Revista Colombiana de Matemáticas
Volumen IV (1970) págs 7 - 15

ON THE MAXIMALITY OF $Sp(L)$ IN $Sp_n(k)$

by

Nelo ALLAN

Let k be the quotient field of a Dedekind domain O, $(k \neq O)$ and let $G = Sp_n(k)$ be the Symplectic Group over k. G acts on the $2n$-dimensional vector space V. Let L be a lattice in V, and let $Sp(L)$ be the stabilizer of L in $Sp_n(k)$. Our purpose is to investigate whether or not there exists a subgroup of $Sp_n(k)$ which contains $Sp(L)$ as a subgroup of finite index. Although in several points we need only weaker assumptions, to describe our methods we shall assume that all residue class fields of k are finite. First of all we would like to point out that the O-module $A(Sp(L),O)$ generated by $Sp(L)$ in $M_n(k)$, is an order, i.e., it is a subring which is a finitely generated O-module and generates $M_n(k)$ over k. Also is $\Gamma \supset Sp(L)$ as subgroup of finite index, the O-module $A(\Gamma, O)$ is an order containing $A(Sp(L),O)$. The mapping $\sigma: g \to -J^t g J = g^{-1}$, $J = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}$ induces as involution in $M_n(k)$ i.e., an antiautomorphism of order 2 and as Γ and $Sp(L)$ are groups, σ leaves invariant both orders $A(\Gamma, O)$ and $A(Sp(L),O)$. On the other hand given a σ-invariant order L in $M_n(k)$, it is easy to see that $L \cap Sp_n(k)$ is a group which contains $Sp(L)$ as subgroup of finite index if $L \supset A(Sp(L),O)$. Our problem is then to calculate the σ-invariant orders, in particular the maximal ones, containing $A(Sp(L),O)$. We show that $A(Sp(L),O)$ is contained in precisely one maximal σ-invariant order N, and $N = A(Sp(L),O)$ if and only if the elementary divisors (see § 3) of L are square free. Consequently $Sp(L)$ is contained in at most one maximal group in $Sp_n(k)$, and it is maximal if and only if the elementary divisors of L are square free. We also give a rough estimate on the index of $Sp(L)$ in the maximal group.

1. The order $A(Sp(L),O)$.

Let k be the quotient field of a Dedekind domain O. Let $G = Sp_n(k)$ be the Symplectic Group over k, i.e., G is the group of all $2n$ by $2n$ matrices $g \in M_{2n}(k)$ such that ${}^t gJg = J$ where $J = \begin{pmatrix} 0 & E_n \\ -E_n & 0 \end{pmatrix}$, E_n being the n by n identity matrix and ${}^t g$ being the transpose matrix of g. Let $V = k^{2n}$ be the standard $2n$-dimensional vector space over k, with basis $\{ e_1, \ldots, e_{2n} \}$. If we write each vector x as a column matrix, then we have an alternating form defined by $f(x, y) = {}^t xJy$. Let $\{ a_1, \ldots, a_n \}$ be ideals in O such that a_i divides a_{i+1} for all $i = 1, \ldots, n-1$; we consider the lattice $L = Oe_1 + \ldots + Oe_n + a_1 e_{n+1} + \ldots + a_n e_{2n}$. Let $Sp(L)$ be the group of the $Sp_n(k)$ units of L, i.e., $Sp(L) = \{ g \in M_n(k) | gL = L \}$. Let $\mathbf{L}$ be an order in $M_{2n}(k)$; fixed $1 \leq i, j \leq 2n$ we shall denote by $\mathbf{L}_{ij}$ the ideal generated by the (i, j)-entry of all $g \in \mathbf{L}$. We say that $\mathbf{L}$ is a direct summand if as O-module, $\mathbf{L} = \sum_{i,j=1}^{2n} \mathbf{L}_{ij} e_{ij}$ where e_{ij} are the matrix units of $M_{2n}(k)$. This happens if in particular all $e_{ii} \in \mathbf{L}$, and in this case we must have $\mathbf{L}_{ii} = O$, otherwise by considering powers of $\mathbf{L}_{ij} e_{ij}$, $\mathbf{L}$ would not be a finite O-module. Let $g \in M_{2n}(k)$, and let us define $\sigma(g) = -J {}^t gJ$; σ is clearly an involution of the algebra $M_{2n}(k)$, and G is precisely the set of all $g \in M_{2n}(k)$ such that $g\sigma(g) = E_{2n}$. If we write the matrices $g \in M_{2n}(k)$ in four n by n blocks, say $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$, then $\sigma(g) = \begin{pmatrix} {}^t D & -{}^t B \\ -{}^t C & {}^t A \end{pmatrix}$. We say that $\mathbf{L}$ is σ-invariant if $\mathbf{L} = J {}^t\mathbf{L} J$, i.e., if for all $g \in \mathbf{L}$, $\sigma(g) \in \mathbf{L}$. Clearly if $\mathbf{L}$ is any order, then $\mathbf{L} \cap \sigma(\mathbf{L})$ is σ-invariant. If $\mathbf{L}$ is σ-invariant, then $\mathbf{L}_{ij} = \mathbf{L}_{n+j\, n+i}$, $\mathbf{L}_{n+i\, j} = \mathbf{L}_{n+j\, i}$, and $\mathbf{L}_{i\, n+j} = \mathbf{L}_{j\, n+i}$, for all $i, j = 1, \ldots, n$. If $\mathbf{L}$ is direct summand, then the converse is also true. If Δ is a subgroup of $Sp_n(k)$, then we shall denote by $A(\Delta, O)$ the O-module generated by Δ in $M_{2n}(k)$. From the fact that Δ is a group it follows that $A(\Delta, O)$ is an order and $\sigma(g) \in A(\Delta, O)$ whenever $g \in A(\Delta, O)$. If M is the order of all O-endomorphisms of a lattice L, then we shall set $End_\sigma(L) = \mathbf{M} \cap \sigma\mathbf{M}$. If a and b are fractional ideals in k, then $[a : b]$

will denote the ideal $(a/b) \cap O$. If L is σ-invariant, then $L \cap Sp_n(k)$ is a group; if, moreover, L is direct summand, then it is not true in general that $L = L'$, where $L' = A(L \cap Sp_n(k), O)$.

LEMMA 1: If $e_{ii} \in L'$, for all $i = 1, \ldots, 2n$, then $L = L'$.

PROOF: Clearly L is direct summand, and $L' \subset L$, or $L'_{ij} \subset L_{ij}$ for all (i,j). We consider elements $g = g(A,D) = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix} \in Sp_n(k)$, (i.e. $^tAD = E_n$), with $A = E_n + ae_{ij}$, $i \neq j$, $i,j = 1, \ldots, n$, and $a \in L_{ij}$; consequently $e_{ii} g e_{jj} = ae_{ij}$ lies in L', hence $L'_{ij} \supset L_{ij}$, or $L'_{ij} = L_{ij}$ and, since $L'_{ii} = O$, this is true for all $i,j = 1, \ldots, n$; by the σ-invariance we get the same result for all $i,j = n+1, \ldots, 2n$. Now we consider elements $g = g(H) = \begin{pmatrix} E & H \\ 0 & E \end{pmatrix} \in Sp_n(k)$, i.e., $^tH = H$, and choose $H = a(e_{ij} + e_{ji})$, $i,j = 1, \ldots, n$, $i \neq j$ and $a \in L_{i\,n+j} = L_{j\,n+i}$; thus $e_{ii} g e_{n+j\,n+j} = ae_{i\,n+j} \in L'$, or $L'_{i\,n+j} = L_{i\,n+j}$. Similar argument applied to $^tg(H)$, but with $a \in L_{n+i\,j} = L_{n+j\,i}$ yields $L'_{n+i\,j} = L_{n+i\,j}$, for all $i,j = 1, \ldots, n$, $i \neq j$. To complete our proof, it suffices to consider $g(H)$ and $^tg(H)$, $H = ae_{ii}$ where $a \in L_{i\,n+i}$, and $a \in L_{n+i\,i}$, respectively.

q.e.d.

Before calculating the order $A(Sp(L),O)$ we shall observe that $Sp(L) = End_\sigma(L) \cap Sp_n(k)$.

LEMMA 2: [1] The order $L = A(Sp(L),O)$ is precisely $End_\sigma(L)$; it is direct summand and

$$L_{ij} = L_{n+j\,n+i} = [a_j ; a_i] = a_i^{-1} L_{n+j\,i} = a_j L_{i\,n+j}$$

PROOF: First of all we observe that $g = g(H)$, $H = ae_{jj}$, $j = 1, \ldots, n$, $a \in a_j^{-1}$, lies in $End_\sigma(L)$ because $g^{-1} = g(-H)$, and if $x \in L$, $gx = x + ax_{n+j} e_j$ and $ax_{n+j} \in O$. Similar argument applies to $^tg(H)$ with $a \in a_j$. Consequently $L_{n+j\,j} \supset a_j$, $L_{j\,n+j} \supset a_j^{-1}$, and $a_j e_{n+j\,j}$, $a_j^{-1} e_{j\,n+j} \subset L$; hence $e_{jj} \in L$ for all $j = 1, \ldots, 2n$, L is direct summand and by lemma 1, $L = End_\sigma(L)$. Hence

1.) This lemma has been mistated in [2] p. 7.

$L_{n+j\,j} = a_j$ and $L_{j\,n+j} = a_j^{-1}$. Now let a be an ideal . Then for all x L $(ae_{ij})x$, $(ae_{n+j\;n+i})x \subset L$ if and only if ax_je_i, $ax_{n+i}e_{n+j} \subset L$, $a \subset O$ and $aa_i \subset a_j$, or equivalently $a = (a_j/a_i) \cap O = [\, a_j : a_i]$. Consequently $L_{ij} = [\, a_j : a_i]$. Finally as $(L_{ij}e_{ij})(L_{j\,n+j}e_{j\,n+j}) = L_{ij}L_{j\,n+j}e_{i\,n+j}$ and as $(L_{i\,n+i})^{-1} = L_{n+i\,i}$ we get that $L_{ij}L_{j\,n+j} = L_{i\,n+j}$ and similarly $L_{n+i\,n+j}L_{n+j\,j} = L_{n+i\,j}$. Therefore $L_{i\,n+j} = [\, a_j : a_i]\, a_j^{-1}$ and $L_{n+i\,j} = [\, a_i : a_j]\, a_j$

q. e. d.

We shall introduce the matrix notation : $\mathbf{L} = \begin{pmatrix} L_{11} \cdots L_{1n} \\ L_{n1} \cdots L_{nn} \end{pmatrix}$ and set $a_{ij} = a_i/a_j$, we get that

$$A(Sp(L), O) = \begin{pmatrix} O & a_{21} \cdots a_{n1} & a_1^{-1} & a_1^{-1} \cdots a_1^{-1} \\ O & O \cdots a_{n2} & a_1^{-1} & a_2^{-1} \cdots a_2^{-1} \\ & & & \\ O & O \cdots O & a_1^{-1} & a_2^{-1} \cdots a_n^{-1} \\ a_1 & a_2 \cdots a_n & O & O \cdots O \\ a_2 & a_2 \quad\;\; a_n & a_{21} & O \cdots O \\ & & & \\ a_n & a_n \cdots a_n & a_{n1} & a_{n2} \cdots O \end{pmatrix}$$

We say that a σ- invariant order in $M_n(k)$ is maximal if it is not properly contained in any other σ- invariant order.

THEOREM 1 : There exists at most one maximal σ- invariant order containing $\mathbf{L} = A(Sp(L), O)$, and $\mathbf{L}$ is maximal if and only if the elementary divisors of L are square free .

PROOF : Let $\mathbf{M}$ be any σ- invariant order containing $\mathbf{L}$. If $\mathbf{M} = (M_{ij})$, then $M_{ij} \supset L_{ij}$ for all $i, j = 1, \ldots, 2n$. Consequently $e_{ii} \in \mathbf{M}$, $\mathbf{M}$ is direct summand, and $M_{i\,n+i} = a_i^{-1} = (M_{n+i\,i})^{-1}$, $i = 1, \ldots, n$. Now $\mathbf{M} = J^t\mathbf{M}J$ implies that

$$[(J^tMJ)_{n+i\,n+j}e_{n+i\,n+j}](a_j e_{n+j\,j})(M_{jk}e_{jk}) = M_{ji}M_{jk}a_j e_{n+i\,k}$$

Hence $M_{ji}M_{jk}a_j \subset M_{n+i\,k}$ for all $i, j, k = 1, \ldots, n$. In particular if $i = k$ we have

$$(M_{jk})^2 a_j \subset M_{n+kk} = a_k \quad \text{or} \quad (M_{jk})^2 a_{jk} \subset O$$

Now from

$$(M_{in+j}e_{in+j})(a_j e_{n+jj}) = M_{in+j}a_j e_{ij}$$

$$(a_i^{-1}e_{in+i})(M_{n+ij}e_{n+ij}) = a_i^{-1}M_{n+ij}e_{ij}$$

and from

$$(M_{ij}e_{ij})(a_j^{-1}e_{jn+j}) = M_{ij}a_j^{-1}e_{in+j}\,,\ (a_i e_{n+ii})(M_{ij}e_{ij}) = a_i M_{ij}e_{n+ij}$$

we get that

$$M_{ij} = M_{in+j}a_j = M_{n+ij}a_i^{-1} \quad \text{for all} \quad i, j = 1, \ldots, n \qquad (1)$$

Let now $j > k$ and write $a_{jk} = b_{jk}^2 t_{jk}$ with b_{jk}, t_{jk} integral ideals such that t_{jk} is square free ; if we set $M_{jk} = P/Q$, $(P,Q) = 1$, P,Q integral ideals, then $Q^2 | a_{jk}$ or $Q | b_{jk}$, i.e., $M_{jk} \subset b_{jk}^{-1}$. If $j < k$, then $M_{jk}^2 \subset a_{kj}$ or $a_{kj} | M_{jk}^2$ hence $b_{kj}t_{kj} | M_{jk}$ or $M_{jk} \subset b_{kj}t_{kj}$. Consequently if a_{n1} is square free, then $b_{jk} = O$, $a_{jk} = t_{jk}$ and $L_{ij} = M_{ij}$ for all $i, j = 1, \ldots, n$ or σ-invariance and (1) imply $L = M$. We now define $N_{jk} = b_{jk}^{-1}$ or $N_{jk} = b_{kj}t_{kj}$ according to whether $j > k$ or $j < k$, $j, k = 1, \ldots, n$, $N_{kk} = N_{n+k\,n+k} = O$, and

$$N_{kj} = N_{n+j\,n+k} = a_j N_{kn+j} = a_k^{-1} N_{n+kj}$$

We claim that the direct sum N of $N_{ij}e_{ij}$, $i, j = 1, \ldots, 2n$ is an order. As $e_{ii} \in N$ for all $i = 1, \ldots, 2n$ it suffices to verify that $N_{ij}N_{jk} \subset N_{ik}$ for all $i, j, k = 1, \ldots, 2n$. We shall consider first the case $i, j, k = 1, \ldots, n$. We have that $i < j < k$ implies

$$b_{ki}^2 t_{ki} = a_{ki} = a_{kj} a_{ji} = (b_{ji} b_{kj})^2 \, t_{ji} t_{kj}$$

or there exists an integral ideal u_{ijk} such that

$$u_{ijk}^2 t_{ki} = t_{ji} t_{kj} , \quad b_{ji} b_{kj} u_{ijk} = b_{ki} , \quad u_{ijk} \mid t_{ji} , t_{kj} , b_{ki}$$

and consequently

$$N_{ij} N_{jk} = b_{ji} t_{ji} b_{kj} t_{kj} = u_{ijk} N_{ik}$$

and if $k < j < i$

$$N_{ij} N_{jk} = b_{ij}^{-1} \, b_{jk}^{-1} = b_{ik}^{-1} u_{kji} = u_{kji} N_{ik}$$

Next for $i < k < j$ we have

$$N_{ij} N_{jk} = t_{ki} b_{ki} (t_{jk} u_{ikj}^{-1}) = N_{ik} (t_{jk} u_{ikj}^{-1}) \ ;$$

similarly $j < k < i$ implies $N_{ij} N_{jk} = N_{ik} (t_{kj} u_{jki}^{-1})$

the two last remaining situations we get $k < i < j$ and $N_{ij} N_{jk} = N_{ik} (t_{ji} u_{kij}^{-1})$, $j < i < k$ and $N_{ij} N_{jk} = N_{ik} (t_{ik} u_{jik}^{-1})$.

Now

$$N_{ij} N_{j\,n+k} = N_{ij} a_k^{-1} N_{jk} \subset a_k^{-1} N_{ik} = N_{i\,n+k}$$

$$N_{n+i\,j} N_{jk} = a_i N_{ij} N_{jk} \subset a_i N_{ik} = N_{n+i\,k}$$

$$N_{n+i\,n+j} N_{n+j\,n+k} = N_{ji} N_{kj} \subset N_{ki} = N_{n+i\,n+k}$$

we observe that $a_{kj} N_{kj} = N_{jk}$, for if $k < j$

$$a_{kj} N_{kj} = a_{kj} b_{jk} t_{jk} = b_{jk}^{-2} t_{jk}^{-1} b_{jk} t_{jk} = b_{jk}^{-1} = N_{jk} \ ,$$

and the other case is similar.

Consequently

$$N_{i\,n+j}\,N_{n+j\,n+k} = a_j^{-1} N_{ij}N_{kj} = a_{kj}\,a_k^{-1} N_{ij}N_{kj} = a_k^{-1} N_{ij}N_{jk} \subset a_k^{-1} N_{ik} = N_{i\,n+k}$$

$$N_{n+i\,n+j}N_{n+j\,k} = a_j N_{ji}N_{jk} \subset a_i N_{ik} = N_{n+i\,k} \,.$$

Finally $M \subset N \cap \sigma(N)$ which is σ-invariant, hence if M is maximal we have $M = N \cap \sigma(N)$. It is also clear that the matrix $g(A,D)$ where $A = E + \xi^{-1} e_{ij}$ $\xi \in b_{ij} \neq O$, ${}^tDA = E$, lies in $M - L$.

q.e.d. |

2. Estimates on indices. |

From now on we shall assume that all the residue class fields with respect to the non archmedian valuations are finite. The following lemma is a corollary of lemma 1 of [1], and we shall use the same notation as in [1].

LEMMA 3: Let Δ_1 and Δ_2 be arithmetic groups in G_k such that $\Delta_2 \supset \Delta_1$. Let us assume that there exists ideals a,b,c of O such that $ab\,A(\Delta_2,O) \subset bA(\Delta_1,O) \subset M_n(O)$, and $cM_n(O) \subset A(\Delta,O)$. Then $[\Delta_2 : \Delta_1]$ is at most the cardinal of $abA(\Delta_2,O)$ *modulo* a^2bc. Moreover if G is the Symplectic Group, then if suffices to consider the number $m(\Delta_2,\Delta_1)$ of classes C in $abA(\Delta_2,O)$ *modulo* $a^2 bc$, such that for all $g \in C$, ${}^tgJg \equiv O$ *modulo* a^2b.

PROOF: If $bag_1 \equiv bag_2$ *modulo* ba^2c, $g_1, g_2 \in \Delta_2$, then $g_1^{-1}g_2 = 1 + (g_1^{-1}a)cw$, $w \in M_n(O)$, and as $g_1^{-1}a \in A(\Delta_1,O)$ we get $g_1^{-1}g_2 \in \Delta_1$; hence our first assertion. If $\Delta_2 \subset Sp_n(k)$, then for all $g \in \Delta_2$, $g^1 = abg$, we have ${}^tg'Jg' \equiv O$ *modulo* a^2b^2 and, a fortiori, ${}^tg'Jg' \equiv O$ *modulo* a^2b, and the same happens to any other element in the class of g^1 *modulo* a^2b.

q.e.d.

We remark that the number of classes $ab\,A(\Delta_2,O)$ *modulo* a^2bc is at most n^λ where λ is the number of elements in O/a^2bc.

For future reference, and complement of lemma 1 of [1], we shall prove:

LEMMA 4 : If L is an order in $M_n(O)$, then $L \cap G_k$ is a group.

PROOF : It is well known that there exists an integral ideal a in O such that $L \supset aM_n(O)$. Let L^* be a maximal O-order containing L. By lemma 1 of [1] $L^* \cap G$ is a group commensurable to G_O and $G_O(a)$; from $L^* \cap G \supset L \cap G \supset G_O(a)$, we get that $g \in L \cap G$ implies $g^m \in G_O(a)$ for some m, i.e., $g^{-1} \in g^{m-1} G_O(a) \subset L \cap G$. Hence our assertion.

q. e. d.

3. Application to maximality.

Let L be a lattice in $V \cong k^{2n}$, and $Sp(L)$ be its stabilizer in $Sp_n(k)$. By [5] p. B5, we can replace L, if necessary, by another lattice L' in such way that the maximality or not of $Sp(L)$ is preserved, and L' is the lattice considered in section 1, for conveniently chosen ideals $\{a_1, \ldots, a_n\}$; moreover $\{1, a_{21}, \ldots, a_{n1}\}$ are invariants of L called the elementary divisors of L. We have

THEOREM 2 : $Sp(L)$ is contained in at most one maximal arithmetic group Δ in $Sp_n(k)$, with index at most $m(\Delta, Sp(L))$. In particular $Sp(L)$ is maximal, as an arithmetic group, in $Sp_n(k)$, if and only if the elementary divisors of L are square free.

PROOF : If Δ is any arithmetic group containing $Sp(L)$, then $A(\Delta, O) \supset A(Sp(L), O)$. By theorem 1 we have that $A(\Delta, O) \subset N \cap \sigma(N)$ i.e., $\Delta \subset (N \cap \sigma(N)) \cap Sp_n(k) = \Delta_N$. If the elementary divisors of L are square free, then by theorem 1 $L = N \cap \sigma(N)$, hence $Sp(L) = \Delta_N$ is maximal in $Sp_n(k)$. If not, the element $g(A,D)$ in theorem 1 lies in Δ_N but not in $Sp(L)$. The estimate on $[\Delta_N : Sp(L)]$ is a consequence of lemma 3 with $a = a_{n1}$ and $b = a_1$.

q. e. d.

Closing this note we would like to remark that the group Δ_N is maximal containing $Sp(L)$ as subgroup of finite index in the case where O/a_n is finite.

REFERENCES

1. ALLAN, N. *Some non Maximal Arithmetic Groups, Revista Colombiana de Matemáticas Vol. II No. 1, 1968, p. 21/28.*
2. ALLAN, N. *Arithmetic Subgroups of Some Classical Groups. Anais da Academia Brasileira de Ciencias, 1966, Vol. 39, No. 1, p. 15/18.*
3. GUTNIK, L. *On the Extension of Integral Subgroups of Some Groups (Russian) Vestnik Leningrad Univ. Ser. Math. Mech. and Astr. Vol. 19 (1957) p. 51/79.*
4. HIJIKATA, H. *Maximal Compact Subgroups of Some p-Adic Classical Groups, yale Notes 1964.*
5. SHIMURA, G. *Arithmetic of Alternating Forms and Quaternion Hermitian Forms. J. Math. Soc. Japan 15 (1963) p. 33/65.*

Departamento de Matemáticas y Estadística
Universidad Nacional de Colombia
Bogotá, Colombia S.A.

(Recibido Octubre de 1969)