BULL. AUSTRAL. MATH. SOC. 20H05
VOL. 13 (1975), 1-12.

Presentations of some classical groups

M.J. Wicks

The groups considered are $\Lambda = GL(2, Z)$, $\Pi = SL(2, Z)$ and $\Theta = PSL(2, Z)$. A presentation of Λ is obtained for which the word problem can be solved by a simple intrinsic algorithm. The presentation is modified to display other features of Λ , and to obtain related presentations of Π and Θ . There is an algorithm which solves the conjugacy problem of Λ .

The groups of the title share a common ancestry which relates them to the (continuous) linear groups. They can be made to act as "motions", in the plane or complex sphere, and this action can be analysed in a transparently effective way. A resort to combinatorial methods (to solve the word problem, for example) may thus be avoided. It is not surprising, and especially since the groups have great importance in a variety of analytic contexts, that their presentations have received little more than passing attention. There is a brief systematic account in [2], §7.2.

There is an alternative heredity, from an ancestor that acts in a much more complicated way. We refer to the automorphism group of a free group (or rank two) of which Λ is a homomorphic image. A presentation which derives from this context is implicit in [4]. The complete details are given in the next section, together with a careful justification.

We then use Tietze transformations to get alternative presentations of Λ . These transformations allow:

the elimination of a defining relation which is a consequence of

---

Received 25 February 1975.

https://doi.org/10.1017/S0004972700024205 Published online by Cambridge University Press

others;

the elimination of a generator which can be expressed in terms of other generators (with some consequential changes in the defining relations);

the inverse of these, which introduce additional defining relations and generators, respectively.

Presentations of Π and Θ result in a direct way, and these in turn may be further modified.

The conjugacy problem of Λ, which could be formulated as the linear problem of unimodular similarity (for 2×2 unimodular matrices), is solved group-theoretically in the final section. The finiteness of the "class number" is an easy consequence of the solution. An illustration of this interplay, at a much deeper level, between problems involving free groups and diophantine questions, is to be found in [1].

1. A presentation of Λ

We take Λ as the concrete group of 2×2 unimodular matrices and assume, as we may, that Λ is generated by $\mathbf{A}$, the 5-tuple whose components (in order) are

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

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

(By the usual abuse of language, we refer to $\mathbf{A}$ as a generating *set* of Λ.)

We let Λ^* be the abstract group with generating set $\mathbf{a} = (a, b, r, s, t)$ and the following defining relations

$$r^2 = s^2 = t^2 = 1, \quad rs = sr, \quad rt = ts,$$

$$ra = a^{-1}r, \quad sa = a^{-1}s, \quad rb = b^{-1}r, \quad sb = b^{-1}s, \quad ta = bt,$$

$$ab^{-1} = btr, \quad a^{-1}b = b^{-1}ts, \quad ba^{-1} = ats, \quad b^{-1}a = a^{-1}tr.$$

There is a great deal of redundancy. However, the aim is to

https://doi.org/10.1017/S0004972700024205 Published online by Cambridge University Press

facilitate computation and the superfluous relations, in the form displayed, should further this objective. The first step towards showing that Λ and Λ^* are isomorphic will be to establish a normal form for the elements of Λ^* (considered as words on $\mathfrak{a}$).

Let $\Delta = \text{gp}(r, s, t)$, the subgroup of Λ^* with the indicated generating set, and note that Δ is a dihedral group of order 8 . The defining relations show that for any w in $\text{gp}(a, b)$ and d in Δ there is w' in $\text{gp}(a, b)$ such that $dw = w'd$. It follows that for any g in Λ^* there is w in $\text{gp}(a, b)$ and d in Δ such that $g = wd$. Further reduction is possible.

We let the *a-length* of g , denoted by $|g|$, be the number of occurrences of a^ε and b^ε , $\varepsilon = \pm 1$, in g . It was implicit above that $|g| = |w|$. The a-length of w may be reduced in one of two ways: by *cancellation*, which removes a trivial part such as $a^{-1}a$; or by *reduction*, which uses a defining relation to replace a part such as ab^{-1} by btr .

Iteration of the two processes - moving elements of Δ rightwards, and decreasing a-length by cancellation or reduction - leads to a u in $\text{gp}(a, b)$ and d in Δ such that $g = ud$ and u has the shortest possible a-length. It is clear that u is freely reduced; but more than that, u is in one of the *subsemigroups* $\Sigma = \text{sgp}(a, b)$ or $\Sigma' = \text{sgp}\left(a^{-1}, b^{-1}\right)$. We say that ud is in *normal form.* (Uniqueness will be shown below.)

It will help to fix ideas in the subsequent argument if we introduce a free group F freely generated by a 5-tuple $\mathfrak{X}$. The natural mappings of $\mathfrak{X}$ onto $\mathfrak{A}$ and $\mathfrak{a}$, respectively, extend to homomorphisms μ and ν of F onto Λ and Λ^* , respectively. Direct calculation shows that each relator of Λ^* , that is, each member of $\ker(\nu)$, is taken by μ into I , the identity matrix. Hence, $\ker(\nu)$ is contained in $\ker(\mu)$.

We now take an arbitrary g_0 in $\ker(\mu)$ and let g be its image under ν . We suppose, without loss of generality, that $g = ud$, where ud is in normal form and u is in Σ . Then u, d are (canonical) images of u_0, d_0 in F and there is an n_0 in $\ker(\nu)$ such that

$g_0 = u_0 d_0 n_0$. Since g_0 and n_0 are both in $\ker(\mu)$, it follows that $u_0 d_0$ is also. Hence, if U, D are the images of u_0, d_0 under μ , we must have $UD = I$.

Consider now any U which corresponds in the obvious way to a u in Σ . Then U is a product of non-negative powers of A and B . An easy induction proves that the elements of (the matrix) U are non-negative, and that the greatest of them is at least $|u|$. For any D , corresponding to an element of Δ , the absolute values of the elements of UD are simply the elements of U in a (possibly) different arrangement.

Return now to the case where U, D are the images of u_0, d_0 , respectively. It follows that $|u| \leq 1$ and inspection shows that $U = D = I$. Hence u_0 and d_0 are trivial and g_0 is in $\ker(\nu)$. This completes the proof that Λ and Λ^* are isomorphic. Note that we have also shown that if ud is in normal form and $ud = 1$, then both u and d are trivial.

The isomorphism allows us to identify corresponding elements of Λ and Λ^* , and to dispense with the distinctive notation. We shall retain the combinatorial point of view, but matrix considerations will be used where convenient. We conclude this section by showing that the normal form is unique.

Suppose then that u, u', d are such that $ud = u'$, where u is in Σ and d in Δ . (There is no essential restriction in this formulation.) Suppose u' is in Σ' and let $u'' = (u')^{-1}$. Then $u''ud$ is in normal form and trivial, so u, u' , and d must be trivial.

Now let u' be in Σ and assume that u and u' are not identical. With a different notation, this reduces to the case in which there are u_1 and u_2 in Σ such that $au_1d = bu_2$. Since $\det(au_1) = \det(bu_2) = 1$, we must have $\det(d) = 1$ and d cannot be t . If $d \neq 1$, at least one element of au_1d would be negative. This is impossible, so $d = 1$. We would then have

$$1 = u_1^{-1}a^{-1}bu_2 = u_1^{-1}b^{-1}tsu_2 = u_1^{-1}b^{-1}u_2'ts ,$$

https://doi.org/10.1017/S0004972700024205 Published online by Cambridge University Press

where u_2' is in Σ' , and hence, the last element is in normal form. This is impossible and there are no such u_1, u_2 .

2. Derived presentations

The first modification will be to a presentation of greater formal simplicity. It is easily seen that $rb = b^{-1}r$ and $sb = b^{-1}s$ can be eliminated. The same is true of the last three defining relations since each may be obtained as a consequence (by conjugation) of $ab^{-1} = btr$. Then $s = trt$, $b = tat$ may be used to eliminate s, b and the defining relations which remain become

$$r^2 = (trt)^2 = t^2 = 1 \ , \quad (tr)^4 = 1 \ ,$$

$$ra = a^{-1}r \ , \quad trta = a^{-1}trt \ , \quad ata^{-1}t = tar \ .$$

The relation $(trt)^2 = 1$ may be eliminated, while the last relation in the form $r = a^{-1}tata^{-1}t$ eliminates r . The relations $ra = a^{-1}r$ and $trta = a^{-1}trt$ are easily seen to be consequences of this new form for r , and the fact that r is an involution. The final presentation, in more traditional form with relators in place of defining relations, is

$$\langle a, t;\ t^2,\ \left(ata^{-1}tat\right)^2,\ \left(ata^{-1}ta\right)^4\rangle \ .$$

While we have not been able to show that this is irreducible, it seems unlikely that Λ is a two-relator group. In view of the calculations which follow, it is somewhat unexpected that the prime 3 does not appear as an exponent, but it may be noted that the second relator is of length 12 .

Another way of simplifying the original presentation is prompted by the fact that there are non-trivial involutions (that is, ones which are not euclidean reflections). We introduce $q = ar$ as a new generator. This allows a to be eliminated with r retained. The defining relations above, for the generating set (a, r, t) , then become

$$q^2 = r^2 = t^2 = (tr)^4 = 1 \ ,$$

$$q(tr)^2 = (tr)^2q \ , \quad qrtrqt = tq \ .$$

https://doi.org/10.1017/S0004972700024205 Published online by Cambridge University Press

The last relation has the consequence $(qt)^3 = (rt)^2$, so $(rt)^2$ is in the centre. Then the penultimate defining relation may be eliminated. If the presentation (with a superfluous relation) is taken in the form

$$q^2 = r^2 = t^2 = (tr)^4 = (qt)^6 = 1 , \quad (qt)^3 = (rt)^2 ,$$

we see Λ as the homomorphic image of a Coxeter group. There is an alternative structure.

We start with dihedral groups of orders 8 and 12 , respectively, and presentations

$$\langle r, t; r^2, t^2, (rt)^4\rangle , \quad \langle q, k; q^2, k^2, (qk)^6\rangle .$$

The subgroups $\mathrm{gp}\left(t, (rt)^2\right)$ and $\mathrm{gp}\left(k, (qk)^3\right)$ are each four-groups, so we may form the free product of the dihedral groups amalgamating these two subgroups with the obvious isomorphism. The result is Λ .

3. Presentations of Π and Θ

The group Π is the subgroup of Λ comprised of proper motions; that is, all those g for which $\det(g) = 1$. For an element ud in normal form the condition is equivalent to $\det(d) = 1$, and hence, to the fact that d is a power of tr . If we let $p = tr$, the set of elements up^m , where u is in Σ or Σ' and $0 \le m < 4$, is a normal form for Π .

Consider now the abstract group Π^* with generating set (a, b, p) and defining relations

$$p^4 = 1 , \quad pa = b^{-1}p , \quad pb = a^{-1}p , \quad ab^{-1} = bp .$$

It may be verified directly that the defining relations of Π^* become relations of Π under the identity mapping of the generators. It is also clear that the defining relations show that every element of Π^* is equal to an element in the normal form described above. An argument similar to that of Section 1 proves that Π and Π^* are isomorphic. The distinctive notation now lapses.

The relation $b = p^3a^{-1}p$ allows b to be eliminated. After some further manipulation we obtain the following defining relations

$$p^4 = 1 \ , \quad ap^2 = p^2a \ , \quad apa = pa^{-1}p \ ,$$

for the generating set (a, p) . A normal form for this presentation is similar to the earlier one, but u is now a member of one of $\text{sgp}(a^{\varepsilon}, pa^{-\varepsilon}p)$, $\varepsilon = \pm 1$.

It may be noted that the final defining relation has the more familiar form $(ap)^3 = 1$. There is a shortage of involutions in Π , but the introduction of $c = ap$ allows a to be eliminated and the defining relations become

$$c^3 = p^4 = 1 \ , \quad cp^2 = p^2c \ .$$

One way of seeing Π as a two-relator group (with the prime 3 concealed) is to use the relation $p = b^{-1}ab^{-1}$ to eliminate p , and to adopt the consequence $b^{-1}ab^{-1} = ab^{-1}a$ as a defining relation. This yields the formally simple presentation

$$\langle a, b; \ aba^{-1}bab^{-1}, \ (ab^{-1}a)^4 \rangle \ .$$

There is a rather full discussion of Θ in [3] so we may deal with it here in summary fashion. It is only necessary to remark that presentations can be obtained from those for Π by the addition of the relation $p^2 = 1$, or an equivalent.

4. The conjugacy problem

The algorithm which solves the word problem of Λ (in the original presentation) can be extended to provide a solution of the conjugacy problem. It seems likely that there will be similar solutions for the other two groups, but we do not consider this in detail.

We need a more detailed syntactic classification of the elements of Λ . As a start, we let Σ_0 be the set of non-trivial elements of Σ ; so that Σ_0 is a free semigroup without identity. The discussion will be easier to follow if we use "$\equiv$" to denote the relation of equality in the semigroup. We let Γ be the centre of Δ - its only non-trivial member is rs - and Φ be the four-group composed of Γ and the coset $t\Gamma$.

https://doi.org/10.1017/S0004972700024205 Published online by Cambridge University Press

Let g be a given element of Λ and let ud, in normal form, be an element in the conjugacy class of g which is of shortest a-length. Conjugation by an involution allows us to assume that u, if it is not 1, is in Σ_0. A further conjugation by t, if necessary, ensures that the initial letter of u is a.

If $|u| > 1$, the length condition entails that d is in Φ. For suppose not and let $u \equiv au_0cd$, where c is a or b. There will be a', one of a^{-1} or b^{-1}, such that $da = a'd$. Then g is a conjugate of $u_0ca'd$, and this goes either to u_0d by cancellation or, in an obvious notation, to $u_0c'd'$ by reduction. In either case, a shorter conjugate of g would be obtained. (Note that though we have not described an explicit algorithm for the calculation of ud for an arbitrary word g, an appropriate procedure is easy to formulate.)

The cases for which $|u| \leq 1$ may be settled by inspection. If $u \equiv a$ and d is in Φ, we may include ud in the previous case. Every member of $\Sigma_0\Phi$ is of infinite order, while the ud which are left are not. Thus, atr and ats are of orders 3 and 6, respectively, and are certainly not conjugate. For the involution ar we have

$$sb^{-1}arbs = sb^{-1}ab^{-1}rs = sb^{-1}btr^2s = trs .$$

Similarly, it may be shown that as is a conjugate of t.

The cases where $u \equiv 1$ remain. Of these, tr and its conjugate ts are the only ones of order 4. Then rs is in Π, while t, r and its conjugate s are not. We can illustrate the linear treatment by showing that t and r are not conjugate.

Let the numbers m, n, x, y be such that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} m & n \\ x & y \end{pmatrix} = \begin{pmatrix} m & n \\ x & y \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} .$$

The fact that t and r have the same trace and determinant ensures that the resulting system of equations simplifies to just two; namely, $x = -m$ and $y = n$. The condition that the conjugating matrix is unimodular leads to the contradictory result that the numbers are integers for which

$2mn = \pm 1$.

We thus have a set F of exceptional representatives (for conjugacy) consisting of 1, rs, tr, atr, ats, t , and r . An element of Λ of finite order is conjugate to a unique member of F . The first five of these are in Π and the last two are not.

A more detailed analysis of conjugation allows us to restrict the representatives of infinite order still more. Some further notation is useful - essentially, to indicate conjugation by elements of Δ . Thus, for any u in Σ_0 and d in Δ there is u^* such that $ud = du^*$ and $|u| = |u^*|$. Of course, it is implied that u^* is in either Σ or Σ' and by taking account of d we could specify u^* more precisely in terms of u . (For example, if u is $u(a, b)$ and $d = t$, then $u^* \equiv u(b, a)$.) However, the reader will easily supply the details without a more refined notation. We use the same device in relations such as $du = u^*d$.

Let $u_i d_i$, $i = 1, 2$, be a pair of conjugate elements in $\Sigma_0\Phi$. Then there will be an element vd such that $u_1 d_1 vd = vdu_2 d_2$. We show first that d is not in Φr .

Suppose d were in Φr and $u_1 v^* d_1 d = vu_2^* dd_2$, where u_2^* is in Σ' . According as v is in Σ or Σ' , the left or the right side of the relation is (essentially) in normal form. It is enough to consider the first alternative as both cases are similar. Thus v is in Σ and since u_2^* is not trivial, v cannot be trivial. If vu_2^* were to go to normal form by cancellations only, then u_2^* would be completely cancelled by a part of v . Length considerations show that this is impossible, since $u_1 v^*$ is in normal form. On the other hand, a reduction would produce d' in Φr and when this had been moved (fully) to the right, the result would be in normal form. But then the two sides of the relation that has been obtained would be "identical", with $d'dd_2$ in Φ and $d_1 d$ not. This contradiction completes the proof that d is not in Φr .

With d in Φ it is sufficient to consider the case in which v is in Σ . For if v is in Σ' , then v^{-1} is in Σ and so is the v^* for

https://doi.org/10.1017/S0004972700024205 Published online by Cambridge University Press

which $dv^{-1} = v^*d$. Then the original relation is equivalent to one of the same form in which v is replaced by v^* and u_1, u_2 are interchanged.

With u_i, v all in Σ and d_i, d all in Φ , the original relation goes to $u_1v^*d_1d = vu_2^*dd_2$, where both sides are in normal form (modulo a gloss for the elements of Δ). It follows that $d_1d = dd_2$, and since Φ is the four-group, that $d_1 = d_2$. We also have $u_1v^* \equiv vu_2^*$. The consequences of this identity depend on whether d_1 is in Γ or $t\Gamma$ and are best considered separately. Note that corresponding to the two alternatives we have $v^* \equiv v$ or $v^* = tvt$, respectively.

LEMMA 1. *Let* u, w *be in* Σ_0 . *If there is* v *in* Σ *and* d *in* Φ *such that* $uv \equiv vw^*$ *, where* $w^* = dwd$ *, then* w *is a cycle of* u *or* tut *(as* d *is in* Γ *or* $t\Gamma$ *, respectively).*

Proof. If $|v| \leq |u|$, there must be u' and w' such that $u \equiv vu'$ and $w^* \equiv w'v$. Then, substituting in the original identity, we have $u' \equiv w'$ and the result follows.

If $|v| > |u|$, there must be v' and v'' such that $v \equiv uv' \equiv v''w^*$. It follows as before that $v' \equiv v''$. Since u is in Σ_0 , $|v'| < |v|$. The relation above satisfies the hypothesis of the lemma with v replaced by v' . Hence, we are either in the first case, or we may complete the proof by induction.

LEMMA 2. *Let* u, w *be in* Σ_0 . *If there is* v *in* Σ *and* d *in* Φ *such that* $uv^* \equiv vw^*$ *, where* $v^* = tvt$ *and* $w^* = dwd$ *, then there exist* u_1, u_2 *in* Σ *such that* $u \equiv u_1u_2$ *and* w *is a cycle of either* $u_1u_2^*$ *or* $u_1^*u_2$ *, where* $u_i^* = tu_it$ *,* $i = 1, 2$.

Proof. If $|v| \leq |u|$, there will be u' such that $u \equiv vu'$ and $w^* \equiv u'v^*$. The result follows.

If $|v| > |u|$, there is v' such that $v \equiv uv'$ and $v^* \equiv v'w^*$. The hypothesis of the lemma is satisfied if v^* is replaced by the shorter v' and d by td . The proof is completed as before.

Let u_id , $i = 1, 2$, be a pair of conjugates with u_i in Σ_0 . If

https://doi.org/10.1017/S0004972700024205 Published online by Cambridge University Press

d is in Γ, Lemma 1 applies. The initial letter of u_i is a and, since a final a can be cycled past d to the initial position, there is no loss of generality in assuming that u_i is either a power of a or its final letter is b. In the case that u_1 is a power of a, the second case of the lemma cannot occur, so that $u_2 \equiv u_1$.

If d is in $t\Gamma$, Lemma 2 applies. We may now assume that the final letter of u_i is a since $bd = da$. It is again true that if u_1 is a power of a, then $u_2 \equiv u_1$.

In terms of the following subsemigroups of Σ_0,

$$A = \text{sgp}(a) \ , \quad B = \text{sgp}(b) \ , \quad C = \bigcup_n (AB)^n \ ,$$

the detailed result may be stated as

THEOREM. *Any member of* Λ *is the conjugate of a member of* F, $A\Phi$, $C\Gamma$ *or* $CA(t\Gamma)$. *The representative is unique in the first two cases. Otherwise, if a pair of representatives* $u_i d_i$, $i = 1, 2$, *are conjugates, then* $d_1 = d_2$; *if* d_1 *is in* Γ, *then* u_2 *is a cycle of either* $u_1(a, b)$ *or* $u_1(b, a)$; *if* d_1 *is in* $t\Gamma$, *then there exist* u, v *such that* $u_1 \equiv uv$ *and* u_2 *is a cycle of either* $u(a, b)v(b, a)$ *or* $u(b, a)v(a, b)$.

Some further comments may be of interest. The elements of $A\Gamma$ are all parabolic and the theorem shows that any parabolic element of Λ is a conjugate of rs or a unique member of $A\Gamma$. Representatives of any arbitrary trace can be found among t and the members of $A(t\Gamma)$.

The result can be interpreted in matrix terms. A representative ud in $\Sigma_0\Phi$ is such that the elements of the matrix ud are of constant sign; for example, they are all non-negative if ud is in either Σ_0 or $\Sigma_0 t$. This fact has the consequence that there are only a finite number of representatives with a given trace. More generally, there are only a finite number of different conjugates in the set of all (unimodular) matrices with a specified characteristic polynomial. It would be interesting to know whether similar methods could be used for the set of non-singular matrices with integral elements. (It would be necessary to obtain a presentation for the corresponding (cancellation) semigroup as a first step.)

Matrices in particular subsets of $\Sigma_0\Phi$ are subject to further arithmetic restrictions. For example, if $(m\ n \mid x\ y)$ is in C, then not only is $m \le n$, $x \le y$, but also $m \le x$ and $n \le y$. In the same vein, the trace $m + y$ can be considered as a function of the sequences of integers which appear as exponents of the powers of a and b when the matrix is expressed in normal form. The conjugate cycles of a representative then correspond to certain symmetries of the trace function. These symmetries are, presumably, inherent in the problem, or in this approach to it. Nevertheless, a closer analysis of this situation might lead to more precise estimates of the class number.

We conclude by drawing attention to the intrusion of semigroups into the characterisation of the normal form and of representatives. There are numerous examples in the literature where "positive words" have featured in a combinatorial investigation, albeit in a rather *ad hoc* way. However, a particular case, which may be germane to the present observation, is furnished by Garside's solution of the conjugacy problem for braid groups.

References

[1] Harvey Cohn, "Markoff forms and primitive words", *Math. Ann.* 196 (1972), 8-22.

[2] H.S.M. Coxeter and W.O.J. Moser, *Generators and relations for discrete groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete, 14. Springer-Verlag, Berlin, Göttingen, Heidelberg, 1957; 3rd ed. 1972).

[3] Morris Newman, *Integral matrices* (Pure and Applied Mathematics, 45. Academic Press, New York and London, 1972).

[4] M.J. Wicks, "A general solution of binary homogeneous equations over free groups", *Pacific J. Math.* 41 (1972), 543-561.

Department of Mathematics,
University of Singapore,
Singapore.