Proceedings of the Royal Society of Edinburgh, **143A**, 893–903, *2013*

On the elliptic points of the Hilbert modular group of the totally real cyclotomic cubic field $\mathbb{Q}(\zeta_9)^+$

A. Arenas
Departament d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via 585, 08007 Barcelona, Spain (angelaarenas@ub.edu)

(MS received 21 February 2012; accepted 4 August 2012)

We determine explicitly the elliptic points with respect to the Hilbert modular group associated with the totally real cyclotomic cubic field $\mathbb{Q}(\zeta+\zeta^{-1})$, where ζ stands for a primitive 9th root of unity.

1. Introduction

Let ζ_9, or simply ζ, stand for a primitive 9th root of unity over $\mathbb{Q}$ (which in practice will be taken to be $e^{2\pi i/9}$). Then, $K := \mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta+\zeta^{-1})$, the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta)$, which will often be denoted simply by $\mathbb{Q}(\alpha)$, with $\alpha := \zeta+\zeta^{-1}$, is a totally real field of degree 3 over $\mathbb{Q}$, and $\mathcal{O}_K$ will stand for its ring of integers.

Denoting by $x \mapsto x'$ and $x \mapsto x''$ the two non-trivial $\mathbb{Q}$-automorphisms of K, it is well known that the (usual or narrow) Hilbert modular group $\Gamma := \mathrm{SL}(2,\mathcal{O}_K)$ acts (discontinuously and not faithfully) on $\mathbb{H}^3$, where $\mathbb{H}$ stands for the Poincaré upper half-plane, as follows:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : (z_1,z_2,z_3) \mapsto \left(\frac{az_1+b}{cz_1+d}, \frac{a'z_2+b'}{c'z_2+d'}, \frac{a''z_3+b''}{c''z_3+d''} \right),$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathcal{O}_K)$$

and z_i are complex numbers with strictly positive imaginary part, for $i=1,2,3$.

We recall that, by definition, a matrix (or the corresponding transformation on $\mathbb{H}^3$) is elliptic if and only if it has a fixed point in $\mathbb{H}^3$ (necessarily unique), and such a fixed point is called an elliptic point of Γ. Obviously, elliptic points of $\mathbb{H}^3$ in the same orbit under the action of Γ will be identified and we determine in this paper a complete set of representatives for the equivalence relation defined by the action of Γ.

There is, of course, an extensive literature devoted to the general study of elliptic points with respect to the Hilbert modular group (and not only in the narrow sense) of a totally real number field (see, for instance, [3, 4, 6]) where a number of complicated formulae appear in order to count the number of elliptic points.

Incidentally, justifications of these formulae rely on very interesting results on the arithmetic of quaternion algebras previously obtained by Eichler in [1]. But, as far as the applications are concerned, concrete and down to earth results seem to appear only in the case of real quadratic fields. Thus, we have been enthralled by the challenge of determining explicitly the elliptic points in the case of the cubic field $K = \mathbb{Q}(\zeta)^+$.

The number of elliptic points in this situation was computed by Weisser in [8], using the most elaborate results of Prestel (see [3]), which seem to throw no light at all on how the elliptic points can be effectively obtained. But Prestel's formulae are strongly based on earlier results of Shimizu (see [4]), which to some extent, via previous results of Eichler [1], seem to be more directly connected with the elliptic points themselves. Thus, even though our primary concern in this paper is with the explicit computation of elliptic points in the case $K = \mathbb{Q}(\zeta)^+$, we have also been challenged to see whether Weisser's results on the number of elliptic points can also be derived directly from Shimizu's formulae. The following contains a detailed description of what we have found out.

But, before we start, we state a few simple facts concerning the field $\mathbb{Q}(\zeta)^+$. The irreducible polynomial of $\alpha = \zeta + \zeta^{-1}$ over $\mathbb{Q}$ is $X^3 - 3X + 1$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, the conjugates of α are α, $\alpha' = \alpha^2 - 2$ and $\alpha'' = 2 - \alpha - \alpha^2$, and if we choose $\zeta = \mathrm{e}^{2\pi\mathrm{i}/9}$, as we do in the following, then $\alpha = 2\cos(2\pi/9) = 1.532088886\ldots$, $\alpha' = 0.347296355\ldots$ and $\alpha'' = -1.879385241\ldots$. It is also easy to see that the ring $\mathcal{O}_K$ of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$, the different is $3(\alpha^2 - 1)\mathcal{O}_K$, the discriminant is 81 (so $3\mathbb{Z}$ is the only prime ideal in $\mathbb{Z}$ that ramifies in $\mathcal{O}_K$), the rational prime 2 remains prime in $\mathcal{O}_K$ and the strict class number of K is 1 (in particular, $\mathcal{O}_K$ is principal).

2. Traces of elliptic matrices

To begin with, we determine the traces of the elliptic matrices.

Proposition 2.1. *The only possible traces of the elliptic matrices of the (narrow) Hilbert modular group* $\mathrm{SL}(2, \mathcal{O}_K)$ *of the maximal real subfield* $K = \mathbb{Q}(\alpha)$ *of the cyclotomic field* $\mathbb{Q}(\zeta)$ *are, up to signs and conjugates,* 0, 1 *and* α.

Proof. The elliptic matrices have finite orders and, consequently, are conjugate in $\mathrm{SL}(2, \mathbb{C})$ to matrices of the type

$$\begin{pmatrix} \xi, 0 \\ 0, \bar{\xi} \end{pmatrix},$$

with ξ a root of unity other than ± 1. As the trace $s = \xi + \bar{\xi}$ lies in $\mathbb{Q}(\zeta)^+$, we see that ξ can only be a 4th, 6th or 9th root of unity other than ± 1, from which the result follows. □

Remark 2.2. It is immediately seen from proposition 2.1 that the orders of elliptic matrices are 2, 3, 9, corresponding (up to signs and conjugates) to $s = 0, 1, \alpha$, respectively (see [8, corollary 1.8]).

Remark 2.3. Without invoking diagonalization of matrices, and recalling that a matrix M in $\mathrm{SL}(2, \mathcal{O}_K)$ is elliptic if and only if $s^2 - 4 \ll 0$, i.e. $s^2 - 4$ is totally

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

negative, where s stands for the trace of M, proposition 2.1 can alternatively be obtained by expressing s in the basis $1, \alpha, \alpha^2$ of K over $\mathbb{Q}$, $s = x + y\alpha + z\alpha^2$, with x, y, z in $\mathbb{Z}$, since $s \in \mathcal{O}_K$, and solving the system of inequalities

$$\begin{aligned} |x + y\alpha + z\alpha^2| &< 2, \\ |x + y\alpha' + z\alpha'^2| &< 2, \\ |x + y\alpha'' + z\alpha''^2| &< 2, \end{aligned}$$

whose solutions are easily seen to be $(0,0,0)$, $\pm(1,0,0)$, $\pm(0,1,0)$, $\pm(-2,1,1)$ and $\pm(2,0,-1)$.

3. Rings of integers and orders

For each trace value s appearing in proposition 2.1, we choose the particular elliptic matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix} \quad \text{in } \mathrm{SL}(2, \mathcal{O}_K).$$

This matrix will often be denoted by M_s, or simply by M if the reference to s is unnecessary.

This particular choice of matrix is harmless in the sense that any other matrix M' having the same trace and determinant as M satisfies the same irreducible equation as M, so sending M to M' defines a K-isomorphism between $K(M)$ and $K(M')$ and, consequently, $M' = AMA^{-1}$, for some invertible A in the ring $\mathcal{M}(2, K)$ of 2×2 matrices with entries in K, by virtue of the Skolem–Noether theorem.

Then, $K(M)$ is a totally imaginary quadratic extension of K contained in the ring $\mathcal{M}(2, K)$, where we consider K 'diagonally' embedded in $\mathcal{M}(2, K)$. $K(M)$ is a field K-isomorphic with $K(\sqrt{s^2 - 4})$, since M satisfies the equation $X^2 - sX + 1 = 0$.

The aim of this section is twofold: first, to find the integral closure of $\mathcal{O}_K = \mathbb{Z}[\alpha]$ in $K(M)$ or, equivalently, in $K(\sqrt{s^2 - 4})$, and, second, to compare the results obtained with the corresponding intersections of $K(M)$ with the maximal order $\mathcal{M}(2, \mathcal{O}_K)$ of $\mathcal{M}(2, K)$ consisting of the matrices with entries of $\mathcal{O}_K$. Obviously, the order of $K(M)$ obtained by intersecting with $\mathcal{M}(2, \mathcal{O}_K)$ is just

$$\begin{aligned} K(M) \cap \mathcal{M}(2, \mathcal{O}_K) &= \{x + yM \mid x, y \in K\} \cap \mathcal{M}(2, \mathcal{O}_K) \\ &= \left\{ \begin{pmatrix} x & -y \\ y & x + ys \end{pmatrix} \;\middle|\; x, y \in K \right\} \cap \mathcal{M}(2, \mathcal{O}_K) \\ &= \left\{ \begin{pmatrix} x & -y \\ y & x + ys \end{pmatrix} \;\middle|\; x, y \in \mathcal{O}_K \right\} \\ &= \mathcal{O}_K + \mathcal{O}_K \cdot M. \end{aligned}$$

So, we start by considering the cases $s = 0$ and α, up to signs and conjugates.

When $s = 0$, as $M_0^2 = -1$ by sending M_0 into $\sqrt{-1}$, we obtain a K-isomorphism between $K(M_0)$ and $K(\sqrt{-1})$. As the discriminants of $\mathbb{Q}(\sqrt{-1})$ and K are coprime, we can apply [2, Kap. 1, Satz 2.11] and conclude that $\mathcal{O}_K[\sqrt{-1}]$ is the ring of integers of $K(\sqrt{-1})$. Consequently, the order $K(M_0) \cap \mathcal{M}(2, \mathcal{O}_K)$ of $K(M_0)$ is maximal.

When $s = \alpha$, the equation for M_α over K is $X^2 - \alpha X + 1 = 0$. Recalling that $\alpha = \zeta + \zeta^{-1}$, we realize it is precisely the equation for ζ over K, so $M_\alpha \mapsto \zeta$ extends

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

to a K-isomorphism from $K(M_\alpha)$ onto $K(\zeta) = \mathbb{Q}(\zeta)$, the cyclotomic field. But the ring of integers of $\mathbb{Q}(\zeta)$ is just $\mathbb{Z}[\zeta]$ (see [2, Kap. 1, § 10]). This entails, as in the preceding case, that $K(M_\alpha) \cap \mathcal{M}(2, \mathcal{O}_K)$ is the maximal order of $K(M_\alpha)$.

Observe that similar results hold if α is replaced by $-\alpha$, $\pm\alpha'$ and $\pm\alpha''$, since the various fields $K(M_s)$, for $s \in \{\pm\alpha, \pm\alpha', \pm\alpha''\}$, are all K-isomorphic.

Applying the Skolem–Noether theorem to the above fields, which are all contained in $\mathcal{M}(2, K)$, we can realize the K-isomorphisms by means of inner automorphisms defined by suitable invertible matrices of $\mathcal{M}(2, K)$. As K-isomorphisms obviously preserve $\mathcal{O}_K$-integrality, we conclude that the orders obtained by intersecting with $\mathcal{M}(2, \mathcal{O}_K)$, which are clearly distinct, are, however, isomorphic under the inner automorphisms just quoted.

We now concentrate on the case $s = \pm 1$. Here

$$M = \begin{pmatrix} 0 & -1 \\ 1 & \pm 1 \end{pmatrix}$$

and $K(M) \simeq K(\sqrt{s^2 - 4}) = K(\sqrt{-3})$. In order to compute the ring of integers of $K(\sqrt{-3})$, and recalling that the prime 3 of $\mathbb{Z}$ totally ramifies in $\mathcal{O}_K$, actually in the form $3\mathcal{O}_K = \beta^3 \mathcal{O}_K$, with $\beta = \alpha + 1$, we observe first that $(3 + \sqrt{-3})/2\beta$ is integral over $\mathcal{O}_K$, since both its trace and norm (over K), namely $3/\beta$ and $3/\beta^2$, lie in $\mathcal{O}_K$. This is a key fact, as the following proposition shows.

PROPOSITION 3.1. *The ring of integers of* $K(\sqrt{-3})$ *is*

$$\mathcal{O}_K\left[\frac{3 + \sqrt{-3}}{2\beta}\right] = \mathcal{O}_K + \mathcal{O}_K \cdot \frac{3 + \sqrt{-3}}{2\beta}.$$

Proof. It suffices to prove that if $x + y \cdot ((3 + \sqrt{-3})/2\beta)$, with x, y in K, is integral over $\mathcal{O}_K$, then both x and y already lie in $\mathcal{O}_K$.

Computing the trace and norm (over K) of such an element, we thus assume that

$$2x + \frac{3}{\beta} y \in \mathcal{O}_K \tag{3.1}$$

and

$$\left(x + \frac{3y}{2\beta}\right)^2 + \frac{3y^2}{4\beta^2} = x^2 + \frac{3}{\beta} xy + \frac{3}{\beta^2} y^2 \in \mathcal{O}_K. \tag{3.2}$$

Squaring (3.1) and then subtracting four times (3.2), i.e. considering the discriminant of the quadratic polynomial $X^2 - (2x + sy)X + (x^2 + y^2 + sxy)$, with $s = \pm 1$, which kills our element, we get that

$$\frac{3}{\beta^2} y^2 \in \mathcal{O}_K. \tag{3.3}$$

If $v_\mathfrak{p}$, for any prime (either ideal or element) of $\mathcal{O}_K$, stands for the normalized valuation associated with $\mathfrak{p}$, we have from (3.3) that

$$0 \leqslant v_\mathfrak{p}\left(\frac{3}{\beta^2} y^2\right) = v_\mathfrak{p}\left(\frac{3}{\beta^2}\right) + 2v_\mathfrak{p}(y)$$

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

for any $\mathfrak{p}$ of $\mathcal{O}_K$, and, as

$$v_{\mathfrak{p}}\left(\frac{3}{\beta^2}\right) = \begin{cases} 1 & \text{if } \mathfrak{p} = \beta, \\ 0 & \text{otherwise,} \end{cases}$$

we infer that $v_{\mathfrak{p}}(y) \geqslant 0$ for all $\mathfrak{p}$, i.e. that $y \in \mathcal{O}_K$. Returning to (3.1), as 2 is prime in $\mathcal{O}_K$, we have that

$$v_{\mathfrak{p}}(x) \geqslant \begin{cases} -1 & \text{if } \mathfrak{p} = 2, \\ 0 & \text{otherwise.} \end{cases}$$

But if $v_2(x) = -1$, then from (3.2) we get that

$$v_2\left(x^2 + \frac{3}{\beta}xy + \frac{3}{\beta^2}y^2\right) = v_2(x^2) = -2.$$

This is a contradiction, and thus completes the proof. □

REMARK 3.2. Since $\sqrt{-3} \in \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\zeta_9)$, we obviously have that $\mathbb{Q}(\zeta_9, \sqrt{-3}) = \mathbb{Q}(\zeta_9)$. Consequently, as previously seen, the ring of integers of $K(\sqrt{-3})$ is $\mathbb{Z}[\zeta_9]$, but the translation in terms of $\sqrt{-3}$ does not seem straightforward to us and for this reason we have supplied a direct proof.

COROLLARY 3.3. *The ring of integers of* $K(M_1)$ *is just*

$$\mathcal{O}_K\left[\frac{1}{\beta}\begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}\right].$$

Consequently, the order $K(M_1) \cap \mathcal{M}(2, \mathcal{O}_K) = \mathcal{O}_K[M_1]$ *is not maximal in* $K(M_1)$.

Proof. M_1 can be identified with $(1+\sqrt{-3})/2$ (since they both satisfy the equation $X^2 - X + 1 = 0$) and, consequently, $(3 + \sqrt{-3})/2\beta$ corresponds to

$$\frac{1}{\beta}(1 + M_1) = \frac{1}{\beta}\begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}.$$

□

REMARK 3.4. If M_1 were identified with $(1 - \sqrt{-3})/2$, then $(3 + \sqrt{-3})/2\beta$ would correspond to

$$\frac{1}{\beta}(2 - M_1) = \frac{1}{\beta}\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix}.$$

But

$$\begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} - \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}.$$

REMARK 3.5. Needless to say, the case $s = -1$ follows exactly the same pattern as the case $s = +1$. In particular, it is obvious that the orders $K(M_1) \cap \mathcal{M}(2, \mathcal{O}_K)$ and $K(M_{-1}) \cap \mathcal{M}(2, \mathcal{O}_K)$ are isomorphic (under an inner automorphism of $\mathcal{M}(2, K)$).

COROLLARY 3.6. *None of the inner automorphisms induced by an invertible matrix of* $\mathcal{M}(2, K)$ *make the orders* $K(M_\alpha) \cap (2, \mathcal{O}_K)$ *and* $K(M_1) \cap \mathcal{M}(2, \mathcal{O}_K)$ *isomorphic.*

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

Proof. Otherwise, such an automorphism would also make $K(M_\alpha)$ and $K(M_1)$ K-isomorphic, in which case their $\mathcal{O}_K$-integral closures would be preserved, but this would obviously contradict the preceding results. □

REMARK 3.7. The orders of corollary 3.6 are, however, $\mathcal{O}_K$-isomorphic as $\mathcal{O}_K$-modules: obviously they are $\mathcal{O}_K$-free of rank 2.

Following Shimizu [4], we denote by Ω the set of sub-rings $\mathcal{O}$ of $\mathcal{M}(2,K)$ such that

(1) $K(\mathcal{O})$ is a totally imaginary maximal subfield of $\mathcal{M}(2,K)$,

(2) $\mathcal{O} = K(\mathcal{O}) \cap \mathcal{M}(2,\mathcal{O}_K)$ and

(3) $\mathcal{O} \cap \Gamma \neq \{\pm 1\}$, where $\Gamma = \mathrm{SL}(2,\mathcal{O}_K)$.

Then, the results of these two sections actually aim at the following.

THEOREM 3.8. *Ω is divided up into three classes under the equivalence relation defined by the inner automorphisms induced by the invertible matrices of $\mathcal{M}(2,K)$. And the orders $K(M_s) \cap \mathcal{M}(2,\mathcal{O}_K)$, for $s = 0, 1$ and α, constitute a complete set of representatives for these classes.*

Proof. It remains to check only that the order $K(M_0) \cap \mathcal{M}(2,\mathcal{O}_K)$ is not isomorphic with either $K(M_1) \cap \mathcal{M}(2,\mathcal{O}_K)$ or $K(M_\alpha) \cap \mathcal{M}(2,\mathcal{O}_K)$ (via inner automorphisms of the matrix ring $\mathcal{M}(2,K)$). But this follows easily from the fact that $K(\sqrt{-1})$ is not K-isomorphic with $K(\zeta) = \mathbb{Q}(\zeta)$, for, otherwise, $\mathbb{Q}(\zeta)$ would contain a primitive 4th root of unity and, consequently, a primitive 36th root of unity, which is clearly impossible. □

4. Number of elliptic points

In trying to count the number of elliptic points, we proceed to apply [4, (48)] (see [5, p. 15], [6, (8)], [3, Satz 3]), for which we need, among other things, to compute the index of the square units U_K^2 of $\mathcal{O}_K$ in the group of totally positive units U_K^+ of $\mathcal{O}_K$.

Following [7, ch. 8, lemma 8.1], the units of $\mathbb{Q}(\zeta)^+$, when ζ is a primitive prime power p^mth root of unity, are generated by -1 and the elements $\zeta^{(1-a)/2}(1-\zeta^a)/(1-\zeta)$, with $1 < a < \frac{1}{2}p^m$, $(a,p) = 1$.

In our case, $p^m = 3^2$, so the only values of a are 2 and 4, and choosing, for instance, $\zeta^{1/2} = \zeta^5$, a simple calculation yields for these elements the values α'' and $\alpha'' - 1$, respectively. As $\mathcal{O}_K^\times$ is invariant under the Galois group of $K|\mathbb{Q}$, we realize that we have proved the following.

LEMMA 4.1. *The group $\mathcal{O}_K^\times$ of units of K is generated by the elements α, $\alpha - 1$ and -1.*

PROPOSITION 4.2. *The group U_K^+ of totally positive units of K coincides with the group U_K^2 of square units of K and, consequently, $(U_K^+ : U_K^2) = 1$. The units are generated by the squares of α and $\alpha - 1$.*

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

Proof. Taking $\zeta = \mathrm{e}^{2\pi \mathrm{i}/9}$ and performing elementary numerical calculations, we see that none of the elements α, $\alpha - 1$ and $\alpha(\alpha - 1)$ is totally positive. Recalling the Dirichlet theorem on the structure of the group of units $\mathcal{O}_K^\times$, the assertion follows immediately. □

Our next step is to find the index $(\mathcal{O}^\times : \mathcal{O}_+^\times)$ in $\mathcal{O}$ of the subgroup $\mathcal{O}_+^\times$, consisting of the elements of $\mathcal{O}^\times$ having totally positive determinant, and where $\mathcal{O}$ stands for the order $K(M) \cap \mathcal{M}(2, \mathcal{O}_K)$ of $K(M)$ and M are the matrices considered in the preceding section, i.e. those of the form M_s, with s being 0, 1 and α. Now the answer is quite easy.

PROPOSITION 4.3. *For the above values of M', the index $(\mathcal{O}^\times : \mathcal{O}_+^\times)$ is always* 1.

Proof. $\mathcal{O}$ consists of the matrices

$$\begin{pmatrix} x & -y \\ y & x + sy \end{pmatrix}$$

with both x and y in $\mathcal{O}_K$. Recalling that a matrix is invertible if and only if its determinant is so, we see that, with our notation, invertibility means that $x^2 + y^2 + sxy \in \mathcal{O}_K^\times$. Viewing $x^2 + y^2 + sxy$ now as a real quadratic form (recall that $\mathcal{O}_K \subset K \subset \mathbb{R}$) we see that its discriminant is (up to squares) $1 - s^2/4$, which turns out to be always strictly positive for our values of s, and from this we immediately get that these real quadratic forms are positive definite, which entails that $\mathcal{O}^\times = \mathcal{O}_+^\times$. □

Our last efforts in this section deal with the special case when $s = 1$, which turns out to be the only case (up to isomorphism) in which the order $\mathcal{O}$ is not maximal in $K(M)$, as the results of § 3 show. For this we have to compute the ratio $h(\mathcal{O})/h(K(M))$, where $h(\mathcal{O})$ and $h(K(M))$ denote the class number of $\mathcal{O}$ and of $K(M)$, respectively. From the formula appearing in [2, Kap. I, Satz 12.12], we may write, with $\tilde{\mathcal{O}}$ standing for the ring of integers of $K(M)$, that

$$\frac{h(\mathcal{O})}{h(K(M))} = \frac{1}{(\tilde{\mathcal{O}}^\times : \mathcal{O}^\times)} \cdot \frac{\#(\tilde{\mathcal{O}}/\mathfrak{f})^\times}{\#(\mathcal{O}/\mathfrak{f})^\times},$$

where $\mathfrak{f}$ denotes the conductor of the extension $\tilde{\mathcal{O}} \supset \mathcal{O}$.

From proposition 3.1, we have that

$$\mathcal{O} = \mathcal{O}_K\left[\frac{3 + \sqrt{-3}}{2}\right] = \mathcal{O}_K + \mathcal{O}_K \cdot \frac{3 + \sqrt{-3}}{2},$$

while

$$\tilde{\mathcal{O}} = \mathcal{O}_K\left[\frac{3 + \sqrt{-3}}{2\beta}\right] = \mathcal{O}_K + \mathcal{O}_K \cdot \frac{3 + \sqrt{-3}}{2\beta}.$$

This entails that the conductor $\mathfrak{f}$ of $\tilde{\mathcal{O}}|\mathcal{O}$ is precisely $\beta\tilde{\mathcal{O}} = (\alpha + 1)\tilde{\mathcal{O}} = \mathcal{O}_K \cdot \beta + \mathcal{O}_K \cdot ((3 + \sqrt{-3})/2)$. Bearing this in mind, we now turn our attention to the rings $\tilde{\mathcal{O}}/\mathfrak{f}$ and $\mathcal{O}/\mathfrak{f}$. For these we have the following.

PROPOSITION 4.4. *Following the preceding assumptions and notation, we have that* $\#(\tilde{\mathcal{O}}/\beta\tilde{\mathcal{O}}) = 6$ *and* $\#(\mathcal{O}/\beta\tilde{\mathcal{O}}) = 2$.

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

Proof. Obviously,

$$\mathcal{O}/\beta\tilde{\mathcal{O}} \simeq \mathcal{O}_K/\beta\mathcal{O}_K \simeq \mathbb{F}_3 \quad \text{(the field of three elements)},$$

so $\#(\mathcal{O}/\beta\tilde{\mathcal{O}})^\times = \#\mathbb{F}_3^\times = 2$. Next,

$$\tilde{\mathcal{O}}/\beta\tilde{\mathcal{O}} \simeq \mathcal{O}_K\left[\frac{3+\sqrt{-3}}{2\beta}\right]\Big/\beta\tilde{\mathcal{O}} \simeq (\mathcal{O}_K/\beta\mathcal{O}_K[T])\Big/\left(T^2 - \frac{3}{\beta}T + \frac{3}{\beta^2}\right),$$

since $T^2 - 3T/\beta + 3/\beta^2$ is the defining polynomial of $(3+\sqrt{-3})/2\beta$, and as both $3/\beta$ and $3/\beta^2$ lie in $\beta\mathcal{O}_K$, we can further write that

$$\tilde{\mathcal{O}}/\beta\tilde{\mathcal{O}} \simeq (\mathcal{O}_K/\beta\mathcal{O}_K)[T]/(T^2) \simeq \mathbb{F}_3[T]/(T^2).$$

As the units of this last ring are easily seen to be the elements of type $a + bT \pmod{T^2}$, with $a, b \in \mathbb{F}_3$ and $a \neq 0$, we see that $\#(\mathbb{F}_3[T]/(T^2))^\times = 2 \cdot 3 = 6$, and our assertion is proved. □

We are now left only with the computation of the value $(\tilde{\mathcal{O}}^\times : \mathcal{O}^\times)$, and here we prefer to use the fact that $\tilde{\mathcal{O}} = \mathbb{Z}[\zeta]$, as shown in § 3. What we find now is the following.

PROPOSITION 4.5. $(\tilde{\mathcal{O}}^\times : \mathcal{O}^\times) = 3$.

Proof. Following [7, ch. 8, lemma 8.1] we see that $\tilde{\mathcal{O}}^\times = (\mathbb{Z}[\zeta])^\times$ is generated either by the primitive 9th root of unity ζ together with the set of generators $\{\alpha, \alpha-1, -1\}$ of $\mathcal{O}_K^\times$, or by ζ_{18} (a primitive 18th root of unity), α and $\alpha - 1$.

As for $\mathcal{O}$, we recall that

$$\mathcal{O} = \mathcal{O}_K\left[\frac{3+\sqrt{-3}}{2}\right] = \mathcal{O}_K\left[\frac{1+\sqrt{-3}}{2}\right]$$

and $(1+\sqrt{-3})/2$ is a primitive 6th root, say ζ_6, of unity.

Moreover, it is easy to write ζ_6 in terms of ζ as $(1+\sqrt{-3})/2 = \zeta_6 = \zeta \cdot \zeta^{1/2} = \zeta \cdot (-\zeta^5) = -\zeta^6$. Now, it is immediate that $\mathcal{O}^\times$ is generated by ζ_6 together with α and $\alpha - 1$ (since $-1 = \zeta_6^3$). The result follows from this. □

The facts already proved lead us to assert the following.

THEOREM 4.6. *For the orders $\mathcal{O}$ appearing above the number $\ell(\mathcal{O})$ of Γ-inequivalent orders of the form $A\mathcal{O}A^{-1}$, with A invertible in $\mathcal{M}(2,K)$ or what amounts to the same thing, the number of Γ-inequivalent elliptic points associated with orders isomorphic with $\mathcal{O}$ under inner automorphisms of $\mathcal{M}(2,K)$ is just* 4.

Proof. We apply [4, (48), § 6] (see [6, (8)] and [5, p. 15]), which reads

$$\ell(\mathcal{O}) = \frac{2^2}{(U_K^+ : U_K^2)(\mathcal{O}^\times : \mathcal{O}_+^\times)} \cdot \frac{h(\mathcal{O})}{h(K(M))}.$$

Now, it suffices to bear in mind propositions 4.2 and 4.3 in all cases, and for $s = 1$ use also propositions 4.4 and 4.5. □

From this we immediately get the following.

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

THEOREM 4.7. *The number of elliptic points in* $\mathbb{H}^3/\Gamma$ *under the action of the Hilbert modular group* $\Gamma = \mathrm{SL}(2, \mathcal{O}_K)$*, for* $K = \mathbb{Q}(\zeta)^+$*, is* $4 \cdot 3 = 12$.

5. Representatives for the elliptic points

We recall, from the end of § 3, that the set Ω introduced by Shimizu consists of three orbits, i.e. three isomorphism classes of orders under the action of the inner automorphisms of $\mathcal{M}(2, K)$, and, from § 4, that each such orbit consists of precisely four non-Γ-equivalent subclasses, as asserted in theorem 4.6 (we recall that $\mathcal{O}$ and $\mathcal{O}'$ in Ω are Γ-equivalent if $\mathcal{O}' = E\mathcal{O}E^{-1}$ for some E in Γ).

In general, it is very hard to make explicit a complete set of representative orders for these subclasses because of the intricate calculations involved (see [1, 3, 4]). However, in our concrete situation, a straightforward argument will allow us to overcome the general difficulties and we end the paper by showing this.

THEOREM 5.1. *Let* $M = M_s$*, with* $s = 0, 1$ *and* α*, and let*

$$A_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix},$$

with $\lambda = 1, \alpha, \alpha - 1$ *and* $\alpha(\alpha - 1)$*. Then, the 12 (elliptic) matrices* $A_\lambda M_s A_\lambda^{-1}$ *constitute a complete set of representatives for the* Γ*-equivalence of orders in* Ω*.*

From this the following corollary is obtained directly.

COROLLARY 5.2. *The 12 fixed points in* $\mathbb{H}^3$ *of the matrices in theorem 5.1 are a full set of representatives for the* Γ*-equivalence of elliptic points with respect to the Hilbert modular group* $\Gamma = \mathrm{SL}(2, \mathcal{O}_K)$ *acting on* $\mathbb{H}^3$*.*

Proof of theorem 5.1. We have to show that (for any fixed s) if $\mathcal{O} = \{x + yM_s \mid x, y \in \mathcal{O}_K\}$, the orders $A_\lambda \mathcal{O} A_\lambda^{-1}$ (obviously contained in $\mathcal{M}(2, \mathcal{O}_K)$, since the A_λ^{-1} are integral matrices), for $\lambda = 1, \alpha, \alpha - 1$ and $\alpha(\alpha - 1)$, are all distinct. To prove this, it suffices to show that $A_\lambda M_s A_\lambda^{-1}$ does not lie in any order of type $E(A_\mu \mathcal{O} A_\mu^{-1})E^{-1}$, for $\mu \in \{1, \alpha, \alpha - 1, \alpha(\alpha - 1)\}$, $\mu \neq \lambda$ and $E \in \Gamma$.

Assume it does, i.e. there exist x, y in $\mathcal{O}_K$ such that

$$A_\lambda M_s A_\lambda^{-1} = EA_\mu(x + yM_s)A_\mu^{-1}E^{-1} = x + yEA_\mu M_s A_\mu^{-1}E^{-1} \tag{5.1}$$

for some

$$E = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{in } \Gamma = \mathrm{SL}(2, \mathcal{O}_K).$$

First observe that the characteristic polynomial (i.e. the defining polynomial of M_s over K) of $A_\lambda M_s A_\lambda^{-1}$, or just of M_s, is $X^2 - sX + 1$, and that of $x + yM_s$ is $X^2 - (2x + ys)X + (x^2 + y^2 - sxy)$ (see § 3). Their respective discriminants are $s^2 - 4$ and $y^2(s^2 - 4)$, so the matrix equality (5.1) entails that $y = \pm 1$.

Next, direct computation shows that

$$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -\lambda \\ \lambda^{-1} & s \end{pmatrix}$$

https://doi.org/10.1017/S0308210512000376 Published online by Cambridge University Press

which allows us to write (5.1) as

$$\begin{aligned}\begin{pmatrix} 0 & -\lambda \\ \lambda^{-1} & s \end{pmatrix} &= x + y \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -\mu \\ \mu^{-1} & s \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= x + y \begin{pmatrix} ac\mu + bd\mu^{-1} - bcs & -a^2\mu - b^2\mu^{-1} + abs \\ c^2\mu + d^2\mu^{-1} - cds & -ac\mu - bd\mu^{-1} + ads \end{pmatrix}, \end{aligned} \tag{5.2}$$

where the last equality has been obtained by simple computation.

Paying attention to the lower left-hand entries in (5.2), with $y = \pm 1$, we have that

$$\lambda^{-1} = y(c^2\mu + d^2\mu^{-1} - cds). \tag{5.3}$$

At this point, observe that $c^2\mu + d^2\mu^{-1} - cds$ may be thought of as the value on the vector (c, d) of the real quadratic form of the matrix

$$\begin{pmatrix} \mu & -s/2 \\ -s/2 & \mu^{-1} \end{pmatrix}$$

with determinant $1 - s^2/4 \gg 0$ (totally positive), so we are dealing with either a positive-definite or a negative-definite real quadratic form, since μ is positive or negative. Bearing this in mind, (5.3) together with those equalities obtained from it by applying the two non-trivial Galois automorphisms (of $\mathrm{Gal}(K|\mathbb{Q})$) entail then that the signs of λ and μ and those of their corresponding conjugates by the Galois automorphisms always coincide if $y = +1$ or always differ if $y = -1$. But this is inconsistent (recall that both λ and μ lie in $\{1, \alpha, \alpha - 1, \alpha(\alpha - 1)\}$) with the facts that (see § 1)

$$\begin{aligned} \alpha > 0, \qquad & \alpha' > 0, \qquad & \alpha'' < 0, \\ \alpha - 1 > 0, \qquad & \alpha' - 1 < 0, \qquad & \alpha'' - 1 < 0 \end{aligned}$$

and (multiplying)

$$\alpha(\alpha - 1) > 0, \qquad \alpha'(\alpha' - 1) < 0, \qquad \alpha''(\alpha'' - 1) > 0.$$

This completes the proof of the theorem. □

Acknowledgements

The author was partly supported by the projects MTM2009-07024 and MTM2012-33830.

References

1 M. Eichler. Zur Zahlentheorie der Quaternionen Algebren. *J. Reine Angew. Math.* **195** (1955), 125–151.
2 J. Neukirch. *Algebraische Zahlentheorie* (Springer, 1992).
3 A. Prestel. Die elliptischen Fixpunkte der Hilbertschen Modulgruppen. *Math. Annalen* **177** (1968), 181–209.
4 H. Shimizu. On discontinuous groups operating on the product of the upper half-planes. *Annals Math.* **77** (1963), 33–71.
5 G. van der Geer. *Hilbert modular surfaces* (Springer, 1988).

6 M.-F. Vignéras. Invariants numériques des groupes de Hilbert. *Math. Annalen* **224** (1976), 189–215.
7 L. C. Washington. *Introduction to cyclotomic fields*, 2nd edn (Springer, 1997).
8 D. Weisser. The arithmetic genus of the Hilbert modular variety and the elliptic fixed points of the Hilbert modular group. *Math. Annalen* **257** (1981), 9–22.

(*Issued 4 October 2013*)