THE HILBERT MODULAR GROUP, RESOLUTION OF THE SINGULARITIES AT THE CUSPS AND RELATED PROBLEMS

by F. HIRZEBRUCH

\S 1. The Hilbert modular group and the cusps.

Let k be a real quadratic field over Q and <u>o</u> the ring of algebraic integers in k. Let $x \mapsto x'$ be the non-trivial automorphism of k. The Hilbert modular group

(1)
$$SL_2(\underline{o}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \underline{o}, ad - bc = 1 \}$$

acts on H x H where H is the upper half plane of ${\mathfrak C}$:

$$\binom{a \ b}{c \ d} (z_1, z_2) = (\frac{az_1 + b}{cz_1 + d}, \frac{a'z_2 + b'}{c'z_2 + d'})$$

The group $G = SL_2(\underline{o})/\{1,-1\}$ acts effectively. For a description of a fundamental domain of G, see Siegel [13].

For any point $x \in H \times H$, the isotropy group $G_x \subset G$ is finite cyclic. The singular points of the complex space $H \times H/G$ correspond bijectively to the finitely many conjugacy classes of maximal finite cyclic subgroups in G. Their number has been determined by Prestel [12] (see also Gundlach [7]). If, for example,

 $D \equiv 1$ (4), $D \neq 0$ (3), D > 5, D square free, $k = Q(\sqrt{D})$, then there are h(-D) singular points of order 2 and h(-3D) singular points of order 3 where h(a) denotes the ideal class number of $Q(\sqrt{a})$. (Assume a to be square free.)

G acts on the projective line $k \cup \{\infty\}$ by

$$x \mapsto \frac{ax+b}{cx+d}$$
.

There are finitely many orbit classes. The elements of $(k \cup \{\infty\})/G$ are called cusps. They correspond bijectively to the ideal classes of \underline{o} . If $x = \frac{m}{n}$ (where

m, $n \in \underline{o}$) belongs to a certain orbit, then (m,n) is a corresponding ideal. We denote by C the group of ideal classes in \underline{o} . (The principal ideals represent the unit element of C.) H x H/G can be compactified by adding finitely many points, namely the cusps. The resulting space

is a compact algebraic surface (compare Gundlach [5]) with isolated singularities (the quotient singularities, as explained above, and the finitely many cusps). We wish to resolve the singularities. This is well-known for the quotient singularities (see, for example, [9] § 3.4). Object of this lecture is to do it for the cusps. For this we have to study the neighborhood of a cusp x in $\overline{H \times H/G}$ and the local ring at x .

We sometimes denote a cusp and a representing element $\frac{m}{n}$ $(m, n \in \underline{o})$ by the same symbol x. Let $G_{\chi} = \{\gamma \mid \gamma \in G, \gamma x = x\}$. We cannot, in general, transform $x = \frac{m}{n}$ to ∞ by an element of G, but it can be done by a matrix A with coefficients in k. Put $\underline{a} = (m, n)$. Then, following Siegel [13], we take

(2)
$$A = \binom{m \ u}{n \ v} \in SL_2(k)/\{1,-1\}$$

where $u, v \in \underline{a}^{-1}$ (fractional ideal) and define

Then

(4)
$$G_{\mathbf{x}}^{\infty} = \left\{ \begin{pmatrix} \varepsilon & w \\ 0 & \varepsilon^{-1} \end{pmatrix} \mid w \in \underline{\mathbf{a}}^{-2} \right\} / \left\{ 1, -1 \right\}$$

where ϵ is a unit of k ./If we agree to consider a matrix always as a projective transformation, then

(5)
$$G_{\mathbf{x}}^{\boldsymbol{\omega}} = \{ \begin{pmatrix} \varepsilon^2 & \mathbf{w} \\ 0 & \mathbf{w} \end{bmatrix} \in \text{unit}, \ \mathbf{w} \in \underline{\mathbf{a}}^{-2} \}.$$

The group U of positive units of k is infinite cyclic. Let e_0 be the generator with $e_0 > 1$. It is called the fundamental unit. Let U⁺ be the group of totally positive units, i.e.

$$\mathbf{U}^{+} = \{ \varepsilon \mid \varepsilon \in \mathbf{U}, \varepsilon > 0, \varepsilon' > 0 \}.$$

Equation (5) is a motivation to study data (M, V) where :

2) V is a subgroup $\neq \{1\}$ of the group U_{M}^{+} of totally positive units which leave M invariant under multiplication (as is well-known $U_{M}^{+} \neq \{1\}$).

Given the data (6) we have a group

(7)
$$\left\{ \begin{pmatrix} \varepsilon & w \\ 0 & 1 \end{pmatrix} \mid \varepsilon \in \mathbb{V} , w \in \mathbb{M} \right\}.$$

In analogy to (4) such groups occur for cusps which are singular points of the compactified orbit spaces F of more general discontinuous groups acting on H × H (subgroups of finite index of certain finite extensions of G). In (4) we have $M = \underline{a}^{-2}$ and $V = U^2$ and $U_M^+ = U^+$.

Data (M,V) as in (6) determine a torus bundle X over the circle :

(8)
$$V \simeq \pi_1(s^1)$$
, $(M \otimes_3 R)/M = Torus$

 $\pi_1(S^1)$ acts on the torus. X is associated to the universal cover of S^1 . The following proposition seems to be well-known. I know it from J.-P. Serre. It follows, for example, from the information given in [5].

PROPOSITION.- If a cusp with data (M,V) is singular point of an algebraic surface F (see above), then its neighborhood boundary is the torus bundle X defined by (8). (For "neighborhood boundary" see, for example, [10].)

The local ring for a cusp (M,V) was described by Gundlach [5]. Let $M^{\circ} \subset R^{2}$ be the Z-module of all $x \in R^{2}$ such that

(9)
$$x_1 w + x_2 w' \in \mathbf{Z}$$
 for all $w \in M$.

 M° has rank 2. We have by (9) a bilinear pairing B: $M^{\circ} \times M \rightarrow Z$.

V acts on B such that $B(\epsilon x, w) = B(x, \epsilon w)$ for $\epsilon \in V$, $x \in M^{\circ}$, $w \in M$.

PROPOSITION.- The local ring for the cusp (M,V) consists of all "convergent" Fourier series

(10)
$$f(z_1, z_2) = \sum_{x \in M^0} a_x e^{2 \pi i (x_1 z_1 + x_2 z_2)}$$

where $a_x \neq 0$ only if both $x_1 > 0$ and $x_2 > 0$ or x = 0, and where $a_{\varepsilon x} = a_x$ for $\varepsilon \in V$. "Convergent" means that f converges for $Im(z_1) \cdot Im(z_2) > c$ where c is a constant depending on f.

§ 2. Binary indefinite quadratic forms.

Let M be a 2-module of rank 2 contained in k. The function (11) $w \mapsto ww' = N(w)$ (norm of w)

is a quadratic form $M \to \mathbb{Q}$ which is indefinite and does not represent 0. We orient M by the basis (β_1, β_2) of M with $\beta_1 \beta_2' - \beta_2 \beta_1' > 0$.

We now study oriented 2-modules M of rank 2 and quadratic forms

 $f: M \rightarrow Q$

which are indefinite and do not represent 0 . No specific field k is given.

We call (M_1, f_1) and (M_2, f_2) equivalent if there exists an isomorphism $M_1 \rightarrow M_2$ of <u>oriented</u> 2-modules which carries f_1 in tf_2 where t is a <u>positive</u> rational number.

Every (M,f) is equivalent to a quadratic form

g:2×2 → 2

where $\mathbf{Z} \times \mathbf{Z}$ is canonically oriented and such that for $(u,v) \in \mathbf{Z} \times \mathbf{Z}$

(12)
$$g(u,v) = au^2 + buv + cv^2$$

with (a,b,c) = 1. Then $b^2 - 4ac$ is called the <u>discriminant of</u> f. It depends only on the equivalence class of f and is a positive integer which is not a perfect square. The real number

$$r_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}$$
, where $\sqrt{b^2 - 4ac} > 0$,

is called the first root of g.

We take the unique continued fraction

$$r_1 = a_1 - \frac{1}{a_2} - \frac{1}{a_3} - \frac{1}{a_4} - \frac{1}$$

where $a_j \in \mathbb{Z}$ and $a_j \ge 2$ for $j \ge 1$. A continued fraction will be denoted by $[a_1, a_2, a_3, \ldots]$. Since r_1 is a quadratic irrationality its continued fraction is periodic from a certain point on. Let (b_1, \ldots, b_p) be its primitive period $(b_j \ge 2)$. Observe that the period (2) cannot occur because $[2, 2, \ldots] = 1$ is rational.

A sequence of integers (b_1, \ldots, b_p) with $b_j \ge 2$ is called a period of length p, two periods are equivalent if they can be obtained from each other by a cyclic permutation. Such an equivalence class is called a cycle. A cycle is primitive if it is not obtainable from another cycle by an "unramified covering" of degree > 1. Cycles are denoted by $((b_1, \ldots, b_p))$. Thus ((2,3)) is primitive, but ((2,3,2,3)) is not. $((b_1, \ldots, b_p))^m$ means the m-fold cover of $((b_1, \ldots, b_p))$. For example $((2,5))^3 = ((2,5,2,5,2,5))$.

THEOREM.- The primitive cycle of the first root depends only on the equivalence class of (M,f). If we associate to each (M,f) this primitive cycle, we obtain a bijective map from the set of equivalence classes of quadratic forms (M,f) to the set of all primitive cycles (where ((2)) is excluded).

This theorem is a suitable modification of classical results. It is related to Gauss' reduction theory of quadratic forms [3]. The continued fractions had to be modified also, but all relevant theorems in Perron [11] can be taken over. To simplify notations we shall indicate a cycle by

where s_j is the number of two's occuring in the corresponding position and where $t_j \ge 3$. For example,

$$((2,2,2,2,3,3,2,5)) = |4,3|0,3|1,5|$$

Let k be a real quadratic field over Q and d its discriminant; it is the discriminant of the quadratic form (11) defined over the module $\underline{o} \subset k$. If a > 0 (square free) and $k = Q(\sqrt{a})$, then

$$d = 4a \qquad \text{if } a \equiv 2,3 \mod 4$$
$$d = a \qquad \text{if } a \equiv 1 \mod 4.$$

Let C be as before the group of ideal classes of <u>o</u> and C⁺ the group of ideal classes with respect to strict equivalence (for which an ideal is equivalent 1 if it is principal with a totally positive generator). We have $|C^+|: |C| = 2$ or 1 depending on whether the fundamental unit e_0 is totally positive or not. The order of C is the class number h(a) for $k = Q(\sqrt{a})$. If the discriminant of k is d, then C⁺ is via (11) in one-to-one correspondence with the set of equivalence classes of quadratic forms (M,f) with discriminant d.

Don Zagier (Bonn) has written a computer program which puts out (the finitely many) primitive cycles for a given discriminant. For d = 257 the primitive cycles are

a) |0,3|14,3|0,17|

c) |0,5| 6,3|2, 9| .

For d = 4.79 the primitive cycles are

I | 0,18|0,9|

II |15, 3|6,3|

III | 2, 7|0,3|0,4|

IV | 1, 5|4,3|0,3|

V | 1, 3|0,3|4,5|

VI | 2, 4|0,3|0,7| .

For $k = Q(\sqrt{257})$ the fundamental unit is not totally positive, the class number h(257) equals 3. For $k = Q(\sqrt{79})$ the fundamental unit is totally positive, the class number h(79) equals 3. The order of C⁺ is 6. The 6 quadratic forms for d = 4.79 are listed by Gauss [3] Art. 187 and numbered from I to VI corresponding to our table above.

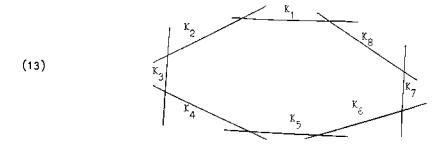
The discriminant d = 20, for example, is not the discriminant of a field k. There is one primitive cycle namely |3,6| which belongs to the module $2\sqrt{5} \oplus 2^{\cdot 1}$ contained in $Q(\sqrt{5})$ and the quadratic form defined on it by (11).

§ 3. Resolution of the cusps.

An isolated singular point x of a complex space of complex dimension 2 admits a resolution by which x is blown up into a system of non-singular curves K_j . For each K_j we have the genus $g(K_j)$ and the self-intersection number $K_j \circ K_j$.

The resolution is minimal (and then uniquely determined) if there is no K_j with $g(K_j) = 0$ and $K_j \circ K_j = -1$. The matrix $(K_i \circ K_j)$ is negative-definite (compare [10]).

The resolution is called <u>cyclic</u> if all $g(K_j)$ are zero (i.e. all curves are rational) and if j can be assumed to run through the residue classes mod q (q \geq 3) such that $K_{j+1} \circ K_j = K_j \circ K_{j+1}^{\bullet} = 1$ for all $j \in \mathbb{Z}/q\mathbb{Z}$ (transversal intersection) and $K_r \circ K_s = 0$ for $r - s \neq 0, 1, -1$. Example (q = 8):



The following result is a consequence of a theorem in § 4.

THEOREM.- <u>A cusp</u> (M,V), see (6), <u>admits a cyclic resolution</u>. M determines by (11) <u>and the theorem in § 2 a primitive cycle</u> $c = ((b_1, \dots, b_p))$. <u>Put</u> $m = [U_M^+: V]$. <u>Then</u> q = pm <u>and</u>

$$((-\kappa_1 \circ \kappa_1, \ldots, -\kappa_q \circ \kappa_q)) = c^m$$
.

(Exceptional cases pm = 1 or $2 \cdot If c^m = ((b))$ or $((b_1, b_2))$ we have a cycle of 3 curves with self-intersection numbers -(b+3), -2, -1 or $-(b_1+1), -1, -(b_2+1)$ respectively.)

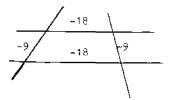
The cyclic resolution is the minimal one with these exceptions which can be blown down to minimal ones looking like this :

$$\rho \quad \times \times$$

<u>Examples</u>.- For $k = \mathbb{Q}(\sqrt{a})$ with $a \ge 1$ (square free) and G as in § 1 we have h(a) cusps (h(a) = order of the ideal class group C, see § 2). Each cusp has the Z-module \underline{a}^{-2} where the ideal \underline{a} represents an element of C. If \underline{a} and \underline{b} give the same element in C, then the Z-modules \underline{a}^{-2} and \underline{b}^{-2} are obtainable from each other by multiplication with a totally positive number and (as fractional ideals) represent the same element of C⁺. Thus we have a homomorphism

$$\rho: C \rightarrow C^+$$
.

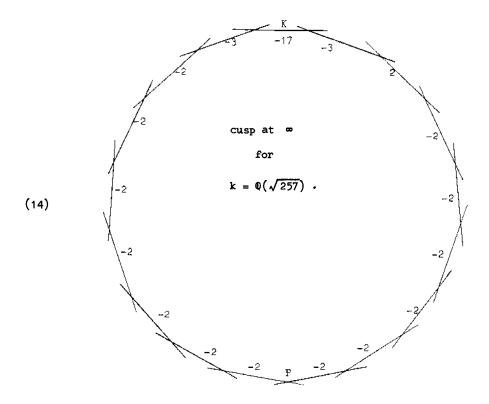
The resolution of a cusp $x \in C$ is given by the equivalence class of the quadratic form belonging to $\rho(x)$ or rather by its corresponding primitive cycle c (§ 2). The cycle of the resolution is c^{m} where m = 2 if the fundamental unit e_{o} of k is totally positive, otherwise m = 1. For $k = Q(\sqrt{79})$ and G as in § 1, we have three cusps. We have to analyze what are the squares in C^{+} and their periods. In the list of § 2 the squares are I, IV, V. The cusps IV, V give the same singularity (the periods are just reversed). They go over into each other by the permutation σ of the factors of $H \times H$ (which leaves the cusp I invariant). The resolution of the cusp I looks like :



where we have indicated the self-intersection numbers. The (minimal) resolution of IV has 16 curves.

For $k = \mathbb{Q}(\sqrt{257})$ we have $C = C^+$ and m = 1. The resolutions of the three cusps are given by the primitive cycles written down in § 2.

The permutation σ on H x H carries the cusp b) into the cusp c) whereas on the cusp a) it carries the curve K with self-intersection number -17 into itself, has the intersection point P of two curves of self-intersection number -2 as fixed point



and otherwise interchanges the curves according to the symmetry of the continued fraction of a quadratic irrationality w, which is equivalent to -w' under $SL_2(\mathbf{Z})$ (Theorem of Galois, see [11] § 23). The corresponding singularity of $(\overline{H \times H/G})/\sigma$ is a quotient singularity admitting a "linear resolution"



(compare [9] § 3.4)

obtained by "dividing" the diagram (14) by σ and using that curves of selfintersection number -1 can be "blown down".

284

§ 4. Construction of cyclic singularities.

Let b_1, b_2, \dots, b_q $(q \ge 3)$ be a sequence of integers ≥ 2 not all equal 2. For q = 3 also sequences (a + 3, 2, 1) and $(a_1 + 1, 1, a_2 + 1)$ with $a \ge 3$ and $a_1 \ge 3$ or $a_2 \ge 3$ are admitted. Let j run through 2/q2. Consider the matrix (c_{rs}) , where $r, s \in 2/q2$, with

 $c_{j+1,j} = c_{j,j+1} = 1$, $c_{jj} = -b_j$, $c_{rs} = 0$ otherwise.

LEMMA.- Under the preceding assumptions the matrix (c_{rs}) is negative-definite.

Let k run through the integers and define b_k to be equal to b_j above if $k \equiv j \mod q$. We now do a construction as in [9] § 3.4. For each k take a copy R_k of C^2 with coordinates u_k , v_k . We define R_k' to be the complement of the line $u_k = 0$ and R_k'' to be the complement of the line $v_k = 0$.

The equations

$$u_{k} = u_{k-1}^{D_{k}} v_{k-1}$$
$$v_{k} = 1/u_{k-1}$$

give a biholomorphic map $\varphi_{k-1} : \mathbb{R}'_{k-1} \to \mathbb{R}''_k$. If we make in the disjoint union $\bigcup \mathbb{R}_k$ the identifications given by the φ_{k-1} we get a complex manifold Y in which we have a string of compact rational curves S_k non-singularly imbedded. S_k is given by $u_k = 0$ "in the k-th coordinate system" and by $v_{k-1} = 0$ in the (k-1)-th coordinate system. S_k , S_{k+1} intersect in just one point transversally. S_i , S_k (i < k) do not intersect, if $k-i \neq 1$. The self-intersection number $S_k \circ S_k$ equals $-b_k$. The complex manifold Y admits a biholomorphic map T : $Y \to Y$ which sends a point with coordinates u_k, v_k in the k-th coordinate system, thus $T(S_k) = S_{k+q}$. The main point is the existence of a tubular neighborhood Y^0 of $\bigcup S_k$ on which the infinite cyclic group $Z = \{T^n \mid n \in Z\}$ operates freely such that Y^0/Z is a complex manifold in which q rational curves $K_1 \cup \ldots \cup K_q = \bigcup S_k'/Z$ are embedded. Their intersection behaviour is given by the negative-definite matrix c_{rs} (see Lemma).

According to Grauert [4] the curves $K_1 \cup \ldots \cup K_q$ can be blown down to a singular point x in a complex space where x has by construction a cyclic resolution as defined in § 3.

THEOREM.- Let $\beta = [b_1, \dots, b_q, b_1, \dots, b_q, \dots]$. Then $M = \mathbf{Z}\beta \oplus \mathbf{Z} \cdot 1$ is a Z-module contained in $k = \mathbf{Q}(\beta)$. Suppose $((b_1, \dots, b_q))$ is the m-th power of a primitive cycle. Then the local ring at the singular point x constructed above is isomorphic to the local ring described in the second proposition of § 1 provided $[U_M^+: V] = m$.

The proof will be published elsewhere.

§ 5. Applications.

The resolution of the cusps can be used to calculate certain numerical invariants of $H \times H/G$, $(H \times H/G)/\sigma$, for example, where σ : $H \times H \rightarrow H \times H$ is the permutation of the factors as before. We have to use a result of Harder [8]. Compare the lecture of Serre in this Seminar. We mention two cases.

1. For a cusp x = (M, V) with a resolution as in the theorem of § 3 we put

$$\varphi(\mathbf{x}) = \frac{1}{3} \left(\sum_{j=1}^{q} K_{j} \circ K_{j} \right) + q$$

The number $\varphi(\mathbf{x})$ is essentially the value at 1 of a certain L-function. $\varphi(\mathbf{x})$ vanishes if the quadratic form f on M (see (11)) is equivalent to -f (under an automorphism of M which need not be orientation preserving).

THEOREM.- Suppose a > 6, square free, $a \neq 0$ (3). Put $k = Q(\sqrt{a})$. Using the notation of § 1 we have :

The signature of the (non-compact) rational homology manifold H \times H/G equals $\sum_{x \in C} \phi(x)$.

2. For a prime $p \equiv 1 \mod 4$ we shall calculate the arithmetic genus \hat{x}_p of the non singular model of the compact algebraic surface $(\overline{H \times H/G})/\sigma$ for $k = Q(\sqrt{p})$. Information on the fixed points (see § 1) is needed. The following result is closely related to theorems of Freitag [2] and Busam [1], see in particular [1] § 7.

THEOREM.- Let p be a prime = 1 mod 4 and p > 5. Put $k = Q(\sqrt{p})$. The arithmetic genus \hat{x}_p is given by

$$48 \hat{\chi}_{p} = 12 \zeta_{k}(-1) + 3h(-p) + 4h(-3p) - p + 8\varepsilon + 12 \delta + 29$$

where $\varepsilon = 1$ for $p \equiv 1 \mod 3$, $\varepsilon = 0$ for $p \equiv 2 \mod 3$, $\delta = 1$ for
 $p \equiv 1 \mod 8$, $\delta = 0$ for $p \equiv 5 \mod 8$. (ζ_{k} is the Zeta-function of the
field k.)

For $\zeta_k(-1)$ we have the following formula [14]

$$\zeta_{k}(-1) = \frac{1}{30} \sum_{\substack{b \text{ odd} \\ 1 \leq b < \sqrt{p}}} \sigma_{1} \left(\frac{p - b^{2}}{4} \right) ,$$

where $\sigma_1(n)$ is the sum of the divisors of n .

By calculations of R. Lundquist, Don Zagier and myself there are exactly 24 primes = 1 mod 4 for which the arithmetic genus equals 1, namely all such primes smaller than the prime 193 and 197, 229, 269, 293, 317. For p = 5the surface $(\overline{H \times H/G})/\sigma$ is rational (Gundlach [6]). Which of the 23 others are rational ?

<u>Final joke</u> : At the end of my dissertation [9] I claim that there are no cycles in a resolution. This is nonsense, as I know for a long time, and as this talk proves, I hope.

REFERENCES

- R. BUSAM <u>Eine Verallgemeinerung gewisser Dimensionsformeln von Shimizu</u>, Inventiones math., <u>11</u>, 110-149 (1970).
- [2] E. FREITAG Die Struktur der Funktionenkörper zu Hilbertschen Modulgruppen (Habilitationsschrift, Heildelberg 1969).
- [3] C. F. GAUSS Untersuchungen über höhere Arithmetik (Disquisitiones Arithmeticae), deutsch herausgegeben von H. Maser 1889, reprinted Chelsea 1965.
- [4] H. GRAUERT Über Modifikationen und exzeptionelle analytische Mengen, Math. Ann. 146, 331-368 (1962).
- K.-B. GUNDLACH Some new results in the theory of Hilbert's modular group, Contributions to function theory, International Colloquium Bombay 1960, p. 165-180.
- [6] K.-B. GUNDLACH Die Bestimmung der Funktionen zur Hilbertschen Moldulgruppe des Zahlkörpers $Q(\sqrt{5})$, Math. Ann. 152, 226-256 (1963).
- [7] K.-B. GUNDLACH Die Fixpunkte einiger Hilbertschen Modulgruppen, Math. Ann. 157, 369-390 (1965).
- [8] G. HARDER Gauss-Bonnet formula for arithmetically defined groups, Ann. Sc.
 E.N.S., Paris, t. 4, 1971, fasc. 3, p. 409-455.
- [9] F. HIRZEBRUCH Über vierdimensionale Riemannsche Flächen mehrdeutiger analytischer Funktionen von zwei komplexen Veränderlichen, Math. Ann. 126, 1-22 (1953).
- [10] F. HIRZEBRUCH The topology of normal singularities of an algebraic surface (d'après Mumford), Séminaire Bourbaki, 1962/63, nº 250, W.A. Benjamin, Inc., 1966.
- [11] O. PERRON Die Lehre von den Kettenbruchen, B. G. Teubner, Leipzig und Berlin, 1913.
- [12] A. PRESTEL Die elliptischen Fixpunkte der Hilbertschen Modulgruppen, Math. Ann. 177, 181-209 (1968).
- [13] C. L. SIEGEL Lectures on advanced analytic number theory, Tata Institute Bombay 1961 (reissued 1965).
- [14] C. L. SIEGEL Berechnung von Zetafunktionen an ganzzahligen Stellen, Göttinger Nachrichten <u>10</u>, 87-102 (1969).