Accepted.

FUCHSIAN GROUPS ASSOCIATED WITH CERTAIN INDEFINITE QUATERNARY QUADRATIC FORMS

by

John Bell Wright

--

A Thesis submitted for the Degree of

MASTER OF ARTS

in the Department

of

MATHEMATICS.

--

THE UNIVERSITY OF BRITISH COLUMBIA

APRIL, 1940

TABLE OF CONTENTS

FUCHSIAN GROUPS ASSOCIATED WITH CERTAIN INDEFINITE QUATERNARY QUADRATIC FORMS

1. Introduction.

The object of this paper is to present a method of determining all integral solutions of the equation

$$(1) \qquad x_1^2 + x_2^2 - D(x_3^2 + x_4^2) = 1,$$

where D is any integer. The procedure follows closely that of Dr. Ralph Hull in his paper[1] "On the Units of Indefinite Quaternion Algebras". For the particular cases, $D \leqq -1$, $D = 0$, the solutions are trivial. For small positive values of D it is easy to determine actual solutions by trial. We shall show that, in the general case, all solutions may be determined from a finite number of special solutions or generators.

We begin by associating our problem with that of finding generators of a corresponding Fuchsian group of linear fractional transformations of the complex plane. In Section 2, we show how this is done and we also develop certain formulas which will be used later. For this Fuchsian group a principal circle and a fundamental polygon can be constructed, and when this is done it is possible to determine the generators of the group. The method of procedure is shown in detail for the

[1] American Journal of Mathematics, vol. LXI, no. 2, April, 1939, pp. 365-374.

four cases, $D = 1$, $D = 3$, $D = 5$, and $D = 7$, and these cases illustrate the different situations that may arise.

From the general theory[2] of Fuchsian groups it is known that the structure of such a group is completely determined by the numbers of its classes of elliptic and parabolic transformations and the genus of the associated Riemann surface. It will be shown in Section 2, that the Fuchsian groups involved in the present problem contain elliptic transformations of order 2 only; may contain hyperbolic transformations; and may, or may not, contain parabolic transformations, according to the form of the integer D. In accord with a restriction on D, described in Section 3, we shall deal chiefly with the case in which no parabolic transformations occur. For these restricted values of D we have only to determine the class number of elliptic transformations, m, and the genus number, h. However, in Section 4, we use formulas of Humbert[3] and Klein[4] to show that h can be computed from D and m. Hence our fundamental problem becomes the determination of m for a given D.

In Section 5, we evaluate m by actually listing, according to certain congruential conditions, the possible classes of elliptic transformations for the restricted values of D. We first obtain an upper limit to the number of these classes,

[2] Fricke - Klein, Automorphe Funktionen, vol. 1.

[3] Humbert, Comptes Rendus, vol. 166, 1918.

[4] Fricke - Klein, op. cit., vol. I.

and then prove that this number is actually attained.

In the last section the results obtained are summarized, and, as a further illustration, canonical generators are exhibited for the cases D = 3, and D = 7. These are the only two, of the four examples of Section 2, that are given by our restricted value of D.

2. The corresponding Fuchsian group of transformations.

Later in this paper we shall have occasion to consider, along with solutions of equation (1), those of the equation

(2) $$x_1^2 + x_2^2 - D(x_3^2 + x_4^2) = N,$$

where N may have integral values other than N = 1. The quaternary quadratic form on the left of (2) may be regarded as the norm form of a certain generalized quaternion algebra, and with this connection in mind, we shall refer to a set of numbers $X = [x_1, x_2, x_3, x_4]$ as an element; that is, an element of the associated quaternion algebra. In almost all cases, the coordinates, x_1, x_2, x_3, and x_4, of the elements employed here will be rational integers, and we shall henceforth use the word "element", without a modifier, in this sense. When the coordinates of an element X satisfy the relation (2), we call N the norm of X, and write $N = f(X) = f[x_1, x_2, x_3, x_4]$. The solutions of equation (1) are integral elements of norm N = 1, which we shall call units.

In order to define the product of two elements it is convenient to represent them as matrices. Then, to the element $X = [x_1, x_2, x_3, x_4]$, we let correspond the matrix

$$(3) \qquad X \longleftrightarrow \left\| \begin{matrix} x_1 + ix_2 & D(x_3 - ix_4) \\ x_3 + ix_4 & x_1 - ix_2 \end{matrix} \right\| , \quad i^2 = -1.$$

The determinant of this matrix (3) is the norm form (2). By means of this representation we obtain the product of two elements X and

$$(4) \qquad Y = [y_1, y_2, y_3, y_4] \longleftrightarrow \left\| \begin{matrix} y_1 + iy_2 & D(y_3 - iy_4) \\ y_3 + iy_4 & y_1 - iy_2 \end{matrix} \right\| ,$$

by matrix multiplication. The product of these matrices, (3) and (4), is the matrix

$$\left\| \begin{matrix} z_1 + iz_2 & D(z_3 - iz_4) \\ z_3 + iz_4 & z_1 - iz_2 \end{matrix} \right\| ,$$

where

$$(5) \qquad \begin{aligned} z_1 &= x_1y_1 - x_2y_2 + D(x_3y_3 + x_4y_4) , \\ z_2 &= x_2y_1 + x_1y_2 - D(x_4y_3 - x_3y_4) , \\ z_3 &= x_3y_1 - x_4y_2 + x_1y_3 + x_2y_4 , \\ z_4 &= x_4y_1 + x_3y_2 - x_2y_3 + x_1y_4 . \end{aligned}$$

To this matrix we let correspond the element $Z = [z_1, z_2, z_3, z_4]$ and so formulas (5) define the product Z of two elements X and Y where,

$$[x_1, x_2, x_3, x_4] \cdot [y_1, y_2, y_3, y_4] = [z_1, z_2, z_3, z_4].$$

This product formula holds true for any value of N for we know that, since the norm is the determinant, the product of two norms is equal to the norm of the product.

The sum of two elements, X and Y, is readily defined by this matrix representation also, but we do not have occasion to use it in the paper.

We call that element, which, when multiplied by the element X, gives the identity element [1,0,0,0], the inverse of element X, and write it as $X^{-1} = [x_1, x_2, x_3, x_4]^{-1}$. This inverse exists if and only if $f(X) = N \neq 0$, and then from relations (5) we can verify that

$$[x_1, x_2, x_3, x_4]^{-1} = \left[\frac{x_1}{N}, -\frac{x_2}{N}, -\frac{x_3}{N}, -\frac{x_4}{N}\right],$$

where N is the norm.

Consider now the set of all elements of norm N = 1, that is, the set of all units. It is easily verified by relations (5) that the product of any two units is itself a unit, and that the inverse of any unit is a unit. From these facts it follows that the set of all units forms a group with respect to the type of multiplication defined above. For each value of D we will obtain a different set of solutions and so a different group. We propose to find the structure of these groups, and so we let any be the group G(D).

This group is easily related to a group of linear fractional transformations of the complex plane. To form the association we make the following correspondence,

$$(6) \qquad [x_1, x_2, x_3, x_4] \longleftrightarrow z = \frac{(x_1 + ix_2)w + D(x_3 - ix_4)}{(x_3 + ix_4)w + x_1 - ix_2},$$

where z and w are complex variables. This set of transformations of the complex plane forms a Fuchsian group, different for different values of D, which we shall call F(D) to distinguish from our group of solutions G(D). In case D > 0, F(D) is an infinite group. Transformations of such a group fall into three classes[5]; hyperbolic, elliptic, and parabolic.

---

[5] Ford, L.R., "Automorphic Functions", 1929, p.67.

From Ford's[6] work we have necessary and sufficient conditions that a transformation be of any one of the three types. We find that a transformation (6) is elliptic if, and only if,

$$|x_1 + ix_2 + x_1 - ix_2| < 2.$$

Since x_1 is an integer this means that $x_1 = 0$, and so we have the type of elliptic unit Y, where

$$(7) \qquad Y = [0, y_2, y_3, y_4], \qquad y_2^2 - D(y_3^2 + y_4^2) = 1.$$

Equations (5) will show that for any elliptic unit

$$Y^2 = [0, y_2, y_3, y_4]^2 = [-1, 0, 0, 0].$$

Again, a transformation is parabolic if and only if

$$x_1 + ix_2 + x_1 - ix_2 = \pm 2,$$

that is, $x_1 = \pm 1$. But from (1) this would mean that

$$(8) \qquad D = \left(\frac{x_2 x_3}{x_3^2 + x_4^2}\right)^2 + \left(\frac{x_2 x_4}{x_3^2 + x_4^2}\right)^2,$$

or that D must be of the form $u^2 + v^2$, where u and v are rational. All transformations which do not satisfy the above conditions are hyperbolic transformations.

The Fuchsian group F(D), of the last paragraph has a common fixed circle, or "principal circle"[7], given by the equation

$$(9) \qquad w\,\overline{w} = D, \text{ where } \overline{w} \text{ is the conjugate of } w,$$

and the transformation (6) carries that principal circle into itself, its interior into its interior, and its exterior into its exterior. We are able to draw the isometric circles

$$(10) \qquad |(x_3 + ix_4)z - x_1 - ix_2|^2 = 1,$$

of the transformation, which we shall denote by $I(X) =$

---

[6] Ford, op. cit., theorem 15, p. 23.

[7] Ibid., p. 67.

I:$[x_1, x_2, x_3, x_4]$ on the accompanying illustrations. These isometric circles are all orthogonal to the principal circle[8]. In this way we can construct a fundamental region for the group F(D), where we take the definition of fundamental region from Ford[9].

Definition 1. Two configurations, (points, curves, regions, etc.) are said to be congruent with respect to a group if there is a transformation of the group other than the identical transformation, which carries one configuration into the other.

Definition 2. A region, connected or not, no two of whose points are congruent with respect to a given group, and such that the neighbourhood of any point on the boundary contains points congruent to points in the given region, is called a fundamental region for the group.

With this region we may associate a Riemann surface in much the same way as a torus is defined by identifying the sides of the fundamental parallelogram in the case of elliptic functions. An important number associated with a Riemann surface is its genus number[10] which we shall require later. In our case the fundamental region is enclosed by arcs of the isometric circles, and so we call it a fundamental polygon. Any one isometric circle of the polygon is carried into another circle or into itself, by a suitable transformation, and these trans-

[8] Ford, op. cit., p. 67.

[9] Ibid., p. 37.

[10] Ibid., p. 227.

formations yield a set of generators and relations for the group F(D).

We illustrate the method of determining generators and relations from the fundamental polygon for the cases D = 1, 3, 5, and 7. The method of procedure is to assign such integral values -- 0, 1, 2,.........., in that order -- to $x_3^2 + x_4^2$ as will yield integral solutions of equation (1) for the given D, and then to determine those solutions. Then we draw the principal circle, and the isometric circles corresponding to the different solutions or transformations. It is to be expected that in this way the whole of the principal circle will be closed off by using relatively small values of $x_3^2 + x_4^2$. In certain cases we find a solution whose corresponding isometric circle does not contribute to the closing off of the principal circle. This is so whenever the centre of the isometric circle lies within a previously determined isometric circle. This happens for the unit [6, 0, 2, -1], of D = 7, for the centre of its isometric circle falls within the isometric circle of the unit [5, 2, 2, 0]. When this happens we proceed with the next value of $x_3^2 + x_4^2$. When the fundamental region has been completely closed off we are able to determine units carrying one part into the other. These units, indicated by arrows in the accompanying figures, form the set of generators for the group F(D). The arrow indicates that the isometric circle where it starts is carried by the unit into that circle to which it points.The vertices of the polygon are divided up into complete sets of congruent vertices which we shall call cycles. In some cases the cycle has a single vertex, but in others there are several vertices. The sum of the angles in the ordinary sense of any one cycle may add to 2π, π, or 0 radians. On multiplying together units necessary to complete the above cycles we will get units which are hyperbolic, elliptic, or parabolic in the respective cases. The three types are illustrated by the following units:

A, of case D = 7, where $\alpha = \pi$,

$C_1 G C_2^{-1} B^{-1}$, of case D = 7, where $\gamma_1 + \gamma_1 + \gamma_3 + \gamma_4 = 2\pi$,

B_1, of case D = 5, where $\beta_1 = 0$.

It will be found that two distinct cases arise according to the nature of the integer D. The examples D = 3 or 7, and D = 5, illustrate the two situations. The groups F(3), F(5), and F(7) can all be generated by a finite number of units. The group F(5) will contain parabolic, as well as elliptic and hyperbolic units, but the groups F(3) and F(7) will have no parabolic units. The vertices of the polygon for F(3) give rise to elliptic cycles only, while those of the polygon for F(7) have elliptic and hyperbolic cycles.

From the foregoing discussion we have the following

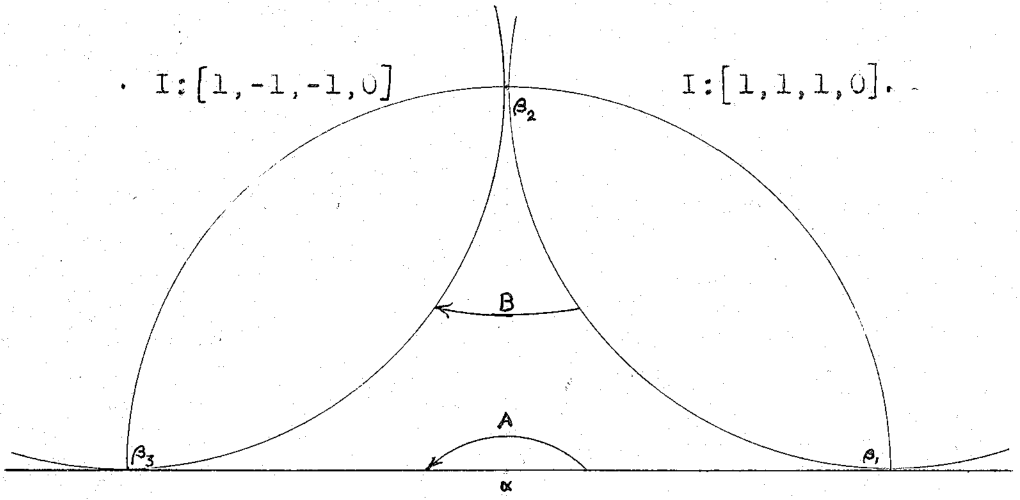
Theorem I. If D is any positive integer, the Fuchsian group F(D) can be generated by a finite number of units, satisfying certain relations. These units may be hyperbolic, elliptic, or parabolic, the latter occurring if and only if D is expressible in the form $u^2 + v^2$, u and v rational.

When the generators of F(D) are obtained, the correspondence (6) gives the like for G(D). It must be noted however that the two units [1,0,0,0] and [-1,0,0,0] both give the identity transformation in F(D), but are distinct inG(D). Hence when the generators of F(D) have been determined we must adjoin the unit [-1,0,0,0] to obtain the group G(D). This gives

Theorem II. The group, G(D), of integral solutions of equation (1), is obtained from the associated Fuchsian group F(D), according to the correspondence (6), by adjoining to the generators of F(D) the unit [-1,0,0,0].

FUNDAMENTAL POLYGON

$F(D) = F(1)$



Generators.

A:[0,1,0,0]

B:[1,1,1,0]

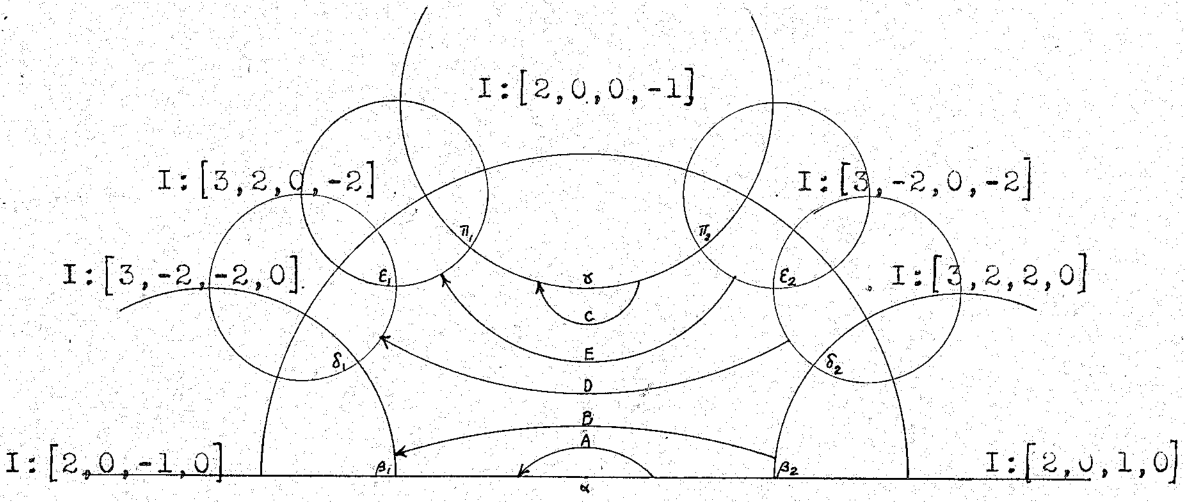
Relations.

α : $A^2 = -1$

β : Parabolic

FUNDAMENTAL POLYGON

F(D) = F(3)

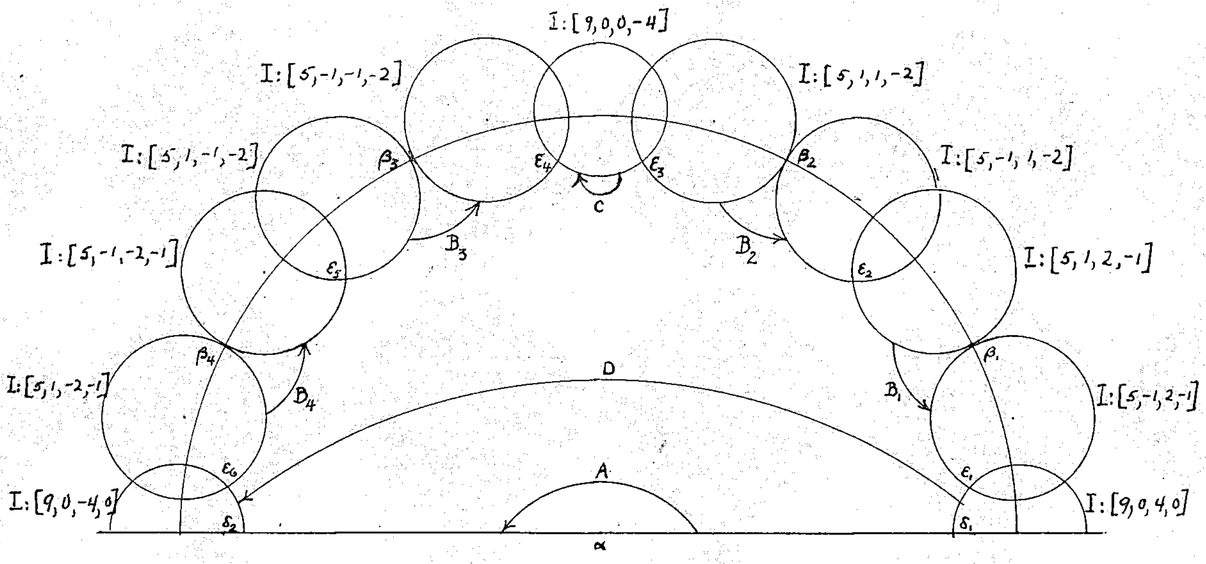


Generators.	
A:	[0,1,0,0]
B:	[2,0,1,0]
C:	[0,2,1,0]
D:	[3,2,2,0]
E:	[2,3,2,0]

Relations.			
α :	A^2	=	-1
γ :	$(C^{-1})^2$	=	-1
π :	$(CE^{-1})^2$	=	-1
ϵ :	$(ED^{-1})^2$	=	-1
δ :	$(DB^{-1})^2$	=	-1
β :	$(BA^{-1})^2$	=	-1

FUNDAMENTAL POLYGON

$F(D) = F(5)$



Generators.

A: $[0,1,0,0]$

B_1: $[-1,5,1,2]$

B_2: $[-1,5,2,1]$

B_3: $[-1,5,2,-1]$

B_4: $[-1,5,1,-2]$

C: $[0,9,4,0]$

D: $[9,0,4,0]$

Relations.

α : $A^2 = -1$

β : Parabolic

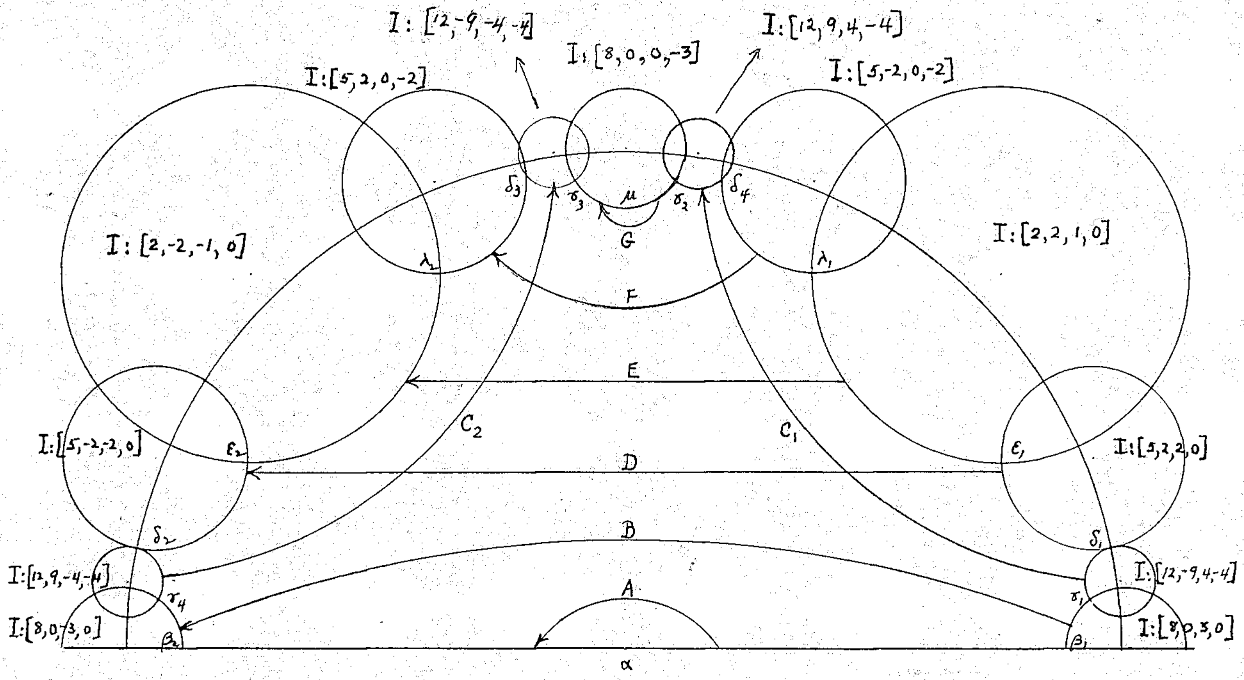
γ : $C^2 = -1$

δ : $(DA^{-1})^2 = -1$

ε : $(B_1^{-1}B_2^{-1}CB_3^{-1}B_4^{-1}D^{-1})^2 = -1$

FUNDAMENTAL POLYGON

$$F(D) = F(7)$$



Generators.

A: [0,1,0,0]

B: [8,0,3,0]

C_1: [9,12,4,4]

C_2: [-9,12,4,-4]

D: [5,2,2,0]

E: [2,2,1,0]

F: [2,5,2,0]

G: [0,8,3,0]

Relations.

α : $A^2 = -1$

β : $(BA^{-1})^2 = -1$

γ : $C_1 G C_2^{-1} B^{-1} = -1$

δ : $(DC_2 F^{-1} C_1^{-1})^2 = -1$

ε : $(ED^{-1})^2 = -1$

λ : $(FE^{-1})^2 = -1$

μ : $(G)^2 = -1$

3. A restriction on D.

It is the purpose of the remainder of this work to determine the number of generators necessary to give the group, F(D), for a given value of D. To this end we find it convenient here to introduce a restriction on D. We shall henceforth consider only those cases for which

$$(11)\qquad D = p_1 \cdot p_2 \cdot \ldots\ldots p_r, \quad p_i \text{ prime}, \quad p_i \equiv 3 (\mathrm{mod}\ 4),$$
$$r \geq 1, \quad p_i \neq p_j \text{ for } i \neq j.$$

This omits all cases in which F(D) has parabolic transformations and in particular the case D = 1. We shall show, however, that it is the principal case to be considered.

We shall first look at some trivial cases. For all values of D we have the solutions for equation (1) given by the units $[\pm 1,0,0,0]$ and $[0,\pm 1,0,0]$. For $D < -1$, or for $D = 0$, these are the only solutions. For $D = -1$ we have eight solutions only; $[\pm 1,0,0,0]$, $[0,\pm 1,0,0]$, $[0,0,\pm 1,0]$, and $[0,0,0,\pm 1]$. Hence we need not consider further the case in which D has negative values or the value zero.

Next, suppose D is expressible as the product SD', where S can be written in the form $\alpha^2 + \beta^2$, α and β integers, and where D' is defined as we have defined D in (11). Then from equation (1) we have

$$x_1^2 + x_2^2 - SD'(x_3^2 + x_4^2) = 1,$$
$$x_1^2 + x_2^2 - D'(\alpha^2 + \beta^2)(x_3^2 + x_4^2) = 1,$$
$$x_1^2 + x_2^2 - D'\{(\alpha x_3 - \beta x_4)^2 + (\beta x_3 + \alpha x_4)^2\} = 1,$$
$$y_1^2 + y_2^2 - D'(y_3^2 + y_4^2) = 1,$$

where

$$y_1 = x_1, \quad y_2 = x_2, \quad y_3 = \alpha x_3 - \beta x_4, \quad y_4 = \beta x_3 + \alpha x_4.$$

Thus every solution of

$$x_1^2 + x_2^2 - SD'(x_3^2 + x_4^2) = 1,$$

corresponds to a solution of

$$y_1^2 + y_2^2 - D'(y_3^2 + y_4^2) = 1.$$

Now, if D is any positive integer, we may write D = SD', where S can be written as $\alpha^2 + \beta^2$, α and β integers, and where D' is 1 or is of the form (11). These considerations lead at once to

Theorem III. If D is any positive integer we may write D = SD', where S = $\alpha^2 + \beta^2$, α and β being integers not both zero, and where D' may be 1 or of the form (11). Then the group G(D) is a subgroup of the group G(D').

It must be noted here that we do not attempt, in this paper, to show how to determine the generators for any values of D other than those of the form (11). However when the present case has been completed it should be a relatively simple matter to extend it to cover all other cases.

In Section 2 we have included the complete polygon and generators for the special case D = 1, since Theorem 3 shows it to be an important case not covered by our restriction on D. Its group of solutions F(D) = F(1) is generated by the two units A = [0,1,0,0], and B = [1,1,1,0], where $A^2 = -1$, and B is a parabolic unit.

4. The invariants of the Fuchsian group.

We have already mentioned that the structure of the group F(D) is determined completely by the number of its classes of elliptic units and the genus number. Let m be the number of classes of elliptic cycles, n the number of classes of hyperbolic cycles, and h the genus of the associated surface. The values m and h are invariants of the group F(D), depending only on the group and not on any particular way of representing it. The value n on the other hand is not invariant, and is only used to establish a relation connecting m and h that we require.

Displacements of the interior of the principal circle brought about by the linear fractional transformations are displacements of hyperbolic geometry. From this consideration the non-Euclidean area, $\mathcal{a}$, of our fundamental polygon is given by[11]

$$\mathcal{a} = (2t - 2)\pi - \Sigma,$$

where 2t is the number of sides to the polygon, counting the X axis as two sides, and Σ is the sum of the angles. But by an analytic proof of Humbert[12] the non-Euclidean area is also given by

$$\mathcal{a} = \pi D\prod_{q}(1 - 1/q) = \pi\phi(D),$$

where ϕ is the usual Euler function. Combining these two results we have

$$(2t - 2)\pi - \Sigma = \pi\phi(D).$$

[11] Coolidge, J. Lowell, The Elements of Non-Euclidean Geometry, 1909, theorem 5, p. 178.

[12] Humbert, op. cit., p.870.

But $\Sigma = m\pi + 2n\pi$, since the sum of the angles of each cycle of elliptic vertices is π, and the sum of the angles of a hyperbolic cycle is 2π. Then

$$(2t - 2)\pi - m\pi - 2n\pi = \pi\,\phi(D),$$

$$(12) \qquad 2(t - n) = \phi(D) + 2 + m.$$

Now the genus number h, of the associated surface is given by the formula[13]

$$2h - 1 = t - n - m.$$

Hence

$$t - n = 2h - 1 + m,$$

and on substituting this value of $t - n$ in (12) we have

$$2(2h - 1 + m) = \phi(D) + 2 + m,$$

$$(13) \qquad 4h = \phi(D) + 4 - m.$$

This formula (13) gives us the required relation, since it enables us to evaluate h when m has been determined. To find the number of generators for the group F(D) we go to the general theory[14] of Fuchsian groups. The linear fractional group, F(D), has a canonical set of $m + 2h$ generators

$$(14) \qquad U_1, U_2, \ldots\ldots, U_m, \quad V_1, V_2, \ldots\ldots, V_h, \quad V_1', V_2', \ldots\ldots V_h',$$

where U_i or V_j represent the units $U_i = [u_{i1}, u_{i2}, u_{i3}, u_{i4}]$ and $V_j = [v_{j1}, v_{j2}, v_{j3}, v_{j4}]$. These generators must satisfy the relations

$$U_1^2 = U_2^2 = \ldots\ldots\ldots = U_m^2 = -1,$$

$$U_1 . U_2 . \ldots\ldots U_m\left[\prod_{j=1}^{h} V_j^{-1} . V_j' . V_j . V_j'^{-1}\right] = -1.$$

[13] Fricke-Klein, op. cit., chapter 3, formula (2), p. 262.

[14] Ibid., pp. 186 - 187.

5. The determination of the number of classes of elliptic units.

The vertices of an elliptic cycle are fixed points of elliptic transformations of F(D)[15] all of which belong to the same class. We recall that two elliptic substitutions of a Fuchsian group are said to be in the same class if one is the transform of the other by a substitution of the group. In other words, two units, A and B, of the group F(D), are in the same class if there exists a unit X, of the group such that $X^{-1}AX = B$. Our task is to determine how many of these separate classes exist for a given D.

The unit [0,1,0,0] is present for every D and it determines one class which is represented by a single vertex. It will appear that any elliptic unit, $B = [0,b_2,b_3,b_4]$, can be transformed into this one by some element $X = [x_1,x_2,x_3,x_4]$, of norm N. It is necessary that we determine the different values that N can assume for our group F(D). Then by studying certain congruential conditions imposed on b_2 we can determine m.

Suppose then that A and B are two units such that B is the transform of A by some element X of norm N > 0. Then

(15) $X^{-1}AX = B$.

This means that

$$\left[\frac{x_1}{N},-\frac{x_2}{N},-\frac{x_3}{N},-\frac{x_4}{N}\right]\cdot\left[a_1,a_2,a_3,a_4\right]\cdot\left[x_1,x_2,x_3,x_4\right] = \left[b_1,b_2,b_3,b_4\right].$$

[15] Ford, op. cit., pp. 60-61.

Then on multiplication as defined by the relations (5) we have

$$(16)\qquad \begin{aligned} Nb_1 &= Na_1 , \qquad b_1 = a_1 , \\ Nb_2 &= \{x_1^2 + x_2^2 + D(x_3^2 + x_4^2)\} a_2 + 2D(x_1 x_4 - x_2 x_3) a_3 \\ &\quad -2D(x_1 x_3 + x_2 x_4) a_4 , \\ Nb_3 &= 2(x_1 x_4 + x_2 x_3) a_2 + (x_1^2 - x_2^2 - Dx_3^2 + Dx_4^2) a_3 \\ &\quad -2(x_1 x_2 + Dx_3 x_4) a_4 , \\ Nb_4 &= 2(x_2 x_4 - x_1 x_3) a_2 + 2(x_1 x_2 - Dx_3 x_4) a_3 \\ &\quad + \{x_1^2 - x_2^2 + Dx_3^2 - Dx_4^2\} a_4 . \end{aligned}$$

We wish to determine the minimum value of N to give an element X which transforms any unit A into a unit B. Since the unit $[0,1,0,0]$ is present for every value of D we simplify our problem by taking

$$A = [a_1 , a_2 , a_3 , a_4] = [0,1,0,0].$$

We must now determine the minimum value of N to give integral solutions x_1, x_2, x_3, and x_4 of (2), satisfying the new relations obtained from (16),

$$(17)\qquad \begin{aligned} b_1 &= 0, \\ Nb_2 &= x_1^2 + x_2^2 + D(x_3^2 + x_4^2), \\ Nb_3 &= 2(x_1 x_4 + x_2 x_3) , \\ Nb_4 &= 2(x_2 x_4 - x_1 x_3) . \end{aligned}$$

From relations (17) it follows that, for B to be in the same class as A, that is N = 1, we must have

$$b_2 = x_1^2 + x_2^2 + D(x_3^2 + x_4^2) = 1 + 2D(x_3^2 + x_4^2) .$$

Then it follows that

$$b_2 \equiv 1 (\mathrm{mod}\ 2D), \qquad b_2 \text{ positive.}$$

Now consider any elliptic unit $B = [0, b_2 , b_3 , b_4]$, where

(18) $\quad b_2^2 - D(b_3^2 + b_4^2) = 1.$

Then

(19) $\quad b_2^2 \equiv 1 (\mathrm{mod}\ D).$

Since D is defined as in (11) the above congruence is equivalent to the set of congruences

(20) $\quad b_2^2 \equiv 1 (\mathrm{mod}\ p_i), \quad i = 1, 2, \ldots\ldots\ldots, r.$

Hence

(21) $\quad b_2 \equiv 1 \text{ or } -1 \ (\mathrm{mod}\ p_1),$

$b_2 \equiv 1 \text{ or } -1 \ (\mathrm{mod}\ p_2),$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$b_2 \equiv 1 \text{ or } -1 \ (\mathrm{mod}\ p_r).$

We then have 2^r distinct possibilities for b_2. But we have also the further two possibilities

$$b_2 \equiv 0 \text{ or } 1 \ (\mathrm{mod}\ 2),$$

and so in all we have 2^{r+1} possible ways of choosing b_2.

From formulas (17) a necessary condition that $X'AX = B$ is that

(22) $\quad Nb_2 = x_1^2 + x_2^2 + D(x_3^2 + x_4^2).$

Since N is chosen positive then b_2 is also positive. From equation (2) we have that

$$x_1^2 + x_2^2 = N + D(x_3^2 + x_4^2),$$

and so we may write for (22)

$$Nb_2 = N + 2D(x_3^2 + x_4^2),$$

(23) $\quad N(b_2 - 1) = 2D(x_3^2 + x_4^2).$

Now suppose that

(24) $\quad D = D_1 D_2,$

where $D_1 = p_1 \cdot p_2, \ldots\ldots p_s$, $D_2 = p_{s+1} \cdot p_{s+2} \cdot \ldots\ldots p_r$, $(1 \leq s \leq r)$, and also suppose that

(25) $$b_2 \equiv 1 \pmod{D_1}, \qquad b_2 \equiv -1 \pmod{D_2}.$$

Then $b_2 + 1$ is divisible by D_2 and $b_2 - 1$ is prime to D_2. In such a case equation (23) shows that N must be divisible by D_2. In the case $b_2 \equiv 0 \pmod 2$, $b_2 - 1$ is odd and so N must be divisible by $2D_2$. In the case $b_2 \equiv 1 \pmod 2$, $b_2 - 1$ is even and we can only say that N is divisible by D_2.

Before we can continue with a theorem regarding the existence of elements X of norm N satisfying the previous conditions, we must prove a lemma which is essential to the proof of the theorem. The lemma and proof follow.

Lemma. If m and n are relatively prime positive integers, and if x_1 and x_2 are integers such that $x_1^2 + x_2^2 = mn$, then there exists a set of integers y_1, y_2, z_1, and z_2 such that

(26) $$y_1^2 + y_2^2 = m, \qquad z_1^2 + z_2^2 = n,$$

(27) $$x_1 = y_1 z_2 + y_2 z_1, \qquad x_2 = y_2 z_2 - y_1 z_1.$$

This lemma is a consequence of the extensive theory of the representation of positive integers as sums of two integral squares. It may also be proved[16] as follows by the means of the ideal theory of the quadratic number field R(i), where $i^2 = -1$, R is the rational field. The given integers x_1 and x_2 determine a principal ideal $((x_1 + ix_2))$ of the field R(i), of norm mn. The greatest common divisors of the ideal $((x_1 + ix_2))$ with the ideals $((m))$ and $((n))$, respectively, are ideals of norms m and n. Since all ideals of R(i) are

[16] This proof of the lemma has been suggested to me by Dr. Ralph Hull.

principal ideals, these common divisors are principal ideals, say $((y_1 + iy_2))$ and $((z_2 - iz_1))$, respectively, where y_1, y_2, z_1, and z_2 satisfy (26). Moreover, since m and n are relatively prime, $((x_1 + ix_2)) = ((y_1 + iy_2))((z_2 - iz_1)) = ((y_1 z_2 + y_2 z_1 + iy_2 z_2 - iy_1 z_1))$. From this equality of ideals it follows that

$$x_1 + ix_2 = \epsilon(y_1 z_2 + y_2 z_1 + iy_2 z_2 - iy_1 z_1),$$

where ϵ is one of the four units 1, -1, i, -i of R(i). If $\epsilon = 1$ we have (27) as desired. If, for example, $\epsilon = i$, we obtain (27), without altering (26), by the replacement of y_1, y_2, z_1, and z_2 by y_1, y_2, z_2, and $-z_1$, respectively. Similarly, if $\epsilon = -1$ or $-i$, we obtain (27), without altering (26), by suitable interchanges of y_1, y_2, z_1, and z_2, and their signs. This completes the proof of the lemma.

We are now ready to prove

Theorem IV. Let $D = D_1 D_2$, where $D_1 = p_1 \cdot p_2 \cdots p_s$, and $D_2 = p_{s+1} \cdot p_{s+2} \cdots p_r$. If $b_2 > 0$, $b_2 \equiv 1 \pmod{D_1}$, and $b_2 \equiv -1 \pmod{D_2}$, there exists an element X of norm $N > 0$, which transforms the unit $A = [0,1,0,0]$ into the unit $B = [0, b_2, b_3, b_4]$, such that $N = f(X) = D_2$ when b_2 is odd, and $N = f(X) = 2D_2$ when b_2 is even.

Case I. b_2 odd, i.e., $b_2 \equiv 1 \pmod 2$.

Let $b_2 = 1 + 2kD_1$, where $k > 0$ because $b_2 > 0$, and k is prime to D_2. Since B is a unit we may write

$$b_2^2 - D(b_3^2 + b_4^2) = 1,$$

$$D(b_3^2 + b_4^2) = b_2^2 - 1 = 1 + 4kD_1 + 4k^2 D_1^2 - 1$$

$$= 4kD_1(1 + kD_1),$$

$$D_1 D_2(b_3^2 + b_4^2) = 4kD_1(1 + kD_1),$$

$$D_2(b_3^2 + b_4^2) = 4k(1 + kD_1).$$

Since D_2 is odd, $b_3^2 + b_4^2$ is divisible by 4. Let $b_3 = 2b_3'$, $b_4 = 2b_4'$. Then

$$D_2(b_3'^2 + b_4'^2) = k(1 + kD_1).$$

Since k is prime to D_2, then $1 + kD_1$ must be a multiple of D_2 so $\left(\frac{1+kD_1}{D_2}\right)$ is an integer. Then

$$b_3'^2 + b_4'^2 = k \cdot \left(\frac{1+kD_1}{D_2}\right).$$

Here $k > 0$, $\left(\frac{1+kD_1}{D_2}\right) > 0$, and the two are relatively prime. The lemma that we have just proved gives the existence of integers y_1, y_2, z_1, and z_2 such that

$$y_1^2 + y_2^2 = \left(\frac{1+kD_1}{D_2}\right),$$

$$z_1^2 + z_2^2 = k,$$

$$b_3' = y_1 z_2 + y_2 z_1, \qquad b_4' = y_2 z_2 - y_1 z_1.$$

Take $x_1 = D_2 y_1$, $x_2 = D_2 y_2$, $x_3 = z_1$, $x_4 = z_2$.

Then

$$x_1^2 + x_2^2 - D(x_3^2 + x_4^2) = D_2^2(y_1^2 + y_2^2) - D(z_1^2 + z_2^2)$$
$$= D_2 = N,$$

$$x_1^2 + x_2^2 + D(x_3^2 + x_4^2) = D_2(1 + kD_1) + Dk$$
$$= D_2 b_2 = Nb_2,$$

$$2(x_1 x_4 + x_2 x_3) = 2D_2(y_1 z_2 + y_2 z_1) = 2D_2 b_3' = Nb_3,$$

$$2(x_2 x_4 - x_1 x_3) = 2D_2(y_2 z_2 - y_1 z_1) = 2D_2 b_4' = Nb_4.$$

Hence the relations (17) are satisfied and so in this case we have proved the existence of a unit X, of norm $N = f(X) = D_2$, which transforms A into B.

Case II. b_2 even, i.e., $b_2 \equiv 0 \pmod 2$.

Let $b_2 = 1+D_1 + 2kD_1$, where $k \geq 0$. Since B is a unit we have

$$D(b_3^2 + b_4^2) = b_2^2 - 1 = D_1(D_1 + 4k^2D_1 + 2 + 4k + 4kD_1),$$
$$D_2(b_3^2 + b_4^2) = D_1(1 + 2k)^2 + 2(1 + 2k)$$
$$= (1 + 2k)(2 + D_1 + 2kD_1).$$

Now obviously $1 + 2k$ is prime to D_2 or we should have $b_2 - 1$ divisible by D_2 in contradiction to our hypothesis. Hence $2 + D_1 + 2kD_1$ must be a multiple of D_2. So we write

$$b_3^2 + b_4^2 = (1 + 2k)\left(\frac{2 + D_1 + 2kD_1}{D_2} \right).$$

Since $k \geq 0$, the two factors are positive. Also

$$-D_1(1 + 2k) + (2 + D_1 + 2kD_1) = 2,$$

so the greatest common divisor of $(1 + 2k)$ and $(2 + D_1 + 2kD_1)$ is 1 or 2. But $(1 + 2k)$ is odd. Hence the two factors are relatively prime. The conditions here are in accord with the hypotheses of the lemma so we have the existence of integers y_1, y_2, z_1, and z_2 such that

$$(23) \qquad y_1^2 + y_2^2 = \left(\frac{2 + D_1 + 2kD_1}{D_2}\right),$$
$$z_1^2 + z_2^2 = 1 + 2k,$$
$$b_3 = y_1 z_2 + y_2 z_1, \qquad b_4 = y_2 z_2 - y_1 z_1.$$

Take $x_1 = D_2 y_1$, $x_2 = D_2 y_2$, $x_3 = z_1$, $x_4 = z_2$, and we can easily show that relations (17) are satisfied by the unit $X = [x_1, x_2, x_3, x_4]$ of norm $N = f(X) = 2D_2$. This completes the proof of Theorem 4.

There remains now only the determination of the value m. Let $B = [0, b_2, b_3, b_4]$ and $B' = [0, b_2', b_3', b_4']$ be two elliptic units of the group F(D). By the previous theorem there exists a unit X and a unit X' such that

$$N = f(X) = f(X') = D_2, \text{ for } b_2 \text{ odd},$$
$$N = f(X) = f(X') = 2D_2, \text{ for } b_2 \text{ even},$$

transforming B and B' into A. This means that

$$X^{-1}BX = A, \qquad X'^{-1}B'X' = A.$$

Then $A = X^{-1}BX = X'^{-1}B'X'$, and so

$$B' = X'X^{-1}B\,XX'^{-1} = (XX'^{-1})^{-1}B(XX'^{-1}).$$

If we can show that (XX'^{-1}) is a unit then we have shown that B and B' are equivalent. Now

$$XX'^{-1} = [x_1, x_2, x_3, x_4]\cdot\left[\frac{x_1'}{N}, -\frac{x_2'}{N}, -\frac{x_3'}{N}, -\frac{x_4'}{N}\right]$$
$$= \frac{1}{N}\Big[\; x_1x_1' + x_2x_2' - D(x_3x_3' + x_4x_4'),$$
$$-x_1x_2' + x_2x_1' - D(x_3x_4' - x_4x_3'),$$
$$x_3x_1' + x_4x_2' - x_1x_3' - x_2x_4',$$
$$-x_3x_2' + x_4x_1' - x_1x_4' + x_2x_3' \;\Big].$$

This product is of norm $N = f(XX'^{-1}) = 1$, so all that remains to show that it is a unit is to show that each of the coordinates is divisible by N, where $N = D_2$, for b_2 odd, and $N = 2D_2$, for b_2 even. In the proof of Theorem 4 our integers x_1, x_2, x_1', and x_2' were chosen to be multiples of D_2. Hence for the case b_2 odd, the coordinates are divisible by D_2 and so XX'^{-1} is a unit. In the case of b_2 even we must show also divisibility of each coordinate by 2. It follows from relations (28) that if b_3 is odd, b_4 even, then $y_1 \equiv z_1$, $y_2 \equiv z_2 \pmod 2$. Then for the coordinates to be divisible by 2 we must have $y_1' \equiv z_1'$, $y_2' \equiv z_2' \pmod 2$, i.e., b_3' odd, b_4' even. This condition is expressed by

(29) $\qquad b_3 \equiv b_3', \quad b_4 \equiv b_4' \pmod 2$.

This then is the criteria that XX'^{-1} be a unit in the case b_2 even. This allows two distinct possibilities for this latter case for we have one unit if b_3 and b_3' are both odd, b_4 and b_4' both even, and another unit when b_3 and b_3' are both even while b_4 and b_4' are odd.

We have therefore, shown that for b_2 odd or even there exists a unit transforming B into B'. Hence the two units B and B' are in the same class of elliptic units.

Now if b_2 is odd we have the 2^r possibilities to choose from and, since there will be a class of elliptic units associated with each choice, we have 2^r possible classes of elliptic units. On the other hand if b_2 is even we have 2 classes of elliptic units, distinguished by certain congruences (29), associated with every one of the 2^r choices of b_2. Hence in this case we have 2.2^r possible classes of elliptic units. In all then we have 3.2^r possible classes of elliptic units and hence $m \leq 3.2^r$.

We have here acquired an upper limit to the value of m. We shall show that this limit is actually attained by proving the existence of solutions of equation (2) where N = 1, 2, D_2, or $2D_2$; D_2 defined as in (24).

Solutions of equation (2) are easily obtained for the cases N = 1, or 2, for in these cases we have the units [0,1,0,0] and [1,1,0,0] respectively. The cases for $N = D_2$, or $N = 2D_2$ are more difficult.

We shall first prove the existence of solutions of the equation

$$(30) \qquad x_1^2 + x_2^2 - D(x_3^2 + x_4^2) = p_i,$$

p_i defined as in (11), $1 \leq i \leq r$. Write $D = p_i D'$. Then

$$(31) \qquad x_1^2 + x_2^2 - p_i D'(x_3^2 + x_4^2) = p_i,$$

$$x_1^2 + x_2^2 = p_i\{1 + D'(x_3^2 + x_4^2)\},$$

$$x_1^2 + x_2^2 \equiv 0 \pmod{p_i}.$$

Since p_i is a prime $\equiv 3 \pmod 4$, we may write

$$(32) \qquad x_1 = p_i x_1', \qquad x_2 = p_i x_2' \quad ,$$

and at the same time

$$x_3 = x_3', \qquad x_4 = x_4' \; .$$

Then on substituting these values in (31) we get

$$p_i^2(x_1'^2 + x_2'^2) - p_i D'(x_3'^2 + x_4'^2) = p_i,$$

$$(33) \qquad p_i(x_1'^2 + x_2'^2) - D'(x_3'^2 + x_4'^2) = 1.$$

If we can show the existence of solutions of (33) the transformation (32) will give the solutions of (31) and of (30).

We now make use of the work of Humbert[17] on the binary Hermitian form

$$ax\bar{x} + bx\bar{y} + \bar{b}\bar{x}y + cy\bar{y},$$

in which a and c are real, and where $\bar{x}$ denotes the conjugate of x. Humbert proves that all such forms, having the same discriminant $\mathcal{D} = b\bar{b} - ac > 0$, are equivalent. In other words, any two such forms, having the same discriminant, can be carried the one into the other, by a linear transformation on the variables. Our quaternary quadratic forms (1) and (33) are of this form with

$$a = 1, \; b = 0, \; c = -D, \; \mathcal{D} = D,$$

and

$$a = p_i, \; b = 0, \; c = -D', \; \mathcal{D} = p_i D' = D,$$

in the respective cases. The discriminants are equal and positive. Hence the two forms are equivalent. Then there exists a linear transformation of the form

$$(34) \qquad x_1' = a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + a_{14}x_4 \, ,$$

$$x_2' = a_{21}x_1 + a_{22}x_2 + a_{23}x_3 + a_{24}x_4 \, ,$$

[17] Humbert, op. cit., vol. 166, 1918, pp. 865-870.

$$x_3' = a_{31}x_1 + a_{32}x_2 + a_{33}x_3 + a_{34}x_4 ,$$

$$x_4' = a_{41}x_1 + a_{42}x_2 + a_{43}x_3 + a_{44}x_4 ,$$

whose determinant is not zero, which will carry (33) into (1). But we can determine a solution $[x_1, x_2, x_3, x_4]$ of (1). Substituting these values for x_1, x_2, x_3, and x_4, in (34) will give values x_1', x_2', x_3', and x_4' which will form a solution $[x_1', x_2', x_3', x_4']$ of (33). Hence we have proved the existence of solutions of (33) and so of (30) as desired.

Now we know that there exist solutions, $[x_1, x_2, x_3, x_4]$ and $[y_1, y_2, y_3, y_4]$, of norms p_i and p_j respectively, of the two equations

$$x_1^2 + x_2^2 - D(x_3^2 + x_4^2) = p_i,$$

$$y_1^2 + y_2^2 - D(y_3^2 + y_4^2) = p_j.$$

Then the product $[x_1, x_2, x_3, x_4]\cdot[y_1, y_2, y_3, y_4]$ according to the formula (5) is an element $[z_1, z_2, z_3, z_4]$ of norm $p_i p_j$ which satisfies the relation

$$z_1^2 + z_2^2 - D(z_3^2 + z_4^2) = p_i p_j.$$

By proceeding in this way we can show solutions of the equations

$$x_1^2 + x_2^2 - D(x_3^2 + x_4^2) = D_2 \text{ or } 2D_2,$$

where D_2 is a product of the form (24). Then this completes the proof of the following

<u>Theorem V</u>. If $D = p_1 \cdot p_2 \cdot \ldots\ldots p_r$, $r \geq 1$, $p_i \neq p_j$ for $i \neq j$, and $p_i \equiv 3 \pmod 4$, then the Fuchsian group F(D), of transformations

$$z = \frac{(x_1 + ix_2)w + D(x_3 - ix_4)}{(x_3 + ix_4)w + x_1 - ix_2},$$

of the complex plane, has exactly 3.2^r distinct classes of elliptic transformations.

6. Conclusion.

We have now completed the discussion for the case that we have chosen. We have determined the number of canonical generators for the Fuchsian group, F(D), of transformations of the complex plane, where D is subject to the restrictions of formula (11). From these generators we can determine generators of our group, G(D), of solutions of the equation (1) by the use of the correspondence (6), and by adjoining the one unit [-1,0,0,0] as mentioned previously. We may sum up our work in the form of

Theorem VI. If $D = p_1 . p_2 . \ldots\ldots p_r$, $r \geq 1$, $p_i \neq p_j$ for $i \neq j$, and p_i prime $\equiv 3 \pmod 4$, then the group G(D) of solutions in integers of the equation

$$x_1^2 + x_2^2 - D(x_3^2 + x_4^2) = 1,$$

is generated by a set of units consisting of the single unit [-1,0,0,0], and a set of m + 2h canonical generators, U_1, U_2, ... U_m, V_1, ... V_h, V_1', V_2', ... V_h', subject to the conditions

$$U_1^2 = U_2^2 = \ldots\ldots\ldots = U_m^2 = -1,$$
$$U_1 . U_2 \ldots\ldots U_m \left[\prod_{j=1}^{h} V_j^{-1} V_j' V_j V_j'^{-1} \right] = -1,$$

where

$$m = 3.2^r,$$
$$4h = \varphi(D) + 4 - m.$$

To illustrate this final result we shall refer to our illustrations of the cases D = 3, and D = 7, which fulfil the hypotheses of the theorem. On the illustrations we listed generators of the Fuchsian groups, F(D), but these are not the required canonical generators of G(D). We shall actually show these special generators and show how they are determined from the given ones.

Case -- $D = 3$.

$D = p_1 = 3$, so $r = 1$. $m = 3.2^r = 3.2 = 6$.

$4h = \varphi(D) + 4 - m = 2 + 4 - 6 = 0$, so $h = 0$.

Then we must have $m + 2h = 6$ canonical generators. By actual trial we are able to obtain these from the units given. We find them to be

$$\begin{aligned} U_1 &= A = [0,1,0,0], \\ U_2 &= C^{-1} = [0,-2,-1,0], \\ U_3 &= CE^{-1} = [0,4,2,1], \\ U_4 &= ED^{-1} = [0,5,2,2], \\ U_5 &= DB^{-1} = [0,4,1,-2], \\ U_6 &= BA^{-1} = [0,-2,0,-1]. \end{aligned}$$

Since $h = 0$ there will be no V_i's. These generators satisfy the relations of our theorem for

$$U_1^2 = U_2^2 = U_3^2 = U_4^2 = U_5^2 = U_6^2 = -1,$$

and

$$U_1 . U_2 . U_3 . U_4 . U_5 . U_6 = A.C^{-1}.CE^{-1}.ED^{-1}.DB^{-1}.BA^{-1} = -1.$$

To the canonical generators we add the unit $[-1,0,0,0]$. Hence we have the group G(D) given by

$$G(3) = \left\{ [-1,0,0,0], [0,1,0,0], [0,-2,-2,0], [0,4,2,1], \right.$$
$$\left. [0,5,2,2], [0,4,1,-2], [0,-2,0,-1] \right\}.$$

Case -- $D = 7$.

$D = p_1 = 7$, so $r = 1$. $m = 3.2^r = 3.2 = 6$.

$4h = \varphi(D) + 4 - m = 6 + 4 - 6 = 4$, so $h = 1$.

Here we have $m + 2h = 6 + 2 = 8$ canonical generators. Six of these will be elliptic and the other two hyperbolic. Again by trial we find them to be

$$
\begin{aligned}
U_1 &= G^{-1} = [0,-8,-3,0]\\
U_2 &= FE^{-1} = [0,6,2,1]\\
U_3 &= ED^{-1} = [0,6,1,2]\\
U_4 &= DC_2F^{-1}C_1^{-1} = [0,-27,-2,-10]\\
U_5 &= BA^{-1} = [0,-8,0,-3]\\
U_6 &= A = [0,1,0,0]\\
V_1 &= C_2^{-1} = [-9,-12,-4,4]\\
V_1' &= G^{-1}F = [-2,-16,-6,1]
\end{aligned}
$$

Again these canonical generators satisfy the relations of the theorem for

$$U_1^2 = U_2^2 = U_3^2 = U_4^2 = U_5^2 = U_6^2 = -1,$$

$$
\begin{aligned}
&U_1 . U_2 . U_3 . U_4 . U_5 . U_6 . V_1^{-1} . V_1' . V_1 . V_1'^{-1}\\
&\quad = G^{-1}.FE^{-1}.ED^{-1}.DC_2F^{-1}C_1^{-1}.BA^{-1}.A.C_2 .G^{-1}F.C_2^{-1}.F^{-1}G\\
&\quad = G^{-1}F\ C_2F^{-1}C_1^{-1}BC_2G^{-1}FC_2^{-1}F^{-1}G.
\end{aligned}
$$

But from the relations on the illustration we have that $C_1^{-1}B = GC_2^{-1}$, and so using this we have

$$= G^{-1}FC_2F^{-1}GC_2^{-1}C_2G^{-1}FC_2^{-1}F^{-1}G = -1.$$

To these eight canonical generators we add the single unit $[-1,0,0,0]$ and we then have the group G(D) determined as follows

$$
\begin{aligned}
G(7) = \{ &[-1,0,0,0], [0,-8,-3,0], [0,6,2,1], [0,6,1,2],\\
&[0,-8,0,-3], [0,1,0,0], [-9,-12,-4,4], [0,-27,-2,-10],\\
&[-2,-16,-6,1] \}.
\end{aligned}
$$

7. Bibliography.

1. Coolidge, J. Lowell,

   The Elements of Non-Euclidean Geometry, The Clarendon Press, Oxford, 1909.

2. Ford, Lester R.,

   Automorphic Functions, McGraw - Hill Book Company, Inc., New York, 1929.

3. Fricke, R. and Klein, F.,

   Automorphe Funktionen.

4. Hull, Ralph,

   On the Units of Indefinite Quaternion Algebras, American Journal of Mathematics, vol LXI, no. 2, April, 1939, pp. 365 - 374.

5. Humbert, G.,

   Comptes Rendus Paris, vol. 166, 1918.