On the rational symplectic group

Yves Benoist

On the rational symplectic group

Yves Benoist

Abstract

This note contains 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.

1 Introduction

In this short elementary note which is dedicated to Jacques Tits 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 a more general form, in [15] is a symplectic version of the "adapted basis theorem" for $\mathbb{Z}$-modules, or of the "Smith normal form" for integral matrices.

1.1 Normal form for the rational symplectic group

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},

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

2020 Math. subject class. Primary 20G30 ; Secondary 11E57
Key words Symplectic group, Cartan decomposition, Smith normal form.

where $J = \begin{pmatrix} \mathbf{0} & \mathbb{1}_n \\ -\mathbb{1}_n & \mathbf{0} \end{pmatrix}$. 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

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

Theorem 1.1. *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 $\mathbf{d} = \mathrm{diag}(d_1,\ldots,d_n)$ with $d_1|d_2|\ldots|d_n$, 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, ..., and d_{n-1} dividing d_n ensures that the diagonal matrix $\mathbf{d}$ is unique.

I use this precise Theorem 1.1 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, and the rational symplectic matrix g shows up as the "holonomy" of ν.

The first reference to Theorem 1.1 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 [12, p.232] and is also used by Clozel, Oh and Ullmo in [11, p.23].

1.2 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 [14] and in [8] 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 1.2. (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 $\mathbf{d} = \mathrm{diag}(d_1,\ldots,d_n)$ with $d_1 \leq d_2 \leq \ldots \leq d_n \leq 1$ 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 1.3. (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 $\mathbf{d} = \mathrm{diag}(\pi^{p_1},\ldots,\pi^{p_n})$ with $p_1 \geq p_2 \geq \ldots \geq p_n \geq 0$ 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.

1.3 Other algebraic semisimple groups

This paper is dedicated to Jacques Tits who, pursuing in his own way the works of E. Cartan over the real and of C. Chevalley over an algebraically closed field, has understood, in a highly efficient and non elementary way, the algebraic semisimple groups.

He has described with A. Borel the structure of algebraic semisimple groups over non algebraically closed fields in [4], [5] and [6].

He has reduced the classification of these semisimple groups to the anisotropic case in [17].

He also has described with F. Bruhat the analog of the Cartan decomposition for semisimple groups over non-archimedean local fields, in [7], [8], [9] and [10], by introducing new geometric spaces that are nowaday called Bruhat-Tits buildings and that extend the space of p-adic norms studied by Goldman and Iwahori in [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].

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

2 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 2.1. (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 1.1 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 $\mathcal{M}p(n,\mathbb{Z})$ of nonzero integral matrices which are proportional to elements of $\mathrm{Sp}(n,\mathbb{R})$,

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

Proposition 2.2. *Let $g \in \mathcal{M}p(n,\mathbb{Z})$. 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 $\mathcal{M}p(n,\mathbb{Z})$ and hence the products $a_j a_{n+j}$ do not depend on the positive integer $j \le n$. 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 2.2, 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 2.3. *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 2.3. Let $v = (x_1,..,x_{2n})$ 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 $\mathrm{Sp}(n,\mathbb{Z})$. □

Proof of Proposition 2.2. 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 2.1, there exists a primitive vector v in $\mathbb{Z}^{2n}$ such that gv is also primitive. According to lemma 2.3, there exists σ, σ' in Γ such that $\sigma g v = e_1$ 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 $(1, 0, \ldots, 0)$. We would like the first row of α to be also of the form $(1, 0, \ldots, 0)$. For that we choose $g' = g\sigma'$ where σ' is the symplectic transformation

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

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 $(1, 0, \ldots, 0)$, 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

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

Now by construction one has

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

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. □

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] A. Borel and J. Tits. Groupes réductifs. *Publ. Math. IHES*, 27:55–150, 1965.

[5] A. Borel and J. Tits. Compléments à l'article: "Groupes réductifs". *Publ. Math. IHES*, 41:253–276, 1972.

[6] A. Borel and J. Tits. Homomorphismes "abstraits" de groupes algébriques simples. *Ann. of Math.*, 97:499–571, 1973.

[7] F. Bruhat and J. Tits. Groupes réductifs sur un corps local. *Publ. Math. IHES*, 41:5–251, 1972.

[8] 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.

[9] 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.

[10] 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.

[11] L. Clozel, H. Oh, and E. Ullmo. Hecke operators and equidistribution of Hecke points. *Invent. Math.*, 144(2):327–351, 2001.

[12] E. Freitag. *Siegelsche Modulfunktionen*. Grundlehren Math. 254. Springer, 1983.

[13] O. Goldman and N. Iwahori. The space of p-adic norms. *Acta Math.*, 109:137–177, 1963.

[14] S. Helgason. *Differential geometry, Lie groups, and symmetric spaces*. Academic Press, 1978.

[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 $Sp(n, Z)$ and their congruence relations. *Proc. Nat. Acad. Sci. U.S.A.*, 49:824–828, 1963.

[17] J. Tits. Classification of algebraic semisimple groups. In *Algebraic Groups and Discontinuous Subgroups*, pages 33–62. Amer. Math. Soc., 1966.

Y. Benoist: CNRS, Université Paris-Saclay, yves.benoist@u-psud.fr