ON SOME REPRESENTATIONS OF $SL(2, Z)$

BY

KLAUS WOHLFAHRT

Introduction

Subgroups of the modular group ${}_1\Gamma = SL(2, Z)$ may effectively be constructed by means of such representations as have been known through F. Klein, E. Hecke and B. Schoeneberg (cf. [3]). This is also true for representations which so far do not seem to occur in the literature and whose kernel is not a congruence subgroup of ${}_1\Gamma$. Any coset decomposition of ${}_1\Gamma$ relative to a subgroup Γ of finite index gives rise to a permutation representation. The case of cycloidal subgroups Γ, which were introduced in H. Petersson [2], is particularly simple and will be treated in detail. Thereby, for any positive integer n, a one-to-one correspondence results between the set of cycloidal subgroups of index n in ${}_1\Gamma$ and a certain set of permutations, each of order at most 2, of n elements.

In a particular case with $n = 9$ the intersection of all the conjugates of Γ is a normal subgroup Δ of index 504 in ${}_1\Gamma$, and the factor group turns out to be isomorphic to the simple group $PSL(2, 8)$ over the Galois-field $GF(8)$.

Another example concerns a congruence cycloidal subgroup of index 7 in ${}_1\Gamma$. The method here leads to a characterization of the matrices of that group.

The idea of associating permutations with modular subgroups has recently also been treated in M. H. Millington [1].

Using Hecke's notation, $U = (1\ 1 \mid 0\ 1)$ and $T = (0\ -1 \mid 1\ 0)$ with $T^2 = (TU)^3 = -I$ generate the modular group. All modular subgroups will be supposed to contain the matrix $-I = (-1\ 0 \mid 0\ -1)$.

Let Γ be a cycloidal subgroup of index n in ${}_1\Gamma$ and $N = \{0, 1, 2, \cdots, n-1\}$ the set of integers 0 through $n - 1$. The cosets in

$$ {}_1\Gamma = \bigcup_{j \in N} \Gamma U^j $$

are permuted by right-hand multiplication by any matrix $L \in {}_1\Gamma$. If the cosets be numbered by the corresponding exponents j, a permutation πL of the elements of N is obtained. Each πL is an element of the symmetric permutation group S_n operating on N, and $\pi : {}_1\Gamma \rightarrow S_n$ is a representation of ${}_1\Gamma$ by permutations. In particular we have $\pi U = \omega$, where $\omega = (012 \cdots (n-1))$ denotes the cyclic permutation changing j into $j + 1 \pmod n$.

Abbreviating $\tau = \pi T$, from $T^2 = -I$ we have $\tau^2 = \iota$, the identity element of S_n. We shall let πL operate on N from the right-hand side, using exponent notation. Thus τ, as an element of S_n, is characterized by

$$ U^j T U^{-j^\tau} \in \Gamma \qquad (j \in N), $$

Received October 8, 1968.

and therefore τ describes the correspondence between the sides of a fundamental domain of Γ, which may be taken to be a connected set of n modular triangles in the upper half-plane with common cusp ∞. The relations in ${}_1\Gamma$ now imply $\tau^2 = (\tau\omega)^3 = \iota$.

2

We have associated with each cycloidal subgroup Γ of index n in ${}_1\Gamma$ a permutation $\tau \in S_n$ satisfying $\tau^2 = (\tau\omega)^3 = \iota$. This map may be reversed by means of the following

LEMMA. *Let n be a positive integer and S_n the symmetric group of permutations of the elements of $N = \{0, 1, 2, \cdots, n-1\}$ with identity element ι and $\omega = (012 \cdots (n-1))$. Then, if $\tau \in S_n$ with $\tau^2 = \iota$, if $G = \langle \omega, \tau \rangle$ is the subgroup of S_n generated by ω and τ, and if*

$$H = \{\eta \mid \eta \in G, 0^\eta = 0\}$$

denotes the subgroup of all η in G which fix $0 \in N$, we have

(1) *G operates transitively on N,*
(2) *G admits a coset decomposition $G = \bigcup_{j \in N} H\omega^j$,*
(3) *H is generated by elements $\eta_j = \omega^j \tau \omega^{-j^\tau}$ $(j \in N)$,*
(4) *the intersection of all conjugates of H in G is trivial.*

Proof. (1) is clear and $\eta_j \in H$ $(j \in N)$ easily verified. Let $\gamma \in G$ and so

$$\gamma = \omega^{a_1}\tau\omega^{a_2}\tau \cdots \tau\omega^{a_t}$$

with numbers $a_\nu \in N$ $(1 \leqq \nu \leqq t)$. Choosing $j_\nu \in N$ $(1 \leqq \nu \leqq t)$ according to $j_1 = a_1, j_{\nu+1} \equiv a_{\nu+1} + j_\nu^\tau \bmod n$ $(1 \leqq \nu < t)$ we may write

$$\gamma = \omega^{a_1} \prod_{\nu=1}^{t-1} (\omega^{-j_\nu}\eta_{j_\nu}\omega^{j_\nu^\tau + a_{\nu+1}}) = \prod_{\nu=1}^{t-1} (\eta_{j_\nu}\omega^{j_\nu^\tau + a_{\nu+1} - j_{\nu+1}})\omega^{j_t},$$

i.e. $\gamma = \eta\omega^j$, with $\eta = \prod_{\nu=1}^{t-1} \eta_{j_\nu} \in H$ and $j = j_t \in N$. As $\omega^k \notin H$ unless $k \equiv 0 \bmod n$ this establishes (2). If now $\gamma = \eta\omega^j \in H$, then $\omega^j \in H$ and so $j = 0$. This proves (3). Finally, as $\omega^{-k}H\omega^k$ is the subgroup of all elements of G fixing $k \in N$, (4) is also proved.

3

Let n be a positive integer and $\tau \in S_n$, $\tau^2 = (\tau\omega)^3 = \iota$. There is a representation $\pi : {}_1\Gamma \rightarrow S_n$ with $\pi U = \omega$ and $\pi T = \tau$. The image of π is the subgroup G of S_n occurring in the lemma. By (2) then the inverse image $\Gamma = \pi^{-1}H$ of H under π affords ${}_1\Gamma = \bigcup_{j \in N} \Gamma U^j$ and so is cycloidal of index n in ${}_1\Gamma$. It is clear that Γ induces the representation π in the sense of Section 1. Thus we have the following

THEOREM. *To each cycloidal subgroup Γ of an index n in ${}_1\Gamma$ there corresponds through*

$$U^jTU^{-j^\tau} \in \Gamma \qquad (j \in N)$$

a permutation $\tau \in S_n$ with $\tau^2 = (\tau\omega)^3 = \iota$ and vice versa.

The generators η_j ($j \in N$) of H satisfy certain relations easily read off from τ and $\sigma = \tau\omega$, if these permutations are written in cycles. If (j) is a cycle occurring in τ or in σ, $\eta_j^2 = \iota$ or $\eta_j^3 = \iota$ holds, respectively. To each cycle (jk) of τ a relation $\eta_j \eta_k = \iota$ corresponds, and each cycle (jkl) of σ similarly implies $\eta_j \eta_k \eta_l = \iota$.

By the lemma, (4), the kernel Δ of the representation π is the intersection of the conjugates of Γ in ${}_1\Gamma$. Therefore G is isomorphic to the factor group ${}_1\Gamma/\Delta$, and H to Γ/Δ.

Both groups Γ and Δ are of the same level in ${}_1\Gamma$ as defined in [4], and if one of them is a congruence subgroup of ${}_1\Gamma$ so is the other.

4

We now take up the particular case $n = 9$, $\tau = (14)(26)(37)(58)$. As $\sigma = \tau\omega = (015)(274)(386)$ is of order 3, τ indeed corresponds to some cycloidal subgroup Γ of index 9 in ${}_1\Gamma$.

If Γ were a congruence subgroup of ${}_1\Gamma$, because its level is 9, it would have to contain the principal congruence group ${}_9\Gamma$ (cf. [4]), and ${}_9\Gamma \subset \Delta$ would follow. Now $(TU^3)^6 \equiv -I \bmod 9$, while $\tau\omega^3 = (0317652)$ is not of order 6, so $(TU^3)^6 \notin \Delta$, and Γ is not a congruence subgroup of ${}_1\Gamma$.

By the relations

$$\eta_0^2 = \eta_1 \eta_4 = \eta_2 \eta_6 = \eta_3 \eta_7 = \eta_5 \eta_8 = \eta_0 \eta_1 \eta_5 = \eta_2 \eta_7 \eta_4 = \eta_3 \eta_8 \eta_6 = \iota$$

t is seen that η_0, η_2 and η_7 suffice to generate H and satisfy

$$\eta_0^2 = \eta_0 \eta_2 \eta_7 \eta_2^{-1} \eta_7^{-1} = \iota.$$

This shows—as does already the permutation τ—that the Riemann surface belonging to Γ has genus 1. A. O. L. Atkin has computed the coefficients of the algebraic equation between two generating functions belonging to Γ. He found essentially (unpublished)

$$y^2 = 4 \cdot x^3 + 225 \cdot x^2 + 3840 \cdot x + 16384.$$

If this is put into Weierstrass normal form,

$$Y^2 = 4 \cdot X^3 - g_2 \cdot X - g_3,$$

then $g_2 = 1515$, $g_3 = 23053$ and so

$$\delta = g_2^3 - 27 \cdot g_3^2 = -2^{27} \cdot 3^4,$$

$$j = 12^3 \cdot g_2^3 \cdot \delta^{-1} = -2^{-21} \cdot 3^2 \cdot 5^3 \cdot 101^3.$$

The absolute invariant j not being an integer it may be concluded that the function field of genus 1 belonging to Γ has no complex multiplication.

5

Continuing with the particular case of Section 4, besides $\tau^2 = \tau\eta_2 \eta_7 \eta_2^{-1} \eta_7^{-1} = \iota$

there ought to be other relations in the group H. Indeed, $\eta_7 \eta_2 = \eta_2^2 \tau$ is easily verified, and elimination of η_7 then leads to

$$\eta_2^4 \tau \eta_2^2 \tau \eta_2 \tau = \iota.$$

This may be used to show that $\eta_2^{\mu} \tau \eta_2^{-\mu}$ (μ mod 7), all of order 2, together with ι form an abelian subgroup K, normal in H, of order 8. The factor group is generated by $\eta_2 K$ and so is cyclic or order 7. Therefore, H has order 56 and then G has order 504.

Transformation of $\eta_2 = (0)(1)(2456873)$ by powers of $\eta_7 = (0)(8)(1267543)$ leads to permutations in H which fix any $j = 1, 2, \cdots, 7$ besides 0 while changing the rest of N cyclically. The case $j = 8$ is covered by η_7. Therefore H is doubly transitive as a permutation group on $N' = \{1, 2, \cdots, 8\}$. G is then a triply transitive permutation group of degree 9, and so its order, 504, is a product of the form $9 \cdot 8 \cdot 7 \cdot q$, with q the order of any subgroup of G whose operations fix 3 elements of N. This gives $q = 1$, therefore ι is the only permutation in G fixing more than 2 elements of N. It is not difficult to show now that G is isomorphic to the well-known simple group $PSL(2, 8)$ of 2×2-matrices of determinant 1 with elements in the Galois-field $GF(8)$.

6

The Galois-field $GF(8)$ is an extension of degree 3 of the prime field of characteristic 2, and the elements of this field different from zero form a cyclic group of order 7.

There is a generator ε of this group with $\varepsilon^3 + \varepsilon + 1 = 0$, and so we may write $GF(8) = \{0, 1, \varepsilon, \varepsilon^2, \cdots, \varepsilon^6\}$, and

$$\varepsilon^3 = 1 + \varepsilon, \quad \varepsilon^4 = \varepsilon + \varepsilon^2, \quad \varepsilon^5 = 1 + \varepsilon + \varepsilon^2, \quad \varepsilon^6 = 1 + \varepsilon^2.$$

The matrices

$$A = \begin{pmatrix} \varepsilon & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & \varepsilon^3 \\ 0 & 1 \end{pmatrix}$$

give $B^2 = (BA)^3 = I$, therefore there is a representation

$$D : {}_1\Gamma \to PSL(2, 8)$$

with $DU = A$ and $DT = B$. That D essentially is the representation $\pi : {}_1\Gamma \to G$ is seen as follows: Introducing the projective line of nine points with homogeneous coordinates $\xi, \eta \in GF(8)$ we take $t = \xi\eta^{-1}$ as a projective scale with values in $GF(8) \cup \{\infty\}$. Any $L = (\alpha\, \beta \mid \gamma\, \delta)$ in $PSL(2, 8)$ induces a permutation of these values by

$$t \to L^{-1}t = (\delta t + \beta)(\gamma t + \alpha)^{-1}.$$

In particular, DU, DT and $D(TU)$, respectively, induce

$$(\infty\ 0\ \varepsilon^6\ \varepsilon^2\ \varepsilon^3\ 1\ \varepsilon^4\ \varepsilon^5\ \varepsilon), \quad (\infty)(0\ \varepsilon^3)(\varepsilon^6\ \varepsilon^4)(\varepsilon^2\ \varepsilon^5)(1\ \varepsilon),$$

and

$$(\infty\ 0\ 1)(\varepsilon^6\ \varepsilon^5\ \varepsilon^3)(\varepsilon^2\ \varepsilon\ \varepsilon^4).$$

If the values of the t-scale are suitably labelled by the elements of N, the 3 permutations above, respectively, exactly correspond to ω, τ and σ. This proves the assertion made at the end of Section 5.

7

Another application of the theorem in section 3 arises in the case $n = 7$, $\tau = (12)(36)$. Here $\sigma = \tau\omega = (013)(456)$ is of order 3 and so τ determines a cycloidal subgroup Z of index 7 in ${}_1\Gamma$.

Z is a congruence subgroup of level 7. Indeed, a system of defining relations for the factor group ${}_1\Gamma/{}_q\Gamma$, with ${}_q\Gamma$ the principal congruence group of prime level q, is

$$U^q \equiv T^2 \equiv (TU)^3 \equiv (TU^jTU^k)^2 \equiv \pm I \mod q$$

($jk \equiv 2 \bmod q$) (cf. [3]), and the assertion made then follows from $(\tau\omega^3)^4 = \iota$.

As a consequence $G = \langle\tau, \omega\rangle$ is isomorphic to the simple group ${}_1\Gamma/{}_7\Gamma$ of order 168 and $H = \langle\eta_j \mid j \bmod 7\rangle$ has order 24.

Now from

$$\eta_0 = (12)(36), \quad \eta_3 = (1534)(26), \quad \text{and} \quad \eta_4 = (26)(45)$$

it will be found that $K = \langle\eta_3^2, \eta_4\rangle$ is an abelian (non-cyclic) group of order 4, Klein's "Vierergruppe", and normal in $\langle\eta_0, \eta_3, \eta_4\rangle$. As K is of index 2 in $\langle\eta_3, \eta_4\rangle$ and the latter group does not contain $\eta_0\,\eta_3\,\eta_4 = (124)(365)$ of order 3 as an element, the order of the group generated by η_0, η_3 and η_4 is at least 24. Therefore that group is H and of octahedral type, and K is its unique normal subgroup of order 4. As G is simple, K is not normal in G and H must be the normalizer with respect to G of K. This fact will be used to describe the matrices $L \in$ Z.

Let Λ be the inverse image of K under the permutation representation $\pi : {}_1\Gamma \to G$ defined by $\pi U = \omega$, $\pi T = \tau$. Λ is, of course, a congruence subgroup of level 7 in ${}_1\Gamma$. Because $\eta_4 = \omega^4\tau\omega^{-4}$ is in K, Λ will contain all modular matrices which up to a sign are congruent mod 7 to U^4TU^{-4}. Taking regard of the other elements of K in the same way it is found that Λ consists of all $L \in {}_1\Gamma$ satisfying

$$\pm L \equiv \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}4 & 4\\ 1 & 3\end{pmatrix}, \begin{pmatrix}4 & 2\\ 2 & 3\end{pmatrix} \text{ or } \begin{pmatrix}4 & 1\\ 4 & 3\end{pmatrix} \mod 7.$$

But Z is the inverse image under π of the group H and, because of what has been said above, will be the normalizer of Λ with respect to ${}_1\Gamma$. Therefore Z consists of all modular matrices L such that

$$L\begin{pmatrix}4 & 4t^2\\ t & 3\end{pmatrix}L^{-1} \qquad (t = 1, 2, 4)$$

are congruent mod 7 to matrices

$$\pm\begin{pmatrix} 4 & 4s^2 \\ s & 3 \end{pmatrix}.$$

Evaluating congruences leads to this

THEOREM. *A certain cycloidal subgroup of index* 7 *in* ${}_1\Gamma$ *consists of all* $L = (a\, b \mid c\, d) \in {}_1\Gamma$ *satisfying*

$$a \equiv d^2(4d^3 - c^3) \mod 7 \qquad (7 \nmid c),$$

$$b \equiv c^2(3c^3 - d^3) \mod 7 \qquad (7 \nmid d).$$

Remark. Similar descriptions may be obtained for cycloidal subgroups of indices 5 or 11 in ${}_1\Gamma$.

REFERENCES

1. M. H. MILLINGTON, *On cycloidal subgroups of the modular group*, Proc. London Math. Soc., vol. 19 (1969), pp. 164–176.
2. H. PETERSSON, *Über einen einfachen Typus von Untergruppen der Modulgruppe*, Arch. Math., vol. 4 (1953), pp. 308–315.
3. B. L. VAN DER WAERDEN, *Gruppen von linearen Transformationen*, Erg. Mat., vol. 4, Springer-Verlag, New York, 1958.
4. K. WOHLFAHRT, *An extension of F. Klein's level concept*, Illinois J. Math., vol. 8 (1964), pp. 529–535.

MATHEMATISCHES INSTITUT
HEIDELBERG, GERMANY