ABELIAN QUADRATIC FORMS

K. G. RAMANATHAN

1. Introduction. Hermite [4] in the course of his investigations on the transformation theory of abelian functions, introduced the notion of abelian quadratic forms. They are quadratic forms whose matrices $\mathfrak{S}$ of orders $2n$, satisfy

$$\mathfrak{S}'\mathfrak{J}\mathfrak{S} = k\mathfrak{J}, \qquad \mathfrak{J} = \begin{pmatrix} \mathfrak{O} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{O} \end{pmatrix}$$

where $k \neq 0$ is a real number, and $\mathfrak{E}$ is the unit matrix of order n. Laguerre [7] and, more systematically, Cotty [3] developed an arithmetical theory of abelian forms in four variables. Cotty defined equivalence of abelian forms under what is now known as Siegel's modular group of degree 2 and proved the finiteness of the number of classes of integral abelian forms of given determinant. Siegel's generalization [10] of the theory of elliptic modular functions enables us to discuss completely the reduction theory of abelian forms. The object of the present note is to point out how Siegel's ideas are related to the reduction theory of abelian forms. We define equivalence of abelian forms under Siegel's modular group of degree n and obtain, for reduced abelian forms, properties analogous to those of Minkowski and Gauss. H. J. S. Smith (see [6, pp. 243-269]) showed how Gauss's theory of positive binary forms is related to the well-known modular division of the upper half of the complex z-plane. The generalization of this idea leads to Siegel's symplectic geometry. We also deal with another generalization of the theory of binary quadratic forms which is related to the hermitian modular group studied recently by H. Braun [1]. The researches of Siegel on discontinuous groups show that analogous results may be obtained by considering coset spaces of certain linear groups. In particular we consider the space of cosets of a generalized complex, orthogonal group with regard to a maximal compact subgroup and study reduction in this space in regard to a discontinuous group. We do not consider this at great length since sufficient arithmetical properties of these discontinuous groups are not known.

2. Notation. Symmetric or hermitian matrices shall be denoted by capital German letters, $\mathfrak{S}$, $\mathfrak{H}$, . . . etc. Small German letters $\mathfrak{x}$, $\mathfrak{q}$, . . . shall denote column vectors. $\mathfrak{S}[\mathfrak{C}]$ and $\mathfrak{S}\{\mathfrak{C}\}$ shall stand for $\mathfrak{C}'\mathfrak{S}\mathfrak{C}$ and $\mathfrak{C}^*\mathfrak{S}\mathfrak{C}$ where $\mathfrak{C}'$ stands for the transpose of $\mathfrak{C}$. By a triangle matrix we shall always mean a square matrix $\mathfrak{C} = (c_{kl})$ such that $c_{kl} = 0$ if $k > l$, $c_{kk} = 1$ $(k = 1, \ldots, m)$ and the rest arbitrary. $\mathfrak{W} = (w_{kl})$ shall stand for the $n \times n$ square matrix with $w_{kl} = 1$ if $k + l = n + 1$, otherwise zero. $\mathfrak{E}$ will denote the unit matrix and $\mathfrak{O}$ the zero matrix of order evident from the context. The diagonal elements of a matrix will be written with single subscripts.

Received March 26, 1951.

3. Generalized symplectic matrices. Let K be a field of characteristic $\neq 2$ and $G(n, K)$ the group of matrices $\mathfrak{M}$, of order $2n$, with elements in K and satisfying

$$\mathfrak{M}'\mathfrak{J}\mathfrak{M} = k\mathfrak{J}, \qquad \mathfrak{J} = \begin{pmatrix} \mathfrak{O} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{O} \end{pmatrix}, \tag{1}$$

where $k \neq 0$ is an element of K, and $\mathfrak{E}$ is the unit matrix of order n. We shall call $G(n, K)$ the *generalized K-symplectic group* and its elements the *generalized K-symplectic matrices*. It is evident that since $\mathfrak{J}^2 = -\mathfrak{E}_{2n}$, $G(n, K)$ contains $\mathfrak{M}$ and $\mathfrak{M}'$. Consequently if

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix},$$

where $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$ are $n \times n$ matrices then

$$\begin{aligned} &\mathfrak{A}'\mathfrak{C} = \mathfrak{C}'\mathfrak{A}, \quad \mathfrak{D}'\mathfrak{B} = \mathfrak{B}'\mathfrak{D}, \quad \mathfrak{A}'\mathfrak{D} - \mathfrak{C}'\mathfrak{B} = k\mathfrak{E}, \\ &\mathfrak{A}\mathfrak{B}' = \mathfrak{B}\mathfrak{A}', \quad \mathfrak{C}\mathfrak{D}' = \mathfrak{D}\mathfrak{C}', \quad \mathfrak{A}\mathfrak{D}' - \mathfrak{B}\mathfrak{C}' = k\mathfrak{E}. \end{aligned} \tag{2}$$

It is evident that if $n = 1$ the relation (1) is satisfied automatically provided k is the determinant of $\mathfrak{M}$. In the general case we shall call k the *kernel* of the generalized symplectic matrix $\mathfrak{M}$. Let us call $\mathfrak{M}$ a *K-symplectic matrix* if $\mathfrak{M}$ has kernel unity. The K-symplectic matrices form a subgroup of $G(n, K)$. Let us call a generalized K-symplectic matrix $\mathfrak{S}$ *abelian* if it is symmetric. Then for $\mathfrak{S}$ abelian we have

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}, \quad \mathfrak{A}\mathfrak{B}' = \mathfrak{B}\mathfrak{A}, \quad \mathfrak{A}\mathfrak{C} - \mathfrak{B}^2 = k\mathfrak{E}. \tag{3}$$

k is called the kernel of the abelian form $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$. We shall show that every abelian matrix can, by a K-symplectic transformation, be reduced to the diagonal form. In case $n = 1$ this result is trivial since any two-rowed, square matrix of determinant unity is symplectic.

THEOREM 1. *If $\mathfrak{S}$ is a K-abelian matrix, there exists a K-symplectic matrix $\mathfrak{P}$ with*

$$\mathfrak{P}'\mathfrak{S}\mathfrak{P} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1} \end{pmatrix}, \tag{4}$$

where $\mathfrak{D}$ is a diagonal matrix with elements in K and k is the kernel of $\mathfrak{S}$.

Proof. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$, $\mathfrak{A} = \begin{pmatrix} a & \mathfrak{a}' \\ \mathfrak{a} & \mathfrak{A}_1 \end{pmatrix}$, and $\mathfrak{B} = \begin{pmatrix} b & \mathfrak{b}' \\ \mathfrak{y} & \mathfrak{B}_1 \end{pmatrix}$, $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{y}$ being column vectors of $n - 1$ rows. Let us assume $a \neq 0$. Then $\mathfrak{A} = \begin{pmatrix} a & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{A}_2 \end{pmatrix}\begin{pmatrix} 1 & -a^{-1}\mathfrak{a}' \\ \mathfrak{o} & \mathfrak{E}_{n-1} \end{pmatrix}$ where $\mathfrak{A}_2 = \mathfrak{A}_1 - a^{-1}\mathfrak{a}\mathfrak{a}'$. Let $\mathfrak{B} = \begin{pmatrix} 1 & -\mathfrak{a}^{-1}\mathfrak{a}' \\ \mathfrak{o} & \mathfrak{E} \end{pmatrix}$ then $\mathfrak{Q}_1 = \begin{pmatrix} \mathfrak{B} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{B}'^{-1} \end{pmatrix}$ is K-symplectic. Let

$$\mathfrak{Q}_1'\mathfrak{S}\mathfrak{Q}_1 = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_0 \\ \mathfrak{B}_0' & \mathfrak{C}_0 \end{pmatrix}. \tag{5}$$

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

Then $\mathfrak{A}_0 = \begin{pmatrix} a & \mathfrak{o} \\ \mathfrak{o} & \mathfrak{A}_2 \end{pmatrix}$ and $\mathfrak{B}_0 = \begin{pmatrix} b & \mathfrak{b}' \\ a^{-1}\mathfrak{A}_2\mathfrak{b} & \mathfrak{B}_1 - a^{-1}\mathfrak{a}\mathfrak{b}' \end{pmatrix}$. Let $\mathfrak{T}$ be the symmetric matrix $\mathfrak{T} = a^{-1}\begin{pmatrix} -b & -\mathfrak{b}' \\ -\mathfrak{b} & \mathfrak{O} \end{pmatrix}$ and let $\mathfrak{Q}_2 = \begin{pmatrix} \mathfrak{E}_n & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}$ be a K-symplectic matrix. Then

$$\mathfrak{Q}_2'\mathfrak{Q}_1'\mathfrak{S}\mathfrak{Q}_1\mathfrak{Q}_2 = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_2 \\ \mathfrak{B}_2' & \mathfrak{C}_2 \end{pmatrix}, \tag{6}$$

where $\mathfrak{B}_2 = \begin{pmatrix} o & \mathfrak{o} \\ \mathfrak{o} & a^{-1}\mathfrak{a}\mathfrak{b}' - \mathfrak{B}_1 \end{pmatrix}$ and $\mathfrak{C}_2 = \begin{pmatrix} a^{-1}k & \mathfrak{D} \\ \mathfrak{o} & \mathfrak{C}_3 \end{pmatrix}$. Thus $\begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_3 \\ \mathfrak{B}'_3 & \mathfrak{C}_3 \end{pmatrix}$ is an abelian matrix of kernel k and is an element of $G(n-1, K)$. Also $\mathfrak{B}_3 = a^{-1}\mathfrak{a}\mathfrak{b}' - \mathfrak{B}_1$. It is now evident how the proof can be completed by induction provided we can show that by a K-symplectic transformation we can make the first diagonal element of $\mathfrak{A}$ not zero.

Suppose that the first diagonal element of $\mathfrak{A}$ is zero but not its pth diagonal element $1 < p \leqslant n$. Let $\mathfrak{U}$ be the matrix interchanging the first and the pth columns of $\mathfrak{A}$. Then $\mathfrak{S}\begin{bmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{bmatrix}$ has its first diagonal element not zero. Suppose now that all the diagonal elements of $\mathfrak{A}$ were zero. Let an element in the kth row and lth column of $\mathfrak{A}$ be not zero. By a transformation interchanging the first and lth column we may assume that an element in the first row and lth column is not zero. Put $\mathfrak{U} = \begin{pmatrix} 1 & \mathfrak{o} \\ \mathfrak{y}_1 & \mathfrak{E} \end{pmatrix}$ where $\mathfrak{y}_1$ is a column vector of $n-1$ rows with zero everywhere except in the $(l-1)$th row. Then $\mathfrak{S}\begin{bmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{bmatrix}$ has its first diagonal element not zero provided the characteristic of K is not two.

We therefore come to the case $\mathfrak{A} = \mathfrak{O}$. Then $\mathfrak{J}'\mathfrak{S}\,\mathfrak{J} = \begin{pmatrix} \mathfrak{C} & -\mathfrak{B}' \\ -\mathfrak{B} & \mathfrak{A} \end{pmatrix}$ and we can apply the arguments in the last paragraph to $\mathfrak{C}$. Let now $\mathfrak{A} = \mathfrak{O} = \mathfrak{C}$. Then $|\mathfrak{B}| \neq 0$. Let $\mathfrak{P}_1 = \begin{pmatrix} \mathfrak{E} & \mathfrak{O} \\ \mathfrak{F} & \mathfrak{E} \end{pmatrix}$ be K-symplectic then $\mathfrak{F}$ is symmetric. $\mathfrak{S}[\mathfrak{P}_1] = \begin{pmatrix} \mathfrak{B}\mathfrak{F} + \mathfrak{F}\mathfrak{B}' & * \\ * & * \end{pmatrix}$. Let $\mathfrak{x}$ be the column vector

$$\mathfrak{x} = \mathfrak{B}^{-1}\begin{pmatrix} 1 \\ 0 \\ \cdots \\ 0 \end{pmatrix}$$

and let $\mathfrak{F}$ have $\mathfrak{x}$ for first row and column and zeros elsewhere. Then the first diagonal element of $\mathfrak{S}[\mathfrak{P}_1]$ is not zero since K has characteristic $\neq 2$.

Our theorem is thus completely established.

The theorem could have been proved much more simply if K had not been a finite field, but since this result would be of use in the analytic theory of abelian forms we have given a proof valid even for finite fields.

COROLLARY. *If K is real algebraically closed*[1] *then by a generalized K-symplectic matrix $\mathfrak{Q}$ we can make $\mathfrak{S}[\mathfrak{Q}]$ have the diagonal form with ± 1 in the diagonals.*

Theorem 1 tells us that the determinant of a K-abelian matrix is

$$|\mathfrak{S}| = |\mathfrak{A}\mathfrak{C} - \mathfrak{B}^2| = k^n. \tag{7}$$

Let now $K_0 = K(\sqrt{d})$ where d is an element of K and $\sqrt{d}$ is not in K. Let σ be the generating automorphism of K_0/K so that $\sigma^2 = 1$, the identity automorphism. Let $\mathfrak{M}^{(2n)} = \mathfrak{M}$ be a matrix with elements in K_0 and denote $\mathfrak{M}^*$ by

$$\mathfrak{M}^* = (m_{lk}^{\sigma}) \tag{8}$$

where $\mathfrak{M} = (m_{kl})$. Then $\mathfrak{M}^{**} = \mathfrak{M}$, $(\mathfrak{M}_1\mathfrak{M}_2)^* = \mathfrak{M}_2^*\mathfrak{M}_1^*$, and $(\mathfrak{M}^*)^{-1} = (\mathfrak{M}^{-1})^*$. Let $G(n, K_0)$ be the set of matrices $\mathfrak{M}$ of order $2n$ such that

$$\mathfrak{M}^*\mathfrak{J}\mathfrak{M} = k\mathfrak{J} \tag{9}$$

where $k \neq 0$ is in K. The number k is called the *kernel* of $\mathfrak{M}$. The matrices $\mathfrak{M}$ of kernel unity are called *K_0-hermitian symplectic.* If $\mathfrak{S}$ is a matrix in $G(n, K_0)$ such that $\mathfrak{S}^* = \mathfrak{S}$ we shall call $\mathfrak{S}$ *a K_0-abelian hermitian matrix.* The analogue of Theorem 1 then is

THEOREM 1′. *Any abelian hermitian matrix $\mathfrak{S}$ can by a K_0-hermitian symplectic transformation $\mathfrak{Q}$ be brought into the diagonal form; that is,*

$$\mathfrak{Q}^*\mathfrak{S}\mathfrak{Q} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1} \end{pmatrix} \tag{10}$$

where $\mathfrak{D}$ is a diagonal matrix with elements in K.

The proof of this theorem is similar to that of Theorem 1. For an abelian hermitian matrix $\mathfrak{S}$ we have

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}, \quad |\mathfrak{S}| = |\mathfrak{A}\mathfrak{C} - \mathfrak{B}^2| = k^n. \tag{11}$$

4. Matrices over the real field. Let us now assume that K is the field of all real numbers. Let $G(n, K)$ denote the group of real matrices $\mathfrak{M}$ satisfying (1). The real number k is the kernel of $\mathfrak{M}$. $\mathfrak{M}$ is called a real *generalized symplectic matrix.* The subgroup of $G(n, K)$ with kernel unity is the well-known real symplectic group. We shall prove

LEMMA 1. *The determinant $|\mathfrak{M}|$ of a general symplectic matrix $\mathfrak{M}$ of kernel k is k^n.*

Proof. Let $\mathfrak{M} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$ have kernel k. Let $\mathfrak{P} = \begin{pmatrix} \mathfrak{E} & \mathfrak{O} \\ t\mathfrak{E} & \mathfrak{E} \end{pmatrix}$, with t a real number different from zero, be a symplectic matrix. Then $|\mathfrak{P}| = 1$; also $\mathfrak{M}\mathfrak{P} = \begin{pmatrix} \mathfrak{A} + t\mathfrak{B} & * \\ * & * \end{pmatrix}$.

[1]We use the term real algebraically closed in the sense of Artin and Schreier. See [12, p. 235].

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

Since $|\mathfrak{A} + t\mathfrak{B}| = 0$ has only finitely many real solutions t, it follows that there is a real $t \neq 0$ with $|\mathfrak{A} + t\mathfrak{B}| \neq 0$. Let t be such a real number. Put $\mathfrak{M}\mathfrak{P} = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{C}_1 & \mathfrak{D}_1 \end{pmatrix}$, $|\mathfrak{A}_1| \neq 0$ and consider $\mathfrak{Q} = \begin{pmatrix} \mathfrak{E} & -\mathfrak{A}_1^{-1}\mathfrak{B}_1 \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}$. Since $\mathfrak{M}\mathfrak{P}$ is generalized symplectic, $\mathfrak{A}_1\mathfrak{B}'_1 = \mathfrak{B}_1\mathfrak{A}'_1$ or $\mathfrak{A}_1^{-1}\mathfrak{B}_1$ is symmetric. Consequently, $\mathfrak{Q}$ is a real symplectic matrix. Now

$$\mathfrak{M}\mathfrak{P}\mathfrak{Q} = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{O} \\ \mathfrak{C}_1 & \mathfrak{D}_1 - \mathfrak{C}_1\mathfrak{A}_1^{-1}\mathfrak{B}_1 \end{pmatrix}. \tag{12}$$

But from (2) it follows that $\mathfrak{D}_1 - \mathfrak{C}_1\mathfrak{A}_1^{-1}\mathfrak{B}_1 = k\mathfrak{A}'^{-1}_1$. Since $|\mathfrak{Q}| = 1$ our contention in the lemma follows.

COROLLARY. *If $\mathfrak{M}$ is symplectic then* $|\mathfrak{M}| = 1$.

Let us call *modular* any real symplectic matrix whose elements are rational integers. The modular matrices obviously form a group called the *modular group of degree n*. For any modular matrix $\mathfrak{M}$, we have $|\mathfrak{M}| = 1$.

Call two $n \times n$ matrices $\mathfrak{C}$ and $\mathfrak{D}$ with rational elements a *symmetric pair* if $(\mathfrak{C}\,\mathfrak{D})$ is of rank n and

$$\mathfrak{C}\mathfrak{D}' = \mathfrak{D}\mathfrak{C}'. \tag{13}$$

If $\mathfrak{C}, \mathfrak{D}$ is an integral symmetric pair, there exists a non-singular integral matrix $\mathfrak{P}$ with $\mathfrak{P}^{-1}(\mathfrak{C}\,\mathfrak{D})$ a primitive matrix. We call $\mathfrak{P}$ the *greatest common divisor* (g.c.d.) of $\mathfrak{C}$ and $\mathfrak{D}$. If $\mathfrak{P}$ is unimodular we call $\mathfrak{C}$ and $\mathfrak{D}$ coprime. The g.c.d. is unique up to multiplication on the right by a unimodular matrix. For let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be two g.c.d.'s. Then $\mathfrak{P}_1^{-1}(\mathfrak{C}\,\mathfrak{D})$ is a primitive matrix and can be completed into a unimodular matrix $\mathfrak{U}$. Put $\mathfrak{U}^{-1} = \begin{pmatrix} \mathfrak{X} & * \\ \mathfrak{Y} & * \end{pmatrix}$, then $\mathfrak{P}_1^{-1}(\mathfrak{C}\mathfrak{X} + \mathfrak{D}\mathfrak{Y}) = \mathfrak{E}$. Hence $\mathfrak{P}_2^{-1}(\mathfrak{C}\mathfrak{X} + \mathfrak{D}\mathfrak{Y}) = \mathfrak{P}_2^{-1}\mathfrak{P}_1$ is integral and similarly $\mathfrak{P}_1^{-1}\mathfrak{P}_2$. Hence our contention. We prove

LEMMA 2. *If $\mathfrak{C}, \mathfrak{D}$ is an integral symmetric pair, there is a generalized integral symplectic matrix* $\mathfrak{M} = \begin{pmatrix} * & * \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$.

Proof. Let $\mathfrak{P}$ be the g.c.d. of $\mathfrak{C}$ and $\mathfrak{D}$. Then $\mathfrak{P}^{-1}(\mathfrak{C}\,\mathfrak{D}) = (\mathfrak{C}_1\mathfrak{D}_1)$ is a primitive matrix. Let $(\mathfrak{C}_1\mathfrak{D}_1)$ be completed into a unimodular matrix $\mathfrak{U}$ and let $\mathfrak{U}^{-1} = \begin{pmatrix} \mathfrak{X} & * \\ \mathfrak{Y} & * \end{pmatrix}$. Put

$$\mathfrak{X}_1 = \mathfrak{Y}' + \mathfrak{X}'\mathfrak{Y}\mathfrak{C}_1, \quad \mathfrak{Y}_1 = -\mathfrak{X}' + \mathfrak{X}'\mathfrak{Y}\mathfrak{D}_1.$$

Then $\begin{pmatrix} \mathfrak{X}_1 & \mathfrak{Y}_1 \\ \mathfrak{C}_1 & \mathfrak{D}_1 \end{pmatrix}$ is a modular matrix. Let t be an integer so that $t\mathfrak{P}^{-1}$ is an integral matrix. The matrix

$$\mathfrak{M} = \begin{pmatrix} t\mathfrak{P}'^{-1}\mathfrak{X}_1 & t\mathfrak{P}'^{-1}\mathfrak{Y}_1 \\ \mathfrak{C} & \mathfrak{D} \end{pmatrix}$$

satisfies our requirements and is of kernel t.

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

Let us now call two general integral symplectic matrices $\mathfrak{M}_1$ and $\mathfrak{M}_2$ *associated* if

$$\mathfrak{M}_1 = \mathfrak{M}_2\mathfrak{P} \tag{14}$$

with a modular $\mathfrak{P}$. We write $\mathfrak{M}_1 \sim \mathfrak{M}_2$. This is an equivalence relation since the modular matrices form a group. All integral matrices equivalent to $\mathfrak{M}_1$ form a class. Thus all generalized integral symplectic matrices fall into classes of associate matrices. The matrices in any class have the same kernel.

THEOREM 2. *The number of classes of associate matrices with a given kernel is finite.*

Proof. Let $\mathfrak{M} = \begin{pmatrix}\mathfrak{A} & \mathfrak{B}\\ \mathfrak{C} & \mathfrak{D}\end{pmatrix}$ have kernel k. Let $\mathfrak{P}$ be the g.c.d. of $\mathfrak{C}$ and $\mathfrak{D}$. Then $k\mathfrak{P}^{-1}$ is an integral matrix. Let $\mathfrak{X}_1, \mathfrak{X}_2$ be so chosen that $\mathfrak{C}\mathfrak{X}_1 + \mathfrak{D}\mathfrak{X}_2 = \mathfrak{P}$ and $\begin{pmatrix}\mathfrak{X}_1\\ \mathfrak{X}_2\end{pmatrix}$ can be completed to a modular matrix $\begin{pmatrix}\mathfrak{X}_1 & \mathfrak{X}_3\\ \mathfrak{X}_2 & \mathfrak{X}_4\end{pmatrix} = \mathfrak{Q}$. Then

$$\mathfrak{M}\mathfrak{Q} = \begin{pmatrix}\mathfrak{A}_1 & \mathfrak{B}_1\\ \mathfrak{P} & \mathfrak{D}_1\end{pmatrix}. \tag{15}$$

From (2) we get $\mathfrak{P}\mathfrak{D}'_1 = \mathfrak{D}_1\mathfrak{P}'$ and so $\mathfrak{P}^{-1}\mathfrak{D}_1 = \mathfrak{T}$ is an integral symmetric matrix. Now

$$\mathfrak{M}\mathfrak{Q}\begin{pmatrix}\mathfrak{T} & \mathfrak{E}\\ -\mathfrak{E} & \mathfrak{O}\end{pmatrix} = \begin{pmatrix}\mathfrak{A}_1\mathfrak{T} - \mathfrak{B}_1 & \mathfrak{A}_1\\ \mathfrak{O} & \mathfrak{P}\end{pmatrix}, \tag{16}$$

and $\mathfrak{A}_1\mathfrak{T} - \mathfrak{B}_1 = k\mathfrak{P}'^{-1}$ is an integral matrix. That $\mathfrak{P}$ depends only on the class of $\mathfrak{M}$ is easy to see, for, if $\mathfrak{M}$ can be reduced to $\begin{pmatrix}\mathfrak{A}_2 & \mathfrak{B}_2\\ \mathfrak{O} & \mathfrak{P}_2\end{pmatrix}$ and $\begin{pmatrix}\mathfrak{A}_3 & \mathfrak{B}_3\\ \mathfrak{O} & \mathfrak{P}_3\end{pmatrix}$ by multiplication on the right by modular matrices, then for a suitable modular matrix $\begin{pmatrix}\mathfrak{C}_1 & \mathfrak{C}_2\\ \mathfrak{C}_3 & \mathfrak{C}_4\end{pmatrix}$ we have

$$\begin{pmatrix}\mathfrak{A}_2 & \mathfrak{B}_2\\ \mathfrak{O} & \mathfrak{P}_2\end{pmatrix}\begin{pmatrix}\mathfrak{C}_1 & \mathfrak{C}_2\\ \mathfrak{C}_3 & \mathfrak{C}_4\end{pmatrix} = \begin{pmatrix}\mathfrak{A}_3 & \mathfrak{B}_3\\ \mathfrak{O} & \mathfrak{P}_3\end{pmatrix}, \tag{17}$$

which means $\mathfrak{C}_3 = \mathfrak{O}$, $\mathfrak{C}_4$ is unimodular and $\mathfrak{P}_2\mathfrak{C}_4 = \mathfrak{P}_3$.

Let $\mathfrak{U}$ be a unimodular matrix so that $\mathfrak{P}\mathfrak{U} = \mathfrak{F} = (f_{kl})$ where $f_{kl} = 0$, $k > l$, and $0 \leqslant f_{kl} < f_k$ $(k < l = 1, \ldots, n)$. Thus

$$\mathfrak{M}\mathfrak{Q}\begin{pmatrix}\mathfrak{T} & \mathfrak{E}\\ -\mathfrak{E} & \mathfrak{O}\end{pmatrix}\begin{pmatrix}\mathfrak{U}'^{-1} & \mathfrak{O}\\ \mathfrak{O} & \mathfrak{U}\end{pmatrix} = \begin{pmatrix}k\mathfrak{F}'^{-1} & \mathfrak{H}\\ \mathfrak{O} & \mathfrak{F}\end{pmatrix} = \begin{pmatrix}\mathfrak{F}_1 & \mathfrak{H}\\ \mathfrak{O} & \mathfrak{F}\end{pmatrix}. \tag{18}$$

Now $\mathfrak{F}_1^{-1}\mathfrak{H}$ is symmetric. Consider $\begin{pmatrix}\mathfrak{E} & \mathfrak{K}\\ \mathfrak{O} & \mathfrak{E}\end{pmatrix}$ where $\mathfrak{K}$ is integral symmetric. Choose $\mathfrak{K}$ so that the elements of $\mathfrak{F}_1^{-1}\mathfrak{H} + \mathfrak{K}$ lie between $\frac{1}{2}$ and $-\frac{1}{2}$. The matrix $\begin{pmatrix}\mathfrak{F}_1 & \mathfrak{H}\\ \mathfrak{O} & \mathfrak{F}\end{pmatrix} \times \begin{pmatrix}\mathfrak{E} & \mathfrak{K}\\ \mathfrak{O} & \mathfrak{E}\end{pmatrix}$ has now only a finite number of possibilities for a given k. Our lemma is thus proved.

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

In the case $n = 1$ the number of these classes is $\sigma(k)$, the sum of the divisors of k. In the general case an expression for this number of classes seems to be difficult to find. Hermite and Cotty have shown that if $k = p$, a prime number, and $n = 2$, the number of classes is $1 + p + p^2 + p^3$.

5. Abelian quadratic forms. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be a symmetric real matrix satisfying (1). It is called a real abelian matrix and the associated quadratic form, a real abelian quadratic form. Abelian forms are a generalization of binary quadratic forms. From Theorem 1 and Corollary it follows that there exists a general symplectic matrix $\mathfrak{P}$ with

$$\mathfrak{P}'\mathfrak{S}\mathfrak{P} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & \epsilon\mathfrak{D} \end{pmatrix}, \tag{19}$$

where $\mathfrak{D}$ is a diagonal matrix with ± 1 in the diagonal and $\xi = \operatorname{sgn} k$. This shows that the number of negative signs in the normal form of $\mathfrak{S}$ is either $2p$ $(0 \leqslant p \leqslant n)$ or n. We can thus speak of signature of an abelian matrix without any fear of confusion.

Let $\mathfrak{S}$ be an abelian matrix and $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$ the abelian quadratic form. We say that $\mathfrak{x}'\mathfrak{S}\mathfrak{x}$ is *positive* (*negative*) *definite* if $\mathfrak{x}'\mathfrak{S}\mathfrak{x} > 0 (< 0)$ for real $\mathfrak{x} \neq 0$. It is obvious that a necessary and sufficient condition for positivity is that $k > 0$ and $\mathfrak{A}$ is positive definite. Consequently $|\mathfrak{A}| \neq 0$. Abelian matrices that are not definite are *indefinite.*

Let $\mathfrak{P}$ be a modular matrix. With $\mathfrak{S}$, $\mathfrak{S}[\mathfrak{P}]$ is also abelian. We call two abelian matrices $\mathfrak{S}_1$ and $\mathfrak{S}_2$ *symplectic equivalent*[2] if there is a modular matrix $\mathfrak{P}$ with $\mathfrak{S}_1[\mathfrak{P}] = \mathfrak{S}_2$. This is an equivalence relation and all abelian matrices can be put into classes of equivalent matrices. Let us first confine ourselves to positive abelian forms. It will be observed that our method is a simple generalization of Gauss's theory.

If $ax^2 + 2bxy + cy^2$ is a positive binary form, Gauss's method of reduction consists in first finding an equivalent form with a minimum and then transforming it so that $b/a \leqslant \frac{1}{2}$. We adopt the same procedure.

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be positive abelian with arbitrary real elements and let $\mathfrak{P}'$, $\mathfrak{Q}'$ be an integral symmetric pair. Put $\mathfrak{L} = \begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}$. Consider the determinant of

$$\mathfrak{S}[\mathfrak{L}] = \mathfrak{P}'\mathfrak{A}\mathfrak{P} + \mathfrak{Q}'\mathfrak{B}'\mathfrak{P} + \mathfrak{P}'\mathfrak{B}\mathfrak{Q} + \mathfrak{Q}'\mathfrak{C}\mathfrak{Q}. \tag{20}$$

If for a $\mathfrak{P}$, $\mathfrak{Q}$ this determinant is a minimum at all, then this minimum will be attained when $\mathfrak{L}$ is primitive or $\mathfrak{P}'$, $\mathfrak{Q}'$ is a coprime pair. For if $\mathfrak{R}'$ is the g.c.d. of $\mathfrak{P}'$, $\mathfrak{Q}'$ then $\mathfrak{L}\mathfrak{R}^{-1} = \begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}\mathfrak{R}^{-1}$ and

[2]Using the terminology of Gauss we may call this *proper equivalence.* Hermite and Cotty actually consider equivalence under integral matrices $\mathfrak{P}$ satisfying $\mathfrak{P}'\mathfrak{J}\mathfrak{P} = \pm\mathfrak{J}$. But since the modular matrices form a subgroup of index 2 in this group of $\mathfrak{P}$, there is not much change in our argument if we consider $\mathfrak{P}$ with negative kernel.

$$|\mathfrak{S}[\mathfrak{L}\mathfrak{R}^{-1}]| \leqslant |\mathfrak{S}[\mathfrak{L}]|. \tag{21}$$

So for investigating the minimum of $|\mathfrak{S}[\mathfrak{L}]|$ it will be enough if we confine ourselves to the case when $\mathfrak{P}'$, $\mathfrak{Q}'$ are coprime.

If $|\mathfrak{S}[\mathfrak{L}]|$ is minimum then this minimum will not be altered if we change $\mathfrak{L}$ into $\mathfrak{L}\mathfrak{U}$ with $\mathfrak{U}$ unimodular. Then $\mathfrak{S}[\mathfrak{L}] = \mathfrak{A}_1$ is changed into $\mathfrak{U}'\mathfrak{A}_1\mathfrak{U}$. Since $\mathfrak{A}_1$ is positive definite we can by a proper choice of $\mathfrak{U}$ make $\mathfrak{U}'\mathfrak{A}_1\mathfrak{U}$ reduced in the sense of Minkowski. The coprimality of $\mathfrak{P}'$, $\mathfrak{Q}'$ is unaltered by this. We shall now prove

LEMMA 3. *If* $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ *is positive abelian then there exists an* $\mathfrak{L} = \begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}$ *with* $\mathfrak{P}'$, $\mathfrak{Q}'$ *coprime such that* $|\mathfrak{L}'\mathfrak{S}\,\mathfrak{L}|$ *is minimum.*

Proof. Let $\mathfrak{L}'\mathfrak{S}\,\mathfrak{L} = \mathfrak{A}_1$. In order to prove the lemma we may assume that $\mathfrak{A}_1$ is reduced in the sense of Minkowski. Let $a > 0$ be a large real number. We shall show that $|\mathfrak{A}_1| < a$ has only a finite number of integral solutions $\mathfrak{L}$.

Now

$$\mathfrak{A}_1 = \mathfrak{L}'\mathfrak{S}\mathfrak{L} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}\begin{bmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{bmatrix} = \begin{pmatrix} \mathfrak{A} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{A}^{-1} \end{pmatrix}\begin{bmatrix} \mathfrak{P} + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{Q} \\ \mathfrak{Q} \end{bmatrix}, \tag{22}$$

so that

$$\mathfrak{A}_1 = \mathfrak{A}[\mathfrak{P} + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{Q}] + k\mathfrak{A}^{-1}[\mathfrak{Q}]. \tag{23}$$

Let $\mathfrak{A}_1 = (a_{kl})$ and write $\mathfrak{p}_l$ and $\mathfrak{q}_l$ for the lth columns of $\mathfrak{P}$ and $\mathfrak{Q}$ respectively. Then from (23) we get

$$a_l = \mathfrak{A}[\mathfrak{p}_l + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{q}_l] + k\mathfrak{A}^{-1}[\mathfrak{q}_l]. \tag{24}$$

Since $\mathfrak{A}_1$ is reduced in the sense of Minkowski we get

$$a_1 a_2 \ldots a_n \leqslant \lambda_n |\mathfrak{A}_1| < \lambda_n a = b, \tag{25}$$

λ_n being a constant depending only on n. Since $\mathfrak{A}^{-1}$ is a positive real matrix there exists a $d > 0$ such that for any integral column $\mathfrak{q}$, $d \leqslant k\mathfrak{A}^{-1}[\mathfrak{q}]$. Thus from (24) we get

$$d \leqslant a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n. \tag{26}$$

Since the right side of (24) consists of two positive numbers,

$$\begin{cases} \mathfrak{A}[\mathfrak{p}_l + \mathfrak{A}^{-1}\mathfrak{B}\mathfrak{q}_l] \leqslant a_l, \\ k\mathfrak{A}^{-1}[\mathfrak{q}_l] \leqslant a_l. \end{cases} \tag{27}$$

Using (25), (26), and (27) it follows that

$$a_l \leqslant (b/d^{l-1})^{1/(n-l+1)} = b_1, \tag{28}$$

where b_1 depends only on n, $\mathfrak{A}$, and a. From (27) and (28) our assertion follows.

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

We shall now outline a reduction theory of positive abelian forms. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{B}_0 \\ \mathfrak{B}'_0 & \mathfrak{C}_0 \end{pmatrix}$ be a positive abelian matrix and let $\mathfrak{M} = \begin{pmatrix} \mathfrak{P}_1 & \mathfrak{P}_3 \\ \mathfrak{P}_2 & \mathfrak{P}_4 \end{pmatrix}$ run through all modular matrices. Consider the first "columns" $\begin{pmatrix} \mathfrak{P}_1 \\ \mathfrak{P}_2 \end{pmatrix}$ of these modular matrices. Let $\mathfrak{S}\begin{bmatrix} \mathfrak{P}_1 \\ \mathfrak{P}_2 \end{bmatrix}$ have a minimum determinant. By Lemma 3 there are only a finite number of such first columns. Transform, if necessary, by a matrix $\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}$, where $\mathfrak{U}$ is a unimodular matrix, so that $\mathfrak{S}\begin{bmatrix} \mathfrak{P}_1\mathfrak{U} \\ \mathfrak{P}_2\mathfrak{U} \end{bmatrix}$ is reduced in the sense of Minkowski. Write

$$\mathfrak{S}\left[\mathfrak{M}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}\right] = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{B}'_1 & \mathfrak{C}_1 \end{pmatrix} = \mathfrak{S}_1, \tag{29}$$

so that $|\mathfrak{A}_1|$ is minimum and $\mathfrak{A}_1$ is reduced in the sense of Minkowski. All modular matrices whose first columns $\begin{pmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{pmatrix}$ are the same as that of $\mathfrak{M}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}$ are of the form

$$\mathfrak{M}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}'^{-1} \end{pmatrix}\begin{pmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix} = \mathfrak{M}_1, \tag{30}$$

where $\mathfrak{T}$ is an integral symmetric matrix. Let $\mathfrak{S}_1\begin{bmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{bmatrix} = \begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_2 \\ * & * \end{pmatrix}$; then

$$\mathfrak{B}_2 = \mathfrak{A}_1\mathfrak{T} + \mathfrak{B}_1, \tag{31}$$

so that $\mathfrak{A}_1^{-1}\mathfrak{B}_1$ and $\mathfrak{A}_1^{-1}\mathfrak{B}_2$ are two symmetric matrices which are congruent modulo 1. Thus the integral matrix $\mathfrak{T}$ can be chosen in such a way that the elements of $\mathfrak{A}_1^{-1}\mathfrak{B}_2$ lie between $+\frac{1}{2}$ and $-\frac{1}{2}$. If $\mathfrak{A}_1$ and $\mathfrak{B}_2$ are fixed, automatically the other elements of the matrix $\mathfrak{S}[\mathfrak{M}_1]$ are fixed too. We call $\mathfrak{S}[\mathfrak{M}_1] = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$, which is equivalent to $\mathfrak{S}$, a *symplectic reduced* matrix. It has the properties:

(32)
(i) $|\mathfrak{A}|$ is minimum,
(ii) $\mathfrak{A}$ is reduced in the sense of Minkowski,
(iii) the elements of $\mathfrak{B}^{-1}\mathfrak{A}$ are in absolute value $\leqslant \frac{1}{2}$.

Condition (i) merely asserts that for any coprime pair, *a fortiori* for any integral symmetric pair $\mathfrak{P}$, $\mathfrak{Q}$, we have

$$\left|\begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}\begin{bmatrix} \mathfrak{P} \\ \mathfrak{Q} \end{bmatrix}\right| \geqslant |\mathfrak{A}|. \tag{33}$$

Putting $\mathfrak{P} = \mathfrak{O}$, $\mathfrak{Q} = \mathfrak{E}$ we get

$$|\mathfrak{A}| \leqslant |\mathfrak{C}|. \tag{34}$$

In order now to obtain the analogue of the fundamental Gauss-Minkowski inequality regarding the product of the diagonal elements of a reduced matrix we proceed thus.

Let $\mathfrak{P} = \begin{pmatrix} \mathfrak{E}_{n-1} & 0 \\ 0 & 0 \end{pmatrix}$, $\mathfrak{Q} = \begin{pmatrix} \mathfrak{O} & 0 \\ 0 & 1 \end{pmatrix}$. Then $\mathfrak{P}$, $\mathfrak{Q}$ are coprime. Let t be the last

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

diagonal element of $\mathfrak{A}^{-1}\mathfrak{B}$ and let $\mathfrak{A} = \begin{pmatrix} \mathfrak{A}_0 & \mathfrak{a}' \\ \mathfrak{a} & a \end{pmatrix}$, where $\mathfrak{A}_0$ is a symmetric matrix of $n - 1$ rows. Making use of the identity (23) and the inequality (33) we get

(35) $$|\mathfrak{A}| \leqslant k|\mathfrak{A}_0|^2/|\mathfrak{A}| + t^2|\mathfrak{A}|$$

Since $|t| \leqslant \frac{1}{2}$ it follows that

(36) $$\sqrt{k}|\mathfrak{A}_0| \geqslant \tfrac{1}{2}\sqrt{3}|\mathfrak{A}|.$$

Let us now prove the following useful

LEMMA 4. *Let $\mathfrak{R} = (r_{kl})$ be a positive definite symmetric matrix and let $\mathfrak{R} = \mathfrak{D}[\mathfrak{G}]$ where $\mathfrak{D}$ is a diagonal matrix with diagonal elements $(d_1, \ldots, d_n)$ satisfying*

(37) $$0 < d_k \leqslant \tau d_{k+1} \qquad (k = 1, \ldots, n-1),$$

and $\mathfrak{G}$ is a triangle matrix all of whose elements are in absolute value $\leqslant \tau$. Then

(38) $$r_1 r_2 \ldots r_n \leqslant \mu(n, \tau)|\mathfrak{R}|,$$

where $\mu(n, \tau)$ depends only on n and τ.

Proof. Since $\mathfrak{R} = \mathfrak{D}[\mathfrak{G}]$ we have

(39) $$r_j = d_j + \sum_{k=1}^{j-1} d_k g_{kj}^2,$$

so that

(40) $$1 \leqslant \frac{r_j}{d_j} \leqslant 1 + \sum_{k=1}^{j-1} \frac{d_k}{d_j} g_{kj}^2 \leqslant c_1(\tau, n).$$

Hence

(41) $$r_1 \ldots r_n \leqslant c_1(\tau, n)^n d_1 \ldots d_n = \mu(n, \tau)|\mathfrak{R}|.$$

Let us now write for our reduced matrix, $\mathfrak{A} = \mathfrak{D}[\mathfrak{G}]$. Since $\mathfrak{A}$ is Minkowski reduced, it follows from the Minkowski reduction theory that $\mathfrak{D}$ and $\mathfrak{G}$ satisfy the conditions of Lemma 4 with $\tau = \tau_n$ depending *only* on n. Since $\mathfrak{A}^{-1} = \mathfrak{D}^{-1}[\mathfrak{G}'^{-1}]$ we get $d_n^{-1} = |\mathfrak{A}_0|/|\mathfrak{A}|$. Using (36) we get

(42) $$d_n \leqslant 2(k/3)^{\frac{1}{2}}.$$

Since $|\mathfrak{A}| = d_1 \ldots d_n$ we get, using (37) and (42), the inequality

(43) $$|\mathfrak{A}| = d_1 \ldots d_n \leqslant (2/\sqrt{3})^n \tau_n^{\frac{1}{2}n(n-1)} k^{\frac{1}{2}n}$$

which gives an upper bound for the "minimum" of a positive abelian form. We are now ready to prove the important

THEOREM 3. *If $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ is a symplectic reduced positive abelian matrix with kernel k and $\mathfrak{A} = (a_{kl})$, $\mathfrak{C} = (c_{kl})$ then*

(44) $$|\mathfrak{A}||\mathfrak{C}| \leqslant a_1 \ldots a_n c_1 \ldots c_n \leqslant \mu_n|\mathfrak{S}|,$$

μ_n depending only on n.

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

Proof. Put $\mathfrak{A}^{-1}\mathfrak{B} = -\mathfrak{X}$. Then with the previous notation

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1} \end{pmatrix} \left[\begin{pmatrix} \mathfrak{G} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{G}'^{-1} \end{pmatrix} \begin{pmatrix} \mathfrak{E} & -\mathfrak{X} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix} \right]; \tag{45}$$

using the matrix $\mathfrak{W}$ which satisfies $\mathfrak{W}^2 = \mathfrak{E}$ we get

$$\mathfrak{S}\begin{bmatrix} \mathfrak{E} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{W} \end{bmatrix} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1}[\mathfrak{W}] \end{pmatrix} \begin{bmatrix} \mathfrak{G} & -\mathfrak{G}\mathfrak{X}\mathfrak{W} \\ \mathfrak{O} & \mathfrak{W}\mathfrak{G}'^{-1}\mathfrak{W} \end{bmatrix}. \tag{46}$$

In virtue of (42) and Lemma 4, the diagonal matrix and the triangle matrix on the right of (46) satisfy the conditions of Lemma 4. Therefore from the conclusions of that lemma as applied to (46), our theorem follows.

The conditions (32), (34), and (44) are the analogues of those of Gauss for positive binary forms. We can use them to prove

THEOREM 4. *There are only a finite number of integral, positive, symplectic reduced abelian quadratic forms with a given kernel.*

Proof. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be a symplectic reduced positive integral abelian matrix. From (34) and (44) we get

$$|\mathfrak{A}| \leqslant \mu_n^{\frac{1}{2}} k^{\frac{1}{2}n}. \tag{47}$$

$\mathfrak{A}$ is an integral matrix reduced in the sense of Minkowski. From Minkowski's reduction theory it follows that there are only a finite number of integral $\mathfrak{A}$ satisfying (47). From (32), $\mathfrak{A}^{-1}\mathfrak{B}$ has all its elements between $-\frac{1}{2}$ and $+\frac{1}{2}$. Since $\mathfrak{B}$ is an integral matrix, it follows that there are only finitely many integral $\mathfrak{B}$ satisfying this condition. $\mathfrak{A}\mathfrak{C} - \mathfrak{B}^2 = k\mathfrak{E}$ so that $\mathfrak{C} = \mathfrak{A}^{-1}(k\mathfrak{E} + \mathfrak{B}^2)$, hence when $\mathfrak{A}$ and $\mathfrak{B}$ are known $\mathfrak{C}$ is fixed uniquely. Our contention is thus proved.

In the case $n = 1$ our considerations coincide with those of Gauss and Minkowski. For $n > 1$ it is seen that two symplectically equivalent matrices are equivalent in Minkowski's sense but not necessarily conversely. Also a class of positive integral matrices of determinant k^n (in the sense of Minkowski) may not contain an abelian matrix so that in general we do not have a relation between class number in the symplectic sense and class number in the Minkowski sense. We shall, however, find the symplectic reduced positive quaternary integral abelian forms with a given kernel.

Let us consider positive, integral, abelian, quaternary, quadratic forms of kernel 1 or 2. Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be a positive abelian matrix of order 4 and kernel $k = 1, 2$. Let $\mathfrak{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ where a, b, c are rational integers and $\mathfrak{A}$ is Minkowski reduced. If $|\mathfrak{A}| = p$ then

$$0 < a \leqslant c, \quad 2b \leqslant a, \quad ac \leqslant 4p/3. \tag{48}$$

Also let $\mathfrak{A} = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}$ then $|\mathfrak{A}| = p = d_1 d_2$ and $d_1 = a$. From (42) we get

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

$$a = d_1 = \frac{p}{d_2} \geqslant \frac{p\sqrt{3}}{2\sqrt{k}}.$$

Let us consider two cases, $k = 1$ and 2. In the first case $p \leqslant 16/9$ and since p is an integer so $p = 1$. Hence the only symplectic reduced $\mathfrak{S}$ satisfying these conditions is $\mathfrak{A} = \mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = \mathfrak{E}_2$. In the second case $p \leqslant 32/9$ or $p = 1, 2,$ or 3. When $p = 1$ there is no solution. For $p = 2$, $\mathfrak{A} = \mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = 2\mathfrak{E}_2$ is the only solution. For $p = 3$, $\mathfrak{A} = 2\mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = \mathfrak{E}_2$ is the only solution. But these two solutions are symplectic equivalent. Hence

Integral quaternary positive abelian forms of kernel 1 *or* 2 *constitute each a single class.*

Consider now quaternary positive abelian forms of kernel 3. With the same notation as before we have $p = 1, 2, 3, 4, 5$. If $p = 1$ then $\mathfrak{A} = \mathfrak{E}_2$, $\mathfrak{B} = \mathfrak{O}$, $\mathfrak{C} = 3\mathfrak{E}$ is the only solution. If $p = 2$ then $\mathfrak{A} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$, $\mathfrak{B} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\mathfrak{C} = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}$ is a solution. That these two solutions are not symplectically equivalent is easy to see. For if $\begin{pmatrix} \mathfrak{P} & \mathfrak{Q} \\ \mathfrak{P}_1 & \mathfrak{Q}_1 \end{pmatrix}$ is the transforming modular matrix then

$$\mathfrak{P}'\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\mathfrak{P} + \mathfrak{P}'_1\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\mathfrak{P} + \mathfrak{P}'\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\mathfrak{P}_1 + \mathfrak{P}'_1\begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}\mathfrak{P}_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{49}$$

This will mean that $\mathfrak{P}_1 = \mathfrak{O}$ and $\mathfrak{P} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ which contradicts the fact that $\begin{pmatrix} \mathfrak{P} & \mathfrak{Q} \\ \mathfrak{P}_1 & \mathfrak{Q}_1 \end{pmatrix}$ is a modular matrix. Hence

Positive integral abelian quaternary forms of kernel 3 *have at least* 2 *classes represented respectively by* $x_1^2 + x_2^2 + 3x_3^2 + 3x_4^2$ *and* $x_1^2 + 2x_2^2 + 3x_3^2 + 2x_4^2 + 2x_2x_4$.

We can briefly discuss now the reduction theory of indefinite abelian forms. Our method is similar to the usual Hermite method for ordinary quadratic indefinite forms.

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be an abelian matrix of kernel k. By Theorem 1 there exists a generalized symplectic matrix $\mathfrak{P}$ such that $\mathfrak{S} = \mathfrak{P}'\mathfrak{D}\,\mathfrak{P}$, where $\mathfrak{D}$ is an abelian diagonal matrix with ± 1 in the diagonal. Put $\mathfrak{H} = \mathfrak{P}'\mathfrak{P}$ so that $\mathfrak{H}$ is a positive abelian matrix with kernel $|k|$. By the considerations above there is a modular matrix $\mathfrak{M}$ such that $\mathfrak{M}'\,\mathfrak{H}\mathfrak{M}$ is symplectic reduced. Let us then call $\mathfrak{M}'\mathfrak{S}\mathfrak{M}$ *symplectic reduced*. It is evident that $\mathfrak{H}$ and $\mathfrak{S}$ satisfy the matrix equation

$$\mathfrak{H}\mathfrak{S}^{-1}\mathfrak{H} = \mathfrak{S}. \tag{50}$$

Let now $\mathfrak{S}[\mathfrak{M}]$ be symplectic reduced. Put $\mathfrak{S}[\mathfrak{M}] = \mathfrak{S}_1$ and $\mathfrak{H}[\mathfrak{M}] = \mathfrak{H}_1$. Then $\mathfrak{H}_1\mathfrak{S}_1^{-1}\mathfrak{H}_1 = \mathfrak{S}_1$. Put now $\mathfrak{H}_2 = \mathfrak{H}_1\begin{bmatrix} \mathfrak{E} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{W} \end{bmatrix}$ and $\mathfrak{S}_2 = \mathfrak{S}_1\begin{bmatrix} \mathfrak{E} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{W} \end{bmatrix}$. Then $\mathfrak{H}_2\mathfrak{S}_2^{-1}\mathfrak{H}_2 = \mathfrak{S}_2$. Furthermore, by (45) and (46), the matrix $\mathfrak{H}_2$ satisfies the condition of

Lemma 4 and hence by a well-known theorem of Siegel there are only a finite number of integral matrices $\mathfrak{S}_2$ with the given kernel k. Thus

THEOREM 5. *There are only a finite number of symplectic reduced integral abelian indefinite matrices with a given kernel.*

It remains now only to point out the geometrical aspect of the problem. In the case of positive binary form $ax^2 + 2bxy + cy^2$, H. J. S. Smith proceeded in the following way. To this positive form associate the complex number $z = a^{-1}(-b + i\sqrt{k})$, where $k = b^2 - ac$, which becomes a point in the upper half of the complex z-plane. The reduction theory of binary forms thus is equivalent to the construction of a fundamental domain for the ordinary modular group. We shall copy this procedure for abelian forms.

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}' & \mathfrak{C} \end{pmatrix}$ be positive real abelian. By the principle of completion of squares we may write

$$\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{A}^{-1} \end{pmatrix} \begin{bmatrix} \mathfrak{E} & \mathfrak{A}^{-1}\mathfrak{B} \\ \mathfrak{O} & \mathfrak{E} \end{bmatrix}$$

where $\mathfrak{A}^{-1}\mathfrak{B}$ is symmetric and k is the kernel of $\mathfrak{S}$. Let us put $\mathfrak{A}^{-1}\mathfrak{B} = \mathfrak{X}$ and $\mathfrak{Y} = \sqrt{k}\cdot\mathfrak{A}^{-1}$. Then

$$\mathfrak{S} = \sqrt{k}\begin{pmatrix} \mathfrak{Y}^{-1} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{Y} \end{pmatrix} \begin{bmatrix} \mathfrak{E} & -\mathfrak{X} \\ \mathfrak{O} & \mathfrak{E} \end{bmatrix}.$$

Put $\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y}$. Then $\mathfrak{Z}$ is a complex symmetric matrix of order n and its imaginary part is the matrix of a positive definite, quadratic form. Thus

$$\mathfrak{Z} = \mathfrak{X} + i\mathfrak{Y} = -\mathfrak{A}^{-1}\mathfrak{B} + i\sqrt{k}\cdot\mathfrak{A}^{-1}$$

is a point of Siegel's half-space of symmetric complex matrices. Because of the presence of the factor $\sqrt{k}$, the correspondence between abelian forms and points in Siegel's half-space is not (1, 1). However, for every point of Siegel's half-space there is a one-parameter family of positive abelian forms, any member of which can be uniquely fixed by its kernel. Thus positive abelian forms can be represented in a (1, 1) way by points in $(n^2 + n + 1)$-dimensional real space. Siegel's space is thus the space of positive abelian forms of kernel unity. His fundamental theorem that the measure of a fundamental domain of the modular group of degree n is finite, is the analogue of Minkowski's result concerning the volume of a fundamental domain on the determinantal surface.

6. Abelian hermitian forms. Another generalization of the theory of binary quadratic forms is the theory of abelian hermitian forms.

Let K_0 be the field of complex numbers. For any matrix $\mathfrak{M}^{(2n)} = \mathfrak{M}$ of $2n$ rows and columns let $\mathfrak{M}^*$ denote the transpose of the complex conjugate of $\mathfrak{M}$. Let $G(K_0,n)$ be the group of matrices $\mathfrak{M}$ with

$$\mathfrak{M}^*\mathfrak{J}\mathfrak{M} = k\mathfrak{J}, \qquad \mathfrak{J} = \begin{pmatrix} & \mathfrak{O} & \mathfrak{E} \\ - & \mathfrak{O}\mathfrak{E} & \end{pmatrix}, \tag{51}$$

where $k \neq 0$ is a real number. We shall call $G(K_0,n)$ the *generalized h-symplectic*

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

group. The subgroup $g(K_0,n)$ with $k = \pm 1$ will be called the *h-symplectic group*. If $\mathfrak{M}$ satisfies (51) and $\mathfrak{M} = \mathfrak{M}^*$ we call $\mathfrak{M}$ a *h-abelian matrix*. As before the number k shall be called the *kernel* of the generalized h-symplectic matrix. That h-abelian matrices are generalizations of two by two real symmetric matrices is obvious. For put $n = 1$ and let $\mathfrak{M}$ be positive definite binary hermitian. Put $\mathfrak{M} = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$. From (51) it follows that $b = \bar{b}$ or b is real.

Let R be the field of rational numbers and $d < 0$ a rational integer. Let $R(\sqrt{d})$ be an imaginary quadratic field and let G be the group of matrices $\mathfrak{M}$ with coefficients integral in $R(\sqrt{d})$ and satisfying

$$\mathfrak{M}^*\mathfrak{J}\mathfrak{M} = \mathfrak{J}. \tag{52}$$

G is the *h-modular group* considered recently by Braun. The h-modular group is a generalization of the ordinary 2×2 unimodular group in the rational number field. Braun has shown that for a h-modular matrix $\mathfrak{M}$, $|\mathfrak{M}| = \epsilon^2$ where ϵ is a root of unity in $R(\sqrt{d})$

Let $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}$ be a h-abelian matrix of kernel k and let $\mathfrak{P}$ be h-modular. We call $\mathfrak{S}$ and $\mathfrak{P}^*\mathfrak{S}\mathfrak{P}$, *h-equivalent*. The h-equivalent matrices form a class. We shall sketch very briefly the reduction theory of h-abelian, positive matrices.

Let $\mathfrak{P} = \begin{pmatrix} \mathfrak{P}_1 & \mathfrak{P}_3 \\ \mathfrak{P}_2 & \mathfrak{P}_4 \end{pmatrix}$ run over all h-modular matrices and consider the determinant

$$\left| \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix} \left\{ \begin{matrix} \mathfrak{P}_1 \\ \mathfrak{P}_2 \end{matrix} \right\} \right|.$$

We maintain that this has a minimum. This is proved by using the reduction theory of Humbert instead of that of Minkowski. We omit this proof. Let us assume that $\mathfrak{P}$ has been so chosen that $|\mathfrak{A}_1|$ is a minimum, where $\begin{pmatrix} \mathfrak{A}_1 & \mathfrak{B}_1 \\ \mathfrak{B}_1^* & \mathfrak{C}_1 \end{pmatrix} = \mathfrak{S}\{\mathfrak{P}\}$. We can choose $\mathfrak{A}_1$ reduced in the sense of Humbert by multiplying $\mathfrak{P}$ by $\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}^{*-1} \end{pmatrix}$ where $\mathfrak{U}$ is a suitable unimodular matrix in $R(\sqrt{d})$. Consider now all modular matrices $\mathfrak{Q} = \begin{pmatrix} \mathfrak{P}_1\mathfrak{U} & \mathfrak{Q}_1 \\ \mathfrak{P}_2\mathfrak{U} & \mathfrak{Q}_2 \end{pmatrix}$. This is obtained from $\mathfrak{P}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}^{*-1} \end{pmatrix}$ by multiplying on the right by $\begin{pmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}$ where $\mathfrak{T} = \mathfrak{T}^*$ is hermitian and integral in $R(\sqrt{d})$. Let $1, \omega$ be a minimal basis of integers of $R(\sqrt{d})$. Every complex number can be uniquely written in the form $a + b\omega$ where a and b are real. Write $\mathfrak{T} = \mathfrak{T}_1 + \omega\mathfrak{T}_2$ where $\mathfrak{T}_1$ and $\mathfrak{T}_2$ are rational integral matrices. Let

$$\mathfrak{S}\left\{\mathfrak{P}\begin{pmatrix} \mathfrak{U} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{U}^{*-1} \end{pmatrix}\begin{pmatrix} \mathfrak{E} & \mathfrak{T} \\ \mathfrak{O} & \mathfrak{E} \end{pmatrix}\right\} = \begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{B}_2^* & \mathfrak{C}_2 \end{pmatrix}.$$

Then $\mathfrak{A}_2^{-1}\mathfrak{B}_2$ is hermitian and can be written as $\mathfrak{F}_1 + \omega\mathfrak{F}_2$ where $\mathfrak{F}_1$ and $\mathfrak{F}_2$ are real. Choose now $\mathfrak{T}$ in such a way that $\mathfrak{F}_1 + \mathfrak{T}_1$ and $\mathfrak{F}_2 + \mathfrak{T}_2$ have all elements between $-\frac{1}{2}$ and $+\frac{1}{2}$. We shall call $\begin{pmatrix} \mathfrak{A}_2 & \mathfrak{B}_2 \\ \mathfrak{B}_2^* & \mathfrak{C}_2 \end{pmatrix}$ a *h-symplectic reduced matrix.* Thus if $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}$ is a h-symplectic reduced h-abelian matrix, then

(53)
(i) $|\mathfrak{A}|$ is minimum,
(ii) $\mathfrak{A}$ is reduced in the sense of Humbert,
(iii) $\mathfrak{A}^{-1}\mathfrak{B} = \mathfrak{F}_1 + \omega\mathfrak{F}_2$ is such that $\mathfrak{F}_1$ and $\mathfrak{F}_2$ have all their elements in the interval $(-\frac{1}{2}, \frac{1}{2})$.

It is thus evident, as a first result, that

$$|\mathfrak{C}| \geqslant |\mathfrak{A}|. \tag{54}$$

By a known theorem of Humbert, there exists an integral matrix $\mathfrak{A}_p$ determined by the integer n and the field $R(\sqrt{d})$ such that $\mathfrak{A}\{\mathfrak{A}_p\} = \mathfrak{D}\{\mathfrak{R}\}$ where $\mathfrak{D}$ is a diagonal matrix and $\mathfrak{R}$ is a triangle matrix satisfying conditions similar to Lemma 4. We therefore see, in virtue of a lemma of H. Braun's, that the matrix

$$\begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}\begin{Bmatrix} \mathfrak{A}_p & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{A}_p^{*-1}\mathfrak{W} \end{Bmatrix} = \begin{pmatrix} \mathfrak{D} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{D}^{-1}\{\mathfrak{W}\} \end{pmatrix}\begin{Bmatrix} \mathfrak{R} & \mathfrak{R}\mathfrak{A}_p^{-1}\mathfrak{X}\mathfrak{A}_p^{*-1}\mathfrak{W} \\ 0 & \mathfrak{W}\mathfrak{R}\mathfrak{W} \end{Bmatrix} \tag{55}$$

satisfies conditions like those in Lemma 4. Here $\mathfrak{X} = -\mathfrak{A}^{-1}\mathfrak{B}$. Therefore from Humbert's results we get

$$|\mathfrak{A}\{\mathfrak{A}_p\}|\,|\mathfrak{C}\{\mathfrak{A}_p^{*-1}\mathfrak{W}\}| \leqslant \mu_n k^n, \tag{56}$$

where μ_n depends only on n and d. Thus we have the important

THEOREM 6. *An h-reduced h-abelian positive matrix* $\mathfrak{S} = \begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix}$ *satisfies*

$$0 < |\mathfrak{A}| \leqslant |\mathfrak{C}|, \qquad |\mathfrak{A}|\,|\mathfrak{C}| \leqslant \mu_n k^n, \qquad \mathfrak{A}^{-1}\mathfrak{B} = \mathfrak{F}_1 + \omega\mathfrak{F}_2, \tag{57}$$

where μ_n *depends only on* n *and* d, *and* $\mathfrak{F}_1$ *and* $\mathfrak{F}_2$ *have all their elements in the interval* $(-\frac{1}{2}, \frac{1}{2})$.

It is now a simple matter to prove that positive h-abelian integral matrices of a given kernel have only finitely many classes. To extend this to integral indefinite forms use has to be made of Theorem 1′. These considerations are simple and we omit them.

A geometric representation for positive h-abelian forms is possible. As before we write

$$\begin{pmatrix} \mathfrak{A} & \mathfrak{B} \\ \mathfrak{B}^* & \mathfrak{C} \end{pmatrix} = \begin{pmatrix} \mathfrak{A} & \mathfrak{O} \\ \mathfrak{O} & k\mathfrak{A}^{-1} \end{pmatrix}\begin{Bmatrix} \mathfrak{E} & \mathfrak{A}^{-1}\mathfrak{B} \\ \mathfrak{O} & \mathfrak{E} \end{Bmatrix} = \sqrt{k}\begin{pmatrix} \mathfrak{Y}^{-1} & \mathfrak{O} \\ \mathfrak{O} & \mathfrak{Y} \end{pmatrix}\begin{Bmatrix} \mathfrak{E} & -\mathfrak{X} \\ \mathfrak{O} & \mathfrak{E} \end{Bmatrix}, \tag{58}$$

where $\mathfrak{Y} = \sqrt{k}\cdot\mathfrak{A}^{-1}$, $\mathfrak{X} = -\mathfrak{A}^{-1}\mathfrak{B}$. Now $\mathfrak{Y}$ is positive hermitian. Put $\mathfrak{Z} = \mathfrak{X} + i\,\mathfrak{Y}$; then $\mathfrak{Z}$ is a complex matrix of order n and $\mathfrak{Y} = (\mathfrak{Z} - \mathfrak{Z}^*)/2i$ is positive hermitian. This space is also a generalization of the usual upper half of the complex z-plane in the same way as Siegel's. Thus positive h-abelian forms can be represented in a $(1, 1)$ way by points in a $(2n^2 + 1)$-dimensional real space.

It can also be seen that the space of complex matrices $\mathfrak{Z}$ with $(\mathfrak{Z} - \mathfrak{Z}^*)/2i$ positive hermitian is the space corresponding to the hermitian matrix $\mathfrak{T} = \sqrt{d}\begin{pmatrix} \mathfrak{D} & \mathfrak{E} \\ -\mathfrak{E} & \mathfrak{D} \end{pmatrix}$. The h-modular group is the unit group of $\mathfrak{T}$. The reduction theory of positive h-abelian matrices corresponds to construction of a fundamental domain in the $\mathfrak{Z}$-space for the units of $\mathfrak{T}$. The $\mathfrak{Z}$-space is thus the space of positive h-abelian forms of kernel 1. From [**8**] it follows that a fundamental domain in the $\mathfrak{Z}$-space for the h-modular group has a finite measure, in terms of the invariant measure in this homogeneous space. Since $\mathfrak{T}$ can represent zero non-trivially, this fundamental domain is not compact.

7. Generalizations. Siegel's considerations in [**11**] show that the positive abelian forms we have considered can be viewed as constituting homogeneous spaces of cosets G/C of a certain Lie group G by a closed maximal compact subgroup C. The reduction theory of positive abelian forms is equivalent to construction of fundamental domains for certain discrete groups H (the modular group and the h-modular group) acting in these spaces. Minkowski's reduction theory concerns the case where G is the full linear group, C is the orthogonal group, and H is the ordinary unimodular group. These ideas suggest that analogous results might be obtained by considering other types of coset spaces. We shall consider a simple example.

Let G be the group of complex matrices $\mathfrak{C}$ satisfying

$$\mathfrak{C}'\mathfrak{C} = k\mathfrak{E}, \tag{59}$$

$\mathfrak{E} = \mathfrak{E}_n$, and $k \neq 0$ a real number. The real orthogonal group g is a maximal, compact subgroup of G and the coset space G/g is homeomorphic to the space of positive hermitian matrices $\mathfrak{H}$ which satisfy (59). A little calculation shows that every positive hermitian matrix $\mathfrak{H}$ satisfying (59) has the parametric representation

$$\mathfrak{H} = \sqrt{k}\cdot(\mathfrak{E} - i\mathfrak{Y})(\mathfrak{E} + i\mathfrak{Y})^{-1}, \tag{60}$$

where $\mathfrak{Y}$ is a skew symmetric real matrix of order n satisfying $\mathfrak{E} + \mathfrak{Y}^2 > 0$. Let $n > 4$ and H the group of matrices $\mathfrak{C}$ whose elements are Gaussian integers and satisfying

$$\mathfrak{C}'\mathfrak{C} = \mathfrak{E}. \tag{61}$$

This is an infinite group and is a discrete subgroup of G. If $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are hermitian (not necessarily positive) in G we say that $\mathfrak{S}_1$ and $\mathfrak{S}_2$ are *equivalent* if for a matrix $\mathfrak{C}$ in H the relation $\mathfrak{S}_1 = \mathfrak{S}_2\{\mathfrak{C}\}$ holds. All equivalent hermitian matrices fall into a class. To obtain a reduction theory of positive hermitian matrices in G we proceed thus.

Let H_0 be the space of all positive hermitian matrices which are orthogonal. Let R_0 be the space of Humbert reduced positive hermitian matrices of determinant 1. Let Ω be the group of $n \times n$ matrices whose elements are Gaussian integers and whose determinant is ± 1. Let $\mathfrak{C}_1, \mathfrak{C}_2, \ldots$ be representatives of cosets of Ω/H. It can be seen as a simple consequence of Humbert's theory that

https://doi.org/10.4153/CJM-1952-031-8 Published online by Cambridge University Press

only finitely many $\mathfrak{C}_1$, $\mathfrak{C}_2, \ldots$ are such that $R_0(\mathfrak{C}_k^{-1})$ intersects H_0 in a non-empty set. Let $H_k = R_0(\mathfrak{C}_k^{-1}) \cap H_0$ and let

$$F = \sum_k (R_0(\mathfrak{C}_k^{-1}) \cap H_0).$$

Then F is a fundamental domain for H in H_0. Since $n > 4$, this fundamental domain F is non-compact but has a finite measure, in terms of the invariant measure in H. It can be proved that the invariant volume measure is

$$dV = |\mathfrak{E} + \mathfrak{Y}^2|^{\frac{1}{2}(1-n)}\{d\mathfrak{Y}\},$$

where $\{d\,\mathfrak{Y}\}$ is the Euclidean volume element in the space $\mathfrak{E} + \mathfrak{Y}^2 > 0$.

Let now $\mathfrak{S}$ in G be positive hermitian. To each $\mathfrak{S}$ associate a $\mathfrak{S}_1$ such that

(62) $$\sqrt{k}\cdot\mathfrak{S}_1 = \mathfrak{S}.$$

Then $\mathfrak{S}_1$ is a point of H_0. Choose $\mathfrak{C}$ in H in such a way that $\mathfrak{S}_1\{\mathfrak{C}\}$ is in F. We then call $\mathfrak{S}\{\mathfrak{C}\}$ *reduced*. It can then be deduced as a consequence of Humberts' reduction theory that there are only a finite number of classes of integral (Gaussian integers) positive hermitian $\mathfrak{S}$ with a given k. A consequence of this reduction theory is that H has a finite number of generators.

References

1. H. Braun, *Hermitian modular functions* III, Ann. Math., vol. 53 (1951), 143-160.
2. C. Chevalley, *Theory of Lie groups* I (Princeton, 1946).
3. G. Cotty, *Les fonctions abéliennes et la théorie des nombres*, Ann. Fac. Sci. Toulouse, ser. 3, vol. 3 (1911), 209-376.
4. C. Hermite, *Sur la théorie de la transformation des fonctions abéliennes*, Oeuvres, vol. 1 (Paris, 1905), 444-478.
5. P. Humbert, *Réduction de formes quadratiques dans un corps algébrique fini*, Comment. Math. Helv., vol. 23 (1949), 50-63.
6. F. Klein and R. Fricke, *Vorlesungen über die Theorie der Modul-Funktionen*, vol. 1 (Leipzig, 1890), 243-269.
7. E. Laguerre, *Sur le calcul des systèmes linéaires*, Oeuvres, vol. 1 (Paris, 1898), 221-267.
8. K. G. Ramanathan, *The theory of units of quadratic and hermitian forms*, Amer. J. Math., vol. 73 (1951), 233-255.
9. C. L. Siegel, *Einheiten quadratischer Formen*, Abh. Sem. Hansischen Univ., vol. 13 (1939), 209-239.
10. ———, *Symplectic geometry*, Amer. J. Math., vol. 65 (1943), 1-86.
11. ———, *Some remarks on discontinuous groups*, Ann. Math., vol. 46 (1945), 708-718.
12. B. L. van der Waerden, *Moderne Algebra*, vol. 1 (Berlin, 1930).

Tata Institute for Fundamental Research