Defining $\mathbb{A}$ in $G(\mathbb{A})$

Dan Segal

July 23, 2020

It is shown in the papers [NST] and [ST] that for many integral domains $R$, the ring is bi-interpretable with various Chevalley groups $G(R)$. The model theory of adèle rings and some of their subrings has attracted some recent interest ([DM], [D], [AMO]), and it seemed worthwhile to extend the results in that direction.

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

$$R = \mathbb{A},$$

$$R = \prod_{p \in \mathcal{P}} \mathcal{O}_p$$

where $\mathcal{O}$ is the ring of integers of $K$ and $\mathcal{P}$ may be any non-empty set of primes (or places) of $K$. For example, $R$ could be the whole adèle ring of $\mathbb{Q}$, or $\hat{\mathbb{Z}} = \prod_{p \mid \mathcal{P}} \mathbb{Z}_p$.

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

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

The special cases where $R = \mathcal{O}_p$ were established in [NST], §4 and [ST].

For a rational prime $p$ we write $R_p = \prod_{p \in \mathcal{P}, p \mid p} \mathcal{O}_p$.

**Lemma 3** $R$ has a finite subset $S$ such that every element of $R$ is equal to one of the form

$$\xi^2 - \eta^2 + s$$

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

Now by the Chinese Remainder Theorem (and Hensel’s lemma) we can pick a finite subset $S_1$ of $R_3 \times R_3 \times R_3$ such that every element of $R_3 \times R_3 \times R_3$ is of the form (1) with $\xi, \eta \in \mathfrak{o}_p^*$ and $s \in S_1$. Finally, let $S$ be the subset of elements $s \in R$ that project into $S_1$ and have $\mathfrak{o}_p$-component 1 for all $p \mid 30$ (including infinite places if present).

**Remark** If $K = \mathbb{Q}$ one could choose $S \subset \mathbb{Z}$ (diagonally embedded in $R$). 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 $R = A$, 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 (5) below. Also the formula (5) can be replaced by the simpler one:

$$y_2 = u^x u_y u^s \land y_3 = y_1^x y_y^s y_1^s.$$ 

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

$$R_T = \{ r \in R \mid r_p \in T \text{ for every } p \}.$$ 

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

Choose $S$ as in Lemma 3 with 0, 1 $\in S$, and write $S^2 = S.S$.

Let $\Gamma = SL_2(R)/Z$ where $Z$ is 1, $\langle -1 \rangle$ or the centre of SL$_2(R)$. For $\lambda \in R$ write

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

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

Fix $\tau \in R^*$ with $\tau_p = 2$ for $p \nmid 2$, $\tau_p = 3$ for $p \mid 2$. It is easy to verify that

$$C_{\tau}(h(\tau)) = h(R^*) := H. \quad (2)$$

**Proposition 4** The ring $R$ is definable in $\Gamma$.

**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 $\lambda \in R$ and $\mu \in R^*$ we have

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

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

$$u(\lambda) = u^x u^{-y} u(s).$$

It follows that

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

2
is definable.

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

\[
u(\beta) * u(\alpha) = u(\beta \alpha).
\] (3)

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

\[
y_1 * y_2 = y_3 \iff \Gamma \models P(y_1, y_2, y_3).
\] (4)

Say \( \alpha = \xi^2 - \eta^2 + s \), \( \beta = \zeta^2 - \rho^2 + t \). Then

\[
u(\beta \alpha) = u(\beta)^{xy} u(\beta)^{-y} u(s)^{zt} u(s)^{-t} u(st)
\]

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 \( s, t \in S \)

\[
y_1 = u^x u^{-r} u(t), \quad y_2 = u^y u^{-y} u(s),
\]

\[
y_3 = y_1^x y_2^y u(s)^{zt} u(s)^{-t} u(st).
\] (5)

\[\]

**Proposition 5** The group \( \Gamma \) is interpretable in \( R \).

**Proof.** When \( \Gamma = \text{SL}_2(R) \), clearly \( \Gamma \) is definable as the set of \( 2 \times 2 \) 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 \( A \sim B \) iff there exists \( Z \in \{ \pm 1_2 \} \) with \( B = AZ \), resp. \( Z \in H \) with \( Z^2 = 1 \) and \( B = AZ \). □

To complete the proof of Theorem \( \square \) it remains to establish **Step 1** and **Step 2** below.

We take \( v = v(1) \) as another parameter, and set \( w = uvu = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \).

Then \( u(\lambda)^w = v(\lambda) \), so \( V := v(R) = U^w \) is definable. Note the identity (for \( \xi \in R^* \)):

\[
h(\xi) = v(\xi) u(\xi^{-1}) v(\xi) w^{-1} = w^{-1} u(\xi) w. u(\xi^{-1}) w^{-1} u(\xi).
\] (6)

**Step 1:** The ring isomorphism from \( R \) to \( U \subset M_2(R) \) is definable. Indeed, this is just the mapping

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

**Step 2:** The map \( \theta \) 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 \( R \) via \( u(\lambda) \mapsto \lambda \).
Assume for simplicity that $\Gamma = \text{SL}_2(R)$. We start by showing that the restriction of $\theta$ 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

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

Thus the restriction of $\theta$ to $H$ is definable.

Next, set $W := \{x \in \Gamma \mid x_p \in \{1,w\} \text{ for every } p \}$. To see that $W$ is definable, observe that an element $x$ is in $W$ if and only if there exist $y, z \in u(R_{(0,1)})$ such that

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

Note that $u(R_{(0,1)})$ is definable by (the proof of) Proposition 3.

Put

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

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

$$\tilde{v}(g) = v(-a^{-1}c) \in V$$

$$\tilde{h}(g) = h(a^{-1}) \in H$$

$$\tilde{u}(g) = u(a^{-1}b) \in U.$$ 

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

$$x = \tilde{v}(g) \iff x \in V \cap HUG$$

$$y = \tilde{u}(g) \iff y \in U \cap HVG$$

$$z = \tilde{h}(g) \iff z \in H \cap VGU.$$

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 $a_p \in \mathfrak{g}_p^*$ take $x_p = 1$. If $a_p \in p\mathfrak{g}_p$ and $b_p \in \mathfrak{g}_p^*$ take $x_p = w$. If both fail, take $x_p = 1$ when $a_p \neq 0$ and $x_p = w$ when $a_p = 0$ and $b_p \neq 0$. This covers all possibilities since for almost all $p$ at least one of $a_p$, $b_p$ is a unit in $\mathfrak{g}_p$, and $a_p$, $b_p$ are never both zero.

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

$$gx = \tilde{v}(gx)\tilde{h}(gx)\tilde{u}(gx).$$
We claim that the restriction of $\theta$ to $W$ is definable. Let $x \in W$ and put $P = \{p \mid x_p = 1\}$, $Q = \{p \mid x_p = w\}$. Then $(u^x)_p$ is $u$ for $p \in P$ and $v$ for $p \in Q$, so $u^x \in \Gamma_1$ and

$$\tilde{u}(u^x)_p = \begin{cases} u & (p \in P) \\ 1 & (p \in Q) \end{cases}.$$ 

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

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

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

$$A.x\theta = \tilde{v}(gx)\theta.$$

(of course the products here are matrix products, definable in the language of $\Gamma$ in view of Proposition 4).

This completes the proof of Theorem 1 for $\Gamma = \text{SL}_2(R)$. When $\Gamma = \text{SL}_2(R)/Z$, the same formulae now define $\theta$ as a map from $\Gamma$ into the set of $2 \times 2$ matrices with entries in $U$ modulo the appropriate definable equivalence relation. ■

Now we turn to the proof of Theorem 2. This largely follows [ST], §§3, 4, 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 $\alpha$ is denoted $U_\alpha$, and $Z$ denotes the centre of $G$. Put $\Gamma = G(R)$.

Let $S$ be any integral domain with infinitely many units. According to [ST], Theorem 1.5 we have

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

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

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

Given this, the proof of Corollary 1.6 of [ST] now shows that $U_\alpha(R)$ is a definable subgroup of $\Gamma$; the result is stated for integral domains but the argument remains valid, noting that in the present case $R/2R$ is finite.

Associated to each root $\alpha$ there is a morphism $\varphi_\alpha : \text{SL}_2 \to G$ sending $u(r) = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$ to $x_\alpha(r)$ and $v(r) = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$ to $x_{-\alpha}(r)$ ([S], Chapter 3). This morphism is defined over $\mathbb{Z}$ and satisfies

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

**Lemma 6** $K_\alpha = U_{-\alpha}(R)U_{\alpha}(R)U_{-\alpha}(R)U_{\alpha}(R)U_{-\alpha}(R)U_{\alpha}(R)U_{-\alpha}(R)U_{\alpha}(R)$. 

5
Proof. This follows from the corresponding identity in SL₂(R), which in turn follows from (6) and the fact that \( w = uuw \). ■

We may thus infer that each \( K_\alpha \) is a definable subgroup of \( G(R) \). Fixing a root \( \gamma \), we identify \( R \) with \( U_\gamma(R) \) by \( r \mapsto r' = x_\gamma(r) \). Proposition 4 now shows that \( R \) is definable in \( G(R) \).

As above, \( G(R) \) is \( R \)-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 we need to establish

1. The ring isomorphism \( R \to U_\gamma(R); r \mapsto x_\gamma(r) \in M_d(R) \) is definable in ring language. This follows from the definition \( x_\gamma(r) = \exp(rX_\gamma) = 1 + rM_1(\gamma) + \ldots + r^qM_q(\gamma) \) where each \( M_i(\gamma) \) is a matrix with integer entries ([S], Chaps. 2, 3).

2. The group isomorphism \( \theta: G(R) \to G(R') \subseteq M_d(U_\gamma(R)) \) is definable in group language.

To begin with, Lemma 3.5 of [ST] shows that for each root \( \alpha \), the restriction of \( \theta \) to \( U_\alpha(R) \) is definable (this is established for \( R \) an integral domain, but the proof is valid in general). Next, we observe that \( G(R) \) has ‘finite elementary width’ in the sense of [ST]:

**Lemma 7** There is a finite sequence of roots \( \beta_i \) such that

\[
G(R) = \prod_{i=1}^{N} U_{\beta_i}(R).
\]

**Proof.** This relies on results from Chapter 7 of [S]. Specifically, Corollary 2 to Theorem 18 asserts that if \( R \) is a PID, then (in the above notation) \( G(R) \) is generated by the groups \( K_\alpha \). 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 \( K_\alpha \); 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 \( \alpha_1, \ldots, \alpha_n \) it follows (if \( R \) is a PID) that

\[
G(R) = \left( \prod_{j=1}^{n} K_{\alpha_j} \right) \cdot \left( \prod_{j=1}^{n} K_{\alpha_j} \right) \cdots \left( \prod_{j=1}^{n} K_{\alpha_j} \right) \quad (N_1 \text{ factors}).
\]

As each of the rings \( \mathfrak{a}_p \) is a PID (or a field), the same holds for our ring \( R \) in general.

The result now follows by Lemma 6, taking \( N = 8nN_1 \). ■

Thus \( \theta \) is definable as follows: for \( g \in G(R) \) and \( A \in M_d(U_\gamma(R)) \), \( g\theta = A \) if and only if there exist \( v_i \in U_{\beta_i}(R) \) and \( A_i \in M_d(U_\gamma(R)) \) such that \( g = v_1 \ldots v_N \).
\( A = A_1 \cdots A_N \) and \( A_i = v_i \theta \) for each \( i \). Here \( A_1 \cdot A_2 \) etc denote matrix products, which are definable in the language of \( G \) because the ring operations on \( R' = U_n(R) \) are definable in \( G \).

This completes the proof.

Acknowledgment. Thanks to Jamshid Derakhshan for references and advice.

References

[AMO] P. D’Aquino, A. J. Macintyre and M. Otero, Some model-theoretic perspectives on the structure sheaves of \( \hat{\mathbb{Z}} \) and the ring of finite adèles over \( \mathbb{Q} \), arXiv: 2002.06660 [math. AC]

[D] J. Derakhshan, Model theory of adèles and number theory, arXiv:2007.09237 [math.LO], 2020

[DM] J. Derakhshan and A. Macintyre, Model theory of adèles I, arXiv: 1603.09698 [math.LO]

[NST] A. Nies, D. Segal and K. Tent, Finite axiomatizability for profinite groups, arXiv:1907.02262v4 [math.GR], 2020

[ST] D. Segal and K. Tent, Defining \( R \) and \( G(R) \), arXiv:2004.13407v3 [math.GR], 2020

[S] R. Steinberg, Lectures on Chevalley groups, A. M. S. University Lecture Series 66, 2016.