(Z)$, hence maximal. We shall discuss cases (b) and (c).

*LEMMA 9.* *If $r$ is odd, then $L' = M_n(Z)$. If $r$ is even, and if $L' \supset L$, then $L'$ contains $L^{**}$ and it is either $M_n(Z)$ or the order generated by $L$ and $2^{-1} e_{n-1\,n}$.*

*Proof.* We start observing that if for some $i, j, k$, $e_{ii}, e_{jj}, e_{kk} \epsilon L'$, and if $L' = (A_{ij})$, then $A_{ij}\, e_{ij} \subset L'$, and $A_{ij} A_{jk} \subset A_{ik}$. Also $e_{ii} \in L'$, implies that $A_{ii} = Z$, because $L'$ is a finitely generated $Z$-module. Consequently $A_{ij} = A_{ji} = Z$ provided that $e_{ij}, e_{ji}$ lie in $L'$. Therefore in the case (b), $r$ odd, $A_{ij} = Z$ for all $i, j \neq n$, and in the case (c),

$r$ even , $A_{ij} = Z$ for all $i, j \neq n-1$ , $n$. We shall treat first the case where $r$ is even. From $2e_{nj} \in L'$, $j \neq n-1$ we get that $e_{ji} g(2e_{nj}) = 2g_{in} e_{jj} \in L'$ for all $j \neq n, n-1$, and $i \neq n-1$ ; hence $2A_{in} \subset Z$ if $i \neq n-1$. Similarly $2A_{n-1\,j} \subset Z$, $j \neq n$ and in this case a similar argument shows that $4A_{n-1\,n} \subset Z$ . If for some $g \in L'$, $g_{nn} = a/2$ , $a$ odd, we get $e_{n-1\,n} g\, 2e_{nn-1} = ae_{n-1\,n-1} \in L'$, or $ae_{nn}$, $ae_{n-1\,n-1} \in L'$ and $(a^3/2)\, e_{nn} \in L'$ which is absurd. Hence $A_{nn} = Z$, and similarly $A_{n-1\,n-1} = Z$. Let $g \in L'$, $g_{n-1\,n} = a/4$ , $a$ odd, then $2e_{n\,n-1}\, g(e_{n-1\,n-1} + e_{nn}) = 2g_{n-1\,n-1}\, e_{n\,n-1} + (a/2)\, e_{nn}$ or $(a/2)\, e_{nn} \in L'$ which is absurd. Now from $(e_{nn} + e_{n-1\,n-1})\, ge_{in} = g_{ni} e_{nn} + g_{n-1i} e_{n-1\,n}$, $i \neq n$ , we get that $A_{ni}$, and similarly $A_{i\,n-1}$, $i \neq n-1$, are integral. If for some $g \in L'$ , $g_{n-1\,i} = a/2$ , $a$ odd , $i \neq n$ , then $(e_{n-1\,n-1} + e_{nn})\, ge_{ij} = g' = (a/2)\, e_{n-1\,j} + g_{n\,i} e_{nj} \in L'$ , $j \neq n-1$ , and we may assume that $g_{ni} = 1$ . Now $g' = H^{-1}((a/2)e_{j,n-1} + e_{jn})\, H \subset L'$ and by observing that $H = J_p \perp J_q \perp J(1)$ modulo 2 , we may choose $j$ even and greater that $2q$ , hence the $(i-1, i)$-th entry , $h_{i-1\,i}$, of $H$ is odd . Hence $(e_{i-1,i})\, g''(e_{n-1\,n-1} + e_{nn}) = (b/2)e_{i-1,\,n} + ce_{i-1,n-1} + de_{i-1\,n}$, with $b$ odd, lies in $L'$ . Now if we multiply this element by $(a/2)e_{i-1,\,i-1} + e_{n\,i-1}$ on the right, we get in $L'$ an element $(ab/4)e_{n-1,n} + \cdots$, which is impossible. Hence $A_{in}$ is integral for all $i \neq n-1$ , and similarly $A_{n-1\,j}$ is integral for all $j \neq n$. We have only one possibility left for non integral ideal which is $A_{n-1\,n}$. It is easy to see that $(1/2)e_{n-1\,n}$ and $L$ generate an order which contains $e_{n-1\,n-1}$ and $e_{nn}$.

q.e.d.

From this we immediately get :

*THEOREM 1 . Let $\bar{G}$ be either $SO(H)$ or $O(H)$ . In the cases (a) and (b) , $\bar{G}_Z$ is maximal in $\bar{G}_Q$ . In case (c) there exists at most one maximal group in $\bar{G}_Q$ containing $\bar{G}_Z$, namely $\Gamma = L' \cap \bar{G}$ .*

*THEOREM 2. Let $\overline{G}$ be either $SO(H)$ or $O(H)$. If $H$ is an integral unimodular symmetric matrix of signature $(p+r, p)$ with either $r=0$, $H$ odd and $p>2$, or $p>1$, then $N(\overline{G}_Z) = \overline{G}_Z$.*

*Proof.* By lemma 2 it suffices to discuss our three cases namely, $H$ even, $H$ odd and $m$ odd, and $H$ odd and $m$ even. If $g$ normalizes $\overline{G}_Z$, then it permutes the maximal orders containing $A(\overline{G}_Z, Z)$. If $H$ is even, or $m=r$ is odd, $M_n(Z)$ is the only maximal order containing the above order hence $g$ normalizes $M_n(Z)$. By [2], p.105 every matrix in $N(\overline{G}_Z)$ has all its entries algebraic integral and as the only units in $Q$ are $\pm 1$ and its class number is one, we get that $\overline{G}_Z$ is self normalizer. Let us study now the case where $m$ is even and $H$ odd. In this case there are three posibilities for $g$ normalizing $\overline{G}_Z$, namely either $g$ normalizes $M_n(Z)$, or $g$ normalizes $L'$ or permutes them. The first case is trivial. Let us assume first that $g$ is rational. As the group generated by $g$ and $\overline{G}_Z$ is arithmetic the only possibility for $g \in N(\overline{G}_Z)$ is $g \in L'$; in this case if we write $g = (g_{ij})$, $g^{-1} = (g'_{ij})$, then $g_{n-1\,n}$ and $g'_{n-1\,n}$ are non integral, and as $g$ normalizes $L$ we get that $(g^{-1}(2e_{n\,n-1})\,g)_{n-1\,n} = 2g_{n-1\,n}\,g'_{n-1\,n} \in Z$ which is absurd. Let $g \in N(\overline{G}_Z)$, $g = g'\sqrt{a}$, by [2], p. 122, and let $k = Q(\sqrt{a})$ and $O$ the ring of its integers. Let $L''$ be the order generated by $g$ and $L$ in $M_n(k)$. Then $L''$ is either $M_n(O)$, or the extension of $L'$ to $M_n(k)$, or a different order. In the two first cases the above arguments apply with $Z$ replaced by $O$. We write $L'' = (A''_{ij})$ and observe that $4A''_{ij}$ is always integral, hence the only possibility for a new order arises precisely when $a=2$. In this case the only possible entries of $g$ which are not in $O$ are the ones lying either in the $(n-1)$-*th* row, or in the $n$-*th* column. Proceeding like in the proof of lemma 8 we can show that $2A''_{n-1\,j}$

and $2A''_{in}$ are all integral provided that $i \neq n\text{-}1$ and $j \neq n$. Hence in the matrix $g'$ the only possible non integral entries lie in the $(n\text{-}1)$-th row and in the $n$-th column, and if we multiply this column and this row by 2 we get an integral matrix. Hence $ord\,(det(g')) \geq -2$ ; on the other hand $1 = det(g) = 2^{\lambda} det(g')$ where $n = 2\lambda$, and this implies that $\lambda \leq 2$ which is absurd.

q. e. d.

*THEOREM 3. Let $\overline{G}$ be either $SO(H)$ or $O(H)$. Let $H$ be an unimodular integral symmetric matrix of signature $(p+r, p)$ with either $r = 0$, $H$ odd and $p > 2$, or otherwise $p > 1$. If $r$ is not an odd multiple of 4, then $\overline{G}_Z$ is maximal in $\overline{G}_R$.*

*Proof.* In the case where $H$ is even, or in the case where $H$ is odd an $r$ is odd, our result is included in theorems 1 and 2, because by [2], p. 105, if $\overline{G}_Z$ is maximal in $\overline{G}_Q$, then $N(\overline{G}_Z)$ is the unique maximal arithmetic group containing $\overline{G}_Z$. If we prove that in the other case the group $\Gamma = L' \cap \overline{G}$ of theorem 1 coincides with $\overline{G}_Z$, then by the same reason, theorem 2 will imply our claims. Let $H$ be odd and $r$ even $\geq 0$ ; by lemmas 1 and 2, replacing $H$ if necessary by an integrally equivalent matrix $H = J_q \perp V$ with $V = J(1)$ if $r = 0$, or $V$ is definite and $V \equiv B \perp J(1)$ modulo 2, $B$ even, and if $V = (v_{ij})$, $i, j \neq 1, \dots, m$, then $v_{m-1\ n-1} = m$ or according to whether $V$ is definite or not. Let $g \in \Gamma$, $g$ not integral, and write in blocks $g = (a_{ij})$, $i, j = 1, 2, 3$. If $y$ denote the last column of $a_{33}$, then $y_i \in Z$, $i \neq m\text{-}1$, and $y_{m-1} = g_{n-1\ n} = a/2$, with a odd. Now if we look at the equations of $\overline{G}$, given in lemma 4, we get ${}^t a_{23} a_{13} + {}^t a_{13} a_{23} + {}^t a_{33} V a_{33} = V$, and the entries $(m,n)$ of both sides yield the following equation $({}^t a_{33} V a_{33})_{mm} = {}^t y V y + b = v_{mm}$, $b$ even, or $a^2 (v_{m-1\ m-1}/4) + a y_m v_{m\,m-1} + y_m^2 v_{mm} + b = v_{mm}$.

If $m$ is not divisible by 4 we get a contradiction since the left hand side is not integral. In the other cases $8|m$ or $m=0$, we get $y_r + y_r^2 \equiv 1$ modulo 2, which is absurd. Let now $m=4$. We consider the following matrices :

$$U = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & 0 & -1 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 2 & -1 & -2 & -1 \\ -1 & 2 & 0 & 0 \\ -2 & 0 & 4 & 1 \\ -1 & 0 & 1 & 1 \end{pmatrix}$$

$$g^* = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad U^{-1}g^*U = \begin{pmatrix} -1 & 0 & 0 & 2 \\ -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1/2 \\ -2 & 0 & -2 & 0 \end{pmatrix}$$

It is clear that ${}^tUU = V$ and that $U$ satisfies the requirement of the first part of lemma 1. Also $g^* \in SO(E_4)$ and hence $U^{-1}g^* \in SO(V)$, hence $g^{**} = diagonal\{E_{2p}, g^*\} \in SO(H)$. It is easy to see that this matrix lies in $SO(H)^o \cap L'$. Therefore $L' \cap SO(H)^o_Q \neq SO(H)^o_Z$, and $\bar{G}_Z$ is not maximal in $\bar{G}_Q$.

Next if $m=4+8s$, then $H$ is integrally equivalent to $J_{2p} \perp V'$, $V' = \phi_{8s} \perp E_4$. We let $U' = diagonal\{E_{8s}, U\}$ and we set $V^* = {}^tU'V'U' = \phi_{8s} \perp V$; clearly $V^* \equiv J_{2q} \perp J(1)$ modulo 2 hence we can proceed as in lemma 9 to get that $A(SO(H)^o_Z, Z)$ in contained in $L'$; again we can complete $U^{-1}g^*U$ to an element of $SO(H)^o \cap L'$ to get the non maximality of $SO(H)^o_Z$. Hence we proved :

*THEOREM 4. If* $r$ *is an odd multiple of* 4 *and if* $p \geq 1$, *then* $\bar{G}_Z$ *is not maximal in* $\bar{G}_Q$, *for* $\bar{G} = O(H)$, $SO(H)$, *or* $O(H)^o$. *Moreover if* $p \geq 2$, *then* $N(\bar{G}_Z) = \bar{G}_Z$, *for* $\bar{G} = O(H)$ *or* $SO(H)$.

Finally we would like to point out that the question of the maximality or not of $\bar{G}_Z$ in $\bar{G}_Q$ remains open in the cases where $p = 1$, and in the case of $SO(H)^o$, $H$ odd and $r$ even.

## *BIBLIOGRAPHY*


1. N. ALLAN, *A note on Symmetric Matrices*, Rev. Colombiana Mat., 3 (1969), 45-50.
2. N. ALLAN, *The problem of maximality of arithmetic groups*, Proc. and Symp. in Pure and Applied Math., A. M. S., IX, (1966), 104-109.
3. N. ALLAN, *A note on the arithmetic of the Orthogonal Group*, Anais da Academia Brasileira de Ciencias, 38 (1966), 243-244.
4. N. ALLAN, *Maximality of Some Arithmetic Groups*, Monografías Matemáticas, No. 9, Bogotá, 1970.



*Department of Mathematics*
*University of Wisconsin*
*Parkside, Wisconsin, U. S. A.*



*(Recibido en noviembre de 1972)*