DET KGL. DANSKE VIDENSKABERNES SELSKAB
MATEMATISK-FYSISKE MEDDELELSER, BIND XXV, NR. 18

A STUDY CONCERNING THE CONGRUENCE SUBGROUPS OF THE MODULAR GROUP

BY

JAKOB NIELSEN

KØBENHAVN
I KOMMISSION HOS EJNAR MUNKSGAARD
1950

Printed in Denmark
Bianco Lunos Bogtrykkeri

Among the subgroups of the modular group the congruence subgroups with respect to a prime have been the chief subject of detailed studies during the initial development of the theory of elliptic modular functions by Felix Klein, Adolf Hurwitz, Walter Dyck, Gierster and other authors. Most of their papers on this subject are contained in volumes X—XX of the *Mathematische Annalen.* An elaborate exposition has been given in volume I of the *Theorie der elliptischen Modulfunktionen* by F. Klein and R. Fricke (Teubner, Leipzig 1890), where more information about the literature on the subject is to be found.

The way in which the question of the congruence groups is approached in these previous investigations contains elements of an arithmetical character, of function theory, non-euclidean geometry, topology, and group theory. It seems worth while to give an introduction to the theory of congruence groups in which the rôle of these separate elements and especially the abstract group-theoretical characteristics are brought out more clearly. For all primes which satisfy a certain arithmetical condition (given in section I) I shall attempt to give such a deduction on the following pages.

I.

Let q be a prime greater than 5. (Without this restriction some special reservations concerning the values 2, 3 and 5 would be necessary in the sequel and, on the other hand, no new facts of interest concerning these cases are obtained. Hence we omit them for simplicity.)

We put $q = 2r+1$, thus $r = \frac{q-1}{2}$.

All congruences occurring in the sequel are to be understood modulo q unless otherwise stated.

For every residue class $c \not\equiv 0$ the congruence

$$0 \equiv c^{2r} - 1 = (c^{r} - 1)(c^{r} + 1)$$

holds, hence

$$c^{r} \equiv 1 \text{ or } -1,$$

since q is a prime. If r is the least positive exponent satisfying this congruence, we say that c belongs to r.

We restrict q by the condition that 2 belongs to r. No further restriction will be imposed on q.

If c is not the zero class, $c \not\equiv 0$, it possesses a reciprocal class c^{-1} defined by the congruence $cc^{-1} \equiv 1$. Since $-2r \equiv 1$, we get in particular

$$2^{-1} \equiv -r \equiv r + 1, \tag{1}$$

and hence the classes of r and $r+1$ belong to r. Thus the congruence

$$r^{2y} \equiv 1,$$

which is equivalent to

$$r^{y} \equiv \pm 1,$$

implies

$$y \equiv 0 \text{ modulo } r.$$

Hence the expression r^{2y} yields all quadratic residues exactly once, if y ranges over a complete system of residue classes modulo r.

II.

In this section we define some simple auxiliary functions of an arithmetical character.

II, 1. Let z denote the set of all residue classes ϱ modulo q except the zero class:

$$\varrho \not\equiv 0. \tag{z}$$

This set z forms a group by multiplication. On this set we define a function $\tau(\varrho)$, which is a residue class modulo r, by

$$(2) \qquad r^{2\tau(\varrho)} \equiv \varrho^2, \quad \varrho \not\equiv 0 .$$

It follows from the last remark in section I that the residue class $\tau(\varrho)$ is uniquely determined by the definition (2). This definition of $\tau(\varrho)$ may also be written

$$(3) \qquad r^{\tau(\varrho)} \equiv \pm \varrho .$$

It is immediately inferred that τ has the following properties

$$\left.\begin{array}{ll} (4) & \tau(-\varrho) \equiv \tau(\varrho), \\ (5) & \tau(\varrho_1 \varrho_2) \equiv \tau(\varrho_1) + \tau(\varrho_2), \\ (6) & \tau(\pm 1) \equiv 0 . \end{array}\right\} \text{ modulo } r.$$

In consequence of (5) and (6) we get

$$(7) \qquad \tau(\varrho) + \tau(\varrho^{-1}) \equiv 0 \text{ modulo } r.$$

In particular

$$(8) \qquad \tau(r) \equiv 1 \equiv \tau(-r) \equiv \tau(r+1) \text{ modulo } r$$

and hence for the reciprocal class

$$(9) \qquad \tau(2) \equiv -1 \equiv \tau(-2) \text{ modulo } r.$$

II, 2. Let Z denote the set of all "three-sets" $[\varrho, \sigma, \omega]$, where ω denotes a residue class modulo r, and ϱ and σ denote residue classes modulo q with the additional condition that ϱ is an element of z:

$$(Z) \qquad [\varrho, \sigma, \omega], \quad \left\{\begin{array}{ll} \varrho \not\equiv 0 & \text{modulo } q \\ \sigma \text{ arbitrary} & \text{modulo } q \\ \omega \text{ arbitrary} & \text{modulo } r. \end{array}\right.$$

Z comprises $\frac{1}{2} q(q-1)^2$ elements. We now put

$$(10) \qquad \varphi(\varrho, \sigma) \equiv \varrho(\varrho\sigma - 1)$$

and define on the set Z a function g, which is itself a three-set, by

$$(11) \quad g[\varrho, \sigma, \omega] = [\varrho_g, \sigma_g, \omega_g] \equiv [-\varrho^{-1}, \varphi(\varrho, \sigma),\ \omega + \tau(\varrho)],$$

τ being the function defined in II, 1; the congruence sign refers to modulus q for the first two numbers in the three-set and to modulus r for the last one. Since $-\varrho^{-1} \not\equiv 0$, the three-set $g\,[\varrho, \sigma, \omega]$ belongs to Z. We can thus repeat the operation g, and we get

$$g_2\,[\varrho, \sigma, \omega] = g\,[\varrho_g, \sigma_g, \omega_g] \equiv [\varrho, \sigma, \omega],$$

since

$$(12)\quad \begin{cases} -(-\varrho^{-1})^{-1} \equiv \varrho, \\ \varphi(-\varrho^{-1}, \varrho(\varrho\sigma - 1)) \equiv -\varrho^{-1}\{-\varrho^{-1}\varrho(\varrho\sigma - 1) - 1\} \\ \qquad \equiv \varrho^{-1}\{\varrho\sigma - 1 + 1\} \equiv \sigma, \\ \omega + \tau(\varrho) + \tau(-\varrho^{-1}) \equiv \omega \text{ modulo } r \text{ by (4) and (7).} \end{cases}$$

Hence g is an involutory transformation of the set Z into itself. This transformation leaves no three-set invariant. In particular, the congruences

$$\sigma_g \equiv \sigma \text{ modulo } q$$
$$\omega_g \equiv \omega \text{ modulo } r$$

cannot hold simultaneously.

In fact, if $\varrho \not\equiv \pm 1$, then $\tau(\varrho) \not\equiv 0$ modulo r, and thus

$$\omega_g \equiv \omega + \tau(\varrho) \not\equiv \omega \text{ modulo } r;$$

if $\varrho \equiv \pm 1$, we get from (10)

$$\sigma_g \equiv \sigma \mp 1 \not\equiv \sigma.$$

The elements of Z are thus distributed in pairs by g.

II, 3. Let z' denote the set of all residue classes ϱ modulo q except 0 and -1:

$$(z')\qquad \varrho \not\equiv \begin{cases} 0 \\ -1. \end{cases}$$

On this set z' we define a function $f(\varrho)$, which is itself a residue class modulo q, by

$$(13)\qquad f(\varrho) \equiv -(1 + \varrho^{-1}).$$

In virtue of the condition (z') the class ϱ^{-1} exists, and it is neither 0 nor -1. Hence $f(\varrho)$ is neither 0 nor -1. We can thus repeat the application of f and get

$$f_2(\varrho) = f(f(\varrho)) \equiv -1+(1+\varrho^{-1})^{-1} \equiv -(1+\varrho)(1+\varrho)^{-1}+\varrho(1+\varrho)^{-1},$$

$$(14) \qquad f_2(\varrho) \equiv -(1+\varrho)^{-1},$$

$$f_3(\varrho) = f(-(1+\varrho)^{-1}) \equiv -1+1+\varrho$$

$$(15) \qquad f_3(\varrho) \equiv \varrho.$$

This shows that f is a one-one transformation of order 3 in the set z'.

We may therefore arrange the elements of z' in cyclical subsets of three elements except when invariant under f. We repeat for convenience the general cycle as expressed by (13), (14), and (15):

$$(16) \qquad \varrho \to -(1+\varrho^{-1}) \to -(1+\varrho)^{-1} \to \varrho$$

and note the special case, having regard to (1):

$$(17) \qquad 1 \to -2 \to r \to 1.$$

The latter is not invariant, since we have assumed $q \neq 3$.

It is observed that

$$(18) \qquad \varrho \cdot f(\varrho) \cdot f_2(\varrho) \equiv \varrho(1+\varrho^{-1})(1+\varrho)^{-1} \equiv 1.$$

II, 4. Let Z' denote the set of three-sets with the first symbol belonging to z':

$$(Z') \qquad [\varrho, \sigma, \omega], \quad \begin{cases} \varrho \not\equiv 0 \text{ and } -1 & \text{modulo } q \\ \sigma \text{ arbitrary} & \text{modulo } q \\ \omega \text{ arbitrary} & \text{modulo } r. \end{cases}$$

Z' contains $\frac{1}{2} q(q-1)(q-2)$ elements. On this set we define a function G, which is itself a three-set, by

$$(19) \qquad G[\varrho, \sigma, \omega] = [\varrho_G, \sigma_G, \omega_G] \equiv [f(\varrho), \varphi(\varrho, \sigma), \omega+\tau(\varrho)].$$

This three-set belongs to Z', since $f(\varrho)$ belongs to z'. For the same reasons as with Z, this transformation G leaves no three-set invariant; in particular, the second and third symbol are not invariant simultaneously. By repeating this operation we get

$$\tag{20} \left\{ \begin{aligned} G_2[\varrho,\sigma,\omega] &= G[\varrho_G,\sigma_G,\omega_G] = [\varrho_{G_2},\sigma_{G_2},\omega_{G_2}] \\ &\equiv [f_2(\varrho),\varphi_2(\varrho,\sigma),\omega+\tau(\varrho)+\tau(f(\varrho))], \\ \varphi_2(\varrho,\sigma) &\equiv f(\varrho)\{f(\varrho)\varphi(\varrho,\sigma)-1\} \\ &\equiv -(1+\varrho^{-1})\{-(1+\varrho^{-1})\varrho(\varrho\sigma-1)-1\} \\ &\equiv (1+\varrho)\{(1+\varrho^{-1})(\varrho\sigma-1)+\varrho^{-1}\} \\ &\equiv (1+\varrho)\{(1+\varrho)\sigma-1\}, \end{aligned} \right.$$

and with one more repetition

$$\tag{21} \left\{ \begin{aligned} & G_3[\varrho,\sigma,\omega] = G[\varrho_{G_2},\sigma_{G_2},\omega_{G_2}] \equiv [\varrho,\sigma,\omega], \text{ since} \\ & \qquad f_3(\varrho) \equiv \varrho \text{ by } (15), \\ & \quad \varphi_3(\varrho,\sigma) \equiv f_2(\varrho)\{f_2(\varrho)\varphi_2(\varrho,\sigma)-1\} \\ & \qquad \equiv -(1+\varrho)^{-1}\{-(1+\varrho)^{-1}(1+\varrho)((1+\varrho)\sigma-1)-1\} \\ & \qquad \equiv (1+\varrho)^{-1}\{(1+\varrho)\sigma-1+1\} \equiv \sigma, \\ & \omega+\tau(\varrho)+\tau(f(\varrho))+\tau(f_2(\varrho)) \equiv \omega \text{ modulo } r \text{ by } (18), (5) \text{ and } (6). \end{aligned} \right.$$

Thus G is a one-one transformation of Z' of order 3 without any invariant element, and it distributes the elements of Z' in cycles of three each, the explicit scheme being

$$\tag{22} \begin{aligned} [\varrho,\sigma,\omega] &\rightarrow \left[-(1+\varrho^{-1}),\varrho(\varrho\sigma-1),\omega+\tau(\varrho)\right] \\ &\rightarrow \left[-(1+\varrho)^{-1},(1+\varrho)\{(1+\varrho)\sigma-1\},\omega+\tau(\varrho)+\tau(1+\varrho^{-1})\right] \\ &\rightarrow \left[\varrho,\sigma,\omega\right]. \end{aligned}$$

III.

Let $r(q+1)$ simple, oriented polygons be given, each of which has q sides. We intend to combine these polygons into a two-dimensional, closed, orientable manifold Φ by certain identifications of pairs of sides. This is done in an abstract, purely topological way so that (in this section and the next two) no question of metric comes in.

As in section II, the symbol ω denotes residue classes modulo r, while ϱ and σ denote residue classes modulo q. Let r of the polygons be denoted by $P(\omega)$ and called "central polygons", the remaining qr polygons being denoted by $P(\sigma, \omega)$ and called "peripheric polygons"; here ω ranges over all residue classes modulo r and σ over all residue classes modulo q. Let $s(\sigma, \omega)$ denote the sides of $P(\omega)$, the numbering σ of these sides proceeding in the positive sense of the oriented polygons, and $s(\varrho, \sigma, \omega)$ the sides of $P(\sigma, \omega)$, the numbering ϱ likewise proceeding in the positive sense. With these denotations we define the following identifications:

(A) For all values of σ and ω the side $s(\sigma, \omega)$ of $P(\omega)$ and the side $s(0, \sigma, \omega)$ of $P(\sigma, \omega)$ coincide with opposite senses.

This disposes of all sides of all central polygons and of the sides $s(0, \sigma, \omega)$ of all peripheric polygons. So we are left with all sides $s(\varrho, \sigma, \omega)$, $\varrho \not\equiv 0$, of the peripheric polygons, and these sides thus correspond to the set Z of three-sets. For these sides we define:

(B) The coincidence of these sides in pairs is given by the involutory transformation g: The side $s(\varrho, \sigma, \omega)$ coincides with $s(\varrho_g, \sigma_g, \omega_g)$ with opposite senses.

Since the two last numbers of the three-set are not left invariant simultaneously, no side coincides with a side of the same polygon.

We now establish the cycles of vertices resulting from these identifications by turning around these vertices in the positive sense. Starting in the central polygon $P(\omega)$ we leave it over the side $s(\sigma, \omega)$ and enter across the coinciding side $s(0, \sigma, \omega)$ according to definition (A) into the peripheric polygon $P(\sigma, \omega)$. The preceding side of this polygon is $s(-1, \sigma, \omega)$, which coincides with the side $s(1, \sigma+1, \omega)$ of the peripheric polygon $P(\sigma+1, \omega)$ according to definition (B). The preceding side of this polygon is $s(0, \sigma+1, \omega)$, which coincides with the side $s(\sigma+1, \omega)$ of the central polygon $P(\omega)$, and the preceding side of this polygon is $s(\sigma, \omega)$, with which we started. So we get a cycle of vertices as illustrated by fig. 1.

In this process σ and ω are arbitrary within their range. Therefore all vertices of central polygons are involved. We may also remark that, if we leave an arbitrary peripheric polygon $P(\sigma, \omega)$ by crossing its side $s(-1, \sigma, \omega)$ and turn in the positive sense, we get the cycle of vertices just now established. Likewise, if we leave $P(\sigma, \omega)$ by crossing its side $s(0, \sigma, \omega)$ and turn in the positive sense, we get a cycle of vertices of the same type, σ being replaced by $\sigma - 1$.

In the remaining cycles of vertices, therefore, only peripheric polygons are involved and, turning always in the positive sense, we have to leave $P(\sigma, \omega)$ by crossing a side $s(\varrho, \sigma, \omega)$, where

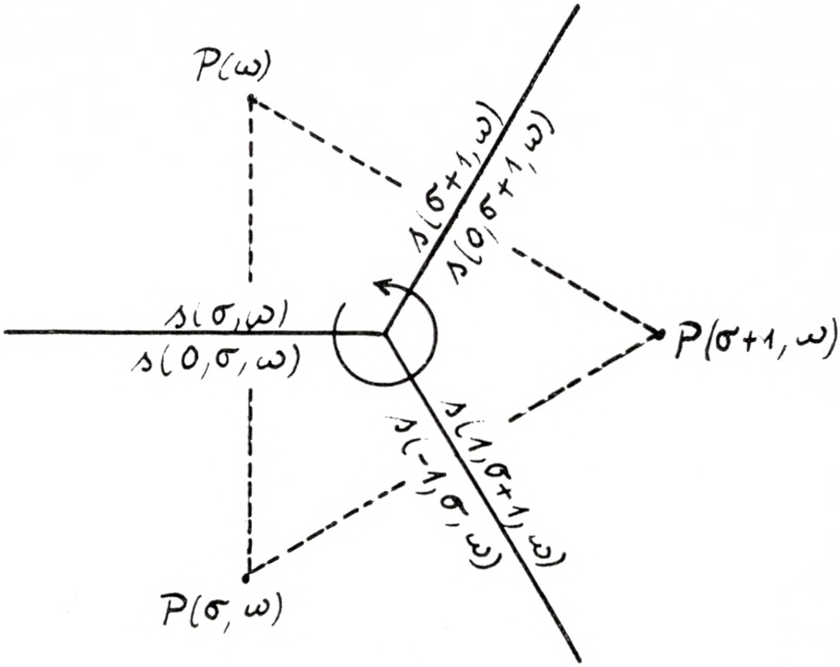

Fig. 1.

ϱ belongs to the set z', ($\varrho \not\equiv 0$ and -1); thus the three-set $[\varrho, \sigma, \omega]$ belongs to Z'. This side coincides with $s(\varrho_g, \sigma_g, \omega_g) = s(-\varrho^{-1}, \varphi(\varrho, \sigma), \omega + \tau(\varrho))$ of $P(\varphi(\varrho, \sigma), \omega + \tau(\varrho))$, and the preceding side of this polygon, which we have to cross in *leaving* the polygon, is

$$s(-\varrho^{-1} - 1, \varphi(\varrho, \sigma), \omega + \tau(\varrho)) = s(\varrho_G, \sigma_G, \omega_G).$$

Therefore we *leave* the next polygon by crossing the side $s(\varrho_{G_2}, \sigma_{G_2}, \omega_{G_2})$, and again we *leave* the next polygon by crossing the starting side $s(\varrho, \sigma, \omega)$ in virtue of (21). So again, we have a cycle of three vertices, as illustrated by fig. 2; compare (22).

In both cases the three polygons arranged round a vertex are different.

It follows from this construction that Φ is a closed surface. Moreover, it is orientable, since the orientation of any two neighbour polygons are in accordance, the common side being oppositely sensed.

We conclude this section by computing the genus p of Φ.

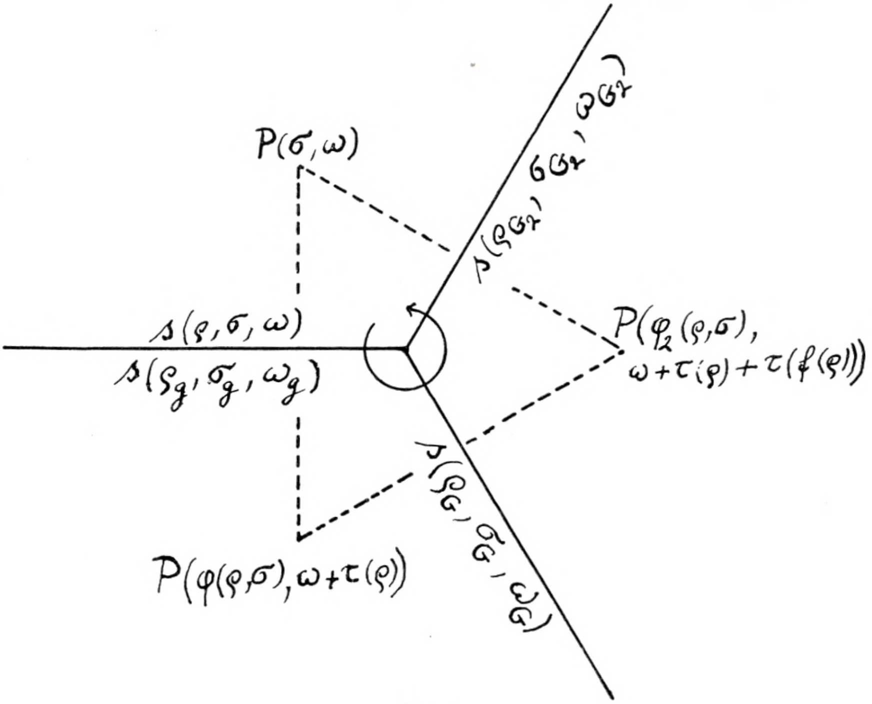
$P(\sigma,\omega)$
$s(\varrho_{G^2}, \sigma_{G^2}, \omega_{G^2})$
$s(\varrho,\sigma,\omega)$
$s(\varrho_g,\sigma_g,\omega_g)$
$P(\varphi_2(\varrho,\sigma), \omega+\tau(\varrho)+\tau(f(\varrho)))$
$s(\varrho_G,\sigma_G,\omega_G)$
$P(\varphi(\varrho,\sigma),\omega+\tau(\varrho))$

Fig. 2.

The number of polygons is $\alpha_2 = (q+1)\,r$. Thus the number of different sides on Φ is $\alpha_1 = \frac{1}{2}\,q\,(q+1)\,r$, and the number of vertices on Φ is $\alpha_0 = \frac{1}{3}\,q\,(q+1)\,r$. From this we get by Euler's formula

$$2-2p = \alpha_0 - \alpha_1 + \alpha_2 = r\,(q+1)\left(1-\frac{1}{6}\,q\right) = \frac{1}{12}\,(q-1)\,(q+1)\,(6-q)$$

and hence

$$(23) \qquad p = 1+\frac{1}{24}\,(q^2-1)\,(q-6) = \frac{1}{24}\,(q+2)\,(q-3)\,(q-5).$$

We list the smallest values:

$q =$	3	5	7	11	13	$\cdots$
$p =$	0	0	3	26	50	$\cdots$

(23) also holds for $q = 3$ and $q = 5$, which might have been included in the preceding considerations by adding a few special remarks. In these cases the structure af Φ is that of a tetrahedron or dodecahedron, respectively.

IV.

In this section we establish by a well-known process[1] the fundamental group (Poincaré group) of Φ by generators and generational relations in a special form derived from the construction of Φ. Inside each polygon we select a representative point, which may be denoted by the same symbol $P(\omega)$ or $P(\sigma, \omega)$ as the polygon itself. From each representative point we draw an oriented path, called "elementary path", to the representative point of each of the q neighbouring polygons and denote it by $a(\text{---})$, the paranthesis including the same symbols as the side $s(\text{---})$ which we cross in leaving the first polygon. So, according to definition (A), $a(\sigma, \omega)$ leads from $P(\omega)$ to $P(\sigma, \omega)$, and $a(0, \sigma, \omega)$ leads from $P(\sigma, \omega)$ to $P(\omega)$. We therefore have

$$a(0, \sigma, \omega) = a(\sigma, \omega)^{-1}. \tag{24}$$

Similarly, for $\varrho \neq 0$, according to definition (B), $a(\varrho, \sigma, \omega)$ leads from $P(\sigma, \omega)$ to $P(\varphi(\varrho, \sigma), \omega + \tau(\varrho))$, and we have for its inverse

$$a(\varrho_g, \sigma_g, \omega_g) = a(-\varrho^{-1}, \varphi(\varrho, \sigma), \omega + \tau(\varrho)) = a(\varrho, \sigma, \omega)^{-1}, \quad \varrho \neq 0. \tag{25}$$

These paths form on Φ a network N of triangles as indicated in fig. 1 and 2 by dotted lines, and this network N is dual to the network of polygons (e.g. the dual of the dodecahedron network is the icosahedron network).

Every path on the network N between two representative points is a chain of elementary paths. We choose the point $P(0)$

[1] See for instance H. Seifert and W. Threlfall, *Lehrbuch der Topologie*, § 46.

as starting point. Next we define for each representative point an individual path on N connecting $P(0)$ with that point in the following way: First, let the point be a $P(\omega)$ and let the path envisaged be called $h(\omega)$. For $\omega = 0$ we take the path $h(0)$ to be empty. Then, by induction, when $h(\omega - 1)$ is defined, we put

$$(26)\quad h(\omega) = h(\omega - 1)\, a(0, \omega - 1)\, a(r, 0, \omega - 1)\, a(0, r+1, \omega),$$
$$\omega \equiv 1, 2, \cdots, r-1 \text{ modulo } r.$$

[To control this, $h(\omega - 1)$ leads from $P(0)$ to $P(\omega - 1)$, $a(0, \omega - 1)$ leads from $P(\omega - 1)$ to $P(0, \omega - 1)$, $a(r, 0, \omega - 1)$ leads from $P(0, \omega - 1)$ to $P(r+1, \omega)$ by (10) and (8) and, finally, $a(0, r+1, \omega)$ leads from $P(r+1, \omega)$ to $P(\omega)$.] Next, if the representative point is a $P(\sigma, \omega)$, we put for the path $h(\sigma, \omega)$ leading from $P(0)$ to $P(\sigma, \omega)$

$$(27)\qquad h(\sigma, \omega) = h(\omega)\, a(\sigma, \omega)$$

for all values of σ and ω.

The fundamental group of Φ is the group of homotopy classes of closed curves issued from a fixed point, for which we here choose $P(0)$. Every closed path on N issued from $P(0)$ can be composed of certain closed paths depending on the single elementary paths, namely the h_1 leading from $P(0)$ to the starting point of the elementary path a followed by this path a itself and then by the h_2^{-1} leading from its end-point back to $P(0)$. We denote the homotopy class of such a path by $k(\text{———})$ with the same symbols in the parenthesis as for the corresponding elementary path $a(\text{———})$. This finite set of k's then generate the fundamental group.

If a general closed path issued from $P(0)$ is written down as a composition of the a's, then its homotopy class is the product of the corresponding k's, as is seen by inserting between any two consecutive a-factors the corresponding $h^{-1}h$ of their common point. Any equation between the a's therefore yields a relation between the corresponding k's. So we get from (24) and (25) for all values of ϱ, σ, ω, for which these equations hold,

$$(28)\qquad k(\sigma, \omega)\, k(0, \sigma, \omega) = 1,$$

$$(29)\qquad k(\varrho, \sigma, \omega)\, k(-\varrho^{-1}, \varphi(\varrho, \sigma), \omega + \tau(\varrho)) = 1, \quad \varrho \not\equiv 0,$$

the symbol 1 indicating the identity of the fundamental group. (29) may also be written

$$(29)\qquad k(\varrho, \sigma, \omega)\, k(\varrho_g, \sigma_g, \omega_g) = 1.$$

The homotopy class derived from the elementary path $a(\sigma, \omega)$ is according to the above definition the homotopy class of the product

$$h(\omega)\, a(\sigma, \omega)\, h(\sigma, \omega)^{-1},$$

$h(\omega)$ and $h(\sigma, \omega)$ being abbreviations for certain products of the a's as defined above. Inserting $h(\sigma, \omega)$ from (27) we find that this reduces to the empty product. Hence

$$(30)\qquad k(\sigma, \omega) = 1,$$

and then (28) yields

$$(31)\qquad k(0, \sigma, \omega) = 1.$$

Consider the product of a's making up $h(\omega)$. The corresponding product of k's is the homotopy class of

$$h(0)\, h(\omega)\, h(\omega)^{-1},$$

which reduces to the empty product. Thus the product of the k's corresponding to the a's in $h(\omega)$ is 1. (27) together with (30) then shows that this also holds for the $h(\sigma, \omega)$.

This fact together with (30) and (31), when applied to (26), yields the relation $k(r, 0, \omega - 1) = 1$ for the values of ω indicated in (26). We prefer to write this relation

$$(32)\qquad k(r, 0, \omega) = 1, \quad \omega \equiv 0, 1, \cdots, r-2 \text{ modulo } r,$$

and we emphasize the fact that the value $\omega \equiv -1$ modulo r is not included in this relation (32).

Finally, the homotopy class derived from the elementary path $a(\varrho, \sigma, \omega)$, $\varrho \not\equiv 0$, is the homotopy class of the product

$$h(\sigma, \omega)\, a(\varrho, \sigma, \omega)\, h(\varphi(\varrho, \sigma), \omega + \tau(\varrho))^{-1}$$

in consequence of the definition (B) of coincidence. This only yields the identical relation $k(\varrho,\sigma,\omega) = k(\varrho,\sigma,\omega)$, since the h's do not contribute.

To these relations we have to add the relations derived from the fact that the cycle of three a's surrounding a vertex of Φ bounds a simply connected piece of Φ and thus belongs to the homotopy class of identity. For a vertex of the type of fig. 1 this yields the relation

$$(33) \qquad k(\sigma,\omega)\,k(-1,\sigma,\omega)\,k(0,\sigma+1,\omega) = 1,$$

and for a vertex of the type of fig. 2 the relation

$$34) \quad k(\varrho,\sigma,\omega)\,k(f(\varrho),\varphi(\varrho,\sigma),\omega+\tau(\varrho))\,k(f_2(\varrho),\varphi_2(\varrho,\sigma),\omega+\tau(\varrho) \\ +\tau(f(\varrho)) = 1,$$

in which $\varrho \not\equiv 0$ and -1. With the use of the symbol G this relation reads

$$(34) \qquad k(\varrho,\sigma,\omega)\,k(\varrho_G,\sigma_G,\omega_G)\,k(\varrho_{G_2},\sigma_{G_2},\omega_{G_2}) = 1.$$

This completes the establishment of the generational relations of the fundamental group. Looking over the result, we see that we may omit the $k(\sigma,\omega)$ and their reciprocals, the $k(0,\sigma,\omega)$, since they are identity according to (30) and (31). Then relation (28) disappears, and (33) reduces to

$$(35) \qquad k(-1,\sigma,\omega) = 1,$$

while (29), (32), and (34) remain unaltered. We thus have the following result:

The fundamental group of Φ may be generated by the elements $k(\varrho,\sigma,\omega)$, $\varrho \not\equiv 0$, with (29), (32), (34), *and* (35) *as generational relations.*

One might suggest the elimination even of the $k(r,0,\omega)$ for $\omega \not\equiv -1$ modulo r and of the $k(-1,\sigma,\omega)$ in consequence of (32) and (35), and at the same time of their reciprocals $k(2,r+1,\omega+1)$ and $k(1,\sigma+1,\omega)$. This would, however, destroy the full generality of relation (34), into which some of them enter for special values of ϱ,σ,ω. We therefore prefer to keep them, but we may note at once the consequences as to the reciprocals. We put them in the form

$$k(2, r+1, \omega) = 1, \quad \omega \not\equiv 0 \text{ modulo } r, \tag{36}$$

$$k(1, \sigma, \omega) = 1. \tag{37}$$

If we put $\varrho = r$, $\sigma = 0$ in (34), we get by (10), (17), (8), and (6)

$$k(r, 0, \omega)\, k(1, r+1, \omega+1)\, k(-2, r, \omega+1) = 1.$$

Here the central factor drops out in virtue of (37). The reciprocal of the last factor is $k(r+1, 0, \omega)$ by (29), (10), (1), and (9). Thus, if $\omega \not\equiv -1$ modulo r, the first factor drops out in virtue of (32), and we get

$$k(-2, r, \omega) = 1, \quad \omega \not\equiv 0 \text{ modulo } r, \tag{38}$$

$$k(r+1, 0, \omega) = 1, \quad \omega \not\equiv -1 \text{ modulo } r. \tag{39}$$

If $\omega \equiv -1$ modulo r, we get

$$k(r, 0, -1) = k(r+1, 0, -1), \tag{40}$$

and for their reciprocals

$$k(2, r+1, 0) = k(-2, r, 0). \tag{41}$$

These last six relations (36) to (41) need not be included in the generational relations of the fundamental group, since they are consequences of the generational relations (29), (32), (34), and (35) established above.

V.

Let F denote the abstract group generated by three elements S, T, U subject to the relations

$$S^q = 1, \qquad T^2 = 1, \qquad U^3 = 1, \qquad STU = 1.$$

Eliminating U by means of the last relation we get for F a representation by two generators S and T with generational relations

$$S^q = 1 \tag{42}$$

$$T^2 = 1 \tag{43}$$

$$(ST)^3 = 1. \tag{44}$$

We use this latter form and pay attention to relations (42) and (43) by only regarding exponents of S and T as residue classes modulo q or modulo 2, respectively. So (44) is the real working relation and, for convenience, we write it in different, but equivalent forms:

$$(ST)^3 = 1,\quad STS = TS^{-1}T,\quad TST = S^{-1}TS^{-1},\quad (TS^{-1})^3 = 1. \tag{45}$$

As a consequence of (45) we get

$$TS^{-2}T = (TS^{-1}T)^2 = (STS)^2 = STS^2TS. \tag{46}$$

We now take q to mean a prime $q = 2r+1$ subject to the same restrictions as in section I and define the functions $\tau(\varrho)$, $f(\varrho)$ and $\varphi(\varrho, \sigma)$ and the transformations g and G as before. Moreover we introduce a function $\pi(\omega)$ = the smallest non-negative residue of ω modulo r:

$$\pi(\omega) \equiv \omega \text{ modulo } r, \qquad 0 \leqq \pi(\omega) < r.$$

We denote by W the following element of F:

$$W = TS^rTS^{-2}TS^r = TS^{r+1}TS^2TS^{r+1}, \tag{47}$$

these two products being equal in virtue of (46). We also note the reciprocal of W:

$$W^{-1} = S^{r+1}TS^2TS^{r+1}T = S^rTS^{-2}TS^rT. \tag{48}$$

Regarding as before ϱ and σ as residue classes modulo q and ω as a residue class modulo r, we introduce the subgroup H of F generated by the following elements:

$$k(\varrho, \sigma, \omega) = W^{\pi(\omega)} S^{\sigma} TS^{\varrho} TS^{\varrho^{-1}} TS^{-\varphi(\varrho,\sigma)} W^{-\pi(\omega+\tau(\varrho))}, \quad \varrho \not\equiv 0. \tag{49}$$

We set out to prove that these elements satisfy the relations (29), (32), (34), and (35) established in the preceding section for the fundamental group of Φ.

If in (29) we insert the values given by (49), we get

$$W^{\pi(\omega)} S^{\sigma} TS^{\varrho} TS^{\varrho^{-1}} TS^{-\varphi(\varrho,\sigma)} W^{-\pi(\omega+\tau(\varrho))}$$
$$\cdot W^{\pi(\omega+\tau(\varrho))} S^{\varphi(\varrho,\sigma)} TS^{-\varrho^{-1}} TS^{-\varrho} TS^{-\sigma} W^{-\pi(\omega)} = 1 .$$

Here we have made use of (12) in the last two factors.

In (32) we have with $\omega \not\equiv -1$ modulo r:

$$k(r, 0, \omega) = W^{\pi(\omega)} TS^{r} TS^{-2} TS^{r} W^{-\pi(\omega+1)} = 1$$

by (8) and (47), for $\pi(\omega+1) = \pi(\omega)+1$, since $\omega \not\equiv -1$ modulo r.

In (34) we get by inserting from (49)

$$W^{\pi(\omega)} S^{\sigma} TS^{\varrho} TS^{\varrho^{-1}} \underline{TS^{-\varphi(\varrho.\sigma)} W^{-\pi(\omega+\tau(\varrho))}}$$
$$\cdot \underline{W^{\pi(\omega+\tau(\varrho))} S^{\varphi(\varrho,\sigma)} T} S^{f(\varrho)} TS^{f(\varrho)^{-1}} \underline{TS^{-\varphi_2(\varrho,\sigma)} W^{-\pi(\omega+\tau(\varrho)+\tau(f(\varrho)))}}$$
$$\cdot \underline{W^{\pi(\omega+\tau(\varrho)+\tau(f(\varrho)))} S^{\varphi_2(\varrho,\sigma)} T} S^{f_2(\varrho)} TS^{f_2(\varrho)^{-1}} TS^{-\sigma} W^{-\pi(\omega)},$$

since by (21)

$$\varphi(f_2(\varrho), \varphi_2(\varrho, \sigma)) = \varphi_3(\varrho, \sigma) \equiv \sigma \text{ modulo } q$$

and

$$\tau(\varrho) + \tau(f(\varrho)) + \tau(f_2(\varrho)) \equiv 0 \text{ modulo } r.$$

Here the underlined parts cancel. Moreover we have by (13) and (14) for the exponents of those powers of S which thereby become neighbours

$$\varrho^{-1} + f(\varrho) \equiv \varrho^{-1} - (1+\varrho^{-1}) = -1,$$
$$f(\varrho)^{-1} + f_2(\varrho) \equiv -(1+\varrho^{-1})^{-1} - (1+\varrho)^{-1} \equiv -(1+\varrho)^{-1}(1+\varrho) \equiv -1.$$

We therefore get

$$W^{\pi(\omega)} S^{\sigma} TS^{\varrho} (TS^{-1})^{3} S^{1+f_2(\varrho)^{-1}} TS^{-\sigma} W^{-\pi(\omega)} = 1$$

by using (45) and (14).

Finally, in (35) we find by (45)

$$k(-1, \sigma, \omega) = W^{\pi(\omega)} S^{\sigma} T S^{-1} T S^{-1} T S^{-(\sigma+1)} W^{-\pi(\omega+0)} = 1.$$

The elements (49) therefore also satisfy relations (36)—(41), since these are formal consequences of the four relations just proved. Especially we remark concerning the elements occurring in (40) that by (49) and (1) and (47)

$$(50) \qquad k(r, 0, -1) = W^{r-1} T S^{r} T S^{-2} T S^{r} W^{-\pi(0)} = W^{r}.$$

Thus W^r is an element of H.

VI.

It is inferred from what has just been proved that the subgroup H of F defined in the preceding section is one-one isomorphic either with the fundamental group of Φ or with a factor group of that group. We set out to prove that the first case occurs. This is done by constructing from the group F a set of polygons and of identifications by the $k(\varrho, \sigma, \omega)$ which correspond to the construction of Φ in section III. (This construction is based on a procedure indicated by W. Dyck in a footnote on pages 41—42 of *Mathematische Annalen*, vol. XX. Instead of the pair —2 and r used in the present investigations, Dyck uses a general pair of mutually reciprocal primitive roots α and δ modulo q, thus without imposing any restriction on q.)

Let a triangle *stu* be given with angles equal to $\frac{\pi}{q}$, $\frac{\pi}{2}$ and $\frac{\pi}{3}$, respectively; see fig. 3. As we assume $q \geqq 7$, the triangle is situated in the non-euclidean plane. A reflection in *st* followed by a reflection in *su* is a rotation about s through an angle $\frac{2\pi}{q}$ in the positive sense. We denote this rotation by S, and hence S^q is identity. Similarly, T is a half-rotation about t, and U is a third of a full rotation about u, if they are taken to be the product of two analogous reflections. The product of reflections shows that $STU = 1$.[1] Hence S, T, and U generate a group of

[1] A product is read like a composed function: First carry out U, then T, finally S.

motions in the non-euclidean plane, which is our group F, and which we now generate by S and T with relations (42), (43), and (44). The shadowed triangle stu_0 of fig. 3 being derived from stu by reflection at st, the triangle su_0u is a fundamental domain for the group F. In fig. 3 this triangle is inscribed with the symbol of identity. Let the triangle derived from it by an arbitrary element e of F be denoted with the symbol e. If e ranges over the whole of F, these triangles cover the entire non-euclidean plane. This is illustrated by fig. 4 for the case of $q = 7$.[1]

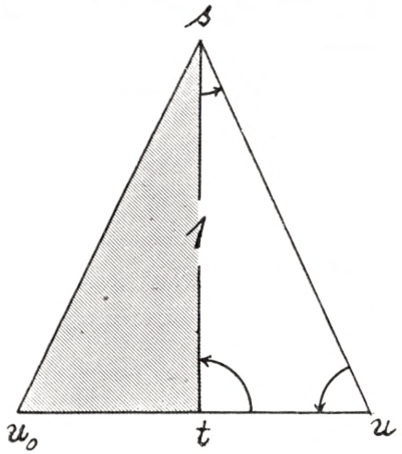

Fig. 3.

The triangles $1, S, S^2, \cdots, S^{q-1}$ form a polygon $P(0)$ with center at the point s, which will also be called the representative point $P(0)$. In the triangle S^σ the side opposite $P(0)$ is called $s(\sigma, 0)$. Then $S^\sigma TS^{-\sigma}$ is a half-rotation about the center of this side, and it carries the "central" polygon $P(0)$ into the "peripheric" polygon $P(\sigma, 0)$, which has its side $s(0, \sigma, 0)$ coinciding with $s(\sigma, 0)$ with opposite senses conforming to the orientation of the plane. The other sides of $P(\sigma, 0)$ are numbered $s(\varrho, \sigma, 0)$ in the positive sense.

This star of $q+1$ polygons, each consisting of q triangles (each triangle being half white, half shadowed) is shown by fig. 5 for $q = 7$.

The triangles of the central polygon $P(0)$ bear the signature S^ϱ, those of $P(0, 0)$ consequently TS^ϱ, and those of $P(\sigma, 0)$ consequently $S^\sigma TS^\varrho$. The side of the latter opposite the center $P(\sigma, 0)$ is $s(\varrho, \sigma, 0)$. The triangle adjacent to $S^\sigma TS^\varrho$ along $s(\varrho, \sigma, 0)$ is $S^\sigma TS^\varrho T$, because the triangle T is adjacent to the triangle 1 along the corresponding side $u_0 u$. In order to make the side $s(-2, r, 0)$ of the peripheric polygon $P(r, 0)$ coincide with the side $s(r+1, 0, 0)$ of the peripheric polygon $P(0, 0)$ with opposite senses we must carry the triangle $S^r TS^{-2} T$ adjacent to $s(-2, r, 0)$

[1] The figures 4 and 5 have been reproduced from Klein-Fricke, *Elliptische Modulfunktionen*, vol. I.

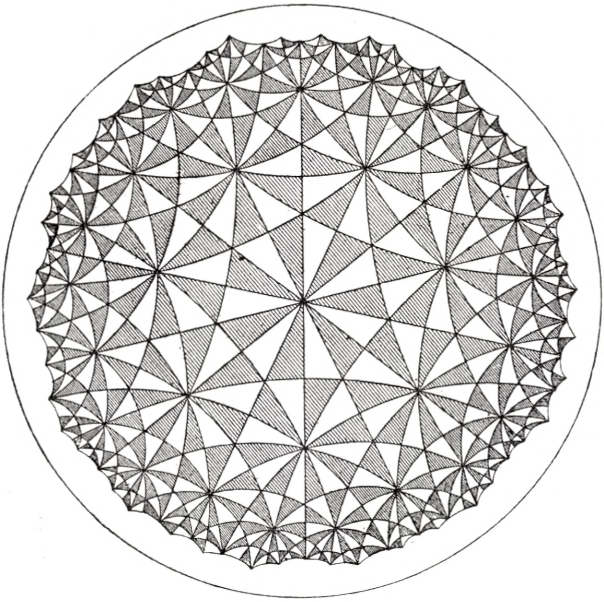

Fig. 4.

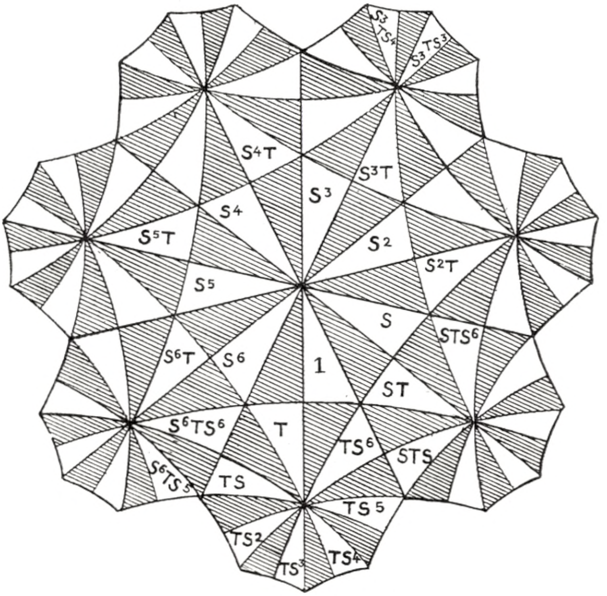
S^3TS^4
S^3TS^3
S^4T
S^3T
S^3
S^4
S^5T
S^2
S^2T
S^5
S
STS^6
S^6T
S^6
1
ST
S^6TS^6
T
TS^6
STS
S^6TS^5
TS
TS^5
TS^2
TS^3
TS^4

Fig. 5.

into the triangle TS^{r+1}, and this is done by the motion

$$TS^{r+1}(S^r TS^{-2} T)^{-1} = TS^{r+1} TS^2 TS^{r+1} = W,$$

see (47). The same motion W carries $s(2, r+1, 0)$ into $s(r, 0, 0)$ for analogous reasons:

$$TS^r (S^{r+1} TS^2 T)^{-1} = TS^r TS^{-2} TS^r = W.$$

Thus W can be thought of as a translation sliding the whole star downwards along the vertical diameter of fig. 5 at a distance equal to the length of that diameter. If this displacement is repeated ω times, we get a star composed of a central polygon $P(\omega)$, whose triangles are $W^\omega S^\varrho$, and q peripheric polygons, $P(\sigma,\omega)$, whose triangles are $W^\omega S^\sigma TS^\varrho$. Take $\omega < r$, thus $\omega = \pi(\omega)$. If for $\varrho \not\equiv 0$ we want the side $s(\varrho, \sigma, \omega)$ of this last triangle to coincide with the side $s(\varrho_g, \sigma_g, \omega_g) = s(-\varrho^{-1}, \varphi(\varrho, \sigma), \pi(\omega + \tau(\varrho)))$ of the triangle $W^{\pi(\omega+\tau(\varrho))} S^{\varphi(\varrho,\sigma)} TS^{-\varrho^{-1}}$ with opposite senses, we make the adjacent triangle of the latter, thus $W^{\pi(\omega+\iota(\varrho))} S^{\varphi(\varrho,\sigma)} TS^{-\varrho^{-1}} T$ coincide with the triangle $W^{\pi(\omega)} S^\sigma TS^\varrho$. This is evidently done by the element $k(\varrho, \sigma, \omega)$ defined in (49).

The r stars derived from the first one by W^ω, $\omega = 0, 1, \cdots, r-1$, form a singly connected piece Ω of the plane, bounded by a polygon, whose sides correspond in pairs by those elements $k(\varrho, \sigma, \omega)$ which are not equal to 1. This shows that the construction of the subgroup H of F is a materialization of the fundamental group of the two-dimensional manifold Φ defined in section III by abstract identification. The group H is here realized as a group of motions in the non-euclidean plane, which is a model of the universal covering surface of Φ.

The fundamental domain Ω of H consists of $r(q+1)$ polygons containing q triangles each. This shows that

$$j = r(q+1)q = \frac{1}{2} q(q^2-1) \tag{51}$$

is the index of H in F.

If the non-euclidean plane is denoted by D, we may speak of Φ as D modulo H, which means that points of D corresponding by elements of H are considered as identical. In the same way, D modulo F evidently is a non-euclidean manifold of genus zero, three points of which are singular with respect to the metric, namely those corresponding to s, t, and u. They may be called conical points. D modulo H is a closed manifold, which covers D modulo F with j sheets, and which possesses no conical points. Accordingly, H possesses no elements of a finite order.

VII.

We now want to prove that the covering of D modulo F by D modulo H is regular. This is equivalent to the assertion that H is self-conjugate in F. In order to prove this it is sufficient to prove that the generators $k(\varrho, \sigma, \omega)$ of H are transformed into elements of H by the generators T and S of F.

In preparation for this proof we state the following facts beforehand:

$$TWT^{-1} = W^{-1}. \tag{52}$$

This is immediately seen from (47) and (48). Also the definition of $\pi(x)$ implies:

$$\pi(\pi(x)) = \pi(x), \tag{53}$$

$$\pi(x) + \pi(-x) = \begin{cases} 0 \text{ if } x \equiv 0 \text{ modulo } r \\ r \text{ if } x \not\equiv 0 \text{ modulo } r, \end{cases} \tag{54}$$

$$r^{2\pi(x)} \equiv r^{2x} \text{ modulo } q, \tag{55}$$

since $r^{2r} \equiv 1$.

We now transform $k(\varrho, \sigma, \omega)$ (where it is remembered that $\varrho \not\equiv 0$) by T and get by (49), (52), and (10)

$$\begin{aligned} Tk(\varrho, \sigma, \omega)\, T^{-1} &= TW^{\pi(\omega)} S^{\sigma} TS^{\varrho} TS^{\varrho^{-1}} TS^{-\varphi(\varrho, \sigma)} W^{-\pi(\omega + \tau(\varrho))} T \\ &= W^{-\pi(\omega)} TS^{\sigma} TS^{\varrho} TS^{\varrho^{-1}} TS^{-\varrho(\varrho\sigma - 1)} TW^{\pi(\omega + \tau(\varrho))}. \end{aligned} \tag{56}$$

On the other hand, suppose $\sigma \not\equiv 0$ and $\sigma \not\equiv \varrho^{-1}$ and consider the product

$$k(\sigma, 0, -\omega)\, k(\sigma^{-1}(\varrho\sigma-1), -\sigma, \tau(\sigma)-\omega)\, k(-\varrho^{-1}(\varrho\sigma-1)^{-1}, -\varrho(\varrho\sigma-1), \tau(\sigma)+\tau(\sigma^{-1}(\varrho\sigma-1))-\omega)$$

$$= W^{\pi(-\omega)} S^0\, TS^{\sigma}\, TS^{\sigma^{-1}}\, \underline{TS^{\sigma}\, W^{-\pi(\tau(\sigma)-\omega)}}$$

$$\cdot\, \underline{W^{\pi(\tau(\sigma)-\omega)} S^{-\sigma}}\, TS^{\sigma^{-1}(\varrho\sigma-1)}\, TS^{\sigma(\varrho\sigma-1)^{-1}}\, \underline{TS^{\varrho(\varrho\sigma-1)}\, W^{-\pi(\tau(\sigma)+\tau(\sigma^{-1}(\varrho\sigma-1))-\omega)}}$$

$$\cdot\, \underline{W^{\pi(\tau(\sigma)+\tau(\sigma^{-1}(\varrho\sigma-1))-\omega)} S^{-\varrho(\varrho\sigma-1)}}\, TS^{-\varrho^{-1}(\varrho\sigma-1)^{-1}}\, TS^{-\varrho(\varrho\sigma-1)}\, TS^0\, W^{-\pi(\tau(\sigma)+\tau(\sigma^{-1}(\varrho\sigma-1))+\tau(\varrho^{-1}(\varrho\sigma-1)^{-1})-\omega)}.$$

It should be noted that all reciprocals occurring herein exist owing to the assumptions for ϱ and σ, and the first argument for all three k's is $\not\equiv 0$. Now the underlined parts in the product cancel. Moreover we get for the exponents of the powers of S which thereby become neighbours

$$\sigma^{-1} + \sigma^{-1}(\varrho\sigma - 1) = \sigma^{-1}\varrho\sigma \equiv \varrho,$$

$$\sigma(\varrho\sigma-1)^{-1} - \varrho^{-1}(\varrho\sigma-1)^{-1} \equiv (\varrho\sigma-1)^{-1}(\sigma\varrho\varrho^{-1} - \varrho^{-1}) \equiv (\varrho\sigma-1)^{-1}\varrho^{-1}(\varrho\sigma-1) \equiv \varrho^{-1}.$$

Finally, with the use of (5) and (7),

$$\tau(\sigma) + \tau(\sigma^{-1}(\varrho\sigma-1)) + \tau(\varrho^{-1}(\varrho\sigma-1)^{-1})$$

$$\equiv \tau\{\sigma \cdot \sigma^{-1}(\varrho\sigma-1) \cdot \varrho^{-1}(\varrho\sigma-1)^{-1}\} \equiv \tau(\varrho^{-1}) \equiv -\tau(\varrho) \text{ modulo } r.$$

The above product therefore is equal to

$$W^{\pi(-\omega)}TS^{\sigma}TS^{\varrho}TS^{\varrho^{-1}}TS^{-\varrho(\varrho\sigma-1)}TW^{-\pi(-\omega-\tau(\varrho))}.$$

Comparing this with (56) and slightly reducing the last argument of the third k we get

$$(57)\quad \left\{\begin{aligned} Tk(\varrho,\sigma,\omega)\,T^{-1} = W^{-\pi(\omega)-\pi(-\omega)} & \\ \cdot k(\sigma,0,-\omega) & \\ \cdot k(\sigma^{-1}(\varrho\sigma-1),-\sigma,\tau(\sigma)-\omega) & \\ \cdot k(-\varrho^{-1}(\varrho\sigma-1)^{-1},-\varrho(\varrho\sigma-1),\tau(\varrho\sigma-1)-\omega) & \\ \cdot W^{\pi(\omega+\tau(\varrho))+\pi(-\omega-\tau(\varrho))}. & \end{aligned}\right.$$

In consequence of (54) the first factor of the right hand product is either 1 or W^{-r}, and the last one is either 1 or W^{r}. Hence, by (50), the right hand member is an element of H.

We still have to supplement this result by a consideration of the cases $\sigma \equiv 0$ and $\sigma \equiv \varrho^{-1}$, which were excluded in the preceding computation. The two cases exclude each other. Assuming $\sigma \equiv \varrho^{-1}$, we get

$$(57')\quad \left\{\begin{aligned} Tk(\varrho,\varrho^{-1},\omega)\,T^{-1} &= TW^{\pi(\omega)}S^{\varrho^{-1}}TS^{\varrho}TS^{\varrho^{-1}}TS^{0}W^{-\pi(\omega+\tau(\varrho))}T \\ &= W^{-\pi(\omega)}TS^{\varrho^{-1}}TS^{\varrho}TS^{\varrho^{-1}}W^{\pi(\omega+\tau(\varrho))} \\ &= W^{-\pi(\omega)-\pi(-\omega)}k(\varrho^{-1},0,-\omega)\,W^{\pi(\omega+\tau(\varrho))+\pi(-\omega-\tau(\varrho))}. \end{aligned}\right.$$

Thus except for powers of W^{r} all the generators of the type $\sigma \equiv \varrho^{-1}$ are transformed by T into all generators of the type $\sigma \equiv 0$. Therefore the inverse is evidently also true. The explicit formula is

$$(57'')\quad Tk(\varrho,0,\omega)\,T^{-1} = W^{-\pi(\omega)-\pi(-\omega)}k(\varrho^{-1},\varrho,-\omega)\,W^{\pi(\omega+\tau(\varrho))+\pi(-\omega-\tau(\varrho))}.$$

We have thus proved that $THT^{-1} = H$.

In order to prove that $SHS^{-1} = H$ we start with generators of the following form:

$$\begin{aligned} k(r, r^{2\varkappa}, \varkappa) &= W^{\pi(\varkappa)} S^{r^{2\varkappa}} T S^{r} T S^{-2} T S^{-r(rr^{2\varkappa}-1)} W^{-\pi(\varkappa+1)} \\ &= W^{\pi(\varkappa)} S^{r^{2\varkappa}} W S^{-r^{2(\varkappa+1)}} W^{-\pi(\varkappa+1)} \end{aligned}$$

(by (49), (1), (8), and (47)). We form their product for increasing values of $\varkappa$ from $\varkappa = 0$ to $\varkappa = n-1$ and denote this product by $\Psi(n)$:

$$(58) \qquad \Psi(n) = k(r, r^{2\cdot 0}, 0)\, k(r, r^{2\cdot 1}, 1) \cdots k(r, r^{2(n-1)}, n-1), \qquad n \geq 0,$$

and remark that $\Psi(0)$ means the empty product. We then get

$$\Psi(n) = S W^{n} S^{-r^{2n}} W^{-\pi(n)}$$

and from this we get some sort of commutation formula for S and W:

$$(59) \qquad S W^{n} = \Psi(n)\, W^{\pi(n)} S^{r^{2n}}.$$

This is applied to

$$S k(\varrho, \sigma, \omega) S^{-1} = S W^{\pi(\omega)} S^{\sigma} T S^{\varrho} T S^{\varrho^{-1}} T S^{-\varrho(\varrho\sigma-1)} W^{-\pi(\omega+\tau(\varrho))} S^{-1},$$

and we get for the first two factors of the right hand product

$$S W^{\pi(\omega)} = \Psi(\pi(\omega))\, W^{\pi(\omega)} S^{r^{2\omega}}$$

in consequence of (59), (53), and (55). Similarly, for the last two factors:

$$\begin{aligned} W^{-\pi(\omega+\tau(\varrho))} S^{-1} &= \left[S W^{\pi(\omega+\tau(\varrho))} \right]^{-1} = \\ &= \left[\Psi(\pi(\omega+\tau(\varrho)))\, W^{\pi(\omega+\tau(\varrho))} S^{r^{2(\omega+\tau(\varrho))}} \right]^{-1}, \end{aligned}$$

where we note that $r^{2\tau(\varrho)} = \varrho^{2}$ according to (2). Hence

$$\begin{aligned} S k(\varrho, \sigma, \omega) S^{-1} &= \Psi(\pi(\omega))\, W^{\tau(\omega)} S^{\sigma + r^{2\omega}} T S^{\varrho} T S^{\varrho^{-1}} T S^{-\varrho^{2}(\sigma + r^{2\omega}) + \varrho} \\ &\qquad W^{-\pi(\omega+\tau(\varrho))}\, \Psi(\pi(\omega+\tau(\varrho)))^{-1} \\ &= \Psi(\pi(\omega))\, k(\varrho, \sigma + r^{2\omega}, \omega)\, \Psi(\pi(\omega+\tau(\varrho)))^{-1}. \end{aligned}$$

Since the Ψ's are elements of H defined by (58), this completes the proof of the invariance of H in F. The last formula together with (57), (57′), and (57″) states explicitly the elements of H into which the generators of H are transformed by the generators of F.

VIII.

Let M' denote the set of all matrices

$$(M') \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = 1,$$

with integer elements and determinant 1. This set M' forms a group by multiplication. The matrices

$$(M'') \qquad E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad -E = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

constitute a self-conjugate subgroup M'' of M'. The quotient group

$$(M) \qquad M = M'/M''$$

is the modular group, the group of all linear fractional substitutions with integer coefficients.

The (principal) *congruence subgroup modulo* q of M means the set C of elements of M represented by those matrices which modulo q are congruent to an element of M'':

$$(C) \qquad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \pm E \text{ modulo } q.$$

It is immediately seen that this set C forms a group and, furthermore, that this group is self-conjugate in M.

Usually, the two matrices

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

are taken as generators of M. Since

$$T^2 = -E, \quad (ST)^3 = -E,$$

they satisfy the relations

$$T^2 = 1, \quad (ST)^3 = 1 \tag{60}$$

as generators of M, and it is well known that (60) is a complete set of generational relations for M. Since

$$S^{\beta} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix},$$

all powers of S are different in M, but

$$S^q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \equiv E \text{ modulo } q,$$

and hence S^q belongs to C. The same then is true of the transforms of S^q with arbitrary matrices m from M':

$$mS^q m^{-1} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} 1-\alpha\gamma q & \alpha^2 q \\ -\gamma^2 q & 1+\alpha\gamma q \end{pmatrix}. \tag{61}$$

Here a and γ range over all pairs of relatively prime integers, and the resulting matrix does not depend on β and δ.

We can now form a subgroup Q of C, namely the one generated by all elements (61). Evidently Q is self-conjugate in M (and thus also in C), and the quotient group M/Q is obtained by using S and T as generators and adding to the relations (60) of M the single relation

$$S^q = 1.$$

Thus M/Q is one-one isomorphic to the abstract group F of section V, and we write

$$M/Q = F. \tag{62}$$

We now take the modulus q to be a prime subject to the conditions of section I and use the notations introduced in the previous sections. It is remembered that all congruences are understood modulo q unless otherwise stated.

It turns out that (on account of the assumption $q > 5$) the group C contains more elements than its self-conjugate subgroup Q. We want to find a set of generators and generational relations for the quotient group C/Q and to establish the quotient group of C in M, for which, by a well-known theorem of group theory, we have

$$M/C = \frac{M/Q}{C/Q}.$$

When speaking of matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ as representatives of the quotient group M/C, the integers $\alpha, \beta, \gamma, \delta$ may be freely replaced by other members of their residue class modulo q and, moreover, the sign of all four numbers may be changed simultaneously. Under such operations the determinant remains $\equiv 1$ modulo q. We apply this to the following products:

$$S^r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$$

$$TS^r = \begin{pmatrix} 0 & -1 \\ 1 & r \end{pmatrix}$$

$$S^{-2}\,TS^r = \begin{pmatrix} -2 & -1-2\,r \\ 1 & r \end{pmatrix} \equiv \begin{pmatrix} -2 & 0 \\ 1 & r \end{pmatrix}$$

$$TS^{-2}\,TS^r \equiv \begin{pmatrix} -1 & -r \\ -2 & 0 \end{pmatrix}$$

$$S^r\,TS^{-2}\,TS^r \equiv \begin{pmatrix} -1-2\,r & -r \\ -2 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & -r \\ -2 & 0 \end{pmatrix}$$

$$W = TS^r\,TS^{-2}\,TS^r \equiv \begin{pmatrix} 2 & 0 \\ 0 & -r \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 \\ 0 & 2^{-1} \end{pmatrix}.$$

Thus modulo q we have for W a diagonal matrix as a representative matrix. For the powers of W we thus get

$$W^n \equiv \begin{pmatrix} 2^n & 0 \\ 0 & 2^{-n} \end{pmatrix},$$

and these are all different for $0 \leq n < r$ in consequence of the assumption of section I that 2 belongs to r. For $n = r$, however,

$$W^r \equiv \pm E. \tag{63}$$

Thus W^r belongs to C, but no smaller power of W.

In the same way we want to find a matrix representing the product $k(\varrho, \sigma, \omega)$, defined by (49), and we get in turn:

$$\begin{aligned}
&S^{\sigma} && = \begin{pmatrix} 1 & \sigma \\ 0 & 1 \end{pmatrix} \\
&S^{\sigma}T && = \begin{pmatrix} \sigma & -1 \\ 1 & 0 \end{pmatrix} \\
&S^{\sigma}TS^{\varrho} && = \begin{pmatrix} \sigma & \varrho\sigma-1 \\ 1 & \varrho \end{pmatrix} \\
&S^{\sigma}TS^{\varrho}T && = \begin{pmatrix} \varrho\sigma-1 & -\sigma \\ \varrho & -1 \end{pmatrix} \\
&S^{\sigma}TS^{\varrho}TS^{\varrho^{-1}} && \equiv \begin{pmatrix} \varrho\sigma-1 & -\varrho^{-1} \\ \varrho & 0 \end{pmatrix} \\
&S^{\sigma}TS^{\varrho}TS^{\varrho^{-1}}T && \equiv \begin{pmatrix} -\varrho^{-1} & -\varrho\sigma+1 \\ 0 & -\varrho \end{pmatrix} \\
(64)\qquad &S^{\sigma}TS^{\varrho}TS^{\varrho^{-1}}TS^{-\varrho(\varrho\sigma-1)} && \equiv \begin{pmatrix} -\varrho^{-1} & 0 \\ 0 & -\varrho \end{pmatrix}.
\end{aligned}$$

Now $k(\varrho, \sigma, \omega)$ arises if we apply the factors $W^{\pi(\omega)}$ in front and $W^{-\pi(\omega+\tau(\varrho))}$ in the rear of (64). But since both W and the element (64) are represented by diagonal matrices when considered as elements of M/C, they are interchangeable, and we therefore multiply (64) by $W^{\pi(\omega)-\pi(\omega+\tau(\varrho))}$. Now

$$\pi(\omega)-\pi(\omega+\tau(\varrho)) \equiv -\tau(\varrho) \text{ modulo } r.$$

Hence, in virtue of (63), we only have to multiply (64) by

$$W^{-\tau(\varrho)} \equiv \begin{pmatrix} 2^{-\tau(\varrho)} & 0 \\ 0 & 2^{\tau(\varrho)} \end{pmatrix} \equiv \begin{pmatrix} (-r)^{\tau(\varrho)} & 0 \\ 0 & (-r)^{-\tau(\varrho)} \end{pmatrix} \equiv \begin{pmatrix} \pm\varrho & 0 \\ 0 & \pm\varrho^{-1} \end{pmatrix}$$

in consequence of (1) and (3). In both places we have the positive sign, or in both places the negative sign. We hereby get

$$(65) \qquad k(\varrho, \sigma, \omega) \equiv \pm E.$$

The $k(\varrho, \sigma, \omega)$ are by their definition products of S and T. (65) shows that they belong to C. Together with the generators (61) they generate a certain subgroup C' of C. For this we have

$$M/C' = \frac{M/Q}{C'/Q} = \frac{F}{H}$$

by (62) and the fact that the $k(\varrho, \sigma, \omega)$ generate H when they are considered as elements of F. Thus the index of C' in M is equal to the index j of H in F, which was found in (51).

On the other hand, the index of C in M may be easily established: In a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ of M' the elements α and β cannot both be divisible by q. But take any two numbers α_0 and β_0 which are not both $\equiv 0$ modulo q. Then two numbers a and b exist such that $\alpha = \alpha_0 + aq$ and $\beta = \beta_0 + bq$ are relatively prime. Let γ_0 and δ_0 be so chosen that $\alpha\delta_0 - \beta\gamma_0 = 1$. Then the relation $\alpha\delta - \beta\gamma = 1$ holds for $\gamma = \gamma_0 + v\alpha$, $\delta = \delta_0 + v\beta$ with arbitrary values for v. The choice of residue classes modulo q for α_0 and β_0 admits $q^2 - 1$ combinations. For each of them there are q possible choices of the class of v. Since at least one of α and β are $\not\equiv 0$, the choice of v implies q different residue classes for at least one of the numbers γ and δ. Thus, in all, the matrices fall into $q(q^2 - 1)$ residue classes modulo q. Taking the simultaneous change of sign for all elements of a matrix into consideration, this corresponds to $\frac{1}{2}\, q(q^2 - 1)$ different representative matrices for the elements of M/C. Since this number coincides with the value j in (51), and since C' is known to be a subgroup of C, we infer that $C' = C$.

We can thus generate the congruence subgroup modulo q of M by taking the generators (61) and (65) together. This system reduces to a finite system of generators for C by the matrix m in (61) being made to range over a suitable set of j matrices which are mutually non-congruent modulo q. The usual point of interest is not so much C as $C/Q = H$. This group then is generated by elements $k(\varrho, \sigma, \omega)$, $\varrho \not\equiv 0$, with (29), (32), (34), and (35) as generational relations. The quotient group of C in M, which is at the same time the quotient group of H in F, has S and T as generators, and a system of defining relations is obtained by adding the relations $k(\varrho, \sigma, \omega) = 1$ expressed in S and T to the relations (42), (43), and (44) of F.

This system of relations is, of course, capable of abundant reduction, and no attempt is made here to reduce it to simple forms. It is for instance well known[1] that in the special case of $q = 7$ the step from F to F/H can be carried out by adding one single relation to the relations of F, namely the relation $(S^4 T)^4 = 1$.

[1] See Burnside, *Theory of Groups of Finite Order*, p. 422.

Note.

After the preceding study had been sent to the printer, it came to my knowledge that Mr. Hermann Frasch had, in vol. 108 of the *Mathematische Annalen* in 1933, published an article *Die Erzeugung der Hauptkongruenzgruppen für Primzahlstufen,* which had escaped my attention. On examining this earlier article I found a rather far-reaching consonance with my own investigations especially concerning the arithmetical formalism, which I had treated explicitly beforehand in section II, but which is contained implicitly in Frasch's development, and also concerning the choice of generators $k(\varrho, \sigma, \omega)$, which correspond to the $U_{\lambda, \mu, \nu, T}$ in Frasch's notation, and therefore also the relations between these generators. Moreover, Frasch goes into the question of the reduction of this system of relations, which I leave aside.

If, nevertheless, I maintain the publication of my investigations unaltered, I do so on the ground that the chief means of research is different in the two papers. Frasch bases his work on the powerful method of Reidemeister and Schreier for the abstract characterization of subgroups of given abstract groups contained in vol. V of the *Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität.* (By the way, this method would not be necessary for the establishment of a system of generators, since such a system follows directly from formula (9) on page 231 of Frasch's paper). On the other hand, my treatment is based on the most elementary notions of two-dimensional topology without recurrence to Reidemeister and Schreier's method. Upon comparing these two ways of approach I found that they throw some light on each other and that this might justify what could otherwise be called a re-publication of results. For instance, the choice of the $h(\omega)$ and $h(\sigma, \omega)$ in section IV can be taken as an illustration of Schreier's condition (F). The establishment of a complete system of generational relations by simple considerations of surface topology must, in each special case, be simpler than the general mechanism of the Reidemeister-Schreier method, which leads Frasch to rather elaborate calculations. But I am pleased to call attention to Frasch's interesting use of this method, following an earlier paper by Rademacher, the more so as his section 7 hints at more general applications and even touches on the illustration by means of surface topology.

Indleveret til selskabet den 13. december 1949.
Færdig fra trykkeriet den 30. marts 1950.