JOURNAL OF NUMBER THEORY 21, 176–184 (1985)

The Conjugacy Problem of the Modular Group and the Class Number of Real Quadratic Number Fields

CHARLES TRAINA

Department of Mathematics and Computer Science,
St. John's University, Grand Central
and Utopia Parkways, Jamaica, New York 11439

Communicated by O. Taussky Todd

Received September 14, 1983

We shall discuss the conjugacy problem of the modular group, and show how its solution, in conjunction with a theorem of Olga Taussky can be used to compute the class number of certain real quadratic number fields. © 1985 Academic Press, Inc.

1. INTRODUCTION

We propose to reverse the case of the theorem which had been mentioned [1948] by Olga Taussky in a letter to Wilhelm Magnus. She observed that all elements of order two (i.e., with trace zero) are conjugate in $PSL(2, Z)$ and, similarly, all elements of order three with trace $+1$, since the corresponding quadratic fields have class number one. Exercise 4, p. 133 in Magnus [2] is based on this remark which can also be derived most easily from the Kurosh subgroup theorem according to which the elements of finite order in a free product are conjugates of elements of finite order in the factors, $PSL(2, Z)$ being the free product of a group of order 3 and a group of order 2. (Since, in the upper complex half plane $z=i$ is a fixed point of an element of order 2 in $PSL(2, Z)$, the images of $z=i$ under the action of this group must be exactly the fixed points of the other elements of order 2 which are of the form $(a+i)/c$, where a, c are integers, $c>0$, and c divides a^2+1.) In our paper, we shall again use the abstract theory of $PSL(2, Z)$ to derive results about numbers of ideal classes in real quadratic number fields.

We shall call a modification of the Latimer and MacDuffee Theorem [5] the Taussky Theorem, whose statement is as follows:

THEOREM. (Olga Taussky). *Let M be a matrix in $SL(2, Z)$ with a trace $t \geqslant 3$. Let ω_1, ω_2 be the roots of the characteristic equation of M. Then the*

0022-314X/85 $3.00

number of ideal classes in the ring $R(\omega)$, generated by ω_1, ω_2, equals the number of conjugacy classes of M in $GL(2, Z)$. In certain cases, $R(\omega)$ is identical with the ring of algebraic integers in the field $\mathbb{Q}(\sqrt{\Delta})$, where $\Delta \geqslant 3$ is a positive integer. Specifically,

$$\Delta = t^2 - 4 \qquad \textit{for} \quad t \equiv 1 \pmod 2, \textit{ if } \Delta \textit{ is square free.}$$

$$\Delta = \tfrac{1}{4}t^2 - 1 \qquad \textit{for} \quad t \equiv 0 \pmod 2, \textit{ if } \Delta \textit{ is square free.}$$

We shall first discuss the conjugacy problem in the abstract group $PSL(2, Z)$ (the ordinary modular group) and then in the group $SL(2, Z)$ as a subgroup of $GL(2, Z)$, where now the elements are given as matrices. Then we shall show how the Taussky theorem enables us to compute quickly a few class numbers some of which we take from a table published in Hasse [1].

2. The Conjugacy Problem of the Modular Group

Consider the homogeneous modular group $SL(2, Z)$ with presentation $\langle a, b; a^2 = b^3 = -1 \rangle$, where $a = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $b = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$, and we write 1 for the 2×2 identity matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and trace $(a) = 0$, trace $(b) = 1$.

Up to conjugation any word $W \in SL(2, Z)$ other than $\pm 1, a^{\pm 1}, \pm b^{\pm 1}$ can be expressed as

$$W = W(a, b) = \pm ab^{\varepsilon_1}ab^{\varepsilon_2} \cdots ab^{\varepsilon_n} \tag{1}$$

where $\varepsilon_i = \pm 1$ for $i = 1, 2, \ldots, n$, with the upper sign in (1) holding if there are an even number of factors $a^{-1}b^{\varepsilon} = -ab^{\varepsilon}$ in (1), and the lower sign holding if there are an odd number of factors $a^{-1}b^{\varepsilon} = -ab^{\varepsilon}$ in (1).

We call (1) the *normal form* of an element of $SL(2, Z)$ other than $a^{\pm 1}$, $\pm b^{\pm 1}$, ± 1, and *the positive integer n is called the syllable length of W.*

We will make use of the following result for the trace, which we will now write as tr, of words in two generators. Let U, V be any two elements of $SL(2, Z)$ and let $W = W(U, V)$ be a word in U and V (note that U and V are generators of a group G_2). Put tr $U = x_1$, tr $V = x_2$, tr $UV = z$. We may consider x_1, x_2, z as indeterminates. It is known that

$$\operatorname{tr} W = f_w(x_1, x_2, z)$$

is a polynomial with integral coefficients in these indeterminates, and we call f_w the *Fricke polynomial of W.* We shall say that *W is in standard form* if

$$W = U^{n_1}V^{m_1}U^{n_2}V^{m_2} \cdots U^{n_l}V^{m_l} \tag{2}$$

where $n_i, m_i \in Z - \{0\}$, $i = 1, 2, \ldots, l$, and *we shall call l the syllable length of W* as a word in U and V.

We have an explicit expression for tr W, where W is defined by (2). We need some auxiliary polynomials which are essentially the Chebychev polynomials and the associated Chebychev functions which are defined most easily in terms of trigonometric functions as polynomials in $2\cos\varphi$ by the formulas

$$T_n(2\cos\varphi) = 2\cos n\varphi, \qquad P_n(2\cos\varphi) = \frac{\sin(n+1)\varphi}{\sin\varphi}, \qquad n \in Z. \quad (3)$$

We then have tr $U^n = T_{|n|}(x_1)$ and the following:

THEOREM. *If W is defined by* (2), *then* tr W *is a polynomial of exact degree l in z. The coefficient of z^l is*

$$\prod_{\nu=1}^{l} P_{n_\nu - 1}(x_1) P_{m_{\nu-1}}(x_2).$$

The remaining coefficients can be defined recursively.

Remark 1. If we put $y = -\mathrm{tr}\,(\bar{a}\bar{b})$ (an indeterminate), where $\bar{a}, \bar{b}$ are elements of $SL(2, Z)$ with $\mathrm{tr}(\bar{a}) = 0$, $\mathrm{tr}(\bar{b}) = 1$, then from the previous theorem, the trace of an element of $SL(2, Z)$ in normal form

$$\bar{a}\bar{b}^{\varepsilon_1} \cdots \bar{a}\bar{b}^{\varepsilon_n}, \ \varepsilon_i = \pm 1, \ i = 1, \ldots, n \qquad (1')$$

is a polynomial $P_n(y)$ with integral coefficients of exact degree n, the syllable length of (1′) in y. Let $\bar{P} = -\bar{a}\bar{b}$, $\bar{Q} = \bar{a}\bar{b}^{-1}$. Then, tr $\bar{P} = $ tr $\bar{Q} = y$.

We recall that the trace of elements of $SL(2, Z)$ satisfies the following properties: for any $U, V \in SL(2, Z)$,

(i) $\mathrm{tr}\, U = \mathrm{tr}\, U^{-1}$

(ii) $\mathrm{tr}(UV) = \mathrm{tr}(VU)$

(iii) $\mathrm{tr}(VUV^{-1}) = \mathrm{tr}\, U$

(iv) $\mathrm{tr}(UV) = \mathrm{tr}\, U \cdot \mathrm{tr}\, V - \mathrm{tr}(UV^{-1})$.

THEOREM 1. *If n is odd* (*even*) *then* tr $(\bar{a}\bar{b}^{\varepsilon_1}\bar{a}\bar{b}^{\varepsilon_2} \cdots \bar{a}\bar{b}^{\varepsilon_n})$ *is an odd* (*even*) *polynomial in $y = -\mathrm{tr}(\bar{a}\bar{b})$ of degree n.*

Proof. The proof is by induction with respect to the syllable length n, using the properties of the trace. As a consequence of this, one obtains the following: the mapping $\bar{a} \mapsto \bar{a}$, $\bar{b} \mapsto \bar{b}^{-1}$ defines an automorphism of the modular group which induces the ring automorphism $y \mapsto -y$ in the polynomial ring $Z[y]$ which contains the characters of the modular group, Therefore, we have

THEOREM 2. *Let $P_n(y)$ be the trace of $\bar{a}\bar{b}^{\varepsilon_1}\bar{a}\bar{b}^{\varepsilon_2}\cdots\bar{a}\bar{b}^{\varepsilon_n}$. Then $P_n(-y)$ is the trace of $\bar{a}\bar{b}^{-\varepsilon_1}\bar{a}\bar{b}^{-\varepsilon_2}\cdots\bar{a}\bar{b}^{-\varepsilon_n}$. If n is odd, $P^n(-y)=-P_n(y)$. If n is even, $P_n(y)=P_n(-y)$.*

We wish to obtain an estimate for the number of distinct trace polynomials $P_n(y)$. As a step toward obtaining this estimate, we consider the following:

PROBLEM. To find the number of cyclically different words $ab^{\varepsilon_1}ab^{\varepsilon_2}\cdots ab^{\varepsilon_n}$, $\varepsilon_i=\pm 1$, $i=1, 2, ..., n$.

Let c_n denote this number. There are altogether 2^n words under consideration. Let γ_n denote the number of cyclically inequivalent words of length n which are also not cyclically equivalent to a proper power (=exponent > 1). Let d denote the divisors of n. We shall write $d\,|\,n$.

Since when cyclically reduced, two words are cyclically equivalent if and only if they are cyclic permutations of each other, we have

1. *Claim:* $c_n=\sum_{d|n}\gamma_d$
2. *Claim:* $\sum_{d|n} d\gamma_d=2^n$.

By the Moebius inversion theorem, we find $\gamma_d=(1/d)\sum_{\delta|d}2^{d/\delta}\mu(\delta)$, where δ is a divisor of d, $\mu(\delta)$ is the Moebius function. Therefore,

$$c_n=\sum_{d|n}(1/d)\sum_{\delta|d}2^{d/\delta}\mu(\delta).$$

Incidentally, γ_d is the exact number of irreducible polynomials in x of degree d with coefficients in a field of 2 elements and highest coefficient 1, and c_n is the exact number of irreducible polynomials of positive degree $\leqslant n$ (and highest coefficient 1).

THEOREM 3. *The number of distinct trace polynomials for* $\mathrm{tr}(\bar{a}\bar{b}^{\varepsilon_1}\bar{a}\bar{b}^{\varepsilon_2}\cdots\bar{a}\bar{b}^{\varepsilon_n})$ *with* $\mathrm{tr}(\bar{a})=0$, $\mathrm{tr}(\bar{b})=1$, *is at most* $2^{[(n+1)/2]}$, *where* $[(\mathrm{n}+1)/2]$ *denotes the greatest integer* $\leqslant\frac{1}{2}(n+1)$.

Proof. Let ρ_n denote the number of distinct trace polynomials for $\mathrm{tr}(\bar{a}\bar{b}^{\varepsilon_1}\bar{a}\bar{b}^{\varepsilon_2}\cdots\bar{a}\bar{b}^{\varepsilon_n})$. Since $P_n(y)=\mathrm{tr}(\bar{a}\bar{b}^{\varepsilon_1}\bar{a}\bar{b}^{\varepsilon_2}\cdots\bar{a}\bar{b}^{\varepsilon_n})$ is of exact degree n, there can be at most $n+1$ terms in $P_n(y)$. Moreover, since $P_n(y)$ is odd (even) according to whether n is odd (even), $P_n(y)$ will in fact have at most $[\frac{1}{2}(n+1)]$ terms. For each of these terms, other than the lead term, there are two choices, either it does or does not occur. Thus, there can be at most $2^{[(n+1)/2]}$ distinct polynomials for a given n. Therefore, $\rho_n\leqslant 2^{[(n+1)/2]}$.

As a step towards the solution to the conjugacy problem of $SL(2, Z)$ as a subgroup of $GL(2, Z)$ we have, with eight exceptions, a canonical form for the representatives of the conjugacy classes of elements of $SL(2, Z)$.

THEOREM 4. *Every matrix in $SL(2, Z)$ with a trace $t \neq \pm 2, \pm 1, 0$ is conjugate in $GL(2, Z)$ with a product*

$$W = \pm P^{\alpha_1} Q^{\beta_1} P^{\alpha_2} Q^{\beta_2} \cdots P^{\alpha_s} Q^{\beta_s}$$

where $P = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = -ab$, $Q = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) = ab^{-1}$; $\alpha_1, \beta_1, ..., \alpha_s, \beta_s \in Z^+$. *We shall now call s* the syllable length of *W (as a word in P and Q) and* $L = \alpha_1 + \beta_1 + \cdots + \alpha_s + \beta_s$ the length of *W.*

Proof. The presentation of $SL(2, Z)$ gives immediately this result.

As an immediate consequence of Theorem 4 we deduce the following:

THEOREM 5. *Every element in $SL(2, Z)$ with a positive trace $\geqslant 3$ is conjugate with an element in which all entries are positive.*

The polynomials $P_n(y)$ introduced in Remark 1 as the trace of a word in $SL(2, Z)$ in normal form (1), again enter the picture for our words in $\bar{P}$ and $\bar{Q}$. Specifically, we have

THEOREM 6. *If we put* tr $\bar{P} =$ tr $\bar{Q} = y$ *(an indeterminate), our traces for* $\bar{W} = \bar{P}^{\alpha_1} \bar{Q}^{\beta_1} \cdots \bar{P}^{\alpha_s} \bar{Q}^{\beta_s}$; $\alpha_1, \beta_1, ..., \alpha_s, \beta_s \in Z^+$, *become our trace polynomials $P_n(y)$. Their* degree is the length *(i.e., the number* $L = \alpha_1 + \beta_1 + ... + \alpha_s + \beta_s$, *not the syllable length s) of $\bar{W}$.*

Proof. The result follows immediately from the definitions of $\bar{P}$ and $\bar{Q}$ and Remark 1.

Theorem 6 provides an easy test for nonconjugacy of positive words in $SL(2, Z)$.

COROLLARY 6.1. *Two words W and W', positive words in $\bar{P}$ and $\bar{Q}$, of different lengths can never be conjugate in $GL(2, Z)$.*

Our canonical form given in Theorem 4 provides an estimate, in the form of a lower bound, for the trace of a positive word in P and Q.

THEOREM 7. *Let $W \in SL(2, Z)$ be given as a product*

$$W = P^{\alpha_1} Q^{\beta_1} P^{\alpha_2} Q^{\beta_2} \cdots P^{\alpha_s} Q^{\beta_s},$$

where $P = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $Q = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $\alpha_1, \beta_1, ..., \alpha_s, \beta_s \in Z^+$. *Then, for every positive integer s,* tr $W > 2^s$. *Thus,* tr *W goes to infinity with the syllable length s.*

Proof. The proof is by an induction on the syllable length s, and the remark that for a given s tr W is minimal if all exponents α_i, β_j, are minimal, i.e., equal to $+1$. Therefore, the trace of W cannot be less than that of W_0^s where

$$W_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

and clearly $2^s < \operatorname{tr} W_0^s = (\frac{3}{2} + \frac{1}{2}\sqrt{5})^s + (\frac{3}{2} - \frac{1}{2}\sqrt{5})^s \leqslant 3^s$.

In order to compute the class number of the real quadratic number field associated with an element of $SL(2, Z)$ having a positive trace $\geqslant 3$ by the theorem of Olga Taussky, we need to discuss the conjugacy problem of $SL(2, Z)$ as a subgroup of $GL(2, Z)$. We shall first discuss the conjugacy problem in the abstract group $PSL(2, Z)$, the quotient group of $SL(2, Z)$ with respect to its center $= \{\pm 1\}$.

Since $PSL(2, Z)$ is a free product, of a cyclic group of order two $= \langle a; a^2 = 1 \rangle$, and a cyclic group of order three $= \langle b; b^3 = 1 \rangle$, the solution to the conjugacy problem for $PSL(2, Z)$ is given by Theorem 4.2 of Magnus, Karrass, and Solitar [4]. We will call the normal form for a cyclically reduced element of $PSL(2, Z)$ other than $a, b^{\pm 1}, 1$ (up to conjugation) to be the product given by

$$ab^{\varepsilon_1} ab^{\varepsilon_2} \cdots ab^{\varepsilon_n}, \ \varepsilon_i = \pm 1, i = 1, 2, ..., n, \tag{4}$$

where n is the syllable length (which corresponds, apart from a ± sign, to our words in P and Q); the solution to the conjugacy problem for $PSL(2, Z)$ can be stated as:

Two cyclically reduced elements of $PSL(2, Z)$ in normal form are conjugate only if they are cyclic permutations of each other. (Note, for a given syllable length n we know the number of cyclically different words (4), it is c_n).

In $SL(2, Z)$ from the normal form (1) of a cyclically reduced element, the conjugacy problem has the same solution apart from a splitting of each conjugacy class of $PSL(2, Z)$ into two classes, differing by a ± sign. If W is an element, it can be conjugate with $-W$ only if its trace is zero, a case we do not need. Now in $SL(2, Z)$ within $GL(2, Z)$ the conjugacy classes become larger but, (since the index of $SL(2, Z)$ within $GL(2, Z)$ is 2) not more than two classes of $SL(2, Z)$ can combine into a single class in $GL(2, \mathrm{Z})$. Now, the conjugacy of P and Q in $GL(2, Z)$ ($P = XQX^{-1}$, where $X = (\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}) \in GL(2, Z) - SL(2, Z)$) provides exactly this coagulation. Together with Theorem 4 and Corollary 6.1 we have proved

THEOREM 8. *Two words M and M' can be conjugate in $GL(2, Z)$ only if they have the same syllable lengths and if the sets of exponents α, β coincide* *apart from their arrangement. (Note that P and Q are conjugate, and that therefore we can exchange the α and β.)*

3. Computation of Class Numbers

The theorem of Olga Taussky together with Theorem 8 enables us to compute a few class numbers quickly. From Theorem 8, distinct conjugacy classes can arise from different syllable lengths or from different sets of exponents α, β.

The trace t of W, a positive word in P and Q, is a monotonically increasing function in each of the α, β (an inductive argument on the syllable length shows this). For $s=1$ we have

$$t = 2 + \alpha_1\beta_1,$$

and the minimum value is 3. For $s=2$,

$$t = (1+\alpha_1\beta_1)(1+\alpha_2\beta_2) + \beta_1\alpha_2 + \alpha_1\beta_2 + 1,$$

and the minimum value is 7. For $s=3$,

$$\begin{aligned} t = {} & (1+\alpha_1\beta_1)(1+\alpha_2\beta_2)(1+\alpha_3\beta_3) + \alpha_1\beta_2 + \alpha_1\beta_3 \\ & + \alpha_2\beta_3 + \alpha_2\beta_1 + \alpha_3\beta_1 + \alpha_3\beta_2 + \alpha_1\beta_2\alpha_3\beta_3 \\ & + \alpha_2\beta_2\alpha_3\beta_1 + \alpha_1\beta_1\alpha_2\beta_3 + 1, \end{aligned}$$

and the minimum value is 18, with the next larger value at least 26.

According to the theorem of Olga Taussky, we have that for $t=3, 4, 5, 8, 9, 12$ we obtain the integers in the full number field $\mathbb{Q}(\sqrt{\Delta})$ where $\Delta = 5, 3, 21, 15 ,77, 35$. Following the notation of Hasse [1], h denotes the class number of the number field $\mathbb{Q}(\sqrt{\Delta})$.

We see immediately that the class number for $\Delta = 5, 3, 21$ is 1 and for $\Delta = 15$ the class number is 2.

Proof. $t=3$ is the absolute minimum value of the traces of all M (positive words in P and Q). It occurs only once for $s=1$, $\alpha_1 = \beta_1 = 1$. Therefore, $h=1$ for $\mathbb{Q}(\sqrt{5})$.

Similarly, $t=4$ must occur only for $s=1$. Therefore,

$$t = 4 = 2 + \alpha_1\beta_1, \qquad \therefore \alpha_1\beta_1 = 2.$$

Therefore, $(\alpha_1, \beta_1) = (2, 1)$ or $(1, 2)$ (which is the same). Thus, $h=1$ for $\mathbb{Q}(\sqrt{3})$.

Similarly, for $t=5$ we must have $s=1$, since for $s=2$ the minimum value of $t=7$. Therefore,

$$t=5=2+\alpha_1\beta_1; \qquad \alpha_1\beta_1=3.$$

Therefore, $(\alpha_1, \beta_1)=(3, 1)$ or $(1, 3)$, and again we have $h=1$ for $\mathbb{Q}(\sqrt{21})$.

However, the picture changes for $t=8, \Delta=15$. Again, we must have $s=1$, because for $s=2$ we have the minimum value for the trace equal to 7, but the next larger number for $s=2$ is at least 10. Therefore,

$$t=8=2+\alpha_1\beta_1, \qquad \therefore (\alpha_1, \beta_1)=(6, 1) \text{ or } (3, 2).$$

Therefore, $h=2$. (Note that by Theorem 8, the sets of exponents (6, 1), (3, 2) correspond to two nonconjugate elements $M=P^6Q^1$ and $M'=P^3Q^2$).

How can one obtain square free integers for Δ? One way of obtaining square free integers is by means of twin primes. Suppose $2n-1, 2n+1$ are twin primes. If we put $t=4n$ then $\Delta=\frac{1}{4}t^2-1=(2n-1)(2n+1)$ is square free. We can use this technique to construct number fields with class number at least 3.

EXAMPLES. (1) Set $t=4n=36$.

$$\therefore 2n-1=17,$$
$$2n+1=19.$$

Therefore $\Delta=323$, so that we have the number field $\mathbb{Q}(\sqrt{323})$. For $s=1$ we have

$$t=36=2+\alpha_1\beta_1; \qquad \alpha_1\beta_1=34.$$

Therefore, $(\alpha_1, \beta_1)=(1, 34)$ or $(2, 17)$.

For $s=2$ we have

$$t=36=(1+\alpha_1\beta_1)(1+\alpha_2\beta_2)+\alpha_1\beta_2+\beta_1\alpha_2+1.$$

Therefore, $(\alpha_1, \beta_1; \alpha_2, \beta_2)=(2, 1; 4, 2)$. $t=36$ does not occur again for $s=2$. Therefore, $h \geqslant 3$.

(2) Take $t=4n=60$.

$$2n-1=29,$$
$$2n+1=31.$$

Therefore $\Delta=899$, so that our number field is that of $\mathbb{Q}(\sqrt{899})$.

For $s=1$, $t=60=2+\alpha_1\beta_1$, $\therefore \alpha_1\beta_1=58$. Therefore, $(\alpha_1, \beta_1)=(1, 58)$ or $(2, 29)$.

For $s=2$, $t=60=(1+\alpha_1\beta_1)(1+\alpha_2\beta_2)+\alpha_1\beta_2+\beta_1\alpha_2+1$. Take $(\alpha_1, \beta_1; \alpha_2, \beta_2)=(1, 1; 2, 11)$. Therefore, $h \geqslant 3$.

As final illustrations of our results we construct two real quadratic number fields having class number of at least 4.

Examples. (1) Consider $t=32$. By the theorem of Olga Taussky, $\Delta=255=3\cdot 5\cdot 17$, and we have the number field $\mathbb{Q}(\sqrt{255})$.

For $s=1$, we have $t=32=2+\alpha_1\beta_1$. $\alpha_1\beta_1=30$. Therefore, $(\alpha_1, \beta_1)=(30, 1)$ or $(3, 10)$ or $(2, 15)$ or $(5, 6)$. Therefore, $h \geqslant 4$. By theorem 7, $t=32$ cannot occur for $s \geqslant 4$. By direct computation, $t=32$ does not occur for $s=2$, $s=3$. Hence, $h=4$.

(2) Consider $t=37$. Then, $\Delta=1365=3\cdot 5\cdot 7\cdot 13$ and we have the full number field $\mathbb{Q}(\sqrt{1365})$.

For $s=1$ we have: $t=37=2+\alpha_1\beta_1; \alpha_1\beta_1=35$. Therefore, $(\alpha_1, \beta_1)=(1, 35)$ or $(5, 7)$.

For $s=2$, $t=37=(1+\alpha_1\beta_1)(1+\alpha_2\beta_2)+\alpha_1\beta_2+\beta_1\alpha_2+1$. We find, $(\alpha_1, \beta_1; \alpha_2, \beta_2)=(1, 1; 1, 11)$.

For $s=3$ direct computation shows $(\alpha_1, \beta_1; \alpha_2, \beta_2; \alpha_3, \beta_3)=(2, 1; 1, 1; 2, 1)$. Therefore, $h \geqslant 4$. By Theorem 7, $t=37$ cannot occur for $s \geqslant 4$.

Acknowledgment

I wish to thank Dr. Wilhelm Magnus for suggesting this topic, and for his constant and invaluable help to its completion.

References

1. H. Hasse, "Number Theory," Springer-Verlag, Berlin/Heidelberg/New York, 1980.
2. W. Magnus, "Noneuclidean Tesselations and Their Groups," Academic Press, New York/London, 1974.
3. W. Magnus, The uses of 2 by 2 matrices in combinatorial group theory. A survey. *Resultate Math.* **4**, (1981), 171–192.
4. W. Magnus, A. Karrass and D. Solitar, "Combinatorial Group Theory," Dover, New York, 1976.
5. O. Taussky, On a theorem of Latimer and MacDuffee, *Canad. J. Math.* **1** (1949), 300–302.
6. C. Traina, Trace polynomial for two generator subgroups of $SL(2, \mathbb{C})$, *Proc. Amer. Math. Soc.* **79**, No. 3 (1980), 369–372.