<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Arithmetic subgroups of the symplectic group</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Chahal, Jasbir Singh</td>
</tr>
<tr>
<td><strong>Citation</strong></td>
<td>Osaka Journal of Mathematics. 14(3) P.487–P.500</td>
</tr>
<tr>
<td><strong>Issue Date</strong></td>
<td>1977</td>
</tr>
<tr>
<td><strong>Text Version</strong></td>
<td>publisher</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="https://doi.org/10.18910/11337">https://doi.org/10.18910/11337</a></td>
</tr>
<tr>
<td><strong>DOI</strong></td>
<td>10.18910/11337</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Osaka University Knowledge Archive: OUKA</td>
</tr>
</tbody>
</table>

Osaka University Knowledge Archive: OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University
ARITHMETIC SUBGROUPS OF THE
SYMPLECTIC GROUP

JASBIR SINGH CHAHAL

(Received September 27, 1976)

1. Let \( k \) be a field and \( n \) a positive rational integer. The symplectic group \( \text{Sp}(n, k) \) of order \( n \) over \( k \) is the group of \( 2n \times 2n \) matrices

\[
X = \begin{pmatrix} A & B \\ C & D \end{pmatrix}
\]

over \( k \), each \( A, B, C, D \) being an \( n \times n \) matrix, such that

\[
X'JX = J,
\]

where \( X' \) denotes the transpose of the matrix \( X \) and

\[
J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix},
\]

\( E \) being \( n \times n \) unit matrix. Let \( f: k^{2n} \times k^{2n} \rightarrow k \) be the skew symmetric bilinear form associated with \( J \). Then \( \text{Sp}(n, k) \) can be identified with the group of automorphisms \( \sigma \) of \( 2n \)-dimensional vector space \( k^{2n} \), such that \( \sigma \) leaves \( f \) invariant, i.e.,

\[
f(\sigma x, \sigma y) = f(x, y)
\]

for all \( x, y \) in \( k^{2n} \). It is easy to check that \( X \) is in \( \text{Sp}(n, k) \), if and only if

\[
\begin{align*}
A'C - C'A &= 0 = B'D - D'B \\
A'D - C'B &= E
\end{align*}
\]

and for \( X \) in \( \text{Sp}(n, k) \),

\[
X^{-1} = \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix}
\]

The group \( \text{Sp}(n, k) \) is generated by the matrices of the form

\[
\begin{pmatrix} E & T \\ 0 & E \end{pmatrix}, \begin{pmatrix} U & 0 \\ 0 & U^{-1} \end{pmatrix} \text{ and } \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}
\]

(6)
where $T$ is an $n \times n$ symmetric matrix and $U$ is in $GL(n, k)$.

For real symplectic group $Sp(n, R)$, the Siegel modular group $Sp(n, Z)$ is the subgroup of $Sp(n, R)$ consisting of integral matrices. $Sp(n, Z)$ is generated by integral matrices of the form (6).

Suppose $G \subseteq GL(n, C)$ is a matrix algebraic group defined over $Q$ and let for a subring $A$ of $C$, $G(A)$ denote the group of $A$-rational points of $G$. For a positive rational integer $m$, the principal congruence subgroup $G(Z, m)$ of level $m$ is the kernel of the natural map

$$\pi: G(Z) \to G(Z/mZ).$$

Obviously, $G(Z, m)$ is a normal subgroup (of finite index) in $G(Z)$.

**Definition 1.1.** (i) Two subgroups $G_1$ and $G_2$ of a group $G$ are said to be commensurable, if $G_1 \cap G_2$ is of finite index in both $G_1$ and $G_2$.

(ii) A subgroup $\Gamma$ of $G(R)$ is said to be arithmetic, if it is commensurable with $G(Z)$.

(iii) An arithmetic subgroup of $G(R)$ containing the principal congruence subgroup of level $m$ is called an arithmetic subgroup of level $m$.

Gutnik and Pjateckii-Šapiro determined (up to conjugacy) all the maximal arithmetic subgroups of $SL(n, R)$ of a given level. Our purpose here is to determine all the maximal arithmetic subgroups of $Sp(2, R)$ of a square free level. This is done in article 5. In article 2, we have proved that the denominators of the entries of the elements of such a group are bounded, in article 3, we prove that the prime divisors of the squares of these denominators are divisors of $m$. Article 4 is purely technical.

I am indebted to Professor K.G. Ramanathan for suggesting to me this problem and to Professor S. Raghavan for his valuable suggestions.

2. Arithmetic subgroups

**Theorem 2.1.** Suppose $\Gamma$ is an arithmetic subgroup of $Sp(n, R)$ of level $m$. Then each $X=(x_{ij})$ in $\Gamma$ can be written as

$$X = 1/(\sqrt{\lambda})X_1,$$

where $X_1$ is an integral matrix and $\lambda$ is a positive integer. Further, $m^2x_{ij}$ are algebraic integers and $m^3X^2$ is an integral matrix.

**Proof.** Proof is essentially due to [4]. Because $\Gamma$ is arithmetic, $Sp_a(Z, m)$ is of finite index, say $r$ in $\Gamma$. Let $t=\Gamma \cap \Gamma^{(t)}$ the subgroup generated by the $t^{th}$ powers of elements of $\Gamma$. Then $\Gamma^{(t)}$ is a normal subgroup of $\Gamma$ and is contained in $Sp_a(Z, m)$.

Let $X=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be in $\Gamma$. We can choose a rational integer $x$ such that if
\[ X^* = \begin{pmatrix} E & xmE \\ 0 & E \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A^* & B^* \\ C^* & D^* \end{pmatrix}, \]

then \( \det(A^*) = \det(A + xmC) \neq 0 \). Because proving the first assertion for \( X \) is equivalent to proving it for \( X^* \), we can assume that \( \det(A) \neq 0 \).

For an \( n \times n \) symmetric matrix \( T \in M(n, \mathbb{Z}) \), \( \begin{pmatrix} E & tmT \\ 0 & E \end{pmatrix} \) and \( \begin{pmatrix} E & 0 \\ tmT & E \end{pmatrix} \) are in \( \Gamma^{(i)} \). Therefore,

\[
X \begin{pmatrix} E & tmT \\ 0 & E \end{pmatrix} X^{-1} \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} tmATC' & tmATA' \\ * & * \end{pmatrix},
\]

\[
X^{-1} \begin{pmatrix} E & 0 \\ tmT & E \end{pmatrix} X \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} * & * \\ tmA'TA & * \end{pmatrix}
\]

are the integral matrices and hence

\[
\begin{align*}
tmA'TA' &= (y_{ij}) \quad (i) \\
tmA'TA &= (x_{ij}) \quad (ii)
\end{align*}
\]

are in \( M(n, \mathbb{Z}) \).

Because \( \det(A) \neq 0 \), for each \( j \), there exists \( i = i(j) \), such that \( a_{ij} \neq 0 \). We put \( \lambda_j = \frac{1}{a_{ij}} \). Choosing \( T = E_{ij} \), we see that

\[
a_{rj} a_{sj} = \frac{y_{rs}}{tm}
\]

is a rational number. From (9), \( a_{ij} = a_{ij}^{(i)} \). \( \lambda_j \) with \( \lambda_j \in \mathbb{Q} \) and \( a_{ij}^{(i)} \in \mathbb{Q} \). Therefore \( A = A_1 \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_n \end{pmatrix} \), where \( A_1 \in \text{GL}(n, \mathbb{Q}) \). Now choosing \( g \) in \( \mathbb{Z} \), such that \( T = gA_1^{-1}(E_{ij} + E_{ji})A_1^{-1} \) with \( i \neq j \), is integral, we can see from (8)–(ii) that \( \lambda_i \cdot \lambda_j \in \mathbb{Q} \). Therefore \( A = 1/(\sqrt{\lambda}) \cdot A_1 \) with \( \lambda \) in \( \mathbb{Q} \) and \( A_1 \) in \( \text{GL}(n, \mathbb{Q}) \). From (7) we see again that \( tmATC' \) is in \( M(n, \mathbb{Z}) \) and hence \( C = 1/(\sqrt{\lambda}) C_1 \) with \( C_1 \) in \( M(n, \mathbb{Q}) \).

By a similar argument

\[
X^{-1} \begin{pmatrix} E & 0 \\ tmT & E \end{pmatrix} X \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} = \begin{pmatrix} -tmB'TA & * \\ * & * \end{pmatrix}
\]

is integral and hence we get \( B = 1/(\sqrt{\lambda}) B_1 \) with \( B_1 \in M(n, \mathbb{Q}) \). Using (4) we get \( D = 1/(\sqrt{\lambda}) D_1 \), \( D_1 \in M(n, \mathbb{Q}) \). Putting these together we get \( X = \frac{1}{\sqrt{\lambda}} \cdot X_1 \),

where

\[
X_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}.
\]
It is obvious that we can assume that \( \lambda \) is a positive integer and this proves the first assertion.

Now because \( \text{Sp}_n(\mathbb{Z}, m) \) is of finite index in \( \Gamma \), the characteristic roots of any \( X \) in \( \Gamma \) are algebraic integers and hence \( \text{tr}(X) \) is an algebraic integer. If \( U \) is in \( \text{SL}_n(\mathbb{Z}, m) \), \( T \in M(n, \mathbb{Z}) \) is symmetric, then

\[
\text{tr}(mUTC) = \text{tr} \begin{pmatrix} U & 0 \\ 0 & U^{-1} \end{pmatrix} \begin{pmatrix} E & mT \\ 0 & E \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} - \text{tr} \begin{pmatrix} U & 0 \\ 0 & U^{-1} \end{pmatrix} \begin{pmatrix} A & C \\ B & D \end{pmatrix}
\]

is an algebraic integer.

Taking \( U=T=E \), it follows that \( \text{tr}(mC) \) is an algebraic integer. If \( C=(c_{ij}) \), then for \( i \neq j \), taking \( U=E+mE_{ij} \) and \( T=E \), we see that

\[
m^2c_{ij} = \text{tr}(m^2E_{ij}C) = \text{tr}(m(E_{ij}+mE)EC) - \text{tr}(mC)
\]

and taking \( U=E, T=E_{ii}, \)

\[
m^2c_{ii} = \text{tr}(mE_{ii}C)
\]

are algebraic integers. Hence \( m^2C \) is a matrix of algebraic integers. Considering \( J^{-1} \Gamma J \) instead of \( \Gamma \), it is immediate that \( m^2B \) is a matrix of algebraic integers. Considering

\[
\begin{pmatrix} E & 0 \\ mE & E \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} * & * \\ C+mA & * \end{pmatrix}
\]

and

\[
\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E & 0 \\ mE & E \end{pmatrix} = \begin{pmatrix} * & * \\ C+mD & * \end{pmatrix}
\]

it follows that \( m^3A \) and \( m^3D \) are matrices of algebraic integers. Now \( m^6X^2 = \frac{m^6}{\lambda} X^2 \lambda \lambda \)

is in \( M(2n, \mathbb{Q}) \) and its entries are algebraic integers, hence because \( \mathbb{Z} \) is integrally closed, \( X^2 \) is integral.

3. Let \( \Gamma \) be an arithmetic subgroup of \( \text{Sp}(n, \mathbb{R}) \) of level \( m \). Then each \( X \) in \( \Gamma \) can be written as

\[
X = \frac{1}{\sqrt{\lambda(X)}} A(X),
\]

where \( \lambda(X) \) is a positive integer and \( A(X) \) is an integral matrix, such that the ideal generated by its entries is \( \mathbb{Z} \). Then the maps

\[
\begin{align*}
A: \Gamma & \to M(2n, \mathbb{Z}) \\
\lambda: \Gamma & \to \mathbb{Z}
\end{align*}
\]
are well defined. For a rational prime $p$, let $\alpha_p(X)=v_p(\lambda(X))$, i.e., the greatest integer $l$, such that $p^l$ divides $\lambda(X)$. Let $\alpha_p(\Gamma)\equiv l.u.b.\{\alpha_p(X)|X\in\Gamma\}$. Since $\Gamma$ is arithmetic, $\alpha_p(\Gamma)$ is a non-negative integer. In fact, by Th. 2.1, $\alpha_p(\Gamma)\leq v_p(m^p)$. In this section we prove that if $n=2$, then any prime divisor of $\lambda(X)$ for any $X$ in $\Gamma$ is a divisor of $m$.

**Lemma 3.1.** Suppose $k$ is an arbitrary field and $M=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is in $M(4, k)$ with $A, B, C, D$ two rowed square matrices, such that $A'C-C'A=0=B'D-D'B$ and $A'D-C'B=E$ with some $\beta \in k$. Then there exist $M_1$ and $M_2$ in $Sp(2, k)$, such that $M_1MM_2=\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$, each block being again a $2\times 2$ matrix.

**Proof.** Choose $P$ and $Q$ in $SL(n, k)$ such that if

$$U=\begin{pmatrix} P & 0 \\ 0 & P^{-1} \end{pmatrix} \quad \text{and} \quad V=\begin{pmatrix} Q & 0 \\ 0 & Q^{-1} \end{pmatrix},$$

then

$$UMV=\begin{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} & * \\ * & \end{pmatrix}.$$ 

If $a=b=0$, then we put $M_1=U, M_2=V$. Otherwise, if necessary, replacing $U$ and $V$ by $R$ and $VR$ respectively, where,

$$R=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

we can assume that $a \neq 0$. Multiplying on the left by

$$U_1=\begin{pmatrix} E \\ \begin{pmatrix} c_{11} & -c_{21} \\ a & \end{pmatrix} \\ \begin{pmatrix} c_{21} \\ a \end{pmatrix} \end{pmatrix}$$

we obtain

$$U_1UMV=\begin{pmatrix} (a & 0 \\ 0 & b) & * \\ * & \end{pmatrix}.$$
If \( b \neq 0 \), one can assume by multiplying on the left by

\[
\begin{pmatrix}
    E & 0 \\
    0 & 0 \\
    0 & -\frac{d}{b}
\end{pmatrix}
\]

that \( d = 0 \). The condition \( A'C - C'A = 0 \) then implies that \( c = 0 \). If \( b = 0 \), again the above condition implies that \( c = 0 \). Putting \( M_1 = U_2 U_1 U \) and \( M_2 = V \), where

\[
U_2 =
\begin{pmatrix}
    1 & 0 \\
    0 & 0 \\
    0 & 0
\end{pmatrix}
\]

the proof is complete.

**Lemma 3.2.** For a rational prime \( p \), let \( \phi_p : \mathbb{Z} \to F_p \) be the natural map and the map \( A = (a_{ij}) \to \bar{A} = (\phi_p(a_{ij})) \) induced by \( \phi_p \) from \( M(n, \mathbb{Z}) \to M(n, F_p) \) be again denoted by \( \phi_p \). If \( p \) does not divide \( m \), then

\[
\phi_p : SL_d(\mathbb{Z}, m) \to SL(n, F_p)
\]

is surjective. Hence if \( k = F_p \) in lemma 3.1, then there exist \( L_i \) in \( Sp_2(\mathbb{Z}, m) \), such that \( \phi_p(L_i) = M_i \), \( i = 1, 2 \).

Proof. It is enough to remark that \( SL(n, F_p) \) is generated by the matrices of the form \( E + xE_{ij}, i \neq j \) and \( x \in F_p \).

**Theorem 3.3.** Suppose \( \Gamma \) is an arithmetic subgroup of \( Sp(2, R) \) of level \( m \). If for a rational prime \( p \), \( \alpha_p(\Gamma) > 0 \), then \( p \) divides \( m \).

Proof. Suppose \( p \) does not divide \( m \). Let \( X \in \Gamma \), such that \( \alpha_p(X) > 0 \). By lemma 3.2, there exist \( L_1 \) and \( L_2 \) in \( Sp_2(\mathbb{Z}, m) \) such that \( \phi_p(L_1 A(X) L_2) = M_1 A(X) M_2 = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \). Because \( A(X) \neq 0 \), we can assume that \( A \neq 0 \). Let \( P, Q \in SL_2(\mathbb{Z}, m) \), such that \( P \bar{A} Q = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \) with \( a_i \neq 0 \). If

\[
U = \begin{pmatrix} P & 0 \\ 0 & P^{-1} \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} Q & 0 \\ 0 & Q^{-1} \end{pmatrix},
\]

we put \( L = U L_1 A(X) L_2 V \). Then

\[
L = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} * \\ * \end{pmatrix}
\]
with \( a_i \neq 0 \). If \( Y = 1 / (\sqrt{\lambda(X)})L \), we can see that \( Y \) is in \( \Gamma \). Hence \( \alpha_p(Y') > v_p(m^p) \), for a sufficiently large \( l \) and this is a contradiction.

4. Suppose \( p \) is a rational prime, such that \( \alpha_p(\Gamma) > 0 \). We define

\[
\Sigma_p(\Gamma) = \{ A(X) | X \in \Gamma \text{ and } \alpha_p(X) > 0 \}
\]

and

\[
\Sigma_p^*(\Gamma) = \{ A(X) | X \in \Gamma, \alpha_p(X) = \alpha_p(\Gamma) \}.
\]

Obviously, \( \Sigma_p^*(\Gamma) \subseteq \Sigma_p(\Gamma) \). We have written each \( X \) in \( \Gamma \) uniquely as

\[
X = \frac{1}{\sqrt{\lambda(X)}} A(X),
\]

where \( \lambda(X) \) is a positive integer and the ideal generated by the coefficients of \( A(X) \) over \( \mathbb{Z} \) is \( \mathbb{Z} \) itself. Let \( A(X) \in \Sigma_p^*(\Gamma) \) and \( A(Y) \in \Sigma_p(\Gamma) \). Then

\[
XY = \frac{1}{\sqrt{\lambda(X) \cdot \lambda(Y)}} A(X) \cdot A(Y) \in \Gamma.
\]

Since

\[
\alpha_p(\Gamma) = \alpha_p(X) = v_p(\lambda(X)) \geq v_p(\lambda(Y)) = \alpha_p(Y) > 0,
\]

we have \( v_p(\lambda(X) \cdot \lambda(Y)) > \alpha_p(\Gamma) \). In view of (\(*\)), \( p \) has to divide the ideal generated by the coefficients of \( A(X)A(Y) \), otherwise \( \alpha_p(XY) > \alpha_p(\Gamma) \). Therefore,

\[
\phi_p(\Sigma_p^*(\Gamma)) = \phi_p(\Sigma_p(\Gamma)) = 0.
\]

Consider the 4-dimensional vector space \( V = F_p^4 \). Let \( V_p(\Gamma) \) be the subspace of \( V \) generated by \( \phi_p(\Sigma_p(\Gamma)) \) over \( F_p \). Then \( \alpha_p(\Gamma) > 0 \) implies that

\[
0 < \dim V_p(\Gamma) < 4.
\]

We need to get some more informations about \( V_p(\Gamma) \). For any field \( k \), let us denote by \( Sp(n, k)_0 \) the subgroup of \( Sp(n, k) \) generated by the elements of the form

\[
\begin{pmatrix} E & T \\ 0 & E \end{pmatrix}, \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} U & 0 \\ 0 & U^{-1} \end{pmatrix},
\]

where \( T \) is an \( n \times n \) symmetric matrix over \( k \) and \( U \in SL(n, k) \).

**Lemma 4.1.** Suppose \( \sigma \) is in \( Sp(2, F_p)_0 \) and \( \begin{pmatrix} A & B \\ C & D \end{pmatrix} \) is in \( \sigma^{-1} \Sigma_p(\Gamma) \sigma \). Then \( \begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix} \) is also in \( \sigma^{-1} \Sigma_p(\Gamma) \sigma \).
Proof. This lemma is a trivial consequence of (5). It is easy to check that 
\( \phi_p(Sp(2, \mathbb{Z})) \) contains \( Sp(2, F_p) \). If \( F \) is in \( Sp(2, \mathbb{Z}) \), such that \( \phi_p(F)=\sigma \), then

\[
\begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix} = F^{-1}A(X^{-1})F = \sigma^{-1}A(X^{-1})\sigma
\]
and \( A(X^{-1}) \) is in \( \Sigma_p(\Gamma) \).

**Lemma 4.2.** If \( \alpha_p(\Gamma)=1 \), then \( \dim V_p(\Gamma)=2 \). If \( \alpha_p(\Gamma)>1 \), then \( \dim V_p(\Gamma)\leq 2 \). If \( \dim V_p(\Gamma)=2 \), then \( V_p(\Gamma) \) is not a hyperbolic space (with respect to the skew symmetric bilinear form \( f \) associated with \( J \)). Hence there exists \( \sigma \) in \( Sp(2, F_p) \), such that if \( \alpha_j=\sigma(e_j) \), where

\[
e_j = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad e_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}
\]

is the standard basis for \( V \), then \( V_p(\Gamma)=\bigoplus_{j=1}^{\dim V_p(\Gamma)} F_p\alpha_j \).

Proof. We have already seen that \( 4>\dim V_p(\Gamma)>0 \). We first rule out the case \( \dim V_p(\Gamma)=3 \). If \( \dim V_p(\Gamma)=3 \), then \( V_p(\Gamma) \) contains a hyperbolic subspace, say \( \langle \alpha_1, \alpha_3 \rangle \), such that there exists another hyperbolic subspace \( \langle \alpha_2, \alpha_4 \rangle \) with

\[
V = \langle \alpha_1, \alpha_3 \rangle \perp \langle \alpha_2, \alpha_4 \rangle \tag{13}
\]
and \( V_p(\Gamma)=\bigoplus_{j=1}^{3} F_p\alpha_j \). Now \( V \) can also be written as

\[
V = \langle e_1, e_3 \rangle \perp \langle e_2, e_4 \rangle \tag{14}
\]
as an orthogonal sum of hyperbolic spaces; the linear transformation defined by

\[
\sigma(e_j) = \alpha_j \tag{15}
\]
leaves \( f \) invariant. Any \( \sigma \in Sp(2, k) \) for an arbitrary field \( k \) can be written as \( \sigma=\alpha_1 \cdot \sigma_2 \), where \( \sigma_1 \) is the product of the matrices of the form \( \begin{pmatrix} E & T \\ 0 & E \end{pmatrix} \) and

\[
\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}, \quad T \in M(2, k) \text{ is symmetric and } \sigma_2 = \begin{pmatrix} U & 0 \\ 0 & U^{-1} \end{pmatrix}, \quad \text{with } U \in GL(2, k).
\]
Hence there exists \( \sigma^* \in Sp(n, k)_0 \) and \( \beta \in k^* \), such that \( \sigma(e_j) = \beta_1 \cdot \sigma^*(e_i) \). Therefore, we can assume that \( \sigma \) appearing in (15) is in \( Sp(2, F_p)_0 \). From (12) it follows that for any \( A(X) \) in \( \Sigma_p(\Gamma) \), \( \sigma^{-1}(A(X)\sigma)(e_j)=0 \) for \( j=1, 2, 3 \). Hence
By lemma 4.1 for each $A(X)$ in $\Sigma_p(\Gamma)$,

$$\sigma^{-1}A(X)\sigma = \begin{pmatrix} 0 & 0 & 0 & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & * \end{pmatrix}. $$

Now dimension of $F_p$-subspace generated by $\sigma^{-1}\Sigma^*_p(\Gamma)\sigma$ is equal to $\dim V_p(\Gamma) = 3$ which is a contradiction.

Now we suppose that $\alpha_p(\Gamma) = 1$ and $\dim V_p(\Gamma) = 1$. For a suitable $\alpha_1$ in $V_p(\Gamma)$, we write $V$ as in (13) and define $\sigma$ by (15). Then for each $A(X)$ in $\Sigma^*_p(\Gamma)$,

$$\sigma^{-1}A(X)\sigma = (0 \ C_2 \ C_3 \ C_4),$$

where $C_i:=\begin{pmatrix} c_{i1} \\ c_{i2} \\ c_{i3} \\ c_{i4} \end{pmatrix}$ and $C_i:=\gamma C_j$ for some $\gamma$ in $F_p$. Choosing $\sigma_0$ suitably in $Sp(2, F_p)\sigma$ and replacing $\sigma$ by $\sigma \cdot \sigma_0$, we can assume that

$$\sigma^{-1}A(X)\sigma = \begin{pmatrix} x & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad x \neq 0. \quad (16)$$

If $X$ is in $\Gamma$, such that $\alpha_p(X) = 1$, it follows that $\det(X) = 1$ is divisible by $p$, a contradiction.

Finally, we prove that if $\dim V_p(\Gamma) = 2$, then it is not a hyperbolic space. Suppose it is. Then $V_p(\Gamma) = \langle \alpha_1, \alpha_3 \rangle$ and $V = \langle \alpha_1, \alpha_3 \rangle \perp \langle \alpha_2, \alpha_4 \rangle$ and $\sigma$ defined by $\sigma(e_j) = \alpha_j$ leaves $f$ invariant. Thus each element of $\sigma^{-1}\Sigma^*_p(\Gamma)\sigma$ is of the form

$$\begin{pmatrix} (0 \ 0) & (0 \ 0) \\ (0 \ *) & (0 \ *) \\ (0 \ 0) & (0 \ 0) \\ (0 \ *) & (0 \ *) \end{pmatrix}.$$ 

We choose $\sigma$ in such a fashion that there exists $\sigma^{-1}A(X)\sigma$ in $\sigma^{-1}\Sigma^*_p(\Gamma)\sigma$ with 0 in the $(4, 4)^{th}$ entry. But this can be seen to contradict the fact
\[ \sigma^{-1}(A(X)\sigma)^2 = 0. \]

and this proves the lemma.

Let \( \sigma \) be as in Lemma 4.2. Then for all \( A(X) \) in \( \Sigma_\phi(\Gamma) \),

\[ \sigma^{-1}A(X)\sigma = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} \quad (17) \]
each block being \( 2 \times 2 \) matrix.

**Lemma 4.3.** Suppose \( \alpha_\phi(\Gamma) > 2 \). Then there exists an \( F \) in \( Sp(2, \mathbb{Z}) \), such that if \( \Gamma \neq F^{-1}\Gamma F \), then

(i) For each \( X \) in \( \Gamma \) with \( \alpha_\phi(X) = \alpha_\phi(\Gamma) \),

\[ A(X) = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \]

with \( C \equiv 0 \pmod{\phi} \) and \( A \equiv D \equiv 0 \pmod{\phi} \).

(ii) \( \Gamma \) contains \( Sp_2(\mathbb{Z}, m) \).

**Proof.** Let \( \sigma \) be given by lemma 4.2 and \( F \in Sp(2, \mathbb{Z}) \), such that \( \phi_\phi(F) = \sigma \).

(i) Let \( \dim V_\phi(\Gamma) = 2 \). We fix \( A(X_0) = \begin{pmatrix} pA_0 & B_0 \\ pC_0 & pD_0 \end{pmatrix} \) in \( \Sigma_\phi^*(\Gamma) \); \( A_0, B_0, C_0, D_0 \) being integral matrices. We can find \( T \in SL(2, \mathbb{Z}) \), such that if \( \sigma_0 = \phi_\phi(T) \), then \( \sigma_0^{-1}B_0 \sigma_0 = \begin{pmatrix} b_1 & 0 \\ b_2 & b_2 \end{pmatrix} \), \( b_1 \neq 0 \). Therefore, if necessary, replacing \( F \) by

\[ FT^{-1} \]

(17) still holds and we can assume that

\[ A(X_0) = \begin{pmatrix} pA_0 & \begin{pmatrix} b_1^{(2)} \\ b_2^{(2)} \end{pmatrix} \\ pC_0 & \begin{pmatrix} b_1^{(2)} \\ b_2^{(2)} \end{pmatrix} \end{pmatrix} \]

with \( p \) not dividing \( b_1^{(2)} \). Because \( \alpha_\phi(\Gamma) > 2 \), this implies that if \( A(X) \) is in \( \Sigma_\phi^*(\Gamma) \) with \( A(X) = \begin{pmatrix} pA & B \\ pC & pD \end{pmatrix} \) and \( A(X_0) \cdot A(X) = \begin{pmatrix} * & * \\ * & G \end{pmatrix} \), then \( G \equiv 0 \pmod{\phi} \) and hence first row of \( C \) is \( \equiv 0 \pmod{\phi} \). Because \( \dim V_\phi(\Gamma) = 2 \), we can choose \( A(X_1) \) in \( \Sigma_\phi^*(\Gamma) \), such that all entries in its 4th column are not divisible by \( p \). If \( A(X_1) \cdot A(X) = \begin{pmatrix} * & * \\ * & G_1 \end{pmatrix} \), then \( G_1 \equiv 0 \pmod{\phi^2} \) and it follows that second row of \( C \) is also \( \equiv 0 \pmod{\phi^2} \).

(ii) \( \dim V_\phi(\Gamma) = 1 \). We can assume that for each element \( A(X) \) of \( \Sigma_\phi^*(\Gamma) \), \( (16) \) is true. Because \( \alpha_\phi(\Gamma) > 2 \), using similar arguments as earlier, one can see that for each \( A(X) \) in \( \Sigma_\phi^*(\Gamma) \), \( \sigma^{-1}A(X)\sigma = \)
ARITHMETIC SUBGROUPS OF THE SYMPLECTIC GROUP

\[
\left( \begin{array}{ccc}
\rho( ) & \rho( ) & x \\
\rho( ) & \rho( ) & \rho( ) \\
\rho^2( ) & \rho( ) & \rho^2( ) \\
\rho( ) & \rho( ) & \rho( )
\end{array} \right), \quad p \neq x.
\]

Since \( m \) is square-free, for a suitable \( r, s \) and \( t \) in \( \mathbb{Z} \) and multiplying \( X \) on the right or left by matrices of the form

\[
\left( \begin{array}{cc}
E & 0 \\
rm & sm \\
sm & E
\end{array} \right)
\]

one can see that there exist \( X_1 \) and \( X_2 \) in \( \Gamma_1 \) with \( \alpha_p(X_1) = \alpha_p(X_2) = \alpha_p(\Gamma_1) \), such that

\[
A(X_1) = \left( \begin{array}{cccc}
\rho^2( ) & \rho( ) & y & \rho^2( ) \\
* & \cdots & * & \\
* & \cdots & * & \\
* & \cdots & * & \\
\end{array} \right)
\]

\[
A(X_2) = \left( \begin{array}{cccc}
\rho^2( ) & \rho( ) & * & u \cdot p \\
* & \cdots & * & \\
* & \cdots & * & \\
* & \cdots & * & \\
\end{array} \right)
\]

with \( p \) not dividing \( y, z \) and \( u \). Now \( \alpha_p(\Gamma_1) > 2 \) implies that \( p^3 | A(X_i)A(X) \), \( i = 1, 2 \). From \( p | A(X_i)A(X) \) it follows that

\[
A(X) = \left( \begin{array}{cccc}
\rho( ) & \rho( ) & x & \rho( ) \\
\rho^2( ) & \rho( ) & \rho( ) & \rho( ) \\
\rho^2( ) & \rho( ) & \rho( ) & \rho^2( ) \\
\rho( ) & \rho( ) & \rho( ) & \rho( )
\end{array} \right),
\]

whereas \( p^3 | A(X_2)A(X) \) implies now that

\[
A(X) = \left( \begin{array}{cc}
pA & B \\
p^2C & pD
\end{array} \right),
\]

where \( A, B, C, D \) being integral matrices and this proves (i). (ii) is trivial.

Now suppose \( \Gamma \) is maximal. From lemma 4.3, it follows that if \( \alpha_p(\Gamma_1) > 2 \), then the group generated by \( \Gamma_1 \) and the matrices of the form
where \( V_{ij} \in M(2, \mathbb{Z}) \), such that \( \begin{pmatrix} E + mV_{11} & mV_{12} \\ mV_{21} & E + mV_{22} \end{pmatrix} \) is in \( Sp_2(\mathbb{Z}, m) \), is an arithmetic subgroup of \( Sp(2, \mathbb{R}) \) and because \( \Gamma_1 \) is maximal, must coincide with \( \Gamma \). Now if \( P = \begin{pmatrix} pE_2 & 0 \\ 0 & E_2 \end{pmatrix} \), \( U = FP \), where \( F \) is given by lemma 4.3 and \( \Gamma_2 = U^{-1}\Gamma U \), then \( \Gamma_2 \) has the following properties:

1. \( \Gamma_2 \subseteq Sp(2, \mathbb{R}) \) and is a maximal arithmetic subgroup of level \( m \).
2. If \( \alpha_s(\Gamma) > 2 \), then \( \alpha_s(\Gamma_2) \leq \alpha_s(\Gamma) - 2 \)
3. \( \alpha_s(\Gamma_2) \leq \alpha_s(\Gamma) \) for all primes \( q \neq p \).

Hence if we repeat this process sufficiently many times for each prime, we get the following

**Theorem 4.4.** Suppose \( \Gamma \) is a maximal arithmetic subgroup of \( Sp(2, \mathbb{R}) \) of level \( m \). Then there exists an arithmetic subgroup \( \Gamma^* \) of \( Sp(2, \mathbb{R}) \) of level \( m \), such that there exists \( U \in Sp(2, \mathbb{Q}) \), such that \( \Gamma = U^{-1}\Gamma^*U \) and \( 0 \leq \alpha_s(\Gamma^*) \leq 2 \) for all \( p \).

5. Let \( S_1 = \{ p_1, \ldots, p_s \} \) and \( S_2 = \{ p_{s+1}, \ldots, p_{s+t} \} \) be disjoint sets of rational primes. For \( R_1 = \{ q_1, \ldots, q_s \} \subseteq S_1 \) and \( R_2 = \{ q_{s+1}, \ldots, q_{s+g} \} \subseteq S_2 \), we put

\[
\begin{aligned}
u &= p_1 \cdots p_s, \\
u &= p_{s+1} \cdots p_{s+t}, \\
x &= q_1 \cdots q_s, \\
y &= q_{s+1} \cdots q_{s+g}.
\end{aligned}
\]

Let

\[
\Gamma(S_1, R_1; S_2, R_2) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \middle| A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, C = \begin{pmatrix} c_{11} & a_{12} \\ c_{21} & a_{22} \end{pmatrix}, D = xy \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix} \right\},
\]

where \( a_{ij}, b_{ij}, c_{ij}, d_{ij} \in \mathbb{Z} \) and \( A'C - C'A = 0 \) if \( B'D - D'B = A'D - C'B = xyE \).

Let \( \Gamma(S_1, S_2) \) be the subgroup generated by \( \bigcup_{n_i \leq n_j} \Gamma(S_1, R_1; S_2, R_2) \). We put \( \Gamma_0(S_1, S_2) = \Gamma(S_1, \phi; S_2, \phi) \).

**Theorem 5.1.** \( \Gamma(S_1, S_2) \) is a subgroup of \( Sp(2, \mathbb{R}) \) and \( \Gamma_0(S_1, S_2) \) is a normal subgroup of \( \Gamma(S_1, S_2) \). Further, \( \{ \Gamma(S_1, R_1; S_2, R_2) \mid R_i \subseteq S_i, i = 1, 2 \} \) are generators of \( G = \Gamma(S_1, S_2) \) and each element of \( G \) is of order 2 and hence \( G \) is Abelian. Order of \( G \) is \( 2^k \), where \( s \leq k \leq 2^{s+t} \). Therefore, \( \Gamma(S_1, S_2) \) is arithmetic.
Proof. All statements are either trivial or can be easily checked.

**Theorem 5.2.** \( \Gamma(\phi, \phi) = \text{Sp}(2, \mathbb{Z}) \) and if \( S_1 \neq S_2 \) or \( S_2 \neq S_2' \), then \( \Gamma(S_1, S_2) \) is not conjugate to \( \Gamma(S_1', S_2') \).

Proof. If there exists \( T \in \text{GL}(4, \mathbb{R}) \), such that \( T^{-1} \Gamma(S_1, S_2) T = \Gamma(S_1', S_2') \),

(i) If \( p \) is in \( S_1 = \{ p_1, \ldots, p_s \} \) but not in \( S_1' \), then it is enough to prove that \( \Gamma(S_1, S_2) \) contains an element of the form \( X = \frac{1}{\sqrt{p}} X_1, X_1 \in \text{M}(4, \mathbb{Z}) \), because, then \( T^{-1} X T \) cannot be in \( \Gamma(S_1', S_2') \). For this let \( u = p_1 \cdots p_s, u_j = \frac{u}{p_j} \). Choose \( a_j^{(1)} \) and \( a_j^{(2)} \) in \( \mathbb{Z} \), such that

\[
p_j a_j^{(1)} a_j^{(2)} \equiv 1 \pmod{u_j}; \quad j = 1, \ldots, s.
\]

Let

\[
b_j = \frac{b_j a_j^{(1)} a_j^{(2)} - 1}{u_j^2}
\]

and

\[
X_j = \begin{pmatrix} p_j a_j^{(1)} E & u_j E \\ p_j u_j p_j E & p_j a_j^{(2)} E \end{pmatrix}.
\]

Then for each \( j, \frac{1}{\sqrt{p_j}} \cdot X_j \) is in \( \Gamma(S_1, S_2) \).

(ii) If \( S_2 \neq S_2' \), let us assume that \( q_1 \in \{ q_1, \ldots, q_h \} \subseteq S_2' \), and \( S_2 = \{ q_1, \ldots, q_h \} \).

Again it is enough to prove that \( \Gamma(S_1, S_2) \) contains an element of the form \( \frac{1}{\sqrt{p_j}} \cdot \frac{1}{q_i} Y_1 \) with \( Y_1 \in \text{M}(4, \mathbb{Z}) \). Let \( X_1 \) be as in the case (i) above and we simply put

\[
Y_1 = \begin{pmatrix} q_i p_i a_i^{(1)} E & u_i \begin{pmatrix} 1 & 0 \\ 0 & q_i \end{pmatrix} \\ p_i u_i b_i \begin{pmatrix} q_i^2 & 0 \\ 0 & q_i \end{pmatrix} & q_i p_i a_i^{(2)} E \end{pmatrix}.
\]

**Theorem 5.3.** Any maximal arithmetic subgroup \( \Gamma \) of \( \text{Sp}(2, \mathbb{R}) \) of square-free level \( m \) is conjugate to \( \Gamma(S_1, S_2) \) for some disjoint subsets \( S_1 \) and \( S_2 \) of prime divisors of \( m \).

Proof. By theorem 4.4, we can find a subgroup \( \Gamma^* \) of \( \text{Sp}(2, \mathbb{R}) \), such that \( 0 \leq \alpha_p(\Gamma^*) \leq 2 \) for all \( p \) and \( \Gamma \) is conjugate to \( \Gamma^* \). If \( \alpha_p(\Gamma^*) = 0 \) for all \( p \), then \( \Gamma^* \subseteq \text{Sp}(2, \mathbb{Z}) = \Gamma(\phi, \phi) \) and since \( \Gamma \) is maximal, \( \Gamma^* = \text{Sp}(2, \mathbb{Z}) \). Let \( p_1, \ldots, p_s \) be the primes for which \( \alpha_p(\Gamma^*) = 1 \) and \( p_{s+1}, \ldots, p_{s+m} \), the one for which \( \alpha_p(\Gamma^*) = 2 \). Then by theorem 3.3, \( p_j \) divides \( m \) for all \( j \).
For each \( j \), let \( \sigma_j \) be the element of \( \text{Sp}(2, F_{P_j})_0 \) given by lemma 4.2, with \( \Gamma \) replaced by \( \Gamma^* \). Then for each \( X \) in \( \Gamma^* \) with \( \alpha_p(X) = \alpha_p(\Gamma^*) \),

\[
\sigma_j^{-1} \phi_p(A(X)) \sigma_j = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}
\]

and if \( j \leq s \) or \( j \geq s + t + 1 \), where \( t \) is such that \( p_{s+t+1}, \ldots, p_{s+w} \) are supposed to be all the prime divisors of \( m \) for which \( \alpha_p(\Gamma^*) = 2 \) and \( \dim V_p(\Gamma^*) = 2 \), then for all \( X \in \Gamma^* \),

\[
\sigma_j^{-1} \phi_p(A(X)) \sigma_j = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.
\]

It can be checked that for each \( j \), \( \phi_{p_j}(\text{Sp}_2(\mathbb{Z}, p_1 \cdot \cdot \cdot p_{s+w})_{P_j}) \) contains \( \text{Sp}(2, F_{p_j})_0 \) and for \( F_j \) in \( \text{Sp}_2(\mathbb{Z}, p_1 \cdot \cdot \cdot p_{s+w})_{P_j} \) and \( i \neq j \), \( \phi_{p_j}(F_j) = E \). Let \( F_j \in \text{Sp}_2(\mathbb{Z}, p_1 \cdot \cdot \cdot p_{s+w})_{P_j} \), such that \( \phi_{p_j}(F_j) = \sigma_j \) and for \( j > s+t \), let \( G_j = F_j \begin{pmatrix} 1/p_j E_2 & 0 \\ 0 & E_2 \end{pmatrix} \). If \( F = F_1 \cdot \cdot \cdot F_{s+t+1} \cdot \cdot \cdot G_{s+w+1} \), then it is easy to check that \( F^{-1} \Gamma^* F \subseteq \Gamma(S_1, S_2) \), where \( S_1 = \{p_1, \ldots, p_s\} \) and \( S_2 = \{p_{s+1}, \ldots, p_{s+w}\} \). Maximality implies that \( F^{-1} \Gamma F = \Gamma^*(S_1, S_2) \).

**Corollary 5.4.** Suppose \( \Gamma \) is an arithmetic subgroup of \( \text{Sp}(2, \mathcal{R}) \) of square-free level \( m \). Then \( [\Gamma/\Gamma \cap \text{Sp}(2, \mathbb{Z})] = 3^l \) for some non-negative integer \( l \).

**Proof.** \( 3^l = [\Gamma/\Gamma \cap \text{Sp}(2, \mathbb{Z})][\Gamma \cap \text{Sp}(2, \mathbb{Z})/\text{Sp}_2(\mathbb{Z}, m)] \).

**Corollary 5.5.** Let \( m = p_1 \cdot \cdot \cdot p_s, p_i \neq p_j, \) if \( i \neq j \). Then the number (up to conjugacy) of maximal arithmetic subgroups of \( \Gamma \subseteq \text{Sp}(2, \mathcal{R}) \) of level \( m \) is \( 3^s \). If \( \Gamma \) is such a subgroup and \( \Gamma \subseteq \text{Sp}(2, \mathcal{Q}) \), then there exists \( T \in \text{Sp}(2, \mathcal{Q}) \) such that \( \Gamma = T^{-1} \text{Sp}(2, \mathcal{Z}) T \).

**Proof.** The numbers of tuples \( (S_1, S_2) \), such that \( S_1 \) and \( S_2 \) are disjoint subsets of \( \{p_1, \ldots, p_s\} \) is \( 3^s \).

**References**


