PAPERS COMMUNICATED

89. *On the Transformation Theory of Siegel's Modular Group of the n-th. Degree.*

By Masao SUGAWARA.

(Comm. by T. TAKAGI, M.I.A., Nov. 12, 1937.)

C. L. Siegel[1] has defined the modular group of the n-th. degree in the following way:

Let E and 0 be n-dimensional unit and zero matrix respectively; J the $2n$-demensional matrix defined by

$$J=\begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}. \tag{1}$$

Then the $2n$-demensional matrices with rational integral components, satisfying the relation $M'JM=J$ are called the (homogeneous) *modular substitutions of the n-th. degree*,[2] and the group which they form, the *modular group of the n-th. degree.*

The usual modular substitutions resp. group are the modular substitutions resp. group of the 1st. degree in this sense, and some of their classical properties are extended by Siegel to the case of the n-th. degree. I will show in the following lines, how one can found the "transformation theory" for this modular group analogously to the classical one, in defining suitably the "transformation of the degree m."

We define first the *principal congruence group mod. m* in the usual manner; namely as the group $\Gamma(m)$ formed by modular substitutions $M^{(m)}$ satisfying the congruence

$$M^{(m)}\equiv\pm\begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix} \quad \text{mod. } m\,.$$

It is obviously an invariant subgroup of the modular group $\Gamma=\Gamma(1)$. Now I give the following

Definition: The $2n$-dimensional matrices T with rational integral components satisfying the relations

$$T'JT=mJ\,, \tag{2}$$

---

1) C. L. Siegel: Ueber die analytische Theorie der quadratischen Formen. I, Cf. also Krazer, Lehrbuch der Thetafunktionen.

2) Siegel calls these matrices "canonical," according to their signification in the theory of algebraic functions of the genus n. The inhomogeneous (or proper) modular substitution of the n-th. degree is the substitution bearing on the symmetrical matrices X of the dimension n: $X_1=(AX+B)\ (CX+D)^{-1}$ where A, B, C, D are n-dimensional matrices so that $M=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is "canonical." I confine myself in the following exposition to the direct consideration of *homogeneous* substitutions, as the transit to the inhomogeneous considerations present no difficulty: one has only to take the quotient group by the invariant subgroup consisting of two elements $\pm\begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix}$.

where J is the matrix defined by (1) and m is a natural number, are called the *transformations of the degree m.*

Let A, B, C, D be n-dementional "components" of $T: T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$. Then (2) is equivalent to the following conditions A, B, C, D:

$$(2') \qquad A'C=AC', \qquad B'D=D'B, \qquad A'D-C'B=mE.$$

So it is clear, that the above definition is equivalent to the classical one, when $n=1$.

We can easily prove that: If T is a transformation of the degree m, and $M_1, M_2 \in \Gamma$, M_1TM_2 is also a transformation of the same degree; If $M^{(m)} \in \Gamma(m)$, the matrix $T^{-1}M^{(m)}T$ is a modular substitution; and if $M^{(m)}$ runs over all the matrices in $\Gamma(m)$, the matrices $T^{-1}M^{(m)}T$ form an invariant subgroup of Γ which we call the *transformation group produced by T.*

If $T_1=MT$ and $M \in \Gamma$, T and T_1 produce the same transformation group.

Next, we define the primitivity of the transformation by the *Definition:* A transformation $T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of the degree m is called *primitive* if and only if it is possible to find a symmetrical pair of n-dimensional matrices U, V without left hand common divisor so that the congruences

$$UA+VC\equiv 0, \qquad UB+VD\equiv 0 \qquad \text{mod. } m.$$

are satisfied.

By the lemma 42 of Siegel, l. c. we can then form a modular substitution $M=\begin{pmatrix} U & V \\ X & Y \end{pmatrix}$ with the matrices U, V. So we can give to this definition also the following form:

T is primitive if and only if there exists a modular substitution M so that all the components in the upper half of the matrix MT be divisible by m.

The equivalency of this definition to the classical one in the case $n=1$ can be shown by elementary considerations. But in the general case it was difficut to me to find a simple relation between this definition and the existence of a left hand common divisor of A, B, C, D. It is, however, easy to prove that:
If T is an arbitrary primitive transformation, M_1TM_2 is also primitive and all primitive transformation of the same degree are obtained in this form.

Because by left hand multiplication of a modular substitution MM_1^{-1} to M_1TM_2, we have a transformation MTM_2 whose components in the upper half are divisible by m. For the proof of the second part, we can take for T a particular primitive transformation $\begin{pmatrix} mE & 0 \\ 0 & E \end{pmatrix}$.

Let T_1 be a primitive transformation of the degree m, then we can choose a modular substitution M_1 such that the substitution $T^{-1}M_1^{-1}T_1$ has rational integral components. For such M_1 $M_2=T^{-1}M_1^{-1}T_1$ becomes a modular substitution because $(T^{-1}M_1^{-1}T_1)'J(T^{-1}M_1^{-1}T_1)=J$.

The transformation groups produced by primitive transformations are therefore conjugate to each other in Γ.

We show finally that the number of the transformation group is finite.

We call two transformation T_1, T_2 *equivalent* if there exists $M\in\Gamma$, so that $T_1=MT_2$. This relation is obviously reflexive, symmetric and transitive. The equivalent transformations form a *class*. The transformations in a same class produce the same transformation group, as it was already remarked. So we have only to show the finiteness of the number of classes.

I prove now the following,

Theorem. From each class, one can choose the representative of the form,

$$T_0=\begin{pmatrix} A_0 & B_0 \\ C_0 & D_0 \end{pmatrix}, \quad A_0=(a_{ik}), \quad B_0=(b_{ik}), \quad D_0=(d_{ik}), \quad i,k=1,\ldots\ldots,n,$$

where the following conditions are satisfied:

a) $C_0=0$,

b) $a_{ik}=0$ for $i>k$, $i=1,\ldots\ldots,n$; $a_{kk}>a_{ik}\geqq 0$, for $i<k$, $k=1,\ldots\ldots,n$,

c) $A_0'D_0=mE$, so that in particular $a_{kk}\,d_{kk}=m$, $k=1,\ldots\ldots,n$; $d_{ik}=0$ for $i<k$,

d) $d_{kk}>b_{ik}\geqq 0$ for $i\leqq k$, $k=1,\ldots\ldots,n$,

e) $B_0'D_0=D_0'B_0$.

Each class contains just one representive of this form.

Corollary. The number of classes is finite.

Namely, the number of the matrices A is finite because of the 2nd conditions of b) and c). The matrix D_0 is determined with A_0, for from c) follows $D_0=m(A_0^{-1})'$. D_0 being determined, there is only finite possibilities for $b_{ik}(i\leqq k)$. But with these $b_{ik}(i\leqq k)$ are determined the other $b_{ik}(i>k)$ by the condition e).

To prove the theorem, we reduce a given transformation $T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ to the "normal form," by step by step multiplication of suitable modular substitutions from the left hand side. *Firstly*, let us remark, that in virture of the last relation in (2'), the left hand common divisor G of A' and C' can not have the determinant 0. Therefore there exists a non singular matrix G_0 such that $X_1=G_0^{-1}C'$, $Y_1=-G_0^{-1}A'$ have no more left hand common divisor. These matrices X, Y form as is easily seen, a symmetrical pair of matrices. Hence by the lemma 42 of Siegel l. c., we can form a modular substitution $M_1=\begin{pmatrix} U_1 & V_1 \\ X_1 & Y_1 \end{pmatrix}$ and have $C_1=0$ in $M_1T=\begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix}$.

Secondly, remark that we can get $A_0=UA_1$ in choosing a suitable n-dimentional unimodular matrix U_1 so that A_0 satisfies the condition b). We obtain $T_2=M_2T_1=\begin{pmatrix} A_0 & B_2 \\ 0 & D_0 \end{pmatrix}$ in taking the modular substitution

$M_2=\begin{pmatrix} U & 0 \\ 0 & U^{-1} \end{pmatrix}$. Here the matrix D_0 satisfies c), as T_2 is another transformation.

We take, in the *third* place, a modular substitution of the form $M_3=\begin{pmatrix} E & V \\ 0 & E \end{pmatrix}$ where $V=(v_{ik})$ is a symmetrical matrix. In choosing suitably v_{ik}, $i \leqq k$, $k=1, \ldots\ldots, n$, we can realise d) in $M_3T_2=\begin{pmatrix} A_0 & B_2+VD_0 \\ 0 & D_0 \end{pmatrix}=\begin{pmatrix} A_0 & B_0 \\ 0 & D_0 \end{pmatrix}=T_0$. The condition e) is again automatically satisfied, as T_0 is also a transformation.

It remains to show the uniqueness of our representive in a given class. Let $T=\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ and $\overline{T}=\begin{pmatrix} \overline{A} & \overline{B} \\ \overline{C} & \overline{D} \end{pmatrix}$ be two matrices satisfying the conditions a)–e), and $\overline{T}=MT$, $M \in \Gamma$. We have only to show that it follows hereof $M=\begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix}$.

Put $M=\begin{pmatrix} U & V \\ X & Y \end{pmatrix}$. From $MT=\overline{T}$ follow the equations in taking account of

$$C=\overline{C}=0\,; \quad UA=\overline{A}\,, \quad UB+VD=\overline{B}\,, \quad XA=0\,, \quad XB+YD=\overline{D}\,.$$

From the third equation folllows $X=0$ as $|A| \neq 0$. Then U must be unimodular, for $M \in \Gamma$. From the first equation follows then $U=E$. Therefore Y must also $=E$. $V=0$ follows at last from the 2nd equation $B+VD=\overline{B}$ and the fact that both B and $\overline{B}$ satisfy the condition d).