Defining $\mathbb{A}$ in SL_2

Dan Segal

July 8, 2020

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:

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

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 R could be $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, or the whole adèle ring of $\mathbb{Q}$.

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

The special case $R = \mathfrak{o}_{\mathfrak{p}}$ is established in [NST], §4.

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

Lemma 2 *R has a finite subset S such that every element of R is equal to one of the form*

$$\xi^2 - \eta^2 + s \tag{1}$$

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 $\mathfrak{o}_{\mathfrak{p}}$ 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 (1) 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 $R_2 \times R_3 \times R_5$ such that every element of $R_2 \times R_3 \times R_5$ is of the form (1) with $\xi, \eta \in \mathfrak{o}_{\mathfrak{p}}^*$ and $s \in S_1$. Finally, let S be the subset of elements $s \in R$ that project into S_1 and have $\mathfrak{o}_{\mathfrak{p}}$-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 R). The plethora of parameters in the argument below can then be replaced by just three - $h(\tau),\ u(1),\ v(1)$ - or even two when $R = \mathbb{A}$, in which case we replace $h(\tau)$ by $h(2)$, which can be expressed in terms of $u(1)$ and $v(1)$ by (6). The formula (5) is also cleaner: $y_2 = u^x u^{-y} u^s \wedge y_3 = y_1^x y_1^{-y} y_1^s$.

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

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

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 2, with $0,\ 1 \in S$, and write $S^2 = S.S$.

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

write

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

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

Fix $\tau \in R^*$ 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

$$\mathrm{C}_G(h(\tau)) = h(R^*) := H. \tag{2}$$

Proposition 3 *The ring R is definable in G.*

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

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

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

$$u(\beta) * u(\alpha) = u(\beta\alpha). \tag{3}$$

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

$$y_1 * y_2 = y_3 \Longleftrightarrow G \models P(y_1, y_2, y_3). \tag{4}$$

Say $\alpha = \xi^2 - \eta^2 + s$, $\beta = \zeta^2 - \rho^2 + t$. 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 $s, t \in S$

$$\begin{aligned} &y_1 = u^z u^{-r} u(t),\ y_2 = u^x u^{-y} u(s), \\ &y_3 = y_1^x y_1^{-y} u(s)^z u(s)^{-r} u(st). \end{aligned} \tag{5}$$

■

Proposition 4 *The group G is interpretable in R.*

Proof. When $G = \mathrm{SL}_2(R)$, clearly G 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 $A \sim B$ iff there exists $Z \in \{\pm 1_2\}$ with $B = AZ$, resp. $Z \in H$ with $Z^2 = 1$ and $B = AZ$. ■

Theorem 5 *The ring R is bi-interpretable with the group G.*

Proof. 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 $\xi \in R^*$):

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

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

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

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

Assume for simplicity that $G = \mathrm{SL}_2(R)$. 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

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

Thus the restriction of θ to H is definable.

Next, set

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

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

$$G_1 = \{g \in G \mid g_{11} \in R^*\}.$$

If $g = (a, b; c, d) \in G_1$ 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 $G_1 = VHU$, so G_1 is definable; these three functions on G_1 are definable since

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

Let $g = (a, b; c, d)$. Then $gw = (-b, a; -d, c)$. We claim that there exists $x \in W$ such that $gx \in G_1$. 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 $gx \in G_1$, 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 $u^x \in G_1$ 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 $gx \in G_1$ and

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

(of course the products here are matrix products, definable in the language of G in view of Proposition 3).

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

References

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