COLLOQUIUM MATHEMATICUM

VOL. LIV 1987 FASC. 1

FAITHFUL INTEGRAL AND MODULAR REPRESENTATIONS OF THE KLEIN BOTTLE GROUP

BY

HUGO H. TORRIANI (CAMPINAS)

A direct proof of the nonexistence of faithful unimodular representations of order two over arbitrary domains for the Klein bottle group is given. Countably many inequivalent faithful representations of order two for that group over monogenic ring extensions of the ring Z of rational integers and over fields of prime characteristic are constructed. A simple proof of the nonexistence of subgroups of $GL(2, Z)$ isomorphic to $Z \oplus Z$ is also given.

1. Faithful integral representations. Let K be the fundamental group of the Klein bottle. We recall that K has a presentation given by two generators a, b and the relation $abab^{-1} = 1$. Let σ be the homomorphism of the additive group Z of rational integers onto $\mathrm{Aut}(Z)$ that maps the integer 1 onto the automorphism -1 of Z. Then K is isomorphic to the semidirect product $Z \times_\sigma Z$.

By [1] (cf. also [4] and [2], Part 2, p. 157) one knows that every polycyclic group has a faithful representation in $SL(n, Z)$ for some n. For K one has, e.g., the faithful representation

$$(-1)^s \begin{pmatrix} (-1)^s & 0 & r \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix}$$

in $SL(3, Z)$. The question then arises as to whether three is the least possible order for faithful integral representations of K. The following result settles that question in a direct fashion:

THEOREM 1. *There are no faithful representations of K of order two over the rational integers.*

Proof. Assume there are matrices

$$\alpha = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

in $GL(2, Z)$ such that $\alpha\beta = \beta\alpha^{-1}$, and let $\delta = \det(\alpha)$. If $\delta = 1$, we obtain $q(x+w) = r(x+w) = 0$. If $x+w = 0$, then $\beta^2 = \pm I$, where I is the identity matrix; and if $x+w \neq 0$, then $\alpha = \pm I$. Hence $\delta = -1$, but then $(p+s)(x+w) = 0$, so that either $\alpha^2 = \pm I$ or $\beta^2 = \pm I$.

COROLLARY. *There are no faithful representations of K in* $\mathrm{SL}(2, R)$ *for any domain R of any characteristic.*

Remark. In Section 3 we shall give a simple proof of the nonexistence of faithful representations of $Z \oplus Z$ of order two over the rational integers. Theorem 1 then results as an immediate consequence, but the proof given above is shorter. In addition, the Corollary holds for arbitrary domains.

Let $R[T]$ be the ring of polynomials in the indeterminate T with coefficients in a domain R, W an element of R that is neither zero nor a unit, $(WT-1)$ the ideal in $R[T]$ generated by the polynomial $WT-1$, and $R[W^{-1}]$ the quotient ring $R[T]/(WT-1)$.

THEOREM 2. *Let w be an integer such that $|w| \geqslant 2$. Then K has countably many inequivalent faithful representations of order two over $S = Z[w^{-1}]$. A fortiori, K has countably many inequivalent faithful rational representations of order two.*

Proof. Let μ and ν be nonzero integers and $M(\mu, \nu)$ the subgroup of $\mathrm{GL}(2, S)$ generated by the matrices

$$\alpha = \begin{pmatrix} w^{\mu} & 0 \\ 0 & w^{-\mu} \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 0 & w^{\nu} \\ w^{\nu} & 0 \end{pmatrix}.$$

Then $\alpha\beta\alpha\beta^{-1} = I$, and the induced mapping of K onto $M(\mu, \nu)$ is injective. Alternatively, let x be a positive integer and let y and z be nonnegative integers such that $x^2 - yz = 1$ and either $y \neq 0$ or $z \neq 0$. Let τ be a nonzero integer and $N(x, y, z, \tau)$ the subgroup of $\mathrm{GL}(2, S)$ generated by the matrices

$$A = \begin{pmatrix} x & y \\ z & x \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} w^{\tau} & 0 \\ 0 & -w^{\tau} \end{pmatrix}.$$

Then $ABAB^{-1} = I$, and as A^r is not a diagonal matrix unless $r = 0$, the induced mapping of K onto $N(x, y, z, \tau)$ is injective.

COROLLARY. *There are countably many inequivalent faithful representations of K in* $\mathrm{SL}(3, S)$, *and a fortiori in* $\mathrm{SL}(3, Q)$, *where Q is the rational field.*

2. Faithful modular representations. If S is a domain of nonzero characteristic and K is a subgroup of $\mathrm{GL}(2, S)$, then obviously the transcendence degree of S over the prime field must be at least one. The first construction of Theorem 2 has the following modular analog:

THEOREM 3. *Let p be any prime number, and X a transcendental over Z/pZ. Then K has countably many inequivalent faithful representations of order two over $S = (Z/pZ)[X, X^{-1}]$. A fortiori K has countably many inequivalent faithful representations of order two over the function field $F = (Z/pZ)(X)$.*

COROLLARY. *There are countably many inequivalent faithful representations of* K *in* $\mathrm{SL}(3, S)$, *and a fortiori in* $\mathrm{SL}(3, F)$.

We shall now modify the second construction of Theorem 2 to exhibit other faithful representations of K of order two over fields of odd characteristic.

THEOREM 4. *Let* p *be an odd prime,* X *a transcendental over* Z/pZ, Y *an element in the algebraic closure of* $(Z/pZ)(X)$ *such that* $Y^2 = X^2 - 1$, *and* W *an element of* $R = (Z/pZ)[X, Y]$ *not in* Z/pZ. *Then* K *has countably many inequivalent faithful representations of order two over* $S = R[W^{-1}]$. *A fortiori,* K *has countably many inequivalent faithful representations of order two over the function field* $F = (Z/pZ)(X, Y)$.

Proof. Consider the subgroup of $\mathrm{GL}(2, S)$ generated by the matrices

$$A = \begin{pmatrix} X & Y \\ Y & X \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} W^\tau & 0 \\ 0 & -W^\tau \end{pmatrix},$$

where τ is a nonzero integer. Then $ABAB^{-1} = I$, and for the injectivity we need only to prove that A^r is not a diagonal matrix unless $r = 0$. For this purpose we set

$$P = \begin{pmatrix} \bar{1} & \bar{1} \\ \bar{1} & -\bar{1} \end{pmatrix},$$

where $\bar{z}$ denotes the canonical image of $z \in Z$ in Z/pZ, and verify that

$$P^{-1}AP = \begin{pmatrix} X+Y & 0 \\ 0 & X-Y \end{pmatrix}.$$

If $r > 0$, it follows that

$$A^r = \begin{pmatrix} \xi & \eta \\ \eta & \xi \end{pmatrix},$$

where

$$\xi = \bar{2}^{-1}[(X+Y)^r + (X-Y)^r] \quad \text{and} \quad \eta = \bar{2}^{-1}[(X+Y)^r - (X-Y)^r].$$

A computation shows that

$$\eta = Y \sum_{j=0}^{r'-1} (-1)^j \left[\sum_{k=1}^{r'-j} \binom{r}{r-2k+1}^- \binom{r'-k}{j}^- \right] X^{r-2j-1}$$

if $r = 2r'$, and

$$\eta = Y \sum_{j=0}^{r'} (-1)^j \left[\sum_{k=0}^{r'-j} \binom{r}{r-2k}^- \binom{r'-k}{j}^- \right] X^{r-2j-1}$$

if $r = 2r' + 1$. In either case the coefficient of X^{r-1} is $\bar{2}^{r-1}$, and the assumption that $\eta = 0$ leads to a contradiction.

COROLLARY. *There are countably many inequivalent faithful representations of K in* $\mathrm{SL}(3, S)$, *and a fortiori in* $\mathrm{SL}(3, F)$.

Remark. The proof can be shortened by taking W to be a transcendental over F, but the resulting representation will then have coefficients in a field of transcendence degree two over Z/pZ.

3. The rank of $\mathrm{GL}(2, Z)$. Our purpose in this section is to show by elementary means that $\mathrm{GL}(2, Z)$ does not contain any subgroup isomorphic to $Z \oplus Z$. Let R be any commutative ring with identity. If A is any matrix of order two over R, we call

$$\Delta A = (\operatorname{tr} A)^2 - 4 \cdot \det A$$

the discriminant of A. Our basic device is the following result on the spectrum of commuting operators on the R-module $R \oplus R$.

LEMMA. *Let R be as above and let*

$$A = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \quad \textit{and} \quad B = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

be two commuting matrices over R. (Neither A nor B need be invertible.) Then $z^2 \Delta A = r^2 \Delta B$.

Proof. Since $AB = BA$, we have $ry = qz$ and $(p-s)z = r(x-w)$. A straightforward verification then yields the Lemma.

THEOREM 5. *There are no faithful representations of $Z \oplus Z$ of order two over the rational integers.*

Proof. Let g and g' be generators of $Z \oplus Z$ and let ϱ be a monomorphism of $Z \oplus Z$ into $\mathrm{GL}(2, Z)$. Over the complex field C, $\varrho(g)$ is similar to exactly one of the following matrices:

(i) $$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \quad \text{for some } \lambda \in C;$$

(ii) $$\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad \text{for some } \lambda \in C;$$

(iii) $$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \quad \text{for some } \lambda, \mu \in C, \text{ with } \lambda \neq \mu.$$

If J is any one of these matrices, then $\det J = \pm 1$ and $\operatorname{tr} J \in Z$, so that $\lambda = \pm 1$ in cases (i) and (ii). Since $\varrho(g)$ generates an infinite cyclic group in $\mathrm{GL}(2, Z)$, case (i) cannot occur. Suppose $\varrho(g)$ is similar to a matrix of type (ii). Then there exists a matrix U with integer coefficients and nonzero determinant such that $\varrho(g)^U = U^{-1} \varrho(g) U$ is a matrix of that type. Now

$\varrho(g')^U$ commutes with $\varrho(g)^U$, and $\det\varrho(g')^U = \pm 1$ and $\operatorname{tr}\varrho(g')^U \in Z$. Therefore,

$$\varrho(g')^U = \begin{pmatrix} \varepsilon & \gamma \\ 0 & \varepsilon \end{pmatrix},$$

where $\varepsilon = \pm 1$ and γ is a rational number, which implies that ϱ is not injective. Hence there exists $V \in \mathrm{GL}(2, C)$ such that $D = \varrho(g)^V$ is a matrix of type (iii), and an analogous reasoning shows that $D' = \varrho(g')^V$ is of the same type. If

$$\varrho(g) = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \quad \text{and} \quad \varrho(g') = \begin{pmatrix} p' & q' \\ r' & s' \end{pmatrix},$$

this implies that $r \neq 0$ and $r' \neq 0$.

Now set $D = \mathrm{diag}(\lambda, \mu)$ and $D' = \mathrm{diag}(\lambda', \mu')$. Since $\lambda\mu = \pm 1$ and $\lambda + \mu = n \in Z$, λ and μ are roots of $X^2 - nX \pm 1 = 0$. If we set $d = n^2 \mp 4$, it follows that λ and μ are units of the field $Q(\sqrt{d})$, where Q is the rational field. Analogously, from $\lambda'\mu' = \pm 1$ and $\lambda' + \mu' = n' \in Z$ we see that λ' and μ' are units of $Q(\sqrt{d'})$, where $d' = n'^2 \mp 4$. By our Lemma, $Q(\sqrt{d}) = Q(\sqrt{d'})$. Now the mapping $\mathrm{diag}(v, \pm v^{-1}) \mapsto (v, \pm 1)$ is an isomorphism of the group generated by D and D' onto a subgroup of $U(d) \oplus (Z/2Z)$, where $U(d)$ is the group of units of $Q(\sqrt{d})$. But $U(d)$ is either finite or isomorphic to $Z \oplus (Z/2Z)$ (cf., e.g., [3], p. 76); hence the subgroup of $\mathrm{GL}(2, Z)$ generated by $\varrho(g)$ and $\varrho(g')$ cannot be isomorphic to $Z \oplus Z$.

REFERENCES

[1] L. Auslander, *On a problem of Philip Hall*, Ann. of Math. (2) 86 (1967), pp. 112–116.

[2] D. J. S. Robinson, *Finiteness Conditions and Generalized Soluble Groups*, Parts 1–2, Ergeb. Math. Grenzgeb. 62–63, Springer-Verlag, Berlin–Heidelberg–New York 1972.

[3] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris 1967.

[4] R. G. Swan, *Representations of polycyclic groups*, Proc. Amer. Math. Soc. 18 (1967), pp. 573–574.

IMECC, UNICAMP
CAMPINAS (SÃO PAULO)

Reçu par la Rédaction le 15.5.1983