AN EXTENSION OF F. KLEIN'S LEVEL CONCEPT

BY
KLAUS WOHLFAHRT

Introduction

In the theory of elliptic modular functions F. Klein's concept of the level of a congruence subgroup of the modular group has proved of fundamental importance. That this concept should be extendable to apply, in particular, to arbitrary subgroups of finite index seems never to have been sufficiently appreciated. Such a generalization was, in effect, provided for by R. Fricke, who introduced the notion of the "class" of a modular subgroup, but there is no evidence in his work to suggest that he perceived of it in that light. It is therefore remarkable that, for a congruence subgroup, the identity of the two concepts is a consequence of one of R. Fricke's theorems.

It is the purpose of this note to introduce a general level concept for the modular group and to show its usefulness in investigations into the structure of that group. There will be occasion to throw some light on the connection between certain modular subgroups and Riemann surfaces associated with them. Account will also be taken of some recent results, concerning the structure of the modular group, of I. Reiner and of M. Newman, as well as of old results of R. Fricke.

A theorem of R. Fricke

We take for the modular group ${}_1\Gamma$ the group of all 2×2 matrices with rational integral elements and determinant 1. Any $L \in {}_1\Gamma$ induces a linear transformation of Poincaré's half-plane. If this transformation is different from the identity map and leaves a rational point ζ or ∞ fixed it is of parabolic type and L is called a parabolic matrix. It is well known that such a matrix has the form $\pm A^{-1}U^{m}A$ where $A \in {}_1\Gamma$ and $\zeta = A^{-1}\infty$ is a parabolic fixed point of the induced transformation or, as we shall say, of L. Here $U = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and m is a rational integer, not zero and uniquely determined by L. The modulus $|\, m \,|$ of m will be called the amplitude of the parabolic matrix L.

The group consisting of the two matrices $\pm I$, where $I = \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$, will be denoted by E. Then let Γ be any subgroup of ${}_1\Gamma$ and, for convenience, let $-I \in \Gamma$, so that the quotient group Γ/E is isomorphic to the group of linear transformations induced by the matrices of Γ. If Γ contains parabolic matrices P their fixed points are called cusps of Γ.

If ζ is a cusp of Γ the subgroup of all matrices of Γ with fixed point ζ is generated by $-I$ and a certain parabolic matrix P. While P is not uniquely determined by Γ and ζ, the choice is only between $\pm P$, $\pm P^{-1}$ of a common amplitude m. This number will be called the amplitude of ζ relative to Γ.

Received May 15, 1963.

If η is a cusp equivalent to ζ under Γ, i. e. if $\eta = L\zeta$ with $L \in \Gamma$, then η and ζ have equal amplitudes relative to Γ. We now make the following

DEFINITION. *Let Γ be any subgroup of ${}_1\Gamma$ and denote by $C(\Gamma)$ the subset of all cusp amplitudes relative to Γ in the set N of all positive rational integers. If $C(\Gamma)$ is nonempty and bounded in N, the least common multiple of all the numbers in $C(\Gamma)$ is a number $m \in N$ and will be called the level of Γ. If $C(\Gamma)$ is empty or unbounded, the level of Γ is defined to be the number zero.*

If Γ is of finite index in ${}_1\Gamma$, the number of equivalence classes of cusps under Γ is positive and finite. The level of Γ will then be positive.

For any positive integer m we now define the subgroup ${}_m\hat{\Gamma}$ of ${}_1\Gamma$ as the group generated by all parabolic $P \in {}_1\Gamma$ of amplitude m. The groups ${}_m\hat{\Gamma}$ were originally introduced by R. Fricke [3] and have recently reappeared as I. Reiner's groups $\Delta(m)$ (see [11]) and also in J. L. Brenner [1]. ${}_m\hat{\Gamma}$ may alternatively be defined as the least normal subgroup of ${}_1\Gamma$ containing both $-I$ and U^m. Omitting an easy proof we have

THEOREM 1. *If the subgroup Γ has positive level m then $\Gamma \supset {}_m\hat{\Gamma}$. Conversely, if ${}_m\hat{\Gamma} \subset \Gamma \subset {}_1\Gamma$ for some positive integer m then the level of Γ divides m and so is positive.*

If we regard any positive integer as a divisor of zero, we have an immediate

COROLLARY. *The inclusion $\Gamma_1 \subset \Gamma_2$ implies the relation $m_2 \mid m_1$ between the corresponding levels, provided only that m_2 is positive.*

The principal congruence groups

$${}_m\Gamma = \{L \in {}_1\Gamma : L \equiv \pm I \mod m\}$$

are known to be normal subgroups of finite index in ${}_1\Gamma$. Any subgroup of ${}_1\Gamma$ which contains a principal congruence group is called a congruence subgroup and is, of course, of finite index in ${}_1\Gamma$.

For congruence subgroups Γ, F. Klein has defined the level of Γ to be the least positive integer l with $\Gamma \supset {}_l\Gamma$ (or any multiple of l, but we ignore here the latter possibility). We shall see that this is equal to our general level m of Γ.

This is true, at any rate, for principal congruence groups ${}_m\Gamma$, which have all cusp amplitudes equal to m. But if Γ is any congruence subgroup, from $\Gamma \supset {}_l\Gamma$ we have, by the corollary above, $m \mid l$ with m the general level of Γ. That $l \mid m$ is also true, and therefore $l = m$, will follow from a result of R. Fricke (see [3, p. 417], and [12]), which we state as

THEOREM 2. *If Γ is a congruence subgroup of the (general) level m then ${}_m\Gamma \subset \Gamma$.*

For then $\Gamma \supset {}_m\Gamma$ and $\Gamma \supset {}_l\Gamma$, implying $\Gamma \supset {}_{(m,l)}\Gamma$. Therefore $(m, l) \geqq l$ by the minimum property of l, and $l \mid m$ follows.

To prove Theorem 2, let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be any matrix of ${}_m\Gamma$. It will suffice to take $M \equiv I \bmod m$. We have to show that M is in Γ. If R and S are any two matrices of Γ then M will belong to Γ if and only if RMS does. If we choose R and S from ${}_m\Gamma$, as we shall do, our hypothesis $M \in {}_m\Gamma$ will not be affected on replacing M by RMS. Changing M in the manner just indicated allows for simplifying assumptions to be made without loss of generality.

The first of these is $(d, l) = 1$, where l denotes Klein's level of Γ. If this is not originally true then $d \neq \pm 1$. But $(d, mc) = 1$ is easily inferred from $M \in {}_m\Gamma$ and so $c \neq 0$. Using Dirichlet's theorem on primes in an arithmetic progression we can find an integer g such that $d + gmc$ and l are relatively prime. On taking MU^{gm} in place of M our assumption is justified.

Next we assume $b \equiv 0 \bmod l$. Since $U^{hm}M$ has $b + hmd$ in place of b, this is permitted if the congruence $b + hmd \equiv 0 \bmod l$ can be solved for h. This is so for $(md, l) | b$. But from $(d, l) = 1$ and $m \mid l$ we have $(md, l) = m$, reducing the condition to $b \equiv 0 \bmod m$, a consequence of $M \in {}_m\Gamma$.

Similarly, $c \equiv 0 \bmod l$ may be assumed to hold.

Since M has determinant 1 our assumptions imply $ad \equiv 1 \bmod l$. But then M is congruent mod l to the matrix

$$M_0 = \begin{pmatrix} a & ad - 1 \\ 1 - ad & d(2 - ad) \end{pmatrix}$$

and so $L = M^{-1}M_0 \in {}_l\Gamma$. Therefore L is in Γ and M may be replaced by $M_0 = ML$. Now M_0 is the product

$$M_0 = \begin{pmatrix} 1 & 0 \\ d - 1 & 1 \end{pmatrix} \begin{pmatrix} a & a - 1 \\ 1 - a & 2 - a \end{pmatrix} \begin{pmatrix} 1 & d - 1 \\ 0 & 1 \end{pmatrix}$$

of three matrices each of which, unless it reduces to the matrix I, is parabolic of amplitude a multiple of m by virtue of $a \equiv d \equiv 1 \bmod m$. Therefore they are matrices of Γ, and $M_0 \in \Gamma$ follows, to complete the proof.

We conclude this section by an application of Fricke's theorem. The modular group can be shown to contain a subgroup of index 7 and with exactly two equivalence classes of cusps, of amplitudes 1 and 6 respectively. If this subgroup were a congruence subgroup, by Theorem 2 it would have to contain the principal congruence group ${}_6\Gamma$. But as $({}_1\Gamma : {}_6\Gamma) = 72$ is not divisible by 7 this is not possible. Our subgroup of index 7 is therefore not a congruence subgroup.

A class of normal subgroups

With any subgroup Γ of ${}_1\Gamma$ a Riemann surface S is associated by taking equivalence classes of the points of Poincaré's half-plane under Γ and local uniformizing parameters in the usual manner (see [6]). If Γ is of finite index in ${}_1\Gamma$, S will be compact. This, by the way, is the basis for a short proof of the well-known theorem that a function automorphic with respect to Γ, which is regular and bounded in the upper half-plane, is necessarily constant.

It is trivially verified that ${}_1\hat{\Gamma} = {}_1\Gamma$. Now let $m \geqq 2$, $\Gamma = {}_m\Gamma$ and let p denote the genus of S. Γ has no elliptic fixed points and all cusp amplitudes equal m. The same applies to the group $\hat{\Gamma} = {}_m\hat{\Gamma}$, which is contained in Γ according to Theorem 1. The Riemann surface $\hat{S}$ associated with $\hat{\Gamma}$ is therefore a smooth unlimited covering of S. It is, in fact, the universal covering.

We prove the last statement by showing that the quotient group $\Gamma/\hat{\Gamma}$ of all covering transformations of $\hat{S}$ over S has the structure of a fundamental group of the compact Riemann surfaces of genus p. Indeed, in the particular system of generators of Γ with defining relations, obtained by H. Petersson [6], [7], the elliptic generators are missing and the parabolic ones as well as $-I$ are in $\hat{\Gamma}$. There remain $2p$ generators G_ν, H_ν $(1 \leqq \nu \leqq p)$ and one defining relation

$$\prod_{\nu=1}^{p} G_\nu H_\nu G_\nu^{-1} H_\nu^{-1} \equiv I \qquad (\text{modulo } \hat{\Gamma}).$$

The same reasoning applies to any normal subgroup of finite index, of level m and without elliptic matrices, in place of ${}_m\Gamma$, and so to all normal subgroups of finite index except the groups Γ^2, Γ^3 in M. Newman [5].

Now the genus of ${}_m\Gamma$ is zero if $m \leqq 5$ and positive in all other cases and the universal covering surface of a compact Riemann surface S of positive genus is infinite-sheeted over S. The considerations above them imply

THEOREM 3. *For $1 \leqq m \leqq 5$ we have ${}_m\hat{\Gamma} = {}_m\Gamma$, while for $m \geqq 6$, ${}_m\hat{\Gamma}$ is a subgroup of infinite index in ${}_m\Gamma$.*

In particular, if $m \geqq 6$ then ${}_m\hat{\Gamma}$ does not contain any principal congruence group. This settles a question left open in I. Reiner [11], where the groups ${}_m\hat{\Gamma}$ are denoted by $\Delta(m)$. Theorem 3 was recently also proved by M. I. Knopp [4].

We shall now take up a method of I. Reiner [10] to construct a class of normal subgroups ${}_m\Gamma^s$ of finite index in ${}_1\Gamma$. ${}_m\Gamma^s$ will be of level m and not be a congruence subgroup except for $s = 1$. In view of Theorem 3 we suppose $m \geqq 6$. Leaving suffixes aside for the moment we put $\Gamma = {}_m\Gamma$, $\hat{\Gamma} = {}_m\hat{\Gamma}$.

Let $\mathrm{P} = \Gamma/\hat{\Gamma}$, P' the commutator subgroup of P and $\tilde{\Gamma}$ the inverse image of P' under the canonical mapping of Γ onto P. Then $\hat{\Gamma} \subset \tilde{\Gamma} \subset \Gamma$, $\tilde{\Gamma}$ is a normal subgroup in Γ and $\Delta = \Gamma/\tilde{\Gamma}$ is the free abelian group of $2p$ generators. All this follows readily from the results on the structure of the quotient group P as stated above. The rest of the argument is exactly like I. Reiner's in [10, p. 142] with Δ replacing $\Delta(m)$, and will not be repeated.

Instead of I. Reiner's groups $\Omega(p, s)$ an infinite set of groups ${}_m\Gamma^s$ $(m \geqq 6; s \geqq 1)$ is thus arrived at with the following properties.

(1) ${}_m\Gamma^s$ is a normal subgroup of finite index in ${}_1\Gamma$.
(2) ${}_m\Gamma^s$ is generated by ${}_m\tilde{\Gamma}$ and the s^{th} powers of the matrices in ${}_m\Gamma$.
(3) ${}_m\hat{\Gamma} \subset {}_m\Gamma^s \subset {}_m\Gamma$.
(4) ${}_m\Gamma^s$ is of level m.

(5) ${}_m\Gamma^s = {}_n\Gamma^t$ implies $m = n$ and $s = t$.
(6) ${}_m\Gamma^s$ does not contain any principal congruence group except for $s = 1$.

Properties (1), (2) correspond to like properties in the groups $\Omega(p, s)$. They follow readily from the construction, as does (3). In fact, ${}_m\tilde{\Gamma} \subset {}_m\Gamma^s$.

Since ${}_m\Gamma$ is of level m, (4) follows from (3), Theorem 1 and its corollary.

For m fixed and $s \neq t$ the groups Δ^s and Δ^t are distinct by construction. So then are ${}_m\Gamma^s$ and ${}_m\Gamma^t$. This proves (5) in view of the fact that groups of different levels are certainly distinct.

Finally, let ${}_m\Gamma^s$ contain a principal congruence group, i.e. let it be a congruence subgroup. In view of (4) Theorem 2 gives ${}_m\Gamma \subset {}_m\Gamma^s$. This is true for $s = 1$ when, in fact, ${}_m\Gamma = {}_m\Gamma^s$ holds. (6) then follows from (5).

Normal subgroups of level 6

As before, let E be the normal subgroup of ${}_1\Gamma$ consisting of $\pm I$. Let P' be the commutator subgroup of the quotient group $\mathrm{P} = {}_1\Gamma/\mathrm{E}$ and ${}_1\Gamma'$ the inverse image of P' in the canonical mapping of ${}_1\Gamma$ onto P. We use a well-known arithmetic characterization of the matrices $L = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in {}_1\Gamma$ belonging to ${}_1\Gamma'$ which may be found, for instance, in H. Petersson [8]. The condition is

$$ab + 3bc + cd \equiv 0 \mod 6.$$

Incidentally, M. Newman's groups Γ^2, Γ^3 (see [5]) are characterized, respectively, by

$$ab + bc + cd \equiv 0 \mod 2 \qquad \text{and} \qquad ab + cd \equiv 0 \mod 3.$$

This makes $\Gamma^2 \cap \Gamma^3 = {}_1\Gamma'$ obvious.

It follows that ${}_1\Gamma'$ is a congruence subgroup and of level 6.

We shall now state a result due to R. Fricke [2]. To do so we need a function $h(c, d)$ of the pairs c, d of coprime rational integers and with values in the field $K = Q(\xi_3)$, where $\xi_3 = \exp(\frac{1}{3}\pi i)$, of the third roots of unity over the rationals. $h(c, d)$ may be recursively computed from the relations

$$h(0, 1) = 0, \qquad h(-d, c) + h(c, d) = 1, \qquad h(c, c + d) = \xi_3 h(c, d).$$

Then, according to Fricke, there is a one-to-one mapping of the set of normal subgroups Γ in ${}_1\Gamma$ satisfying ${}_6\hat{\Gamma} \subset \Gamma \subset {}_1\Gamma'$ onto the set of ideals H of algebraic integers of K. Any such Γ is characterized arithmetically by

$$\Gamma = \left\{ L = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in {}_1\Gamma' : h(c, d) \in H \right\},$$

where H is the ideal corresponding to Γ. Furthermore, the number of classes of cusps equivalent under Γ is equal to the norm of H.

M. Newman shows [5, Theorem 6] that the group Γ^6 generated by $-I$ and the sixth powers of modular matrices is contained in ${}_1\Gamma'$ and that $({}_1\Gamma' : \Gamma^6) = 36$. On the other hand, $U^6 \in \Gamma^6$. Then, Γ^6 being a normal subgroup in ${}_1\Gamma$, ${}_6\hat{\Gamma} \subset \Gamma^6$.

Thus Γ^6 is of level 6 and the question arises as to the ideal H of K corresponding to Γ^6 in Fricke's mapping.

The answer is easy to find. Since $({}_1\Gamma : \Gamma^6) = 216$ and Γ^6 is of level 6, this group has exactly 36 inequivalent cusps. Therefore H has norm 36. But $H = (6)$ is the only ideal in K with this norm and hence follows

THEOREM 4. *The subgroup Γ^6 of ${}_1\Gamma$ generated by $-I$ and the sixth powers of the matrices of ${}_1\Gamma$ consists of all $L = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in {}_1\Gamma'$ which have $h(c, d) \equiv 0 \bmod (6)$.*

Remark. The numbers $h(c, d)$ are closely related to the periods of an integral of the first kind belonging to the Riemann surface, of genus $p = 1$, associated with ${}_1\Gamma'$. This connection may be used to establish the results of R. Fricke [2] as given above.

Modular subgroups of small indices

By a slight generalization of the results of R. Fricke [2] a subgroup Γ of level 6 and index 7 in ${}_1\Gamma$ can be constructed consisting of all $L = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in the modular group ${}_1\Gamma$ which have $h(c, d) \equiv 0 \bmod (1 + 2\xi_3)$. That Γ is not a congruence subgroup has already been inferred from Theorem 2. The same is then also true of the transformed groups $A^{-1}\Gamma A$ $(A \in {}_1\Gamma)$.

Thus, from Theorem 5 below it follows that 7 is the least positive integer μ such that there is a modular subgroup Γ, which is not a congruence subgroup, of index μ in ${}_1\Gamma$.

THEOREM 5. *Let Γ be a subgroup in ${}_1\Gamma$ of index $\mu \leqq 6$. Then Γ is a congruence subgroup.*

Two remarks will precede the proof of the theorem. We first note that the index μ of a modular subgroup Γ is equal to the sum of the amplitudes of a complete set of cusps inequivalent under Γ, as is clear from the usual method of constructing a fundamental domain for Γ out of the classical one for ${}_1\Gamma$. Any positive integer m appearing as the level of a modular subgroup Γ of index μ is then the least common multiple of the parts in an unrestricted partition of μ into positive integers.

We also need the fundamental topological equation

$$\mu = 12(p - 1) + 6\sigma + 3e_2 + 4e_3,$$

which may be found in H. Petersson [8, formula (1)].

Here σ is the number of equivalence classes of cusps under Γ, while e_2 and e_3, respectively, denote the corresponding class numbers for elliptic fixed points of Γ of orders 2 and 3. The formula shows, in particular, that there does not exist a subgroup Γ with $\mu = 5$, $\sigma = 2$, which would have cusp amplitudes $m_1 = 2$, $m_2 = 3$ and therefore be of level 6. But then any subgroup Γ of index $\mu \leqq 5$ is of level $m \leqq 5$ and so, by Theorems 1 and 3, a congruence subgroup.

To prove Theorem 5 it is, therefore, sufficient to consider subgroups of index 6. If the level m of Γ does not exceed 5, Γ is disposed of as above. As the number 6 cannot be partitioned into parts whose least common multiple exceeds 6 we are left with groups Γ which have $\mu = m = 6$. There is then either $\sigma = 1$ (cusp amplitude 6) or $\sigma = 3$ (amplitudes 1, 2, 3). It is a result of H. Petersson that the latter case is impossible, while in the former there exist the following groups Γ, all congruence subgroups, and no others:

$p = 1,$	$e_2 = e_3 = 0$		1 group,
$p = 0,$	$e_2 = 4,$	$e_3 = 0$	3 groups,
$p = 0,$	$e_2 = 0,$	$e_3 = 3$	2 groups.

With these results the theorem is proved.

Remark. H. Petersson [9] asserts the truth of Theorem 5. His (unpublished) proof of it consists in a systematic search, in particular, for all modular subgroups of index less than 7.

References

1. J. L. Brenner, *The linear homogeneous group, III*, Ann. of Math. (2), vol. 71 (1960), pp. 210–223.
2. R. Fricke, *Über die ausgezeichneten Untergruppen vom Geschlechte $p = 1$, welche in der Gruppe der linearen ω-Substitutionen enthalten sind*, Math. Ann., vol. 30 (1887), pp. 345–400.
3. F. Klein and R. Fricke, *Vorlesungen über die Theorie der elliptischen Modulfunktionen, Band I*, Leipzig, 1890.
4. M. I. Knopp, *A note on subgroups of the modular group*, Proc. Amer. Math. Soc., vol. 14 (1963), pp. 95–97.
5. M. Newman, *The structure of some subgroups of the modular group*, Illinois J. Math., vol. 6 (1962), pp. 480–487.
6. H. Petersson, *Zur analytischen Theorie der Grenzkreisgruppen I*, Math. Ann., vol. 115 (1937), pp. 23–67.
7. ———, *Automorphe Formen als metrische Invarianten I*, Math. Nachr., vol. 1 (1948), pp. 158–212.
8. ———, *Über einen einfachen Typus von Untergruppen der Modulgruppe*, Arch. Math., vol. 4 (1953), pp. 308–315.
9. ———, *Über die Kongruenzgruppen der Stufe 4*, J. Reine Angew. Math., vol. 212 (1963), pp. 63–72.
10. I. Reiner, *Normal subgroups of the unimodular group*, Illinois J. Math., vol. 2 (1958), pp. 142–144.
11. ———, *Subgroups of the unimodular group*, Proc. Amer. Math. Soc., vol. 12 (1961), pp. 173–174.
12. K. Wohlfahrt, *Über Dedekindsche Summen und Untergruppen der Modulgruppe*, Abh. Math. Sem. Univ. Hamburg, vol. 23 (1959), pp. 5–10.

University of Münster
Münster, Germany