Math. Z. 252, 295–313 (2006) **Mathematische Zeitschrift**

DOI: 10.1007/s00209-005-0854-1

The Margulis-Platonov conjecture for $\mathrm{SL}_{1,D}$ and 2-generation of finite simple groups

Andrei S. Rapinchuk

Department of Mathematics, University of Virginia, Charlottesville, VA 22904, USA
(e-mail: asr3x@virginia.edu)

Received: 9 January 2004; in final form: 29 March 2005 /
Published online: 16 August 2005 – © Springer-Verlag 2005

In memory of my grandparents

Abstract. We give a new proof of the Margulis-Platonov conjecture for the groups $SL_{1,D}$ which is shorter than the previous proofs and in which the use of the classification of finite simple groups is limited to the fact that every such group is generated by two elements. The argument is based on further development of the methods of [18].

1. Introduction

Let D be a finite dimensional central division algebra over a global field K, and $G = \mathbf{SL}_{1,D}$ be the simple algebraic K-group associated with the group $SL(1, D)$ of elements in the multiplicative group $D^{\times}$ having reduced norm one. The goal of this paper is to give a new proof of the Margulis-Platonov conjecture (MP) for the group G which is considerably shorter than the existing proofs (see below) and in which the use of the classification of finite simple groups is limited to the fact that every such group is 2-generated. For the reader's convenience, we recall the statement of (MP) in the context of an arbitrary simple simply connected algebraic K-group G : *Let $\mathcal{A}$ be the set of all nonarchimedean valuations v of K such that G is anisotropic over the completion K_v, and $\delta\colon G(K) \to G_{\mathcal{A}} := \prod_{v\in\mathcal{A}} G(K_v)$ be the diagonal map. Then for any noncentral normal subgroup H of $G(K)$ there exists an open normal subgroup W of $G_{\mathcal{A}}$ such that $H = \delta^{-1}(W)$; in particular, if $\mathcal{A} = \emptyset$ then $G(K)$ does not have any proper noncentral normal subgroups.* We refer to [13], Ch. IX, and [17], Appendix A, for a discussion of (MP) and the available results. So, our purpose is to give a new proof of the following.

Theorem 1. (Segev-Seitz [20] , [23]) *The group $G = \mathbf{SL}_{1,D}$ satisfies the Margulis-Platonov conjecture (MP).*

To put our proof of this fact into perspective, we will give a brief survey of the previous results in this direction. The first proof of the theorem was obtained by Segev [20] and Segev and Seitz [23]. More precisely, in [16], the proof of (MP) for $\mathbf{SL}_{1,D}$ was reduced to proving that $D^\times$ does not have normal subgroups N such that $D^\times/N$ is a nonabelian finite simple group (cf. Proposition 1 below). The truth of this statement was conjectured in [16] for all finite dimensional division algebras over arbitrary fields (Conjecture (FSQ)) and verified for algebras of degree two and three (notice that already the case of cubic algebras required an extensive use of the classification of finite simple groups). In his paper [20], Segev made a major step towards proving (FSQ) for division algebras of arbitrary degree. Among revolutionary techniques introduced and efficiently used by Segev was the notion of the commuting graph Δ_F of a (finite nontrivial) group F : the vertex set of Δ_F is $F - \{e\}$, and two (distinct) vertices are connected iff the corresponding elements commute in F. As any graph, Δ_F has the natural distance function and the associated notion of diameter diam Δ_F (which is either a positive integer or ∞). Segev [20] proved that a finite simple group F whose commuting graph either (α) has diameter $\geqslant 5$, or (β) is balanced[1] cannot be a quotient of the multiplicative group $D^\times$ of a finite dimensional division algebra D. Then, in [23], Segev and Seitz used the classification and detailed description of finite simple groups to verify that for every (known) finite simple group the commuting graph satisfies one of the conditions (α) or (β) which completed the proof of Conjecture (FSQ) and gave the first proof of the above theorem.

Subsequently, in [17], the techniques of [20] were merged with some methods of the theory of valuations to, first, establish a congruence subgroup theorem for subgroups of finite index in $D^\times$, and, second, to use it for eliminating some finite nonsolvable groups as potential quotients of $D^\times$. We only mention that the congruence subgroup theorem proved in [17] asserts that if D is a finite dimensional division algebra over a finitely generated field K, then given a normal subgroup of finite index $N \subset D^\times$ such that diam $\Delta_{D^\times/N} \geqslant 4$, there exists a nontrivial valuation $\tilde{v}$ of D such that N is open in $D^\times$ in the topology defined by $\tilde{v}$ (which is sometimes called $\tilde{v}$-adic). One easily derives from this theorem that a finite simple group F with diam $\Delta_F \geqslant 4$ cannot be a quotient of $D^\times$ for a finite dimensional division algebra D over any field. This result considerably reduces the amount of computations with finite simple groups needed to prove (FSQ) as checking that diam $\Delta_F \geqslant 4$ for every nonabelian finite simple group F is a much easier task than verifying one of the conditions (α) or (β). On the other hand, the results of [17] fell short of proving a stronger conjecture, stated in [21], that all finite quotients of $D^\times$ are in fact solvable. The reason is that there are numerous examples of minimal nonsolvable groups (MNSG) whose commuting graph has diameter three (see [22]). However the congruence subgroup theorem as stated in [17] cannot be extended to the "diam $\geqslant 3$" situation as there are examples of normal subgroups of finite index $N \subset D^\times$ such that diam $\Delta_{D^\times/N} = 3$ but N is not open in D with respect to any single nontrivial valuation (see Example 8.4 in [17]). Thus, the techniques of

[1] See [20], §4, for the precise formulation of the "balance" condition; we only mention that it is stronger than "diam $\Delta_F \geqslant 4$" condition.

[17] turned out to be insufficient to eliminate the MNSGs with commuting graph having diameter three as potential quotients of $D^{\times}$.

The solvability of all finite quotients of $D^{\times}$ was established in [18] by refining the methods developed in [17]. Namely, it was shown that the congruence subgroup theorem of [17] remains valid if the assumption diam $\Delta_{D^{\times}/N} \geqslant 4$ is replaced with one technical condition which we termed "condition $(3\frac{1}{2})$" as it is weaker than "diam $\geqslant 4$" condition but stronger than "diam $\geqslant 3$" condition (see [18], §1, for the precise formulation). On the other hand, we have been able to verify that all the MNSGs satisfy condition $(3\frac{1}{2})$, so the modified congruence subgroup theorem applies in all cases where the quotient is a MNSG. The verification of $(3\frac{1}{2})$ for the MNSGs relied on the classification of finite simple groups, but the amount of computations was significantly smaller than in [23] (30 journal pages versus 100). Besides, the solvability of finite quotients enabled us to give another proof of (MP) which does not use the reduction obtained in [16].

These results suggest that the amount of the theory of finite simple groups needed to prove (MP) or similar results can be reduced via proving a congruence subgroup theorem for normal subgroups of finite index in $D^{\times}$ under weaker assumptions (on the commuting graph of the quotient). From this perspective, the critical threshold appears to be the case where diam $\Delta_{D^{\times}/N} = 3$. Indeed, it was shown in [22] by a relatively short argument that for every MNSG the commuting graph has diameter $\geqslant 3$, so a congruence subgroup theorem in diameter $\geqslant 3$ would enable one to give a more efficient proof of the solvability of finite quotients of $D^{\times}$. On the other hand, one can show by example (see §5) that no congruence subgroup theorem can be establsihed if diam $\Delta_{D^{\times}/N} \leqslant 2$. One should keep in mind, however, that as follows from Example 8.4 in [17], the assumption diam $\Delta_{D^{\times}/N} = 3$ does not guarantee in the general case that N is open in $D^{\times}$ with respect to the topology defined by a single nontrivial valuation $\tilde{v}$ of D. Nevertheless, the subgroup N constructed in Example 8.4 is open with respect to the topology defined by a pair of nontrivial valuations of D. So, we inquired in [18] if the condition diam $\Delta_{D^{\times}/N} = 3$ implies that N is open in $D^{\times}$ in the topology defined by a finite set $\tilde{T}$ of nontrivial (height one) valuations of D. In the present paper, we give the affirmative answer to this question for a finite dimensional division algebra D over a global field K, and then use this result to prove (MP).

Theorem 1. *Let D be a finite dimensional central division algebra over a global field K. Suppose $N \subset D^{\times}$ is a normal subgroup of finite index such that the commuting graph of $D^{\times}/N$ has diameter $\geqslant 3$. Then there exists a finite set $\tilde{T}$ of valuations of D such that N is open in $D^{\times}$ in the $\tilde{T}$-adic topology.*

The format of the paper is as follows. In §2 we show that Theorem 1 implies (MP). In §§3-4 we prove Theorem 1. The considerations in §3, which are valid over any field, reduce the proof of Theorem 1 to establishing certain properties for a specific subring of K (we notice that this part basically boils down to extending some results in §§2-3 of [18] to the case of several valuations). In §4, we prove some results about subrings of a global field (see Proposition 4), and derive with their help the required properties of the subring of K constructed in §3. We notice that both parts of the proof of Theorem 1 rely in an essential way on the results from [18] establishing the existence of so-called strongly leveled maps and their properties. Finally, in §5, we construct an example where diam $\Delta_{D^\times/N} = 2$ but N is not open in $D^\times$ with respect to any finite set of valuations of D.

The author would like to thank Gopal Prasad and Yoav Segev for their suggestions that helped to improve the exposition. Thanks are also due to the referee who read the manuscript very carefully and pointed out a large number of small errors. Finally, partial support from NSF grant DMS-0138315 and BSF grant No. 2000-171 is gratefully acknowledged.

2. Theorem 1 implies (MP)

First, we need to recall the notions involved in the statement of Theorem 1 as these will be extensively used throughout the paper (for all unexplained notations we refer the reader to [18]). Let D be a finite dimensional central division algebra over a field K, and $\tilde{T} = \{\tilde{v}_1, \ldots, \tilde{v}_r\}$ be a finite set of valuations of D. For each $\tilde{v} \in \tilde{T}$, we let $\tilde{\Gamma}_{\tilde{v}}$ (resp., $\mathcal{O}_{D,\tilde{v}}$) denote its value group (resp., the valuation ring). Given $\alpha_i \in (\tilde{\Gamma}_{\tilde{v}_i})_{\geqslant 0}$ for $i = 1, \ldots, r$, we let

$$\mathfrak{m}(\alpha_1, \ldots, \alpha_r) = \{x \in D^\times \mid \tilde{v}_i(x) > \alpha_i \text{ for all } i = 1, \ldots, r\} \cup \{0\};$$

clearly, $\mathfrak{m}(\alpha_1, \ldots, \alpha_r)$ is a 2-sided ideal of $\mathcal{O}_{D,\tilde{T}} := \cap_{\tilde{v} \in \tilde{T}} \mathcal{O}_{D,\tilde{v}}$. The ideals $\mathfrak{m}(\alpha_1, \ldots, \alpha_r)$ form a fundamental system of neighborhoods of zero for a topology on D compatible with the ring structure; this topology will be called $\tilde{T}$*-adic*. Thus, a subgroup $N \subset D^\times$ is $\tilde{T}$-adically open iff it contains the *congruence subgroup* $1 + \mathfrak{m}(\alpha_1, \ldots, \alpha_r)$ for some $\alpha_i \in (\tilde{\Gamma}_{\tilde{v}_i})_{\geqslant 0}$.

Next, we need to elaborate on the reduction, given in Theorem 2.1 of [16], of (MP) to proving that $D^\times$ cannot have a nonabelian finite simple group as a quotient. The argument therein made use of the fact, resulting from the classification, that any central (i.e. preserving all conjugacy classes) automorphism of a finite simple group is inner. For our purposes, we need to observe that the following weaker version of Theorem 2.1 can be established without this fact. The proof almost verbatim repeats the argument given in [16] and is reproduced here only for the sake of completeness.

Proposition 1. *Let D be a finite dimensional central division algebra over a global field K, and $G = \mathbf{SL}_{1,D}$. If (MP) fails for $G(K)$ then there exists a normal subgroup $N \subset D^\times$ such that the quotient $F := D^\times/N$ can be embedded into the tower* Inn $S \subseteq F \subseteq$ Aut S *where S is a nonabelian finite simple group.*

Proof. We first recall that the set $\mathcal{A}$ of nonarchimedean anisotropic valuations for G coincides with the set T_0 of all nonarchimedean valuations v of K such that $D_v := D \otimes_K K_v$ is a division algebra. Furthermore, a nonarchimedean valuation v of K belongs to T_0 iff it can be (uniquely) extended to a valuation $\tilde{v}$ of D, in which case the topology on D induced by the embedding $D \hookrightarrow D_v$ coincides with the topology defined by $\tilde{v}$. We need to note the following easy consequence of the analysis of the multiplicative structure of local division algebras given in [19].

Lemma 1. *Let D be a finite dimensional division algebra over a global field K, and $\tilde{T}$ be a finite set of valuations of D. Then for any $\tilde{T}$-adically open subgroup $N \subset D^{\times}$, the quotient $D^{\times}/N$ is solvable. Consequently, if $\delta\colon G(K) \to G_{\mathcal{A}}$ is the diagonal map as in the statement of (MP) then for any noncentral open normal subgroup $W \subset G_{\mathcal{A}}$, the quotient $G(K)/\delta^{-1}(W)$ is solvable.*

Proof. For the first assertion, it is enough to show that if $\tilde{T} = \{\tilde{v}_1, \dots, \tilde{v}_r\}$ then the quotient $H = D^{\times}/(1 + \mathfrak{m}(\alpha_1, \dots, \alpha_r))$ is solvable for any $\alpha_i \in (\Gamma_{\tilde{v}_i})_{\geqslant 0}$. Clearly, there is an embedding (in fact, an isomorphism)

$$H \hookrightarrow \prod_{i=1}^{r} D_{\tilde{v}_i}^{\times}/(1 + \mathfrak{P}_{\tilde{v}_i}(\alpha_i)),$$

where $D_{\tilde{v}_i}$ is the completion of D with respect to $\tilde{v}_i$ (which can be identified with $D \otimes_K K_{v_i}$, v_i being the restriction of $\tilde{v}_i$ to K), and $\mathfrak{P}_{\tilde{v}_i}(\alpha_i) = \{x \in D_{\tilde{v}_i}^{\times} \mid \tilde{v}_i(x) > \alpha_i\} \cup \{0\}$. In addition, let $\mathfrak{P}_{\tilde{v}_i} := \mathfrak{P}_{\tilde{v}_i}(0)$ be the valuation ideal in $D_{\tilde{v}_i}$, and $U_{\tilde{v}_i}$ be the group of units. Then it follows from the computations in [19] that: (1) $D_{\tilde{v}_i}^{\times}/U_{\tilde{v}_i} \simeq \mathbb{Z}$ (2) $U_{\tilde{v}_i}/(1 + \mathfrak{P}_{\tilde{v}_i})$ is a finite cyclic group, and (3) $(1 + \mathfrak{P}_{\tilde{v}_i})/(1 + \mathfrak{P}_{\tilde{v}_i}(\alpha_i))$ is a finite p_i-group where p_i is the characteristic of the residue algebra for $\tilde{v}_i$ (we notice that although [19] deals with algebras over local fields of characteristic zero, these results remain valid in any characteristic, without any change in the proofs). The facts (1)-(3) imply that $D_{\tilde{v}_i}^{\times}/(1 + \mathfrak{P}_{\tilde{v}_i}(\alpha_i))$ is solvable for all i, and the solvability of H follows. For the second assertion, we notice that according to the remarks preceeding the lemma, the pullback of the $\mathcal{A}$-adic topology via $\delta\colon G(K) \to G_{\mathcal{A}}$ coincides with the topology on $G(K) = SL(1, D)$ induced by the $\tilde{T}_0$-adic topology on D, where $\tilde{T}_0$ consists of the extensions of valuations in T_0 to D. In other words, if $\tilde{T}_0 = \{\tilde{v}_1, \dots, \tilde{v}_r\}$ then for any open normal subgroup $W \subset G_{\mathcal{A}}$, there exist $\alpha_i \in (\Gamma_{\tilde{v}_i})_{\geqslant 0}$ such that $\delta^{-1}(W) \supset G(K) \cap 1 + \mathfrak{m}(\alpha_1, \dots, \alpha_r)$, so the second assertion of the lemma follows from the first.

In the sequel, we will refer to the pullback of the $\mathcal{A}$-adic topology via $\delta\colon G(K) \to G_{\mathcal{A}}$ as the $\mathcal{A}$-adic topology on $G(K)$, and the bar will be used to denote the closure with respect to this topology. Thus, (MP) states that every noncentral normal subgroup $H \subset G(K)$ is $\mathcal{A}$-adically open. We will be using the fact, due to Margulis [12] and Prasad [14], that any noncentral normal subgroup $H \subset G(K)$ has finite index; in particular, such H is $\mathcal{A}$-adically open iff it is $\mathcal{A}$-adically closed. Now, if (MP) fails, there exists a noncentral normal subgroup $H \subset G(K)$ such that $\bar{H} \neq H$. Since the congruence subgroups with respect to $\tilde{T}_0$ are normal in $D^{\times}$, there exists an $\mathcal{A}$-adically open subgroup $W \subset \bar{H}$ normalized by $D^{\times}$. Then $W = \overline{W \cap H}$ and $\bar{H} = HW$ so that $W/(W \cap H) \simeq \bar{H}/H$ is nontrivial. Thus, replacing H with $W \cap H$, we may assume that $\bar{H} \lhd D^{\times}$. Pick a subgroup $B \subset \bar{H}$ containing H such that $B \lhd \bar{H}$ and $S := \bar{H}/B$ is a (finite) simple group $\neq \{1\}$. Then $\bar{B} = \bar{H}$. It is known (cf. [15], and also [13], Theorem 9.3, for characteristic zero) that $[\bar{H}, \bar{H}]$ is $\mathcal{A}$-adically open, so the inclusion $[\bar{H}, \bar{H}] \subset B$ is impossible, and therefore S is nonabelian. We claim that $B \lhd D^{\times}$. Indeed, let $m = [G(K) : H]$, and let M be the subgroup generated by x^m for all $x \in G(K)$. Then M is an infinite normal subgroup of $D^{\times}$ contained in H; in particular, $[G(K) : M] < \infty$.

Now, let $R = \cap_{g \in D^\times} g^{-1}Bg$. Clearly, $R \lhd D^\times$ and $\bar{H} \supset R \supset M$, implying that $[G(K) : R] < \infty$. The quotient $\bar{H}/R$, being a product of copies of S, is a perfect group. On the other hand, according to Lemma 1, the quotient $\bar{H}/\bar{R}$ must be solvable. Thus, $\bar{R} = \bar{H}$. It follows from [15], Proposition 3 (cf. also [13], Proposition 9.3) that for any $x \in \bar{R}/R$ one has $D^\times/R = (\bar{R}/R)C(x)$ where $C(x)$ is the centralizer of x in $D^\times/R$. In particular, any normal subgroup of $\bar{R}/R$ is normal in $D^\times/R$, implying that $B \lhd D^\times$. The action of $D^\times$ on $S = \bar{H}/B$ by conjugation induces a homomorphism $\alpha \colon D^\times \to \mathrm{Aut}\, S$; notice that $\mathrm{Im}\, \alpha \supset \mathrm{Inn}\, S$. Set $N = \mathrm{Ker}\, \alpha$. Then by construction $F := D^\times/N$ satisfies $\mathrm{Inn}\, S \subseteq F \subseteq \mathrm{Aut}\, S$, as required. The proof of the proposition is complete.

We will need one corollary of Proposition 1, the proof of which uses the well-known consequences of the classification of finite simple groups that every such group is 2-generated. In fact, it is the only place in the paper where the classification is used, so the rest of the paper (including the proof of Theorem 1) is classification-independent.

Corollary 1. *Notations as in Proposition 1, if (MP) fails for $G(K)$ then $D^\times$ has a nonsolvable quotient $F = D^\times/N$ such that the commuting graph Δ_F has diameter $\geqslant 3$.*

Indeed, it is enough to show that for any group F satisfying $\mathrm{Inn}\, S \subseteq F \subseteq \mathrm{Aut}\, S$, where S is a nonabelian finite simple group, one has $\mathrm{diam}\, \Delta_F \geqslant 3$. It follows from the classification of finite simple groups that S is always generated by two elements (the book [10] cites the paper [2] as the primary source for this result; we notice that in [9], Proposition 2.2, a much stronger statement was derived from [11], viz. that every finite simple group can be generated by two elements one of which is an involution). So, suppose $S = \langle a, b \rangle$, and let i_a and i_b be the corresponding inner automorphisms. We claim that the distance between i_a and i_b in Δ_F is $\geqslant 3$. Indeed, otherwise there would be a nontrivial automorphism $\sigma \in F \subset \mathrm{Aut}\, S$ that commutes with both i_a and i_b. Then $\sigma(a) = a$ and $\sigma(b) = b$, implying that $\sigma = \mathrm{id}_S$ as a and b generate S, a contradiction.

We remark that all we need from the classification is that every nonabelian finite simple group S contains two elements a, b satisfying the following property:

$$\text{if } \sigma \in \mathrm{Aut}\ S \text{ is such that } \sigma(a) = a \text{ and } \sigma(b) = b \text{ then } \sigma = \mathrm{id}_S$$

In many situations, such elements are much easier to construct than two generating elements. For example, in the groups of Lie type over sufficiently large fields, properly chosen regular elements in two opposite maximal unipotent subgroups will work. We will not, however, elaborate on this.

Now, to derive (MP) from Theorem 1, let us assume that (MP) fails. Then by the above corollary there exists a finite nonsolvable quotient $F = D^\times/N$ such that the commuting graph Δ_F has diameter $\geqslant 3$. On the other hand, by Theorem 1, N is $\tilde{T}$-adically open for some finite $\tilde{T}$, and then by Lemma 1 the quotient $D^\times/N$ is solvable. A contradiction.

3. Proof of Theorem 1: results over general fields

In this section, D denotes a finite dimensional division algebra over an *arbitrary* field K. Our goal is to extend some results proven in [17] and [18] for a single valuation to the case of several valuations. Thus, the main result (see Theorem 2 below) describes some conditions under which a normal subgroup of finite index $N \subset D^{\times}$ is $\tilde{T}$-adically open with respect to a finite set $\tilde{T}$ of valuations of D.

We begin by recalling (cf. [18], Propositions 5.2 and 5.3) that since the diameter of the commuting graph of $D^{\times}/N$ is $\geqslant 3$, there exists a (surjective) strongly leveled map $\varphi\colon N \to \Gamma$ to a partially ordered group Γ having an s-level $\alpha \in \Gamma_{\geqslant 0}$, i.e.

$$1 \pm N_{>\alpha} \subseteq N_{\leqslant 0},$$

and in addition $N_{\geqslant 0} \not\subset K$ (where $N_{>\alpha} = \{x \in N | \varphi(x) > \alpha\}$ etc). As in [18], we let $\mathcal{R}$ denote the subring of D generated by $N_{\geqslant 0}$. An important property of $\mathcal{R}$ is that $\mathcal{R} \cap N \subset N_{\geqslant -\beta}$ for some $\beta \in \Gamma_{\geqslant 0}$ (Theorem 5.8(3) in [18]).

Theorem 2. *Let $N \subset D^{\times}$ be a normal subgroup of finite index such that* diam $\Delta_{D^{\times}/N} \geqslant 3$, $\varphi\colon N \to \Gamma$ *be the s-leveled map constructed in* [18], *and $\mathcal{R}$ be the subring of D generated by $N_{\geqslant 0}$. Assume that there exists a finite set T of height one valuations of K such that $\mathcal{R} \cap K \subset \mathcal{O}_{K,v}$ for all $v \in T$ and that $\mathcal{R} \cap K$ is open in K in the T-adic topology. Then*

(1) *each $v \in T$ uniquely extends to a valuation $\tilde{v}$ of D such that $\mathcal{R} \subset \mathcal{O}_{D,\tilde{v}}$;*
(2) *N is open in $D^{\times}$ with respect to the $\tilde{T}$-adic topology where $\tilde{T} = \{\tilde{v} |\ v \in T\}$.*

The proof of Theorem 2 is organized as follows. First, we extend the T-adic topology on K to a topology on D and prove that $\mathcal{R}$ is open in D with respect to this topology. The latter fact is crucial for proving part (1) of Theorem 2 (cf. Proposition 2). We then use the above-mentioned result from [18] that $\mathcal{R} \cap N \subset N_{-\beta}$ for some $\beta \in \Gamma_{\geqslant 0}$ to prove part (2) of Theorem 2 (cf. Proposition 3).

Beginning to implement this program, we fix a basis $\omega_1, \dots \omega_{n^2}$ of D over K. Given a height one valuation v of K, we let $|\ |_v$ denote the corresponding absolute value. Then

$$||a_1\omega_1 + \cdots + a_{n^2}\omega_{n^2}||_v = \max_{\overline{i=1,n^2}} |a_i|_v \tag{1}$$

defines a norm of D which makes it into a normed vector space over $(K, |\ |_v)$. One easily verifies that the topology τ_v and the notion of boundedness on D associated with $||\ ||_v$ do not depend on the choice of a basis (the topology τ_v sometimes will be refered to as the v-adic topology). Let $\delta\colon D \to \prod_{v \in T}(D, \tau_v)$ be the diagonal embedding. The pullback of the direct product topology will be called the T-adic topology (on D) and denoted τ_T. Clearly, the presentation $D = K\omega_1 + \cdots + K\omega_{n^2}$ sets up a homeomorphism between (D, τ_T) and the direct product of n^2 copies of K endowed with the T-adic topology.

Assertion (1) of Theorem 2 is established in the following.

Proposition 2. *Let $T = \{v_1, \dots, v_r\}$ be a finite set of height one valuations of K satisfying the following two conditions*

(i) $\mathcal{R} \cap K \subset \cap_{v \in T} \mathcal{O}_{K,v}$;

(ii) *$\mathcal{R} \cap K$ is open in K with respect to the T-adic topology.*

Then each valuation $v \in T$ uniquely extends to a valuation $\tilde{v}$ of D such that $\mathcal{R} \subset \mathcal{O}_{D,\tilde{v}}$, and $\mathcal{R}$ is open in D with respect to the $\tilde{T}$-adic topology where $\tilde{T} = \{\tilde{v} \mid v \in T\}$.

Proof. Since $\mathcal{R} \not\subset K$, one can pick a basis $\omega_1 = 1, \omega_2, \dots, \omega_{n^2}$ of D over K which is contained in $\mathcal{R}$ (cf. Proposition 2.5.2 in [18]). Then

$$(\mathcal{R} \cap K)\omega_1 + \cdots + (\mathcal{R} \cap K)\omega_{n^2} \subset \mathcal{R},$$

so it follows from (ii) and the remarks preceding the statement of the proposition that $\mathcal{R}$ is open with respect to the T-adic topology τ_T on D.

The norm (1) obviously extends to $D_v = D \otimes_K K_v$. At the same time, D_v has a different norm. Namely, we have $D_v = M_{n_v}(\mathcal{D}_v)$ for some central division algebra $\mathcal{D}_v$ over K_v and some integer $n_v \geqslant 1$. Then the valuation v extends to a valuation $\check{v}$ of $\mathcal{D}_v$, and

$$||(a_{ij})||_{\check{v}} = \max_{i,j=\overline{1,n_v}} |a_{ij}|_{\check{v}}, \tag{2}$$

where $|\ |_{\check{v}}$ is the absolute value associated with $\check{v}$, defines a norm on D_v as a vector space over K_v. Since $\dim_{K_v} D_v < \infty$, the norms $||\ ||_v$ and $||\ ||_{\check{v}}$ are equivalent, and therefore give rise to the same topology and the same notion of boundedness. Let $D_T = \prod_{v \in T} D_v$ be endowed with the topology of direct product, and for a subset $S \subset T$, let $\mathrm{pr}_S \colon D_T \to D_S$ be the corresponding projection. We need the following generalization of Lemma 5.3 in [17].

Lemma 2. *Let $\mathcal{B} \subset D_T$ be an open subring. If $v_0 \in T$ is such that $\mathrm{pr}_{\{v_0\}}(\mathcal{B})$ is unbounded then $\mathcal{B} = \mathrm{pr}_{T-\{v_0\}}(\mathcal{B}) \oplus M_{n_{v_0}}(\mathcal{D}_{v_0})$.*

Proof. The fact that $\mathcal{B}$ is open means that

$$\mathcal{B} \supset \prod_{v \in T} M_{n_v}(\mathfrak{a}_{\check{v}}(\delta_{\check{v}})) \tag{3}$$

for some nonnegative $\delta_{\check{v}}$ in the value group of $\check{v}$, where

$$\mathfrak{a}_{\check{v}}(\delta_{\check{v}}) = \{x \in \mathcal{D}_v^{\times} \mid \check{v}(x) > \delta_{\check{v}}\} \cup \{0\}.$$

As $\mathrm{pr}_{\{v_0\}}(\mathcal{B}) \subset M_{n_{v_0}}(\mathcal{D}_{v_0})$ is open and unbounded, by Lemma 5.3 in [17], $\mathrm{pr}_{\{v_0\}}(\mathcal{B}) = M_{n_{v_0}}(\mathcal{D}_{v_0})$. It follows from (3) that $\mathcal{B}$ contains an element $a = (a_v)$ such that $a_v = 0$ for all $v \neq v_0$, and a_{v_0} is invertible in $M_{n_{v_0}}(\mathcal{D}_{v_0})$. Then

$$a\mathcal{B} \subset \{0\} \oplus \cdots \oplus M_{n_{v_0}}(\mathcal{D}_{v_0}) \oplus \cdots \oplus \{0\}$$

and $\mathrm{pr}_{\{v_0\}}(a\mathcal{B}) = a_{v_0} M_{n_{v_0}}(\mathcal{D}_{v_0}) = M_{n_{v_0}}(\mathcal{D}_{v_0})$. This implies that

$$\mathcal{B} \supset a\mathcal{B} = \{0\} \oplus \cdots \oplus M_{n_{v_0}}(\mathcal{D}_{v_0}) \oplus \cdots \oplus \{0\},$$

immediately yielding the lemma.

Continuing the proof of Proposition 2, we consider the embedding $D \to D_T$, and will use the bar to denote the closure in D_T. Since $\mathcal{R}$ is T-adically open in D, we have

$$\overline{\mathcal{R}} \cap D = \mathcal{R}. \tag{4}$$

We claim that $\mathrm{pr}_{\{v\}}(\overline{\mathcal{R}})$ is bounded for all $v \in T$. Indeed, suppose $\mathrm{pr}_{v_{i_0}}(\overline{\mathcal{R}})$ is unbounded. Then by Lemma 2,

$$\overline{\mathcal{R}} = \mathrm{pr}_{T-\{v_{i_0}\}}(\overline{\mathcal{R}}) \oplus M_{n_{v_{i_0}}}(\mathcal{D}_{v_{i_0}}). \tag{5}$$

The fact that the subring $\mathcal{R} \cap K$ is open in K means that it contains a subset of the form

$$\mathfrak{a}(\delta_1, \dots, \delta_r) = \{x \in K^\times \mid v_i(x) > \delta_i \text{ for all } i = 1, \dots, r\} \cup \{0\}$$

for some positive δ_i in the value group of v_i. By the theorem on weak approximation (cf., for example, [1], Ch. II, Lemma 6.1), there exists $a \in K^\times$ such that

$$v_i(a) > \delta_i \text{ for all } i \neq i_0 \text{ and } v_{i_0}(a) < 0.$$

Again, it follows from the theorem on weak approximation that

$$(a, \dots, a, 0) \in \overline{\mathfrak{a}(\delta_1, \dots, \delta_r)},$$

implying that $(a, \dots, a) \in \mathrm{pr}_{T-\{v_{i_0}\}}(\overline{\mathcal{R}})$. So, we conclude from (5) that $(a, \dots, a) \in \overline{\mathcal{R}}$. In conjunction with (4), this gives $a \in \mathcal{R} \cap K$. However, since $a \notin \mathcal{O}_{v_{i_0}}$, this contradicts condition (i). This shows that for any $v \in T$, the subring $\mathcal{R}(v) := \mathrm{pr}_v(\overline{\mathcal{R}}) \cap D$ is open in D with respect to the topology τ_v and is bounded with respect to the norm $\|\ \|_v$. Furthermore, being generated by $N_{\geqslant 0}$, the subring $\mathcal{R}$ is invariant under conjugation by any element of N, so the same is true for $\overline{\mathcal{R}}$, and therefore also for $\mathcal{R}(v)$. It follows that $\mathcal{R}(v)$ satisfies both requirements of Theorem 2.4 in [18], and by that theorem, v uniquely extends to a valuation $\tilde{v}$ of D such that $\mathcal{R} \subset \mathcal{O}_{D,\tilde{v}}$. Finally, we observe that the completion of D with respect to $\tilde{v}$ can be identified with D_v. Since $\dim_{K_v} D_v < \infty$, the topologies on D_v defined by $\|\ \|_v$ and by (the absolute value associated with) $\tilde{v}$ coincide. It follows that the T-adic and $\tilde{T}$-adic topologies on D coincide, and therefore $\mathcal{R}$ is $\tilde{T}$-adically open.

We will derive assertion (2) of Theorem 2 from Proposition 3 below which we will formulate in a slightly more general setting. Let $N \subset D^\times$ be a subgroup of finite index, and $\varphi \colon N \to \Gamma$ be a leveled map to a partially ordered group Γ, i.e. there exists $\alpha \in \Gamma_{\geqslant 0}$ such that

$$N_{<-\alpha} + 1 \subset N_{<-\alpha} \tag{6}$$

Let $\tilde{T} = \{\tilde{v}_1, \dots, \tilde{v}_r\}$ be a finite set of valuations of D, $\tilde{v}_i \colon D^\times \to \tilde{\Gamma}_{\tilde{v}_i}$, such that each v_i is *associated* with φ. This means that there exists a homomorphism $\theta_i \colon \Gamma \to \tilde{\Gamma}_{\tilde{v}_i}$ of ordered groups such that the diagram

$$\begin{tikzcd} N \arrow[r, "\varphi"] \arrow[d, "\iota"'] & \Gamma \arrow[d, "\theta_i"] \\ D^\times \arrow[r, "\tilde{v}_i"] & \tilde{\Gamma}_{\tilde{v}_i} \end{tikzcd}$$

in which ι is the natural embedding, commutes. The following statement generalizes Proposition 3.2 in [18] to the case of several valuations.

Proposition 3. *Let $\tilde{T} = \{\tilde{v}_1, \dots, \tilde{v}_r\}$ be a finite set of valuations of D such that each $\tilde{v}_i$ is associated with the given leveled map $\varphi\colon N \to \Gamma$. Suppose there exist a $\tilde{T}$-adically open subring $\mathcal{M} \subset D$ and an element $\beta \in \Gamma_{\geqslant 0}$ such that*

$$\mathcal{M} \cap N \subset N_{>-\beta}. \tag{7}$$

Then N is $\tilde{T}$-adically open in $D^\times$.

Proof. We need to show that there exist $\delta_i \in (\tilde{\Gamma}_{\tilde{v}_i})_{\geqslant 0}$ such that

$$1 + \mathfrak{m}(\delta_1, \dots, \delta_r) \subset N, \tag{8}$$

where $\mathfrak{m}(\delta_1, \dots, \delta_r) = \{x \in D^\times | \tilde{v}_i(x) > \delta_i \text{ for all } i = 1, \dots, r\} \cup \{0\}$. To this end, we will show that for each coset Na of N in $D^\times$, there exists $0 \leqslant \gamma_i = \gamma_i(Na) \in \tilde{\Gamma}_{\tilde{v}_i}$ for each $i = 1, \dots, r$ such that

$$1 + (Na \cap \mathfrak{m}(\gamma_1, \dots, \gamma_r)) \subset N. \tag{9}$$

Then, since N has finite index in $D^\times$ and $\tilde{\Gamma}_{\tilde{v}_i}$ is totally ordered, the maximum $\delta_i := \max \gamma_i(Na)$, taken over all cosets of N in $D^\times$, exists for each $i = 1, \dots, r$, and the elements $\delta_1, \dots \delta_r$ obviously satisfy (8).

Since $\mathcal{M}$ is open in $\mathcal{O}_{D,\tilde{T}} = \cap_{\tilde{v} \in \tilde{T}} \mathcal{O}_{D,\tilde{v}}$, there exist $\lambda_i \in (\tilde{\Gamma}_{\tilde{v}_i})_{\geqslant 0}$ for $i = 1, \dots, r$ such that $\mathfrak{m}(\lambda_1, \dots, \lambda_r) \subset \mathcal{M}$, and then it follows from (7) that

$$\mathfrak{m}(\lambda_1, \dots, \lambda_r) \cap N \subset N_{>-\beta}. \tag{10}$$

Lemma 3. (1) *For $m, n \in N$ such that $\tilde{v}_i(m) < \tilde{v}_i(n) - \theta_i(\alpha + \beta) - \lambda_i$ for all $i = 1, \dots, r$, the element $c = m + n$ belongs to N.*

(2) *For any $d \in D^\times$, there exist $\beta_i(d) \in \tilde{\Gamma}_{\tilde{v}_i}$, $i = 1, \dots, r$, such that*

$$d + \{n \in N \mid \tilde{v}_i(n) < \beta_i(d) \text{ for all } i = 1, \dots, r\} \subset N.$$

Proof. (1) Pick $a, b \in N$ so that $\varphi(a) = \alpha$ and $\varphi(b) = \beta$. We have $\tilde{v}_i(m^{-1}na^{-1}b^{-1}) > \lambda_i$ for all $i = 1, \dots, r$ (recall that the $\tilde{\Gamma}_{\tilde{v}_i}$'s are commutative), i.e. $m^{-1}na^{-1}b^{-1} \in \mathfrak{m}(\lambda_1, \dots, \lambda_r)$. It follows from (10) that $\varphi(m^{-1}na^{-1}b^{-1}) > -\beta$, and therefore $\varphi(m^{-1}na^{-1}) > 0$. Thus, $\varphi(n^{-1}m) < -\alpha$, i.e. $n^{-1}m \in N_{<-\alpha}$. Now,

$$n^{-1}m + 1 \in N_{<-\alpha} + 1 \subset N_{<-\alpha} \subset N,$$

yielding $c = n(n^{-1}m + 1) \in N$.

(2) Since D is infinite, $D = N - N$ (cf. [3] , [24]), so there exists $s \in N$ such that $d + s \in N$. Set

$$\beta_i(d) = \min(\tilde{v}_i(s), \tilde{v}_i(d + s)) - \theta_i(\alpha + \beta) - \lambda_i.$$

Suppose now that $t \in N$ satisfies $\tilde{v}_i(t) < \beta_i(d)$ for all $i = 1, \dots, r$. Then, in particular, $\tilde{v}_i(t) < \tilde{v}_i(s) - \theta_i(\alpha + \beta) - \lambda_i$ for all $i = 1, \dots, r$, so it follows from

(1) that $t - s \in N$ (observe that $\tilde{v}_i(-s) = \tilde{v}_i(s)$). Moreover, since $\alpha, \beta \in \Gamma_{\geqslant 0}$ and $\lambda_i \in (\tilde{\Gamma}_{\tilde{v}_i})_{\geqslant 0}$, we have $\tilde{v}_i(t) < \tilde{v}_i(s)$, and therefore $\tilde{v}_i(t - s) = \tilde{v}_i(t)$ as $\tilde{v}_i$ is a valuation. Thus, $\tilde{v}_i(t - s) < \tilde{v}_i(d + s) - \theta_i(\alpha + \beta) - \lambda_i$ for all $i = 1, \ldots, r$, and therefore

$$d + t = (d + s) + (t - s) \in N$$

according to (1). The proof of the lemma is complete.

Now, fix a representative a of a given coset Na and let

$$\gamma_i = \gamma_i(Na) := |\tilde{v}_i(a)| + |\beta_i(a)|,$$

where $\beta_i(a)$ is as in Lemma 3(2) (here, as usual, for $\gamma \in \tilde{\Gamma}_{\tilde{v}_i}$, we let $|\gamma| = \max\{\gamma, -\gamma\}$), for $i = 1, \ldots, r$. Suppose $na \in Na \cap \mathfrak{m}(\gamma_1, \ldots, \gamma_r)$. Then for any $i = 1, \ldots, r$ one has

$$\tilde{v}_i(n) = \tilde{v}_i(na) - \tilde{v}_i(a) > (|\tilde{v}_i(a)| + |\beta_i(a)|) - \tilde{v}_i(a) \geqslant |\beta_i(a)|,$$

implying that

$$1 + na = n(n^{-1} + a) \in N$$

as $\tilde{v}_i(n) < -|\beta_i(a)| \leqslant \beta_i(a)$ for all $i = 1, \ldots, r$, and therefore by Lemma 3(2), $n^{-1} + a \in N$. It follows that $1 + na \in N$, proving (9) and completing the proof of Proposition 3.

Now, to prove assertion (2) of Theorem 2, we observe that: (A) since φ constructed in [18] is s-leveled, it is also leveled, i.e. (6) holds (cf. [18], §4); (B) if $\tilde{T}$ is as in Theorem 2, then each $\tilde{v} \in \tilde{T}$ is associated with φ because $N_{\geqslant 0} \subset \mathcal{R} \subset \mathcal{O}_{D,\tilde{v}}$. Since $\mathcal{R}$ is $\tilde{T}$-adically open in D (cf. Proposition 2) and satisfies (7) by Theorem 5.8(3) in [18], Proposition 3 yields assertion (2) of Theorem 2.

4. Proof of Theorem 1: specialization to the case of a global field

For a global field P, we let V^P denote the set of all (nonarchimedean) valuations of P. In view of Theorem 2, to complete the proof of Theorem 1, it remains to establish the following.

Theorem 3. *Suppose K is a global field. Then in the above notations there exists a finite subset $T \subset V^K$ such that $\mathcal{R} \cap K$ is contained in the valuation ring $\mathcal{O}_{K,v}$ for all $v \in T$ and is open in K in the T-adic topology.*

A first important step in the proof is the following (probably, known) statement.

Proposition 4. *Let L be a global field, $R \subset L$ be a subring containing the identity and such that $L = R\left[\frac{1}{t}\right]$ for some nonzero $t \in R$. Set*

$$T = \{\, v \in V^L \mid R \subset \mathcal{O}_{L,v} \,\}.$$

Then T is finite and R is T-adically open in L.

Proof. Clearly, if $R \subset \mathcal{O}_{L,v}$ and $v(t) = 0$, then $L = R[t^{-1}] \subset \mathcal{O}_{L,v}$, which is impossible. This shows that T is contained in $V(t) := \{v \in V^L \mid v(t) \neq 0\}$. However, it is well-known that $V(t)$ is finite ([1], Ch. II, Thm. 12.1), and the finiteness of T follows. The openness of R with respect to the T-adic topology requires a bit more work.

First, we observe that it is enough to show that R is open in L with respect to the T'-adic topology for some finite subset $T' \subset V^L$ containing T. Indeed, given this, we have

$$R = \overline{R} \cap L, \tag{1}$$

where $\overline{R}$ is the closure of R in $L_{T'} = \prod_{v \in T'} L_v$. Consider now an arbitrary $v \in T' - T$. As $R \not\subset \mathcal{O}_{L,v}$, R is unbounded with respect to v. Applying Lemma 2 repeatedly to $D = L$, we conclude that

$$\overline{R} = \mathrm{pr}_T(\overline{R}) \oplus L_{T'-T}.$$

Comparing with (1), we obtain that $R = \mathrm{pr}_T(\overline{R}) \cap L$, and since $\mathrm{pr}_T(\overline{R})$ is open in L_T, the openness of R in L with respect to the T-adic topology follows.

To continue the argument, we need two lemmas.

Lemma 4. (well-known) *Let k be either the field of rational numbers $\mathbb{Q}$ or the field of rational functions $\mathbf{F}_q(t)$ in one variable over the field $\mathbf{F}_q$ with q elements, and $A \subset k$ be a subring containing respectively $\mathbb{Z}$ or $\mathbf{F}_q[t]$. Set*

$$S = \{\ v \in V^k \mid A \subset \mathcal{O}_{k,v}\ \}.$$

Then A coincides with $\mathcal{O}_k(S) = \bigcap_{v \in S} \mathcal{O}_{k,v}$. In addition if there exists $a \in A$ such that $k = A\left[\frac{1}{a}\right]$ then S is finite.

Proof. First, we recall that if E is a PID with the field of fractions $\mathcal{E}$ then any subring $A \subset \mathcal{E}$ containing E coincides with the localization E_U with respect to some multiplicative subset $U \subset E$. Indeed, set $U = \{u \in E | u^{-1} \in A\}$; then $E_U \subset A$. On the other hand, suppose $\alpha \in A$ and $\alpha = \frac{a}{b}$ where $a, b \in E$ are relatively prime. There exist $x, y \in E$ such that $xa + yb = 1$, and then $\frac{1}{b} = x\alpha + y \in A$. So, $b \in U$ and $\alpha \in E_U$. Applying this fact in our situation, we obtain that S consists of valuations corresponding to those prime elements of $E = \mathbb{Z}$ or $\mathbf{F}_q[t]$ that do not occur in the elements of U. Clearly, the ring $\mathcal{O}_k(S)$ coincides with the localization $E_U = A$, as claimed. The finiteness of S, if $k = A\left[\frac{1}{a}\right]$, has already been established in the beginning of the proof of Proposition 4.

Notation. For a field extension ℓ/k and a set of valuations S of k we will write $\tilde{S}|S$ to indicate that $\tilde{S}$ consists of *all* extensions of valuations in S to ℓ.

Lemma 5. *Let ℓ/k be a finite field extension, S be a finite set of height one valuations of k, and $\tilde{S}|S$. Set*

$$\mathcal{O}_k(S) = \bigcap_{v \in S} \mathcal{O}_{k,v} \quad \text{and} \quad \mathcal{O}_\ell(\tilde{S}) = \bigcap_{w \in \tilde{S}} \mathcal{O}_{\ell,w},$$

and suppose that $\mathcal{O}_\ell(\tilde{S})$ is finitely generated as $\mathcal{O}_k(S)$-module. Let $R \subset \ell$ be a subring such that $\ell = R\left[\dfrac{1}{t}\right]$ for some nonzero $t \in R$. It $R \cap k$ is S-adically open in k then R is $\tilde{S}$-adically open in ℓ.

Proof. Suppose $S = \{v_1, \dots, v_l\}$, $\tilde{S} = \{w_1, \dots, w_m\}$, and $a_1, \dots, a_r$ generate $\mathcal{O}_\ell(\tilde{S})$ as $\mathcal{O}_k(S)$-module. Since $\ell = R\left[\dfrac{1}{t}\right]$, for each $j = 1, \dots, r$ there exists $i_j \geqslant 0$ such that $t^{i_j} a_j \in R$. Then for $i := \max_{j=1,\dots,r} i_j$ one has $t^i a_j \in R$ for all $j = 1, \dots, r$. Furthermore, being S-adically open, the ring $R \cap k$ contains

$$\mathfrak{m}_{k,S}(\alpha_1, \dots, \alpha_l) = \{x \in k^\times \mid v_i(x) > \alpha_i \ \text{ for all } i = 1, \dots, l\} \cup \{0\}$$

for some $\alpha_i \in (\Gamma_{v_i})_{\geqslant 0}$. By the weak approximation theorem, $\mathfrak{m}_{k,S}(\alpha_1, \dots, \alpha_l)$ contains a nonzero element, say u. Then

$$\begin{aligned} ut^i \mathcal{O}_\ell(\tilde{S}) &= ut^i(\mathcal{O}_k(S)a_1 + \dots + \mathcal{O}_k(S)a_r) \\ &= (u\mathcal{O}_k(S))(t^i a_1) + \dots + (u\mathcal{O}_k(S))(t^i a_r) \subset R. \end{aligned} \tag{2}$$

Set $\beta_j = \max(0, w_j(ut^i))$ for $j = 1, \dots, m$. Then, using (2), we obtain that

$$\mathfrak{m}_{\ell,\tilde{S}}(\beta_1, \dots, \beta_m) = \{x \in \ell \mid w_j(x) > \beta_j \ \text{ for all } \ j = 1, \dots, m\ \}$$

is contained in $ut^i \mathcal{O}_\ell(\tilde{S}) \subset R$, proving the openness of R in the $\tilde{S}$-adic topology.

Remark. In most cases, the assumptions of Lemma 5 can be verified using the following well-known fact: If ℓ/k is a finite separable extension and $\mathcal{O}_k(S)$ is noetherian then $\mathcal{O}_\ell(\tilde{S})$ is a finitely generated $\mathcal{O}_k(S)$-module. For the sake of completeness, we briefly indicate the proof. It follows from ([4], ch. VI, §7, n° 1, cor. 3) that if v is a valuation of k such that $\mathcal{O}_k(S) \subset \mathcal{O}_{k,v}$ then $v \in S$. So, we conclude, using ([4], ch. VI, §1, n° 3, thm. 3), that $\mathcal{O}_\ell(\tilde{S})$ is the integral closure of $\mathcal{O}_k(S)$ in ℓ. Since $\mathcal{O}_k(S)$ is integrally closed, our claim follows from ([4], ch. V, §1, n° 7, prop. 18).

To complete the proof of Proposition 4, we now consider the cases of characteristic zero and positive characteristic separately.

Case 1. char $L = 0$. We have $L = R\left[\dfrac{1}{t}\right]$, where $t \in R$, and $R \supset \mathbb{Z}$. First, without loss of generality we may assume that $t \in \mathbb{Z}$. Indeed, replacing t with ct, where $c \in \mathbb{Z}$, we reduce to the case where t is an algebraic integer, so we have an equation

$$t^n + a_{n-1}t^{n-1} + \dots + a_0 = 0$$

with $a_i \in \mathbb{Z}$, $a_0 \neq 0$. Then

$$\frac{1}{t} = -\frac{1}{a_0}\left(t^{n-1} + a_{n-1}t^{n-2} + \cdots + a_1\right) \in R\left[\frac{1}{a_0}\right],$$

and therefore $R\left[\frac{1}{a_0}\right] = L$. So, assume from now on that $t \in \mathbb{Z}$. Then $\mathbb{Q} = (R \cap \mathbb{Q})\left[\frac{1}{t}\right]$. Set

$$S = \{v \in V^{\mathbb{Q}} \mid R \cap \mathbb{Q} \subset \mathcal{O}_{\mathbb{Q},v}\},$$

and let $\tilde{S}|S$ be the corresponding set of valuations of L. Obviously, $\tilde{S} \supset T$ as $R \subset \mathcal{O}_{L,v}$ implies $R \cap \mathbb{Q} \subset \mathcal{O}_{\mathbb{Q},v|\mathbb{Q}}$, and therefore $v|\mathbb{Q} \in S$. By Lemma 4, S is finite and $R \cap \mathbb{Q} = \mathcal{O}_{\mathbb{Q}}(S)$, in particular, $R \cap \mathbb{Q}$ is S-adically open. According to the above remark, $\mathcal{O}_L(\tilde{S})$ is a finitely generated $\mathcal{O}_{\mathbb{Q}}(S)$-module, so by Lemma 5, R is $\tilde{S}$-adically open in L. Then the openness of R with respect to the T-adic topology follows from the argument given in the beginning of the proof of Proposition 4.

Case 2. char $L = p > 0$. We have $\mathbf{F}_p[t] \subset R$, and we may assume that t is transcendental over $\mathbf{F}_p$. Consider $k = \mathbf{F}_p(t)$, noticing that L/k is a finite extension, although not necessarily separable. Let

$$S = \{\ v \in V^k \ \mid\ R \cap k \subset \mathcal{O}_{k,v}\ \}.$$

As in Case 1, S is finite (since $k = (R \cap k)\left[\frac{1}{t}\right]$) and the set $\tilde{S}$ of valuations of L such that $\tilde{S}|S$ satisfies $\tilde{S} \supset T$, so it is enough to prove that R is $\tilde{S}$-adically open. But this again follows from Lemmas 4 and 5 exactly as in Case 1 if one can prove that $\mathcal{O}_L(\tilde{S})$ is a finitely generated $\mathcal{O}_k(S)$-module. If L/k is separable, this immediately follows from the remark made after Lemma 5, but in the general case one more step is needed. Let n be the largest integer for which $t^{1/p^n} \in L$; then L is separable over $F := \mathbf{F}_p(t^{1/p^n})$ (cf., for example, [8], Thm. 5.1.2). Let S_1 be the set of places of F such that $S_1|S$. Then $\tilde{S}|S_1$ and $\mathcal{O}_L(\tilde{S})$ is a finitely generated $\mathcal{O}_F(S_1)$-module, so it is enough to establish that $\mathcal{O}_F(S_1)$ is a finitely generated $\mathcal{O}_k(S)$-module. We claim that

$$\mathcal{O}_F(S_1) = \mathcal{O}_k(S)\left[t^{1/p^n}\right], \tag{3}$$

and the required fact will follow. Given $\alpha \in \mathcal{O}_F(S_1)$, we have $\alpha^{p^n} \in \mathcal{O}_k(S)$, and therefore $\alpha^{p^n} = \frac{f(t)}{g(t)}$ where $f(t), g(t) \in \mathbf{F}_p[t]$ and $\frac{1}{g(t)} \in \mathcal{O}_k(S)$. Then $\alpha^{p^n} = \frac{h(t)}{g(t)^{p^n}}$, where $h(t) = f(t)g(t)^{p^n-1}$ and

$$\alpha = \frac{h(t^{1/p^n})}{g(t)},$$

yielding (3).

The proof of Proposition 4 is now complete.

Remarks. 1. It is known that for any extension of global fields L/k and any set S of nonarchimedean valuations of k, the ring $\mathcal{O}_L(\tilde{S})$ is a finitely generated $\mathcal{O}_k(S)$-module; in other words, $\mathcal{O}_k(S)$ is "un anneau japonais" in the terminology of [6]-[7] (this follows, for example, from Corollary 7.6.6 in [7], but one can give a more straightforward argument). This fact enables one to prove Proposition 4 without singling out Cases 1 and 2, however we chose to give a self-contained elementary argument.

2. Brian Conrad indicated to us that subrings $R \subset K$ such that $K = R\left[\frac{1}{t}\right]$ for some nonzero $t \in R$ were analyzed in [6], cor. 16.3.3 ("Artin-Tate Lemma") from a different perspective, and we thank him for this information.

The rest of the proof of Theorem 3 can be divided into two parts: we first reduce our task to proving the existence of a subfield $P \subset D$ with a certain special property (see Proposition 5), and then construct such a subfield P by considering the cases of characteristic zero and positive characteristic separately.

Proposition 5. *Suppose there exists an infinite subfield $P \subset D$ such that for some nonzero $t \in \mathcal{R} \cap P$ one has $P = (\mathcal{R} \cap P)\left[\frac{1}{t}\right]$. Then there exists a finite subset $T \subset V^K$ such that $\mathcal{R} \cap K$ is contained in $\mathcal{O}_{K,v}$ for all $v \in T$ and is open in K in the T-adic topology.*

Proof. Without loss of generality, we may assume that $t \in N$ (otherwise, one can replace t with $t^{[D^\times:N]}$). Then t normalizes $\mathcal{R}$, and therefore the subring $\mathcal{C} \subset D$ generated by $\mathcal{R}$ and t^{-1} has the following property

$$\text{for any } x \in \mathcal{C} \text{ there exists } d > 0 \text{ such that } t^d x \in \mathcal{R} \tag{4}$$

It follows from our assumptions that $\mathcal{C} \supset P$, so one can consider $\mathcal{C}$ as a right vector space over P. We claim that $\dim_P \mathcal{C} < \infty$. For this, it suffices to show that $\dim_P D < \infty$. Set $L = KP$. As P is infinite, the extension L/P is finite. On the other hand, since D is finite dimensional over K, is is also finite dimensional over L, and the fact that $\dim_P D < \infty$ follows. Then a standard argument shows that $\mathcal{C}$ is a division ring, so it can alternatively be described as the division subring of D generated by $\mathcal{R}$. It follows that $\mathcal{C}$ is normalized by N. Since $\mathcal{R} \not\subset K$ and $[D^\times : N] < \infty$, by [5] we obtain that $\mathcal{C} = D$.

Now, it follows from (4) that $L = (\mathcal{R} \cap L)\left[\frac{1}{t}\right]$, so by Proposition 4 there exists a finite subset $\tilde{T} \subset V^L$ such that $\mathcal{R} \cap L$ is contained in $\mathcal{O}_{L,w}$ for all $w \in \tilde{T}$ and is open in L in the $\tilde{T}$-adic topology. Then the set $T \subset V^K$ consisting of the restrictions of places in $\tilde{T}$ to K is as required.

Conclusion of the proof of Theorem 3. Now, it remains to constructed a subfield $P \subset D$ with the properties described in Proposition 5. This is done using the following.

Lemma 6. *Let P be a global field, S be a subset of V^P, nonempty if* char $P > 0$, *and $\mathcal{O}_P(S)$ be the ring of S-integers in P, i.e.*

$$\mathcal{O}_P(S) = \{x \in P^\times \mid v(x) \geqslant 0 \quad \forall v \in V^P - S\} \cup \{0\}$$

Given any nonzero element $a \in \mathcal{O}_P(S)$ of infinite order, P is generated over $\mathcal{O}_P(S)$ by a^{-1} and the elements $(a^i - 1)^{-1}$ for $i = 1, 2, \dots$.

Proof. A given $x \in P^\times$ can be written as $x = \dfrac{\alpha}{\beta}$ for some nonzero $\alpha, \beta \in \mathcal{O}_P(S)$. Since the quotient $\mathcal{O}_P(S)/\beta\mathcal{O}_P(S)$ is finite, there exist integers $i > j > 0$ such that $a^i \equiv a^j (\mathrm{mod}\ \beta\mathcal{O}_P(S))$, i.e. $a^i - a^j = \beta\gamma$ with $\gamma \in \mathcal{O}_P(S)$. Then

$$x = \frac{\alpha\gamma}{a^j(a^{i-j} - 1)},$$

and our claim follows.

The crucial fact for the rest of the argument is that

$$1 \pm N_{>\alpha} \subset \mathcal{R}^\times \tag{5}$$

(cf. [18], Proposition 4.2(1)). Pick $a \in N_{>\alpha}$, and let $P = F(a)$, where F is the prime subfield (i.e. $F = \mathbb{Q}$ in characteristic zero and $F = \mathbf{F}_p$ in characteristic $p > 0$). We claim that P satisfies the requirements of Proposition 5. The proof relies on the fact that according to (5),

$$a^i - 1 \in \mathcal{R}^\times \ \text{ for all } \ i = 1, 2, \dots \tag{6}$$

Now, we consider the cases of characteristic zero and positive characteristic separately.

<u>Case 1.</u> char $K = 0$. Let $A = \mathbb{Z}[a] \subset \mathcal{R}$. It is enough to find a nonzero $c \in \mathbb{Z}$ such that

$$A\left[\frac{1}{c}\right] = \mathcal{O}_P(S) \tag{7}$$

for some $S \subset V^P$. Indeed, then $a \in \mathcal{O}_P(S)$ and $(\mathcal{R} \cap P)\left[\dfrac{1}{c}\right]$ contains $\mathcal{O}_P(S)$ and the elements $(a^i - 1)^{-1}$ for all $i = 1, 2, \dots$. Then by Lemma 6, $(\mathcal{R} \cap P)\left[\dfrac{1}{ac}\right]$ $= (\mathcal{R} \cap P)\left[\dfrac{1}{a}, \dfrac{1}{c}\right]$ coincides with P, so $t = ac$ is a required element. To find $c \in \mathbb{Z}$ satisfying (7), we first find a nonzero $c_1 \in \mathbb{Z}$ such that the element $c_1 a$ is integral over $\mathbb{Z}$. Then the ring $\mathbb{Z}[c_1 a]$ has rank $[P : \mathbb{Q}]$ as $\mathbb{Z}$-module, and therefore the index $[\mathcal{O}_P : \mathbb{Z}[c_1 a]]$, where $\mathcal{O}_P$ is the ring of algebraic integers in P, is finite; we denote it by c_2. We claim that $c = c_1 c_2$ satisfies (7) for $S = \{v \in V^P \mid v(c) \neq 0\}$. Indeed, $a = c_1^{-1}(c_1 a) \in \mathcal{O}_P(S)$, yielding the inclusion $\subset$. Conversely, we have

$$\mathcal{O}_P \subset \frac{1}{c_2}\mathbb{Z}[c_1 a] \subset A\left[\frac{1}{c}\right],$$

so $\mathcal{O}_P\left[\frac{1}{c}\right] \subset A\left[\frac{1}{c}\right]$. On the other hand, $\mathcal{O}_P\left[\frac{1}{c}\right]$ coincides with the integral closure of $\mathbb{Z}\left[\frac{1}{c}\right]$, which is nothing but $\mathcal{O}_P(S)$ for the set S specified above.

<u>Case 2.</u> char $K = p > 0$. Clearly, a is transcendental over $F = \mathbf{F}_p$, so $\mathbf{F}_p[a]$ is a polynomial ring and $P = \mathbf{F}_p(a)$ is a field of rational functions. We notice that $\mathbf{F}_p[a]$ coincides with $\mathcal{O}_P(S)$ where $S = \{v_\infty\}$ and v_∞ is defined by $v_\infty\left(\frac{f}{g}\right) = \deg g - \deg f$. Then $\mathcal{R} \cap P$ contains $\mathcal{O}_P(S)$ and also, according to (6), the elements $(a^i - 1)^{-1}$ for all $i = 1, 2, \ldots$. So, it follows from Lemma 6 that $(\mathcal{R} \cap P)\left[\frac{1}{a}\right] = P$, hence $t = a$ is a required element.

5. Examples

We will now construct an example showing that no congruence subgroup theorem can be established for finite index normal subgroups $N \subset D^\times$ such that diam $\Delta_{D^\times/N} = 2$. So, Theorem 1 is the best possible result that can be obtained along these lines. The example below is an elaboration on the example given in [17], §4.

For simplicity, we will use the algebra $D = \left(\frac{-1, -1}{\mathbb{Q}}\right)$ of ordinary ("Hamiltonian") quaternions over $\mathbb{Q}$, however a similar construction can be implemented for algebras of any index. We have $\mathrm{Nrd}_{D/\mathbb{Q}}(D^\times) = \mathbb{Q}_+$, the group of positive rationals. It is well-known that $D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra only for $p = 2$ implying that D has only one (nonarchimedean) valuation $\tilde{v}$, which is obtained by extending the 2-adic valuation of $\mathbb{Q}$. Let

$$H = \{p_1^{\alpha_1} \cdots p_r^{\alpha_r} \mid \alpha_1 + \cdots + \alpha_r \equiv 0 (\mathrm{mod}\ 2)\}.$$

Clearly, H is a subgroup of index 2 in $\mathbb{Q}_+$, so $M := \mathrm{Nrd}_{D/\mathbb{Q}}^{-1}(H)$, where $\mathrm{Nrd}_{D/\mathbb{Q}}$ is the reduced norm, is a subgroup of index two in $D^\times$. We claim that for any subgroup $W \subset D^\times$ open with respect to the $\tilde{v}$-adic topology, one has

$$D^\times = WM \qquad (1)$$

Let $\mathcal{D} = D \otimes_{\mathbb{Q}} \mathbb{Q}_2$. Since W is $\tilde{v}$-adically open in $D^\times$, there exists an open subgroup $\mathcal{W} \subset \mathcal{D}^\times$ such that $\mathcal{W} \cap D^\times = W$. Then $\mathcal{I} := \mathrm{Nrd}_{\mathcal{D}/\mathbb{Q}_2}(\mathcal{W})$ is an open subgroup of $\mathbb{Q}_2^\times$ as it contains $(\mathcal{W} \cap \mathbb{Q}_2^\times)^2$, which is open in $\mathbb{Q}_2^\times$. Next, we claim that

$$\mathrm{Nrd}_{D/\mathbb{Q}}(W) = \mathbb{Q}_+ \cap \mathcal{I}. \qquad (2)$$

The inclusion $\subset$ here is obvious, while the opposite inclusion is derived from the weak approximation property for the algebraic group $\mathbf{SL}_{1,D}$ associated with $SL(1, D)$, i.e. from the fact that $SL(1, D)$ is dense in $SL(1, \mathcal{D})$ (we refer to [13], §7.3, regarding weak approximation in algebraic groups; we indicate only that weak approximation in $\mathbf{SL}_{1,D}$ follows from the fact that being defined by a single quadratic equation, this group is a rational variety (cf. [13], prop. 7.3), or from the general result ([13], prop. 7.9) about weak approximation in simply connected algebraic groups over number fields). Indeed, suppose $s \in \mathbb{Q}_+ \cap \mathcal{I}$, i.e. $s = \mathrm{Nrd}_{D/\mathbb{Q}}(x) = \mathrm{Nrd}_{\mathcal{D}/\mathbb{Q}_2}(y)$ for some $x \in D$, $y \in \mathcal{W}$. Then $x^{-1}y \in \mathcal{U} := SL(1, \mathcal{D}) \cap (x^{-1}\mathcal{W})$, so $\mathcal{U}$ is a nonempty open subset of $SL(1, \mathcal{D})$. Invoking weak approximation for $\mathbf{SL}_{1,D}$, we conclude that there exists $z \in SL(1, D) \cap \mathcal{U}$. Then $xz \in \mathcal{W} \cap D^\times = W$, so $s = \mathrm{Nrd}_{D/\mathbb{Q}}(xz) \in \mathrm{Nrd}_{D/\mathbb{Q}}(W)$, proving (2).

Combined with the openness of $\mathcal{I}$, (2) implies that for a given W there exists $d = d(W)$ such that the arithmetic progression $\{1 + 2^d n \mid n = 1, 2, \dots\}$ is contained in $\mathrm{Nrd}_{D/\mathbb{Q}}(W)$. However, by the Prime Number Theorem, this progression contains a prime, which, of course, does not belong to H. Thus, $W \not\subset M$, so (1) follows as M has index two. We notice that (1) implies, in particular, that M is not open in the $\tilde{v}$-adic topology.

Now, let $\mathcal{W} \subset \mathcal{D}^\times$ be an open normal subgroup of finite index such that the quotient $\mathcal{D}^\times/\mathcal{W}$ is nonabelian (explicit example: as we observed in [17], 8.4, for $\mathcal{W} = \mathbb{Q}_2^\times(1 + \mathfrak{P})$, where $\mathfrak{P}$ is the valuation ideal in $\mathcal{D}$, the quotient $\mathcal{D}^\times/\mathcal{W}$ is the symmetric group on three letters). Set $W = D^\times \cap \mathcal{W}$ and observe that $D^\times/W \simeq \mathcal{D}^\times/\mathcal{W}$ as $D^\times$ is dense in $\mathcal{D}^\times$. Let $N = M \cap W$. Then it follows from (1) that

$$D^\times/N \simeq D^\times/M \times D^\times/W,$$

implying that $D^\times/N$ is a nonabelian group with nontrivial center, hence its commuting graph has diameter two. On the other hand, as we observed above, M is not $\tilde{v}$-adically open in $D^\times$, so N cannot be open either. Since D does not have any valuations other than $\tilde{v}$, this means in effect that N is not open in D with respect to *any* set of valuations.

In connection with the above example, we would like to point out that there are numerous finite groups with trivial center and the commuting graph having diameter two. The simplest example is as follows. Let $H = (\mathbb{Z}/2\mathbb{Z})^3$ and consider the group ring $\mathbf{F}_p[H]$, where p is a prime > 2. Let $\varepsilon\colon \mathbf{F}_p[H] \to \mathbf{F}_p$ denote the augmentation homomorphism, and $V = \mathrm{Ker}\ \varepsilon$. Then $V^H = \{0\}$, implying that the center of $G := H \ltimes V$ is trivial. On the other hand, let $g_1, g_2 \in G$, where $g_i = (h_i, v_i)$. Let $D \subset H$ be the subgroup generated by h_1 and h_2. Then $\dim \mathbf{F}_p[H]^D = [H : D] \geqslant 2$, and therefore $\dim V^D \geqslant 1$. Pick $v \in V^D - \{0\}$; then the element $(0, v)$ is a nonidentity element that commutes with both g_1 and g_2, proving that $\operatorname{diam} \Delta_G = 2$ as G is noncommutative.

We do not know, however, if the group G constructed above can be realized as a quotient of the multiplicative group of some finite dimensional division algebra. So, it might still be true that if $G = D^\times/N$ and $\operatorname{diam} \Delta_G = 2$ then $Z(G)$ is nontrivial.

References

[1] Cassels, J.W.S., Frölich, A. (ed.): Algebraic number theory. Proc. of an Instructional Conf. Organized by the London Math. Soc., Academic Press, London and New York, 1967

[2] Aschbacher, M., Guralnick, R.: Some applications of the first cohomology group. J. Algebra **90**, 446–460 (1984)

[3] Bergelson, V., Shapiro, D.B.: Multiplicative subgroups of finite index in a ring. Proc. AMS **116**, 885–896 (1992)

[4] Bourbaki, N.: Algèbre commutative. ch. V-VI, Masson, Paris, 1985

[5] Faith, C.: On conjugates in division rings. Canad. J. Math. **10**, 374–380 (1958)

[6] Grothendieck, A.: Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. I. Publ. math. IHES **20**, 259 (1964)

[7] Grothendieck, A.: Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II. Publ. math. IHES **24**, 231 (1965)

[8] Koch, H.: Number Theory: Algebraic Numbers and Functions. Graduate Studies in Mathematics, vol. **24**, AMS, 2000

[9] Liebeck, M.W., Shalev, A.: The probability of generating a finite simple group. Geom. Dedicata **56**, 103–113 (1995)

[10] Lubotzky, A., Segal, D.: Subgroup Growth. Birkhäuser, 2003

[11] Malle, G., Saxl, J., Weigel, T.: Generation of classical groups. Geom. Dedicata **49**, 85–116 (1994)

[12] Margulis, G.A.: Finiteness of quotients of discrete subgroups. Funct. Anal. Appl. **13**, 178–187 (1979)

[13] Platonov, V.P., Rapinchuk, A.S.: Algebraic Groups and Number Theory. Academic Press, 1993

[14] Prasad, G.: Strong approximation for semi-simple groups over function fields. Ann. Math. **105**, 553–572 (1977)

[15] Raghunathan, M.S.: On the group of norm 1 elements in a division algebra. Math. Ann. **279**, 457–484 (1988)

[16] Rapinchuk, A., Potapchik, A.: Normal subgroups of $SL_{1,D}$ and the classification of finite simple groups. Proc. Indian Acad. Sci. (Math. Sci.) **106**, 329–368 (1996)

[17] Rapinchuk, A.S., Segev, Y.: Valuation-like maps and the congruence subgroup property. Invent. Math. **144**, 571–607 (2001)

[18] Rapinchuk, A.S., Segev, Y., Seitz, G.M.: Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable. J. AMS **15**, 929–978 (2002)

[19] Riehm, C.: The norm 1 group of a p-adic division algebra. Am. J. Math. **92**, 499–523 (1970)

[20] Segev, Y.: On finite homomorphic images of the multiplicative group of a division algebra. Ann. Math. **149**, 219–251 (1999)

[21] Segev, Y.: Some applications of Wedderburn's factorization theorem. Bull. Austral. Math. Soc. **59**, 105–110 (1999)

[22] Segev, Y.: The commuting graph of minimal nonsolvable groups. Geom. Ded. **88**, 55–66 (2001)

[23] Segev, Y., Seitz, G.M.: Anisotropic groups of type A_n and the commuting graph of finite simple groups. Pacific J. Math. **202**, 125–226 (2002)

[24] Turnwald, G.: Multiplicative subgroups of finite index in rings. Proc. AMS **120**, 377–381 (1994)