# SÉminaire N. Bourbaki 

# F. Hirzebruch <br> The Hilbert modular group, resolution of the singularities at the cusps and related problems 

Séminaire N. Bourbaki, 1971, exp. n ${ }^{\circ}$ 396, p. 275-288
[http://www.numdam.org/item?id=SB_1970-1971__13__275_0](http://www.numdam.org/item?id=SB_1970-1971__13__275_0)
© Association des collaborateurs de Nicolas Bourbaki, 1971, tous droits réservés.
L'accès aux archives du séminaire Bourbaki (http://www.bourbaki. ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

## Numdam

## THE HILBERT MODULAR GROUP, RESOLUTION OF

## THE SINGULARITIES AT THE CUSPS AND RELATED PROBLEMS

by F. HIRZEBRUCH
§ 1. The Hilbert modular group and the cusps.
Let $k$ be a real quadratic field over Q and o the ring of algebraic integers in $k$. Let $x \mapsto x^{\prime}$ be the non-trivial automorphism of $k$. The Hilbert modular group

$$
\mathrm{SL}_{2}(\underline{o})=\left\{\left.\left(\begin{array}{ll}
a & b  \tag{1}\\
c & d
\end{array}\right) \right\rvert\, a, b, c, d \in \underline{o}, a d-b c=1\right\}
$$

acts on $H \times H$ where $H$ is the upper half plane of $C$ :

$$
\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right)\left(z_{1}, z_{2}\right)=\left(\frac{a z_{1}+b}{c z_{1}+d}, \frac{a^{\prime} z_{2}+b^{\prime}}{c^{\prime} z_{2}+d^{\prime}}\right) .
$$

The group $\mathrm{G}=\mathrm{SL}_{2}(\underline{0}) /\{1,-1\}$ 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 $G \subset \subset$ 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,

$$
D \equiv 1(4), \quad D \neq 0(3), \quad D>5, \quad D \text { square free, } k=Q(\sqrt{D}) \text {, }
$$

then there are $h(-D)$ singular points of order 2 and $h(-3 D)$ singular points of order 3 where $h(a)$ denotes the ideal class number of $(\sqrt{a})$. (Assume a to be square free.)
$G$ acts on the projective line $k \cup\{\infty\}$ by

$$
x \mapsto \frac{a x+b}{c x+d}
$$

There are finitely many orbit classes. The elements of $(k \cup\{\infty\}) / G$ are called cusps. They correspond bijectively to the ideal classes of ㅇ. If $x=\frac{m}{n}$ (where
$m, n \in O$ ) belongs to a certain orbit, then ( $m, n$ ) is a corresponding ideal. We denote by $C$ the group of ideal classes in ㅇ. (The principal ideals represent the unit element of $C$.) $H \times H / G$ can be compactified by adding finitely many points, namely the cusps. The resulting space

$$
\overline{\mathrm{H} \times \mathrm{H} / \mathrm{G}}=(\mathrm{H} \times \mathrm{H} / \mathrm{G}) \cup \mathrm{C}
$$

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 $G_{x}=\{\gamma \mid \gamma \in G, \gamma x=x\}$. We cannot, in general, transform $x=\frac{m}{n}$ to $\infty$ 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

$$
A=\left(\begin{array}{ll}
m & u  \tag{2}\\
n & v
\end{array}\right) \in \operatorname{SL}_{2}(k) /\{1,-1\}
$$

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

$$
\begin{equation*}
G_{x}^{\infty}=A^{-1} G_{x} A . \tag{3}
\end{equation*}
$$

Then

$$
G_{x}^{\infty}=\left\{\left.\left(\begin{array}{cc}
\varepsilon & w  \tag{4}\\
0 & \varepsilon^{-1}
\end{array}\right) \right\rvert\, w \in \underline{a}^{-2}\right\} /\{1,-1\}
$$

where $\varepsilon$ is a unit of $k$. .'If we agree to consider a matrix always as a projective transformation, then

$$
G_{x}^{\infty}=\left\{\left.\left(\begin{array}{cc}
\varepsilon^{2} & w  \tag{5}\\
0 & 1
\end{array}\right) \right\rvert\, \varepsilon \text { unit, } w \in \underline{a}^{-2}\right\} .
$$

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

$$
U^{+}=\left\{\varepsilon \mid \varepsilon \in U, \varepsilon>0, \varepsilon^{\prime}>0\right\} .
$$

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

1) $M$ is a $Z$-module of rank 2 contained in $k$;
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 $\left.\mathrm{U}_{\mathrm{M}}^{+} \neq\{1\}\right)$.

Given the data (6) we have a group

$$
\left\{\left.\left(\begin{array}{ll}
\varepsilon & \mathrm{w}  \tag{7}\\
0 & 1
\end{array}\right) \right\rvert\, \varepsilon \in \mathrm{V}, \mathrm{w} \in \mathrm{M}\right\}
$$

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 $H \times H$ (subgroups of finite index of certain finite extensions of $G$ ). In (4) we have $M=a^{-2}$ and $V=U^{2}$ and $U_{M}^{+}=U^{+}$.

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

$$
\begin{equation*}
V \simeq \pi_{1}\left(s^{1}\right), \quad\left(M \otimes_{2} R\right) / M=\text { Torus } \tag{8}
\end{equation*}
$$

$\pi_{1}\left(s^{1}\right)$ 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 sur-
face $F$ (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 $M^{0} \subset R^{2}$ be the $Z$-module of all $x \in R^{2}$ such that

$$
\begin{equation*}
x_{1} w+x_{2} w^{\prime} \in \mathbf{z} \quad \text { for all } w \in M \tag{9}
\end{equation*}
$$

$\mathrm{M}^{\circ}$ has rank 2 . We have by (9) a bilinear pairing

$$
B: M^{\circ} \times M \quad \rightarrow \quad \mathrm{Z}
$$

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

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

$$
\begin{equation*}
f\left(z_{1}, z_{2}\right)=\sum_{x \in \mathbf{M}^{0}} a_{x} e^{2 \pi i\left(x_{1} z_{1}+x_{2} z_{2}\right)} \tag{10}
\end{equation*}
$$

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 $\operatorname{Im}\left(z_{1}\right) \cdot \operatorname{Im}\left(z_{2}\right)>c$ where c is a constant depending on $f$.
§ 2. Binary indefinite quadratic forms.

Let $M$ be a $\mathbf{Z}$-module of rank 2 contained in $k$. The function

$$
\begin{equation*}
\left.w \longmapsto w w^{\prime}=N(w) \quad \text { (norm of } w\right) \tag{11}
\end{equation*}
$$

is a quadratic form $M \rightarrow$ (Q wich is indefinite and does not represent 0 . We orient $M$ by the basis $\left(\beta_{1}, \beta_{2}\right)$ of $M$ with $\beta_{1} \beta_{2}{ }^{\prime}-\beta_{2} \beta_{1}^{\prime}>0$.

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

$$
f: M \rightarrow \mathbb{Q}
$$

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

We call $\left(M_{1}, f_{1}\right)$ and $\left(M_{2}, f_{2}\right)$ equivalent if there exists an isomorphism $M_{1} \rightarrow M_{2}$ of oriented Z-modules which carries $f_{1}$ in $t f_{2}$ where $t$ is a positive rational number.

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

$$
\mathrm{g}: \mathbf{Z} \times \mathbf{Z} \rightarrow \mathbf{Z}
$$

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

$$
\begin{equation*}
g(u, v)=a u^{2}+b u v+c v^{2} \tag{12}
\end{equation*}
$$

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

$$
r_{1}=\frac{-b+\sqrt{b^{2}-4 a c}}{2 a}, \quad \text { where } \sqrt{b^{2}-4 a c}>0
$$

is called the first root of $g$.

We take the unique continued fraction

$$
r_{1}=a_{1}-\frac{1}{a_{2}}-\frac{1}{a_{3}}-\frac{1}{a_{4}}-
$$

where $a_{j} \in \mathbb{Z}$ and $a_{j} \geq 2$ for $j>1$. A continued fraction will be denoted by $\left[a_{1}, a_{2}, a_{3}, \ldots\right]$. Since $r_{1}$ is a quadratic irrationality its continued fraction is periodic from a certain point on. Let $\left(b_{1}, \ldots, b_{p}\right)$ be its primitive period $\left(b_{j} \geq 2\right)$. Observe that the period (2) cannot occur because $[2,2, \ldots]=1$ is rational.

A sequence of integers $\left(b_{1}, \ldots, b_{p}\right)$ with $b_{j} \geq 2$ 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 $\left(\left(b_{1}, \ldots, b_{p}\right)\right)$. Thus $((2,3))$ is primitive, but $((2,3,2,3))$ is not. $\left(\left(b_{1}, \ldots, b_{p}\right)\right)^{m}$ means the m-fold cover of $\left(\left(b_{1}, \ldots, b_{p}\right)\right)$. 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

$$
\left|s_{1}, t_{1}\right| s_{2}, t_{2}\left|s_{3}, t_{3}\right| \ldots,
$$

where $s_{j}$ is the number of two's occuring in the corresponding position and where $t_{j} \geq 3$. 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 $o \subset k$. If $a>0$ (square free) and $k=\mathbf{Q}(\sqrt{a})$, then

$$
\begin{array}{ll}
d=4 a & \text { if } a \equiv 2,3 \bmod 4 \\
d=a & \text { if } a \equiv 1 \quad \bmod 4 .
\end{array}
$$

Let $C$ be as before the group of ideal classes of $ㅇ$ 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 $\left|C^{+}\right|:|C|=2$ or 1 depending on whether the fundamental unit $e_{o}$ is totally positive or not. The order of $C$ is the class number $h(a)$ for $k=\mathbb{Q}(\sqrt{a})$. 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 discri$\operatorname{minant} d$.

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) $\quad|0,3| 14,3|0,17|$
b) $\quad|2,3| 6,5|0,9|$
c) $\quad|0,5| 6,3|2,9|$.

For $d=4.79$ the primitive cycles are
$|0,18| 0,9 \mid$
II
$|15,3| 6,3 \mid$
III
| 2, 7|0,3|0,4|
IV
$|1,5| 4,3|0,3|$
$v \quad|1,3| 0,3|4,5|$
VI
$|2,4| 0,3|0,7|$.

For $k=\mathbb{Q}(\sqrt{257})$ the fundamental unit is not totally positive, the class number $h(257)$ equals 3 . For $k=(\sqrt{79})$ the fundamental unit is totally positive, the class number $h(79)$ equals 3 . The order of $C^{+}$is 6 . The 6 quadratic forms for $d=4 \cdot 79$ are listed by Gauss [3] Art. 187 and numbered from I to VI corresponding to our table above.

The discriminant $\mathrm{d}=20$, for example, is not the discriminant of a field $k$. There is one primitive cycle namely $|3,6|$ which belongs to the module $\mathbf{z} \sqrt{5} \oplus \mathrm{z} \cdot 1$ contained in $\mathbb{Q}(\sqrt{5})$ 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 $g\left(K_{j}\right)$ and the self-intersection number $K_{j}$ 。 $K_{j}$ 。

The resolution is minimal (and then uniquely determined) if there is no $K_{j}$ with $g\left(K_{j}\right)=0$ and $K_{j} \circ K_{j}=-1$. The matrix $\left(K_{i} \circ K_{j}\right)$ is negative-definite (compare [10]).

The resolution is called cyclic if all $g\left(K_{j}\right)$ are zero (i.e. all curves are rational) and if $j$ can be assumed to run through the residue classes $\bmod q(q \geq 3)$ such that $K_{j+1} \circ K_{j}=K_{j} \circ K_{j+1}^{\bullet}=1$ for all $j \in \mathbf{Z} / q \mathbf{Z}$ (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 $\oint 4$.

THEOREM.- A cusp $(M, V)$, see (6), admits a cyclic resolution. $M$ determines by (11) and the theorem in $\S 2$ a primitive cycle $c=\left(\left(b_{1}, \ldots, b_{p}\right)\right)$. Put $m=\left[U_{M}^{+}: V\right]$. Then $q=p m$ and

$$
\left(\left(-K_{1} \circ K_{1}, \ldots,-K_{q} \circ K_{q}\right)\right)=c^{m}
$$

(Exceptional cases $p m=1$ or 2 . If $c^{m}=((b))$ or $\left(\left(b_{1}, b_{2}\right)\right)$ we have a cycle of 3 curves with self-intersection numbers $-(b+3),-2,-1$ or $-\left(b_{1}+1\right),-1,-\left(b_{2}+1\right)$ respectively. $)$

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


Examples.- For $k=\mathbb{Q}(\sqrt{a})$ with $a>1$ (square free) and $G$ as in $\S 1$ we have $h(a)$ cusps $(h(a)=$ order of the ideal class group $C$, see § 2). Each cusp has the $\mathbf{z}$-module $\underline{a}^{-2}$ where the ideal $\underline{a}$ represents an element of $\mathbf{C}$. If $\underline{a}$ and $\underline{b}$ give the same element in $C$, then the $\mathbf{z}$-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 $\mathrm{C}^{+}$. Thus we have a homomor-
phism

$$
\rho: C \quad \rightarrow \quad C^{+} .
$$

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 $k=\mathbb{Q}(\sqrt{79})$ and $G$ as in § 1 , we have three cusps. We have to analyze what are the squares in $\mathrm{C}^{+}$and their periods. In the list of $\S 2$ 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 $\sigma$ 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 $\sigma$ on $H \times H$ carries the cusp $b$ ) into the cusp c) whereas on the cusp a) it carries the curve $K$ with self-intersection number $\mathbf{- 1 7}$
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 $\mathrm{SL}_{2}(\mathbf{Z})$ (Theorem of Galois, see [11] § 23). The corresponding singularity of $(\overline{\mathrm{H} \times \mathrm{H} / \mathrm{G}}) / \sigma \quad$ is a quotient singularity admitting a "linear resolution"

obtained by "dividing" the diagram (14) by $\sigma$ and using that curves of selfintersection number -1 can be "blown down".
§ 4. Construction of cyclic singularities.
Let $b_{1}, b_{2}, \ldots, b_{q}(q \geq 3)$ be a sequence of integers $\geq 2$ not all equal 2 . For $q=3$ also sequences $(a+3,2,1)$ and $\left(a_{1}+1,1, a_{2}+1\right)$ with $a \geq 3$ and $a_{1} \geq 3$ or $a_{2} \geq 3$ are admitted. Let $j$ run through $\mathbf{Z} / q \mathbf{Z}$. Consider the matrix ( $c_{r s}$ ), where $r, s \in \mathbf{Z} / q \mathbf{Z}$, with

$$
c_{j+1, j}=c_{j, j+1}=1, \quad c_{j j}=-b_{j}, \quad c_{r s}=0 \quad \text { otherwise }
$$

LEMMA.- Under the preceding assumptions the matrix $\left(c_{r s}\right)$ is negative-definite.
Let $k$ run through the integers and define $b_{k}$ to be equal to $b_{j}$ above if $k \equiv j \bmod q$. 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 $R_{k}^{\prime}$ to be the complement of the line $u_{k}=0$ and $R_{k}^{\prime \prime}$ to be the complement of the line $v_{k}=0$.

The equations

$$
\begin{aligned}
u_{k} & =u_{k-1}^{b_{k}} v_{k-1} \\
v_{k} & =1 / u_{k-1}
\end{aligned}
$$

give a biholomorphic map $\varphi_{k-1}: R_{k-1}^{\prime} \rightarrow R_{k}^{\prime \prime}$. If we make in the disjoint union $U R_{k}$ the identifications given by the $\varphi_{k-1}$ 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 $S_{k}$ o $S_{k}$ equals $-b_{k}$. The complex manifold $Y$ admits a biholomorphic map $T: Y \rightarrow Y$ which sends a point with coordinates $u_{k}, v_{k}$ in the $k-t h$ coordinate system to the point with the same coordinates in the $(k+q)$-th coordinate system, thus $T\left(S_{k}\right)=S_{k+q}$. The main point is the existence of a tubular neighborhood $Y^{0}$ of $U S_{k}$ on which the infinite cyclic group $Z=\left\{\mathrm{T}^{n} \mid \mathrm{n} \in \mathrm{Z}\right\}$ operates freely such that $Y^{\circ} / Z$ is a complex manifold in which $q$ rational curves
$K_{1} \cup \ldots U K_{q}=U S_{k} / Z$ are embedded. Their intersection behaviour is given by
the negative-definite matrix $c_{r s}$ (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 $\S 3$.

THEOREM.- Let $B=\left[\mathrm{b}_{1}, \ldots, \mathrm{~b}_{\mathrm{q}}, \mathrm{b}_{1}, \ldots, \mathrm{~b}_{\mathrm{q}}, \ldots\right]$. Then $\mathrm{M}=\mathrm{ZB} \oplus \mathrm{Z} \cdot 1$ is a z -module contained in $k=\mathbb{Q}(\beta)$. Suppose $\left(\left(b_{1}, \ldots, b_{q}\right)\right)$ 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 $\S 1$ provided $\left[U_{M}^{+}: V\right]=m$.

The proof will be published elsewhere.

## § 5. Applications.

The resolution of the cusps can be used to calculate certain numerical invariants of $H \times H / G,(\overline{H \times H / G}) / \sigma$, for example, where $\sigma: H \times H \rightarrow H \times H$ 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 $\S 3$ we put

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

The number $\varphi(x)$ is essentially the value at 1 of a certain L-function. $\varphi(x)$ 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 $k=\Phi(\sqrt{a}) \cdot$ Using the notation of $\S 1$ we have :

The signature of the (non-compact) rational homology manifold $\mathrm{H} \times \mathrm{H} / \mathrm{G}$
equals $\sum_{x \in C} \varphi(x)$.
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 $\equiv 1 \bmod 4$ and $\mathrm{p}>5$. Put $k=\mathbb{Q}(\sqrt{\mathrm{P}})$. The arithmetic genus $\hat{X}_{p}$ is given by

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

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

For $\zeta_{\mathrm{k}}(-1)$ 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 $\equiv 1$ 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 $p=5$ the surface $(\overline{\mathrm{H} \times \mathrm{H} / \mathrm{G}}) / \sigma$ is rational (Gundlach [6]). Which of the 23 others are rational ?

Final joke : 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

[1] R. BUSAM - Eine Verallgemeinerung gewisser Dimensionsformeln von Shimizu, Tnventiones math., 11, 110-149 (1970).
[2] E. FREITAG - Die Struktur der Funktionenkorper zu Hilbertschen Modulgruppen (Habilitationsschrift, Heildelberg 1969).
[3] C. F. GAUSS - Untersuchungen uber hohere 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).
[5] K.-B. GUNDLACH - Some new results in the theory of Hilbert's modular group, Contributions to function theory, International Colloquium Bombay 1960, p. 16y-180.
[6] K.-B. GUNDLACH - Die Bestimmung der Funktionen zur Hilbertschen Moldulgruppe des Zahlkurpers $\mathbb{Q}(\sqrt{5})$, 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 - Uber vierdimensionale Riemannsche Flachen mehrdeutiger analytischer Funktionen von zwei komplexen Veranderlichen, 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, Guttinger Nachrichten 10, 87-102 (1969).

