Normal subgroups of the multiplicative group of a division algebra, and valuations

A. Rapinchuk

Introduction

One of the goals of this paper (which grew out of our notes [R]) is to present a recent result of Segev [S1] from the perspective provided by the Platonov-Margulis conjecture (refered to as (PM) in the sequel). Referring to [PR3], Ch.IX, for a discussion of this conjecture in the context of arbitrary (simple simply connected) algebraic groups, we recall here that for the algebraic group defined by the group $SL(1, D)$ of elements of reduced norm one in a finite dimensional central division algebra D over a global field K, (PM) states that any noncentral normal subgroup $N \subset SL(1, D)$ is open in $SL(1, D)$ with respect to the topology defined by the set T of all nonarchimedean valuations v of K such that $D \otimes_K K_v$ is a division algebra. (It is worthwhile to observe that T can be naturally identified with the set of all nonarchimedean valuations of D, so (PM) in effect speculates about the openness of noncentral normal subgroups of $SL(1, D)$ with respect to the topology defined by valuations of D. One should also bear in mind two finiteness results in this setting: any noncentral normal subgroup $N \subset SL(1, D)$ has finite index (cf. [M1], [Pr]), and T is always finite which follows, for example, from Theorem 6.7 in [PR3].)

The initial results on (PM) were purely arithmetic. First, it was shown in [PR1] that if D is a quaternion algebra for which $T = \emptyset$, then $SL(1, D)$ is a perfect group, i.e. $SL(1, D) = [SL(1, D), SL(1, D)]$. Using some techniques of [PR1], Margulis [M2] proved (PM) for $G = SL(1, D)$, D a quaternion algebra, in full. In [PR2], the methods and results of [PR1] were extended from quaternion algebras to algebras of arbitrary degree to prove that $[SL(1, D), SL(1, D)]$ is T-adically open in $SL(1, D)$ for D of arbitrary degree. Raghunathan [Ra] elaborated on this result and showed that if $U \subset SL(1, D)$ is a T-adically open subgroup, then so is its commutator subgroup $[U, U]$. Tomanov [T] extended Margulis's result from quaternion algebras to algebras of degree 2^d, $d \geq 1$, and moreover reduced (PM) to algebras of odd degree.

An essentially new approach to (PM) was proposed in our paper [RPo]. First, we used some results from [Ra] to reduce (PM) to the assertion that the multiplicative group D^* doesn't have normal subgroups Δ such that D^*/Δ is a (nonabelian) finite simple group. As this statement (in contrast to (PM)) makes sense for division algebras over arbitrary fields, we conjectured its truth for all finite dimensional division algebras and proved this for algebras of degree 2 and 3 over arbitrary fields. The argument for a cubic division algebra D was based on the observation that given any two elements x, y of a quotient $G = D^*/N$, then

$$G = C(x,y)C(x)C(x,y)$$

where $C(x)$ is the centralizer of x in G, and $C(x,y) = \bigcup_{z \in yC(x)} C(z)$. To bring this to a contradiction, one shows, using the classification of finite simple groups and a case-by-case analysis, that every (known) noncommutative finite simple group has a pair of elements that fail to satisfy this property. Though this argument didn't seem to apply to division algebras of higher degree, it did create the general feeling that the quotients of D^* should have elements with relatively large centralizers, or more generally, satisfy some form of the commutativity condition.

A major further progress in this direction was achieved by Segev [S1] who came up with the idea to use the diameter of the commuting graph of G to measure how far G is from being commutative, and to consider groups having "large" diameter. Analyzing additive properties of elements that are far apart in the commuting graph, he proved that D^* cannot have quotients that are finite simple groups whose commuting graph either has diameter > 4 or is balanced. Furthermore, in a joint paper [SSe], Segev and Seitz showed that any (known) finite simple group either has diameter > 4 or is balanced. This completed (modulo the classification of finite simple groups) the proof of our conjecture that D^* cannot have finite simple groups as quotients, yielding, in particular, the truth of the Platonov-Margulis conjecture for the groups of the form $SL(1, D)$.

One cannot help noticing, however, that though Segev's result eventually implies (PM), his argument is not really associated with the general philosophy suggested by (PM), which is hypothetical openness of normal subgroups with respect to a system of valuations[1]. This prompted us to try to understand Segev's result from the perspective provided by (PM). To some extent, this task was accomplished in our notes [R] where we used some facts about

[1]We observe that Segev ([S1] , §6) constructs a homomorphism of the normal subgroup under consideration to a totally ordered group and remarks in 6.9 that this homomorphism behaves on this normal subgroup like a valuation, but doesn't make essential use of this fact later. For us, however, this remark was really the starting point.

valuations to indicate a shortcut in Segev's argument. In the present paper we develop this approach proving a variant of the "congruence subgroup theorem" for finite dimensional division algebras over arbitrary fields. This fact enables one to recover Segev's result [S1], but can also be used for some other purposes (cf. §8).

In §1, after some preliminaries, we prove (cf. Lemma 1) that if subgroup $\Delta \subset D^*$ of finite index is open with respect to a nontrivial valuation of D, then there exists a nontrivial homomorphism $\varphi\colon \Delta \to \Gamma$ to a totally ordered group Γ and $\alpha \in \Gamma$, $\alpha \geq 0$, such that for $\Delta_-(\alpha) := \{x \in \Delta \mid \varphi(x) < -\alpha\}$ one has:

$$\Delta_-(\alpha) + 1 \subset \Delta_-(\alpha). \tag{1}$$

A considerable part of the paper is devoted to reversing this condition, viz. to proving that for a subgroup of finite index $\Delta \subset D^*$, a nontrivial homomorphism $\varphi\colon \Delta \to \Gamma$ onto a totally ordered group, satisfying (1) for some nonnegative $\alpha \in \Gamma$, gives rise to a nontrivial valuation on D with respect to which Δ turns out to be open. We prove furthermore (cf. Proposition 1) that given condition (1), the openness of Δ follows automatically from the existence of a valuation associated with φ, so the subsequent §§2-4 deal only with constructing such a valuation. After some preparations in §2, we prove in §§3 and 4 the existence of the valuation in the commutative ($D = K$) and noncommutative cases, respectively.

The next section of the paper, §§5-6, dealing with constructing a homomorphism $\varphi\colon \Delta \to \Gamma$ satisfying (1) in case Δ is normal in D^* and the commuting graph of the quotient D^*/Δ either has diameter > 4 or is balanced (we refer to §6 for precise definitions), heavily relies on Segev's paper [S1]. In fact, condition (1) is a formal consequence of 6.3 in [S1], however in view of the following reasons we found it more appropriate to include a full argument rather than just to give a reference. Firstly, a lot of material in [S1] preceeding 6.3 is simply not necessary for the validation of (1). Secondly, most constructions in [S1] are implemented under the additional assumption that D^*/Δ is simple, and it is important for our purposes to show explicitly that this assumption is not necessary either. In §5 we associate with a fixed element $x \in D^* - \Delta$ a certain pre-order relation $\mathcal{R}_x$ on Δ compatible with the group structure, which gives rise to a homomorphism $\varphi\colon \Delta \to \Gamma$ onto a partially ordered group Γ (this relation is slightly different from the one that results from Segev's argument). Then in §6 we show that under the above assumptions on the commuting graph of D^*/Δ, there exists an $x \in D^*$ for which $\mathcal{R}_x$ is a linear order relation, and moreover, condition (1) is satisfied for $\alpha = 0$. We would like to emphasize that §6 is assembled entirely from fragments of Segev's argument: we just picked from §§2-4 of his paper [S1] all that is necessary for our purposes. Needless to say that we claim no credit for the content of §6 and included this material only for the reader's convenience.

Putting together the results of §§1-6, we obtain the following theorem which is the main result of the paper.

Main Theorem *Let D be a finite dimensional algebra over a finitely generated field K. If $\Delta \subset D^*$ is a normal subgroup of finite index such that the commuting graph of the quotient D^*/Δ either has diameter > 4 or is balanced, then Δ is open in D^* with respect to a certain nontrivial valuation of D.*

The concluding sections, §§7 and 8, contain a discussion and some applications of the main theorem. First of all, at this point it is the only known congruence subgroup theorem over arbitrary (finitely generated) fields. Though its assumptions are satisfied if D^*/Δ is a nonabelian finite simple group (cf. [SSe]), we do not actually obtain any examples here as these groups cannot be realized as quotients of D^* (cf. [S1]). So, we show in §7, using the 2-adic quaternion division algebra, that the symmetric group S_3 can be realized as D^*/Δ; on the other hand, it follows from the main theorem that each time this happens, Δ is open in D^* with respect to a nontrivial valuation of D as the commuting graph of S_3 is disconnected. Of course, this example can be generalized using p-adic division algebras of higher degree, but undoubtedly, some additional analysis is required to understand what solvable groups satisfy the assumptions of the theorem and whether or not these assumptions can be weakened (that some form of the "noncommutativity" condition is necessary follows from the example given in the beginning of §3).

Finally, in §8 we develop a technique for eliminating some (hopefully, all) nonsolvable finite groups as possible quotients of D^*. The key observation is that if a finite group G is realized as $G = D^*/\Delta$ where Δ is open in D^* with respect to a nontrivial valuation v of D, then a certain group $\bar{G}$ which is a quotient of a normal subgroup $H \subset G$ with abelian G/H by a solvable normal subgroup, can be realized as $\bar{G} = \bar{D}^*/\bar{\Delta}$, where $\bar{D}$ is the residue algebra of D with respect to v. Now, assume this reduction process can be continued, i.e. $\bar{\Delta}$ is open in $\bar{D}$ with respect to a valuation $\bar{v}$, etc. Then, if the center of the original division algebra D was a finitely generated field (which we may always assume to be the case), after a series of consecutive reductions we will obtain a division algebra $\mathcal{D}$ over a finite field which must be commutative by Wedderburn's theorem. On the other hand, by construction, the multiplicative group $\mathcal{D}^*$ should have as a quotient a finite group $\mathcal{G}$ which contains the nonsolvable "part" of G, yielding a contradiction if G was not solvable to begin with. This approach allows one to recover Segev's result (cf. Theorem 7), but applies also to some nonsolvable nonsimple groups[2]. For example, we show that the symmetric group S_n where $n = p$ or $n = p + 1$, p a prime > 3, cannot be obtained as a quotient of D^* (cf. Proposition 6). The possibility to extend this approach to other nonsolvable groups depends now only on availability of information regarding what finite groups either have diameter > 4 or are balanced. It seems plausible (though has not been checked) that the elements constructed in [SSe] to prove that for any nonabelian finite simple group F the commuting graph $\mathfrak{F}$ is either balanced or has diameter > 4 will also work (at least, in most cases) to generalize this fact to any group H such that $\mathrm{Int}\, F \subset H \subset \mathrm{Aut}\, F$ where F is a nonabelian finite simple group. If this is indeed the case,we would obtain that none of such groups can be realized as D^*/Δ. However, an ultimate goal in this direction would be to prove a recent conjecture (cf. [S2]) that **all** finite quotients of D^* should be solvable (so far this has been established only for cubic division algebras, cf. [RoS]), and in the end of §8 we describe a group-theoretic result (having to do with the commuting graph of some specific groups) that would enable one to do that.

The work on this paper began when the author was visiting the University of Bielefeld as a guest of the GIF project (summer 1998), and continued with partial support from the NSF and BSF USA-Israel.

[2]We observe that Segev does make essential use of simplicity, so his argument may not work for nonsimple groups.

1 On subgroups open with respect to a valuation

Let D be a finite dimensional division algebra over a field K, $\Delta \subset D^*$ be a proper finite index normal subgroup of its multiplicative group. For technical reasons, it is convenient to assume that $-1 \in \Delta$. *This assumption* doesn't really result in a loss of generality and *will be kept throughout the paper.* The goal of §§1-4 is to establish a criterion for Δ to be open in D^* with respect to a nontrivial valuation v of D.

Given a (nontrivial) linearly ordered additive (but not necessarily abelian) group Γ, for $\alpha \in \Gamma$, $\alpha \geq 0$, we let $\Gamma_-(\alpha)$ (resp., $\Gamma_+(\alpha)$) denote the set of $\gamma \in \Gamma$ satisfying $\gamma < -\alpha$ (resp., $\gamma > \alpha$). Next, given a surjective homomorphism $\varphi\colon \Delta \to \Gamma$, we let $\Delta_{\pm}(\varphi, \alpha) = \varphi^{-1}(\Gamma_{\pm}(\alpha))$. If the homomorphism φ is clear from the context, we will simplify this notation to just $\Delta_{\pm}(\alpha)$. Also, we will write $\Gamma_{\pm}$ and $\Delta_{\pm}$ instead of $\Gamma_{\pm}(0)$ and $\Delta_{\pm}(0)$, respectively.

Suppose now that v is a valuation of D with the value group $\tilde{\Gamma} = v(D^*)$[3] and the valuation ring $O_{D,v}$. Associated with any $\delta \in \tilde{\Gamma}$, $\delta \geq 0$, one has a two-sided ideal

$$\mathfrak{m}_{D,v}(\delta) = \{x \in D^* \mid v(x) > \delta\} \cup \{0\}$$

of $O_{D,v}$. The ideals $\{\mathfrak{m}_{D,v}(\delta)\}$ for all nonnegative $\delta \in \tilde{\Gamma}$ form a fundamental system of neighborhoods of zero for the natural topology on D associated with the valuation v (sometimes referred to as the v-adic topology), cf. details in [Bo], §5, n° 1. This topology makes D^* into a topological group, and the openness of a subgroup $\Delta \subset D^*$ is equivalent to the fact that there exists a $\delta \in \tilde{\Gamma}$ such that $1 + \mathfrak{m}_{D,v}(\delta) \subset \Delta$. Of course, we will write O, $\mathfrak{m}$, etc. instead of $O_{D,v}$, $\mathfrak{m}_{D,v} \ldots$ if this may not lead to a confusion.

Lemma 1 *Let v be a valuation of D, and $\Delta \subset D^*$ be a v-adically open subgroup having finite index m. If $\varphi\colon \Delta \to \Gamma := v(\Delta)$ is the restriction of v, then there exists an $\alpha \in \Gamma$ such that*

$$\Delta_-(\alpha) + 1 \subset \Delta_-(\alpha). \tag{1}$$

Proof. By our assumption there exists a $\delta \in \tilde{\Gamma}$, $\delta \geq 0$, such that $1 + \mathfrak{m}(\delta) \subset \Delta$. There exists an $\alpha \in \Gamma$ with the property $\alpha \geq \delta$ (one can take, for example,

[3]We recall that $\tilde{\Gamma}$ is automatically abelian (this follows, for example, from Theorems 9, 10 in Ch. 2 of [Sc]).

$\alpha = \delta^m$ where $m = [D^* : \Delta]$), and we claim that for any such α condition (1) holds true. Indeed, for any $x \in \Delta_-(\alpha)$ we have

$$1 + x = (1 + x^{-1})x \in \Delta,$$

as $1 + x^{-1} \in 1 + \mathfrak{m}(\alpha) \subset 1 + \mathfrak{m}(\delta) \subset \Delta$. Furthermore, since v is a valuation, we have

$$\varphi(1 + x) = v(1 + x) = v(x) < -\alpha$$

as $v(x) < 0 = v(1)$. So, $1 + x \in \Delta_-(\alpha)$, as required.

From now on our efforts will be focused on reversing this lemma, viz. on proving that a nontrivial homomorphism $\varphi\colon \Delta \to \Gamma$ to a linearly ordered (not necessarily abelian) group Γ satisfying (1) for some nonnegative $\alpha \in \Gamma$ gives rise to a nontrivial valuation v of D with respect to which Δ turns out to be open. To describe the relationship between φ and v in precise terms, we need the following.

Definition. Let $\varphi\colon \Delta \to \Gamma$ be a homomorphism onto a totally ordered group. We say that a valuation $v\colon D^* \to \tilde{\Gamma}$ is *associated* with φ if there exists a homomorphism $\theta\colon \Gamma \to \tilde{\Gamma}$ of ordered groups such that the diagram

$$\begin{array}{ccc} \Delta & \xrightarrow{\varphi} & \Gamma \\ \iota\downarrow & & \downarrow\theta \\ D^* & \xrightarrow{v} & \tilde{\Gamma} \end{array} \tag{2}$$

in which ι is the natural embedding, commutes. Furthermore, we say that v *extends* φ if θ is injective.

After some preparations in §2, we will examine the existence of a valuation v associated with φ in the commutative and noncommutative cases, respectively. As the following proposition shows, once the existence of v has been established, the openness of Δ with respect to v is an automatic consequence of (1).

Proposition 1 *Assume the homomorphism $\varphi\colon \Delta \to \Gamma$ satisfies (1) and admits an associated let valuation v. Then Δ is open in D^* in the v-adic topology.*

Proof. We need to show that there exists a $\delta \in \tilde{\Gamma}$ such that $1 + \mathfrak{m}(\delta) \subset \Delta$. We begin with the following two lemmas.

Lemma 2 *For $a, b \in \Delta$ such that $v(a) < v(b) - \theta(\alpha)$, the element $c = a + b$ belongs to Δ.*

Proof. We obviously have $\varphi(a) < \varphi(b) - \alpha$, hence $\varphi(b^{-1}a) < -\varphi(b) + \varphi(a) < -\alpha$, i.e. $b^{-1}a \in \Delta_-(\alpha)$. Then

$$b^{-1}a + 1 \in \Delta_-(\alpha) + 1 \subset \Delta_-(\alpha) \subset \Delta$$

in view of (1), and therefore $c = b(b^{-1}a + 1) \in \Delta$.

Lemma 3 *For any $z \in D^*$, there exists a $\gamma(z) \in \tilde{\Gamma}$ such that for any $t \in \Delta$ with the property $v(t) < \gamma(z)$, one has $z + t \in \Delta$.*

Proof. Since $D = \Delta - \Delta$ (cf. [BSh], [Tu]), there exists an $s \in \Delta$ such that $z + s \in \Delta$. Set $\gamma(z) = \min(v(s), v(z+s)) - \theta(\alpha)$. Suppose now that $t \in \Delta$ satisfies $v(t) < \gamma(z)$. Then, in particular, $v(t) < v(s) - \theta(\alpha)$, so it follows from Lemma 2 that $t - s \in \Delta$; moreover, $v(t - s) = v(t)$ as v is a valuation and $v(t) < v(s)$. Thus $v(t - s) < v(z + s) - \theta(\alpha)$, and

$$z + t = (z + s) + (t - s) \in \Delta$$

again according to Lemma 2.

Now, we pick a complete system $a_1, \ldots, a_r$ of representatives of cosets D^*/Δ, and let

$$\delta' = \max_{i=\overline{1,r}} \mid v(a_i) \mid, \quad \delta'' = \max_{i=\overline{1,r}} \mid \gamma(a_i) \mid,$$

(where as usual for $\gamma \in \tilde{\Gamma}$, we let $\mid \gamma \mid = \max(\gamma, -\gamma)$), and $\delta = \delta' + \delta''$. We claim that

$$1 + \mathfrak{m}(\delta) \subset \Delta.$$

Indeed, pick a $b \in \mathfrak{m}(\delta)$, $b \neq 0$. One can write $b = a_i c$ for some i and some $c \in \Delta$. Then

$$v(c) = v(b) - v(a_i) \geq v(b) - \delta' > \delta''.$$

It follows that

$$1 + b = (c^{-1} + a_i)c \in \Delta$$

as $v(c^{-1}) < -\delta'' \leq \gamma(a_i)$, and therefore $c^{-1} + a_i \in \Delta$.

2 Towards proving the existence of an associated valuation

We will be exploiting the well-known connection between valuations and valuation rings. Let $\mathcal{A}$ be the subring of D generated by $\Delta_+(\alpha)$, $\mathcal{O} = \{x \in D \mid x\mathcal{A} \subset \mathcal{A}\}$, and $\tilde{\mathcal{O}}$ be the set of elements $x \in D$ that are integral over $\mathcal{O}$, i.e. satisfy an equation

$$x^d + a_1 x^{d-1} + \cdots + a_d = 0$$

for some $d \geq 1$ with $a_i \in \mathcal{O}$. (If D is commutative, then $\tilde{\mathcal{O}}$ is obviously the integral closure of $\mathcal{O}$ in D, however $\tilde{\mathcal{O}}$ may not be a subring for D noncommutative.)

Theorem 1 *1) For any $x \in D^*$, either x or x^{-1} belongs to $\tilde{\mathcal{O}}$.*
2) Assume (1). Then $\tilde{\mathcal{O}} \cap \Delta_-(\alpha) = \emptyset$.

PROOF. Let $m = [D^* : \Delta]$. Then for any $x \in D^*$ one has $x^m \in \Delta$. Moreover, replacing x with x^{-1} if necessary, we may (and we will) assume in addition that $\varphi(x^m) \geq 0$. Then $x^m \Delta(\alpha) \subset \Delta(\alpha)$, implying that $x^m \mathcal{A} \subset \mathcal{A}$, i.e. $x^m \in \mathcal{O}$, and eventually $x \in \tilde{\mathcal{O}}$, proving 1).

For 2), we will first establish that

$$\mathcal{A} \cap \Delta_-(\alpha) = \emptyset. \tag{1}$$

We need the following.

Lemma 4 *Assume that φ satisfies condition (1) §1. Then*

$$\Delta_-(\alpha)\Delta_-(\alpha) + 1 \subset \Delta_-(2\alpha).$$

PROOF. Let $s_1, s_2 \in \Delta(\alpha)$. We have $-1 \in \Delta$ and $\varphi(-1) = 0$ implying that $-\Delta_-(\alpha) = \Delta_-(\alpha)$. So, it follows from condition (1) §1 that $s_1 - 1 = -(-s_1 + 1)$ and $s_2 + 1$ both belong to $\Delta_-(\alpha)$; in particular, the expressions $\varphi(s_1 - 1)$ and $\varphi(s_2 + 1)$ make sense. We will consider two cases.

CASE 1. $\varphi(s_2 + 1) \geq \varphi(s_1 - 1)$. We have

$$\varphi((s_2 + 1)^{-1}(s_1 - 1)s_2) \leq \varphi(s_2) < -\alpha,$$

and therefore $(s_2+1)^{-1}(s_1-1)s_2+1 \in \Delta_-(\alpha)$. Then the identity

$$s_1s_2+1 = (s_2+1)[(s_2+1)^{-1}(s_1-1)s_2+1].$$

implies that $s_1s_2+1 \in \Delta_-(2\alpha)$.

CASE 2. $\varphi(s_2+1) \leq \varphi(s_1-1)$. This case is considered similarly using the identity

$$s_1s_2+1 = [s_1(s_2+1)(1-s_1)^{-1}+1](1-s_1).$$

Assume now that (1) is false, and pick an element $w \in \Delta_-(\alpha)$ which admits a presentation

$$w = b_1 + \cdots + b_l, \quad b_i \in \Delta_+(\alpha)$$

with minimal possible l (obviously, $l > 1$ as $\Delta_-(\alpha) \cap \Delta_+(\alpha) = \emptyset$). Then

$$w - b_l = b_1 + \cdots + b_{l-1}.$$

But since $wb_l^{-1}-1 \in \Delta_-(2\alpha)$ by Lemma 4, we see that $w - b_l = (wb_l^{-1}-1)b_l \in \Delta_-(\alpha)$, which contradicts the minimality of l, thereby proving (1).

Now, suppose $z \in \Delta_-(\alpha) \cap \tilde{\mathcal{O}}$. Then z satisfies an equation

$$z^d + a_1z^{d-1} + \cdots + a_d = 0$$

with $a_i \in \mathcal{O}$. It follows that

$$z = -(a_1 + \cdots + a_dz^{-(d-1)}) \in \mathcal{O}, \quad \text{i.e.} \quad z\mathcal{A} \subset \mathcal{A}.$$

Since $z^{-1} \in \Delta_+(\alpha)$, the inclusion $z\mathcal{A} \subset \mathcal{A}$ entails $1 \in \mathcal{A}$, which in turn implies that $z \in \mathcal{A}$, contadicting (1). The proof of the theorem is complete.

3 The commutative case

In [C], Chevalley established the congruence subgroup property for an arbitrary finitely generated subgroup $E \subset K^*$ where K is a number field. More precisely, he proved that given a subgroup $E' \subset E$ of finite index and any finite set S of valuations of K for which E is contained in the group K_S^* of S-units, one can pick finitely many (nonarchimedean) valuations $v_1, \ldots, v_r \notin S$ such that for a suitable integer n, the congruence subgroup

$$\{x \in E \mid v_i(x-1) \geq n, \ i = 1, \ldots r\}$$

is contained in E' (in other words, E' is open in E for the topology defined by a certain finite collection of valuations). However, this fact is no longer true if one considers infinitely generated subgroups, in particular, the multiplicative group K^* itself. For example, if $K = \mathbb{Q}$, then the group $\mathbb{Q}^*_+$ of positive rationals is not open in $\mathbb{Q}^*$ with respect to the topology defined by any finite set of nonarchimedean valuations (though, of course, it is open with respect to the archimedean one). As a more sophisticated example (in which even the archimedean valuation doesn't help) one can consider the subgroup

$$\Gamma = \{x \in \mathbb{Q}^* \mid x = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r} \text{ and } \alpha_1 + \cdots + \alpha_r \equiv 0 (\operatorname{mod} 2)\}.$$

To see that Γ is not open in $\mathbb{Q}$ with respect to any finite set of valuations, one needs to observe that any open subgroup must contain a certain arithmetic progression $1 + d\mathbb{Z}$ which always contains a prime while Γ does not.

The following statement gives a criterion for a subgroup $\Delta \subset K^*$ of finite index, K is an arbitrary field, to be open with respect to a single valuation.

Theorem 2 *Let K be a field, $\Delta \subset K^*$ be a subgroup of finite index m. Then Δ is open with respect to some nontrivial valuation v of K if and only if there exists a nontrivial homomorphism $\varphi\colon \Delta \to \Gamma$ onto a totally ordered group Γ and an $\alpha \in \Gamma$, $\alpha \geq 0$, such that $\Delta_-(\alpha) + 1 \subset \Delta_-(\alpha)$. The valuation v and the homomorphism φ are associated, and moreover, v extends φ if either $\alpha = 0$ or Γ has height one. Furthermore, if K is finitely generated, then there exists a unique (up to equivalence) valuation of K having height one and associated with φ.*

PROOF. We consider $\mathcal{A}$, $\mathcal{O}$, and $\tilde{\mathcal{O}}$ introduced in the beginning of §2. Since K is commutative, $\tilde{\mathcal{O}}$ is a subring of K. Moreover, it follows from Theorem 1 that $\tilde{\mathcal{O}}$ is a valuation ring and $\tilde{\mathcal{O}} \neq K$. By ([Bo], §3, n° 2-3) or ([Sc], Ch.1, Thm.3), there exists a nontrivial valuation $v\colon K^* \to \tilde{\Gamma} := K^*/\tilde{\mathcal{O}}^*$ whose valuation ring coincides with $\tilde{\mathcal{O}}$. It follows from our construction that $\Delta_{\geq 0} = \{x \in \Delta \mid \varphi(x) \geq 0\}$ is contained in $\tilde{\mathcal{O}}$, implying that $v(\Delta_{\geq 0})$ is contained in $\tilde{\Gamma}_{\geq 0} = \{x \in \tilde{\Gamma} \mid x \geq 0\}$; in particular, for $a \in \Delta$, the fact that $\varphi(a) = 0$ implies that $v(a) = 0$. All this allows us to conclude that there exists a homomorphism of ordered groups $\theta\colon \Gamma \to \tilde{\Gamma}$ for which the diagram (2) §1 commutes, so that v is associated with φ.

If θ is not injective, then $\operatorname{Ker}\theta \cap \Gamma_- \neq \emptyset$, implying $\Delta_- \cap \tilde{\mathcal{O}} \neq \emptyset$ which immediately contradicts assertion 2) of Theorem 1 if $\alpha = 0$. In any case, $\operatorname{Ker}\theta$

is a proper isolated subgroup of Γ which forces $\mathrm{Ker}\,\theta$ to be trivial if Γ has height one as in this case there are no nontrivial proper isolated subgroups.

Once the existence of a valuation v associated with φ has been established, the openness of Δ in K^* with respect to the corresponding v-adic topology follows from Proposition 1.

Suppose now that K is finitely generated. Then it follows from Cor. 1 in n° 3 and Prop. 3 in n° 2 of [Bo], §10, that $\tilde{\Gamma} = v(K^*)$ has finite height, so there exists a homomorphism of ordered groups $\mu\colon \tilde{\Gamma} \to \bar{\Gamma}$ with $\bar{\Gamma}$ onto a group $\bar{\Gamma}$ of height one, and then the valuation $\bar{v} = \mu \circ v$ is the required valuation of K having height one and associated with φ. To establish the uniqueness, suppose that v_1 and v_2 are two valuations with this property, i.e. for each $i = 1, 2$ there exists a commutative diagram of the form

$$\begin{array}{ccc} \Delta & \stackrel{\varphi}{\to} & \Gamma \\ \iota \downarrow & & \downarrow \theta_i \\ K^* & \stackrel{v_i}{\to} & \tilde{\Gamma}_i \end{array}.$$

Being isolated subgroups of Γ with quotients having height one, $\mathrm{Ker}\,\theta_i$ for $i = 1, 2$ must coincide. This implies that the valuation rings $\mathcal{O}_{v_1}$ and $\mathcal{O}_{v_2}$ also coincide. Indeed, for an $x \in \mathcal{O}_{v_1}$, $x \neq 0$, one has $x^m \in \Delta$, and there are two possibilities: 1) $\varphi(x^m) \geq 0$, and 2) $\varphi(x^m) < 0$. In the first case, $v_2(x^m) = \theta_2(\varphi(x^m)) \geq 0$, and eventually $v_2(x) \geq 0$. In the second case we have $v_1(x^m) = \theta_1(\varphi(x^m)) \leq 0$ which in conjunction with $v_1(x) \geq 0$ (as $x \in \mathcal{O}_{v_1}$) implies that actually

$$\varphi(x^m) \in \mathrm{Ker}\,\theta_1 = \mathrm{Ker}\,\theta_2,$$

so $v_2(x^m) = \theta_2(\varphi(x^m)) = 0$, and $v_2(x) = 0$. In either case, $v_2(x) \geq 0$, i.e. $x \in \mathcal{O}_{v_2}$, proving the inclusion $\mathcal{O}_{v_1} \subset \mathcal{O}_{v_2}$; by symmetry we obtain the opposite inclusion. Thus, $\mathcal{O}_{v_1} = \mathcal{O}_{v_2}$ which implies that v_1 and v_2 are equivalent (cf. [Bo], §3, Prop. 3).

4 The noncommutative case.

Theorem 3 *Let D be a central division algebra of degree n over a finitely generated field K (i.e. $\dim_K D = n^2$), $\Delta \subset D^*$ be a subgroup of finite index m. Then Δ is open with respect to a nontrivial valuation w of D if and only* *if there exists a homomorphism $\varphi: \Delta \to \Gamma$ onto a totally ordered group Γ (not necessarily abelian) and an $\alpha \in \Gamma$, $\alpha \geq 0$, such that $\Delta_{-}(\alpha) + 1 \subset \Delta_{-}(\alpha)$. Given such a φ, the corresponding valuation w is always associated with φ and moreover can be chosen to have height one. Furthermore, w extends φ if either $\alpha = 0$ or Γ has height one.*

First, we will use Theorem 2 to construct valuations on maximal subfields of D, and then show that all these valuations agree on the center.

Proposition 2 *Let $M \subset D$ be a subfield containing K, $\Delta_M := \Delta \cap M$, and $\varphi_M: \Delta_M \to \Gamma_M := \varphi(\Delta_M)$ be the restriction of φ to Δ_M. Then there exists a unique valuation v_M of M having height one and associated with φ_M. The restriction $v_0 = v_M \mid K$ does not depend on the choice of M, and the group $\Delta_K = \Delta \cap K$ is v_0-adically open in K^*.*

PROOF. Pick an $a \in D$ such that $\varphi(a) = \alpha$ if $\alpha > 0$, and $\varphi(a) > 0$ if $\alpha = 0$, and let P denote a maximal subfield of D containing a. Then $\Gamma_P \neq 0$, $\alpha \in \Gamma_P$, so by Theorem 1 there exists a valuation v_P of the field P having height one and associated with the homomorphism $\varphi_P: \Delta_P \to \Gamma_P = \varphi(\Delta_P)$. In particular, there exists a commutative diagram of the form:

$$\begin{array}{ccc} \Delta_P & \overset{\varphi_P}{\to} & \Gamma_P \\ \iota \downarrow & & \downarrow \theta_P \\ P^* & \overset{v_P}{\to} & \tilde{\Gamma}_P \end{array} \tag{1}$$

in which θ_P is a homomorphism of ordered groups. Since

$$[\tilde{\Gamma}_P : v_P(K^*)] \leq [P : K] < \infty \tag{2}$$

(cf. [Sc], Lemma 1.15) and v_P is nontrivial, there exists a $b \in K^*$ for which $v_P(b) < -\theta_P(\alpha)$, and then $b^m \in \Delta_K$ and $v_P(b^m) < -\theta(\alpha)$, implying that the set

$$\Delta_{-}(K, \alpha) = \{x \in \Delta_K \mid v_P(x) < -\theta_P(\alpha)\}$$

is nonempty. Let $v_0 = v_P \mid K^*$. To ascertain that Δ_K is open in K^*, we observe that since v_P is associated with φ_P and $\alpha \in \varphi_P(P^*)$, the subgroup Δ_P is v_P-adically open in P^* by Proposition 1, i.e. there exists a positive $\beta_P \in \tilde{\Gamma}_P$ such that

$$1 + \mathfrak{m}_{P,v_P}(\beta_P) \subset \Delta_P.$$

In view of (2) there exists a $\beta \in \Gamma_0 := v_P(K^*)$ with the property $\beta \geq \beta_P$, and then

$$1 + \mathfrak{m}_{K,v_0}(\beta) \subset \Delta_K, \tag{3}$$

proving the openness of Δ_K.

Now, to prove the proposition we will slightly generalize on the proof of Theorem 1. Let $\mathcal{A}$ be the subring of D generated by $\Delta_+(\alpha)$ and $\mathcal{O} = \{x \in D \mid x\mathcal{A} \subset \mathcal{A}\}$. Let $\tilde{\mathcal{O}}_M$ be the integral closure of $\mathcal{O} \cap M$ in M. The the same argument as in the proof of Theorem 1 shows that $\tilde{\mathcal{O}}_M$ is a valuation ring in M. Next, we observe that $\Delta_-(K, \alpha) \subset K^* \cap \Delta_-(\alpha)$; in particular $K^* \cap \Delta_-(\alpha) \neq \emptyset$. Combining this with Theorem 1, 2), we obtain that $\tilde{\mathcal{O}}_M \neq M$, so there exists a nontrivial valuation $\tilde{v}_M$ of M associated with $\tilde{\mathcal{O}}_M$. As we already mentioned in the proof of Theorem 2, since M is finitely generated, the value group $\tilde{v}_M(M^*)$ has finite height and therefore admits a surjection $\mu\colon \tilde{v}_M(M^*) \to \tilde{\Gamma}_M$ onto a group of height one. Then the valuation $v_M = \mu \circ \tilde{v}_M$ is as desired. Finally, we observe that both restrictions $v_M \mid K$ and $v_0 = v_P \mid K$ are valuations of K having height one and associated with the same homomorphism $\varphi_K\colon \Delta_K \to \Gamma_K$, so $v_M \mid K = v_0 \mid K$ by the last assertion of Theorem 2.

Proof of Theorem 3. The necessity follows from Proposition 1 exactly as in the proof of Theorem 1, so only sufficiency requires a proof. Let v_0 be as in the previous proposition, and $\beta \in \Gamma_0 = v_0(K^*)$ be chosen to satisfy (3). Also, let $H = \mathrm{Ker}(\Delta_K \xrightarrow{v_0} \Gamma_0)$. We observe that $H\Delta_-(K, \alpha) = \Delta_-(K, \alpha) \subset \Delta_-(\alpha)$.

Let K_{v_0} be the completion of K with respect to v_0. It is well-known that v_0 extends to any finite dimensional central division algebra $\mathcal{D}/K_{v_0}$ (cf., for example, [Sc], Ch.2, Thm.9). Thus, to prove that v_0 extends to a valuation of D it suffices to show that $A = D \otimes_K K_{v_0}$ is a division algebra. In any case, $A \simeq M_d(\mathcal{D})$ for some central division algebra $\mathcal{D}$ over K_{v_0} and some $d \geq 1$, and v_0 extends to a valuation u of $\mathcal{D}$. Our goal is to show that in fact $d = 1$.

We recall that given a vector space V over K_{v_0} of finite dimension l, one can define a norm $|| \ ||$ on V by picking a basis $a_1, \ldots, a_l$ and letting

$$|| \alpha_1 a_1 + \cdots \alpha_l a_l || = \max_{i=\overline{1,l}} | \alpha_i |_{v_0} \tag{4}$$

where $| \ |_{v_0}$ is the absolute value associated with v_0, and any two norms on V as a vector space over K_{v_0} are equivalent (cf. [L]). It follows that the topology and the notion of boundedness on A defined by a norm of the form (4) for any basis of A over K_{v_0} coincide with those associated with the norm

$$|| (a_{ij}) ||= \max_{i,j=\overline{1,d}} | a_{ij} |_u$$

constructed using some identification $A \simeq M_d(\mathcal{D})$ where $| \ |_u$ is the absolute value corresponding to u. It is well-known that for $a, b \in A$ the coordinates of ab are given by bilinear functions in terms of the coordinates of a and b, and for $a \in A^*$ the coordinates of a^{-1} are given by polynomials in terms of the coordinates of a and $(\mathrm{Nrd}_{A/K}(a))^{-1}$, which makes the operations of taking the product and taking the inverse continuous on A and A^*, respectively; in particular, A^* is a topological group. In what follows D will be endowed with the topology induced from A.

Now, we let $\mathcal{A}$ and $\mathcal{B}$ denote the subrings of D generated by $\Delta_+(\alpha)$ and $H\Delta_+(\alpha)$, respectively.

Lemma 5 *$\mathcal{B}$ is a proper open subring of D.*

Proof. Let $\mathbb{G} = \mathbf{GL}_{1,D}$ be the algebraic group associated with D^*. We claim that $\Delta_+(\alpha)$ is Zariski dense in $\mathbb{G}$. Indeed, since $\mathbb{G}$ is connected, D^* is dense in $\mathbb{G}$, and Δ has finite index in D^*, we conclude that Δ is Zariski dense in $\mathbb{G}$. Furthermore, if $\Theta = \{x \in \Delta \mid \varphi(x) \geq 0\}$, then $\Delta = \Theta \cup (\Theta)^{-1}$, implying

$$\mathbb{G} = \overline{\Theta} \cup \overline{(\Theta)}^{-1}$$

where the bar denotes the Zariski closure, hence $\overline{\Theta} = \mathbb{G}$. Finally, since $\Delta_+(\alpha) \neq \emptyset$ and $\Theta\Delta_+(\alpha) \subset \Delta_+(\alpha)$, we obtain the Zariski density of $\Delta_+(\alpha)$. It follows that one can pick a basis $a_1, \ldots, a_{n^2}$ of D over K contained in $\Delta_+(\alpha)$. Since $Ha_i \subset \mathcal{B}$ for any i and $1 + \mathfrak{m}_{K,v_0}(\beta) \subset H$, we obtain that

$$\sum_{i=1}^{n^2} \mathfrak{m}_{K,v_0}(\beta)a_i \subset \mathcal{B},$$

and the openness of $\mathcal{B}$ in D follows.

To complete the proof of the lemma, we will show that $\mathcal{B} \cap \Delta_-(K, \alpha) = \emptyset$. Assume the contrary, i.e. there exists an $x \in \Delta_-(K, \alpha)$ which admits a presentation of the form

$$x = \sum_i h_i t_i$$

with $h_i \in H$, $t_i \in \Delta_+(\alpha)$. Pick an i_0 satisfying $\varphi(h_{i_0}) = \min_i \varphi(h_i)$. Then

$$h_{i_0}^{-1}x = \sum_i (h_{i_0}^{-1}h_i)t_i. \tag{5}$$

But $\varphi(h_{i_0}^{-1}h_i) \geq 0$, so $(h_{i_0}^{-1}h_i)t_i \in \Delta_+(\alpha)$, and the right-hand side of (5) belongs to $\mathcal{A}$. On the other hand, in view of

$$h_{i_0}^{-1}x \in H\Delta_-(K,\alpha) \subset \Delta_-(\alpha),$$

and we obtain a contradiction with Theorem 1, 2).

Let $\bar{\mathcal{B}}$ denote the closure of $\mathcal{B}$ in A. Since $\mathcal{B}$ is open in D, we have $\bar{\mathcal{B}} \cap D = \mathcal{B}$, in particular $\bar{\mathcal{B}} \neq A$. Now, we are in a position to use the following lemma.

Lemma 6 *If $B \subset A$ is an open unbounded subring, then $B = A$.*

Proof. The openness of B means that there exists a nonnegative $\delta \in \bar{\Gamma} := u(\mathcal{D}^*)$ such that $M_d(\mathfrak{d}(\delta)) \subset B$ where

$$\mathfrak{d}(\delta) = \{x \in \mathcal{D}^* \mid u(x) > \delta\} \cup \{0\}.$$

On the other hand, since B is unbounded, one can pick a pair of indices $s, t \in \{1, \ldots, d\}$ satisfying the following property:

(*) for any $\epsilon \in \bar{\Gamma}$, $\epsilon > 0$, there exists a matrix $a(\epsilon) = (a_{ij}(\epsilon)) \in B$ with $u(a_{st}(\epsilon)) < -\epsilon$.

Let us fix *any* pair of indices s_0, t_0 with this property.

We will need some additional notations: Given a pair of indices $s, t \in \{1, \ldots, d\}$ and a subset $S \subset \mathcal{D}$, we let

$$R(s, S) = \{(a_{ij}) \in M_d(\mathcal{D}) \mid a_{ij} = 0 \text{ for } i \neq s, \text{ and } a_{sj} \in S \text{ for all } j\},$$

and

$$C(t, S) = \{(a_{ij}) \in M_d(\mathcal{D}) \mid a_{ij} = 0 \text{ for } j \neq t, \text{ and } a_{it} \in S \text{ for all } i\}.$$

Then

$$C(t_0, \mathfrak{d}(\delta)a_{s_0t_0}(\epsilon)) = C(s_0, \mathfrak{d}(\delta))a(\epsilon) \subset B$$

for any $\epsilon > 0$. But since $\mathfrak{d}(\delta)a_{s_0t_0}(\epsilon) \supset \mathfrak{d}(\delta - \epsilon)$ and

$$\cup_{\epsilon > 0}\mathfrak{d}(\delta - \epsilon) = \mathcal{D},$$

we obtain the inclusion

$$C(t_0, \mathcal{D}) \subset B. \tag{6}$$

Similarly,

$$R(s_0, \mathcal{D}) \subset B. \tag{7}$$

Then (6) shows that for any $s \in \{1, \dots, d\}$, the pair s, t_0 satisfies (*), and then (7) implies that $B = M_d(\mathcal{D})$, as claimed.

It follows from the lemma that $\bar{\mathcal{B}}$ is bounded. Let us show that this is impossible if $d > 1$. Indeed, from the decomposition $\Delta = \Theta \cup (\Theta)^{-1}$, where $\Theta = \{x \in \Delta \mid \varphi(x) \geq 0\}$, passing to the closure we obtain

$$\overline{\Delta} = \overline{\Theta} \cup \overline{(\Theta)^{-1}}$$

where now the bar denotes the closure in the topology defined by v_0. On the other hand, the index $[A^* : \overline{\Delta}]$ divides $m = [D^* : \Delta]$, implying that for any $a \in A^*$, either a^m or a^{-m} belongs to $\overline{\Theta}$. Now, suppose $d > 1$, pick an element $s \in \mathcal{D}^*$ such that $u(s) \neq 0$, and consider the element $t = \mathrm{diag}(s, s^{-1}, 1, \dots, 1) \in A^*$. After replacing s with s^{-1} if necessary, we may (and we will) assume that $t^m \in \bar{\mathcal{B}}$. On the other hand, $\Theta\mathcal{B} \subset \mathcal{B}$ implies that $\bar{\Theta}\bar{\mathcal{B}} \subset \mathcal{B}$. Let $b \in \bar{\mathcal{B}}$ be an element such that $b_{11}, b_{22} \neq 0$. Then the sequence $(t^m)^n b$, $n = 1, 2, \dots$, is contained in $\bar{\mathcal{B}}$ and is unbounded, contradicting the boundedness of $\bar{\mathcal{B}}$.

Thus, $d = 1$ and therefore v_0 extends to a valuation w of D with the value group $\tilde{\Gamma} := w(D^*)$. It remains to be shown that w is associated with the original homomorphism $\varphi\colon \Delta \to \Gamma$, i.e. there exists a homomorphism of ordered groups $\theta\colon \Gamma \to \tilde{\Gamma}$ for which the following diagram is commutative:

$$\begin{array}{ccc} \Delta & \xrightarrow{\varphi} & \Gamma \\ \iota\downarrow & & \downarrow\theta \\ D^* & \xrightarrow{w} & \tilde{\Gamma} \end{array}.$$

It suffices to show that for $x \in \Delta$, $\varphi(x) \geq 0$ implies $w(x) \geq 0$ as this will automatically give $w(\mathrm{Ker}\,\varphi) = \{0\}$, yielding a group homomorphism $\theta\colon \Gamma \to \tilde{\Gamma}$. So, fix an $x \in \Delta$ such that $\varphi(x) \geq 0$, and let $M \subset D$ be a maximal subfield containing x. According to Proposition 2 there exists a valuation v_M of M having height one and associated with $\varphi_M = \varphi \mid (\Delta \cap M)$, and moreover, $v_M \mid K = v_0$, i.e. v_M is an extension of v_0. On the other hand, $w \mid M$ is also an extension of v_0. Since $D \otimes_K K_{v_0}$ is a division algebra,

$M \otimes_K K_{v_0}$ is a field implying that the extension of v_0 to M is unique (cf. [Bo], §8, Prop. 2), hence $v_M = w \mid M$. Since v_M is associated with φ_M, we have $w(x) = v_M(x) \geq 0$, as required. Now that the existence of a valuation w associated with the homomorphism $\varphi: \Delta \to \Gamma$ has been established, the openness of Δ in D^* follows from Proposition 1.

Remark. Theorem 3 establishes the existence of a valuation associated with a homomorphism $\varphi: \Delta \to \Gamma$ in a more general situation than we previously considered in [R]. More precisely, the argument in [R] was given under the additional assumption that the homomorphism φ is constant on D^*-conjugacy classes in Δ, in particular, the group Γ is abelian. This assumption holds true for the homomorphism constructed in Segev's paper [S1], and might also be true for the homomorphisms arising in other applications. Since this assumption allows to simplify and shorten the argument, we decided to reproduce here the argument from [R] with minor changes.

So, we assume that $\varphi: \Delta \to \Gamma$ is constant on D^*-conjugacy classes in Δ and satisfies condition (1) §1. It is a consequence of Wedderburn's factorization theorem (cf. [Ro]) that for $x \in D^*$, the reduced norm $\mathrm{Nrd}_{D/K}(x)$ is the product of n conjugates of x, implying that for $x \in \Delta$, one has $\mathrm{Nrd}_{D/K}(x) \in \Delta$, and

$$\varphi(x^n) = \varphi(\mathrm{Nrd}_{D/K}(x)). \tag{8}$$

By Proposition 2 there exists a height one valuation $v_0: K^* \to \Gamma_0$ associated with the restriction $\varphi_K: \Delta \cap K \to \Gamma_K = \varphi(\Delta \cap K)$, so that $v_0 \mid_{\Delta\cap K} = \theta \circ \varphi \mid_{\Delta \cap K}$ for a certain homomorphism of ordered groups $\theta: \Gamma_K \to \Gamma_0$. Consider the following map:

$$w: D^* \to \tilde{\Gamma} := \frac{1}{n}\Gamma_0, \quad w(x) = \frac{1}{n} v_0(\mathrm{Nrd}_{D/K}(x)). \tag{9}$$

It follows from (8) that $n\Gamma \subset \Gamma_K$ implying that θ extends to a homomorphism of ordered groups $\tilde{\theta}: \Gamma \to \tilde{\Gamma}$, and then in view of (9) we have $w \mid_{\Delta} = \theta \circ \varphi$, i.e. w is associated with φ. So, it remains to prove that w is a valuation of D. Since w is a group homomorphism by construction, for the property $w(a+b) \geq \min(w(a), w(b))$ it suffices to verify the following implication:

$$w(a) \geq 0 \implies w(a+1) \geq 0 \tag{10}$$

for any $a \in D^*$, $a \neq -1$. Now, suppose we know that for any maximal subfield $P \subset D$ such that P/K is separable, $\tilde{P} := P \otimes_K K_{v_0}$ is a field, and will derive

(10) from this assumption. Since $w((1+a)^{p^r}) = w(1+a^{p^r})$ if $p = \operatorname{char} D > 0$, it suffices to prove (10) only for elements which are separable over K. Any such element a is contained in a maximal subfield P which is separable over K (cf. [Pi], §13.5). Since $\tilde{P}$ is a field, v_0 admits a unique extension u to P given by:

$$u(x) = \frac{1}{n} v_0(\mathrm{N}_{P/K}(x)), \tag{11}$$

where $\mathrm{N}_{P/K}$ is the usual norm in the field extension (cf. [L]). Using the fact that $\mathrm{Nrd}_{D/K}(x) = \mathrm{N}_{P/K}(x)$ for all $x \in P$ (cf. [DK], p. 28), we conclude from (9) and (11) that $u = w \mid P$. In other words, the restriction $w \mid P$ is a valuation, and (10) follows.

It remains to show that condition (1) §1 implies that for every maximal separable subfield $P \subset D$, $\tilde{P} = P \otimes_K K_{v_0}$ is a field. Suppose otherwise. Then $\tilde{P} \simeq \prod_{i=1}^r P_i$, where P_i/K_{v_0} is a finite extension of degree n_i, $n_1 + \cdots n_r = n$, and $r > 1$. (We recall that P_i's are precisely the completions of P with respect to different extension of v_0 to P (cf. [Bo], §8, Cor. 2), and $\tilde{P}$ gets endowed with the direct product of the topologies defined by those extensions; this topology coincides with the unique topology on $\tilde{P}$ as a finite dimensional vector spece over K_{v_0}.) We will assume (as we may) that $n_1 \leq n_i$ for all i (in particular, $n_1 \leq n/2$), and pick an element $x \in K_{v_0}$ such that $v_0(x) > n\tilde{\theta}(\alpha)$. We let

$$y = (x^{-1} + 1, x^{2m} + 1, \ldots, x^{2m} + 1) \in \tilde{P},$$

where $m = [D^* : \Delta]$, and then using weak approximation pick a sequence $z_1, \ldots, z_d, \ldots \in P$ converging to y. Observe that the function $f \colon \tilde{P} \to K_{v_0}$ defined by:

$$f(t) = \prod_{i=1}^{r} \mathrm{N}_{P_i/K_{v_0}}(t_i) \quad \text{for} \quad t = (t_1, \ldots t_r) \in \tilde{P},$$

is continuous and coincides with the norm $\mathrm{N}_{P/K}(t)$ on P. It follows that

$$f(z_d) \to f(y) = x^{-n_1}(x+1)^{n_1}(x^{2m}+1)^{n-n_1},$$

implying that $v_0(f(y)) < -nn_1\tilde{\theta}(\alpha) \leq -n\tilde{\theta}(\alpha)$, hence

$$v_0(f(z_d)) = v_0(\mathrm{N}_{P/K}(z_d)) = v_0(\mathrm{Nrd}_{D/K}(z_d)) < -n\tilde{\theta}(\alpha)$$

for all sufficiently large d. We have: $z_d^m \in \Delta$ and

$$v_0(\mathrm{Nrd}_{D/K}(z_d^m)) = n\theta(\varphi(z_d^m)) < -n\tilde{\theta}(\alpha),$$

and therefore $\varphi(z_i) < -\alpha$, i.e. $z_i^m \in \Delta_-(\alpha)$. On the other hand,

$$f(-z_i^m + 1) \to f(-y^m + 1) = (-(x^{-1}+1)^m + 1)^{n_1}(-(x^{2m}+1)^m + 1)^{n-n_1}.$$

We have:

$$-(x^{-1}+1)^m + 1 = x^{-m}a \quad , \quad -(x^{2m}+1)^m + 1 = x^{2m}b$$

where $a = -(1+x)^m + x^m$ and $b = -(1 + (x^{2m}+1) + \cdots + (x^2m+1)^{m-1})$, and therefore

$$f(-y^m + 1) = x^{m(2n-3n_1)} \cdot a^{n_1} \cdot b^{n-n_1}.$$

So, we conclude from $v_0(a) \geq 0$ and $v_0(b) \geq 0$ that $v_0(f(-y^m+1)) > 0$, implying that $v_0(f(-z_d^m+1)) = v_0(\mathrm{Nrd}_{D/K}(-z_d^m+1)) > 0$ for all sufficiently large d. This shows that those d's the inclusion $-z_d^m+1 \in \Delta_-(\alpha)$ is impossible as it would imply that

$$v_0(\mathrm{Nrd}_{D/K}(-z_d^m + 1)) = n\theta(\varphi(-z_d^m + 1)) \leq -n\tilde{\theta}(\alpha) \leq 0.$$

Thus, we obtain a contradiction with condition (1) §1, proving the claim.

5 The relation $\mathcal{R}_x$

Fix an element $x \in D^* - \Delta$ and associate with it a binary relation $\mathcal{R}_x$ on Δ as follows: For $a, b \in \Delta$ we write $a\mathcal{R}_x b$ if and only if for any $m \in \Delta$ such that $mx + b \in \Delta$ we necessarily have $mx + a \in \Delta$.

Lemma 7 *For any $x \in D^* - \Delta$, the relation $\mathcal{R}_x$ on Δ has the following properties:*

(i) *$\mathcal{R}_x$ is reflexive and transitive;*

(ii) *$a\mathcal{R}_x b$ implies $(na)\mathcal{R}_x(nb)$ and $(an)\mathcal{R}_x(bn)$ for any $n \in \Delta$;*

(iii) *$a\mathcal{R}_x b$ and $c\mathcal{R}_x d$ imply $(ac)\mathcal{R}_x(bd)$;*

(v) *$a\mathcal{R}_x b$ implies $b^{-1}\mathcal{R}_x a^{-1}$.*

Thus, $\mathcal{R}_x$ is a pre-order relation on Δ compatible with the group structure.

PROOF. (i) is obvious. If $mx+nb \in \Delta$ where $m \in \Delta$, then $(n^{-1}m)x+b \in \Delta$ which in view of our definition implies $(n^{-1}m)x+a \in \Delta$, and finally $mx+na \in \Delta$, proving that $(na)\mathcal{R}_x(nb)$. For $(an)\mathcal{R}_x(bn)$ we argue similarly observing that $mx+bn \in \Delta$ implies $(m(xn^{-1}x^{-1}))x+b \in \Delta$ and $m(xn^{-1}x^{-1}) \in \Delta$ as Δ is normal in D^*. Using (ii) in the set-up of (iii), we obtain that $(ac)\mathcal{R}_x(bc)$ and $(bc)\mathcal{R}_x(bd)$, so $(ac)\mathcal{R}_x(bd)$ by (i). Finally, multiplying $a\mathcal{R}_x b$ by a^{-1} on the left and b^{-1} on the right, we obtain $b^{-1}\mathcal{R}_x a^{-1}$. The lemma is proven.

Now, suppose we have been able to find an element $x \in D^* - \Delta$ so that the relation $\mathcal{R} = \mathcal{R}_x$ is linear. Let

$$\Delta'(\mathcal{R}) = \{a \in \Delta \mid a\mathcal{R}1\}.$$

Then $U(\mathcal{R}) = \Delta'(\mathcal{R}) \cap \Delta'(\mathcal{R})^{-1}$ is a normal subgroup of Δ, and $\mathcal{R}$ induces a linear order relation on $\Gamma = \Delta/U(\mathcal{R})$. If $\varphi\colon \Delta \to \Gamma$ is the canonical homomorphism, then $\Delta_-(\varphi)$ coincides with $\Delta_-(\mathcal{R}) = \Delta'(\mathcal{R}) - U(\mathcal{R})$. Furthermore, we claim that Γ is always nontrivial. Indeed, otherwise we would have $\Delta'(\mathcal{R}) = \Delta$. It follows from $D = \Delta - \Delta$ that there exists $m \in \Delta$ such that $mx+1 \in \Delta$, so $\Delta'(\mathcal{R}) = \Delta$ would imply that $mx + \Delta \subset \Delta$, and consequently $x + \Delta \subset \Delta$. Then $1 + \Delta x^{-1} \subset \Delta x^{-1}$, and therefore $x^{-1} + \Delta \subset \Delta x^{-1}$. This means that there is no $n \in \Delta$ such that $x^{-1} + n \in \Delta$, contradicting $D = \Delta - \Delta$. Summarizing all this, we obtain the following.

Proposition 3 *Suppose that for an element $x \in D^* - \Delta$ the relation $\mathcal{R} = \mathcal{R}_x$ is linear and*

$$\Delta_-(\mathcal{R}) + 1 \subset \Delta_-(\mathcal{R}). \tag{1}$$

Then there exists a homomorphism $\varphi\colon \Delta \to \Gamma$ onto a nontrivial totally ordered group such that $\Delta_- + 1 \subset \Delta_-$ (i.e. condition (1) §1 is satisfied for $\alpha = 0$).

REMARK. The relation $\mathcal{R}_x$ is slightly different from the relation $\mathcal{S}_x$ which can be obtained from Segev's construction (however which does not appear in [S1] explicitly): $a\mathcal{S}_x b$ means that whenever $m(g^{-1}xg)+b \in \Delta$ for $m \in \Delta$, $g \in D^*$, we always have $m(g^{-1}xg) + a \in \Delta$. An important advantage of $\mathcal{S}_x$ over $\mathcal{R}_x$ is that $\mathcal{S}_x$ is conjugation invariant by construction. On the other hand, $\mathcal{R}_x$ is a bit easier to analyze which might play a role in future applications.

6 Verification of condition (1) §5: fragments of Segev's argument

We fix a normal subgroup $\Delta \subset D^*$ of finite index, and for any $a \in D^*$ we let a^* denote its image in $G = D^*/\Delta$. The two most important ingredients of Segev's argument are: the set

$$N(a) = \{n \in \Delta \mid a + n \in \Delta\}$$

associated with any element $a \in D^* - \Delta$, and the commuting graph $\mathfrak{G}$ of G, i.e. the nonoriented graph whose vertex set is $G - \{1^*\}$ and in which two vertices a^* and b^* are connected if and only if the elements a^* and b^* commute in G. We let d denote the distance function of $\mathfrak{G}$. The following observation (first made in [RPo], see the proof of Proposition 7.1) will be used repeatedly: for any $a \in D^* - \Delta$ and any $n \in \Delta - N(a)$ the elements a^* and $(a+n)^*$ commute in G, hence $d(a^*, (a+n)^*) \leq 1$ (indeed, $(a+n)^* = (an^{-1}+1)^*$, $a^* = (an^{-1})^*$, and the elements an^{-1} and $an^{-1}+1$ commute in D^*). In other words, if $a, b \in D^* - \Delta$ and either $a+b$ or $a-b$ belongs to Δ, then $d(a^*, b^*) \leq 1$ (we recall that by our assumption $-1 \in \Delta$).

The crucial role in Segev's argument is played by the fact that if for $a, b \in D^* - \Delta$, the elements a^* and b^* are sufficiently far apart in $\mathfrak{G}$, then it is possible to establish certain inclusions between $N(a)$, $N(b)$, and $N(a+b)$.

Lemma 8 ([S1], 2.3 and 3.9) *Suppose $a, b, c \in D^* - \Delta$ are related by the equation $a + b = c$. Then*

(i) *if $d(a^*, b^*) > 2$, then $N(c) \subset N(a) \cap N(b)$;*

(ii) *if $d(a^*, b^*) > 2$ and $d(a^*, c^*) > 2$, then $N(b) = N(c) \subset N(a) \cap N(-a)$;*

(iii) *if $d(a^*, b^*) > 4$, then either $N(a) = N(c) \subset N(b) \cap N(-b)$, or $N(b) = N(c) \subset N(a) \cap N(-a)$;*

(iv) *if $d(a^*, b^*) > 2$ and $d(a^*, (a^{-1}b)^*) > 3$, then either $a^* = c^*$, in which case $N(a) = N(c) \subset N(b) \cap N(-b)$, or $N(b) = N(c) \subset N(a) \cap N(-a)$.*

Proof. (i) Suppose there exists an $n \in N(c) - (N(a) \cap N(b))$, and suppose for definiteness that $a \notin N(a)$. From the equation

$$c + n = (a + n) + b.$$

we conclude that $d((a+n)^*, b^*) \leq 1$ as $c+n \in \Delta$. Since $d(a^*, (a+n)^*) \leq 1$, we obtain $d(a^*, b^*) \leq 2$ - a contradiction.

(ii) By (i), $N(c) \subset N(a) \cap N(b)$. Since $b = c - a$, (i) implies that $N(b) \subset N(c) \cap N(-a)$, and (ii) follows.

(iii) Since at least one of the distances $d(a^*, c^*)$ or $d(b^*, c^*)$ is > 2, this follows immediately from (ii).

(iv) If $c^* = a^*$, i.e. $1 + a^{-1}b \in \Delta$, then $d(b^*, c^*) > 2$, and it follows from (ii) that $N(a) = N(c) \subset N(b) \cap N(-b)$. So, we may assume that $1 + a^{-1}b \notin \Delta$. Suppose there exists an $n \in N(b) - N(c)$. Then $(a+b+n)^*$ commutes with a^* and $(a+b)^*$, hence also with $(1+a^{-1}b)^*$. It follows that

$$a^* \ , \ (a+b+n)^* \ , \ (1+a^{-1}b)^* \ , \ (a^{-1}b)^*$$

is a path in $\mathfrak{G}$, implying that $d(a^*, (a^{-1}b)^*) \leq 3$ - a contradiction. Thus, $N(b) \subset N(c)$ which in combination with (i) implies that

$$N(b) = N(c) \subset N(a). \tag{1}$$

Now, let $c_1 = (-a) + b$. Then $c_1 \notin \Delta$ as otherwise we would have $d((-a)^*, b^*)$ $= d(a^*, b^*) \leq 1$. Suppose first that $c_1^* = (-a)^*$. Then as we have seen in the beginning, $N(-a) = N(c_1) \subset N(b) \cap N(-b)$. In combination with (1) this implies $N(c) = N(\pm a) = N(\pm b)$, and (iv) follows. If $c_1^* \neq (-a)^*$, then arguing as above we obtain $N(b) = N(c_1) \subset N(-a)$, and again (iv) follows.

The proof of the lemma is now complete.

Part (iv) of the lemma motivates the following.

Definition. ([S1], §4) We say that $a^*, b^* \in \mathfrak{G}$ (or their lifts $a, b \in D^*$) form a *balancing pair* if each of the following five pairs of vertices

$$(a^*, b^*) \quad , \quad (a^*, a^*b^*) \quad , \quad (b^*, a^*b^*) \quad , \quad (a^*, (a^{-1}b)^*) \quad , \quad (b^*, (a^{-1}b)^*)$$

is at a distance of at least three. $\mathfrak{G}$ (or G) is said to be *balanced* if it contains at least one balancing pair.

It is easy to see that if $a^*, b^* \in \mathfrak{G}$ is a balancing pair, then so is b^*, a^*. Indeed, it suffices to observe that

$$d(b^*, b^*a^*) = d(b^*, a^*b^*), \quad \text{etc.}$$

as the pair (b^*, b^*a^*) is conjugate to the pair (b^*, a^*b^*) by the element b^*, etc. (cf. [S1], 4.2). Also, any pair of the form $((a^*)^{\pm 1}, (b^*)^{\pm 1})$ is balancing.

Now, we are able to formulate the main result of this section.

Theorem 4 *Suppose the commuting graph $\mathfrak{G}$ of D/Δ^* either has diameter > 4, or is balanced. Then there exists an $x \in D^*$ such that the relation $\mathcal{R} = \mathcal{R}_x$ is linear and the corresponding $\Delta_- = \Delta' - (\Delta' \cap (\Delta')^{-1})$, where $\Delta' = \{z \in \Delta \mid z\mathcal{R}1\}$, satisfies $\Delta_- + 1 \subset \Delta_-$.*

PROOF. We will need the following two notations from [S1]. For $x \in D^* - \Delta$, we let

$$P(x) = \{mx \mid m \in \Delta \text{ and } mx + 1 \in \Delta\}.$$

Then the elements $z \in \Delta$ satisfying $z\mathcal{R}_x 1$ can be characterized as those with the property $z + a \in \Delta$ for all $a \in P(x)$. We also let

$$O(x) = \{x_1 \in \Delta x \mid -1 \notin N(x_1) \cup N(x_1^{-1})\}.$$

Now, the argument splits into two cases.

CASE 1. *D^* contains elements x, y for which either $d(x^*, y^*) > 4$, or which form a balancing pair and for one of them, say x, we have $O(x) = \emptyset$.*

Lemma 9 *Let $\Delta'' = \Delta - \Delta'$ and suppose that*

$$1 \pm \Delta'' \subset \Delta'. \tag{2}$$

Then

1) *$\mathcal{R}$ is a linear order relation;*
2) *for $\Delta_- = \Delta' - U$, where $U = \Delta' \cap (\Delta')^{-1}$, we have $\Delta_- + 1 \subset \Delta_-$.*

PROOF. For 1), we need to show that $\Delta' \cup (\Delta')^{-1} = \Delta$. Suppose there exists a $z \in \Delta - (\Delta' \cup (\Delta')^{-1})$. Then because of (2), both elements $z+1$ and $z^{-1}+1$ belong to Δ'. Moreover, in view of

$$(z+1)^{-1} + (z^{-1}+1)^{-1} = 1,$$

it follows from (2) that one of the elements $(z+1)^{-1}$ or $(z^{-1}+1)^{-1}$ also has to belong to Δ'. But then at least one of

$$z = (z+1)(z^{-1}+1)^{-1} \quad \text{or} \quad z^{-1} = (z^{-1}+1)(z+1)^{-1}$$

belongs to Δ' - a contradiction.

If $z \in \Delta_-$, then $z^{-1} \in \Delta''$, implying $1 + z^{-1} \in \Delta'$. It follows that $z + 1 = z(1 + z^{-1}) \in \Delta'$. If we assume, however, that $(z + 1)^{-1} \in \Delta'$, we would have

$$z^{-1} = (z^{-1} + 1)(z + 1)^{-1} \in \Delta',$$

a contradiction, proving 2).

In view of Lemma 8, (iii) and (iv), it follows from our assumptions on x and y that for any $a \in \Delta x$, $b \in \Delta y$ we have one of the inclusions $N(a) \supset N(b)$, or $N(a) \subset N(b)$. We claim that by switching x and y if necessary we can ensure also the following.

(**) For any $a \in P(x)$, there exists a $b \in P(y)$ such that $N(a) \supset N(b)$.

Indeed, the negation of (**) means that there exists an $a \in P(x)$ such that for any $b \in P(y)$ we have $N(a) \not\supset N(b)$, in which case $N(a) \subset N(b)$, and (**) holds with x and y interchanged. Observe now that the inclusion in (**) can be upgraded to

$$N(b) \subset N(a) \cap N(-a). \tag{3}$$

Indeed, if (3) is false, then according to Lemma 8, (iii) and (iv), we would have $N(a) \subset N(b) \cap N(-b)$. Since $N(b) \subset N(a)$, this would imply $N(\pm a) = N(\pm b)$, in particular, yielding (3).

So, we suppose that (**), and consequently (3), holds. Then picking for an arbitrary $a \in P(x)$ an element $b \in P(y)$ satisfying (3), we obtain

$$1 \in N(b) \subset N(a) \cap N(-a),$$

which implies that $-1 \in N(a)$. Since this is true for any $a \in P(x)$, we conclude that $-1 \in \Delta'$. This implies that $-\Delta' = \Delta'$, and therefore also $-\Delta'' = \Delta''$.

Proposition 4 (cf. [S1], proof of Theorem 3.17) *Suppose that $a \in \Delta x$, $b \in \Delta y$ satisfy (3). Then for any $n \in \Delta - N(a)$, one has*

$$N(b) \subset N(a + n) \cap N(b + n). \tag{4}$$

Proof. Let $c_1 = a + b$. It follows from Lemma 8(i) that $N(c_1) = N(b)$. On the other hand, from

$$c_1 = (a + n) + (b - n)$$

one concludes that

$$N(c_1) \subset N(a+n) \cap N(b-n). \tag{5}$$

Indeed, we first observe that $b-n \notin \Delta$, as otherwise we would have $-n \in N(b)$, and therefore in view of (3), $n \in N(a)$ - a contradiction. Now, if $d(a^*, b^*) > 4$ we obtain from $d((a+n)^*, a^*) \leq 1$ and $d((b-n)^*, b^*) \leq 1$ that $d((a+n)^*, (b-n)^*) > 2$, and (5) follows from Lemma 8(i).

In the balanced case, we observe that if $O(x) = \emptyset$, then also

$$\{x_1 \in \Delta x \mid 1 \notin N(x_1) \cup N(x_1^{-1})\} = \emptyset.$$

Since $n \notin N(a)$, we have $1 \notin N(n^{-1}a)$, implying that $1 \in N(a^{-1}n)$. This means that $1 + a^{-1}n \in \Delta$, and therefore $a + n = am$ for some $m \in \Delta$. Then $(a+n)^* = a^*$, and therefore $d((a+n)^*, (b-n)^*) = d(a^*, (b-n)^*) > 2$. So, (5) follows from Lemma 8(i). (If $O(y) = \emptyset$, then the same argument shows that $b - n = bm$, and again $d((a+n)^*, (b-n)^*) = d((a+n)^*, b^*) > 2$.)

Similarly, for $c_2 = a - b$ we have $N(c_2) = N(-b)$. Arguing as above, we see that neither of $a+n$ and $b+n$ belongs to Δ, and $d((a+n)^*, (b+n)^*) > 2$. So, from

$$c_2 = (a+n) - (b+n).$$

we obtain the inclusion

$$N(c_2) = N(-b) \subset N(a+n) \cap N(-(b+n)),$$

which in combination with (5) readily yields (4).

Now, suppose $n \in \Delta''$. This means that there exists an $a \in P(x)$ such that $n \notin N(a)$. Pick a $b \in P(y)$ satisfying (3). Then by Proposition 4 we have the inclusion (4) which in view of $1 \in N(b)$ implies that both $a + n + 1$ and $b + n + 1$ belong to Δ. If $n + 1 \notin \Delta$, we would have

$$d(a^*, (n+1)^*) \leq 1 \quad \text{and} \quad d(b^*, (n+1)^*) \leq 1,$$

and therefore $d(a^*, b^*) \leq 2$ - a contradiction. Thus, $n + 1 \in \Delta$, proving that $1 + \Delta'' \subset \Delta$. This implies, in particular, that $1 + b \in \Delta'$ as otherwise we would have $-(1+b) \in \Delta''$, and therefore $-b = 1 - (1+b) \in \Delta$ - a contradiction. It follows that for any $z = mx$ with $m \in \Delta$ such that $z + 1 \in \Delta$, we have $z + 1 + b \in \Delta$, i.e. $z + 1 \in N(b)$. Now we conclude from (4) that

$$a + (z + 1 + n) \quad \text{and} \quad b + (z + 1 + n) \ \in \Delta.$$

Again, if $z+1+n \notin \Delta$, we would have

$$d(a^*, (z+1+n)^*) \leq 1 \quad \text{and} \quad d(b^*, (z+1+n)^*) \leq 1,$$

and therefore $d(a^*, b^*) \leq 2$ - a contradiction. Thus, $z+(n+1) \in \Delta$, proving that $(n+1)\mathcal{R}_x 1$, i.e. $n+1 \in \Delta'$. This verifies condition (2) in Lemma 9, and application of the latter completes the proof.

Case 2. *There exists a balancing pair $x, y \in D^*$ such that both $O(x)$ and $O(y)$ are nonempty.*

Replacing x and y with appropriate elements from $x\Delta$ and $y\Delta$ respectively, we may assume that

$$-1 \notin N(x) \cup N(x^{-1}) \quad \text{and} \quad 1 \notin N(y) \cup N(y^{-1}). \tag{6}$$

The crucial properties of these elements are described in the following proposition.

Proposition 5 (cf. [S1], 4.6) *Let $x, y \in D^* - \Delta$ be a pair of balancing elements satisfying (6). Then*

1) $N(x) = N(y)$;

2) if $a \in \Delta x$ and $1 \notin N(a)$, then $N(a) \subset N(x)$;

3) if $a \in \Delta x$ and $1 \in N(a)$, then $N(x) \subset N(a)$.

We need the following.

Lemma 10 ([S1], 3.13) *Suppose $x \in D^* - \Delta$ has the property: $-1 \notin N(x) \cup N(x^{-1})$, and $y \in D^* - \Delta$ is such that $d(x^*, y^*) > 3$ and $d(x^*, (x^{-1}y)^*) > 3$. Then for any $b \in \Delta y$ with the property $1 \notin N(b)$, one has $N(b) \subset N(x)$.*

Proof. Assume the contrary and pick an $s \in N(b) - N(x)$. Then in the sequence

$$x^* \ , \ (x+b+s)^* \ , \ (1+x^{-1}b)^* \ , \ (x^{-1}b)^*$$

any two juxtaposed elements commute (observe that $(x+b+s)^*$ commutes with x^* and $(x+b)^*$, hence with $(1+x^{-1}b)^*$). Since $d(x^*, (x^{-1}b)^*) > 3$, one of the elements $x+b+s$ or $1+x^{-1}b$ must belong to Δ.

Suppose $1 + x^{-1}b \in \Delta$. Then $x^{-1}(b+1) + (-x^{-1}+1) \in \Delta$, implying that $(x^{-1}(b+1))^*$ and $(x^{-1}-1)^*$ commute, and therefore so do $(b+1)^*$ and $(x^{-1}-1)^*$. It follows that

$$x^* \ , \ (x^{-1}-1)^* \ , \ (b+1)^* \ , \ b^*$$

is a path in $\mathfrak{G}$, contradicting $d(x^*, y^*) > 3$.

Thus $1 + x^{-1}b \notin \Delta$ (in other words, $x^* \neq (x+b)^*$), so $x + b + s \in \Delta$, i.e. $s \in N(x+b)$. It follows from Lemma 8(iv) that $N(x+b) = N(b) \subset N(x)$, implying $s \in N(x)$ - a contradiction.

Proof of Proposition 5 In view of (6), it follows from the previous lemma that $N(y) \subset N(x)$. Changing x to $-x$ and y to $-y$, we can rewrite (6) as follows:

$$-1 \notin N(-y) \cup N((-y)^{-1}) \ \text{ and } \ 1 \notin N(-x) \cup N((-x)^{-1}).$$

Then the same argument shows that $N(-x) \subset N(-y)$, i.e. $N(x) \subset N(y)$. Thus, $N(x) = N(y)$. Now, the previous lemma in conjunction with 1) immediately implies 2). For 3), we observe that according to Lemma 8(iv), we have one of the inclusions: $N(a) \subset N(y)$ or $N(y) \subset N(a)$. But since $1 \notin N(y)$, the first one is impossible, and we obtain $N(x) = N(y) \subset N(a)$.

Remark. The following consequence of Proposition 5, though not needed for further argument, is worth mentioning. Since x, y^{-1} and x^{-1}, y are also balancing pairs satisfying (6), we obtain from 1) that $N(x^{\pm 1}) = N(y^{\pm 1})$, so (6) can actually be strengthened to:

$$\pm 1 \notin N(x) \cup N(x^{-1}) \cup N(y) \cup N(y^{-1}).$$

It follows that $-x, y$ is also a balancing pair satisfying (6), and using Proposition 5, 1), one more time we eventually obtain that

$$N(\pm x^{\pm 1}) = N(\pm y^{\pm 1}).$$

Let $\mathcal{S} = \{z \in \Delta \mid zN(x) \subset N(x)\}$.

Lemma 11 *$\Delta' = \mathcal{S}$, and $\Delta_- = N(x)$.*

PROOF. Suppose $z \in \mathcal{S}$. If $z \notin \Delta'$, then there exists an $m \in \Delta$ such that $mx + 1 \in \Delta$, but $mx + z \notin \Delta$. This implies that $z^{-1}mx + 1 \notin \Delta$, i.e. $1 \notin N(z^{-1}mx)$. Then according to Proposition 5, 2), $N(z^{-1}mx) \subset N(x)$, so $N(mx) \subset N(zx) \subset N(x)$, and therefore $1 \in N(mx) \subset N(x)$ - a contradicton. Conversely, suppose $z \in \Delta'$, but $zN(x) \not\subset N(x) = N(y)$. It follows from Lemma 8(iv) that then $N(x)$ is a proper subset of $zN(x)$ which in view of Proposition 5, 3), means that $1 \in N(zx)$. In other words, $1 + zx \in \Delta$, i.e. $z^{-1}+x \in \Delta$. But since $z \in \Delta'$, we have $1\mathcal{R}z^{-1}$, so the latter implies $1+x \in \Delta$, i.e. $1 \in N(x)$ - a contradiction. Now, we can conclude that Δ_- coincides with the set of those $z \in \Delta$ for which $zN(x)$ is properly contained in $N(x)$. This is equivalent to $N(x)$ being properly contained in $z^{-1}N(x)$ which according to Proposition 5, 2) and 3), is equivalent to $1 \in z^{-1}N(x)$, i.e. $z \in N(x)$.

It follows from Lemma 8(iv) that for any $z \in \Delta$, one always has one of the inclusions $\subset$ or $\supset$ between $zN(x) = N(zx)$ and $N(y) = N(x)$, which in view of Lemma 11 implies that $\mathcal{R} = \mathcal{R}_x$ is a linear relation on Δ with $\Delta_- = N(x)$. So, it remains to verify that

$$\Delta_- + 1 \subset \Delta_-. \tag{7}$$

We first observe that

$$N(x) \subset N(x+1) \quad \text{and} \quad N(y) \subset N(y+1). \tag{8}$$

We will prove the first inclusion; the argument for the second one is exactly the same. Suppose $m \in N(x) - N(x+1)$. It follows from Lemma 8(iv) and Proposition 5, 1), that $N(x+y) = N(x) = N(y)$; in particular, $m \in N(x+y)$. From

$$x + 1 + m = (x + y + m) + (-y + 1),$$

we conclude that $(x + 1 + m)^* \neq 1^*$ commutes with $(-y + 1)^*$. Since x and y^{-1} also form a balancing pair satisfying (6), the same argument applies to it yielding that $(x+1+m)^*$ commutes with $(-y^{-1}+1)^*$ as well. So, $(x+1+m)^*$ commutes with $y^* = (-y + 1)^*(-y^{-1} + 1)^{*-1}$. It follows that

$$x^* \ , \ (x+1)^* \ , \ (x+1+m)^* \ , \ y^*$$

is a path in the commuting graph, implying that $d(x^*, y^*) \leq 3$ - a contradiction, proving (8).

Now, let $m \in \Delta_- = N(x) = N(y)$. Then in view of (8)

$$x + 1 + m \in \Delta, \tag{9}$$

implying that x^* and $(1+m)^*$ commute. Similarly, y^* and $(1+m)^*$ also commute. So, the assumption $1 + m \notin \Delta$ would imply that $d(x^*, y^*) \leq 2$ - a contradiction. Thus, $1 + m \in \Delta$ which in view of (9) implies that in fact $1 + m \in N(x) = \Delta_-$, proving (7) and completing the proof of Theorem 5.

REMARK. Condition (2) in Lemma 9 is essentially equivalent to "U-Hypothesis" in [S1], so Lemma 9 can be interpreted as a statement claiming that the truth of U-Hypothesis implies Theorem 4. The rest of the argument in Case 1 almost verbatim reproduces §3 from [S1] where Segev validates U-Hypothesis in the case under consideration; we just deleted the material irrelevant as far as Theorem 4 is concerned. On the contrary, consideration of Case 2 is not based on U-Hypothesis which creates some shortcut compared to Segev's argument. So, it would be of some interest to see if similar modifications are possible in Case 1, too.

7 Main Theorem

Putting together Theorems 3 and 4, and Proposition 3, we obtain the following.

Theorem 5 *Let D be a finite dimensional algebra over a finitely generated field K. If $\Delta \subset D^*$ is a normal subgroup of finite index such that the commuting graph of the quotient D^*/Δ either has diameter > 4 or is balanced, then Δ is open in D^* with respect to a certain nontrivial valuation of D of height one.*

We will show in the next section how this theorem can be used to eliminate certain finite groups as possible quotients of D^*, in particular, to recover the result of Segev [S1]. However, it is important to point out that the theorem enables one to derive not only negative, but also positive information on the finite quotients of D^*. Namely, there are finite solvable groups that can be obtained as a quotient of D^* for an appropriate D and, on the other hand, satisfy the assumptions of Theorem 5. Then the congruence subgroup information furnished by Theorem 5 in principle allows to describe **all** situations in which such groups do occur as quotients of D^*. We will discuss some results of this kind elsewhere, limiting ourselves here to one simple example of such a group.

Let D be a quaternion division algebra over the field $K = \mathbb{Q}_2$ of 2-adic numbers. The 2-adic valuation extends from K to D, and we let $\mathcal{O}$ and $\mathfrak{P}$ denote the corresponding valuation ring and the valuation ideal. Let $\Delta \subset D^*$ denote the subgroup generated by K^* and $1+\mathfrak{P}$. Then Δ is obviously normal in D^*, and we claim that

$$D^*/\Delta \simeq S_3.$$

First, we observe that the order of D^*/Δ is 6. Indeed, letting $U = \mathcal{O}^*$, we will have $\Delta U = \langle \Pi^2, U \rangle$, where $\Pi \in \mathfrak{P}$ is a prime element, and therefore has index 2 in D^*. On the other hand, $\Delta U/\Delta \simeq U/(U \cap \Delta)$ has order 3 as

$$U \cap \Delta = (U \cap K^*)(1 + \mathfrak{P}) = 1 + \mathfrak{P}$$

(as the residue field of K is $\mathbf{F}_2$) and $U/(1 + \mathfrak{P}) \simeq \mathbf{F}_4^*$. It remains to observe that conjugation by Π induces on the latter quotient a nontrivial automorphism of $\mathbf{F}_4/\mathbf{F}_2$, hence D^*/Δ is nonabelian. We observe that in this example Δ is open in D^* with respect to the 2-adic valuation *by construction.* However, Theorem 5 indicates that this is not accidental: since S_3 has a disconnected commuting graph (because the centralizer of (123) coincides with the cyclic subgroup $\langle (123) \rangle$), whenever $D^*/\Delta \simeq S_3$ where D is a finite dimensional division algebra over a finitely generated field, Δ is *always* open with respect to a nontrivial valuation of K!

Of course, the field $K = \mathbb{Q}_2$ in the previous example is not finitely generated, however the division algebra D considered there is obtained from the algebra $\mathbb{H}$ of the Hamiltonian quaternions over the rationals by extending scalars from $\mathbb{Q}$ to $\mathbb{Q}_2$, and it follows from the weak approximation theorem that $\mathbb{H}/(\mathbb{H} \cap \Delta) \simeq S_3$. More generally, the following statement shows that as far as the finite quotients are concerned, we can always limit ourselves to division algebras over finitely generated fields.

Lemma 12 *Let D be a finite dimensional division algebra (not necessarily central) over a field K. Given a surjective homomorphism $\theta\colon D^* \to G$ onto a finite group G, there exists a finitely generated subfield $k \subset K$ and a division k-subalgebra $\tilde{D} \subset D$ such that $D = \tilde{D} \otimes_k K$ and the restriction $\theta \mid_{\tilde{D}^*} \colon \tilde{D}^* \to G$ is surjective.*

Indeed, let $\{a_i\}$ be a basis of D over K and let k denote the subfield of K obtained by adjoining to the prime subfield $P \subset K$ the structure constants for this basis (which are the elements $c_{ij}^l \in K$ from the product relations $a_i a_j = \sum_l c_{ij}^l a_l$), and also all coordinates of a certain complete system of representatives of cosets $D^*/\mathrm{Ker}\,\theta$. Let $\tilde{D}$ be the k-linear span of $\{a_i\}$. The fact that $c_{ij}^l \in k$ ensures that $\tilde{D}$ is closed under multiplication, hence a k-algebra satisfying $D = \tilde{D} \otimes_k K$. Being a finite dimensional algebra without zero divisors, $\tilde{D}$ is a division algebra. Finally, by our construction $D^* = \tilde{D}^*\mathrm{Ker}\,\theta$, so the restriction $\theta\,|_{\tilde{D}^*} \colon \tilde{D}^* \to G$ is surjective.

8 Elimination by reduction

In this section we will describe a strategy, based on Theorem 5, for eliminating some finite groups as possible quotients of D^*. The idea, described already in [R], is to replace the original division algebra D with the residue algebra $\bar{D}$ relative to the valuation constructed in Theorem 5 and to reiterate this process.

Let $\mathfrak{S}$ be a class of finite groups satisfying the following properties:

(i) any group $G \in \mathfrak{S}$ is nonsolvable (in particular, the trivial group $\{e\}$ is not in $\mathfrak{S}$);

(ii) if $G \in \mathfrak{S}$ and $N \subset G$ is a normal subgroup with an abelian quotient G/N, then N has a quotient belonging to $\mathfrak{S}$;

(iii) if $G \in \mathfrak{S}$ and $M \subset G$ is a solvable normal subgroup, then G/M has a quotient belonging to $\mathfrak{S}$;

(iv) given a finite dimensional division algebra D over a finitely generated field K and a homomorphism $D^* \xrightarrow{\theta} G$, where $G \in \mathfrak{S}$, there exists a height one valuation v of D such that $\mathrm{Ker}\,\theta$ is v-adically open.

While conditions (i)–(iii) are self-explanatory, condition (iv) is satisfied if every group $G \in \mathfrak{S}$ either has diameter > 4, or is balanced (cf. Theorem 5).

Theorem 6 *Let $\mathfrak{S}$ be a class of finite groups satisfying conditions (i)–(iv) above. Then for any finite dimensional division algebra D, the multiplicative group D^* does not have finite quotients belonging to $\mathfrak{S}$.*

PROOF. Assume the contrary. Then according to Lemma 12 there exists a finite dimensional division algebra D over a finitely generated field K for which there exists an epimorphism $\theta\colon D^* \to G$ onto a group $G \in \mathfrak{S}$. Using property (iv) of $\mathfrak{S}$, we pick a valuation $v\colon D^* \to \tilde{\Gamma}$ of D such that $T = \operatorname{Ker}\theta$ is v-adically open, i.e. there exists an $\alpha > 0$ in $\tilde{\Gamma}$ with the property

$$1 + \mathfrak{m}(\alpha) \subset T \tag{1}$$

in the standard notations (cf. §1). Let $\mathcal{O}$ be the corresponding valuation ring with the valuation ideal $\mathfrak{m}$, and $\bar{D} = \mathcal{O}/\mathfrak{m}$ be the corresponding residue algebra. We claim that its multiplicative group $\bar{D}^*$ also has a quotient belonging to $\mathfrak{S}$. Indeed, let $U = O^*$ be the group of v-adic units in D, and $M = (T \cap U)(1 + \mathfrak{m})$. Then $H = U/M$ is a quotient of $\bar{D}^* \simeq U/(1 + \mathfrak{m})$, and it suffices to show that H has a quotient belonging to $\mathfrak{S}$. First, we observe that the group $L = U/(T \cap U)$ is isomorphic to TU/T which embeds into $G = D^*/T$ as a normal subgroup with abelian quotient (since $D^*/U \simeq \tilde{\Gamma}$ is abelian). So, applying property (ii), we conclude that L has a quotient belonging to $\mathfrak{S}$. To prove the existence of such a quotient for H, we need the following.

Lemma 13 *$R = M/(T \cap U)$ is a solvable group.*

PROOF. There exists a complete system of coset representatives for $M/(T \cap U)$ consisting of elements of the form $1 + x_i$ where $x_i \in \mathfrak{m}$. Let $\beta = \min\limits_{i=\overline{1,d}} v(x_i)$, $\beta > 0$. Then $M = (T \cap U)(1 + \bar{\mathfrak{m}}(\beta))$ where

$$\bar{\mathfrak{m}}(\beta) = \{x \in D^* \mid v(x) \geq \beta\} \cup \{0\}.$$

It is easy to verify that for any $\beta > 0$, $\bar{\mathfrak{m}}(\beta)$ is a two-sided ideal of $\mathcal{O}$ and that $1 + \bar{\mathfrak{m}}(\beta)$ is a normal subgroup of D^*. Moreover, a standard computation shows that

$$[1 + \bar{\mathfrak{m}}(\beta), 1 + \bar{\mathfrak{m}}(\beta)] \subset 1 + \bar{\mathfrak{m}}(2\beta),$$

implying that for any integer $n > 0$, the n-th term of the derived series of $1 + \bar{\mathfrak{m}}(\beta)$ is contained in $1 + \bar{\mathfrak{m}}(2^n\beta)$. Now, since the value group $\tilde{\Gamma}$ has height one, there exists an $n > 0$ such that $2^n\beta > \alpha$, and then it follows from (1) that the n-th term of the derived series of $M/(T \cap U)$ is the trivial group, proving the lemma.

Now, if L/V is a quotient of L belonging to $\mathfrak{S}$, then L/RV is a quotient of $H = L/R$ and at the same time a quotient of L/V by a solvable group $RV/V \simeq R/(R \cap V)$. So, it follows from property (iii) that L/RV has a quotient belonging to $\mathfrak{S}$. This quotient will also be a quotient of H, proving our claim that $\bar{D}^*$ has a quotient belonging to $\mathfrak{S}$. Moreover, since $\bar{D}$ is finite dimensional over the residue field $\bar{K}$ of K with respect to the restriction of v (cf. [Sc], Lemma 1.18), we can apply Lemma 12 to infer the existence of a finite dimensional division algebra $\tilde{D}$ over some finitely generated subfield $k \subset \bar{K}$ such that $\tilde{D}^*$ also has a quotient belonging to $\mathfrak{S}$.

Now, to conclude the proof of the theorem we may assume in addition that our division algebra D over a finitely generated field K was chosen to satisfy the following minimality requirement: the transcendence degree $t = \mathrm{tr.deg_P K}$ over the prime subfield $P \subset K$ is minimal possible over all finite dimensional algebras over finitely generated fields whose multiplicative group has a quotient belonging to $\mathfrak{S}$. Observe that the restriction of the valuation v introduced above to K is nontrivial (cf. [Sc], Lemma 1.13); in particular, if $t = 0$ then $\bar{K}_v$ is a finite field (as K is an algebraic number field of finite degree), implying by Wedderburn's Theorem that $\bar{D}$ is a field, which obviously precludes $\bar{D}^*$ from having a quotient belonging to $\mathfrak{S}$, contrary to what was established above.

Suppose $t > 0$. If v is trivial on P (in particular, if char $K > 0$), then $P \subset \bar{K}_v$ and

$$\mathrm{tr.deg}_P \bar{K}_v < \mathrm{tr.deg}_P K$$

(cf. [Bo], §10, n° 3, Cor. 4). It follows the subfield $k \subset \bar{K}$ constructed above has transcendence degree $< t$ over the prime subfield, while the multiplicative group of the k-algebra $\tilde{D}$ still has a quotient belonging to $\mathfrak{S}$ - a contradiction.

If v is nontrivial on P, then to get a contradiction one may need to use this procedure twice. Namely, the field k constructed above will have positive characteristic and transcendence degree $\leq t$ (cf. *loc. cit.,* Cor. 1), which implies that the above procedure applied to $\tilde{D}$ will yield another finite dimensional division algebra $\tilde{\tilde{D}}$ over a field of transcendence degree $< t$ over the prime subfield whose multiplicative group still has a quotient belonging to $\mathfrak{S}$ which eventually gives a contradiction.

For the first application of Theorem 6, we let $\mathfrak{S}$ be the class of all non-abelian finite simple groups. Then the conditions (i)–(iii) for this $\mathfrak{S}$ are obvious, and the condition (iv) follows from Theorem 5 and the result of

Segev and Seitz [SSe] that the commuting graph of any (known) finite simple group either has diameter > 4, or is balanced. Thus, one recovers from Theorem 6 the result of Segev.

Theorem 7 ([S1]) *The multiplicative group of a finite dimensional division algebra does not admit nonabeian finite simple groups as quotients.*

It should be pointed out that this approach based on Theorems 5 and 6 allows one to exclude some other nonsolvable, but nonsimple, groups as possible quotients of D^* which does not seem feasible by Segev's techniques.

Proposition 6 *The multiplicative group of a finite dimensional division algebra does not have quotients isomorphic to S_n where $n = p$ or $p + 1$, p a prime ≥ 5.*

PROOF. It suffices to verify that $\mathfrak{S} = \{S_n, A_n\}$ satisfies properties (i)-(iv) above. Properties (i)-(iii) are obvious, property (iv) follows from Theorem 5 and the fact that for S_n or A_n, where $n = p$ or $p + 1$, p a prime ≥ 5, the commuting graph is disconnected. To see this, we let $g = (12 \ldots n)$ or $(12 \ldots n-1)$ depending on whether $n = p$ or $p+1$. Then $g \in A_n$, and $\langle g \rangle - \{e\}$ is a connected component of the commuting graph for both S_n and A_n. [4]

Generally speaking, this approach reduces the problem of showing that a certain finite nonsolvable group cannot be realized as a quotient of D^* to a purely group-theoretic problem of embedding this group into a class of finite groups that satisfies conditions (i)-(iii) and verifying that for all members of this class the commuting graph either has diameter > 4 or is balanced. Unfortunately, the information on commuting graphs of finite groups available at this point is rather limited. After the analysis of finite simple groups carried out by Segev and Seitz [SSe], the next class of groups for which the same result can most probably be established by similar methods with minimum additional efforts is the class of groups H satisfying $\mathrm{Int}\, F \subset H \subset \mathrm{Aut}\, F$ for some finite simple group F. If this, indeed, can be done, we will obtain that none of such groups can occur as a quotient of D^*.

Inspired by the results of [S1] and [RoS], Segev [S2] formulated a conjecture that all finite quotients of D^* should be solvable, and we close this

[4] After the paper was submitted, my student Tim Woodcock has checked that the commuting graph of S_n has diameter > 4 for any n, which enables one to prove the proposition for any $n \geq 5$.

paper with a statement of the group-theoretic result that would lead to the proof of this conjecture using the above approach.

For a fixed nonabelian finite simple group F, and let $\mathfrak{S}(F)$ denote the class of finite groups G having the following structure: G has a normal subgroup N such that: (1) G/N is solvable, (2) N is isomorphic to $F^d = F \times \cdots F$ for some $d > 0$, (3) N does not have any proper subgroups normal in G (we observe that this condition simply means that the action of G by conjugation on the factors of $N \simeq F^d$ is transitive), and (4) the centralizer of N in G is trivial. We note that if a finite group L is not solvable, then it has a quotient G that belongs to $\mathfrak{S}(F)$ for some nonabelian finite simple group F. The conditions (i)–(iii) for $\mathfrak{S}(F)$ being obvious, we obtain the following conditional result.

Theorem 8 *Suppose that*

(***) *for any group $G \in \mathfrak{S}(F)$, the commuting graph either has diameter > 4 or is balanced.*

Then the multiplicative group of a finite dimensional division algebra cannot have quotients belonging to $\mathfrak{S}(F)$. Consequently, if (***) is true for all finite simple groups, then any finite quotient of the multiplicative group of a finite dimensional division algebra is solvable. [5]

So far, (***) has not been seriously analyzed, and therefore it is difficult to make any predictions. However, it looks plausible that even if (***) is not true for all cases, the desired result may still be achieved by using a suitable adaptation of our method based on somewhat weaker assumptions on the commuting graph.

References

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

[DK] P. Draxl, M. Kneser, SK_1 *von Sciefkörpern,* Lect. Notes in Math. **778,** Springer, 1980.

[5]The observation that our reduction method allows to prove Theorem 8 was made jointly with Y. Segev.

[Bo] N. Bourbaki, *Algèbre commutative,* Ch. VI, Masson, Paris, 1985.

[C] C. Chevalley, *Deux théorèmes d'arithmétiques,* J. Math. Soc. Japan, **3**(1954), 36–44.

[L] S. Lang, *Algebra,* Addison-Wesley, 1965.

[M1] G.A. Margulis, *Finiteness of quotients of discrete groups,* Funct. Analysis and Appl., **13**(1979), 178–187.

[M2] G.A. Margulis, *On the multiplicative group of a quaternion algebra over a global field,* Sov. Math. Dokl., **21**(1980), 780–784.

[Pi] R. Pierce, *Associative Algebras,* GTM **88**, Springer, 1982.

[PR1] V.P. Platonov, A.S. Rapinchuk, *On the group of rational points of three-dimensional groups,* Sov. Math. Dokl., **20**(1979), 693–697.

[PR2] V.P. Platonov, A.S. Rapinchuk, *The multiplicative structure of division algebras over number fields and the Hasse norm principle,* Proc. Steklov Inst. Math. **165**(1985), 187–205.

[PR3] V. Platonov, A. Rapinchuk, *Algebraic Groups and Number Theory,* "Pure and Applied Mathematics" series, N 139, Academic Press, 1993.

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

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

[R] A. Rapinchuk, *Some remarks concerning Segev's paper "On finite homomorphic images of the multiplicative group of a division algebra".* Notes (summer 1997).

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

[Ro] L. Rowen, *Ring Theory,* vol. II, Academic Press, 1988.

[RoS] L. Rowen, Y. Segev, *The finite quotients of the multiplicative group of a division algebra of degree 3 are solvable,* Israel J. of Math. **111**(1999), 373-380.

[Sc] O.F.G. Schilling, *The Theory of Valuations,* AMS, 1950.

[S1] Y. Segev, *On finite homomorphic images of the multiplicative group of a division algebra,* Ann. of Math., **149**(1999), 219–251.

[S2] Y. Segev, *Some applications of Wedderburn's factorization theorem,* Bull. Austral. Math. Soc., **59**(1999), 105-110.

[SSe] Y. Segev, G. Seitz, *Anisotropic groups of type A_n and the commuting graph of finite simple groups,* preprint (1997).

[T] G. Tomanov, *On the reduced norm 1 group of a division algebra over a global field,* Math. USSR Izvestiya, **39**(1992), 895–904.

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

Department of Mathematics
University of Virginia
Charlottesville VA 22903
USA

e-mail: asr3x@weyl.math.virginia.edu