



On the rational symplectic group

Yves Benoist

► To cite this version:

| Yves Benoist. On the rational symplectic group. 2023. hal-03744454v5

HAL Id: hal-03744454

<https://hal.science/hal-03744454v5>

Preprint submitted on 13 Jan 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

On the rational symplectic group

Yves Benoist

Abstract

We give a short proof of an elementary classical result: any rational symplectic matrix can be put in diagonal form after right and left multiplication by integral symplectic matrices. We also give a new proof for its extension to Chevalley groups due to Steinberg by using the Cartan-Bruhat-Tits decomposition over p -adic fields.

1 Introduction

In this expository paper I present a short proof of a classical theorem I needed in [1]: a decomposition of the group $\mathrm{Sp}(n, \mathbb{Q})$ of symplectic matrices with rational coefficients that gives a parametrization of the double quotient $\mathrm{Sp}(n, \mathbb{Z}) \backslash \mathrm{Sp}(n, \mathbb{Q}) / \mathrm{Sp}(n, \mathbb{Z})$ where $\mathrm{Sp}(n, \mathbb{Z})$ is the subgroup of symplectic matrices with integral coefficients.

This decomposition which can already be found in [15] is a symplectic version of the “adapted basis theorem” for $\mathbb{Z}$ -modules, or of the “Smith normal form” for integral matrices.

In Section 2 we state precisely this decomposition that we call the “symplectic Smith normal form”.

In Section 3 we explain the analogy with the Cartan-Bruhat-Tits decomposition.

In Section 4 we recall the relevance of Bruhat-Tits buildings in this kind of decomposition.

2020 Math. subject class. Primary 20G30 ; Secondary 11E57

Key words Symplectic group, Cartan decomposition, Smith normal form.

In Section 5 we give an elementary proof of the symplectic Smith normal form.

In Section 6 we give a non-elementary proof of the symplectic Smith normal form that will be applied to other simply-connected split semisimple algebraic groups $\mathbf{G}$ defined over $\mathbb{Q}$ in the last section. Indeed we explain how this symplectic Smith normal form can be deduced from the Cartan-Bruhat-Tits decomposition together with the strong approximation theorem.

In Section 7 we explain the extension due to Steinberg of the Smith normal form to the simply-connected $\mathbb{Q}$ -split groups, see Theorem 7.1.

The last two sections are a concrete illustration of a classical strategy: if you want to prove a theorem over a global field, prove it first over local fields and then use a local-global principle.

I would like to thank Hee Oh for a very helpful comment on a first draft of this note.

2 The symplectic Smith normal form

For any commutative ring R with unity, we denote by $\mathrm{Sp}(n, R)$ the symplectic group with coefficients in R . This group is the stabilizer of the symplectic form ω on R^{2n} given by, for all x, y in R^{2n} ,

$$\omega(x, y) = {}^t x J y$$

where $J = \begin{pmatrix} \mathbf{0} & \mathbf{1}_n \\ -\mathbf{1}_n & \mathbf{0} \end{pmatrix}$. Equivalently, one has

$$\mathrm{Sp}(n, R) := \{g \in \mathrm{GL}(2n, R) \mid {}^t g J g = J\},$$

If we write the elements of the symplectic group as block matrices with blocks of size n , one has

$$\mathrm{Sp}(n, R) = \left\{ g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid {}^t \alpha \gamma = {}^t \gamma \alpha, {}^t \beta \delta = {}^t \delta \beta, {}^t \alpha \delta - {}^t \gamma \beta = \mathbf{1}_n \right\}.$$

Theorem 2.1. *Let $g \in \mathrm{Sp}(n, \mathbb{Q})$. Then there exist two matrices σ and σ' in $\mathrm{Sp}(n, \mathbb{Z})$ and a positive integral diagonal matrix $\mathbf{d} = \mathrm{diag}(d_1, \dots, d_n)$ with $d_1 | d_2 | \dots | d_n$, and such that*

$$g = \sigma \begin{pmatrix} \mathbf{d} & \mathbf{0} \\ \mathbf{0} & \mathbf{d}^{-1} \end{pmatrix} \sigma'.$$

The condition that the coefficients d_j are positive integers with d_1 dividing d_2 , with d_2 dividing d_3 , $\dots$, and d_{n-1} dividing d_n ensures that the diagonal matrix $\mathbf{d}$ is unique.

I use this precise Theorem 2.1 as a key tool for an apparently completely unrelated problem in my paper [1]. This problem is the construction of functions f on the cyclic group $\mathbb{Z}/d\mathbb{Z}$ of odd order whose convolution square is proportional to their square. Indeed the construction relies on an auxiliary abelian variety endowed with a unitary $\mathbb{Q}$ -endomorphism ν , the symplectic form ω shows up as a polarization of the abelian variety, and the rational symplectic matrix g shows up as the “holonomy” of ν .

The first reference to Theorem 2.1 that I know is Shimura’s paper [15, Prop. 1.6]. Moreover in [16], Shimura points out the relevance of this theorem to show the commutativity of a Hecke algebra and hence to better understand the modular forms on Siegel upper halfspace. This theorem is also in [9, p.232] and is also used by Clozel, Oh and Ullmo in [8, p.23].

As we have seen, there is a version of Theorem 2.1 for the linear group $\mathrm{SL}(n, \mathbb{Q})$, see for instance Proposition 5.1. More generally, there is also a version of Theorem 2.1 for any simply-connected split semisimple algebraic group $\mathbf{G}$ defined over $\mathbb{Q}$, if one chooses suitably the $\mathbb{Z}$ -form, see Section 7.

3 The symplectic group over local fields

Before going on I would like to emphasize the analogy of this theorem with two classical theorems. These two classical theorems are valid for all algebraic semisimple groups G and are due respectively to E. Cartan and to F. Bruhat and J. Tits. I will not quote here their general formulation that can be found respectively in [12] and in [5] but only the special case where G is the symplectic group.

The first theorem is a decomposition theorem over the real field $\mathbb{R}$ due to E. Cartan which is called either the “polar decomposition” or the “Cartan decomposition”. We set

$$\begin{aligned} \mathrm{SO}(2n) &:= \{g \in \mathrm{GL}(2n, \mathbb{R}) \mid {}^t g g = \mathbf{1}_{2n}\} \text{ and} \\ \mathrm{Sp}(n) &:= \mathrm{Sp}(n, \mathbb{R}) \cap \mathrm{SO}(2n). \end{aligned}$$

Note that the group $\mathrm{Sp}(n)$ is a maximal compact subgroup of the group $\mathrm{Sp}(n, \mathbb{R})$.

Theorem 3.1. (Cartan) *Let $g \in \mathrm{Sp}(n, \mathbb{R})$. Then there exist two matrices σ and σ' in $\mathrm{Sp}(n)$ and a positive real diagonal matrix $\mathbf{d} = \mathrm{diag}(d_1, \dots, d_n)$ with $d_1 \leq d_2 \leq \dots \leq d_n \leq 1$ such that*

$$g = \sigma \begin{pmatrix} \mathbf{d} & \mathbf{0} \\ \mathbf{0} & \mathbf{d}^{-1} \end{pmatrix} \sigma'.$$

The second theorem is a decomposition theorem over a local non archimedean field k due to F. Bruhat and J. Tits. We denote by $\mathcal{O}_k$ the ring of integers of k and choose a uniformizer π in k , i.e. a generator of the maximal ideal of $\mathcal{O}_k$.

Note again that the group $\mathrm{Sp}(n, \mathcal{O}_k)$ is a maximal compact subgroup of the group $\mathrm{Sp}(n, k)$.

Theorem 3.2. (Bruhat, Tits) *Let $g \in \mathrm{Sp}(n, k)$. Then there exist two matrices σ and σ' in $\mathrm{Sp}(n, \mathcal{O}_k)$ and a diagonal matrix $\mathbf{d} = \mathrm{diag}(\pi^{p_1}, \dots, \pi^{p_n})$ with $p_1 \geq p_2 \geq \dots \geq p_n \geq 0$ integers such that*

$$g = \sigma \begin{pmatrix} \mathbf{d} & \mathbf{0} \\ \mathbf{0} & \mathbf{d}^{-1} \end{pmatrix} \sigma'.$$

The analogy between these three theorems is striking. It extends the analogy between the Smith normal form of an integral matrix and the singular value decomposition of a real matrix.

In this analogy *the group of integers points of a group defined over the rational* should be handled as *the maximal compact subgroup of a group defined over the real*. This rough analogy is an equality when dealing with non archimedean local field. Indeed, when k is a non-archimedean local field, the group of integer points is an open compact subgroup.

4 Bruhat-Tits buildings

F. Bruhat and J. Tits have described the analog of the Cartan decomposition for semisimple groups over non-archimedean local fields, in [4], [5], [6] and [7], by introducing new geometric spaces that are nowadays called Bruhat-Tits buildings and that extend the space of p -adic norms studied by Goldman and Iwahori in [10].

As explained in the book [13], these Bruhat-Tits buildings are very useful.

One of the reason is that they are $K(\pi, 1)$ -spaces for the lattices in semisimple p -adic groups.

Another reason is that they played the role of a model to follow in order to understand other finitely generated groups, like Coxeter groups, Artin groups, Baumslag-Solitar groups or Mapping class groups.

The relevance of the Bruhat-Tits buildings became even clearer to me when I used them with Hee Oh to prove a general polar decomposition for p -adic symmetric spaces in [2]. This polar decomposition was a key ingredient in our proof of equidistribution of S -integral points on rational symmetric spaces in [3].

5 The symplectic adapted basis

In this section we come back to elementary consideration and we discuss the structure of the *rational symplectic group* $\mathrm{Sp}(n, \mathbb{Q})$, and its relation with the *integral symplectic group* $\mathrm{Sp}(n, \mathbb{Z})$.

We first recall the well-known undergraduate “adapted basis theorem” for $\mathbb{Z}$ -module or, equivalently, the “Smith normal form” for integral matrices. We denote by $\mathcal{M}(n, \mathbb{Z})$ the ring of $n \times n$ integral matrices.

Proposition 5.1. (Smith) *Let $g \in \mathcal{M}(n, \mathbb{Z})$. Then there exist σ and σ' in $\mathrm{SL}(n, \mathbb{Z})$ and an integral diagonal matrix $\mathbf{a} = \mathrm{diag}(a_1, \dots, a_n)$ with $a_1 | a_2 | \dots | a_n$, and such that*

$$g = \sigma \mathbf{a} \sigma'.$$

Theorem 2.1 follows from the following proposition which is a variation of the “adapted basis theorem” which takes into account the existence of a symplectic form. We introduce the set $\mathcal{Mp}(n, \mathbb{Z})$ of nonzero integral matrices which are proportional to elements of $\mathrm{Sp}(n, \mathbb{R})$,

$$\mathcal{Mp}(n, \mathbb{Z}) := \{g \in \mathcal{M}(2n, \mathbb{Z}) \mid {}^t g J g = \lambda^2 J \text{ for some } \lambda \text{ in } \mathbb{R}^*\}.$$

Proposition 5.2. *Let $g \in \mathcal{Mp}(n, \mathbb{Z})$. Then there exist two matrices σ and σ' in $\mathrm{Sp}(n, \mathbb{Z})$ and a positive integral diagonal matrix $\mathbf{a} = \mathrm{diag}(a_1, \dots, a_{2n})$ with $a_1 | a_2 | \dots | a_n$, with $a_n | a_{2n}$ and such that*

$$g = \sigma \mathbf{a} \sigma'.$$

Note that the matrix $\mathbf{a}$ is also in $\mathcal{Mp}(n, \mathbb{Z})$ and hence the products $a_j a_{n+j}$ do not depend on the positive integer $j \leq n$. Indeed it is equal to λ^2 . In particular, one has $a_{2n}|a_{2n-1}|\dots|a_{n+1}$.

For the proof of Proposition 5.2, we need the following lemma. We recall that a nonzero vector v of $\mathbb{Z}^k$ is primitive if it spans the $\mathbb{Z}$ -module $\mathbb{R}v \cap \mathbb{Z}^k$.

Lemma 5.3. *The group $\mathrm{Sp}(n, \mathbb{Z})$ acts transitively on the set of primitive vectors in $\mathbb{Z}^{2n}$.*

Denote by $e_1, \dots, e_n, f_1, \dots, f_n$ the canonical basis of $\mathbb{Z}^{2n}$ so that our symplectic form is $\omega = e_1^* \wedge f_1^* + \dots + e_n^* \wedge f_n^*$.

Proof of Lemma 5.3. Let $v = (x_1, \dots, x_{2n})$ be a primitive vector in $\mathbb{Z}^{2n}$. We want to find $\sigma \in \mathrm{Sp}(n, \mathbb{Z})$ such that $\sigma v = e_1$.

This is true for $n = 1$. Using the subgroups $\mathrm{Sp}(1, \mathbb{Z})$ for the planes $\mathbb{Z}e_j \oplus \mathbb{Z}f_j$, with $j = 1, \dots, n$, we can assume that

$$x_{n+1} = \dots = x_{2n} = 0.$$

In this case the vector $(x_1, \dots, x_n)$ is primitive in $\mathbb{Z}^n$.

Since $\mathrm{SL}(n, \mathbb{Z})$ acts transitively on the set of primitive vectors in $\mathbb{Z}^n$, we can find a block diagonal matrix $\sigma = \mathrm{diag}(\sigma_0, {}^t\sigma_0^{-1})$, with $\sigma_0 \in \mathrm{SL}(n, \mathbb{Z})$ such that $\sigma v = e_1$. This matrix σ belongs to $\mathrm{Sp}(n, \mathbb{Z})$. $\square$

Proof of Proposition 5.2. Set $\Gamma := \mathrm{Sp}(n, \mathbb{Z})$. The proof is by induction on n . It relies on a succession of steps, in the spirit of the Smith normal form, in which one multiplies on the right or on the left the matrix g by an “elementary” matrix to obtain a simpler matrix $g' \in \Gamma g \Gamma$. We have to pay attention that at each step the elementary matrix is symplectic.

We can assume that the gcd of the coefficients of g is equal to 1. We denote by λ the positive real factor such that g/λ belongs to $\mathrm{Sp}(n, \mathbb{R})$. Note that λ^2 is a positive integer. At the end of the proof we will see that $a_1 = 1$ and $a_{n+1} = \lambda^2$.

1st step: *We find $g' \in \Gamma g \Gamma$ such that $g'e_1 = e_1$.*

Since the coefficients of the integral matrix g are relatively prime, by Proposition 5.1, there exists a primitive vector v in $\mathbb{Z}^{2n}$ such that gv is also primitive. According to lemma 5.3, there exists σ, σ' in Γ such that $\sigma gv = e_1$ and $\sigma'e_1 = v$. Then the matrix $g' := \sigma g \sigma'$ satisfies $g'e_1 = e_1$.

2nd step: We find $g' \in \Gamma g \Gamma$ with $g'e_1 = e_1$ and $\omega(g'e_j, f_1) = 0$ for $j > 1$.

By the first step, we can assume that

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \text{ with } \alpha e_1 = e_1 \text{ and } \gamma e_1 = 0$$

In particular the first column of the integral matrix α is $(1, 0, \dots, 0)$. We would like the first row of α to be also of the form $(1, 0, \dots, 0)$. For that we choose $g' = g\sigma'$ where σ' is the symplectic transformation

$$\sigma' = \mathbf{1}_n + \sum_{1 < j \leq n} \alpha_{1,j} (f_j \otimes f_1^* - e_1 \otimes e_j^*) \in \mathrm{Sp}(n, \mathbb{Z}),$$

where $\alpha_{1,j}$ are the coefficients of the first row of the matrix α .

3rd step: We find $g' \in \Gamma g \Gamma$ such that $g'e_1 = e_1$ and $g'f_1 = \lambda^2 f_1$.

By the second step, we can assume, writing $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ that both the first row and first column of α are $(1, 0, \dots, 0)$, and the first column of γ is $(0, \dots, 0)$. We would also like the first row of β to be $(0, \dots, 0)$. For that we choose $g' = g\sigma'$ where σ' is the symplectic transformation

$$\sigma' = \mathbf{1}_n - \beta_{1,1} e_1 \otimes f_1^* - \sum_{1 < j \leq n} \beta_{1,j} (e_j \otimes f_1^* + e_1 \otimes f_j^*) \in \mathrm{Sp}(n, \mathbb{Z}).$$

Now by construction one has

$$\begin{aligned} \omega(g'e_j, f_1) &= 0 \quad \text{for } j < n, \\ \omega(g'e_1, f_1) &= 1 \quad \text{and} \\ \omega(g'f_j, f_1) &= 0 \quad \text{for } j \leq n. \end{aligned}$$

Since g'/λ is symplectic, this implies that $g'^{-1}f_1 = \lambda^{-2}f_1$, or equivalently, $g'f_1 = \lambda^2 f_1$ as required.

4th step: *Conclusion.*

By the third step, we can assume that $ge_1 = e_1$ and $gf_1 = \lambda^2 f_1$. Therefore g preserves the symplectic $\mathbb{Z}$ -submodule of $\mathbb{Z}^{2n}$ orthogonal of $\mathbb{Z}e_1 \oplus \mathbb{Z}f_1$, which admits $e_2, \dots, e_n, f_2, \dots, f_n$ as $\mathbb{Z}$ -basis. We conclude by applying the induction hypothesis to the restriction $g' \in \mathcal{M}p(n-1, \mathbb{Z})$ of g to this $\mathbb{Z}$ -module. $\square$

6 The strong approximation theorem

In this section, we give a non elementary proof of the decomposition theorem 2.1 for $\mathrm{Sp}(n, \mathbb{Q})$. We will deduce this theorem from the Bruhat-Tits decomposition theorem 3.2 for $\mathrm{Sp}(n, \mathbb{Q}_p)$ thanks to the strong approximation theorem.

First, I recall the strong approximation theorem. I will not quote here the general formulation for a simply-connected isotropic $\mathbb{Q}$ -simple algebraic group defined over $\mathbb{Q}$ that can be found in [14] but only the special case where G is the symplectic group.

For $p = 2, 3, 5, \dots$ a prime number, we denote by $\mathbb{Q}_p$ the p -adic local field and by $\mathbb{Z}_p$ its ring of integers.

We denote by $\widehat{\mathbb{Q}} = \prod'_p \mathbb{Q}_p$ the locally compact ring of finite adèles which is the restricted product of the $\mathbb{Q}_p$ with respect to the open subrings $\mathbb{Z}_p$. The product $\widehat{\mathbb{Z}} := \prod_p \mathbb{Z}_p$ is then a maximal compact open subring of $\widehat{\mathbb{Q}}$.

Note that, thanks to the diagonal embedding, $\mathbb{Q}$ is a dense subring in $\widehat{\mathbb{Q}}$. This means that $\widehat{\mathbb{Q}} = \mathbb{Q} + \widehat{\mathbb{Z}}$ and that $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$.

By construction the symplectic group $\mathrm{Sp}(n, \widehat{\mathbb{Q}})$ is a locally compact group that contains $\mathrm{Sp}(n, \widehat{\mathbb{Z}})$ as a maximal compact open subgroup. It also contains the group $\mathrm{Sp}(n, \mathbb{Q})$.

Here is the strong approximation theorem for the symplectic group.

Theorem 6.1. *The group $\mathrm{Sp}(n, \mathbb{Q})$ is dense in $\mathrm{Sp}(n, \widehat{\mathbb{Q}})$.*

This means that,

$$\mathrm{Sp}(n, \widehat{\mathbb{Q}}) = \mathrm{Sp}(n, \mathbb{Q})\mathrm{Sp}(n, \widehat{\mathbb{Z}})$$

and that

$$\mathrm{Sp}(n, \mathbb{Z}) \text{ is dense in } \mathrm{Sp}(n, \widehat{\mathbb{Z}}).$$

If we collect together the Bruhat-Tits decomposition in Theorem 3.2 for all p -adic fields $k = \mathbb{Q}_p$, one gets

Theorem 6.2. *Let $g \in \mathrm{Sp}(n, \widehat{\mathbb{Q}})$. Then there exist two matrices σ and σ' in $\mathrm{Sp}(n, \widehat{\mathbb{Z}})$ and a positive integral diagonal matrix $\mathbf{d} = \mathrm{diag}(d_1, \dots, d_n)$ with*

$d_1|d_2|\dots|d_n$ such that

$$g = \sigma \begin{pmatrix} \mathbf{d} & \mathbf{0} \\ \mathbf{0} & \mathbf{d}^{-1} \end{pmatrix} \sigma'.$$

We can now give the non-elementary proof of the symplectic Smith normal form.

Proof of Theorem 2.1. Let $g \in \mathrm{Sp}(n, \mathbb{Q})$.

According to the combined Bruhat-Tits decomposition theorem 6.2, one can write

$$g = \sigma \mathbf{a} \sigma'$$

with σ, σ' in $\mathrm{Sp}(n, \widehat{\mathbb{Z}})$ and with $\mathbf{a} = \begin{pmatrix} \mathbf{d} & \mathbf{0} \\ \mathbf{0} & \mathbf{d}^{-1} \end{pmatrix}$ where $\mathbf{d} = \mathrm{diag}(d_1, \dots, d_n)$ is a positive integral diagonal matrix with $d_1|d_2|\dots|d_n$.

According to the strong approximation theorem 6.1, one can write

$$\sigma = \sigma_0 \eta$$

with σ_0 in $\mathrm{Sp}(n, \mathbb{Z})$ and with η in an arbitrarily small neighborhood of $\mathbf{1}$ in $\mathrm{Sp}(n, \widehat{\mathbb{Z}})$. More precisely we choose η such that the element $\sigma'_0 := \mathbf{a}^{-1} \eta \mathbf{a} \sigma'$ belongs to $\mathrm{Sp}(n, \widehat{\mathbb{Z}})$. Then one has the equality

$$g = \sigma_0 \mathbf{a} \sigma'_0$$

where both σ_0 and $\sigma'_0 = \mathbf{a}^{-1} \sigma_0^{-1} g$ belong to $\mathrm{Sp}(n, \mathbb{Z})$. □

7 Chevalley groups

Let $\mathbf{G}$ be a simply-connected Chevalley group. See [17] for a concrete presentation of the group $\mathbf{G}(\mathbb{Z})$, and see [11] for other nice examples of $\mathbb{Z}$ -models of simple algebraic groups over $\mathbb{Q}$. This $\mathbf{G}$ is a reductive scheme-group over $\mathbb{Z}$ such that as a $\mathbb{Q}$ -group $\mathbf{G}$ is a $\mathbb{Q}$ -split simply connected quasi-simple algebraic group. By construction, this algebraic group contains a $\mathbb{Q}$ -split maximal torus $\mathbf{A}$ such that the group of integral points $\mathbf{N}(\mathbb{Z})$ of the normalizer of $\mathbf{A}$ surjects onto the Weyl group of $(\mathbf{A}(\mathbb{C}), \mathbf{G}(\mathbb{C}))$.

Since $\mathbf{G}$ is simply connected and $\mathbb{R}$ -isotropic, by strong approximation, the group $\mathbf{G}(\mathbb{Q})$ is dense in $\mathbf{G}(\widehat{\mathbb{Q}})$. On the other hand, for all prime integer p , one can consider the simply connected simple p -adic Lie group $G := \mathbf{G}(\mathbb{Q}_p)$,

its split maximal torus $A := \mathbf{A}(\mathbb{Q}_p)$ and its normalizer $N := \mathbf{N}(\mathbb{Q}_p)$. The maximal compact subgroup $K := \mathbf{G}(\mathbb{Z}_p)$ is a good compact subgroup in the sense that one has the equality $N = (N \cap K)A$. Hence, according to Bruhat-Tits, one has the decomposition $\mathbf{G}(\mathbb{Q}_p) = \mathbf{G}(\mathbb{Z}_p)\mathbf{A}(\mathbb{Q}_p)\mathbf{G}(\mathbb{Z}_p)$.

Therefore the same proof as in Chapter 6 gives the following theorem due to Steinberg in [17, Theorem 21]

Theorem 7.1. *Let $\mathbf{G}$ be a simply connected Chevalley group and $g \in \mathbf{G}(\mathbb{Q})$. Then there exist two elements σ and σ' in $\mathbf{G}(\mathbb{Z})$ and an element $\mathbf{a}$ in $\mathbf{A}(\mathbb{Q})$ such that*

$$g = \sigma \mathbf{a} \sigma'.$$

Remark. Such a decomposition is not true when we replace $\mathbb{Q}$ by a number field $\mathbb{K}$ whose ring of integer $\mathcal{O}$ is not principal. Here is an example with

$$\mathbf{G}(\mathbb{K}) := \mathrm{SL}(2, \mathbb{K}), \quad \mathbf{G}(\mathcal{O}) := \mathrm{SL}(2, \mathcal{O}),$$

$$\mathbf{A}(\mathbb{K}) := \left\{ \mathbf{a} = \begin{pmatrix} \mathbf{d} & \mathbf{0} \\ \mathbf{0} & \mathbf{d}^{-1} \end{pmatrix} \mid \mathbf{d} \in K^* \right\}.$$

In this case the product $\mathbf{G}(\mathcal{O}) \mathbf{A}(\mathbb{K}) \mathbf{G}(\mathcal{O})$ is not equal to $\mathbf{G}(\mathbb{K})$. For instance, when $K = \mathbb{Q}[i\sqrt{5}]$ and $\mathcal{O} = \mathbb{Z}[i\sqrt{5}]$, this product does not contain the matrix

$$g = \begin{pmatrix} (1-i\sqrt{5})/2 & i\sqrt{5} \\ -1 & 2 \end{pmatrix}.$$

Indeed the element $\mathbf{d} \in K^*$ should be a unit in all completion $K_{\mathfrak{p}}$ except for the prime ideal $\mathfrak{p}_0 = 2\mathbb{Z} \oplus (1+i\sqrt{5})\mathbb{Z}$ in which case it should be a uniformizer. Such an element $\mathbf{d}$ would be a generator of the ideal $\mathfrak{p}_0$. This is a contradiction, since this ideal $\mathfrak{p}_0$ is not principal.

References

- [1] Y. Benoist. Convolution and square in abelian groups II. hal (2022) 60 p.
- [2] Y. Benoist and H. Oh. Polar decomposition for p -adic symmetric spaces. *Int. Math. Res. Not.* 24, (2007):1–20, 2007.

- [3] Y. Benoist and H. Oh. Effective equidistribution of S -integral points on symmetric varieties. *Ann. Inst. Fourier*, 62:1889–1942, 2012.
- [4] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. *Publ. Math. IHES*, 41:5–251, 1972.
- [5] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. II. Schémas en groupes. Existence d’une donnée radicielle valuée. *Publ. Math. IHES*, 60:197–376, 1984.
- [6] F. Bruhat and J. Tits. Schémas en groupes et immeubles des groupes classiques sur un corps local. *Bull. Soc. Math. France*, 112:259–301, 1984.
- [7] F. Bruhat and J. Tits. Schémas en groupes et immeubles des groupes classiques sur un corps local. II. Groupes unitaires. *Bull. Soc. Math. France*, 115:141–195, 1987.
- [8] L. Clozel, H. Oh, and E. Ullmo. Hecke operators and equidistribution of Hecke points. *Invent. Math.*, 144(2):327–351, 2001.
- [9] E. Freitag. *Siegelsche Modulfunktionen*. Grundlehren Math. 254. Springer, 1983.
- [10] O. Goldman and N. Iwahori. The space of p -adic norms. *Acta Math.*, 109:137–177, 1963.
- [11] B. Gross. Groups over $\mathbf{Z}$. *Invent. Math.*, 124:263–279, 1996.
- [12] S. Helgason. *Differential geometry, Lie groups, and symmetric spaces*. Academic Press, 1978.
- [13] T. Kaletha and G. Prasad. *Bruhat-Tits buildings: a new approach*. Cambridge Univ. Press, 2022.
- [14] V. Platonov and A. Rapinchuk. *Algebraic groups and number theory*. Pure and Applied Mathematics. Academic Press, 1994.
- [15] G. Shimura. Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan*, 15:33–65, 1963.
- [16] G. Shimura. On modular correspondences for $Sp(n, \mathbf{Z})$ and their congruence relations. *Proc. Nat. Acad. Sci. U.S.A.*, 49:824–828, 1963.
- [17] R. Steinberg. *Lectures on Chevalley groups*. Yale Univ., 1968.

Y. BENOIST: CNRS, Université Paris-Saclay,

yves.benoist@u-psud.fr