JOURNAL OF RESEARCH of the National Bureau of Standards—B. Mathematical Sciences
Vol. 72B, No. 4, October–December 1968

On the Multipliers of the Dedekind Modular Function

Joseph Lehner*

Institute for Basic Standards, National Bureau of Standards, Washington, D.C. 20234

(September 20, 1968)

The Dedekind modular function is defined by $\eta(\tau)=e^{\pi i\tau/12}\prod_{1}^{\infty}(1-e^{2\pi im\tau})$, Im $\tau>0$, and satisfies the transformation equation $(c\tau+d)^{-1/2}\eta(A\tau)=v(A)\eta(\tau)$ for every $A\epsilon\Gamma$, the modular group, where $v(A)$ is a complicated 24th root of unity depending on A. Let G be the set of all $A\epsilon\Gamma$ for which $v(A)=1$. *Then G is not a group*, but there are groups that are subsets of G, eg., $\{S^{24}\}$, where $S=\begin{pmatrix}1&1\\0&1\end{pmatrix}\cdot$ *Main Theorem.* Every subgroup of Γ that is a subset of G is cyclic. Moreover $G\subset\Gamma'$, the commutator subgroup of Γ.

Key Words: Cancellation; commutator subgroup; modular group; multiplier; word.

1. Let Γ be the matrix modular group, that is, $\Gamma=SL(2,Z)$, $Z=$ integers. The well-known Dedekind modular function $\eta(\tau)$ is defined by

$$\eta(\tau)=x^{1/24}\prod_{1}^{\infty}(1-x^m)=e^{\pi i\tau/12}\prod_{1}^{\infty}(1-e^{2\pi im\tau}), \tag{1}$$

where, throughout, $x=e^{2\pi i\tau}$ and Im $\tau>0$. The function η is a *modular form* of dimension $-1/2$ with *multiplier system* v; this means that

$$(c\tau+d)^{-1/2}\eta(A\tau)=v(A)\eta(\tau) \tag{2}$$

for each $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}\epsilon\Gamma$. Here $A\tau=(a\tau+b)/(c\tau+d)$ and $(c\tau+d)^{-1/2}$ is defined uniquely by setting, for each complex number u,

$$-\pi<\arg u\leqq\pi. \tag{3}$$

Moreover, the multiplier v is of modulus 1 and satisfies a consistency condition

$$v(AB)(c_{AB}\tau+d_{AB})^{1/2}=v(A)v(B)(c_AB\tau+d_A)^{1/2}(c_B\tau+d_B)^{1/2}, \tag{4}$$

where in general we write $A=\begin{pmatrix}a_A&b_A\\c_A&d_A\end{pmatrix}$. It is the multiplier system v that we wish to study.

The difficulty arises because η is a form of *fractional* dimension. For a form of dimension $-r$ the exponent r would occur in (4) instead of 1/2. Hence if r is integral, v is a homomorphism of Γ into the group of complex numbers of modulus 1. The subset G of Γ on which v is identically 1 is a subgroup of Γ.

This is no longer the case when r ceases to be an integer. *Then G is not a group*, but it does contain subgroups of Γ. For example, we see from (1) that $v(S^{24m})=1$, where

*University of Maryland and the National Bureau of Standards.

$$S=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}. \tag{5}$$

Hence the cyclic group $\{S^{24}\}$ is contained in G.

The main object of this paper is to establish the following conjecture of Rademacher:

THEOREM 1. *If H is a subgroup of Γ and a subset of G, then H is cyclic.*

We shall see that $G\subset\Gamma'$, the commutator subgroup of Γ. Thus H is a subgroup of Γ'. Since Γ' is free of rank 2, it follows from Theorem 1 that H is of infinite index in Γ' and is not normal. On the other hand, as well shall see later, G is of index 2 in Γ' in the sense that $\Gamma'=G\cup GS^{12}$ is a disjoint union and $v(AS^{12})=-1$ for every $A\epsilon G$.

2. We shall first treat a simpler case, namely, $\eta^2(\tau)$ with multipliers v^2. Here v^2 is a homomorphism and so, letting

$$G_1=\{A\epsilon\Gamma|v^2(A)=+1\},$$

we have

$$\Gamma'\subset G_1.$$

THEOREM 2. $G_1=\Gamma'$.

Since $[\Gamma:\Gamma']=12$—recall that we are dealing with the matrix groups—we have only to show that $[\Gamma:G_1]=12$. Since by (1) and (5), $v^2(S^h)=\exp \pi ih/6$, we see that $1, S, S^2, \ldots, S^{11}$ lie in different cosets of Γ/G_1. q.e.d.

We have already defined

$$G=\{A\epsilon\Gamma|v(A)=1\}.$$

Clearly $G\subset G_1$ and so

$$G\subset\Gamma'.$$

However, G is not a group. In fact, $-\begin{pmatrix}1 & 6\\ 0 & 1\end{pmatrix}\epsilon G$ but its inverse $-\begin{pmatrix}1 & -6\\ 0 & 1\end{pmatrix}$ does not. To discover what groups are contained in G, we must study (4) in detail.

Let us recall that we are writing modular matrices as

$$A=\begin{pmatrix}a_A & b_A\\ c_A & d_A\end{pmatrix},\ a_Ad_A-b_Ac_A=1.$$

If $c_A=0$, then $a_A=d_A=\pm 1$ and $A=\pm S^m$, $m=\pm b_A$. Define as usual

$$\operatorname{sgn} u=u/|u| \text{ for } u\neq 0.$$

For the systematic treatment of (4) we write $v(AB)=\sigma(A,B)v(A)v(B)$, so that

$$\sigma(A,B)=(c_AB\tau+d_A)^{1/2}(c_B\tau+d_B)^{1/2}(c_{AB}\tau+d_{AB})^{-1/2}. \tag{6}$$

Clearly $\sigma^2(A,B)=1$. Using the convention (3) together with (6) we obtain the following values:

$$v(I)=1,\ v(-I)=\exp(-\pi i/2),\ I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

$$\sigma(S^m,A)=\sigma(A,S^m)=1 \tag{7}$$

$$\sigma(A,A^{-1})=1,\ c_A\neq 0;\ \sigma(A,A^{-1})=\operatorname{sgn} d_A,\ c_A=0.$$

The last equation shows that

$$v(A^{-1}) = \bar{v}(A),\ c_A \neq 0;\ v(A^{-1}) = \operatorname{sgn} d_A \cdot \bar{v}(A),\ c_A = 0. \tag{8}$$

Next,

$$v(-A) = v(A) i \operatorname{sgn} c_A,\ c_A \neq 0;\ v(-A) = -v(A) i \operatorname{sgn} d_A,\ c_A = 0. \tag{9}$$

Finally we have the following table, in which a missing entry means that the sign is irrelevant.

c_A	c_B	c_{AB}	$\sigma(A, B)$
$+$	$+$	$+$	$+1$
$+$	$+$	$-$	-1
$+$	$-$		$+1$
$-$	$+$		$+1$
$-$	$-$	$-$	$+1$
$-$	$-$	$+$	-1
0	$+$		$\operatorname{sgn} d_A$
$+$	0		$\operatorname{sgn} d_B$
0	$-$		$+1$
$-$	0		$+1$

(10)

Let

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Note that

$$T^2 = R^3 = -I. \tag{11}$$

We introduce a symbol

$$V^{\epsilon} = -\epsilon R^{\epsilon},\ \epsilon = \pm 1,\ V^1 = V. \tag{12}$$

In V^{ϵ}, ϵ *is not an exponent,* and in fact we have

$$(V^{\epsilon})^{-1} = -V^{-\epsilon},\ VV^{-1} = V^{-1}V = -I,$$
$$VV = -V^{-1},\ V^{-1}V^{-1} = V. \tag{13}$$

Furthermore

$$TV=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}=S,\ TV^{-1}=\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}. \tag{14}$$

LEMMA 1. *Let*

$$A=TV^{\epsilon_1}\ \ldots\ TV^{\epsilon_m}=\begin{pmatrix}a_A & b_A\\ c_A & d_A\end{pmatrix},\ \epsilon_i^2=1.$$

Then

$$a_A>0,\ b_A\geqslant 0,\ c_A\geqslant 0,\ d_A>0.$$

This is an immediate consequence of (14). The set of words of this form is therefore a semigroup.

We partition the elements of Γ, aside from $\pm T$ and $\pm V^\epsilon$, into 8 classes, as follows. Each element can be written uniquely as a power product of T and V, apart from sign. We set ($\epsilon_1^2=1$)

$$\begin{aligned}
C_1&=\{A\epsilon\Gamma|A=TV^{\epsilon_1}\ \ldots\ TV^{\epsilon_m}\},\\
C_2&=\{A\epsilon\Gamma|A=V^{\epsilon_1}T\ \ldots\ V^{\epsilon_m}T\},\\
C_3&=\{A\epsilon\Gamma|A=TV^{\epsilon_1}\ \ldots\ V^{\epsilon_m}T\},\\
C_4&=\{A\epsilon\Gamma|A=V^{\epsilon_1}T\ \ldots\ TV^{\epsilon_m}\},\\
-C_i&=\{A\epsilon\Gamma|-A\epsilon C_i\},\ i=1,2,3,4.
\end{aligned} \tag{15}$$

Since $(TV^\epsilon)^{-1}=V^{-\epsilon}T$, we observe that (in an obvious notation)

$$C_1^{-1}=C_2,\ C_3^{-1}=-C_3,\ C_3=C_1T,\ C_4^{-1}=-C_4,\ C_4=-TC_1 \tag{16}$$

Lemma 1 can now be restated: $A\epsilon C_1$ implies $a_A,\ d_A>0$; $b_A,\ c_A\geqslant 0$.

LEMMA 2. $v(S^m)=\exp(\pi im/12)$, $v(-S^m)=\exp(\pi i(m-6)/12)$, $v(\pm T)=\exp(\mp\pi i/4)$, $v(TV^\epsilon)=\exp(\pi i\epsilon/12)$.

The first values are immediate from the definition (1), and $v(T)$ is obtained from the classical transformation formula

$$\eta(T\tau)=(-i\tau)^{1/2}\eta(\tau).$$

Then use $R=TS$, $V^\epsilon=-\epsilon R^\epsilon$, and (8), (9), (10).

LEMMA 3. *When* $A\epsilon C_1$, $v(A)=exp(\pi i(\nu/12)$, *where*

$$\nu=\nu(A)=\sum_{i=1}^m\epsilon_i.$$

The lemma is true when $m=1$, by Lemma 2. Suppose it is true for all words $\prod_1^h TV^{\epsilon_i}$, $h<m$, and let $A=\prod_1^m TV^{\epsilon_i}$. What we need to show is $v(ATV^\epsilon)=v(A)v(TV^\epsilon)$, in other words,

$$\sigma(A,TV^\epsilon)=1. \tag{*}$$

Now by Lemma 1, $c_A\geqslant 0$. When $\epsilon=1$, $TV^\epsilon=S$ and when $c_A=0$, $A=S^m$ (by Lemma 1). In both cases (*) follows from (7). In the remaining case $c_A>0$ and $\epsilon=-1$, and (*) follows from line 1 of table (10) and (14), since

$$\begin{pmatrix} \cdot & \cdot \\ \geqslant 0 & >0 \end{pmatrix}\begin{pmatrix} 1 & \cdot \\ 1 & \cdot \end{pmatrix}=\begin{pmatrix} \cdot & \cdot \\ >0 & \cdot \end{pmatrix}.$$

3. We are now ready to begin the proof of Theorem 1. We assume there is a subgroup of Γ' that is contained in G and is not cyclic. This subgroup, then, contains a free group H of rank 2 as a subgroup and $H \subset G$. We denote by $\{A, B\}$ the group generated by A and B.

Every $A \epsilon \Gamma'$ falls into one and only one of the 8 classes of (15). If we write $A = \pm T^{\epsilon} V^{\epsilon_1} \ldots V^{\epsilon_m} T^{\epsilon'}$ with ϵ, $\epsilon' = 0$, 1 and $\epsilon_i^2 = 1$, we can define the *length* of A to be m and denote it by $|A|$. From all $H = \{A, B\}$ select one, say $H_0 = \{A_0, B_0\}$, such that $|A_0| + |B_0|$ is a minimum. This minimum is positive; call it ρ.

When we multiply two words, there may be internal cancellations. For example, suppose $A_0 = \left(\prod_1^m TV^{\epsilon_i}\right) \cdot T$, $B_0 = \prod_1^n TV^{\eta_i}$. Then if $\epsilon_m = -\eta_1$, the factor $V^{\epsilon_m} TTV^{\eta_1}$ will disappear from $A_0 B_0$. Let $|A_0| \geqslant |B_0|$ and suppose B_0 cancels completely in $A_0 B_0$. Then $|A_0 B_0| = |A_0| - |B_0|$ and $|A_0 B_0| + |B_0| = |A_0| < \rho$. Since $\{A_0, B_0\} = \{A_0 B_0, B_0\}$, this is a contradiction. Hence there is a smallest interger $h \geqslant 0$ such that

$$w = \operatorname{sgn}(\epsilon_{m-h} + \eta_{1+h}) \tag{17}$$

is not zero. Similarly, by considering $B_0 A_0$, $B_0^{-1} A_0$, and $B_0 A_0^{-1}$, we deduce the existence of minimal nonnegative integers j, k, l such that

$$z = \operatorname{sgn}(\eta_{n-j} + \epsilon_{1+j}), \qquad x = \operatorname{sgn}(-\eta_{1+k} + \epsilon_{1+k}), \qquad y = \operatorname{sgn}(\eta_{n-l} - \epsilon_{m-l}) \tag{18}$$

are all nonzero. We shall use the quantities x, y, z, w systematically.

From now on we write A for A_0 and B for B_0.

Next we must develop rules that will enable us to multiply elements of the different classes. In the event of internal cancellations we shall have to take account of the relations (11) and (13). The following possibilities arise:

$$V^{\epsilon} TTV^{-\epsilon} = TV^{\epsilon} V^{-\epsilon} T = I, \ \epsilon = \pm 1 \tag{19}$$

$$V^{\epsilon} TTV^{\eta} = uV^{-u}, \ TV^{\epsilon} V^{\eta} T = -uTV^{-u} T, \ \eta = \pm 1 \tag{20}$$

where $u = \operatorname{sgn}(\epsilon + \eta) \neq 0$. Suppose (19) occurs in the product AB. Then the exponent sum $\nu(AB) = \nu(A) + \nu(B)$. If (20) occurs, $\nu(AB) = \nu(A) + \nu(B) - \epsilon - \eta - u = \nu(A) + \nu(B) - 3u$, since either $\epsilon = \eta = u = 1$ or $\epsilon = \eta = u = -1$. Furthermore, we multiply the word AB by u in the first case of (20) and by $-u$ in the second case.

An example will make the technique clear. Consider BA, where $A \epsilon C_1$, $B \epsilon C_3$. Let $A = \prod_1^m TV^{\epsilon_i}$, $B = \left(\prod_1^n TV^{\eta_i}\right) \cdot T$. Here we have a cancellation of the type $V^{\eta} TTV^{\epsilon}$. Since z, defined in (18), is the sign of the first nonvanishing sum $\eta_n + \epsilon_1$, $\eta_{n-1} + \epsilon_2$, . . ., we have $BA = zDT$ with $D \epsilon C_1$ and $\nu(D) = \nu(B) + \nu(A) - 3z$.

On the other hand suppose A is as before but $B \epsilon C_1$, $B = \prod_1^n TV^{\eta_i}$. Then in AB^{-1} there is a cancellation of the type $TV^{\epsilon} V^{-\eta} T$, so that $AB^{-1} = yDT$, since $-y = \operatorname{sgn}(\epsilon_{m-l} - \eta_{n-l})$. Also $\nu(D) = \nu(A) - \nu(B) + 3y$.

One final rule. If $A \epsilon \pm C_3$ or $\pm C_4$, then for every appearance of A^{-1} in the word we are considering we must multiply by -1, since

$$\left\{\left(\pm \prod_1^m TV^{\epsilon_i}\right) \cdot T\right\}^{-1} = -\left(\pm \prod_1^m TV^{-\epsilon_{m-i}}\right) \cdot T \text{ and } \left\{\left(\pm \prod_1^{m-1} V^{\epsilon_i} T\right) \cdot V^{\epsilon_m}\right\}^{-1} = -\left(\pm \prod_1^m V^{-\epsilon_{m-i}}\right) \cdot V^{-\epsilon_1}.$$

4. We now proceed as follows. The generators A, B of H lie in the classes $\pm C_i$, $i=1, \ldots, 4$. For each possible pair A, B we shall exhibit a word $W(A, B)$ that does not belong to G.

Since $A, B \epsilon G$, $\{A\}, \{B\} \subset G$.

LEMMA 4. *If $A \epsilon -C_1$ or $A \epsilon -C_2$, then $\{A\} \not\subset G$.*

Suppose first $A=-C_1$, $c_A=0$. Then $-A \epsilon C_1$ and, by Lemma 1, $A=-S^m$. By Lemma 2, $v(A) = \exp(\pi i(m-6)/12)$, $v(A^2)=v(S^{2m})=\exp(\pi i \cdot 2m/12)$. Hence $v(A)$, $v(A^2)$ cannot both equal 1, i.e., A and A^2 do not both belong to G. Next assume $c_A \neq 0$; it follows from Lemma 1 that $c_A < 0$. Hence $-A$ has all entries positive except $b_A \geqslant 0$ and so the c of $-A^2$ is positive. By line 1 of table 10, $\sigma(-A, -A)=1$. Therefore

$$v(A^2)=v(-A \cdot -A)=(v(-A))^2.$$

By (9), $v(A)$ and $v(-A)$ are not both real, hence $v(A)=v(A^2)=1$ is impossible.

Since $(-C_2)^{-1}=-C_1$, the result follows for $-C_2$.

LEMMA 5. *Let $D \epsilon C_1$, $\epsilon=\pm 1$. Then*

$$\sigma(D, \epsilon T)=\sigma(\epsilon T, D)=\sigma(-T, DT)=1.$$

These results are proved by reference to table (10) and (7). By Lemma 1, $c_D \geqslant 0$, $d_D > 0$. Note that when $c_D > 0$, the c of $D \cdot \epsilon T$ and of ϵTD has sign ϵ.

The proof is now divided into cases: $A \epsilon \pm C_i$, $B \epsilon \pm C_j$, $i, j=1, \ldots, 4$, where we may obviously assume $j \geqslant i$. Lemma 4 shows we need not consider the classes $-C_1$ or $-C_2$. And in view of (16) we may disregard the classes $-C_3$ and $-C_4$ as well as C_2. There remain the cases: $A \epsilon C_1$, $B \epsilon C_1, C_3, C_4$; $A \epsilon C_3$, $B \epsilon C_3, C_4$; $A, B \epsilon C_4$. In each case we shall write the "cancellation rules" (cf. end of sec. 3) and exhibit a word in A and B for which $v=-1$.

$A \epsilon C_1$, $B \epsilon C_1$

	AB	AB^{-1}	$A^{-1}B$	$A^{-1}B^{-1}$	BA^{-1}	$B^{-1}A$
multiply by	1	y	$-x$	1	$-y$	x
add to exponent sum	0	$3y$	$3x$	0	$-3y$	$-3x$.

Here x, y are defined in (18) and

$$A=\prod_1^m TV^{\epsilon_i}, \qquad B=\prod_1^n TV^{\eta_i}.$$

Recall also (Lemma 6) that $\nu(A) \equiv \nu(B) \equiv 0 \pmod{24}$. The words for which $v=-1$ are as follows:

$$y>0; \qquad B^{-1}ABA^{-1}BA^{-1}$$

$$y<0, \qquad x>0; \qquad B^{-1}AB^{-1}$$

$$y<0, \qquad x<0; \qquad B^{-1}ABA^{-1}B^{-1}A.$$

$A \epsilon C_1$, $B \epsilon C_3$

	AB	AB^{-1}	$A^{-1}B$	$A^{-1}B^{-1}$	BA^{-1}	$B^{-1}A$	$B^{-1}A^{-1}$
multiply by	1	1	$-x$	$-z$	1	x	1
add to exponent sum	0	0	$3x$	$3z$	0	$-3x$	0.

Recall that when B^{-1} occurs a minus sign must be prefixed. Also $\nu(A) \equiv 0$, $\nu(B) \equiv 3 \pmod{24}$ by Lemma 6. The words are:

$$x > 0; \quad B^{-1}AB^{-1}$$

$$x < 0, \quad z > 0; \quad BA^{-1}B^{-1}AB$$

$$x < 0, \quad z < 0; \quad B^{-1}AB^{-1}A^{-1}B^{-1}.$$

AϵC$_1$, BϵC$_4$

	AB	$A^{-1}B$	$A^{-1}B^{-1}$	BA	BA^{-1}	$B^{-1}A$
multiply by	$-w$	1	1	1	$-y$	1
add to exponent sum	$-3w$	0	0	0	$-3y$	0.

Here $\nu(A) \equiv 0$, $\nu(B) \equiv -3 \pmod{24}$. When B^{-1} occurs, multiply by -1. The words are:

$$w > 0; \quad A^{-1}BAB$$

$$w < 0, \quad y > 0; \quad ABA^{-1}BA^{-1}$$

$$w < 0; \quad y < 0; \quad B^{-1}ABA^{-1}B^{-1}A$$

AϵC$_3$, BϵC$_3$

	AB	AB^{-1}	$A^{-1}B$	$A^{-1}B^{-1}$	BA	BA^{-1}	$B^{-1}A$	$B^{-1}A^{-1}$
multiply by	w	$-y$	$-x$	$-z$	z	y	x	$-w$
add to exponent sum	$-3w$	$3y$	$3x$	$3z$	$-3z$	$-3y$	$-3x$	$3w.$

When A^{-1} or B^{-1} occurs, prefix a minus sign; $\nu(A) \equiv \nu(B) \equiv 3 \pmod{24}$. The words are:

$$w < 0; \quad AB$$

$$z < 0; \quad BA$$

$$w, z > 0, \quad xy < 0; \quad ABA^{-1}BA^{-1}B$$

$$w, z > 0; \quad x, y > 0; \quad AB^{-1}A^{-1}B$$

$$w, z > 0; \quad x, y < 0; \quad A^{-1}B^{-1}A^{-1}BAB^{-1}.$$

AϵC$_3$, BϵC$_4$

In this case no internal cancellation ever occurs. We have, since $\nu(A) \equiv 3$, $\nu(B) \equiv -3 \pmod{24}$,

$$AB^{-1}A = -DT, \qquad D\epsilon C_1$$

with $\nu(D) \equiv 9 \pmod{24}$; the minus sign is caused by the presence of B^{-1}. Hence

$$v(AB^{-1}A) = v(D)v(-T) = \exp((\pi i/12)(9+3)) = -1.$$

$A \epsilon C_4$, $B \epsilon C_4$

	AB	AB^{-1}	$A^{-1}B$	BA	BA^{-1}	$B^{-1}A$	$B^{-1}A^{-1}$
multiply by	$-w$	y	x	z	$-y$	$-x$	w
add to exponent sum	$-3w$	$3y$	$3x$	$3z$	$-3y$	$-3x$	$3w.$

When A^{-1} or B^{-1} occurs, prefix a minus sign; $\nu(A) \equiv \nu(B) \equiv -3 \pmod{24}$. The words are:

$$x > 0, \quad y > 0; \quad A^{-1}B^{-1}A^{-1}BAB^{-1}$$

$$x > 0, \quad y < 0; \quad A^{-1}BA^{-1}$$

$$x < 0, \quad y > 0; \quad B^{-1}AB^{-1}$$

$$x < 0, \quad y < 0; \quad AB^{-1}A^{-1}BAB.$$

This completes the proof of Theorem 1.

5. We conclude with a list of generators for all cyclic subgroups of Γ' that are contained in G. Let $\{A\}$ be such a subgroup; then we may assume A is in one of the classes C_1, C_3, C_4 in view of Lemma 4 and (16).

Suppose $A \epsilon C_1$. Since $A \epsilon G$ we have $\nu(A) \equiv 0 \pmod{24}$ by Lemma 6. Suppose $c_A \neq 0$, i.e., $c_A > 0$. For $l \geqslant 1$, $A^l \epsilon C_1$ and $\nu(A^l) = l\nu(A)$. Thus the condition on $\nu(A)$ insures $v(A^l) = 1$, $l \geqslant 1$. Also the c of A^l is positive and so $v(A^{-l}) = \bar{v}(A^{-l}) = 1$, by (8). If $c_A = 0$ we have $A = S^m$, $24|m$ is necessary and sufficient for $\{S^m\}$ to lie in G. But $\nu(S^m) = m$. Thus $A \epsilon C_1$ generates a cyclic group contained in G if and only if

$$\nu(A) \equiv 0 \pmod{24}.$$

Next let $A \epsilon C_3$. By Lemma 6 we have $\nu(A) \equiv 3 \pmod{24}$. Also $c_A > 0$ always. Let $h \geqslant 0$ be the smallest integer such that

$$t = \operatorname{sgn}(\epsilon_{m-h} + \epsilon_{1+h}) \tag{21}$$

is not zero, where $A = \left(\prod_1^m TV^{\mathscr{E}_i}\right) \cdot T$. If such an h does not exist, we would have $A^2 = -I$ and $\{A\}$ could not be a subgroup of the free group Γ'. Hence the existence of t is a necessary condition on A.

Multiplying A by A involves a concellation that has the effect of multiplying the word by t and adding $-3t$ to the exponent sum. Hence for $l \geqslant 1$,

$$A^l = t^{l-1}DT,\ D \epsilon C_1,\ \nu(D) \equiv 3l - 3(l-1)t \pmod{24}$$

and

$$v(A^l) = \exp\{(\pi i/12)(-3t^{l-1} + 3l - 3(l-1)t\}.$$

Hence $t=1$ is necessary and sufficient for $v(A^l)=1$, $l>0$. Since the c of $A^l=\pm DT$ is never zero, $v(A^{-l})=1$ also when $t=1$.

By similar reasoning we develop conditions in the case $A\epsilon C_4$ and then have the following

THEOREM 3. *Necessary and sufficient that a modular matrix A generate a group that is a subgroup of* Γ' *and a subset of G is that A satisfy the following conditions: A or* A^{-1} *lies in* C_1, C_3, *or* C_4 *and*

$$v(A') \equiv 0 \ (mod\ 24),\ if\ A.\epsilon C_1$$

$$v(A') \equiv 3 \ (mod\ 24)\ and\ t=1,\ if\ A'\epsilon C_3$$

$$v(A') \equiv -3 \ (mod\ 24)\ and\ t=-1,\ if\ A'\epsilon C_4.$$

Here A' *is A or* A^{-1} *and t is defined by* (21).

(Paper 72B4–275)