ON UNITARY GROUPS ASSOCIATED TO DIVISION ALGEBRAS OF DEGREE THREE

KATHRIN MAURISCHAT

Abstract. We study rational points of unitary groups associated to involutions of the second kind on central division algebras of degree three. We characterize the torsion points and show that special unitary groups do not contain hermitian or skew-hermitian elements. We give criteria for S-arithmetic points.

Contents

1. Introduction

This paper is concerned with results on unitary groups which arise from involutions of the second kind on division algebras of degree three over a number field. Those are inner forms of special unitary matrix groups $SU_3(H)$ defined by a hermitian matrix $H \in \mathrm{GL}_3$. Albert [1] proved that simple division algebras D of odd prime degree over number fields carry an involution α of the second kind if and only if they have a maximal subfield which is cyclic Galois not only over the center E but over its subfield F fixed by the involution, and that these algebras are cyclic (see section 2). Equivalently, D carries an involution of the second kind if and only if its corestriction along E/F is trivial [6]. The unitary group U consists of those $g \in D$ such that $\alpha(g)g = 1$, and the special unitary group SU consists of those elements which additionally are of reduced norm one, $\mathrm{N}_{rd}(g) = 1$.

2010 *Mathematics Subject Classification.* 11R52, 22E40, 51F25.

Key words and phrases. Division algebras, unitary groups, S-arithmetic points, discrete cocompact subgroups.

Although there exist far-developed theories for division algebras, like local-global principles, cohomology theories, or Brauer-Severi varieties, they remain not to be understood comprehensively apart from quaternion quaternion algebras. In particular, the structure of the unitary groups is rather unstudied. For example, it is a non-trivial task to find explicit S-arithmetic points on the unitary groups for a prescribed set of primes S.

Our results can be summarized in two groups. The first one is concerned with points of finite order in unitary groups. It is a simple result that in arbitrary odd degree the special unitary group SU does not contain elements of even order (theorem 3.1). But consequently, reflections in special unitary groups of complex vector spaces of odd dimension can never be realized as rational points on division algebras. More precisely:

Corollary 1.1. *Let $d > 0$ be an odd integer. Let H be a hermitian matrix in $M_d(\mathbb{C})$, and let $SU_d(H) = \{g \in \mathrm{SL}_d(\mathbb{C}) \mid \bar{g}'Hg = H\}$ denote the associated special unitary group. Let $r \in SU_d(H)$ be a reflection. Then r is not contained in any global division algebra (D, α) of degree d with involution α of the second kind such that for some infinite place v, $SU_v \cong SU_d(H)$. Similarly, no hermitian or skew-hermitian element of $SU_d(H)$ arises in this way.*

Making the reasonable assumption that E is an imaginary quadratic extension over the totally real field F, the elements of finite order in unitary groups of division algebras of degree three can be characterized precisely. A unitary element g has finite order if and only if it generates a cyclic extension $F[g]$ over the ground field F fixed by the involution (theorem 3.2). In particular, in case $F = \mathbb{Q}$ the special unitary group SU will be torsion free as long as E is not $\mathbb{Q}(\sqrt{-3})$ (corollary 3.3).

The second group of results is concerned with S-arithmetic subgroups of the special unitary group. For this, the structure of the algebra D and its involution α must allow an integral model. We use the special cyclic presentation of D

$$D \;=\; L \oplus Lz \oplus Lz^2\,,$$

where L is C_6-Galois over the totally real field F, the center of D being an imaginary quadratic extension E of F, and assume the cyclic presentation as well as the involution is defined over $\mathfrak{o}_F$. Then the special unitary group SU gives rise to a group scheme $\mathbb{SU}$ defined over the integers $\mathfrak{o}_F$. A criterion for this is given by proposition 3.4. We also give a criterion for definiteness in proposition 3.5.
Arithmetic subgroups provide prototypes of discrete subgroups of the local groups $\mathbb{SU}(F_\mathfrak{p})$, which under mild assumptions, such as the compactness of $\mathbb{SU}(F_v)$ at some infinite place v ([4], [5]), are known to be cocompact. While they arise at many points in modern mathematics, there is no explicitly computed example of a discrete cocompact global subgroup for the special unitary groups in question so far.
Searching for non-trivial points on $\mathbb{SU}(F)$, the cyclic structure of D suggests a number of simple choices. Unitary monomial elements lz^j, $l \in L^\times$ are discussed in propositions 4.1 and 4.5. In particular, if S is a set of prime ideals $\mathfrak{p}$ not dividing 2, which are inert in E but split in L, and such that $F_\mathfrak{p}$ does not contain the third

roots of unity, then the single unitary monomials with $l \in \mathfrak{o}_L(S)$ are the trivial ones already contained in $\mathfrak{o}_E^\times$. Prime ideals $\mathfrak{p}$ satisfying this assumption lead to proper special unitary groups $SU_3(F_\mathfrak{p})$, i.e. non-split and non-isomorphic to $\mathrm{SL}_3(E_\mathfrak{p})$. The assumption on $F_\mathfrak{p}$ not containing the sixth roots of unity may seem artificial at a first glance. But if E is chosen to be the Kummer extension $F(\zeta_3)$, this is satisfied for all inert primes. The result implies that non-trivial elements of the promising S-arithmetic subgroups $\mathbb{SU}(\mathfrak{o}_F(S))$ belong to non-obvious subfields of D.
Results for unitary elements $l_0 + l_1 z + l_2 z$ such that the coefficients L_j are eigenvectors under the conjugation τ are discussed in proposition 4.2.
Let ρ be a generator of $\mathrm{Gal}(L/E)$. There is an obvious extension of ρ to D by action on the coefficients, which coincides with conjugation by z. If the involution is defined reasonably, the fixed points $\mathbb{U}(F)^\rho$ and $\mathbb{SU}(F)^\rho$ give rise to group schemes themselves. By theorem 4.6, their S-arithmetic points are monomials, if S consists of primes which are either inert or ramified in E such that $F_\mathfrak{p}$ does not contain the third roots of unity.

Our results give necessary criteria for the coordinates of rational unitary points giving restrictions to their order and their denominators. We close with a concrete example in section 4.3.

Acknowledgements. The author thanks Cristina Ballantine and Brooke Feigon for their encouragement to publish the results in hand separately from the joint work.

2. Involutions of the second kind

Let E/F be an extension of number fields of degree two, and denote by τ the non-trivial Galois automorphism, which we often identify with conjugation $\tau(x) = \bar{x}$. Let D be a central simple division algebra over E. An involution of the second kind on D is an anti-automorphism α which restricted to the center E equals τ. A division algebra carries an involution of the second kind if and only if the norm algebra of D splits. In the special case that the algebra D has odd degree over E, the exposition relies on the existence of a cubic subfield $L \subset D$ such that its discriminant is isomorphic to E [6, 19.14], or equivalently, such that $M = L^\tau$ is a cyclic Galois extension of F. In particular, we will use the following explicit cyclic presentation of D.

Theorem 2.1. [1] *Let E/F be a quadratic extension of number fields and denote by τ its non-trivial automorphism. Let D be a central simple division algebra over E of degree three. Then D carries an involution of the second kind extending τ if and only if the following two conditions are satisfied.*

(i) *There exists a maximal subfield L in D such that L/F is C_6-Galois. Consequently, a cyclic realization of D is given by*

$$D = L \oplus Lz \oplus Lz^2,$$

subject to the relations $z^3 = a \in E^\times$ *and* $zl = \rho(l)z$ *for all* $l \in L$*, where* ρ *is a non-trivial element of* $Gal(L/E)$*.*

(ii) *The norm equation* $\mathrm{N}_{E/F}(a) = \mathrm{N}_{M/F}(b)$ *has a solution* $b \in M = L^\tau$*.*

In this case, an involution α *of the second kind is given by*

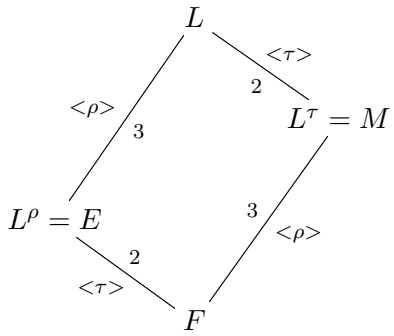
$$\alpha\,|_L = \tau \quad \text{and} \quad \alpha(z) = \frac{b}{a}z^2\,.$$

Any other involution β *of the second kind is conjugate to* α *by some element* $c \in M^\times$*,*

$$\beta(d) = c^{-1}\alpha(d)c\,,$$

for all $d \in D$*, and in particular* $\beta(z) = c^{-1}\rho^2(c)\alpha(z)$*. Moreover, a cyclic algebra as described in (i) is a division algebra if and only if* a *is not a norm of* L*,* $a \notin \mathrm{N}_{L/E} = \mathrm{N}_{L/E}(L^\times)$*.*

For the field extension L/F we have the following picture.



The structure constant a of D being unique up to factors $\mathrm{N}_{L/E}(l)$ for $l \in L$, it is always possible to choose $a \in \mathfrak{o}_E$, the ring of integers of E. Notice that the property $a \notin \mathrm{N}_{L/E}$ together with $a\bar{a} = \mathrm{N}_{M/F}(b)$ force $a \in E \setminus F$. As otherwise $a^2 = \mathrm{N}_{M/F}(b) \in \mathrm{N}_{L/E}$, but then $a = \mathrm{N}_{M/F}(b^2a^{-1})$ belongs to $\mathrm{N}_{L/E}$, too. Throughout this paper, we refer to a division algebra D with constants $a \in \mathfrak{o}_E \setminus \mathfrak{o}_F$ and $b \in M$ satisfying the special cyclic presentation of theorem 2.1.
We use the embedding of the cyclic algebra $D = L \oplus Lz \oplus Lz^2$ to the matrix ring $M_3(L)$ defined by

$$L \ni l \mapsto \begin{pmatrix} l & & \\ & \rho(l) & \\ & & \rho^2(l) \end{pmatrix}, \quad z \mapsto \begin{pmatrix} & 1 & \\ & & 1 \\ a & & \end{pmatrix}.$$

We often identify $g = l_0 + l_1 z + l_2 z^2$, $l_j \in L$, with its image

$$g = g(l_0, l_1, l_2) = \begin{pmatrix} l_0 & l_1 & l_2 \\ a\rho(l_2) & \rho(l_0) & \rho(l_1) \\ a\rho^2(l_1) & a\rho^2(l_2) & \rho^2(l_0) \end{pmatrix}. \tag{1}$$

With respect to this embedding, the involution α is realized as

$$\alpha(g) \;=\; \begin{pmatrix} \bar{l}_0 & \underset{a}{\underline{\rho(\rho(b)\rho^2(b)\bar{l}_2)}} & \underset{a}{\underline{\rho^2(\rho(b)\bar{l}_1)}} \\ \rho(b)\bar{l}_1 & \rho(\bar{l}_0) & \underset{a}{\underline{\rho^2(\rho(b)\rho^2(b)\bar{l}_2)}} \\ \rho(b)\rho^2(b)\bar{l}_2 & \rho(\rho(b)\bar{l}_1) & \underset{a}{\underline{\rho^2(\bar{l}_0)}} \end{pmatrix}. \tag{2}$$

3. Unitary groups

Let D be a central division algebra with involution α of the second kind over E/F. The involution α gives rise to a non-degenerate hermitian form h on D,

$$\begin{aligned} h : D \times D &\longrightarrow D \\ (x, y) &\mapsto \alpha(x)y\,. \end{aligned}$$

That is, for all $\lambda, \mu, x, y \in D$ we have

$$h(x\lambda, y\mu) \;=\; \alpha(\lambda)\alpha(x)y\mu = \alpha(\lambda)h(x, y)\mu$$

as well as

$$\alpha\big(h(x, y)\big) \;=\; \alpha(y)x \;=\; h(y, x)\,.$$

The unitary group of this hermitian form is

$$U \;=\; \{g \in D^\times \mid h(gx, gy) = h(x, y) \text{ for all } x, y \in D\} \;=\; \{g \in D^\times \mid \alpha(g)g = 1\}\,,$$

and the special unitary group

$$SU \;=\; \{g \in U \mid \mathrm{N}_{rd}(g) = 1\}$$

is the subgroup of reduced norm one.

3.1. **Elements of finite order.** In case of odd degree we have the following simple theorem, which has corollary 1.1 as a surprising consequence.

Theorem 3.1. *Let D be a division algebra of odd degree with involution of the second kind central over E/F.*

(a) *The unitary eigenvectors $g \in U$ of the involution α belong to $E^\times$ and are forth roots of unity.*
(b) *The special unitary group SU does not contain elements of even order. In particular, it does not contain reflections.*

Proof of theorem 3.1. For (a), if $1 = \alpha(g)g = \pm g^2$, then the degree of the field $E[g]$ generated by g is at most two. But the degree must divide the odd degree of D. So g belongs to E and satisfies $g^4 = 1$.
For (b), if there is an element of finite even order, then there is an element of order two. But the unique element g of order two in $D^\times$ is $-1 \notin SU$. Because, in the subfield $E[g] \subset D$ the equation $g^2 = 1$ has the solutions $g = \pm 1 \in E$. □

The next result holds for imaginary quadratic extensions E/F. It is of particular interest for definite algebras (see section 3.3 below).

Theorem 3.2. *Let E be an imaginary quadratic extension of the totally real field F. Let D be a division algebra of degree three with involution α of the second kind central over E/F.*

(a) *Let $K \subset D$ be a C_3-Galois extension field of F. An element $x \in KE$ that belongs to U has finite order.*
(b) *An element $g \in U$ has finite order if and only if $F[g]/F$ is a cyclic Galois extension.*
(c) *An element $g \in U$ has infinite order if and only if $E[g]/F$ is S_3-Galois or non-Galois.*

Proof of theorem 3.2. Concerning (a), the composition field KE is a C_6-Galois extension of F. If $\mathrm{Gal}(K/F) =< \sigma >$, then (id, τ), $(\sigma, \tau\sigma)$, and $(\sigma^2, \tau\sigma^2)$ are the three pairs of complex conjugate embeddings to the complex numbers, and $\alpha \mid_{KE} = \tau$. If $\alpha(x)x = 1$ for an element $x \in KE$, then x is of absolute value one with respect to each embedding. Being algebraic, x is a root of unity.
For (b), if $ord(g) = n < \infty$, then $F[g]/F$ is a cyclotomic extension. The Galois group is a subquotient of $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$, so cyclic. Conversely, if $\mathrm{Gal}(F[g]/F)$ is cyclic, then by degree considerations it is either trivial, C_2, C_3, or C_6. If $\mathrm{Gal}(F[g]/F) = 1$, then $g \in F \cap U = \{\pm 1\}$. If $\mathrm{Gal}(F[g]/F) = C_2$, then $F[g] = E$ is the unique degree two extension of F in D, and $g \in E \cap U$ is a root of unity. If $\mathrm{Gal}(F[g]/F) = C_3$, then $E \cap F[g] = F$. The element g being unitary, the involution α is an automorphism of $F[g]$ which extends τ to $E[g]$, which then is C_6-Galois over F. The order of g is finite by part (a). If $\mathrm{Gal}(F[g]/F) = C_6$, then $E[g] = F[g]$, and we are again in the situation of part (a).
The extension $F[g]/F$ is not cyclic if and only if $E[g]/F$ is either non-Galois or S_3-Galois. So (c) is equivalent to (b). □

Corollary 3.3. *In case $F = \mathbb{Q}$, the elements of SU of finite order belong to E and are third roots of unity. In particular, SU is torsion free unless E is $\mathbb{Q}(\zeta_3)$.*

Proof of corollary 3.3. Let $g \in SU$ be an element of finite order. The extension $\mathbb{Q}[g]/\mathbb{Q}$ is cyclotomic and of degree at most three. Because there aren't any cubic cyclotomic fields, $\mathbb{Q}[g]$ is contained in the unique quadratic extension E of $\mathbb{Q}$ contained in D. If g is non-trivial, then its order is odd by theorem 3.1. This can only be the case if $E = \mathbb{Q}[\zeta_3]$. For all other choices of E there are no elements of finite order apart from one. □

3.2. **Integer-valued points.** Let D be as in section 3, and let $\mathfrak{o}_D$ be the maximal order of D given by its integral elements. We define a unitary group scheme $\mathbb{U}$ over $\mathfrak{o}_F$ forcing its F-valued points to coincide with U,

$$\mathbb{U}(R) \;=\; \{g \in \mathfrak{o}_D \otimes_{\mathfrak{o}_F} R \mid \alpha(g)g = 1\}$$

for all extension rings R of $\mathfrak{o}_F$. Similarly, we have the special unitary group scheme $\mathbb{SU}$ such that $\mathbb{SU}(F) = SU$,

$$\mathbb{SU}(R) \;=\; \{g \in \mathfrak{o}_D \otimes_{\mathfrak{o}_F} R \mid \alpha(g)g = 1,\ \mathrm{N}_{rd}(g) = 1\}\,.$$

Let the division algebra D of degree three with involution of the second kind over E/F be given by the cyclic presentation of section 2. One may also define unitary schemes over F, thereby giving in the notion of $\mathfrak{o}_F$-valued points. For example, one can use the embedding of D into $M_3(L)$ as L-algebra given by (1). But this

is defined over $\mathfrak{o}_L$ if and only if a is a unit in $\mathfrak{o}_E$. There is an extension of the involution α on $M_3(L)$,

$$(3)\quad \alpha\left(\begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix}\right) = \begin{pmatrix} \bar{m}_{00} & \rho(b^{-1})\bar{m}_{10} & \rho(b^{-1})\rho^2(b^{-1})\bar{m}_{20} \\ \rho(b)\bar{m}_{01} & \bar{m}_{11} & \rho^2(b^{-1})\bar{m}_{21} \\ \rho(b)\rho^2(b)\bar{m}_{02} & \rho^2(b)\bar{m}_{12} & \bar{m}_{22} \end{pmatrix},$$

and a group scheme $\mathbb{D}$ defined over F as a subscheme of $M_3(L)$ such that $\mathbb{D}(F) \subset M_3(L)$ coincides with the image of D, and unitary group schemes with F-valued points U, SU can be defined directly as subgroups of $\mathrm{GL}_3(L)$. We will refer to these schemes as the cyclic presentations associated to theorem 2.1. As long as we are concerned with K-valued points, K an extension of F, the two notions coincide, and we will make frequent use of the cyclic presentation. We can at least talk about the set Λ of $\mathfrak{o}_L$-points of $\mathbb{D}(F)$ meaning those with matrix entries in $\mathfrak{o}_L$, $\Lambda = \mathfrak{o}_L \oplus \mathfrak{o}_L z \oplus \mathfrak{o}_L z^2$. But notice that in case $a \notin \mathfrak{o}_E^\times$ or $b \notin \mathfrak{o}_M^\times$ the involution α will neither act on $M_3(\mathfrak{o}_L)$ nor on the $\mathfrak{o}_L$-points Λ of $\mathbb{D}(F)$.
In contrary, α acts on $\mathbb{D}(\mathfrak{o}_F) = \mathfrak{o}_D$, as for an integral element $d \in \mathfrak{o}_D$, the minimal polynomial f belongs to $\mathfrak{o}_E[X]$, and the polynomial with conjugate coefficients $\bar{f} \in \mathfrak{o}_E[X]$ is a minimal polynomial for $\alpha(d)$. But if and only if $\mathfrak{o}_D$ coincides with Λ, then $\mathbb{D}$ is already defined over $\mathfrak{o}_F$, and thus is a matrix realization of the group scheme given by the maximal order $\mathfrak{o}_D$ of integers in D, and the notions of integral points of $\mathbb{U}$ and $\mathbb{SU}$ coincide with the notions of the $\mathfrak{o}_L$-valued points of the corresponding cyclic presentation group.

Proposition 3.4. *The order $\Lambda = \mathfrak{o}_L + \mathfrak{o}_L z + \mathfrak{o}_L z^2$ of D equals the maximal order $\mathfrak{o}_D$ of integral elements if and only if a is a unit in $\mathfrak{o}_E$.*

Proof of proposition 3.4. First notice that Λ is contained in $\mathfrak{o}_D$. By [8, 11.6], the order Λ is maximal if and only if for all prime ideals $\mathfrak{p}$ of $\mathfrak{o}_E$ the localization $\Lambda_\mathfrak{p}$ is a maximal order in $D_\mathfrak{p}$. Assume $a \in \mathfrak{o}_E \setminus \mathfrak{o}_E^\times$, and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_E$ which contains a. Because $b \in M$ is chosen such that $a\bar{a} = \mathrm{N}_{L/E}(b)$, the element $b^{-1}z^2 \in D$ has minimal polynomial $X^3 - \frac{a}{\bar{a}}$. Because $v_\mathfrak{p}(\frac{a}{\bar{a}}) = 0$, the element $b^{-1}z^2$ is an integer of $D_\mathfrak{p}$. But $b^{-1} \notin \mathfrak{o}_{L_\mathfrak{p}}$. So the maximal order $\mathfrak{o}_{D_\mathfrak{p}}$ is strictly larger than $\Lambda_\mathfrak{p}$.
On the other hand, the discriminant of Λ is given by its generator

$$disc(\Lambda) = \det(\mathrm{tr}_{rd}(b_{jk}b_{j'k'}))$$

for the $\mathfrak{o}_E$-basis $b_{jk} = e_j z^k$, $j,k = 0,1,2$, of Λ. Here e_j, $j = 0,1,2$, is any $Gal(L/E)$-invariant $\mathfrak{o}_E$-basis of $\mathfrak{o}_L$. Because $\mathrm{tr}_{rd}(lz) = 0 = \mathrm{tr}_{rd}(lz^2)$ for all $l \in L$, we easily compute

$$disc(\Lambda) = \det\begin{pmatrix} \mathrm{tr}(e_j e_k) & 0 & 0 \\ 0 & 0 & a\,\mathrm{tr}(e_j\rho(e_k)) \\ 0 & a\,\mathrm{tr}(e_j\rho^2(e_k)) & 0 \end{pmatrix} = \left(-a^2\, disc(\mathfrak{o}_L)\right)^3.$$

Because $\mathfrak{o}_L$ is the maximal $\mathfrak{o}_E$-order (of integral elements) in L, the order $\mathfrak{o}_D$ of integral elements is an $\mathfrak{o}_L$-module, and the different $\mathfrak{D}$ of $\mathfrak{o}_D$ is an $\mathfrak{o}_L$-module, too.

Consequently, the ideal norm $\mathrm{N}(\mathfrak{D})$ of $\mathfrak{D}$ is divisible by $disc(\mathfrak{o}_L)$. But by [8, 25.10],

$$disc(\mathfrak{o}_D) \;=\; \big(\mathrm{N}(\mathfrak{D})\big)^3\,,$$

and further, maximal orders belong to minimal discriminants and vice versa. So in case $a \in \mathfrak{o}_E^\times$ is a unit, $disc(\Lambda)$ is minimal, and consequently $\Lambda = \mathfrak{o}_D$. □

3.3. **Definiteness.** Assume the ground field F to be totally real, and let $E = F(\sqrt{-d})$, where $d \in \mathfrak{o}_F$ is square free and totally positive, be an imaginary quadratic extension. The hermitian form h is called totally definite, if it is definite at all the archimedean places, or equivalently, if the unitary group $\mathbb{SU}(F_v)$ is compact for all $v \mid \infty$. At an archimedean place v we have $F_v \cong \mathbb{R}$ and $E_v \cong \mathbb{C}$. So $L_v \cong \mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}$, where the embedding $L \hookrightarrow \mathbb{C}\oplus\mathbb{C}\oplus\mathbb{C}$ is given by the three embeddings of L to E_v, which we again denote by ρ^j, $l \mapsto (\rho^0(l), \rho(l), \rho^2(l))$. Using the cyclic presentation, $\mathbb{D}(F_v)$ is isomorphic to $M_3(\mathbb{C})$ equipped with the involution (3). But on $M_3(\mathbb{C})$ we have an obvious involution β of the second kind given by conjugate transpose, $\beta(m) = \bar{m}'$, and $M_3(\mathbb{C})$ being central simple, there exists $H \in \mathrm{GL}_3(\mathbb{C})$ such that $\alpha(m) = H^{-1}\beta(m)H^{-1}$. Obviously, this is satisfied by

$$H \;=\; \begin{pmatrix} \rho^0(b) & & \\ & \rho(b) & \\ & & \rho^2(b) \end{pmatrix}\,,$$

and $m \in M_3(\mathbb{C})$ belongs to $\mathbb{U}(F_v)$ if and only if

$$\bar{m}'Hm \;=\; H\,.$$

Thus, $\mathbb{U}(F_v)$ is isomorphic to the unitary group associated to the standard hermitian form given by H. This is definite if and only if $\rho^0(b)$, $\rho(b)$ and $\rho^2(b)$ have the same sign. In view of $\mathrm{N}_{M/F}(b) = \mathrm{N}_{E/F}(a)$ being positive for any embedding $L \hookrightarrow \mathbb{C}$, we actually have $\epsilon_v = 1$ for all v. That is, b must be totally positive. We have found a simple criterion for definiteness.

Proposition 3.5. *Assume the division algebra of theorem 2.1 is defined over an imaginary quadratic extension E of a totally real number field F. Then the involution defined by the totally real number b is totally definite if and only if b is totally positive.*

4. Results on rational points of the unitary group

4.1. **Points distinguished by the cyclic structure.** In the situation of theorem 2.1 we assume the field E to equal $F(\sqrt{-d})$, where $-d$ is a square-free element of $\mathfrak{o}_F$. By the embedding (1), an element of $\mathbb{D}(F)$ is given by the first row (l_0, l_1, l_2) of the corresponding matrix, $l_0, l_1, l_2 \in L$. The unitary condition $g\alpha(g) = 1$ with respect to α given by (2) for such an element is

$$l_0\bar{l}_0 + \rho(b)l_1\bar{l}_1 + \rho(b)\rho^2(b)l_2\bar{l}_2 \;=\; 1 \tag{4}$$

together with

$$a\bar{l}_0\rho(l_2) + \rho(b)\bar{l}_1\rho(l_0) + \rho(b)\rho^2(b)\bar{l}_2\rho(l_1) = 0. \tag{5}$$

The determinant (reduced norm) condition is

$$N_{L/E}(l_0) + aN_{L/E}(l_1) + a^2 N_{L/E}(l_2) - a\,\mathrm{tr}_{L/E}(l_0\rho(l_1)\rho^2(l_2)) = 1. \tag{6}$$

So an element $g = g(l_0, l_1, l_2)$ satisfying (4) and (5) belongs to the unitary group $U = \mathbb{U}(F)$ defined by the involution α on the division algebra. If it additionally satisfies (6), then it belongs to the special unitary group $SU = \mathbb{SU}(F)$. We have an action of $Gal(L/E) =< \rho >$ on the cyclic algebra $\mathbb{D}(F) = L \oplus Lz \oplus Lz^2$ by automorphisms given by the action on the coefficients

$$\rho(l_0 + l_1 z + l_2 z^2) \;=\; \rho(l_0) + \rho(l_1)z + \rho(l_2)z^2\,,$$

for all $l_j \in L$. This coincides with the inner automorphism given by conjugation with z, $\rho(d) = zdz^{-1}$. The $Gal(L/E)$-fixed points of $\mathbb{D}(F)$ obviously are those with coefficients $l_j \in E$.
We collect some simple properties.

Proposition 4.1. (a) *If for an element $g(l_0, l_1, l_2) \in \mathbb{U}(F)$ one of the coefficients is zero, then $g = lz^j$, $l \in L$, is monomial.*

(b) *The monomial elements $g = lz^j$, $j = 0, 1, 2$, of $\mathbb{U}(F)$ are given by those $l \in L$ satisfying the norm equation $\mathrm{N}_{L/M}(l) = 1$, $\rho(b)\,\mathrm{N}_{L/M}(l) = 1$, $\rho(b)\rho^2(b)\,\mathrm{N}_{L/M}(l) = 1$, for $j = 0$, $j = 1$, $j = 2$, respectively.*

(c) *The monomial elements g of $\mathbb{SU}(F)$ are the elements given by $g = l \in L^\times$ satisfying the norm equations*

$$\mathrm{N}_{L/M}(l) \;=\; 1 \;=\; \mathrm{N}_{L/E}(l)\,. \tag{7}$$

In particular, the $Gal(L/E)$-fixed monomial elements are given by the third roots of unity contained in E.

Proof of proposition 4.1. If $l_k = 0$, then by the unitary condition (5) a second coefficient l_n, $n \neq k$, is zero, too. So $g = l_j z^j$ for the remaining $j \neq k, n$. This is (a).
Concerning (b), for a monomial element $g = lz^j$ the unitary condition (4) clearly simplifies to the stated ones. Concerning (c), $g = lz^j \in \mathbb{SU}(F)$ must satisfy the determinant condition (6), $a^j\,\mathrm{N}_{L/E}(l) = 1$. Because a and a^2 don't belong to $\mathrm{N}_{L/E}$, we have $j = 0$, and hence (7). In the special case $l \in E^\times$, we have $l\bar{l} = 1 = l^3$, i.e. l is a third root of unity. □

By Hilbert 90 an element $l \in L^\times$ satisfying the first condition of (7) in proposition 4.1 is of the form

$$l \;=\; \frac{y_0 + \sqrt{-d}y_1}{y_0 - \sqrt{-d}y_1}$$

with $y_0, y_1 \in M$. In order to satisfy the second condition non-trivially, we may assume y_1 to be non-zero and normalize it $y_1 = 1$. Then the second condition is $\mathrm{tr}_{L/E}(y_0\rho(y_0)) = d$.
Although conjugation of the coefficients $l_j \in L$, $l_0 + l_1 z + l_2 z^2 \mapsto \bar{l}_0 + \bar{l}_1 z + \bar{l}_2 z^2$, does not define an algebra homomorphism, we can ask for elements of $\mathbb{U}(F)$ and $\mathbb{SU}(F)$ whose coefficients are fixed under conjugation, respectively mapped to their negative, i.e. $l_j \in M$ for all j, respectively $l_j \in \sqrt{-d}M$ for all j.

Proposition 4.2. (a) *The single element of* $\mathbb{SU}(F)$ *given by a first row* (l_0, l_1, l_2) *such that* $\bar{l}_j = \epsilon l_j$, $j = 0, 1, 2$, *with* $\epsilon \in \{\pm 1\}$, *is the identity.*

(b) *The elements of* $\mathbb{U}(F)$ *given by a first row* (l_0, l_1, l_2) *such that* $\bar{l}_j = l_j$, $j = 0, 1, 2$, *are* $g = \pm 1$, $g = lz$ *if* $l \in M$ *is a solution of* $\rho(b)l^2 = 1$, *and* $g = lz^2$ *if* $l \in M$ *is a solution of* $\rho(b)\rho^2(b)l^2 = 1$.

(c) *The elements of* $\mathbb{U}(F)$ *given by a first row* (l_0, l_1, l_2) *such that* $\bar{l}_j = -l_j$, $j = 0, 1, 2$, *are* $g = l$ *if* $l \in \sqrt{-d}M$ *is a forth root of unity,* $g = \sqrt{-d} \cdot lz$ *if* $l \in M$ *is a solution of* $d\rho(b)l^2 = 1$, *and* $g = \sqrt{-d} \cdot lz^2$ *if* $l \in M$ *is a solution of* $d\rho(b)\rho^2(b)l^2 = 1$.

Proof. Let $\epsilon \in \{\pm 1\}$. Let (l_0, l_1, l_2) be the first row of an element g of $\mathbb{U}(F)$ satisfying $\bar{l}_j = \epsilon l_j$ for $j = 0, 1, 2$. As $a \in E \setminus F$, condition (5) splits into two conditions

$$l_0\rho(l_2) = 0 \quad \text{and} \quad l_1\rho(l_0) + \rho^2(b)l_2\rho(l_1) = 0.$$

By the first one, l_0 or l_2 is zero. Then, by the second condition the other one or l_1 is zero, too. So $g = lz^k$ is monomial. The proposition now follows easily by evaluation of condition (4). □

4.2. S**-arithmetic points.** We assume F to be totally real and E/F to be imaginary quadratic. In working with integer valued points we have to take into account the discussion of their definition in section 3.2. But even in the case of $a \in E^\times$ or $b \in M^\times$ not being units in the corresponding rings of integers, to ask for possible denominators of the coefficients of the F-valued points in the cyclic presentation is interesting.

We answer this question in two special cases. First, for the case of monomial elements. Second, notice that in case the quantity b defining the involution α can be chosen to belong to F, the subgroups $\mathbb{U}(F)^\rho$ and $\mathbb{SU}(F)^\rho$ of $Gal(E/F)$-fixed points in $\mathbb{U}(F)$ and $\mathbb{SU}(F)$, respectively, give themselves rise to group schemes over F. They are associated to the unitary, respectively, special unitary group for the hermitian form on E^3 induced by the involution (3) restricted to the subalgebra $M_3(E)$ of $M_3(L)$. We characterize the denominators of $\mathbb{U}(F)^\rho$ and $\mathbb{SU}(F)^\rho$ in this case.

Definition 4.3. For a set S of prime ideals of the number field F we denote by $\mathfrak{o}_F(S)$ the subring of F in which exactly the prime ideals in S are invertible.

Definition 4.4. (a) We say a prime ideal $\mathfrak{p}$ of F satisfies **Property A** for the extension $L/E/F$, if $\mathfrak{p}$ does not contain two, and if $\mathfrak{p}$ is inert in E but splits in L.

(b) We say a prime ideal $\mathfrak{p}$ of F satisfies **Property B** for the extension E, if $\mathfrak{p}$ does not contain two, and $\mathfrak{p}$ is either inert or ramified in E such that $F_\mathfrak{p}$ does not contain the sixth roots of unity.

Proposition 4.5. *Let* S *be a set of primes* $\mathfrak{p}$ *of* F *satisfying Property A, and for which the valuations* $v_\mathfrak{p}(b)$ *are zero. Then the monomial elements* $g = lz^j \in \mathbb{SU}(F)$ *with* $l \in \mathfrak{o}_L(S)$ *are the third roots of unity contained in* E.

Here $\mathfrak{o}_L(S)$ denotes $\mathfrak{o}_L(S) = \mathfrak{o}_E(S)\lambda_0 + \mathfrak{o}_E(S)\lambda_1 + \mathfrak{o}_E(S)\lambda_2$ for any integral basis $\lambda_0, \lambda_1, \lambda_2$ of $\mathfrak{o}_L$.

Proof of proposition 4.5. For $\mathfrak{p} \in S$ let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ be the prime ideals of $\mathfrak{o}_L$ above $\mathfrak{p}$, so $\mathfrak{p}\mathfrak{o}_L = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{o}_L$. Recall the field M is the subfield of L fixed by conjugation. Because $\mathfrak{p}$ is unramified in E, the prime ideals $\mathfrak{p}_k$ are defined by their intersection with M, $\mathfrak{p}_k = (\mathfrak{p}_k \cap \mathfrak{o}_M)$. For $l \in \mathfrak{o}_L(S)$, there are integers r_k such that $v_{\mathfrak{p}_k}(l) = r_k$, $k = 1, 2, 3$. Let $g = lz^j$ satisfy the unitary condition (4), $1 = c(j, b)\,\mathrm{N}_{L/M}(l)$ where $c(0, b) = 1$, $c(1, b) = \rho(b)$, $c(2, b) = \rho(b)\rho^2(b)$ have $\mathfrak{p}_k$-valuation zero. But then $v_{\mathfrak{p}_k}(\mathrm{N}_{L/M}(l)) = 2r_k$ must be zero, so $r_1 = r_2 = r_3 = 0$. Varying $\mathfrak{p}$ in S we obtain $l \in \mathfrak{o}_L^\times$. Because M/F is totally real, the unit group $\mathfrak{o}_M^\times$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^r$ for some $r \geq 2$. Let $e_1, \ldots, e_r$ be generators of the non-torsion part. Then $\mathfrak{o}_L^\times = \mathfrak{o}_E^\times \times < e_1, \ldots, e_r >$. Accordingly, write $l = \xi e_1^{s_1} \cdots e_r^{s_r}$. Then the unitary condition is

$$1 = c(j, b)\xi\bar{\xi} \cdot e_1^{2s_1} \cdots e_r^{2s_r}\,.$$

In particular, when $j = 0$ this is satisfied only if $s_1 = \cdots = s_r = 0$ and $1 = \xi\bar{\xi}$. In case $g = l \in \mathbb{SU}(F)$ the determinant condition $1 = \mathrm{N}_{L/E}(\xi) = \xi^3$ implies ξ is a third root of unity. □

Theorem 4.6. *For the division algebra of theorem 2.1 assume that for the structure constant $a \in \mathfrak{o}_E$ the involution is given by some $b \in F$. Let S be a set of prime ideals $\mathfrak{p}$ of F satisfying Property B and for which the valuations $v_{\mathfrak{p}}(b)$ are zero. Then, apart from the monomial solutions $g = lz^j$, where $l \in \mathfrak{o}_E^\times$ with $b^j l\bar{l} = 1$, there is no element in $\mathbb{U}(F)$ given by coordinates (l_0, l_1, l_2) with $l_j \in \mathfrak{o}_E(S)$ for $j = 0, 1, 2$ in the cyclic presentation. In particular, the elements of $\mathbb{SU}(F)^\rho$ of this kind are the third roots of unity contained in E.*

In the case of the coincidence of the maximal order of integer points $\mathfrak{o}_D$ with the cyclic order $\Lambda = \mathfrak{o}_L \oplus \mathfrak{o}_L z \oplus \mathfrak{o}_L z^2$, theorem 4.6 implies the triviality of the $\mathfrak{o}_F(S)$-valued points of $\mathbb{SU}^\rho$. We formulate this in the Kummer case, i.e. in case $E = F(\zeta_3)$.

Corollary 4.7. *For the division algebra of theorem 2.1 assume $E = F(\zeta_3)$, and assume the constants are $a \in \mathfrak{o}_E^\times$ and $b \in \mathfrak{o}_F^\times$. Then for all sets S of prime ideals of F ramified or unramified and non-split in E the group $\mathbb{SU}(\mathfrak{o}_F(S))^\rho$ of $\mathfrak{o}_F(S)$-valued points is $\{1, \zeta_3, \bar{\zeta}_3\}$.*

For the proof of theorem 4.6 we need the following lemma.

Lemma 4.8. *Consider the system of equations*

$$l_0\bar{l}_0 + bl_1\bar{l}_1 + b^2 l_2\bar{l}_2 = 0, \tag{8}$$

$$a\bar{l}_0 l_2 + b\bar{l}_1 l_0 + b^2\bar{l}_2 l_1 = 0. \tag{9}$$

(a) Assume for a prime p and an integer n that $p^n \equiv 5 \mod 6$. Let $a \in \mathbb{F}_{p^{2n}} \setminus \mathbb{F}_{p^n}$ satisfy $a\bar{a} = b^3$ for some $b \in \mathbb{F}_{p^n}^\times$. Then the above system of equations only has the trivial solution $(l_0, l_1, l_2) = (0, 0, 0)$ for $l_j \in \mathbb{F}_{p^{2n}}$, $j = 0, 1, 2$.

(b) Let p be an odd prime and such that for some n the finite field $\mathbb{F}_{p^n}$ does not contain the third roots of unity. On the residue class ring $R = \mathbb{F}_{p^n}[\pi]/(\pi^2)$ let conjugation be given by $\bar{\pi} = -\pi$. Let $a \in R^\times \setminus \mathbb{F}_{p^n}^\times$ and $b \in \mathbb{F}_{p^n}^\times$ satisfy the relation $a\bar{a} = b^3$. Then the above system of equations with $l_0, l_1, l_2 \in R$ only has the solutions $(l_0, l_1, l_2) \equiv (0, 0, 0) \mod \pi$.

Proof of lemma 4.8. For (a), if one of the l_j is zero, then by (9) another one is zero. But then by (8), the remaining one must be zero, too. So for a non-trivial solution we have $l_0 l_1 l_2 \neq 0$. For (b), the same argument holds for a non-trivial solution mod π. So in both cases we may assume without loss of generality $l_2 = 1$, because the equations are homogeneous. Then equations (8) and (9) simplify to

$$l_0\bar{l}_0 + bl_1\bar{l}_1 + b^2 = 0, \tag{10}$$

$$a\bar{l}_0 + b\bar{l}_1 l_0 + b^2 l_1 = 0. \tag{11}$$

From (11) and its conjugate we obtain the following system of linear equations for $l_1, \bar{l}_1$,

$$\begin{pmatrix} b^2 & bl_0 \\ b\bar{l}_0 & b^2 \end{pmatrix} \begin{pmatrix} l_1 \\ \bar{l}_1 \end{pmatrix} = \begin{pmatrix} -a\bar{l}_0 \\ -\bar{a}l_0 \end{pmatrix}.$$

Multiplying by the adjunct $\begin{pmatrix} b^2 & -bl_0 \\ -b\bar{l}_0 & b^2 \end{pmatrix}$ of the matrix involved we get

$$b^2(b^2 - l_0\bar{l}_0) \begin{pmatrix} l_1 \\ \bar{l}_1 \end{pmatrix} = \begin{pmatrix} -ab^2\bar{l}_0 + \bar{a}bl_0^2 \\ ab\bar{l}_0^2 - \bar{a}b^2 l_0 \end{pmatrix}.$$

Concerning case (a), there are two possibilities. First, assume $b^2 - l_0\bar{l}_0 \neq 0$. Then the linear equation has the solution $l_1 = \frac{\bar{a}bl_0^2 - ab^2\bar{l}_0}{b^2(b^2 - l_0\bar{l}_0)}$. Inserting

$$l_1\bar{l}_1 = \frac{a\bar{a}b^2(l_0\bar{l}_0)^2 - a^2b^3\bar{l}_0^3 - \bar{a}^2b^3l_0^3 + a\bar{a}b^4l_0\bar{l}_0}{b^4(b^2 - l_0\bar{l}_0)^2}$$

into (10) yields

$$0 = (b^3 - a\overline{a^{-1}l_0^3})(b^3 - \bar{a}a^{-1}l_0^3).$$

Notice that the condition $p^n \equiv 5 \mod 6$ is satisfied only for primes $p \equiv 5 \mod 6$ and odd n. Equivalently, there exists no primitive sixth root of unity in the finite field $\mathbb{F}_{p^n}$. The last equation being equivalent to $l_0^3 = a^2$, we obtain $(l_0\bar{l}_0)^3 = (a\bar{a})^2 = b^6$, which is equivalent to $l_0\bar{l}_0 = b^2$. This is a contradiction to the assumption.
Second, assume $l_0\bar{l}_0 = b^2$. In this case the linear system above forces $\bar{a}bl_0^2 = ab^2\bar{l}_0$. Inserting $l_0\bar{l}_0$ into (10) yields $l_1\bar{l}_1 = -2b$, and multiplying the original equation (11) by $\bar{a}l_0$ yields

$$a\bar{l}_0\bar{l}_1 + \bar{a}l_0l_1 = -b^3.$$

These two equations imply

$$(l_0l_1 - a)(\overline{l_0l_1} - \bar{a}) = (l_0\bar{l}_0)(l_1\bar{l}_1) - (a\overline{l_0l_1} + \bar{a}l_0l_1) + a\bar{a} = -2b^3 + b^3 + b^3 = 0.$$

Equivalently, $l_0l_1 = a$. But if so, $l_0\bar{l}_0l_1\bar{l}_1 = a\bar{a} = b^3$, so $l_1\bar{l}_1 = b$. This is a contradiction to $l_1\bar{l}_1 = -2b$.

In case (b) exactly the same argument read modulo π runs through. So in neither case we obtain a non-trivial solution satisfying the conditions of proposition 4.8. □

Proof of theorem 4.6. We notice that Property B for a prime ideal $\mathfrak{p}$ is equivalent to the condition that the étale extension $E_{\mathfrak{p}}/F_{\mathfrak{p}}$ is a field extension, and such that the residue class field $\kappa_{F_{\mathfrak{p}}}$ does not contain a primitive sixth root of unity. So $\kappa_{F_{\mathfrak{p}}} \cong \mathbb{F}_{p^n}$, and either $p = 3$ or $p^n \equiv 5 \mod 6$.
Assume (l_0, l_1, l_2) gives rise to an element g of $\mathbb{U}(F)$ with $l_j \in \mathfrak{o}_E(S)$, $j = 0, 1, 2$. If actually each $l_j \in \mathfrak{o}_E$, then all the summands of condition (4) are non-negative. For a suitably chosen embedding of F into $\mathbb{R}$, we have $l_0\bar{l}_0 = 0$ or $l_0\bar{l}_0 = 1$. So either $l_0 = 0$ or $l_1 = l_2 = 0$. By (5), in the first case one of l_1, l_2 is zero, too. So in order to satisfy condition (4), g must be monomial, $g = lz^j$ for an element $l \in \mathfrak{o}_E^\times$ of norm one. Applying proposition 4.1, we only obtain the trivial solutions $(l_0, l_1, l_2) = (\zeta_3^k, 0, 0)$ in $\mathbb{SU}(F)$.
For a non-trivial solution with $l_j \in \mathfrak{o}_E(S)$, $j = 0, 1, 2$, and $l_j \notin \mathfrak{o}_E$ for at least one j, there exists a prime ideal $\mathfrak{p} \in S$ and an integer $r > 0$ such that $\mathfrak{p}^r l_j$ belongs to the ring $\mathfrak{o}_{E_{\mathfrak{p}}}$ of $\mathfrak{p}$-adic integers, $j = 0, 1, 2$. We assume r to be chosen minimal with this property. Let π be a uniformizing element of the prime ideal in $\mathfrak{o}_{E_{\mathfrak{p}}}$. We obtain a tuple $(l_0', l_1', l_2') = \pi^r(l_0, l_1, l_2)$ which satisfies the two unitary conditions (4), (5) for (l_0, l_1, l_2) and leads to the two homogeneous conditions (8) and (9) of lemma 4.8 (a) for (l_0', l_1', l_2') modulo (π), in case $E_{\mathfrak{p}}/F_{\mathfrak{p}}$ is unramified. Respectively, if $E_{\mathfrak{p}}/F_{\mathfrak{p}}$ is ramified, (l_0', l_1', l_2') modulo (π^2) satisfy the conditions (8) and (9) of lemma 4.8 (b). Because $b \in \mathfrak{o}_{F_{\mathfrak{p}}}^\times$ by assumption, lemma 4.8 applies. So (l_0', l_1', l_2') must be zero modulo (π). This contradicts the minimal choice of r. □

The following restriction for the denominators of $\mathbb{U}(F)^\rho$ is a consequence of the proof of theorem 4.6.

Corollary 4.9. *For the division algebra of theorem 2.1 assume $b \in F$. Let $g(l_0, l_1, l_2)$ be an element of $\mathbb{U}(F)^\rho$. Then the denominators of $l_j \in E$ are not contained in prime ideals $\mathfrak{p}$ of E lying over prime ideals of F satisfying Property B such that $v_{\mathfrak{p}}(b) = 0$.*

Proof of corollary 4.9. Let $\mathfrak{p}$ be a prime satisfying the conditions above and consider $g(l_0, l_1, l_2)$ as an element of $\mathbb{U}(F_{\mathfrak{p}})^\rho$. If $g(l_0, l_1, l_2) \notin \mathbb{U}(\mathfrak{o}_{F_{\mathfrak{p}}})^\rho$, then there is an integer $r > 0$ (again chosen minimally) such that $\pi^r(l_0, l_1, l_2) = (l_0', l_1', l_2')$ satisfies (8) and (9) modulo (π) , and by lemma 4.8, $(l_0', l_1', l_2') \equiv (0, 0, 0)$ modulo π, contradicting the minimal choice of r. □

The notion of $\mathfrak{o}_F(S)$-valued points becomes relevant when there is a $\mathfrak{o}_F$-structure on the special unitary group $\mathbb{SU}$. Then the group $\mathbb{SU}(\mathfrak{o}_F(S))$ is an arithmetic subgroup of $\mathbb{SU}(F_{\mathfrak{p}})$. In particular, if $\mathbb{SU}(F_v)$ is compact for some archimedean place v, the quotient will be cocompact ([4], [5]). Any explicit description of $\mathbb{SU}(\mathfrak{o}_F(S))$, or of some congruence subgroup allows to deduce properties of the quotient $\mathbb{SU}(\mathfrak{o}_F(S))\backslash\mathbb{SU}(F)$. But the following example gives evidence that by choosing a cyclic presentation, i.e. controlling the involution α, even the explicit detection of non-trivial elements of $\mathbb{SU}(\mathfrak{o}_F(S))$ is sophisticated.

4.3. **Example.** For simplicity we assume the ground field F to equal the rationals $\mathbb{Q}$, but this example generalizes to arbitrary totally real ground fields, when the elements of finite order in D can be controlled. Let $E = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, where $\zeta_3 = \frac{1}{2}(-1+\sqrt{-3})$. Let $M/\mathbb{Q}$ be a totally real C_3-Galois extension such that $L = EM$ be C_6-Galois over $\mathbb{Q}$. We assume that the norm of L/E is not surjective on $\mathfrak{o}_E^\times$ (that is, L does not contain the ninth roots of unity). For example, one could choose M to be generated by the polynomial $f(X) = X^3 - 13X + 13$. Choose the structure constant $a = \zeta_3^j$ of the division algebra D in theorem 2.1 to be a power of ζ_3, where $j \not\equiv 0 \mod 3$. Then $a \notin \mathrm{N}_{L/M}$ and D is indeed a division algebra. Because $a\bar{a} = 1$, we may choose the involution constant $b = 1$. So the involution (2) written with respect to the cyclic presentation is

$$\alpha \,:\, \begin{pmatrix} l_0 & l_1 & l_2 \\ a\rho(l_2) & \rho(l_0) & \rho(l_1) \\ a\rho^2(l_1) & a\rho^2(l_2) & \rho^2(l_0) \end{pmatrix} \mapsto \begin{pmatrix} \bar{l}_0 & \bar{a}\rho(\bar{l}_2) & \bar{a}\rho^2(\bar{l}_1) \\ \bar{l}_1 & \rho(\bar{l}_0) & \bar{a}\rho^2(\bar{l}_2) \\ \bar{l}_2 & \rho(\bar{l}_1) & \rho^2(\bar{l}_0) \end{pmatrix} .$$

The unitary groups $\mathbb{U}$ and $\mathbb{SU}$ are defined over $\mathbb{Z}$, and the different notions of integer valued points coincide. At infinity the involution $\alpha : M_3(\mathbb{C}) \to M_3(\mathbb{C})$ is simply given by the conjugate transpose, $\alpha(g) = \bar{g}'$. In particular, $\mathbb{U}(\mathbb{R})$ and $\mathbb{SU}(\mathbb{R})$ are compact (see proposition 3.5).

The subfield $E(z)$ of D is isomorphic to $\mathbb{Q}(\zeta_9)$. Theorem 4.6, corollary 4.7 and corollary 4.9 imply that for elements $l_0 + l_1 z + l_2 z^2 \in E(z)$ to belong to $\mathbb{U}(\mathbb{Q})$ it is necessary that the primes p occurring in the denominators of l_0, l_1, l_2 are split in E. In particular, for a set S of primes $p \equiv 5 \mod 6$, the subgroup $\mathbb{SU}(\mathbb{Z}(S))^\rho$ is given by the third roots of unity $1, \zeta_3, \zeta_3^2$ in E. Notice that $\mathbb{SU}(\mathbb{Z}(S))^\rho$ is the intersection of $\mathbb{SU}(\mathbb{Z}(S))$ with $E(z)^\times$ Additionally, assume that the primes of S actually satisfy Property A, that is L_p is a split algebra. Then by proposition 4.5 respectively corollary 3.3, the intersection of $\mathbb{SU}(\mathbb{Z}(S))$ with L is $\{1, \zeta_3, \zeta_3^2\}$, too:

In S-arithmetic subgroups (S satisfying Property A), the elements belonging to the two obvious subfields L and $E(z)$ of D are the trivial ones contained in $\mathfrak{o}_E^\times$.

The meaning of Property A is the following. Let p be a prime such that E_p is non-split and L_p is split. So D_p is split, and the embedding (1) identifies $D_p = D \otimes_{\mathbb{Z}} \mathbb{Q}_p$ with $M_3(E_p)$ by the isomorphism $L_p \cong E_p \oplus E_p \oplus E_p$ given by the three embeddings ρ^j of L into E_p. Then $\mathbb{SU}(\mathbb{Q}_p)$ is isomorphic to $SU_3(E_p)$, the up to equivalence unique special unitary group over E_p/F_p of degree three (see [9, 1.9]). And the isomorphism is given by the above embedding. Then for $S = \{p\}$ the group $\mathbb{SU}(\mathbb{Z}(S)) = \mathbb{SU}(\mathbb{Z}[\frac{1}{p}])$ is an arithmetic subgroup of $SU_3(E_p)$. Because $\mathbb{SU}(\mathbb{R})$ is compact, $\mathbb{SU}(\mathbb{Z}(S))$ is cocompact in $SU_3(E_p)$ (see [4], [5]). For the resulting quotient it is natural to study the action of the arithmetic subgroup on the affine Bruhat-Tits tree, the quotients becoming finite graphs. In case p is ramified, this is the $(p+1)$-regular SL_3-tree, in case p is unramified, we obtain a $(p+1, p^3+1)$-bi-regular tree. In view of lemma 4.10, the finite quotient graphs modulo $\mathbb{SU}_0 \cap \mathbb{SU}(\mathbb{Z}[\frac{1}{p}])$ will be Ramanujan ([7]), respectively, bi-Ramanujan ([2]). The latter case was treated in [3], and this article is in some sense its conceptional continuation.

Lemma 4.10. *In the cyclic presentation of the division algebra let* $E = \mathbb{Q}(\zeta_3)$, $a = \zeta_3^j$, *(*$j \not\equiv 0 \mod 3$*), and* $b = 1$. *Then the special unitary group* $\mathbb{SU}(\mathbb{Q})$ *is the direct product of* $\mu_3 =< \zeta_3 >$ *with a torsion-free subgroup* $\mathbb{SU}_0$.

Proof. By corollary 3.3, the elements of finite order are $\mu_3 \subset E^\times$. We have an exact sequence

$$1 \longrightarrow \mu_3 \longrightarrow \mathbb{SU}(\mathbb{Q}) \longrightarrow \mathbb{SU}_0 \longrightarrow 1\,,$$

which splits because μ_3 belongs to the center of $D^\times$. □

References

[1] A. A. Albert: *Involutorial simple algebras and real Riemann matrices,* Ann. Math., Vol 36, No. 4 (1935), 886-964.

[2] C. Ballantine, D. Ciubotaru: *Ramanujan bigraphs associated with SU*(3) *over a p-adic field,* Proc. am. math. soc. Vol. 39, Nr. 6 (2011), 1939-1953.

[3] C. Ballantine, B. Feigon, R. Ganapathy, J. Kool, K. Maurischat and A. Wooding: *Explicit construction of Ramanujan bigraphs,* in Women in Numbers Europe: Research Directions in Number Theory, Association for Women in Mathematics Series, vol. 2, Springer (2015), 1-16.

[4] A. Borel: *Some finiteness properties of the adèle groups over number fields,* Publ. Math. IHES 16 (1963), 5-30.

[5] A. Borel, G. Harder: *Existence of discrete cocompact subgroups of reductive groups over local fields,* Journal reine angew. Mathematik, Vol. 298 (1978), page 53-64.

[6] M.-A. Knus, A. Merkurjev, M. Rost, J.-P. Tignol: *The book of involutions,* AMS (1998)

[7] A. Lubotzky, R. Philips, P. Sarnak: *Ramanujan graphs,* Combinatorica, Vol. 8 (1988), 261-277.

[8] I. Reiner: *Maximal orders,* Academic Press, London (1975).

[9] J. Rogawski: *Automorphic representations of unitary groups in three variables,* Princeton University Press (1990).

Kathrin Maurischat, Mathematisches Institut, Heidelberg University, Im Neuenheimer Feld 205, 69120 Heidelberg, Germany

E-mail address: maurischat@mathi.uni-heidelberg.de