A NOTE ON THE SPECIAL UNITARY GROUP OF A DIVISION ALGEBRA

B.A. SETHURAMAN AND B. SURY

Abstract. If D is a division algebra with center a number field K and with an involution of the second kind, it is unknown if the group $SU(1, D)/[U(1, D), U(1, D)]$ is trivial. We show that, by contrast, if K is a function field in one variable over a number field, and if D is an algebra with center K and with an involution of the second kind, the group $SU(1, D)/[U(1, D), U(1, D)]$ can be infinite in general. We give an infinite class of examples.

1. Introduction

Let K be a number field, and let D be a division algebra with center K, with an involution of the second kind, τ. Let $U(1, D)$ be the unitary group of D, that is, the set of elements in D^* such that $d\tau(d) = 1$. Let $SU(1, D)$ be the special unitary group, that is, the set of elements of $U(1, D)$ with reduced norm 1. An old theorem of Wang [7] shows that for any central division algebra over a number field, $SL(1, D)$ is the commutator subgroup of D^*. It is an open question (see [4, p.536]) whether the group $SU(1, D)$ equals the group $[U(1, D), U(1, D)]$ generated by unitary commutators.

We show in this note that, by contrast, if K is a function field in one variable over a number field, and if D is an algebra with center K and with an involution of the second kind, the group $SU(1, D)$ modulo $[U(1, D), U(1, D)]$ can be infinite in general. More precisely, we prove :

Theorem 1.1. *Let $n \geq 3$, and let ζ be a primitive n-th root of one. Then, there exists a division algebra D of index n with center $\mathbb{Q}(\zeta)(x)$ which has an involution of the second kind such that the corresponding group $SU(1, D)/[U(1, D), U(1, D)]$ is infinite.*

Date: October 1, 2004.

This work was done when the first-named author visited the Indian Statistical Institute, Bangalore. He would like to thank the institute for the wonderful hospitality during his stay there.

Mathematical Reviews Subject Classification : 16K20,12E15.

Our algebra will be the symbol algebra $D = (a, x; \zeta, K, n)$ where $K = \mathbb{Q}(\zeta)(x)$ and $a \in \mathbb{Q}$ is such that $[\mathbb{Q}(\zeta)(\sqrt[n]{a}) : \mathbb{Q}(\zeta)] = n$. This is the K-algebra generated by two symbols r and s subject to the relations $r^n = a$, $s^n = x$, and $sr = \zeta rs$. If we write L for the K subalgebra of D generated by r, it is clear that L is just the field $\mathbb{Q}(\zeta, \sqrt[n]{a})(x)$. The Galois group L/K is generated by σ that sends r to ζr: note that conjugation of L by s has the same effect as σ on L. An easy computation shows that x^n is the smallest power of x that is a norm from L to K, so standard results from cyclic algebras ([3, Chap. 15.1] for instance) show that D is indeed a division algebra. It is well known that D has a valuation on it that extends the x-adic valuation on K. This valuation will be crucial in proving our theorem.

2. The valuation on D

We recall here how the x-adic valuation is defined on D. Recall first how the x-adic (discrete) valuation is defined on any function field $E(x)$ over a field E: it is defined on polynomials $f = \sum_i a_i x^i$ $(a_i \in E)$ by $v(f) = min\{i \mid a_i \neq 0\}$, and on quotients of polynomials f/g by $v(f/g) = v(f) - v(g)$. The value group Γ_L is $\mathbb{Z}$, while the residue $\overline{L}$ is E. This definition gives valuations on all three fields $\mathbb{Q}(\zeta + \zeta^{-1})(x)$, K, and L, all of which we will refer to as v. These fields have residues (respectively) $\mathbb{Q}(\zeta + \zeta^{-1})$, $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta, \sqrt[n]{a})$ with respect to v. It is standard that the valuation v on $\mathbb{Q}(\zeta + \zeta^{-1})(x)$ extends uniquely to K, a fact that will be crucial to us.

With v as above, we define a function, also denoted v, from D^* to $(1/n)\mathbb{Z}$ as follows: first, note that each d in D^* can be uniquely written as $d = l_0 + l_1 s + \cdots + l_{n-1} s^{n-1}$, for $l_i \in L$. (We will call each expression of the form $l_i s^i$, $i = 0, 1, \cdots n-1$, a *monomial*.) Define $v(s) = 1/n$, and $v(l_i s^i)$ as $v(l_i) + iv(s)$. Note that the n values $v(l_i s^i); 0 \leq i < n$ are all distinct, since they lie in different cosets of $\mathbb{Z}$ in $(1/n)\mathbb{Z}$. Thus, exactly one of these n monomials has the least value among them, and we define $v(d)$ to be the value of this monomial. It is easy to check that v indeed gives a valuation on D. We find $\Gamma_D = (1/n)\mathbb{Z}$, so $\Gamma_D/\Gamma_K = \mathbb{Z}/n\mathbb{Z}$. Also, the residue $\overline{D}$ contains the field $\mathbb{Q}(\zeta, \sqrt[n]{a})$. The fundamental inequality ([5, p.21]) $[D : K] \geq [\Gamma_D/\Gamma_K][\overline{D} : \overline{K}]$ shows that $\overline{D} = \overline{L} = \mathbb{Q}(\zeta, \sqrt[n]{a})$.
Note that since D is valued, the valuation v (restricted to K) extends uniquely from K to D ([6]).

3. Computation of $SU(1,D)$ and $[U(1,D),U(1,D)]$

Write k for the field $\mathbb{Q}(\zeta+\zeta^{-1})(x)$, and τ for the nontrivial automorphism of K/k that sends ζ to ζ^{-1}. Note that since a and x belong to the field k, we may define an involution on D that extends the automorphism of K/k by the rule $\tau(fr^is^j)=\tau(f)\zeta^{ij}r^is^j$ for any $f\in K$ (so $\tau(r)=r$, $\tau(s)=s$; see [2, Lemma 7].)

Proof of the theorem. Let d be in $U(1,D)$, so $d\tau(d)=1$. Since v and $v\circ\tau$ are two valuations on D that coincide on k, and since v extends uniquely from k to K, and then uniquely from K to D, we must have $v\circ\tau=v$. Thus, we find $2v(d)=0$, that is, d must be a unit. Then, for any d and e in $U(1,D)$, we take residues to find $\overline{ded^{-1}e^{-1}}=\overline{d}\overline{e}\overline{d}^{-1}\overline{e}^{-1}$. However, $\overline{D}=\overline{L}=\mathbb{Q}(\zeta)(\sqrt[n]{a})$ is commutative, so $\overline{d}$ and $\overline{e}$ commute, so $\overline{ded^{-1}e^{-1}}=1$.

Note that we have a natural inclusion of $\overline{L}$ in the v-units of L; we identify $\overline{L}$ with its image in L. Under this identification, for any $l\in\overline{L}\subseteq L$, $\overline{l}=l$. Since the commutator of two elements in $U(1,D)$ has residue 1, it suffices to find infinitely many elements in $SU(1,D)\cap\overline{L}$ to show that $SU(1,D)$ modulo $[U(1,D),U(1,D)]$ is infinite.

Write L_1 and L_2 (respectively) for the subfields $\mathbb{Q}(\zeta+\zeta^{-1})(r)$ and $\mathbb{Q}(\zeta)$ of $\overline{L}$; note that L_2 is the residue field of K. Then the involution τ on D acts as the nontrivial automorphism of $\overline{L}/L_1$, so for any $l\in\overline{L}$, $l\tau(l)$ is the norm map from $\overline{L}$ to L_1. The automorphism σ of L/K restricts to an automorphism (also denoted by σ) of $\overline{L}/L_2$, and it is standard that the reduced norm of l viewed as an element of D is just the norm of l from L to K ([3, Chap. 16.2] for instance), and hence the norm of l from $\overline{L}$ to L_2. We thus need to find infinitely many $l\in\overline{L}$ such that $N_{\overline{L}/L_1}(l)=N_{\overline{L}/L_2}(l)=1$.

Now, the set $S_1=\{l\in\overline{L}: N_{\overline{L}/L_1}(l)=1\}$ is indexed by the L_1 points of the torus $T_1=R^{(1)}_{\overline{L}/L_1}\mathbf{G_m}$ (see [4], § 2.1). Similarly, the set $S_2=\{l\in\overline{L}: N_{\overline{L}/L_2}(l)=1\}$ is indexed by the L_2 points of the torus $T_2=R^{(1)}_{\overline{L}/L_2}\mathbf{G_m}$. To show that $S_1\cap S_2$ is infinite, we switch to a common field by noting that the groups $T_1(L_1)$ and $T_2(L_2)$ are just the k_0 points of the groups $(R_{L_1/k_0}T_1)$ and $(R_{L_2/k_0}T_2)$ respectively, where $k_0=\mathbb{Q}(\zeta+\zeta^{-1})$. Thus, it suffices to check that $(R_{L_1/k_0}T_1\cap R_{L_2/k_0}T_2)(k_0)$ is infinite, and for this, it is sufficient to check that $(R_{L_1/k_0}T_1\cap R_{L_2/k_0}T_2)^0(k_0)$ is infinite. As both $R_{L_1/k_0}T_1$ and $R_{L_2/k_0}T_2$ are k_0-tori, the connected component $(R_{L_1/k_0}T_1\cap R_{L_2/k_0}T_2)^0$ is a k_0-torus as well, since it is a connected commutative group defined over k_0 consisting of semisimple elements. So, its k_0 points are Zariski dense in its $\overline{\mathbb{Q}}$ points by a theorem of Grothendieck (see p.120 of [1]). Hence, it suffices to check that there are infinitely many $\overline{\mathbb{Q}}$ points in $(R_{L_1/k_0}T_1 \cap R_{L_2/k_0}T_2)^0$. But for this, it clearly suffices to check that there are infinitely many $\overline{\mathbb{Q}}$ points in $(R_{L_1/k_0}T_1 \cap R_{L_2/k_0}T_2)$.

Write any $l \in \overline{L}$ as $l = X + (\zeta - \zeta^{-1})Y$ where $X, Y \in L_1$. Then, $X = \sum_{i=0}^{n-1} x_i r^i$ and $Y = \sum_{i=0}^{n-1} y_i r^i$ where $x_i, y_i \in k_0$. Consider the equations $N_{\overline{L}/L_1}(l) = 1$ and $N_{\overline{L}/L_2}(l) = 1$. Rewrite these in terms of powers of r, invoking the actions of σ and τ and using the fact that $r^n = a$. The first equation now involves the $2n$ variables x_i, y_i and has coefficients in L_1. Equating the coefficients of r^i $(i = 0, \ldots, n-1)$ on both sides, we get n equations in the variables x_i, y_i with coefficients in k_0. Similarly, the second equation involves the variables x_i, y_i and has coefficients in L_2. Using the fact that $(\zeta - \zeta^{-1})^2 \in k_0$ and equating the coefficients of 1 and $\zeta - \zeta^{-1}$ on both sides, we get two equations in the variables x_i, y_i with coefficients in k_0. As $n \geq 3$, we have $n + 2 < 2n$ and these equations have infinitely many common solutions over $\overline{\mathbb{Q}}$. This proves the theorem.

4. Concrete illustration for $n = 3$

We illustrate the theorem for $n = 3$ by concretely constructing infinitely many elements in $SU(1, D)/[U(1, D), U(1, D)]$. We take $a = 2$ for simplicity. Write $l = a + b\sqrt{-3}$, where a and b are in L_1. Then $N_{\overline{L}/L_1}(l) = a^2 + 3b^2 = 1$ has a parametrized set of solutions $a = \dfrac{s^2 - 3}{s^2 + 3}$, $b = \dfrac{2s}{s^2 + 3}$, for $s \in L_1$. Write $s = t_0 + t_1 r + t_2 r^2$ for $t_i \in \mathbb{Q}$ and substitute in a and b above. Then compute $N_{\overline{L}/L_2}(l)$, noting that $\sigma(s) = (t_0 + \omega t_1 r + \omega t_2 r^2)$. We solve for the t_i so that $N_{\overline{L}/L_2}(l) = 1$. We claim that if we take $t_0 = 1$ and $t_1 = 0$, then for arbitrary $t_2 = t$, $N_{\overline{L}/L_2}(l) = 1$. Indeed, $l = u/v$ where

$$u = 2\omega + t^2 r - 2t\omega^2 r^2,$$

$$v = 2 + t^2 r + tr^2.$$

Then, an easy computation, using $r^3 = 2$, shows that

$$N_{\overline{L}/L_2}(u) = (2\omega + t^2 r - 2t\omega^2 r^2)(2\omega + t^2\omega r - 2t\omega r^2)(2\omega + t^2\omega^2 r - 2tr^2) = -8t^3 + 2t^6.$$

Similarly,

$$N_{\overline{L}/L_2}(v) = (2 + t^2 r + tr^2)(2 + t^2\omega r + t\omega^2 r^2)(2 + t^2\omega^2 r + t\omega r^2) = -8t^3 + 2t^6.$$

Thus, we have an infinite set of solutions and we are done. (Actually, the parametric solution above was first obtained using Mathematica^{TM}. The program gives other parametric solutions as well, for instance, $t_0 = 0, t_1 = -\frac{1}{2t_2}$.)

References

[1] A.Borel, *Linear algebraic groups*, Spriner-Verlag, 2nd edition, 1991.

[2] Patrick J. Morandi and B.A. Sethuraman, *Noncrossed product division algebras with a Baer ordering,* Proc. Amer. Math. Soc., **123** 1995, 1995–2003.

[3] Richard S. Pierce, *Associative Alegbras*, Graduate Texts in Mathematics, 88, Springer-Verlag, 1982.

[4] V.P.Platonov & A.S.Rapinchuk, *Algebraic groups and number theory*, Academic Press 1994.

[5] O.F.G Schilling, The Theory of Valuations, Math Surveys, No. 4., Amer. Math. Soc., Providence, R.I., 1950.

[6] Adrian R. Wadsworth, *Extending valuations to finite dimensional division algebras,* Proc. Amer. Math. Soc., **98** 1986, 20–22.

[7] S.Wang, *On the commutator group of a simple algebra,* Amer. J. Math., **72** 1950, 323-334.

Dept. of Mathematics, California State University Northridge, Northridge CA 91330, U.S.A.

E-mail address: `al.sethuraman@csun.edu`

URL: `http://www.csun.edu/~asethura/`

Stat-Math Unit, Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560 059, India

E-mail address: `sury@isibang.ac.in`