Pacific Journal of Mathematics

A CLASS OF ALGEBRAIC SURFACES OF GENERAL TYPE CONSTRUCTED FROM QUATERNION ALGEBRAS

IRA H. SHAVEL

Vol. 76, No. 1 November 1978

PACIFIC JOURNAL OF MATHEMATICS
Vol. 76, No. 1, 1978

A CLASS OF ALGEBRAIC SURFACES OF GENERAL TYPE CONSTRUCTED FROM QUATERNION ALGEBRAS

IRA H. SHAVEL

This paper is concerned with a class of algebraic surfaces of general type constructed from indefinite division quaternion algebras whose centers are totally real number fields. These surfaces are quotients of the product of two upper half planes by Fuchsian groups obtained from the unit groups of maximal orders of such algebras. In the case where the field is real quadratic, we give smoothness conditions for the resulting surfaces and list all smooth surfaces of geometric genus 0. Finally, we give a lower bound for the torsion part of $H^2(Z)$.

0. Introduction. From the unit group of a maximal order in a suitable quaternion algebra A over a totally real number field k, one can construct certain Fuchsian groups Γ which can be identified with discrete subgroups of $GL_2^+(R)^n$. Γ acts via fractional linear transformation on the product of n copies of the upper half plane to yield a quotient which is known to be a projective algebraic variety. If one takes A to be the total matrix algebra $M_2(k)$, then one obtains the Hilbert modular group of k and the corresponding Hilbert modular variety.

In [4] Hirzebruch studied Hilbert modular surfaces as algebro-geometric and number theoretic objects. The present investigation is primarily geometric, and is concerned with the case where A is division. Unlike Hilbert modular varieties, if A is division the varieties are automatically compact. This avoids the necessity to first compactify and then resolve the resulting cusp singularities.

By a surface we mean a nonsingular, two-dimensional projective algebraic variety. The present surfaces are of general type and have irregularity 0. Those of geometric genus 0 have $c_1^2 = 8$, which distinguishes them topologically from previously known geometric genus 0 general type surfaces which all had $c_1^2 \leqq 3$.

In §1 we describe the basic objects, and in §§2 and 3 we determine the numerical invariants of the surfaces. Necessary and sufficient conditions for smoothness are given in §4. In §5 we give a lower bound for the torsion part of $H^2(Z)$, and in the final section we list all examples of geometric genus 0 surfaces of this type arising from real quadratic fields.

This paper is in part based on the author's doctoral dissertation submitted to the State University of New York at Stony Brook. I

would like to thank my advisor, Professor Michio Kuga, for his constant encouragement and valuable guidance.

1. **Preliminaries.** Let A be a division quaternion algebra with center a totally real number field k of degree m over $\boldsymbol{Q}$. Fix a maximal order $\mathfrak{O}$ of A and let $\mathfrak{o}$ denote the ring of integers of k. For a prime $\mathfrak{p}$ of k, $k_\mathfrak{p}$ will denote the $\mathfrak{p}$-adic completion of k, and $A_\mathfrak{p}$ will denote the $k_\mathfrak{p}$-algebra $A \otimes_k k_\mathfrak{p}$. A is determined up to isomorphism by its center k and a finite set $S(A)$ of prime divisors of k for which $A_\mathfrak{p}$ is division. A is said to ramify at these primes. For all other $\mathfrak{p}$, $A_\mathfrak{p}$ is isomorphic to $M_2(k_\mathfrak{p})$. Denote this algebra by $A(k, S(A))$.

Assume that the first n infinite primes are not in $S(A)$, while the remaining $m - n$ are in $S(A)$. We then have an isomorphism f of $A \otimes_Q \boldsymbol{R}$ with $M_2(\boldsymbol{R})^n \oplus \boldsymbol{H}^{m-n}$ the direct sum of n copies of $M_2(\boldsymbol{R})$ and $m - n$ copies of the Hamiltonian quaternions $\boldsymbol{H}$. The subgroup A^+ of A consisting of those units of A having totally positive reduced norm can be identified via f with a subgroup of $GL_2^+(\boldsymbol{R})^n \times \boldsymbol{H}^{*m-n}$, and projecting to the first n factors gives an injection of A^+ into $GL_2^+(\boldsymbol{R})^n$. Identify A^+ with its image in $GL_2^+(\boldsymbol{R})^n$. Let $U(\mathfrak{O})$ denote the units of $\mathfrak{O}$ and $\Gamma(1)$ denote those units of $\mathfrak{O}_n$ having reduced norm (nr) 1. $\Gamma(1)$ is a discrete subgroup of $SL_2(\boldsymbol{R})$. Let $E = U(\mathfrak{O}) \cap A^+$ and let B denote the normalizer of $\mathfrak{O}$ in A^+. The centers of $\Gamma(1)$, E and B are $\{\pm 1\}$, U_k the units of $\mathfrak{o}$, and k^*, respectively. Let j denote the map "modulo center." The $j(\Gamma(1))$, $j(E)$ and $j(B)$ act faithfully on H^n the product of n upper half planes via fractional linear transformation in each component. If A is division, that is, if $S(A)$ is nonempty, the quotient space is compact. Moreover, since H^n is complex analytically homeomorphic to a bounded domain in $\boldsymbol{C}^n$, the quotient is a projective algebraic variety. When there is no danger of confusion we write Γ for $j(\Gamma)$.

The following theorem is fundamental.

THEOREM 1.1 (Eichler-Strong Approximation). *Let $\mathfrak{A}$ be a two-sided integral $\mathfrak{O}$-ideal. Let b be an element of $\mathfrak{o}$ whose images via all embeddings of k into $\boldsymbol{R}$ corresponding to ramified infinite primes of A are positive. Let α be an element of $\mathfrak{O}$ such that $nr(\alpha) \equiv b \pmod^* \mathfrak{A} \cap \mathfrak{o}$. Then there exists β in $\mathfrak{O}$ such that $\beta \equiv \alpha \pmod{\mathfrak{A}}$ and $nr(\beta) = b$. (Recall that* mod* *is multiplicative congruence.)*

Proof. See Eichler [2].

COROLLARY 1.2. *For k a real quadratic field and a quaternion algebra over k unramified at both real primes $nr(U(\mathfrak{O})) = U_k$.*

Proof. Put $\mathfrak{A} = \mathfrak{O}$ and $\alpha = 1$. Then, for any $b \in U_k$, $1 - b \in \mathfrak{o} = \mathfrak{O} \cap \mathfrak{o}$ and there exists $\beta \in \mathfrak{o}$ such that $nr(\beta) = b$ completing the proof.

For the remainder of this section assume k to be real quadratic and $n = 2$. Let U_k be the units of k and let U_k^+ be the totally positive units of k. $j(U_k \cdot \Gamma(1)) = j(\Gamma(1))$. Therefore, $j(E)/j(\Gamma(1)) \cong E/U_k \cdot \Gamma(1)$. Consider the following exact sequences in which the first maps are inclusions and the second are reduced norms.

$$1 \longrightarrow \Gamma(1) \longrightarrow E \longrightarrow U_k^+ \longrightarrow 1$$
$$1 \longrightarrow \Gamma(1) \longrightarrow U_k \cdot \Gamma(1) \longrightarrow U_k^2 \longrightarrow 1$$

Thus, $j(E)/j(\Gamma(1)) \cong E/U_k \cdot \Gamma(1) \cong U_k^+/U_k^2$. U_k is isomorphic to the product of $\{\pm 1\}$ and an infinite cyclic group generated by a fundamental unit ε_k of U_k. Thus we have:

PROPOSITION 1.3. *Let k be a real quadratic field. If ε_k can be chosen to be totally positive then $j(\Gamma(1))$ is an index 2 subgroup of $j(E)$. If ε_k cannot be chosen to be totally positive then $j(\Gamma(1))$ and $j(E)$ coincide.*

The elements of B normalize $\mathfrak{O}$ and are therefore generators of two-sided principal ideals of $\mathfrak{O}$. The set of all (two-sided) $\mathfrak{O}$-ideals forms an abelian group generated by the maximal ideals, and the decomposition of an ideal as a product of maximal ideals is unique. Corresponding to each maximal $\mathfrak{o}$-ideal $\mathfrak{p}$ there is a unique maximal $\mathfrak{O}$-ideal such that $nr(\mathfrak{P}) = \mathfrak{p}$. In addition, if $\mathfrak{p} \in S(A)$, $\mathfrak{p}\mathfrak{O} = \mathfrak{P}^2$ and if $\mathfrak{p} \notin S(A)$, $\mathfrak{p}\mathfrak{O} = \mathfrak{P}$. Thus, an $\mathfrak{O}$-ideal has a unique expression of the form $\mathfrak{P}_{i_1}\mathfrak{P}_{i_2} \cdots \mathfrak{P}_{i_r}\mathfrak{a}$ where $\mathfrak{a}$ is an ideal of k, the $\mathfrak{P}_i$ correspond to $\mathfrak{p}_i$ in $S(A)$, and $\{i_1, \cdots, i_r\}$ is a subset of $\{1, \cdots, |S(A)|\}$.

Assume that k has class number 1. This implies that the class number of A is also 1. Choose generators Π_i for the $\mathfrak{P}_i$. For $\alpha \in B$, $\alpha\mathfrak{O} = \Pi_{i_1} \cdots \Pi_{i_r}\, a\, \mathfrak{O}$ with some $a \in k^*$. Thus, $\alpha = \Pi_{i_1} \cdots \Pi_{i_r}\lambda\varepsilon$ where $\varepsilon \in U(\mathfrak{O})$ and $\lambda \in k^*$. Then B has the description:

$$B = \{\Pi_{i_1} \cdots \Pi_{i_r}\lambda\varepsilon \mid \lambda \in k^*,\ \varepsilon \in U(\mathfrak{O}) \quad \text{and} \quad nr(\Pi_{i_1} \cdots \Pi_{i_r}\varepsilon) \quad \text{is totally positive}\}\,.$$

From this it follows that $j(B)/j(E)$ is isomorphic to a finite direct product of groups of order 2.

Choose generators π_i of the $\mathfrak{p}_i \in S(A)$ such that $nr(\Pi_i) = \pi_i$. If all of the π_i are totally positive, then $j(B)/j(E)$ has order $2^{|S(A)|}$. If ε_k is totally positive and some Π_i is not totally positive, then exactly half of the products of the Π_i will be admissable coset representative for $j(B)/j(E)$. Therefore, the order will be $2^{|S(A)|-1}$. Corollary 1.2

guarantees the existence of ε_0 and η in $U(\mathfrak{O})$ with $nr(\varepsilon_0) = \varepsilon_k$ and $nr(\eta) = -1$. If ε_k is not totally positive and some $nr(\Pi_{i_1} \cdots \Pi_{i_r})$ is not totally positive, then either $nr(\Pi_{i_1} \cdots \Pi_{i_r}\varepsilon_0)$ or $nr(\Pi_{i_1} \cdots \Pi_{i_r}\varepsilon_0\eta)$ will be totally positive. Thus, all possible products of the Π_i lead to admissable coset representatives and $j(B)/j(E)$ has order $2^{|S(A)|}$.

Summarizing we have:

PROPOSITION 1.4. *$j(B)/j(E)$ is isomorphic to the product of l cyclic groups of order 2 where l is given by:*

$$l = \begin{cases} |S(A)| & \text{if } \varepsilon_k \text{ is not totally positive, or if } \varepsilon_k \text{ is totally positive and so are all of the } \pi_i. \\ |S(A) - 1 & \text{if } \varepsilon_k \text{ is totally positive and some } \pi_i \text{ is not totally positive.} \end{cases}$$

2. **The numerical invariants.** Throughout this section, Γ will be a discrete subgroup of $GL_2^+(\boldsymbol{R})^n$ commensurable with $\Gamma(1)$ acting freely on H^n. $U(\Gamma)$ will denote the surface $\Gamma\backslash H^2$.

Let Ω^p be the sheaf of germs of holomorphic p-forms on $U(\Gamma)$ and let $h^{p,q}$ be the (complex) dimension of $H^q(U, \Omega^p)$. Since $U(\Gamma)$ is Kähler, by the Hodge theory one has $h^{p,q} = h^{q,p}$ and $b^r = \sum_{p+q=r} h^{p,q}$. As a consequence of the universal coefficient theorem and Poincaré duality $b^1 = b^3$. The geometric genus p_g, irregularity q, and arithmetic genus p_a of $U(\Gamma)$ are $h^{0,2}$, $h^{0,1}$ and $h^{0,2} - h^{0,1} + h^{0,0}$, respectively.

As a transformation group Γ can be identified with an irreducible subgroup of $SL_2(\boldsymbol{R})^n$ (see Shimizu [7]). This allows us to apply the following proposition which is a corollary of a theorem of Matsushima and Shimura [6].

PROPOSITION 2.1. *Let Γ be a discrete irreducible subgroup of $SL_2(\boldsymbol{R})^n$ acting freely on H^n with compact quotient. Then for $\Gamma\backslash H^n$:*

(a) $h^{p,q} = 0$ *for* $p \neq q$ *and* $p + q \neq n$,

(b) $h^{n-q,q} = \binom{n}{q}(\delta_{n-q,q} + h^{n,0})$

where $\binom{n}{q}$ is the qth binomial coefficient and δ_{ij} is the Kronecker delta symbol.

COROLLARY 2.2. *For $U(\Gamma)$, $h^{0,1} = 0$ and $h^{1,1} = 2p_g + 2$.*

Thus, $b^2 = 4p_g + 2$ and $b^1 = b^3 = 0$. Since $U(\Gamma)$ is connected and orientable, $b^4 = b^0 = 1$. To summarize:

THEOREM 2.3. *For $U(\Gamma)$, the Euler number $E = 4p_g + 4$, $p_a = p_g + 1$, $b^2 = 4p_g + 2$ and $q = 0$.*

Let T^* be the holomorphic cotangent bundle over $U(\Gamma)$ and K the canonical line bundle $\Lambda^2 T^*$ over $U(\Gamma)$. Let F be a complex analytic line bundle over a complex manifold U. Let $c(F)$ denote its Chern class and let c_i denote the ith Chern class of U. For simplicity, put $H^p(U, F)$ for the pth cohomology group of U with coefficients in the sheaf of germs of local holomorphic sections of F. The mth plurigenus of $U(\Gamma)$ P_m is the dimension of $H^0(U(\Gamma), mS)$.

THEOREM 2.4. (Riemann-Roch-Kodaira-Hirzebruch) *For an algebraic surface V and a complex analytic line bundle F over V*

$$h^0(V, F) - h^1(V, F) + h^2(V, F) = \frac{1}{2}(c(F)^2 + c(F)\cdot c_1) + \frac{1}{12}(c_1^2 + c_2)$$

where $h^p(V, F)$ is the dimension of $H^p(V, F)$.

Proof. See Hirzebruch [3].

For $V = U(\Gamma)$, $c(K) = -c_1$ and $c_2 = E(U(\Gamma)) = E$. Putting $F = K$ we have:

$$\begin{aligned} h^0(U(\Gamma), K) - h^1(U(\Gamma), K) + h^2(U(\Gamma), K) &= \frac{1}{2}(c(K)^2 + c(K)\cdot c_1) + \frac{1}{12}(c_1^2 + E) \\ &= \frac{1}{12}(c_1^2 + E)\,. \end{aligned}$$

$h^i(U(\Gamma), K) = h^{2,i}$ for $i = 0, 1, 2$. Thus, $p_g + 1 = p_a = 1/12(c_1^2 + E)$ and $c_1^2 = 8p_a$.

To determine the plurigenera, apply the Reimann-Roch theorem to the line bundle mK for $m \geqq 2$, and note that for the quotient V of a discontinuous group of automorphisms acting freely on a bounded domain in $\boldsymbol{C}^2$, $h^1(V, mK)$ and $h^2(V, mK)$ both vanish for $m \geqq 2$.

$$\begin{aligned} P_m = h^0(U(\Gamma), mK) &= \frac{1}{2}(c(mK)^2 + c(mK)\cdot c_1) + \frac{1}{12}(c_1^2 + c_2) \\ &= \frac{1}{2}(m^2 c_1^2 - m c_1^2) + p_a \\ &= 4p_a(m^2 - m) + p_a \\ &= (2m - 1)^2 p_a\,. \end{aligned}$$

We summarize:

THEOREM 2.5. *For* $U(\Gamma)$
(a) $c_1^2 = 8p_a$
(b) $P_m = p_a(2m-1)^2$, $m \geqq 2$.

COROLLARY 2.6. $U(\Gamma)$ *is of general type.*

Proof. c_1^2 and P_2 are both positive. $U(\Gamma)$ has no exceptional curves of the first kind. In fact, $U(\Gamma)$ is a minimal model. To see this, suppose there were a rational curve on $U(\Gamma)$. Such a curve would be given by a nonconstant holomorphic map of $P^1(\boldsymbol{C})$ into U. This would lift to a holomorphic map into H^2 which would, by Liouville's theorem, be constant. Thus, there can be no rational curves on $U(\Gamma)$, and by Kodaira's definition $U(\Gamma)$ is of general type.

3. **The Euler number.** Let A have center k a totally real field of degree m and let $S(A)$ be nonempty. Assume further that A is unramified at the n real primes corresponding to the n embeddings $\psi_{\infty,1} \cdots \psi_{\infty,n}$ of k to $\boldsymbol{R}$, and ramifies at the remaining $m-n$ real primes corresponding to $\psi_{\infty,n+1} \cdots \psi_{\infty,m}$.

The Gauss-Bonnet form on H^n is

$$\omega = \left(\frac{-1}{2\pi}\right)^n \frac{dx_1 \wedge dy_1}{y_1^2} \wedge \cdots \wedge \frac{dx_n \wedge dy_n}{y_n^2} \quad \text{where} \quad z_i = x_i + \sqrt{-1}\, y_i .$$

Under the assumption that $\Gamma(1)$ acts freely on H^n, the Euler number of the quotient variety $\Gamma(1)\backslash H^n$ can be computed from the Gauss-Bonnet formula

$$E(\Gamma(1)) = \int_F \omega \tag{1}$$

where F is a fundamental domain for the action of $\Gamma(1)$. It suffices to determine $E(\Gamma(1))$, since the Euler number is multiplicative in finite unramified covers, i.e., if $\Gamma \supset \Gamma(1)$, Γ acts freely and $[\Gamma\colon \Gamma(1)] = l$, then $lE(\Gamma) = E(\Gamma(1))$. The calculation of the integral in (1) is given explicitly by Shimizu [7] in terms of the value of the Dedekind zeta function $\zeta_k(s)$ at 2:

$$E(\Gamma(1)) = \frac{(-1)^n 2^{-m+1} d^{3/2} h(k) \zeta_k(2)}{\pi^{2m}[U_k\colon U_k']h(A)} \prod_{\mathfrak{p} \in S'(A)} (N\mathfrak{p} - 1) \tag{2}$$

where $h(k)$ is the class number of k, $h(A)$ is the class number of a maximal order of A, d is the absolute discriminant of k, U_k' are the units ε of k for which $\Psi_{\infty,i}(\varepsilon) > 0$, $n+1 \leqq i \leqq m$, $S'(A)$ is the subset of $S(A)$ consisting of the finite primes, and N is the norm map from k to $\boldsymbol{Q}$. $h(A)$ is the same for all maximal orders and

coincides with the order $h_0(k)$ of the Ray class group of k modulo $S(A) - S'(A)$. $h_0(k)\cdot[U_k\colon U_k'] = h(k)\cdot 2^{m-n}$. Using this (2) becomes

$$E(\Gamma(1)) = \frac{(-1)^n 2^{n-2n+1} d^{3/2}\zeta_k(2)}{\pi^{2m}} \prod_{\mathfrak{p}\in S'(A)} (N\mathfrak{p}-1)\,. \tag{3}$$

For the remainder of this section, let k be the real quadratic field $\boldsymbol{Q}(\sqrt{d})$ and put $m = n = 2$. $\zeta_k(s) = \zeta(s)\cdot L(s,\chi)$, where $\zeta(s)$ is the Riemann zeta function and $L(s,\chi)$ is the Dirichlet L-series with real numerical character χ having conductor d. For positive integral values of s, Leopoldt [5] gives the following formula:

$$L(2n,\chi) = \frac{\tau(\chi)}{2}\left(\frac{2\pi}{d}\right)^{2n}\frac{B_{\chi,2n}}{(2n)!}$$

where $\tau(\chi)$ is the Gauss sum $\sum_{r=1}^{d-1}\chi(r)e^{2\pi ir/d}$ and $B_{\chi,2n}$ is the generalized Bernoulli number which is given by the MacLaurin expansion

$$\sum_{l=0}^{\infty}\frac{B_{\chi,l}}{l!}t^l = \frac{\sum_{r=1}^{d-1}\chi(r)te^{rt}}{e^{dt}-1}\,. \tag{4}$$

Noting that $E(\Gamma(1))$ is a positive integer (see Theorem 2.3), using the fact that $|\tau(\chi)| = \sqrt{d}$ and taking absolute values of both sides of (3) we obtain

THEOREM 3.1. *If $k = (\boldsymbol{Q}\sqrt{d})$, $d>0$ and $\Gamma(1)\backslash H^2$ is nonsingular then the Euler number is given by:*

$$E(\Gamma(1)) = \frac{|B_{\chi,2}|}{12}\prod_{\mathfrak{p}\in S(A)}(N\mathfrak{p}-1)\,.$$

Expanding the exponentials in (4) we have:

$$\begin{aligned}\sum_{l=0}^{\infty}\frac{B_{\chi,l}}{l!}t^l &= \frac{\sum_{r=1}^{d-1}\chi(r)t(1+rt+(rt)^2/2!+\cdots)}{dt+(dt)^2/2!+(dt)^3/3!+\cdots}\\ &= \frac{\sum_{r=1}^{d-1}\chi(r)+t\sum_{r=1}^{d-1}r\chi(r)+t^2\sum_{r=1}^{d-1}r^2/2!\chi(r)+\cdots}{d(1+dt/2!+(dt)^2/3!+\cdots)}\,.\end{aligned} \tag{5}$$

Since χ is nontrivial,

$$\sum_{r=1}^{d-1}\chi(r) = 0 \quad\text{and}$$

$$t\sum_{r=1}^{d-1}r\chi(r) = t\sum_{r=1}^{d-1}(d-r)\chi(d-r) = -t\sum_{r=1}^{d-1}r\chi(d-r) = -t\sum_{r=1}^{d-1}r\chi(-r)\,.$$

Noting that $\chi(-1) = 1$ we have:

$$t\sum_{r=1}^{d-1} r\chi(r) = -t\sum_{r=1}^{d-1} r\chi(r) \quad \text{and} \quad t\sum_{r=1}^{d-1} r\chi(r) = 0 .$$

Putting this in (5) and comparing coefficients yields:

$$B_{\chi,2} = \frac{1}{d}\sum_{r=1}^{d-1} r^2\chi(r) . \tag{6}$$

Using this formula and a PDP-10 computer at SUNY-Stony Brook, James Maiorana computed $B_{\chi,2}$ for all $d < 750$. The following table gives $B_{\chi,2}$ and d for all cases where $B_{\chi,2}$ is less than 200.

d	$B_{\chi,2}$	d	$B_{\chi,2}$
5	0.8	88	92
8	2	89	104
12	4	92	80
13	4	93	72
17	8	97	136
21	8	101	76
24	12	104	100
28	16	105	144
29	12	109	108
33	24	113	144
37	20	120	136
40	28	124	160
41	32	129	200
44	28	133	136
53	28	136	184
56	40	137	192
57	56	140	152
60	48	141	144
61	44	149	140
65	64	152	164
69	48	157	172
73	88	165	176
76	76	173	156
77	48	197	196
85	72		

The next proposition gives upper and lower bounds for $|B_{\chi,2}|$ in terms of d. As a consequence of the lower bound, it is only necessary to look at fields with fairly small discriminants to find all $\Gamma(1)$-type surfaces having small geometric genus.

PROPOSITION 3.2.

$$\frac{3d^{3/2}}{50} < |B_{\chi,2}| < \frac{d^{3/2}}{6} .$$

Proof. $L(2, \chi) = (\tau(\chi)/d^2)\pi^2 B_{\chi,2}$. Since $L(2, \chi) < \zeta(2) = \pi^2/6$, $|B_{\chi,2}| < d^{3/2}/6$. $\zeta_k(2) = \zeta(2)L(2, \chi) > 1$, that is, $|L(2, \chi)| = d^{-3/2}\pi^2|B_{\chi,2}| > 6/\pi^2$. Thus,

$$|B_{\chi,2}| > \frac{6d^{3/2}}{\pi^4} > \frac{3d^{3/2}}{50}.$$

4. Smoothness. In this section we give necessary and sufficient conditions for subgroups of B which contain $\Gamma(1)$ to yield smooth surfaces. We begin by assuming that k is totally real.

For $\gamma \in A^* - k^*$, $k(\gamma)$ is a maximal subfield of A, and is therefore, a quadratic extension of k. Moreover, for an element $\gamma \in A^+$, $j(\gamma)$ is the identity automorphism of H^2 if and only if $\gamma \in k^*$.

LEMMA 4.1. *Let K be a totally imaginary quadratic extension of k, and let ϕ be a k-linear isomorphism (an embedding) of K into A. Then, for $a \in K^* - k^*$, $\phi(a) = \gamma$ is an element of A^+, and $j(\gamma)$ has a unique fixed point on H^2 which is the same for all $a \in K^* - k^*$. Conversely, if $j(\gamma) \in j(A^+)$, $j(\gamma) \neq 1$, has a fixed point on H^2, then $k(\gamma)$ is isomorphic to a totally imaginary quadratic extension of k.*

Proof. See Shimura [8].

The next two propositions are well known.

PROPOSITION 4.2 (Hasse). *A is isomorphic to $M_2(k)$ if and only if A is isomorphic to $M_2(k_\mathfrak{p})$ for all primes $\mathfrak{p}$ of k.*

PROPOSITION 4.3. *A quadratic extension K of k splits A, that is $K \otimes_k A \cong M_2(K)$, if and only if K can be embedded in A.*

PROPOSITION 4.4. *A quadratic extension K of k can be embedded in A if and only if $K_\mathfrak{p} = K \otimes_k k_\mathfrak{p}$ can be embedded in $A_\mathfrak{p}$ for all primes $\mathfrak{p}$ of k.*

Proof. If K can be embedded in A then it is clear that $K_\mathfrak{p}$ can be embedded in $A_\mathfrak{p}$ for all $\mathfrak{p}$.

Put $C = A \otimes_k K$. By the last proposition, to demonstrate the other implication it is sufficient to show that $C_\mathfrak{q} \cong M_2(K_\mathfrak{q})$ for all primes $\mathfrak{q}$ of K. The Hasse invariant inv[ ] of a simple algebra over a local field is an element of $\boldsymbol{Q}/\boldsymbol{Z}$. For quaternion algebras inv[ ] $\equiv 0 \pmod{\boldsymbol{Z}}$ if the algebra is nondivision and $\equiv 1/2 \pmod{\boldsymbol{Z}}$ if the algebra is division. If C is an algebra over L and L' is a finite extension of L of degree l then $\text{inv}[C \otimes_L L'] = l \cdot \text{inv}[C]$. In the

present situation there are three cases to consider:

(a) $\mathfrak{p} \notin S(A)$. $\text{inv}[A] = 0$ so for $\mathfrak{q}$ lying above $\mathfrak{p}$, $\text{inv}[C_\mathfrak{q}] = 0$.

(b) $\mathfrak{p} \in S(A)$ and only one prime of K lies above. $[K_\mathfrak{q}: k_\mathfrak{p}] = 2$, so $\text{inv}[C_\mathfrak{q}] = 2 \cdot \text{inv}[A_\mathfrak{p}] = 0$.

(c) $\mathfrak{p} \in S(A)$ and only one primes of K lie above $\mathfrak{p}$. Then $K_\mathfrak{q} \cong k_\mathfrak{p}$ and $\text{inv}[C_\mathfrak{q}] = 1/2$. Thus, $C_\mathfrak{q}$ is division but by assumption $K_\mathfrak{p} \cong k_\mathfrak{p} \oplus k_\mathfrak{p}$ can be embedded in C. This is impossible since $K_\mathfrak{p}$ has zero divisors.

Thus, only the first two cases are possible and, therefore, for all $\mathfrak{q}$ $C_\mathfrak{q}$ is isomorphic to $M_2(K_\mathfrak{q})$. By Proposition 4.2 $C \cong M_2(K)$ and by Proposition 4.3 K can be embedded in A.

PROPOSITION 4.5. *A quadratic extension K of k can be embedded in A if and only if only one prime of K lies above each prime in $S(A)$.*

Proof. In the proof of the last proposition, it was shown that if a quadratic extension of k can be embedded in A, then no prime of $S(A)$ can have two primes of K lying above it. Now, suppose there is only one prime of K lying above each $\mathfrak{p} \in S(A)$, then $K_\mathfrak{p}$ is a quadratic extension $k_\mathfrak{p}$. Since $\text{inv}[A_\mathfrak{p}] = 1/2$, any quadratic extension of $k_\mathfrak{p}$ splits $A_\mathfrak{p}$. Thus, $K_\mathfrak{p}$ can be embedded in $A_\mathfrak{p}$ for all primes $\mathfrak{p} \in S(A)$. For $\mathfrak{p} \notin S(A)$, $A_\mathfrak{p} \cong M_2(k_\mathfrak{p})$. $K_\mathfrak{p}$ is either isomorphic to $k_\mathfrak{p} \oplus k_\mathfrak{p}$ or is a quadratic extension of $k_\mathfrak{p}$. In the first case $K_\mathfrak{p}$ can be embedded in $M_2(k_\mathfrak{p})$ on the diagonal, and in the second case it can be embedded via (left) regular representation. Thus, $K_\mathfrak{p}$ can be embedded in $A_\mathfrak{p}$ for all $\mathfrak{p}$ and applying Proposition 4.4 yields the desired result.

PROPOSITION 4.6. *Assume that k has class number $h(k) = 1$. Then $\Gamma(1)$ has a fixed point on H^2 if and only if there is an integer $N > 2$ such that $k(\zeta_N)$ can be embedded in A, where ζ_N is a primitive Nth root of unity.*

Proof. If $\gamma \neq \pm 1$ has a fixed point on H^2, then γ is an element of a finite subgroup of $\Gamma(1)$ and there is a minimal integer N such that $\gamma^N = 1$. Conversely, let ϕ be an embedding of $k(\zeta_N)$ into A and put $\gamma = \psi(\zeta_N)$. γ is in some maximal order $\mathfrak{O}'$ of A. $h(k) = 1$ implies that all maximal orders in A are conjugate, i.e., there is an $x \in A^*$ such that $x^{-1}\mathfrak{O}'x = \mathfrak{O}$. $x\gamma x^{-1}$ also has order N, so we may as well assume that γ is in $\mathfrak{O}$. $nr(\gamma^N) = nr(\gamma)^N = 1$. Thus, $nr(\gamma) = \pm 1$ and either γ or γ^2 is in $\Gamma(1)$. This completes the proof.

For the remainder of this section k will be a real quadratic field.

If $\boldsymbol{Q}(\zeta_N)$ can be embedded in A then $[\boldsymbol{Q}(\zeta_N): \boldsymbol{Q}]$ divides 4 and so $N \in \{3, 4, 5, 6, 8, 10, 12\}$. Putting $\zeta_N = e^{2\pi i/N}$ we have:

$$\begin{aligned}
&N = 3 \text{ or } 6, && \boldsymbol{Q}(\zeta_N) = \boldsymbol{Q}(\sqrt{-3})\\
&N = 4, && \boldsymbol{Q}(\zeta_N) = \boldsymbol{Q}(\sqrt{-4})\\
&N = 5 \text{ or } 10, && \boldsymbol{Q}(\zeta_N) \supset \boldsymbol{Q}(\sqrt{5})\\
&N = 8, && \boldsymbol{Q}(\zeta_N) = \boldsymbol{Q}(\sqrt{2}, i) \supset \boldsymbol{Q}(\sqrt{8})\\
&N = 12 && \boldsymbol{Q}(\zeta_N) = \boldsymbol{Q}(\sqrt{3}, i) \supset \boldsymbol{Q}(\sqrt{12}).
\end{aligned}$$

$k(\zeta_N)$ is not a subfield of $\boldsymbol{R}$. Thus, if $\boldsymbol{Q}(\zeta_N)$ can be embedded in A, $[k(\zeta_N): k] = 2$. For $N = 5$ or 10 d must be 5, and for $N = 8$ or 12 k coincides with $\boldsymbol{Q}(\sqrt{8})$ or $\boldsymbol{Q}(\sqrt{12})$, respectively. Therefore, for $d \neq 5$, the only possibilities for N are 3, 4, and 6, and elements of order 8 or 12 can only occur for $d = 8$ or $d = 12$, respectively.

PROPOSITION 4.7. *Assume k has class number* 1. *Then $\Gamma(1)$ acts freely on H^2 if and only if all of the following hold:*

(a) *Some prime in $S(A)$ splits in $k(\sqrt{-3})/k$.*

(b) *Some prime in $S(A)$ splits in $k(\sqrt{-1})/k$.*

(c) *If $d = 5$, some prime in $S(A)$ splits in $k(\zeta_5)/k$.*

Proof. $\Gamma(1)$ has an element of order 3 if and only if it has an element of order 6, and this is the case if and only if $\boldsymbol{Q}(\zeta_3)$ can be embedded in A. $\boldsymbol{Q}(\zeta_3)$ can be embedded in A if and only if $k(\sqrt{-3})$ can be and by Proposition 4.5 this is equivalent to none of the primes in $S(A)$ splitting in $k(\sqrt{-3})/k$.

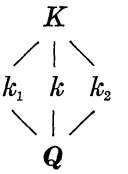
$\Gamma(1)$ contains an element of order 4 (resp. order 8) if and only if $\boldsymbol{Q}(\zeta_4)$ (resp. $\boldsymbol{Q}(\zeta_8)$) can be embedded in A, which is the same as $k(\sqrt{-1})$ admitting an embedding into A. This is equivalent to none of the primes in $S(A)$ splitting in $k(\sqrt{-1})/k$.

If $\Gamma(1)$ contains an element of order 12 then it also contains elements of orders 3 and 4, and $k(\sqrt{-3})$ and $k(\sqrt{-1})$ can be embedded in A. Conversely, if $k(\sqrt{-3})$ and $k(\sqrt{-1})$ can both be embedded in A, then $\Gamma(1)$ contains elements of orders 3 and 4 and hence an element of order 12.

Finally, if $d = 5$ there exists an element of order 5 or 10 if and only if $k(\zeta_5)$ can be embedded in A.

$K = k(\sqrt{-3})$ (resp. $k(\sqrt{-1})$) is a biquadratic extension of $\boldsymbol{Q}$ and has the three quadratic subfields k, $k_1 = \boldsymbol{Q}(\sqrt{-3})$ (resp. $\boldsymbol{Q}(\sqrt{-4})$) and $k_2 = \boldsymbol{Q}(\sqrt{D})$ where D is the discriminant of $\boldsymbol{Q}(\sqrt{-3d})$ (resp. $\boldsymbol{Q}(\sqrt{-d})$).

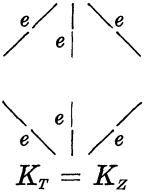
(1)



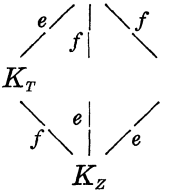
In view of the last proposition, we would like to determine how primes split in K/k in terms of the three quadratic extensions of $\boldsymbol{Q}$. Let $G = \mathrm{Gal}(K/\boldsymbol{Q})$, $\mathfrak{q}$ be a finite prime of K lying above $\mathfrak{p}$ of k and $p\boldsymbol{Z}$ of $\boldsymbol{Q}$, G_Z be the decomposition group of $\mathfrak{q}$ and G_T be the inertia group of $\mathfrak{q}$. Put K_Z = the decomposition field of $\mathfrak{q}$ and K_T = the inertia field of $\mathfrak{q}$. K_Z is the largest field contained in K in which $p\boldsymbol{Z}$ splits completely, and K is the largest field contained in K in which $p\boldsymbol{Z}$ is unramified. Moreover, K_Z is contained in K_T. In a relative quadratic extension a prime either ramifies (e), splits (g) or remains prime (f).

The possibilities for diagram (1) are:

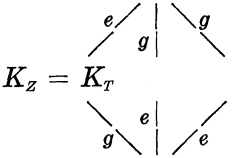
(I) $K_T = K_Z = \boldsymbol{Q}$.



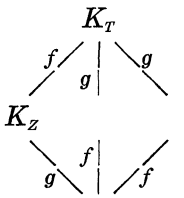
(II) K_T = some intermediate field (say k_1) and $K_Z = \boldsymbol{Q}$.



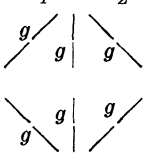
(III) $K_T = K_Z$ = some intermediate field.



(IV) $K_T = K$, K_Z is an intermediate field.



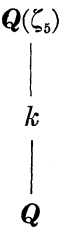
(V) $K_T = K_Z = K$.



(VI) $K_T = K$, $K_Z = \boldsymbol{Q}$. This situation does not occur because G_Z/G_T must be cyclic.

Examining these diagrams we conclude that $\mathfrak{p}$ splits in K/k if and only if $p\boldsymbol{Z}$ splits in k_1 or k_2.

In the case $d = 5$ we have the diagram



$\mathfrak{p}$ splits in $\boldsymbol{Q}(\zeta_5)/k$ if and only if $p\boldsymbol{Z}$ splits completely in $\boldsymbol{Q}(\zeta_5)/\boldsymbol{Q}$ and this is the case if and only if $p \equiv 1 \pmod 5$.

Combining these results with Proposition 4.7 yields:

THEOREM 4.8. *Assume that k is a real quadratic field and $h(k) = 1$. Then $\Gamma(1)$ acts freely on H^2 if and only if all of the following hold:*

(1) $(-3/p) = 1$ *or* $(D/p) = 1$ *for some* $\mathfrak{p} \in S(A)$, *where* $p\boldsymbol{Z} = \mathfrak{p} \cap \boldsymbol{Z}$ *and D is the discriminant of* $\boldsymbol{Q}(\sqrt{-3d})$.

(2) $(-1/p) = 1$ *or* $(\Delta/p) = 1$ *for some* $\mathfrak{p} \in S(A)$ *where* $p\boldsymbol{Z} = \mathfrak{p} \cap \boldsymbol{Z}$ *and Δ is the discriminant of the field* $\boldsymbol{Q}(\sqrt{-d})$.

(3) *If* $d = 5$, *there exists* $\mathfrak{p} \in S(A)$ *such that* $p\boldsymbol{Z} = \mathfrak{p} \cap \boldsymbol{Z}$ *and* $p \equiv 1 \pmod 5$.

THEOREM 4.9. *Assume k has class number* 1 *and assume further that a fundamental unit ε_k of k greater than* 0 *is totally positive. Then E acts freely on H^2 if and only if both of the following hold:*

(1) $\Gamma(1)$ *acts freely.*

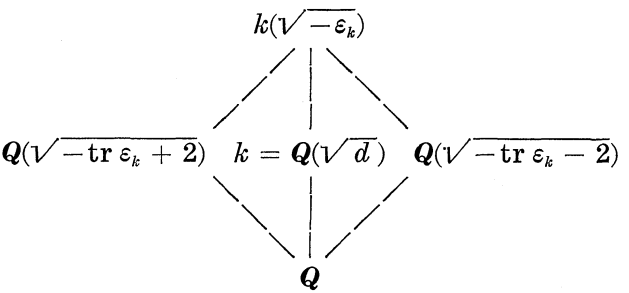
(2) *Some* $\mathfrak{p} \in S(A)$ *splits in* $k(\sqrt{-\varepsilon_k})/k$.

Proof. Suppose $j(\gamma) \in j(E)$, $j(\gamma) \neq 1$, has a fixed point on H^2. By Lemma 4.1 $k(\gamma)$ is totally imaginary quadratic extension of k. $nr(\gamma) = \varepsilon_k^m$, and we may assume m is nonnegative. We can find

$\gamma_1 \in E$ with $j(\gamma_1) = j(\gamma)$ and $nr(\gamma_1) = \varepsilon_k$ or 1. To see this suppose $m = 2l$ (resp. $2l + 1$) and let $\gamma_1 = \gamma\varepsilon_k^{-l}$. Then $nr(\gamma_1) = nr(\gamma)\cdot nr(\varepsilon_k^{-l}) = 1$ (resp. ε_k). If m is even $j(\gamma)$ is in $\Gamma(1)$ and has a fixed point on H^2. If m is odd then $\gamma_1^s = \pm\varepsilon_k^t$ for some s since γ has a fixed point. Choose s to be minimal. $nr(\gamma_1^s) = \varepsilon_k^{2t} = nr(\gamma_1)^s = \varepsilon_k^s$. Put $\gamma_2 = \gamma_1^t$. $j(\gamma_2) = j(\gamma_1)$ and $k(\gamma_2) = k(\gamma)$. By the minimality of s, $\gamma_2 \notin k^*$ but $\gamma_2^2 = \pm\varepsilon_k^t \in k^*$. Since this must be a totally imaginary extension of k, $k(\gamma_2) = k(\sqrt{-\varepsilon_k^t})$. If t is odd then $k(\gamma_2) = k(\sqrt{-\varepsilon_k})$ can be embedded in A and by Proposition 4.5 this is equivalent to none of the primes in $S(A)$ splitting in $k(\sqrt{-\varepsilon_k})/k$. If t is even then $k(\gamma) = k(\sqrt{-1})$ can be embedded in A and $\Gamma(1)$ has a fixed point.

Conversely, suppose ϕ is an embedding of $k(\sqrt{-\varepsilon_k})$ in A. Put $\gamma = \phi(\sqrt{-\varepsilon_k})$. γ is in some maximal order of A which, because k has class number 1, may be assumed to be $\mathfrak{O}$. Moreover, γ is a unit of $\mathfrak{O}$, and by Lemma 4.1 it has totally positive reduced norm. Thus, γ is in E and has a fixed point. This completes the proof.

LEMMA 4.10. *$k(\sqrt{-\varepsilon_k})$ is an extension of $\boldsymbol{Q}$ with Galois group $\boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$. Moreover, we have the following diagram of subfields:*



where tr *is the trace map from k to $\boldsymbol{Q}$.*

Proof. Let α denote $\sqrt{-\varepsilon_k}$ and β denote $\sqrt{-\varepsilon_k'}$ where prime denotes Galois conjugation in k and the square roots are chosen such that $\mathrm{Im}\,(\alpha) > 0$ and $\mathrm{Im}\,(\beta) > 0$. $(\alpha\beta)^2 = 1$, therefore $\alpha\beta = \pm 1$, but α and β are purely imaginary, and $\mathrm{Im}\,(\alpha)$ and $\mathrm{Im}\,(\beta)$ are both positive. Therefore $\alpha\beta = -1$ and $\alpha = (-1/\beta)$. Put $\xi = \alpha + \beta$ and $\eta = \alpha - \beta$. Then

(1) $\xi^2 = (\alpha + \beta)^2 = -\varepsilon_k - \varepsilon_k' + 2\alpha\beta = -\mathrm{tr}\,\varepsilon_k - 2 \in k(\sqrt{-\varepsilon_k})$.

(2) $\eta^2 = (\alpha - \beta)^2 = -\varepsilon_k - \varepsilon_k' - 2\alpha\beta = -\mathrm{tr}\,\varepsilon_k + 2 \in k(\sqrt{-\varepsilon_k})$.

Adjoining ξ and η to $\boldsymbol{Q}$ give two distinct intermediate quadratic extensions of $\boldsymbol{Q}$ neither of which is k, whose compositum coincides with $k(\sqrt{-\varepsilon_k})$. Therefore, $k(\sqrt{-\varepsilon_k})$ is a biquadratic extension of $\boldsymbol{Q}$ and the lemma follows.

THEOREM 4.11. *Assume k has class number 1, and let ε_k be a fundamental unit of k greater than 0. Then B acts freely on H^2 if and only if all of the following hold:*

(1) *E acts freely on H^2.*

(2) *For all totally positive $\pi_{i_1}\pi_{i_2}\cdots\pi_{i_l}$, there exists $\mathfrak{p}\in S(A)$ such that $\mathfrak{p}$ splits in the extension $k(\sqrt{-\pi_{i_1}\cdots\pi_{i_l}})/k$, where $\{i_1, \cdots, i_l\}\subset\{1, \cdots, |S(A)|\}$.*

(3) *For all totally positive $\pi_{i_1}\pi_{i_2}\cdots\pi_{i_l}\varepsilon_k$, there exists $\mathfrak{p}\in S(A)$ such that $\mathfrak{p}$ splits in the extension $k(\sqrt{-\pi_{i_1}\cdots\pi_{i_l}\varepsilon_k})/k$, where $\{i_1, \cdots, i_l\}\subset\{1, \cdots, |S(A)|\}$.*

Proof. Fix a set of generators for the maximal $\mathfrak{O}$-ideals $\mathfrak{P}_i$ which correspond to the $\mathfrak{p}_i$ in $S(A)$, and choose a set of generators π_i for the $\mathfrak{p}_i$ for the $\mathfrak{p}_i$ in $S(A)$ such that $\pi_i > 0$ and $nr(\Pi_i) = \pi_i$. Suppose $\gamma\in B$ has a fixed point on H^2. Recall that γ is of the form $\Pi_{i_1}\cdots\Pi_{i_l}\varepsilon\lambda$ where $\varepsilon\in U(\mathfrak{O})$, $\lambda\in k^*$ and $nr(\Pi_{i_1}\cdots\Pi_{i_l}\varepsilon\lambda)$ is totally positive. For simplicity, denote the product $\Pi_{i_1}\cdots\Pi_{i_l}$ by $\Pi_1\cdots\Pi_l$. Replace γ by $\gamma_1 = \Pi_1\cdots\Pi_l\varepsilon$. By Lemma 4.1 $k(\gamma_1)$ is a totally imaginary quadratic extension of k. Let r be the least positive integer for which $\gamma_1^r\in k^*$. Form the two-sided $\mathfrak{O}$-ideals $\gamma_1\mathfrak{O} = \mathfrak{P}_1\cdots\mathfrak{P}_l\mathfrak{a}$ and $\gamma_1^r\mathfrak{O} = \mathfrak{P}_1^r\cdots\mathfrak{P}_l^r\mathfrak{a}^r$ where $\mathfrak{a}$ is an ideal of k. Since $\gamma_1^r\in k^*$, r must be even. Put $r = 2s$ and $\gamma_2 = \gamma_1^s$. $k\subsetneq k(\gamma_2)\subset k(\gamma_1)$ and $[k: k(\gamma_1)] = 2$. Thus, $k(\gamma_2) = k(\gamma_1)$ and $j(\gamma_1)$ and $j(\gamma_2)$ have the same fixed point.

If s is even then $\gamma_2 = a\varepsilon^s$ where $a\in k^*$ and $nr(\varepsilon)$ is totally positive. Therefore, E has a fixed point. If s is odd, say $s = 2t+1$, then $\gamma_2 = \Pi_1^{2t+1}\cdots\Pi_l^{2t+1}a = \Pi_1\cdots\Pi_l\varepsilon^{2t+1}b$ where a and $b\in k^*$. $nr(\gamma_2^2) = nr(\gamma_2)^2 = \gamma_2^4$ since $\gamma_2^2\in k^*$. Thus,

$$\gamma_2^2 = \pm nr(\gamma_2) = \pm nr(\Pi_1)\cdots nr(\Pi_l)nr(\varepsilon^{2t+1})b^2 = \pm\pi_1\cdots\pi_l\varepsilon_0 b^2$$

where $\varepsilon_0\in U_k$. $\varepsilon_0 = \varepsilon_k^q$. Therefore, $k(\gamma_2) = k(\sqrt{-\pi_1\cdots\pi_l(\varepsilon_k)})$ where ε_k appears only if q is odd, and the minus-sign is chosen because the extension must be totally imaginary. Thus, if $j(\gamma)$ has a fixed point on H^2, $k(\sqrt{-\pi_1\cdots\pi_l(\varepsilon_k)})$ can be embedded in A which is equivalent to none of the $\mathfrak{p}_i$ in $S(A)$ splitting in $k(\sqrt{-\pi_1\cdots\pi_l(\varepsilon_k)})/k$.

Conversely, suppose ϕ is an embedding of $k(\sqrt{-\pi_1\cdots\pi_l(\varepsilon_k)})$ in A. Put $\gamma = \phi(\sqrt{-\pi_1\cdots\pi_l(\varepsilon_k)})$. By Lemma 4.1, γ has totally positive reduced norm. Consider the ideals $\gamma\mathfrak{O}$ and $\gamma^2\mathfrak{O}$. Noting that $\phi(\gamma^2) = \gamma^2$ we have $\gamma^2\mathfrak{O} = \pi_1\cdots\pi_l\mathfrak{O} = \mathfrak{P}_1^2\cdots\mathfrak{P}_l^2$. Thus, $\gamma\mathfrak{O}$ is a two-sided $\mathfrak{O}$-ideal and γ normalizes $\mathfrak{O}$. Therefore, γ is in B and has a fixed point on H^2.

5. The torsion part of $H^2(Z)$. Let Γ be a subgroup of B acting freely on H^2 and put $U = \Gamma\backslash H^2$. $\pi_1(U)$ is isomorphic to $j(\Gamma)$ and, therefore, $H_1(U, Z)$ is isomorphic to $j(\Gamma)/j(\Gamma)'$ where $j(\Gamma)'$ is the commutator subgroup of $j(\Gamma)$. The exact sequence

$$0 \longrightarrow Z \longrightarrow R \longrightarrow R/Z \longrightarrow 0$$

induces a long exact cohomology sequence. Consider the following fragment of that sequence:

$$\begin{aligned} &\cdots \longrightarrow H^1(U, R) \longrightarrow H^1(U, R/Z) \\ &\xrightarrow{\delta} H^2(U, Z) \longrightarrow H^2(U, R) \longrightarrow \cdots . \end{aligned} \tag{1}$$

By the universal coefficient theorem

$$H_3(U, R/Z) \cong \mathrm{Ext}\,(H^4(U, Z), R/Z) \oplus \mathrm{Hom}\,(H^3(U, Z), R/Z)\,. \tag{2}$$

Since $H^4(U, Z)$ is free, the Ext term vanishes, and the right hand side of (2) is just the Pontryagin dual of $H^3(U, Z)$ which, since $b^3 = 0$, is isomorphic to itself. Applying Poincaré duality to both sides of (2) then yields:

$$H^1(U, R/Z) \cong H_1(U, Z)\,.$$

In (1) δ is injective because $b^1 = 0$, and since $H^2(U, R) \cong R^{4p^g+2}$, the image of δ is precisely the torsion subgroup of $H^2(U, Z)$. Thus, $H^2(U, Z)_{\mathrm{tor}} \cong H_1(U, Z)$.

We now specialize to the case where $\Gamma = \Gamma(1)$ and k is real quadratic. The strategy is to build a normal subgroup M of $\Gamma(1)$ which contains $\Gamma(1)'$ for which $\Gamma(1)/M$ is known.

For a maximal ideal $\mathfrak{p}$ of $\mathfrak{o}$ and the corresponding $\mathfrak{P}$ of $\mathfrak{O}$, let $\Phi_{\mathfrak{p}}$ and $\Phi_{\mathfrak{P}}$ denote the maps reduction mod $\mathfrak{p}$ and $\mathfrak{P}$, respectively. When the context makes it clear which map we mean, we will simply write Φ.

LEMMA 5.1. *Let* $N\mathfrak{p} = q = p^f$ *and* F_q *= the field having* q *elements. Then*

(a) *For* $\mathfrak{p} \notin S(A)$ *the following diagram commutes:*

$$\begin{array}{ccc} \mathfrak{O} & \xrightarrow{\Phi} & M_2(F_q) \\ \downarrow{\scriptstyle nr} & & \downarrow{\scriptstyle \det} \\ \mathfrak{o} & \xrightarrow{\Phi} & F_q \end{array}\,.$$

(b) *For* $\mathfrak{p} \in S(A)$ *the following diagram commutes:*

$$\begin{array}{ccc} \mathfrak{O} & \xrightarrow{\Phi} & \boldsymbol{F}_{q^2} \\ \Big\downarrow nr & & \Big\downarrow N = \textit{norm from } \boldsymbol{F}_{q^2} \textit{ to } \boldsymbol{F}_q \\ \mathfrak{o} & \xrightarrow{\Phi} & \boldsymbol{F}_q \end{array}.$$

Proof. (a) $\mathfrak{O}$ can be taken to be $M_2(\mathfrak{o})$. By definition, the reduced norm coincides with determinant and the diagram commutes.

(b) Take $x \in \mathfrak{O}$. $k(x) = K$ is either a quadratic extension of k or coincides with k. Since x is integral over $\mathfrak{o}$, $x \in \mathfrak{o}_K$ the ring of integers of K. If $K = k$, $\Phi_{\mathfrak{P}}(x) = \Phi_{\mathfrak{p}}(x) \in \boldsymbol{F}_q$ and $nr(x) = x^2$. Then $N(\Phi_{\mathfrak{P}}(x)) = \Phi_{\mathfrak{p}}(x)^2$ and $\Phi_{\mathfrak{p}}(nr(x)) = \Phi_{\mathfrak{p}}(x^2)$, and the diagram commutes. Suppose $K \neq k$. The canonical involution ι of A induces Galois conjugation on K and $nr(x) = xx^{\iota} = N_{K/k}(x)$. Put $\mathfrak{q} = \mathfrak{o}_K \cap \mathfrak{P}$. Then $\Phi_{\mathfrak{P}}$ restricted to $\mathfrak{o}_K$ is $\Phi_{\mathfrak{q}}$ and the following diagram commutes:

$$\begin{array}{ccc} \mathfrak{o}_K & \xrightarrow{\Phi} & \mathfrak{o}_K/\mathfrak{q} \\ \Big\downarrow N_{K/k} & & \Big\downarrow N \\ \mathfrak{o} & \xrightarrow{\Phi} & \mathfrak{o}/\mathfrak{p} \end{array}.$$

This completes the proof.

LEMMA 5.2. (a) *For* $\mathfrak{p} \notin S(A)$, $\Phi(\Gamma(1)) = SL_2(\boldsymbol{F}_q)$.

(b) *For* $\mathfrak{p} \in S(A)$, $\Phi(\Gamma(1)) = \{x \in \boldsymbol{F}_{q^2} \mid N(x) = 1\} = U(q)$ *where* N *is the norm map from* $\boldsymbol{F}_{q^2}$ *to* $\boldsymbol{F}_q$.

Proof. $\Phi(\Gamma(1)) \subset SL_2(\boldsymbol{F}_q)$ (resp. $U(q)$). To shown the equality take $x \in SL_2(\boldsymbol{F}_q)$ (resp. $U(q)$. By Lemma 5.1 $nr(\Phi^{-1}(x)) \equiv 1 \pmod{\mathfrak{p}}$. Since A is totally indefinite and $nr(\Phi^{-1}(x))$ is integral, we can apply Theorem 1.1 to obtain $\alpha \in \mathfrak{O}$ such that $\Phi^{-1}(x) \equiv \alpha \pmod{\mathfrak{P}}$ and $nr(\alpha) = 1$. Moreover, since $nr(\alpha)$ is a unit of k, α is a unit of $\mathfrak{O}$. This completes the proof.

Let $\Gamma(\mathfrak{P})$ denote the kernel of the restriction of Φ to $\Gamma(1)$. For $\mathfrak{p}$ in $S(A)$

$$1 \longrightarrow U(q) \longrightarrow \boldsymbol{F}_{q^2}^* \xrightarrow{N} \boldsymbol{F}_q^* \longrightarrow 1$$

is an exact sequence of abelian groups, and $\boldsymbol{F}_{q^2}^*$ and $\boldsymbol{F}_q^*$ are cyclic of orders $q^2 - 1$ and $q - 1$, respectively. Thus, $U(q)$ is cyclic of order $q + 1$.

Put $M_0 = \bigcap_{\mathfrak{p} \in S(A)} \Gamma(\mathfrak{P})$. Since the $\mathfrak{P}_i$ are pairwise relatively prime, $M_0 = \Gamma(\mathfrak{P}_1 \cdots \mathfrak{P}_r)$ and $\mathfrak{O}/\mathfrak{P}_1 \cdots \mathfrak{P}_r = \mathfrak{O}/\mathfrak{P}_1 \times \mathfrak{O}/\mathfrak{P}_2 \times \cdots \times \mathfrak{O}/\mathfrak{P}_r$. The following lemma is an easy extension of Lemma 5.1.

LEMMA 5.3. *For* $\mathfrak{p}_i \in S(A)$

$$\begin{array}{ccc} \mathfrak{O} & \xrightarrow{\Phi_{\mathfrak{P}_1 \cdots \mathfrak{P}_r}} & \mathfrak{O}/\mathfrak{P}_1 \times \cdots \times \mathfrak{O}/\mathfrak{P}_r \\ \downarrow nr & & \downarrow N \\ \mathfrak{o} & \xrightarrow{\Phi_{\mathfrak{p}_1 \cdots \mathfrak{p}_r}} & \mathfrak{o}/\mathfrak{p}_1 \times \cdots \times \mathfrak{o}/\mathfrak{p}_r \end{array}$$

commutes where $N =$ *the product of the norm maps from* $\boldsymbol{F}_{q_i^2}$ *to* $\boldsymbol{F}_{q_i}$.

Since $\Gamma(1)/\Gamma(\mathfrak{P}_i) \cong U(q_i)$ for $\mathfrak{p}_i \in S(A)$, $\Phi_{\mathfrak{P}_1 \cdots \mathfrak{P}_r}(\Gamma(1)) \cong U(q_1) \times \cdots \times U(q_r)$. Thus, $\Gamma(1)/M_0 \cong U(q_1) \times \cdots \times U(q_r)$ is abelian and $\Gamma(1) \supset M_0 \supset \Gamma(1)'$.

For $\mathfrak{p} \notin S(A)$

$$1 \longrightarrow \Gamma(\mathfrak{P}) \longrightarrow \Gamma(1) \xrightarrow{\Phi} SL_2(\boldsymbol{F}_q) \longrightarrow 1$$

is exact. $SL_2(\boldsymbol{F}_2)$ is isomorphic to S_3 and has a normal subgroup A_3 of index 2. For simplicity, let A_3 also denote the copy of A_3 in $SL_2(\boldsymbol{F}_2)$. For a prime $\mathfrak{p}_2$ lying above $2\boldsymbol{Z}$ with $N\mathfrak{p}_2 = 2$, put $M(\mathfrak{p}_2) = \Phi_{\mathfrak{p}_2}^{-1}(A_3)$. The sequence

$$1 \longrightarrow \Gamma(\mathfrak{P}_2) \longrightarrow M(\mathfrak{p}_2) \xrightarrow{\Phi} A_3 \longrightarrow 1$$

is exact. Thus $M(\mathfrak{p}_2)/\Gamma(\mathfrak{P}_2) \cong A_3$. Since $\Gamma(1)/\Gamma(\mathfrak{P}_2) \cong S_3$, $\Gamma(1)/M(\mathfrak{p}_2)$ is of order 2.

$PSL_2(\boldsymbol{F}_3)$ is isomorphic to A_4 and A_4 contains the Klein 4-group V as a normal subgroup of index 3.

$$1 \longrightarrow \{\pm 1\} \longrightarrow SL_2(\boldsymbol{F}_3) \xrightarrow{J} PSL_2(\boldsymbol{F}_3) \longrightarrow 1$$

is exact where J is the map "modulo $\{\pm 1\}$." Let V also denote the copy of V in $PSL_2(\boldsymbol{F}_3)$. $J^{-1}(V)$ is a normal subgroup of $SL_2(\boldsymbol{F}_3)$ of index 3. Put $M(\mathfrak{p}_3) = \Phi^{-1}(J^{-1}(V))$. The sequence

$$1 \longrightarrow \Gamma(\mathfrak{P}_3) \longrightarrow M(\mathfrak{p}_3) \xrightarrow{\Phi} J^{-1}(V) \longrightarrow 1$$

is exact. Thus, $\Gamma(1)/M(\mathfrak{p}_3) \cong SL_2(\boldsymbol{F}_3)/J^{-1}(V)$ is of order 3.

For $l = 2$ and 3 we make the definition:

$$M(l) = \begin{cases} M(\mathfrak{p}) & \text{if there is only one prime } \mathfrak{p} \text{ lying above } l\boldsymbol{Z} \text{ having norm } l \text{ which is not in } S(A). \\ M(\mathfrak{p}) \cap M(\mathfrak{p}') & \text{if there are two distinct primes lying above } l\boldsymbol{Z} \text{ neither of which is in } S(A). \\ \Gamma(1) & \text{otherwise.} \end{cases}$$

Finally, define M to be $M_0 \cap M(2) \cap M(3)$.

For $\mathfrak{p}$ and $\mathfrak{p}'$ two distinct primes lying above $2\boldsymbol{Z}$ (resp. $3\boldsymbol{Z}$) and having norms 2 (resp. 3), the quotient of $\Gamma(1)/(M(\mathfrak{p}) \cap M(\mathfrak{p}'))$ by $M(\mathfrak{p})/(M(\mathfrak{p}) \cap M(\mathfrak{p}'))$ is isomorphic to $\Gamma(1)/M(\mathfrak{p})$ which has order 2 (resp. 3). The order of $M(\mathfrak{p})/(M(\mathfrak{p}) \cap M(\mathfrak{p}'))$ is 2 or 1 (resp. 3 or 1). It is of order 2 (resp. order 3) if and only if $M(\mathfrak{p}) \cdot M(\mathfrak{p}')$ properly contains $M(\mathfrak{p})$ which is the case if and only if $M(\mathfrak{p}) \neq M(\mathfrak{p}')$. Since $\mathfrak{p}$ and $\mathfrak{p}'$ are distinct ideals, $M(\mathfrak{p})/(M(\mathfrak{p}) \cap M(\mathfrak{p}'))$ has order 2 (resp. 3) and $\Gamma(1)/(M(\mathfrak{p}) \cap M(\mathfrak{p}'))$ has order 4 (resp. 9).

We have calculated the order of $\Gamma(1)/M$, but we are interested in the order of $j(\Gamma(1))/j(M)$. If M contains -1 then $j(\Gamma(1))/j(M)$ is isomorphic to $\Gamma(1)/M$. If M does not contain -1 then $j(\Gamma(1))/j(M)$ is isomorphic to $\Gamma(1)/\{\pm 1\}M$, and $|j(\Gamma(1))/j(M)| = 1/2|\Gamma(1)/M|$. $-1 \notin M$ if and only if $-1 \notin$ some $\Gamma(\mathfrak{P}_i)$. This is equivalent to some $U(q_i)$ containing -1 and this is the case if and only if some q_i is odd.

We summarize this discussion as:

THEOREM 5.4. *Suppose k is a real quadratic field and $\Gamma(1)$ acts freely on H^2. Put $U = \Gamma(1)\backslash H^2$. Then the order of $H^2(U, \boldsymbol{Z})_{\text{tor}}$ is divisible by $a \cdot b \cdot c \cdot \prod_{\mathfrak{p} \in S(A)} (N\mathfrak{p} - 1)$ where*

$$a = \begin{cases} 1/2 & \text{if for some } \mathfrak{p} \in S(A) \quad N\mathfrak{p} \text{ is odd.} \\ 1 & \text{otherwise.} \end{cases}$$

$$b = \begin{cases} 4 & \text{if there are two distinct primes lying above } 2\boldsymbol{Z} \\ & \text{neither of which is in } S(A). \\ 2 & \text{if there is only one prime lying above } 2\boldsymbol{Z} \text{ having} \\ & \text{norm 2 which is not in } S(A). \\ 1 & \text{otherwise.} \end{cases}$$

$$c = \begin{cases} 9 & \text{if there are two distinct primes lying above } 3\boldsymbol{Z} \\ & \text{neither of which is in } S(A). \\ 3 & \text{if there is only one prime lying above } 3\boldsymbol{Z} \text{ having} \\ & \text{norm 3 which is not in } S(A). \\ 1 & \text{otherwise .} \end{cases}$$

6. Examples. In this section we will determine all $p_g = 0$ (non-singular) surfaces arising from groups lying between $\Gamma(1)$ and B and algebras over real quadratic fields of class number 1.

In practice it is a simple matter to apply the conditions of Theorems 4.8 and 4.9, but the conditions of Theorem 4.10 are considerably more difficult to verify partly because the extensions are not always Galois. The following lemmas are helpful in this regard.

LEMMA 6.1. *The primes* $\mathfrak{p}_i = \pi_i\mathfrak{o}$, $1 \leqq x \leqq l$, *all ramify in* $k(\sqrt{-\pi_1 \cdots \pi_l(\varepsilon_k)})/k$.

Proof. For any $\mathfrak{p} = \pi\mathfrak{o}$ among the $\mathfrak{p}_1, \cdots, \mathfrak{p}_l$ consider the $\mathfrak{p}$-adic valuation $|\ |_\mathfrak{p}$ of k and the corresponding value group $V_\mathfrak{p}$. The $\mathfrak{p}$-adic completion $k_\mathfrak{p}$ of k also has value group $V_\mathfrak{p}$. Let $\mathfrak{q}$ be the extension of $\mathfrak{p}$ to $k(\sqrt{-\pi_1 \cdots \pi_l(\varepsilon_k)})$. Put $\alpha = \sqrt{-\pi_1 \cdots \pi_l(\varepsilon_k)}$. The $\mathfrak{q}$-adic valuation of α is $\sqrt{|N\alpha|_\mathfrak{p}} = \sqrt{|\pi|_\mathfrak{p}}$. Thus $|V_\mathfrak{q}/V_\mathfrak{p}| = 2$ and $\mathfrak{p}$ ramifies in $k(\alpha)/k$.

LEMMA 6.2. *Let* K *be an algebraic number field with minimal polynomial* $f(x) \in \boldsymbol{Z}[x]$. *Then the discriminant* $d(f)$ *of* $f(x)$ *divides the absolute discriminant* $d(K)$ *of* K *and the quotient is the square of an integer,* i.e., $d(f) = m^2 d(K)$. *Moreover, if* p *does not divide* m *then the number of distinct irreducible factors of* $f(x)$ *in* $\boldsymbol{Z}[x]/p\boldsymbol{Z}[x]$ *is the same as the number of primes of* K *lying above* $(p\boldsymbol{Z})$.

Proof. See Borevich and Shafarevich [1].

In cases where Lemma 6.2 is not applicable one can either factor the polynomial p-adically or use the following lemma.

LEMMA 6.3. *Let* F *be a local field with prime element* π *and let* $f(x)$ *be a monic polynomial in* $F[x]$ *with integral coefficients. Put* $r = \operatorname{ord}_\pi(d(f))$. *Then, if* $f(x)$ *factors modulo* π^{r+1} *as a product of* t *irreducible polynomials then* f *factors in* $F[x]$ *as a product of* t *irreducible polynomials.*

Proof. See Borevich and Shafarevich [1].

The integer r in Lemma 6.3 is sometimes fairly large. In these cases the following observation is useful.

LEMMA 6.4. *The minimal of* $k(\sqrt{-\pi_1 \cdots \pi_r(\varepsilon_k)})/\boldsymbol{Q}$ *is of the form* $f(x) = x^4 + ax^2 + b$. $f(x)$ *can factor as a product of quadratic polynomials in only the following three distinct ways:*

$$\left(x^2 - \frac{-a + \sqrt{a^2 - 4b}}{2}\right)\left(x^2 - \frac{-a - \sqrt{a^2 - 4b}}{2}\right)$$

$$(x^2 + \sqrt{2\sqrt{b} - a}\,x + \sqrt{b})(x^2 - \sqrt{2\sqrt{b} - a}\,x + \sqrt{b})$$

$$(x^2 + \sqrt{-2\sqrt{b} - a}\,x - \sqrt{b})(x^2 - \sqrt{-2\sqrt{b} - a}\,x - \sqrt{b}).$$

Moreover, if it factors in any two of these ways then it must factor completely.

As was remarked earlier, the lower bound for $|B_{\chi,2}|$ given in Proposition 3.2 provides an upper bound for the possible discriminants that can lead to surfaces of any given geometric genus. For example, if we are interested in $p_g = 0$ surfaces $\Gamma(1)\backslash H^2$, then $|B_{\chi,2}| \leqq 24$ since the Euler number is 4. In this case $d < 55$.

For simplicity we write $A(d; \mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_t)$ for the algebra having center $k = \boldsymbol{Q}(\sqrt{d})$ and $S(A) = \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_t\}$. We denote a prime of k lying above $p\boldsymbol{Z}$ by $\mathfrak{p}_p$. If there are two distinct primes lying above $p\boldsymbol{Z}$ we denote these $\mathfrak{p}_p$ and $\mathfrak{p}'_p$. Finally, put $U(\Gamma) = \Gamma\backslash H^2$. We identify a group Γ lying between E and B with the primes of k corresponding to a complete set of coset representatives for $j(\Gamma)/j(E)$. For example, if the representatives are Π and 1 with $\Pi^2\mathfrak{O} = \mathfrak{p}\mathfrak{O}$, then we denote this group by $\Gamma_\mathfrak{p}$ or more compactly by Γ_p (and $\Gamma_{\mathfrak{p}'}$ by Γ'_p).

EXAMPLE 1. $A(12; \mathfrak{p}_2, \mathfrak{p}_5)$.

$2\boldsymbol{Z}$ ramifies and $5\boldsymbol{Z}$ remains prime in $\boldsymbol{Q}(\sqrt{12})$. Thus, $E(U(\Gamma(1))) = (4/12)(25-1)(2-1) = 8$. $(-1/5) = 1$. Therefore, by Theorem 4.8 $U(\Gamma(1))$ is smooth.

$\varepsilon_k = 2 + \sqrt{3}$ which is totally positive has trace 4. Since $5\boldsymbol{Z}$ splits in $\boldsymbol{Q}(\sqrt{-6})$, $\mathfrak{p}_5$ splits in $k(\sqrt{-\varepsilon_k})$ (see Lemma 4.10). Thus, $k(\sqrt{-\varepsilon_k})$ cannot be embedded in A and by Theorem 4.9 $U(E)$ is a smooth $p_g = 0$ surface.

EXAMPLE 2. $A(13; \mathfrak{p}_3, \mathfrak{p}_{13})$ and $A(13; \mathfrak{p}'_3, \mathfrak{p}_{13})$. $13\boldsymbol{Z}$ ramifies and $3\boldsymbol{Z}$ splits in $\boldsymbol{Q}(\sqrt{13})$. $E(U(\Gamma(1))) = 4/12(13-1)(3-1) = 8$. Thus, $U(\Gamma(1))$ is a candidate for a smooth $p_g = 1$ surface. To check for smoothness, note that $(-1/13) = 1$ and $(-3/13) = 1$. Then, by Theorem 4.8, $U(\Gamma(1))$ is smooth.

$\varepsilon_k = 3/2 + \sqrt{13}/2$ and is not totally positive. Therefore, $j(\Gamma(1))$ and $j(E)$ coincide.

To find $p_g = 0$ surfaces we must look for index 2 subgroups of $j(B)$. The possible sets of coset representatives are $\{\Pi_{13}, 1\}$, $\{\Pi'_3, 1\}$ and $\{\Pi'_3\Pi_{13}, 1\}$. In view of Lemma 6.1, the last group cannot lead to a smooth surface.

Let us begin by considering Γ_3 and the algebra $A(13; \mathfrak{p}_3, \mathfrak{p}_{13})$ where $\pi_3 = 1/2 + \sqrt{13}/2$. π_3 is not totally positive. By Theorem 4.11 we must check whether $k(\sqrt{-\pi_3\varepsilon_k}) = \boldsymbol{Q}(\sqrt{-(4+\sqrt{13})}) = K$ can be embedded in A. The minimal polynomial of $K/\boldsymbol{Q}$ is $f(x) = x^4 + 8x^2 + 3$ and $d(f) = 2^8 \cdot 13^2 \cdot 3$. 13^2 divides $d(K)$ because $13\boldsymbol{Z}$ ramifies in $k/\boldsymbol{Q}$. $f(x) \equiv (x+3)^2(x-3)^2 \pmod{13}$ and by Lemma 6.2 there are two primes of K lying above $13\boldsymbol{Z}$. Since $\mathfrak{p}_{13}$ is the only prime of k lying above $13\boldsymbol{Z}$, $\mathfrak{p}_{13}$ must split in K. Therefore $U(\Gamma_3)$ is smooth.

Now consider $A(13; \mathfrak{p}_3', \mathfrak{p}_{13})$ and Γ_3'. $\pi_{13} = -1/2 + \sqrt{13}/2)$. $K = k(\sqrt{-\pi_{13}\varepsilon_k}) = Q(\sqrt{(-5-\sqrt{13})/2})$. $f(x) = x^4 + 5x^2 + 3$ and $d(f) = 2^4 \cdot 3 \cdot 13^2$. $f(x) \equiv (x-2)^2(x+2)^2 \pmod{13}$ and $U(\Gamma_3')$ is smooth.

Consider Γ_{13}. $\pi_{13} = \sqrt{13}$. We must check whether $K = k(\sqrt{-\pi_{13}\varepsilon_k}) = Q(\sqrt{(-13-3\sqrt{13})/2})$ can be embedded in A. $f(x) = x^4 + 13x^2 + 13$ and $d(f) = 2^4 \cdot 3^4 \cdot 13^2$. In this case we cannot use Lemma 6.2. Instead we will factor $f(x)$ 3-adically. 13 is a 3-adic square because $(13/3) = 1$. In fact $\sqrt{13} = (1, 7, 16, \cdots)$. $2\sqrt{13} - 13 = (1, 1, 19, \cdots)$ which is again a 3-adic square and thus, $f(x)$ factors in the second way listed in Lemma 6.4. $a^2 - 4b = 117 = 3^2 \cdot 13$. Again, this is a 3-adic square and by the lemma $f(x)$ factors completely. Thus, there are four distinct primes of K lying above $3\boldsymbol{Z}$ and K cannot be embedded in A for either choice of A. This leads to two more smooth $p_g = 0$ surfaces $U(\Gamma_{13})$.

EXAMPLE 3. $A(17; \mathfrak{p}_2, \mathfrak{p}_{13})$, $A(17; \mathfrak{p}_2', \mathfrak{p}_{13})$, $A(17; \mathfrak{p}_2, \mathfrak{p}_{13}')$ and $A(17; \mathfrak{p}_2', \mathfrak{p}_{13}')$. Both $2\boldsymbol{Z}$ and $13\boldsymbol{Z}$ split in $Q(\sqrt{17})$. $E(U(\Gamma(1))) = 8/12 \cdot (13-1)(2-1) = 8$. $(-1/13) = 1$ and $(-3/13) = 1$. Thus, $U(\Gamma(1))$ is a smooth $p_g = 1$ surface.

$\varepsilon_k = 4 + \sqrt{17}$ and is not totally positive. The possible coset representatives for index 2 subgroups of B are $\{\Pi_2', 1\}$, $\{\Pi_{13}', 1\}$ and $\{\Pi_2'\Pi_{13}', 1\}$. As before we can immediately eliminate the last case.

Let $\pi_2 = ((3 + \sqrt{17})/2)$, $\pi_2' = ((-3 + \sqrt{17})/2)$, $\pi_{13} = 2 + \sqrt{17}$ and $\pi_{13}' = -2 + \sqrt{17}$. None of these are totally positive.

Consider Γ_2 and the appropriate algebras. $K = k(\sqrt{-\pi_2\varepsilon_k}) = Q(\sqrt{(-29 - 7\sqrt{17})/2})$. $f(x) = x^4 + 29x^2 + 2$ and $d(f) = 2^5 \cdot 7^4 \cdot 17^2$. $f(x) \equiv (x^2+2)(x-5)(x+5) \pmod{13}$. Thus, three primes of K lie above $13\boldsymbol{Z}$ and either $\mathfrak{p}_{13}$ or $\mathfrak{p}_{13}'$ splits in K/k. We would like to factor $g(x) = x^2 - (29 + 7\sqrt{17})/2$ $\mathfrak{p}_{13}$-adically and $\mathfrak{p}_{13}'$-adically. By Lemma 6.3 it suffices to factor $g(x) \bmod \pi_{13}$ and $\bmod \pi_{13}'$.

$$\begin{aligned} -(29 + 7\sqrt{17})/2 &\equiv -(29 + 7\sqrt{17})/2 + (2 + \sqrt{17})(1 + 3\sqrt{17})/2 \pmod{\pi_{13}} \\ &\equiv 12 \pmod{13} \end{aligned}$$

12 is a square modulo 13 and thus, $g(x)$ factors. Therefore, there are two primes of K lying above $\mathfrak{p}_{13}$ and $U(\Gamma_2)$ is smooth if the algebra is chosen to be $A(17; \mathfrak{p}_2, \mathfrak{p}_{13})$.

$$\begin{aligned} -(29+7\sqrt{17})/2 &\equiv -(29+7\sqrt{17})/2+(2-\sqrt{17})(-1+3\sqrt{17})/2 \pmod{\pi_{13}'} \\ &\equiv 11 \pmod{13} \end{aligned}$$

11 is not a square modulo 13. We conclude that $U(\Gamma_2)$ is not smooth if the algebra is chosen to be $A(17; \mathfrak{p}_2, \mathfrak{p}_{13}')$.

Consider Γ_2'. $K = k(\sqrt{-\pi_2'\varepsilon_k}) = Q(\sqrt{(-5-\sqrt{17})/2})$. $f(x) = x^4 +$

$5x^2 + 2$ and $d(f) = 2^5 \cdot 17^2$. $f(x) \equiv (x^2 - 5)(x + 4)(x - 4) \pmod{13}$. Thus, there are three primes of K lying above $13\boldsymbol{Z}$. Again to factor $g(x) = x^2 - (-5 - \sqrt{17})/2$ $\mathfrak{p}'_{13}$-adically it suffices to factor $g(x)$ modulo π'_{13}.

$$\begin{aligned}(-5 - \sqrt{17})/2 &\equiv (-5 - \sqrt{17})/2 + (2 + \sqrt{17})(-1 + \sqrt{17})/2 \pmod{\pi_{13}} \\ &\equiv 5 \pmod{13}\end{aligned}$$

Thus, $g(x)$ does not factor $\mathfrak{p}_{13}$-adically. We conclude that Γ'_2 and $A(17; \mathfrak{p}'_2, \mathfrak{p}_{13})$ do not lead to a smooth surface.

$$\begin{aligned}(-5 - \sqrt{17})/2 &\equiv (-5 - \sqrt{17})/2 + (2 - \sqrt{17})(1 + \sqrt{17})/2 \pmod{\pi'_{13}} \\ &\equiv 3 \pmod{13}\end{aligned}$$

Thus, $g(x)$ factors modulo π'_{13} and $U(\Gamma'_2)$ is smooth if the algebra is chosen to be $A(17; \mathfrak{p}'_2, \mathfrak{p}'_{13})$.

Consider Γ_{13}. $K = k(\sqrt{-\pi_{13}\varepsilon_k}) = \boldsymbol{Q}(\sqrt{-25 - 6\sqrt{17}})$, $f(x) = x^4 + 50x^2 + 13$ and $d(f) = 2^{12} \cdot 3^4 \cdot 13 \cdot 17^2$. $f(x)$ factors 2-adically as a product of three irreducible polynomials. Thus, one of $\mathfrak{p}_2$ or $\mathfrak{p}'_2$ splits in K/k, but this provides no information about which of these primes splits. Instead we factor $g(x) = x^2 - (25 + 6\sqrt{17})$ $\mathfrak{p}_2$-adically and $\mathfrak{p}'_2$-adically. $d(g) = 4(25 + 6\sqrt{17})$. By Lemma 6.3 it is sufficient to factor $g(x)$ modulo π_2^3 and modulo $\pi_2'^3$. $\pi_2^3 = (45 + 11\sqrt{17})/2$ and

$$\begin{aligned}-25 - 6\sqrt{17} &\equiv -25 - 6\sqrt{17} + (-3 + \sqrt{17})(45 + 11\sqrt{17})/2 \pmod{\pi_2^3} \\ &\equiv 1 \pmod{8}.\end{aligned}$$

Thus, $g(x)$ factors $\mathfrak{p}_2$-adically. We conclude that $U(\Gamma_{13})$ is smooth if the algebra is chosen to be $A(17; \mathfrak{p}_2, \mathfrak{p}_{13})$. $\pi_2'^3 = (45 - 11\sqrt{17})/2$ and

$$\begin{aligned}-25 - 6\sqrt{17} &\equiv -25 - 6\sqrt{17} + (3 + \sqrt{17})(45 - 11\sqrt{17})/2 \pmod{\pi_2'^3} \\ &\equiv 5 \pmod{8}.\end{aligned}$$

Thus, $g(x)$ does not factor $\mathfrak{p}'_2$-adically. We conclude that $U(\Gamma_{13})$ is not smooth if the algebra is chosen to be $A(17; \mathfrak{p}'_2, \mathfrak{p}_{13})$.

Finally, consider Γ'_{13}. $K = k(\sqrt{-\pi'_{13}\varepsilon_k}) = \boldsymbol{Q}(\sqrt{-9 - 2\sqrt{17}})$ and $d(f) = 2^{12} \cdot 13 \cdot 17^2$. Let $g(x) = x^2 - (-9 - 2\sqrt{17})$. Again, we factor $g(x)$ modulo π_2^3 and modulo $\pi_2'^3$.

$$\begin{aligned}-9 - 2\sqrt{17} &\equiv -9 - 2\sqrt{17} + (-16 + 4\sqrt{17})(45 + 11\sqrt{17})/2 \pmod{\pi_2^3} \\ &\equiv 5 \pmod{8}\end{aligned}$$

$$\begin{aligned}-9 - 2\sqrt{17} &\equiv -9 - 2\sqrt{17} + (-29 - 7\sqrt{17})(45 - 11\sqrt{17})/2 \pmod{\pi_2'^3} \\ &\equiv 1 \pmod{8}\end{aligned}$$

Thus, $U(\Gamma'_{13})$ is smooth if $A = (17; \mathfrak{p}'_2, \mathfrak{p}'_{13})$ and is not smooth if $A = A(17; \mathfrak{p}_2, \mathfrak{p}'_{13})$.

The following are all $p_g = 0$ (nonsingular) surfaces arising from Γ lying between $\Gamma(1)$ and B.

(I) Smooth $\Gamma(1)$-surfaces having geometric genus 0.

(1) $A(8; \mathfrak{p}_2, \mathfrak{p}_5)$
(2) $A(12; \mathfrak{p}_2, \mathfrak{p}_{13})$
(3) $A(12; \mathfrak{p}_2, \mathfrak{p}'_{13})$

(II) Smooth E-surfaces ($E \supsetneq \Gamma(1)$) having geometric genus 0.

(1) $A(12; \mathfrak{p}_2, \mathfrak{p}_5)$
(2) $A(12; \mathfrak{p}_3, \mathfrak{p}_{13})$
(3) $A(12; \mathfrak{p}_3, \mathfrak{p}'_{13})$
(4) $A(21; \mathfrak{p}_2, \mathfrak{p}_5)$
(5) $A(21; \mathfrak{p}_2, \mathfrak{p}'_5)$
(6) $A(24; \mathfrak{p}_3, \mathfrak{p}_5)$
(7) $A(24; \mathfrak{p}_3, \mathfrak{p}'_5)$

(III) Smooth geometric genus 0 surfaces from Γ, $E \subsetneq \Gamma \subset B$.

	Algebra	Group
(1)	$A(5; \mathfrak{p}_5, \mathfrak{p}_{31})$	Γ_5
(2)	$A(5; \mathfrak{p}_5, \mathfrak{p}_{31})$	Γ_{31}
(3)	$A(5; \mathfrak{p}_5, \mathfrak{p}'_{31})$	Γ_5
(4)	$A(5; \mathfrak{p}_5, \mathfrak{p}'_{31})$	Γ'_{31}
(5)	$A(5; \mathfrak{p}_2, \mathfrak{p}_{41})$	Γ_2
(6)	$A(5; \mathfrak{p}_2, \mathfrak{p}_{41})$	Γ_{41}
(7)	$A(5; \mathfrak{p}_2, \mathfrak{p}'_{41})$	Γ_2
(8)	$A(5; \mathfrak{p}_2, \mathfrak{p}'_{41})$	Γ'_{41}
(9)	$A(8; \mathfrak{p}_3, \mathfrak{p}_7)$	Γ_3
(10)	$A(8; \mathfrak{p}_3, \mathfrak{p}'_7)$	Γ_3
(11)	$A(13; \mathfrak{p}_3, \mathfrak{p}_{13})$	Γ_3
(12)	$A(13; \mathfrak{p}_3, \mathfrak{p}_{13})$	Γ_{13}
(13)	$A(13; \mathfrak{p}'_3, \mathfrak{p}_{13})$	Γ'_3
(14)	$A(13; \mathfrak{p}'_3, \mathfrak{p}_{13})$	Γ_{13}

For the next 4 examples it is necessary to specify the particular primes. In $Q(\sqrt{17})$ both $13Z$ and $2Z$ split. Let $\mathfrak{p}_2$ be the ideal generated by $(3+\sqrt{17})/2$ and $\mathfrak{p}'_2$ be the ideal generated by $(-3+\sqrt{17})/2$. Similarly, $\mathfrak{p}_{13}$ is generated by $2+\sqrt{17}$ and $\mathfrak{p}'_{13}$ is generated by $-2+\sqrt{17}$.

(15)	$A(17; \mathfrak{p}_2, \mathfrak{p}_{13})$	Γ_{13}
(16)	$A(17; \mathfrak{p}_2, \mathfrak{p}_{13})$	Γ_2
(17)	$A(17; \mathfrak{p}'_2, \mathfrak{p}'_{13})$	Γ'_2
(18)	$A(17; \mathfrak{p}'_2, \mathfrak{p}'_{13})$	Γ'_{13}

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
2. M. Eichler, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren*

über algebraishen Zahlkörpern undihre L-Reihen, J. Reine Angew. Math., **179** (1938), 227–251.

3. F. Hirzebruch, *Topological Methods in Algebraic Geometry*, Springer-Verlag, New York, 1966.

4. F. Hirzebruch, *Hilbert Modular Surfaces*, L'Eiseignement Mathematique, Université Genève, 1973.

5. H. W. Leopoldt, *Eine Verallgemeinerang der Bernoullischen Zahlen*, Abh. Math. Seminar, Hamburg, **22** (1958), 131–140.

6. Y. Matsushima and G. Shimura, *On the cohomology groups attached to certain vector valued differential forms on the product of the upper half planes*, Ann. of Math. (2), **78** (1963), 417–449.

7. H. Shimizu, *On discontinuous groups operating on the product of the upper half planes*, Ann. of Math. (2), **77** (1963), 33–71. For correction see: H. Shimizu, *On zeta functions of quaternion algebras*, Ann. of Math. (2), **81** (1965), 166–193.

8. G. Shimura, *Introduction to Arithmetic Theory of Automorphic Functions*, Princeton University Press, Princeton, 1971.

Received July 26, 1977.

THE UNIVERSITY OF NEBRASKA-LINCOLN
LINCOLN, NE 68508

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

RICHARD ARENS (Managing Editor)
University of California
Los Angeles, California 90024

C. W. CURTIS
University of Oregon
Eugene, OR 97403

C. C. MOORE
University of California
Berkeley, CA 94720

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, California 90007

R. FINN AND J. MILGRAM
Stanford University
Stanford, California 94305

ASSOCIATE EDITORS

E. F. BECKENBACH B. H. NEUMANN F. WOLF K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA, RENO
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF HAWAII
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics
Vol. 76, No. 1 November, 1978