A NOTE ON REGULAR COVERINGS OF CLOSED ORIENTABLE SURFACES

by JENS MENNICKE

(Received 14 September, 1960)

1. The object of this note is to study the regular coverings of the closed orientable surface of genus 2.

Let the closed orientable surface F_h of genus h be a covering of F_2 and let $\hat{\mathfrak{F}}$ and $\mathfrak{F}$ be the fundamental groups respectively. Then $\hat{\mathfrak{F}}$ is a subgroup of $\mathfrak{F}$ of index $n = h-1$. A covering is called regular if $\hat{\mathfrak{F}}$ is normal in $\mathfrak{F}$.

Conversely, let $\hat{\mathfrak{F}}$ be a normal subgroup of $\mathfrak{F}$ of finite index. Then there is a uniquely determined regular covering F_h such that $\hat{\mathfrak{F}}$ is the fundamental group of F_h. The covering F_h is an orientable surface. Since the index n of $\hat{\mathfrak{F}}$ in $\mathfrak{F}$ is supposed to be finite, F_h is closed, and its genus is given by $n = h-1$.

The fundamental group $\mathfrak{F}$ can be defined by

$$\mathfrak{F} = \{a, b, c, d \mid a\, b\, c\, d\, a^{-1}b^{-1}c^{-1}d^{-1} = 1\}.$$

If we add the relations $a = b = c = d$, then all relations become trivial, and we obtain the free cyclic group as a factor group of $\hat{\mathfrak{F}}$. Thus $\mathfrak{F}$ possesses finite factor groups of arbitrary order. In terms of geometry, every closed orientable surface of genus $h \geqq 2$ does occur as a regular covering of the surface of genus 2. Every fundamental group $\hat{\mathfrak{F}}$ is a normal subgroup of $\mathfrak{F}$.

This simple remark may justify a study of the regular coverings of F_2. In the present paper we shall draw attention to the corresponding finite factor groups of $\mathfrak{F}$.

For a finite group which can occur as a factor group of $\mathfrak{F}$ the minimal number e of generators clearly cannot exceed 4. For $e = 2$, every finite group occurs as a factor group of $\mathfrak{F}$. For $e = 3$, there are necessary conditions. We shall give the following. Consider a finite group $\mathfrak{G}$, its lower central series $\mathfrak{G}_0 = \mathfrak{G}$, $\mathfrak{G}_i = (\mathfrak{G}, \mathfrak{G}_{i-1})$ and the corresponding factors $\mathfrak{C}_i = \mathfrak{G}_{i-1}/\mathfrak{G}_i$. A necessary condition that a finite group $\mathfrak{G}$ with minimally 3 generators can occur as a factor group of $\mathfrak{F}$ is that the second factor $\mathfrak{C}_2$ of the lower central series can be generated by 2 elements. (In general, this factor would have 3 generators.)

For $e = 4$, there is an analogous condition.

In a second part, we shall continue some considerations which we have begun in the joint paper [2]. Consider the quaternion algebra $\mathfrak{A}$ over the ring Γ of rational integers with the norm

$$N = x^2 + y^2 - 3u^2 - 3v^2.$$

This algebra consists of all matrices

$$\begin{pmatrix} x+iy & 3u+3iv \\ u-iv & x-iy \end{pmatrix}.$$

Consider the group $\mathfrak{U}$ of $+1$-units (with norm $+1$) of $\mathfrak{A}$ and the centre $\mathfrak{Z} = (1, Z)$,

$$Z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We shall prove that the factor group of $\mathfrak{U}$ with respect to the centre $\mathfrak{Z}$ contains $\mathfrak{F}$ as a subgroup of index 2.

$\mathfrak{A}$ has as a homomorphic image the algebra $\mathfrak{A}_m$ with the same norm over the residue-class ring Γ_m modulo an arbitrary integer m. The group of $+1$-units of $\mathfrak{A}_m$ contains as a subgroup of index 1 or 2 the homomorphic image of the group of $+1$-units of $\mathfrak{A}$. Thus this homomorphism yields a large class of finite factor groups of $\mathfrak{F}$. We shall investigate the structure of these factor groups.

2. In this section we shall prove the following theorem.

THEOREM 1. *A finite factor group of the fundamental group $\mathfrak{F}$ cannot have a minimal number e of generators exceeding* 4.

For $e = 2$, every finite 2-generated group occurs as a factor group of $\mathfrak{F}$.

For $e = 3$ or 4, a necessary condition for a finite group $\mathfrak{G}$ to be a factor group of $\mathfrak{F}$ is that the second factor of the lower central series is at most 2- or 5-generated respectively.

Proof. It is not new that $\mathfrak{F}$ possesses a free factor group of rank 2. Cf. [9].

Add the relations $a = d$, $b = c$. Then the relation $abcda^{-1}b^{-1}c^{-1}d^{-1} = 1$ becomes trivial, and we obtain as a factor group the free group of rank 2. This proves that every 2-generated finite group is a factor group of $\mathfrak{F}$.

The non-trivial part of Theorem 1 is the necessary condition for 3-generated groups.

For convenience, we recall the definition of the lower central series of a group $\mathfrak{G}$.

$$\mathfrak{G}_0 \supseteq \mathfrak{G}_1 \supseteq \mathfrak{G}_2 \ldots \supseteq \mathfrak{G}_c,$$

$$\mathfrak{G}_0 = \mathfrak{G},\ \mathfrak{G}_i = (\mathfrak{G}, \mathfrak{G}_{i-1}) = \{x^{-1}y^{-1}xy \mid x \in \mathfrak{G},\ y \in \mathfrak{G}_{i-1}\}.$$

The groups $\mathfrak{G}_i$ are all characteristic in $\mathfrak{G}$, and the factors $\mathfrak{C}_i = \mathfrak{G}_{i-1}/\mathfrak{G}_i$ are, of course, abelian groups.

For the proof of the condition for 3-generated groups, we need a lemma.

LEMMA 1. *Let $\mathfrak{G}$ be a finite 3-generated group such that the second factor $\mathfrak{C}_2$ of the lower central series has minimally 3 generators. Then $\mathfrak{G}$ has the following factor group $\overline{\mathfrak{G}}$:*

$$\left.\begin{array}{l} u^m, v^n, w^l \in (\overline{\mathfrak{G}}, \overline{\mathfrak{G}}), \\ k_1 = u^{-1}v^{-1}uv = (u, v),\ k_2 = (v, w),\ k_3 = (w, u), \\ k_1^p = k_2^p = k_3^p = 1, \\ k_1, k_2, k_3 \in Z(\overline{\mathfrak{G}}). \end{array}\right\} \qquad (\overline{\mathfrak{G}})$$

$Z(\overline{\mathfrak{G}})$ is the centre of $\overline{\mathfrak{G}}$, p is some prime, and m, n, l are integers such that $p \mid m, n, l$. The commutator subgroup of $\overline{\mathfrak{G}}$ lies in the centre and is elementary abelian of order p^3.

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

Proof of Lemma 1. Let u, v, w be generators of the factor group $\mathfrak{G}^* = \mathfrak{G}/\mathfrak{G}_2$. Assume that $\mathfrak{C}_1$ has 2 generators $r\mathfrak{G}_1$, $s\mathfrak{G}_1$. Then we have in $\mathfrak{G}^*$:

$$u = kr^{\alpha_1}s^{\beta_1},$$
$$v = k'r^{\alpha_2}s^{\beta_2},$$
$$w = k''r^{\alpha_3}s^{\beta_3},$$

where $k, k', k'' \in \mathfrak{G}_1/\mathfrak{G}_2$.

In $\mathfrak{G}^*$ the commutator subgroup lies in the centre. We can apply the commutator calculus given in [15], p. 80 ff. Applying this calculus, we deduce that

$$k_1 = (u, v) = (r, s)^{\alpha_1\beta_2 - \alpha_2\beta_1},$$
$$k_2 = (v, w) = (r, s)^{\alpha_2\beta_3 - \alpha_3\beta_2},$$
$$k_3 = (w, u) = (r, s)^{\alpha_3\beta_1 - \alpha_1\beta_3}.$$

The elements k_1, k_2, k_3 generate $\mathfrak{C}_2$. Our formulae show that $\mathfrak{C}_2$ is generated by (r, s), which contradicts our assumption that $\mathfrak{C}_2$ has minimally 3 generators. Hence $\mathfrak{C}_1$ cannot be generated by less than 3 elements.

For the following, we need some simple arguments of extension theory. Cf. [15], § 6 ff. and particularly § 8.

$\mathfrak{G}^*$ is a central extension of an abelian group with an abelian factor group. Thus $\mathfrak{G}^*$ can be defined as follows:

$$\left.\begin{aligned} &u^m, v^n, w^l \in (\mathfrak{G}^*, \mathfrak{G}^*), \\ &k_1^q = k_2^r = k_3^s = 1, \\ &k_1, k_2, k_3 \in Z(\mathfrak{G}^*). \end{aligned}\right\} \qquad (\mathfrak{G}^*)$$

The first relation determines the factor system of the extension, and the second and third relations say that the normal subgroup is abelian and that the extension is central, i.e. the automorphisms are trivial.

Since $\mathfrak{C}_1$ cannot be generated by less than 3 elements, we conclude that $(m, n, l) = d > 1$. From our assumption on $\mathfrak{C}_2$ we conclude that $(q, r, s) = d' > 1$. The formula $u^{-m}v^{-1}u^m v = (u, v)^m$ yields $q \mid m$; similarly $q \mid n$, $r \mid l, m$, $s \mid n, l$. Hence $d' \mid d$.

Now let p be a prime such that $p \mid d'$. Add the relations $k_1^p = k_2^p = k_3^p = 1$ to $(\mathfrak{G}^*)$. This yields the factor group $\overline{\mathfrak{G}}$ of $\mathfrak{G}^*$:

$$\left.\begin{aligned} &u^m, v^n, w^l \in (\overline{\mathfrak{G}}, \overline{\mathfrak{G}}), \\ &k_1^p = k_2^p = k_3^p = 1, \\ &k_1, k_2, k_3 \in Z(\overline{\mathfrak{G}}). \end{aligned}\right\} \qquad (\overline{\mathfrak{G}})$$

This is the factor group $\overline{\mathfrak{G}}$ required in Lemma 1.

We shall now prove that $\overline{\mathfrak{G}}$ cannot be a factor group of $\mathfrak{F}$. This will complete the proof of our necessary condition for finite 3-generated factor groups of $\mathfrak{F}$.

If there is a homomorphism of $\mathfrak{F}$ onto $\overline{\mathfrak{G}}$, then we can write

$$a \to a' = ku^{x_1}v^{y_1}w^{z_1},$$
$$b \to b' = k'u^{x_2}v^{y_2}w^{z_2},$$
$$c \to c' = k''u^{x_3}v^{y_3}w^{z_3},$$
$$d \to d' = k'''u^{x_4}v^{y_4}w^{z_4},$$

where $k, k', k'', k''' \in Z(\overline{\mathfrak{G}})$.

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

The group $\mathfrak{G}$ has an elementary abelian factor group of order p^3 which is defined by $u^p = v^p = w^p = 1$, $k_1 = k_2 = k_3 = 1$. The induced homomorphism of $\mathfrak{H}$ on this factor group of $\mathfrak{G}$ must be *onto*.

Reduce the elements x_i, y_i, z_i modulo p and take the matrix

$$A = (x_i \quad y_i \quad z_i) \qquad (i = 1, \ldots, 4).$$

Then the statement that the above homomorphism must be onto yields that the rank of A must be precisely 3.

The element $R' = a'b'c'd'a'^{-1}b'^{-1}c'^{-1}d'^{-1}$ lies in the commutator group of $\mathfrak{G}$; hence it can be expressed by means of k_1, k_2, k_3:

$$R' = k_1^{\alpha} k_2^{\beta} k_3^{\gamma}.$$

Since the commutator group of $\mathfrak{G}$ is elementary abelian of order p^3, the relation $R' = 1$ yields the equations

$$\alpha = \beta = \gamma = 0,$$

which hold in the prime field of characteristic p.

By means of the above mentioned commutator calculus, it is not too difficult to evaluate α, β, γ explicitly. We obtain:

$$\begin{aligned}
-y_1(x_2+x_3+x_4)-y_2(-x_1+x_3+x_4)+y_3(x_1+x_2-x_4)+y_4(x_1+x_2+x_3) &= 0,\\
-z_1(x_2+x_3+x_4)-z_2(-x_1+x_3+x_4)+z_3(x_1+x_2-x_4)+z_4(x_1+x_2+x_3) &= 0,\\
-z_1(y_2+y_3+y_4)-z_2(-y_1+y_3+y_4)+z_3(y_1+y_2-y_4)+z_4(y_1+y_2+y_3) &= 0.
\end{aligned}$$

We can pass from x_1, x_2, x_3, x_4 to $x_2+x_3+x_4$, $-x_1+x_3+x_4$, $x_1+x_2-x_4$, $x_1+x_2+x_3$ by means of a non-singular linear transformation. Hence we can assume that

$$x_2+x_3+x_4 = x \neq 0.$$

Then we have

$$\begin{aligned}
xy_1 &= -y_2(-x_1+x_3+x_4)+y_3(x_1+x_2-x_4)+y_4(x_1+x_2+x_3),\\
xz_1 &= -z_2(-x_1+x_3+x_4)+z_3(x_1+x_2-x_4)+z_4(x_1+x_2+x_3).
\end{aligned}$$

We substitute these terms for y_1, z_1 in the matrix A. After elementary transformations of A we obtain the matrix

$$A' = \begin{pmatrix} 0 & 0 & 0 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \\ x_4 & y_4 & z_4 \end{pmatrix}.$$

If we substitute y_1, z_1 in the third of the three above equations, then we obtain

$$x^{-1}(x_2y_3z_4+x_3y_4z_2+x_4y_2z_3-x_4y_3z_2-x_2y_4z_3-x_3y_2z_4) = 0.$$

The term in brackets is exactly the determinant of the last three rows of the matrix A'. Hence the matrices A and A' have a rank at most 2. This completes the proof of our necessary condition for 3-generated finite factor groups of $\mathfrak{H}$.

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

The condition for 4-generated factor groups is readily proven by the identity

$$abcda^{-1}b^{-1}c^{-1}d^{-1} = (a, d)(a, c)(a, b)(b, d)(b, c)(c, d),$$

which holds in the factor group $\mathfrak{H}/\mathfrak{H}_2$ of the lower central series.

This completes the proof of Theorem 1.

3. In this section, we shall continue some considerations which we have begun in [2]. Many of the subsequent ideas are due to a collaboration with P. Bergau.

We shall recall briefly some results from [2]. It is convenient to extend the fundamental group $\mathfrak{H}$ to a group $\mathfrak{P}$ as follows:

$$\left.\begin{aligned} &A^2 = B^2 = C^2 = D^2 = E^2 = F^2 = 1, \\ &ABCDEF = 1. \end{aligned}\right\} \qquad (\mathfrak{P})$$

$\mathfrak{H}$ is the subgroup of $\mathfrak{P}$ of index 2 which consists of all even products of generators.

The group $\mathfrak{P}$ can be represented as a tessellation group in the hyperbolic plane. Consider the tessellation $\{6, 4\}$ with regular hexagons such that 4 hexagons meet at each vertex. Consider the group of hyperbolic motions which is generated by the reflections in the vertices of this tessellation. This group is isomorphic with $\mathfrak{P}$. The generators A, B, C, D, E, F are the reflections in the vertices of a basic hexagon.

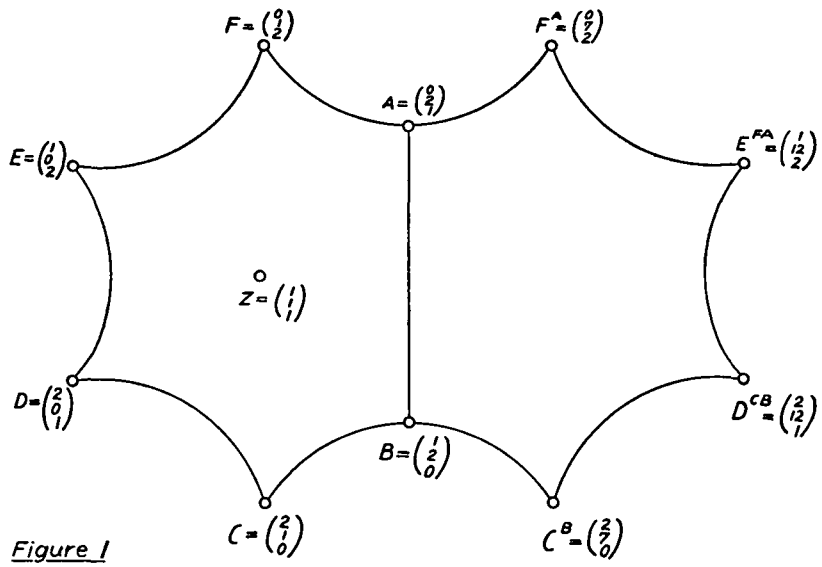

Figure 1

In [2] the hyperbolic plane was imbedded into the projective plane by means of the quadratic form

$$f(\mathfrak{x}, \mathfrak{x}) = -\tfrac{1}{3}(x^2+y^2+z^2)+\tfrac{4}{3}(xy+xz+yz), \qquad (1)$$

and integral coordinates were found for the vertices of the basic hexagon in such a way that all the vertices of the tessellation were shown to have integral coordinates which satisfy

$$f(\mathfrak{x}, \mathfrak{x}) = 1. \qquad (2)$$

(2) determines the homogeneous coordinates of the vertices up to a common factor ± 1.

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

It was stated without proof in [2] that all points with integral coordinates which satisfy (2) are vertices of the tessellation. Since this statement is essential for the subsequent considerations, we shall give a proof here.

The tessellation group $\mathfrak{P}$ has a fundamental domain consisting of the basic hexagon and an adjacent hexagon. All points of the hyperbolic plane are congruent to points in the fundamental domain by means of motions of $\mathfrak{P}$.

Suppose that there is a point P with integral coordinates satisfying (2) which is not a vertex of our tessellation. The motions of $\mathfrak{P}$ can be represented by orthogonal matrices with integral elements, so that they map onto itself the set of points with integral coordinates satisfying (2). Hence, there is no loss of generality in assuming that P lies in the fundamental domain.

The adjacent hexagon is obtained from the basic hexagon by the side-reflection σ with respect to the line (A, B) (fig. 1). We can write σ as an orthogonal matrix with integral elements:

$$\sigma = \begin{pmatrix} 1 & 0 & 0 \\ 4 & -1 & 4 \\ 0 & 0 & 1 \end{pmatrix},$$

which again maps onto itself the set of points with integral coordinates satisfying (2). Hence we can assume that P lies in the basic hexagon.

Let

$$\mathfrak{p} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

be the coordinates of P. The centre Z of the basic hexagon has the coordinates

$$\mathfrak{z} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

The hyperbolic cosine of the distance between two points with coordinates $\mathfrak{x}$, $\mathfrak{y}$ in the hyperbolic plane can be expressed by means of the quadratic form (1):

$$d = \frac{f(\mathfrak{x}, \mathfrak{y})}{\sqrt{\{f(\mathfrak{x}, \mathfrak{x})\}}\sqrt{\{f(\mathfrak{y}, \mathfrak{y})\}}}.$$

Cf. [11], p. 183 and [8]. For the points P, Z this expression reduces to

$$d = \frac{x+y+z}{\sqrt{3}}. \tag{3}$$

The hyperbolic cosine $d = \frac{1}{2}(e^x + e^{-x})$ is a monotonic function of the distance x.

The maximum of d in (3) in the basic hexagon is $d = \sqrt{3}$, which is attained if P is one of the vertices. The minimum of d is obviously $d = 1$. Hence we have the inequality

$$\sqrt{3} \leqq x+y+z \leqq 3. \tag{4}$$

We can write (2) in the form

$$-\tfrac{1}{3}(x+y+z)^2 + 2(xy+xz+yz) = 1. \tag{5}$$

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

We conclude that $\frac{1}{3}(x+y+z)^2$ must be an integer. From (4) we obtain

$$x+y+z = 3.$$

Eliminating x from (5) by means of the last equation, we obtain a diophantine equation in y, z:

$$(3-y-z)(y+z)+yz = 2.$$

One can readily verify that this equation has but a finite number of solutions which yield exactly the vertices of the basic hexagon. Hence there are no points with integral coordinates satisfying (2) which are not vertices of the tessellation.

For our purposes, it will be convenient to introduce another quadratic form instead of (1):

$$g = r^2-3s^2-3t^2. \tag{6}$$

The transformation from (1) to (6) is given by

$$\left.\begin{aligned} x &= 2r+3s-2t \\ y &= r-2t \\ z &= t \end{aligned}\right\}, \qquad \left.\begin{aligned} r &= y+2z \\ s &= \tfrac{1}{3}(x+y+z)-y-z \\ t &= z \end{aligned}\right\}.$$

In Fig. 2 we have given the new coordinates of the vertices of the basic hexagon. We represent the reflections in the vertices as orthogonal matrices:

$$\left.\begin{aligned} A &= \begin{pmatrix} 31 & 48 & -24 \\ -16 & -25 & 12 \\ 8 & 12 & -7 \end{pmatrix}, \quad B = \begin{pmatrix} 7 & 12 & 0 \\ -4 & -7 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \\ D &= \begin{pmatrix} 7 & 0 & -12 \\ 0 & -1 & 0 \\ 4 & 0 & -7 \end{pmatrix}, \quad E = \begin{pmatrix} 31 & 24 & -48 \\ -8 & -7 & 12 \\ 16 & 12 & -25 \end{pmatrix}, \quad F = \begin{pmatrix} 49 & 60 & -60 \\ -20 & -25 & 24 \\ 20 & 24 & -25 \end{pmatrix}. \end{aligned}\right\} \tag{7}$$

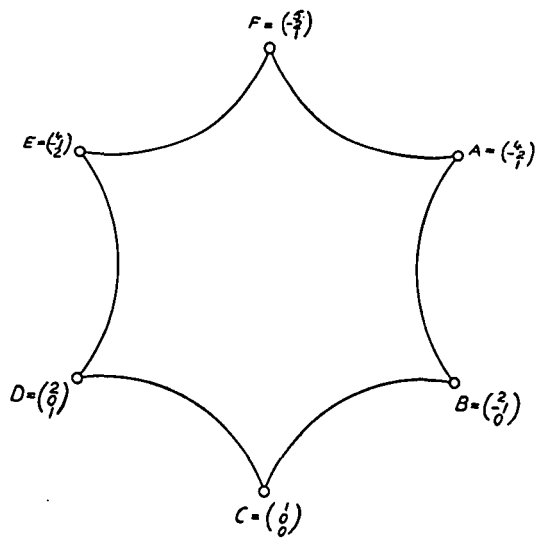

Figure 2

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

The full orthogonal group with respect to (6) over the ring of rational integers contains $\mathfrak{P}$ as a subgroup of index 12. The corresponding cosets are represented by the reflections in the mid-points of the sides of the basic hexagon, and by a rotation of 90° about each of the 6 vertices.

In the full orthogonal group, all vertices are congruent. It is not difficult to show that there are exactly 4 orthogonal matrices with integral elements which leave one vertex fixed. Hence the above enumeration of cosets of $\mathfrak{P}$ in the full orthogonal group is complete, and the index is exactly 12.

We shall now apply, in a slightly modified form, an argument of L. E. Dickson which he has given in his proof for the exceptional isomorphisms between certain orthogonal groups of rank 3 and linear homogeneous groups of rank 2 over Galois fields. Since Dickson's argument is given in detail in [7], § 178, p. 164 ff., it will be sufficient to state our result.

Let a, b, c, d be integers satisfying

$$a^2+b^2-3c^2-3d^2 = 1. \tag{8}$$

Then the orthogonal group of all matrices

$$X = \begin{pmatrix} a^2+b^2+3c^2+3d^2 & -6(ad-bc) & -6(ac+bd) \\ -2(ad+bc) & a^2-b^2-3c^2+3d^2 & 2(ab+3cd) \\ -2(ac-bd) & 2(-ab+3cd) & a^2-b^2+3c^2-3d^2 \end{pmatrix} \tag{9}$$

is isomorphic with the linear homogeneous group of all matrices

$$Y = \begin{pmatrix} a+bi & 3c+3di \\ c-di & a-bi \end{pmatrix}. \tag{10}$$

The adjective " homogeneous " indicates that a, b, c, d are determined up to a common factor ± 1. Clearly this does not affect the matrix X.

Not every element of the full orthogonal group can be represented in the form (9), e.g. the reflection in the mid-point of the segment (A, B), which is given by

$$\tau = \begin{pmatrix} 11 & 18 & -6 \\ -6 & -10 & 3 \\ 2 & 3 & -2 \end{pmatrix},$$

cannot be so represented. We must investigate which elements can be expressed in the form (9), and hence are mapped by the above isomorphism onto elements of the linear homogeneous group.

The matrices (7) can be expressed by (9), being the matrices of the set (9) corresponding to the following matrices of the set (10):

$$\left.\begin{array}{lll} A = \begin{pmatrix} 4i & 6+3i \\ 2-i & -4i \end{pmatrix}, & B = \begin{pmatrix} 2i & 3 \\ 1 & -2i \end{pmatrix}, & C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \\ D = \begin{pmatrix} 2i & 3i \\ -i & -2i \end{pmatrix}, & E = \begin{pmatrix} 4i & 3+6i \\ 1-2i & -4i \end{pmatrix}, & F = \begin{pmatrix} 5i & 6+6i \\ 2-2i & -5i \end{pmatrix}. \end{array}\right\} \tag{11}$$

Hence all elements of $\mathfrak{P}$ can be expressed by (9). An elementary calculation yields that the above mentioned 12 representatives of the cosets of $\mathfrak{P}$ in the full orthogonal group cannot be expressed by (9). Hence the subgroup of the full orthogonal group which is mapped onto the linear homogeneous group is exactly $\mathfrak{P}$.

Obviously (10) is a matrix representation of the quaternion algebra $\mathfrak{A}$ with the norm

$$N = a^2 + b^2 - 3c^2 - 3d^2 \tag{12}$$

over the ring of rational integers. Let $\mathfrak{U}$ be the group of $+1$-units of this algebra. Consider the element

$$Z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{and} \quad \mathfrak{Z} = (1, Z). \tag{13}$$

The group $\mathfrak{Z}$ lies in the centre of $\mathfrak{U}$, and one can easily verify that it is exactly the centre of $\mathfrak{U}$. Define

$$\mathfrak{U}^+ = \mathfrak{U}/\mathfrak{Z}. \tag{14}$$

Then we have:

THEOREM 2. *Consider the group $\mathfrak{U}$ of $+1$-units (with norm $+1$) of the quaternion algebra ithw the norm* (12) *over the ring of rational integers, and the factor group $\mathfrak{U}^+$ of $\mathfrak{U}$ modulo the centre. $\mathfrak{U}^+$ is isomorphic to $\mathfrak{P}$:*

$$\mathfrak{U}^+ \cong \mathfrak{P}. \tag{15}$$

This isomorphism is given by (11).

4. Let Γ be the ring of rational integers, Γ_m the residue-class ring modulo an arbitrary integer m, and $\mathfrak{A}_m$ the quaternion algebra over Γ_m with the norm (12). There is a natural homomorphism of $\mathfrak{A}$ onto $\mathfrak{A}_m$ which is induced by $\Gamma \to \Gamma_m$. The group of units of $\mathfrak{A}$ is mapped homomorphically into the group of units of $\mathfrak{A}_m$.

In this section, we shall investigate this homomorphism, which, by Theorem 2, induces a homomorphism of $\mathfrak{P}$ onto a finite factor group of $\mathfrak{P}$.

We shall first treat the case $(m, 6) = 1$.

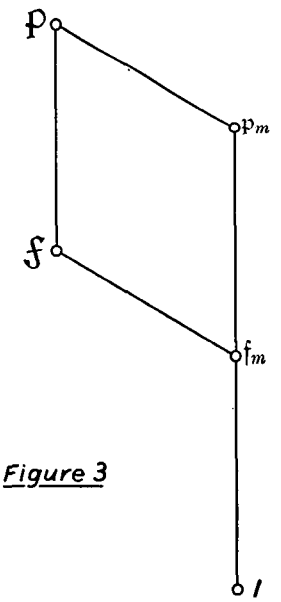

Figure 3

THEOREM 3. *Let $(m, 6) = 1$.*

(a) The group of $+1$-units of $\mathfrak{A}_m$ is isomorphic to the special linear group $SL(2, m)$.

(b) The group of $+1$-units of $\mathfrak{A}$ is mapped onto $SL(2, m)$.

(c) Define Z as in (13), *but over Γ_m, and $\mathfrak{Z} = (1, Z)$. The induced factor group of $\mathfrak{P}$ is isomorphic to $SL(2, m)/\mathfrak{Z}$.*

(d) Let $\mathfrak{p}_m$ be the normal subgroup consisting of those elements of $\mathfrak{P}$ which are congruent to 1 modulo m, and $\mathfrak{f}_m$ the corresponding subgroup of $\mathfrak{F}$. Then the induced homomorphism of $\mathfrak{F}$ is characterised by Fig. 3*:*

$$\mathfrak{P}/\mathfrak{p}_m \cong \mathfrak{F}/\mathfrak{f}_m \cong SL(2, m)/\mathfrak{Z}.$$

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

Proof. Consider the $+1$-units of $\mathfrak{A}_m$:

$$Y = \begin{pmatrix} a+bi & 3c+3di \\ c-di & a-bi \end{pmatrix} \quad \text{with} \quad a^2+b^2-3c^2-3d^2 \equiv 1 \pmod{m}, \tag{16}$$

and the elements of $SL(2, m)$:

$$\overline{Y} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{with} \quad \alpha\delta-\beta\gamma \equiv 1 \pmod{m}. \tag{17}$$

We shall try to establish the isomorphism between the group of $+1$-units of $\mathfrak{A}_m$ and $SL(2, m)$ as a linear relation $\phi(Y) = \overline{Y}$ between the coefficients of Y, $\overline{Y}$ respectively:

$$\begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} \equiv (\rho_{ij}) \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \pmod{m}. \tag{18}$$

In order to determine the coefficients ρ_{ij} of (18), put

$$\phi\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{19}$$

Moreover, the function ϕ must satisfy the condition

$$\phi(Y_1)\phi(Y_2) = \phi(Y_1\ Y_2). \tag{20}$$

(19) and (20) yield a certain system of equations for the coefficients ρ_{ij} which can be solved as follows:

$$\left.\begin{aligned} \alpha &\equiv\ \ a+\rho_{13}c+\rho_{14}d \\ \beta &\equiv -b-\rho_{14}c+\rho_{13}d \\ \gamma &\equiv\ \ b-\rho_{14}c+\rho_{13}d \\ \delta &\equiv\ \ a-\rho_{13}c-\rho_{14}d \end{aligned}\right\} \pmod{m}, \tag{21}$$

$$\rho_{13}^2+\rho_{14}^2 \equiv 3 \pmod{m}. \tag{22}$$

The congruence (22) can always be solved.

The determinant of (21) is 12 (mod m). Hence, because of $(m, 6) = 1$, the correspondence (21) between (16) and (17) is one to one. Hence (21) defines an isomorphism between the group of $+1$-units of $\mathfrak{A}_m$ and the group $SL(2, m)$.

We shall now prove that the homomorphism of the group of $+1$-units of $\mathfrak{A}$ into the group $SL(2, m)$ is onto.

$SL(2, m)$ is generated by the elements

$$U = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad V = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

It will be sufficient to show that U, V have counterimages which are units in $\mathfrak{A}$.

U has a unit counterimage, by (19). We must investigate the counterimages of V.

Express a, b, c, d in terms of α, β, γ, δ by means of (21), and put $\alpha = \gamma = \delta = 1$, $\beta = 0$.

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

Then we have

$$\left.\begin{aligned} a &\equiv 1 \\ b &\equiv b_0 \\ c &\equiv c_0 \\ d &\equiv d_0 \end{aligned}\right\} \pmod{m},$$

$$1+b_0^2-3c_0^2-3d_0^2 \equiv 1 \pmod{m}.$$

The corresponding equations in integers are

$$\left.\begin{aligned} a &= 1+xm, \\ b &= b_0+ym, \\ c &= c_0+um, \\ d &= d_0+vm, \end{aligned}\right\} \tag{23}$$

$$1+b_0^2-3c_0^2-3d_0^2 = 1+km. \tag{24}$$

V has a unit counterimage if there are integers x, y, u, v such that

$$(1+xm)^2+(b_0+ym)^2-3(c_0+um)^2-3(d_0+vm)^2 = 1. \tag{25}$$

We obtain from (25)

$$k+2x+2b_0y-6c_0u-6d_0v+m(x^2+y^2-3u^2-3v^2) = 0.$$

Split up this equation, obtaining

$$k+2x+2b_0y-6c_0u-6d_0v+mw = 0, \tag{26}$$

$$x^2+y^2-3u^2-3v^2 = w. \tag{27}$$

Put

$$\left.\begin{aligned} x &= x_0-b_0r+3c_0s+3d_0t, \\ y &= b_0x_0+r, \\ u &= c_0x_0+s, \\ v &= d_0x_0+t, \end{aligned}\right\} \tag{28}$$

where x_0, r, s, t are parameters. Substitute (28) in (26) and (27), obtaining

$$2(1+km)x_0+mw = -k, \tag{29}$$

$$f(r, s, t) = (1+b_0^2)r^2+3(3c_0^2-1)s^2+3(3d_0^2-1)t^2-6b_0c_0rs-6b_0d_0rt+18c_0d_0st, \tag{30}$$

$$f(r, s, t) = w-(1+km)x_0^2 = N, \quad \text{say.} \tag{31}$$

(29) is a linear diophantine equation in x_0, w which can always be solved. (30) is an indefinite ternary quadratic form. (31) says that this form must represent a certain number N which comes from a solution of (29). Thus we have reduced the problem of evaluating a unit counterimage for V to the problem of representing a certain number by a certain ternary quadratic form.

We can apply the theory of quadratic forms. There is a theorem of A. Meyer [**10**, p. 189] which gives sufficient conditions under which there is but one class in the genus of an indefinite ternary quadratic form.

Let A be the matrix of f, and Ω the g.c.d. of the two-rowed minors of A. Then the determinant d of A can be written as $d = \Omega^2\lambda$, where λ is an integer. The form F with the matrix

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

$A^{-1}d/\Omega$ is called the reciprocal form of f. A form is called properly primitive if the g.c.d. of all coefficients is 1 and the coefficients of r^2, s^2, t^2 are all odd.

In our special case we have

$$\Omega = 3, \quad \lambda = 1+b_0^2-3c_0^2-3d_0^2 = 1+km,$$

$$F = 9(3c_0^2+3d_0^2-1)r^2+3(-3d_0^2+b_0^2+1)s^2+3(-3c_0^2+b_0^2+1)t^2 + 18b_0c_0rs+18b_0d_0rt+18c_0d_0st.$$

Now Meyer's criterion is as follows:

An indefinite ternary quadratic form has but one class in its genus if the following conditions hold:

(1) the form f and its reciprocal form F are both properly primitive;

(2) the numbers Ω, λ are relatively prime and neither is divisible by 4.

One can easily verify that in our case one can fulfil these conditions. If b_0 is odd, replace it by b_0+m, and similarly for c_0, d_0, so that $b_0 \equiv c_0 \equiv d_0 \equiv 0$ modulo 2. Then f and F are both properly primitive. Ω and λ are relatively prime, because the congruence $1+b_0^2 \equiv 0$ modulo 3 has no solutions. Moreover, we have $\lambda = 1+b_0^2-3c_0^2-3d_0^2 \equiv 1$ modulo 4. Thus all conditions of Meyer's criterion are fulfilled, and we conclude that there is but one class in the genus of f.

If there is but one class in the genus of an indefinite ternary quadratic form f, then the number N is represented by f if and only if the congruence

$$f \equiv N \pmod{p^{\mu+1}} \tag{31a}$$

is solvable for every prime $p \mid 2d$, where p^μ is the highest power of p dividing N or $4N$ according as p is odd or even. Cf. [**10**, p. 186].

From (29), (31) and (24) we deduce that

$$m^2N \equiv 1 \pmod{(1+km)},$$
$$N \not\equiv 0 \pmod 2 \quad \text{and} \quad \pmod 3.$$

Hence $(N, 2d) = 1$, and $\mu = 0$ for p odd and $\mu = 2$ for $p = 2$.

For p odd and $p \neq 3$ the form $f \pmod p$ has rank 2. It is not difficult to see that a binary quadratic form in the prime field of characteristic p represents all numbers of this field. Hence (31a) is solvable.

For $p = 3$, f reduces to

$$f \equiv (1+b_0^2)r^2 \pmod 3.$$

Hence (31a) is not solvable only when $N \equiv -(1+b_0^2) \pmod 3$. One can easily see that the solution x_0, w of (29) can be chosen such that $N \not\equiv -(1+b_0^2) \pmod 3$.

For $p = 2$, (31a) takes the form

$$f \equiv N \pmod 8.$$

We had chosen b_0, c_0, d_0 even. We can even choose $b_0 \equiv c_0 \equiv d_0 \equiv 0 \pmod 4$. Then we have

$$f \equiv r^2-3s^2-3t^2 \pmod 8.$$

The congruence (31a) is not solvable only when $N \equiv -1 \pmod 8$. One can readily verify that the solution x_0, w of (29) can be chosen such that $N \not\equiv -1 \pmod 8$.

Hence (31a) can be solved for all relevant primes. We conclude that f represents the number N of (31).

This proves that V has a counterimage which is a unit in $\mathfrak{U}$.

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

To prove the third assertion of Theorem 3, we need only remark that (21) maps the element $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ of $\mathfrak{A}_m$ onto the element $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$ of $SL(2, m)$.

We shall now prove the last part of Theorem 3. The induced factor group of $\mathfrak{F}$ must be of index either 1 or 2 in $SL(2, m)/\mathfrak{H}$. Consider the generators

$$U = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, \qquad W = \begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}$$

of $SL(2, m)/\mathfrak{H}$. They satisfy the relations

$$U^2 = W^3 = (UW)^m = 1. \tag{32}$$

Assume that $SL(2, m)/\mathfrak{H}$ has a subgroup of index 2. Then the commutator subgroup is contained in this subgroup. Add the relation

$$U^{-1}W^{-1}UW = 1$$

to (32). Then we obtain the trivial group as a factor group, which contradicts our assumption that there is a subgroup of index 2. Hence the induced factor group of $\mathfrak{F}$ is as in Theorem 3, and our proof of Theorem 3 is complete.

For the remaining cases, it will be convenient to have the following lemma.

LEMMA 2. *Let $m = m_1m_2$ and $(m_1, m_2) = 1$. Then the group $\mathfrak{U}_m$ of $+1$-units of $\mathfrak{A}_m$ is the direct product of the corresponding groups for m_1, m_2:*

$$\mathfrak{U}_m \cong \mathfrak{U}_{m_1} \times \mathfrak{U}_{m_2}. \tag{33}$$

Proof. Let $\mathfrak{K}_{m_1}, \mathfrak{K}_{m_2}$ be the normal subgroups of those $+1$ units of $\mathfrak{U}_m$ which are $\equiv 1$ modulo m_1, m_2 respectively. Consider an element of $\mathfrak{U}_m$:

$$Y = \begin{pmatrix}a+bi & 3c+3di\\ c-di & a-bi\end{pmatrix}$$

with $a^2+b^2-3c^2-3d^2 \equiv 1 \pmod m$.

Determine a', b', c', d' modulo m such that

$$\left.\begin{aligned}a' &\equiv a\\ b' &\equiv b\\ c' &\equiv c\\ d' &\equiv d\end{aligned}\right\} \pmod{m_2}, \qquad \left.\begin{aligned}a' &\equiv 1\\ b' &\equiv 0\\ c' &\equiv 0\\ d' &\equiv 0\end{aligned}\right\} \pmod{m_1}.$$

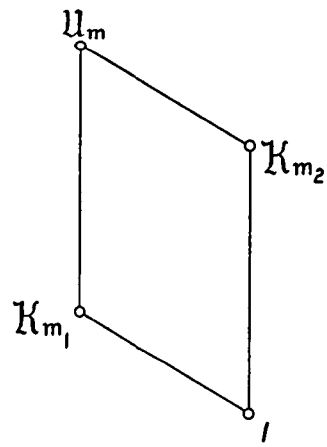

Figure 4

Put

$$Y_1 = \begin{pmatrix}a'+b'i & 3c'+3d'i\\ c'-d'i & a'-b'i\end{pmatrix},$$

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

and determine Y_2 by $Y_2 = Y_1^{-1}Y$. Then we have $Y_1 \in \mathfrak{K}_{m_1}$, $Y_2 \in \mathfrak{K}_{m_2}$. Thus we can decompose every element Y of $\mathfrak{U}_m$ into a product of elements of $\mathfrak{K}_{m_1}, \mathfrak{K}_{m_2}$. Obviously the intersection of $\mathfrak{K}_{m_1}$ and $\mathfrak{K}_{m_2}$ is 1, which completes the proof of the lemma.

Next we consider the case $m = 3^s z$, $(z, 6) = 1$. We shall prove

THEOREM 4. *Let* $m = 3^s z$, $(z, 6) = 1$.

(*a*) *The group* $\mathfrak{U}_{3^s}$ *of* $+1$*-units of* $\mathfrak{A}_{3^s}$ *is an extension of a 2-generated 3-group of order* 3^{3s-1} *with a factor group elementary abelian of order* 4.

(*b*) *The group of* $+1$*-units of* $\mathfrak{A}$ *is mapped onto the group of* $+1$*-units of* $\mathfrak{A}_m$.

(*c*) *The induced factor group of* $\mathfrak{P}$ *is a factor group of* $\mathfrak{U}_m$ *with respect to a normal subgroup of order* 2. *The induced factor group of* $\mathfrak{F}$ *is of index* 2 *in the factor group of* $\mathfrak{P}$.

Proof. (*a*) Consider the group $\mathfrak{U}_{3^s}$.

First take $s = 1$. The congruence

$$a^2 + b^2 \equiv 1 \pmod 3$$

has only the solutions $a \equiv \pm 1$, $b \equiv 0$ and $a \equiv 0$, $b \equiv \pm 1$. Now take $s \geqq 1$. The elements with $a \equiv +1$, $b \equiv 0 \pmod 3$ form a normal subgroup $\mathfrak{N} = \mathfrak{N}_{3^s}$, which is of index 4.

For $s = 1$, this group is of order 9. Every $+1$-unit of $\mathfrak{A}_{3^{s-1}}$ can be extended in exactly 3^3 ways to a $+1$-unit of $\mathfrak{A}_{3^s}$. Thus the group $\mathfrak{N}_{3^s}$ has the order 3^{3s-1}.

We shall now prove that $\mathfrak{N}$ is generated by the elements

$$R = \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix}, \qquad S = \begin{pmatrix} -2 & 3i \\ -i & -2 \end{pmatrix}.$$

$\mathfrak{N}_{3^{s-1}}$ is a factor group of $\mathfrak{N}_{3^s}$ with a kernel $\mathfrak{K}$ of order 3^3. This kernel is generated by the elements

$$Q_1 = \begin{pmatrix} 1+3^{s-1}i & 0 \\ 0 & 1-3^{s-1}i \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 1 & 0 \\ 3^{s-1} & 1 \end{pmatrix}, \quad Q_3 = \begin{pmatrix} 1 & 0 \\ 3^{s-1}i & 1 \end{pmatrix}.$$

We assert that $\mathfrak{K}$ is contained in the Frattini subgroup $\phi(\mathfrak{N})$. $\mathfrak{N}$ is a p-group (with $p = 3$). In a p-group, the Frattini subgroup contains the commutator subgroup. Define

$$Q_4 = \begin{pmatrix} 1 & 3^{s-1} \\ 3^{s-2} & 1 \end{pmatrix}, \qquad Q_5 = \begin{pmatrix} 1 & -3^{s-1}i \\ 3^{s-2}i & 1 \end{pmatrix}.$$

Then we have

$$Q_6 = Q_4 S Q_4^{-1} S^{-1} = \begin{pmatrix} 1+3^{s-1}i & 0 \\ 3^{s-1} & 1-3^{s-1}i \end{pmatrix},$$

$$Q_7 = Q_5 R Q_5^{-1} R^{-1} = \begin{pmatrix} 1+3^{s-1}i & 0 \\ 3^{s-1}i & 1-3^{s-1}i \end{pmatrix},$$

$$Q_6 R Q_6^{-1} R^{-1} = \begin{pmatrix} 1 & 0 \\ -3^{s-1}i & 1 \end{pmatrix}, \qquad Q_7 S Q_7^{-1} S^{-1} = \begin{pmatrix} 1 & 0 \\ -3^{s-1} & 1 \end{pmatrix}.$$

This proves that $\mathfrak{K}$ is contained in the commutator group of $\mathfrak{N}$, and hence in the Frattini subgroup $\phi(\mathfrak{N})$.

One can easily verify that for $s = 2$, $\mathfrak{N}$ is generated by R, S. Assume that for $s > 2$, $\mathfrak{N}_{3^{s-1}}$ is generated by $R\mathfrak{K}, S\mathfrak{K}$. Then $\mathfrak{N}_{3^s}$ is generated by $R, S, \mathfrak{K}$, and because of $\mathfrak{K} \subset \phi(\mathfrak{N}_{3^s})$ by R, S.

The factor group $\mathfrak{U}_{3^s}/\mathfrak{A}$ is elementary abelian of order 4. Take as generators

$$T = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad Z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then the group $\mathfrak{U}_{3^s}$ is generated by R, S, T, Z. The group $\mathfrak{Z} = (1, Z)$ is a direct factor.

(*b*) We shall now prove that for $m = 3^s z$, $(z, 6) = 1$, the group $\mathfrak{U}$ of $+1$-units of $\mathfrak{A}$ is mapped onto the group $\mathfrak{U}_m$ of $+1$-units of $\mathfrak{A}_m$.

$\mathfrak{U}_m$ is a direct product, by Lemma 2. Take as generators for $\mathfrak{U}_m$ the generators of the direct factors. For R this would be

$$\begin{pmatrix} a+bi & 3c+3di \\ c-di & a-bi \end{pmatrix}$$

with

$$\left.\begin{aligned} a &\equiv -2 \\ b &\equiv 0 \\ c &\equiv 1 \\ d &\equiv 0 \end{aligned}\right\} \pmod{3^s}, \qquad \left.\begin{aligned} a &\equiv 1 \\ b &\equiv 0 \\ c &\equiv 0 \\ d &\equiv 0 \end{aligned}\right\} \pmod{z}. \tag{34}$$

The congruences (34) have a unique solution modulo $3^s z$. We must show that there is a $+1$-unit in $\mathfrak{A}$ which has the solution of (34) as its image. The proof is essentially the same as for Theorem 3, and we can omit it here, as well as the explicit consideration of the other generators.

(*c*) In order to prove the last statement of Theorem 4, we first remark that for $m = 3^s$ the induced factor group of $\mathfrak{P}$ is $\mathfrak{U}_{3^s}/\mathfrak{Z}$, the subgroup $\mathfrak{Z}$ of $\mathfrak{U}_{3^s}$ being factored out. In order to obtain the induced factor group of $\mathfrak{P}$ for $m = 3^s z$, form the direct product according to Lemma 2, and factor out the subgroup $\mathfrak{Z}$ of order 2.

Now take the generators (11) of $\mathfrak{P}$. Obviously the products AC, BC, DC, EC, FC generate the subgroup $\mathfrak{F}$. For all these products we have $a \equiv \pm 1$, $b \equiv 0 \pmod 3$. Hence this is valid for all elements of $\mathfrak{F}$. However, it does not hold for the element C of $\mathfrak{P}$. So we have a criterion for $\mathfrak{F}$ which is purely arithmetical. This criterion is inherited by the induced homomorphism modulo $m = 3^s z$. Hence the induced factor group of $\mathfrak{F}$ is of index 2 in the factor group of $\mathfrak{P}$. This completes the proof of Theorem 4.

Notice that in terms of Theorem 3(*d*) and Fig. 3 the statement that the induced factor group of $\mathfrak{F}$ is of index 2 in the factor group of $\mathfrak{P}$ is equivalent to $\mathfrak{p}_m \subset \mathfrak{F}$.

Last we consider the case $m = 2^r 3^s z$, $(z, 6) = 1$. We shall prove

THEOREM 5. *Let* $m = 2^r 3^s z$, $(z, 6) = 1$.

(*a*) *The group* $\mathfrak{U}_{2^r}$ *is a 2-group of order* 2^{3r-1} *for* $r > 1$ *and* 2^3 *for* $r = 1$. *It has a direct factor of order 2:*

$$\mathfrak{U}_{2^r} = \mathfrak{Z}_2 \times \mathfrak{U}^*_{2^r}.$$

For $r > 1$, $\mathfrak{U}_{2^r}$ *has minimally 5 generators, and for* $r = 1$ *it has 3 generators.*

(*b*) *By Lemma 2 and* (*a*) *we have*

$$\mathfrak{U}_m = \mathfrak{Z}_2 \times \mathfrak{U}^*_{2^r} \times \mathfrak{U}_{3^s z} = \mathfrak{Z}_2 \times \mathfrak{U}^*_m.$$

The group $\mathfrak{U}$ *of* $+1$*-units of* $\mathfrak{A}$ *is mapped onto the subgroup* $\mathfrak{U}^*_m$ *of the group* $\mathfrak{U}_m$ *of* $+1$*-units of* $\mathfrak{A}_m$.

(*c*) *The induced factor group of* $\mathfrak{P}$ *is a factor group of* $\mathfrak{U}^*_m$ *with respect to a subgroup of order 2, except for* $m = 2$, *where the factor group of* $\mathfrak{P}$ *is* $\mathfrak{U}^*_2$. *The induced factor group of* $\mathfrak{F}$ *is of index 2 or 1 in the factor group of* $\mathfrak{P}$ *according as* $s > 0$ *or* $s = 0$.

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

Proof. (*a*) Consider the groups $\mathfrak{U}_{2^r}$.

For $r \leqq 2$, these groups are exceptional.

For $r = 1$, one can easily verify that $\mathfrak{U}_2$ is elementary abelian of order 2^3, and generated by the elements

$$B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \qquad P_1 = \begin{pmatrix} 1+i & 1 \\ 1 & 1+i \end{pmatrix}.$$

For $r = 2$, the group $\mathfrak{U}_4$ is elementary abelian of order 2^5, and generated by the elements

$$F = \begin{pmatrix} i & 2+2i \\ 2+2i & i \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 2-i \\ 2-i & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 2i & -1 \\ 1 & 2i \end{pmatrix},$$

$$C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1+2i & 0 \\ 0 & 1+2i \end{pmatrix}.$$

For $r > 2$, we shall prove that $\mathfrak{U}_{2^r}$ is of order 2^{3r-1}. Consider a solution of the congruence

$$a'^2 + b'^2 - 3c'^2 - 3d'^2 \equiv 1 \pmod{2^{r-1}}.$$

Write this congruence as a congruence modulo 2^r:

$$a'^2 + b'^2 - 3c'^2 - 3d'^2 \equiv 1 + k2^{r-1} \pmod{2^r},\ k = 0, 1.$$

The solutions with $k = 0$ form a subgroup of index 2. Take a solution modulo 2^{r-1} with $k = 0$, and put

$$\left.\begin{aligned} a &\equiv a' + x2^{r-1} \\ b &\equiv b' + y2^{r-1} \\ c &\equiv c' + u2^{r-1} \\ d &\equiv d' + v2^{r-1} \end{aligned}\right\} \pmod{2^r},$$

where x, y, u, v take the values 0, 1 independently. Then a, b, c, d is a solution of the congruence modulo 2^r. Thus for every solution modulo 2^{r-1} with $k = 0$ there are 2^4 solutions modulo 2^r. The solutions modulo 2^{r-1} with $k = 1$ cannot be extended to solutions modulo 2^r.

Assume that the order of $\mathfrak{U}_{2^{r-1}}$ is 2^{3r-4}. Then the order of $\mathfrak{U}_{2^r}$ is $2^{3r-4+4-1} = 2^{3r-1}$.

For $r > 2$, the group $\mathfrak{U}_{2^r}$ is generated by the elements

$$F = \begin{pmatrix} 5i & 6+6i \\ 2-2i & -5i \end{pmatrix}, \quad A = \begin{pmatrix} 4i & 6+3i \\ 2-i & -4i \end{pmatrix}, \quad B = \begin{pmatrix} 2i & 3 \\ 1 & -2i \end{pmatrix},$$

$$C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad P = \begin{pmatrix} -1+2^{r-1} & 0 \\ 0 & -1+2^{r-1} \end{pmatrix}.$$

The proof is as in Theorem 4(*a*), and we can omit it here.

F, A, B, C generate a subgroup $\mathfrak{U}^*_{2^r}$ of index 2, and the group $\mathfrak{Z}_2 = (1, P)$ is a direct factor:

$$\mathfrak{U}_{2^r} = \mathfrak{Z}_2 \times \mathfrak{U}^*_{2^r}.$$

This statement will follow from the proof of (*b*).

https://doi.org/10.1017/S2040618500034316 Published online by Cambridge University Press

(*b*) We shall prove that P has no counterimage which is a unit in $\mathfrak{A}$. Consider the equations

$$\begin{aligned} a &= -1+2^{r-1}+x2^r, \\ b &= y2^r, \\ c &= u2^r, \\ d &= v2^r, \\ a^2+b^2-3c^2-3d^2 &= 1. \end{aligned}$$

From these equations we deduce that

$$-1+2^{r-2}+2x(-1+2^{r-1})+2^r(x^2+y^2-3u^2-3v^2)=0.$$

For $r>2$, this equation is not solvable in integers. Hence P has no counterimage which is a unit in $\mathfrak{A}$. The same result holds for P_2 and P_1.

The elements F, A, B, C have unit counterimages in $\mathfrak{A}$. Hence all elements of $\mathfrak{U}^*_{2^r}$ have unit counterimages, and the group $\mathfrak{U}$ of $+1$-units of $\mathfrak{A}$ is mapped onto $\mathfrak{U}^*_{2^r}$.

From this it follows, in particular, that the group $\mathfrak{H}_2=(1,P)$ is a direct factor in $\mathfrak{U}_{2^r}$. For the remaining part of the proof of statement (*b*), we can proceed as in the proof of Theorem 4 (*b*).

(*c*) For the first part of the statement (*c*) and for the second part if $s>0$, we can refer to the proof of Theorem 4 (*c*).

If $s=0$, according to the remark at the end of the proof of Theorem 4 (*c*) we must show that $\mathfrak{p}_m \not\subset \mathfrak{H}$.

Take the module $m'=2^r3z$, and take a $+1$-unit

$$Y'=\begin{pmatrix} a+bi & 3c+3di \\ c-di & a-bi \end{pmatrix}$$

of $\mathfrak{U}_{m'}$ such that

$$\begin{aligned} a &\equiv 1,\ b\equiv c\equiv d\equiv 0 \pmod{2^rz}, \\ a &\equiv 0,\ b\equiv 1,\ c\equiv d\equiv 0 \pmod 3. \end{aligned}$$

We have $Y'\in\mathfrak{U}^{**}_{m'}$, and hence, by Theorem 5 (*b*), Y' has a counterimage Y which is a unit in $\mathfrak{A}$. Now Y is not contained in $\mathfrak{H}$, by the criterion given in the proof of Theorem 4 (*c*). But $Y\in\mathfrak{p}_m$ for $m=2^rz$. Hence $\mathfrak{p}_m\not\subset\mathfrak{H}$.

This completes the proof of Theorem 5.

I am indebted to Professor Macbeath for very valuable comments which led to some augmentations and linguistic improvements.

REFERENCES

1. F. Bachmann, *Aufbau der Geometrie aus dem Spiegelungsbegriff* (Heidelberg, 1959).

2. P. Bergau and J. Mennicke, Über topologische Abbildungen der Brezelfläche vom Geschlecht 2, *Math. Zeit.* **74** (1960), 414–435.

3. J. L. Brenner, The linear homogeneous group, *Ann. of Math.* **39** (1938), 472–493.

4. J. L. Brenner, The linear homogeneous group, II, *Ann. of Math.* **45** (1944), 101–109.

5. J. L. Brenner, The linear homogeneous group, III, *Ann. of Math.* **71** (1960), 210–223.

6. H. S. M. Coxeter and J. Moser, *Generators and relations for discrete groups* (Erg. d. Math., N. F. **14,** 1957).

7. L. E. Dickson, *Linear groups, with an exposition of the Galois field theory* (New York, 1958).

8. W. Fenchel, On the projective geometric foundations of the non-Euclidean geometry, *Mat. Tidsskr.* B. 1941, 18–30 (Danish).

9. L. Goeritz, Die Abbildungen der Brezelfläche und der Vollbrezel vom Geschlecht 2, *Hamb. Abh.* **9** (1933), 244–259.

10. B. W. Jones, *The arithmetic theory of quadratic forms* (New York, 1950).

11. F. Klein, *Elementary mathematics from an advanced standpoint—Geometry* (New York, 1939).

12. I. Reiner, Normal subgroups of the unimodular group, *Illinois J. Math.* **2** (1958), 142–144.

13. H. Seifert and W. Threlfall, *Lehrbuch der Topologie* (New York, 1947).

14. B. L. Van der Waerden, *Gruppen von linearen Transformationen* (Erg. d. Math. **4**, 1935).

15. H. Zassenhaus, *The theory of groups* (New York, 2nd ed. 1958).

THE UNIVERSITY
GLASGOW