Title	Arithmetic subgroups of the symplectic group
Author(s)	Chahal, Jasbir Singh
Citation	Osaka Journal of Mathematics. 1977, 14(3), p. 487-500
Version Type	VoR
URL	https://doi.org/10.18910/11337
rights	
Note	

Chahal, J.S.
Osaka J. Math.
14 (1977), 487-500

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 $Sp(n, k)$ of order n over k is the group of $2n\times 2n$ matrices

$$X=\begin{pmatrix} A & B \\ C & D \end{pmatrix} \tag{1}$$

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

$$X'JX=J\,, \tag{2}$$

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 $Sp(n, k)$ can be identified with the group of automorphisms σ of $2n$-dimensional vector space k^{2n}, such that σ leaves f invariant, i.e.,

$$f(\sigma x, \sigma y)=f(x, y) \tag{3}$$

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

$$\left.\begin{aligned} A'C-C'A&=0=B'D-D'B \\ A'D-C'B&=E \end{aligned}\right\} \tag{4}$$

and for X in $Sp(n, k)$,

$$X^{-1}=\begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix} \tag{5}$$

The group $Sp(n, k)$ is generated by the matrices of the form

$$\begin{pmatrix} E & T \\ 0 & E \end{pmatrix},\ \begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix} \text{ and } \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \tag{6}$$

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

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

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

$$\pi: G(\boldsymbol{Z}) \rightarrow G(\boldsymbol{Z}/m\boldsymbol{Z}).$$

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

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 Γ of $G(\boldsymbol{R})$ is said to be *arithmetic*, if it is commensurable with $G(\boldsymbol{Z})$.

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

Gutnik and Pjateckii-Šapiro determined (upto conjugacy) all the maximal arithmetic subgroups of $SL(n, \boldsymbol{R})$ of a given level. Our purpose here is to determine all the maximal arithmetic subgroups of $Sp(2, \boldsymbol{R})$ 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 Γ is an arithmetic subgroup of $Sp(n, \boldsymbol{R})$ of level m. Then each $X=(x_{ij})$ in Γ can be written as*

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

where X_1 is an integral matrix and λ is a positive integer. Further, m^3x_{ij} are algebraic integers and m^6X^2 is an integral matrix.

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

Let $X=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be in Γ. 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 $M(n, \boldsymbol{Z})$, $\begin{pmatrix} E & tmT \\ 0 & E \end{pmatrix}$ and $\begin{pmatrix} E & 0 \\ tmT & E \end{pmatrix}$ are in $\Gamma^{(t)}$. Therefore,

$$\left.\begin{aligned} X\begin{pmatrix} E & tmT \\ 0 & E \end{pmatrix}X^{-1} - \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} &= \begin{pmatrix} tmATC' & tmATA' \\ * & * \end{pmatrix}, \\ X^{-1}\begin{pmatrix} E & 0 \\ tmT & E \end{pmatrix}X - \begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} &= \begin{pmatrix} * & * \\ tmA'TA & * \end{pmatrix} \end{aligned}\right\} \tag{7}$$

are the integral matrices and hence

$$\left.\begin{aligned} tmATA' &= (y_{ij}) \quad \text{(i)} \\ tmA'TA &= (z_{ij}) \quad \text{(ii)} \end{aligned}\right\} \tag{8}$$

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

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 $T = E_{jj}$, we see that

$$a_{rj}a_{sj} = \frac{y_{rs}}{tm} \tag{9}$$

is a rational number. From (9), $a_{sj} = a_{sj}^{(1)}$. λ_j with $\lambda_j^2 \in \boldsymbol{Q}$ and $a_{sj}^{(1)} \in \boldsymbol{Q}$. Therefore $A = A_1\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_n \end{pmatrix}$, where $A_1 \in GL(n, \boldsymbol{Q})$. Now choosing g in 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 $\lambda_i \cdot \lambda_j \in \boldsymbol{Q}$. Therefore $A = 1/(\sqrt{\lambda}) \cdot A_1$ with λ in $\boldsymbol{Q}$ and A_1 in $GL(n, \boldsymbol{Q})$. From (7) we see again that $tmATC'$ is in $M(n, \boldsymbol{Z})$ and hence $C = 1/(\sqrt{\lambda})\, C_1$ with C_1 in $M(n, \boldsymbol{Q})$.

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 $B_1 \in M(n, \boldsymbol{Q})$. Using (4) we get $D = 1/(\sqrt{\lambda})D_1$, $D_1 \in M(n, \boldsymbol{Q})$. 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 λ is a positive integer and this proves the first assertion.

Now because $Sp_n(\boldsymbol{Z}, m)$ is of finite index in Γ, the characteristic roots of any X in Γ are algebraic integers and hence $tr(X)$ is an algebraic integer. If U is in $SL_n(\boldsymbol{Z}, m)$, $T \in M(n, \boldsymbol{Z})$ is symmetric, then

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

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

$$m^2 c_{ji} = tr(m^2 E_{ij} C) = tr(m(E_{ij}+mE)EC) - tr(mC)$$

and taking $U=E$, $T=E_{ii}$,

$$mc_{ii} = tr(mE_{ii}C)$$

are algebraic integers. Hence m^2C is a matrix of algebraic integers. Considering $J^{-1}\Gamma J$ instead of Γ, 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 $m^6X^2 = \frac{m^6}{\lambda} X_1^2$ is in $M(2n, \boldsymbol{Q})$ and its entries are algebraic integers, hence because $\boldsymbol{Z}$ is integrally closed, X^2 is integral.

3. Let Γ be an arithmetic subgroup of $Sp(n, \boldsymbol{R})$ of level m. Then each X in Γ 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 $\boldsymbol{Z}$. Then the maps

$$\left.\begin{aligned} A&\colon \Gamma \to M(2n, \boldsymbol{Z}) \\ \lambda&\colon \Gamma \to \boldsymbol{Z} \end{aligned}\right\} \qquad (10)$$

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 $\alpha_p(\Gamma)=l.u.b.\{\alpha_p(X)\mid X\in\Gamma\}$. Since Γ is arithmetic, $\alpha_p(\Gamma)$ is a non-negative integer. Infact, by Th. 2.1, $\alpha_p(\Gamma)\leqslant v_p(m^6)$. In this section we prove that if $n=2$, then any prime divisor of $\lambda(X)$ for any X in Γ 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 $A'D-C'B=\beta\cdot E$ 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 2×2 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

$$UMV=\begin{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix} & * \\ \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22}\end{pmatrix} & * \end{pmatrix}.$$

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

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

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

$$U_1=\begin{pmatrix} E & 0 \\ \begin{pmatrix} -\dfrac{c_{11}}{a} & -\dfrac{c_{21}}{a} \\ -\dfrac{c_{21}}{a} & 0\end{pmatrix} & E\end{pmatrix}$$

$$U_1UMV=\begin{pmatrix} \begin{pmatrix} a & 0 \\ 0 & b\end{pmatrix} & * \\ \begin{pmatrix} 0 & c \\ 0 & d\end{pmatrix} & * \end{pmatrix}.$$

If $b \neq 0$, one can assume by multiplying on the left by

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

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 $M_1=U_2U_1U$ and $M_2=V$, where

$$U_2=\begin{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{pmatrix},$$

the proof is complete.

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

$$\phi_p\colon SL_n(\boldsymbol{Z}, m) \to SL(n, \boldsymbol{F}_p) \tag{11}$$

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

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

Theorem 3.3. *Suppose Γ is an arithmetic subgroup of $Sp(2, \boldsymbol{R})$ 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 $Sp_2(\boldsymbol{Z}, m)$ such that $\phi_p(L_1A(X)L_2)= M_1\overline{A(X)}M_2=\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$. Because $\overline{A(X)} \neq 0$, we can assume that $A \neq 0$. Let P, $\underset{\sim}{Q} \in SL_2(\boldsymbol{Z}, m)$, such that $\bar{P}A\bar{Q}=\begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}$ with $a_1 \neq 0$. If

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

we put $L=UL_1A(X)L_2V$. Then

$$\bar{L}=\begin{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} & * \\ 0 & * \end{pmatrix}$$

with $a_1 \neq 0$. If $Y = 1/(\sqrt{\lambda(X)})L$, we can see that Y is in Γ. Hence $\alpha_p(Y^l) > v_p(m^6)$, 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

$$\sum\nolimits_p (\Gamma) = \{A(X) \mid X \text{ in } \Gamma \text{ and } \alpha_p(X > 0\}$$

and

$$\sum\nolimits_p^* (\Gamma) = \{A(X) \mid X \text{ in } \Gamma,\ \alpha_p(X) = \alpha_p(\Gamma)\} .$$

Obviously, $\sum_p^* (\Gamma) \subseteq \sum_p (\Gamma)$. We have written each X in Γ 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 $\boldsymbol{Z}$ is $\boldsymbol{Z}$ itself. Let $A(X) \in \sum_p^* (\Gamma)$ and $A(Y) \in \sum_p (\Gamma)$. Then

$$XY = \frac{1}{\sqrt{\lambda(X) \cdot \lambda(Y)}} A(X) \cdot A(Y) \in \Gamma . \tag{$*$}$$

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,

$$\phi_p(\sum\nolimits_p^* (\Gamma) \sum\nolimits_p (\Gamma)) = \phi_p(\sum\nolimits_p (\Gamma) \sum\nolimits_p^* (\Gamma)) = 0 . \tag{12}$$

Consider the 4-dimensional vector space $V = \boldsymbol{F}_p^4$. Let $V_p(\Gamma)$ be the subspace of V generated by $\phi_p(\sum_p^*(\Gamma))V$ over $\boldsymbol{F}_p$. 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

$$\begin{pmatrix} E & T \\ 0 & E \end{pmatrix}, \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \text{ and } \begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix},$$

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

Lemma 4.1. *Suppose σ is in $Sp(2, \boldsymbol{F}_p)_0$ and $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is in $\sigma^{-1} \sum_p (\Gamma) \sigma$. Then $\begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix}$ is also in $\sigma^{-1} \sum_p (\Gamma) \sigma$.*

Proof. This lemma is a trivial consequence of (5). It is easy to check that $\phi_p(Sp(2, \boldsymbol{Z}))$ contains $Sp(2, \boldsymbol{F}_p)_0$. If F is in $Sp(2, \boldsymbol{Z})$, such that $\phi_p(F)=\sigma$, then

$$\begin{pmatrix} D' & -B' \\ -C' & A' \end{pmatrix} = \overline{F^{-1}}\overline{A(X^{-1})}\overline{F} = \sigma^{-1}\overline{A(X^{-1})}\sigma$$

and $A(X^{-1})$ is in $\sum_p(\Gamma)$.

Lemma 4.2. If $\alpha_p(\Gamma)=1$, *then* $\dim V_p(\Gamma)=2$. *If* $\alpha_p(\Gamma)>1$, *then* $\dim V_p(\Gamma)\leqslant 2$. *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* σ *in* $Sp(2, \boldsymbol{F}_p)_0$, *such that if* $\alpha_j=\sigma(e_j)$, *where*

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \cdots, e_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

is the standard basis for V, *then* $V_p(\Gamma)=\bigoplus_{j=1}^{\dim V_p(\Gamma)} \boldsymbol{F}_p\alpha_j$.

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 $V_p(\Gamma)=\bigoplus_{j=1}^{3}\boldsymbol{F}_p\alpha_j$. 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 σ_1 is the product of the matrices of the form $\begin{pmatrix} E & T \\ 0 & E \end{pmatrix}$ and $\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}$, $T\in M(2, k)$ is symmetric and $\sigma_2=\begin{pmatrix} U & 0 \\ 0 & U'^{-1} \end{pmatrix}$, with $U\in GL(2, k)$. Hence there exists $\sigma^*\in Sp(n, k)_0$ and $\beta_i\in k^*$, such that $\sigma(e_i)=\beta_i\cdot\sigma^*(e_i)$. Therefore, we can assume that σ appearing in (15) is in $Sp(2, \boldsymbol{F}_p)_0$. From (12) it follows that for any $A(X)$ in $\sum_p(\Gamma)$, $\sigma^{-1}(\overline{A(X)}\sigma)(e_j)=0$ for $j=1, 2, 3$. Hence

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

By lemma 4.1 for each $A(X)$ in $\sum_p(\Gamma)$,

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

Now dimension of $\boldsymbol{F}_p$-subspace generated by $\sigma^{-1}\overline{\sum_p^*(\Gamma)}\sigma$ 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 α_1 in $V_p(\Gamma)$, we write V as in (13) and define σ by (15). Then for each $A(X)$ in $\sum_p^*(\Gamma)$,

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

where $C_i=\begin{pmatrix}c_{i1}\\c_{i2}\\c_{i3}\\c_{i4}\end{pmatrix}$ and $C_i=\gamma C_j$ for some γ in $\boldsymbol{F}_p$. Choosing σ_0 suitably in $Sp(2,\boldsymbol{F}_p)_0$ and replacing σ by $\sigma\cdot\sigma_0$, we can assume that

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

If X is in Γ, 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 σ defined by $\sigma(e_j)=\alpha_j$ leaves f invariant. Thus each element of $\sigma^{-1}\overline{\sum_p(\Gamma)}\sigma$ is of the form

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

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

$$\sigma^{-1}(\overline{A(X)}\sigma)^2 = 0\,.$$

and this proves the lemma.

Let σ be as in Lemma 4.2. Then for all $A(X)$ in $\sum_p(\Gamma)$,

$$\sigma^{-1}\overline{A(X)}\sigma = \begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix} \tag{17}$$

each block being 2×2 matrix.

Lemma 4.3. *Suppose $\alpha_p(\Gamma)>2$. Then there exits an F in $Sp(2, \boldsymbol{Z})$, such that if $\Gamma_1=F^{-1}\Gamma F$, then*

(i) *For each X in Γ_1 with $\alpha_p(X)=\alpha_p(\Gamma)$,*

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

with $C\equiv 0 (\bmod p^2)$ and $A\equiv D\equiv 0 \ (\bmod p)$.

(ii) *Γ_1 contains $Sp_2(\boldsymbol{Z}, m)$.*

Proof. Let σ be given by lemma 4.2 and $F\in Sp(2, \boldsymbol{Z})$, such that $\phi_p(F)=\sigma$.

(i) Let $\dim V_p(\Gamma)=2$. We fix $A(X_0)=\begin{pmatrix} pA_0 & B_0 \\ pC_0 & pD_0 \end{pmatrix}$ in $\sum_p^*(\Gamma_1)$; A_0, B_0, C_0, D_0 being integral matrices. We can find $T\in SL(2, \boldsymbol{Z})$, such that if $\sigma_0=\phi_p(T)$, then $\sigma_0^{-1}\bar{B}_0\sigma_0=\begin{pmatrix} b_1 & 0 \\ b_{12} & b_2 \end{pmatrix}$, $b_1\neq 0$. Therefore, if necessary, replacing F by $F\begin{pmatrix} T & 0 \\ 0 & T'^{-1} \end{pmatrix}$, ((17) still holds and) we can assume that

$$A(X_0) = \begin{pmatrix} pA_0 & \begin{pmatrix} b_{11}^{(0)} & pb_{12}^{(0)} \\ b_{21}^{(0)} & b_{22}^{(0)} \end{pmatrix} \\ pC_0 & pD_0 \end{pmatrix},$$

with p not dividing $b_{11}^{(0)}$. Because $\alpha_p(\Gamma_1)>2$, this implies that if $A(X)$ is in $\sum_p^*(\Gamma_1)$ with $A(X)=\begin{pmatrix} pA & B \\ pC & pD \end{pmatrix}$ and $A(X_0)\cdot A(X)=\begin{pmatrix} * & * \\ * & G \end{pmatrix}$, then $G\equiv 0 \ (\bmod p^2)$ and hence first row of C is $\equiv 0 \ (\bmod p^2)$. Because $\dim V_p(\Gamma)=2$, we can choose $A(X_1)$ in $\sum_p^*(\Gamma_1)$, 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 $G_1\equiv 0 \ (\bmod p^2)$ and it follows that second row of C is also $\equiv 0 \ (\bmod p^2)$.

(ii) $\dim V_p(\Gamma)=1$. We can assume that for each element $A(X)$ of $\sum_p^*(\Gamma_1)$, (16) is true. Because $\alpha_p(\Gamma)>2$, using similar arguments as earlier, one can see that for each $A(X)$ in $\sum_p^*(\Gamma_1)$, $\sigma^{-1}A(X)\sigma=$

$$\begin{pmatrix} \begin{pmatrix} p(\ ) & p(\ ) \\ p^2(\ ) & p(\ ) \end{pmatrix} & \begin{pmatrix} x & p(\ ) \\ p(\ ) & p(\ ) \end{pmatrix} \\ \begin{pmatrix} p^2(\ ) & p^2(\ ) \\ p^2(\ ) & p(\ ) \end{pmatrix} & \begin{pmatrix} p(\ ) & p^2(\ ) \\ p(\ ) & p(\ ) \end{pmatrix} \end{pmatrix}, \quad p \nmid x.$$

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

$$\begin{pmatrix} E & 0 \\ \begin{pmatrix} rm & sm \\ sm & 0 \end{pmatrix} & E \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \begin{pmatrix} 1 & 0 \\ -tm & 1 \end{pmatrix} & 0 \\ 0 & \begin{pmatrix} 1 & tm \\ 0 & 1 \end{pmatrix} \end{pmatrix}$$

one can see that there exist X_1 and X_2 in Γ_1 with $\alpha_p(X_1)=\alpha_p(X_2)=\alpha_p(\Gamma_1)$, such that

$$A(X_1)=\begin{pmatrix} p^2(\ ) & p^2(\ ) & y & p^2(\ ) \\ * & \cdots & \cdots & * \\ \vdots & & & \\ * & \cdots & \cdots & * \end{pmatrix}$$

$$A(X_2)=\begin{pmatrix} p^2(\ ) & p^2(\ ) & z & u\cdot p \\ * & \cdots & \cdots & * \\ \vdots & & & \\ * & \cdots & \cdots & * \end{pmatrix}$$

with p not dividing y, z and u. Now $\alpha_p(\Gamma_1)>2$ implies that $p^3 \mid A(X_i)A(X)$, $i=1, 2$. From $p \mid A(X_1)A(X)$ it follows that

$$A(X)=\begin{pmatrix} p(\ ) & p(\ ) & x & p(\ ) \\ p^3(\ ) & p(\ ) & p(\ ) & p(\ ) \\ p^3(\ ) & p^3(\ ) & p(\ ) & p^3(\ ) \\ p^3(\ ) & p(\ ) & p(\ ) & p(\ ) \end{pmatrix},$$

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

$$A(X)=\begin{pmatrix} pA & B \\ p^2C & pD \end{pmatrix},$$

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

Now suppose Γ is maximal. From lemma 4.3, it follows that if $\alpha_p(\Gamma_1)>2$, then the group generated by Γ_1 and the matrices of the form

$$\begin{pmatrix} E+mV_{11} & \dfrac{m}{p}V_{12} \\ mpV_{21} & E+mV_{22} \end{pmatrix},$$

where $V_{ij}\in M(2, \boldsymbol{Z})$, such that $\begin{pmatrix} E+mV_{11} & mV_{12} \\ mV_{21} & E+mV_{22} \end{pmatrix}$ is in $Sp_2(\boldsymbol{Z}, m)$, is an arithmetic subgroup of $Sp(2, \boldsymbol{R})$ and because Γ_1 is maximal, must coincide with Γ_1. 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 Γ_2 has the following properties:

(1) $\Gamma_2\subseteq Sp(2, \boldsymbol{R})$ and is a maximal arithmetic subgroup of level m.

(2) If $\alpha_p(\Gamma)>2$, then $\alpha_p(\Gamma_2)\leqslant\alpha_p(\Gamma)-2$

(3) $\alpha_q(\Gamma_2)\leqslant\alpha_q(\Gamma)$ 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 Γ is a maximal arithmetic subgroup of $Sp(2, \boldsymbol{R})$ of level m. Then there exists an arithmetic subgroup Γ^* of $Sp(2, \boldsymbol{R})$ of level m, such that there exists $U\in Sp(2, \boldsymbol{Q})$, such that $\Gamma=U^{-1}\Gamma^*U$ and $0\leqslant\alpha_p(\Gamma^*)\leqslant 2$ for all p.*

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

$$u=p_1\cdots p_s\,,\quad v=p_{s+1}\cdots p_{s+t}\,,$$

$$x=q_1\cdots q_f\,,\quad y=q_{s+1}\cdots q_{s+g}\,.$$

Let

$$\Gamma(S_1, R_1; S_2, R_2)=\frac{1}{y\sqrt{x}}\left\{X=\begin{pmatrix} A & B \\ C & D \end{pmatrix}\middle| A=\begin{pmatrix} a_{11}xy & a_{12}xy \\ a_{21}xy & a_{22}xy \end{pmatrix},\right.$$

$$B=\begin{pmatrix} b_{11} & b_{12}v \\ b_{21}v & b_{22}v \end{pmatrix},\ C=\begin{pmatrix} c_{11}uy^2 & c_{12}uy^2 \\ c_{21}uy^2 & c_{22}uy \end{pmatrix},\ D=xy\begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix},$$

$$\left.\text{where } a_{ij}, b_{ij}, c_{ij}, d_{ij}\in\boldsymbol{Z} \text{ and } A'C-C'A=0=B'D-D'B;\ A'D-C'B=xy^2E\right\}.$$

Let $\Gamma(S_1, S_2)$ be the subgroup generated by $\bigcup\limits_{\substack{R_1,R_2\\ R_i\subseteq S_i}}\Gamma(S_1, R_1; S_2, R_2)$. 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 $Sp(2, \boldsymbol{R})$ 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 $G=\Gamma(S_1, S_2)/\Gamma_0(S_1, S_2)$ and each element of G is of order 2 and hence G is Abelian. Order of G is 2^k, where $s\leqslant k\leqslant 2^{s+t}$. Therefore, $\Gamma(S_1, S_2)$ is arithmetic.*

Proof. All statements are either trivial or can be easily checked.

Theorem 5.2. $\Gamma(\phi, \phi)=Sp(2, \boldsymbol{Z})$ *and if* $S_1 \neq S_1'$ *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 $T \in GL(4, \boldsymbol{R})$, such that $T^{-1}\Gamma(S_1, S_2)T=\Gamma(S_1', S_2')$, then we can assume that $T \in GL(4, \boldsymbol{Q})$.

(i) If p is in $S_1=\{p_1, \cdots, p_s\}$ but not in S_1', then it is enough to prove that $\Gamma(S_1, S_2)$ contains an element of the form $X=\frac{1}{\sqrt{p}}X_1$, $X_1 \in M(4, \boldsymbol{Z})$, because, then $T^{-1}XT$ 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 $\boldsymbol{Z}$, such that

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

Let

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

and

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

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 $q_1 \in \{q_1, \cdots, q_h\}-S_2'$, and $S_2=\{q_1, \cdots, q_h\}$. Again it is enough to prove that $\Gamma(S_1, S_2)$ contains an element of the from $\frac{1}{\sqrt{p_j}}\cdot\frac{1}{q_1}\cdot Y_1$ with $Y_1 \in M(4, \boldsymbol{Z})$. Let X_1 be as in the case (i) above and we simply put

$$Y_1=\begin{pmatrix} q_1 p_1 a_1^{(1)}E & u_1\begin{pmatrix}1 & 0\\ 0 & q_1\end{pmatrix} \\ p_1 u_1 b_1\begin{pmatrix}q_1^2 & 0\\ 0 & q_1\end{pmatrix} & q_1 p_1 a_1^{(2)}E \end{pmatrix}.$$

Theorem 5.3. *Any maximal arithmetic subgroup* Γ *of* $Sp(2, \boldsymbol{R})$ *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 Γ^* of $Sp(2, \boldsymbol{R})$, such that $0 \leqslant \alpha_p(\Gamma^*) \leqslant 2$ for all p and Γ is conjugate to Γ^*. If $\alpha_p(\Gamma^*)=0$ for all p, then $\Gamma^* \subseteq Sp(2, \boldsymbol{Z})=\Gamma(\phi, \phi)$ and since Γ is maximal, $\Gamma^*=Sp(2, \boldsymbol{Z})$. Let $p_1, \cdots, p_s$ be the primes for which $\alpha_p(\Gamma^*)=1$ and $p_{s+1}, \cdots, p_{s+w}$, the one for which $\alpha_p(\Gamma^*)=2$. Then by theorem 3.3, p_j divides m for all j.

For each j, let σ_j be the element of $Sp(2, \boldsymbol{F}_{p_j})_0$ given by lemma 4.2, with Γ replaced by Γ^*. Then for each X in Γ^* with $\alpha_p(X)=\alpha_p(\Gamma^*)$,

$$\sigma_j^{-1}\phi_{p_j}(A(X))\sigma_j=\begin{pmatrix}0 & * \\ 0 & 0\end{pmatrix}$$

and if $j\leqslant s$ or $j\geqslant s+t+1$, where t is such that $p_{s+t+1}, \cdots, p_{s+w}$ are supposed to be all the prime divisors of m for which $\alpha_{p_j}(\Gamma^*)=2$ and $\dim V_{p_j}(\Gamma^*)=2$, then for all $X\in\Gamma^*$,

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

It can be checked that for each j, $\phi_{p_j}\left(Sp_2\left(\boldsymbol{Z}, \frac{p_1\cdots p_{s+w}}{p_j}\right)\right)$ contains $Sp(2, \boldsymbol{F}_{p_j})_0$ and for F_j in $Sp_2\left(\boldsymbol{Z}, \frac{p_1\cdots p_{s+w}}{p_j}\right)$ and $i\neq j$, $\phi_{p_i}(F_j)=E$. Let $F_j\in Sp_2\left(\boldsymbol{Z}, \frac{p_1\cdots p_{s+w}}{p_j}\right)$, such that $\phi_{p_j}(F_j)=\sigma_j$ and for $j>s+t$, let $G_j=F_j\begin{pmatrix}1/p_jE_2 & 0 \\ 0 & E_2\end{pmatrix}$. If $F=F_1\cdots F_{s+t}G_{s+t+1}\cdots G_{s+w}$, then it is easy to check that $F^{-1}\Gamma^*F\subseteq\Gamma(S_1, S_2)$, where $S_1=\{p_1, \cdots, p_s\}$ and $S_2=\{p_{s+1}, \cdots, p_{s+t}\}$. Maximality implies that $F^{-1}\Gamma F=\Gamma^*(S_1, S_2)$.

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

Proof. $3^k=[\Gamma/\Gamma\cap Sp(2, \boldsymbol{Z})][\Gamma\cap Sp(2, \boldsymbol{Z})/Sp_2(\boldsymbol{Z}, m)]$.

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

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

JOHNS HOPKINS UNIVERSITY

References

[1] A. Borel: *Density properties for certain subgroups of semi-simple groups without compact components*, Ann. of Math. **72** (1960), 179–188.

[2] A. Borel: *Density and maximality of arithmetic subgroups*, J. Reine Angew. Math. **224** (1966), 78–89.

[3] L.A. Gutnik and I.I. Pjateckiĭ-Šapiro,: *Maximal discrete subgroups of the unimodular group*, Trans. Moscow Math. Soc. (1966), AMS translation, 316–332.

[4] K.G. Ramanathan: *Discontinuous groups* II, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. **22** (1964), 145–164.