J. Eur. Math. Soc. 25, 3325–3358 (2023) DOI 10.4171/JEMS/1255

Dan Segal · Katrin Tent

Defining R and $G(R)$

Received May 11, 2020

Abstract. We show that for Chevalley groups $G(R)$ of rank at least 2 over an integral domain R each root subgroup is (essentially) the double centralizer of a corresponding root element. In many cases, this implies that R and $G(R)$ are bi-interpretable, yielding a new approach to bi-interpretability for algebraic groups over a wide range of rings and fields.

For such groups it then follows that the group $G(R)$ is (finitely) axiomatizable in the appropriate class of groups provided R is (finitely) axiomatizable in the corresponding class of rings.

Keywords. Chevalley groups, bi-interpretation

1. Introduction

A Chevalley–Demazure group scheme G assigns to each commutative ring R a group $G(R)$. If R is an integral domain with field of fractions k, one can realize $G(R)$ as the group of R-points of $G(k)$, where $G(k)$ is taken in a given matrix representation (see e.g. [1, §1]). Group-theoretic properties of $G(R)$ tend to reflect ring-theoretic properties of R. In this paper we consider properties that are expressible in first-order language; specifically, we establish sufficient conditions for $G(R)$ to be *bi-interpretable* with R. This is a slightly subtle concept, defined in [29, Def. 3.1] (cf. [20, Chapter 5]); see §3 below. A bi-interpretation sets up a bijective correspondence between first-order properties of the group and first-order properties of the ring. Results of this nature for R a field go back to Mal'tsev [24] and Zilber [40].

Theorem 1.1. *Let G be a simple adjoint Chevalley–Demazure group scheme of rank at least* 2*, and let R be an integral domain. Then R and $G(R)$ are bi-interpretable, assuming in case G is of type E_6, E_7, E_8, or F_4 that R has at least two units.*

Dan Segal (corresponding author): All Souls College, Oxford OX1 4AL, GB;
segal@maths.ox.ac.uk

Katrin Tent: Fachbereich Mathematik und Informatik, Westfälische Wilhelms-Universität Münster, Einsteinstrasse 62, 48149 Münster, Germany; tent@wwu.de

Mathematics Subject Classification (2020): Primary 20G35; Secondary 03C60

For convenience, we will refer to the final assumption as ‘the units condition’; it is automatically satisfied when $\mathrm{char}(R) \neq 2$. The condition is used in the proof, but may not be essential.

Throughout the paper, G will denote a simple Chevalley–Demazure group scheme defined by a root system Φ of rank at least 2, and R will be a commutative integral domain. The group scheme G is *not assumed to be adjoint*; indeed, the proof yields the same result without this assumption, under the alternative condition that $G(R)$ have *finite elementary width*: that is, there exists $N \in \mathbb{N}$ such that every element of $G(R)$ is equal to a product of N elementary root elements $x_\alpha(r)$, $\alpha \in \Phi$, $r \in R$. (When referring below to Theorem 1.1, we will mean both versions of the result.)

In particular, we have (see §5):

Corollary 1.2. *The – not necessarily adjoint – group $G(R)$ is bi-interpretable with R in each of the following cases:*

(i) *R is a field;*

(ii) *G is simply connected, and R is* (1) *a local domain,* (2) *the ring of S-integers in a number field k with respect to a finite set S of places of k, or* (3) *the ring of integers in a global function field.*

For related results (in some ways less general, in some ways more) see [26], [11] and [6].

These results have consequences related to ‘first-order rigidity’. A group (or ring) X is *first-order rigid* (or *relatively axiomatizable*) *in a class* $\mathcal{C}$ if any member of $\mathcal{C}$ elementarily equivalent to X is isomorphic to X. For example, Avni, Lubotzky and Meiri [5] prove that all higher-rank non-uniform arithmetic groups are first-order rigid in the class of f.g. groups.

A stronger condition is relative *finite axiomatizability*, or *FA*: X is FA in $\mathcal{C}$ if there is a first-order sentence such that X is the unique member of $\mathcal{C}$ (up to isomorphism) that satisfies this sentence. When $\mathcal{C}$ is the class of finitely generated groups, resp. rings, the latter property is often called *QFA*, or quasi-finitely axiomatizable; see [3, 27], and for recent variations on this theme [28]. (This should not be confused with the notion of quasi-finite axiomatizability used in model theory; see e.g. [29, Chapter 3], [2].)

Suppose that $G(R)$ is bi-interpretable with R. Then $G(R)$ is first-order rigid, resp. FA in $\mathcal{C}$ if and only if R has this property relative to $\mathcal{C}'$, provided the ‘reference classes’ $\mathcal{C}$ and $\mathcal{C}'$ are suitably chosen. In particular, in §4 we establish

Corollary 1.3. *Assume that G and R satisfy the hypotheses of Theorem 1.1. If R is first-order rigid, resp. FA, in* (a) *the class of finitely generated rings,* (b) *the class of profinite rings,* (c) *the class of locally compact* (*or t.d.l.c.*) *topological rings, then $G(R)$ has the analogous property in* (a) *the class of finitely generated groups,* (b) *the class of profinite groups,* (c) *the class of locally compact* (*or t.d.l.c.*) *topological groups.*

In most cases the converse of this corollary is also valid; see §4.

It is important to note that in cases (b) and (c), the first-order axioms can *a priori* only determine the group up to isomorphism *as an abstract group* (cf. [28, §1.2]); in most of the cases under consideration, this is sufficient to determine the group as a topological group; see Proposition 4.4.

In §5 we deduce

Corollary 1.4. (i) *Let R be an integral domain. If G is adjoint and the group $G(R)$ is finitely generated then $G(R)$ is FA among f.g. groups, assuming that the units condition holds.*

(ii) *Let $\mathfrak{o}_S$ be the ring of S-integers in a global field ($S \supseteq S_\infty$, with $S = S_\infty$ in the function-field case). If G is adjoint or simply connected then the S-arithmetic group $G(\mathfrak{o}_S)$ is FA among f.g. groups.*

(iii) *If G is adjoint or simply connected and R is one of the complete local rings $\mathbb{F}_q[[t_1,\dots,t_n]]$, $\mathfrak{o}_q[[t_1,\dots,t_n]]$ ($n \geq 0$) then $G(R)$ is FA in the class of profinite groups.*

(iv) *If k is a local field then $G(k)$ is FA in the class of locally compact groups.*

(Here $\mathfrak{o}_q = \mathbb{Z}_p[\zeta]$, where $q = p^f$ and ζ is a primitive $(q-1)$th root of unity). For the fact that the S-arithmetic groups in (ii) are indeed finitely generated see [8, 9].)

Our final result moves away from integral domains. The model theory of adèle rings and some of their subrings has attracted some recent interest [14, 16, 17], and it seems worthwhile to extend the results in that direction.

Let $\mathbb{A}$ denote the adèle ring of a global field K, with $\mathrm{char}(K) \neq 2, 3, 5$. We consider subrings of $\mathbb{A}$ of the following kind:

$$A = \mathbb{A}, \quad A = \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{o}_{\mathfrak{p}} \tag{1}$$

where $\mathfrak{o}$ is the ring of integers of K and $\mathcal{P}$ may be any non-empty set of primes (or places) of K. For example, A could be the whole adèle ring of $\mathbb{Q}$, or $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

Theorem 1.5. *Let G be a simple Chevalley–Demazure group scheme of rank at least 2, or else one of the groups SL_2, $\mathrm{SL}_2/\langle -1\rangle$, PSL_2. Let A be as in (1). Then A is bi-interpretable with the group $G(A)$.*

When $|\mathcal{P}| = 1$, this is included in Theorem 1.1 for groups of higher rank, and is established in [28, §4] for groups of type SL_2.

The main point of the paper is to show how results like Theorem 1.1 may be deduced from the fact that *root subgroups are definable*. This in turn is a (relatively straightforward) consequence of our main structural result.

The root subgroup of G associated to a root α is denoted U_α. It seems to be part of the folklore that for a field k, the subgroup $U_\alpha(k)$ is equal to its own double centralizer in $G(k)$. We will need a more general version of this; as we could not find a reference, and the result for some rings is perhaps somewhat unexpected, we will present three different approaches to the proof, each applicable to a slightly different range of cases.

Theorem 1.6. *Assume that R satisfies the units condition. Let U be a root subgroup of G and let $1 \neq u \in U(R)$. Write Z for the centre of G. Then*

$$\mathrm{C}_{G(R)}\mathrm{C}_{G(R)}(u) = \mathrm{Z}(\mathrm{C}_{G(R)}(u)) = U(R)Z(R) \tag{2}$$

unless G is of type C_n (including $B_2 = C_2$), U belongs to a short root α and $R^* = \{\pm 1\}$, in which case

$$\mathrm{Z}(\mathrm{C}_{G(R)}(u)) \leq U(R)U_1(R)U_2(R)Z(R) \tag{3}$$

where U_1 and U_2 are root subgroups belonging to long roots adjacent to α in a B_2 subsystem.

In the exceptional case, $\mathrm{Z}(\mathrm{C}_{G(R)}(u))$ actually turns out to be two-dimensional: the precise description is given in §8.

If one assumes that R has at least four units, the theorem can be proved very quickly, and we do this in §2 below. Remaining cases are dealt with in §§6, 7 and 8; these can be skipped by the reader unconcerned with 'difficult' rings such as $\mathbb{Z}$.

As for definability, we shall deduce

Corollary 1.7. *Assuming the units condition, for each root α the root subgroup $U_\alpha(R)$ is definable, unless possibly $G = \mathrm{Sp}_4(R)$, $\mathrm{char}(R) = 0$ and $R/2R$ is infinite; in any case $U_\alpha(R)Z(R)$ is definable.*

Definable here means 'definable with parameters': a subset H in a group Γ is *definable* if there are a first-order formula φ and elements $g_1, \dots, g_m \in \Gamma$ such that

$$H = \{h \in \Gamma \mid \varphi(h, g_1, \dots, g_m) \text{ holds}\}.$$

This is good enough for the proof of Theorem 1.1, which appears in §3.

Remark. Essentially the same proof establishes Corollary 1.7 whenever G is a k-isotropic algebraic group with the maximal k-torus defined over R, provided R has at least four units. Whether the other results can be extended in this direction remains to be seen (cf. [5, 6, 21]).

Regarding Chevalley groups of rank 1. It is easy to verify both Theorem 1.6 and Corollary 1.7 for groups G of type A_1.

It is shown in [28, §4] that $\mathrm{SL}_2(R)$ is bi-interpretable with R if R is a profinite local domain; thus Corollary 1.4(iii) holds also for $G = \mathrm{SL}_2$.

We do not know if the other cases hold for SL_2. It seems extremely unlikely that $\mathrm{SL}_2(\mathbb{Z})$ can be FA or even first-order rigid, as it is virtually free; results of Sela [30, 31] concerning free products imply that $\mathrm{PSL}_2(\mathbb{Z})$ is not first-order rigid, and so not bi-interpretable with $\mathbb{Z}$.

In the proofs we have frequent recourse to the Chevalley commutator formula, summarized for convenience in the Appendix.

2. Double centralizers and definability of root groups

Following [1] we denote by T the distinguished maximal torus of G determined by Φ. Let N denote the normalizer of T in G, so that the Weyl is group $W = N/T$. We will sometimes use the fact that W permutes the root subgroups, and acts transitively on the set of short roots and on the set of long roots. Each $w \in W$ has a coset representative $n_w \in N(R)$ (in fact, in the subgroup generated by root elements of the form $x_a(\pm 1)$) [12, §7.2 and Lemma 6.4.4]. Thus all long (resp. short) root subgroups are conjugate in $G(R)$.

The field of fractions of R will be denoted k, and its algebraic closure $\overline{k}$. Sometimes we identify G with $G(\overline{k})$. We write $\pi : G \to G/Z$ for the quotient map.

We begin by clarifying the relation between the R-points of the algebraic group U_α and the 1-parameter group $x_\alpha(R)$; this is the link between Corollary 1.7 and the main theorems.

Lemma 2.1. *Let $U = U_\alpha$ be a root subgroup. Then*

$$U \cap G(R) = U(R) = x_\alpha(R), \tag{4}$$

$$UZ \cap G(R) = U(R)Z(R). \tag{5}$$

Proof. (4): If R is a PID, or more generally an intersection of PIDs such as a Dedekind ring, this follows from [34, Lemma 49 (b)]. In the general case, it is a consequence of the fact that the morphism x_α from the additive group scheme to G is a closed immersion ([13, Thm. 4.1.4]; [15, exp. XX, remark following Cor. 5.9]).

(5): Say $g = x_\alpha(\xi)z \in G(R)$ where $\xi \in \overline{k}$ and $z \in Z$. Then

$$x_\alpha(\xi)\pi = g\pi \in G(R)\pi \subseteq (G/Z)(R),$$

whence $\xi \in R$ by (4) applied to the group scheme G/Z. Thus $x_\alpha(\xi) \in U(R)$ and so $z \in Z(R)$. ■

The main step in the proof of Theorem 1.6 is

Lemma 2.2. *Assume that if G is of type E_n or F_4 then $R^* \neq 1$, and if G is of type C_n then $R^* \neq \{\pm 1\}$. Then there exists a finite set $Y \subseteq \mathrm{C}_{G(R)}(U)$ such that $\mathrm{C}_G(Y) \subseteq UZ$.*

To deduce the main case of the theorem, observe that Z is contained in

$$V := \mathrm{C}_G(\mathrm{C}_G(u)) \leq \mathrm{C}_G(\mathrm{C}_{G(R)}(u)) \leq \mathrm{C}_G(Y) \leq UZ.$$

Thus if V has positive dimension we have equality throughout. This is obvious if $\mathrm{char}(k) = 0$; if G is of classical type, it is easy to see in a matrix representation that $V \geq U$ (cf. §8). In all other cases, the results of [22, 32, 33] show that $\dim(V) = 1$. Now (2) follows by (5). The proof of Theorem 1.5 for groups of type C_n is completed in §8.

The slickest proof of Lemma 2.2 uses what we call ‘torus witnesses’. Let α and β be linearly independent roots. A *torus witness* for (α, β) is an element $s \in T(R)$ that centralizes U_α and acts effectively on U_β:

$$s \in \mathrm{C}_{T(R)}(U_\alpha), \quad \mathrm{C}_{U_\beta}(s) = 1.$$

Note that s centralizes, respectively acts effectively on, a root group U_γ if and only if it does the same to $U_\gamma(R)$.

In most cases we can use ‘elementary torus elements’ $h_\gamma(t) \in T(R)$, defined by

$$h_\gamma(t) = x_\gamma(t)x_{-\gamma}(-t^{-1})x_\gamma(t) \cdot x_\gamma(1)x_{-\gamma}(-1)x_\gamma(1)$$

([34, Lemma 20], [12, Lemma 6.4.4]). Now $h_\gamma(t)$ acts on U_β by

$$x_\beta(r)^{h_\gamma(t)} = x_\beta(t^{-A_{\gamma\beta}}r)$$

where

$$A_{\gamma\beta} = \frac{2(\gamma, \beta)}{(\gamma, \gamma)} \in \{0, \pm 1, \pm 2, \pm 3\}$$

(see [12, p. 194]).

We first deal with the case where R contains at least four units:

Proposition 2.3. *Assume that $|R^*| \geq 4$. Then for each pair (α, β) of linearly independent roots there is a torus witness $s_{\alpha,\beta}$.*

Proof. Let $r \in R^*$ be such that $r^2 \neq 1 \neq r^3$. If β is orthogonal to α, then we put $s_{\alpha,\beta} = h_\beta(r)$. Now suppose α and β are non-orthogonal. If α and β span a diagram of type A_2, then there is a root $\gamma \neq \pm\alpha, -\beta$ such that $(\alpha, \beta) \neq (\alpha, \gamma)$. In this case, the actions of $h_\beta(r)$ and $h_\gamma(r)$ on U_α are inverse to each other and so $s_{\alpha,\beta} = h_\beta(r)h_\gamma(r)$ is as required. If α, β span a diagram of type B_2 or G_2, there is a root γ orthogonal to α and non-orthogonal to β and we put $s_{\alpha,\beta} = h_\gamma(r)$. ■

Other cases will be considered later.

Proposition 2.4. *Let α be a positive root. Suppose that for every positive root $\beta \neq \alpha$ there exists a torus witness s_β for (α, β). Set $Y = \{s_\beta \mid \beta \in \Phi_+\}$. Then*

$$\mathrm{C}_G(Y) \leq U_\alpha Z.$$

Proof. We recall the Bruhat decomposition ([12, Thm. 8.4.3], [34, p. 21]). Order the positive roots as $\alpha_1, \ldots, \alpha_m$ and write $U_i = U_{\alpha_i}$. For $w \in W$ put

$$S(w) = \{i \mid w(\alpha_i) \in \Phi_-\}$$

where Φ_- is the set of negative roots. Then each element of G can be written uniquely in the form

$$g = u_1 \ldots u_m \cdot tn_w \cdot v_1 \ldots v_m \tag{6}$$

where $w \in W, t \in T, u_i, v_i \in U_i$ and $v_i = 1$ unless $i \in S(w)$.

We may suppose that $\alpha = \alpha_1$. For each $i \geq 2$ there is a torus witness $s_i \in Y$ for (α_1, α_i). Now let $g \in \mathrm{C}_G(Y)$, and write g in the form (6). Then for each $j \geq 2$ we have

$$g = g^{s_j} = u_1^{s_j} \dots u_m^{s_j} \cdot tn_w^{s_j} \cdot v_1^{s_j} \dots v_m^{s_j}.$$

Now s_j fixes u_1 and v_1, and moves each non-identity element of U_j; it also normalizes N and each U_i. It follows by the uniqueness of expression that $u_j = v_j = 1$. This holds for each $j \geq 2$, and we conclude that

$$g = u_1 tn_w v_1.$$

As $tn_w = v_1^{-1} g u_1^{-1}$ fixes $u \in U_\alpha$, but conjugates U_α to $U_{w(\alpha)}$, it follows that $w(\alpha) = \alpha$; in particular, $1 \notin S(w)$, and so $v_1 = 1$.

It remains only to prove that $tn_w \in Z = \mathrm{Z}(G)$. Let γ be a root. If $\alpha + \gamma \notin \Phi$ then $U_\gamma \leq \mathrm{C}_G(U_\alpha)$. If $\alpha + \gamma$ and $\alpha - \gamma$ are both roots then either $2\alpha + \gamma \notin \Phi$ or $2\alpha - \gamma \notin \Phi$, and then $U_{\alpha \pm \gamma} \leq \mathrm{C}_G(U_\alpha)$. It follows that tn_w centralizes at least one of

$$U_\gamma,\ U_{-\gamma},\ U_{\alpha \pm \gamma}.$$

As $w(\alpha) = \alpha$ this implies that $w(\gamma) = \gamma$, and as γ was arbitrary it follows that $w = 1$. Thus $tn_w = t \in T$, and acts on root subgroups in the following manner:

$$x_\gamma(\xi)^t = x_\gamma(\chi(\gamma)\xi)$$

for a certain character χ. Now χ is trivial on α and on one of $\gamma, -\gamma, \alpha + \gamma, \alpha - \gamma$ so it is trivial on all of them. Thus t acts trivially on every root subgroup, and so $t \in \mathrm{Z}(G)$ as required. ■

The 'generic case' of Theorem 1.6, where $|R^*| \geq 4$, is now completely established.

For the remainder of this section, we will take as given the conclusion of this theorem (in its general form), and show that it implies Corollary 1.7.

Fix a root α, set $U = U_\alpha$ and fix $u \in U$, $u \neq 1$. We begin with

Lemma 2.5. *$U(R)Z(R)$ is a definable subgroup of $G(R)$.*

Proof. It is clear that the double centralizer of an element u is definable, taking u as a parameter. So if U satisfies (2) we are done.

Otherwise, (3) holds, $\Phi = C_n$ and α is a short root. Set $V = \mathrm{Z}(\mathrm{C}_{G(R)}(u))$. Thus

$$U(R)Z(R) \leq V \leq U_{-\beta}(R)U(R)U_{2\alpha+\beta}(R)Z(R)$$

where α, β make a pair of fundamental roots in a B_2 subsystem of Φ.

Let $g = x_{-\beta}(r)x_\alpha(s)x_{2\alpha+\beta}(t)z \in V$ where $z \in Z$. The commutation relations give

$$[g, x_{\alpha+\beta}(1)] = x_\alpha(\pm r)x_{2\alpha+\beta}(\pm r)x_{2\alpha+\beta}(\pm 2s),$$
$$[g, x_{-\alpha-\beta}(1)] = x_{-\beta}(\pm 2s)x_\alpha(\pm t)x_{-\beta}(\pm t).$$

Now g lies in $U(R)Z(R)$ if and only if $r = t = 0$, which holds if and only if

$$[g, x_{\alpha+\beta}(1)] \in U_{2\alpha+\beta}(R)Z(R) \quad \text{and} \quad [g, x_{-\alpha-\beta}(1)] \in U_{-\beta}(R)Z(R).$$

As $2\alpha + \beta$ and $-\beta$ are long roots, each of the two groups on the right is definable, as is V. Hence $U(R)Z(R)$ is definable in this case too. ■

Now we can complete the

Proof of Corollary 1.7. If G is adjoint then $Z = 1$ and $U(R) = U(R)Z(R)$ is definable, by Lemma 2.5. This holds in particular when $\Phi = G_2$ [34, p. 23].

If Φ is not of type A_n, D_{2m+1} or E_6 we have $Z^2 = 1$ (*loc. cit.*), so in all these cases we have

$$U(2R) = (U(R)Z(R))^2,$$

which is definable. If also $R/2R$ is finite, then $U(R)$ is the union of finitely many cosets of $U(2R)$, and so definable with the help of a few parameters. If $\Phi = B_2$ then either G is adjoint or $G \cong \mathrm{Sp}_4$. If the characteristic of R is odd then $2R = R$. If $\mathrm{char}(R) = 2$ and $Z^2 = 1$ then $Z = 1$, and there is nothing to prove. The case where $\mathrm{char}(R) = 0$, $R/2R$ is infinite and $G \cong \mathrm{Sp}_4$ is the special case in the statement of the corollary. Thus we may assume that $\Phi \notin \{G_2, B_2\}$.

Now we separate cases. Note that if $U_\beta(R)$ is definable for some root γ, then so is $U_\gamma(R)$ for every root γ of the same length as β, as these subgroups are all conjugate in $G(R)$. This will be used repeatedly without special mention.

Case 1: There is a root β such that α and β make a pair of fundamental roots in a subsystem of type A_2. Now the commutator formula shows that

$$U_{\alpha+\beta}(R) = [U_\alpha(R)Z(R), x_\beta(1)],$$

so $U_{\alpha+\beta}(R)$ is definable; and $\alpha + \beta$ has the same length as α.

Case 2: There is no such β. Then there exist roots β and γ such that α, β, γ form a fundamental system of type B_3 or C_3, with β in the middle and of the same length as γ. Moreover, $U_\beta(R)$ is definable by Case 1.

Now if α is short and β is long, then $2\alpha + \beta$ is a long root, so $U_{2\alpha+\beta}(R)$ is definable. The formula

$$[x_\alpha(1), x_\beta(r)z] = x_{\alpha+\beta}(\pm r)x_{2\alpha+\beta}(\pm r) \quad (z \in Z)$$

shows that if $g \in U_{\alpha+\beta}(R)$ then there exist $v \in U_\beta(R)Z(R)$ and $w \in U_{2\alpha+\beta}(R)$ such that $gw^{-1} = [x_\alpha(1), v]$. As

$$U_{\alpha+\beta}U_{2\alpha+\beta} \cap U_{\alpha+\beta}Z = U_{\alpha+\beta}$$

it follows that $g \in U_{\alpha+\beta}(R)$ if and only if $g \in U_{\alpha+\beta}(R)Z(R)$ and there exist v, w as above satisfying $gw^{-1} = [x_\alpha(1), v]$. Thus $U_{\alpha+\beta}(R)$ is definable; as $\alpha + \beta$ is short the result follows for $U_\alpha(R)$.

Suppose finally that α is long and β is short. The preceding argument, swapping the roles of α and β, shows that $g \in U_{2\beta+\alpha}(R)$ if and only if $g \in U_{2\beta+\alpha}(R)Z(R)$ and there exist $v \in U_\alpha(R)Z(R)$ and $w \in U_{\beta+\alpha}(R)$ such that $gw^{-1} = [x_\alpha(1), v]$. Also $U_{\beta+\alpha}(R)$ is definable becaue $\beta + \alpha$ is short like β, and so $U_{2\beta+\alpha}(R)$ is definable. This finishes the proof as $2\beta + \alpha$ is long like α.

3. Bi-interpretation

In this section we shall assume Corollary 1.7 and deduce Theorem 1.1.

A bi-interpretation between R and $G(R)$ has four ingredients, which we describe in the form they occur here (which is not the most general form). 'Definability' will be in one of two first-order languages, the language L_{gp} of group theory and the language L_{rg} of ring theory. We set $\Gamma = G(R)$, in an attempt to avoid a forest of symbols.

(1) An interpretation of R in Γ; in most cases, this consists in an identification of R with a definable abelian subgroup R' of Γ such that addition in R' is the group operation in Γ, and multiplication in R' is definable in Γ (thus the ring structure on R' is L_{gp}-definable); in one special case, we instead take R' to be the image in $\Gamma/\mathrm{Z}(\Gamma)$ of a definable abelian subgroup of Γ (the target of an interpretation can be the quotient of Γ by a definable equivalence relation, see [20, §5.3]).

(2) An interpretation of Γ in R; namely, for some $d \in \mathbb{N}$ an identification of Γ with a subgroup $\Gamma^\dagger$ of $\mathrm{GL}_d(R)$, where $\Gamma^\dagger$ is definable in L_{rg} (thus the group structure on $\Gamma^\dagger$ is L_{rg}-definable, being just matrix multiplication).

(3) An L_{gp}-definable group isomorphism from Γ to $\Gamma^{\dagger\prime}$, the image of $\Gamma^\dagger$ in $\mathrm{GL}_d(R')$.

(4) An L_{rg}-definable ring isomorphism from R to $R'^\dagger$, the image of R' in $\mathrm{GL}_d(R)$.

We assume to begin with that each root group $U_\alpha(R)$ is definable; the small changes needed to deal with the exceptional case in Corollary 1.7 are indicated at the end of this section.

Interpreting R in $G(R)$

Lemma 3.1. *If $U_1, \ldots, U_q$ are distinct positive root subgroups then the mapping $\pi_1 : U_1(R) \ldots U_q(R) \to U_1(R)$ that sends $u_1 \ldots u_q$ to u_1 (in the obvious notation) is definable.*

Proof. If $g = u_1 \ldots u_q$ then

$$\{u_1\} = gU_q(R) \ldots U_2(R) \cap U_1(R)$$

(cf. [34, Lemma 18, Cor. 2]). ■

Lemma 3.2. *Let α and β be any two roots. Then the mapping*

$$c_{\alpha\beta} : U_\alpha(R) \to U_\beta(R), \quad x_\alpha(r) \mapsto x_\beta(r),$$

is definable.

Proof. Suppose first that α and β are the same length. Then there exist an element w in the Weyl group such that $w(\alpha) = \beta$, and a representative n_w for w, with $n_w \in N(R)$, such that $x_\alpha(r)^{n_w} = x_\beta(\eta r)$ for all $r \in R$, where $\eta = \pm 1$ [12, Lemma 7.2.1]. So we can define $c_{\alpha\beta}(g) = g^{\eta n_w}$.

Now suppose that α is long and β is short. We can find a short root μ and a long root ν such that $\mu + \nu = \gamma$ is a short root. The commutator formula gives (for a suitable choice of sign)

$$[x_\mu(\pm 1), x_\nu(s)] = x_\gamma(s)u_3 \dots u_q$$

where $u_i \in U_{j\mu + l\nu}$, $j + l = i$ (and $q \leq 5$) , so by Lemma 3.1 the map $c_{\nu\gamma}$ is definable. It follows by the first case that $c_{\alpha\beta} = c_{\alpha\nu}c_{\nu\gamma}c_{\gamma\beta}$ is definable.

Finally, if α is short and β is long we have $c_{\alpha\beta} = c_{\beta\alpha}^{-1}$. ∎

Lemma 3.3. *Let α, β and γ be any roots. The mapping*

$$m_{\alpha\beta\gamma} : U_\alpha(R) \times U_\beta(R) \to U_\gamma(R), \quad (x_\alpha(r), x_\beta(s)) \mapsto x_\gamma(rs),$$

is definable.

Proof. By the preceding lemma we may suppose that α and γ are short and that $\gamma = \alpha + \beta$. Then apply the same argument to the formula

$$[x_\alpha(\pm r), x_\beta(s)] = x_\gamma(rs)u_3 \dots u_q. \qquad ∎$$

Now we interpret R in Γ as follows: fix a root α_0, set $R' = U_{\alpha_0}(R)$ and identify $r \in R$ with $r' = x_{\alpha_0}(r)$. Then $m_{\alpha_0\alpha_0\alpha_0}$ defines multiplication in R'. Since addition in R' is simply the group operation, we may infer

Corollary 3.4. *Let f be a polynomial over $\mathbb{Z}$. Then the mapping $U_{\alpha_0}(R) \to U_{\alpha_0}(R)$ given by $r' \mapsto f(r')$ is L_{gp}-definable.*

Interpreting $G(R)$ in R

The group scheme G is defined as follows (see e.g. [1, §1]). Fix a faithful representation of the Chevalley group $G(\mathbb{C})$ in $\mathrm{GL}_d(\mathbb{C})$. The ring $\mathbb{Z}[G] = \mathbb{Z}[X_{ij}; i, j = 1, \dots, d]$ is the $\mathbb{Z}$-algebra generated by the co-ordinate functions on G, taken with respect to a suitably chosen basis for the vector space $\mathbb{C}^d$. For a ring R we define

$$G(R) = \mathrm{Hom}(\mathbb{Z}[G], R).$$

Thus an element $g \in G(R)$ may be identified with the matrix $(X_{ij}(g))$, and the group operation is given by matrix multiplication.

Let T_{ij} be independent indeterminates. The kernel of the obvious epimorphism $\mathbb{Z}[\mathbf{T}] \to \mathbb{Z}[G]$ is an ideal, generated by finitely many polynomials $P_l(\mathbf{T})$, $l = 1, \dots, s$, say. For a matrix $g = (g_{ij}) \in \mathrm{M}_d(R)$, we have

$$g \in G(R) \iff P_l(g_{ij}) = 0 \; (l = 1, \dots, s). \tag{7}$$

Thus $G(R)$ is L_{rg}-definable as a subset of $\mathrm{M}_d(R)$.

Definable isomorphisms

To complete **Step (3)**, we exhibit a definable isomorphism $\theta : G(R) \to G(R') \subseteq \mathrm{M}_d(R')$. The definition of such a θ is obvious; the work is to express this definition in first-order language.

We recall the construction of $G(R)$ in more detail (cf. [34, Chapters 2 and 3]). For each root α there is a matrix $X_\alpha \in \mathrm{M}_d(\mathbb{Z})$ such that

$$x_\alpha(r) = \exp(rX_\alpha) = 1 + rM_1(\alpha) + \cdots + r^q M_q(\alpha) \quad (r \in R) \tag{8}$$

where $M_i(\alpha) = X_\alpha^i / i!$ has integer entries, and q is fixed (usually $q \le 2$).

We have chosen a root subgroup $U_0 = U_{\alpha_0}(R)$ and identified it with the ring R by $r \mapsto r' = x_{\alpha_0}(r)$. We have identified $\Gamma = G(R)$ with a group of matrices. Now define $\theta : \Gamma \to \mathrm{M}_d(R') = U_0^{d^2} \subseteq \Gamma^{d^2}$ by

$$g\theta = (g'_{ij}).$$

If we give R' the ring structure inherited from R, this map is evidently a group isomorphism from Γ to its image in $\mathrm{GL}_d(R')$.

Lemma 3.5. *For each root α the restriction of θ to $U_\alpha(R)$ is definable.*

Proof. Let α be a root, fix i and j, and write θ_{ij} for the map $g \mapsto g'_{ij}$. Let m_l denote the (i, j) entry of the matrix $M_l(\alpha)$. Then for $g = x_\alpha(r)$ we have

$$g\theta_{ij} = (1 + m_1 r + \cdots + m_q r^q)'.$$

As $r' = x_{\alpha_0}(r) = gc_{\alpha\alpha_0}$, it follows from Corollary 3.4 that the restriction of θ_{ij} to $U_\alpha(R)$ is definable, and as this holds for all i, j it establishes the claim. ∎

Say the roots are $\alpha_1, \ldots, \alpha_q$. For a natural number N put

$$X_N = \Big(\prod_{i=1}^{q} U_{\alpha_i}(R)\Big) \ldots \Big(\prod_{i=1}^{q} U_{\alpha_i}(R)\Big)$$

with N factors. Thus X_N is a definable set, every product of N elementary root elements lies in X_N, and the preceding lemma implies that the restriction of θ to X_N is definable.

If $G(R)$ has finite elementary width N then $G(R) = X_N$ and so θ is definable.

Suppose alternatively that G is adjoint. Then

$$\bigcap_{i=1}^{q} \mathrm{C}_G(x_{\alpha_i}(1)) = \mathrm{Z}(G) = 1 \tag{9}$$

(see Lemma 2.2 and the discussion following it).

We quote

Lemma 3.6 ([35, Cor. 5.2]). *There exists $L \in \mathbb{N}$ such that for each root α and every $g \in G(R)$ the commutator $[x_\alpha(1), g]$ is a product of $3L$ elementary root elements.*

Taking $N = 3L + 1$ we see that each $x_\alpha(1)^g \in X_N$. Set $v_i = x_{\alpha_i}(1)\theta$. Now let $g \in G(R)$ and $h \in G(R')$. If $g\theta = h$ then for $i = 1, \dots, q$ there exists $x_i \in X_N$ such that

$$x_{\alpha_i}(1)^g = x_i, \quad x_i\theta = v_i^h.$$

Conversely, if this holds then $v_i^h = v_i^{g\theta}$ for each i, so $g\theta \cdot h^{-1}$ centralizes each v_i; as θ is an isomorphism it follows from (9) that $g\theta = h$. Thus the statement '$g\theta = h$' is expressible by a first-order formula, and θ is definable.

To complete **Step (4)**, define $\psi : R \to U_0 \subseteq \mathrm{M}_d(R)$ by $r\psi = r' = x_{\alpha_0}(r)$. This is a ring isomorphism by definition, when U_0 is given the appropriate ring structure. The expression (8) now implies

Lemma 3.7. *The map ψ is L_{rg}-definable.*

When $U_\alpha(R)$ is not definable

Set $K = \mathrm{Z}(\Gamma)$ and write $\sim : \Gamma \to \Gamma/K$ for the quotient map. Corollary 1.7 shows that each of the subgroups $U_\alpha(R)K$ is definable. Lemmas 3.1–3.3 remain valid, with essentially the same proofs, if each $U_\alpha(R)$ is replaced by $U_\alpha(R)K$. As $U_\alpha(R) \cap K = 1$ the map $\sim$ restricts to an isomorphism $U_\alpha(R) \to \widetilde{U_\alpha(R)K} = \widetilde{U_\alpha(R)}$, and we define $R' := \widetilde{U_{\alpha_0}(R)}$, setting $r' = \widetilde{x_{\alpha_0}(r)}$. Then Corollary 3.4 remains valid if $U_{\alpha_0}(R)$ is replaced by $\widetilde{U_{\alpha_0}(R)}$.

The interpretation of Γ in R is as above.

We have a definable ring isomorphism $\psi : R \to \widetilde{U_0}$ as in Lemma 3.7.

Similarly, the group isomorphism $\theta : \Gamma \to \mathrm{M}_d(R') = \widetilde{U_0}^{d^2} \subseteq \widetilde{\Gamma}^{d^2}$ is definable: in the proof of Lemma 3.5, we replace each U_i by U_iK, and then apply the map $\sim$ to each root element that appears in the discussion.

The bi-interpretability of Γ with R is now established in all cases.

4. Axiomatizability

In §3 we set up a bi-interpretation of a specific shape between a group Γ and a ring R, spelt out explicitly in points (1)–(4) at the beginning of the section. As is well known, this implies a close correspondence between first-order properties of the two structures; here we explore some of the consequences (professional model theorists are invited to skip the next few paragraphs!).

The interpretation of R in Γ involves two or three formulae: one, and if necessary two, define the subset (it was $U_\alpha(R)$), or its quotient $(U_\alpha(R)\mathrm{Z}(\Gamma)/\mathrm{Z}(\Gamma))$, which we called R'; the third defines a binary operation m on R'. Let P_1 be a sentence that expresses the facts

(1) each of the definable mappings denoted π_1 in Lemma 3.1 actually is a well defined mapping;

(2) the definition of m does define a binary operation on the set R';

(3) $(R', +, m)$ is a commutative integral domain, where $+$ is the group operation inherited from Γ.

Let us call this ring A_Γ.

The sentence $P_1 = P_1(\mathbf{g})$ involves some parameters $g_1, \dots, g_r$ from $G(R)$. Let P_1' denote the sentence $\exists h_1, \dots, h_r\ P_1(\mathbf{h})$. We shall use this convention for other sentences later.

Now if H is any group that satisfies P_1', the same formulae define a ring A_H. For each L_{rg} formula α there is an L_{gp} formula α^* such that $A_H \models \alpha$ iff $H \models \alpha^*$, since ring operations in A_H are expressible in terms of the group operation in H. (Note that α^* will involve parameters, obtained by substituting h_i for g_i.)

Analogously, the equations on the right-hand side of (7) may be expressed as a formula in L_{rg}, that for any ring S defines a subset $G(S)$ of S^{d^2}; and if S is an integral domain, the set $G(S)$ with matrix multiplication is a group. For each L_{gp} formula β there is an L_{rg} formula $\beta^\dagger$ such that $G(S) \models \beta$ iff $S \models \beta^\dagger$.

Now in §3 we give (i) an L_{gp} formula that defines a group isomorphism $\theta : \Gamma \to G(A_\Gamma)$, and (ii) an L_{rg} formula that defines a ring isomorphism $\psi : R \to A_{G(R)}$. The assertions that these formulae actually define such isomorphisms can be expressed by (i) an L_{gp} sentence P_2 and (ii) an L_{rg} sentence P_3, say.

The results of §3 amount to this: if the group G and the ring R satisfy the hypotheses of Theorem 1.1, then $G(R)$ satisfies the conjunction of P_1' and P_2', and R satisfies P_3', where P_3' is obtained from P_3 by adding an existential quantifier over the (ring) variables corresponding to the matrix entries of the original parameters g_i.

The correspondence $\alpha \to \alpha^*$ implies that any ring axioms satisfied by R can be expressed as properties of the group $\Gamma = G(R)$. If these axioms happen to determine the ring up to isomorphism, the existence of θ then shows that the corresponding properties of Γ, in conjunction with P_1' and P_2', determine Γ up to isomorphism. In the same way, if $G(R)$ happens to be determined by some family of group axioms, then a corresponding family of ring properties, together with P_3, will determine R.

To apply this observation we need

Proposition 4.1. (i) *If $G(R)$ is a finitely generated group then R is a finitely generated ring.*

(ii) *If $G(R)$ is a Hausdorff topological group then R is a Hausdorff topological ring, and R is profinite, locally compact or t.d.l.c. if $G(R)$ has the same property.*

Proof. (i) Suppose $G = \langle g_1, \dots, g_m \rangle$. The entries of the matrices $g_i^{\pm 1}$ generate a subring S of R, and then $G(R) = G(S)$. Choose a root α. Then

$$U_\alpha(R) = U_\alpha(k) \cap G(R) = U_\alpha(k) \cap G(S) = U_\alpha(S).$$

As the map $r \mapsto x_a(r)$ is bijective it follows that $R = S$.

(ii) Suppose that $G(R)$ is a (Hausdorff) topological group. Let $U_0 = U_{\alpha_0}$ be the root group discussed in §3. Then $U_0(R)$ is closed in the topology, by Lemma 2.1. Thus with the subspace topology $U_0(R)$ is a topological group; it is locally compact, compact or totally disconnected if $G(R)$ has the same property.

We have seen that R is isomorphic to a ring R', where the additive group of R' is $U_0(R)$. It remains to verify that the ring multiplication in R' is continuous. This in turn follows from the facts (a) the commutator defines a continuous map $G(R) \times G(R) \to G(R)$ and (b) the projection mapping π_1 described in Lemma 3.1 is continuous, because $U_1(R) \dots U_q(R)$ is a topological direct product. ■

We have stated the proposition for $G(R)$ for the sake of clarity. However, a more general version is required:

Proposition 4.2. *Let H be a group that satisfies P_1' and P_2', and put $S = A_H$. Then* (i) *and* (ii) *of Proposition 4.1 hold with S in place of R and H in place of $G(R)$.*

Proof. (i) P_1 and P_2 ensure that S is a commutative integral domain and that $H \cong G(S)$. Now the result follows from the preceding proposition.

(ii) We have $S = U$ (or $S = UZ/Z$) where U (or UZ) is defined as a double centralizer (or similar, cf. Lemma 2.5) in H (and $Z = \mathrm{Z}(H)$). It follows that U (or UZ) is closed in the topology of H. Thus S inherits a topology, which makes $(S, +)$ a topological group with the given properties. The continuity of multiplication follows as before: the assumption that the mapping π_1 is well defined implies that the corresponding product of definable subgroups is actually a topological direct product, and hence that π_1 is continuous; the other ingredients in the definition of multiplication are clearly continuous. ■

Now we can deduce Corollary 1.3, in a slightly more general form.

Theorem 4.3. *Assume that G and R satisfy the hypotheses of Theorem 1.1. Let Σ be a set of sentences of L_{rg} such that $R \models \Sigma$. Then there is a set $\tilde{\Sigma}$ of sentences of L_{gp}, finite if Σ is finite, such that $G(R) \models \tilde{\Sigma}$ and such that:*

(i) *Suppose that $G(R)$ is a finitely generated group. If R is the unique f.g. ring* (*up to isomorphism*) *satisfying Σ then $G(R)$ is the unique f.g. group* (*up to isomorphism*) *that satisfies $\tilde{\Sigma}$.*

(ii) *If R is the unique profinite, locally compact, or t.d.l.c. ring* (*up to isomorphism*) *satisfying Σ then $G(R)$ is the unique profinite, locally compact, or t.d.l.c. group* (*up to isomorphism*) *that satisfies $\tilde{\Sigma}$.*

Proof. For each $\sigma \in \Sigma$ there is a formula σ^* such that for any group H that satisfies P_1', we have $H \models \sigma^*$ iff $A_H \models \sigma$. We take $\tilde{\Sigma} = \Sigma^* \cup \{P_1', P_2'\}$. The result now follows from Proposition 4.2 by the preceding discussion. ■

Remark. Theorem 4.3 has a converse, in most cases. *If $G(R)$ is axiomatizable* (*or FA*) *among groups that are profinite, l.c. or t.d.l.c. then R is similarly axiomatizable in the corresponding class of rings*. The proof is the same, using a suitable analogue of Proposition 4.2 (ii): in this case, it is easy to see that for a ring S, the group $G(S) \subseteq \mathrm{M}_d(S)$ defined by the polynomial equations (7) inherits an appropriate topology from S.

We are not entirely sure whether the analogue of (i) holds in all cases. Assume that $G(R)$ is generated by its root subgroups, and *either* (i) the root system Φ is simply laced *or* (ii) $|R/2R|$ is finite and $\Phi \neq G_2$ *or* (iii) $|R/6R|$ is finite. Then using the idea of Lemma 3.3 one can show that if R is finitely generated as a ring then $G(R)$ is a finitely generated group. Thus we can assert: *Let R be a f.g. integral domain and assume* (i), (ii) *or* (iii). *If $G(R)$ is first-order rigid, resp. FA, among f.g. groups, then R has the same property among f.g. rings.*

Topological vs. algebraic isomorphism

In Theorem 4.3, the phrase 'up to isomorphism' refers to isomorphism as *abstract groups*. In part (ii), to infer that $G(R)$ is first-order rigid, or FA, in the appropriate class of topological groups, one needs to show that abstract isomorphism with $G(R)$ implies topological isomorphism. In most of the cases under discussion, this is true.

A 'local field' means one with a non-discrete locally compact topology, and a *locally compact* group means one that is not discrete.

Proposition 4.4. (i) *Let k be a local field. Then any locally compact group abstractly isomorphic to $G(k)$ is topologically isomorphic to $G(k)$.*

(ii) *Let R be a complete local domain with finite residue field κ, and assume that G is simply connected. Then any profinite group abstractly isomorphic to $G(R)$ is topologically isomorphic to $G(R)$, unless possibly* $\mathrm{char}(\kappa) = 2$ *and G is of type B_n or C_n, or* $\mathrm{char}(\kappa) = 3$ *and G is of type G_2.*

Proof. (i) This is equivalent to the claim that $G(k)$ is determined up to topological isomorphism by its algebraic structure.

The Bruhat decomposition of $G(k)$ is algebraically determined (e.g. by the proof of Corollary 1.7), and it expresses $G(k)$ as a finite union of products of copies of k (the root subgroups) and of k^* (the torus). It follows that any topology on G is determined by its restriction to the root sugroups, identified with k. It follows from Lemma 3.3 that the algebraic stucture of k is determined by that of G. Now a local field that is algebraically isomorphic to k is topologically isomorphic to k: this is clear from the classification of local fields (see e.g. [39, Chapter 1]).

In many cases a stronger result holds: *every isomorphism with $G(k)$ is continuous.* This holds when $k \neq \mathbb{C}$ (it may be deduced from [34, Lemma 77]; cf. [10, §9]), but obviously not for $k = \mathbb{C}$.

(ii) This follows from the *congruence subgroup property*: if K is a normal subgroup of finite index in $G(R)$ then K contains the congruence subgroup $\ker(G(R) \to G(R/I))$ for some ideal I of finite index in R; see [1, Thm. 1.9]. Thus every subgroup of finite index in $G(R)$ is open. Hence if $f : G(R) \to H$ is an isomorphism, where H is a profinite group, then $f^{-1}(K)$ is open in $G(R)$ for every open subgroup K of H, so f is continuous; and a continuous isomorphism between profinite groups is a homeomorphism.

Alternatively, it follows from [23, Cor. 3.4] that $G(R)$ is finitely generated as a profinite group provided the Lie algebra over κ associated to Φ is perfect. As $G(R)$ in this case is virtually a pro-p group, this in turn implies that every subgroup of finite index is open [18, Thm. 1.17]. ■

5. Applications

As before, G is a simple Chevalley–Demazure group scheme defined by a root system Φ of rank at least 2 and R is a commutative integral domain.

The group $G(R)$ has finite elementary width in the following cases:

(1) When R is a field, by the Bruhat decomposition ([12, Thm. 8.4.3], [34, Cor. 1, p. 21]).

(2) When R is a local ring and G is simply connected, by a theorem of Abe [1, Prop. 1.6] together with [19, Cor. 1].

(3) When G is simply connected and R is the ring of S-integers in a global field ($S \supseteq S_\infty$ a finite set of places, $S = S_\infty$ in the function-field case): Tavgen [36, Thm. A], Trost [36, Thm. 1.3].

To apply Theorem 4.3, we need to pick out from this list those rings that are also FA. Now [3, Prop. 7.1] says that *every f.g. commutative ring* is FA in the class of f.g. rings; it is shown in [28, Thm. 4.4] that *every regular, unramified complete local ring with finite residue field is FA* in the class of profinite rings. (These rings are $\mathbb{F}_q[[t_1, \dots, t_n]]$, $\mathfrak{o}_q[[t_1, \dots, t_n]]$, $n \geq 0$, where $\mathfrak{o}_q = \mathbb{Z}_p[\zeta]$, $q = p^f$, ζ a primitive $(q-1)$th root of unity).

It is also the case that every locally compact field is FA in the class of all locally compact rings. We are grateful to Matthias Aschenbrenner for supplying the proof of Proposition 5.2 sketched below.

Thus we may deduce – invoking Proposition 4.1 (i) for part (i) –

Corollary 5.1. (i) *If $G(R)$ is finitely generated and G is adjoint then $G(R)$ is FA among f.g. groups* (*assuming that the units condition holds*).

(ii) *If R is a ring of S-integers as in* (3) *above then the S-arithmetic group $G(R)$ is FA among f.g. groups, assuming that G is simply connected.*

(iii) *The profinite groups $G(R)$, $R = \mathbb{F}_q[[t_1, \dots, t_n]]$ or $R = \mathfrak{o}_q[[t_1, \dots, t_n]]$, $n \geq 0$, are FA among profinite groups, if G is adjoint or simply connected.*

(iv) *If k is a local field then $G(k)$ is FA among locally compact groups.*

Proposition 5.2 (M. Aschenbrenner). *Let k be a locally compact field. Then k is determined up to isomorphism within the class of locally compact rings by finitely many first-order sentences.*

Proof. The first axiom asserts that k is a field. Now we consider the cases.

1. If $k = \mathbb{R}$, then k is axiomatized by saying that k is Euclidean, that is, (a) -1 is not of the form $x^2 + y^2$ and (b) for every $x \in k$ either x or $-x$ is a square. (This implies that

k is an ordered field for a (unique) ordering whose set of non-negative elements is given by the squares; and no other local field is orderable.)

2. If $k = \mathbb{C}$, then k is axiomatized by saying that every element is a square.

3. Let $k = \mathbb{F}_q((t))$ where q is a power of a prime p. Ax [7] provides a formula φ_p that defines the valuation ring in any henselian discretely valued field of residue characteristic p. We can then make a sentence which expresses that the characteristic of the field is p and the residue field of the valuation ring defined by φ_p has size q. This sentence determines k up to isomorphism among all local fields.

4. The remaining case is where k is a finite extension of $\mathbb{Q}_p$. Then we use Ax's formula φ_p again to express that the ramification index and residue degree of k have given values e and f. Then $(k : \mathbb{Q}_p) = ef$. Let h be the minimal polynomial of a primitive element for k over $\mathbb{Q}_p$, and let $g \in \mathbb{Q}[t]$, of degree $ef = \deg(h)$, have coefficients sufficiently close to those of h that Krasner's Lemma applies, i.e. g has a zero $\beta \in k$ and $k = \mathbb{Q}_p(\beta)$. Then k is determined among local fields by: $p \neq 0$; the formula φ_p defines in k a valuation ring with residue field of characteristic p, ramification index e, and residue degree f; and the polynomial g has a zero in k. ■

6. Torus witnesses in some exceptional groups

Returning to the proof of Lemma 2.2, begun in §2, we now establish the existence of the required torus witnesses for some exceptional groups, under the blanket assumption that $R^* \neq \{1\}$. A similar approach works for the other groups as well, but different methods will enable us in §§7 and 8 to dispense with any conditions on R^*.

We begin with the following basic observation:

Lemma 6.1. *Suppose that Φ is a root system of rank at least 2 and $r \in R^* \setminus \{1\}$. If $\alpha, \beta \in \Phi$ and γ is orthogonal to α and non-orthogonal to β, then $s_{\alpha,\beta} = h_\gamma(r)$ is a torus witness for (α, β)* ***unless*** *$A_{\gamma\beta} = \pm 2$ and $r = -1$, or $A_{\gamma\beta} = \pm 3$ and $r^3 = 1$.*

Note also that if $\mathrm{char}(R) \neq 2$ and α, β are non-orthogonal with $A_{\alpha\beta} \neq 2$, then $s_{\alpha,\beta} = h_\alpha(-1)$ is a torus witness.

Lemma 6.2. *Let $\Phi \in \{E_6, E_7, E_8, F_4\}$ and suppose $\alpha, \beta \in \Phi$ are orthogonal. Then there is a root γ orthogonal to α and non-orthogonal to β unless $\Phi = F_4$ and α, β are both long.*

Proof. Let $\Phi = E_n, n = 6, 7, 8$. Let $a_1, \ldots, a_n$, $n \in \{6, 7, 8\}$, be a set of fundamental roots where a_{n-3} is the branching point. We may assume that $\alpha = a_1$. If β does not involve a_2, we can choose γ as a root in the subdiagram spanned by $a_3, \ldots, a_n$ and non-orthogonal to β.

Now suppose β is a positive root involving a_2 and orthogonal to α. If there is a fundamental root a_i, $3 \leq i \leq n$, which is non-orthogonal to β, put $\gamma = a_i$. Otherwise an easy calculation (starting from a_n) shows that for $n = 7, 8$ we have

$$\beta = \epsilon_n\big(a_1 + 2a_2 + 2a_{n-5} + \tfrac{5}{2}a_{n-4} + \tfrac{3}{2}a_{n-2} + 3a_{n-3} + 2a_{n-1} + a_n\big),$$

whereas for $n = 6$ we must have

$$\beta = \epsilon_6\big(\tfrac{5}{4}a_1 + \tfrac{5}{2}a_2 + \tfrac{3}{2}a_4 + 3a_3 + 2a_5 + a_6\big).$$

In either case, β is non-orthogonal to a_2. For $n = 6, 7, 8$ let

$$\gamma = a_1 + 2(a_2 + \cdots + a_{n-3}) + a_{n-2} + a_{n-1}.$$

Then γ is orthogonal to α, but not to β.

Let now $\Phi = F_4$. Let $a_1, \ldots, a_4$ be a set of fundamental roots where a_1 is long and a_4 is short. First assume that $\alpha = a_1$. If β is short and orthogonal to α then either it is contained in the subdiagram spanned by a_3, a_4 and we choose γ in this A_2-subdiagram non-orthogonal to β; or else we have $\beta \in \{a_1 + 2a_2 + 2a_3 + a_4, a_1 + 2a_2 + 3a_3 + a_4, a_1 + 2a_2 + 3a_3 + 2a_4\}$ and $\gamma = a_4$ or $\gamma = a_3 + a_4$ is as required.

Next assume $\alpha = a_4$ is short. If β is a positive root orthogonal to α and contained in the subdiagram spanned by a_1, a_2, then we find γ as before. Otherwise we have $\beta \in \{a_2 + 2a_3 + a_4, a_1 + a_2 + 2a_3 + a_4, a_1 + 2a_2 + 2a_3 + a_4\}$ and $\gamma = a_1$ or $\gamma = a_1 + a_2$ is as required. ■

Lemma 6.3. *Let $\Phi \in \{E_6, E_7, E_8, F_4\}$ and suppose $\alpha, \beta \in \Phi$ are non-orthogonal and $R^* \neq \{1\}$. Then there is a torus witness for (α, β).*

Proof. If α, β are non-orthogonal, then (replacing β by $-\beta$ if necessary) we may assume that they form a basis for the rank 2 subdiagram spanned by α and β. By [4, Thm. 7], α, β can be extended to a system of fundamental roots for Φ. If in the associated diagram there is a neighbour γ of β with $A_{\gamma\beta} \neq \pm 2$ and γ is not a neighbour of α, then $h_\gamma(r)$, $r \in R^* \setminus \{1\}$, is as required. We now deal with the remaining situations separately either by finding a suitable γ or by giving the witness directly.

Let $\Phi = E_n$, $n = 6, 7, 8$. Since any pair of adjacent fundamental roots is contained in an A_3 subdiagram, we may assume that $\alpha = a_2$, $\beta = a_1$ so $\gamma = a_1 + a_2 + a_3$ is as required.

Let $\Phi = F_4$. Let $a_1, \ldots, a_4$ be the resulting fundamental system where a_1 is long and a_4 is short. First assume $\alpha = a_2$, $\beta = a_1$, so $\gamma = a_2 + 2a_3$ is as required. If $\alpha = a_3$, $\beta = a_4$, then $\gamma = a_2 + a_3$ is as required. If $\alpha = a_1$, $\beta = a_2$, and $\mathrm{char}(R) \neq 2$, then $h_\alpha(-1)$ is as required. If $\mathrm{char}(R) = 2$, then $h_{a_3}(r)$ for $r \in R^* \setminus \{1\}$ works. ■

We can now summarize the existence of torus witnesses as follows:

Proposition 6.4. *Suppose $\Phi \in \{E_6, E_7, E_8, F_4\}$ and let $\alpha, \beta \in \Phi$ be linearly independent. Then there is a torus witness for (α, β)* except *possibly if $R^* = \{\pm 1\}$, $\Phi = F_4$, and α, β are orthogonal and both long.*

This completes the proof of Lemma 2.2 for $\Phi \in \{E_6, E_7, E_8\}$.

Assume finally that G is of type F_4. Let $a_1, \ldots, a_4$ be fundamental roots of Φ where a_1, a_2 are long, a_3, a_4 are short and $\alpha = a_1$. By Proposition 6.4 there is a torus witness $s_{\alpha,\beta}$ for each root $\beta \neq \pm\alpha$, with the exception of the following long roots:

(1) $b_2 = a_1 + 2a_2 + 2a_3$,

(2) $b_3 = a_1 + 2a_2 + 2a_3 + 2a_4$,

(3) $b_4 = a_1 + 2a_2 + 4a_3 + 2a_4$.

Note that the root subgroups $U_1, \dots, U_4$ corresponding to a_1, b_2, b_3, b_4 commute elementwise.

To complete the proof of Lemma 2.2 for $G = F_4$ set

$$Y = \{s_{\alpha,\beta} \mid \beta \in \Phi_+ \setminus \{a_1, b_2, b_3, b_4\}\} \cup \{x_{-b_i}(1) \mid i = 1, 2, 3\}.$$

Note that each $x_{-b_i}(1)$ centralizes each U_j $(j \neq i)$, and commutes with no element of $U_i \setminus \{1\}$.

Let $g \in \mathrm{C}_G(Y)$. We have to show that $g \in U_1 Z$.

Arguing as in the proof of Proposition 2.4 we conclude that g is of the form

$$g = u_1 u_2 u_3 u_4 z \quad \text{where} \quad u_i \in U_i,\ i = 1, 2, 3, 4,\ z \in Z.$$

Since $x_{-b_3}(1)$ centralizes g and U_1, U_2, U_4, we have $u_3 = 1$. We see similarly that $u_2 = u_4 = 1$, and the result follows.

7. The building for G_2

Another way to study centralizers is to examine the action of $G = G(\bar{k})$ on the building associated to G. This method is practical for groups of rank 2; we illustrate it here in the case of G_2, by proving

Proposition 7.1. *Let G be of type G_2 and let U be a root group of G. Then there exists a finite set $Y \subseteq \mathrm{C}_{G(R)}(U)$ such that $\mathrm{C}_G(Y) \subseteq U$.*

If G is a Chevalley group of type G_2, we have $\mathrm{Z}(G) = 1$ (see [34, p. 23]), and the associated spherical building Δ is a *generalized hexagon*, i.e. a bipartite graph of diameter 6, girth 12 and valencies at least 3 (see [25] for more details).

For vertices $x_0, \dots, x_m$ in Δ,

$$G^{[i]}_{x_0,\dots,x_m}$$

denotes the subgroup of G fixing all elements at distance at most i from some $x_j \in \{x_0, \dots, x_m\}$.

For $i = 0$, this is just the pointwise stabilizer of $\{x_0, \dots, x_m\}$ in G and we omit the superscript. In this notation, a *root subgroup* for a generalized hexagon Δ is of the form

$$U = G^{[1]}_{x_1,\dots,x_5}$$

for a simple (i.e. without repetitions) path $(x_1, \dots, x_5)$ in Δ. Thus our aim is to construct a finite set $Y \subseteq G(R)$ centralizing $G^{[1]}_{x_1,\dots,x_5}$ such that

$$g \in \mathrm{C}_G(Y) \quad \text{implies} \quad g \in G^{[1]}_{x_1,\dots,x_5}.$$

The generalized hexagon Δ associated to a Chevalley group of type G_2 is a *Moufang hexagon*, i.e. for any simple path $x_0, \dots, x_6$ in Δ the root subgroup $G^{[1]}_{x_1,\dots,x_5}$ acts regularly on the set of neighbours of x_0 different from x_1 and regularly on the set of neighbours of x_6 different from x_5 (see [37]). As a consequence, we have

$$G^{[1]}_{x_0,x_1,\dots,x_5} = 1. \tag{10}$$

We will repeatedly use the following:

Remark 7.2. For any vertex $x \in \Delta$, the stabilizer G_x is a parabolic subgroup of G and acts on the set of neighbours of x as the Zassenhaus group $\mathrm{PSL}_2(\overline{k})$. In particular, if $g \in G$ fixes at least three neighbours of x, then it fixes all neighbours of x.

Furthermore, for a path (x, y) the stabilizer $G_{x,y}$ contains a regular abelian normal subgroup acting as the additive group of $\overline{k}$ on the set of neighbours of y different from x.

Most arguments rely on the following observation:

Remark 7.3. Let H be a group acting on a set X, let $g \in H$ and let A be the set of fixed points of g. Any $h \in H$ centralizing g leaves the set A invariant.

In light of (10) this remark immediately implies

Corollary 7.4. *For any root element $u \in G^{[1]}_{x_1,\dots,x_5} \setminus \{1\}$, each $g \in \mathrm{C}_G(u)$ fixes x_3.*

For any 12-cycle $(x_0, \dots, x_{12} = x_0)$ in Δ, the group $G_{x_0,\dots,x_{12}}$ is a maximal torus in G. We let $U_i = G^{[1]}_{x_i,\dots,x_{i+4}}$ $(i = 0, \dots, 11)$ denote the corresponding root subgroups (where addition is modulo 12), so $U_1 = U$. In this notation we see that for $1 \neq v \in U_i$ and $g \in \mathrm{C}_G(v)$ we have $g \in G_{x_{i+2}}$ by Corollary 7.4.

The bipartition of the vertices leads to two types of paths $(x_0, \dots, x_6)$ depending on the type of the initial vertex x_0 (note that x_0 and x_6 have the same type). Since G acts transitively on ordered cycles of length 12 (of the same bipartition type), the isomorphism type of a root subgroup only depends on the type of the root group with respect to this bipartition.

It follows easily from the commutation relations that the root subgroups corresponding to long roots consist of *central elations*, i.e. for one type of path $(x_0, \dots, x_6)$ we have $G^{[1]}_{x_1,\dots,x_5} = G^{[3]}_{x_3}$.

First assume that $U = U_1 = G^{[3]}_{x_3}$. Since U centralizes U_j for $j = 10, 11, 0, 1, 2, 3, 4$, we may choose Y to contain a non-trivial element from each of the $U_j(R)$, $j = 10, 11, 0, 1, 2, 3, 4$. We add five further elements $y_i = v_i^{h_i}$ to Y where

$$\begin{aligned} &v_1, v_2 \in U_3(R), \quad v_3 \in U_4(R), \quad v_4 \in U_{11}(R), \quad v_5 \in U_{10}(R), \\ &h_1 \in U_{11}(R), \quad h_2, h_3 \in U_0(R), \quad h_4 \in U_3(R), \quad h_5 \in U_2(R), \end{aligned}$$

and $v_i \neq 1, h_i \neq 1$ for each i. These centralize U because for $i = 1,\ 2$ we have $[U, y_i] \subseteq G^{[3]}_{x_5^{h_i}} \cap G^{[3]}_{x_3} = 1$, $[U, y_3] \subseteq G^{[3]}_{x_6^{h_3}} \cap G^{[3]}_{x_3} = 1$, $[U, y_4] \subseteq G^{[3]}_{x_1^{h_4}} \cap G^{[3]}_{x_3} = 1$ and $[U, y_5] \subseteq G^{[1]}_{x_0^{h_5}} \cap G^{[3]}_{x_3} = 1$.

Now suppose that g centralizes Y. Then $g \in G_{x_0,\ldots,x_6}$. We claim that $g \in G^{[1]}_{x_i}$ for $i = 1,\ldots,5$. Since g commutes with y_1, g fixes $x_5^{h_1} \neq x_3, x_5$. By Remark 7.2 this implies that $g \in G^{[1]}_{x_4}$. Using y_4 we see similarly that $g \in G^{[1]}_{x_2}$.

Similarly, since g commutes with y_2, g fixes $x_5^{h_2}$ and hence also $x_4^{h_2} \neq x_2, x_4$. This implies that $g \in G^{[1]}_{x_3}$. Finally, g fixes $x_6^{h_3}$ and $x_0^{h_5}$ because g commutes with y_3 and y_5; as before we conclude from Remark 7.2 that $g \in G^{[1]}_{x_1,x_5}$, and the claim follows.

Now assume that $U = U_1 \neq G^{[3]}_{x_3}$, and so $U_{2i} = G^{[3]}_{x_{2i+2}}$ for $i = 0,\ldots,5$. Then U commutes elementwise with U_{10}, U_0, U_2, U_4, and we choose Y to contain a nontrivial element from each of $U_{10}(R)$, $U_0(R)$, $U_2(R)$, $U_4(R)$.

This ensures, by Remark 7.3, that any element centralizing Y must lie in

$$G_{x_0,x_2,x_4,x_6} = G_{x_0,x_1,x_2,x_3,x_4,x_5,x_6}.$$

As in the previous case, we extend Y by four or six further elements $y_i = v_i^{h_i}$, where $v_i \neq 1$, $h_i \neq 1$ for each i,

$$\begin{array}{llll} v_1 \in U_4(R), & v_2 \in U_2(R), & v_3 \in U_1(R), & v_4 \in U_{10}(R), \\ h_1 \in U_0(R), & h_2 \in U_{10}(R), & h_3 \in U_3(R), & h_4 \in U_2(R), \end{array}$$

and if $\mathrm{char}(R) = 3$ also

$$v_5 \in U_{10}(R), \quad v_6 \in U_4(R), \quad h_5 \in U_3(R), \quad h_6 \in U_{11}(R).$$

Note that y_1 and y_2 centralize U because

$$[U, y_1] \in G^{[3]}_{x_6^{h_1}} \cap G^{[1]}_{x_2} = 1, \quad [U, y_2] \in G^{[3]}_{x_4^{h_2}} \cap G^{[1]}_{x_0} = 1.$$

Now let $g \in \mathrm{C}_G(Y)$. Then g centralizes y_1, and therefore fixes $x_6^h \neq x_4, x_6$. By Remark 7.2 we get $g \in G^{[1]}_{x_5}$. In a similar way we find that $g \in G^{[1]}_{x_1}$ and $g \in G^{[1]}_{x_3}$.

It remains to show that $g \in G^{[1]}_{x_i}$ for $i = 2$ and $i = 4$. We distinguish two cases according to the characteristic of R. First assume that $\mathrm{char}(R) \neq 3$ and extend the path $(x_1,\ldots,x_5)$ to a simple path $(x_1,\ldots,x_7)$. For any $v \in G^{[1]}_{x_3,\ldots,x_7} \setminus \{1\}$ and $1 \neq u \in U_1$ the commutator relations (see §10) with $\mathrm{char}(k) \neq 3$ imply that $[u, v] \neq 1$. This shows that x_1, x_3 are the only neighbours y of x_2 such that $G^{[1]}_y$ meets U_1 non-trivially.

On the other hand, for any simple path $(x_1', x_2, x_3, x_4, x_5)$ the actions of the root groups U_1 and $U_1' = G^{[1]}_{x_1',x_2,x_3,x_4,x_5}$ on the neighbours of x_6 agree, by Remark 7.2. Since the root groups are abelian, we therefore have $[U, w] = 1$ for any $w \in U_1'$.

This shows in particular that $y_3 \in \mathrm{C}_{G(R)}(U)$. By the previous remark $x_1' = x_1^{h_3}$ and x_3 are the only neighbours of x_2 such that $y_3 \in G^{[1]}_{x_1',x_3}$, and so g fixes x_1'. Again by Remark 7.2 we conclude that $g \in G^{[1]}_{x_2}$. Similarly, we see that $y_3 \in \mathrm{C}_{G(R)}(U)$, and find that $g \in G^{[1]}_{x_4}$ as required.

Finally, assume that $\mathrm{char}(R) = 3$. Then the commutation relations show that $[U_1, U_3] = 1$ and hence

$$U_1 = G^{[2]}_{x_2,x_4}.$$

As $h_5 \in U_3$ and $v_5 \in U_{10} = G^{[3]}_{x_0}$, we have $[U, y_5] \in U_1 \cap G^{[3]}_{x_0^h} = 1$, so $y_5 \in \mathrm{C}_{G(R)}(U)$. Now Corollary 7.4 implies that g fixes $x_0^{h_5}$ and hence also $x_1^{h_5} \neq x_1, x_3$. As before we infer that $g \in G^{[1]}_{x_2}$. The same argument using y_6 shows finally that $g \in G^{[1]}_{x_4}$, and concludes the proof.

8. Root witnesses in the classical groups

In this section we establish Lemma 2.2 for the groups of classical type, and complete the proof of Theorem 1.6.

Proposition 8.1. *Let G be a Chevalley group of type A_n, B_m, C_m or D_m ($n \geq 1$, $m \geq 2$), and let R be an integral domain. Let U be a root subgroup of G. Write Z for the centre of G. There exists a set $Y \subseteq \mathrm{C}_{G(R)}(U)$ consisting of root elements such that*

$$\mathrm{C}_G(Y) \subseteq UZ, \tag{11}$$

unless G is of type C_n, U belongs to a short root α and $R^* = \{\pm 1\}$, in which case

$$\mathrm{C}_G(Y) \subseteq UU_1U_2Z \tag{12}$$

where U_1 and U_2 are root subgroups belonging to long roots adjacent to α in a C_2 subsystem.

Proof. Suitable sets Y are exhibited in the lemmas below for particular forms of G: the universal groups SL_n and Sp_{2m} for A_n, C_m respectively, and for orthogonal versions of B_m and D_m. Now if v is a unipotent element and $v^g \in vZ$ then $v^g = v$, because Z consists of semisimple elements (Jordan decomposition); hence both statements involving Y remain true if $\mathrm{C}_{G(R)}$ is replaced by 'centralizer modulo Z'. It follows easily that if (11) or (12) holds, then it remains valid when G is replaced by G/Z. In particular, they hold for the adjoint form of each group, and any group 'between' SL_n and PSL_n.

The result for the universal forms (in cases B_m and D_m) follows directly from the established cases because root elements in $G(R)$ lift to root elements in the covering group. ∎

The precise description of $\mathrm{Z}(\mathrm{C}_{G(R)}(u))$ for $1 \neq u \in U$ in case (12) is given below in Proposition 8.4.

We use the notation of [12, §11.3] for the classical groups. Throughout, R denotes an integral domain, and e_{ij} the matrix with one non-zero entry equal to 1 in the (i, j) place. We call a set $Y \subseteq \mathrm{C}_{G(R)}(U_\alpha)$ satisfying (11), resp. (12) a *witness set* for U_α.

In most cases, the verification that Y has the required properties is a relatively straightforward matrix calculation, which we omit. Of course it will suffice to consider just one root of each length.

The special linear group

The root subgroups in SL_n are

$$U_{ij} = 1 + \overline{k}e_{ij}, \quad i \neq j.$$

Lemma 8.2. *Let $G = \mathrm{SL}_n$, $n \geq 2$. Then a witness set for U_{12} is*

$$Y = \{1 + e_{pq} \mid p \neq 2,\, q \neq 1\}.$$

Symplectic groups and even orthogonal groups

Now we consider $C_m(\overline{k})$ and $D_m(\overline{k})$ as groups of $2m \times 2m$ matrices, as described in [12, §11.3]. Here $n = 2m$ and we re-label the matrix entries writing $-i$ in place of $m + i$ ($i = 1, \ldots, m$). For $1 \leq |i| < |j| \leq m$ set

$$\alpha_{ij} = e_{ij} + \varepsilon e_{-j,-i}, \tag{13}$$

where $\varepsilon = \pm 1$ depends on (i, j) in a manner to be specified.

We now separate cases.

Case 1: $G = C_m = \mathrm{Sp}_{2m}$. In this case, ε is -1 or 1 according as i and j have the same or opposite signs. The root subgroups in G are

$$\begin{aligned} U_i &= 1 + \overline{k}e_{i,-i} && \text{(long roots)}, && 1 \leq |i| \leq m, \\ U_{ij} &= 1 + \overline{k}\alpha_{ij} && \text{(short roots)}, && 1 \leq |i| < |j| \leq m, \end{aligned}$$

taking $\varepsilon = -1$ if $ij > 0$, and $\varepsilon = 1$ if $ij < 0$.

Lemma 8.3. *Let $G = \mathrm{Sp}_{2m}$. A witness set for the long root group U_1 is*

$$X_1 = \big\{1 + e_{i,-i} \mid i \notin \{-1, 2\}\big\} \cup \{1 + \alpha_{1j} \mid 2 \leq j \leq m\}$$

and a witness set for the short root group U_{12} is

$$X_2 = \{1 + e_{i,-i} \mid i \neq -1, 2\} \cup \{1 + \alpha_{1j} \mid j \neq \pm 1, -2\}.$$

Now let $v = 1 + r\alpha_{12} \in U_{12}$, $0 \neq r \in R$. To identify the subgroup $\mathrm{Z}(\mathrm{C}_{G(R)}(v))$ more precisely, set

$$\xi = (e_{1,-2} - e_{2,-1}) - (e_{-1,2} - e_{-2,1}) + \sum_{|i|>2} e_{ii}.$$

Then $\xi \in \mathrm{C}_{G(R)}(v)$. If $g \in ZUU_1U_2$ and g commutes with ξ we find that

$$g = \pm(1 + c\alpha_{12})(1 + ae_{1,-1})(1 - ae_{-2,2}) = \pm(1 + c\alpha_{12}) \cdot \varphi(a) \tag{14}$$

for some $a, c \in \overline{k}$, where $\varphi : \overline{k} \to U_1U_{-2}$ is the 'diagonal' homomorphism

$$r \mapsto 1 + r(e_{1,-1} - e_{-2,2}) = (1 + re_{1,-1})(1 - re_{-2,2}).$$

Now we can state

Proposition 8.4. *Let G and v be as above. Then*

$$\mathrm{Z}(\mathrm{C}_{G(R)}(v)) \leq \pm U_{12}(R)\cdot\varphi(R), \tag{15}$$

$$\mathrm{Z}(\mathrm{C}_{G(R)}(v)) = \pm U_{12}(R) \qquad \text{if } R^* \neq \{\pm 1\}, \tag{16}$$

$$\mathrm{Z}(\mathrm{C}_{G(R)}(v)) = \pm U_{12}(R)\cdot\varphi(R) \quad \text{if } R^* = \{\pm 1\} \text{ and } \mathrm{char}(R) \neq 2. \tag{17}$$

Proof. We have already established that $\mathrm{C}_G(\mathrm{C}_{G(R)}(v)) \leq \pm U_{12}\cdot\varphi(\overline{k})$. If g is given by (14), both c and a appear as entries in the matrix g, so if $g \in G(R)$ then $a, c \in R$ and (15) follows.

Suppose now that $R^* \neq \{\pm 1\}$ and pick $t \in R^*$ with $t^2 \neq 1$. The torus element

$$\tau := h_{1,-2}(t) = t(e_{11} + e_{22}) + t^{-1}(e_{-2,-2} + e_{-1,-1})$$

lies in $\mathrm{C}_{G(R)}(v)$. So if g in (14) is in $\mathrm{Z}(\mathrm{C}_{G(R)}(v))$ then τ commutes with $\varphi(a)$, and hence with $\varphi(a) - 1 = r(e_{1,-1} - e_{-2,2})$. But

$$\tau^{-1}\cdot r(e_{1,-1} - e_{-2,2})\cdot\tau = t^{-2}re_{1,-1} - t^2re_{-2,2},$$

so

$$t^{-2}r = t^2r = r,$$

hence $r = 0$ and we conclude that $g \in \pm U_{12}(R)$. This proves (16).

Assume now that $R^* = \{\pm 1\}$ and $\mathrm{char}(R) \neq 2$. To establish (17) it will suffice to show that $e_{1,-1} - e_{-2,2}$ commutes with every matrix in $\mathrm{C}_{G(R)}(v)$.

For clarity we take $n = 3$; the argument is valid for any $n \geq 2$. A matrix commuting with v is of the form

$$g = \begin{bmatrix} x & \bullet & \bullet & \bullet & -b & \bullet \\ 0 & x & 0 & b & 0 & 0 \\ 0 & \bullet & \bullet & \bullet & 0 & \bullet \\ 0 & a & 0 & y & 0 & 0 \\ -a & \bullet & \bullet & \bullet & y & \bullet \\ 0 & \bullet & \bullet & \bullet & 0 & \bullet \end{bmatrix},$$

where the blank entries are arbitrary. If g is symplectic then

$$2ax = 2by = 0, \quad xy + ab = 1.$$

It follows that *either* $x = 0$, in which case $ab = 1$, whence $a = \pm 1 = b$ and $y = 0$, *or* $x \neq 0$, in which case $a = 0$, $xy = 1$ and similarly then $x = \pm 1 = y$ and $b = 0$. Thus in any case $x = y$ and $a = b$. This now implies that g commutes with $e_{1,-1} - e_{-2,2}$. ∎

Remark. The precise nature of $\mathrm{Z}(\mathrm{C}_{G(R)}(v))$ in the remaining case where $R^* = 1$ and $\mathrm{char}(R) = 2$ we leave open.

Case 2: $G = D_m \leq \mathrm{O}_{2m}$. In this case, $\varepsilon = -1$ for all i, j. The root subgroups in G are

$$U_{ij} = 1 + \overline{k}\alpha_{ij}, \quad 1 \leq |i| < |j| \leq m.$$

Lemma 8.5. *Let $G = D_m \leq \mathrm{O}_{2m}$. A witness set for the root group U_{12} is*

$$X_3 = \{1 + \alpha_{ij} \mid (i, j) \in S\} \tag{18}$$

where

$$S = \{(i, j) \mid 3 \leq |i| < |j| \text{ or } i = 1 < |j|\} \cup \{(-1, 2)\}. \tag{19}$$

Remark. The same calculation actually establishes a little more:

$$\mathrm{C}_{\mathrm{O}_{2m}}(X_3) \subseteq \pm U_{12}. \tag{20}$$

This will be used below.

Odd orthogonal groups

Now we take $G = B_m \leq \mathrm{O}_{2m+1}$, and write elements of G as matrices

$$g = \begin{pmatrix} x & a \\ b^T & h \end{pmatrix} =: (x, a, b; h)$$

where $x = x(g) \in \overline{k}$, $a = a(g)$ and $b = b(g)$ are in $\overline{k}^{2m}$ and $h = h(g) \in M_{2m}(\overline{k})$. For $h \in M_{2m}(\overline{k})$ we write

$$h^* = (1, 0, 0; h).$$

The rows and columns are labelled $0, 1, \ldots, m, -1, \ldots, -m$.

We begin with a couple of elementary observations.

Lemma 8.6. *Let $g = (x, 0, 0; h)$. Then $g \in \mathrm{O}_{2m+1}(\overline{k})$ if and only if $h \in \mathrm{O}_{2m}(\overline{k})$ and $x = \pm 1$.*

Lemma 8.7. *Let $w \in M_{2m}(\overline{k})$. Then $g = g(x, a, b; h)$ commutes with w^* if and only if*

$$hw = wh, \quad aw = a, \quad bw^T = b.$$

The root elements are

$$\begin{aligned} u_i(r) &= 1 + r(2e_{i0} - e_{0,-i}) - r^2 e_{i,-i} && \text{(short roots)}, \quad 1 \leq |i| \leq m, \\ u_{ij}(r) &= 1 + r\alpha_{ij} && \text{(long roots)}, \quad 1 \leq |i| < |j| \leq m, \end{aligned}$$

where α_{ij} are as in (13) with $\varepsilon = -1$ for all pairs i, j.

Now let $r \neq 0$ and consider the long root element $v^* = u_{12}(r)$ (so v is the corresponding root element in D_m). We have

$$\mathrm{C}_G(v^*) \supseteq X_3^*$$

where X_3 is defined above in (18). Now Lemma 8.7 implies: if $g = g(x, a, b; h) \in \mathrm{Z}(\mathrm{C}_G(v^*))$ then $a\alpha_{ij}$ and $b\alpha_{ji}$ are zero for all pairs $(i, j) \in S$ (see (19)). This now implies that $a = b = 0$.

It follows by Lemma 8.6 that $x = \pm 1$ and $h \in \mathrm{O}_{2m}(\overline{k})$, and then by (20) that

$$h \in \pm U_{12}$$

(here U_{12} is the corresponding root group in D_m).

Thus

$$g = (\pm 1, 0, 0; \pm(1 + s\alpha_{12})) = \pm u_{12}(s) \cdot (\eta, 1, \ldots, 1)$$

for some $s \in \overline{k}$ and $\eta = \pm 1$.

Finally, we note that $u_1(1) \in \mathrm{C}_G(v^*)$. It follows that $(\eta, 1, \ldots, 1)$ commutes with $u_1(1)$, which forces $\eta = 1$. Thus $g = \pm u_{12}(s)$. We have established

Lemma 8.8. *Let $G = B_m \leq \mathrm{O}_{2m+1}$. A witness set for the long root group U_{12} is*

$$X_4 = X_3^* \cup \{u_1(1)\}.$$

Assume henceforth that $m \geq 3$. We consider finally the short root group U_1. We see that $\mathrm{C}_G(U_1)$ contains the set

$$X_5 = \{u_{ij}(1) \mid i \neq -1,\ j \neq 1\} \cup \{u_1(1)\}.$$

Now let $g = g(x, a, b; h) \in \mathrm{C}_G(X_5)$. One finds after some calculation that

$$g = (x, se_{-1}, 2e_1; x\mathbf{1}_{2m} + ye_{1,-1}).$$

(This calculation requires $m \geq 3$; the conclusion is false when $m = 2$.)

Then $\det(g) = x^{2m+1}$ so x is invertible; replacing s by $-x^{-1}s$ and y by $x^{-1}y$ we have

$$g = x(1, -se_{-1}, 2se_1; \mathbf{1}_{2m} + ye_{1,-1}). \tag{21}$$

Then

$$g \cdot u_1(-s) = x(\mathbf{1} + (s^2 + y)e_{1,-1}) \in \mathrm{O}_{2m+1},$$

which implies $x^2 = 1$ and $2(s^2 + y) = 0$.

If $\mathrm{char}(k) \neq 2$ we infer that $g = \pm u_1(s)$.

Suppose now that k has characteristic 2. In this case the mapping $\pi : g \mapsto h(g)$ is an injective homomorphism [12, p. 187]. If g is of the form (21) and $y = w^2$ then $g\pi = u_1(w)\pi \in U_1\pi$, and so $g \in U_1$.

Thus in any case we have $g \in \pm U_1$. We have established

Lemma 8.9. *Let $G = B_m \leq \mathrm{O}_{2m+1}$, where $m \geq 3$. Then a witness set for the short root group U_{12} is*

$$X_5 = \{u_{ij}(1) \mid i \neq -1,\ j \neq 1\} \cup \{u_1(1)\}.$$

9. Adelic groups

Let $\mathbb{A}$ denote the adèle ring of a global field K with $\mathrm{char}(K) \neq 2, 3, 5$. We consider subrings of $\mathbb{A}$ of the following kind:

$$A = \mathbb{A}, \quad A = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{o}_{\mathfrak{p}}$$

where $\mathfrak{o}$ is the ring of integers of K and $\mathcal{P}$ is a non-empty set of primes (or places) of K. Here we establish

Theorem 9.1. *The ring A is bi-interpretable with each of the groups* $\mathrm{SL}_2(A)$*,* $\mathrm{SL}_2(A)/\langle -1\rangle$*,* $\mathrm{PSL}_2(A)$*.*

Theorem 9.2. *Let G be a simple Chevalley–Demazure group scheme of rank at least* 2*. Then A is bi-interpretable with the group $G(A)$.*

For a rational prime p we write $A_p = \prod_{\mathfrak{p}\in\mathcal{P},\,\mathfrak{p}|p} \mathfrak{o}_{\mathfrak{p}}$.

Lemma 9.3. *A has a finite subset S such that every element of A is equal to one of the form*

$$\xi^2 - \eta^2 + s \tag{22}$$

with $\xi, \eta \in A^*$ and $s \in S$.

Proof. In any field of characteristic not 2 and size > 5, every element is the difference of two non-zero squares. It follows that the same is true for each of the rings $\mathfrak{o}_{\mathfrak{p}}$ with $N(\mathfrak{p}) > 5$ and odd.

If $N(\mathfrak{p})$ is 3 or 5 then every element of $\mathfrak{o}_{\mathfrak{p}}$ is of the form (22) with $\xi, \eta \in \mathfrak{o}_{\mathfrak{p}}^*$ and $s \in \{0, \pm 1\}$. If $\mathfrak{p}$ divides 2, the same holds if S is a set of representatives for the cosets of $4\mathfrak{p}$ in $\mathfrak{o}$.

Now by the Chinese Remainder Theorem (and Hensel's lemma) we can pick a finite subset S_1 of $A_2 \times A_3 \times A_5$ such that every element of $A_2 \times A_3 \times A_5$ is of the form (22) with $\xi, \eta \in \mathfrak{o}_{\mathfrak{p}}^*$ and $s \in S_1$. Finally, let S be the subset of elements $s \in A$ that project into S_1 and have $\mathfrak{o}_{\mathfrak{p}}$-component 1 for all $\mathfrak{p} \nmid 30$ (including infinite places if present). ∎

Remark. If $K = \mathbb{Q}$ one could choose $S \subset \mathbb{Z}$ (diagonally embedded in A). The plethora of parameters in the following argument can then be replaced by just three – $h(\tau)$, $u(1)$, $v(1)$ – or even two when $A = \mathbb{A}$, in which case we replace $h(\tau)$ by $h(2)$, which can be expressed in terms of $u(1)$ and $v(1)$ by the formula (27) below. Also the formula (26) can be replaced by the simpler one: $y_2 = u^x u^{-y} u^s \wedge y_3 = y_1^x y_1^{-y} y_1^s$.

For a finite subset T of $\mathbb{Z}$ let

$$A_T = \{r \in A \mid r_{\mathfrak{p}} \in T \text{ for every } \mathfrak{p}\}.$$

This is a definable set, since $r \in A_T$ if and only if $f(r) = 0$ where $f(X) = \prod_{t\in T}(X - t)$.

Choose S as in Lemma 9.3 with $0, 1 \in S$, and write $S^2 = S \cdot S$.

Let $\Gamma = \mathrm{SL}_2(A)/Z$ where Z is 1, $\langle -1\rangle$ or the centre of $\mathrm{SL}_2(A)$. For $\lambda \in A$ write

$$u(\lambda) = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \quad v(\lambda) = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}, \quad h(\lambda) = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \quad (\lambda \in A^*)$$

(matrices interpreted modulo Z; note that $\lambda \mapsto u(\lambda)$ is bijective for each choice of Z).

Fix $\tau \in A^*$ with $\tau_{\mathfrak{p}} = 2$ for $\mathfrak{p} \nmid 2$, $\tau_{\mathfrak{p}} = 3$ for $\mathfrak{p} \mid 2$. It is easy to verify that

$$\mathrm{C}_{\Gamma}(h(\tau)) = h(A^*) =: H. \tag{23}$$

Proposition 9.4. *The ring A is definable in Γ.*

Proof. We take $h := h(\tau)$ and $\{u(c) \mid c \in S^2\}$ as parameters, and put $u := u(1)$. 'Definable' will mean definable with these parameters. For $\lambda \in A$ and $\mu \in A^*$ we have

$$u(\lambda)^{h(\mu)} = u(\lambda\mu^2).$$

Now (23) shows that H is definable. If $\lambda = \xi^2 - \eta^2 + s$ and $x = h(\xi),\ y = h(\eta)$ then $u(\lambda) = u^x u^{-y} u(s)$; thus

$$U := u(A) = \bigcup_{s \in S} \{u^x u^{-y} u(s) \mid x, y \in H\}$$

is definable.

The map $u : A \to U$ is an isomorphism from $(A, +)$ to U. It becomes a ring isomorphism with multiplication $*$ if one defines

$$u(\beta) * u(\alpha) = u(\beta\alpha). \tag{24}$$

We need to provide an L_{gp} formula P such that for $y_1, y_2, y_3 \in U$,

$$y_1 * y_2 = y_3 \iff \Gamma \models P(y_1, y_2, y_3). \tag{25}$$

Say $\alpha = \xi^2 - \eta^2 + s$ and $\beta = \zeta^2 - \rho^2 + t$. Then

$$u(\beta\alpha) = u(\beta)^x u(\beta)^{-y} u(s)^z u(s)^{-r} u(st)$$

where $x = h(\xi),\ y = h(\eta),\ z = h(\zeta)$ and $r = h(\rho)$.

So we can take $P(y_1, y_2, y_3)$ to be a formula expressing the statement: there exist $x, y, z, r \in H$ such that for some $s, t \in S$,

$$y_1 = u^z u^{-r} u(t), \quad y_2 = u^x u^{-y} u(s), \quad y_3 = y_1^x y_1^{-y} u(s)^z u(s)^{-r} u(st). \tag{26}$$

■

Proposition 9.5. *The group Γ is interpretable in A.*

Proof. When $\Gamma = \mathrm{SL}_2(A)$, clearly Γ is definable as the set of 2×2 matrices with determinant 1 and group operation matrix multiplication. For the other cases, it suffices to note that the equivalence relation 'modulo Z' is definable by $B \sim C$ iff there exists $Z \in \{\pm 1_2\}$ with $C = BZ$, resp. $Z \in H$ with $Z^2 = 1$ and $C = BZ$. ■

To complete the proof of Theorem 9.1 it remains to establish **Step 1** and **Step 2** below.

We take $v = v(1)$ as another parameter, and set $w = uvu = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then $u(\lambda)^w = v(\lambda)$, so $V := v(A) = U^w$ is definable. Note the identity (for $\xi \in A^*$)

$$h(\xi) = v(\xi)u(\xi^{-1})v(\xi)w^{-1} = w^{-1}u(\xi)w \cdot u(\xi^{-1}) \cdot w^{-1}u(\xi). \tag{27}$$

Step 1: The ring isomorphism from A to $U \subset \mathrm{M}_2(A)$ is definable. Indeed, this is just the mapping

$$r \mapsto \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}.$$

Step 2: The map θ sending $g = (a, b; c, d)$ to $(u(a), u(b); u(c), u(d)) \in \Gamma^4$ is definable; this is a group isomorphism when U is identified with A via $u(\lambda) \mapsto \lambda$.

Assume for simplicity that $\Gamma = \mathrm{SL}_2(A)$. We start by showing that the restriction of θ to each of the subgroups $U,\ V\ ,\ H$ is definable. Recall that $u(0) = 1$ and $u(1) = u$.

If $g \in U$ then $g\theta = (u, g; 1, u)$. If $g = v(-\lambda) \in V$ then $g^{-w} = u(\lambda) \in U$ and $g\theta = (u, 1; g^{-w}, u)$.

Suppose $g = h(\xi) \in H$. Then $g = w^{-1}xwyw^{-1}x$ where $x = u(\xi)$, $y = u(\xi^{-1})$, and $g\theta = (y, 1; 1, x)$. So $g\theta = (y_1, y_2; y_3, y_4)$ if and only if

$$y_4 * y_1 = u, \quad y_2 = y_3 = 1, \quad g = w^{-1}y_4wy_1w^{-1}y_4.$$

Thus the restriction of θ to H is definable.

Next, set

$$W := \left\{x \in \Gamma \mid x_{\mathfrak{p}} \in \{1, w\} \text{ for every } \mathfrak{p}\right\}.$$

To see that W is definable, observe that an element x is in W if and only if there exist $y, z \in u(A_{\{0,1\}})$ such that

$$x = yz^w y \quad \text{and} \quad x^4 = 1.$$

Note that $u(A_{\{0,1\}})$ is definable by (the proof of) Proposition 9.4.

Put

$$\Gamma_1 = \{g \in \Gamma \mid g_{11} \in A^*\}.$$

If $g = (a, b; c, d) \in \Gamma_1$ then $g = \widetilde{v}(g)\widetilde{h}(g)\widetilde{u}(g)$ where

$$\begin{aligned} \widetilde{v}(g) &= v(-a^{-1}c) \in V, \\ \widetilde{h}(g) &= h(a^{-1}) \in H, \\ \widetilde{u}(g) &= u(a^{-1}b) \in U. \end{aligned}$$

This calculation shows that in fact $\Gamma_1 = VHU$, so Γ_1 is definable; these three functions on Γ_1 are definable since

$$\begin{aligned} x = \widetilde{v}(g) &\iff x \in V \cap HUg, \\ y = \widetilde{u}(g) &\iff y \in U \cap HVg, \\ z = \widetilde{h}(g) &\iff z \in H \cap VgU. \end{aligned}$$

Let $g = (a, b; c, d)$. Then $gw = (-b, a; -d, c)$. We claim that there exists $x \in W$ such that $gx \in \Gamma_1$. Indeed, this may be constructed as follows: If $a_{\mathfrak{p}} \in \mathfrak{o}_{\mathfrak{p}}^*$ take $x_{\mathfrak{p}} = 1$. If $a_{\mathfrak{p}} \in \mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$ and $b_{\mathfrak{p}} \in \mathfrak{o}_{\mathfrak{p}}^*$ take $x_{\mathfrak{p}} = w$. If both fail, take $x_{\mathfrak{p}} = 1$ when $a_{\mathfrak{p}} \neq 0$ and $x_{\mathfrak{p}} = w$

when $a_{\mathfrak{p}} = 0$ and $b_{\mathfrak{p}} \neq 0$. This covers all possibilities since for almost all $\mathfrak{p}$ at least one of $a_{\mathfrak{p}}, b_{\mathfrak{p}}$ is a unit in $\mathfrak{o}_{\mathfrak{p}}$, and $a_{\mathfrak{p}}, b_{\mathfrak{p}}$ are never both zero.

As $gx \in \Gamma_1$, we may write

$$gx = \widetilde{v}(gx)\widetilde{h}(gx)\widetilde{u}(gx).$$

We claim that the restriction of θ to W is definable. Let $x \in W$ and put $P = \{\mathfrak{p} \mid x_{\mathfrak{p}} = 1\}$, $Q = \{\mathfrak{p} \mid x_{\mathfrak{p}} = w\}$. Then $(u^x)_{\mathfrak{p}}$ is u for $\mathfrak{p} \in P$ and v for $\mathfrak{p} \in Q$, so $u^x \in \Gamma_1$ and

$$\widetilde{u}(u^x)_{\mathfrak{p}} = \begin{cases} u & (\mathfrak{p} \in P), \\ 1 & (\mathfrak{p} \in Q). \end{cases}$$

Recalling that $u = u(1)$ and $1 = u(0)$ we see that

$$x\theta = \begin{pmatrix} \widetilde{u}(u^x) & \widetilde{u}(u^x)^{-1}u \\ u^{-1}\widetilde{u}(u^x) & \widetilde{u}(u^x) \end{pmatrix}.$$

We can now deduce that θ is definable. Indeed, $g\theta = A$ holds if and only if there exists $x \in W$ such that $gx \in \Gamma_1$ and

$$A \cdot x\theta = \widetilde{v}(gx)\theta \cdot \widetilde{h}(gx)\theta \cdot \widetilde{u}(gx)\theta$$

(of course the products here are matrix products, definable in the language of Γ in view of Proposition 9.4).

This completes the proof of Theorem 9.1 for $\Gamma = \mathrm{SL}_2(A)$. When $\Gamma = \mathrm{SL}_2(A)/Z$, the same formulae now define θ as a map from Γ into the set of 2×2 matrices with entries in U modulo the appropriate definable equivalence relation. ■

Now we turn to the proof of Theorem 9.2. This largely follows §3, but is simpler because we are dealing here with 'nice' rings. Henceforth G denotes a simple Chevalley–Demazure group scheme of rank at least 2. The root subgroup associated to a root α is denoted U_α, and Z denotes the centre of G. Put $\Gamma = G(A)$.

Let S be any integral domain with infinitely many units. According to Theorem 1.6 we have

$$U_\alpha(S)Z(S) = \mathrm{Z}(C_{G(S)}(v))$$

whenever $1 \neq v \in U_\alpha(S)$. This holds in particular for the rings $S = \mathfrak{o}_{\mathfrak{p}}$. Take $u_\alpha \in U_\alpha(A)$ to have $\mathfrak{p}$-component $x_\alpha(1)$ for each $\mathfrak{p} \in \mathcal{P}$ (or every $\mathfrak{p}$ when $A = \mathbb{A}$); then

$$U_\alpha(A)Z(A) = \mathrm{Z}(C_{G(A)}(u_\alpha)).$$

Given this, the proof of Corollary 1.7 now shows that $U_\alpha(A)$ is a definable subgroup of Γ (the result is stated for integral domains but the argument remains valid, noting that in the present case $A/2A$ is finite).

Associated to each root α there is a morphism $\varphi_\alpha : \mathrm{SL}_2 \to G$ sending $u(r)$ to $x_\alpha(r)$ and $v(r)$ to $x_{-\alpha}(-r)$ (see [12, Chapter 6] or [34, Chapter 3]). This morphism is defined over $\mathbb{Z}$ and satisfies

$$K_\alpha := \mathrm{SL}_2(A)\varphi_\alpha \leq G(A).$$

Lemma 9.6. $K_\alpha = U_{-\alpha}(A)U_\alpha(A)U_{-\alpha}(A)U_\alpha(A)U_{-\alpha}(A)U_\alpha(A)U_{-\alpha}(A)U_\alpha(A)$.

Proof. This follows from the corresponding identity in $\mathrm{SL}_2(A)$, which in turn follows from (27) and the fact that $w = uvu$. ∎

We may thus infer that each K_α is a definable subgroup of $G(A)$. Fixing a root γ, we identify A with $U_\gamma(A)$ by $r \mapsto r' = x_\gamma(r)$. Proposition 9.4 now shows that A is definable in $G(A)$.

As above, $G(A)$ is A-definable as a set of $d \times d$ matrices that satisfy a family of polynomial equations over $\mathbb{Z}$, with group operation matrix multiplication.

To complete the proof of Theorem 9.2 we need to establish

Step 1′: The ring isomorphism $A \to U_\gamma(A)$, $r \mapsto r' = x_\gamma(r) \in \mathrm{M}_d(A)$, is definable in ring language. This follows from (8) in §3.

Step 2′: The group isomorphism $\theta : G(A) \to G(A') \subseteq \mathrm{M}_d(U_\gamma(A))$ is definable in group language.

To begin with, Lemma 3.5 shows that for each root α, the restriction of θ to $U_a(A)$ is definable (this is established for A an integral domain, but the proof is valid in general). Next, we observe that $G(A)$ has finite elementary width:

Lemma 9.7. *There is a finite sequence of roots β_i such that*

$$G(A) = \prod_{i=1}^{N} U_{\beta_i}(A).$$

Proof. This relies on results from [34, Chapter 8]. Specifically, [34, Cor. 2 to Thm. 18] asserts that if R is a PID, then (in the above notation) $G(R)$ is generated by the groups K_α. It is clear from the proof that each element of $G(R)$ is in fact a product of bounded length of elements from various of the K_α; an upper bound is given by the sum N_1, say, of the following numbers: the number of positive roots, the number of fundamental roots, and the maximal length of a Weyl group element as a product of fundamental reflections. If the positive roots are $\alpha_1, \ldots, \alpha_n$ and R is a PID it follows that

$$G(R) = \Big(\prod_{j=1}^{n} K_{\alpha_j}\Big) \ldots \Big(\prod_{j=1}^{n} K_{\alpha_j}\Big) \quad (N_1 \text{ factors}).$$

As each of the rings $\mathfrak{o}_\mathfrak{p}$ is a PID (or a field), the analogous statement holds with A in place of R.

The result now follows by Lemma 9.6, taking $N = 8nN_1$. ∎

Thus θ is definable as follows: for $g \in G(A)$ and $M \in \mathrm{M}_d(U_\gamma(A))$, $g\theta = M$ if and only if there exist $v_i \in U_{\beta_i}(A)$ and $M_i \in \mathrm{M}_d(U_\gamma(A))$ such that $g = v_1 \ldots v_N$, $M = M_1 \ldots M_N$ and $M_i = v_i\theta$ for each i. Here $M_1 \cdot M_2$ etc. denote matrix products, which are definable in the language of G because the ring operations on $A' = U_\gamma(A)$ are definable in G.

This completes the proof of Theorem 9.2. ∎

10. Appendix

We recall some commutator formulae ([12, Thms. 5.2.2 and 4.1.2], or [34, Chapter 3, Cor. to Lemma 15]). Here Φ is a root system and $\alpha, \beta \in \Phi$. If $\alpha + \beta \notin \Phi$ then $[x_\alpha(r), x_\beta(s)] = 1$. If $\alpha + \beta \in \Phi$ then α and β span a root system Φ_1 of rank 2 and there are three possibilities (assuming without loss of generality that α is short, if α and β are of different lengths). Here $\varepsilon = \pm 1$.

If $\Phi_1 = A_2$ then

$$\begin{aligned}[x_\alpha(r), x_\beta(s)] &= x_{\alpha+\beta}(\varepsilon rs),\\ [x_{-\alpha}(r), x_{\alpha+\beta}(s)] &= x_\beta(\varepsilon rs).\end{aligned}$$

If $\Phi_1 = B_2$ then

$$\begin{aligned}[x_\alpha(r), x_\beta(s)] &= x_{\alpha+\beta}(\varepsilon rs)x_{2\alpha+\beta}(\pm r^2 s),\\ [x_\alpha(r), x_{\alpha+\beta}(s)] &= x_{2\alpha+\beta}(\pm 2rs),\\ [x_{-\alpha}(r), x_{\alpha+\beta}(s)] &= x_\beta(\pm 2rs),\\ [x_{-\alpha}(r), x_{2\alpha+\beta}(s)] &= x_{\alpha+\beta}(\pm rs)x_\beta(\pm r^2 s),\\ [x_{\alpha+\beta}(r), x_{-\beta}(s),] &= x_\alpha(\varepsilon rs)x_{2\alpha+\beta}(\pm r^2 s).\end{aligned}$$

If $\Phi_1 = G_2$ then

$$\begin{aligned}[x_\beta(r), x_\alpha(s)] &= x_{\alpha+\beta}(\varepsilon rs)x_{2\alpha+\beta}(-\varepsilon rs^2)x_{3\alpha+\beta}(-rs^3)x_{3\alpha+2\beta}(\pm r^2 s^3),\\ [x_{\alpha+\beta}(r), x_a(s)] &= x_{2\alpha+\beta}(-2rs)x_{3\alpha+\beta}(-3\varepsilon rs^2)x_{3\alpha+2\beta}(\pm 3r^2 s),\\ [x_{2\alpha+\beta}(r), x_a(s)] &= x_{3\alpha+\beta}(3\varepsilon rs),\\ [x_{\alpha+\beta}(r), x_{-\beta}(s)] &= x_\alpha(-\varepsilon rs)x_{2\alpha+\beta}(\pm r^2 s)x_{3\alpha+2\beta}(\pm r^3 s)x_{3\alpha+\beta}(\pm r^3 s^2).\end{aligned}$$

(There are other possible combinations of signs, depending on the choice of Chevalley basis. We assume for convenience that the basis is chosen so as to obtain this particular form for the commutator formulae.)

Acknowledgments. We would like to thank Matthias Aschenbrenner, Brian Conrad, Jamshid Derakhshan, Philippe Gille, Bob Guralnick, Franziska Jahnke, Martin Liebeck, Evgeny Plotkin, Gopal Prasad, Donna Testermann, Nikolai Vavilov, Richard Weiss and Boris Zilber for their valuable input on various questions.

References

[1] Abe, E.: Chevalley groups over local rings. Tohoku Math. J. (2) **21**, 474–494 (1969) Zbl 0188.07201 MR 258837

[2] Ahlbrandt, G., Ziegler, M.: Quasi-finitely axiomatizable totally categorical theories. Ann. Pure Appl. Logic **30**, 63–82 (1986) Zbl 0592.03018 MR 831437

[3] Aschenbrenner, M., Khélif, A., Naziazeno, E., Scanlon, T.: The logical complexity of finitely generated commutative rings. Int. Math. Res. Notices **2020**, 112–166 Zbl 1476.03047 MR 4050565

[4] Aslaksen, H., Lang, M. L.: Extending π-systems to bases of root systems. J. Algebra **287**, 496–500 (2005) Zbl 1128.17007 MR 2134157

[5] Avni, N., Lubotzky, A., Meiri, C.: First order rigidity of non-uniform higher rank arithmetic groups. Invent. Math. **217**, 219–240 (2019) Zbl 1454.20001 MR 3958794

[6] Avni, N., Meiri, C.: On the model theory of higher-rank arithmetic groups. arXiv:2008.01793v2 (2020)

[7] Ax, J.: On the undecidability of power series fields. Proc. Amer. Math. Soc. **16**, 846 (1965) Zbl 0199.03003 MR 177890

[8] Behr, H.: 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**, 79–118 (1998) Zbl 0923.20038 MR 1603845

[9] Borel, A., Serre, J.-P.: Cohomologie d'immeubles et de groupes S-arithmétiques. Topology **15**, 211–232 (1976) Zbl 0338.20055 MR 447474

[10] Borel, A., Tits, J.: Homomorphismes "abstraits" de groupes algébriques simples. Ann. of Math. (2) **97**, 499–571 (1973) Zbl 0272.14013 MR 316587

[11] Bunina, E. I.: Isomorphisms and elementary equivalence of Chevalley groups over commutative rings. Sb. Math. **210**, 1067–1091 (2019) Zbl 1472.20110 MR 3985726

[12] Carter, R. W.: Simple Groups of Lie Type. Pure Appl. Math. 28, Wiley, London (1972) Zbl 0248.20015 MR 0407163

[13] Conrad, B.: Reductive group schemes. Notes for the SGA 3 Summer School (Luminy, 2011); http://math.stanford.edu/~conrad/papers/luminysga3.pdf

[14] D'Aquino, P., Macintyre, A. J., Otero, M.: Some model-theoretic perspectives on the structure sheaves of $\widehat{\mathbb{Z}}$ and the ring of finite adèles over $\mathbb{Q}$. arXiv:2002.06660 (2020)

[15] Demazure, M., Grothendieck, A. (eds.): Schémas en groupes. III. Lecture Notes in Math. 153, Springer, Berlin (1970) Zbl 0212.52810 MR 0274460

[16] Derakhshan, J.: Model theory of adeles and number theory. arXiv:2007.09237 (2020)

[17] Derakhshan, J., Macintyre, A.: Model theory of adeles I. Ann. Pure Appl. Logic **173**, art. 103074, 43 pp. (2022) Zbl 07458668 MR 4354273

[18] Dixon, J. D., du Sautoy, M. P. F., Mann, A., Segal, D.: Analytic Pro-p Groups. 2nd ed., Cambridge Stud. Adv. Math. 61, Cambridge Univ. Press, Cambridge (1999) Zbl 0934.20001 MR 1720368

[19] Hazrat, R., Stepanov, A., Vavilov, N., Zhang, Z.: Commutator width in Chevalley groups. Note Mat. **33**, 139–170 (2013) Zbl 1294.20059 MR 3071318

[20] Hodges, W.: Model Theory. Encyclopedia Math Appl. 42, Cambridge Univ. Press, Cambridge (1993) Zbl 0789.03031 MR 1221741

[21] Kramer, L., Röhrle, G., Tent, K.: Defining k in $G(k)$. J. Algebra **216**, 77–85 (1999) Zbl 0935.20031 MR 1694590

[22] Lawther, R., Testerman, D. M.: Centres of centralizers of unipotent elements in simple algebraic groups. Mem. Amer. Math. Soc. **210**, no. 988, vi+188 pp. (2011) Zbl 1266.20061 MR 2780340

[23] Lubotzky, A., Shalev, A.: On some Λ-analytic pro-p groups. Israel J. Math. **85**, 307–337 (1994) Zbl 0819.20030 MR 1264349

[24] Mal'tsev, A. I.: The elementary properties of linear groups. In: Certain Problems in Mathematics and Mechanics (In Honor of M. A. Lavrent'ev), Izdat. Sibirsk. Otdel. Akad. Nauk SSSR, Novosibirsk, 110–132 (1961) (in Russian); English transl. in: A. I. Maltsev: The Metamathematics of Algebraic Systems, Chapter XX, North-Holland, Amsterdam (1971) Zbl 0228.20013 MR 0265480

[25] van Maldeghem, H.: Generalized Polygons. Monogr. Math. 93, Birkhäuser, Basel (1998) Zbl 0914.51005 MR 1725957

[26] Myasnikov, A. G., Sohrabi, M.: Bi-interpretability with $\mathbb{Z}$ and models of the complete elementary theories of $\mathrm{SL}_n(O)$, $\mathrm{T}_n(O)$ and $\mathrm{GL}_n(O)$, $n \geq 3$. arXiv:2004.03585 (2020)

[27] Nies, A.: Separating classes of groups by first-order sentences. Internat. J. Algebra Comput. **13**, 287–302 (2003) Zbl 1059.20002 MR 2000873

[28] Nies, A., Segal, D., Tent, K.: Finite axiomatizability for profinite groups. Proc. London Math. Soc. (3) **123**, 597–635 (2021) Zbl 07492740 MR 4368683

[29] Pillay, A.: Geometric Stability Theory. Oxford Logic Guides 32, Clarendon Press, Oxford Univ. Press, New York (1996) Zbl 0871.03023 MR 1429864

[30] Sela, Z.: Diophantine geometry over groups. VII. The elementary theory of a hyperbolic group. Proc. London Math. Soc. (3) **99**, 217–273 (2009) Zbl 1241.20049 MR 2520356

[31] Sela, Z.: Diophantine geometry over groups X: the elementary theory of free products of groups. arXiv:1012.0044 (2010)

[32] Simion, I. I.: Double centralizers of unipotent elements in simple algebraic groups of type G_2, F_4 and E_6. J. Algebra **382**, 335–367 (2013) Zbl 1286.20062 MR 3034486

[33] Simion, I. I.: Double centralizers of unipotent elements in simple algebraic groups of type E_7 and E_8. J. Pure Appl. Algebra **219**, 930–977 (2015) Zbl 1306.20052 MR 3282118

[34] Steinberg, R.: Lectures on Chevalley Groups. Univ. Lecture Ser. 66, Amer. Math. Soc., Providence, RI (2016) Zbl 1361.20003 MR 3616493

[35] Stepanov, A.: Structure of Chevalley groups over rings via universal localization. J. Algebra **450**, 522–548 (2016) Zbl 1337.20057 MR 3449702

[36] Tavgen', O. I.: Bounded generability of Chevalley groups over rings of S-integer algebraic numbers. Izv. Akad. Nauk SSSR Ser. Mat. **54**, 97–122, 221–222 (1990) (in Russian) Zbl 0697.20032 MR 1044049

[37] Tits, J., Weiss, R. M.: Moufang Polygons. Springer Monogr. Math., Springer, Berlin (2002) Zbl 1010.20017 MR 1938841

[38] Trost, A. A.: Bounded generation by root elements for Chevalley groups defined over rings of integers of function fields with an application in strong boundedness. arXiv:2108.12254 (2021)

[39] Weil, A.: Basic Number Theory. Springer, Berlin (1967) Zbl 0176.33601 MR 0234930

[40] Zil'ber, B. I.: Some model theory of simple algebraic groups over algebraically closed fields. Colloq. Math. **48**, 173–180 (1984) Zbl 0567.20030 MR 758524