Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable

Andrei S. Rapinchuk[1] Yoav Segev[2] Gary M. Seitz[3]

Abstract. We prove that finite quotients of the multiplicative group of a finite dimensional division algebra are solvable. Let D be a finite dimensional division algebra having center K and let $N \subseteq D^\times$ be a normal subgroup of finite index. Suppose $D^\times/N$ is not solvable. Then we may assume that $H := D^\times/N$ is a *minimal nonsolvable group* (MNS group for short), i.e., a nonsolvable group all of whose proper quotients are solvable. Our proof now has two main ingredients. One ingredient is to show that the commuting graph of a finite MNS group satisfies a certain property which we denote *property* $(3\frac{1}{2})$. This property includes the requirement that the diameter of the commuting graph should be ≥ 3, but is, in fact, stronger. Another ingredient is to show that if the commuting graph of $D^\times/N$ has the property $(3\frac{1}{2})$, then N is open with respect to a nontrivial height one valuation of D (assuming without loss, as we may, that K is finitely generated). After establishing the openness of N (when $D^\times/N$ is an MNS group) we apply the Nonexistence Theorem whose proof uses induction on the transcendence degree of K over its prime subfield, to eliminate H as a possible quotient of $D^\times$, thereby obtaining a contradiction and proving our main result.

1. Introduction

The purpose of this paper is to prove the following.

Main Theorem. *Let D be a finite dimensional division algebra. Then any finite quotient of the multiplicative group $D^\times$ is solvable.*

This result is a culmination of research done in the last several years trying to restrict the structure of finite quotients of $D^\times$. One of the principal motivations for this research was the work done on the Margulis-Platonov conjecture (MP) for anisotropic algebraic groups of inner type A_n over global fields; these are precisely the groups of the form $\mathbf{SL}_{1,D}$ associated

[1]Partially supported by grants from the NSF and by BSF grant no. 97-00042.
[2]Partially supported by BSF grant no. 97-00042.
[3]Partially supported by grants from the NSF and by BSF grant no. 97-00042.
Key words and phrases. division algebra, multiplicative group, finite homomorphic images, valuations
Mathematics Subject Classification Primary: 16K20, 16U60 Secondary: 20G15, 05C25
Date: January 30, 2001.

with the group $SL(1,D)$ of elements having reduced norm 1 in some finite dimensional division algebra D. Referring the reader to Ch. IX in [**?**] and Appendix A in [**?**] for a discussion of (MP), we only point out here that (MP) for $\mathbf{SL}_{1,D}$ was reduced in [**?**] to the following statement which is meaningful for division algebras over arbitrary fields: $D^\times$ does not have quotients that are nonabelian finite simple groups. This fact was verified in [**?**] for division algebras of degree 2 and 3, and stated for arbitrary finite dimensional division algebras as a conjecture. The affirmative resolution of this conjecture was obtained in [**?**] and [**?**]. In [**?**] techniques were developed for analyzing finite quotients $D^\times/N$ using the commuting graph[1] of $D^\times/N$, and some of the constructions in [**?**] were basically equivalent to proving the openness of N with respect to a nontrivial valuation of D under the assumption that the commuting graph of $D^\times/N$ either has diameter ≥ 5 or is "balanced". Valuations were explicitly used for the first time in [**?**] where the following "openness theorem" was obtained: if the diameter of the commuting graph of $D^\times/N$ is ≥ 4, then N is open in $D^\times$ with respect to a nontrivial valuation of D (Theorem 1 in [**?**]).

Let us see now how can the openness of N be used to restrict the structure of the finite quotient $D^\times/N$ (and eventually to eliminate nonsolvable finite groups as quotients of $D^\times$). First, since D is finite dimensional, Wedderburns' theorem allows us to assume that K is infinite (else D is finite and hence commutative). Now in §8 of [**?**], the following "nonexistence" result was actually established (it was however stated in a slightly less general form).

Nonexistence Theorem. *Let $\mathcal{G}$ be a class of finite groups. Call a member $G \in \mathcal{G}$* minimal *if no proper quotient of G belongs to $\mathcal{G}$. Assume that*

(1) *the members of $\mathcal{G}$ are not solvable;*
(2) *if $G \in \mathcal{G}$ and $M \lhd G$ with G/M solvable, then $M \in \mathcal{G}$;*
(3) *if $G \in \mathcal{G}$ and $M \lhd G$ is a solvable normal subgroup, then $G/M \in \mathcal{G}$;*
(4) *if $G \in \mathcal{G}$ is a minimal member, then given a finite dimensional division algebra D over a finitely generated field and a surjective homomorphism $\phi\colon D^\times \to G$, the kernel* $\operatorname{Ker}\phi$ *must be open in $D^\times$ with respect to a nontrivial height one valuation of D.*

Then no member of $\mathcal{G}$ can be a quotient of the multiplicative group of any finite dimensional division algebra.

We refer the reader to the beginning of §2 for the definition of a (height one) valuation and for the notion of openness. We note that a sketch of the proof of the Nonexistence Theorem is given at the beginning of §6.

In view of the Nonexistence Theorem, the above mentioned "openness theorem" (Theorem 1 in [**?**]) implies that if $\mathcal{G}$ is a class of finite groups satisfying (1)-(3) of the Nonexistence Theorem, and whose minimal members G have the property that $diam(\Delta_G) \geq 4$, then no member of $\mathcal{G}$ is a quotient of any $D^\times$ (cf. "Nonexistence Theorem at Diameter ≥ 4" in [**?**]). This theorem applies to some important classes. For example, since by [**?**] the commuting

[1]We recall that the commuting graph Δ_H of a finite group H is the graph whose vertex set is $H \smallsetminus \{1\}$ and whose edges are pairs of commuting elements; of course, Δ_H has a natural distance function d_H which, in particular, allows one to talk about the diameter of Δ_H, denoted $diam(\Delta_H)$.

graph of nonabelian finite simple groups has diameter ≥ 4, it applies to the class $\mathcal{G}$ of nonabelian finite simple groups, eliminating them as possible quotients of $D^\times$. However, Theorem 1 of [**?**] falls short of extending the Nonexistence Theorem to the class $\mathcal{G} = \mathcal{NS}$ of all finite nonsolvable groups. This is because the diameter of the commuting graph of *minimal nonsolvable groups* (i.e., nonsolvable finite groups all of whose proper quotients are solvable) may be equal to 3 (and is always ≥ 3, cf. [**?**]). Thus our goal in this paper is to formulate a condition which holds in minimal nonsolvable groups and that allows us to prove an "openness theorem" which guarantees that condition (4) of the Nonexistence Theorem holds for minimal nonsolvable finite groups.

Before we proceed we mention that the Main Theorem was conjectured by Segev in [**?**]. This conjecture was formulated in view of the results in [**?**], [**?**] and also the results with L. Rowen [**?**] and [**?**] that finite quotients of $D^\times$, where D is a division algebra of degree 3 or 5, are solvable (the last two results were obtained using very different tools, e.g., "Wedderburns' factorization theorem").

By Example 8.4 in [**?**], there are finite quotients $D^\times/N$ such that $diam(\Delta_{D^\times/N}) = 3$, but N is *not* open with respect to any nontrivial height one valuation of D. Thus to apply the Nonexistence Theorem, we need to work with a property of $\Delta_{D^\times/N}$ which is stronger than $diam(\Delta_{D^\times/N}) \geq 3$, but weaker than $diam(\Delta_{D^\times/N}) \geq 4$. Here it is,

Property $(3\frac{1}{2})$ There are two elements $x, y \in H \smallsetminus \{1\}$ such that for all $a, b \in H \smallsetminus \{1\}$ satisfying $[x, a] = [y, b] = 1$, there exists $h \in H$ with the property $d_H(x^h, y) \geq 3$ and $[a^h, b] \neq 1$, where as usual $x^h = h^{-1}xh$ and $[x, a] = x^{-1}a^{-1}xa$.

Theorem 1. *Let D be a finite dimensional division algebra over a finitely generated infinite field, $N \subseteq D^\times$ be a normal subgroup of finite index. If $H = D^\times/N$ satisfies property $(3\frac{1}{2})$, then N is open in $D^\times$ with respect to a nontrivial height one valuation of D.*

We observe that if Δ_H has diameter ≥ 4, i.e. there are elements $x, y \in H \smallsetminus \{1\}$ with $d_H(x, y) \geq 4$, then property $(3\frac{1}{2})$ is automatically satisfied (indeed, one can take $h = 1$), so our Theorem 1 contains the openness Theorem 1 of [**?**] (proved in [**?**] under the diameter ≥ 4 condition).

As we indicated Theorem 1 can be applied in the case when $D^\times/N$ is a minimal nonsolvable group because of the following

Theorem 2. *Let H be a minimal finite nonsolvable group (i.e. any proper quotient of H is solvable). Then H has the property $(3\frac{1}{2})$.*

The proof of Theorem 2 is carried out in §7; it depends on the classification of finite simple groups and uses detailed information about their structure. As we explained above, Theorems 1 and 2, in conjunction with the Nonexistence Theorem yield the Main Theorem.

As an application of our Main Theorem, we mention that when the center of D, K, is a global field, our Main Theorem together with a theorem due to Margulis and Prasad (see [**?**], [**?**] and §6) implies that finite quotients of $SL(1, D)$ are solvable (Corollary **??** in §6). Now the Margulis-Platonov conjecture for the groups $\mathbf{SL}_{1,D}$ says that any noncentral normal subgroup M of $SL(1, D)$ is open (with respect to the T-adic topology, where T is a finite set

of valuations of D). Indeed, the above mentioned theorem of Margulis and Prasad implies that M has finite index in $SL(1,D)$, hence $SL(1,D)/M$ is solvable and it follows that M contains some term of the derived series of $SL(1,D)$. Since by a theorem of Raghunathan [**?**] all the terms of the derived series of $SL(1,D)$ are open (again when K is a global field), we conclude that M is open. Hence our Main Theorem implies that the Margulis-Platonov conjecture holds true for the groups $\mathbf{SL}_{1,D}$ (see Theorem **??** in §**??**). The proof of (MP) in this case was carried out in [**?**] and [**?**] using the reduction given in [**?**] which the above proof does not require.

We now briefly describe the methods employed in the proof of Theorem 1. First, we show in §§**??**-**??** that a required valuation can be constructed given a homomorphism $\varphi\colon N \to \Gamma$ to a partially ordered group Γ with some special properties. A result of this kind was proved in [**?**] assuming that Γ is totally ordered and φ is a *valuation-like map,* i.e. there exists a nonnegative $\alpha \in \Gamma$, called a *level* of φ, such that

$$N_{<-\alpha} + 1 \subseteq N_{<-\alpha}, \tag{VL}$$

where for $\gamma \in \Gamma$ we let $N_{<\gamma} := \{n \in N \mid \varphi(n) < \gamma\}$. In order to prove Theorem 1 we need to deal with the situation where φ still has a level, but the group Γ is no longer guaranteed to be totally ordered (in this case we call φ a *leveled maps*). In §§**??**-**??** we define the notion of a valuation associated with a leveled map. We then single out a set of conditions on a given leveled map that ensure the existence of a valuation associated with it and the openness of N with respect to this valuation. Having done that, we show in §**??** how to construct a leveled map $\varphi\colon N \to \Gamma$ with these conditions given that $D^\times/N$ satisfies property $(3\frac{1}{2})$ (without getting into technical details, we point out that the conditions include the requirements that $\Gamma_K := \varphi(K^\times)$ be a nontrivial totally ordered subgroup of Γ and that φ has a level in Γ_K; note that since $diam(\Delta_{D^\times/N}) \geq 3$, we have $K^\times \subseteq N$). The argument in §**??** involves a new concept of *strongly leveled* maps, some properties of which are analyzed in §**??**. We note that both the notion of a leveled map and of a strongly leveled map are closely related to condition (U3) of the U-hypothesis in §3 of [**?**].

We conclude the introduction with two questions that naturally arise in the context of the investigation of the normal subgroup structure of algebraic groups over arbitrary fields. In the first question we ask whether the hypothesis of Theorem 1 can be replaced by the mere hypothesis that the diameter of $\Delta_{D^\times/N}$ is ≥ 3.

Question 1: *Let D be a finite dimensional division algebra over a finitely generated infinite field, and $N \subseteq D^\times$ be a normal subgroup of finite index. Does the fact that the commuting graph of $D^\times/N$ has diameter ≥ 3 imply that N is open in $D^\times$ with respect to a finite set T of nontrivial height one valuations of D?*

This question was first raised in [**?**], but still remains unresolved. We remark that

Remark. The Nonexistence Theorem holds true even when in (4), $\operatorname{Ker}\phi$ is required to be open with respect to a finite set T of nontrivial height one valuations of D, but this more general version of the Nonexistence Theorem is not used in this paper (cf. Remark 8.3 in [**?**]).

By the above remark, a positive answer to Question 1 would give an alternative proof of the Main Theorem which requires less information about minimal nonsolvable groups, viz. instead of the technically complicated Theorem 2 the fact, proved in [**?**], that the diameter of the commuting graph of any minimal nonsolvable group is ≥ 3 would be sufficient. Other applications would include detailed information about possible finite quotients of $D^\times$ which may eventually lead to some form of their classification (we recall that finite subgroups of $D^\times$ were classified by Amitsur [**?**]).

The second question that came up in discussions of G. Prasad with Rapinchuk deals with extending our Main Theorem to other types of algebraic groups.

Question 2 (Prasad, Rapinchuk): *Let G be an absolutely simple algebraic group over an infinite field K. Is it true that all finite quotients of $G(K)$ are solvable?*

We recall that if G is K-isotropic, then the subgroup $G(K)^+$ generated by the K-rational points of the unipotent radicals of K-defined parabolics does not have proper noncentral normal subgroups (Tits [**?**]), so any finite quotient of $G(K)$ is in fact a quotient of $W(G,K) = G(K)/G(K)^+$ which was termed the Whitehead group of G by Tits [**?**]; furthermore, $W(G,K)$ is known to be abelian at least for most classical types. For K-anisotropic groups the situation is different as very little is known about them when K is a general field. However, Some optimism regarding Question 2 can be based on the fact that at least over global fields simplicity problems reduce to the groups of type A_n (cf. [**?**] Ch. IX), and the Main Theorem strongly suggests the affirmative answer to Question 2 for anisotropic inner forms of type A_n.

We are grateful to Gopal Prasad for the inspiring interest he had shown in this work, for reading and listening to portions of this manuscript very carefully and for his helpful detailed remarks.

2. The existence of a valuation associated with a leveled map

Throughout this paper, D is a finite dimensional central division algebra over an infinite field K, and $N \subseteq D^\times$ is a finite index subgroup such that $-1 \in N$. Recall that a valuation of D is a group homomorphism $v : D^\times \to \tilde{\Gamma}$, from $D^\times$ onto a linearly ordered group $\tilde{\Gamma}$ satisfying $v(x+y) \geq \min\{v(x), v(y)\}$, whenever $x + y \neq 0$. The group $\tilde{\Gamma}$ and the valuation v are said to have height one if $\tilde{\Gamma}$ is isomorphic to a subgroup of the additive group $(\mathbb{R}, +)$ of the reals. Throughout Γ denotes a *partially ordered* group[1], such that $\Gamma_{>0} \neq \emptyset$, where $\Gamma_{>0} = \{\gamma \in \Gamma \mid \gamma > 0\}$. We will consider *surjective* homomorphisms $\varphi\colon N \to \Gamma$.

Definitions 2.1. Let Γ be a partially ordered group such that the set of positive elements of Γ is nonempty. Let $\varphi\colon N \to \Gamma$ be a surjective homomorphism. Then

[1]The following conventions will be kept throughout the paper: the operation on Γ will be denoted *additively,* though Γ is *not* assumed to be commutative; the order relation will be denoted $\leq$ (so, for any $\alpha, \beta, \gamma, \delta \in \Gamma$ with $\alpha \leq \gamma$ and $\beta \leq \delta$ we have $\alpha + \beta \leq \gamma + \delta$).

(1) We say that φ is a *leveled map* if there exists a nonegative $\alpha \in \Gamma$ (called a *level* of φ) such that

(i) $$N_{<-\alpha} + 1 \subseteq N_{<-\alpha},$$

where $N_{<-\alpha} = \{x \in N \mid \varphi(x) < -\alpha\}$. Note that we automatically have $N_{<-\alpha} \neq \emptyset$.

(2) A valuation $v\colon D^\times \to \tilde{\Gamma}$ is *associated* with φ if there exists a nontrivial homomorphism $\theta\colon \Gamma \to \tilde{\Gamma}$ of (partially) ordered groups such that the diagram

(ii) $$\begin{array}{ccc} N & \stackrel{\varphi}{\longrightarrow} & \Gamma \\ \iota\downarrow & & \downarrow\theta \\ D^\times & \stackrel{v}{\longrightarrow} & \tilde{\Gamma}, \end{array}$$

in which ι is the inclusion map, commutes.

We note that the notion of a leveled map extends the notion of a valuation-like map from [**?**] and will eventually lead to valuations. We fix the following notation.

Notation 2.2. Let Γ be a nontrivial partially ordered group (not necessarily abelian but written additively!), and let $\varphi\colon N \to \Gamma$ be a (surjective) homomorphism (which will always be clear from the context).

(1) For $\beta \in \Gamma$, we let $\Gamma_{<\beta}$ (resp., $\Gamma_{\leq\beta}, \Gamma_{>\beta}$, etc.) denote the set of $\gamma \in \Gamma$ satisfying $\gamma < \beta$ (resp., $\gamma \leq \beta$, $\gamma > \beta$, etc.).

(2) For a subset $M \subseteq N$, $M_{<\beta}$ (resp., $M_{\leq\beta}, M_{>\beta}$, etc.) denote the set of $m \in M$ satisfying $\varphi(m) < \beta$ (resp., $\varphi(m) \leq \beta$, $\varphi(m) > \beta$, etc.).

(3) For a subfield L of D, write $N_L := N \cap L$, $\varphi_L := \varphi\,|_{N_L}\colon N_L \to \Gamma_L$, where $\Gamma_L := \varphi(N_L)$.

(4) Given a (surjective) valuation $v\colon D^\times \to \tilde{\Gamma}$ (note that $\tilde{\Gamma}$ is necessarily abelian, cf. Remark 2.2 in [**?**]), we let $\mathcal{O}_{D,v} = \{x \in D^\times \mid v(x) \geq 0\} \cup \{0\}$ denote the valuation ring of v. For any $\delta \in (\tilde{\Gamma})_{\geq 0}$, $\mathfrak{m}_{D,v}(\delta) = \{x \in D^\times \mid v(x) > \delta\} \cup \{0\}$ will denote the corresponding ideal of $\mathcal{O}_{D,v}$. These ideals form a fundamental system of open neighborhoods of zero for the natural topology on D associated with v which is sometimes referred to as the v-adic topology. We will write $\mathcal{O}_v$, or simply $\mathcal{O}$, instead of $\mathcal{O}_{D,v}$ if this will not lead to a confusion.

Theorem 5.1 in [**?**] asserts that given a nontrivial valuation-like map $\varphi\colon N \to \Gamma$ to a totally ordered group Γ, then (for a finitely generated field K) there exists a height one valuation v of D associated with φ, and N is open in the v-adic topology. In §§**??**-**??** we extend this result and prove

Theorem 2.3. *Suppose K is finitely generated and that $\varphi\colon N \to \Gamma$ is a surjective homomorphism onto a nontrivial partially ordered group Γ. Let $\mathcal{R}$ be the subring of D generated by $N_{\geq 0}$. Assume that*

(1) $N_{\geq 0} \nsubseteq K$;
(2) $\Gamma_K := \varphi(N \cap K^\times)$ *is a nontrivial totally ordered group;*
(3) φ *is a leveled map having a level* $\alpha \in (\Gamma_K)_{\geq 0}$;
(4) $\mathcal{R}$ *is a proper subring of D.*

Then there exists a height one valuation $v\colon D^\times \to \tilde{\Gamma}$ *associated with* φ. *Suppose in addition that*

(4′) *There exists* $\gamma \in \Gamma_{\geq 0}$ *such that* $\mathcal{R} \cap N \subseteq N_{>-\gamma}$.

(*which in particular implies* (4)) *Then* N *is open with respect to the corresponding* v*-adic topology.*

In this section we show that under the hypotheses (1) – (4) of Theorem **??**, there exists a height one valuation v associated with φ. The next section focuses on proving that if in addition we assume hypothesis (4′) of Theorem **??**, then N is open with respect to *any* valuation associated with φ (Theorem **??**).

The assumptions that the group Γ_K is totally ordered and the homomorphism $\varphi_K\colon N_K \to \Gamma_K$ admits a level $\alpha \in \Gamma_K$ mean that φ_K is a valuation-like map in the sense of [**?**]. By Theorem 4.1.1 and Proposition 2.6 in [**?**], there exists a nontrivial valuation $v_0\colon K^\times \to \tilde{\Gamma}_0$ associated with φ_K, and N_K is open in $K^\times$ with respect to the topology defined by this valuation, i.e. there exists $\delta \in (\tilde{\Gamma}_0)_{\geq 0}$ such that

$$1 + \mathfrak{m}_{K,v_0}(\delta) \subseteq N_K, \tag{iii}$$

where $\mathfrak{m}_{K,v_0}(\delta) = \{x \in K^\times \mid v_0(x) > \delta\} \cup \{0\}$. Furthermore, by Theorem 4.1.2 in [**?**], since K is finitely generated, we may (and we will) assume that the height of v_0 is one. We will show that v_0 (uniquely) extends to a valuation $v\colon D^\times \to \tilde{\Gamma}$, and that this valuation is associated with φ.

We pick a basis $a_1, \ldots, a_{n^2}$ of D over K (where $n^2 = \dim_K D$), and we define a norm $||\ ||_{v_0}$ on D by

$$||\ \alpha_1 a_1 + \cdots + \alpha_{n^2} a_{n^2}\ ||_{v_0} = \max_{i=\overline{1,n^2}} |\ \alpha_i\ |_{v_0} \tag{iv}$$

where $|\ |_{v_0}$ is the absolute value associated with v_0. (One easily shows that the topological notion of boundedness associated with norms of the form (**??**) constructed using different bases, coincide). The existence of an extension of v_0 will be derived from the following result analogous to Theorem 5.2 in [**?**].

Theorem 2.4. *Let* D *be a central division algebra of degree* n *over an arbitrary field* K, v_0 *be a valuation of* K *having height one. Assume there exists a subring* $\mathcal{B} \subsetneqq D$ *such that*

(a) $\mathcal{B}$ *is open in* D *with respect to the topology defined by the norm* $||\ ||_{v_0}$;

(b) *there exists a positive integer* k *such that* $d\mathcal{B}d^{-1} \subseteq \mathcal{B}$ *for all* $d \in (D^\times)^k = \{x^k \mid x \in D^\times\}$.

Then v_0 *extends to a height one valuation* v *of* D *such that* $\mathcal{B}$ *is contained in the corresponding valuation ring* $\mathcal{O}_v$.

Proof. Let $A = D \otimes_K K_{v_0}$, where K_{v_0} is the completion of K with respect to v_0. Then $A \simeq M_d(\mathcal{D})$ for some integer $d \geq 1$ and some central division algebra $\mathcal{D}$ over K_{v_0}. The valuation v_0 extends from K_{v_0} to a valuation u on $\mathcal{D}$ by the formula

$$u(x) = \frac{1}{l} v_0(\mathrm{Nrd}_{\mathcal{D}/K_{v_0}}(x)) \quad \text{for any} \quad x \in \mathcal{D}^\times,$$

where l is the degree of $\mathcal{D}$ (cf., for example, [**?**]), so it suffices to establish that our assumptions force $d = 1$, since then the restriction $u\mid_D$ of u to D provides a height one extension of v_0. Note that since the height of v_0 is one, the definition of u makes sense and the height of u is one; in particular, u admits an associated absolute value $|\ |_u$.

The norm $||\ ||_{v_0}$ extends from D to A by means of equation (**??**) (just think of $\alpha_1, \dots, \alpha_{n^2}$ as elements of K_{v_0}), and we saw in the proof of Theorem 5.2 in [**?**] that the closure $\bar{\mathcal{B}}$ of $\mathcal{B}$ in A is a proper open subring. Then according to Lemma 5.3 in [**?**], $\bar{\mathcal{B}}$ is bounded. To obtain a contradiction if $d > 1$, we will use a different norm on $A \simeq M_d(\mathcal{D})$:

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

Since both $||\ ||_{v_0}$ and $||\ ||_u$ are norms on A as a vector space over K_{v_0}, they are equivalent because $\dim_{K_{v_0}} A < \infty$ and K_{v_0} is complete (cf. [**?**]); in particular, they give rise to the same notion of boundedness on A.

It follows from assumption (b) in the statement of the theorem that $d\bar{\mathcal{B}}d^{-1} \subseteq \bar{\mathcal{B}}$ for any $d \in (A^\times)^k$. Now, suppose $d > 1$. Since the subring $\bar{\mathcal{B}} \subseteq M_d(\mathcal{D})$ is open, it contains $M_d(\mathfrak{m}_{\mathcal{D},u}(\delta))$, for some nonnegative δ in the value group of u, in particular there exists $b = (b_{ij}) \in \bar{\mathcal{B}}$ with $b_{12} \neq 0$ (as $\mathfrak{m}_{\mathcal{D},u}(\delta) \neq 0$). Pick also $s \in \mathcal{D}^\times$ so that $|\ s\ |_u > 1$, and let $t = \mathrm{diag}(s, s^{-1}, 1, \dots 1) \in A^\times$. Now consider the sequence

$$d_l := t^{lk} \in A^\times, \quad l = 1, 2, \dots\ .$$

Then for $b_l = d_l b d_l^{-1} \in \bar{\mathcal{B}}$, the (12)-entry is $(b_l)_{12} = s^{lk} b_{12} s^{lk}$, so $|\ (b_l)_{12}\ |_u \to \infty$ as $l \to \infty$, contradicting the boundedness of $\bar{\mathcal{B}}$. Thus, $d = 1$, i.e. $A = \mathcal{D}$, and the restriction $v = u\mid_D$ provides a height one extension of v_0. Since $\bar{\mathcal{B}}$ is bounded, it is contained in the valuation ring of u, (because for an element $x \in \mathcal{D}^\times$ which is not in the valuation ring of u one has $|\ x^l\ |_u \to \infty$ as $l \to \infty$) implying the inclusion $\mathcal{B} \subseteq \mathcal{O}_v$. □

To prove the existence of v asserted in Theorem **??**, we will apply Theorem **??** to the subring $\mathcal{R} \subseteq D$ generated by $N_{\geq 0}$. The following proposition establishes the properties required for its application.

Proposition 2.5. *Let $\varphi\colon N \to \Gamma$ be a (nontrivial surjective) leveled map having a level $\alpha \in (\Gamma_K)_{\geq 0}$. Assume that the group Γ_K is nontrivial and totally ordered, and let $v_0\colon K^\times \to \tilde{\Gamma}_0$ be a valuation associated with φ_K . Then*

(1) *there exists $\varepsilon \in (\tilde{\Gamma}_0)_{\geq 0}$, such that the subring $\mathcal{R}_K \subseteq K$ generated by $(N_K)_{\geq 0}$ contains $\mathfrak{m}_{K,v_0}(\varepsilon)$.*

Suppose in addition that $N_{\geq 0} \nsubseteq K$. Then

(2) *$N_{\geq 0}$ contains a basis of D over K;*
(3) *if v_0 has height one, then the subring $\mathcal{R} \subseteq D$ generated by $N_{\geq 0}$ is open with respect to the topology defined by the norm $||\ ||_{v_0}$* (see (**??**)).

Proof. First note that as we already remarked, the existence of v_0 is guaranteed by the hypotheses of the proposition.

(1): Let $\delta \in (\tilde{\Gamma}_0)_{\geq 0}$, be as in (**??**). We pick $c \in N_K$ such that $v_0(c) > 0$ (which exists since N_K has finite index in $K^\times$). Then $c(1 + \mathfrak{m}_{K,v_0}(\delta)) \subseteq N_K$ and $v_0(c(1 + \mathfrak{m}_{K,v_0}(\delta))) \subseteq (\tilde{\Gamma}_0)_{>0}$. Since Γ_K is totally ordered and v_0 is associated with φ_K, this implies that

$$c(1 + \mathfrak{m}_{K,v_0}(\delta)) \subseteq (N_K)_{>0} \subseteq \mathcal{R}_K,$$

i.e. $c\mathfrak{m}_{K,v_0}(\delta) \subseteq \mathcal{R}_K$. Then $\varepsilon := \delta + v_0(c)$ is as required.

(2): Let V be the K-linear span of $N_{\geq 0}$; since $N_{\geq 0}$ is closed under multiplication, V is a subring of D. Moreover, V is invariant under conjugation by N. Let Ω be an algebraically closed field containing K. Since N has finite index in $D^\times$, it is Zariski dense in $(D \otimes_K \Omega)^\times \simeq GL_n(\Omega)$. Thus, $V \otimes_K \Omega$ is a subalgebra of $D \otimes_K \Omega \simeq M_n(\Omega)$ invariant under conjugation by $GL_n(\Omega)$. However, there are no proper noncentral conjugation invariant subalgebras $R \subseteq M_n(\Omega)$. (For the sake of completeness, we recall a proof of this well-known fact. Let T be the diagonal torus in $GL_n(\Omega)$. Then R is not centralized by T as otherwise it would be centralized by all semi-simple elements in $GL_n(\Omega)$, and therefore by $GL_n(\Omega)$ itself. Thus, R contains an eigenvector for T for some nontrivial character, i.e. an off-diagonal matrix unit e_{ij}, $i \neq j$. But all off-diagonal matrix units are conjugate under $GL_n(\Omega)$, so R contains all of them. Finally, $e_{ij}e_{ji} = e_{ii}$, which puts diagonal matrix units inside R as well.) Since $N_{\geq 0} \nsubseteq K$, we conclude that $V \otimes_K \Omega = M_n(\Omega)$, and therefore $V = D$, as required.

(3): According to (2), $N_{\geq 0}$ contains a basis $\omega_1, \dots, \omega_{n^2}$ of D over K. Let ε be as in (1). Then

$$\mathfrak{m}_{K,v_0}(\varepsilon)\omega_1 + \cdots \mathfrak{m}_{K,v_0}(\varepsilon)\omega_{n^2} \subseteq \mathcal{R},$$

giving the openness of $\mathcal{R}$ in D. □

Proof of the existence of the valuation v asserted in Theorem **??**. According to condition (4) in the statement of Theorem **??**, the subring $\mathcal{B} = \mathcal{R}$ is proper. By Proposition **??**(3), it is also open with respect to the topology defined by the norm $|| \; ||_{v_0}$, i.e. satisfies condition (a) in Theorem **??**. Furthermore, since Γ is an ordered group, $\Gamma_{\geq 0}$ is a normal subset of Γ, implying that $N_{\geq 0}$ is a normal subset of N, so $\mathcal{R}$ is normalized by N. Since $N \supseteq (D^\times)^k$ for $k = (|D^\times : N|)!$, condition (b) holds as well. Thus, according to Theorem **??**, v_0 extends to a height one valuation $v\colon D^\times \to \tilde{\Gamma}$ and, moreover, $\mathcal{R}$ is contained in its valuation ring $\mathcal{O}_v$. The latter means that $N_{\geq 0} \subseteq \mathcal{O}_v$, i.e. for $x \in N$, $\varphi(x) \geq 0$ implies $v(x) \geq 0$. We conclude that $v(\operatorname{Ker} \varphi) = \{0\}$, and the arising homomorphism $\theta\colon \Gamma \to \tilde{\Gamma}$ is, in fact, a homomorphism of ordered groups, so v is associated with φ.

3. The openness theorem

To conclude the proof of Theorem **??**, it remains to establish the openness of N. In ([**?**], Prop. 2.6) we showed that if N admits a valuation-like map $\varphi\colon N \to \Gamma$ with Γ *totally* ordered, then N will be open in $D^\times$ with respect to *any* valuation v of D associated with φ. In this section we will prove a similar result which, in particular, completes the proof of Theorem **??**.

Theorem 3.1. *Let $\varphi\colon N \to \Gamma$ be a surjective homomorphism onto a partially ordered group satisfying conditions* (1)–(3) *and* (4′) *in the statement of Theorem* **??**. *If a valuation $v\colon D^\times \to \tilde{\Gamma}$ is associated with φ, then N is open in $D^\times$ with respect to the v-adic topology.*

(We note that the assumption, made in Theorem **??**, that K be finitely generated is not necessary for the validity of Theorem **??**). One of the ingredients of the proof is the following elaboration on Proposition 2.6 in [**?**].

Proposition 3.2. *Let $\varphi\colon N \to \Gamma$ be a leveled map admitting an associated valuation $v\colon D^\times \to \tilde{\Gamma}$. Assume that for the valuation ring $\mathcal{O}_v$ of v there exists $\beta \in \Gamma_{\geq 0}$ such that*

$$\mathcal{O}_v \cap N \subseteq N_{>-\beta}. \tag{i}$$

Then N is open in $D^\times$ with respect to the v-adic topology.

Proof. Let $\alpha \in \Gamma_{\geq 0}$ be a level of φ. We need to show that there exists a $\delta \in \tilde{\Gamma}_{\geq 0}$, such that

$$1 + \mathfrak{m}(\delta) \subseteq N, \tag{ii}$$

where $\mathfrak{m}(\delta) = \{x \in D^\times \mid v(x) > \delta\} \cup \{0\}$. For that we will show that for each coset Na of N in $D^\times$, there exists $\gamma(Na) = \gamma \in \tilde{\Gamma}_{\geq 0}$ such that

$$1 + (Na \cap \mathfrak{m}(\gamma)) \subseteq N. \tag{iii}$$

Then, since N has a finite index in $D^\times$, the maximum $\delta = \max \gamma(Na)$, taken over all cosets of N in $D^\times$, exists (recall that $\tilde{\Gamma}$ is totally ordered!) and obviously satisfies (**??**). Since v is associated with φ, there exists a nontrivial homomorphism of ordered groups $\theta\colon \Gamma \to \tilde{\Gamma}$ for which the diagram (ii) of §2 is commutative. To establish the existence of $\gamma(Na)$, we need the following.

Lemma 3.3. (1) *For $m, n \in N$ such that $v(m) < v(n) - \theta(\alpha + \beta)$, the element $c = m + n$ belongs to N.*

(2) *For any $d \in D^\times$, there exists $\beta_d \in \tilde{\Gamma}$ such that*

$$d + \{n \in N \mid v(n) < \beta_d\} \subseteq N.$$

Proof. (1): Recall that $\alpha \in \Gamma_{\geq 0}$ is a level of φ and $\beta \in \Gamma_{\geq 0}$ is as in Proposition **??**. Pick $a, b \in N$ so that $\varphi(a) = \alpha$ and $\varphi(b) = \beta$; then $v(a) = \theta(\alpha)$ and $v(b) = \theta(\beta)$. We have $v(m^{-1}na^{-1}b^{-1}) > 0$ (note that $\tilde{\Gamma}$ is commutative!), so $m^{-1}na^{-1}b^{-1} \in \mathcal{O}_v$, hence $\varphi(m^{-1}na^{-1}b^{-1}) > -\beta = \varphi(b^{-1})$ according to (**??**). It follows that $\varphi(m^{-1}na^{-1}) > 0$, and therefore $\varphi(n^{-1}m) < \varphi(a^{-1}) = -\alpha$, i.e. $n^{-1}m \in N_{<-\alpha}$. Now,

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

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

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

$$\beta_d = \min(v(s), v(d + s)) - \theta(\alpha + \beta).$$

Suppose now that $t \in N$ satisfies $v(t) < \beta_d$. Then, in particular, $v(t) < v(s) - \theta(\alpha + \beta)$, so it follows from (1) that $t - s \in N$ (observe that $v(-s) = v(s)$). Moreover, since $\alpha, \beta \in \Gamma_{\geq 0}$, we have $v(t) < v(s)$, and therefore $v(t - s) = v(t)$ as v is a valuation. Thus, $v(t - s) < v(d + s) - \theta(\alpha + \beta)$, and

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

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

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

$$\gamma = \gamma(Na) := \mid v(a) \mid + \mid \beta_a \mid,$$

where β_a is as in Lemma **??**(2) (here, as usual, for $\gamma \in \tilde{\Gamma}$, we denote $\mid \gamma \mid = \max\{\gamma, -\gamma\}$). Suppose $na \in Na \cap \mathfrak{m}(\gamma)$. Then

$$v(n) = v(na) - v(a) > (\mid v(a) \mid + \mid \beta_a \mid) - v(a) \geq \mid \beta_a \mid,$$

implying that

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

as $v(n^{-1}) < - \mid \beta_a \mid \leq \beta_a$, and therefore by Lemma **??**(2), $n^{-1} + a \in N$. This proves (**??**) and completes the proof of Proposition **??**. □

Remark 3.4. Proposition **??** immediately generalizes to the situation when there is a finite set $T = \{v_1, \dots, v_r\}$ of valuations associated with a given leveled map $\varphi\colon N \to \Gamma$: if $\mathcal{O}_{v_i}$ is the valuation ring of v_i and $\mathcal{O}_T = \cap_{i=1}^r O_{v_i}$, then the condition

$$N \cap O_T \subseteq N_{>-\beta}$$

for some $\beta \in \Gamma_{\geq 0}$, implies that N is open in $D^\times$ with respect to the topology defined by T.

Proof of Theorem **??**. By the definition of an associated valuation, v is nontrivial. In view of Proposition **??**, all we have to show is that under assumptions made in the statement of the theorem there exists $\beta \in \Gamma_{\geq 0}$, satisfying (**??**). We will need the following.

Lemma 3.5. *Let $\mathcal{O} \subseteq K$ be an integrally closed ring, $\tilde{\mathcal{O}} \subseteq D$ be a subring which is integral over $\mathcal{O}$ and contains a basis $\omega_1, \dots, \omega_{n^2}$ of D/K. Then there exists $t \in \mathcal{O}$, $t \neq 0$, such that*

$$\tilde{\mathcal{O}} \subseteq \frac{1}{t} \left(\mathcal{O}\omega_1 + \dots + \mathcal{O}\omega_{n^2}\right).$$

Proof. The equation $h(x, y) := \mathrm{Trd}_{D/K}(xy)$ defines a nondegenerate symmetric bilinear form on D. Since $\mathcal{O}$ is integrally closed, $\mathrm{Trd}_{D/K}(\tilde{\mathcal{O}}) \subseteq \mathcal{O}$ (indeed, suppose $a \in \tilde{\mathcal{O}}$, and let $L \subseteq D$ be a maximal subfield containing a; then a belongs to $\mathcal{O}_L :=$ integral closure of $\mathcal{O}$ in L, so the required inclusion follows from the following two facts: 1) $\mathrm{Trd}_{D/K}(a) = \mathrm{Tr}_{L/K}(a)$ (cf. [**?**]); 2) $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subseteq \mathcal{O}$ (cf. [**?**], Ch. V, §1, n° 6, cor. 2)). Let $t = \det\left(h(\omega_i, \omega_j)\right)$; then $t \in \mathcal{O}$, $t \neq 0$. Take an arbitrary $a \in \tilde{\mathcal{O}}$ and write it as

$$a = \alpha_1\omega_1 + \dots \alpha_{n^2}\omega_{n^2}$$

with $\alpha_i \in K$. We need to show that in fact $\alpha_i \in \dfrac{1}{t}\mathcal{O}$ for all i. However, the α_i's can be determined from the following linear system

$$\sum_{i=1}^{n^2} \alpha_i h(\omega_i, \omega_j) = A_j, \quad j = 1, \dots, n^2,$$

where $A_j := \mathrm{Trd}_{D/K}(a\omega_j) \in \mathcal{O}$. Since the determinant of this system is t, we obtain from Cramer's Rule that $\alpha_i \in \dfrac{1}{t}\mathcal{O}$, as required. □

Let $\mathcal{O}_{v_0} = \mathcal{O}_v \cap K$ be the valuation ring of the restriction $v_0 = v\mid_K : K^\times \to v(K^\times) =: \tilde{\Gamma}_0$ (note that v_0 is nontrivial as v is such and $[D : K] < \infty$, and that v_0 is associated with φ_K). To apply Lemma **??**, we observe that $\mathcal{O}_v$ is integral over $\mathcal{O}_{v_0}$. Indeed, let $a \in \mathcal{O}_v$ and L be a maximal subfield of D containing a. The existence of a valuation of D extending v_0 implies that $v\mid_L$ is the *only* extension of v_0 to L (cf. [**?**]), with $\mathcal{O}_v \cap L$ as the valuation ring. On the other hand, it is known (cf. [**?**], Ch. VI, §1, n° 3, cor. 3) that the integral closure of $\mathcal{O}_{v_0}$ in L coincides with the intersection of the valuation rings of all extensions of v_0 to L. Thus, $\mathcal{O}_v \cap L$ is integral over $\mathcal{O}_{v_0}$, and eventually $\mathcal{O}_v$ is integral over $\mathcal{O}_{v_0}$. We also note that $\mathcal{O}_{v_0}$, being a valuation ring, is integrally closed (cf. [**?**], Ch. VI, §1, n° 3, cor. 1). Since $N_{\geq 0} \not\subseteq K$, according to Proposition **??**(2) there exists a basis $\omega_1, \dots, \omega_{n^2} \in N_{\geq 0} \subseteq \mathcal{O}_v$. Applying Lemma **??**, we obtain that there exists a nonzero $t \in \mathcal{O}_{v_0}$ such that

$$\mathcal{O}_v \subseteq \frac{1}{t}\left(\mathcal{O}_{v_0}\omega_1 + \dots + \mathcal{O}_{v_0}\omega_{n^2}\right). \tag{iv}$$

In view of $\dfrac{1}{t} = \dfrac{t^{d-1}}{t^d}$, we can replace t with t^d in (**??**), where $d = (\mid K^\times : N_K \mid)!$, and assume that $t \in N_K$. In fact, we may (and we will) even assume that $t \in (N_K)_{\geq 0}$ (indeed, if $\varphi(t) < 0$, then $v(t) = 0$ (because $t \in \mathcal{O}_{v_0}$ and because v is associated with φ), and one can simply take in (**??**) $t = 1$). Furthermore, let $\varepsilon \in (\tilde{\Gamma}_0)_{\geq 0}$ be as in Proposition **??**(1), i.e. $\mathfrak{m}_{K,v_0}(\varepsilon) \subseteq \mathcal{R}_K$ (the subring generated by $(N_K)_{\geq 0}$). Since $\mid \tilde{\Gamma}_0 : v_0(N_K) \mid < \infty$, one can pick $s \in (N_K)_{>0}$ satisfying $v(s) > \varepsilon$. Then $s\mathcal{O}_{v_0} \subseteq \mathcal{R}_K$. Now, set $f = st$. Then $f \in (N_K)_{>0}$ and

$$O_v \subseteq \frac{1}{f}\left(\mathcal{R}_K\omega_1 + \dots + \mathcal{R}_K\omega_{n^2}\right) \subseteq \frac{1}{f}\mathcal{R}$$

where $\mathcal{R} \subseteq D$ is the subring generated by $N_{\geq 0}$. It follows now from condition $(4')$ in the statement of Theorem **??** that

$$O_v \cap N \subseteq \frac{1}{f}\left(\mathcal{R} \cap N\right) \subseteq \frac{1}{f}N_{>-\gamma} \subseteq N_{>-\beta}$$

for $\beta = \gamma + \varphi(f) \in \Gamma_{\geq 0}$, verifying the required assumption in Proposition **??** and completing the proof of Theorem 3.1 .

4. Strongly leveled maps

The purpose of this section and of the following §?? is to show that when $N \lhd D^\times$ and $D^\times/N$ satisfies property $(3\frac{1}{2})$, N admits a leveled map satisfying all the hypotheses (1)-(3) and (4′) made in Theorem ??. In fact we will show in §5 that the mere assumption that $\Delta_{D^\times/N}$ has diameter ≥ 3 implies the existence of a strongly leveled map $\varphi\colon N \to \Gamma$, which we now define.

Definition 4.1. Let $\varphi\colon N \to \Gamma$ be a surjective homomorphism onto a partially ordered group Γ (with $\Gamma_{>0} \neq \emptyset$). We say that φ is a *strongly leveled map* (or an *s-leveled map* for short) if there exists $\alpha \in \Gamma_{\geq 0}$ (called an *s-level* of φ) such that

$$1 \pm N_{>\alpha} \subseteq N_{\leq 0}. \tag{SL}$$

We note that although we keep the assumption $-1 \in N$, we are not assuming that $-1 \in \operatorname{Ker}\varphi$, which explains the presence of $\pm$ in (SL). Now, if $\alpha \in \Gamma_{\geq 0}$ is an s-level of φ, then for any $n \in N_{<-\alpha}$ one has

$$\varphi(1+n) = \varphi(n(1+n^{-1})) \leq \varphi(n) < -\alpha$$

as $1 + n^{-1} \in 1 + N_{>\alpha} \subseteq N_{\leq 0}$, i.e. $1 + n \in N_{<-\alpha}$. Thus, any s-leveled map is leveled (with the same level). We also observe that given an s-level, say α, of φ, any $\beta \in \Gamma_{\geq\alpha}$ is an s-level of φ as well.

We let $\mathcal{A}$ (resp., $\mathcal{R}$) denote the subring of D generated by $N_{>\alpha}$ (resp., by $N_{\geq 0}$); obviously, $\mathcal{A}$ (resp., $\mathcal{R}$) coincides with the set of all elements of the form $\epsilon_1 a_1 + \cdots + \epsilon_l a_l$ with $\epsilon_i = \pm 1$ and $a_i \in N_{>\alpha}$ (resp., $a_i \in N_{\geq 0}$). We also set $U := \operatorname{Ker}\varphi$. The arguments in §5 and the hypotheses of Theorem ?? involve certain properties of the rings $\mathcal{A}$ and $\mathcal{R}$ and of s-leveled maps. Some of these properties will be established in this section.

Proposition 4.2. *Let $\varphi\colon N \to \Gamma$ be a strongly leveled map having an s-level α. Then,*
(1) *$\mathcal{R} \cap N_{<-\alpha} = \emptyset$; in particular $\mathcal{R} \neq D$.*
(2) *If $K^\times \subseteq N$ and the subgroup $\Gamma_K := \varphi(K^\times)$ is totally ordered, then $\Gamma_K \neq \{0\}$ and φ possesses an s-level belonging to $(\Gamma_K)_{\geq 0}$.*
(3) *If there exists $\mu \in \Gamma_{\geq 0}$ such that $\mathcal{A} \cap N \subseteq N_{>-\mu}$, then there exists $\gamma \in \Gamma_{\geq 0}$ such that $\mathcal{R} \cap N \subseteq N_{>-\gamma}$.*

We begin with the following proposition which establishes some properties of the ring $\mathcal{A}$.

Proposition 4.3. (1) $1 \pm N_{>\alpha} \subseteq U$;
(2) $U \pm \mathcal{A} \subseteq U$;
(3) $1 \notin \mathcal{A}$;
(4) *given $m \in \mathcal{A} \cap N_{\geq 0}$, the element $\beta := \varphi(m)$ is an s-level for φ.*

Proof. (1): Let $n \in N_{>\alpha}$ and $\epsilon \in \{1, -1\}$. Then $1 + \epsilon n \in N_{\leq 0}$ by the definition of an s-leveled map, so we need to show only that $(1+\epsilon n)^{-1} \in N_{\leq 0}$. We notice that

$$(1+\epsilon n)^{-1} = 1 - \epsilon n(1+\epsilon n)^{-1}. \tag{i}$$

Since $1+\epsilon n \in N_{\leq 0}$, we obtain that $n(1+\epsilon n)^{-1} \in N_{>\alpha}$, so it follows from (**??**) that $(1+\epsilon n)^{-1} \in N_{\leq 0}$, as required.

(2)&(3): Since $UN_{>\alpha} \subseteq N_{>\alpha}$, we obtain using (1) that for $u \in U$ and $n \in N_{>\alpha}$, one has

$$u \pm n = u(1 \pm u^{-1}n) \in U.$$

Thus, $U \pm N_{>\alpha} \subseteq U$, and (2) follows. As $0 = 1 - 1 \notin U$, (2) implies (3).

(4): If $n \in N_{>\beta}$, where $\beta = \varphi(m)$, then $nm^{-1} \in N_{\geq 0}$, implying that $n = (nm^{-1})m \in \mathcal{A}$. Thus $N_{>\beta} \subseteq \mathcal{A}$ and then by (2), $1 \pm N_{>\beta} \subseteq N_{\leq 0}$, hence, by definition, β is an s-level for φ. □

Proof of Proposition **??**. (1): The inclusion $N_{\geq 0}N_{>\alpha} \subseteq N_{>\alpha}$ implies that $\mathcal{R}\mathcal{A} \subseteq \mathcal{A}$. Now, if $z \in \mathcal{R} \cap N_{<-\alpha}$, then $z^{-1} \in N_{>\alpha} \subseteq \mathcal{A}$, so $1 = zz^{-1} \in \mathcal{A}$, contradicting Proposition **??**(3).

(2): We take an arbitrary $s \in N_{>\alpha}$, and let $p(x) = a_t x^t + a_{t-1}x^{t-1} + \cdots + a_0$ be the minimal polynomial of s over K. Since $\Gamma_K = \varphi(K^\times)$ is totally ordered, $\delta = \min\{\varphi(a_i) \mid a_i \neq 0\}$ is defined; we choose a j so that $\delta = \varphi(a_j)$. Multiplying by a_j^{-1}, we obtain the following relation

$$b_t s^t + \cdots + b_0 = 0,$$

where $b_i = a_j^{-1}a_i$, and $b_i \in N_{\geq 0}$ for all i such that $b_i \neq 0$. Of course $b_0 \neq 0$, and we have,

$$b_0 = -(b_t s^t + \cdots + b_1 s) \in \mathcal{A} \cap N_{\geq 0},$$

so according to Proposition **??**(4), $\beta = \varphi(b_0) \in (\Gamma_K)_{\geq 0}$ is an s-level for φ. Furthermore, $b_0 \notin U$, as otherwise we would have $1 = b_0^{-1}b_0 \in U\mathcal{A} \subseteq \mathcal{A}$, contradicting Proposition **??**(3). Thus, $\Gamma_K \simeq K^\times/(K^\times \cap U)$ is nontrivial.

(3): Again, take an arbitrary $s \in N_{>\alpha}$. Then $sN_{\geq 0} \subseteq N_{>\alpha}$, implying $s\mathcal{R} \subseteq \mathcal{A}$. Thus, $\mathcal{R} \cap N \subseteq (s^{-1}\mathcal{A}) \cap N = s^{-1}(\mathcal{A} \cap N)$. It follows that

$$\mathcal{R} \cap N \subseteq s^{-1}(\mathcal{A} \cap N) \subseteq s^{-1}N_{>-\mu} \subseteq N_{>-\gamma}$$

for $\gamma := \mu + \varphi(s)$.

5. Strongly leveled maps in diameter ≥ 3 and property $(3\frac{1}{2})$

In this section $-1 \in N \subseteq D^\times$ is a *normal* subgroup of finite index. The purpose of this section is to show that the mere hypothesis that $diam(\Delta_{D^\times/N}) \geq 3$, implies the existence of a strongly leveled map $\varphi\colon N \to \Gamma$ having an s-level α. Furthermore, $\mathcal{A} \cap N \subseteq N_{>-\mu}$, for some $\mu \in \Gamma_{\geq 0}$, where $\mathcal{A}$ is the subring of D generated by $N_{>\alpha}$. The additional assumption that $D^\times/N$ satisfies property $(3\frac{1}{2})$ is used only to show that in this case we can furthermore choose φ so that the subgroup $\varphi(K^\times) \subseteq \Gamma$ is totally ordered (where K is the center of D and note that when $diam(\Delta_{D^\times/N}) \geq 3$, $K^\times \subseteq N$). Then, together with Proposition **??** this implies that φ satisfies all the hypotheses (1)-(3) and (4′) of Theorem **??** of §2. This is proved in Theorem **??** at the end of this section.

We start by recalling some notation, definitions and preliminary results from §§1-3 of [**?**] and §§6-7 of [**?**]. For an element $x \in D^\times$, we let x^* denote its image in $D^\times/N$. In addition $\Delta = \Delta_{D^\times/N}$ is the commuting graph of $D^\times/N$, and $d(\ ,\ )$ is the distance function in Δ.

$$\text{Given } x \in D^\times, \text{ we let } N(x) = \{n \in N \mid x + n \in N\}.$$

Recall that $\emptyset \subsetneqq N(x) \subsetneqq N$, for any $x \in D^\times \smallsetminus N$ (Lemma 1.8 in [**?**]). For $x \in D^\times \smallsetminus N$ we define the relation $\mathfrak{P}_{x^*}$ on N (§6 in [**?**]) by

$$m\mathfrak{P}_{x^*}n \quad \Leftrightarrow \quad N(mx) \subseteq N(nx) \qquad m, n \in N.$$

The relation $\mathfrak{P}_{x^*}$ is independent of the coset representative x, and is a preorder relation compatible with the group structure (Lemma 6.4 in [**?**]). It follows that

$$U_{x^*} = \{n \in N \mid N(nx) = N(x)\}$$

is a normal subgroup of N yielding the partially ordered group $\Gamma_{x^*} := N/U_{x^*}$ with the order relation $\leq_{x^*}$ induced by $\mathfrak{P}_{x^*}$, and the (canonical) homomorphism $\varphi_{x^*}\colon N \to \Gamma_{x^*}$. Let us recall further the notation

$$\mathbb{P}_{x^*} = \{a \in xN \mid 1 \in N(a)\},$$

and that by 1.8(5) in [**?**], $\mathbb{P}_{x^*} \neq \emptyset$, for $x \in D^\times \smallsetminus N$.

Proposition 5.1. *Let $x \in D^\times \smallsetminus N$.*
(1) *For $n \in N \smallsetminus N(x)$, the elements x^* and $(x+n)^*$ commute in G^*, hence $d(x^*, (x+n)^*) \leq 1$.*
(2) *Let $n \in N$ and $g \in D^\times$, then $N(nx) = nN(x)$, $N(xn) = N(x)n$ and $N(x^g) = g^{-1}N(x)g$ (where $x^g = g^{-1}xg$).*
(3) *If $n^{-1} \in N(x^{-1})$, then $x + n \in xN$; in particular, $n \notin N(x)$.*
(4) *$N_{\leq_{x^*}0} = \{n \in N \mid n \in N(a),\ \forall a \in \mathbb{P}_{x^*}\}$, in particular, $\varphi_{x^*}(m) \leq_{x^*} \varphi_{x^*}(n)$, iff $na + m \in N$, for all $a \in \mathbb{P}_{x^*}$.*
(5) *If $a \in xN$ and $n \in N(a)$, then $\varphi_{x^*}(m) \leq_{x^*} \varphi_{x^*}(n)$ implies that $m \in N(a)$.*

Proof. Part (1) is 2.1 in [**?**] and part (2) comes from 1.8(1) and 1.8(2) in [**?**]. Part (3) is immediate from the definitions. Parts (4) and (5) are Lemmas 6.5(1) and 6.5(3) in [**?**]. □

The next proposition gives some preliminary results when $diam(\Delta) \geq 3$. Most of these results were already established in [**?**].

Proposition 5.2. *Suppose $x, y \in D^\times \smallsetminus N$ are such that $d(x^*, y^*) \geq 3$, and let $a \in xN$, $b \in yN$, and $\epsilon \in \{1, -1\}$. Then*
(1) *$a + b \notin N$ and $N(a + b) = N(a) \cap N(b)$.*
(2) *If $\epsilon \in N(a)$, then $N(b) \subseteq N(ab) \cap N(ba)$.*
(3) *If $\epsilon \in N(a^{-1})$, then $N(ab) \cup N(ba) \subseteq N(b) \cap N(-b)$.*
(4) *If $1 \in N(a)$ then $1 + a \in U_{y^*}$.*
(5) *If $1 \in N(a)$, then $N(a^{-1}) \subseteq N_{\leq_{y^*}0}$, but $N(a^{-1}) \nsubseteq U_{y^*}$.*
(6) *$N_{<_{y^*}0} \neq \emptyset$, and $N_{\leq_{y^*}0} \nsubseteq K^\times$.*

Proof. Parts (1), (2) and (3) are respectively Lemmas 6.8(1), 6.9(2) and 6.9(3), and (4) is a particular case of Lemma 7.2 in [**?**]. To prove (5) suppose $1 \in N(a)$ and let $c \in \mathbb{P}_{y^*}$. By (2) and (3) we have

$$N(a^{-1}) \subseteq N(a^{-1}c) \subseteq N(c).$$

As this holds for all $c \in \mathbb{P}_{y^*}$, Proposition **??**(4) implies that $N(a^{-1}) \subseteq N_{\leq_{y^*} 0}$. Next, by (2) $N(a^{-1}c^{-1}) \subseteq N(a^{-1}) \cap N(c^{-1})$, so for $n \in N(a^{-1}c^{-1})$ we have $n \in N_{\leq_{y^*} 0}$, and $n \in N(c^{-1})$. By Proposition **??**(3), $n^{-1} \notin N(c)$, so $n^{-1} \notin U_{y^*}$, and it follows that $n \notin U_{y^*}$. The first part of (6) follows from (5). For the second part assume $1 \in N(a) \cap N(b)$. As in the proof of (5), $N(a^{-1}b^{-1}) \subseteq N_{<_{y^*} 0}$. By [**?**], [**?**], there exists $n, m \in N$ such that $a^{-1}b^{-1} = n - m$. But since $K^\times \subseteq N$, we can not have $m, n \in K$. Note however, that $m, -n \in N(a^{-1}b^{-1})$, so we see that $N(a^{-1}b^{-1}) \nsubseteq K$. □

Proposition 5.3. *Let $x, y \in D^\times \smallsetminus N$ with $d(x^*, y^*) \geq 3$. Let $a \in \mathbb{P}_{x^*}$, $b \in \mathbb{P}_{y^*}$ and set $z = a^{-1}b^{-1}$. Then*
(1) *For $n \in N(a^{-1}b^{-1})$ we have $(N(a) \cap N(b)) \pm n^{-1} \subseteq N(a) \cap N(b)$.*
(2) *For all $n \in N(z)$ we have $1 \pm n^{-1} \in N_{\leq_{z^*} 0}$.*
(3) *$N(z) \subseteq N_{\leq_{z^*} 0}$ and for $m \in N(z)$ we have that $\varphi_{z^*}(m^{-1})$ is an s-level of φ_{z^*}.*
(4) *φ_{y^*} (and φ_{x^*}) possess an s-level.*

Proof. (1): Note that by Proposition **??**(3), for $\nu = \pm 1$ we have $N(a^{-1}b^{-1}) \subseteq N(\nu a^{-1}) \cap N(\nu b^{-1})$. Let now $n \in N(a^{-1}b^{-1})$, then

$$a + b = (a + n^{-1}) + (b - n^{-1})$$

however, since $\pm n \in N(a^{-1}) \cap N(b^{-1})$, we have $a + n^{-1} \in aN$ and $b - n^{-1} \in bN$ (Proposition **??**(3)). Thus using Proposition **??**(1) we get $N(a + b) = N(a + n^{-1}) \cap N(b - n^{-1})$. Writing $a + b = (a - n^{-1}) + (b + n^{-1})$ and arguing similarly we get that $N(a + b) = N(a - n^{-1}) \cap N(b + n^{-1})$. So

$$N(a + b) = N(a + \epsilon n^{-1}) \cap N(b + \epsilon n^{-1}), \qquad \epsilon \in \{1, -1\}.$$

Let now $m \in N(a) \cap N(b) = N(a + b)$. Then $a + \epsilon n^{-1} + m \in N \ni b + \epsilon n^{-1} + m$, so if $\epsilon n^{-1} + m \notin N$, then by Proposition **??**(1), $a^*, (\epsilon n^{-1} + m)^*, b^*$ is a path in Δ, contradicting $d(a^*, b^*) \geq 3$. This shows that $m \pm n^{-1} \in N(a) \cap N(b)$.

(2): Let $n \in N(z)$; since $1 \in N(a) \cap N(b)$, we see that by (1), $1 \pm n^{-1} \in N$. Let $c \in \mathbb{P}_{z^*}$. By Proposition **??**(4) (as $d(x^*, z^*) \geq 3 \leq d(y^*, z^*)$), we have $c + 1 \in U_{x^*} \cap U_{y^*} \subseteq N(a) \cap N(b)$. By (1), $c + 1 \pm n^{-1} \in N(a) \cap N(b)$. As this holds for all $c \in \mathbb{P}_{z^*}$, we get that $1 \pm n^{-1} \in N_{\leq_{z^*} 0}$ (Proposition **??**(4)).

(3): Let $m \in N(z)$, then $m \in N(a^{-1})$. Since $d(x^*, z^*) \geq 3$, it follows from Proposition **??**(5) that $m \in N_{\leq_{z^*} 0}$. Set $\alpha = \varphi_{z^*}(m^{-1})$ and note that $0 \leq_{z^*} \alpha \in \Gamma_{z^*}$. Let $n \in N_{>_{z^*} \alpha}$, then $\varphi_{z^*}(n^{-1}) <_{z^*} \varphi_{z^*}(m)$, so by Proposition **??**(5), $n^{-1} \in N(z)$. By part (2), $1 \pm n \in N_{\leq_{z^*} 0}$.

(4): What we saw in (3) in fact is that if $d(r^*, s^*) \geq 3$, then $\varphi_{(r^{-1}s^{-1})^*}$ possess an s-level. So take $r = x^{-1}$ and $s = y^{-1}x$ and be done. □

Proposition 5.4. *Let $x, y \in D^\times \smallsetminus N$ with $d(x^*, y^*) \geq 3$. Let $0 \leq \alpha \in \Gamma_{y^*}$ be an s-level of φ_{y^*} and let $\mathcal{A}$ be the subring of D generated by $N_{>_{y^*}\alpha}$. Suppose $a \in \mathbb{P}_{x^*}$, $b \in \mathbb{P}_{y^*}$ and let $m \in N(a^{-1}b^{-1})$. Then for $\mu >_{y^*} \varphi_{y^*}(m^{-1})$, we have that $0 \leq \mu \in \Gamma_{y^*}$ and $\mathcal{A} \cap N \subseteq N_{>-\mu}$.*

Proof. First we claim that

$$N(a^{-1}b^{-1}) \pm 1 \subseteq N(a^{-1}b^{-1}). \tag{i}$$

Indeed set $z = a^{-1}b^{-1}$ and let $n \in N(z)$. By Proposition **??**(2),

$$n^{-1}(n \pm 1) = 1 \pm n^{-1} \in N_{\leq_{z^*} 0},$$

this means that $\varphi_{z^*}(n \pm 1) \leq_{z^*} \varphi_{z^*}(n)$. By proposition **??**(5), as $n \in N(z)$ also $n \pm 1 \in N(z)$ and (**??**) is proved.

Set $\leq = \leq_{y^*}$, $\varphi = \varphi_{y^*}$ and let $m \in N(z)$. As $m \in N(a^{-1})$, Proposition **??**(5) implies that $m \in N_{\leq 0}$, so $\mu > 0$. Hence to complete the proof it suffices to show that

$$\mathcal{A} \cap N \subseteq N_{\geq \varphi(m)}. \tag{ii}$$

Let $n \in \mathcal{A} \cap N$. We must show that $\varphi(n) \geq \varphi(m)$, i.e., that $nt + m \in N$, for all $t \in \mathbb{P}_{y^*}$ (see Proposition **??**(4)). We have

$$nt + m = (n+1)t + (-t + m). \tag{iii}$$

Now

$$-t + m = (1+t)(-1 + (1+t)^{-1}(1+m)) \in N(a^{-1}b^{-1}), \tag{iv}$$

indeed $t + 1 \in U_{(a^{-1}b^{-1})^*}$ by Proposition **??**(4), and by (**??**), $1 + m \in N(a^{-1}b^{-1})$. It follows (using also Proposition **??**(2)) that $(1+t)^{-1}(1+m) \in N(a^{-1}b^{-1})$ and then by (**??**) again $-1 + (1+t)^{-1}(1+m) \in N(a^{-1}b^{-1})$, so we see from (**??**) that $-t + m \in N(a^{-1}b^{-1}) \subseteq N(a^{-1})$. In particular, by Proposition **??**(5), $-t + m \in N_{\leq 0}$. On the other hand, by Proposition **??**(2) we have $n + 1 \in \operatorname{Ker} \varphi = U_{y^*}$, and therefore $(n+1)t \in \mathbb{P}_{y^*}$. Hence, by (**??**) and Proposition **??**(4), $nt + m \in N$, completing the proof of (**??**) and of the proposition. □

We now turn to the proof that (after perhaps interchanging x and y) the subgroup $\varphi_{y^*}(K^\times) \subseteq \Gamma_{y^*}$ is totally ordered. This does not follow from the hypothesis that $d(x^*, y^*) \geq 3$, because as we will see, the fact that $\varphi_{y^*}(K^\times)$ is totally ordered implies that N is open with respect to a single valuation. This is not generally true when $d(x^*, y^*) = 3$ (see Example 8.4 in [**?**]). Hence we will need the following crucial additional hypothesis.

Property $(3\frac{1}{2})$: Given a finite group H and elements c, d in the commuting graph Δ_H of H (having distance function $d_H(\ ,\ )$), we will say that (H, c, d) *satisfy property* $(3\frac{1}{2})$, *if for every $a, b \in \Delta_H$ such that $[c, a] = 1 = [d, b]$, there exists $h \in H$ satisfying $d_H(c^h, d) \geq 3$ and $[a^h, b] \neq 1$. When the group H is understood from the context, we will just say that c, d satisfy property* $(3\frac{1}{2})$.

As we mentioned in the introduction (see Theorem 2), a crucial point for us in this paper is that property $(3\frac{1}{2})$ is satisfied by minimal nonsolvable finite groups (see §**??**). We need some notation.

Notation 5.5. (1) Given $r \in D^\times \smallsetminus N$ we denote by $\dot{N}(r) = N(r) \cap K$. Note that though $N(r)$ is always nonempty, $\dot{N}(r)$ may well be empty.

(2) For $r, s \in D^\times \smallsetminus N$, we define $\mathrm{In}_K(r^*, s^*)$ and $\mathrm{Inc}_K(r^*, s^*)$ as we define $\mathrm{In}(\ ,\ )$ and $\mathrm{Inc}(\ ,\ )$ in [**?**], pg. 228, using $\dot{N}(\ )$ instead of $N(\ )$: $\mathrm{In}_K(r^*, s^*)$ means that for all pairs $(a, b) \in (rN \times sN)$, either $\dot{N}(a) \subseteq \dot{N}(b)$ or $\dot{N}(b) \subseteq \dot{N}(a)$ and $\mathrm{Inc}_K(r^*, s^*)$ means that $\mathrm{In}_K(r^*, s^*)$ holds and, in addition, given $c \in \mathbb{P}_{r^*}$, there exists $d \in \mathbb{P}_{s^*}$ with $\dot{N}(c) \supseteq \dot{N}(d)$.

For the sake of completeness we include here the following lemma which is actually part of Lemma 6.12 in [**?**].

Lemma 5.6. *Let $x, y \in D^\times \smallsetminus N$. Then*
(1) *If $\mathrm{In}_K(x^*, y^*)$, then either $\mathrm{Inc}_K(x^*, y^*)$ or $\mathrm{Inc}_K(y^*, x^*)$.*
(2) *If $\mathrm{Inc}_K(y^*, x^*)$, then $\mathrm{In}_K(y^*, y^*)$.*

Proof. Suppose $\mathrm{Inc}_K(x^*, y^*)$ does not hold. Then there is $a \in \mathbb{P}_{x^*}$ such that $\dot{N}(a) \subseteq \dot{N}(b)$, for all $b \in \mathbb{P}_{y^*}$, so $\mathrm{Inc}_K(y^*, x^*)$ holds, proving (1). Now, assume $\mathrm{Inc}_K(y^*, x^*)$ and let $b, c \in yN$ be such that $\dot{N}(b) \nsubseteq \dot{N}(c)$. Pick $n \in \dot{N}(b)$, $n \notin \dot{N}(c)$. Then $\dot{N}(n^{-1}b) \ni 1 \notin \dot{N}(n^{-1}c)$ (we note that $n \in K^\times$, so $\dot{N}(n^{-1}c) = n^{-1}\dot{N}(c)$, for any $c \in D^\times \smallsetminus N$). By $\mathrm{Inc}_K(y^*, x^*)$, we can pick $a \in \mathbb{P}_{x^*}$ with $\dot{N}(n^{-1}b) \supseteq \dot{N}(a)$. Since $1 \notin \dot{N}(n^{-1}c)$, the inclusion $\dot{N}(a) \subseteq \dot{N}(n^{-1}c)$ is impossible, so by $\mathrm{In}_K(x^*, y^*)$ we have $\dot{N}(n^{-1}c) \subseteq \dot{N}(a) \subseteq \dot{N}(n^{-1}b)$, hence $\dot{N}(c) \subseteq \dot{N}(b)$, as required. □

Proposition 5.7. *Let $x^*, y^* \in D^\times/N$ such that $d(x^*, y^*) \geq 3$ and x^*, y^* satisfy property $(3\frac{1}{2})$. Then*
(1) *$\mathrm{In}_K(x^*, y^*)$ holds.*
(2) *After perhaps interchanging x^*, y^* we have that the subgroup $\varphi_{y^*}(K^\times) \subseteq \Gamma_{y^*}$ is totally ordered.*

Proof. Let $c \in xN$ and $d \in yN$ such that $\dot{N}(c) \nsubseteq \dot{N}(d)$ and $\dot{N}(d) \nsubseteq \dot{N}(c)$. Picking $n \in \dot{N}(c) \smallsetminus \dot{N}(d)$ and replacing c, d with $-n^{-1}c, -n^{-1}d$, we may assume that $-1 \in \dot{N}(c) \smallsetminus \dot{N}(d)$. By our assumption, there exists $k \in \dot{N}(d) \smallsetminus \dot{N}(c)$. Since by Proposition 5.1(1) we have

$$[c^*, (c+k)^*] = [(d-1)^*, d^*] = 1,$$

and by hypothesis c^*, d^* satisfy property $(3\frac{1}{2})$, there exists $g \in D^\times$ such that $d((c^g)^*, d^*) \geq 3$ and $((c+k)^g)^* = (c^g + k)^*$ does not commute with $(d-1)^*$. Note however that $-1 \in N(c^g)$ and it follows from Proposition **??**(2) that $k \in N(d) \subseteq N(dc^g)$. In view of Proposition **??**(1) and the fact that $dc^g + k \in N$, we have

$$[(c^g + k)^*, (d-1)^*] = [d^*(c^g + k)^*, (d-1)^*] = [((dc^g + k) + (d-1)k)^*, ((d-1)k)^*] = 1.$$

This is a contradiction.

(2): By (1), $\mathrm{In}_K(x^*, y^*)$ holds so by Lemma **??**(1), we may assume (after perhaps interchanging x^* and y^*) that $\mathrm{Inc}_K(y^*, x^*)$ holds. By Lemma **??**(2), $\mathrm{In}_K(y^*, y^*)$ holds. Let $k \in K^\times$ and assume $k \notin N_{\leq_{y^*}0}$. Let $b \in yN$, with $k \notin N(b) \ni 1$. Then $1 \notin N(k^{-1}b) \ni k^{-1}$. From $\mathrm{In}_K(y^*, y^*)$, we see that $k^{-1} \in N(s)$, for all $s \in \mathbb{P}_{y^*}$, so $k^{-1} \in N_{\leq_{y^*}0}$. This means that the subgroup $\varphi_{y^*}(K^\times) \subseteq \Gamma_{y^*}$ is totally ordered. □

The following theorem summarizes the results of §§4-5.

Theorem 5.8. *Let $y \in D^\times \smallsetminus N$ be an element for which there exists $x \in D^\times \smallsetminus N$ with $d(x^*, y^*) \geq 3$. Set $\varphi = \varphi_{y^*}$ and $\Gamma = \Gamma_{y^*}$. Then*

(1) *Γ is nontrivial and $N_{\geq 0} \nsubseteq K^\times$.*
(2) *φ is a strongly leveled map.*
(3) *If $\mathcal{R} \subseteq D$ is the subring generated by $N_{\geq 0}$, then $\mathcal{R} \cap N \subseteq N_{>-\gamma}$ for some $\gamma \in \Gamma_{\geq 0}$.*

Furthermore, if x^*, y^* satisfy property $(3\frac{1}{2})$ then after interchanging x^* and y^* if necessary we have that $\Gamma_K = \varphi(K^\times)$ is a nontrivial totally ordered subgroup of Γ and that φ possess an s-level in $(\Gamma_K)_{\geq 0}$.

Proof. Part (1) follows from Proposition **??**(6) and part (2) is Proposition **??**(4). Part (3) is a consequence of Proposition **??** and Proposition **??**(3). Assume that x^*, y^* satisfy property $(3\frac{1}{2})$. Then by Proposition **??**(2), after perhaps interchanging x^* and y^* we have that Γ_K is totally ordered, so Proposition **??**(2) completes the proof. □

6. The main theorem: proof and applications

Combining Theorem **??** and Theorem **??**, we obtain the following.

Theorem 6.1. *Let D be a finite dimensional division algebra over a finitely generated infinite field, $N \subseteq D^\times$ be a normal subgroup of finite index. If $D^\times/N$ satisfies property $(3\frac{1}{2})$, then N is open in $D^\times$ with respect to a nontrivial height one valuation of D.*

Indeed, observe that if $x^*, y^* \in D^\times/N$ satisfy property $(3\frac{1}{2})$, then we may assume without loss that $d_{D^\times/N}(x^*, y^*) \geq 3$, so Theorem **??** applies and yields the homomorphism $\varphi_{y^*} \colon N \to \Gamma_{y^*}$ satisfying all hypotheses (1)-(3) and (4′) of Theorem **??**. So Theorem **??** completes the proof.

Another ingredient in the proof of our Main Theorem is the Nonexistence Theorem stated in the introduction. For the reader's convenience we give here a brief summary of its proof, referring to [**?**] for the details.

Sketch of the proof of The Nonexistence Theorem. Suppose the conclusion of the theorem is false, and let $H \in \mathcal{G}$ be a member of minimal possible order which is a quotient of the multiplicative group of some finite dimensional central division algebra. Consider hereafter only finite dimensional division algebras D such that H is a quotient of $D^\times$ and let K denote the center of D. If there exists such a D having a positive characteristic, we will consider only division algebras in this positive characteristic; otherwise, all algebras considered will have characteristic zero. We show that we may choose D so that K is finitely

generated over its prime subfield K_0; in particular, the transcendence degree $t = \mathrm{tr.deg}_{K_0} K$ is finite. We furthermore choose D so that t is minimal (we observe that, due to Wedderburns' theorem, $t > 0$). Let $N = \mathrm{Ker}(D^\times \to H)$. It follows from condition (4) in the Nonexistence Theorem that N is open in $D^\times$ with respect to a nontrivial height one valuation v of D as H was chosen to be minimal. Let $\bar{D} := \bar{D}_v$ be the residue division algebra. We show that the openness of N implies the existence of a normal subgroup $\bar{N} \subseteq \bar{D}^\times$ such that the following holds. There exists $M_1 \lhd H_1 \lhd H$ with M_1, H/H_1 solvable and $\bar{D}^\times/\bar{N} \cong H_1/M_1$. However, conditions (1)-(3) together with the minimality of H imply that $H_1 = H$ and $M_1 = \{1\}$, i.e., H will be a quotient of $\bar{D}^\times$ as well. But, by our characteristic choices (together with valuation theory), $\bar{D}_v$ will have the same characteristic as D, and then a result in valuation theory implies that the transcendence degree of the center of $\bar{D}_v$ over its prime subfield will be strictly less than t. This is a contradiction, and the Nonexistence Theorem follows. □

Now, the class $\mathcal{G} = \mathcal{NS}$ of all nonsolvable groups obviously satisfies conditions (1)-(3) of the Nonexistence Theorem. Furthermore, by Theorem 2 of the introduction, which will be proved in §**??**, minimal members of $\mathcal{NS}$ satisfy property $(3\frac{1}{2})$. In conjunction with Theorem **??** this implies that condition (4) holds for $\mathcal{NS}$ as well. Thus we obtain

Main Theorem. *Let D be a finite dimensional division algebra. Then any finite quotient of the multiplicative group $D^\times$ is solvable.*

The rest of the section is devoted to applications of the Main Theorem primarily to the normal subgroups of the group $SL(1, D)$ of elements in $D^\times$ having reduced norm one.

Corollary 6.2. *Let $N \subseteq SL(1, D)$ be a subgroup of finite index which is normal in $D^\times$. Then the quotient $SL(1, D)/N$ is solvable.*

Proof. The group $D^\times$ acts on $SL(1, D)/N =: B$ by conjugation, and we let M denote the kernel of this action. Then

$$B/Z(B) \simeq \mathrm{Int}\, B \hookrightarrow D^\times/M.$$

But the group $D^\times/M$ is finite (as a subgroup of the automorphism group of the finite group B), hence solvable by the Main Theorem, and the solvability of B follows. □

Here is one case where Corollary **??** gives the solvability of *all* finite quotients of $SL(1, D)$.

Corollary 6.3. *Let D be a finite dimensional division algebra over a global field K. Then any finite quotient of $SL(1, D)$ is solvable.*

Proof. Let $N \subseteq SL(1, D)$ be a normal subgroup of a finite index m. We denote by N_0 the subgroup generated by the elements g^m, $g \in SL(1, D)$. Then $N_0 \subseteq N$ and $N_0 \lhd D^\times$. Since $SL(1, D)$ does not have finite exponent (this follows from its Zariski density in the corresponding algebraic group $\mathbf{SL}_{1,D}$ which is isomorphic to $\mathbf{SL}_n$ over the algebraic closure of K), N_0 is noncentral and therefore, by a theorem[1] due to Margulis and Prasad (see [**?**],

[**?**]), N_0 has a finite index in $SL(1,D)$. By Corollary **??**, the quotient $SL(1,D)/N_0$ is solvable, and then so is $SL(1,D)/N$. □

Remark. In view of the Margulis-Prasad theorem, Corollary **??** in effect yields the solvability of any quotient of $SL(1,D)$ by a noncentral normal subgroup.

The question whether or not Corollary **??** extends to division algebras over arbitrary fields remains open (we note that this is exactly Question 2 of the introduction for the algebraic group $G = \mathbf{SL}_{1,D}$ associated with $SL(1,D)$). Obviously, for the affirmative answer it would be sufficient to show that any finite index normal subgroup $N \subseteq SL(1,D)$ contains a finite index subgroup $N_0 \subseteq SL(1,D)$ which is normal in $D^\times$. In other words, one needs to show that $\bigcap_{g\in D^\times}(gNg^{-1})$ has finite index in $SL(1,D)$, or equivalently, that among the subgroups gNg^{-1}, $g \in D^\times$, there are only finitely many distinct. In this regard, we observe that one of the ingredients of the proof of the Margulis-Prasad theorem is the fact that if G is an absolutely simple simply connected algebraic group over a global field K, then there exists an S-arithmetic subgroup $\Gamma \subseteq G(K)$ for a sufficiently large finite set of places S such that $\Gamma N = G(K)$ for any noncentral normal subgroup $N \subseteq G(K)$, implying $G(K)/N \simeq \Gamma/(\Gamma \cap N)$. If $\mathrm{char}\, K = 0$, then Γ is always finitely generated (cf. [**?**], Theorem 5.11), and if $\mathrm{char}\, K > 0$ then one can enlarge S to make Γ finitely generated (cf. Behr [**?**]). Then Γ, and therefore also $G(K)$, has only finitely many homomorphisms to any given finite group. In the set-up above, this gives the finiteness of the number of distinct conjugates gNg^{-1}, $g \in D^\times$. To what extent this kind of an argument can be generalized to arbitrary (finitely generated) fields remains to be seen.

We now turn to Margulis-Platonov conjecture (conjecture (MP)). We refer the reader to Ch. IX in [**?**] and Appendix A in [**?**] for a detailed discussion of (MP). The proof of (MP) for $G = \mathbf{SL}_{1,D}$ was recently completed in [**?**] and [**?**], using a reduction obtained in [**?**]. One application of our Main Theorem is a short proof of (MP) for $G = \mathbf{SL}_{1,D}$ which does not require the reduction of [**?**].

Theorem 6.4. *Let D be a division algebra over a global field K. Then the group $G = \mathbf{SL}_{1,D}$ satisfies the Margulis-Platonov conjecture.*

Proof. We recall that (MP) for the group $G = \mathbf{SL}_{1,D}$ is equivalent to the statement that if T is the (finite) set of all nonarchimedean places v of K for which $D \otimes_K K_v$ is a division algebra, then for any noncentral normal subgroup $N \subseteq G(K) = SL(1,D)$ there should exist an open normal subgroup $W \subseteq \prod_{v\in T} G(K_v) =: G_T$ such that $N = G(K) \cap \delta^{-1}(W)$, where $\delta\colon G(K) \to G_T$ is the diagonal embedding if $T \neq \emptyset$, and δ is the trivial map otherwise. In other words, N is open in $G(K)$ with respect to the topology defined by the valuations in T (which is sometimes called the T-adic topology). It was first proved in [**?**] (cf. also [**?**], §9.2) that if K is a number field then $N = [SL(1,D), SL(1,D)]$ is T-adically open. This fact was extended to arbitrary global fields by Raghunathan [**?**] who proved the following

[1]This theorem states that if G is an absolutely simple simply connected algebraic group over a global field K, then any noncentral normal subgroup $N \subseteq G(K)$ has finite index.

more general result: if $U \subseteq SL(1,D)$ is a T-adically open subgroup, then its commutator subgroup $[U,U]$ is also T-adically open. In effect, this implies that *any* term of the derived series for $SL(1,D)$ is T-adically open. Now, given an arbitrary noncentral normal subgroup $N \subseteq SL(1,D)$, it has finite index by the Margulis-Prasad theorem, and then the quotient $SL(1,D)/N$ is solvable by our Corollary **??**. This implies that N contains some term of the derived series of $SL(1,D)$, and the openness of N follows. □

7. Property $(3\frac{1}{2})$ for minimal nonsolvable groups

The purpose of this section is to prove Theorem 2 of the introduction, i.e., to show that minimal nonsolvable groups satisfy property $(3\frac{1}{2})$ of the introduction. Recall that for any group H, the *commuting graph* of H is the graph whose vertex set is $H \smallsetminus \{1\}$ and whose edges are commuting pairs of elements. We denote by Δ_H the commuting graph of H and by $d_H(\ ,\ )$, the usual distance function on H. So for $x, y \in \Delta_H$, $d_H(x,y)$ is the minimal number of edges in a path from x to y in Δ_H (it is ∞ if no such path exists).

Notation 7.1. Let Δ be a graph with distance function $d(\ ,\ )$ and let $x, y \in \Delta$.
(1) $\Delta(x) := \{y \in \Delta \mid d(x,y) = 1\}$.
(2) Given an integer $i \geq 1$, we denote $\Delta^{\leq i} = \{y \in \Delta \mid d(x,y) \leq i\}$. The set $\Delta^{\geq i}$ is defined similarly.
(3) Let H be a group. For $c, d \in H$, we let $c^d = d^{-1}cd$, $[c,d] = c^{-1}d^{-1}cd$ and c^H is the conjugacy class of c in H.

A *minimal nonsolvable group* is a finite group G such that G is not solvable, but G/M is solvable for every $1 \neq M \lhd G$. Throughout this section the following property of a finite group H will be considered.

Property $(3\frac{1}{2})$: There are two elements $c, d \in \Delta_H$ having the following property:
There exists a subgroup $H_1 \subseteq H$ such that for every $a \in \Delta_H(c)$ and $b \in \Delta_H(d)$, there exists $h \in H_1$ satisfying $d_H(c^h, d) \geq 3$ and $[a^h, b] \neq 1$.

When a group H satisfies property $(3\frac{1}{2})$ with some elements $c, d \in \Delta_H$, where $H_1 = H$, we will just say that H satisfies property $(3\frac{1}{2})$; or (H, c, d) satisfy property $(3\frac{1}{2})$, when we want to emphasis the elements c, d. When we want to emphasize the subgroup H_1 and the elements c, d, we will write (H, c, d, H_1) satisfies property $(3\frac{1}{2})$ (or (H, c, d, H_1) do not satisfy property $(3\frac{1}{2})$).

The purpose of this section is to prove the following theorem.

Theorem 7.2. *Let G be a minimal nonsolvable group. Then G satisfies property $(3\frac{1}{2})$.*

One may think of property $(3\frac{1}{2})$ as a property distinguishing a minimal nonsolvable group G from a direct product (of more than one group), in terms of the commuting graph. As the reader will notice, if G is a direct product, then G does not have the property $(3\frac{1}{2})$, and indeed, this may be thought of as a "reason" that certain direct products can be quotients of the multiplicative group of D while other groups ("close" to being wreath products, such as minimal nonsolvable groups) can not.

Notation 7.3. Throughout this section, G is a minimal nonsolvable group. Recall that G has a unique minimal normal subgroup K such that there exists a subgroup $L \leq K$ satisfying: L is a nonabelian simple group and K is the direct product of the distinct conjugates $L^{g_1}, \ldots, L^{g_n}$ of L, $n \geq 1$. Furthermore, G acts transitively by conjugation on the set $\{L^{g_1}, \ldots, L^{g_n}\}$, G/K is solvable and $C_G(K) = 1$. The notation K, L and $g_1, \ldots, g_n$ are fixed throughout this section. We further fix L_i to denote L^{g_i}, $1 \leq i \leq n$ and we assume $L_1 = L$. Given an element $x \in K$, $x_i \in L_i$, $(1 \leq i \leq n)$, denote the elements so that $x = x_1 \cdots x_n$. Note that when $n = 1$, G is an almost simple group, i.e, $L \subseteq G \subseteq \mathrm{Aut}(L)$.

In subsection **??** below, we will establish some further notation for G and other notation to be used throughout this section. Then we will formulate certain conditions on L that imply Theorem **??**. These conditions are given in Proposition **??**. We formulate the *generic* condition separately (see (a) of Proposition **??**).

Proposition 7.4. *Assume that there exists six distinct nonidentity conjugacy classes $B, C_1, \ldots, C_5$ of $\mathrm{Aut}(L)$ contained in L, such that $d_{\mathrm{Aut}(L)}(r, s) \geq 3$, for all $r \in B$ and $s \in \bigcup_{i=1}^{5} C_i$. Then G satisfies Property $(3\frac{1}{2})$.*

Subsection **??** is devoted to proving,

Theorem 7.5. *Let L be a nonabelian finite simple group. Then L contains six distinct nonidentity $\mathrm{Aut}(L)$-conjugacy classes $B, C_1, \ldots, C_5$ such that $d_{\mathrm{Aut}(L)}(r, s) \geq 3$, for all $r \in B$ and $s \in \bigcup_{i=1}^{5} C_i$, provided L is not isomorphic to one of the following groups:*

$$PSL(2, q),\ q = 5, 7, 8, 9, 11, 16 \text{ or } 27, \quad PSL(3, 4) \text{ or } PSO^{+}(8, 2).$$

It follows from Theorem **??** and proposition **??** that if L is not one of the 9 exceptional cases of Theorem **??**, then G satisfies property $(3\frac{1}{2})$. The purpose of the final subsection **??** is to show that in the 9 exceptional cases G also satisfies property $(3\frac{1}{2})$ and this is done using the results of subsection **??**.

7.1. Conditions on L that guarantee property $(3\frac{1}{2})$.

Throughout §**??**, we let

(i) $$X := \{L^{g_1}, \ldots, L^{g_n}\}.$$

and

(ii) $\Sigma \subseteq Sym(X)$ is the permutation group on X induced from the conjugation action of G.

Of course Σ is a solvable transitive permutation group on X. We mention that in Lemmas **??**, **??** and **??** and in the notation given in the next paragraph, we think of X as an arbitrary finite set and we think of $\Sigma \subseteq \mathrm{Sym}(X)$ as an arbitrary transitive solvable permutation group. Otherwise X and Σ are reserved to denote as in (**??**) and (ii).

We will use notation as in §2 of [**?**]. Thus given $\tau \in \mathrm{Sym}(X)$ and $Y \subseteq X$, we let $\tau(Y) := \{\tau(y) \mid y \in Y\}$, $\Sigma(Y) := \{\sigma \in \Sigma \mid \sigma(Y) = Y\}$ is the global stabilizer of Y in Σ,

$\Sigma_Y := \{\sigma \in \Sigma \mid \sigma(y) = y,\ \forall y \in Y\}$, is the pointwise stabilizer of Y in Σ. $\Sigma^Y := \Sigma(Y)/\Sigma_Y$ is the action of Σ on Y.

We use similar notation for actions on partitions. A partition $\mathcal{P}$ of X is a collection $\mathcal{P} := \{V_1, \dots, V_k\}$ of nonempty subsets of X such that V_i are pairwise disjoint and their union is X.

Given a partition $\mathcal{P}$ of X we write $\Sigma(\mathcal{P})$ for the subgroup of all permutations $\sigma \in \Sigma$ such that $\sigma(V_i) \in \mathcal{P}$, for all $1 \leq i \leq k$. We write $\Sigma_{\mathcal{P}}$ for the subgroup of all permutations $\sigma \in \Sigma$ such that $\sigma(V_i) = V_i$, for all $1 \leq i \leq k$. Finally, write $\Sigma^{\mathcal{P}} = \Sigma(\mathcal{P})/\Sigma_{\mathcal{P}}$.

We fix the following notation, except in the case when $n = 1$,

(iii) $\mathcal{M} := \{X_1, \dots, X_m\}$ $(m \geq 1)$, is a partition of X stabilized by Σ (i.e., $\Sigma = \Sigma(\mathcal{M})$), such that $|X_i| \geq 2$ and such that Σ^{X_i} is primitive.

When $n = 1$, we let $\mathcal{M} = \{L\}$. We will consider conjugacy classes C of $\mathrm{Aut}(L)$ contained in L. All such conjugacy classes are automatically assumed to be nonidentity conjugacy classes. Given such a class $C \subseteq L$, $C^{g_i} \subseteq L_i$ denotes the corresponding $\mathrm{Aut}(L_i)$ conjugacy class, $1 \leq i \leq n$ (recall that L_i, g_i are as in Notation **??**).

In order to construct elements in K satisfying various properties we need some information about actions of solvable groups on partitions. This is done in the next three lemmas.

Lemma 7.1.1. *Let $n \geq 2$ and let Σ be a transitive solvable permutation group on a set X of size n. Let $\mathcal{M} = \{X_1, \dots, X_m\}$ $(m \geq 1)$, be a partition of X stabilized by Σ, such that $|X_i| \geq 2$. Then there exists a partition $\mathcal{Q}_1 = \{V_1, \dots, V_e\}$ of X, with $2 \leq e \leq 3$ such that for all $\sigma \in \Sigma$, $\Sigma_{\sigma(\mathcal{Q}_1)} \subseteq \Sigma_{\mathcal{M}}$.*

Proof. We'll think of $\Sigma^{\mathcal{M}}$ as a permutation group on $\{1, \dots m\}$. Partition the set $\{1, \dots m\}$ into f parts, $1 \leq f \leq 5$, $\mathcal{J} = \{J_1, \dots, J_f\}$, such that $\Sigma^{\mathcal{M}}_{\mathcal{J}} = 1$. The existence of the partition $\mathcal{J}$ is guaranteed by Theorem 1.2 in [**?**] (see also Proposition 2.5 in [**?**]). If $m = 1$ then $\mathcal{Q}_1$ can be any partition of X. Otherwise write $X_i = \{x_i^1, \dots, x_i^t\}$ (so $|X_i| = t$). We define V_1 as follows

$$V_1 = \bigcup_{i \in J_1} \{x_i^1\} \cup \bigcup_{i \in J_2} \{x_i^1, x_i^2\} \cup \bigcup_{i \in J_3} \{x_i^1, x_i^2, x_i^3\}$$

where $\cup \bigcup_{i \in J_3} \{x_i^1, x_i^2, x_i^3\}$ occurs if and only if $f > 2$ and $t > 2$. If $2 \leq f \leq 3$ we define

$$V_2 = \bigcup_{i \in J_1} (X_i \smallsetminus \{x_i^1\}) \cup \bigcup_{i \in J_2} (X_i \smallsetminus \{x_i^1, x_i^2\}) \cup \bigcup_{i \in J_3} Y_i$$

where $\cup \bigcup_{i \in J_3} Y_i$ occurs if and only if $f = 3$. If $f = 2$, we let $\mathcal{Q}_1 = \{V_1, V_2\}$. If $f = 3$ and $t = 2$, we let $Y_i = X_i$ and we let $\mathcal{Q}_1 = \{V_1, V_2\}$. If $f = 3$ and $t > 2$, we let $Y_i = X_i \smallsetminus \{x_i^1, x_i^2, x_i^3\}$ and we let $\mathcal{Q}_1 = \{V_1, V_2\}$.

If $f = 4$, or $f = 5$ and $t = 2$, we let

$$V_2 = \bigcup_{i \in J_3} Y_i \cup \bigcup_{i \in J_4} \{x_i^1, x_i^2\}$$

where $Y_i = \{x_i^1\}$ if $t = 2$ and $Y_i = \emptyset$ otherwise. Next, if $f = 5$ and $t > 2$, we let

$$V_2 = \bigcup_{i \in J_4} \{x_i^1\} \cup \bigcup_{i \in J_5} \{x_i^1, x_i^2\}$$

Finally we let $V_3 = X \setminus (V_1 \cup V_2)$. The reader can easily verify that $\Sigma_{\mathcal{Q}_1}^{\mathcal{M}}$ stabilizes the partition $\mathcal{J}$ and hence acts trivially on $\mathcal{M}$, i.e., $\Sigma_{\mathcal{Q}_1} \subseteq \Sigma_{\mathcal{M}}$ and hence $\Sigma_{\sigma(\mathcal{Q}_1)} \subseteq \Sigma_{\mathcal{M}}$, for all $\sigma \in \Sigma$. □

Lemma 7.1.2. *Let $n \geq 2$ and let Σ be a transitive solvable permutation group on a set X of size n. Let $\mathcal{M} = \{X_1, \ldots, X_m\}$ $(m \geq 1)$, be a partition of X stabilized by Σ, such that $|X_i| \geq 2$ and such that Σ^{X_i} is primitive. Let $\mathcal{P}_i = \{X_i^1, \ldots, X_i^f\}$ be a partition of X_i, $1 \leq i \leq m$, and define the partition $\mathcal{Q}_2 = \{W_1, \ldots, W_f\}$ of X by*

$$W_t = \bigcup_{j=1}^{m} X_j^t \qquad 1 \leq t \leq f.$$

Then,

(1) *If $\Sigma^{X_i} \not\cong \mathrm{S}_4$, then there exists partitions $\mathcal{P}_i$, $1 \leq i \leq m$, so that $2 \leq f \leq 3$ and so that the partition $\mathcal{Q}_2$ satisfies $\Sigma_{\mathcal{M},\mathcal{Q}_2} = 1$.*
(2) *If $\Sigma^{X_i} \cong \mathrm{S}_4$, then the partitions $\mathcal{P}_i$ of X_i to singletons $1 \leq i \leq m$, yield a partition $\mathcal{Q}_2$ so that $f = 4$ and $\Sigma_{\mathcal{M},\mathcal{Q}_2} = 1$.*
(3) *If $\Sigma^{X_i} \cong \mathrm{S}_4$, then given subsets $Y_i^1, Y_i^2 \subseteq X_i$, with $|Y_i^j| = 2$ and $X_i = Y_i^1 \cup Y_i^2$, $1 \leq i \leq m$, the partitions $\mathcal{P}_i := \{Y_i^1, Y_i^2\}$, $1 \leq i \leq m$ yield a partition $\mathcal{Q}_2$ such that $\Sigma_{\mathcal{M},\mathcal{Q}_2}$ fixes Y_i^j as a set, for all $1 \leq i \leq m$ and $1 \leq j \leq 2$.*

Proof. In (1) take $\mathcal{P}_i$ so that $\Sigma_{\mathcal{P}_i}^{X_i} = 1$. The existence of $\mathcal{P}_i$ in (1) is guaranteed by Corollary 2.2 in [**?**], which says that given a primitive solvable permutation group H on a set Ω, there exists a partition $\mathcal{P}$ of Ω to at most 3 parts so that $H_{\mathcal{P}} = 1$. Parts (2) and (3) are obvious. □

Lemma 7.1.3. *Let $n \geq 2$ and let Σ be a transitive solvable permutation group on a set X of size n. Let $\mathcal{M} := \{X_1, \ldots, X_m\}$ $(m \geq 1)$, be a partition of X stabilized by Σ, such that $|X_i| \geq 2$ and such that Σ^{X_i} is primitive. Let $\mathcal{Q}_1 = \{V_1, \ldots, V_e\}$, $2 \leq e \leq 3$ and $\mathcal{Q}_2 = \{W_1, \ldots, W_f\}$, $2 \leq f \leq 4$, be partitions of X as in Lemma **??** and Lemma **??** respectively. Then*

(1) *If $\mathcal{Q}_2$ is as in part (1) or (2) of Lemma **??**, then for all $\sigma \in \Sigma$, we have $\Sigma_{\sigma(\mathcal{Q}_1),\,\mathcal{Q}_2} = 1$.*
(2) *If $\mathcal{Q}_2$ is as in part (3) of Lemma **??**, then for all $\sigma \in \Sigma$, we have $\Sigma_{\sigma(\mathcal{Q}_1),\,\mathcal{Q}_2} \subseteq \Sigma_{\mathcal{M}}$, and for all $1 \leq i \leq m$, we have, $\Sigma_{\sigma(\mathcal{Q}_1),\mathcal{Q}_2}^{X_i}$ is contained in the subgroup of $Sym(X_i)$ fixing Y_i^j as a set, for $j = 1, 2$, where Y_i^j are as in part (3) of Lemma **??**.*

Proof. Let $\sigma \in \Sigma$. By the construction of $\mathcal{Q}_1$ we have $\Sigma_{\sigma(\mathcal{Q}_1),\mathcal{Q}_2} \subseteq \Sigma_{\mathcal{M},\mathcal{Q}_2}$, so Lemma **??** completes the proof. □

Notation 7.1.4. Let $\mathcal{P} = \{U_1, \ldots, U_t\}$ be a partition of X and let $C_1, \ldots, C_t \subseteq L$ be distinct $\mathrm{Aut}(L)$ conjugacy classes. We let

$$x(U_1, \ldots, U_t,\, C_1, \ldots, C_t),$$

denote the set of elements x of K satisfying

$$x_j \in C_i^{g_j} \text{ if and only if } L_j \in U_i, \quad \text{for } 1 \leq j \leq n \text{ and } 1 \leq i \leq t.$$

where K and $g_1, \ldots, g_n$ are as in Notation **??**.

Lemma 7.1.5. *Let $\mathcal{Q}_1 = \{V_1, \ldots, V_e\}$ be a partition of X such that $\Sigma_{\mathcal{Q}_1} \leq \Sigma_{\mathcal{M}}$. Let $\mathcal{Q}_2 = \{W_1, \ldots, W_f\}$ be a partition of X as in Lemma **??**. Let $B_1, \ldots, B_e \subseteq L$ be distinct $\mathrm{Aut}(L)$ classes and $C_1, \ldots, C_f \subseteq L$ be distinct $\mathrm{Aut}(L)$ classes. Let $x \in x(V_1, \ldots V_e, B_1, \ldots, B_e)$ and $y \in x(W_1, \ldots W_f, C_1, \ldots, C_f)$. Then,*

(1) *If $\mathcal{Q}_2$ is as in part (1) or (2) of Lemma **??**, then $C_G(x^g, y)$ normalizes L_j, for all $g \in G$ and $1 \leq j \leq n$.*
(2) *Suppose $\mathcal{Q}_2$ is as in part (3) of Lemma **??**, and set $Y_i^j = \{L_{i_1^j}, L_{i_2^j}\}$, $1 \leq i \leq m$ and $1 \leq j \leq 2$. Then $C_G(x^g, y)$ normalizes $L_{i_1^j} L_{i_2^j}$, $1 \leq i \leq m$ and $1 \leq j \leq 2$, where Y_i^j are as in part (3) of Lemma **??**.*

Proof. Let $g \in G$ and let $\sigma \in \Sigma$ be the image of g in Σ. Note that by the choice of x, the image of $C_G(x^g)$ in Σ fixes the partition $\sigma(\mathcal{Q}_1)$. Hence the image of $C_G(x^g)$ in Σ, acts trivially on $\mathcal{M}$ (of course $\mathcal{M}$ is as in (iii) of subsection **??**). Let Θ be the image of $C_G(x^g, y)$ in Σ. Then, by the above, and by the choice of y, $\Theta \subseteq \Sigma_{\sigma(Q_1),Q_2}$, so the lemma holds by the choice of $\mathcal{Q}_2$. □

Lemma 7.1.6. *Let $\mathcal{B}, \mathcal{C} \subseteq L$ be two $\mathrm{Aut}(L)$ conjugacy classes. Consider the set of cyclic subgroups $\{\langle u \rangle \mid u \in \mathcal{B}\}$ and let $\mathcal{O}_1, \ldots, \mathcal{O}_\mu$ be the orbits of L (via conjugation) on this set. Assume that for all $v \in \mathcal{C}$ and all $t \in \Delta_{\mathrm{Aut}(L)}(v)$ and every orbit $\mathcal{O} \in \{\mathcal{O}_1, \ldots, \mathcal{O}_\mu\}$, there exists $\langle u' \rangle \in \mathcal{O}$ such that one of the following holds:*

(a) $d_{\mathrm{Aut}(L)}(u', v) \geq 4$, or
(b) $d_{\mathrm{Aut}(L)}(u', v) \geq 3 \leq d_{\mathrm{Aut}(L)}(u', t)$, or
(c) (c1) There exists a unique minimal path $\pi(u', t) := u', s, t$ from u' to t in $\Delta_{\mathrm{Aut}(L)}$ (unique up to replacing s by a power of s).
(c2) For s as in (c1), there exists $h' \in L$ such that $d_{\mathrm{Aut}(L)}((u')^{h'}, v) \geq 3$ and $[s^{h'}, t] \neq 1$.

Then $(\mathrm{Aut}(L), u, v, L)$ satisfies property $(3\frac{1}{2})$, for all $u \in \mathcal{B}$ and $v \in \mathcal{C}$.

Proof. First notice that hypothesis (a) implies hypothesis (b) (with the same u'). Let $u \in \mathcal{B}$ and $v \in \mathcal{C}$ and let $a \in \Delta_{\mathrm{Aut}(L)}(u)$ and $b \in \Delta_{\mathrm{Aut}(L)}(v)$. Let $\mathcal{O}$ be the orbit of $\langle u \rangle$ under the action of L (via conjugation). Suppose there exists $\langle u' \rangle \in \mathcal{O}$ such that $d_{\mathrm{Aut}(L)}(u', v) \geq 3 \leq d_{\mathrm{Aut}(L)}(u', b)$. Let $h \in L$ such that $\langle u^h \rangle = \langle u' \rangle$. If $[a^h, b] = 1$, then since $[a^h, u'] = 1$, we get $d_{\mathrm{Aut}(L)}(u', b) \leq 2$, a contradiction. So $[a^h, b] \neq 1$ as required.

Suppose there exists $\langle u' \rangle \in \mathcal{O}$ as in hypothesis (c) (where in hypothesis (c) replace t by b). Let $q \in L$, with $\langle u^q \rangle = \langle u' \rangle$. Then $s \in \langle a^q \rangle$, otherwise, $[a^q, b] \neq 1$ and we are done. Let h' be as in (c2) and set $h = qh'$. Then $d_{\mathrm{Aut}(L)}(u^h, v) \geq 3$, but $[a^h, b] \neq 1$, as required. □

Lemma 7.1.7. *Let $x, y \in K$ such that $d_G(x, y) = 3$. Assume that x, a, b, y is a path in Δ_G such that there exists $j \in \{1, \ldots n\}$ with $a, b \notin C_G(L_j)$. Assume further that $x_j \neq 1 \neq y_j$,*

that $d_{\mathrm{Aut}(L)}(x_j, y_j) \geq 3$*, and that* $[a^q, b] = 1$*, for all* $q \in G$ *such that* $d_G(x^q, y) \geq 3$*. Then* $a, b \in N_G(L_j)$*.*

Proof. Let $q \in L_j$ such that $d(x^{q^{-1}}, y) \geq 3$. Then $[a, b^q] = 1$. Assume that $L_j^a \neq L_j$. We have,

$$w^{ab^q} = ((w^a)^{q^{-1}})^{bq} = w^{abq}, \qquad \text{for all } w \in L_j. \tag{iv}$$

Case 1: $L_j^b \neq L_j$.
In this case we have,

$$w^{b^q a} = w^{q^{-1}ba}, \qquad \text{for all } w \in L_j. \tag{v}$$

If $L_j^{ab} \neq L_j$, then $w^{abq} = w^{ab}$, so from (**??**) and (**??**) we get that

$$w^{ab} = w^{q^{-1}ab}, \qquad \text{for all } w \in L_j, \tag{vi}$$

that is $w = w^{q^{-1}}$, for all $w \in L_j$ which implies that q is in the center of L_j. This is a contradiction since we can choose $q \neq 1$ (e.g. $q = x_j$) and L_j is simple.

Hence we may assume that $L_j^{ab} = L_j$. We get that $w^{abq} = w^{q^{-1}ab}$, for all $w \in L_j$. It follows that $(ab)q(ab)^{-1} = q^{-1}$. Hence ab inverts every element $q \in L_j$ such that $d(x^{q^{-1}}, y) \geq 3$. Note however that for $q \in \{x_j, y_j, y_j^{-1}x_j^{-1}\}$, we have $d(x^{q^{-1}}, y) \geq 3$, so since ab inverts them, we conclude that $[x_j, y_j] = 1$, contradicting $d_{\mathrm{Aut}(L_j)}(x_j, y_j) \geq 3$.

Case 2: $L_j^b = L_j$.
Here $L_j^{ab} \neq L_j$. Let $w \in L_j$. By (**??**), $w^{ab^q} = w^{ab}$. Hence we get that $w^{ba} = w^{b^q a}$ and it follows that $w^b = w^{b^q}$, for all $w \in L_j$, and hence $b = b^q$, for all q. In particular, b centralizes $q = x_j$. But then thinking of b as an element of $\mathrm{Aut}(L_j)$, we get that $1 \neq b \in C_{\mathrm{Aut}(L_j)}(x_j, y_j)$ contradicting the hypotheses of the lemma.

It follows that $a \in N_G(L_j)$. Notice now that our hypotheses are symmetric with respect to x and y, so by symmetry, $b \in N_G(L_j)$. □

Proposition 7.1.8. *Each one of the following hypotheses imply that* G *has the property* $(3\frac{1}{2})$*:*

(*a*) *There exists six distinct conjugacy classes* $B, C_1, \ldots, C_5$ *of* $\mathrm{Aut}(L)$*, contained in* L*, such that for every* $u \in B$ *and* $v \in \bigcup_{i=1}^5 C_i$*, we have,* $d_{\mathrm{Aut}(L)}(u, v) \geq 3$*.*

(*b*) *There exists conjugacy classes* $B, C_1, \ldots, C_5$ *of* $\mathrm{Aut}(L)$*, contained in* L*, such that* $C_1, \ldots, C_5$ *are distinct and such that for every* $\mathcal{C} \in \{C_1, \ldots, C_5\}$ *if we set* $\mathcal{B} := B$*, then* $(\mathrm{Aut}(L), u, v, L)$ *has the property* $(3\frac{1}{2})$*, for all* $u \in \mathcal{B}$ *and* $v \in \mathcal{C}$*.*

(*c*) *There exists distinct* $\mathrm{Aut}(L)$ *conjugacy classes* $B_1, \ldots, B_3 \subseteq L$ *and distinct* $\mathrm{Aut}(L)$ *classes* $C_1, \ldots, C_f \subseteq L$ *such that,*

  (*c*1) *If* $\Sigma^{X_i} \ncong \mathrm{S}_4$*,* $f = 3$*, while if* $\Sigma^{X_i} \cong \mathrm{S}_4$*,* $f = 4$*.*

  (*c*2) *For every* $\mathcal{B} \in \{B_1, \ldots, B_3\}$ *and* $\mathcal{C} \in \{C_1, \ldots, C_f\}$*, we have that* $(\mathrm{Aut}(L), u, v, L)$ *has the property* $(3\frac{1}{2})$*, for all* $u \in \mathcal{B}$ *and* $v \in \mathcal{C}$*.*

Proof. We show that there are elements $x, y \in K$ such that (G, x, y) satisfy property $(3\frac{1}{2})$. Let y be the following element. First we let $\mathcal{Q}_2 := \{W_1, \ldots, W_f\}$ be a partition of X satisfying the following. In (a) and (b) we request that $2 \leq f \leq 5$ and that $\Sigma_{\mathcal{Q}_2} = 1$. In (c) we request that $\Sigma_{\mathcal{M},\mathcal{Q}_2} = 1$. We let

$$y \in x(W_1, \ldots, W_f, C_1, \ldots C_f\}$$

(see Notation **??**). Next we pick x as follows. In the cases (a) and (b), we let $x \in K$ be an element such that $x_i \in B^{g_i}$, and $d_{\mathrm{Aut}(L)}(x_i, y_i) \geq 3$, for all $1 \leq i \leq n$. The existence of x_i in (a) is guaranteed by the hypotheses and in (b) it is part of the definition of property $(3\frac{1}{2})$. In case (c), we first pick a partition $\mathcal{Q}_1 = \{V_1, \ldots V_e\}$, $2 \leq e \leq 3$ of X such that $\Sigma_{\mathcal{Q}_1} \subseteq \Sigma_{\mathcal{M}}$. We let $x \in x(V_1, \ldots, V_e, B_1, \ldots, B_e)$ such that $d_{\mathrm{Aut}(L)}(x_i, y_i) \geq 3$ (again using the definition of property $(3\frac{1}{2})$). The existence of $\mathcal{Q}_2$ is guaranteed by Theorem 1.2 in [**?**] (see also Proposition 2.5 of [**?**]) in cases (a) and (b) and by Lemma **??** (1) and (2), in case (c). The existence of $\mathcal{Q}_1$ in case (c) is guaranteed by Lemma **??**. It is clear that in (a) and (b), the image of $C_G(y)$ in Σ is contained in $\Sigma_{\mathcal{Q}_2} = 1$, so $C_G(y)$ normalizes L_i, for all $1 \leq i \leq n$. Also in (c), by Lemma **??**(1), $C_G(x^g, y)$ normalizes L_i, $1 \leq i \leq n$, for all $g \in G$. From the choice of x_i, $1 \leq i \leq n$, we get that $d_G(x, y) \geq 3$.

We now show that (G, x, y) satisfy property $(3\frac{1}{2})$. Notice that given $g \in G$, in all three cases (a), (b) and (c), we can find $h \in K$, such that $d_G(x^{gh}, y) \geq 3$. This is because $C_G(x^g, y)$ normalizes L_i, for all i, and then our hypotheses allow us to find $h_i \in L_i$, such that $d_{\mathrm{Aut}(L_i)}((x^g)_i^{h_i}, y_i) \geq 3$, and then for $h = h_1 \cdots h_n$, we have $d_G(x^{gh}, y) \geq 3$.

Assume that (G, x, y) fail to satisfy property $(3\frac{1}{2})$. Then there exists a path x, a, b, y in Δ_G such that for all $g \in G$ with $d_G(x^g, y) \geq 3$, we have $[a^g, b] = 1$. Let $j, k \in \{1, \ldots, n\}$ such that $a \notin C_G(L_k)$ and $b \notin C_G(L_j)$. Let $q \in G$ with $L_k^q = L_j$, and such that $d_{\mathrm{Aut}(L_i)}((x^q)_i, y_i) \geq 3$, for all $1 \leq i \leq n$ (and hence $d_G(x^q, y) \geq 3$). The existence of q is guaranteed since Σ is transitive and by the previous paragraph of the proof. Then x^q, a^q, b, y is a path in Δ_G and replacing x by x^q and a by a^q we may assume that $a, b \notin C_G(L_j)$. By Lemma **??**, a and b normalize L_j. Notice now that for every $g \in L_j$ such that $d_{\mathrm{Aut}(L_j)}(x_j^g, y_j) \geq 3$, we have $d_G(x^g, y) \geq 3$, so $[a^g, b] = 1$. Thinking of a, b as elements of $\mathrm{Aut}(L_j)$, we see that $(\mathrm{Aut}(L_j), x_j, y_j, L_j)$ do not satisfy property $(3\frac{1}{2})$. This is a contradiction to hypothesis (b) and (c2), in the cases (b) and (c). It is a contradiction in case (a) as well, because in case (a), $(\mathrm{Aut}(L_j), x_j, y_j, L_j)$ has the property $(3\frac{1}{2})$ as well. To see this note that for any two conjugacy classes $\mathcal{B}$ and $\mathcal{C}$ of L such that $d_{\mathrm{Aut}(L)}(u, v) \geq 3$, for all $u \in \mathcal{B}$ and $v \in \mathcal{C}$, $(\mathrm{Aut}(L), u, v, L)$ satisfy property $(3\frac{1}{2})$, for any $u \in \mathcal{B}$ and $v \in \mathcal{C}$, because failure to do so violates the simplicity of L. □

In our applications of part (b) of Proposition **??** we will use the following corollary.

Corollary 7.1.9. *Suppose that there are* $\mathrm{Aut}(L)$ *conjugacy classes* $B, C_1, \ldots, C_5$*, contained in* L*, such that* $C_1, \ldots, C_5$ *are distinct and such that* L *is transitive via conjugation on* $\{\langle u \rangle \mid u \in B\}$*. For* $1 \neq w \in \mathrm{Aut}(L)$*, let* $\delta(w) := |\{u \in B \mid d_{\mathrm{Aut}(L)}(u, w) \leq 2\}|$*. Assume that* $\delta(w) < \frac{1}{2}|B|$*, for all* $1 \neq w \in \mathrm{Aut}(L)$*, or, more generally, that* $\delta(v) + \delta(w) < |B|$*, for all* $1 \neq w \in \mathrm{Aut}(L)$ *and* $v \in \bigcup_{i=1}^{5} C_i$*. Then* G *has the property* $(3\frac{1}{2})$*.*

Proof. We show that L satisfies hypothesis (b) of Proposition **??**. For that we show that if we set $\mathcal{B} := B$, then for all $\mathcal{C} \in \{C_1, \dots, C_5\}$, the pair $\mathcal{B}, \mathcal{C}$ satisfies hypothesis (b) of Lemma **??**. By our assumptions, given $v \in \bigcup_{i=1}^{5} C_i$ and $1 \neq w \in \mathrm{Aut}(L)$, there exists $u' \in B$ such that $d_{\mathrm{Aut}(L)}(u', v) \geq 3 \leq d_{\mathrm{Aut}(L)}(u', w)$. Let now $\mathcal{C} \in \{C_1, \dots, C_5\}$ and pick $v \in \mathcal{C}$ and $t \in \Delta_{\mathrm{Aut}(L)}(v)$. Then there exists $u' \in B$ such that $d_{\mathrm{Aut}(L)}(u', v) \geq 3 \leq d_{\mathrm{Aut}(L)}(u', t)$. Hence u' is the element required in part (b) of Lemma **??**. □

The purpose of the next three Lemmas is to handle the case when $L = \mathrm{A}_5$ and $\Sigma^{X_i} \cong \mathrm{S}_4$, in theorem **??**. Though these Lemmas are formulated for general L, the reader may think of A_5. We assume that $C_1, C_2, C_3 \subseteq L$ are three distinct $\mathrm{Aut}(L)$ conjugacy classes.

Notation 7.1.10. Suppose $\Sigma^{X_i} \cong \mathrm{S}_4$. We let $\mathcal{Q}_1 = (V_1, \dots V_e)$ be as in Lemma **??** and we let $\mathcal{Q}_2 = (W_1, W_2)$ be as in part (3) of Lemma **??**, and the sets $Y_i^j = \{L_{i_1^j}, L_{i_2^j}\}$, $1 \leq i \leq m$ and $1 \leq j \leq 2$, are as given in part (3) of Lemma **??**. We let $x \in x(V_1, \dots, V_e, C_1, \dots C_e)$ and $y \in x(W_1, W_2, C_1, C_2)$.

Lemma 7.1.11. *The following two assertions hold:*

(1) *Let $k, l \in \{1, \dots n\}$ be two distinct indices. Let $x_k x_l, y_k y_l \in L_k L_l$ such that $C_{\mathrm{Aut}(L_k)}(x_k, y_k) = 1$. Then there exists at most one orbit $\mathcal{O}_l \subseteq x_l^{\mathrm{Aut}(L_l)} \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_l)}(y_l)$ under the action of $C_{\mathrm{Aut}(L_l)}(y_l)$ (acting by conjugation), such that for $x_l' \in \mathcal{O}_l$, we have $C_{\mathrm{Aut}(L_k L_l)}(x_k x_l', y_k y_l) \neq 1$.*

(2) *Assume that $\Sigma^{X_i} \cong \mathrm{S}_4$ and let x, y be as in Notation **??**. Assume further that $d_{\mathrm{Aut}(L_i)}(x_i, y_i) \geq 3$, for all $1 \leq i \leq n$, and that $d_G(x, y) \geq 3$. Then for each $1 \leq l \leq n$ there exists at most one orbit $\mathcal{O}_l \subseteq x_l^{\mathrm{Aut}(L_l)} \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_l)}(y_l)$ under the action of $C_{\mathrm{Aut}(L_l)}(y_l)$, such that for $h \in L_l$ with $x_l^h \in \mathcal{O}_l$ we have $d_G(x^h, y) \leq 2$.*

Proof. (1): Suppose that $x_l', x_l'' \in x_l^{\mathrm{Aut}(L_l)} \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_l)}(y_l)$ are such that there exists $1 \neq q \in C_{\mathrm{Aut}(L_k L_l)}(x_k x_l', y_k y_l)$ and $1 \neq s \in C_{\mathrm{Aut}(L_k L_l)}(x_k x_l'', y_k y_l)$. Now q^2 normalizes each L_j, $j = k, l$, so since $C_{\mathrm{Aut}(L_k)}(x_k, y_k) = 1 = C_{\mathrm{Aut}(L_l)}(x_l', y_l)$, $q^2 = 1$, and q interchanges L_k and L_l. Thus $x_k^q = x_l'$, $y_k^q = y_l$.

Next, as above we must have $x_k^s = x_l''$, $y_k^s = y_l$, and $s^2 = 1$, so $s = uvq$, with $u \in C_{\mathrm{Aut}(L_k)}(y_k)$ and $v \in C_{\mathrm{Aut}(L_l)}(y_l)$. Then

$$x_l'' = x_k^s = (x_k^q)^{q^{-1}uvq} = (x_l')^{(q^{-1}uvq)} = (x_l')^{q^{-1}uq}.$$

but $q^{-1}uq \in C_{\mathrm{Aut}(L_l)}(y_l)$, so we see that x_l' and x_l'' are in the same orbit of $x_l^{\mathrm{Aut}(L)} \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_l)}(y_l)$ under the action of $C_{\mathrm{Aut}(L_l)}(y_l)$.

(2): Let $l \in \{1, \dots, n\}$. Without loss we may assume that $L_l \in Y_1^1$ and we'll denote $\{L_k\} = Y_1^1 \smallsetminus \{L_l\}$. Let $h, h' \in L_l$ such that $x_l^h, x_l^{h'} \in \Delta^{\geq 3}_{\mathrm{Aut}(L_l)}(y_l)$. Let $1 \neq q \in C_G(x^h, y)$. Notice that by the choice of x, y and by Lemma **??**, q normalizes $L_k L_l$ and if $q \in C_G(L_k L_l)$, then $q \in C_G(x, y)$, contradicting $d_G(x, y) \geq 3$. Similarly given $s \in C_G(x^{h'}, y)$, s restricts to a nontrivial automorphism of $L_k L_l$. It follows from part (1) that if $d_G(x^h, y) \leq 2 \geq d_G(x^{h'}, y)$,

then $x_l^h, x_l^{h'}$ are in the same orbit under the action of $C_{\mathrm{Aut}(L_l)}(y_l)$, so part (2) follows from part (1). □

Lemma 7.1.12. *Assume $\Sigma^{X_i} \cong \mathrm{S}_4$ and let $x, y \in K$ be as in Notation **??**. Suppose that for all $v \in C_1 \cup C_2$ and $1 \leq j \leq 3$ and each $u \in C_j$, we have that $u^L \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ is nonempty and is not contained in an orbit of $C_{\mathrm{Aut}(L)}(v)$ on $\Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ (acting via conjugation). Then for all $g \in G$, there exists $h \in K$ such that $d_G(x^{gh}, y) \geq 3$ and such that $d_{\mathrm{Aut}(L_i)}((x^{gh})_i, y_i) \geq 3$, for all $1 \leq i \leq n$.*

Proof. Let $g \in G$ and set $z := x^g$. By Lemma **??**, $C_G(z, y)$ normalizes $L_{i_1^j} L_{i_2^j}$, $1 \leq i \leq m$ and $1 \leq j \leq 2$. For each $L_i \in \{L_1, \ldots, L_n\}$, pick $r_i \in L_i$ so that $z_i^{r_i} \in \Delta^{\geq 3}_{\mathrm{Aut}(L_i)}(y_i)$. This can be done by hypothesis. Replacing z by z^r (where $r = r_1 \cdots r_n$), we may assume that $d_{\mathrm{Aut}(L_i)}(z_i, y_i) \geq 3$, for all $1 \leq i \leq n$. Let $1 \leq i \leq m$ and $1 \leq j \leq 2$ and set $k = i_1^j$, $l = i_2^j$. Set $h_k = 1$ and pick $h_l \in L_l$, so that $d_{\mathrm{Aut}(L)}(z_l^{h_l}, y_l) \geq 3$ and $C_{\mathrm{Aut}(L_k L_l)}(z_k z_l^{h_l}, y_k y_l) = 1$. This can be done using the hypotheses of the Lemma and using Lemma **??**(1). By construction $h = h_1 \cdots h_n$ satisfies $d_G(x^{gh}, y) \geq 3$ and $d_{\mathrm{Aut}(L_i)}((x^{gh})_i, y_i) \geq 3$, for all $1 \leq i \leq n$, as required. □

Lemma **??** below is our tool for showing that when $L \cong \mathrm{A}_5$ and $\Sigma^{X_i} \cong \mathrm{S}_4$, G satisfies property $(3\frac{1}{2})$. Since this Lemma is quite technical, a word of explanation is in place. Suppose $\Sigma^{X_i} \cong \mathrm{S}_4$ and that we found elements x, y as in Notation **??** such that $d_G(x, y) \geq 3$ and such that $d_{\mathrm{Aut}(L_i)}(x_i, y_i) \geq 3$, for all i. We wish to show that (G, x, y) satisfies property $(3\frac{1}{2})$. For that we need enough elements $h \in L_j$ (some j), such that $d_G(x^h, y) \geq 3$. Thus we consider the set $x_j^{L_j} \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_j)}(y_j)$ and we want to pick $h \in L_j$ such that x_j^h is in this set. The fact that $d_{\mathrm{Aut}(L)}(x_j^h, y_j) \geq 3$ "almost" guarantees $d_G(x^h, y) \geq 3$, except perhaps when x_j^h belongs to the "bad" orbit of Lemma **??**(2) (with respect to the action of $C_{\mathrm{Aut}(L_j)}(y_j)$ via conjugation). Since we don't know which is the "bad" orbit, we must make sure that: (1) there is more than one orbit, and (2) that for *each* orbit of $C_{\mathrm{Aut}(L_j)}(y_j)$ on the set $x_j^{\mathrm{Aut}(L_j)} \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_j)}(y_j)$, there is an element $x_j^h \in x_j^{L_j} \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_j)}(y_j)$ but not in this orbit and such that furthermore $h \in L_j$ has some additional "nice" properties. This is the content of hypothesis (b) of Lemma **??**.

Lemma 7.1.13. *Assume that for each $v \in C_1 \cup C_2$ we have,*

(a) *For all $1 \leq j \leq 3$, $C_{\mathrm{Aut}(L)}(v)$ has more than one orbit on $C_j \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ (acting via conjugation).*

(b) *For each orbit $\mathcal{O}$ of $C_{\mathrm{Aut}(L)}(v)$ on $C_j \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$, each $u \in C_j$, $s \in \Delta_{\mathrm{Aut}(L)}(u)$ and $t \in \Delta_{\mathrm{Aut}(L)}(v)$, there exists $h \in L$ such that $u^h \in \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v) \smallsetminus \mathcal{O}$ and $[s^h, t] \neq 1$.*

Assume further that,

(c) *For every $\mathcal{B}, \mathcal{C} \in \{C_1, \ldots, C_3\}$, we have that $(\mathrm{Aut}(L), u, v, L)$ has the property $(3\frac{1}{2})$, for all $u \in \mathcal{B}$ and $v \in \mathcal{C}$.*

Then G satisfies property $(3\frac{1}{2})$.

Proof. If $\Sigma^{X_i} \ncong \mathrm{S}_4$, then by hypothesis (c) the hypotheses of part (c) of Proposition **??** hold, so by that proposition, we are done.

Hence we may assume that $\Sigma^{X_i} \cong \mathrm{S}_4$. Let x, y be as in Notation **??**. Notice that our hypothesis (b) implies the hypotheses of Lemma **??**, hence replacing x by a conjugate of x, we may (and we do) assume that $d_G(x,y) \geq 3$ and $d_{\mathrm{Aut}(L_i)}(x_i, y_i) \geq 3$, for all $1 \leq i \leq n$. Assume that (G, x, y) fail to satisfy property $(3\frac{1}{2})$. Then there exists a path x, a, b, y in Δ_G such that for all $g \in G$ with $d_G(x^g, y) \geq 3$, we have $[a^g, b] = 1$. By the transitivity of Σ and using Lemma **??**, we may replace x by a conjugate of x, so that we may assume that there exists $j \in \{1, \ldots, n\}$ such that $a, b \notin C_G(L_j)$. By Lemma **??**, $a, b \in N_G(L_j)$. Identify now L_j with L (via conjugation by g_j^{-1}). Let $k \in \{1, \ldots, 3\}$ be such that $x_j \in C_k$. Let $\mathcal{O}$ be an orbit of $C_{\mathrm{Aut}(L_j)}(y_j)$ on $C_k \cap \Delta^{\geq 3}_{\mathrm{Aut}(L_j)}(y_j)$ such that for $h \in L_j$ with $x_j^h \in \Delta^{\geq 3}_{\mathrm{Aut}(L_j)}(y_j) \smallsetminus \mathcal{O}$, we have $d_G(x^h, y) \geq 3$ (We take $\mathcal{O}$ to be the "bad" orbit of Lemma **??**(2) if it exists and otherwise $\mathcal{O}$ is any orbit). Note now that by hypothesis (b), there exists $q \in L_j$ such that $x_j^q \in \Delta^{\geq 3}_{\mathrm{Aut}(L_j)}(y_j) \smallsetminus \mathcal{O}$ and $[a^q, b] \neq 1$. But then also $d_G(x^q, y) \geq 3$ and this supplies a contradiction to the choice of the path x, a, b, y. □

7.2. **The generic case.**

In this subsection L is a finite nonabelian simple group such that L is not isomorphic to one of the groups $PSL(2,q)$, $q = 5, 7, 8, 9, 11, 16$ or 27; $PSL(3,4)$ or $PSO^+(8,2)$.

We consider the following condition,

(*Gen*) There exists six distinct nonidentity conjugacy classes $B, C_1, \ldots, C_5$ of $\mathrm{Aut}(L)$ contained in L, such that $d_{\mathrm{Aut}(L)}(r, s) \geq 3$, for all $r \in B$ and $s \in \bigcup_{i=1}^5 C_i$.

The purpose of this subsection is to prove Theorem **??**, i.e., to prove,

Theorem 7.2.1. *L satisfies (Gen).*

We start with the Alternating groups.

Lemma 7.2.2. *Let $L \cong \mathrm{A}_n$. Then,*
(1) *If $n \geq 7$ is odd. Then L satisfies (Gen).*
(2) *If $n \geq 8$ is even. Then L satisfies (Gen).*

Proof. (1): Let B be the $\mathrm{Aut}(L)$ conjugacy class of n cycles. Note that if $C \subseteq L$ is an $\mathrm{Aut}(L)$ conjugacy class of elements of L having precisely one fixed point, or having precisely two fixed points than $d_{\mathrm{Aut}(L)}(b, c) \geq 3$, for all $b \in B$ and $c \in C$. It is clear that when $n \geq 9$, there are at least 5 distinct classes C as above. If $n = 7$, then for all conjugacy classes $C \neq B$, $b \in B$ and $c \in C$, one has $d_{\mathrm{Aut}(L)}(b, c) = \infty$, so clearly (*Gen*) holds in this case as well.

(2): Let B be the conjugacy class of $n-1$ cycles. Note that if $C \subseteq L$ is an $\mathrm{Aut}(L)$ conjugacy class of elements of L having no fixed points, or having precisely two fixed points then $d_{\mathrm{Aut}(L)}(b, c) \geq 3$, for $b \in B$ and $c \in C$. It is easily checked that for $n \geq 8$ there are at least 5 distinct classes C as above. □

For the Sporadic groups we have,

Lemma 7.2.3. *Assume L is a Sporadic group not isomorphic to J_2 or McL. Then (Gen) holds for L.*

Proof. It is easy to check (using the ATLAS) that L contains an $\mathrm{Aut}(L)$ conjugacy class B such that $\langle b\rangle \smallsetminus \{1\}$ is a connected component of $\Delta_{\mathrm{Aut}(L)}$. Since the number of $\mathrm{Aut}(L)$ conjugacy classes contained in L is ≥ 6, we are done. □

Lemma 7.2.4. *Assume $L \cong J_2$. Then L satisfies (Gen).*

Proof. Let $B \subseteq L$ be the class of elements of order 7. Then for $b \in B$ we have $C_{\mathrm{Aut}(L)}(b) = \langle b\rangle\langle t\rangle$, where t is an (outer) involution with $C_L(t) \cong SL(3,2) : 2$. It follows that if $C_1, \ldots, C_5$ are the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $5, 5, 10, 10, 12$, then $B, C_1, \ldots, C_5$ satisfy (Gen). □

Lemma 7.2.5. *Assume $L \cong McL$. Then L satisfies (Gen).*

Proof. Let B be the class of elements of order 11. Then for $b \in B$, we have, $C_{\mathrm{Aut}(L)}(b) = \langle b\rangle\langle t\rangle$, where t is an (outer) involution with $C_L(t) \cong \mathrm{M}_{11}$. It follows that if $C_1, \ldots, C_5$ are $\mathrm{Aut}(L)$ conjugacy classes of elements of order $7, 9, 10, 12, 14$, then $B, C_1, \ldots, C_5$ satisfy (Gen). □

The groups of Lie type

The remainder of this subsection is devoted to the groups of Lie type. Let $L = L(q)$ be a simple group of Lie type defined over a field of order $q = p^a$, p a prime. Let G be the corresponding algebraic group, so that $L = (G_\sigma)'$ for σ a Frobenius morphism of G. Until the end of subsection **??** we let $A = \mathrm{Aut}(L)$. We will exhibit elements $x, y_1, \ldots, y_5 \in L$ such that $x^A, y_1^A, \ldots y_5^A$ are six distinct $\mathrm{Aut}(L)$ conjugacy classes satisfying condition (Gen).

We use the following notation for certain groups of Lie type. For $\epsilon = \pm 1$ we let $A_n^\epsilon, D_n^\epsilon, E_6^\epsilon$ be groups of Lie type as follows. If $\epsilon = 1$, these are just the (untwisted) Chevalley groups, $A_n(q), D_n(q), E_6(q)$, respectively; while if $\epsilon = -1$, we have the twisted groups ${}^2A_n(q), {}^2D_n(q), {}^2E_6(q)$.

Elements of A can be expressed as a product of inner, diagonal, field, and graph automorphisms (see Thms 30 and 36 of [**?**]). It is also known that automorphisms of L extend to morphisms of G commuting with σ. Now G_σ is the group of inner and diagonal automorphisms of L, so that A/G_σ is generated by images of field and graph automorphisms of G restricted to L. For example, if σ is a field morphism of G corresponding to $q = p^a$, there is a field morphism μ corresponding to p such that $\mu^a = \sigma$ and μ acts on L generating the group of field automorphisms.

Throughout this subsection, the term "graph automorphism" of G will be used somewhat loosely. Let τ be a standard graph automorphism of G (see p.156 of [**?**]). We will refer to any element in τG of order equal to that of τ as a graph automorphism. Typically there exist just one or two G-classes of such elements. For instance in E_6 there are two classes of

such morphisms. They have fixed points F_4 and C_4, except for $p = 2$, where the fixed points are F_4 and the centralizer in F_4 of a long root element of E_6 contained in F_4.

When $L = PSp(4, q), F_4(q)$ or $G_2(q)$ with $p = 2, 2, 3$ respectively, there is an endomorphism δ the algebraic group G, that commutes with σ and interchanges root group corresponding to long and short roots. Also δ^2 generates the group of field morphisms. Here $A = L\langle\delta_L\rangle$, where δ_L is the restriction of δ to L. We will call δ_L a "special graph automorphism". When $q = p^a$, with a odd, the involution $\tau = (\delta_L)^a$ has fixed point group ${}^2B_2(q)$, ${}^2F_4(q)$ or ${}^2G_2(q)$, respectively, and τ is called an "involutory special graph automorphism".

When there is no danger of confusion we will sometimes identify an automorphism of L with its extension to G.

Lemma 7.2.6. *Let $u \in L$ be a regular unipotent element. Then $C_A(u) = U\langle\delta\rangle J$ where $U < G_\sigma$ is a unipotent group, δ generates the group of field automorphisms of L and J is the group of graph (or special graph) automorphisms.*

Proof. As u is regular we have $C_G(u)$ a unipotent group. Hence $C_{G_\sigma}(u)$ is a unipotent group. On the other hand, any unipotent element that is the product of root elements from positive root groups with nontrivial contribution for each fundamental root is regular and all regular unipotent elements are conjugate in G (see III, 1.8 of [**?**]). So it follows from the action of standard field and graph automorphisms that each fix regular unipotent elements. The result follows. □

Lemma 7.2.7. *Let $a \in A \smallsetminus G_\sigma$ have prime power order r^e with $a^r \in G_\sigma$. Then a is the restriction to L of a morphism δ of G commuting with σ. Moreover, one of the following holds:*

(i) There does not exist a graph or special graph automorphism τ such that $a \in G_\sigma\tau$. In this case $G_\delta = G(q_o)$ for $q_o < q$.

(ii) $a \in G_\sigma\tau$ for some graph automorphism τ of G. In this case $C_L(a)$ is contained in $D_\sigma = D(q)$, where $D^\sigma = D < G$ is either a parabolic subgroup (only if $p = |\tau|$) or a reductive group of semisimple rank strictly less than that of G.

(iii) $a \in G_\sigma\tau$ where τ is an involutory special graph automorphism of $PSp(4, q), F_4(q)$ or $G_2(q)$. If $|a| = 2$, then $C_L(a) =^2 B_2(q)$, ${}^2F_4(q)$ or ${}^2G_2(q)$, respectively. Otherwise, $C_L(a)$ is contained in a proper parabolic subgroup of $PSp(4, q)$ or $F_4(q)$ or a subgroup $SL_2(q) \cdot SL_2(q)$ of $G_2(q)$, respectively.

Proof. Fix $a \in A \smallsetminus G_\sigma$ and recall that a is the restriction to L of a morphism commuting with σ. There is an element $g \in G_\sigma$ such that a is induced by $g \cdot \mu$ for μ a field, graph-field, graph, or special graph automorphism of G commuting with σ.

First suppose μ can be chosen as a field or graph-field automorphism of G. Regarding $g \cdot \mu$ as a member of the coset $G\mu \subseteq Aut(G)$ (automorphisms as abstract group), we can apply Lang's theorem (see I, 2.2 of [**?**]) to see that $g \cdot \mu$ is G-conjugate to μ. Since $G_\mu = G(q_o)$ for q_o a proper divisor of q, part (i) follows.

Now suppose $a \in G_\sigma\tau$ for some graph automorphism τ of G commuting with σ. We have $C_L(a) \leq C_G(a)_\sigma$ and $|\tau| = r$. So $r = 2$ except possibly for $G = D_4$ where $r = 3$. If $|a| = |\tau|$

then a is a graph automorphism of G and the centralizers of such automorphisms are known (for example see 1.1 of [**?**]). It follows that either $C_G(a)$ is reductive and we obtain the result by setting $D = C_G(a)$, or else $p = r$ and $C_G(a)$ has a nontrivial unipotent radical and so by the Borel-Tits theorem it is contained in a canonical parabolic subgroup D of G. Furthermore, since $C_G(a)$ is σ-invariant, the unipotent radical of $C_G(a)$ is σ-invariant. Consequently, D can be chosen to be σ-invariant.

Now assume $|a| > |\tau|$ and let $t = a^r$. If $p \neq r$, then t is contained in a maximal torus of G, so $C_G(t)$ is a subsystem subgroup and a induces an involutory (or order 3) semisimple automorphism of this group (it cannot centralize $C_G(t)$ as maximal tori are selfcentralizing). The result follows with $D = C_G(a)$. Otherwise, $C_G(a)$ is contained in a σ-invariant canonical parabolic D, completing the proof of (ii).

Finally assume we are in the situation of (iii), so that $|a| = 2^e$. If a is an involution, then it is well known that $C_L(a) = {}^2B_2(q), {}^2F_4(q)$ or ${}^2G_2(q)$. Otherwise, $1 \neq a^2 \in L$ so $C_L(a)$ centralizes an involution in L and the assertion follows from well-known information on involution centralizers in these groups. □

The Exceptional Groups

Let L be a finite exceptional group.

Proposition 7.2.8. *Condition (Gen) holds if* $L = E_8(q), E_7(q), E_6^\epsilon(q), F_4(q)$.

Proof. In nearly all cases we take x to be a regular unipotent element of L, so Lemma **??** implies $C_A(u) = U\langle\delta, \tau\rangle$, where δ generates the group of field automorphisms and τ is a graph automorphism, if such exists. We will first choose y_1, y_2 as certain semisimple elements. The remaining elements will usually be taken as non-conjugate generators of $\langle y_1\rangle$ or $\langle y_2\rangle$.

In the following table we provide information on the order of the elements y_1, y_2. The numbers indicated are orders of elements in universal covers of certain subgroups of L. Except for the case $y_2 \in E_6^\epsilon(q)$, the order of a given element y_i will be the number indicated divided by a small constant, which can be deduced from comments below. In the exceptional case the order is presented as a product, indicating that the element is the product of two elements of the given orders. In the case of $L = {}^2E_6(q)$ the order of one element divides the order of the other, so in this case the product has order less than the number given.

G	y_1	y_2
$E_8(q)$	$q^9 - 1/q - 1$	$q^9 + 1/q + 1$
$E_7(q)$	$q^8 - 1/q - 1$	$q^7 + 1$
$E_6^\epsilon(q)$	$q^9 - \epsilon/(q^3 - \epsilon)$	$(q^5 - \epsilon)(q + 1)$
$F_4(q)$	$q^4 + 1$	$q^4 - 1$

The existence of the elements indicated follows immediately from the following containments, which in turn follow via Lang's theorem from the existence of standard subsystems of the root system.

$E_8(q) \geq A_8^\epsilon$ (an image of $SL(9,q), SU(9,q)$ with kernel of order $(3, q-\epsilon)$)
$E_7(q) \geq A_7^\epsilon(q)$ (an image of $SL(8,q), SU(8,q)$ with kernel of order $(4, q-\epsilon)$)
$E_6^\epsilon(q) > A_2^\epsilon(q^3)$ and $A_5^\epsilon(q)A_1(q)$ (central product, no central 3-element).
$F_4(q) > B_4(q) > D_4^\epsilon(q)$ (simply connected)
(In the last case y_1 is the image of an irreducible element of $SO^-(8,q)'$, while y_2 correponds to an element of $GL_4(q) < SO^+(8,q)$).

Lemma 7.2.9. *Let $y_i \in L$ as above. Then either $C_G(y_i)$ is a maximal torus, T, of G or $L = F_4(2)$ and $i = 2$.*

Proof. We have $y_i \in T$ for a maximal torus $T < G$, so it will suffice to show that $C_G(y_i)$ is connected and has dimension equal to that of T. We first consider the dimension of the centralizer. Now $\dim C_G(y_i) = \dim C_{L(G)}(y_i)$ (see p.28 of [**?**]), so it suffices to show that $\dim C_{L(G)}(y_i) = \dim(T)$.

We determine the action of y_i on $L(G)$ by first computing the restriction of $L(G)$ to the subgroups indicated above. We do this at the level of algebraic groups, where the information is given explicitly in 2.1 of [**?**]. The results are as follows

$L(E_8) \downarrow A_8 = L(A_8) \oplus V_{A_8}(\lambda_3) \oplus V_{A_8}(\lambda_6)$
$L(E_7) \downarrow A_7 = L(A_7) \oplus V_{A_7}(\lambda_4)$
$L(E_6) \downarrow A_1A_5 = L(A_1A_5) \oplus (V_{A_1}(\lambda_1) \otimes V_{A_5}(\lambda_3))$
$L(E_6) \downarrow A_2A_2A_2 = L(A_2A_2A_2) \oplus V_{A_2A_2A_2}((\lambda_1, \lambda_1, \lambda_1)) \oplus V_{A_2A_2A_2}((\lambda_2, \lambda_2, \lambda_2))$
$L(F_4) \downarrow D_4 = L(D_4) \oplus V_{D_4}(\lambda_1) \oplus V_{D_4}(\lambda_3) \oplus V_{D_4}(\lambda_4)$.

In the second E_6 case $V_{A_2A_2A_2}((\lambda_1, \lambda_1, \lambda_1))$ is just the tensor product of natural 3-dimensional modules, one for each A_2 factor. In the last case the modules $V_{D_4}(\lambda_i)$ are the three 8-dimensional orthogonal representations. We also note that $V_{A_k}(\lambda_i)$ is the i-th wedge of a usual module.

Consider the action of an element y_i on $L(G)$. We can write down the precise eigenvalues of y_i on the natural module of the above classical group. Using this, we can determine the precise action on $L(G)$. In all but two cases we find that $C_{L(G)}(y_i)$ has dimension equal to the rank of G just using the order of y_i and that the fixed points are contained in the Lie algebra of the classical group indicated. One exception is $L = F_4(q)$ and $y_i = y_2$. Here $y_i \in GL_4(q)$ and on one of the orthogonal modules the SL_4 factor acts as $SO^+(6,q)$, fixing a 2-space. So when $q = 2, y_2$ has extra fixed points. This case is allowed for in the statement. The other exception is where $G = E_6 > A_1A_5$ with $y_i = y_2 = ab$, with a in the A_5 factor and b a noncentral element in the A_1 factor. Let $a_0 \in \langle a \rangle$ have prime order for a primitive divisor of $|a|$. Then $\dim(C_{L(G)}(a_o)) = 8$ and so $C_G(a_o) = A_1T_5$. Then $C_G(y_2) \leq C_G(a_o) \cap C_G(b)$, a maximal torus, as required.

Finally, we must show that $C_G(y_i)$ is connected. Let $\tilde{G}$ be the simply connected cover of G, $\tilde{y}_i$ a preimage of y_i, and $\tilde{T}$ the preimage of T. By II, 3.9 of [**?**] centralizers of semisimple elements in $\tilde{G}$ are connected. So we are done except perhaps when $G = E_6$ or E_7 and there is an element $\tilde{g} \in \tilde{G}$ such that $\tilde{y}_i^{\tilde{g}} = \tilde{y}_i z$, where $1 \neq z$ is a generator of $Z(\tilde{G})$. Here z has order 3 (respectively 2) so $\tilde{g}$ centralizes $\tilde{t} = \tilde{y}_i^3$ (respectively $\tilde{y}_i^2$). However, arguing as above

we find that $C_{\tilde{G}}(\tilde{t}) = \tilde{T}$, which is a contradiction (A slight modification is necessary in this argument when $L = {}^2E_6(2)$ with $y_i = y_2$. Here $\tilde{t}$ has order 11 and $C_G(\tilde{t}) = A_1T_5$, which cannot contain such an element $\tilde{g}$). □

It will be convenient to settle the $F_4(2)$ case at this point. Here we take $x = y_1$ of order 17. Then Lemmas **??** and **??** imply that $C_A(x) = \langle x \rangle$, so we obtain the result provided there exist sufficient number of classes of elements of different order. But there are already enough classes of unipotent elements (e.g. unipotents of type A_1, A_2, F_4, B_2, C_3 in the Bala-Carter notation (see pp.174-177 of [**?**] and note that these classes exist in all characteristics).

Set $C_i = \langle y_i \rangle$ and $A_i = N_A(C_i)/C_A(C_i)$. In addition, write $q = p^a$, for p a prime.

Lemma 7.2.10. *(i) $C_A(y_i) = T_i$, a maximal torus of G_σ.*

(ii) For $i = 1, 2$, $|A_i|$ divides l_i , where $(l_1, l_2) = (18a, 18a), (32a, 14a), (18a, 20a), (16a, 16a)$, according to $G = E_8, E_7, E_6, F_4$, respectively. In the last case we can take $(l_1, l_2) = (8a, 8a)$, if $p \neq 2$.

Proof. Lemma **??** shows that $C_A(y_i) \subseteq T\langle \delta, \tau \rangle$, where $T \subseteq C_A(y_i)$ is a maximal torus of G_σ and where δ, τ are in the coset of a field and graph (or special graph) automorphism. The latter only occurs for $G = E_6$ or for F_4 with $p = 2$. Suppose $a \in C_A(y_i) \smallsetminus T$, which we may take to have prime power order. Then by Lemma **??**, $a \in A \smallsetminus G_\sigma$, and we may apply Lemma **??**. If **??**(i) holds, then $y_i \in G(q_o)$ and primitive divisor arguments rule out all cases except for $y_1 \in E_8(q)$ and $y_2 \in F_4(q)$. Then y_i is contained in a maximal torus of $G(q_o)$ so 1.6 of [**?**] implies $|y_i| \leq (q_o + 1)^8, (q_o + 1)^4$, respectively. This is impossible. If **??**(ii) holds, then $L = E_6^\epsilon(q)$. Suppose $|a| = 2$. Then by 1.1 of [**?**] either $p > 2$ and $C_G(a) = F_4, C_4$ or $p = 2$ and $C_G(a) = F_4$ or $C_{F_4}(u)$ for u a long root element. Taking fixed points under σ and using order considerations we see that none of these have order divisible by $|y_i|$. Suppose $|a| > 2$. If $p = 2$, then $C_L(a^2)$ is contained in a canonical parabolic of L, say P. Order considerations show that the Levi must be of type $A_5(q)^\epsilon$. But then a must induce an involutory outer automorphism of this Levi centralizing the image of y_i. But there is no such automorphism. We have a similar contradiction if $p > 2$, from consideration of the action of a on the subsystem group $D = C_L(a^2)$. The arguments are similar if **??**(iii) holds. If $|a| = 2$, then y_i is in a maximal torus of ${}^2F_4(q)$ and hence has order at most $(q + 1)^2$, a contradiction. And if $|a| > 2$, then y_i is in a proper parabolic of ${}^2F_4(q)$, giving a numerical contradiction. This proves (i).

Now consider *(ii)*. We determine the normalizer $N_{G_\sigma}(C_i)$ from Carter [**?**]. This normalizer modulo T_i is the centralizer in the Weyl group of that element in the Weyl group determining the maximal torus. We use the information in Carter [**?**] to find this centralizer. We then obtain a bound for the full normalizer in A by multiplying by the order of the group of field and graph (including special graph) automorphisms. □

We are now in position to prove Proposition **??**. Lemmas **??** and **??** imply $d(x, y_i) \geq 3$ for $i = 1, 2$. Obviously this will also hold for any generators of C_i. So if we can find 5 such elements no two of which are conjugate in A, then we have the assertion.

Consider the orbits on the generators of C_i. We have $\phi(|C_i|) \geq \sqrt{|C_i|}$, where ϕ is the Euler function. So the number of nonconjugate generators is at least

$$\sqrt{|C_1|}/|A_1| + \sqrt{|C_2|}/|A_2|.$$

Suppose that this number is less than 5. One checks that if $G = E_8$, then $q = 2$ and otherwise $q \leq 4$, with the one exception of $F_4(8)$.

It remains to work through these small values of q. For all cases other than $L(q) = {}^2E_6(2)$ one can use the precise numerical information to check that there are indeed at least 5 A-classes of generators of the groups C_i.

Assume $L = {}^2E_6(2)$. Let $x = y_1$ be an element of order 19. So x lies in a torus, T of G_σ of order $2^9 + 1/2^3 + 1 = 19 \cdot 3$. Lemma **??** implies that $C_A(x) = T$. Suppose t is an element of order 3 in this torus. From the construction of y_1 we see that $C_G(t) = A_2A_2A_2$ and $C_L(t) = PSU(3, 8)$. Consequently, if we choose elements y_i not conjugate to elements of $PSU(3, 8)$, then $d(x, y_i) \geq 3$. But this is easy as there are sufficiently many unipotent classes with this property. This completes the proof of Proposition **??**. □

Lemma 7.2.11. *Condition (Gen) holds if $L = G_2(q)(q \neq 2), {}^3D_4(q)$, or ${}^2F_4(q)'$.*

Proof. First assume $L = G_2(q)$. Then $L \geq A_2^\epsilon(q)$ which contains an element x of order $q^2 + \epsilon q + 1$. We take $\epsilon = 1$, unless this number is divisible by 3, in which case we set $\epsilon = -1$. The maximal subsystem subgroups of G are of type $A_1\tilde{A}_1$ and A_2 (also $\tilde{A}_2$ for $p = 3$). Using this together with our choice of ϵ and the fact that x is in no proper parabolic subgroup of L, we see that if $1 \neq g \in C_{G_\sigma}(x)$, then $C_G(g)$ is a torus. Also Lemma **??** implies $C_A(x) = \langle x \rangle$.

We can now take y_i to be a nontrivial unipotent element multiplied by any semisimple element in its centralizer. It is easy to find enough choices. Using the Bala-Carter notation for unipotent elements we take $y_1 = G_2$, a regular unipotent element, $y_2 = G_2(a_1)$ (a regular unipotent element in an A_2 subgroup), y_3 a unipotent element of type A_1, and $y_4 = y_3z$, where z is a semisimple element in $\tilde{A}_1$, the centralizer of the A_1 subgroup containing y_3. If $p \neq 3$ let y_5 be unipotent of type $\tilde{A}_1$. If $p = 3$, then root elements for long and short roots are conjugate in A, but here there is an extra class of 3-central elements and y_5 is taken as a representative of this class.

The cases $Y = {}^3D_4(q)$ and ${}^2F_4(q)'$ are handled similarly. Here we take x to be a semisimple element of order $q^4 + q^2 + 1$ or $q^2 + q\sqrt{2q} + q + \sqrt{2q} + 1$, respectively. These numbers are factors of $q^6 - 1$ and $q^6 + 1$, respectively, and we argue as above that $C_A(x)$ is a torus and that no nonidentity element of this torus centralizes a nontrivial unipotent element. So again we choose elements y_i with nontrivial unipotent part. The existence of such elements follows easily as in the G_2 case, from the containments $SL(2, q) \cdot SL(2, q^3) < {}^3D_4(q)$ and ${}^2B_2(q) \cdot {}^2B_2(q) < {}^2F_4(q)$, except when $L = {}^2F_4(2)'$. Here we take x to have order 13. Then $C_A(x) = \langle x \rangle$ and we need only show that there are at least 5 A-classes within L of elements having order not dividing 13. This can be easily checked from the ATLAS.

This leaves the rank 1 Suzuki and Ree groups. □

Lemma 7.2.12. *Condition (Gen) holds if $L = {}^2G_2(q)(q > 3)$ or ${}^2B_2(q)(q > 2)$.*

Proof. Let x be an element of order $q+\sqrt{3q}+1$ or $q\pm\sqrt{2q}+1$ according to $L={}^2G_2(q)$ or ${}^2B_2(q)$. As in other cases $C_A(x)=\langle x\rangle=T$, a torus, and $C_L(t)=T$ for each nonidentity element $t\in T$. It only remains to exhibit appropriate elements $y_1,\dots,y_5$.

For ${}^2G_2(q)$ this is easy. Let y_1,y_2,y_3 be elements of order $3,3,9$, respectively. We choose these elements so that $C_L(y_1)$ is a Sylow 3-group, while $C_L(y_2)$ contains an involution t (recall that ${}^2G_2(q)\geq L_2(q)\times\langle t\rangle$). Now let $y_4=y_2t$ and let y_5 be an element of order $q-1$.

Suppose $L={}^2B_2(q)$, with $q>8$. We note that 5 divides $q^2+1=(q+\sqrt{2q}+1)(q-\sqrt{2q}+1)$. Choose x so that $|x|$ is the factor not divisible by 5. Now choose elements $y_1,\dots,y_5$ such that $|y_1|=2,|y_2|=4,|y_3|=q-1,|y_4|=5$, and $|y_5|=q\pm\sqrt{2q}+1$, where we choose signs so that $|x|\cdot|y_5|=q^2+1$. The result follows.

Finally, consider $L={}^2B_2(8)$. Let x have order 13. Then $C_A(x)=\langle x\rangle$. Then choose y_1,y_2,y_3,y_4,y_5 as elements of order $2,4,4,5,7$, noting that there are two classes of elements of order 4 in A (see ATLAS). □

The Classical groups

Lemma 7.2.13. *Condition (Gen) holds in each of the following situations:*
(i) $L=PSp(2n,q)$ *for* $n\geq 2$ *and* $L\neq PSp(4,2)$.
(ii) $L=PSL(n,q)$ *for* $n\geq 3$ *and* $L\neq PSL(3,2),PSL(3,4)$.
(iii) $L=PSU(n,q)$ *for* $n\geq 3$.

Proof. For $L=PSp(2n,q),PSL(n,q)$, or $PSU(n,q)$ for n odd, let x be a generator of the image in L of a cyclic irreducible torus (Singer cycle) of $Sp(2n,q),SL(n,q)$ or $SU(n,q)$, respectively. Then $|x|=q^n+1/(2,q-1)$, $q^n-1/(q-1)(n,q-1)$, or $q^n+1/(q+1)(n,q+1)$, respectively. If $L=PSU(n,q)$ with n even, take x of order $q^n-1/(q+1)(n,q+1)$, except for the cases $(n,q)=(4,3)$ and $(6,2)$, which we postpone until later in the proof.

We claim $C_A(x)$ is a maximal torus of G_σ, with $\langle x\rangle$ of index $(2,q-1),(n,q-1),(n,q+1)$, respectively. We first use the action on the usual module to argue that $C_{G_\sigma}(x)=T$, a maximal torus. Some care must be taken in this as we are working in the simple group rather than the linear group. In cases where the classical group has a nontrivial center let $y\in\langle x\rangle$ be an element of prime order for a primitive divisor of $|x|$. The order of the center is not divisible by this prime so $C_L(y)$ is covered by the centralizer in the corresponding linear group. As y has distinct eigenvalues on the natural module we have $C_{G_\sigma}(y)=T$ and hence $C_{G_\sigma}(x)=T$.

If $C_A(x)>T$, then x is centralized by an element $a\in A\smallsetminus G_\sigma$ such that aG_σ has prime order and a has prime power order. Lemma **??** together with primitive divisor arguments reduce us to the case where $aG_\sigma=\tau G_\sigma$ for τ a graph or graph field automorphism of $PSL_n^\epsilon(q)$ or an involutory special graph automorphism of $PSp(4,q)$. If a is in the coset of a special graph automorphism, then **??**(iii) shows that x is contained in a parabolic subgroup of $PSp(4,q)$ or ${}^2B_2(q)$. The former is clearly impossible. In the latter case q^2+1 divides the order of ${}^2B_2(q)$, but a variation of 1.6 of [**?**] which is proved in the reference cited for this result shows that semisimple elements of ${}^2B_2(q)$ have order at most $(\sqrt{q}+1)^2$, a contradiction. Hence, $L=PSL^\epsilon(q)$. Let D be as in **??**(ii). If D is reductive, then D_σ cannot contain x (although

it may contain an element of order a primitive prime divisor of $|x|$. For example this happens in certain cases where D is a symplectic group or an orthogonal group. It also happens when τ is a graph field automorphism of $L = PSL(n,q)$ for n odd and $G_\delta \cong PGU(n,\sqrt{q}))$.

Suppose D is parabolic, forcing $p = 2$. Since x does not centralize an involution of L we must have $|a| = 2$. The parabolic case arose here when $D = C_G(a)$ had nontrivial unipotent radical. But this only occurs for n even where D is the centralizer of a root element in the corresponding symplectic group. But then $x \notin D_\sigma$. We have now proved the claim.

Choose elements as follows. Consider the subgroups $Sp(2r,q) \times Sp(2n-2r,q) \leq Sp(2n,q)$ for $1 \leq r \leq n$; $SL(r,q) \times SL(n-r,q) \leq SL(n,q)$ for $2 \leq r \leq n$; and $SU(r,q) \times SU(n-r,q) \leq SU(n,q)$ for $2 \leq r \leq n$. Let u_r be a regular unipotent element of the first factor and s_{n-r} any semisimple element in the second factor. Set $d_r = u_r s_{n-r}$.

We claim that $C_A(d_r) \cap C_A(x) = 1$. Suppose $1 \neq g$ is in the intersection. First note that $C_A(d_r) = C_A(u_r) \cap C_A(s_{n-r})$. By the claim $g \in T$ and so g is a semisimple element of G. Now $C_G(g)$ is a σ-invariant reductive group containing both x and u_r. Using the fact that $x \in C_G(g)$ together with primitive divisor arguments, we find that there are few possibilities for $C_L(g)$. In particular, either $C_G(g)_\sigma$ is irreducible on the natural module so that groups such as $PSp(2a,q^b)$ with $n = ab$ occur, or $L = PSU(n,q)$ with n even and $C_{G_\sigma}(g) = PGL_{\frac{n}{2}}(q^2)$. In each case $C_G(g)'$ is a commuting product of several isomorphic simple groups with $\langle\sigma\rangle$ permuting the components transitively. But now consider the embedding of u_r in this centralizer. On the one hand u_r is a diagonal element in the commuting product. On the other hand u_r has a single nontrivial Jordan block on the natural module. This is a contradiction.

We have shown that $d(x,d_r) \geq 3$. It remains to show that there are enough such elements. In the symplectic case this is clear if $n \geq 5$, since here we can simply take $y_i = u_i$ for $1 \leq i \leq 5$. For smaller symplectic groups we take as many unipotent elements as possible and then adjust them by semisimple factors. For example if $L = PSp(4,q), q > 4$, we set $y_1 = u_2$ (a regular unipotent element), $y_2 = u_1$ and $y_i = u_1 z_i$ for $3 \leq i \leq 5$, where z_3, z_4, z_5 are nonidentity semisimple elements of $Sp(2,q)$ of different orders. If $L = PSp(4,4)$, then $|x| = 17$. Then $C_A(x) = \langle x\rangle$ so we can take $y_1, \ldots, y_5$ any nonconjugate elements of order different from 17. Suppose $L = PSp(4,3)$. Here $|x| = 5$ and $C_A(x) = \langle x,t\rangle$, where t is an involution with $C_L(t) = S_6$ (regard L as $PSU(4,2)$ and $C_L(x)$ as $Sp(4,2)$). From ATLAS we see that L contains 4 A-classes of elements of order 6 only two of which reside in $C_L(t)$. Also root elements of order 3 cannot lie in $C_L(t)$. Consequently we can take $y_1, \ldots, y_5$ as elements of order $3, 6, 6, 9, 12$, respectively.

Now consider the cases $L = PSL(n,q), PSU(n,q)$. Note that $PSU(4,2) \cong PSp(4,3)$ was handled in the previous paragraph. For $n \geq 6$ we just use $u_2, \ldots, u_6$. For smaller values of $n \geq 4$ multiply the u_i by semisimple elements as above. The details are quite easy, except for the case $PSL(4,3)$. Here we take $y_1 = u_4, y_2 = u_2, y_3 = u_2 s, y_4 = u_2 t, y_5 = z$, where s, t are elements of order $2, 4$ centralizing u_2 and z has order 13.

At this point we consider the previously excluded cases $L = PSU(4,3)$ and $L = PSU(6,2)$. In these cases take x to be a semsimple element of order $7, 11$ respectively. We then find that $C_A(x) = \langle x\rangle \times Z$ where Z is cyclic of order $q+1$ with $Z \cap L = 1$. If $1 \neq z \in Z$, then

$C_L(z) = SU(n-1,q)$. We can now choose elements $y_1, \dots, y_5$ as follows. If $L = PSU(6,2)$ let y_1 be a regular unipotent element, y_2 of order $15, y_3$ of order 7 in a subgroup $SL(3,4), y_4$ a regular unipotent element in $SL(3,4)$, and y_5 an element of order 10. If $L = PSU(4,3)$, let y_1 be a regular unipotent element, y_2 an element of order $5, y_3$ an element of order 6 (there are two classes, choose the one not represented in $SU(3,3)$), y_4 an element of order 4 in $PSL(2,9)$, and y_5 a unipotent element of $PSL(2,9)$. From what has been established so far, we obtain the result in both these cases.

We use a slightly different argument for $L = PSL(3,q), PSU(3,q)$ as there are fewer classes of unipotent elements. Let x be as before and set $y_1 = u_3$ (a regular unipotent element) and $y_2 = u_2$ (a root element). We are assuming $q \neq 2, 4$ for $PSL(3,q)$ so we can take $y_3 = u_2 s$, for $1 \neq s$ of order dividing $q-1, q+1$, respectively. There is a cyclic maximal torus of $SL(3,q)$ and $SU(3,q)$ of order q^2-1 and y_4, y_5 are taken as images in $PSL(3,q)$ (resp. $PSU(3,q)$) of members of this torus. We need to verify that there are two such classes and that they have distance at least 3 from x.

The latter statement is established as above, by looking at the full centralizer of an element centralizing both x and y_i for $i = 4, 5$. For the former, first note that A-fusion in the torus is controlled by the normalizer, which induces a group of order $4a$, where $q = p^a$. Hence, in order to get two nonidentity classes it will suffice that $(q^2-2)/3 \cdot 4a \geq 2$. This holds provided $q \neq 2, 3, 4, 5, 8$. If $q = 3$ or 5, the torus in question has an element of order 8 so we can choose elements y_4, y_5 of order 4 and 8. Similarly we can choose elements of different order when $q = 8$. So we have the result, except for the case $PSU(3,4)$. Here we note that there are at least two classes of elements of order 5 and we take y_4, y_5 such elements. □

Lemma 7.2.14. *Let $L = PSL(2,q)$. Condition (Gen) holds except when $q = 5, 7, 8, 9, 11, 16,$ or 27.*

Proof. Let x be a nonidentity unipotent element, so that $C_A(x) = U\langle\delta\rangle$ for δ a field automorphism. Then **??**(i) implies $d(x,y) \geq 3$ for any semisimple element $y \in L$ such that y is not centralized by a nontrivial field automorphism of L. In particular this will hold if y is taken as a generator of a cyclic maximal torus of order $(q-1)/d$ or $(q+1)/d$, for $d = (2, q-1)$. Using the Euler ϕ-function we see that there are at least $\sqrt{(q-1)/d}, \sqrt{(q+1)/d}$ such elements, respectively. Under the action of the normalizer of this torus the generators fall into classes of length $2a$. Consequently, we can find at least 5 such conjugacy classes provided

$$2(\sqrt{(q-1)/d})/2a \geq 5.$$

So the assertion holds provided $q - 1 \geq 25da^2$. A direct check shows that this condition is satisfied except for the following cases:

$$p = 2,\ a \leq 11; \qquad p = 3,\ a \leq 7; \qquad p = 5,\ a \leq 4; \qquad p = 7,\ a \leq 3;$$

$$p = 11, 13, 17,\ a \leq 2 \qquad q = 19, \dots, 47.$$

All cases, except $PSL(2,13)$ and $PSL(2,25)$ can be checked directly, using precise information on the number of generators of the tori. For example, if $L = PSL(2,64)$ there are 48 generators of a torus of order 65, falling into 4 orbits under the normalizer in A. The

cases can all be settled in this way and details are left to the reader. Consider $PSL(2,13)$. Choose $y_1, \dots, y_5$ of order $2, 3, 6, 7, 7$ (note that A has 3 classes of elements of order 7). Since $C_A(x) = \langle x \rangle$, the result follows. Finally, consider $PSL(2,25)$. Here we take x to be an element of order 13. Then $C_A(x)$ has order 26 and the involution in this group has L-centralizer equal to $\langle x \rangle$. So just choose elements $y_1, \dots, y_5$ of order $3, 4, 5, 6, 12$ to get the result. □

The final lemma of this subsection deals with orthogonal groups. We ignore odd dimensional orthogonal groups in even characteristic, as these were handled previously as symplectic groups.

Lemma 7.2.15. *Let $L = PSO^\epsilon(n,q)'$ for $n \geq 7$. Then (Gen) holds unless $L = PSO^+(8,2)$.*

Proof. For later reference we first note that $SO^\epsilon(2k,q)$ contains an element of order $q^k - \epsilon$, which generates a maximal torus. For $p > 2$, this element is not contained in $SO^\epsilon(2k,q)'$, although the derived group does contain the square of the element.

First assume that $n = 2k+1$ is odd, so that there are no graph automorphisms. Take x to be a regular unipotent element. Then $C_A(x) = U\langle\delta\rangle$, for δ a field automorphism. It will suffice to find a sufficient number of semisimple elements y centralized by no element of $U\langle\delta\rangle$. We note that **??**(i) shows that elements of $U\langle\delta\rangle \smallsetminus U$ have fixed points on G of the form $G(q_o)$ for $q_o < q$ (as usual we identify an automorphism of L with an extension to G).

Temporarily exclude $L = PSO(7,3)'$. In the remaining cases choose elements as follows. Let $y_1 \in SO^+(2k,q)'$ have order $(q^k - 1)/2$ and $y_2 \in SO^-(2k,q)'$ have order $(q^k + 1)/2$. Similarly, choose elements a_3, a_4 of order $(q^{k-1}+1)/2, (q^{k-1}-1)/2$, respectively, in groups $SO^-(2k-2,q)', SO^+(2k-2,q)'$ and let b_3, b_4 be nontrivial semisimple elements of $C_L(SO^\pm(2k-2,q)') \cong SO(3,q)'$. Set $y_3 = a_3b_3$ and $y_4 = a_4b_4$. If k is odd, let y_5 be a power of y_2 of order $(q^k+1)/(q+1)$ and if k is even, let $y_5 = a_5b_5$, where $a_5 \in \langle a_3 \rangle$ has order $(q^{k-1}+1)/(q+1)$ and $b_5 = b_3$.

We claim that $C_{G_\sigma}(y_i)$ is a maximal torus for $1 \leq i \leq 5$. The claim is equivalent to the assertion that $C_G(y_i)$ is a maximal torus. If this is not the case then $C_G(y_i)$ contains a simple component which would centralize the preimage of y_i in its action on the natural module, hence stabilize each eigenspace. However, by choice of y_i each eigenspace either has dimension 1 or the eigenvalue is -1 with corresponding eigenspace being nondegenerate of dimension at most 2. In any case the eigenspace can afford only the trivial action of the simple factor, a contradiction. This gives the claim and then Lemma **??**(i) implies $C_A(y_i)$ is torus. Then the first paragraph gives $d(x, y_i) \geq 3$ for $i = 1, \dots, 5$.

If $L = PSO(7,3)'$, set y_1, y_2, y_3, y_4, y_5 elements of order $10, 13, 20, 14, 7$, respectively. Using ATLAS we see that none of these elements is centralized by a nontrivial unipotent element of L. On the other hand, $C_A(x) = U$ a unipotent group. So the result holds here as well.

Now suppose $n = 2k$. First assume $k \geq 5$. We again take u to be a regular unipotent element, but here we must be more careful as $C_A(u) = U\langle\tau,\delta\rangle$ where τ is a graph automorphism which centralizes large parts of maximal tori. Let y_1 be the image in L of an element of $SO^\epsilon(2k,q)'$ of order $(q^k - \epsilon)/d$, where $d = 1$ or 2, according to whether q is even or odd.

There exist subgroups $SO^{-\epsilon}(2k-4,q) \times SO^-(4,q)$ and $SO^\epsilon(2k-4,q) \times SO^+(4,q)$ of $SO^\epsilon(2k,q)$. From the first subgroup we take $y_2 = a_2b_2$ and $y_3 = a_3b_3$ where $a_2 = a_3$ is

the image in L of an element of order $q^{k-2}+\epsilon$ while b_2, b_3 are images of elements of order q^2-1, q^2+1, respectively. For p odd, the elements a_i, b_i do not lie in the derived group of $SO^\epsilon(n,q)$, but their product does.

Let $y_4 = a_4b_4$ be in the second group, with a_4 of order $q^{k-2}-\epsilon$ and b_4 of order q^2-1 (if $q=2$ choose b_4 to be in one of the $SL(2,2)$ factors of $SO^+(4,2)$). Each of y_2, y_3, y_4 are products of two elements and these elements may not have relatively prime orders. So the order of y_i may be less than that of the product of the orders of the factors. More important than the order is the action of a preimage of y_i on the orthogonal module and this action is clear from the description.

We require one more element. If $q^k-\epsilon$ has a primitive prime divisor of order less than $|y_1|$, then we can take y_5 to be an element of this order. If there is no such element, then either (i) $q^k-\epsilon = p^{2^s}+1$; or (ii) $q^k-\epsilon = 2^k-1 = r$, with r prime; or (iii) $q^k-\epsilon = 3^k-1 = 2r$ with r prime. In the last two cases there are $r-1$ generators of $\langle y_1\rangle$ and we can choose y_5 as a generator not A-conjugate to y_1 (eigenvalue arguments show that $N_A(\langle y_i\rangle)/C_A(y_i)$ has order at most $2k$). If (i) holds we can factor $q^{k-2}+\epsilon$, take an element $a_5 \in \langle a_3\rangle$ of order a primitive prime divisor and then set $y_5 = a_5b_5$, where $b_5 = b_3^2$ (we use the square to obtain an element in $SO^-(4,q)'$).

We claim that for $1 \le i \le 5$, $C_A(y_i)$ is a torus of G_σ. As above, eigenspace arguments show that $C_{G_\sigma}(y_i)$ is a torus. Next, **??**(i) and primitive divisor arguments reduce consideration to elements in the coset of a graph automorphism. Let a be as in **??**(ii), with $|a|$ a power of 2. Note that a is in the image of the full orthogonal group. If $p=2$, then a is an involution, as y_i centralizes no involution in G_σ. Then a is of type b_j in the notation of [**?**] and 8.7 of [**?**] shows that semisimple elements in $C_L(a)$ have fixed points on the orthogonal module. This is a contradiction as y_i has no fixed points.

Suppose p is odd. Let $\hat{a}$ and $\hat{y}_i$ denote preimages of a, y_i in $SO(n,q)$. Then $\hat{a}$ centralizes $\hat{y}_i$ modulo the center, so $\hat{a}$ centralizes $\hat{y}_i^2$. Consider the eigenspaces of $\hat{a}$. If β is an eigenvalue other then ± 1, then β^{-1} must also be an eigenvalue of equal multiplicity as otherwise, $\hat{a}$ would not preserve the orthogonal form. As $\det(\hat{a}) = -1$, we see that the eigenspace for eigenvalue -1 must be nondegenerate of odd multiplicity. However, by choice of y_i we see that $\hat{y}_i^2$ leaves invariant no subspace of odd dimension. This establishes the claim and the result follows.

We are left with the cases $L = PSO^\epsilon(8,q)'$, excluding $L \cong PSO^+(8,2)$. First assume $q > 5$ for $\epsilon = 1$ and $q > 3$ for $\epsilon = -1$.

Let x be a regular unipotent element. Choose y_1 to be the image in L of an element of order $q^4 - \epsilon/d$ in $SO^\epsilon(8,q)'$ for $d = 1$ or 2. Write $q = p^a$.

We first claim that $C_A(y_1)$ is a maximal torus of G_σ and that $N_A(\langle y_1\rangle)/C_A(\langle y_1\rangle)$ has order dividing $16a$.

Using the description of $\langle y_1\rangle$ as a maximal torus, we see that it is normalized by a group of field automorphisms of L of order a. Next argue that for $\epsilon = 1$ no element in the coset of a nontrivial triality graph automorphism can normalize $\langle y_1\rangle$. Indeed, triality morphisms

permute the 8-dimensional orthogonal representations, whereas if $v \in \langle y_1 \rangle$ has order a primitive prime divisor of $|y_1|$, then $\hat{v} \in SL_4(q)$ has no fixed points on two of these modules, but a 2-dimensional fixed point space on the third.

The usual arguments show that $C_A(y_1)$ is a maximal torus of G_σ and $N_{G_\sigma}(\langle y_1 \rangle)$ induces a group of order 8 (the centralizer of an element of order 4 in the Weyl group). The claim now follows from the structure of A.

At this point we argue as in **??** that we can choose $y_2, \ldots, y_5$ as nonconjugate generators of $\langle y_1 \rangle$. For $q > 11$ this follows easily from numerical estimates, and in smaller cases one uses precise information on the number of generators. The result follows.

This leaves us with several small cases. If $L \cong PSO^-(8,2)$, let $x \in L$ be an element of order 17. Then $C_A(x) = \langle x \rangle$ and so we can take $y_1, \ldots, y_5$ as any classes corresponding to elements of L having order other than 17.

If $L \cong PSO^-(8,3)$, let $x \in L$ be an element of order 41. Then $C_A(x) = \langle x, t \rangle$, for t an involution. The only possibility is that $C_L(t) = L_2(81)$. This centralizer is diagonal in a group $A_1^4 < G = D_4$. Let $y_1, \ldots, y_5$ be unipotent elements of type $A_1, A_1A_1, A_1A_1A_1, A_3, D_4$ (in the Bala-Carter notation), respectively. From the action on the orthogonal module we see that none of these is represented in $C_L(t)$.

Assume $L = PSO^+(8,5)$. Let x (a regular unipotent element) and y_1 be as before. Here $\langle y_1 \rangle$ has 48 generators so by the above claim there are at least 3 orbits on generators so we take additional orbit representatives y_2, y_3. Now set $y_4 = a_4b_4$, for $a_4 \in SO^-(6,5)$ of order $5^3 + 1$ and $b_4 \in SO^-(2,5)$ of order $5 + 1$ and $y_5 = a_5b_5$, for $a_5 = a_4^6$ and $b_5 = a_4^2$. The earlier arguments show that $C_A(y_i)$ is a torus for each i and the result follows.

Finally, consider $L = PSO^+(8,3)'$. Here we take x to be an element of order 20, realized as an element of order 5 in $SO^-(4,3)$ times an element of order 4 in a commuting $SO^-(4,3)$. Write $x = x_5x_4$ a product of commuting elements of order $5, 4$, respectively. Then $C_A(x) = C_A(x_5) \cap C_A(x_4)$. Each of $C_A(x_5)$ and $C_A(x_4)$ contains a unique subgroup $SO^-(4,3)' \cong PSL(2,9)$. Hence $C_A(x)$ normalizes each factor of $SO^-(4,3)' \times SO^-(4,3)'$. We now argue that $|C_A(x)| = 80$ and that if $1 \neq r \in C_A(x)$ then either r has A-centralizer contained in $O^-(4,3) \cdot O^-(4,3)$ or r is an involution with $C_L(r)' = SO^-(6,3)'$. Choose y_1, y_2 as elements of order $13, 26$, respectively, and let y_3, y_4, y_5 be unipotent elements of types $A_1A_1A_1, D_4, D_4(a_1)$ respectively. The result follows.

□

7.3. **The nongeneric cases.**

The purpose of this subsection is to show that when L is one of the groups,

$$PSL(2,q), \quad q = 5,\ 7,\ 8,\ 9,\ 11,\ 16,\ 27; \quad PSL(3,4) \text{ or } PSO^+(8,2),$$

then G satisfies property $(3\frac{1}{2})$. Since $\mathrm{A}_5 \cong PSL(2,5)$ is the only simple group such that L contains only three $\mathrm{Aut}(L)$ conjugacy classes and it required much of our attention in subsection **??**, we delay it to the end of this subsection. We start with,

Lemma 7.3.1. *Assume $L \cong PSL(2,8)$, then G has the property $(3\frac{1}{2})$.*

Proof. Let $B_1, B_2, B_3 \subseteq L$ be the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $3, 7, 9$, respectively. Let $C_1, \ldots, C_4 \subseteq L$ be the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $3, 7, 9, 2$ respectively.

We show that the hypotheses (c) of Proposition **??** hold; to show hypothesis (c2) of Proposition **??**, we prove that the assumptions in part (a) or (b) of Lemma **??** are satisfied. We first claim that:

(*) For all $u, v \in \bigcup_{i=1}^{3} B_i$ such that $\langle u \rangle \cap \langle v \rangle = 1$, $d_{\mathrm{Aut}(L)}(u, v) > 3$.

Indeed, assume $u \in B_1$ is of order 3. Then it is easy to check that every element $w \in \Delta^{\leq 3}_{\mathrm{Aut}(L)}(u)$, must either centralize u or one of the 9 involutions in $N_L(\langle u \rangle) \cong D_{18}$. Thus if $w \in L$, then either w belongs to the subgroup of order 9 in $C_L(u)$, or w is an involution. Also since $\langle u \rangle \cap \langle v \rangle = 1$, v can not belong to the subgroup of order 9 in $C_L(u)$. If $u \in B_2$, then (*) is obvious and if $u \in B_3$, then $u^3 \in B_1$ and we saw that $d_{\mathrm{Aut}(L)}(u^3, v) > 3$, and hence also $d_{\mathrm{Aut}(L)}(u, v) > 3$. This shows (*), and hence hypothesis (a) of Lemma **??**, for $\mathcal{B} \in \{B_1, \ldots, B_3\}$ and $\mathcal{C} \in \{C_1, \ldots, C_3\}$ holds. It remains to show that:

(**) Let $\mathcal{C}$ be the class of involutions of $\mathrm{Aut}(L)$. Then for each $j \in \{1, 2, 3\}$, if we set $\mathcal{B} = B_j$, then the pair $\mathcal{B}, \mathcal{C}$ satisfy hypothesis (b) of Lemma **??**.

Indeed let $v \in \mathcal{C}$ be an involution and $1 \neq t \in C_{\mathrm{Aut}(L)}(v)$. We'll find $u' \in \mathcal{B}$ such that

(i) $$d_{\mathrm{Aut}(L)}(u', v) \geq 3 \leq d_{\mathrm{Aut}(L)}(u', t),$$

note that we may assume that the order of t is a prime. Assume t is an involution. The reader may easily verify that we can choose $u' \in \mathcal{B}$ not inverted by t or v and that such a u' satisfies (**??**). Assume that t has order 3 (t is an outer automorphism). Note that $C_L(t) \cong S_3$ and so any $u' \in B_1$ such that $u' \notin C_L(t)$ is of distance ≥ 3 from t in $\Delta_{\mathrm{Aut}(L)}$. Thus any $u' \in B_1$ not inverted by v satisfies property (**??**). A similar argument shows that any element $u' \in B_2 \cup B_3$, not inverted by v satisfies (**??**). □

Lemma 7.3.2. *Assume $L \cong PSL(2, 7)$, then G has the property $(3\frac{1}{2})$.*

Proof. The proof here is similar to the proof of Lemma **??**. Let $B_1, B_2, B_3 \subseteq L$ be the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $3, 4, 7$, respectively. Let $C_1, \ldots, C_4 \subseteq L$ be the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $3, 4, 7, 2$ respectively.

We show that the hypotheses in (c) of Proposition **??** holds; again, to show hypothesis (c2) of Proposition **??**, we prove that the assumptions in part (a) or (b) of Lemma **??** are satisfied. We claim that:

(*) (1) For $u \in B_3$ and $1 \neq v \in L$, with $\langle u \rangle \neq \langle v \rangle$, we have $d_{\mathrm{Aut}(L)}(u, v) > 3$.
(2) For $u \in B_1$, we have $|B_1 \cap \Delta^{\leq 3}_{\mathrm{Aut}(L)}(u)| = 8$, and $|B_2 \cap \Delta^{\leq 3}_{\mathrm{Aut}(L)}(u)| = 6$.
(3) For $u \in B_2$, we have $|B_1 \cap \Delta^{\leq 3}_{\mathrm{Aut}(L)}(u)| = 8$, and $|B_2 \cap \Delta^{\leq 3}_{\mathrm{Aut}(L)}(u)| = 10$.

Part (1) of (*) is obvious. For part (2) of (*) assume $u \in B_1$ is of order 3. Let $t \in C_{\mathrm{Aut}(L)}(u)$ be the unique involution. Then every element at distance ≤ 3 from u in $\Delta_{\mathrm{Aut}(L)}$ centralizes one

of the 7 involutions in $C_{\mathrm{Aut}(L)}(t) \cong \mathrm{D}_{12}$. Since there are 4 outer such involutions (including t) and 3 inner such involutions, part (2) of (*) follows.

Assume next that $u \in B_2$. Then every element at distance ≤ 3 from u in $\Delta_{\mathrm{Aut}(L)}$, centralizes one of the 9 involutions in $C_{\mathrm{Aut}(L)}(u^2) \cong \mathrm{D}_{16}$. Since there are 4 outer such involutions and 5 inner such involutions, part (3) of (*) follows. Now (*) implies that hypothesis (a) of Lemma **??** holds for all $\mathcal{B} \in \{B_1, \dots B_3\}$ and $\mathcal{C} \in \{C_1, \dots, C_3\}$. It remains to show:

(**) Let $\mathcal{C}$ be the class of involutions of $\mathrm{Aut}(L)$. Then for each $j \in \{1, 2, 3\}$, if we set $\mathcal{B} = B_j$, then the pair $\mathcal{B}, \mathcal{C}$ satisfy hypothesis (b) of Lemma **??**.

Indeed let $v \in \mathcal{C}$ be an involution and $1 \neq t \in C_{\mathrm{Aut}(L)}(v)$. We'll find $u' \in \mathcal{B}$ such that (**??**) holds. Note again that we may assume that t has prime order, so we may assume that t is an involution. Since $C_{\mathrm{Aut}(L)}(v) \cong \mathrm{D}_{16}$ has 4 outer involutions and 5 inner involutions, it follows that $|B_1 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(v)| = 8$ and that $|B_2 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(v)| = 10$. Also, if $t \notin L$, then $|B_1 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(t)| = 8$, and $|B_2 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(t)| = 6$. An easy counting argument now shows (**). □

Lemma 7.3.3. *Assume $L \cong \mathrm{A}_6$, then G has the property $(3\frac{1}{2})$.*

Proof. Let $B_1, B_2, B_3 \subseteq L$ be the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $3, 4, 5$ and let $C_1, C_2, C_3, C_4 \subseteq L$ be the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $2, 3, 4, 5$, respectively. We show that given $\mathcal{B} \in \{B_1, \dots B_3\}$ and $\mathcal{C} \in \{C_1, \dots, C_4\}$, hypothesis (b) or hypothesis (c) of Lemma **??** holds for $\mathcal{B}, \mathcal{C}$. Then, by Proposition **??**(c), G has the property $(3\frac{1}{2})$.

Write $B_1 = B_1^1 \cup B_1^2$, where B_1^1 is the L-class of 3-cycles and B_1^2 is the other L-class of elements of order 3. Given $1 \neq v \in L$ and $t \in C_{\mathrm{Aut}(L)}(v)$, we'll find $u_1^1 \in B_1^1$, $u_1^2 \in B_1^2$, $u_2 \in B_2$ and $u_3 \in B_3$ (depending on t), such that each $u' \in \{u_1^1, u_1^2, u_2, u_3\}$ satisfies the requirements in hypothesis (b) or (c) of Lemma **??**. If u' satisfies the requirements in hypothesis (c) of Lemma **??**, we'll write $\pi(u', t)$ for the unique path of hypothesis (c), and we'll indicate an $h' \in L$ as required in hypothesis (c). We note now that given $1 \neq v \in L$, if we can show that for all $t \in C_{\mathrm{Aut}(L)}(v)$, there exists u_1^1 as above, and if, in addition, $C_{\mathrm{Aut}(L)}(v)$ contains an element interchanging B_1^1 and B_1^2, then we can also find u_1^2 as above. Note further that to establish hypothesis (b) or (c) of Lemma **??**, we may assume without loss that the order of t is a prime. Thus we distinguish the following cases.

Case 1: $v = (12)(34)$.
Here $C_{\mathrm{Aut}(L)}(v)$ contains an involution interchanging B_1^1 and B_1^2 so we only need to establish the existence of u_1^1, u_2 and u_3. To simplify we denote $u_1 = u_1^1$. Since $C_{\mathrm{Aut}(L)}(v)$ is a 2-group, we may assume that t is an involution.
Subcase 1: $t \in L$.
If $t = (13)(24)$ take $u_1 = (145), u_2 = (1346)(25)$ and $u_3 \in B_3$ not inverted by v or t. The case $t = (14)(23)$ is a conjugate case. If $t = (12)(56)$, take $u_1 = (136)$, $u_2 = (1236)(45)$ and $u_3 \in B_3$ not inverted by v or t. Hypothesis (b) holds in this case. The case $t = (34)(56)$ is a conjugate case.
Subcase 2: t is a transposition or a product of 3 transpositions.

Suppose t is a transposition. Then $t = (12), (34)$, or (56). Let $u_1 = (135)$. We now list the path $\pi(u_1, t)$ and the element h', for the 3 possibilities of t.

$$t = (12) \qquad \pi(u_1, t) = (135), \quad (46), \quad (12); \qquad h' = (124).$$

$$t = (34) \qquad \pi(u_1, t) = (135), \quad (26), \quad (34); \qquad h' = (124).$$

$$t = (56) \qquad \pi(u_1, t) = (135), \quad (24), \quad (56); \qquad h' = (456)$$

We have $u_1^{h'} = (135)^{(124)}$ (resp. $(135)^{(124)}$, $(135)^{(456)}$), so $u_1^{h'} = (235)$ (resp. (235), (136)) so in all cases $u_1^{h'} \in \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$. Also, $(46)^{(124)} = (16) \notin \Delta_{\mathrm{Aut}(L)}((12))$, $(26)^{(124)} = (46) \notin \Delta_{\mathrm{Aut}(L)}((34))$ and $(24)^{(456)} = (25) \notin \Delta_{\mathrm{Aut}(L)}((56))$. We get hypothesis (c).

Next let $u_2 = (1235)(46)$ if $t = (34)$ or (56), and let $u_2 = (1345)(26)$ if $t = (12)$. Finally, let $u_3 \in B_3$, be an element not inverted by v. We get hypothesis (b).

Suppose now that t is a product of 3 transpositions. If $t = (1i)(2j)(56)$, we take $u_1 = (1j5)$, $u_2 = (1i25)(j6)$ and $u_3 \in B_3$, while if $t = (12)(34)(56)$, we take $u_1 = (135)$, $u_2 = (1235)(46)$ and $u_3 \in B_3$. We get hypothesis (b).

SUBCASE 3: $L\langle t\rangle \cong \mathrm{PGL}(2, 9)$.

We note that $\Delta^{\leq 2}_{\mathrm{Aut}(L)}(t)$ centralizes one of the 11 involutions in $C_{\mathrm{Aut}(L)}(t) \cong D_{20}$ and hence $B_1 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(t) = \emptyset$, $\mid B_2 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(t) \mid = 10$ and $\mid B_3 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(t) \mid = 24$. Thus any $u_1 \in B_1$, such that $d_{\mathrm{Aut}(L)}(u_1, v) \geq 3$ will do. Next note that any two distinct elements $r, s \in B_2 \cap \Delta^{\leq 2}_{\mathrm{Aut}(L)}(t)$, satisfy $\langle r^2, s^2\rangle \cong D_{10}$. So one of $u_2 = (1235)(46)$ or $u_2 = (1236)(45)$ is at distance ≥ 3 from both v and t in $\Delta_{\mathrm{Aut}(L)}$. Finally, any element $u_3 \in B_3 \smallsetminus \Delta^{\leq 2}_{\mathrm{Aut}(L)}(t)$ which is not inverted by v, is at distance ≥ 3 from both v and t in $\Delta_{\mathrm{Aut}(L)}$. Hypothesis (b) holds in this case.

CASE 2: $v = (123)$.

If $t = (456)$ (or (465)), let $u_1^1 = (145)$. Then

$$\pi(u_1^1, t) = (145), \quad (23), \quad (456).$$

We take $h' = (126)$. Then $(u_1^1)^{h'} = (145)^{(126)} = (245) \in \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ and $(23)^{h'} = (23)^{(126)} = (36) \notin \Delta_{\mathrm{Aut}(L)}(456)$. We get hypothesis (c).

Next we let $u_1^2 = (124)(356)$, $u_2 = (2345)(16)$ and we take $u_3 \in B_3$, to get hypothesis (b).

If $t = (123)(456)$ take $u_1^1 = (145)$. Let $u_1^2 = (124)(356)$. Then

$$\pi(u_1^2, t) = (124)(356), \quad (15)(26)(34), \quad (123)(456).$$

We take $h' = (124)$. Then $(u_1^2)^{h'} = u_1^2 \in \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ and $((15)(26)(34))^{h'} = ((15)(26)(34))^{(124)} = (13)(25)(46) \notin \Delta_{\mathrm{Aut}(L)}(123)(456)$.

Next we let $u_2 = (3456)(12)$ and take $u_3 \in B_3$, to get hypothesis (b). The case when $t = (132)(465)$, $(123)(465)$ or $(132)(465)$ are handled similarly.

If $t = (45)$, let $u_1^1 = (346)$. Then

$$\pi(u_1^1, t) = (346), \quad (12), \quad (45).$$

We take $h' = (125)$. Then $(u_1^1)^{h'} = u_1^1$, and $(12)^{h'} = (12)^{(125)} = (25) \notin \Delta_{\mathrm{Aut}(L)}((45))$. We get hypothesis (c).

Next we let $u_1^2 = (124)(356)$, $u_2 = (2346)(15)$ and $u_3 \in B_3$, to get hypothesis (b). The cases $v = (46)$ or (56) are conjugate cases.

In cases 3 and 4 below, $C_{\mathrm{Aut}(L)}(v)$ contains an element interchanging B_1^1 and B_1^2 so we only need to establish the existence of u_1^1, u_2 and u_3. To simplify we denote $u_1 = u_1^1$.

Case 3: $v = (1234)(56)$.

Assume that $t = (56)$. Let $u_1 = (125)$. Then

$$\pi(u_1, t) = (125), \quad (34), \quad (56).$$

We take $h' = (356)$. Then $u_1^{h'} = (125)^{(356)} = (126) \in \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ and $(34)^{h'} = (34)^{(356)} = (45) \notin \Delta_{\mathrm{Aut}(L)}((56))$. We get hypothesis (c).

Next let $u_2 = (2346)(15)$ and $u_3 \in B_3$, to get hypothesis (b).

Assume that $t = (13)(24)$, then any u_i at distance ≥ 3, from t in $\Delta_{\mathrm{Aut}(L)}$, $1 \leq i \leq 3$, will give us hypothesis (b).

Case 4: $v = (12345)$.

Here t is the unique (outer) involution in $C_{\mathrm{Aut}(L)}(u)$. Take $u_1 \in B_1$ (any such u_1), $u_2 \in B_2$ such that u_2 is not centralized by one of the 5 involutions in $C_L(t) \cong \mathrm{D}_{10}$. Finally, take $u_3 \in B_3$ such that u_3 is not centralized by one of the 6 outer involutions in $C_{\mathrm{Aut}(L)}(t)$. Hypothesis (b) holds in this case. □

Lemma 7.3.4. *Let $L \cong PSL(3,4)$ and let B be the conjugacy class of elements of $\mathrm{Aut}(L)$ of order 7. Let $1 \neq w \in \mathrm{Aut}(L)$, then*

$$\delta(w) := |\{u \in B \mid d_{\mathrm{Aut}(L)}(u, w) \leq 2\}| < \frac{1}{2}|B|.$$

It follows that G has the property $(3\frac{1}{2})$.

Proof. By Corollary **??**, to show that G has the property $(3\frac{1}{2})$, it suffices to show that $\delta(w) < \frac{1}{2}|B|$, for all $1 \neq w \in \mathrm{Aut}(L)$, and that L contains at least five distinct $\mathrm{Aut}(L)$ classes. Since L contains the five $\mathrm{Aut}(L)$ classes $C_1, \cdots, C_5$ of elements of order $2, 3, 4, 5, 7$ respectively, it remains to show that $\delta(w) < \frac{1}{2}|B|$, for all $1 \neq w \in \mathrm{Aut}(L)$.

Note that we may assume that the order of w is a prime number. Let C be the conjugacy class of w in $\mathrm{Aut}(L)$. Let $u \in B$, and recall that $C_{\mathrm{Aut}(L)}(u) = \langle u \rangle \times S_u$, with $S_u \cong S_3$. Let $t \in S_u$ be an involution and let $r \in S_u$ be an element of order 3. Then $C_{\mathrm{Aut}(L)}(r) \cong 7 : 6 \times 3$ and $C_{\mathrm{Aut}(L)}(r) \cap C_{\mathrm{Aut}(L)}(t) \cong 7 : 6$. Since any element in $\Delta^{\leq 2}_{\mathrm{Aut}(L)}(u)$ centralizes some element of prime order in $C_{\mathrm{Aut}(L)}(u)$, we see that any element in $\Delta^{\leq 2}_{\mathrm{Aut}(L)}(u)$, whose order is a prime number either centralizes one of the 3 involutions in S_u or is an outer automorphism of L of order 3 and centralizes r. We use the notation of the ATLAS, pg. 24, for the conjugacy classes of elements in $\mathrm{Aut}(L)$.

If $C = 5A$, then $\delta(w) = 0$, so assume that $C \neq 5A$. The computations of $\delta(w)$ for $C = 3B$ or $3C$ are slightly different and will be postponed to the end of the proof. To compute $\delta(w)$

we count the number of pairs

$$\delta(C,B) := \{(u,w) \mid u \in B, w \in C \text{ and } d_{\mathrm{Aut}(L)}(u,v) \leq 2\},$$

in two ways. Let $t \in S_u$ be an involution and set $M = C_{\mathrm{Aut}(L)}(t) \cong L_3(2) : 2 \times 2$. As we noted, every $w \in C$ with $d_{\mathrm{Aut}(L)}(u,w) \leq 2$ centralizes one of the three involutions in S_u, hence we get that $\delta(C,B)$ is at most $3 \cdot |B| \cdot |M \cap C|$. On the other hand $\delta(C,B) = |C| \cdot \delta(w)$ so we see that

$$\delta(w) \leq 3 \cdot |B| \cdot \frac{|M \cap C|}{|C|}.$$

Hence we must show that

$$\frac{|M \cap C|}{|C|} < \frac{1}{6}.$$

Since the number $\frac{|M|}{|\mathrm{Aut}(L)|}$ appears many times in our calculations, we note that $\frac{|M|}{|\mathrm{Aut}(L)|} = \frac{1}{360}$. Table 1 summarizes our computation. We now explain our computations briefly, only in case we feel an explanation is needed. We note that the second column of the table gives the number of M-classes in $C \cap M$ and if it is more than one the third column gives the order of the possible centralizers.

C		$\lvert C_M(w)\rvert$	$\lvert C_{\mathrm{Aut}(L)}(w)\rvert$	$\frac{\lvert M\cap C\rvert}{\lvert C\rvert}$
2A	1	2^5	$2^8 \cdot 3$	$\frac{24}{360}$
3A	1	$2^2 \cdot 3$	$2^2 \cdot 3^3$	$\frac{9}{360}$
7A	1	14	42	$\frac{3}{360}$
2B	1	$2^3 \cdot 3$	$2^5 \cdot 3^3$	$\frac{36}{360}$
2C	2	$\lvert M\rvert, 2^5$	$2^5 \cdot 3 \cdot 7$	$\frac{1}{360} + \frac{21}{360} = \frac{22}{360}$
2D	1	24	240	$\frac{10}{360}$

Table 1

Notice that in the cases $C = 2B, 2D$, $C \cap M$ is contained in a subgroup of M isomorphic to $L_3(2) : 2$ and for $w \in C \cap M$, $w \notin L$. Hence $|C_M(w)| = |C_{M \cap L}(w)| \cdot 4 = 6 \cdot 4 = 24$. Also, for $C = 2C$, we have that $(C \cap M) \setminus \{t\}$ is contained in the subgroup $(M \cap L) \times \langle t \rangle$, so for $w \in (C \cap M) \setminus \{t\}$, we have $|C_M(w)| = 2^5$.

Next assume that $C = 3B$ or $3C$. We now must count the number of pairs $\delta(C,B)$ in a slightly different way. Given $u \in B$, we already saw that every $w \in C$ with $d_{\mathrm{Aut}(L)}(u,w) \leq 2$ centralizes the unique subgroup $\langle r \rangle$ of order 3 in $C_{\mathrm{Aut}(L)}(u)$. Now $C_{\mathrm{Aut}(L)}(r) \cong 7 : 6 \times 3$,

so there are $7 \cdot 6 + 2 = 44$ elements of order 3 in $C_{\mathrm{Aut}(L)}(r)$. Hence $\delta(C, B) \leq 44 \cdot |B|$ and also $\delta(C, B) = |C| \cdot \delta(w)$. So $\delta(w) \leq \frac{44}{|C|}|B|$ and we need to show that $\frac{44}{|C|} < \frac{1}{2}$. But $|C| \geq \frac{|\mathrm{Aut}(L)|}{60 \cdot 6} = \frac{2^8 \cdot 3^3 \cdot 5 \cdot 7}{2^3 \cdot 3^2 \cdot 5} = 2^5 \cdot 3 \cdot 7$, and hence $\frac{44}{|C|} < \frac{1}{2}$. □

Lemma 7.3.5. *Let $L \cong PSO^+(8, 2)$ and let B be the conjugacy class of elements of $\mathrm{Aut}(L)$ of order 7. Let C be any nonidentity conjugacy class of elements in $\mathrm{Aut}(L)$, and let $w \in C$. Then, $\delta(w) := |\{u \in B \mid d_{\mathrm{Aut}(L)}(u, w) \leq 2\}| \leq \frac{3}{10}|B|$, unless either C is the class of central involutions of $\mathrm{Aut}(L)$, or C is a class of outer automorphisms, in which case $\delta(w) \leq \frac{3}{5}|B|$. It follows that G has the property $(3\frac{1}{2})$.*

Proof. Let $C_1, \ldots, C_5 \subseteq L$ be any five distinct $\mathrm{Aut}(L)$ conjugacy classes such that C_i is not the class of central involutions, for all $1 \leq i \leq 5$. Notice that once we will prove the numerical bounds on $\delta(w)$, all the hypotheses of Corollary **??** will be satisfied and so by Corollary **??** it will follow that G has the property $(3\frac{1}{2})$.

The calculations here are very similar to those in the proof of Lemma **??**. Here also for $u \in B$, we have $C_{\mathrm{Aut}(L)}(u) = \langle u \rangle \times S_u$, with $S_u \cong S_3$. The same assertions made in **??** hold here so we may consider only conjugacy classes C such that the order of the elements in C is a prime number. Let $t \in S_u$ be an involution and let $r \in S_w$ be an element of order 3. Recall that $C_{\mathrm{Aut}(L)}(r) \cong G_2(2) \times 3$ and that $C_{\mathrm{Aut}(L)}(r) \cap C_{\mathrm{Aut}(L)}(t) \cong G_2(2)$. Again, as in the proof of Lemma **??**, any element in $\Delta^{\leq 2}_{\mathrm{Aut}(L)}(u)$, whose order is a prime number, either centralizes one of the 3 involutions in S_u or is an outer automorphism of L of order 3 and centralizes r. As in the proof of Lemma **??**, this fact will be used in the calculations below.

We use the notation of the ATLAS, pg. 86, for the conjugacy classes of elements in $\mathrm{Aut}(L)$. We start by dealing with classes C which are not outer automorphisms of order 3. Let $t \in S_u$ be an involution, and set $M = C_{\mathrm{Aut}(L)}(t) \cong PSp(6, 2) \times 2$. As in the proof of Lemma **??**, for $w \in C$, we have

$$\delta(w) \leq \frac{3 \cdot |M \cap C|}{|C|} \cdot |B|.$$

so we must compute $\frac{|M \cap C|}{|C|}$. As in the case of $PSL(3, 4)$ we have $\frac{|M|}{|\mathrm{Aut}(L)|} = \frac{1}{360}$.

Table 2 summarizes our computations. The 5-th column of Table 2 indicates to which class (or classes) of $PSp(6, 2)$, $C \cap M \cap L$ corresponds to. In the case of the outer automorphisms $\{2\mathrm{F}, 2\mathrm{G}\}$, the 5-th column indicates the class of the projection of the involution to $PSp(6, 2)$, in $PSp(6, 2) \times 2$.

The case $C = 2B$ is the same as $C = 2C$ or $C = 2D$. The case $C = 3A$ is the same as $C = 3B$ or $C = 3C$. The case $C = 5A$ is the same as $C = 5B$ or $C = 5C$.

Next assume that $C = 3F$ or $3G$. We now must count the number of pairs $\delta(C, B)$ in a slightly different way. Given $u \in B$, we already saw that every $w \in C$ with $d_{\mathrm{Aut}(L)}(u, w) \leq 2$ centralizes the unique subgroup $\langle r \rangle$ of order 3 in $C_{\mathrm{Aut}(L)}(u)$. Now $C_{\mathrm{Aut}(L)}(r) \cong G_2(2) \times 3$. We first count the outer 3-elements in this group. These have the form r or r^2 times an element of order 1 or 3 in $G_2(2)' \cong PSU(3, 3)$. This group has 28 Sylow 3 subgroups, each

C		$\lvert C_M(u)\rvert$	$\lvert C_{\mathrm{Aut}(L)}(u)\rvert$	$C \cap M \cap L$	$\frac{\lvert M\cap C\rvert}{\lvert C\rvert}$
2A	1	$2^{10}\cdot 3^2$	$2^{13}\cdot 3^4$	2B	$\frac{72}{360}$
2B	1	$2^{10}\cdot 3^2\cdot 5$	$2^{11}\cdot 3^2\cdot 5$	2A	$\frac{2}{360}$
2E	2	$2^{10}\cdot 3, 2^8\cdot 3$	$2^{11}\cdot 3^2$	2C, 2D	$\frac{6}{360}+\frac{24}{360}=\frac{30}{360}$
3A	1	$2^5\cdot 3^3\cdot 5$	$2^7\cdot 3^5\cdot 5$	3A	$\frac{36}{360}$
3D	1	$2^4\cdot 3^4$	$2^4\cdot 3^6$	3B	$\frac{9}{360}$
3E	1	$2^3\cdot 3^3$	$2^4\cdot 3^5$	3C	$\frac{18}{360}$
5A	1	$2^2\cdot 3\cdot 5$	$2^3\cdot 3\cdot 5^2$	5A	$\frac{10}{360}$
7A	1	14	42	7A	$\frac{3}{360}$
2F	2	$\lvert M\rvert$, $2^{10}\cdot 3^2\cdot 5$	$2\cdot\lvert PSp(6,2)\rvert$	1A, 2A	$\frac{1}{360}+\frac{63}{360}=\frac{64}{360}$
2G	3	$2^{10}\cdot 3^2$, $2^{10}\cdot 3$, $2^8\cdot 3$	$2^{10}\cdot 3^2$	2B, 2C, 2D	$\frac{1}{360}+\frac{3}{360}+\frac{12}{360}=\frac{16}{360}$

Table 2

of order 27. So $\delta(C,B)\le 28\cdot 27\cdot 2\cdot|B|$. Also $\delta(C,B)=|C|\cdot\delta(w)$, hence $\delta(w)\le\frac{28\cdot 27\cdot 2}{|C|}\cdot|B|$. It suffices to show $\frac{28\cdot 27\cdot 2}{|C|}<\frac{3}{5}$, which is easy. □

Lemma 7.3.6. *Let $L\cong PSL(2,27)$, then G has the property $(3\frac{1}{2})$.*

Proof. Let B be the $\mathrm{Aut}(L)$ class of elements of order 13. We show that $\delta(w):=|\{u\in B\mid d_{\mathrm{Aut}(L)}(u,w)\le 2\}|<\frac{1}{2}|B|$, for all $1\ne w\in\mathrm{Aut}(L)$. Since L contains the five distinct $\mathrm{Aut}(L)$ conjugacy classes $C_1,\dots,C_5$ of elements order 2, 3, 7, 13 and 14 respectively, Corollary **??** completes the proof.

Now given $u\in B$, we have $C_{\mathrm{Aut}(L)}(u)=\langle u\rangle\langle t\rangle$, where t is an outer involution in $\mathrm{Aut}(L)$. It follows that $\Delta^{\le 2}_{\mathrm{Aut}(L)}(u)=C_{\mathrm{Aut}(L)}(t)\smallsetminus\{1\}$. Next we have that $M:=C_{\mathrm{Aut}(L)}(t)\cong 26:6$. Let $1\ne w\in\mathrm{Aut}(L)$. The counting argument of Lemma **??** shows that to prove that $\delta(w)<\frac{1}{2}|B|$, it suffices to show that $\frac{|M\cap C|}{|C|}<\frac{1}{2}$, where C is the conjugacy class of w in $\mathrm{Aut}(L)$. This is an easy calculation using the ATLAS (where, of course, we may assume that the order of w is a prime number). □

Lemma 7.3.7. *Let $L\cong PSL(2,11)$ or $PSL(2,16)$. Then G has the property $(3\frac{1}{2})$.*

Proof. Again, as in the proof of Lemma **??**, it suffices to show that there exists a conjugacy class B of L such that $\delta(w):=|\{u\in B\mid d_{\mathrm{Aut}(L)}(u,w)\le 2\}|<\frac{1}{2}|B|$, for all $1\ne w\in\mathrm{Aut}(L)$;

and that L contains at least five $\mathrm{Aut}(L)$ classes. For $PSL(2,11)$, let B be the class of elements of order 11, and for $PSL(2,16)$, let B be the class of elements of order 17. Since in both cases, given $u \in B$, we have $C_{\mathrm{Aut}(L)}(u) = \langle u \rangle$, it is immediate that $\delta(w) < \frac{1}{2}|B|$, for all $1 \neq w \in \mathrm{Aut}(L)$. Also $L \cong PSL(2,11)$ has the $\mathrm{Aut}(L)$ classless of elements of order 2, 3, 5, 6 and 11 and $L \cong PSL(2,16)$ has the $\mathrm{Aut}(L)$ classes of elements of order 2, 3, 5, 15 and 17, so the proof of the lemma is complete. □

Lemma 7.3.8. *Assume $L \cong \mathrm{A}_5$, then G has the property $(3\frac{1}{2})$.*

Proof. Let $C_1, C_2, C_3 \subseteq L$ be the $\mathrm{Aut}(L)$ conjugacy classes of elements of order $3, 5, 2$, respectively. We show that L together with the classes $C_1, \ldots, C_3$ satisfy all the hypotheses (a), (b) and (c) of Lemma **??**.

Hypothesis (c): We must show that given $\mathcal{B}, \mathcal{C} \in \{C_1, C_2, C_3\}$, the pair $\mathcal{B}, \mathcal{C}$ satisfies hypothesis (c) of Lemma **??**. For that we use Lemma **??**. Given $\mathcal{C} \in \{C_1, \ldots, C_3\}$, $1 \neq v \in \mathcal{C}$ and $t \in C_{\mathrm{Aut}(L)}(v)$, we'll find $u_1 \in C_1$, $u_2 \in C_2$ and $u_3 \in C_3$, such that each $u' \in \{u_1, u_2, u_3\}$ satisfies the requirements in hypothesis (a), (b) or (c) of Lemma **??**. Then, by Lemma **??**, this will show that hypothesis (c) of Lemma **??** holds. If u' satisfies the requirements in hypothesis (c) of Lemma **??** we'll write $\pi(u', t)$ for the unique path in hypothesis (c), and we'll indicate an $h' \in L$ as required in hypothesis (c2). Note that we may assume without loss that the order of t is a prime.

When $\mathcal{C} = C_3$, we may assume without loss that $v = (12)(34)$. If

$$v = (12)(34) \quad \text{and} \quad t = (13)(24)$$

take $u_1 = (145)$, $u_2 \in C_2$ and $u_3 = (14)(25)$. The case $t = (14)(23)$ is a conjugate case. If

$$v = (12)(34) \quad \text{and} \quad t = (12)$$

take $u_1 = (235)$ and $u_2 \in C_2$. For $u_3 = (13)(25)$, we have

$$\pi(u_3, t) = (13)(25), \quad (12)(35), \quad (12).$$

Let $h' = (13)(24)$. Then $u_3^{h'} = (13)(25)^{(13)(24)} = (13)(45) \in \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ and $(12)(35)^{(13)(24)} = (15)(34) \notin \Delta_{\mathrm{Aut}(L)}((12))$. The case $t = (34)$ is a conjugate case.

When $\mathcal{C} = C_1$, we may assume that

$$v = (123) \quad \text{and} \quad t = (45)$$

We take $u_1 = (234)$ and $u_2 \in C_2$. For $u_3 = (14)(25)$, we have

$$\pi(u_3, t) = (14)(25), \quad (12)(45), \quad (45).$$

Let $h' = (245)$. Then $u_3^{h'} = (14)(25)^{(245)} = (15)(24) \in \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v)$ and $(12)(45)^{h'} = (12)(45)^{(245)} = (14)(25) \notin \Delta_{\mathrm{Aut}(L)}((45))$. Finally hypothesis (a) of Lemma **??** clearly holds when $\mathcal{C} = C_2$, for any $\mathcal{B} \in \{C_1, C_2, C_3\}$.

Hypotheses (a) and (b): First we note that to show hypotheses (a) and (b) of Lemma **??**, it is enough to show that they hold for *some* $v_1 \in C_1$ and *some* $v_2 \in C_2$. We thus start

by picking

$$v_1 = (123) \qquad \text{and} \qquad v_2 = (12345).$$

We now list the orbit representatives of $C_{\mathrm{Aut}(L)}(v_l)$ on $C_j \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v_t)$, $l = 1, 2$ and $1 \leq j \leq 3$. We have $C_{\mathrm{Aut}(L)}(v_1) = \langle (123) \rangle \times \langle (45) \rangle$, and the orbit representatives are,

$$\{(124), (142), (145)\} \qquad \{(12345), (12435), (13245), (13425)\} \qquad \{(12)(34), (14)(25)\}.$$

We have $C_{\mathrm{Aut}(L)}(v_2) = \langle (12345) \rangle$, and the orbit representatives are,

$$\{(123), (132), (124), (142)\} \qquad \{(12354), (12453), (12543), (13254)\} \qquad \{(12)(34), (13)(24)\}.$$

We now show that hypothesis (b) of Lemma **??** holds for all possible choices of j and u.

We start with $v = v_1$. For $j = 1$, let $u \in C_1$ and let $h_1, h_2 \in L$ such that $u^{h_1} = (124)$ and $u^{h_2} = (142)$. Then $d_{\mathrm{Aut}(L)}(u^{h_i}, v_1) > 3$, for $i = 1, 2$, so for any orbit $\mathcal{O}$ of $C_{\mathrm{Aut}(L)}(v_1)$ on $C_1 \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v_1)$, either $h = h_1$ or $h = h_2$ will satisfy all the requirements of hypothesis (b). Similarly, for $j = 2$, it is enough to note that $d_{\mathrm{Aut}(L)}(w, v_1) = \infty$, for all $w \in C_2$, and that for $u \in C_2$, u^L meets at least two of the orbits of $C_{\mathrm{Aut}(L)}(v_1)$ on $C_2 \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v_1)$.

Suppose $j = 3$. Let $\mathcal{O}$ be an orbit of $C_{\mathrm{Aut}(L)}(v_1)$ on $C_3 \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v_1)$. Let $u \in C_3$ be an involution. Let $s \in \Delta_{\mathrm{Aut}(L)}(u)$ and let $t \in \Delta_{\mathrm{Aut}(L)}(v_1)$. Suppose $(12)(34) \in \mathcal{O}$ and let $q \in L$, with $u^q = (14)(25)$. If $t \neq (45)$, or $s^q \neq (12)(45)$, then $[s^q, t] \neq 1$, so taking $h = q$, we see that hypothesis (b) holds. Thus $t = (45)$ and $s^q = (12)(45)$. Let $h = q(245)$. Then $u^h = (14)(25)^{(245)} = (15)(24) = (14)(25)^{(45)} \notin \mathcal{O}$, and $s^h = (12)(45)^{(245)} = (14)(25)$, so $[s^h, t] \neq 1$ and again hypothesis (b) holds. Next suppose that $(14)(25) \in \mathcal{O}$. Let $q \in L$, with $u^q = (12)(34)$. If $t \neq (45)$, or $s^q \neq (12)$, then $[s^q, t] \neq 1$, so taking $h = q$, we see that hypothesis (b) holds. Thus $t = (45)$ and $s^q = (12)$. Let $h = q(13)(24)$. Then $u^h = (12)(34) \notin \mathcal{O}$, and $s^h = (34)$, so $[s^h, t] \neq 1$ and again hypothesis (b) holds.

Suppose now that $v = v_2$. Note that for all $1 \leq j \leq 3$ and all $w \in \Delta^{>1}(v_2)$, $d_{\mathrm{Aut}(L)}(w, v_2) = \infty$. It follows that given $u \in C_1 \cup C_2 \cup C_3$, to show that hypothesis (b) holds, it suffices to show that u^L meets at least 2 orbits of $C_{\mathrm{Aut}(L)}(v_2)$ on $C_j \cap \Delta^{\geq 3}_{\mathrm{Aut}(L)}(v_2)$ and this is easy. □

References

[Am] S. Amitsur *Finite subgroups of division rings,* Trans. AMS, **80**(1955), 361-386.

[AsSei] M. Aschbacher, G.M. Seitz, *Involutions in Chevalley groups over fields of even order*, Nagoya Math. J. **63**(1976), 1–91.

[Atlas] J.H. Conway et al, *Atlas of finite groups*, Clarendon Press, Oxford 1985.

[Be] H. Behr, *Arithmetic groups over function fields. I. A complete characterization of finitely generated and finitely presented arithmetic subgroups of reductive algebraic groups,* J. Reine Angew. Math., **495**(1998), 79-118.

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

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

[C] R.W. Carter, *Conjugacy classes in the Weyl group*, Compositio Math. **25**(1972), 1–59.

[C1] _____ *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, Wiley-Interscience, 1985.

[L] S. Lang, *Algebra,* Addison-Wesley, 1965.
[LaLiSei] R. Lawther, M.W. Liebeck, G.M. Seitz, *Fixed point ratios in actions of finite exceptional groups of Lie type*, to appear.
[LiSei] M.W. Liebeck, G. M. Seitz, *Reductive Subgroups of Exceptional Algebraic Groups*, Memoirs, AMS, **580**(1996), 1–111.
[Mar] G.A. Margulis, *Finiteness of quotients of discrete groups,* Funct. Analysis and Appl., **13**(1979), 178-187.
[Pi] R. Pierce, *Associative Algebras,* GTM **88**, Springer, 1982.
[PR] V.P. Platonov, A.S. Rapinchuk, *Algebraic Groups and Number Theory,* "Pure and Applied Mathematics" series, N 139, Academic Press, 1993.
[PR1] ——— *The multiplicative structure of division algebras over number fields and the Hasse norm principle,* Proc. Steklov Inst. Math. **165**(1985), 187-205.
[Pr] G. Prasad, *Strong approximation for semi-simple groups over function fields,* Ann. Math., **105**(1977), 553-572.
[Ra] M.S. Raghunathan, *On the group of norm 1 elements in a division algebra,* Math. Ann., **279**(1988), 457-484.
[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.
[RS] A. S. Rapinchuk, Y. Segev *Valuation-like maps and the congruence subgroup property*, to appear in Invent. Math.
[RoS1] 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.
[RoS2] ——— *The multiplicative group of a division algebra of degree 5 and Wedderburn's Factorization Theorem*, Contemp. Math. **259**(2000), 475–486.
[S1] Y. Segev *On finite homomorphic images of the multiplicative group of a division algebra*, Ann. Math. 149 (1999), 219-251.
[S2] ——— *Some applications of Wedderburn's factorization theorem,* Bull. Austral. Math. Soc., **59**(1999), 105-110.
[S3] ——— *The commuting graph of minimal nonsolvable groups*, to appear in Geom. Ded.
[SSei] Y. Segev, G. Seitz, *Anisotropic groups of type A_n and the commuting graph of finite simple groups,* to appear in Pacific J. Math.
[Ser] A. Seress, *Trivial set-stabilizers in finite permutation groups*, J. LMS (2), **53**(1996), no. 2, 243-255.
[SpSt] T.A. Springer, R. Steinberg, *Conjugacy Classes*, Springer Lecture Notes 131 (eds: A. Borel, et al), Springer, Berlin, 1970.
[St] R. Steinberg, *Lectures on Chevalley Groups*, Yale University Lecture Notes, 1967.
[Ti1] J. Tits, *Algebraic and abstract simple groups,* Ann. Math., **80**(1964), no. 2, 313-329.
[Ti2] ——— *Groupes de Whitehead de groupes algebriques simples sur un corps (d'apres V.P. Platonov et al.),* Sem. Bourbaki, 1977, exp. 505. Lecture Notes in Math., **677**(1978), 218-236.
[Tu] G. Turnwald, *Multiplicative subgroups of finite index in rings,* Proc. AMS **120**(1994), 377-381.
[W] A.R. Wadsworth, *Extending valuations to finite-dimensional division algebras,* Proc. AMS, **98**(1986), 20-22.

Andrei S. Rapinchuk, Department of Mathematics, University of Virginia, Charlottesville, Virginia 22904, USA

E-mail address: asr3x@weyl.math.virginia.edu

Yoav Segev, Department of Mathematics, Ben-Gurion University, Beer-Sheva 84105, Israel

E-mail address: yoavs@math.bgu.ac.il

Gary M. Seitz, Department of Mathematics, University of Oregon, Eugene OR 97403-1226, USA

E-mail address: seitz@math.uoregon.edu