Bulletin

de la SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Tome 148
Fascicule 3

2020

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Pages 383-595

Bull. Soc. Math. France
148 (3), 2020, p. 383-595

Sommaire

Bull. Soc. Math. France
148 (3), 2020, p. 383-595

Contents

Bull. Soc. Math. France
148 (3), 2020, p. 383-397

THE ARNOUX–YOCCOZ MAPPING CLASSES VIA PENNER'S CONSTRUCTION

BY LIVIO LIECHTI & BALÁZS STRENNER

ABSTRACT. — We give a new description of the Arnoux–Yoccoz mapping classes as a product of two Dehn twists and a finite order element. The construction is analogous to Penner's construction of mapping classes with small stretch factors.

RÉSUMÉ (*Les homéomorphismes de Arnoux–Yoccoz via la construction de Penner*). — Nous donnons une nouvelle description des homéomorphismes de Arnoux–Yoccoz comme un produit de deux twists de Dehn et d'un élément d'ordre fini. Cette construction est analogue à celle des homéomorphismes pseudo-Anosovs de petite dilatation donnée par Penner.

1. Introduction

The mapping class group of a surface S is the group of isotopy classes of orientation-preserving homeomorphisms of S. Motivated by studying geometric structures on 3-manifolds, Thurston [24] modernized the theory of mapping class groups in the 1970s by giving a classification of elements into three types:

Texte reçu le 11 mai 2018, modifié le 4 octobre 2019, accepté le 19 octobre 2020.

LIVIO LIECHTI, Département de Mathématiques, Université de Fribourg, Chemin du Musée 23, 1700 Fribourg, Suisse • *E-mail :* livio.liechti@unifr.ch
BALÁZS STRENNER, Georgia Institute of Technology, School of Mathematics, Atlanta GA 30332, USA • *E-mail :* strennerb@gmail.com

Mathematical subject classification (2010). — 57M20, 57M99, 37E30.

Key words and phrases. — Penner's construction, Arnoux–Yoccoz, Pseudo-Anosov, Dehn twist.

The first author was supported by the Swiss National Science Foundation (grant nr. 175260).

© Société Mathématique de France
0037-9484/2020/383/$ 5.00
doi:10.24033/bsmf.2809

finite order, reducible and pseudo-Anosov. This article concerns the third type. A mapping class is *pseudo-Anosov* if it has a representative homeomorphism ϕ and singular measured foliations $\mathcal{F}^u$ and $\mathcal{F}^s$ on S such that $\phi(\mathcal{F}^u) = \lambda\mathcal{F}^u$ and $\phi(\mathcal{F}^s) = \lambda^{-1}\mathcal{F}^s$ for some $\lambda > 1$. The number λ is independent of choice of representative homeomorphism, and it is called the *stretch factor* or *dilatation* of the pseudo-Anosov mapping class.

Thurston showed that stretch factors of pseudo-Anosov mapping classes of the closed orientable surface S_g are algebraic integers with degree bounded above by $6g - 6$. He claimed without proof in [24] that the degree $6g - 6$ was realizable, but this statement was only recently proven in [22]. For some time, however, even the fact that pseudo-Anosov stretch factors of arbitrarily large degrees exist was not justified. This fact was first shown by Arnoux and Yoccoz [4] in 1981. They constructed a pseudo-Anosov mapping class $\tilde{h}_g$ on S_g for each $g \geq 3$ with a stretch factor of algebraic degree g. After stating the main results, we will recall the construction in Section 2.1 and give more reasons for why the Arnoux–Yoccoz examples are of importance.

Despite the mapping classes $\tilde{h}_g$ probably being the single most widely studied explicit family of pseudo-Anosov mapping classes, to this day, no constructions have been known other than the original approach by Arnoux and Yoccoz.

The goal of this paper is to present a new description as a product of two Dehn twists and a finite order mapping class. We hope that this new description will shed new light on the examples and help construct new analogous families of mapping classes that might also serve as interesting examples. An alternative description of the Arnoux–Yoccoz mapping classes was also asked for by Margalit in Section 10 of [16].

THEOREM 1.1. — *The Arnoux–Yoccoz mapping class $\tilde{h}_g$ on the surface S_g is conjugate to $\tilde{f}_g = r \circ T_a \circ T_b^{-1}$, where T_a and T_b^{-1} are positive and negative Dehn twists about the curves a and b pictured on Figure 1.1, and r is a rotation of the surface by one click in either direction.*

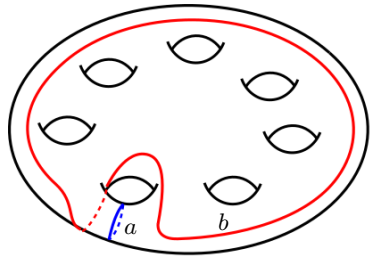

FIGURE 1.1. The surface S_g with a rotational symmetry of order g. This figure shows the case $g = 7$.

For the proof, we use the fact, shown by the second author in [23, Section 5], that the mapping classes $\tilde{h}_g$ arise as lifts of mapping classes on nonorientable surfaces. More precisely, there is a pseudo-Anosov mapping class h_g (see Section 2.2 for the definition) on the closed nonorientable surface N_{g+1} of genus $g+1$ for each $g \geq 3$, such that $\tilde{h}_g$ is the lift of h_g by the double cover $S_g \to N_{g+1}$. We will deduce Theorem 1.1 from the following.

THEOREM 1.2. — *The nonorientable Arnoux–Yoccoz mapping class h_g on the surface N_{g+1} is conjugate to $f_g = r \circ T_c$, where T_c is a Dehn twist about the two-sided curve c pictured in Figure 1.2, and r is a rotation of the surface by one click in either direction.*

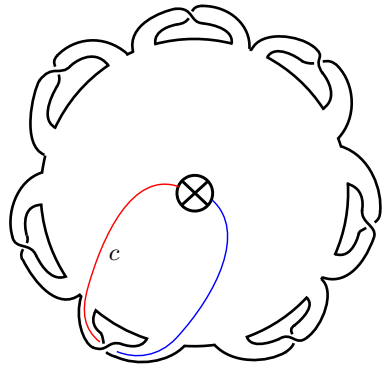

FIGURE 1.2. The circle with an X inside it indicates a crosscap: the inside of the circle is not part of the surface and antipodal points of the circle are identified. A disk with one crosscap is, therefore, a Möbius strip. So, this figure shows a nonorientable surface obtained by attaching g twisted bands to the boundary of a Möbius strip. The surface has one boundary component. By gluing a disk to the boundary component, we obtain the closed surface N_{g+1}.

The direction of twisting about T_c is important, see Figure 3.2 later for the reason behind this. On a nonorientable surface, there is no notion of positive or negative twisting, so we specify the direction of the Dehn twist T_c by the coloring of the curve c on Figure 1.2 as follows. By cutting out the crosscap in the middle and cutting the twisted bands, we obtain an orientable surface with an embedding in $\mathbf{R}^2$ coming from the figure. Our cut-up surface inherits the orientation of $\mathbf{R}^2$. The blue and red parts of our curve indicate the parts where the twisting behaves like a positive and negative twist, respectively, with respect to the orientation of the cut-up surface.

In Proposition 2.3, we show that both f_g^g and $\tilde{f}_g^g$ arise from Penner's construction. In this sense, the mapping classes f_g and $\tilde{f}_g$ are analogous to the pseudo-Anosov mapping classes with small stretch factors constructed by Penner in [20].

History and motivation. — The Sah–Arnoux–Fathi invariant (for short, the SAF invariant) is an invariant of interval exchange transformations and measured foliations that measures certain dynamical properties. In genus 2, the invariant foliations of all pseudo-Anosov mapping classes have a nonvanishing SAF invariant [17, 7]. The Arnoux–Yoccoz examples were the first examples of pseudo-Anosov mapping classes in genus 3 and higher, whose invariant foliations had vanishing SAF invariants. For more on pseudo-Anosov maps with vanishing a SAF invariant, see [3, 8, 9, 23].

The Arnoux–Yoccoz examples are interesting also because they are known not to arise from Thurston's construction [24], the first general construction of pseudo-Anosov mapping classes. This was shown by Hubert and Lanneau [12], using the fact that the extension fields $\mathbf{Q}(\lambda_g+\lambda_g^{-1})$ are not totally real, where λ_g denotes the stretch factor of $\tilde{h}_g$. Since the examples that arise from Thurston's construction have certain special properties (for one of these properties, see the next paragraph), the Arnoux–Yoccoz mapping classes have become valuable exotic examples.

A further motivation for studying the Arnoux–Yoccoz examples comes from Teichmüller theory. The two invariant measured foliations of a pseudo-Anosov mapping class give rise to a *singular Euclidean metric* or *flat structure* on the surface. The *Veech group* of a flat surface is the group of its affine symmetries. The infinite cyclic group formed by the powers of the pseudo-Anosov map is always part of the Veech group. It is not known, however, whether the Veech group can possibly equal this infinite cyclic group [14, Problem 6]. In many cases (for example, for pseudo-Anosov maps arising from Thurston's construction), the Veech group is known to contain free groups, hence it is known not to be cyclic. Since the Arnoux–Yoccoz examples do not arise from Thurston's construction, presumably they might be good candidates for cyclic Veech groups. In the $g = 3$ case, however, Hubert, Lanneau and Möller [13] found additional elements in the Veech group of the Arnoux–Yoccoz flat surface, hence that Veech group is not cyclic. It remains an open question whether the Arnoux–Yoccoz surfaces have cyclic Veech groups when $g \geq 4$.

For other work on the Arnoux–Yoccoz mapping classes and their flat surfaces, see [1, 5, 6, 18, 11].

Generalizations. — The Arnoux–Yoccoz example in the $g = 3$ case was generalized by Arnoux and Rauzy in Section 3 of [2], see also Section 4.2 of [21]. On the surface N_4, one example in the Arnoux–Rauzy family is the third power of the Arnoux–Yoccoz mapping class h_3, which is conjugate to $T_{r^{-2}(c)} \circ T_{r^{-1}(c)} \circ T_c$

by our Theorem 1.2. We believe that other members of Arnoux–Rauzy family include the mapping classes $T_{r^{-2}(c)} \circ T_{r^{-1}(c)} \circ T_c^k$ where $k \geq 1$, but we will not give a proof of this.

In a follow-up paper [15], we will generalize the twist-and-rotation construction in Theorem 1.2 in a different way in order to construct minimal pseudo-Anosov stretch factors on various different nonorientable surfaces. In particular, we will show that the Arnoux–Yoccoz example h_3 has a minimal stretch factor on N_4 among pseudo-Anosov mapping classes with an orientable invariant foliation.

2. Background

2.1. The orientable Arnoux–Yoccoz examples. — In this section, we recall the original construction of the orientable Arnoux–Yoccoz mapping classes $\tilde{h}_g$ from [4]. We give this description in order to provide context only. The content of this section will not be used in the proofs.

Fix some $g \geq 3$ and let α be the unique real number in $(0, 1)$ satisfying $\alpha + \cdots + \alpha^g = 1$. We construct a measured foliation $\mathcal{F}$ on the surface S_g as follows. Start with the rectangle on Figure 2.1 foliated by vertical leaves. Equip $\mathcal{F}$ with a measure so that the width of the rectangle is 2. Identify the two vertical sides to obtain a foliated annulus. Divide the top and bottom boundary components of this annulus into $2g$ intervals each, as shown in Figure 2.1 and identify each interval on the top side with the interval on the bottom side that has the same length, so that shaded rectangles above the core of the annulus are joined to shaded rectangles below the core of the annulus, and empty rectangles are joined to empty rectangles. We obtain a measured foliation $\mathcal{F}$ on the surface S_g. The two-sided simple closed curve γ obtained from the core of the annulus is transverse to $\mathcal{F}$, and the first return map of $\mathcal{F}$ with respect to γ induces the subdivision of S_g into the $2g$ rectangles shown in Figure 2.1.

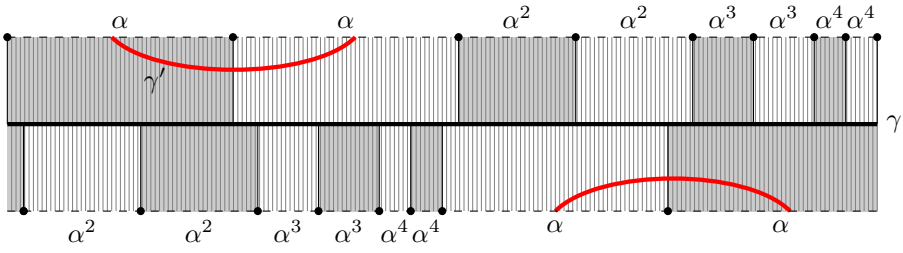

FIGURE 2.1. Construction of the mapping class $\tilde{h}_4$ by Arnoux and Yoccoz.

The key observation is that the two-sided simple closed curve γ' in Figure 2.1 is also transverse to $\mathcal{F}$, has the length 2α, and the first return map of $\mathcal{F}$ induces a decomposition into rectangles, which is isomorphic to the original decomposition, up to scaling the measure by a factor of α. Therefore, there are homeomorphisms of the surface that map γ to γ' and $\mathcal{F}$ to $\frac{1}{\alpha}\mathcal{F}$. These homeomorphisms are all isotopic via a leaf-preserving isotopy, and, therefore, they belong to the same mapping class. The mapping class $\tilde{h}_g$ is defined to be this mapping class.

2.2. Nonorientable Arnoux–Yoccoz examples. — In [23], the second author constructed a mapping class h_g on the closed nonorientable surface N_{g+1} of genus $g+1$ in a way that is analogous to the construction described in Section 2.1.

Consider the rectangle in Figure 2.2 together with the vertical measured foliation of width 1, but now identify the two vertical sides with a flip to obtain a foliated Möbius strip. Divide the boundary component of length 2 to intervals as shown in the figure and identify pairs of intervals of equal length by translations.

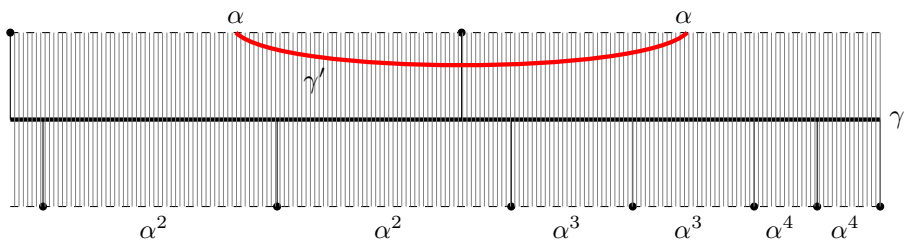

FIGURE 2.2. Construction of the mapping class h_4 by the second author.

Let γ be the core of the Möbius strip and let γ' be the one-sided curve in the figure that is also transverse to the foliation $\mathcal{F}$. As before, the first return maps of the foliation on γ and γ' each induce decompositions of the surface into g foliated rectangles, and there are homeomorphisms that map γ to γ' and $\mathcal{F}$ to $\frac{1}{\alpha}\mathcal{F}$. Once again, all these homeomorphisms are isotopic, and, hence, they define the same mapping class. The mapping class h_g is defined to be this mapping class.

Our approach to proving that a mapping class constructed in a different way is conjugate to h_g is to use the fact (immediate from the construction) that the triple $(\mathcal{F}, \gamma, \gamma')$ uniquely determines h_g up to conjugation. To be more specific, we state this fact formally as follows.

LEMMA 2.1. — *Let $g \geq 3$ and let f_1 and $f_2 = h_g$ be pseudo-Anosov mapping classes with unstable measured foliations $\mathcal{F}_1$ and $\mathcal{F}_2$ on the surface N_{g+1}. Let γ_1 and γ_2 be one-sided simple closed curves on N_{g+1}, transverse to $\mathcal{F}_1$ and $\mathcal{F}_2$, respectively. If there is a homeomorphism $\phi : N_{g+1} \to N_{g+1}$, such that $\phi(\mathcal{F}_1) = \mathcal{F}_2$, $\phi(\gamma_1) = \gamma_2$ and $\phi(f_1(\gamma_1)) = f_2(\gamma_2)$, then f_1 and f_2 are conjugate in the mapping class group of N_{g+1}.*

2.3. Penner's construction of pseudo-Anosov mapping classes. — Consider the annulus $A = \{z \in \mathbf{C} : 1 \leq |z| \leq 2\}$ and define the positive Dehn twist in A by the formula $T(z) = z \cdot e^{2\pi i(1-|z|)}$. Given a two-sided simple closed curve c in a surface S, its *marking* is an embedding $\phi_c : A \to S$, where c is the image of the circle $\{z : |z| = \frac{3}{2}\}$. The Dehn twist about the marked curve (c, ϕ_c) is defined as $\phi_c \circ T \circ \phi_c^{-1}$ on $\phi_c(A)$ and as the identity otherwise. When the marking is clear from the context, we denote this Dehn twist simply by T_c. Note that if the surface S is orientable, then T_c is a positive twist if ϕ_c is orientation-preserving and a negative twist if ϕ_c is orientation-reversing.

Two marked two-sided simple closed curves c_1 and c_2 are said to *intersect inconsistently* if $\phi_{c_1}^{-1} \circ \phi_{c_2}$ is orientation-reversing at all points where the composition is defined. A pair of simple closed curves on a surface is in *minimal position* if one cannot decrease their intersection number by isotoping them. A collection of curves on a surface is said to *fill* the surface if they are in pairwise minimal position, and the complementary regions of the curves are disks and once-punctured disks.

Penner gave the following construction of pseudo-Anosov mapping classes in [19] (see also [10]).

THEOREM 2.2 (Penner's construction). — *Let $c_1, \ldots, c_n$ be a filling collection of pairwise inconsistently intersecting marked two-sided simple closed curves on a surface S. Then, any product of the Dehn twists $T_{c_1}, \ldots, T_{c_n}$ containing each twist at least once is pseudo-Anosov.*

For an orientable surface, the filling and the inconsistently intersecting property implies that the collection of curves is a union of two multicurves Γ_1 and Γ_2, and the allowable products contain positive twists about the curves in Γ_1 and negative twists about the curves in Γ_2.

One nice property of Penner's construction is that the stretch factor and the invariant measured foliations are straightforward to compute. We explain the process briefly here; for more details, see [19, 20, 10, 22]. By smoothing out the intersections of the collection $\{c_1, \ldots, c_n\}$, one obtains a bigon track τ that is invariant under each twist T_{c_i}, and, hence, under any product of them as well. This process is illustrated in Figure 3.1. Each curve c_i is carried on τ, and its characteristic measure μ_i is a 0-1-valued measure on τ that takes the value 1 on the branches of τ traversed by c_i and the value 0 on the other branches. The cone C generated by the measures μ_i is invariant under the Dehn twists T_{c_i}.

Moreover, a product f of T_{c_i} containing all twists at least once acts on C by a Perron–Frobenius matrix (a matrix with nonnegative entries that has a power whose entries are all positive). The largest eigenvalue of this matrix has multiplicity 1, and it is the stretch factor of f. The corresponding eigenvectors define a positive measure on τ that is unique up to scaling, and this train-track measure defines the unstable foliation of f.

PROPOSITION 2.3. — *The mapping classes f_g^g and $\tilde{f}_g^g$ arise from Penner's construction.*

Proof. — We have

$$f_g^g = T_{r^{-(g-1)}(c)} \circ \cdots \circ T_c.$$

and

$$\tilde{f}_g^g = T_{r^{-(g-1)}(a)} \circ T^{-1}_{r^{-(g-1)}(b)} \circ \cdots \circ T_a \circ T_b^{-1}.$$

Figure 3.1A shows that the marked curve c and its rotated copies intersect inconsistently (red intersects blue at every intersection). Furthermore, any pair of curves intersects exactly once and, hence, minimally, and the complement of the union of the curves consists of discs. Hence, f_g^g does, indeed, arise from Penner's construction.

In the second case, $A = \{a, \ldots, r^{g-1}(a)\}$ and $B = \{b, \ldots, r^{g-1}(b)\}$ are filling multicurves, and we twist only positively along curves in A and negatively along curves in B, and, hence, $\tilde{f}_g^g$ also arises from Penner's construction. □

3. Proofs

In this section, we give the proofs of Theorem 1.1 and Theorem 1.2.

Proof of Theorem 1.2. — By Lemma 2.1, the proof reduces to the study of the unstable foliation of f_g and the image of the core curve γ of the crosscap under f_g.

First we describe the unstable foliation of f_g. Although f_g does not arise from Penner's construction, its gth power does, since

$$f_g^g = T_{r^{-(g-1)}(c)} \circ \cdots \circ T_c.$$

The invariant foliations of f_g and its powers are the same, and, therefore, we may use the process described in Section 2.3 for f_g^g to find the unstable foliation of f_g.

Figure 3.1A shows the curve c and its iterates under the rotation r, and Figure 3.1B shows the invariant bigon track of f_g^g obtained by smoothing out the intersections of these curves. Note that this bigon track is invariant not only under all twists $T_{r^i(c)}$, but also under r.

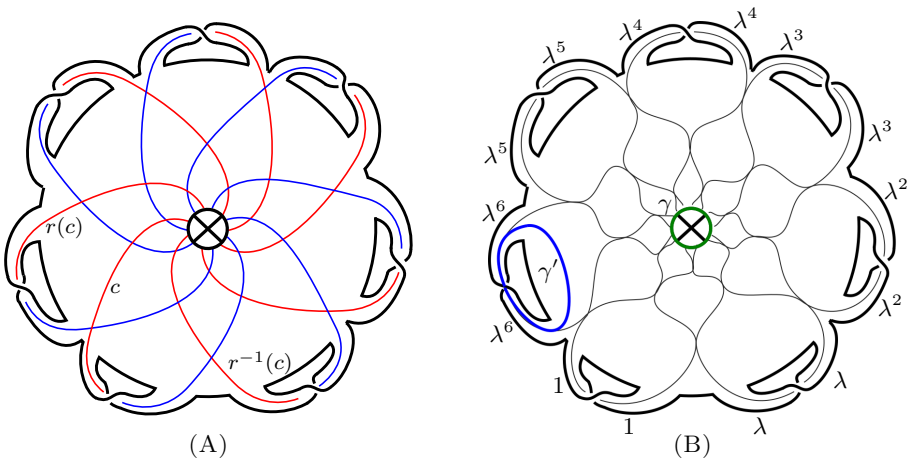

FIGURE 3.1

For $i = 0, \dots, g-1$, let μ_i be the characteristic measure of the curve $r^{-i}(c)$. The mapping class T_c acts on the cone C generated by the characteristic measures μ_i by the matrix which has 1s on the diagonal and in the first row, and 0s otherwise, and r acts by a permutation matrix. So, for example, when $g = 7$, the acting matrix of $f_g = r \circ T_c$ on the cone C is

$$M_g = \begin{pmatrix} 0&1&0&0&0&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&1 \\ 1&1&1&1&1&1&1 \end{pmatrix},$$

the companion matrix of the polynomial $x^7 - x^6 - \cdots - x - 1$. In general, the characteristic polynomial is $x^g - x^{g-1} - \cdots - x - 1$. The action of f_g^g on C is given by M_g^g, so by the construction described in Section 2.3, the stretch factor and the unstable foliation of f_g^g are the largest eigenvalue and the corresponding eigenvector for M_g^g. As a consequence, the stretch factor and the unstable foliation of f_g are given by the largest eigenvalue and the corresponding eigenvector for M_g. Hence, the stretch factor λ of f_g is the largest real root of $x^g - x^{g-1} - \cdots - x - 1$. The corresponding eigenvector is $(1, \lambda, \lambda^2, \dots, \lambda^{g-1})$, and, therefore, the unstable foliation of f_g is given by the measure $\sum_{i=0}^{g-1} \lambda^i \mu_i$ on our bigon track. Note that $\lambda = 1/\alpha$, where α was defined in Section 2.1.

Now we explain how to redraw Figure 3.1B analogously to Figure 2.2. (Note, however, that Figure 3.1B depicts the case $g = 7$, while Figure 2.2 shows the

case $g = 4$.) A large regular neighborhood of γ on Figure 3.1B is the disk with the crosscap in the middle (hence a Möbius strip), but without the twisted bands attached. Since a bigon in the complement of a bigon track does not give rise to a singularity of the unstable measured foliation, we can isotope the foliation so that its leaves point radially inwards from the boundary of the Möbius strip, and so that the foliation is nonsingular in the interior of the Möbius strip. Note that, up to homeomorphism preserving the leaves and the transverse measure of the foliation, every nonsingular measured foliation of the Möbius strip whose leaves meet the boundary transversally is the vertical foliation of a rectangle with the two vertical sides identified by an involution. This is the model of Figure 2.2, but without the identifications on the boundary. Therefore, the only thing left to check is that attaching the twisted bands as in Figure 3.1B induces the correct identifications of the boundary in the Möbius rectangle model.

The effect of attaching the twisted bands is that intervals on the boundary of the Möbius strip are identified. The lengths of these intervals with respect to the unstable measured foliation are the measures on the branches of the bigon track inside the twisted bands, that is, $\lambda^{g-1}, \lambda^{g-1}, \dots, 1, 1$. When the Möbius strip is drawn as a rectangle with its vertical sides identified, the $2g$ intervals of length $\lambda^{g-1}, \lambda^{g-1}, \dots, 1, 1$ appear on the horizontal sides. Note that we obtain exactly the pattern of Figure 2.2, with the difference that our intervals are a factor λ^g longer. Since the bands in Figure 3.1B are twisted, the pairs of intervals are glued together in an orientation-reversing way, just like gluing by translation in Figure 2.2 results in orientation-reversing gluings. Therefore, the bigon track in Figure 3.1B does, indeed, produce the measured foliation pictured on Figure 2.2, up to scaling the measure by λ^g.

The curve $\gamma' = h_g(\gamma)$ in Figure 2.2 corresponds to the curve γ' on Figure 3.1B. It remains to show that $\gamma' = f_g(\gamma)$. After applying the twist T_c on the curve γ on Figure 3.2A, we obtain the curve shown on Figure 3.2B. After rotation by one click, this curve does, indeed, map to γ'. □

Proof of Theorem 1.1. — Consider the orientable double cover of the nonorientable surface in Figure 1.2. One way to construct this covering surface is to cut along the twisted bands on Figure 3.1B, remove the central crosscap, and glue together two copies of the resulting surface. We can think about the two copies as the upper and lower half of the cylinder pictured in Figure 3.3. The upper and lower boundaries of this cylinder are subdivided into $2g$ intervals, which correspond to the $2g$ intervals obtained by cutting the twisted bands. The orientation-reversing involution of this cylinder that identifies the upper and lower half is the reflection about the center of the picture in the ambient three-dimensional space. When the intervals along the boundaries are identified in the manner shown, the quotient of the surface is our nonorientable surface with the twisted bands, with the boundary collapsed to one point.

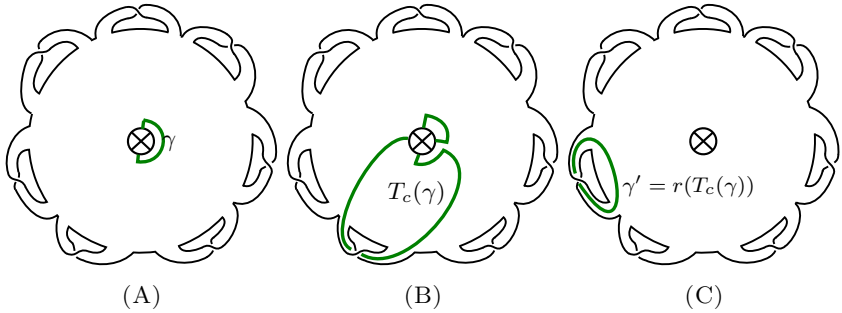

FIGURE 3.2. The curves γ, $T_c(\gamma)$, and $\gamma' = r(T_c(\gamma))$. To go from the second figure to the third, we isotope a small piece of $T_c(\gamma)$ through the crosscap. This is possible, because the antipodal points of the circle containing the X are identified. The direction of the twisting about c is matters: one can compute directly that the curve $T_c^{-1}(\gamma)$ defines an element of the fundamental group that does not correspond to the core curve of one of the twisted bands.

Note that the rotation r of N_{g+1} lifts to the rotation of the cylinder by two intervals.

By flattening out the cylinder, we obtain the representation in Figure 3.4A. The lift of the curve c along which we twist in the definition of f_g has two components, as shown in Figure 3.4A. A Dehn twist about the curve c on N_{g+1} lifts to the product of a positive twist along one of the lifts of c and a negative twist about the other lift.

To find out which twist is positive and which twist is negative, recall that $T_c(\gamma)$ is a curve that runs in a small neighborhood of one of the twisted bands

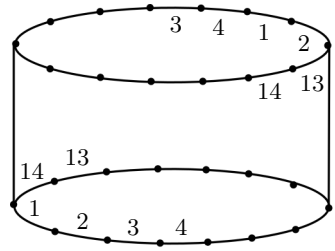

FIGURE 3.3. The orientable double cover of the surface on Figure 1.2 when $g = 7$.

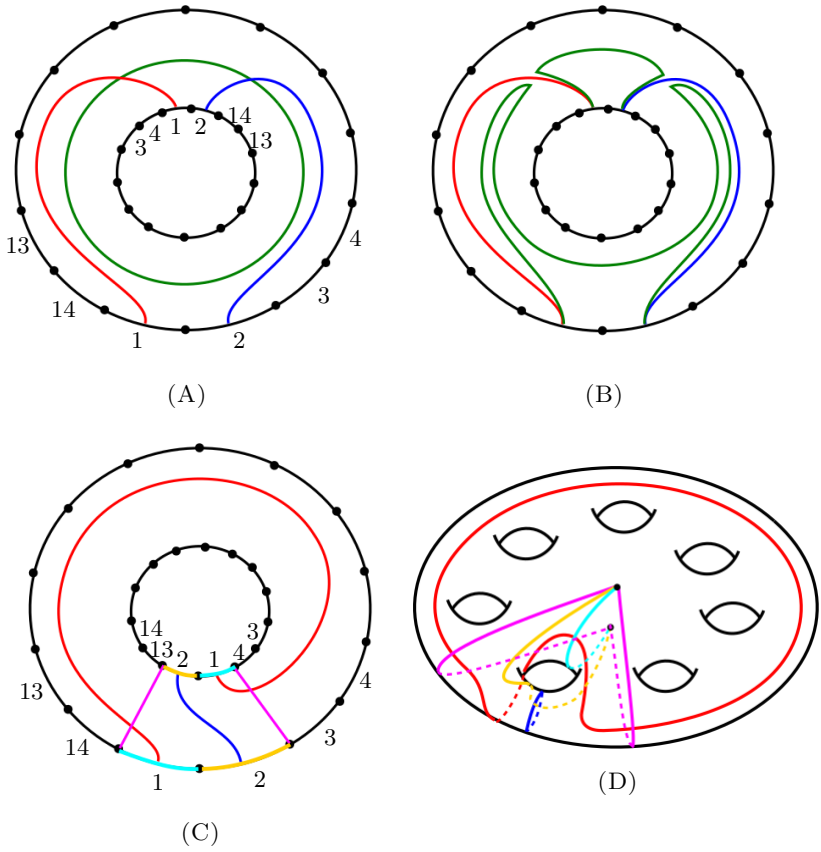

FIGURE 3.4

(Figures 3.2A and 3.2B). The core curve of the annulus in Figure 3.4A is the lift of γ, so its image under the two twists should run in a small neighborhood of two consecutive intervals of the boundary of the annulus. That happens when the twist is positive along the curve on the right and negative along the curve on the left in Figure 3.4B.

After changing Figure 3.4A by rotating the inner boundary by 180 degrees, we obtain the representation shown in Figure 3.4C. By subdividing this surface along the arcs shown and their rotated copies, we can see that this surface can be represented in $\mathbf{R}^3$ as the surface in Figure 3.4D. The two twisting curves correspond to the curves shown in Figure 1.1, and we, indeed, twist positively along the curve a and negatively along the curve b. □

Remarks on the order of composition and the direction of twisting. — Recall from Theorem 1.1 the definition of the curves a and b and the rotation r. Consider also the curve b' in Figure 3.5 that winds around the hole to avoid a in the direction opposite of b.

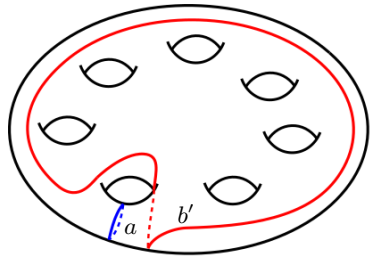

FIGURE 3.5

The following statement summarizes the ways in which the definition of the mapping class $\tilde{f}_g = r \circ T_a \circ T_b^{-1}$ is flexible.

PROPOSITION 3.1. — *The following statements hold.*

1. T_a *commutes with both* T_b^{-1} *and* $T_{b'}^{-1}$.
2. $\tilde{f}_g$ *is conjugate to* $r^{\pm 1} \circ T_a \circ T_b^{-1}$, $T_a \circ T_b^{-1} \circ r^{\pm 1}$, $r^{\pm 1} \circ T_a^{-1} \circ T_{b'}$ *and* $T_a^{-1} \circ T_{b'} \circ r^{\pm 1}$.
3. $\tilde{f}_g^{-1}$ *is conjugate to* $T_a^{-1} \circ T_b \circ r^{\pm 1}$, $r^{\pm 1} \circ T_a^{-1} \circ T_b$, $T_a \circ T_{b'}^{-1} \circ r^{\pm 1}$ *and* $r^{\pm 1} \circ T_a \circ T_{b'}^{-1}$.

Proof. — The first statement holds, because a is disjoint from b and b'.

For the first expression in the second statement, note that in Figure 1.1, the rotation by 180 degrees about the axis intersecting a and b symmetrically commutes with both T_a and T_b^{-1} but conjugates r to r^{-1}. The second expression is conjugate to the first by r. For the third and fourth expressions, note that the reflection about the plane that intersects all g holes of the surface commutes with r and conjugates T_a to T_a^{-1} and T_b to $T_{b'}^{-1}$.

The third statement follows from the second by taking the inverse. □

To summarize, the order of the two twists, the direction of the rotation, and whether we twist first or rotate first do not matter.

In the nonorientable case, we have the following.

PROPOSITION 3.2. — *The mapping class* f_g *is conjugate to* $r^{\pm 1} \circ T_c$ *and* $T_c \circ r^{\pm 1}$. *The inverse* f_g^{-1} *is conjugate to* $T_c^{-1} \circ r^{\pm 1}$ *and* $r^{\pm 1} \circ T_c^{-1}$.

Proof. — This follows by conjugating by r and by an involution of the surface that rotates about an axis and leaves the curve c invariant. This involution commutes with T_c and conjugates r to r^{-1}. □

We also remark that it can be shown by studying their flat surfaces that h_g is conjugate to h_g^{-1}, and $\tilde{h}_g$ is conjugate to $\tilde{h}_g^{-1}$ when $g = 3$, but not when $g > 3$. Therefore, one indeed needs to be careful about the definitions, because the direction in which b winds around the hole does matter.

Acknowledgements. — We are grateful to Pierre Arnoux, Dan Margalit, and Thomas Schmidt for helpful comments on an earlier version of this paper. We also thank the referees for their constructive feedback.

BIBLIOGRAPHY

[1] P. Arnoux – "Un exemple de semi-conjugaison entre un échange d'intervalles et une translation sur le tore", *Bull. Soc. Math. France* **116** (1988), no. 4, p. 489–500 (1989).

[2] P. Arnoux & G. Rauzy – "Représentation géométrique de suites de complexité $2n + 1$", *Bull. Soc. Math. France* **119** (1991), no. 2, p. 199–215.

[3] P. Arnoux & T. A. Schmidt – "Veech surfaces with nonperiodic directions in the trace field", *J. Mod. Dyn.* **3** (2009), no. 4, p. 611–629.

[4] P. Arnoux & J.-C. Yoccoz – "Construction de difféomorphismes pseudo-Anosov", *C. R. Acad. Sci. Paris Sér. I Math.* **292** (1981), no. 1, p. 75–78.

[5] J. P. Bowman – "Orientation-reversing involutions of the genus 3 Arnoux-Yoccoz surface and related surfaces", in *In the tradition of Ahlfors-Bers. V*, Contemp. Math., vol. 510, Amer. Math. Soc., Providence, RI, 2010, p. 13–23.

[6] ———, "The complete family of Arnoux-Yoccoz surfaces", *Geom. Dedicata* **164** (2013), p. 113–130.

[7] K. Calta – "Veech surfaces and complete periodicity in genus two", *J. Amer. Math. Soc.* **17** (2004), no. 4, p. 871–908.

[8] K. Calta & T. A. Schmidt – "Infinitely many lattice surfaces with special pseudo-Anosov maps", *J. Mod. Dyn.* **7** (2013), no. 2, p. 239–254.

[9] H. T. Do & T. A. Schmidt – "New infinite families of pseudo-Anosov maps with vanishing Sah-Arnoux-Fathi invariant", *J. Mod. Dyn.* **10** (2016), p. 541–561.

[10] A. Fathi – "Démonstration d'un théorème de Penner sur la composition des twists de Dehn", *Bull. Soc. Math. France* **120** (1992), no. 4, p. 467–484.

[11] W. P. Hooper & B. Weiss – "Rel leaves of the Arnoux–Yoccoz surfaces", *Selecta Math. (N.S.)* **24** (2018), no. 2, p. 875–934.

[12] P. Hubert & E. Lanneau – "Veech groups without parabolic elements", *Duke Math. J.* **133** (2006), no. 2, p. 335–346.

[13] P. Hubert, E. Lanneau & M. Möller – "The Arnoux-Yoccoz Teichmüller disc", *Geom. Funct. Anal.* **18** (2009), no. 6, p. 1988–2016.
[14] P. Hubert, H. Masur, T. Schmidt & A. Zorich – "Problems on billiards, flat surfaces and translation surfaces", in *Problems on mapping class groups and related topics*, Proc. Sympos. Pure Math., vol. 74, Amer. Math. Soc., Providence, RI, 2006, p. 233–243.
[15] L. Liechti & B. Strenner – "Minimal pseudo-Anosov stretch factors on nonoriented surfaces", *Algebr. Geom. Topol.* **20** (2002), no. 1, p. 451–485.
[16] D. Margalit – "Problems, questions, and conjectures about mapping class groups", in *Breadth in contemporary topology: 2017 Georgia International Topology Conference*, Proc. Sympos. Pure Math., vol. 102, Amer. Math. Soc., Providence, RI, 2019, p. 157–186.
[17] C. T. McMullen – "Teichmüller geodesics of infinite complexity", *Acta Math.* **191** (2003), no. 2, p. 191–223.
[18] ———, "Cascades in the dynamics of measured foliations", *Ann. Sci. Éc. Norm. Supér. (4)* **48** (2015), no. 1, p. 1–39.
[19] R. C. Penner – "A construction of pseudo-Anosov homeomorphisms", *Trans. Amer. Math. Soc.* **310** (1988), no. 1, p. 179–197.
[20] ———, "Bounds on least dilatations", *Proc. Amer. Math. Soc.* **113** (1991), no. 2, p. 443–450.
[21] G. Poggiaspalla, J. H. Lowenstein & F. Vivaldi – "Geometric representation of interval exchange maps over algebraic number fields", *Nonlinearity* **21** (2008), no. 1, p. 149–177.
[22] B. Strenner – "Algebraic degrees of pseudo-Anosov stretch factors", *Geom. Funct. Anal.* **27** (2017), no. 6, p. 1497–1539.
[23] ———, "Lifts of pseudo-Anosov homeomorphisms of nonorientable surfaces have vanishing SAF invariant", *Math. Res. Lett.* **25** (2018), no. 2, p. 677–685.
[24] W. P. Thurston – "On the geometry and dynamics of diffeomorphisms of surfaces", *Bull. Amer. Math. Soc. (N.S.)* **19** (1988), no. 2, p. 417–431.

Bull. Soc. Math. France
148 (3), 2020, p. 399-409

NOMBRE DE CLASSES DE CONJUGAISON D'ÉLÉMENTS D'ORDRE FINI DANS LES GROUPES DE BROWN-THOMPSON

par Hajer Hmili Ben Ammar & Isabelle Liousse

Résumé. — Nous étendons un résultat de Matucci ([13]) sur le nombre de classes de conjugaison d'éléments d'ordre fini dans le groupe de Thompson T. D'après [12], le groupe de Brown-Thompson $T_{r,m}$ ne contient pas d'élément d'ordre q lorsque $\mathrm{pgcd}(m-1,q)$ ne divise pas r. Nous montrons que si $\mathrm{pgcd}(m-1,q)$ divise r alors il y a exactement $\varphi(q)\cdot\mathrm{pgcd}(m-1,q)$ classes de conjugaison d'éléments d'ordre q dans $T_{r,m}$, où φ est la fonction phi d'Euler. Comme corollaire, nous obtenons que le groupe de Thompson T n'est isomorphe à aucun des groupes $T_{r,m}$ avec $m\neq 2$ et tout morphisme de T dans $T_{r,m}$, avec $m\neq 2$ et $r\neq 0\ mod\,(m-1)$, est trivial.

Texte reçu le 22 janvier 2019, modifié le 7 mai 2019, accepté le 28 novembre 2019.

Hajer Hmili Ben Ammar, Unité d'analyse mathématique et applications, Département de mathématiques, Faculté des Sciences de Tunis, Tunisie • *E-mail :* hajermido@yahoo.fr
Isabelle Liousse, Laboratoire Paul Painlevé, Université de Lille, 59655 Villeneuve d'Ascq Cédex, France • *E-mail :* liousse@univ-lille.fr

Classification mathématique par sujets (2010). — 20E45, 37E10, 37E15.

Mots clefs. — Groupes de Thompson, Groupes de Brown, Éléments de torsion, Classes de conjugaison, Homéomorphismes PL du cercle, Isomorphismes.

Hajer Hmili remercie l' Unité d'analyse mathématique et applications de la Faculté des Sciences de Tunis et exprime sa gratitude à son mari Mourad Ben Ammar pour son soutien. Isabelle Liousse remercie le Labex CEMPI (ANR-11-LABX-0007-01), le projet ANR Gromeov (ANR-19-CE40-0007) et le CNRS pour sa délégation 2019-20.

© Société Mathématique de France
0037-9484/2020/399/$ 5.00
doi:10.24033/bsmf.2810

Abstract (*Number of conjugacy classes of torsion elements in Brown-Thompson groups*). — We extend a result of Matucci ([13]) on the number of conjugacy classes of finite order elements in the Thompson group T. According to [12], if $gcd(m-1,q)$ is not a divisor of r then there does not exist element of order q in the Brown-Thompson group $T_{r,m}$. We show that if $gcd(m-1,q)$ is a divisor of r then there are exactly $\varphi(q).gcd(m-1,q)$ conjugacy classes of elements of order q in $T_{r,m}$, where φ is the Euler function phi. As a corollary, we obtain that the Thompson group T is isomorphic to none of the groups $T_{r,m}$, for $m \neq 2$ and any morphism from T into $T_{r,m}$, with $m \neq 2$ and $r \neq 0 \ mod\,(m-1)$, is trivial.

1. Introduction et définitions

En 1965, R. Thompson découvrit les premiers exemples de groupes $T \subset V$ de présentation finie, simples et infinis. Le groupe T [resp. V] se représente comme groupe d'homéomorphismes [resp. échanges d'intervalles] affines par morceaux du cercle (voir [6], [14]). En 1987, K. Brown ([5]) a défini une famille $T_{r,m} \subset V_{r,m}$ englobant T et V et les groupes $V_{r,m}$ sont isomorphes aux groupes $G_{r,m}$ de Higman ([10]).

Plus précisément, soit r un entier strictement positif, on note $\mathbb{S}_r$ le cercle $\mathbb{R}/r\mathbb{Z}$ de longueur r. Le cercle de longueur 1 est $\mathbb{S}_1$, nous le noterons plus classiquement $\mathbb{S}^1$.

Définition. — Un homéomorphisme f du cercle $\mathbb{S}_r$ est *affine par morceaux* s'il existe une subdivision finie $0 < a_1 < a_2 < \cdots < a_p = r$ de l'intervalle $[0,r]$ et un relevé $\tilde{f}$ de f à $\mathbb{R}$ tels que $\tilde{f}_{|[a_i,a_{i+1}]}(x) = \lambda_i x + \beta_i$, $\lambda_i, \beta_i \in \mathbb{R}$.

Les points a_i sont appelés *points de coupure* de f et les nombres λ_i, *pentes de* f.

Le groupe des homéomorphismes affines par morceaux de $\mathbb{S}_r$ préservant l'orientation est noté $PL^+(\mathbb{S}_r)$.

Définition. — Soient r et $m \geq 2$ deux entiers strictement positifs. On définit le *groupe de Brown-Thompson* $T_{r,m}$ comme l'ensemble des éléments f de $PL^+(\mathbb{S}_r)$ tels que :

- les pentes de f appartiennent à $\langle m \rangle = \{m^s, s \in \mathbb{Z}\}$.
- les points de coupure de f appartiennent à $\mathbb{Z}[\frac{1}{m}] = \{N.m^s | N, s \in \mathbb{Z}\}$,
- les images par f de 0 et des points de coupure de f appartiennent à $\mathbb{Z}[\frac{1}{m}]$.

Le *groupe de Thompson* T est $T_{1,2}$.

De nombreux auteurs se sont intéressés aux invariants et à la question d'isomorphicité pour ces groupes de type Thompson ([1], [2], [3], [4], [5], [10], [12], [13], [14], ...).

Dans cet article, nous nous concentrons sur les obstructions à l'isomorphicité entre groupes $T_{r,m}$ issues des éléments d'ordre fini et de leurs classes de conjugaison. Le calcul du nombre de ces classes fût effectué pour $G_{r,m}$ par Higman ([10], section 6), pour T par Matucci ([13]) puis ultérieurement par Geoghegan-Varisco ([8]) et Fossas ([7]). Comme dans [13] et [8], nous utilisons la représentation comme groupe d'homéomorphismes affines par morceaux du cercle et disposons ainsi d'un invariant dynamique suplémentaire : le nombre de rotation de Poincaré. Nous indiquons sa définition et ses premières propriétés (voir [9] ou [11]).

DÉFINITION. — Soit f un homéomorphisme du cercle $\mathbb{S}_r$, on définit le *nombre de rotation sur* $\mathbb{S}_r$ de f par :

$$\rho(f) = \lim_{n\to\infty} (\tilde{f}^n(0)/rn) \,(mod\, 1) \in \mathbb{S}^1.$$

Ce nombre ne dépend pas du choix du relevé $\tilde{f}$ et satisfait les propriétés classiques :

PROPRIÉTÉS. —
- $\rho(R_\alpha) = \frac{\alpha}{r}$ *où* $R_\alpha(x) = x + \alpha \,(mod\, r)$,
- $\rho(f^n) = n\,\rho(f)$ *pour tout* $n \in \mathbb{Z}$,
- *si* f *est d'ordre fini* $q \in \mathbb{N}^{>1}$ *alors* $\rho(f) = \frac{p}{q}$ *avec* $p < q$ *et* $p \wedge q = 1$,
- *soit* $h : \mathbb{S}_r \to \mathbb{S}_{r'}$ *un homéomorphisme préservant l'orientation alors* $\rho(h \circ f \circ h^{-1}) = \rho(f)$.

Commençons par cette observation : tout élément d'ordre q est conjugué dans $PL^+(\mathbb{S}^1)$ à une rotation d'angle $\frac{p}{q}$ avec $p \wedge q = 1$, une conjuguante est construite par moyennisation (voir par exemple [11], Proposition 11.2.2). Comme deux rotations d'angles différents ne sont jamais C^0-conjuguées, le nombre de classes de conjugaison d'éléments d'ordre q dans $PL^+(\mathbb{S}^1)$ est exactement le nombre d'entiers $p < q$ premiers avec q c'est à dire $\varphi(q)$ (la fonction phi d'Euler).

Le Théorème 7.1.5 de [13] (voir aussi [8] et [7]) exprime qu'il est encore vrai pour le groupe de Thompson T : « *dans* T*, tout rationnel de* $\mathbb{S}^1$ *est réalisé comme nombre de rotation d'une unique classe de conjugaison d'éléments d'ordre fini* ».

Ici, nous établissons que cette propriété n'est plus satisfaite par les autres groupes $T_{r,m}$:

THÉORÈME 1.1. — *Soient* $r \geq 1$, $m \geq 2$ *et* $q \geq 2$ *des entiers.*

A. Si $\mathrm{pgcd}(m-1, q)$ *ne divise pas* r *alors il y a* 0 *classes de conjugaison d'éléments d'ordre* q *dans* $T_{r,m}$.

B. Si $\mathrm{pgcd}(m-1, q)$ *divise* r *alors il y a* $\mathrm{pgcd}(m-1, q)$ *classes de conjugaison d'éléments d'ordre* q *et de nombre de rotation* $\frac{p}{q}$ *dans* $T_{r,m}$*, pour tout entier* p *premier avec* q.

C. Si $\mathrm{pgcd}(m-1, q)$ *divise* r *alors il y a* $\varphi(q) \cdot \mathrm{pgcd}(m-1, q)$ *classes de conjugaison d'éléments d'ordre* q *dans* $T_{r,m}$.

Nous en déduisons le

COROLLAIRE 1.2. — *Tout rationnel de $\mathbb{S}^1$ est réalisé comme nombre de rotation d'une unique classe de conjugaison d'éléments d'ordre fini dans $T_{r,m}$ si et seulement si $m = 2$.*

Le groupe de Thompson T n'est isomorphe à aucun des groupes $T_{r,m}$ avec $m \neq 2$ et tout morphisme de T dans $T_{r,m}$, avec $m \neq 2$ et $r \neq 0 \ mod\,(m-1)$, est trivial.

Ce corollaire contraste avec le résultat d'ubiquité de F montré par Brin ([3]). Notre approche diffère de celles de [13], [8] et [7] au sens où elle est essentiellement basée sur un critère dû à Bieri et Strebel [1].

REMARQUE 1.3. — Considérons un entier $m \in \mathbb{N}^{>1}$. La réduction modulo $m-1 : \mathbb{Z} \to \mathbb{Z}_{m-1} = \mathbb{Z}/(m-1)\mathbb{Z} = \{0, \dots, m-2\}$, $n \mapsto [n]$ envoie m sur 1. Par conséquent, elle s'étend en un morphisme d'anneaux $\mathbb{Z}[\frac{1}{m}] \to \mathbb{Z}_{m-1}$, $\frac{n}{m^s} \mapsto [n]$ qui coïncide avec l'application quotient par l'idéal principal $(m-1)\mathbb{Z}[\frac{1}{m}]$.

Maintenant, toute application affine de $\mathbb{Z}[\frac{1}{m}]$ dans lui même de la forme $x \mapsto m^k x + \frac{N}{m^l}$ passe au quotient par cet idéal et l'application quotient est la translation $\mathbb{Z}_{m-1} \to \mathbb{Z}_{m-1}$, $[x] \mapsto [x] + [a]$.

Par récurrence sur le nombre d'intervalles où il est affine et par continuité en ses points de coupure, tout PL_m-homéomorphisme $f : [a, b] \to [a', b']$ induit une application $\bar{f}_m : \mathbb{Z}_{m-1} \to \mathbb{Z}_{m-1}$ qui est la translation $[x] \mapsto [x] + [a' - a]$ et l'application $f \mapsto \bar{f}_m$ est compatible avec la composition.

Finalement, les classes de conjugaisons dans $T_{r,m}$ des éléments de torsion de nombre de rotation $\frac{1}{q}$ sont caractérisées par l'image de 0 dans $\mathbb{Z}_{m-1}$. D'autre part, un point de $\mathbb{Z}_{m-1}$ est ainsi réalisé si et seulement si il est solution de l'équation de congruence $qa \equiv r$ (voir e.g. (2) $\Rightarrow$ (1) de la Proposition 3.3). On retrouve essentiellement le Théorème 1.1 en notant que cette équation n'a pas de solution si r ne divise pas $\mathrm{pgcd}(q, m-1)$ et en a $\mathrm{pgcd}(q, m-1)$ sinon.

2. Préliminaires

2.1. Critère de Bieri-Strebel pour les groupes de Brown-Thompson. — Nous reprennons ici le critère général de Bieri-Strebel déterminant à quelles conditions deux intervalles réels sont échangés par une application affine par morceaux avec points de coupure et pentes prescrites (voir le Théorème A 4.1 de [1]).

DÉFINITION. —
- Un *m-intervalle* est un intervalle réel dont les extrémités sont dans $\mathbb{Z}\left[\frac{1}{m}\right]$.
- Un homéomorphisme $f : I \to I'$ est dit PL_m s'il est affine par morceaux avec pentes dans $\langle m \rangle$ et points de coupure dans $\mathbb{Z}\left[\frac{1}{m}\right]$.
- Deux intervalles I et I' sont dits *PL_m-équivalents* s'il existe un homéomorphisme PL_m entre-eux.

PROPOSITION 2.1 ([1], [12]). — *Deux m-intervalles I et I' sont PL_m-équivalents si et seulement si $|I|-|I'| \in (m-1).\mathbb{Z}\left[\frac{1}{m}\right]$, où $|I|$ représente la longueur de l'intervalle I.*

Démonstration. — Soient $I=[a,c]$ et $I'=[a',c']$ avec $a,a',c,c' \in \mathbb{Z}\left[\frac{1}{m}\right]$. Supposons qu'il existe f un homéomorphisme PL_m entre I et I'. Notons $a=b_0<b_1<\cdots<b_{n-1}<b_n=c$, $b_i \in \mathbb{Z}\left[\frac{1}{m}\right]$, les points de coupure de f et $\lambda_i=m^{k_i}$, $k_i \in \mathbb{Z}$, la pente de f sur $[b_{i-1},b_i]$. Nous allons montrer que $|I|-|I'|=(c-a)-(c'-a') \in (m-1).\mathbb{Z}\left[\frac{1}{m}\right]$.

Comme

$$c-a=\sum_i (b_i-b_{i-1}) \quad \text{et} \quad c'-a'=\sum_i \lambda_i(b_i-b_{i-1}),$$

on a

$$(c-a)-(c'-a')=\sum_i (1-\lambda_i)(b_i-b_{i-1})$$

et

$$(1-\lambda_i)=-(m-1)\sum_{p=0}^{k_i-1} m^p=(m-1)M_i \quad \text{avec } M_i \in \mathbb{Z}$$

et finalement

$$(c-a)-(c'-a')=(m-1)\sum_i M_i(b_i-b_{i-1}) \in (m-1)\mathbb{Z}\left[\frac{1}{m}\right].$$

Réciproquement, supposons

$$(*) \qquad |I|-|I'| \in (m-1)\mathbb{Z}\left[\frac{1}{m}\right].$$

Quitte à composer à la source et au but par des rotations d'angles convenables dans $\mathbb{Z}\left[\frac{1}{m}\right]$, on peut supposer que $I=[0,b]$ et $I'=[0,b']$ avec $b,b' \in \mathbb{Z}\left[\frac{1}{m}\right]$ positifs.

La condition $(*)$ se traduit par le fait qu'il existe $a \in \mathbb{Z}\left[\frac{1}{m}\right]$ tel que $b'=b+(m-1)a$ et il s'agit de construire un PL_m-homéomorphisme $f:[0,b] \to [0,b+(m-1)a]$ pour tous $a,b \in \mathbb{Z}\left[\frac{1}{m}\right]$ avec $b \geq 0$ et $b+(m-1)a \geq 0$. L'inverse d'un homéomorphisme PL_m entre m-intervalles étant PL_m, on peut aussi supposer, quitte à échanger b et b', que $a \geq 0$.

CAS 1 ($a<b$ ($0 \leq b-a \leq b$)). — L'application $f_0:[0,b] \to [0,b+(m-1)a]$ définie par

$$f_0(x)=\begin{cases} x & \text{si } x \in [0,b-a] \\ m(x-(b-a))+(b-a) & \text{si } x \in [b-a,b] \end{cases}$$

est l'homéomorphisme PL_m cherché.

Cas 2 ($a \geq b$). — Choisissons $p \in \mathbb{N}$ tel que $0 \leq m^{-p}a < b$. D'après le cas 1, il existe $f_0 : [0, b] \to [0, b+(m-1)m^{-p}a]$ ayant les propriétés requises. On définit alors $f_1 : [0, b + (m-1)m^{-p}a] \to [0, b + (m-1)a]$ par

$$f_1(x) = \begin{cases} x & \text{si } x \in [0, b] \\ m^p(x-b)+b & \text{si } x \in [b, b+(m-1)m^{-p}a]. \end{cases}$$

L'application cherchée est $f = f_1 \circ f_0$. □

Conséquence (Isomorphisme de Bieri-Strebel). — *Soient $m > 1$ un entier, si r et r' sont deux entiers positifs congrus modulo $m-1$ alors les groupes $T_{r,m}$ et $T_{r',m}$ sont isomorphes. Par suite tout $T_{r',m}$ est isomorphe à l'un des $m-1$ groupes $T_{r,m}$, $r \in 1, \ldots, m-1$.*

Remarque 2.2. — Tous les intervalles dyadiques sont PL_2-équivalents et par suite tous les groupes $T_{r,2}$ sont isomorphes à T.

2.2. Nombres de rotation des éléments d'ordre fini. —

Proposition 2.3 ([12]). — *Soient $m \geq 2$, $r \geq 1$ et $q \geq 1$ des entiers.*

1. *Si le groupe $T_{r,m}$ contient un élément d'ordre q alors pour tout $p \in \mathbb{N}^*$, le groupe $T_{r,m}$ contient un élément d'ordre fini de nombre de rotation $\frac{p}{q}$.*
2. *Le groupe $T_{r,m}$ contient un élément d'ordre q si et seulement si* $\mathrm{pgcd}(m-1, q)$ *divise r.*

Démonstration. — Nous supposons $q \geq 2$, pour $q = 1$ le résultat est trivial.

Premier item. Supposons qu'existe $f \in T_{r,m}$ d'ordre q. On a $\rho(f) = \frac{n}{q}$ où les entiers n et q sont premiers entre-eux. Par Bezout, il existe u et v entiers tels que $1 = un + vq$.

Soit $p \in \mathbb{N}^*$, on définit un élément d'ordre fini de $T_{r,m}$ par $g = f^{up}$. On a $\rho(g) = \rho(f^{up}) = up\rho(f) = \frac{upn}{q} = \frac{p(1-vq)}{q} = \frac{p}{q} - pv = \frac{p}{q}(mod\, 1)$.

Deuxième item.

Condition nécessaire. Supposons que r soit un multiple de $\mathrm{pgcd}(q, m-1)$. D'après Bezout, $r = uq+v(m-1)$, donc $r = uq$ modulo $(m-1)$. L'isomorphisme de Bieri-Strebel implique que les groupes $T_{uq,m}$ et $T_{r,m}$ sont isomorphes. De plus, le groupe $T_{uq,m}$ contient la rotation $x \mapsto x + u$ d'ordre q et de nombre de rotation $\frac{1}{q}$.

Condition suffisante. Par hypothèse et d'après le premier item, il existe $f \in T_{r,m}$ d'ordre q et $\rho(f) = \frac{1}{q}$. Fixons $\tilde{f}$ un relevé de f à $\mathbb{R}$ et identifions f à $\tilde{f}(mod\, r)$.

La f-orbite de 0 est ordonnée comme suit $0 < f(0) < \cdots < f^{q-1}(0) < r$.

Les q intervalles $I_i := [f^{i-1}(0), f^i(0)]$, $i = 1, \cdots, q$, sont tous PL_m-équivalents, donc d'après le critère de Bieri-Strebel, $|I_i| = |I_1| \, mod\, (m-1)\mathbb{Z}\left[\frac{1}{m}\right]$ et

$|I_1| = f(0)$. Par conséquent

$$r = |I_1| + \cdots + |I_q| = qf(0) \, mod \, (m-1)\mathbb{Z}\left[\frac{1}{m}\right].$$

On en déduit qu'il existe des entiers u, v, s tels que $r - qf(0) = (m-1)\frac{v}{m^s}$ et $f(0) = \frac{u}{m^s}$. Ainsi, $m^s r - qu = (m-1)v$, autrement dit $m^s r = qu + (m-1)v$. Ceci implique que $m^s r$ est un multiple du $\mathrm{pgcd}(q, m-1)$. Les entiers $(m-1)$ et m^s étant premiers entre-eux, on conclut que r est un multiple de $\mathrm{pgcd}(q, m-1)$. □

2.3. Critère de Conjugaison PL_m. —

Proposition 2.4. — *Soient f_1 et f_2 deux éléments de $T_{r,m}$ d'ordre fini q et de nombre de rotation $\frac{1}{q}$, on note $f_i(0) = \frac{N_i}{m^{s_i}}$, $i = 1, 2$. Les propriétés suivantes sont équivalentes :*

1. *f_1 et f_2 sont PL_m-conjugués (dans $T_{r,m}$),*
2. *$N_2 - N_1$ est un multiple de $m-1$,*
3. *$f_1(0) - f_2(0) \in (m-1)\mathbb{Z}[\frac{1}{m}]$ (autrement dit, les intervalles $[0, f_1(0)]$ et $[0, f_2(0)]$ sont PL_m-équivalents).*

Démonstration. —

Lemme 2.5. — *Soit $a = \frac{N_a}{m^{s_a}} \in \mathbb{Z}[\frac{1}{m}]$, tout homéomorphisme $f \in T_{r,m}$ d'ordre q, de nombre de rotation $\frac{1}{q}$ et vérifiant $f(0) = a$ est PL_m-conjugué à la rotation R_{N_a} de $\mathbb{S}_{qN_a}$.*

Démonstration. — L'intervalle $[0, r[$ s'écrit $\bigcup_{i=1}^{q} I_i$, où $I_i = [f^{i-1}(0), f^i(0)]$.

On considère l'application affine $H_1 : I_1 = [0, a] \to [0, N_a]$, $x \mapsto m^{s_a}.x$ et on définit par récurrence $H_i : I_i \to [(i-1)N_a, iN_a]$ par $H_{i+1} = R_{N_a} \circ H_i \circ f^{-1}$.

On vérifie facilement que l'application $H : \mathbb{S}_r \to \mathbb{S}_{qN_a}$ définie par $H_{|I_i} = H_i$ est un PL_m-homéomorphisme qui conjugue f à R_{N_a}. □

(1) $\implies$ (2). D'après le lemme précèdent, f_i est PL_m-conjuguée à la rotation R_{N_i} de $\mathbb{S}_{qN_i}$. Il nous reste à étudier à quelles conditions deux telles rotations sont PL_m-conjuguées.

Soit $h : \mathbb{S}_{qN_1} \to \mathbb{S}_{qN_2}$ une PL_m-conjugaison entre R_{N_1} et R_{N_2}, quitte à composer au but h par la rotation $R_{-h(0)}$ de $\mathbb{S}_{qN_2}$, on peut supposer que $h(0) = 0$.

Les intervalles $[0, N_1]$ et $[0, N_2]$ étant PL_m-équivalents, l'entier $N_2 - N_1 \in (m-1)\mathbb{Z}[\frac{1}{m}]$ et par suite $N_2 - N_1$ est un multiple de $m-1$.

(2) $\implies$ (1). Si $N_2 - N_1$ est un multiple de $(m-1)$ alors $[0, N_1]$ et $[0, N_2]$ sont PL_m-équivalents et on peut reprendre la preuve du lemme précédent avec pour H_1 l'homéomorphisme de Bieri-Strebel qui échange ces 2 intervalles.

(2) $\Longleftrightarrow$ (3) résulte du calcul suivant :

$$f_1(0) - f_2(0) = \frac{N_1}{m^{s_1}} - \frac{N_2}{m^{s_2}} = N_1(m^{-s_1} - 1) - N_2(m^{-s_2} - 1) + (N_1 - N_2)$$
$$= (N_1 - N_2)\, mod\, (m-1)\mathbb{Z}\left[\frac{1}{m}\right]. \qquad \square$$

3. Classes de conjugaison d'éléments d'ordre fini dans les groupes de Brown-Thompson

LEMME 3.1. — *Soient p et $q > 1$ deux entiers premiers entre-eux et $u > 0$, v entiers tels que $up + vq = 1$.*

Deux éléments f_1 et f_2 de $T_{r,m}$ d'ordre fini q et de nombre de rotation $\frac{p}{q}$ sont PL_m-conjugués si et seulement si f_1^u et f_2^u (de nombre de rotation $\frac{1}{q}$) sont PL_m-conjugués.

La preuve de ce lemme résulte du fait que la PL_m-conjugaison se transmet aux puissances et des généralités suivantes :

On a $\rho(f^u) = \frac{up}{q} = \frac{1-vq}{q} = \frac{1}{q}$ et $(f^u)^p = f^{1-vq} = f$ dès que f est d'ordre fini q.

REMARQUE 3.2. — Une conséquence de ce lemme est qu'étant donnés p et q deux entiers premiers entre-eux, le nombre de classes de conjugaison d'éléments d'ordre fini q et de nombre de rotation $\frac{p}{q}$ ne dépend pas de p.

3.1. Classes de conjugaisons dans $T_{r,2}$. — Soit $q \in \mathbb{N}^*$, d'après l'invariance par conjugaison topologique du nombre de rotation et la remarque précédente, il suffit de déterminer le nombre de classes de conjugaison d'éléments d'ordre q et de nombre de rotation $\frac{1}{q}$.

La Proposition 2.3 indique que $T_{r,2}$ contient un élément f_1 d'ordre q et de nombre de rotation $\frac{1}{q}$. Tous les intervalles dyadiques étant PL_2-équivalents par la Remarque 2.2, l'item (3) de la Proposition 2.4 est vérifié pour tout autre $f_2 \in T_{r,2}$ d'ordre q et de nombre de rotation $\frac{1}{q}$. On en déduit qu'il y a exactement une classe de conjugaison d'éléments d'ordre q et de nombre de rotation $\frac{1}{q}$; le résultat de Matucci en découle.

3.2. Preuve du Théorème 1.1. —

Preuve de l'item A. — Il résulte directement de l'item (2) de la Proposition 2.3.

Preuve de l'item B. — Par la Remarque 3.2, il suffit d'établir le résultat pour $p = 1$.

PROPOSITION 3.3. — *Soient* $q \in \mathbb{N}^{>1}$ *et* $a = \frac{N_a}{m^{s_a}} \in \mathbb{Z}[\frac{1}{m}] \cap]0, r[$. *Les propriétés suivantes sont équivalentes*

1. *Il existe* $f \in T_{r,m}$ *d'ordre* q, *vérifiant* $f(0) = a$ *et de nombre de rotation* $\frac{1}{q}$.
2. $r - qa \in (m-1)\mathbb{Z}[\frac{1}{m}]$.
3. $r - qN_a$ *est un multiple de* $m - 1$.

Démonstration. — (1) $\implies$ (2). Comme dans la preuve de la Proposition 2.3, les q intervalles $I_i := [f^{i-1}(0), f^i(0)[$, $i = 1, \cdots, q$, sont tous PL_m-équivalents et forment une partition de $[0, r[$. Par conséquent $r = q|I_1| = qf(0) \, mod \, (m-1)\mathbb{Z}[\frac{1}{m}]$.

(2) $\implies$ (1). Supposons que $r - qa \in (m-1)\mathbb{Z}[\frac{1}{m}]$ et considérons la rotation $R_a : x \mapsto x + a$ sur le cercle de longueur $qa \in \mathbb{Z}[\frac{1}{m}]$. Soit h l'homéomorphisme PL_m qui vaut l'identité sur $[0, a]$ et qui envoie $[a, qa]$ sur $[a, r]$ (son existence est assurée par le critère de Bieri-Strebel, Proposition 2.1).

Ainsi l'homéomorphisme $f_a = h \circ R_a \circ h^{-1} \in T_{r,m}$ est d'ordre q, de nombre de rotation $\frac{1}{q}$ et satisfait $f_a(0) = a$.

(2) $\iff$ (3) est conséquence du calcul suivant :

$$\begin{aligned} & r - qa = r - q\frac{N_a}{m^{s_a}} = \frac{rm^{s_a} - qN_a}{m^{s_a}} \in (m-1)\mathbb{Z}\left[\frac{1}{m}\right] \\ \iff \quad & rm^{s_a} - qN_a = r(m^{s_a} - 1) + (r - qN_a) \text{ est un multiple de } m-1 \\ \iff \quad & r - qN_a \text{ est un multiple de } m - 1. \end{aligned}$$

□

Nous pouvons maintenant calculer le nombre de classes de conjugaison d'éléments d'ordre q de nombre de rotation $\frac{1}{q}$ dans $T_{r,m}$. D'après les Propositions 2.4 et 3.3, cette quantité est égale au nombre de classes modulo $(m-1)$ d'entiers N tels que $r - qN$ est un multiple de $m - 1$, nous affirmons que c'est $d = \text{pgcd}(m-1, q)$.

En effet, sous la condition d divise r, le critère d'isomorphisme de Bieri-Strebel nous permet de supposer que $r = qu$. Posons $P = u - N$, on a $r - qN = q(u-N) = qP$, le problème se ramène à déterminer le nombre de classes modulo $(m-1)$ d'entiers P tels que qP est un multiple de $m - 1$.

Puisque $m - 1 = m_0.d$ et $q = q_0.d$ avec $m_0 \wedge q_0 = 1$, l'entier qP est un multiple de $m - 1$ si et seulement si $q_0 P$ est un multiple de m_0 et donc si et seulement si P est un multiple de m_0. Par conséquent, il y a exactement d tels entiers entre 0 et $m - 2$.

Preuve de l'item C. — D'après l'invariance par conjugaison topologique du nombre de rotation et la Remarque 3.2, le nombre de classes de conjugaison d'éléments d'ordre q dans $T_{r,m}$ est $\varphi(q) \cdot \text{pgcd}(m-1, q)$, si $\text{pgcd}(m-1, q)$ divise r et 0 si non.

4. Problèmes d'isomorphisme et de plongement entre groupes de Brown-Thompson. Preuve du Corollaire 1.2

PROPOSITION 4.1. — *Soit* $m \in \mathbb{N}^{>1}$.

1. *Parmi les groupes* $T_{r,m}$*, pour* $0 < r \leq m-1$*, seul le groupe* $T_{m-1,m}$ *contient des éléments d'ordre quelconque. Ainsi, il n'existe pas de morphisme injectif* $T_{m-1,m} \to T_{r,m}$*, pour* $0 < r < m-1$.
2. *Si* $m_1 - 1$ *possède un diviseur premier qui ne divise pas* $m_2 - 1$ *alors il n'existe pas de morphisme injectif* $T_{1,m_2} \to T_{1,m_1}$.

Démonstration. — (1) Puisque pour tout $q \in \mathbb{N}^{>1}$, $\gcd(m-1, q)$ est un diviseur de $m-1$, le groupe $T_{m-1,m}$ contient des éléments de tout ordre. Réciproquement, si $0 < r < m-1$, $\gcd(m-1, m-1) = m-1$ ne divise pas r et il n'existe pas d'élément d'ordre $m-1$ dans $T_{r,m}$.

(2) Soit d un diviseur premier de $m_1 - 1$ ne divisant pas $m_2 - 1$. D'une part, $\gcd(m_1 - 1, d) = d$ ne divise pas $r = 1$ et T_{1,m_1} ne contient pas d'élément d'ordre d. D'autre part, $\gcd(m_2 - 1, d) = 1$ divise $r = 1$ et T_{1,m_2} contient des éléments d'ordre d. Par conséquent, il n'existe pas de morphisme injectif $T_{1,m_2} \to T_{1,m_1}$. □

Preuve du Corollaire 1.2. — Comme T est simple, tout morphisme de T dans $T_{r,m}$ est injectif ou trivial. D'après l'item (1) de la Proposition 4.1, si T s'injecte dans $T_{r,m}$, pour $0 < r \leq m-1$, alors $r = m-1$. De plus, $T_{m-1,m}$ contient $m-1$ classes de conjugaison d'éléments d'ordre $m-1$ et de nombre de rotation $\frac{1}{m-1}$ alors que T n'en contient qu'une. Ces groupes ne sont isomorphes que lorsque $m-1 = 1$, correspondant au seul cas où tout rationnel se réalise comme nombre de rotation d'une unique classe de conjugaison d'éléments d'ordre fini. □

Remerciements. — Nous adressons un grand remerciement au referee anonyme pour ses remarques, corrections, simplifications et surtout pour avoir partagé avec nous sa vision plus algébrique éclairant les mécanismes des preuves utilisés ici : la Remarque 1.3 lui est intégralement due.

BIBLIOGRAPHIE

[1] R. BIERI & R. STREBEL – *On groups of PL-homeomorphisms of the real line*, Mathematical Surveys and Monographs, vol. 215, American Mathematical Society, Providence, RI, 2016.

[2] M. G. BRIN – « The chameleon groups of Richard J. Thompson : automorphisms and dynamics », *Inst. Hautes Études Sci. Publ. Math.* (1996), no. 84, p. 5–33 (1997).

[3] ———, « The ubiquity of Thompson's group F in groups of piecewise linear homeomorphisms of the unit interval », *J. London Math. Soc. (2)* **60** (1999), no. 2, p. 449–460.

[4] M. G. Brin & F. Guzmán – « Automorphisms of generalized Thompson groups », *J. Algebra* **203** (1998), no. 1, p. 285–348.
[5] K. S. Brown – « Finiteness properties of groups », *J. Pure Appl. Algebra* **44** (1987), no. 1-3, p. 45–75.
[6] J. W. Cannon, W. J. Floyd & W. R. Parry – « Introductory notes on Richard Thompson's groups », *Enseign. Math. (2)* **42** (1996), no. 3-4, p. 215–256.
[7] A. Fossas – « On the number of conjugacy classes of torsion elements on Thompson's group T », *preprint* (2016).
[8] R. Geoghegan & M. Varisco – « On Thompson's group T and algebraic K-theory », *ArXiv e-prints* (2014).
[9] M.-R. Herman – « Sur la conjugaison différentiable des difféomorphismes du cercle à des rotations », *Inst. Hautes Études Sci. Publ. Math.* (1979), no. 49, p. 5–233.
[10] G. Higman – *Finitely presented infinite simple groups*, Department of Pure Mathematics, Department of Mathematics, I.A.S. Australian National University, Canberra, 1974, Notes on Pure Mathematics, No. 8 (1974).
[11] A. Katok & B. Hasselblatt – *Introduction to the modern theory of dynamical systems*, Encyclopedia of Mathematics and its Applications, vol. 54, Cambridge University Press, Cambridge, 1995, With a supplementary chapter by Katok and Leonardo Mendoza.
[12] I. Liousse – « Rotation numbers in Thompson-Stein groups and applications », *Geom. Dedicata* **131** (2008), p. 49–71.
[13] F. Matucci – *Algorithms and classification in groups of piecewise-linear homeomorphisms*, ProQuest LLC, Ann Arbor, MI, 2008, Thesis (Ph.D.)–Cornell University.
[14] M. Stein – « Groups of piecewise linear homeomorphisms », *Trans. Amer. Math. Soc.* **332** (1992), no. 2, p. 477–514.

Bull. Soc. Math. France
148 (3), 2020, p. 411-438

SYMMETRIC KILLING TENSORS ON NILMANIFOLDS

BY VIVIANA DEL BARCO & ANDREI MOROIANU

ABSTRACT. — We study left-invariant symmetric Killing 2-tensors on two-step nilpotent Lie groups endowed with a left-invariant Riemannian metric and construct genuine examples, which are not linear combinations of parallel tensors and symmetric products of Killing vector fields.

RÉSUMÉ (*Tenseurs de Killing symétriques sur les nilvariétés*). — Nous étudions les 2-tenseurs de Killing symétriques invariants à gauche sur les groupes de Lie nilpotents de longueur 2 munis d'une métrique riemannienne invariante à gauche, et nous construisons des exemples de tels tenseurs qui ne sont pas des combinaisons linéaires de tenseurs parallèles et de produits symétriques de champs de vecteurs de Killing.

1. Introduction

A symmetric Killing tensor on a Riemannian manifold (M, g) is a smooth function defined on the tangent bundle of M, which is polynomial in the vectorial coordinates and constant along the geodesic flow. As such, symmetric

Texte reçu le 3 décembre 2018, modifié le 4 septembre 2019, accepté le 14 février 2020.

VIVIANA DEL BARCO, Université Paris-Saclay, CNRS, Laboratoire de mathématiques d'Orsay, 91405, Orsay, France and Universidad Nacional de Rosario, CONICET, 2000, Rosario, Argentina • *E-mail :* viviana.del-barco@math.u-psud.fr
ANDREI MOROIANU, Université Paris-Saclay, CNRS, Laboratoire de mathématiques d'Orsay, 91405, Orsay, France • *E-mail :* andrei.moroianu@math.cnrs.fr

Mathematical subject classification (2010). — 53D25, 22E25.

Key words and phrases. — Symmetric Killing tensors, Geodesic flow, Two-step nilpotent Lie groups.

V. del Barco supported by FAPESP grants 2015/23896-5 and 2017/13725-4.

© Société Mathématique de France
0037-9484/2020/411/$ 5.00
doi:10.24033/bsmf.2811

Killing tensors have been extensively studied by physicists in the context of integrable systems, since they define first integrals of the equation of motion. More recently, they started to be the subject of systematic research in differential geometry. An account of their properties and constructions in modern language can be found in [6, 7, 16]. In this context, symmetric Killing tensors are characterized as symmetric tensor fields having vanishing symmetrized covariant derivatives.

Trivial examples of symmetric Killing tensors on Riemannian manifolds are parallel ones, as well as Killing vector fields. Symmetric tensor products of these particular tensors generate the subalgebra of *decomposable* symmetric Killing tensors. Thus, the following question arises: when does this subalgebra coincide with the whole algebra of symmetric Killing tensors? This is an open question in general (see, for instance, [3, Question 3.9]), but it has already been considered in some particular contexts. For instance, in the case of Riemannian manifolds with constant curvature, it is known that every symmetric Killing tensor is decomposable [17, 18]. On the contrary, there are Riemannian metrics on the 2-torus possessing *indecomposable* symmetric Killing 2-tensors [8, 11]. One should notice that this case is extreme, because these metrics lack Killing vector fields.

In this paper, we consider this question in the context of two-step nilpotent Lie groups endowed with a left-invariant Riemannian metric. Our challenge is to establish conditions for these Riemannian Lie groups to carry indecomposable left-invariant symmetric Killing 2-tensors, that is, which are not linear combinations of parallel tensors and symmetric products of Killing vector fields.

First integrals of the geodesic flow given by a left-invariant metric on two-step nilpotent Lie groups have been studied by several authors [4, 10, 13, 14], with particular focus on the integrability of the dynamical system. These works illustrate the difficulties and the importance of constructing first integrals of the equation of motion. Note that in our terminology, indecomposable symmetric Killing tensors correspond to first integrals, which are independent from the trivial ones (defined by the Killing vector fields and the parallel tensors).

Our starting point is the characterization of left-invariant symmetric 2-tensors on Riemannian two-step nilpotent Lie groups, which satisfy the Killing condition (see Proposition 4.1). Afterwards, we address the decomposability of these symmetric Killing 2-tensors.

In our presentation, we will stress on the fact that decomposable left-invariant symmetric Killing tensors can be obtained as a linear combination of symmetric products of Killing vector fields that *are not* left-invariant. This means that the problem can not be reduced to solve linear equations in the Lie algebra. We overcome this difficulty by combining the aforementioned characterization of symmetric Killing tensors together with the description of the Lie algebra

of Killing vector fields of a nilpotent Lie group given by Wolf [20]. We obtain in Proposition 5.5 and Theorem 5.10 that the decomposability of a symmetric Killing 2-tensor depends on the possibility of extending certain linear maps to skew-symmetric derivations of $\mathfrak{n}$.

The algebraic structure of two-step nilpotent Lie algebras of dimension ≤ 7 allows the existence of a large amount of skew-symmetric derivations. In particular, it turns out that the linear maps involved in Theorem 5.10 always extend to skew-symmetric derivations. As a consequence, we obtain that every left-invariant symmetric Killing 2-tensor in Riemannian two-step nilpotent Lie groups of dimension ≤ 7 is decomposable. On the contrary, we show that there are symmetric Killing tensors on two-step nilpotent Lie algebras of dimension 8 that are indecomposable. We actually provide a general construction method of indecomposable symmetric Killing tensors on two-step nilpotent Lie algebras in any dimension ≥ 8.

Taking compact quotients of nilpotent Lie groups admitting indecomposable symmetric Killing 2-tensors, we obtain new examples of compact Riemannian manifolds with indecomposable symmetric Killing tensors but also admitting nontrivial Killing vector fields. Other examples were constructed in [11, 12].

A brief account on the organization of the paper is the following. In Section 2, we introduce notations and give the preliminaries on nilpotent Lie groups endowed with a left-invariant Riemannian metric. We include the description of the Lie algebra of Killing vector fields as a consequence of the result of Wolf on the isometry groups of nilpotent Lie groups endowed with a left-invariant Riemannian metric. Section 3 reviews the basic results on symmetric Killing tensors. In Section 4, we characterize the symmetric endomorphisms on $\mathfrak{n}$ giving rise to left-invariant Killing 2-tensors on the Lie group N. We then show that the space of symmetric Killing 2-tensors decomposes according to the natural decomposition of a two-step nilpotent Lie algebra. Section 5 contains our main results on the decomposability of left-invariant symmetric Killing 2-tensors. We exhibit families of Lie algebras, all of whose left-invariant symmetric Killing 2-tensors are decomposable, i.e., linear combinations of parallel symmetric tensors and symmetric products of Killing vector fields. On the other hand, we show that this is not always the case by constructing examples of two-step nilpotent Lie algebras admitting indecomposable left-invariant symmetric Killing 2-tensors.

In the Appendix, we finally show several results concerning two-step nilpotent Lie groups. These include relevant results on parallel symmetric tensors, which are directly used in Section 5 of the paper, but we also present some more general results, which, we believe, are of independent interest.

2. Preliminaries on nilpotent Lie groups

This section intends to fix notations and to summarize the most relevant features of the geometry of nilpotent Lie groups endowed with a left-invariant metric.

Let N be a Lie group and denote the left and right translations by elements of the group, respectively, by

$$L_h : N \longrightarrow N,\ L_h(p) = hp, \quad R_h : N \longrightarrow N,\ R_h(p) = ph, \qquad h, p \in N.$$

Denote by I_h the conjugation by $h \in N$ on N, that is, $I_h = L_h \circ R_{h^{-1}}$. As usual, $\mathrm{Ad}(h)$ denotes the differential of I_h at e.

For each $h \in N$, L_h is a diffeomorphism of N, so its differential at $p \in N$, $(L_h)_{*p} : T_pN \longrightarrow T_{hp}N$ is an isomorphism. This map extends to an isomorphism from the space of (k,l) tensors $T_pN^{\otimes^k} \otimes T_p^*N^{\otimes^l}$ to $T_{hp}N^{\otimes^k} \otimes T_{hp}^*N^{\otimes^l}$, which we also denote by $(L_h)_{*p}$; we will sometimes omit the point p and simply write $(L_h)_*$. Given a differential form $\omega \in \Gamma(\Lambda^* N)$, the pullback $L_h^*\omega$ is the differential form given by $(L_h)_*\omega = (L_h^*)^{-1}\omega$.

From now on, we assume that N is a connected and simply connected nilpotent Lie group and we denote $\mathfrak{n}$ its Lie algebra. Then, the Lie group exponential mapping $\exp : \mathfrak{n} \longrightarrow N$ is a diffeomorphism [19]. We shall use this fact to write tensor fields on N as functions defined on $\mathfrak{n}$, taking values in the tensor algebra of $\mathfrak{n}$.

Let S be a tensor field on N, that is, a section of the bundle $\bigoplus_{k,l} TN^{\otimes^k} \otimes T^*N^{\otimes^l}$. For each $p \in N$, $S_p \in \bigoplus_{k,l} T_pN^{\otimes^k} \otimes T_p^*N^{\otimes^l}$, so that S defines a function $\Omega_S : \mathfrak{n} \longrightarrow \bigoplus_{k,l} \mathfrak{n}^{\otimes^k} \otimes \mathfrak{n}^{*\otimes^l}$ as follows:

$$\Omega_S(w) := (L_{\exp(-w)})_* S_{\exp w}, \quad w \in \mathfrak{n}. \tag{1}$$

The map Ω_S gives the value of S at $\exp w$, translated to $\mathfrak{n}$ by the appropriate left translation. This is a well-defined map, since $\exp : \mathfrak{n} \longrightarrow N$ is a diffeomorphism. Note that $S_p = (L_p)_{*e}\Omega_S(\exp^{-1} p)$, $p \in N$.

With this notation, we can introduce the usual concept of left-invariant tensors as follows:

Definition 2.1. — A left-invariant tensor field S on N is a tensor field, such that Ω_S is a constant function.

A vector field X on N with $X_e = x$ is left-invariant, if and only if $\Omega_X(w) = x$ for all $w \in \mathfrak{n}$, that is, $(L_{\exp -w})_* X_{\exp w} = x$. Replacing $p = \exp w$, this condition reads as the usual condition $X_p = (L_p)_{*e}x$ for all $p \in N$.

A Riemannian metric g on N is a section of the bundle $T^*N^{\otimes^2}$. Evaluated at the identity $e \in N$, g_e defines an inner product on $\mathfrak{n}$ and $\Omega_g(0) = g_e$. The Riemannian metric g is left-invariant, if and only if $\Omega_g(w) = g_e$, for all $w \in \mathfrak{n}$.

From (1), g is left-invariant, if and only if $(L_p)_*$ is an isometry for all $p \in N$, or $(L_p)^* g = g$.

REMARK 2.2. — There is a one-to-one correspondence between left-invariant tensor fields on N and elements in the tensor algebra of $\mathfrak{n}$. We will sometimes identify the corresponding objects. For instance, a left-invariant symmetric 2-tensor on N will be identified with an element in $\mathrm{Sym}^2\mathfrak{n}$ and vice versa.

Fix g as a left-invariant Riemannian metric on N. We denote also by g the inner product it defines in $\mathfrak{n}$. Let ∇ denote the Levi-Civita connection associated to g. The Koszul formula evaluated on left-invariant vector fields X, Y, Z reads

$$g(\nabla_X Y, Z) = \frac{1}{2}\{g([X,Y],Z) + g([Z,X],Y) + g([Z,Y],X)\}. \tag{2}$$

Then one has, since $(L_p)_*$ is an isometry for all $p \in N$, that $\nabla_X Y$ is left-invariant whenever X, Y are so. Moreover, for any left-invariant vector field X and any left-invariant tensor field S on N, the covariant derivative $\nabla_X S$ is also left-invariant. Thus, ∇ defines a linear map $\nabla : \mathfrak{n} \longrightarrow \mathrm{End}(\mathcal{T}(\mathfrak{n}))$ by $X \mapsto \nabla_X$, where $\mathcal{T}(\mathfrak{n}) = \bigoplus_{k,l} \mathfrak{n}^{\otimes^k} \otimes \mathfrak{n}^{*\otimes^l}$ is the tensor algebra of $\mathfrak{n}$.

To continue, we describe the Killing vector fields of the Riemannian manifold (N, g). Recall that a vector field ξ on N is a Killing vector field, if and only if its flow is given by isometries. In terms of the covariant derivative, ξ is a Killing vector field, if and only if $g(\nabla_X \xi, X) = 0$, for any vector field X.

The Riemannian manifold (N, g) is complete, because it is homogeneous. Therefore, every Killing vector field is complete, and the vector space of Killing vector field is finite dimensional. Endowed with the Lie bracket of vector fields, they constitute a Lie algebra that is isomorphic to the Lie algebra $\mathfrak{iso}(N)$ of the isometry group $\mathrm{Iso}(N)$ of N. We recall the results of Wolf on the structure of this isometry group [20].

The nilpotent Lie group N itself embeds as a subgroup of $\mathrm{Iso}(N)$ through the inclusion $g \in N \mapsto L_g \in \mathrm{Iso}(N)$, since the metric is left-invariant. Denote by $\mathrm{Auto}(N)$ the group of isometries of N that are also group automorphisms; these isometries fix the identity. Wolf shows that these two subgroups determine the isometry group of N and gives its precise algebraic structure.

THEOREM 2.3 ([20]). — *Let N be a connected nilpotent Lie group with a left-invariant metric g. Then, the isometry group* $\mathrm{Iso}(N)$ *is the semidirect product of the group of left translations and the group of isometric automorphism, that is,*

$$\mathrm{Iso}(N) = \mathrm{Auto}(N) \ltimes N,$$

where the action of $\mathrm{Auto}(N)$ *on N is $f \cdot L_h = L_{f(h)}$ for all $h \in N$, $f \in \mathrm{Auto}(N)$.*

The differential of an isometric automorphism $f \in \mathrm{Auto}(N)$ defines an orthogonal automorphism of the Lie algebra $\mathfrak{n}$, $f_{*e} \in \mathrm{Auto}(\mathfrak{n})$. Since N is simply connected, this correspondence is an isomorphism, and we have $\mathrm{Auto}(N) \simeq \mathrm{Auto}(\mathfrak{n})$. Let $[\ ,\ ]$ denote the Lie bracket on $\mathfrak{n}$. Then the Lie algebra of $\mathrm{Auto}(\mathfrak{n})$ is the subspace of skew-symmetric derivations of $\mathfrak{n}$, that is,

$$\mathrm{Dera}(\mathfrak{n}) = \{D \in \mathfrak{so}(\mathfrak{n}) \mid D[x,y] = [Dx,y] + [x,Dy] \text{ for all } x,y \in \mathfrak{n}\}.$$

The result of Wolf implies that the Lie algebra of the isometry group is $\mathfrak{iso}(N) = \mathrm{Dera}(\mathfrak{n}) \ltimes \mathfrak{n}$, where the semidirect product is defined by the canonical action of $\mathrm{Dera}(\mathfrak{n})$ on $\mathfrak{n}$. Therefore, we can distinguish two different types of Killing vector fields on N, namely, those corresponding to elements in the Lie algebra and those corresponding to skew-symmetric derivations.

The Killing vector field ξ_x associated to an element $x \in \mathfrak{n}$ is the right-invariant vector field on N, whose value at e is x: $(\xi_x)_p = (R_p)_{*e}x$, for all $p \in N$. In fact, the flow of this vector field is given by left translations, which are isometries. Given $p \in N$, $(\xi_x)_p = (R_p)_{*e}x = \frac{d}{dt}|_0 \exp tx \cdot p$. However, $R_p = L_p \circ I_{p^{-1}}$, and, hence, $(\xi_x)_p = (L_p)_{*e}(\mathrm{Ad}(p^{-1})x)$. If $w \in \mathfrak{n}$ is such that $p = \exp w$, then $\mathrm{Ad}(p^{-1}) = \mathrm{Ad}(\exp(-w))$, and, thus,

$$(\xi_x)_{\exp w} = (L_{\exp w})_{*e}(\mathrm{Ad}(\exp(-w))). \tag{3}$$

The Killing vector field ξ_D associated to a skew-symmetric derivation D of $\mathfrak{n}$ is constructed as follows. The derivation gives a curve e^{tD} in $\mathrm{Auto}(\mathfrak{n})$, which at the same time induces a curve of isometries $f_t \in \mathrm{Auto}(N)$ by the condition $(f_t)_{*e} = e^{tD}$, so it satisfies $(\xi_D)_p = \frac{d}{dt}|_0 f_t(p)$, $p \in N$. For any automorphism $f : N \longrightarrow N$, one has $f(p) = f(\exp w) = \exp f_{*e}w$. Hence, $(\xi_D)_p = \frac{d}{dt}|_0 \exp((f_t)_{*e}w) = \frac{d}{dt}|_0 \exp(e^{tD}w) = d\exp_w(Dw)$. Taylor's formula for the differential of the exponential map (see [9, Theorem 1.7, Ch. II]) gives

$$(\xi_D)_{\exp w} = d(L_{\exp w})_e(Dw - \frac{1}{2}\operatorname{ad}_w Dw + \frac{1}{6}\operatorname{ad}_w^2 Dw - \ldots). \tag{4}$$

This sum is finite, since $\mathfrak{n}$ is nilpotent.

Using the notation (1) of tensor fields on N as functions defined on $\mathfrak{n}$, and the fact that $\mathrm{Ad}(\exp(-w)) = e^{-\operatorname{ad}_w}$, for every $x \in \mathfrak{n}$ and $D \in \mathrm{Dera}(\mathfrak{n})$, we get from (3)–(4):

$$\Omega_{\xi_x}(w) = \mathrm{Ad}(\exp(-w)) = x - [w,x] + \frac{1}{2}[w,[w,x]] + \ldots, \quad \forall w \in \mathfrak{n}. \tag{5}$$

$$\Omega_{\xi_D}(w) = d\exp_w(Dw) = Dw - \frac{1}{2}[w,Dw] + \frac{1}{6}\operatorname{ad}_w^2 Dw - \ldots, \quad \forall w \in \mathfrak{n}. \tag{6}$$

Note that, in general, these Killing vector fields are not left-invariant. On the one hand, ξ_x is left-invariant, if and only if $\mathrm{Ad}(\exp(-w)) = x$, for all $w \in \mathfrak{n}$, that is, $I_p(x) = x$ for all $p \in N$, which occurs only when x is in the center of N. On the other hand, $\Omega_{\xi_D}(0) = 0$, so ξ_D is left-invariant, if and only if $D = 0$.

At this point, we will focus on the geometry of two-step nilpotent Lie groups endowed with a left-invariant metric. The Lie algebra $\mathfrak{n}$ is said to be two-step nilpotent, if it is nonabelian, and $\mathrm{ad}_x^2 = 0$ for all $x \in \mathfrak{n}$.

The center and the commutator of a Lie algebra $\mathfrak{n}$ are defined as

$$\mathfrak{z} = \{z \in \mathfrak{n} \mid [x, z] = 0, \text{ for all } x \in \mathfrak{n}\}, \qquad \mathfrak{n}' = \mathrm{span}\{[x, y] \mid x, y \in \mathfrak{n}\}.$$

In the particular case of two-step nilpotent Lie groups, $\mathfrak{n}' \subset \mathfrak{z}$, and, thus, (5) and (6) simplify to:

$$\Omega_{\xi_x}(w) = x - [w, x], \quad \Omega_{\xi_D}(w) = Dw - \frac{1}{2}[w, Dw] \qquad w \in \mathfrak{n}. \tag{7}$$

From now on, we assume that $\mathfrak{n}$ is two-step nilpotent and denote as before by N the simply connected group with Lie algebra $\mathfrak{n}$, endowed with the left-invariant metric g defined by the scalar product on $\mathfrak{n}$. We shall describe the main geometric properties of (N, g) through linear objects in the metric Lie algebra $(\mathfrak{n}, g)$, following the work of Eberlein [5].

Let $\mathfrak{v}$ be the orthogonal complement of $\mathfrak{z}$ in $\mathfrak{n}$, so that $\mathfrak{n} = \mathfrak{v} \oplus \mathfrak{z}$ as an orthogonal direct sum of vector spaces. Each central element $z \in \mathfrak{z}$ defines an endomorphism $j(z) : \mathfrak{v} \longrightarrow \mathfrak{v}$ by the equation

$$g(j(z)x, y) := g(z, [x, y]) \quad \text{for all } x, y \in \mathfrak{v}. \tag{8}$$

This endomorphism $j(z)$ belongs to $\mathfrak{so}(\mathfrak{v})$, the Lie algebra of skew-symmetric maps of $\mathfrak{v}$ with respect to g. The linear map $j : \mathfrak{z} \to \mathfrak{so}(\mathfrak{v})$ captures important geometric information of the Riemannian manifold (N, g). Using Koszul's formula (2), the Levi-Civita covariant derivative of g can be given in terms of the $j(z)$ maps by

$$\begin{cases} \nabla_x y = \frac{1}{2}\,[x, y] & \text{if } x, y \in \mathfrak{v}, \\ \nabla_x z = \nabla_z x = -\frac{1}{2} j(z)x & \text{if } x \in \mathfrak{v},\ z \in \mathfrak{z}, \\ \nabla_z z' = 0 & \text{if } z, z' \in \mathfrak{z}. \end{cases} \tag{9}$$

If $D : \mathfrak{n} \longrightarrow \mathfrak{n}$ is a derivation of $\mathfrak{n}$, then by definition $[Dz, x] = D[z, x] - [z, Dx]$, for all $z \in \mathfrak{z}$, $x \in \mathfrak{n}$, so D preserves the center $\mathfrak{z}$. Thus, a skew-symmetric derivation of $\mathfrak{n}$ preserves both $\mathfrak{z}$ and $\mathfrak{v} = \mathfrak{z}^{\perp}$ and for every $x, y \in \mathfrak{v}$ and $z \in \mathfrak{z}$, one has:

$$\begin{aligned} g(j(Dz)x, y) &= g([x, y], Dz) = -g(D[x, y], z) = -g([Dx, y], z) - g([x, Dy], z) \\ &= -g(j(z)Dx, y) - g(j(z)x, Dy) = -g([j(z), D], y), \end{aligned}$$

whence

$$j(Dz) = [D|_{\mathfrak{v}}, j(z)] \quad \text{for all } z \in \mathfrak{z}. \tag{10}$$

Conversely, it is straightforward to check that a skew-symmetric endomorphism on $\mathfrak{n}$ that preserves $\mathfrak{z}$ and $\mathfrak{v}$ and satisfies (10) is a derivation.

3. Symmetric Killing tensors

Let (V, g) be an n-dimensional real vector space. Denote by $\mathrm{Sym}^k V$ the set of symmetric tensor products in $V^{\otimes^k}$. Elements in $\mathrm{Sym}^k V$ are symmetrized tensor products

$$v_1 \cdot \ldots \cdot v_k = \sum_{\sigma \in \mathfrak{S}_k} v_1 \otimes \ldots \otimes v_k, \quad v_1, \ldots, v_k \in V,$$

where $\mathfrak{S}_k$ denotes the group of bijections of the set $\{1, \ldots, k\}$. Symmetric 1-tensors are simply vectors in V.

The inner product g is induced to $\mathrm{Sym}^k V$ by the formula

$$g(v_1 \cdot \ldots \cdot v_k, u_1 \cdot \ldots \cdot u_k) = \sum_{\sigma \in \mathfrak{S}_k} g(v_1, u_{\sigma(1)}) \cdot \ldots \cdot g(v_k, u_{\sigma(k)}), \quad u_i, v_i \in V.$$

The space of symmetric k-tensors on V is identified with the subspace of totally symmetric covariant tensors of degree k. In fact, we can identify a symmetric tensor $S \in \mathrm{Sym}^k V$ with the multilinear map $S : V \times \cdots \times V \longrightarrow \mathbb{R}$ satisfying

$$S(v_1, \ldots, v_k) = g(S, v_1 \cdot \ldots \cdot v_k), \quad v_1, \ldots, v_k \in V. \tag{11}$$

Under this identification, a vector $v \in V$ (symmetric 1-tensor) is identified with its metric dual $g(v, \cdot)$. The inner product g becomes a symmetric 2-tensor, and $g = \frac{1}{2} \sum_{i=1}^n e_i^2$, if $\{e_1, \ldots, e_n\}$ is an orthonormal basis of V. Here, we denote $e_i^2 = e_i \cdot e_i$. In general, symmetric k-tensors are homogeneous polynomials of degree k in the variables $e_1, \ldots, e_n$.

Symmetric 2-tensors $S \in \mathrm{Sym}^2 V$ can also be seen as symmetric endomorphisms on V. In fact, S is a symmetric bilinear form $S : V \times V \longrightarrow \mathbb{R}$ and is related to the inner product by the condition $S(u_1, u_2) = g(Su_1, u_2)$, $u_1, u_2 \in V$. Given an orthonormal basis $\{e_1, \ldots, e_n\}$, if the matrix of S in this basis, as an endomorphism, is $(s_{ij})_{ij}$, then S as a polynomial reads

$$S = \frac{1}{2} \sum_{1 \leq i,j \leq n} s_{ij}\ e_i \cdot e_j. \tag{12}$$

Let (M, g) be a Riemannian manifold. A symmetric k-tensor field on M is a section of the bundle $\mathrm{Sym}^k TM$, which is a subbundle of $TM^{\otimes^k}$. Symmetric 1-tensors are the vector fields on M. The symmetric product of vector fields on M defines symmetric 2-tensors by the formula $(X \cdot Y)_p := X_p \otimes Y_p + Y_p \otimes X_p$.

Under the identification in (11), symmetric tensors correspond to covariant tensor fields, for instance, a vector field X on M corresponds to the 1-form $g(X, \cdot)$. As symmetric bilinear form, $X \cdot Y$ satisfies $(X \cdot Y)(u, v) = g(X, u)g(Y, v) + g(X, v)g(Y, u)$. For every local orthonormal frame $\{E_1, \ldots, E_n\}$, the Riemannian metric g reads $g = \frac{1}{2} \sum_{i=1}^n E_i \cdot E_i$. Finally, note that symmetric 2-tensors on M correspond to sections of $\mathrm{End}(TM)$ that are symmetric with respect to the Riemannian metric.

Let ∇ denote the Levi-Civita connection defined by g on M.

DEFINITION 3.1. — A symmetric k-tensor S is a Killing tensor if

$$(\nabla_X S)(X,\dots,X) = 0, \quad \text{for any vector field } X.$$

Equivalently, a symmetric k-tensor is a Killing tensor if its symmetrized covariant derivative vanishes. This notion generalizes that of Killing vector field, as we shall see below.

A concept related to symmetric Killing tensors is that of Killing forms [16]. A 2-form ω is said to be a Killing form if $X \lrcorner \nabla_X \omega = 0$, for every vector field X in M. Given a Killing 2-form, the symmetric 2-tensor defined as $S^\omega(X,Y) = g((X \lrcorner \omega)^\#, (Y \lrcorner \omega)^\#)$ is a Killing 2-tensor (see Proposition 3.2), where $(X \lrcorner \omega)^\#$ denotes the metric dual of the 1-form $X \lrcorner \omega$. The section of $\mathrm{End}(TM)$ corresponding to the symmetric tensor S^ω is $-T^2$.

We next give a short account of basic results on Killing tensors [8].

PROPOSITION 3.2. —
1. *A vector field ξ is a symmetric Killing 1-tensor, if and only if ξ is a Killing vector field.*
2. *The symmetric product of two Killing vector fields is a symmetric Killing 2-tensor.*
3. *The Riemannian metric g is a symmetric Killing 2-tensor.*
4. *If ω is a Killing 2-form, then S^ω is a symmetric Killing 2-tensor.*

Proof. — The first and third statements are obvious. To check the second one, let ξ, η be two Killing vector fields of M, and let X be a vector field. Then, $\nabla_X(\xi\cdot\eta) = \nabla_X\xi\cdot\eta + \xi\cdot\nabla_X\eta$, which is zero. Finally, from the definition of S^ω we have $(\nabla_X S^\omega)(X,X) = 2g((X \lrcorner \nabla_X\omega)^\#, (X \lrcorner \omega)^\#)$, for any vector field X. □

Now let (N,g) be a simply connected two-step nilpotent Lie group endowed with a left-invariant metric.

Every symmetric k-tensor S on N defines a function Ω_S on $\mathfrak{n}$ as in (1). Then, $\Omega_S(w)$ is a symmetric tensor on $\mathfrak{n}$, for all $w \in \mathfrak{n}$, that is, $\Omega_S(w) \in \mathrm{Sym}^k\mathfrak{n} \subset \mathfrak{n}^{\otimes^k}$. In particular, the left-invariant metric g satisfies $\Omega_g(w) = \frac{1}{2}\sum_{i=1}^n e_i^2$, for all $w \in \mathfrak{n}$, if $\{e_1,\dots,e_n\}$ is an orthonormal basis of $\mathfrak{n}$.

From the definition of symmetric product of vector fields, we immediately have

$$\Omega_{X_1\cdot\ldots\cdot X_k}(w) = \Omega_{X_1}(w)\cdot\ldots\cdot\Omega_{X_k}(w), \quad \text{for all } w \in \mathfrak{n}, \tag{13}$$

for every vector fields $X_1,\dots,X_k$ on N. This allows us to compute the functions corresponding to the symmetric product the Killing vector fields given in (5)

and (6):

$$\Omega_{\xi_x\cdot\xi_y}(w) = x\cdot y - (x\cdot[w,y] + y\cdot[w,x]) + [w,x]\cdot[w,y] \tag{14}$$

$$\Omega_{\xi_x\cdot\xi_D}(w) = x\cdot Dw - ([w,x]\cdot Dw + \frac{1}{2}x\cdot[w,Dw]) + \frac{1}{2}[w,x]\cdot[w,Dw] \tag{15}$$

$$\Omega_{\xi_D\cdot\xi_{D'}}(w) = Dw\cdot D'w - \frac{1}{2}\left(Dw\cdot[w,D'w] + D'w\cdot[w,Dw]\right) + \frac{1}{4}[w,Dw]\cdot[w,D'w]$$

These functions are, in general, nonconstant, so they define symmetric Killing 2-tensors on N that are not always left-invariant. Recall that if S is a left-invariant k-tensor on N and $x\in\mathfrak{n}$, then $\nabla_x S$ is also left-invariant. Thus from Definition 3.1, we have that S is a symmetric Killing tensor if and only if

$$g((\nabla_x S)x, x) = 0, \quad \text{for all } x\in\mathfrak{n}. \tag{16}$$

4. Left-invariant symmetric Killing 2-tensors on two-step nilpotent Lie groups

In this section, we study which symmetric endomorphisms of $\mathfrak{n}$ define left-invariant symmetric Killing 2-tensors on the two-step nilpotent Lie group N endowed with a left-invariant metric g. We start by giving a characterization of such endomorphisms in terms of their behavior with respect to the orthogonal decomposition $\mathfrak{n}=\mathfrak{v}\oplus\mathfrak{z}$.

PROPOSITION 4.1. — *A left-invariant symmetric* 2*-tensor on* N*, identified with an element* $S\in \mathrm{Sym}^2\mathfrak{n}$ *as in Remark 2.2, is a Killing tensor, if and only if*

$$\begin{cases} [Sx,y] = [x,Sy], \ \textit{for all } x,y\in\mathfrak{v}, \\ \mathrm{ad}_x\circ S|_{\mathfrak{z}} \ \textit{is skew-symmetric on } \mathfrak{z} \ \textit{for all } x\in\mathfrak{v}. \end{cases} \tag{17}$$

Proof. — Let $S:\mathfrak{n}\longrightarrow\mathfrak{n}$ be a symmetric endomorphism. From (16), S is a Killing tensor, if and only if $g((\nabla_y S)y,y)=0$ for all $y\in\mathfrak{n}$. By Koszul's formula, we have

$$g((\nabla_y S)y,y) = 2g([y,Sy],y), \tag{18}$$

and, therefore, S is Killing, if and only if

$$g([y,Sy],y)=0 \quad \text{for all } y\in\mathfrak{n}$$

(cf. [10, Proposition 2.4.]). Taking $y=x+z$ with $x\in\mathfrak{v}$ and $z\in\mathfrak{z}$, the last equality reads

$$g(z,[Sz,x]) + g(z,[Sx,x]) = 0 \quad \text{for all } x\in\mathfrak{v}, z\in\mathfrak{z}. \tag{19}$$

The first term of this sum is quadratic in z, whilst the second one is linear. This implies that (19) is equivalent to

$$g(z,[Sx,x])=0 \quad \text{and} \quad g(z,[Sz,x])=0 \quad \text{for all } x\in\mathfrak{v}, z\in\mathfrak{z}.$$

By polarization, the first equation is equivalent to $[Sx, y] = [x, Sy]$ for all $x, y \in \mathfrak{v}$, and the second equation simply says that $\mathrm{ad}_x \circ S|_{\mathfrak{z}}$ is a skew-symmetric endomorphism of $\mathfrak{z}$ for every $x \in \mathfrak{v}$. □

EXAMPLE 4.2. — Let $S \in \mathrm{Sym}^2\mathfrak{n}$ be a symmetric tensor such that $Sz = 0$, for all $z \in \mathfrak{z}$, and $S|_{\mathfrak{v}} = \lambda \mathrm{Id}_{\mathfrak{v}}$, for some $\lambda \in \mathbb{R}$. It is clear that S satisfies the system (17), so S determines a left-invariant Killing tensor on N.

REMARK 4.3. — Killing 2-forms define symmetric Killing 2-tensors as showed in Proposition 3.2. On the other hand, Barberis et al. [2, Theorem 3.1.], proved that a skew-symmetric map $T : \mathfrak{n} \longrightarrow \mathfrak{n}$ defines a Killing 2-form, if and only if T preserves $\mathfrak{z}$ and $\mathfrak{v}$, and verifies $[Tx, y] = [x, Ty]$ and $T[x, y] = 3[Tx, y]$ for every $x, y \in \mathfrak{v}$ (see also [1]). If T is such an endomorphism, then $S := -T^2$ verifies the conditions (17), so it, indeed, defines a symmetric Killing 2-tensor on N (cf. Proposition 3.2 (4) above).

The decomposition $\mathfrak{n} = \mathfrak{v} \oplus \mathfrak{z}$ induces a splitting of the space of symmetric 2-tensors on $\mathfrak{n}$

$$\mathrm{Sym}^2\mathfrak{n} = \mathrm{Sym}^2\mathfrak{v} \oplus (\mathfrak{z} \cdot \mathfrak{v}) \oplus \mathrm{Sym}^2\mathfrak{z}. \tag{20}$$

The elements of $\mathrm{Sym}^2\mathfrak{v}$, $\mathfrak{z} \cdot \mathfrak{v}$ and $\mathrm{Sym}^2\mathfrak{z}$ will be viewed as symmetric endomorphisms of $\mathfrak{n}$ by means of the standard inclusions.

DEFINITION 4.4. — Given $S \in \mathrm{Sym}^2\mathfrak{n}$, denote by $S^{\mathfrak{v}}$, S^{m} and $S^{\mathfrak{z}}$ its components with respect to the above decomposition; we call S^{m} the mixed part of S.

PROPOSITION 4.5. — *For every $S \in \mathrm{Sym}^2\mathfrak{n}$, we have*

1. *The left-invariant symmetric tensor defined by $S^{\mathfrak{z}}$ is always Killing.*
2. *The left-invariant symmetric tensor defined S is a symmetric Killing tensor, if and only if the left-invariant symmetric tensors defined by $S^{\mathfrak{v}}$ and by S^{m} are Killing.*

Proof. — (1) Any element of $\mathrm{Sym}^2\mathfrak{z}$ defines a left-invariant symmetric Killing tensor because it trivially verifies the system (17).

(2) Note that $[Sx, y] = [S^{\mathfrak{v}}x, y]$ and $\mathrm{ad}_x Sz = \mathrm{ad}_x S^{\mathrm{m}}z$ for all $x, y \in \mathfrak{v}$, $z \in \mathfrak{z}$. Moreover, $[S^{\mathrm{m}}x, y] = 0$ and $S^{\mathfrak{v}}z = 0$ for every $x, y \in \mathfrak{v}$, $z \in \mathfrak{z}$. Therefore, S verifies the system (17), if and only if both S^{m} and $S^{\mathfrak{v}}$ verify it. □

DEFINITION 4.6. — A two-step nilpotent Lie algebra $\mathfrak{n}$ is called nonsingular if $\mathrm{ad}_x : \mathfrak{v} \longrightarrow \mathfrak{z}$ is surjective for all $x \in \mathfrak{v} \setminus \{0\}$.

PROPOSITION 4.7. — *Let $\mathfrak{n}$ be a nonsingular two-step nilpotent Lie algebra and let $S \in \mathrm{Sym}^2\mathfrak{n}$. If S defines a Killing tensor on N, then $S^{\mathrm{m}} = 0$.*

Proof. — Since $\mathfrak{n}$ is nonsingular, we have $\mathrm{Im}(\mathrm{ad}_y) = \mathfrak{z}$ for all $y \in \mathfrak{v} \setminus \{0\}$. Let z be any element of $\mathfrak{z}$. Then, $g([x, Sz], z) = 0$, for all $x \in \mathfrak{v}$, because S is Killing, and thus satisfies (17). This implies $z \perp \mathrm{Im}\,\mathrm{ad}_y$, for $y := \mathrm{pr}_{\mathfrak{v}} Sz \in \mathfrak{v}$, which, as $\mathfrak{n}$ is nonsingular, implies that either $z = 0$ or $y = 0$. Therefore, in both cases $\mathrm{pr}_{\mathfrak{v}} Sz = 0$, meaning that $Sz \in \mathfrak{z}$ for every $z \in \mathfrak{z}$. □

EXAMPLE 4.8. — Let $\mathfrak{h}_{2n+1}$ be the Heisenberg Lie algebra of dimension $2n + 1$. The Lie algebra $\mathfrak{h}_{2n+1}$ has a basis $\{x_1, \ldots, x_n, y_1, \ldots, y_n, z\}$, where the nontrivial Lie brackets are $[x_i, y_i] = z$, and $\mathfrak{z} = \mathbb{R}z$ is the center. This is a nonsingular Lie algebra, and $j(z) =: J$ is the canonical complex structure in $\mathbb{R}^{2n}$. Consider the inner product making this basis an orthonormal basis. By Proposition 4.7, the mixed part S^{m} of any symmetric Killing tensor S vanishes. Moreover, the system (17) is equivalent to $[S^{\mathfrak{v}}, J] = 0$. We conclude that S is a symmetric Killing tensor on $\mathfrak{h}_{2n+1}$, if and only if it preserves the decomposition $\mathfrak{h}_{2n+1} = \mathfrak{v} \oplus \mathfrak{z}$ and its restriction to $\mathfrak{v}$ commutes with J (cf. [10, Theorem 3.2]).

The following example shows that there exist two-step nilpotent metric Lie algebras carrying left-invariant symmetric Killing 2-tensors S with $S^{\mathrm{m}} \neq 0$, that is, not preserving the decomposition $\mathfrak{v} \oplus \mathfrak{z}$.

EXAMPLE 4.9. — Let $\mathfrak{n}$ be the Lie algebra of dimension 6 having an orthonormal basis $\{e_1, \ldots, e_6\}$ satisfying the nonzero bracket relations

$$[e_1, e_2] = e_4, \quad [e_1, e_3] = e_5, \quad [e_2, e_3] = e_6.$$

Then, $\mathfrak{z} = \mathrm{span}\{e_4, e_5, e_6\} = \mathfrak{n}'$ and $\mathfrak{v} = \mathrm{span}\{e_1, e_2, e_3\}$.

An element $S \in \mathfrak{z} \cdot \mathfrak{v}$ defines a symmetric Killing tensor on the simply connected Lie group with Lie algebra $\mathfrak{n}$, if and only if $g(\mathrm{ad}_x Sz, z) = 0$, for all $x \in \mathfrak{v}$, $z \in \mathfrak{z}$. Let $Se_4 = ae_1 + be_2 + ce_3$, then $b = g([e_1, Se_4], e_4)$ and $a = g([e_2, Se_4], e_4)$ are zero; thus, $Se_4 = ce_3$. Analogously, one obtains that Se_5 and Se_6 are multiples of e_2 and e_1, respectively. Moreover, $g([e_2, Se_6], e_4) + g([e_2, Se_4], e_6) = 0$ implies that $S(e_6) = -ce_1$, and $g([e_1, Se_5], e_4) + g([e_1, Se_4], e_5) = 0$ implies that $S(e_5) = ce_2$, so, finally, $S = c(e_1 \cdot e_6 - e_2 \cdot e_5 + e_3 \cdot e_4)$.

Proposition 4.5 (1) and Example 4.2 show that every symmetric 2-tensor in $\mathrm{Sym}^2\mathfrak{z}$ and the symmetric tensor $\sum_{i=1}^{3} e_i \cdot e_i \in \mathrm{Sym}^2\mathfrak{v}$ define left-invariant Killing tensors on N. Therefore, the same holds for

$$a_1 \sum_{i=1}^{3} e_i \cdot e_i + a_2(e_1 \cdot e_6 - e_2 \cdot e_5 + e_3 \cdot e_4) + \sum_{4 \leq i \leq j \leq 6} a_{ij} e_i \cdot e_j, \qquad a_i, a_{ij} \in \mathbb{R}.$$

It will follow from the results in the next section that any left-invariant symmetric Killing 2-tensor on N is induced by an element of this form.

To continue, we study left-invariant symmetric Killing 2-tensors on Riemannian products of two-step nilpotent Lie groups. A nilpotent Lie algebra endowed with an inner product $(\mathfrak{n}, g)$ is called *reducible*, if it can be written

as an orthogonal direct sum of ideals $\mathfrak{n} = \mathfrak{n}_1 \oplus \mathfrak{n}_2$. In this case, we endow $\mathfrak{n}_i$ with the inner product g_i, which is the restriction of g to $\mathfrak{n}_i$, for each $i = 1, 2$. Otherwise, $(\mathfrak{n}, g)$ is called *irreducible*.

REMARK 4.10. —
1. If $\mathfrak{n}$ is a reducible two-step nilpotent Lie algebra, then $\dim \mathfrak{z} \geq 2$. Indeed, if $\mathfrak{n}$ decomposes as a direct sum of orthogonal ideals $\mathfrak{n} = \mathfrak{n}_1 \oplus \mathfrak{n}_2$, then the center of $\mathfrak{n}$ is $\mathfrak{z} = \mathfrak{z}_1 \oplus \mathfrak{z}_2$, where $\mathfrak{z}_i$ is the center of $\mathfrak{n}_i$, and both $\mathfrak{z}_i$ are nonzero.
2. If $\mathfrak{n}$ is an irreducible two-step nilpotent Lie algebra, then $j : \mathfrak{z} \longrightarrow \mathfrak{so}(\mathfrak{v})$ is injective. Indeed, it is easy to check that the kernel $\mathfrak{a}$ of $j : \mathfrak{z} \longrightarrow \mathfrak{so}(\mathfrak{v})$ (which is equal to $\mathfrak{z} \cap \mathfrak{n}'^{\perp}$) and its orthogonal $\mathfrak{a}^{\perp}$ in $\mathfrak{n}$ are both ideals of $\mathfrak{n}$. Therefore, if $\mathfrak{n}$ is irreducible, then $\mathfrak{a} = 0$, and, thus, j is injective.

The next results aim to show that left-invariant symmetric Killing 2-tensors on direct products of two-step nilpotent Lie groups are determined by left-invariant symmetric Killing 2-tensors on their factors.

Let $\mathfrak{n}$ be a two-step nilpotent Lie algebra that is decomposable and let $\mathfrak{n}_1$, $\mathfrak{n}_2$ be orthogonal ideals, such that $\mathfrak{n} = \mathfrak{n}_1 \oplus \mathfrak{n}_2$. Then,

$$\mathrm{Sym}^2\mathfrak{n} = \mathrm{Sym}^2\mathfrak{n}_1 \oplus (\mathfrak{n}_1 \cdot \mathfrak{n}_2) \oplus \mathrm{Sym}^2\mathfrak{n}_2. \tag{21}$$

Given $S \in \mathrm{Sym}^2\mathfrak{n}$ we denote by $S_i \in \mathrm{Sym}^2\mathfrak{n}_i$ and $S_{\mathrm{nd}} \in \mathfrak{n}_1 \cdot \mathfrak{n}_2$ the symmetric tensors in $\mathfrak{n}$, such that $S = S_1 + S_{\mathrm{nd}} + S_2$ (S_{nd} is the nondiagonal part of S).

PROPOSITION 4.11. — *Let $S \in \mathrm{Sym}^2\mathfrak{n}$.*
1. *The left-invariant tensor defined by S is a Killing tensor, if and only if $S_1, S_2, S_{\mathrm{nd}}$ are Killing tensors on $\mathfrak{n}$.*
2. *If S defines a left-invariant Killing tensor, then its nondiagonal part S_{nd} satisfies $S_{\mathrm{nd}} \in \mathfrak{z}_1 \cdot \mathfrak{z}_2$.*

Proof. — (1) If S is Killing, for every $x = x_1 + x_2$ and $y = y_1 + y_2$ in $\mathfrak{v} = \mathfrak{v}_1 \oplus \mathfrak{v}_2$ and for every $z = z_1 + z_2 \in \mathfrak{z} = \mathfrak{z}_1 \oplus \mathfrak{z}_2$, we have by (17):

$$[S_1 x, y] - [x, S_1 y] = [S_1 x_1, y_1] - [x_1, S_1 y_1] = [S x_1, y_1] - [x_1, S y_1] = 0$$

and

$$g(z, [S_1 z, x]) = g(z_1, [S_1 z_1, x_1]) = g(z_1, [S z_1, x_1]) = 0,$$

thus showing that S_1 is Killing, and similarly S_2 is Killing too. By linearity, S_{nd} is also Killing. The converse is clear.

(2) If S is Killing, then S_{nd} is Killing, so for all $z = z_1 + z_2 \in \mathfrak{z} = \mathfrak{z}_1 \oplus \mathfrak{z}_2$ and $x_1 \in \mathfrak{v}_1$, we have

$$0 = g(z, [S_{\mathrm{nd}} z, x_1]) = g(z_1, [S_{\mathrm{nd}} z_2, x_1]),$$

thus showing that the subspace $S_{\mathrm{nd}}(\mathfrak{z}_2)$ of $\mathfrak{n}_1$ is actually contained in $\mathfrak{z}_1$. □

It will be useful later to compare the above decomposition of S on a direct sum $\mathfrak{n}_1 \oplus \mathfrak{n}_2$ with the one introduced in Definition 4.4. Consider the decomposition $\mathfrak{n} = \mathfrak{v} \oplus \mathfrak{z}$ and $\mathfrak{n}_i = \mathfrak{v}_i \oplus \mathfrak{z}_i$ for $i = 1, 2$ (one of the $\mathfrak{v}_i$ might also vanish), then $\mathfrak{z} = \mathfrak{z}_1 \oplus \mathfrak{z}_2$ and $\mathfrak{v} = \mathfrak{v}_1 \oplus \mathfrak{v}_2$.

PROPOSITION 4.12. — *If $S \in \mathrm{Sym}^2(\mathfrak{n}_1 \oplus \mathfrak{n}_2)$ defines a left-invariant Killing tensor on N, then $S^{\mathfrak{v}} = S_1^{\mathfrak{v}_1} + S_2^{\mathfrak{v}_2}$, $S^{\mathfrak{z}} = S_1^{\mathfrak{z}_1} + S_2^{\mathfrak{z}_2} + S_{\mathrm{nd}}$, and its mixed part is $S^{\mathrm{m}} = S_1^{\mathrm{m}} + S_2^{\mathrm{m}}$, where S_i^{m} denotes the mixed part of S_i as a tensor on $\mathfrak{n}_i$.*

Proof. — Consider the decompositions $S_i = S_i^{\mathfrak{v}_i} + S_i^{\mathfrak{z}_i} + S_i^{\mathrm{m}}$ of S_i from Definition 4.4. In the expression

$$S = (S_1^{\mathfrak{v}_1} + S_2^{\mathfrak{v}_2}) + (S_1^{\mathrm{m}} + S_2^{\mathrm{m}}) + (S_1^{\mathfrak{z}_1} + S_2^{\mathfrak{z}_2} + S_{\mathrm{nd}})$$

we clearly have $S_1^{\mathfrak{v}_1} + S_2^{\mathfrak{v}_2} \in \mathrm{Sym}^2\mathfrak{v}$, $S_1^{\mathrm{m}} + S_2^{\mathrm{m}} \in \mathfrak{v} \cdot \mathfrak{z}$, and according to Proposition 4.11, $S_1^{\mathfrak{z}_1} + S_2^{\mathfrak{z}_2} + S_{\mathrm{nd}} \in \mathrm{Sym}^2\mathfrak{z}$. □

5. (In)decomposable symmetric Killing tensors

Let N be a two-step nilpotent Lie group endowed with a left-invariant metric g and let $\mathfrak{n}$ be its Lie algebra. By Proposition 3.2, every linear combination of symmetric products of Killing vector fields is a symmetric Killing 2-tensor on N. The metric and, more generally, any parallel symmetric Killing tensors are trivially Killing tensors. We are interested in Killing tensors that are not of these two types, so we introduce the following terminology.

DEFINITION 5.1. — A left-invariant symmetric Killing 2-tensor S is called *decomposable* if it is the sum of a parallel tensor and a linear combination of symmetric products of Killing vector fields. If this is not the case, we say that S is *indecomposable*.

Note that from Theorem A.1 in the Appendix, every parallel symmetric tensor on a two-step nilpotent Lie group is left-invariant.

REMARK 5.2. — Proposition A.3 in the Appendix shows that the eigenspaces of any parallel symmetric tensor induce a decomposition of $\mathfrak{n}$ in an orthogonal direct sum of ideals. Thus, if $\mathfrak{n}$ is irreducible, the only parallel symmetric 2-tensors are the multiples of the metric.

Our first goal is to show that the decomposability of a left-invariant symmetric Killing tensor S only depends on the decomposability of its component $S^{\mathfrak{v}}$ (which by Proposition 4.5 is also a Killing tensor).

LEMMA 5.3. — *Every left-invariant symmetric tensor on N defined by an element $S \in \mathrm{Sym}^2\mathfrak{z}$ is a decomposable Killing 2-tensor.*

Proof. — For $z, z' \in \mathfrak{z}$, the symmetric product of the Killing vectors they define is $\Omega_{\xi_z \cdot \xi_{z'}} = z \cdot z'$, by (7). According to (12), if $\{z_1, \dots, z_n\}$ is an orthonormal basis of $\mathfrak{z}$, then $S = \frac{1}{2} \sum_{1 \leq i,j \leq n} g(Sz_i, z_j) \Omega_{\xi_{z_i} \cdot \xi_{z_j}}$. □

LEMMA 5.4. — *Every left-invariant symmetric Killing 2-tensor defined by an element $S \in \mathfrak{z} \cdot \mathfrak{v}$ is decomposable.*

Proof. — Let $\{z_1, \dots, z_n\}$ be an orthonormal basis of $\mathfrak{z}$. We claim that $S = \sum_{s=1}^{n} \Omega_{\xi_{z_s} \cdot \xi_{Sz_s}}$. By (14), $\Omega_{\xi_{z_s} \cdot \xi_{Sz_s}}(w) = z_s \cdot Sz_s - z_s \cdot [w, Sz_s]$, and thus $\sum_{s=1}^{n} \Omega_{\xi_{z_s} \cdot \xi_{Sz_s}}$ has no component in $\mathrm{Sym}^2 \mathfrak{v}$. Moreover, for $z, z' \in \mathfrak{z}$, one has

$$\begin{aligned} \sum_{s=1}^{n} \Omega_{\xi_{z_s} \cdot \xi_{Sz_s}}(w)(z, z') &= -\sum_{s=1}^{n} g(z_s, z) g([w, Sz_s], z') + g(z_s, z') g([w, Sz_s], z) \\ &= -g([w, Sz], z') - g([w, Sz'], z) = 0, \end{aligned}$$

where the last equality holds because S is Killing and, thus, satisfies (17). Finally, consider $x \in \mathfrak{v}$ and $z \in \mathfrak{z}$; then

$$\sum_{s=1}^{n} \Omega_{\xi_{z_s} \cdot \xi_{Sz_s}}(w)(x, z) = \sum_{s=1}^{m} g(z_s, z) g(Sz_s, x) = g(Sx, z),$$

since S is symmetric. Therefore, $S = \sum_{s=1}^{m} \Omega_{\xi_{z_s} \cdot \xi_{Sz_s}}$, as claimed. □

By Lemma 5.3 and Lemma 5.4 we obtain the following directly:

PROPOSITION 5.5. — *Let $S \in \mathrm{Sym}^2 \mathfrak{n}$ define a left-invariant symmetric Killing tensor, with components denoted by $S^{\mathfrak{v}}$, S^{m}, and $S^{\mathfrak{z}}$, as in Definition 4.4. Then, S is decomposable if and only if $S^{\mathfrak{v}}$ is decomposable.*

Our next aim is to show that if $\mathfrak{n}$ is a reducible two-step nilpotent Lie algebra, then left-invariant symmetric Killing tensors on N are determined by the ones on the factors.

Suppose $\mathfrak{n} = \mathfrak{n}_1 \oplus \mathfrak{n}_2$ as an orthogonal direct sum of ideals. Denote by N, N_1, N_2 the simply connected nilpotent Lie groups with Lie algebras $\mathfrak{n}, \mathfrak{n}_1, \mathfrak{n}_2$, respectively, and consider the left-invariant metrics g_i that g induces on N_i for $i = 1, 2$ (also identified with the corresponding scalar products in $\mathfrak{n}_i$). The fact that $(\mathfrak{n}, g) = (\mathfrak{n}_1, g_1) \oplus (\mathfrak{n}_2, g_2)$ implies that $(N, g) = (N_1, g_1) \times (N_2, g_2)$ as Riemannian manifolds.

PROPOSITION 5.6. — *Let $S \in \mathrm{Sym}^2 \mathfrak{n}$ define a left-invariant symmetric Killing tensor on N. Let $S = S_1 + S_{\mathrm{nd}} + S_2$ be its decomposition described in (21). Then, S is decomposable if and only if the left-invariant tensors defined by S_i are decomposable symmetric Killing tensors on N_i for $i = 1, 2$.*

Proof. — Let $S \in \mathrm{Sym}^2\mathfrak{n}$ and write $S = S_1 + S_{\mathrm{nd}} + S_2$ as in the hypothesis. Suppose that S is a decomposable Killing tensor. By Proposition 4.11, $S_1, S_2, S_{\mathrm{nd}}$ are Killing tensors, and $S_{\mathrm{nd}} \in \mathrm{Sym}^2\mathfrak{z}$; in particular, S_{nd} is decomposable by Lemma 5.3. The fact that S is decomposable in N implies

$$S = \sum_{l=1}^{t} T_l + \sum_{1\leq j,k\leq m} a_{j,k}\Omega_{\xi_j\cdot\xi_k}, \tag{22}$$

where $\{\xi_j\}_{j=1}^m$ is a basis of Killing vector fields of N, $a_{j,k} \in \mathbb{R}$ for $1 \leq j, k \leq m$, and T_l are parallel symmetric tensors on N for $l = 1, \ldots, t$.

For each $j = 1, \ldots, m$ and $i = 1, 2$, the Killing vector field ξ_j defines a Killing vector field ξ_j^i on (N_i, g_i), by restricting ξ_j to $N_i \times \{e\}$ and projecting it to TN_i. In addition, since TN_i is a left-invariant distribution in N, we have that $\Omega_{\xi_j^i} : \mathfrak{n}_i \longrightarrow \mathfrak{n}_i$ is given by $\Omega_{\xi_j^i} = \mathrm{pr}_{\mathfrak{n}_i}(\Omega_{\xi_j}|_{\mathfrak{n}_i})$. Moreover, $\mathrm{pr}_{\mathfrak{n}_i}(\Omega_{\xi_j}|_{\mathfrak{n}_i})\cdot\mathrm{pr}_{\mathfrak{n}_i}(\Omega_{\xi_k}|_{\mathfrak{n}_i}) = \mathrm{pr}_{\mathrm{Sym}^2\mathfrak{n}_i}(\Omega_{\xi_j\cdot\xi_k}|_{\mathfrak{n}_i})$, for all $1 \leq j, k \leq m$, where the last projection is with respect to the decomposition (21). Therefore, $\Omega_{\xi_j^i\cdot\xi_k^i} = \mathrm{pr}_{\mathrm{Sym}^2\mathfrak{n}_i}(\Omega_{\xi_j\cdot\xi_l}|_{\mathfrak{n}_i})$. Similarly, T_l defines parallel symmetric tensors T_l^i on N_i, for $l = 1, \ldots, t$ and $i = 1, 2$. Therefore, restricting and projecting over N_i, for $i = 1, 2$, in (22), we have

$$S_i = \mathrm{pr}_{\mathrm{Sym}^2\mathfrak{n}_i}(S|_{\mathfrak{n}_i}) = \sum_l T_l^i + \sum_{j,k} a_{j,k}\Omega_{\xi_j^i\cdot\xi_k^i},$$

and, thus, S_i is decomposable in $\mathfrak{n}_i$, for $i = 1, 2$.

Conversely, fix $i \in \{1, 2\}$ and suppose S_i is a decomposable left-invariant symmetric Killing tensor on N_i. Then, $S_i = \sum_{l=1}^{t_i} T_l + \sum_{1\leq j,k\leq m_i} a_{j,k}\Omega_{\zeta_j\cdot\zeta_k}$, where T_l are parallel symmetric tensors on N_i for $l = 1, \ldots, t_i$, $a_{j,k} \in \mathbb{R}$ for $1 \leq j, k \leq m_i$, and $\{\zeta_j\}_{j=1}^{t_i}$ is a basis of Killing vector fields of N_i. It is easy to check that both T_l and ζ_j extend to parallel tensors and Killing vector fields of N, respectively, so that S_i is decomposable as a symmetric tensor in N. Hence, $S = S_1 + S_{\mathrm{nd}} + S_2$ is decomposable in N by Lemma 5.3. □

Any two-step nilpotent metric Lie algebra can be written as an orthogonal direct sum of ideals $\mathfrak{n} = \mathfrak{a} \oplus \mathfrak{n}_1 \oplus \cdots \oplus \mathfrak{n}_s$, where $\mathfrak{a}$ is the abelian ideal in Remark 4.10 (2), and each $\mathfrak{n}_i$ is an irreducible two-step nilpotent metric Lie algebra. The proposition above shows that the study of (in)decomposable left-invariant symmetric Killing tensors defined by elements in $\mathrm{Sym}^2\mathfrak{n}$ can be reduced to the study of these objects defined by elements in $\mathrm{Sym}^2\mathfrak{a}$ and in each $\mathrm{Sym}^2\mathfrak{n}_i$. Note that any left-invariant symmetric tensor defined by an element in $\mathrm{Sym}^2\mathfrak{a}$ is parallel, thus Killing and decomposable. Therefore, it is sufficient to study (in)decomposable left-invariant symmetric Killing tensors on de Rham irreducible nilpotent Lie groups. Moreover, by Proposition 5.5, we might reduce our study to the decomposability of left-invariant symmetric Killing tensors defined by elements in $\mathrm{Sym}^2\mathfrak{v}$.

In the rest of this section, we assume that $(\mathfrak{n}, g)$ is an irreducible two-step nilpotent metric Lie algebra. In particular, by Remark 4.10 (2), the map $j : \mathfrak{z} \longrightarrow \mathfrak{so}(\mathfrak{v})$ is injective.

LEMMA 5.7. — *Let $T : \mathfrak{v} \longrightarrow \mathfrak{v}$ be a skew-symmetric endomorphism. Then, T admits at most one extension to a skew-symmetric derivation of $\mathfrak{n}$.*

Proof. — If $D \in \mathrm{Dera}(\mathfrak{n})$ extends T, then for each $z \in \mathfrak{z}$, Dz is uniquely determined by the condition $j(Dz) = [T, j(z)]$ (see (10)), as j is injective. □

PROPOSITION 5.8. — *Let $S \in \mathrm{Sym}^2\mathfrak{v}$ define a left-invariant symmetric Killing tensor. Denote by $\lambda_i \in \mathbb{R}$ $(i = 1, \dots, k)$ the eigenvalues of S in $\mathfrak{v}$ and by $\mathfrak{v}_i$ the corresponding eigenspaces, so that $\mathfrak{v}$ decomposes as an orthogonal direct sum of $\mathfrak{v} = \bigoplus_{i=1}^{k} \mathfrak{v}_i$. Then $[\mathfrak{v}_i, \mathfrak{v}_j] = 0$, for all $i \neq j$, and $j(z)$ preserves $\mathfrak{v}_i$, for all $z \in \mathfrak{z}$, $i = 1, \dots, k$.*

Proof. — Let $x \in \mathfrak{v}_i$, $y \in \mathfrak{v}_j$ be eigenvectors of S associated to the eigenvalues $\lambda_i \neq \lambda_j$. Then, by (17), $[Sx, y] = [x, Sy]$, which leads to $\lambda_i[x, y] = \lambda_j[x, y]$. Therefore, $[\mathfrak{v}_i, \mathfrak{v}_j] = 0$. This implies, by (8), that $j(z)$ preserves each $\mathfrak{v}_i$ for every $z \in \mathfrak{z}$. □

Before studying the general case, let us note that the case where $S \in \mathrm{Sym}^2\mathfrak{v}$ has a unique eigenvalue is trivial:

PROPOSITION 5.9. — *The restriction $g|_{\mathfrak{v}}$ of the metric g to $\mathfrak{v}$ defines left-invariant decomposable symmetric Killing tensor on N.*

Proof. — Let $\{e_1, \dots, e_m\}$ and $\{z_1, \dots, z_n\}$ be orthonormal basis of $\mathfrak{v}$ and $\mathfrak{z}$, respectively. Then,

$$g|_{\mathfrak{v}} = \frac{1}{2}\sum_{i=1}^{m} e_i \cdot e_i = g - \frac{1}{2}\sum_{s=1}^{n} z_s \cdot z_s = g - \frac{1}{2}\sum_{s=1}^{n} \xi_{z_s} \cdot \xi_{z_s},$$

where ξ_{z_s} denotes the Killing vector field defined by z_s on N (which is both left- and right-invariant). Therefore, $g|_{\mathfrak{v}}$ defines a decomposable Killing tensor. □

NOTATION. — Let $S \in \mathrm{Sym}^2\mathfrak{v}$ define a left-invariant symmetric Killing tensor on N and let $\mathfrak{v} = \mathfrak{v}_1 \oplus \cdots \oplus \mathfrak{v}_k$ be the decomposition of $\mathfrak{v}$ as in Proposition 5.8. Denote by $\mathrm{pr}_{\mathfrak{v}_i} : \mathfrak{v} \longrightarrow \mathfrak{v}$ the orthogonal projection onto $\mathfrak{v}_i$.

For $\lambda_1, \cdots, \lambda_k \in \mathbb{R}$, denote $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_k)$. Given $a \in \mathbb{R}$, we define

$$\boldsymbol{\lambda} - a := (\lambda_1 - a, \dots, \lambda_k - a).$$

Let $\Pi^{\boldsymbol{\lambda}}$ be the endomorphism of $\mathfrak{v}$ defined as $\Pi^{\boldsymbol{\lambda}} = \sum_{i=1}^{k} \lambda_i \,\mathrm{pr}_{\mathfrak{v}_i}$. For each $z \in \mathfrak{z}$, we denote by $T_z^{\boldsymbol{\lambda}}$ the skew-symmetric endomorphism of $\mathfrak{v}$ given by

$$T_z^{\boldsymbol{\lambda}} = j(z) \circ \Pi^{\boldsymbol{\lambda}}.$$

We are now ready for the main result of this section:

THEOREM 5.10. — *Let $\mathfrak{n} = \mathfrak{v} \oplus \mathfrak{z}$ be an irreducible two-step nilpotent Lie algebra. Let $S \in Sym^2\mathfrak{v}$ define a left-invariant symmetric Killing tensor. Denote the eigenvalues of S (viewed as endomorphism of $\mathfrak{v}$) by $\lambda_1, \dots, \lambda_k$. Then, S is decomposable if and only if there exists $a \in \mathbb{R}$ such that, for every $z \in \mathfrak{z}$, $T_z^{\boldsymbol{\lambda}-a}$ extends to a skew-symmetric derivation of $\mathfrak{n}$.*

Proof. — Let $\{D_1, \dots, D_d\}$ be a basis of $\mathrm{Dera}(\mathfrak{n})$ and let $\{z_1, \dots, z_n\}$ be an orthonormal basis of $\mathfrak{z}$. Let $\{e_1, \dots, e_m\}$ be an orthonormal basis of $\mathfrak{v}$ adapted to the decomposition $\mathfrak{v} = \mathfrak{v}_1 \oplus \cdots \oplus \mathfrak{v}_k$ of eigenspaces of S, in the sense that there exist $m_0, m_1, \dots, m_k \in \mathbb{N}$, such that $e_{m_{i-1}+1}, \dots, e_{m_i}$ spans $\mathfrak{v}_i$ for every $i = 1, \dots, k$; in particular, $m_0 = 0$ and $m_k = m$. By (12), we then have $S = \frac{1}{2}\sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} \lambda_i \; e_l \cdot e_l$.

By Remark 5.2, if S is decomposable, then there exist constants $a, a_{i,l}, b_{i,t}, c_{s,t}, d_{q,r} \in \mathbb{R}$ and $D'_s, D''_i \in \mathrm{Dera}(\mathfrak{n})$ for $i, l \in \{1, \dots, m\}$, $s, t \in \{1, \dots, n\}$, and $q, r \in \{1, \dots, d\}$ with $a_{i,l} = a_{l,i}$, $c_{s,t} = c_{t,s}$ and $d_{q,r} = d_{r,q}$, such that

$$
\begin{aligned}
(23) \qquad S = ag &+ \sum_{1\le i,l\le m} a_{i,l}\Omega_{\xi_{e_i}\cdot\xi_{e_l}} + \sum_{\substack{1\le i\le m\\ 1\le t\le n}} b_{i,t}\Omega_{\xi_{e_i}\cdot\xi_{z_t}} + \sum_{1\le s,t\le n} c_{s,t}\Omega_{\xi_{z_s}\cdot\xi_{z_t}} \\
&+ \sum_{s=1}^{n}\Omega_{\xi_{D'_s}\cdot\xi_{z_s}} + \sum_{i=1}^{m}\Omega_{\xi_{D''_i}\cdot\xi_{e_i}} + \sum_{1\le q,r\le d} d_{q,r}\Omega_{\xi_{D_q}\cdot\xi_{D_r}}.
\end{aligned}
$$

Evaluating this equation at $w = 0$ and using (7) we obtain $b_{i,t} = 0$, for all i, t, $c_{s,t} = 0$, for $s \neq t$, $a_{i,l} = 0$, for $i \neq l$, $c_{s,s} = -\frac{a}{2}$, and $a_{l,l} = \frac{1}{2}\lambda_i - \frac{a}{2}$, for each $i \in \{1, \dots, k\}$ and $m_{i-1} + 1 \le l \le m_i$. Consequently, (23) becomes

$$
\begin{aligned}
S = ag &+ \sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} \frac{1}{2}(\lambda_i - a)\Omega_{\xi_{e_l}\cdot\xi_{e_l}} - \frac{a}{2}\sum_{s=1}^{n}\Omega_{\xi_{z_s}\cdot\xi_{z_s}} + \sum_{s=1}^{n}\Omega_{\xi_{D'_s}\cdot\xi_{z_s}} \\
&+ \sum_{i=1}^{m}\Omega_{\xi_{D''_i}\cdot\xi_{e_i}} + \sum_{1\le q,r\le d} d_{q,r}\Omega_{\xi_{D_q}\cdot\xi_{D_r}}.
\end{aligned}
$$

We replace by the formulas in (14)–(15) and we obtain, for all $w \in \mathfrak{n}$,

$$
\begin{aligned}
S = &\frac{1}{2}\sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} \lambda_i e_l \cdot e_l + \sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} \frac{1}{2}(\lambda_i - a)\left(-2\; e_l \cdot [w, e_l] + [w, e_l]^2\right) \\
&+ \sum_{s=1}^{n}\left(z_s \cdot D'_s w - \frac{1}{2} z_s \cdot [w, D'_s w]\right) + \sum_{1\le q,r\le d} d_{q,r}\Omega_{\xi_{D_q}\cdot\xi_{D_r}} \\
&+ \sum_{i=1}^{m} e_i \cdot D''_i w - ([w, e_i] \cdot D''_i w + \frac{1}{2} e_i \cdot [w, D''_i w]) + \frac{1}{2}[w, e_i] \cdot [w, D''_i w].
\end{aligned}
$$

The right-hand side is polynomial in the coordinates of w (expressed in the above basis of $\mathfrak{n}$), whereas the left-hand side is constant. The equality above

holds, if and only if the coefficients in each degree coincide. Equality in degree one holds, if and only if

$$\sum_{s=1}^{n} z_s \cdot D'_s w + \sum_{i=1}^{m} e_i \cdot D''_i w = \sum_{i=1}^{k} \sum_{l=m_{i-1}+1}^{m_i} (\lambda_i - a) e_l \cdot [w, e_l].$$

Contracting this equality with z_r for some fixed r in $\{1, \dots, n\}$ gives for any $w \in \mathfrak{v}$:

$$\begin{aligned} D'_r w &= \sum_{i=1}^{k} \sum_{l=m_{i-1}+1}^{m_i} (\lambda_i - a) g([w, e_l], z_r) e_l \\ &= \sum_{i=1}^{k} \sum_{l=m_{i-1}+1}^{m_i} (\lambda_i - a) g(j(z_r)w, e_l) e_l \\ &= j(z_r) \sum_{i=1}^{k} (\lambda_i - a) \operatorname{pr}_{\mathfrak{v}_i} w = T_{z_r}^{\boldsymbol{\lambda}-a} w. \end{aligned}$$

Therefore, D'_r extends $T_{z_r}^{\boldsymbol{\lambda}-a}$ to a skew-symmetric derivation of $\mathfrak{n}$. Since the map $z \mapsto T_z^{\boldsymbol{\lambda}-a}$ is linear, we obtain that $T_z^{\boldsymbol{\lambda}-a}$ extends to a skew-symmetric derivation for all $z \in \mathfrak{z}$.

In order to prove the converse statement, let $S \in \operatorname{Sym}^2 \mathfrak{v}$ define a left-invariant symmetric Killing tensor with eigenvalues $\lambda_1, \dots, \lambda_k$ and let $a \in \mathbb{R}$ be such that for every $z \in \mathfrak{z}$, $T_z^{\boldsymbol{\lambda}-a}$ extends to a derivation D_z of $\mathfrak{n}$, where $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_k)$. We shall explicitly give a linear combination of the metric and products of Killing vector fields as in (23) that is equal to S.

We claim that (23) is satisfied for the following choice of coefficients and derivations: a is the one coming from the hypothesis, $b_{s,t} = 0$ for all s, t, $c_{s,t} = 0$ for $s \neq t$, $c_{s,s} = -\frac{a}{2}$ for $s = 1, \dots n$, $a_{i,l} = 0$ for $i \neq l$ and $\frac{a}{2} + a_{l,l} = \frac{1}{2}\lambda_i$ for each $i = 1, \dots, k$ and $m_{i-1} + 1 \leq l \leq m_i$, $d_{q,r} = 0$ for all q, r, and $D''_i = 0$ for all i, and for $s = 1, \dots, n$, D'_s is the skew-symmetric derivation extending $T_{z_s}^{\boldsymbol{\lambda}-a}$. With these choices, we define the decomposable Killing tensor

(24)

$$\begin{aligned} K &:= ag + \sum_{i=1}^{k} \sum_{l=m_{i-1}+1}^{m_i} \frac{1}{2}(\lambda_i - a) \Omega_{\xi_{e_l} \cdot \xi_{e_l}} - \frac{a}{2} \sum_{s=1}^{n} \Omega_{\xi_{z_s} \cdot \xi_{z_s}} + \sum_{s=1}^{n} \Omega_{\xi_{D'_s}, \xi_{z_s}} \\ &= \frac{1}{2} \sum_{i=1}^{k} \sum_{l=m_{i-1}+1}^{m_i} \lambda_i e_l \cdot e_l + \sum_{i=1}^{k} \sum_{l=m_{i-1}+1}^{m_i} \frac{1}{2}(\lambda_i - a) \left(-2\, e_l \cdot [w, e_l] + [w, e_l]^2 \right) \\ &\quad + \sum_{s=1}^{n} \left(z_s \cdot D'_s w - \frac{1}{2} z_s \cdot [w, D'_s w] \right), \end{aligned}$$

where the last equality follows again from (14)–(15), and we will show that actually $K = S$.

Reasoning as before gives $\sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i}(\lambda_i - a)e_l \cdot [w, e_l] = \sum_{s=1}^{n} z_s \cdot D'_s w$ for all $w \in \mathfrak{v}$. We claim that this also holds for $w \in \mathfrak{z}$. Since the left-hand side vanishes in this case, we need to show that $\sum_{s=1}^{n} z_s \cdot D'_s w = 0$, for all $w \in \mathfrak{z}$.

For every $z, z' \in \mathfrak{z}$, $j(D_z z')$, $j(D_{z'} z)$ are both in $\mathfrak{so}(\mathfrak{v})$; they preserve each $\mathfrak{v}_i$ and are, actually, opposite in each $\mathfrak{v}_i$, since by (10):

$$\begin{aligned} j(D_z z')|_{\mathfrak{v}_i} &= (\lambda_i - a)[j(z)|_{\mathfrak{v}_i}, j(z')|_{\mathfrak{v}_i}] \\ &= -(\lambda_i - a)[j(z')|_{\mathfrak{v}_i}, j(z)|_{\mathfrak{v}_i}] = -j(D_{z'} z)|_{\mathfrak{v}_i}. \end{aligned}$$

Therefore, $j(D_z z') = -j(D_{z'} z)$, and, thus, $D_z z' = -D_{z'} z$, since j is injective.

Now given $w \in \mathfrak{z}$,

$$\begin{aligned} \sum_{s=1}^{n}(z_s \cdot D'_s w)(z, z') &= \sum_{s=1}^{n} g(z_s, z) g(D_{z_s} w, z') + g(z_s, z') g(D_{z_s} w, z) \\ &= -\sum_{s=1}^{n} g(z_s, z) g(D_w z_s, z') + g(z_s, z') g(D_w z_s, z) \\ &= -g(D_w z, z') - g(D_w z', z) = 0, \end{aligned}$$

for all $z, z' \in \mathfrak{z}$, thus proving our claim. From (24), we thus get

$$K = S + \sum_{i=1}^{k} \sum_{l=m_{i-1}+1}^{m_i} \frac{1}{2}(\lambda_i - a)[w, e_l]^2 - \frac{1}{2}\sum_{s=1}^{n} z_s \cdot [w, D'_s w]. \tag{25}$$

Finally, for every $w \in \mathfrak{v}$ we have:

$$\begin{aligned} \sum_{s=1}^{n} z_s \cdot [w, D'_s w] &= \sum_{s=1}^{n}\sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} z_s \cdot [w, e_l]\ g(e_l, D'_s w) \\ &= -\sum_{s=1}^{n}\sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} z_s \cdot [w, e_l]\ g(T_{z_s}^{\boldsymbol{\lambda}-a} e_l, w) \\ &= -\sum_{s=1}^{n}\sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} (\lambda_i - a) z_s \cdot [w, e_l]\ g(j(z_s) e_l, w) \\ &= -\sum_{s=1}^{n}\sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} (\lambda_i - a) z_s \cdot [w, e_l]\ g(z_s, [e_l, w]) \\ &= \sum_{i=1}^{k}\sum_{l=m_{i-1}+1}^{m_i} (\lambda_i - a)[w, e_l]^2, \end{aligned}$$

which together with (25) shows that $S = K$, and so S is decomposable. □

For the statement of the next result, we introduce some terminology. We say that an orthogonal decomposition $\mathfrak{v} = \mathfrak{v}_1 \oplus \ldots \oplus \mathfrak{v}_k$ is $j(\mathfrak{z})$-invariant if it is preserved by $j(z)$ for every $z \in \mathfrak{z}$. Equivalently, such a decomposition is $j(\mathfrak{z})$-invariant if $[\mathfrak{v}_i, \mathfrak{v}_j] = 0$ for all $i \neq j$. In this case, we denote by $j(\mathfrak{z})|_{\mathfrak{v}_i}$ the vector subspace of $\mathfrak{so}(\mathfrak{v}_i)$

$$j(\mathfrak{z})|_{\mathfrak{v}_i} := \{j(z)|_{\mathfrak{v}_i} : \mathfrak{v}_i \longrightarrow \mathfrak{v}_i \mid z \in \mathfrak{z}\}.$$

As a first application of Theorem 5.10, we describe Lie groups for which every left-invariant symmetric Killing 2-tensor is decomposable.

COROLLARY 5.11. — *Let $\mathfrak{n}$ be an irreducible two-step nilpotent Lie algebra, such that one of the following conditions holds:*

- $\dim \mathfrak{z} = 1$*;*
- $\dim \mathfrak{z} \geq 2$*, and for any $j(\mathfrak{z})$-invariant orthogonal decomposition $\mathfrak{v} = \mathfrak{v}_1 \oplus \ldots \oplus \mathfrak{v}_k$, one has that $j(\mathfrak{z})|_{\mathfrak{v}_i}$ is an abelian subalgebra of $\mathfrak{so}(\mathfrak{v}_i)$, for all $i = 1, \ldots, k$ except possibly for one index i_0.*

Then, any left-invariant symmetric Killing 2-tensor on N is decomposable.

Proof. — In view of Proposition 5.5 it is enough to show that any left-invariant symmetric Killing tensor defined by an element in $\mathrm{Sym}^2\mathfrak{v}$ is decomposable. Let $S \in \mathrm{Sym}^2\mathfrak{v}$ and let $\mathfrak{v} = \mathfrak{v}_1 \oplus \ldots \oplus \mathfrak{v}_k$ be the orthogonal decomposition in eigenspaces of S in $\mathfrak{v}$. We apply the converse of Theorem 5.10 to show that S is decomposable.

If $\dim \mathfrak{z} = 1$, then $j(\mathfrak{z})$ is an abelian subalgebra of $\mathfrak{so}(\mathfrak{v})$. Choose $a \in \mathbb{R}$ arbitrarily and let D_z be the endomorphism of $\mathfrak{n}$ that extends $T_z^{\boldsymbol{\lambda}-a}$ by zero, for $z \in \mathfrak{z}$. Then, for all $z' \in \mathfrak{z}$, $j(D_z z') = 0$ by definition, and

$$[D_z|_{\mathfrak{v}}, j(z')] = [T_z^{\boldsymbol{\lambda}-a}, j(z')] = (\lambda - a)[j(z), j(z')] = 0$$

because $\mathfrak{z}$ is of dimension 1. Hence, (10) holds, and, thus, D_z is a skew-symmetric derivation of $\mathfrak{n}$ that extends $T_z^{\boldsymbol{\lambda}-a}$.

For the second case, up to reordering the indexes, one can assume that $j(\mathfrak{z})|_{\mathfrak{v}_i}$ is an abelian subalgebra of $\mathfrak{so}(\mathfrak{v}_i)$, for all $i = 2, \ldots, k$. For each $z \in \mathfrak{z}$, let D_z be the extension by zero of $T_z^{\boldsymbol{\lambda}-\lambda_1}$. We claim that D_z is a derivation of $\mathfrak{n}$ for all z. Indeed, $[T_z^{\boldsymbol{\lambda}-\lambda_1}, j(z')]|_{\mathfrak{v}_1} = 0$, and for $i \geq 2$, we have

$$[T_z^{\boldsymbol{\lambda}-\lambda_1}, j(z')]|_{\mathfrak{v}_i} = (\lambda_i - \lambda_1)[j(z)|_{\mathfrak{v}_i}, j(z')|_{\mathfrak{v}_i}] = 0$$

since $j(\mathfrak{z})|_{\mathfrak{v}_i}$ is an abelian subalgebra of $\mathfrak{so}(\mathfrak{v}_i)$. Therefore, D_z satisfies (10), so it is a derivation of $\mathfrak{n}$.

In both cases, we thus obtain that S is decomposable by Theorem 5.10. □

EXAMPLE 5.12. — Every left-invariant symmetric Killing 2-tensor on the Heisenberg Lie group in Example 4.8 is decomposable. Indeed, the center of $\mathfrak{h}_{2n+1}$ is one-dimensional.

THEOREM 5.13. — *Every left-invariant symmetric Killing 2-tensor on a two-step nilpotent Lie group of dimension ≤ 7 is decomposable.*

Proof. — Let N be a two-step nilpotent Lie group and suppose there is some left-invariant symmetric Killing 2-tensor on N that is indecomposable. By Proposition 5.6, we can assume that its Lie algebra $\mathfrak{n}$ is irreducible. Corollary 5.11 implies that $\dim \mathfrak{z} \geq 2$, and there exists a decomposition $\mathfrak{v} = \mathfrak{v}_1 \oplus \cdots \oplus \mathfrak{v}_k$ in $j(\mathfrak{z})$-invariant subspaces, such that for at least two indices i_0, i_1, the vector subspaces $j(\mathfrak{z})|_{\mathfrak{v}_{i_0}}$ and $j(\mathfrak{z})|_{\mathfrak{v}_{i_1}}$ are not abelian subalgebras of $\mathfrak{so}(\mathfrak{v}_{i_0})$ and $\mathfrak{so}(\mathfrak{v}_{i_1})$, respectively. This, in particular, implies that $\dim \mathfrak{v}_{i_0}$ and $\dim \mathfrak{v}_{i_1}$ are both ≥ 3, and, therefore, $\dim \mathfrak{n} \geq \dim(\mathfrak{z} \oplus \mathfrak{v}_{i_0} \oplus \mathfrak{v}_{i_1}) \geq 8$. □

A second application of Theorem 5.10 is a method to construct two-step nilpotent Lie groups admitting left-invariant indecomposable symmetric Killing 2-tensors.

COROLLARY 5.14. — *Let $S \in \mathrm{Sym}^2\mathfrak{v}$ define a left-invariant symmetric Killing tensor and consider the decomposition of $\mathfrak{v}$ as the orthogonal direct sum of eigenspaces of S, $\mathfrak{v} = \bigoplus_{i=1}^k \mathfrak{v}_i$. If there exist $i \neq j$, such that $j(\mathfrak{z})|_{\mathfrak{v}_i}$ and $j(\mathfrak{z})|_{\mathfrak{v}_j}$ are not subalgebras of $\mathfrak{so}(\mathfrak{v}_i)$ and $\mathfrak{so}(\mathfrak{v}_j)$, respectively, then S is indecomposable.*

Proof. — Suppose that S is decomposable and denote by $\boldsymbol{\lambda}$ the vector of distinct eigenvalues of S viewed as an endomorphism of $\mathfrak{v}$ and by $\mathfrak{v} = \mathfrak{v}_1 \oplus \cdots \oplus \mathfrak{v}_k$ the corresponding decomposition in eigenspaces of S. By Theorem 5.10, there exists $a \in \mathbb{R}$, such that for all $z \in \mathfrak{z}$, $T_z^{\boldsymbol{\lambda}-a}$ extends to a skew-symmetric derivation of $\mathfrak{n}$. Since $i \neq j$, the eigenvalues λ_i and λ_j are distinct, so we may assume that $(\lambda_i - a) \neq 0$ (otherwise just replace i by j).

Given $z \in \mathfrak{z}$, denote by D_z the skew-symmetric derivation of $\mathfrak{n}$ extending $T_z^{\boldsymbol{\lambda}-a}$. Then, (10) gives

$$j(D_z z') = [T_z^{\boldsymbol{\lambda}-a}, j(z')], \text{ for all } z, z' \in \mathfrak{z}. \tag{26}$$

Restricting to $\mathfrak{v}_i$, this equality gives $j(D_z z')|_{\mathfrak{v}_i} = (\lambda_i - a)[j(z)|_{\mathfrak{v}_i}, j(z')|_{\mathfrak{v}_i}]$, which implies that $j(\mathfrak{z})|_{\mathfrak{v}_i}$ is a Lie subalgebra of $\mathfrak{so}(\mathfrak{v}_i)$, since $\lambda_i - a \neq 0$. This contradicts the hypothesis, thus showing that S is indecomposable. □

Next, we present the aforementioned construction method. Let (V, g) be an inner product space and consider a vector subspace $\mathfrak{z} \subset \mathfrak{so}(V, g)$, which is not a Lie subalgebra of $\mathfrak{so}(V, g)$. Set $\mathfrak{v}_1 = \mathfrak{v}_2 := V$, $\mathfrak{n} := \mathfrak{v}_1 \oplus \mathfrak{v}_2 \oplus \mathfrak{z}$ and define an inner product on $\mathfrak{n}$ making $\mathfrak{v}_1$, $\mathfrak{v}_2$, $\mathfrak{z}$ all orthogonal and extending g in $\mathfrak{v}_1 = \mathfrak{v}_2 = V$ (the choice is arbitrary in $\mathfrak{z}$). On $\mathfrak{n}$ we define the Lie bracket, such that

$$[\mathfrak{v}_1 \oplus \mathfrak{v}_2, \mathfrak{z}] = 0, \quad [\mathfrak{v}_1, \mathfrak{v}_2] = 0, \quad g([x_i, y_i], z) = g(z(x_i), y_i), \text{ for } x_i, y_i \in \mathfrak{v}_i.$$

Then, the map $j : \mathfrak{z} \longrightarrow \mathfrak{so}(\mathfrak{v}_1 \oplus \mathfrak{v}_2)$ is given by $j(z) = \left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right)$.

Fix $\alpha \neq 1$ and consider the endomorphism $S = \mathrm{Id}_{\mathfrak{v}_1} + \alpha \mathrm{Id}_{\mathfrak{v}_2}$ of $\mathfrak{v}$. By Proposition 4.1, S defines a left-invariant symmetric Killing 2-tensor. Moreover, since $j(\mathfrak{z})|_{\mathfrak{v}_1}$ and $j(\mathfrak{z})|_{\mathfrak{v}_2}$ (which are both isomorphic to $\mathfrak{z}$) are not Lie subalgebras of $\mathfrak{so}(\mathfrak{v}_1) = \mathfrak{so}(\mathfrak{v}_2)$, Corollary 5.14 shows that S is indecomposable.

The following is an explicit example of this construction.

EXAMPLE 5.15. — Let $\mathfrak{n}$ be the two-step nilpotent Lie algebra of dimension 8 with orthonormal basis $e_1, \ldots, e_6, z_1, z_2$ satisfying the bracket relations

$$[e_1, e_2] = z_1 = [e_4, e_5], \qquad [e_2, e_3] = z_2 = [e_5, e_6].$$

Consider $S \in \mathrm{Sym}^2\mathfrak{n}$ defined by $Se_i = e_i$ for $i = 1, 2, 3$, $Se_i = 2e_i$ for $i = 4, 5, 6$, and $Sz_1 = Sz_2 = 0$. Since S verifies (17), it defines a left-invariant Killing tensor. The decomposition of $\mathfrak{v}$ is given by $\mathfrak{v}_1 = \mathrm{span}\{e_1, e_2, e_3\}$ and $\mathfrak{v}_2 = \mathrm{span}\{e_3, e_4, e_6\}$. For both $i = 1, 2$, $j(\mathfrak{z})|_{\mathfrak{v}_i}$, in the corresponding basis, is spanned by the matrices

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The vector space spanned by these two matrices is clearly not a Lie subalgebra of $\mathfrak{so}(3)$, so the left-invariant symmetric tensor defined by S is indecomposable.

REMARK 5.16. — The above examples of indecomposable symmetric Killing tensors can be used to produce examples on compact nilmanifolds.

Recall that a nilpotent Lie group N admits a cocompact discrete subgroup Γ if and only if its Lie algebra $\mathfrak{n}$ is rational, that is, $\mathfrak{n}$ admits a basis with structure constants in $\mathbb{Q}$ (cf. [15]). In this case, any left-invariant Riemannian metric on N defines a Riemannian metric on the compact manifold $\Gamma \setminus N$, so that the natural projection $p : N \longrightarrow \Gamma \setminus N$ is a locally isometric covering.

Every left-invariant symmetric Killing tensor field S on N projects to a Killing tensor field $\bar{S}$ on $\Gamma \setminus N$, and clearly, if S is indecomposable on N, then $\bar{S}$ is indecomposable on $\Gamma \setminus N$.

Appendix A. Parallel distributions on nilpotent Lie groups

In this section, we will prove a property of parallel tensors on nilpotent Lie groups that was used in Theorem 5.10, but which, we think, is also of independent interest.

THEOREM A.1. — *Every parallel symmetric 2-tensor on a two-step nilpotent Lie group with left-invariant Riemannian metric (N, g) is left-invariant.*

Proof. — Since the Lie algebra $\mathfrak{n}$ is two-step nilpotent, we have $[[\mathfrak{n}, \mathfrak{n}], \mathfrak{n}] = 0$, so the derived algebra $\mathfrak{n}' := [\mathfrak{n}, \mathfrak{n}]$ is contained in the center $\mathfrak{z}$ of $\mathfrak{n}$. Consider first the case where $\mathfrak{n}' = \mathfrak{z}$. It is easy to check that the Ricci tensor of (N, g)

at the identity preserves the decomposition $\mathfrak{n} = \mathfrak{v} \oplus \mathfrak{z}$ (where we recall that $\mathfrak{v} = \mathfrak{z}^{\perp}$) and is positive definite on $\mathfrak{z}$ and negative definite on $\mathfrak{v}$ [5, Proposition 2.5]. In particular, (N, g) carries no parallel vector fields, so its factors (N_i, g_i), $i = 1, \ldots, k$ in the de Rham decomposition are nonflat irreducible Riemannian manifolds. Correspondingly, we write $\mathfrak{n} = T_e N = T_1 \oplus \ldots \oplus T_k$.

Let D be any parallel distribution on N. We claim that D_e (which, of course, determines D) is the direct sum of some of the subspaces T_i. To see this, consider the holonomy group $\mathrm{Hol}_e(N) \subset \mathfrak{so}(\mathfrak{n})$. By the de Rham theorem, $\mathrm{Hol}_e(N) = H_1 \times \ldots \times H_k$, where H_i acts irreducibly on T_i, for each $i = 1, \ldots, k$. Since D is parallel, D_e is a subspace of $T_1 \oplus \ldots \oplus T_k$ invariant by $H_1 \times \ldots \times H_k$. The orthogonal projection denoted by D_i of D onto T_i obviously contains $D_e \cap T_i$, and both are H_i-invariant subspaces of T_i. Thus, $D_i = 0$ or $D_i = T_i$ for every i. Since

$$\bigoplus_i (D_e \cap T_i) \subset D_e \subset \bigoplus_i D_i,$$

to prove our claim, we need to show that $D_e \cap T_j = D_j$ for every j. By the irreducibility of T_j as an H_j-representation, it is enough to show that if $D_j \neq 0$, then $D_e \cap T_j \neq 0$.

Let us fix any $j \in \{1, \ldots, k\}$ with $D_j \neq 0$ and take any nonzero $x_j \in D_j$. Then, there exist $x_i \in D_i$, for every $i \neq j$, such that $x := x_1 + \ldots + x_k \in D$. Every element $h_j \in H_j$ acts trivially on T_i for $i \neq j$, so we get that $D_e \ni h_j(x) = x_1 + \ldots + x_{j-1} + h_j(x_j) + x_{j+1} + \ldots + x_k$, and thus $x_j - h_j(x_j) = x - h_j(x) \in D_e$.

Since H_j is not trivial and T_j is an irreducible H_j-representation, there exists $h_j \in H_j$, such that $h_j(x_j) \neq x_j$. The nonzero vector $x_j - h_j(x_j)$ belongs to $D_e \cap T_j$, thus proving our claim.

In particular, this proves that the Riemannian manifold (N, g) carries only a finite number of parallel distributions. Assume now that K is a parallel symmetric 2-tensor on N. If $\lambda_1, \ldots, \lambda_l$ denote the spectrum of K_e, the corresponding eigenspaces define parallel distributions $V_1, \ldots, V_l$ on N, such that $K = \sum_{i=1}^{l} \lambda_i \mathrm{Id}_{V_i}$. Let us fix $i \in \{1, \ldots, l\}$. For every element $h \in N$, $h_*(V_i)$ belongs to a finite set of parallel distributions, so by continuity, as N is connected, $h_*(V_i) = V_i$. This shows that $h_* K = K$, so K is left-invariant.

For the general case, one defines, as in Remark 4.10 (2), the abelian ideal $\mathfrak{a}$ of $\mathfrak{n}$ by $\mathfrak{a} := \mathfrak{z} \cap \mathfrak{n}'^{\perp}$ and observes that $\tilde{\mathfrak{n}} := \mathfrak{v} \oplus \mathfrak{n}'$ is also an ideal, and $\mathfrak{n} = \tilde{\mathfrak{n}} \oplus \mathfrak{a}$ is an orthogonal direct sum of ideals. Correspondingly, the simply connected Lie group N endowed with the left-invariant metric g is a Riemannian product $(\tilde{N}, \tilde{g}) \times \mathbb{R}^n$, where $n = \dim(\mathfrak{a})$, and $\tilde{g}$ is the restriction of g to $\tilde{\mathfrak{n}}$. By construction, the derived algebra $\tilde{\mathfrak{n}}'$ is equal to the center of $\tilde{\mathfrak{n}}$, so by the first part of the proof, every parallel symmetric tensor on $\tilde{N}$ is left-invariant. Moreover, since $(\tilde{N}, \tilde{g})$ has no parallel vector field, it follows that every parallel symmetric tensor on $(\tilde{N}, \tilde{g}) \times \mathbb{R}^n$ is the sum of a constant symmetric tensor

on $\mathbb{R}^n$ and a parallel symmetric tensor on $\tilde{N}$, and is, thus, left-invariant. This concludes the proof. □

The hypothesis that N is two-step nilpotent is essential in the above theorem, as shown by the following (counter)example.

EXAMPLE A.2. — Assume that G is the simply connected Lie group generated by the solvable 3-dimensional Lie algebra $\mathfrak{g}$ defined by the brackets

$$[e_1, e_2] = 0, \qquad [e_2, e_3] = e_1, \qquad [e_3, e_1] = e_2.$$

Consider the left-invariant metric on G defined by requiring that e_1, e_2, e_3 is orthonormal and denote by E_i the left-invariant vector field on G that is equal to e_i at the identity. The Koszul formula (2) immediately shows that the Levi-Civita connection ∇ of this metric is given by

$$\nabla_{E_1}E_1 = \nabla_{E_2}E_2 = \nabla_{E_3}E_3 = \nabla_{E_1}E_2 = \nabla_{E_2}E_1 = \nabla_{E_1}E_3 = \nabla_{E_2}E_3 = 0,$$
$$\nabla_{E_3}E_1 = E_2, \qquad \nabla_{E_3}E_2 = -E_1.$$

A straightforward computation then shows that the Riemannian curvature of ∇ vanishes, so every symmetric tensor on $\mathfrak{g}$ defines a parallel tensor on G by parallel transport. On the other hand, the left-invariant tensor $E_1 \cdot E_1$ is not parallel (since $\nabla_{E_3}(E_1 \cdot E_1) = 2E_1 \cdot E_2$), so it does not coincide with the parallel tensor on G defined by the parallel transport of $e_1 \cdot e_1$.

We will now show that the eigendistributions of a parallel symmetric endomorphism of TN (which are automatically left-invariant by Theorem A.1) define a decomposition of $\mathfrak{n}$ as orthogonal sum of ideals.

PROPOSITION A.3. — *Let $S \in \mathrm{Sym}^2\mathfrak{n}$ define a left-invariant symmetric tensor on N. Denote by $\lambda_i \in \mathbb{R}$ $(i = 1, \dots, k)$ the eigenvalues of S and by $\mathfrak{n}_i$ the corresponding eigenspaces, so that $\mathfrak{n}$ decomposes in an orthogonal direct sum of $\mathfrak{n} = \bigoplus_{i=1}^k \mathfrak{n}_i$. Then, $\nabla S = 0$, if and only if each $\mathfrak{n}_i$ is an ideal on $\mathfrak{n}$.*

Proof. — The "if" part is obvious, since if each $\mathfrak{n}_i$ is an ideal on $\mathfrak{n}$, then $\mathrm{Id}_{\mathfrak{n}_i}$ is parallel as an endomorphism of $\mathfrak{n}$, and, thus, so is $S = \sum_{i=1}^k \lambda_i \mathrm{Id}_{\mathfrak{n}_i}$.

Conversely, if S is parallel, then each $\mathfrak{n}_i$ defines a left-invariant parallel distribution on N, so it is enough to show that if the left-invariant distribution on N defined by a vector subspace $D \subset \mathfrak{n}$ is parallel, then D is an ideal of $\mathfrak{n}$.

Denote by $D^{\mathfrak{v}} \supset D \cap \mathfrak{v}$ the orthogonal projection of D onto $\mathfrak{v}$. We claim that $D^{\mathfrak{v}} = D \cap \mathfrak{v}$. Let $x \in D^{\mathfrak{v}}$ be some arbitrary element orthogonal to $D \cap \mathfrak{v}$. Then, there exists $z_0 \in \mathfrak{z}$ with $x + z_0 \in D$. For every $z \in \mathfrak{z}$, we have $D \ni \nabla_z(x + z_0) = -\frac{1}{2}j(z)(x)$ (see (9)), whence $j(z)(x) \in D \cap \mathfrak{v}$, for every $z \in \mathfrak{z}$. Moreover, $\nabla_z(j(z)(x)) = -\frac{1}{2}j(z)^2(x)$ clearly belongs to D (as D is parallel) and to $\mathfrak{v}$, so in particular, by the choice of x, it is orthogonal to x. Since $j(z)$

is skew-symmetric, this shows that $j(z)(x) = 0$ for every $z \in \mathfrak{z}$, whence $x = 0$, thus proving our claim.

This shows that $D = (D \cap \mathfrak{v}) \oplus (D \cap \mathfrak{z})$. In order to prove that D is an ideal it is now equivalent to check that for every $x \in D \cap \mathfrak{v}$ and $y \in \mathfrak{v}$, one has $[x, y] \in D$ (all other commutators are automatically 0). This is clear, since $[x, y] = -2\nabla_y x \in D$ as D is parallel. □

As a corollary, we obtain the following result about two-step nilpotent Lie algebras, which is also of independent interest.

COROLLARY A.4. — *Let* $(\mathfrak{n}, g)$ *be a two-step nilpotent metric Lie algebra. Then, there exist* irreducible *two-step nilpotent metric Lie algebras* $(\mathfrak{n}_i, g_i)$ $i \in \{1, \dots, k\}$ *(unique up to reordering) such that*

$$(\mathfrak{n}, g) = \bigoplus_{i=1}^{k} (\mathfrak{n}_i, g_i) \oplus (\mathfrak{a}, g_0),$$

for some abelian metric Lie algebra $(\mathfrak{a}, g_0)$.

Proof. — By definition, every reducible two-step nilpotent Lie algebra is the orthogonal direct sum of ideals, each of them being two-step nilpotent or abelian. The above decomposition, thus, always exists. Consider such a decomposition and denote by N and N_i the simply connected Lie groups with Lie algebras $\mathfrak{n}$ and $\mathfrak{n}_i$, respectively. Then, (N, g) is isometric to the Riemannian product

$$(N_1, g_1) \times \ldots \times (N_k, g_k) \times \mathbb{R}^{\dim(\mathfrak{a})},$$

and, moreover, (N_i, g_i) is an irreducible Riemannian manifold, for each $i \in \{1, \dots, k\}$. Indeed, if some (N_i, g_i) were reducible, then the restriction of the metric g_i to the factors would define parallel symmetric tensors on (N_i, g_i), which by Theorem A.1 have to be left-invariant. By Proposition A.3 this would give a decomposition of $\mathfrak{n}_i$ as an orthogonal direct sum of ideals, thus contradicting its irreducibility.

Therefore, the uniqueness statement follows from the uniqueness (up to reordering) of the de Rham decomposition of Riemannian manifolds. □

Acknowledgment. — The research presented in this paper was done during the visit of the first author at the Laboratoire de Mathématiques d'Orsay, Univ. Paris-Sud. She expresses her gratitude to the LMO for its hospitality and to Fundação de Amparo à Pesquisa do Estado de São Paulo (Brazil) for the financial support. Both authors are grateful to the anonymous referee for the careful reading of the manuscript and useful suggestions that helped to improve the presentation.

BIBLIOGRAPHY

[1] A. Andrada & I. G. Dotti – "Conformal Killing-Yano 2-forms", *Differ. Geom. Appl.* **58** (2018), p. 103–119.

[2] M. L. Barberis, I. G. Dotti & O. Santillán – "The Killing-Yano equation on Lie groups", *Classical Quantum Gravity* **29** (2012), no. 6, p. 1–10.

[3] A. Bolsinov, V. Matveev, E. Miranda & S. Tabachnikov – "Open problems, questions, and challenges in finite-dimensional integrable systems", *Philos. Trans. Roy. Soc. A* **376** (2018), no. 2131.

[4] L. Butler – "Integrable geodesic flows with wild first integrals: the case of two-step nilmanifolds", *Ergodic Theory Dyn. Syst.* **23** (2003), no. 3, p. 771–797.

[5] P. Eberlein – "Geometry of 2-step nilpotent groups with a left invariant metric", *Ann. Sci. École Norm. Sup. (4)* **27** (1994), no. 5, p. 611–660.

[6] K. Heil – *Killing and conformal killing tensors*, Dissertation an der Universität Stuttgart, 2018.

[7] K. Heil, A. Moroianu & U. Semmelmann – "Killing and conformal Killing tensors", *J. Geom. Phys.* **106** (2016), p. 383–400.

[8] ———, "Killing tensors on tori", *J. Geom. Phys.* **117** (2017), p. 1–6.

[9] S. Helgason – *Differential geometry, Lie groups, and symmetric spaces*, Pure and Applied Mathematics, vol. 80, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1978.

[10] A. Kocsard, G. P. Ovando & S. Reggiani – "On first integrals of the geodesic flow on Heisenberg nilmanifolds", *Differ. Geom. Appl.* **49** (2016), p. 496–509.

[11] V. Matveev & V. Shevchishin – "Two-dimensional superintegrable metrics with one linear and one cubic integral", *J. Geom. Phys.* **61** (2011), no. 8, p. 1353–1377.

[12] A. S. Mischenko & A. T. Fomenko – "Euler equations on finite-dimensional Lie groups", *Math. USSR-Izv.* **12** (1978), no. 2, p. 371–389.

[13] R. Montgomery, M. Shapiro & A. Stolin – "A nonintegrable sub-Riemannian geodesic flow on a Carnot group", *J. Dyn. Control Syst.* **3** (1997), no. 4, p. 519–530.

[14] G. P. Ovando – "The geodesic flow on nilmanifolds associated to graphs", *arXiv 1708.09457*.

[15] M. S. Raghunathan – *Discrete subgroups of Lie groups*, Springer, 1972.

[16] U. Semmelmann – "Conformal Killing forms on Riemannian manifolds", *Math. Z.* **245** (2013), p. 503–527.

[17] M. Takeuchi – "Killing tensor fields on spaces of constant curvature", *Tsukuba J. Math.* **7** (1983), p. 233–255.

[18] G. Thompson – "Killing tensors in spaces of constant curvature", *J. Math. Phys.* **27** (1986), no. 11, p. 2693–2699.

[19] V. S. Varadarajan – *Lie groups, Lie algebras, and their representations*, Graduate Texts in Mathematics, vol. 102, Springer-Verlag, New York, 1984, Reprint of the 1974 edition.

[20] J. Wolf – "On locally symmetric spaces of non-negative curvature and certain other locally homogeneous spaces", *Comment. Math. Helv.* **37** (1963), p. 266–295.

Bull. Soc. Math. France
148 (3), 2020, p. 439-465

LE CRISTAL DE DIEUDONNÉ DES SCHÉMAS EN $\mathbb{F}$-VECTORIELS

PAR ARNAUD VANHAECKE

RÉSUMÉ. — Dans cet article on décrit le cristal de Dieudonné d'un schéma en groupes fini localement libre, muni d'une action vectorielle d'un corps fini $\mathbb{F}$. Ces schémas en $\mathbb{F}$-vectoriels apparaissent lorsqu'on considère les points de torsion d'un module p-divisible. Une classe particulière de schémas en $\mathbb{F}$-vectoriels a été classifiée par Raynaud dans [9], ce qui nous permet de déterminer la structure des points de torsion d'un module p-divisible, sous certaines conditions sur son algèbre de Lie.

ABSTRACT (*The Dieudonné crystal of* $\mathbb{F}$*-vector schemes*). — In this paper we describe the Dieudonné crystal of a finite locally free group scheme with a vector action of a finite field $\mathbb{F}$. These $\mathbb{F}$-vector schemes appear when one considers torsion points of p-divisible modules. A particular class of $\mathbb{F}$-vector schemes has been classified by Raynaud in [9], which allows us to determine the structure of torsion points of p-divisible modules, under certain conditions on its the Lie algebra.

1. Introduction

Soit p un nombre premier et $\mathbb{F}$ un corps fini à $q = p^r$ éléments. On note $\Sigma = \operatorname{Spec} \mathrm{W}(\mathbb{F})$, où W désigne le foncteur des vecteurs de Witt. Soit S un schéma sur Σ tel que p soit localement nilpotent sur S. Dans cette introduction on supposera que S est affine, de la forme $\operatorname{Spec} R$ pour R une $\mathrm{W}(\mathbb{F})$-algèbre.

Texte reçu le 1er mai 2019, modifié le 15 décembre 2019, accepté le 20 février 2019.

ARNAUD VANHAECKE, Arnaud Vanhaecke, DMA, 45 rue d'Ulm, 75005 Paris, France • *E-mail :* arnaud.vanhaecke@ens.fr • *Url :* http://www.math.ens.fr/~vanhaecke/

Classification mathématique par sujets (2010). — 14L05, 14L15, 14F30.

Mots clefs. — Cristaux de Dieudonné, schémas en groupes finis, groupes p-divisibles.

© Société Mathématique de France
0037-9484/2020/439/$ 5.00
doi:10.24033/bsmf.2812

Dans [2], les auteurs ont introduit, par la cohomologie cristalline, une théorie de Dieudonné pour les schémas en groupes finis localement libres et les groupes p-divisibles sur S. À G un schéma en groupes fini localement libre (resp. X un groupe p-divisible) sur S on associe de manière fonctorielle un cristal $\mathbb{D}(G)$ (resp. $\mathbb{D}(X)$) sur le site cristallin $\mathrm{CRIS}(S/\Sigma)$. Le foncteur $\mathbb{D}$ et ses propriétés de pleine fidélité ont beaucoup été étudiés (cf. [6] par exemple) mais nous ne ferons pas usage de ces résultats. Nous utiliserons seulement que dans le cas où S est le spectre d'un corps parfait, le cristal de Dieudonné est équivalent au module de Dieudonné et qu'alors $\mathbb{D}$ est une équivalence de catégories.

Un *schéma en $\mathbb{F}$-vectoriels* G sur S est un schéma en groupes fini localement libre tel que pour tout schéma X sur S, $G(X)$ soit un espace vectoriel sur $\mathbb{F}$. C'est-à-dire que G est muni d'une action du groupe multiplicatif $\mathbb{F}^\times$, satisfaisant des conditions supplémentaires. Comme S est affine, $G = \operatorname{Spec} A$, où A est une algèbre de Hopf sur R munie d'une action de $\mathbb{F}^\times$. Cette action satisfait une propriété supplémentaire : l'addition dans $\mathbb{F}^\times \subset \mathbb{F}$ est compatible avec la convolution dans A. Cette propriété correspond à l'axiome que pour tout λ, $\lambda' \in \mathbb{F}$ et $v \in G(X)$, pour X un schéma sur S, $(\lambda + \lambda')v = \lambda v + \lambda' v$[1]. Cette action détermine une graduation indexée par $\mathbb{F}^\vee$, le groupe des caractères de $\mathbb{F}^\times$ à valeurs dans $\bar{\mathbb{Q}}_p$,

$$A = \bigoplus_{\chi \in \mathbb{F}^\vee} A_\chi. \tag{1}$$

Il n'est pas vrai que toute graduation de type $\mathbb{F}^\vee$ sur A donne lieu à une structure de schéma en $\mathbb{F}$-vectoriels sur G. En effet toute action de $\mathbb{F}^\times$ sur A ne s'étend pas nécessairement en une action vectorielle de $\mathbb{F}$. Notons que, comme A est localement libre sur R, il en est de même pour les A_χ. Dans [9], ces schémas ont été étudiés et ils sont classifiés dans le cas où pour tout $\chi \in \mathbb{F}^\vee$ non-trivial, A_χ est localement libre de rang 1 sur R et $A_1 = R \oplus A_1'$, pour A_1 la composante isotypique du caractère trivial, tel que A_1' est localement libre de rang 1. On est donc naturellement intéressé par le rang des A_χ.

Pour simplifier, on suppose $S = \operatorname{Spec} R$ connexe. Alors le rang des A_χ est constant sur R et on peut définir le *caractère de* G comme

$$\mathrm{Ch}_S(G) \coloneqq \sum_{\chi \in \mathbb{F}^\vee} \mathrm{rang}_R(A_\chi)[\chi] \in \mathbb{N}[\mathbb{F}^\vee].$$

Dans cet article on calcule ce caractère à partir du cristal de Dieudonné de G. Le cristal $\mathbb{D}(G)$ est muni d'une action de $\mathbb{F}^\times$ et donc admet une graduation du même type que (1). La relation de convolution implique que cette graduation

1. Noter que cet axiome est légèrement subtil car les deux sommes ne sont pas de même nature.

est de la forme

$$\mathbb{D}(G) = \bigoplus_{\chi \in \mathbb{F}^+} \mathbb{D}(G)_\chi,$$

où $\mathbb{F}^+ \subset \mathbb{F}^\vee$ est l'ensemble des caractères $\chi \in \mathbb{F}^\vee$, tels que si on pose $\chi(0) = 0$, χ est additif. Or, comme G est annulé par p, $\mathbb{D}(G)$ est localement libre comme module sur le faisceau structural du site cristallin de S modulo p (cf. [2, Proposition 4.3.1]). On peut donc parler du rang des $\mathbb{D}(G)_\chi$. On définit le *caractère infinitésimal* de G par

$$\mathfrak{ch}_S(\mathbb{D}(G)) \coloneqq \sum_{\chi \in \mathbb{F}^+} \mathrm{rang}_{R/pR}(\mathbb{D}(G)_\chi)[\chi] \in \mathbb{N}[\mathbb{F}^+],$$

où $\mathrm{rang}_{R/pR}(\mathbb{D}(G)_\chi)$ est le rang, en tant que module sur le faisceau structural du site cristallin de S modulo p, de la composante χ-isotypique de $\mathbb{D}(G)$. Le théorème central de cet article est que le caractère et le caractère infinitésimal de G sont reliés par une relation « exponentielle » :

THÉORÈME 1.1. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur S connexe. Soit $\mathfrak{ch}_S(\mathbb{D}(G)) = \sum_{\chi \in \mathbb{F}^+} n_\chi[\chi]$ le caractère infinitésimal de G et $\mathrm{Ch}_S(G)$ son caractère. Alors on a*

$$\mathrm{Ch}_S(G) = \prod_{\chi \in \mathbb{F}^+} \left(1 + [\chi] + \cdots + [\chi^{p-1}]\right)^{n_\chi}. \tag{2}$$

On montre ce théorème en le réduisant au cas où S est le spectre d'un corps parfait k de caractéristique p. On utilise ensuite que sur le spectre d'un corps parfait le cristal de Dieudonné est équivalent au module de Dieudonné de G. Notons que dans ce cas, on obtient une équivalence entre schémas en $\mathbb{F}$-vectoriels et modules de Dieudonné gradués sur $\mathbb{F}^+$ tels que F et V, respectivement le Frobenius et le Verschibung, définissent des endomorphismes gradués. On prouve ensuite le théorème par un calcul explicite lorsque G est annulé par V, puis par un argument de dévissage on en déduit le théorème dans le cas où V est nilpotent. On conclut finalement par un argument de dualité. Une conséquence de ce théorème est que pour savoir si un schéma en $\mathbb{F}$-vectoriels G est un schéma de Raynaud, il suffit de connaître son caractère infinitésimal, qui ne dépend que du cristal de Dieudonné de G. Cette relation devrait avoir des applications dans des situations où G n'est pas un schéma de Raynaud.

La formule des caractères (2) est apparue dans l'étude des O_D-modules formels spéciaux de Drinfeld (cf. [4]) en vue de la construction d'un modèle formel du premier revêtement de l'espace de Drinfeld (cf. [10]). On note K une extension finie de $\mathbb{Q}_p$ de degré $n = ef$ et D une algèbre à division centrale sur K d'invariant $1/d$, $d \geqslant 2$. On note O_D l'ordre maximal de D et Π une uniformisante de O_D. Un groupe p-divisible muni d'une action de O_D est appelé

O_D-module p-divisible. Maintenant, $\mathbb{F}$ désigne le corps résiduel de O_D, c'est-à-dire que $r = fd$ avec les notations précédentes ; $S = \operatorname{Spec} R$ désigne toujours un schéma sur Σ tel que p est localement nilpotent sur S. Notons que si X est un O_D-module p-divisible sur S alors le schéma des Π-points de torsion $X[\Pi]$ est un schéma en $\mathbb{F}$-vectoriels sur S. Le but de la dernière section est de calculer le caractère des points de torsion de certains modules p-divisibles, en particulier des O_D-module p-divisibles.

Si X est un O_D-module p-divisible sur S, son algèbre de Lie est munie d'une action de $\mathbb{F}$. On note κ le corps résiduel de K et $\mathbb{F}_\kappa^+ \subset \mathbb{F}^+$ l'ensemble des caractères κ-linéaires. L'algèbre de Lie est graduée sur $\mathbb{F}^+$,

$$\operatorname{Lie}(X) = \bigoplus_{\chi \in \mathbb{F}^+} \operatorname{Lie}(X)_\chi,$$

et on dit que l'action de O_D est *stricte* sur X si $\operatorname{Lie}(X)_\chi = 0$ pour tout $\chi \notin \mathbb{F}_\kappa^+$. Si, de plus, pour tout $\chi \in \mathbb{F}_\kappa^+$, $\operatorname{Lie}(X)_\chi$ est localement libre de rang 1 sur S, alors X est appelé *O_D-module formel spécial.* Notons que dans ce cas, X est de hauteur nd^2. L'impulsion de départ de ce travail était de trouver une preuve alternative au résultat suivant :

Proposition 1.2. — *Si X est un O_D-module formel spécial sur S, alors $X[\Pi]$ est un schéma de Raynaud.*

Ce résultat est démontré par exemple dans [11] en utilisant que tout O_D-module formel spécial admet un relèvement en caractéristique zéro, puis qu'un schéma en $\mathbb{F}$-vectoriels étale de rang q est un schéma de Raynaud. L'intérêt est d'avoir des équations explicites pour $X[\Pi]$. À l'aide de la formule des caractères (2), on prouve une condition nécessaire et suffisante pour que $X[\Pi]$ soit un schéma de Raynaud.

Théorème 1.3. — *Soit X un O_D-module p-divisible de hauteur hnd^2, pour h un entier, sur S. Alors $X[\Pi]$ est un schéma de Raynaud si et seulement si $h = 1$ et pour tout $\chi \in \mathbb{F}^+$ on a*

$$\operatorname{rang}_R(\operatorname{Lie}(X)_\chi) = \operatorname{rang}_R(\operatorname{Lie}(X)_{\chi^q}).$$

Ces conditions sont vérifiées pour les O_D-modules formels spéciaux, ou plus généralement pour les O_D-modules formels r-spéciaux considérés dans [8].

2. Schémas en $\mathbb{F}$-vectoriels

On fixe un nombre premier p et un corps fini $\mathbb{F}$ à $q = p^r$ éléments. Dans cette section on rappelle la définition de schéma en $\mathbb{F}$-vectoriels introduite dans [9] et ses premières propriétés. On définira aussi le cristal associé à un schéma en groupes fini et on introduira les caractères du groupe et du cristal.

2.1. Généralités. —

2.1.1. Commençons par définir l'anneau de base D. Soit $\bar{\mathbb{Q}}$ une cloture algébrique de $\mathbb{Q}$, soit $C \subset \bar{\mathbb{Q}}$ le sous-corps engendré sur $\mathbb{Q}$ par $\mu_{q-1}(\bar{\mathbb{Q}})$, les racines $(q-1)$-ièmes de l'unité de $\bar{\mathbb{Q}}$. Soit D' l'anneau des entiers de C. Alors si ξ est une racine $(q-1)$-ième primitive de l'unité on a $\mathbb{Z}[\xi] = D' \subset C = \mathbb{Q}(\xi)$. Soit $\mathfrak{p}$ un idéal premier fixé de D' au-dessus de p. Soit D l'anneau obtenu à partir de D' en inversant $(q-1)$ et les idéaux premiers au-dessus de p différents de $\mathfrak{p}$. Dans la suite de cette section S sera un schéma sur D. Sauf mention explicite du contraire, les schémas en groupes sur S considérés seront tous abéliens.

2.1.2.

DÉFINITION 2.1. — Un foncteur $(\mathbf{Sch}/S)^\circ \to (\mathbf{Vect}/\mathbb{F})$ de la catégorie des schémas sur S vers la catégorie des $\mathbb{F}$-espaces vectoriels sera appelé *schéma en $\mathbb{F}$-vectoriels* s'il est représentable par un schéma fini, localement libre et de présentation finie[2]. C'est donc un schéma en groupes abéliens muni d'une action de $\mathbb{F}$.

Soit G un schéma en $\mathbb{F}$-vectoriels. Comme G est fini sur S, il est relativement affine sur S i.e. il existe un $\mathscr{O}_S$-module $\mathscr{A}$ tel que $G = \mathrm{Spec}_S \mathscr{A}$. De plus, $\mathscr{A}$ est une $\mathscr{O}_S$-algèbre de Hopf qui est munie d'une co-action de $\mathbb{F}$. Notons :

- $\mu\colon \mathscr{A} \otimes_S \mathscr{A} \to \mathscr{A}$ la multiplication,
- $\Delta\colon \mathscr{A} \to \mathscr{A} \otimes_S \mathscr{A}$ la comultiplication,
- $\mathscr{I}$ l'idéal d'augmentation de $\mathscr{A}$, qui est le noyau de la co-unité,
- $[\lambda]\colon \mathscr{A} \to \mathscr{A}$ pour tout $\lambda \in \mathbb{F}$ la co-action de $\mathbb{F}$. Pour tout $\lambda, \lambda' \in \mathbb{F}$ on a les relations

$$[\lambda][\lambda'] = [\lambda\lambda'] \text{ et } [\lambda + \lambda'] = \mu \circ ([\lambda] \otimes [\lambda']) \circ \Delta. \tag{3}$$

Pour $n \geqslant 2$ un entier, la co-associativité (resp. l'associativité) permet de définir la n-ième itération de Δ (resp. μ) comme étant une application $\Delta_n : \mathscr{A} \otimes_S \cdots \otimes_S \mathscr{A} \to \mathscr{A}$ (resp. $\mu_n : \mathscr{A} \to \mathscr{A} \otimes_S \cdots \otimes_S \mathscr{A}$) où $\mathscr{A}$ apparaît n fois.

La proposition suivante est immédiate :

PROPOSITION 2.2. — *Tout schéma en $\mathbb{F}$-vectoriels est annulé par p et est localement de rang une puissance de p.* □

Rappelons que par [1, Théorème 2.4.2 exp. VII_B], si S est le spectre d'un corps, la catégorie des schémas en groupes finis sur S est une catégorie abélienne, il en est donc de même pour la catégorie des schémas en $\mathbb{F}$-vectoriels sur S. De plus, pour un schéma S sur D quelconque la catégorie des schémas en groupes finis localement libres n'est pas abélienne mais elle s'identifie à une sous-catégorie exacte (au sens de Quillen) de la catégorie des faisceaux fppf sur S (cf. [1, Exposé V]. Ainsi, dans ce contexte, on peut parler de suite exacte et

2. Cette condition est automatique si on suppose S localement noetherien.

de foncteur exact. Ces considérations s'appliquent donc aussi à la catégorie des schémas en $\mathbb{F}$-vectoriels sur S.

2.1.3. Supposons dans ce paragraphe que $S = \operatorname{Spec} R$ où R est une D-algèbre. On sait que la catégorie des schémas en groupes finis localement libres et de présentation finie sur S est équivalente à la catégorie des R-algèbres de Hopf finies localement libres et de présentation finie, commutatives et co-commutatives. Les relations 3 nous indiquent alors que se donner un schéma en $\mathbb{F}$-vectoriels G sur S est équivalent à se donner une R-algèbre de Hopf A et un morphisme d'anneaux commutatifs $\iota\colon \mathbb{F} \to \operatorname{End}(A)$. Rappelons que $\operatorname{End}(A)$ est l'anneau des endomorphismes de l'algèbre de Hopf A où l'addition est donnée par la convolution

$$\forall f, g \in \operatorname{End}(A),\ f + g = \mu \circ (f \otimes g) \circ \Delta,$$

et le produit est le produit usuel. On obtient ainsi une équivalence de catégories :

PROPOSITION 2.3. — *Supposons que $S = \operatorname{Spec} R$ pour R une D-algèbre. Le foncteur qui à G, un schéma en $\mathbb{F}$-vectoriels, associe la paire (A, ι) induit une équivalence de catégories*

$$\{G \text{ schéma en } \mathbb{F}\text{-vectoriels sur } S\} \leftrightarrow \left\{ \begin{array}{c} (A,\iota),\ A \text{ une } R\text{-Algèbre de Hopf} \\ \text{finie localement libre, commuta-} \\ \text{tive et co-commutative, de pré-} \\ \text{sentation finie, } \iota\colon \mathbb{F} \to \operatorname{End}(A), \\ \text{morphisme d'anneaux.} \end{array} \right\}.$$

REMARQUE 2.4. — Pour S un schéma quelconque sur D, on obtient sans peine une version faisceautique du théorème précédent : se donner un schéma en $\mathbb{F}$-vectoriels G sur S est équivalent à se donner une $\mathscr{O}_S$-algèbre $\mathscr{A}$, avec les mêmes conditions de finitudes, munie d'un morphisme de faisceaux d'anneaux $\mathbb{F} \to \operatorname{End}(\mathscr{A}) = \operatorname{End}(G)$.

2.1.4. Soit $\mathbb{F}^\vee = \operatorname{Hom}(\mathbb{F}^\times, \mu_{q-1}(D))$ les caractères multiplicatifs de $\mathbb{F}^\times$. Notons que comme l'ordre de $\mathbb{F}^\times$ est $(q-1)$, qui est inversible dans D par construction, $\mathbb{F}^\vee$ est l'ensemble des représentations linéaires de $\mathbb{F}^\times$ à coefficients dans D. En particulier,

$$D[\mathbb{F}^\times] = \prod_{\chi \in \mathbb{F}^\vee} D_\chi,$$

où D_χ est la représentation de $\mathbb{F}^\times$ sur D de rang 1 associée à $\chi \in \mathbb{F}^\vee$. Pour tout $\chi \in \mathbb{F}^\vee$ on note $p_\chi\colon D[\mathbb{F}^\times] \to D_\chi$ le projecteur associé à cette décomposition.

Soit G un schéma en $\mathbb{F}$-vectoriels et $\mathscr{A}$ la $\mathscr{O}_S$-algèbre de Hopf associée. Alors $\mathscr{A}$ est en particulier un faisceau de représentations de $\mathbb{F}^\times$, i.e., par le morphisme

structural $D \to \mathscr{O}_S$, un faisceau en $D[\mathbb{F}^\times]$-modules. Ainsi, par ce qui précède

$$\mathscr{A} = \bigoplus_{\chi \in \mathbb{F}^\vee} \mathscr{A}_\chi,\ \mathscr{A}_\chi = p_\chi(\mathscr{A}).$$

Il est de plus clair que cette décomposition est une graduation de $\mathscr{O}_S$-algèbre de Hopf, i.e. elle est compatible au produit et au co-produit. On a montré la proposition suivante :

PROPOSITION 2.5. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur S, alors sa $\mathscr{O}_S$-algèbre de Hopf $\mathscr{A}$ est munie d'une $\mathbb{F}^\vee$-graduation de $\mathscr{O}_S$-algèbre de Hopf qui détermine la co-action de $\mathbb{F}$.* □

REMARQUE 2.6. — Notons que comme $\mathbb{F}^\times$ agit trivialement sur $\mathscr{O}_S$, la graduation sur le noyau de la co-unité $\mathscr{A} \to \mathscr{O}_S$ est induite par la graduation sur $\mathscr{A}$. Ainsi la graduation de l'idéal d'augmentation est de la forme

$$\mathscr{I} = \bigoplus_{\chi \in \mathbb{F}^\vee} \mathscr{I}_\chi,\ \mathscr{I} = p_\chi(\mathscr{I}).$$

C'est la graduation considérée dans [9].

2.1.5. Soit G un schéma en $\mathbb{F}$-vectoriels sur S et $\mathscr{A}$ sa $\mathscr{O}_S$-algèbre de Hopf graduée associée. On suppose pour simplifier les notations que S soit connexe ; on va s'intéresser au rang des $\mathscr{A}_\chi$ que l'on notera $\mathrm{rang}_S(\mathscr{A}_\chi)$.

DÉFINITION 2.7. — On conserve les notations et hypothèses précédentes. On définit *le caractère de G* par

$$\mathrm{Ch}_S(G) = \sum_{\chi \in \mathbb{F}^\vee} \mathrm{rang}_S(\mathscr{A}_\chi)[\chi] \in \mathbb{N}[\mathbb{F}^\vee].$$

Cette définition a toujours un sens si G est un schéma en groupe fini et plat muni d'une action de $\mathbb{F}^\times$. On remarque que le caractère est invariant par changement de base : pour $S' \to S$ un morphisme on a

$$\mathrm{Ch}_S(G) = \mathrm{Ch}_{S'}(G \otimes_S S').$$

Notons de même que pour tout $\chi \in \mathbb{F}^\vee$ la fonction de rang

$$s \in S \mapsto \dim_{\kappa(s)}(\mathscr{A}_\chi \otimes_S \kappa(s)),$$

où $\kappa(s)$ est le corps résiduel en $s \in S$, est constante sur S égale au rang de $\mathscr{A}_\chi$ comme $\mathscr{O}_S$-module. Ainsi pour tout point géométrique $\mathrm{Spec}(k) \to S$ on a

$$\mathrm{Ch}_S(G) = \mathrm{Ch}_k(G \otimes_S k).$$

Ceci nous permettra de restreindre le calcul du caractère au cas où S est le spectre d'un corps parfait.

2.1.6. Soit G un schéma en $\mathbb{F}$-vectoriels sur S. Soit $G^D = \mathscr{H}\mathrm{om}(G, \mathbb{G}_m)$ le dual de Cartier du schéma en groupe fini et plat sous-jacent. Alors comme $\mathbb{F}^\times$ est commutatif, G^D est muni d'une action de $\mathbb{F}^\times$ définie par :

$$\forall f \in G^D, \lambda \in \mathbb{F}, x \in G,\ (\lambda f)(x) = f(\lambda x)$$

De plus, il est clair que cette action définit naturellement une structure de $\mathbb{F}$-vectoriels sur G. On a

$$\mathrm{Ch}_S(G) = \mathrm{Ch}_S(G^D).$$

Il est important de noter que ceci est faux si on munit G^D de l'action contragrédiente de $\mathbb{F}^\times$.

2.2. Cristaux de Dieudonné gradués. —

2.2.1.

Définition 2.8. — Soit $\chi \in \mathbb{F}^\vee$. On dit que χ est *primitif* s'il est additif. On note $\mathbb{F}^+ \subset \mathbb{F}^\vee$ l'ensemble des caractères primitifs de $\mathbb{F}^\vee$.

Remarque 2.9. —
- On a un isomorphisme d'anneau $D' \cong \mathbb{Z}[\mathbb{F}^\vee]$ qui identifie les racines primitives de l'unité aux caractères primitifs. C'est pourquoi on préfère cette terminologie à celle de « fondamental » dans [9].
- Si χ un caractère primitif, alors χ^p est primitif et ainsi on obtient $\mathbb{F}^+ = \{\chi, \chi^p, \chi^{p^2}, \dots, \chi^{p^{r-1}}\}$. On a de plus un isomorphisme[3] non-canonique $\mathbb{F}^+ \cong \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$, plus précisément, $\mathbb{F}^+$ est un espace principal homogène sous $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$.

On fixe un caractère primitif $\chi_1 \in \mathbb{F}^+$ et on note $\chi_i = \chi_1^{p^{i-1}}$ pour tout entier $i \in [\![1, r]\!]$. Tout caractère non-trivial $\chi \in \mathbb{F}^\vee$ a un unique développement p-adique de la forme

$$\chi = \prod_{i=1}^{r} \chi_i^{a_i}, \text{tel que } a_i \in [\![0, p-1]\!], \text{ pour tout } i \in [\![1, r]\!].$$

Le caractère trivial χ_0 s'écrit de deux manières différentes : on a $\chi_0 = \prod_{i=0}^{p-1} \chi_i^{p-1} = \chi_1^0$.

2.2.2. On introduit quelques notations dans ce paragraphe, suivant principalement [2]. Soit $\Sigma = \mathrm{Spec}\, \mathrm{W}(\mathbb{F})$, c'est un schéma sur D. Supposons que S est un schéma sur Σ tel que p est (Zariski)-localement nilpotent sur S. On note $\sigma\colon \mathrm{W}(\mathbb{F}) \to \mathrm{W}(\mathbb{F})$ l'automorphisme de Frobenius. On considère la catégorie

3. Les isomorphismes sont donnés par les identifications $\mathbb{F}^\times \cong \mu_{q-1}(D) \subset C$.

cristalline $\mathrm{CRIS}(S/\Sigma)$ munie de la topologie fppf. Soit G un schéma en groupes fini et localement libre sur S, alors on définit un préfaisceau sur $\mathrm{CRIS}(S/\Sigma)$ en posant

$$\underline{G}(U,T,\delta) = \mathrm{Hom}(U,G),$$

pour tout objet (U,T,δ) de $\mathrm{CRIS}(S/\Sigma)$. Le préfaisceau $\underline{G}$ est en effet un faisceau fppf (cf. [2, Corollaire 1.1.8]). Soit $\mathscr{O}_{S/\Sigma}$ le faisceau structural usuel sur le site $\mathrm{CRIS}(S/\Sigma)$. On considère le *cristal de Dieudonné (covariant)* de G,

$$\mathbb{D}(G) = \mathscr{E}\mathrm{xt}^1_{S/\Sigma}(\underline{G^D}, \mathscr{O}_{S/\Sigma})^{(\sigma^{-1})},$$

qui est un cristal en $\mathscr{O}_{S/\Sigma}$-modules localement de présentation finie (cf. [2, Corollaire 3.1.3]). Notons qu'on change G par G^D par rapport à la définition de [2] pour avoir un foncteur covariant, et que l'on tord l'action de $\mathrm{W}(\mathbb{F})$ par σ^{-1}. Cette dernière modification nous évitera d'introduire des décalages dans la suite. La dualité de Cartier $G \rightsquigarrow G^D = \mathscr{H}\mathrm{om}_S(G, \mathbb{G}_m)$ est une anti-équivalence exacte des schémas en groupes finis et localement libres sur S, donc cette modification est innocente pour l'application des résultats de [2] dans la suite.

Si G est annulé par p, de rang constant p^d, par exemple si G un schéma en $\mathbb{F}$-vectoriels sur une base S connexe, alors $\mathbb{D}(G)$ est un $\mathscr{O}_{S/\Sigma}/p\mathscr{O}_{S/\Sigma}$-module localement libre de rang fini d (cf. [2, Proposition 4.3.1]) et de plus le foncteur $G \rightsquigarrow \mathbb{D}(G)$ restreint à la catégorie des schémas en $\mathbb{F}$-vectoriels est exact.

2.2.3. Supposons que G est un schéma en $\mathbb{F}$-vectoriels sur S. Alors l'action de $\mathbb{F}^\times$ induit une structure de $\mathscr{O}_{S/\Sigma}$-module $\mathbb{F}^\times$-équivariant sur $\mathbb{D}(G)$, ou de manière équivalente, une graduation de type $\mathbb{F}^\vee$ sur $\mathbb{D}(G)$. Plus précisément, par la fonctorialité de $\mathbb{D}$ l'endomorphisme

$$[\lambda]\colon G \to G,$$

pour $\lambda \in \mathbb{F}^\vee$, induit un morphisme $\lambda\cdot\colon \mathbb{D}(G) \to \mathbb{D}(G)$. De même pour tout $\chi \in \mathbb{F}^\vee$, on peut définir un endomorphisme idempotent $p_\chi\cdot\colon \mathbb{D}(G) \to \mathbb{D}(G)$. On a la proposition suivante :

Proposition 2.10. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur S. Alors*

$$\mathbb{D}(G) = \bigoplus_{\chi\in\mathbb{F}^+} \mathbb{D}(G)_\chi, \quad \textit{où} \quad \mathbb{D}(G)_\chi = p_\chi \cdot \mathbb{D}(G).$$

Ainsi, $\mathbb{D}$ est un foncteur de la catégorie des schémas en $\mathbb{F}$-vectoriels sur S dans la catégorie des $\mathscr{O}_{S/\Sigma}/p\mathscr{O}_{S/\Sigma}$-modules localement libres gradués sur $\mathbb{F}^+$.

Démonstration. — Par ce qui précède, on a

$$\mathbb{D}(G) = \bigoplus_{\chi\in\mathbb{F}^\vee} \mathbb{D}(G)_\chi, \quad \text{où} \quad \mathbb{D}(G)_\chi = p_\chi \cdot \mathbb{D}(G).$$

Il suffit de montrer que pour $\chi \in \mathbb{F}^\vee\backslash\mathbb{F}^+$, $p_\chi \cdot \mathbb{D}(G) = 0$. Or, le foncteur $\mathbb{D}$ est additif et donc on obtient un morphisme d'anneaux

$$\mathrm{End}(G) \to \mathrm{End}(\mathbb{D}(G)).$$

Soit $\lambda, \lambda' \in \mathbb{F}$. Comme le morphisme ci-dessus associe $\lambda\cdot$ à $[\lambda]$ et comme il respecte l'addition, on a

$$(\lambda + \lambda')\cdot = \lambda\cdot + \lambda'\cdot.$$

Si $\chi \in \mathbb{F}^\vee$ alors $\lambda\cdot\colon \mathbb{D}(G)_\chi \to \mathbb{D}(G)_\chi$ équivaut à la multiplication par $\chi(\lambda)$. Ainsi, si $\mathbb{D}(G)_\chi$ est non-nul, $\chi(\lambda + \lambda') = \chi(\lambda) + \chi(\lambda')$, et donc $\chi \in \mathbb{F}^+$.

Rappelons que comme G est annulé par p (cf. 2.2), $\mathbb{D}(G)$ est bien localement libre d'après [2, Proposition 4.3.1 (i)]. □

On pose $S_\mathbb{F} = S \otimes_{\mathbb{Z}_p} \mathrm{W}(\mathbb{F})$. C'est naturellement un schéma sur

$$\mathrm{W}(\mathbb{F}) \otimes_{\mathbb{Z}_p} \mathrm{W}(\mathbb{F}) = \prod_{\chi\in\mathbb{F}^+} \mathrm{W}(\mathbb{F})_\chi,$$

donc, comme S est un schéma sur $\mathrm{W}(\mathbb{F})$, on obtient

$$S_\mathbb{F} = \bigsqcup_{\chi\in\mathbb{F}^+} S_\chi \text{ où } S_\chi = S \otimes_{\mathrm{W}(\mathbb{F})} \mathrm{W}(\mathbb{F})_\chi.$$

Ainsi,

$$\mathscr{O}_{S_\mathbb{F}/\Sigma} = \bigoplus_{\chi\in\mathbb{F}^+} (\mathscr{O}_{S/\Sigma})_\chi.$$

La proposition précédente peut alors s'énoncer de la manière suivante :

Corollaire 2.11. — *Le foncteur $\mathbb{D}$ induit un foncteur exact de la catégorie des schémas en $\mathbb{F}$-vectoriels dans la catégorie des cristaux en $\mathscr{O}_{S_\mathbb{F}/\Sigma}/p\mathscr{O}_{S_\mathbb{F}/\Sigma}$-modules localements libres de rang fini et de présentation finie.* □

Remarque 2.12. — Ce foncteur pour les schémas en $\mathbb{F}$-vectoriels possède les mêmes propriétés que le foncteur sous-jacent pour les schémas en groupes finis et localement libres, i.e pour certaines restrictions sur S il est fidèle, pleinement fidèle ou une équivalence de catégories[4].

4. Par exemple si S est de caractéristique p, localement noetherien d'anneaux locaux à intersection complète, $\mathbb{D}$ est fidèle [6] et si S est le spectre d'un corps parfait c'est une équivalence comme on le rappellera.

Supposons S connexe et fixons G un schéma en $\mathbb{F}$-vectoriels sur S. Alors comme $\mathbb{D}(G)$ est localement libre sur $\mathscr{O}_{S/\Sigma}/p\mathscr{O}_{S/\Sigma}$, on peut définir $\mathrm{rang}_{\mathscr{O}_{S/\Sigma}/p\mathscr{O}_{S/\Sigma}}(\mathbb{D}(G)_\chi)$, le rang de la composante χ-isotypique, pour tout $\chi \in \mathbb{F}^+$.

Définition 2.13. — Soit $\mathscr{F}$ un $\mathscr{O}_{S_{\mathbb{F}}/\Sigma}/p\mathscr{O}_{S_{\mathbb{F}}\Sigma}$-module localement libre de rang fini. On définit le *caractère* de $\mathscr{F}$ par

$$\mathfrak{ch}_S(\mathscr{F}) = \sum_{\chi\in\mathbb{F}^+} \mathrm{rang}_{\mathscr{O}_{S/\Sigma}/p\mathscr{O}_\Sigma}(\mathscr{F}_\chi)[\chi] \in \mathbb{N}[\mathbb{F}^+].$$

On considèrera en particulier $\mathfrak{ch}_S(\mathbb{D}(G))$.

2.2.4. Dans ce paragraphe on suppose que $S = \mathrm{Spec}(k)$ pour k un corps parfait de caractéristique p contenant $\mathbb{F}$. Soit G un schéma en groupes fini et localement libre sur S. On pose

$$D(G) = \Gamma(S/\Sigma, \mathbb{D}(G)).$$

C'est un $\mathrm{W}(k)$-module de longueur finie (cf. [2, Proposition 4.2.10]) muni de deux morphismes $F\colon D(G) \to D(G)^{(\sigma)}$ et $V\colon D(G)^{(\sigma)} \to D(G)$ tels que $FV = VF = p$. C'est le dual du module de Dieudonné de G au sens de [5, Chapitre IV] d'après [2, Théorème 4.2.14], i.e. c'est le module de Dieudonné covariant de G. On sait que D établit une équivalence entre la catégorie des schémas en groupes finis et les modules de Dieudonné sur $\mathrm{W}(k)$ (cf. [5, IV 1.3]).

Si G est un schéma en $\mathbb{F}$-vectoriel alors d'après le corollaire 2.11, $D(G)$ est naturellement un module de Dieudonné gradué sur $\mathbb{F}^+$ au sens suivant :

Définition 2.14. — Soit M un $W(k)$ module muni de deux morphismes $F\colon M \to M^{(\sigma)}$ et $V\colon M^{(\sigma)} \to M$ tels que $FV = VF = 0$. On dit que M est un *module de Dieudonné gradué* sur $\mathbb{F}^+$ si on a de plus une graduation

$$M = \bigoplus_{\chi\in\mathbb{F}^+} M_\chi$$

telle que F et V se restreignent en

$$F\colon M_\chi \to M_{\chi^p},\ V\colon M_{\chi^p} \to M_\chi,$$

pour tout $\chi \in \mathbb{F}^+$.

Ainsi l'équivalence de catégories pour les schémas en groupes finis et localement libres nous donne la caractérisation suivante :

Proposition 2.15. — *Le foncteur D induit une équivalence de catégories*

$$\{\textit{Schémas en } \mathbb{F}\textit{-vectoriels sur } k\} \leftrightarrow \left\{ \begin{array}{c} \mathrm{W}(k)\textit{-modules de Dieudonné} \\ \textit{de longueur finie gradués sur } \mathbb{F}^+ \end{array} \right\}.$$

□

2.2.5. Soit M un $\mathrm{W}(k)$-module de Dieudonné gradué sur $\mathbb{F}^+$. De même que dans la définition 2.13, on peut définir le caractère de M :

$$\mathfrak{ch}_k(M) = \sum_{\chi\in\mathbb{F}^+} \dim_k(M_\chi)[\chi] \in \mathbb{N}[\mathbb{F}^+].$$

Soit à nouveau S un schéma connexe sur Σ tel que p est localement nilpotent sur S. Soit $s\colon \mathrm{Spec}(k) \to S$ un point géométrique. Soit G un schéma en $\mathbb{F}$-vectoriels sur S, alors comme $\mathbb{D}(G)$ est un cristal et qu'il est compatible aux changements de base, on a pour tout élément (U,T,δ) de $\mathrm{CRIS}(S/\Sigma)$ un isomorphisme

$$D(G_k) \cong \mathbb{D}(G_k)_{\mathrm{Spec}\, k} \cong \mathbb{D}(G)_{(U,T,\delta)} \otimes_{\mathscr{O}_T} k.$$

Ainsi, comme $\mathbb{D}(G)$ est un $\mathscr{O}_{S/\Sigma}/p\mathscr{O}_{S/\Sigma}$ module libre de rang fini, on a

$$\mathfrak{ch}_S(\mathbb{D}(G)) = \mathfrak{ch}_k(D(G_k)).$$

Ceci nous permettra de ramener le calcul du caractère sur une base générale au calcul du caractère sur un corps parfait. Le cristal de Dieudonné ne se comporte pas très bien par rapport à la dualité de Cartier. Néanmoins, la description précédente nous donne le résultat suivant :

Lemme 2.16. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur S connexe. Alors*

$$\mathfrak{ch}_S(\mathbb{D}(G)) = \mathfrak{ch}_S(\mathbb{D}(G^D)).$$

Démonstration. — D'après ce qui précède, on peut supposer que $S = \mathrm{Spec}(k)$ où k est un corps parfait de caractéristique p. On pose $\mathrm{W}_\infty = \mathrm{W}(k)[\frac{1}{p}]/\mathrm{W}(k)$ le module dualisant et on définit pour tout $\mathrm{W}(k)$-module de Dieudonné gradué sur $\mathbb{F}^+$, le $\mathrm{W}(k)$-module

$$M^* = \mathrm{Hom}_{\mathrm{W}(k)}(M, \mathrm{W}_\infty).$$

Comme dans le cas des schémas en $\mathbb{F}$-vectoriels, M^* est naturellement muni d'une structure de $\mathrm{W}(k)$-module gradué[5] et $\mathfrak{ch}_k(M) = \mathfrak{ch}_k(M^*)$. Or, d'après [5, Chapitre IV, §5, Corollaire 2], on a un isomorphisme fonctoriel en G, $D(G^D) \cong D(G)^*$. D'où le résultat. □

5. Encore une fois l'action de $\mathbb{F}^\times$ sur M n'est pas l'action contragrédiente, qui ne définit pas une graduation sur $\mathbb{F}^+$, mais l'action de l'opposé de $\mathbb{F}^\times$ qui lui est égale par commutativité.

3. Formule des caractères et $\mathbb{F}$-exponentielle

Dans cette section on démontre la formule des caractères. On commence par définir la $\mathbb{F}$-exponentielle.

DÉFINITION 3.1. — On appelle $\mathbb{F}$-*exponentielle* l'application multiplicative $\exp_{\mathbb{F}}\colon \mathbb{N}[\mathbb{F}^+] \to \mathbb{N}[\mathbb{F}^\vee]$ définie pour $f = \sum_{\chi\in\mathbb{F}^+} n_\chi[\chi] \in \mathbb{N}[\mathbb{F}^+]$ par

$$\exp_{\mathbb{F}}(f) = \prod_{\chi\in\mathbb{F}^+} (1 + [\chi] + [\chi^2] + \cdots + [\chi^{p-1}])^{n_\chi}.$$

Par *multiplicatif* on entend que $\exp_{\mathbb{F}}(f+g) = \exp_{\mathbb{F}}(f)\exp_{\mathbb{F}}(g)$ pour tout $f, g \in \mathbb{N}[\mathbb{F}^+]$. Le but est de démontrer le théorème suivant :

THÉORÈME 3.2. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur un $\mathrm{W}(\mathbb{F})$-schéma connexe S tel que p est localement nilpotent sur S. Alors*

$$\mathrm{Ch}_S(G) = \exp_{\mathbb{F}}(\mathfrak{ch}_S(\mathbb{D}(G))).$$

D'après ce qu'on a expliqué au paragraphe 2.2.5, ce théorème est équivalent au théorème suivant :

THÉORÈME 3.3. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur un corps parfait k de caractéristique p tel que $\mathbb{F} \subset k$. Alors*

$$\mathrm{Ch}_k(G) = \exp_{\mathbb{F}}(\mathfrak{ch}_k(D(G))).$$

Dans toute cette section on suppose que G est un schéma en $\mathbb{F}$-vectoriels sur un corps parfait k de caractéristique p tel que $\mathbb{F} \subset k$. On notera toujours $\sigma\colon k \to k$ l'automorphisme de Frobenius.

3.1. Multiplicativité du caractère. —

3.1.1. Le caractère des modules de Dieudonné gradués sur $\mathbb{F}^+$ est additif, plus précisément, on a directement :

LEMME 3.4. — *Soit*

$$0 \to M' \to M \to M'' \to 0$$

une suite exacte de $\mathrm{W}(k)$-modules de Dieudonné gradués sur $\mathbb{F}^+$, en particulier les morphismes sont gradués. Alors

$$\mathfrak{ch}_k(M) = \mathfrak{ch}_k(M') + \mathfrak{ch}_k(M'').$$ □

Ainsi, d'après le théorème 3.3, on devrait obtenir que Ch_k est multiplicatif. La démonstration du théorème 3.3 repose sur ce fait ; on montre donc dans cette partie la proposition suivante :

Proposition 3.5. — *Soit*

$$0 \to G' \to G \to G'' \to 0$$

une suite exact de schémas en $\mathbb{F}$-vectoriels[6]*. Alors*

$$\mathrm{Ch}_k(G) = \mathrm{Ch}_k(G')\,\mathrm{Ch}_k(G'').$$

3.1.2. Soit G un schéma en $\mathbb{F}$-vectoriels sur k et A son algèbre de Hopf. On suppose que G est connexe, c'est-à-dire que A est une k-algèbre artinienne locale. Rappelons qu'on a une graduation

$$A = \bigoplus_{\chi \in \mathbb{F}^\vee} A_\chi.$$

Définition 3.6. — Soit M un A-module. Supposons que M est gradué sur $\mathbb{F}^\vee$. Alors on dira que M est un *A-module gradué* si pour tout $\chi, \chi' \in \mathbb{F}^\vee$ on a $A_\chi \cdot M_{\chi'} \subset M_{\chi\chi'}$. On dira de plus qu'un élément de M est *homogène* de type $\chi \in \mathbb{F}^\vee$ s'il appartient à M_χ.

Exemple 3.7. — Pour $\chi \in \mathbb{F}^\vee$, on note $A(\chi)$ le A-module libre de rang 1 muni d'une graduation sur $\mathbb{F}^\vee$ telle que pour tout $\mu \in \mathbb{F}^\vee$ on ait $A(\chi)_\mu = A_{\chi^{-1}\mu}$. C'est un A-module gradué. On peut définir de même $M(\chi)$ pour tout A-module gradué M. En particulier, on a les $k(\chi)$ où k est muni de la graduation triviale.

Proposition 3.8. — *Soit M un A-module gradué et libre de rang d sur A. Alors on a une décomposition*

$$M = \bigoplus_{\chi \in \mathbb{F}^\vee} A(\chi)^{d_\chi},$$

telle que $\sum_{\chi \in \mathbb{F}^\vee} d_\chi = d$.

Démonstration. — Il suffit de montrer qu'il existe une A-base de M, constituée d'éléments homogènes. On considère le produit tensoriel $M_k = M \otimes_A k$ pour la co-unité $A \to k$; c'est un k-module gradué sur $\mathbb{F}^\vee$,

$$M_k = \bigoplus_{\chi \in \mathbb{F}^\vee} k(\chi)^{d_\chi}.$$

De plus, $M \to M_k$ est surjectif et respecte la graduation car $k \subset A_{\chi_0}$, c'est-à-dire que $M_\chi \to k(\chi)^{d_\chi} \subset M_k$ est surjectif pour tout $\chi \in \mathbb{F}^\vee$. Ainsi, pour tout $\chi \in \mathbb{F}^\vee$ on peut fixer un ensemble à d_χ éléments homogènes $\mathfrak{B}_\chi \subset M_\chi$ tels que leurs images dans M_k forment une k-base de $k(\chi)^{d_\chi}$. On pose $\mathfrak{B} = \bigcup \mathfrak{B}_\chi$, c'est un ensemble à d éléments que nous notons $v_1, \ldots, v_d$. Par le lemme de

6. Notez que les morphismes de schémas en $\mathbb{F}$-vectoriels sont des morphismes de schémas en groupes qui respectent l'action de $\mathbb{F}$.

Nakayama, $\mathfrak{B}$ est une famille génératrice de M en tant que A-module. On a donc une surjection de A-modules

$$A^d \to M$$
$$(x_1, \dots, x_d) \mapsto \sum_{i=1}^{d} x_i \cdot v_i.$$

Or, c'est une surjection entre k-espaces vectoriels de même dimension et donc c'est un isomorphisme de A-modules. Ce qui montre que $\mathfrak{B}$ est une A-base homogène de M. □

3.1.3. On déduit de la proposition précédente une formule pour les dimensions des composantes isotypiques.

COROLLAIRE 3.9. — *On conserve les notations et hypothèses de la proposition 3.8. On a alors*

$$\dim_k(M_\chi) = \sum_{\mu\mu'=\chi} d_\mu \dim_k(A_{\mu'}),$$

où la somme porte sur les $\mu, \mu' \in \mathbb{F}^\vee$ tels que $\mu\mu' = \chi$. □

Soit G_1, G_2 deux schémas en $\mathbb{F}$-vectoriels sur k tels que G_1 soit connexe. Soit A_1, A_2 leurs algèbres de Hopf respectives. Supposons que l'on a une une surjection $G_2 \to G_1 \to 0$, alors d'après [1, Exposé VII$_B$ 2.4] ce morphisme est plat. Ainsi G_2 est localement libre sur G_1 car G_1 est noetherien. Or, A_1 est Artinien donc A_2 est libre sur A_1 et on peut appliquer la proposition précédente, qui donne une décomposition

$$A_2 = \bigoplus_{\chi \in \mathbb{F}^\vee} A_1(\chi)^{d_\chi}. \tag{4}$$

PROPOSITION 3.10. — *Soit $0 \to G_1 \to G_2 \to G_3 \to 0$ une suite exacte de schémas en $\mathbb{F}$-vectoriels. Supposons que G_3 soit connexe. Alors*

$$\mathrm{Ch}_k(G_2) = \mathrm{Ch}_k(G_1)\,\mathrm{Ch}_k(G_3).$$

Démonstration. — Soit A_i la k-algèbre de Hopf associée à G_i, pour $i \in \{1, 2, 3\}$. D'après ce qui précède, on a la décomposition (4). Or $G_1 = G_2 \times_{G_3} \operatorname{Spec} k$, pour le morphisme unité $\operatorname{Spec} k \to G_3$, donc

$$A_1 = \bigoplus_{\chi \in \mathbb{F}^\vee} k(\chi)^{d_\chi},$$

en particulier $d_\mu = \dim_k(A_{3,\mu})$ pour tout $\mu \in \mathbb{F}^\vee$. Par le corollaire 3.9 on a pour tout $\chi \in \mathbb{F}^\vee$ la relation

$$\dim_k(A_{2,\chi}) = \sum_{\mu\mu'=\chi} \dim_k(A_{3,\mu}) \dim_k(A_{1,\mu'}),$$

ce qui prouve la proposition. □

3.1.4. On est maintenant en mesure de conclure l'argument pour montrer la proposition 3.5, i.e. d'enlever dans la proposition précédente l'hypothèse que G_3 soit connexe. Soit

$$0 \to G' \to G \to G'' \to 0$$

une suite exacte de schémas en $\mathbb{F}$-vectoriels étales sur k. Comme la dualité de Cartier est exacte pour les schémas en groupes finis sur k et comme le dual d'un schéma en groupes fini étale est connexe, on obtient une suite exacte de schémas en groupes connexes

$$0 \to G''^D \to G^D \to G'^D \to 0.$$

Donc, d'après la proposition 3.10 et le lemme 2.16, on obtient

$$\mathrm{Ch}_k(G) = \mathrm{Ch}_k(G^D) = \mathrm{Ch}_k(G''^D)\mathrm{Ch}_k(G'^D) = \mathrm{Ch}_k(G'')\mathrm{Ch}_k(G').$$

Ainsi, le caractère Ch_k est multiplicatif sur les schémas en $\mathbb{F}$-vectoriels étales.

Soit G un schéma en $\mathbb{F}$-vectoriels. Alors, en tant que schéma en groupes fini, comme k est parfait, on a $G \cong G^\circ \times_k G^{\text{ét}}$ où G° est connexe et $G^{\text{ét}}$ est étale. Or, comme cette décomposition est fonctorielle, G° et $G^{\text{ét}}$ sont naturellement des schémas en $\mathbb{F}$-vectoriels. La décomposition nous donne une surjection non canonique $G \to G^\circ$ et on déduit que

$$\mathrm{Ch}_k(G) = \mathrm{Ch}_k(G^\circ)\mathrm{Ch}_k(G^{\text{ét}}).$$

Comme Ch_k est multiplicatif sur les schémas en $\mathbb{F}$-vectoriels étales et sur les schémas en $\mathbb{F}$-vectoriels connexes, on en déduit que Ch_k est multiplicatif, ce qui termine la démonstration de la proposition 3.5. □

3.2. Formule des caractères. — Dans cette partie on démontre le théorème 3.3. On commencera par le démontrer dans le cas où G est de type additif, puis par un dévissage et un argument de dualité, on le montrera en toute généralité.

3.2.1. On commence par rappeler la classification des schémas en groupes finis sur k de type additif (i.e. annulés par V). Soit M un k-espace vectoriel de dimension finie. On peut lui associer un schéma en groupes sur k, annulé par V, en posant pour tout schéma affine $U = \operatorname{Spec} B$ sur k,

$$M \otimes \mathbb{G}_a(U) = M \otimes_k B,$$

où la structure de groupe est déterminée par le groupe additif sous-jacent à l'anneau B. Notons que le Frobenius F sur $\mathbb{G}_a$ induit un Frobenius, toujours noté F de $M \otimes \mathbb{G}_a$. Si, de plus, M est muni d'un opérateur σ-linéaire $F_M \colon M \to M$, alors $M \otimes \mathbb{G}_a$ est muni d'un second Frobenius que l'on note F_M. Le foncteur des modules de Dieudonné sur $\mathrm{W}(k)$ annulés par V, dans les schémas en groupes finis de type additif, défini par $M \rightsquigarrow \ker(F - F_M)$ est alors une équivalence de catégories abéliennes (cf. [3, IV, §3, 6.6-6.7]). Comme ces constructions sont fonctorielles en M, si M est gradué sur $\mathbb{F}^+$, alors $\ker(F - F_M)$ est naturellement

un schéma en $\mathbb{F}$-vectoriels sur k, puisque les Frobenius introduits respectent la graduation. On en déduit la proposition suivante :

PROPOSITION 3.11. — *L'équivalence de catégories abéliennes*

$$\left\{\begin{array}{c} G \text{ schéma en } \mathbb{F}\text{-vectoriels sur } k, \\ \text{de type additif} \end{array}\right\} \leftrightarrow \left\{\begin{array}{c} \mathrm{W}(k)\text{-modules de Dieudonné} \\ \text{gradués annulés par } V \end{array}\right\}$$

définie par $G \rightsquigarrow D(G)$ a pour quasi-inverse le foncteur

$$M \rightsquigarrow \ker\left[(F - F_M)\colon M \otimes \mathbb{G}_a \to M \otimes \mathbb{G}_a\right]. \qquad \square$$

3.2.2. En utilisant la proposition précédente, on démontre dans ce paragraphe le théorème 3.3 pour G de type additif.

Soit G un schéma en $\mathbb{F}$-vectoriels sur k de type additif, A sa k-algèbre de Hopf et $D(G)$ son module de Dieudonné. Soit $x_1, \ldots, x_n$ une base homogène de $D(G)$ et $\chi_i \in \mathbb{F}^+$ le caractère tel que $x_i \in D(G)_{\chi_i}$. Soit $I = \{1, 2, \ldots, n\}$, on a

$$\mathfrak{ch}_k(D(G)) = \sum_{i \in I} [\chi_i].$$

Il suffit donc de montrer que

$$\mathrm{Ch}_k(G) = \prod_{i \in I} \left(\sum_{k \in \{0,1,\ldots,p-1\}} [\chi_i^k] \right).$$

Soit $V = \{0, \ldots, p-1\}^I$, l'ensemble des fonctions de I à valeurs dans $\{0, \ldots, p-1\}$. Alors, en échangeant la somme et le produit dans la relation précédente, on se ramène à montrer que

$$\mathrm{Ch}_k(G) = \sum_{k \in V} \left[\prod_{i \in I} \chi_i^{k(i)} \right]. \tag{5}$$

D'après la proposition 3.11, il existe $a_{i,j} \in k$, pour tout $i, j \in I = \{1, 2, \ldots, n\}$, tel que

$$A = \frac{k[x_1, \ldots, x_n]}{\langle P_i \rangle_{i \in I}}, \text{ où pour tout } i \in I,\ P_i = x_i^p - \sum_{j \in I} a_{i,j} x_j.$$

Donc la famille $\{x_1^{k(1)} \ldots x_n^{k(n)}\}_{k \in V}$ est une base homogène de A sur k. En particulier, pour $k \in V$ on a $x_1^{k(1)} \ldots x_n^{k(n)} \in A_{\chi_1^{k(1)} \cdots \chi_n^{k(n)}}$. Ceci démontre précisément (5) et finit la démonstration du théorème 3.3 pour G de type additif. $\square$

REMARQUE 3.12. — Comme les schémas en groupes finis étales sont de type additif, ceci montre en particulier le théorème pour G étale.

3.2.3. Dans ce paragraphe on conclut la démonstration du théorème 3.3. On commence par le cas où V est nilpotent et on finit par un argument de dualité.

Soit G un schéma en $\mathbb{F}$-vectoriels sur k tel que V est nilpotent. Soit $M = D(G)$ son $\mathrm{W}(k)$-module de Dieudonné gradué. Si on pose pour tout entier $i \geqslant 0$, $M_i = V^i M$, on obtient une filtration décroissante de M dont les quotients successifs sont annulés par V. Comme V respecte la graduation, c'est une filtration décroissante graduée sur $\mathbb{F}^+$ et elle définit donc une filtration décroissante $\{G_i\}_{i\geqslant 0}$ de sous-schémas fermés en $\mathbb{F}$-vectoriels telle que les quotients successifs sont des schémas en $\mathbb{F}$-vectoriels annulés par V. La multiplicativité de Ch_k et l'additivité de $\mathfrak{ch}_k$ nous donnent donc

$$\mathrm{Ch}_k(G) = \prod_{i\geqslant 0} \mathrm{Ch}(G_i/G_{i+1}), \quad \text{et} \quad \mathfrak{ch}_k(M) = \sum_{i\geqslant 0} \mathfrak{ch}_k(M_i/M_{i+1}).$$

Or, au paragraphe précédent on a montré que pour tout $i \geqslant 0$,

$$\mathrm{Ch}_k(G_i/G_{i+1}) = \exp_{\mathbb{F}}(\mathfrak{ch}_k(M_i/M_{i+1})).$$

Ainsi la multiplicativité de $\exp_{\mathbb{F}}$ nous permet de conclure dans ce cas.

Il reste le cas où V est un isomorphisme. Soit G un schéma en $\mathbb{F}$-vectoriels sur k tel que V est un isomorphisme et soit $D(G)$ son module de Dieudonné. Or, dans ce cas F est nilpotent, ainsi V est nilpotent sur G^D. Or, d'après le paragraphe 2.1.6 on a $\mathrm{Ch}_k(G) = \mathrm{Ch}_k(G^D)$ et d'après le lemme 2.16 on a $\mathfrak{ch}_k(D(G)) = \mathfrak{ch}_k(D(G^D))$. On se ramène ainsi au cas où V est nilpotent, ce qui termine la preuve du théorème. □

4. Application aux modules p-divisibles

Dans cette section on donne une application de la formule des caractères à la structure des points de torsions de certains modules p-divisibles. On utilise pour cela la théorie des schémas de Raynaud et leur structure (cf. [9]). Après avoir rappelé ces résultats, on fera quelques rappels sur les cristaux des groupes p-divisibles et on étudiera les points de torsions des modules p-divisibles.

4.1. Schémas de Raynaud. — Dans cette partie on garde les notations de la première section, en particulier S désignera un schéma sur D. On fixe, de plus, un caractère primitif $\chi_1 \in \mathbb{F}^+$ et on note $\chi_i = \chi_1^{p^i}$ le i-ème caractère primitif.

4.1.1. Soit G un schéma en $\mathbb{F}$-vectoriels sur S. Rappelons qu'on a une décomposition de l'idéal d'augmentation de G de la forme

$$\mathscr{I} = \bigoplus_{\chi\in\mathbb{F}^\vee} \mathscr{I}_\chi \text{ pour } \mathscr{I}_\chi = p_\chi(\mathscr{I}).$$

Pour χ et χ' des caractères primitifs, on peut restreindre la co-multiplication aux sommants de $\mathscr{I}$ et obtenir $\Delta_{\chi,\chi'} : \mathscr{I}_{\chi\chi'} \to \mathscr{I}_\chi \otimes_S \mathscr{I}_{\chi'}$. De même, pour la multiplication on obtient $\mu_{\chi,\chi'} : \mathscr{I}_\chi \otimes_S \mathscr{I}_{\chi'} \to \mathscr{I}_{\chi\chi'}$. Comme précédemment,

l'associativité et la co-associativité nous permettent de définir leurs itérations, pour tout $\chi_1, \dots, \chi_n \in \mathbb{F}^\vee$, que l'on notera

$$\Delta_{\chi_1,\dots\chi_n} : \mathscr{I}_{\chi_1\dots\chi_n} \to \mathscr{I}_{\chi_1} \otimes_S \cdots \otimes_S \mathscr{I}_{\chi_n},$$
$$\mu_{\chi_1,\dots,\chi_n} : \mathscr{I}_{\chi_1} \otimes_S \cdots \otimes_S \mathscr{I}_{\chi_n} \to \mathscr{I}_{\chi_1,\dots,\chi_n}.$$

DÉFINITION 4.1. — Soit G un schéma en $\mathbb{F}$-vectoriels sur S. On dit que G est un $\mathbb{F}$-*schéma de Raynaud* si pour tout $\chi \in \mathbb{F}^\vee$ le $\mathscr{O}_S$-module $\mathscr{I}_\chi$ est inversible. On dira de plus que G est un $\mathbb{F}$-*schéma de Raynaud libre* si pour tout $\chi \in \mathbb{F}^\vee$ le $\mathscr{O}_S$-module $\mathscr{I}_\chi$ est un $\mathscr{O}_S$-module libre. S'il n'y a pas de confusion possible, nous dirons simplement que G est un *schéma de Raynaud*.

Il en résulte en particulier que G est de rang q. En particulier, les $\mathbb{F}_p$-schémas de Raynaud sont les schémas en groupes de Oort-Tate étudiés dans [7]. Une des différences dans ce cas est qu'un schéma en $\mathbb{F}_p$-vectoriels localement libre de rang p est toujours un $\mathbb{F}_p$-schéma de Raynaud.

4.1.2. On introduit quelques notations supplémentaires pour énoncer le théorème de classification. Soit G un $\mathbb{F}$-schéma de Raynaud sur S. Alors on considère

- le morphisme $\Delta_i = \Delta_{\chi_i,\dots,\chi_i}$ où le i-ème caractère primitif χ_i est considéré p fois. Cette application peut être considérée canoniquement comme $\Delta_i : \mathscr{I}_{i+1} \to \mathscr{I}_i^p$ puisque $\chi_i^p = \chi_{i+1}$,
- le morphisme $\mu_i = \mu_{\chi_i,\dots,\chi_i}$ où le i-ème caractère primitif χ_i est considéré p fois. De même, on peut considérer cette application comme $\mu_i : \mathscr{I}_i^p \to \mathscr{I}_{i+1}$,
- la composée $w_i = \Delta_i \circ \mu_i$ est un élément de $\mathrm{End}(\mathscr{I}_{i+1})$ et par la définition d'un schéma de Raynaud on peut considérer w_i comme un élément de $\Gamma(S, \mathscr{O}_S)$.

Raynaud a établi le lemme suivant (cf. [9, Prop.1.3.1]) :

LEMME 4.2. — *Il existe $w \in pD^\times$ tel que pour tout i avec $1 \leqslant i \leqslant r$, w_i soit l'image de w par $D \to \Gamma(S, \mathscr{O}_S)$. En particulier, w est indépendant de i et de S.* □

Dans la suite, on notera aussi w l'image dans $\Gamma(S, \mathscr{O}_S)$. De même que précédemment, toujours avec $\chi = \prod_j \chi_j^{a_j}$, on peut définir

- le morphisme $\Delta_\chi = \Delta_{\chi_1,\dots,\chi_r} : \mathscr{I}_\chi \to \mathscr{I}_{\chi_1}^{\otimes a_1} \otimes_S \cdots \otimes_S \mathscr{I}_{\chi_r}^{\otimes a_r}$,
- le morphisme $\mu_\chi = \mu_{\chi_1,\dots,\chi_r} : \mathscr{I}_{\chi_1}^{\otimes a_1} \otimes_S \cdots \otimes_S \mathscr{I}_{\chi_r}^{\otimes a_r} \to \mathscr{I}_\chi$,
- la composée $w_\chi = \Delta_\chi \circ \mu_\chi$ qui est un élément de $\mathrm{End}(\mathscr{I}_\chi)$. On peut considérer w_χ comme un élément de $\Gamma(S, \mathscr{O}_S)$.

Raynaud a également établi le lemme suivant (cf. [9, Prop 1.3.1]) :

LEMME 4.3. — *Soit $\chi \in \mathbb{F}^\vee$. Alors w_χ est dans l'image de $D^\times \to \Gamma(S, \mathscr{O}_S)$. En particulier il est inversible.* □

4.1.3. On énonce maintenant le théorème principal de cette partie, établi par M. Raynaud [9, Prop.1.4.1].

THÉORÈME 4.4 (Classification des schémas de Raynaud). — *Fixons $w \in pD^\times$. L'application définit sur l'ensemble des classes d'isomorphismes de $\mathbb{F}$-schémas de Raynaud*

$$G \mapsto (\mathscr{I}_{\chi_i}, \Delta_i, \mu_i)_{1\leqslant i\leqslant r}$$

est une bijection à valeurs dans l'ensemble des triplets $(\mathscr{I}_{\chi_i}, \Delta_i, \mu_i)_{1\leqslant i\leqslant r}$, constitués de

- *un système $(\mathscr{I}_i)_{1\leqslant i\leqslant r}$ de classes d'isomorphismes de $\mathscr{O}_S$-modules inversibles,*
- *deux systèmes de morphismes*

$$\begin{cases} (\Delta_i \colon \mathscr{I}_{i+1} \to \mathscr{I}_i^p)_{1\leqslant i\leqslant r} \\ (\mu_i \colon \mathscr{I}_i^p \to \mathscr{I}_{i+1})_{1\leqslant i\leqslant r} \end{cases}$$

vérifiant pour tout i, tel que $1 \leqslant i \leqslant r$, la relation $\mu_i \circ \Delta_i = w \cdot \mathrm{id}_{\mathscr{I}_{i+1}}$ dans $\mathrm{End}(\mathscr{I}_{i+1})$. □

On retrouve pour $r = 1$ la classification des schémas en groupes d'ordre premier p établie dans [7].

En particulier, on obtient la description suivante des schémas de Raynaud libres, qui s'applique par exemple si S est le spectre d'un anneau local.

COROLLAIRE 4.5. — *Fixons $w \in pD^\times$. Soit G un $\mathbb{F}$-schéma de Raynaud libre sur S. Alors G est entièrement déterminé à isomorphisme près par la donnée de r couples $(x_i, y_i)_{1\leqslant i\leqslant r}$ d'éléments de $\Gamma(S, \mathscr{O})$ tels que $x_i y_i = w$ pour tout i avec $1 \leqslant i \leqslant r$. De plus, G est isomorphe à*

$$\mathrm{Spec}\, \frac{\mathscr{O}_S[z_1, \ldots, z_r]}{\langle z_i^p - x_i z_{i+1}\rangle_{i=1,\ldots,r}}, \tag{6}$$

où l'indice est considéré modulo r. La co-multiplication est donnée par

$$\Delta(z_i) = z_i \otimes 1 + 1 \otimes z_i + \sum_{\chi\chi' = \chi_i} \frac{x_{i-h} \cdot \cdots \cdot x_{i-1}}{w_\chi w_{\chi'}} \left(\prod_j z_j^{a_j}\right) \otimes \left(\prod_j z_j^{a'_j}\right),$$

pour $\chi = \prod_j \chi_j^{a_j}$, $\chi' = \prod_j \chi_j^{a'_j}$ et h un entier dépendant de χ et χ'. Le dual de Cartier G^D est obtenu en échangeant les rôles de x_i et y_i.

De plus, les familles de couples $(x_i, y_i)_{1\leqslant i\leqslant r}$ et $(x'_i, y'_i)_{1\leqslant i\leqslant r}$, tels que $x_i y_i = x'_i y'_i = w$ pour tout i avec $1 \leqslant i \leqslant r$, définissent des S-schémas en $\mathbb{F}$-vectoriels isomorphes si et seulement s'il existe une famille d'unités $\lambda_i \in \Gamma(S, \mathscr{O}_S)^\times$ telles que

$$x'_i = \lambda_i^p x_i \lambda_{i+1}^{-1} \text{ et } y'_i = \lambda_i^{-p} y_i \lambda_{i+1} \text{ pour tout } 1 \leqslant i \leqslant r.$$ □

DÉFINITION 4.6. — Si G est $\mathbb{F}$-schéma de Raynaud libre sur S de la forme (6) on dira que G est le $\mathbb{F}$-schéma de Raynaud de paramètres $(x_i, y_i)_{1\leqslant i\leqslant r}$.

4.1.4. On suppose maintenant que p est localement nilpotent sur S. Soit $\mathscr{F}$ un cristal en $\mathscr{O}_{S_{\mathbb{F}}/\Sigma}$-modules. Alors on dira que $\mathscr{F}$ est *spécial* si son caractère est de la forme

$$\mathfrak{ch}_S(\mathscr{F}) = \sum_{\chi\in\mathbb{F}^+} [\chi],$$

ou de manière équivalente, que ses composantes isotypiques $\mathscr{F}_\chi$ sont de rang 1 sur $\mathscr{O}_{S/\Sigma}/p\mathscr{O}_{S/\Sigma}$ pour tout $\chi \in \mathbb{F}^+$.

Soit G un schéma en $\mathbb{F}$-vectoriels sur S. Alors G est un schéma de Raynaud si et seulement si son caractère est de la forme

$$\mathrm{Ch}_S(G) = 1 + \sum_{\chi\in\mathbb{F}^\vee} [\chi].$$

Ainsi, par la formule des caractères du théorème 3.2, on a la proposition suivante :

PROPOSITION 4.7. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur S. Alors G est un schéma de Raynaud si et seulement si $\mathbb{D}(G)$ est spécial.*

De plus, on montre que la condition pour être un schéma de Raynaud peut être affaiblie :

COROLLAIRE 4.8. — *Soit G un schéma en $\mathbb{F}$-vectoriels sur S. Alors G est un schéma de Raynaud si et seulement si pour tout $\chi \in \mathbb{F}^+$, le faisceau localement libre $\mathscr{I}_\chi$ est un faisceau inversible.*

Démonstration. — La réciproque est immédiate, on suppose donc que G est un schéma en $\mathbb{F}$-vectoriels sur S tel que $\mathscr{I}_\chi$ est un faisceau inversible pour tout $\chi \in \mathbb{F}^+$. On veut montrer que G est un schéma de Raynaud.

D'après la formule des caractères, pour tout $\chi \in \mathbb{F}^+$, il existe un entier positif n_χ tel que

$$\mathrm{Ch}_S(G) = \prod_{\chi\in\mathbb{F}^+} \left(1 + [\chi] + \cdots + [\chi^{p-1}]\right)^{n_\chi}. \tag{7}$$

Or, d'après notre hypothèse il existe pour tout $\chi \in \mathbb{F}^\vee\backslash\mathbb{F}^+$ un entier positif a_χ tel que

$$\mathrm{Ch}_S(G) = \sum_{\chi\in\mathbb{F}^+} [\chi] + \sum_{\chi\in\mathbb{F}^\vee\backslash\mathbb{F}^+} a_\chi[\chi].$$

On compare cette expression avec le développement du produit dans (7). On obtient pour tout $\chi \in \mathbb{F}^+$ que $n_\chi \leqslant 1$ et que n_χ n'est pas nul ; donc $n_\chi = 1$. Ainsi, G est un schéma de Raynaud. □

4.2. Modules p-divisibles. —

4.2.1. Soit S un $\mathrm{W}(\mathbb{F})$-schéma tel que p soit localement nilpotent. Soit X un groupe p-divisible sur S. Comme pour les groupes finis, on peut alors lui associer un cristal de Dieudonné covariant

$$\mathbb{D}(X) = \mathscr{E}\mathrm{xt}^1_{S/\Sigma}(\underline{X^D}, \mathscr{O}_{S/\Sigma})^{(\sigma^{-1})}.$$

où X^D est le dual de Cartier de X. C'est un cristal en $\mathscr{O}_{S/\Sigma}$-modules localement libre (cf. [2, Théorème 3.3.10]). De plus, si X est de hauteur h sur S, alors $\mathbb{D}(X)$ est localement libre de rang h. D'après [2, Corollaire 3.3.5], on a une suite exacte de $\mathscr{O}_S$-modules, fonctorielle en X et en S,

$$0 \to \omega_{X^D} \to \mathbb{D}(X)_S \to \mathrm{Lie}(X) \to 0, \tag{8}$$

où ω_{X^D} sont les différentielles en la section unité de X^D et $\mathrm{Lie}(X)$ l'algèbre de Lie de X.

Supposons que S soit le spectre d'un corps parfait k. Soit $f\colon X \to X$ une isogénie entre groupes p-divisibles sur k. Alors $G = \ker(f)$ est par définition un schéma en groupes fini et localement libre sur S. Alors d'après [2, Proposition 3.3.13], l'application

$$\mathbb{D}(X^D) \to \mathbb{D}(G^D)$$

est surjective et son noyau est $f \cdot \mathbb{D}(X^D)$, où $f\colon \mathbb{D}(X^D) \to \mathbb{D}(X^D)$ est induit de f par fonctorialité. On en déduit par dualité, en passant au module de Dieudonné et en utilisant le fait que $\mathbb{D}(G)$ et $\mathbb{D}(X)$ sont des cristaux, que

$$\mathbb{D}(G) \cong \mathbb{D}(X)/f \cdot \mathbb{D}(X). \tag{9}$$

4.2.2. On introduit quelques notations. Soit K une extension finie de degré n de $\mathbb{Q}_p$ et O_K son anneau d'entiers. On fixe $\pi \in O_K$ une uniformisante et on note $\kappa = O_K/(\pi)$ son corps résiduel. On note f le degré de κ sur $\mathbb{F}_p$ et e le degré de ramification de K sur $\mathbb{Q}_p$. On garde les notations précédentes, $\kappa^\vee = \mathrm{Hom}(\kappa^\times, \bar{C}^\times)$ les caractères multiplicatifs de κ et $\kappa^+ \subset \kappa^\vee$ les caractères primitifs. On fixe S un schéma sur $\mathrm{W}(\kappa)$ tel que p soit localement nilpotent.

Définition 4.9. — Un *O_K-module p-divisible* sur S est un groupe p-divisible X sur S muni d'un morphisme d'anneaux

$$\iota\colon O_K \to \mathrm{End}(X).$$

Dans la suite de ce paragraphe on fixe un O_K-module p-divisible X sur S. On a une décomposition

$$D \otimes_{\mathbb{Z}_p} \mathrm{W}(\kappa) = \prod_{\chi \in \kappa} D_\chi.$$

On note comme précédemment $p_\chi \colon D \otimes_{\mathbb{Z}_p} \mathrm{W}(\kappa) \to D_\chi$ la projection pour tout $\chi \in \kappa^+$. On obtient des décompositions

$$\mathbb{D}(X) = \bigoplus_{\chi\in\kappa^+} \mathbb{D}(X)_\chi,\ \mathrm{Lie}(X) = \bigoplus_{\chi\in\kappa^+} \mathrm{Lie}(X)_\chi,\ \omega_{X^D} = \bigoplus_{\chi\in\kappa^+} (\omega_{X^D})_\chi, \tag{10}$$

qui sont compatibles avec la suite exacte 8 car elle est fonctorielle en X.

Définition 4.10. — Soit $\mathscr{F}$ un $\mathscr{O}_S$-module (resp. $\mathscr{O}_{S/\Sigma}$-module) localement libre gradué sur κ^+, i.e.

$$\mathscr{F} = \bigoplus_{\chi\in\kappa^+} \mathscr{F}_\chi.$$

Alors on définit son caractère par

$$\mathfrak{ch}_S(\mathscr{F}) = \sum_{\chi\in\kappa^+} \mathrm{rang}_S(\mathscr{F}_\chi)[\chi] \in \mathbb{N}[\kappa^+].$$

Cette définition ne porte pas à confusion avec la définition précédente de $\mathfrak{ch}_S$ puisqu'il dépend de la nature de $\mathscr{F}$. De plus, ces définitions sont compatibles, par exemple si $\mathscr{F}$ est un cristal en $\mathscr{O}_{S/\Sigma}$-modules

$$\mathfrak{ch}_S(\mathscr{F}) = \mathfrak{ch}_S(\mathscr{F}_S).$$

Il est claire que ces caractères sont additifs. Ainsi, la filtration de Hodge 8 nous donne la relation

$$\mathfrak{ch}_S(\mathbb{D}(X)) = \mathfrak{ch}_S(\mathrm{Lie}(X)) + \mathfrak{ch}_S(\omega_{X^D}).$$

On calcule maintenant le caractère d'un O_K-module p-divisible. Ce n'est pas un résultat profond mais plus un exercice que l'on peut résoudre de plusieurs façons ; on propose ici un calcul similaire à celui que l'on ferra pour les O_D-module p-divisibles. On note que $X[\pi]$ et $X[p]$ sont des schémas en κ-vectoriels.

Proposition 4.11. — *Soit X un O_K-module p-divisible de hauteur hn où h est un entier positif. Alors*

$$\mathfrak{ch}_S(\mathbb{D}(X[\pi])) = h\left(\sum_{\chi\in\kappa^+}[\chi]\right),\ \mathfrak{ch}_S(\mathbb{D}(X)) = he\left(\sum_{\chi\in\kappa^+}[\chi]\right).$$

Démonstration. — Comme précédemment, (cf. 2.2.4) on peut supposer que $S = \mathrm{Spec}(k)$ où k est un corps algébriquement clos de caractéristique p.

On note $M = D(X)$, le module de Dieudonné de X, il est gradué sur κ^+, i.e.

$$M = \bigoplus_{\chi\in\kappa^+} M_\chi.$$

Les deux opérateurs F et V induisent $F\colon M_\chi \to M_{\chi^p}$ et $V\colon M_{\chi^p} \to M_\chi$ pour tout $\chi \in \kappa^+$. Comme l'opérateur V est injectif, on en déduit que $\operatorname{rang}_{\mathrm{W}(k)} M_\chi$ est indépendant de $\chi \in \kappa^+$. Ainsi il existe un entier a tel que

$$\mathfrak{ch}_k(M) = a\left(\sum_{\chi\in\kappa^+}[\chi]\right).$$

Or, comme X est de hauteur $hn = hef$, on en déduit que $a = he$, ce qui montre la deuxième égalité.

Montrons la première égalité. D'après (9), on a $D(X[\pi]) = M/\pi M$, c'est un module de Dieudonné gradué sur κ^+. Pour tout $\chi \in \kappa^+$, on a un diagramme commutatif, dont tous les membres ont même rang sur $\mathrm{W}(k)$,

$$\begin{array}{ccc} M_{\chi^p} & \xrightarrow{V} & M_\chi \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ M_{\chi^p} & \xrightarrow{V} & M_\chi. \end{array} \tag{11}$$

Comme les co-noyaux des flèches horizontales sont égaux, les co-noyaux des flèches verticales ont mêmes dimensions sur k (on peut le déduire du lemme du serpent). Ainsi, comme précédemment,

$$\mathfrak{ch}_k(M/\pi M) = h\left(\sum_{\chi\in\kappa^+}[\chi]\right),$$

ce qui montre la première égalité. □

4.2.3. On garde les notations du paragraphe précédent. Soit $d \geqslant 2$ un entier et D l'algèbre à division d'invariant $1/d$ sur K. Alors D contient $\widetilde{K}$, l'extension non-ramifié de K de degré d ; on note $O_{\widetilde{K}}$ son anneau des entiers. On note $\mathbb{F}$ le corps résiduel de D, qui est le corps résiduel de $\widetilde{K}$; on notera q le cardinal de $\mathbb{F}$. Soit O_D l'ordre maximal de D. On fixe un élément primitif $\Pi \in O_D$ tel que $\Pi^d = \pi$. On fixe S un schéma sur $\mathrm{W}(\mathbb{F})$, que l'on supposera connexe, tel que p soit localement nilpotent.

Définition 4.12. — Un *O_D-module p-divisible* sur S est un groupe p-divisible X sur S, muni d'un morphisme d'anneaux

$$\iota\colon O_D \to \operatorname{End}(X).$$

En particulier, un O_D-module p-divisible est un $O_{\widetilde{K}}$-module p-divisible, ainsi les considérations du paragraphe précédent sont toujours valables. Ainsi, la proposition 4.11 nous donne le corollaire suivant :

COROLLAIRE 4.13. — *Soit X un O_D-module p-divisible de hauteur hnd^2 sur S, pour h un entier positif. Alors*

$$\mathfrak{ch}_S(\mathbb{D}(X[\pi]) = hd\left(\sum_{\chi\in\mathbb{F}^+}[\chi]\right). \qquad \square$$

Soit $f = \sum_{\chi\in\mathbb{F}^+} a_\chi[\chi] \in \mathbb{N}[\mathbb{F}^+]$ un caractère. On notera

$$f^{(p)} = \sum_{\chi\in\mathbb{F}^+} a_\chi[\chi^p], \text{ et de même } f^{(q)} = \sum_{\chi\in\mathbb{F}^+} a_\chi[\chi^q].$$

Soit X un O_D-module p-divisible de hauteur hnd^2 sur S, pour h un entier positif. On considère le caractère de $X[\Pi]$, qui est un schéma en $\mathbb{F}$-vectoriels. L'additivité du caractère et le corollaire précédent impliquent alors que

$$\sum_{i=1}^{d} \mathfrak{ch}_S(\mathbb{D}(X[\Pi]))^{(q^i)} = \mathfrak{ch}_S(\mathbb{D}(X[\pi]).$$

Ainsi, d'après la proposition 4.7, si $X[\Pi]$ est $\mathbb{F}$-schéma de Raynaud alors $h = 1$. On veut expliciter une condition sur X pour déterminer si $X[\Pi]$ est un schéma de Raynaud. On a le lemme suivant :

LEMME 4.14. — *Soit X un O_D-module p-divisible sur S. Alors on a la relation suivante :*

$$\mathfrak{ch}_S(\mathbb{D}(X[\Pi]))^{(qp)} - \mathfrak{ch}_S(\mathbb{D}(X[\Pi]))^{(q)} = \mathfrak{ch}_S(\mathrm{Lie}(X)) - \mathfrak{ch}_S(\mathrm{Lie}(X))^{(q)}.$$

Démonstration. — Comme précédemment on peut supposer que $S = \mathrm{Spec}(k)$, le spectre d'un corps algébriquement clos de caractéristique p. Soit $M = D(X)$ le module de Dieudonné de X. Alors on a le diagramme commutatif suivant, dont les lignes et colonnes sont exactes

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & M^{(p)} & \xrightarrow{V} & M & \longrightarrow & \mathrm{Lie}(X) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \Pi} & & \downarrow{\scriptstyle \Pi} & & \downarrow{\scriptstyle \Pi} & & \\
0 & \longrightarrow & M^{(qp)} & \xrightarrow{V} & M^{(q)} & \longrightarrow & \mathrm{Lie}(X)^{(q)} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \Pi} & & \downarrow{\scriptstyle \Pi} & & \downarrow & & \\
 & & (M/\Pi M)^{(qp)} & \xrightarrow{V} & (M/\Pi M)^{(q)} & \longrightarrow & \mathrm{Lie}(X[\Pi])^{(q)} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

On a déjà remarqué que comme V est injectif sur M, $\mathfrak{ch}_k(M) = \mathfrak{ch}_k(M^{(p)})$. On note $K = \ker(\mathrm{Lie}(X) \xrightarrow{\Pi} \mathrm{Lie}(X)^{(q)})$. Par le lemme du serpent on a la suite exacte

$$0 \to K \to (M/\Pi M)^{(qp)} \xrightarrow{V} (M/\Pi M)^{(q)} \to \mathrm{Lie}(X[\Pi])^{(q)} \to 0.$$

Ainsi $\mathfrak{ch}_k((M/\Pi M)^{(qp)}) - \mathfrak{ch}_k((M/\Pi M)^{(q)}) = \mathfrak{ch}_k(\mathrm{Lie}(X[\Pi])^{(q)}) - \mathfrak{ch}_k(K)$. Mais de la dernière suite exacte verticale du diagramme, on a aussi $\mathfrak{ch}_k(\mathrm{Lie}(X[\Pi])^{(q)}) - \mathfrak{ch}_k(K) = \mathfrak{ch}_k(\mathrm{Lie}(X)) - \mathfrak{ch}_k(\mathrm{Lie}(X))^{(q)}$, d'où le lemme. □

On en déduit directement le théorème suivant, qui détermine quand les points de torsion d'un O_D-module formel forment un schéma de Raynaud.

THÉORÈME 4.15. — *Soit X un O_D-module p-divisible sur S de hauteur hnd^2 pour h un entier positif. Alors $X[\Pi]$ est un schéma de Raynaud si et seulement si $h = 1$ et $\mathfrak{ch}_S(\mathrm{Lie}(X)) = \mathfrak{ch}_S(\mathrm{Lie}(X))^{(q)}$.*

Cette condition est par exemple vérifiée pour les O_D-modules formels spéciaux de Drinfeld [4], ou plus généralement pour les O_D-modules formels r-spéciaux considérés par Rapoport-Zink dans [8] comme expliqué dans l'introduction.

Remerciements. — J'aimerais remercier chaleureusement L. Fargues de m'avoir donné les clés du théorème 1.1 et de ses encouragements constants pour sa démonstration. Je remercie aussi S. Bartling et V. Hernandez pour leurs relectures attentives et leur intérêt pour ce travail.

BIBLIOGRAPHIE

[1] M. Artin, J.-E. Bertin, M. Demazure, A. Grothendieck, P. Gabriel, M. Raynaud & J.-P. Serre – *Schémas en groupes*, Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, Institut des Hautes Études Scientifiques, Paris, 1963/1966.

[2] P. Berthelot, L. Breen & W. Messing – *Théorie de Dieudonné cristalline. II*, Lecture Notes in Mathematics, vol. 930, Springer-Verlag, Berlin, 1982.

[3] M. Demazure & P. Gabriel – *Groupes algébriques. Tome I : Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris ; North-Holland Publishing Co., Amsterdam, 1970, Avec un appendice Corps de classes local par Michiel Hazewinkel.

[4] V. G. Drinfeld – « Coverings of p-adic symmetric domains », *Funkcional. Anal. i Priložen.* **10** (1976), no. 2, p. 29–40.

[5] J.-M. Fontaine – *Groupes p-divisibles sur les corps locaux*, Société Mathématique de France, Paris, 1977, Astérisque, No. 47-48.

[6] A. J. de Jong & W. Messing – « Crystalline Dieudonné theory over excellent schemes », *Bull. Soc. Math. France* **127** (1999), no. 2, p. 333–348.
[7] F. Oort & J. Tate – « Group schemes of prime order », *Ann. Sci. École Norm. Sup. (4)* **3** (1970), p. 1–21.
[8] M. Rapoport & T. Zink – « On the Drinfeld moduli problem of p-divisible groups », *Camb. J. Math.* **5** (2017), no. 2, p. 229–279.
[9] M. Raynaud – « Schémas en groupes de type $(p, \dots, p)$ », *Bull. Soc. Math. France* **102** (1974), p. 241–280.
[10] A. Vanhaecke – « Un modèle formel pour le premier revêtement de l'espace symétrique de Drinfeld », (2019).
[11] H. Wang – « L'espace symétrique de Drinfeld et correspondance de Langlands locale I », *Math. Z.* **278** (2014), no. 3-4, p. 829–857.

Bull. Soc. Math. France
148 (3), 2020, p. 467-480

A CONJECTURAL BOUND ON THE SECOND BETTI NUMBER FOR HYPER-KÄHLER MANIFOLDS

BY YOON-JOO KIM & RADU LAZA

ABSTRACT. — In a previous work ([1]), we noted that the known cases of hyper-Kähler manifolds satisfy a natural condition on the LLV decomposition of the cohomology; informally, the Verbitsky component is the dominant representation in the LLV decomposition. Assuming this condition holds for all hyper-Kähler manifolds, we obtain an upper bound for the second Betti number in terms of the dimension.

RÉSUMÉ (*Une majoration conjecturale sur le deuxième nombre de Betti pour les variétés hyper-kählériennes*). — Dans un article précédent, nous avons remarqué que les exemples connus de variétés hyper-kählériennes satisfont une condition naturelle sur la décomposition LLV de la cohomologie; informellement, la composante Verbitsky est la représentation dominante dans la décomposition LLV. Supposons que toutes les variétés hyper-kählériennes satisfait cette condition, nous obtenons un majorant pour le deuxième nombre de Betti en fonction de la dimension de la variété.

1. Introduction

A fundamental open question in the theory of compact hyper-Kähler manifolds is the boundedness question: *are there finitely many diffeomorphism types*

Texte reçu le 23 septembre 2019, modifié le 27 janvier 2020, accepté le 26 février 2020.

YOON-JOO KIM, Stony Brook University, Department of Mathematics, Stony Brook, NY 11794-3651 • *E-mail :* yoon-joo.kim@stonybrook.edu
RADU LAZA, Stony Brook University, Department of Mathematics, Stony Brook, NY 11794-3651 • *E-mail :* radu.laza@stonybrook.edu

Mathematical subject classification (2010). — 14J40, 14F25, 32J27, 53C26.

Key words and phrases. — Hyper-Kähler manifold, Second Betti number.

The two authors were partially supported by NSF grant DMS-1802128.

© Société Mathématique de France
0037-9484/2020/467/$ 5.00
doi:10.24033/bsmf.2813

of hyper-Kählers in a given dimension? In accordance with the Torelli principle, Huybrechts [3, Thm 4.3] proved that there are finitely many diffeomorphism types of hyper-Kähler manifolds, once the dimension and the (unnormalized) Beauville–Bogomolov lattice $(H^2(X,\mathbb{Z}), q_X)$ are fixed. Thus, bounding the hyper-Kähler manifolds is equivalent to bounding the second Betti number $b_2 = b_2(X)$, and then the Beauville–Bogomolov form (e.g., the discriminant). In dimension 2, a compact hyper-Kähler manifold is always a K3 surface, thus $b_2 = 22$. In dimension 4, Beauville and Guan [2] gave a sharp bound $b_2 \leq 23$ (in fact, Guan showed that $3 \leq b_2 \leq 8$ or $b_2 = 23$). For some further partial results on bounding b_2, see Remark 1.2. The purpose of this note is to give a conjectural bound on $b_2(X)$ for an arbitrary compact hyper-Kähler manifold X of dimension $2n$. Our bound depends on a natural conjectural condition satisfied by the Looijenga–Lunts–Verbitsky (LLV) decomposition of the cohomology $H^*(X)$ for hyper-Kähler manifolds X.

To state our results, let us recall that Verbitsky [9] and Looijenga–Lunts [6] noted that the cohomology $H^*(X)$ of a hyper-Kähler manifold admits a natural action by the Lie algebra $\mathfrak{g} = \mathfrak{so}(b_2 + 2)$, generalizing the usual hard Lefschetz theorem. As a $\mathfrak{g}$-module, the cohomology of a hyper-Kähler manifold X decomposes as

$$H^*(X) = \bigoplus_{\mu} V_{\mu}^{\oplus m_\mu}, \tag{1}$$

where V_μ indicates an irreducible $\mathfrak{g}$-module of the highest weight $\mu = (\mu_0, \ldots, \mu_r)$, with $r = \left\lfloor \frac{b_2(X)}{2} \right\rfloor = \operatorname{rk} \mathfrak{g} - 1$. We refer to $\mathfrak{g}$ as the *LLV algebra* of X and to (1) as the *LLV decomposition* of $H^*(X)$ (see [1] for a further discussion). Motivated by the behavior of the LLV decomposition in the known cases of hyper-Kähler manifolds [1], we have made the following conjecture.

Conjecture ([1]). — *Let X be a compact hyper-Kähler manifold of dimension $2n$. Then, the weights $\mu = (\mu_0, \ldots, \mu_r)$ occurring in the LLV decomposition* (1) *of $H^*(X)$ satisfy*

$$\mu_0 + \cdots + \mu_{r-1} + |\mu_r| \leq n. \tag{2}$$

The conjecture holds for all currently known examples of compact hyper-Kähler manifolds (cf. [1, §1]). Furthermore, the equality in (2) holds for *the Verbitsky component*, an irreducible $\mathfrak{g}$-submodule with the highest weight $\mu = (n, 0, \ldots, 0)$ that is always present in $H^*(X)$. This shows that (2) is sharp. Beyond the evidence given by the validity of (2) in the known cases, we have some partial arguments of motivic nature (and depending on standard conjectures) showing that at least (2) is plausible. This will be discussed elsewhere. The purpose of this note is to show that conjecture (2) implies a general bound on $b_2(X)$.

MAIN THEOREM. — *Let X be a compact hyper-Kähler manifold of dimension $2n$. If the condition* (2) *holds for X, then*

$$b_2(X) \leq \begin{cases} \frac{21+\sqrt{96n+433}}{2} & \text{if } H^*_{\mathrm{odd}}(X) = 0 \\ 2k+1 & \text{if } H^k(X) \neq 0 \text{ for some odd } k \end{cases}. \tag{3}$$

REMARK 1.1. — A slightly weaker version of (3) is

$$b_2(X) \leq \max\left\{\tfrac{21+\sqrt{96n+433}}{2}, 4n-1\right\},$$

which reads explicitly

n	1	2	3	4	5	6	7	≥ 8
$b_2(X) \leq$	22	23	23	24	25	26	27	$4n-1$

In low dimensions, our bounds agree with the known results and seem fairly sharp. For instance, we know $\mathrm{K3}^{[n]}$-type hyper-Kähler manifolds have $b_2 = 23$, and OG10 manifolds have $b_2 = 24$. These examples almost reach our maximum bound of b_2 for low dimensions. Similarly, Kum_n type hyper-Kähler manifolds have $H^3(X) \neq 0$ and $b_2 = 7$, also showing that the second inequality in (3) is sharp.

REMARK 1.2. — Sawon [8] and Kurnosov [5] previously obtained the same bounds for $3 \leq n \leq 5$, and also predicted the general formula (3) when $H^*_{\mathrm{odd}}(X) = 0$. However, their results were based on the assumption that an irreducible module V_μ is determined by the shape of its Hodge diamond. In general, the shape of the Hodge diamond of V_μ is controlled only by the first two coefficients μ_0, μ_1 (see [1, §2.2]).

A few words about the proof of our conjectural bound. First, in [1, §1], we already obtained that the condition (2) has consequences on the odd cohomology (specifically, if $b_2 \geq 4n$, then there should be no odd cohomology). A slight generalization of the argument in [1, §1] then gives the second inequality in (3). The main content of this note is the control of the even cohomology under the assumption (2). Essentially, our argument is a representation theoretic refinement of Beauville's argument that $b_2 \leq 23$ for hyper-Kähler fourfolds. Namely, the starting point is Salamon's relation [7], a linear relation satisfied by the Betti numbers of hyper-Kähler manifolds. Inspired by the shape of it, we define a numerical function $s(W)$ for a $\mathfrak{g}$-module W and verify its basic properties, most importantly $s(W_1 \oplus W_2) \leq \max\{s(W_1), s(W_2)\}$. In this setting,

Salamon's relation reads $s(H^*(X)) = \frac{n}{3}$. Now, the punch line is an explicit formula for $s(V_\mu)$ for irreducible $\mathfrak{g}$-modules V_μ (Theorem 3.4), which is obtained by applying the Weyl character formula. Combining it with (2), we conclude

$$\frac{n}{3} = s(H^*(X)) \leq s(V_{(n,0,\dots,0)}) = \frac{8n(b_2+n)}{(b_2+1)(b_2+2)},$$

which, in turn, gives the first inequality in (3).

2. Cohomology of compact hyper-Kähler manifolds

We briefly review some relevant results on the cohomology of hyper-Kähler manifolds. Let X be a compact hyper-Kähler manifold of dimension $2n$ and $H^*(X) = H^*(X, \mathbb{C})$. Let $\mathfrak{g} \subset \mathfrak{gl}(H^*(X))$ be the Lie algebra generated by all the Lefschetz and dual Lefschetz operators associated to elements in $H^2(X)$ (cf. [9], [6]). We call this the Looijenga–Lunts–Verbitsky (LLV) algebra of X. Let

$$(V, q) = (H^2(X), q_X) \oplus U$$

be the Mukai completion of $H^2(X)$ equipped with the Beauville–Bogomolov form and set $r = \lfloor \frac{b_2(X)}{2} \rfloor$. Then, $\mathfrak{g}$ is isomorphic to the special orthogonal Lie algebra $\mathfrak{so}(V, q) \cong \mathfrak{so}(b_2 + 2, \mathbb{C})$ of rank $r + 1$. The cohomology $H^*(X)$ of a hyper-Kähler manifold X admits a $\mathfrak{g}$-module structure, generalizing the hard Lefschetz theorem. We refer to the $\mathfrak{g}$-module irreducible decomposition (1) of $H^*(X)$ as the *LLV decomposition* of the cohomology (see [1, §3] for some examples).

Fix a Cartan and a Borel subalgebra of $\mathfrak{g}$. Representation theory of $\mathfrak{so}(V, q)$ depends on the parity of $\dim V = b_2 + 2$. If $b_2 = 2r$ is even, then we can fix a suitable basis $\varepsilon_0, \dots, \varepsilon_r$ of the dual Cartan subalgebra, such that the $2r + 2$ associated weights of the standard module V are $\pm\varepsilon_0, \dots, \pm\varepsilon_r$. Similarly, if $b_2 = 2r+1$ is odd, then we can choose ε_i, such that V has the $2r+3$ associated weights $0, \pm\varepsilon_0, \dots, \pm\varepsilon_r$. (Note that the index of the basis starts from 0.) Any dominant integral weight μ can be expressed in this basis as

$$\mu = (\mu_0, \dots, \mu_r) = \sum_{i=0}^{r} \mu_i \varepsilon_i.$$

Here, if $b_2 = 2r$ is even, then μ_i satisfy the condition $\mu_0 \geq \cdots \geq \mu_{r-1} \geq |\mu_r| \geq 0$, and μ_i are either all integers or all half-integers. If $b_2 = 2r + 1$ is odd, then $\mu_0 \geq \cdots \geq \mu_r \geq 0$, and μ_i are, again, either all integers or all half-integers. It will be important whether μ_i are integers or half-integers, so we define:

DEFINITION 2.1. — Let $\mu = (\mu_0, \ldots, \mu_r)$ be a dominant integral weight of $\mathfrak{g} = \mathfrak{so}(V, q)$.

(i) If all μ_i are integers, we say μ is *even*. If all μ_i are half-integers (i.e., $\mu_i \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$), we say μ is *odd*.
(ii) An irreducible $\mathfrak{g}$-module V_μ of highest weight μ is called even (respectively, odd), if μ is even (respectively odd).
(iii) A $\mathfrak{g}$-module W is called even (respectively odd) if all of its irreducible components V_μ are even (respectively odd).

By [1, Prop 2.35], the even (odd) cohomology $H^*_{\text{even}}(X)$ is always an even (odd) $\mathfrak{g}$-module.

When μ is even and has multiple 0's at the end of its coordinate expression $(\mu_0, \ldots, \mu_r)$, we will simply omit the last 0's. For example, the notation $(m) = (m, 0, \ldots, 0)$ refers to the integral weight $m\varepsilon_0$. In the geometric situation for hyper-Kähler manifolds, the subalgebra of $H^*(X)$ generated by $H^2(X)$ becomes an irreducible $\mathfrak{g}$-submodule of $H^*(X)$, which we call *the Verbitsky component* of $H^*(X)$. As a $\mathfrak{g}$-module, the Verbitsky component is isomorphic to $V_{(n)}$, and it always occurs with multiplicity 1 in the LLV decomposition.

Let h be the degree operator on $H^*(X)$, the operator acting as multiplication by k on $H^{2n+k}(X)$. For a suitable choice of a Cartan and a Borel subalgebra, we can assume $h = \varepsilon_0^\vee$ (e.g., [1, (2.28)]). By definition, the degree decomposition of the cohomology

$$H^*(X) = \bigoplus_{k=-2n}^{2n} H^{2n+k}(X)$$

is the h-eigenspace decomposition. In general, an arbitrary $\mathfrak{g}$-module admits the h-eigenspace decomposition

$$W = \bigoplus_{k \in \mathbb{Z}} W_k, \tag{4}$$

where W_k denotes the eigenspace of W with eigenvalue k. The eigenvalues k are always integers for the following reason. Let $W(\theta)$ be the weight subspace of W associated to a weight $\theta = \theta_0\varepsilon_0 + \cdots + \theta_r\varepsilon_r$. Then, $h = \varepsilon_0^\vee$ acts on $W(\theta)$ by $\langle \varepsilon_0^\vee, \theta \rangle = 2\theta_0$, which is an integer, since $\theta_0 \in \frac{1}{2}\mathbb{Z}$ for any weight θ.

Consider the LLV decomposition of the cohomology

$$H^*(X) = \bigoplus_{\mu} V_\mu^{\oplus m_\mu}. \tag{1 (restated)}$$

If V_μ is contained in the odd cohomology, then μ is odd by the above discussion. Hence, all μ_i are half-integers, and in particular, we have $\mu_i \geq \frac{1}{2}$ (possibly except for the last $|\mu_r| \geq \frac{1}{2}$, if b_2 is even). If we specifically assume $H^k(X) \neq 0$ for odd $k < 2n$, then there exists at least one irreducible component V_μ with $(V_\mu)_{k-2n} \neq 0$. This means $h = \varepsilon_0^\vee$ acts on some part of V_μ by $k - 2n$, so V_μ

has an associated weight $\theta = \theta_0\varepsilon_0 + \cdots + \theta_r\varepsilon_r$ with $\theta_0 = \frac{k}{2} - n$. This forces $\mu_0 \geq n - \frac{k}{2}$. Summarizing, we have

$$\mu_0 \geq n - \frac{k}{2}, \qquad \mu_1, \ldots, \mu_{r-1}, |\mu_r| \geq \frac{1}{2},$$

which gives the following:

COROLLARY 2.2. — *Let X be a compact hyper-Kähler manifold of dimension $2n$. Assume $H^k(X) \neq 0$ for some odd integer $k < 2n$. Then, there exists a weight μ in (1) with $\mu_0 + \cdots + \mu_{r-1} + |\mu_r| \geq n - \frac{k}{2} + \frac{r}{2}$.* □

Finally, let us recall Salamon's relation. Let $b_k = b_k(X)$ be the k-th Betti number of X. Salamon [7] proved that the Betti numbers of hyper-Kähler manifolds X satisfy a linear relation:

$$\sum_{k=1}^{2n} (-1)^k (6k^2 - 2n) b_{2n+k} = n b_{2n}.$$

One can manipulate the identity into the following form

$$\sum_{k=-2n}^{2n} (-1)^k k^2 b_{2n+k} = \frac{n}{3} e(X), \tag{5}$$

where $e(X) = \sum_{k=-2n}^{2n} (-1)^k b_{2n+k}$ is the topological Euler characteristic of X.

3. Proof of Main Theorem

Inspired by Salamon's relation (5), we define a constant $s(W)$ associated to an arbitrary $\mathfrak{g}$-module W.

DEFINITION 3.1. — Let W be a $\mathfrak{g}$-module and $W = \bigoplus_k W_k$ its h-eigenspace decomposition in (4). Assume $\sum_k (-1)^k \dim W_k \neq 0$ (N.B. This is automatic if W is either even or odd). Then, we define a constant $s(W) \in \mathbb{Q}$ associated to W by

$$s(W) = \frac{\sum_{k\in\mathbb{Z}} (-1)^k k^2 \dim W_k}{\sum_{k\in\mathbb{Z}} (-1)^k \dim W_k}.$$

In particular, if $e(X) \neq 0$, Salamon's relation (5) reads

$$s(H^*(X)) = \frac{n}{3}. \tag{6}$$

The case of odd cohomology will be easily handled by Corollary 2.2. Thus, we can focus on the case of vanishing odd cohomology (in particular, $e(X) \neq 0$). The main content, then, is to bound the value $s(H^*(X))$ in terms of b_2 and the LLV decomposition (1). Once this is done, assuming our conjecture (2),

Salamon's relation (6) leads to the desired inequality (3) between b_2 and n. Let us start from some straightforward properties of the constant $s(W)$.

PROPOSITION 3.2. — *Let $\{W_i\}_{i\in I}$ be a finite set of $\mathfrak{g}$-modules with well-defined $s(W_i)$.*

(i) *If all W_i are simultaneously even or odd, then*

$$\min_i\{s(W_i)\} \leq s\left(\bigoplus_i W_i\right) \leq \max_i\{s(W_i)\}.$$

(ii) $s\left(\bigotimes_i W_i\right) = \sum_i s(W_i)$.

Proof. — It is enough to prove the proposition for two $\mathfrak{g}$-modules W and W'. Assume without loss of generality $s(W) \leq s(W')$ and let us consider the case when W and W' are even (the odd case is similar). In this case, all eigenvalues k of W are even, so we have

$$\sum_k k^2 \dim W_k = s(W)\dim W, \qquad \sum_k k^2 \dim W'_k = s(W')\dim W'.$$

Adding the two equalities and using $s(W) \leq s(W')$ gives us the first item.

For the second item, we compute

$$\begin{aligned}
\sum_k (-1)^k k^2 \dim(W\otimes W')_k &= \sum_k (-1)^k k^2 \Big(\sum_{i+j=k} \dim W_i \dim W'_j\Big) \\
&= \sum_{i,j} (-1)^{i+j}(i^2+2ij+j^2)\dim W_i \dim W'_j \\
&= \Big(\sum_i (-1)^i i^2 \dim W_i\Big) e(W') \\
&\quad + \Big(\sum_j (-1)^j j^2 \dim W'_j\Big) e(W) \\
&\quad + 2\Big(\sum_i (-1)^i i \dim W_i\Big)\Big(\sum_j (-1)^j j \dim W'_j\Big).
\end{aligned}$$

Here, for simplicity, we used the notation $e(W) = \sum_i (-1)^i \dim W_i$ and $e(W') = \sum_j (-1)^j \dim W'_j$. Notice that $\sum_i (-1)^i i \dim W_i = 0$, since by Weyl symmetry, we always have $\dim W_i = \dim W_{-i}$. This proves $\sum_k (-1)^k k^2 \dim(W\otimes W')_k = (\sum_i (-1)^i i^2 \dim W_i) e(W') + (\sum_j (-1)^j j^2 \dim W'_j) e(W)$. Dividing both sides by $e(W\otimes W') = e(W)e(W')$ gives us the result. □

REMARK 3.3. — In fact, we can associate to an arbitrary $\mathfrak{g}$-module W the following formal power series

$$S(W) = \sum_k (-1)^k \dim W_k \cdot \exp(kt) \in \mathbb{Q}[[t]].$$

One can easily show

$$S(W \oplus W') = S(W) + S(W'), \quad S(W \otimes W') = S(W) \cdot S(W'),$$

so that S defines a *ring homomorphism* from the representation ring $K(\mathfrak{g})$ of $\mathfrak{g}$

$$S : K(\mathfrak{g}) \to \mathbb{Q}[[t]].$$

By Weyl symmetry, we have $\dim W_k = \dim W_{-k}$, giving that all the odd degree terms of $S(W)$ vanish. Thus, we can write

$$S(W) = s_0 + s_2 t^2 + s_4 t^4 + \cdots \in \mathbb{Q}[[t]], \qquad s_i = \frac{1}{i!} \sum_k (-1)^k k^i \dim W_k.$$

From this perspective, our constant $s(W)$ is the ratio between the first two coefficients

$$s(W) = \frac{2s_2}{s_0}$$

of the formal power series $S(W)$.

A more interesting result is the explicit computation of $s(W)$ for irreducible $\mathfrak{g}$-modules $W = V_\mu$. Recall that the Lie algebra $\mathfrak{g}$ was isomorphic to $\mathfrak{so}(b_2+2, \mathbb{C})$ and $r = \lfloor \frac{b_2}{2} \rfloor$, so that $\mathfrak{g}$ has rank $r+1$, and a dominant integral weight μ can be written as a tuple $(\mu_0, \ldots, \mu_r)$.

THEOREM 3.4. — *With notations as above, let V_μ be an irreducible $\mathfrak{g}$-module of highest weight μ. If $\mu_r \geq 0$, then*

$$s(V_\mu) = 8 \cdot \frac{(\sum_{i=0}^r \mu_i)\, b_2 + \left(\sum_{i=0}^r (\mu_i - i)^2 - i^2\right)}{(b_2+1)(b_2+2)}.$$

If b_2 is even and $\mu_r < 0$, then $s(V_\mu) = s(V_{\mu'})$ where $\mu' = (\mu_0, \ldots, \mu_{r-1}, -\mu_r)$.

We postpone the proof of Theorem 3.4 to the following section. For now, let us conclude the proof of our main theorem using this result. First, we note the following consequence of Theorem 3.4. Recall from Section 2 that the notation $(m) = (m, 0, \ldots, 0)$ refers to the integral weight $m\varepsilon_0$.

COROLLARY 3.5. — (i) *$s(V_{(m)}) = \frac{8m(b_2+m)}{(b_2+1)(b_2+2)}$ for $m \in \mathbb{Z}_{\geq 0}$.*
(ii) *If μ is even, then $s(V_\mu) \leq s(V_{(m)})$, for $m = \mu_0 + \cdots + \mu_{r-1} + |\mu_r|$.*
(iii) *$s(V_{(m)}) \leq s(V_{(n)})$ for $m \leq n$.*

Proof. — The first item is immediate from letting $\mu = m\varepsilon_0$ in Theorem 3.4. The third item follows from it directly. For the second item, using $s(V_\mu) = s(V_{\mu'})$ in Theorem 3.4, we may assume $\mu_r \geq 0$. Let us temporarily define a function $A(\mu)$ of a dominant integral weight μ by

$$A(\mu) = \sum_{i=0}^r (\mu_i - i)^2.$$

Again using Theorem 3.4, one finds that the second item is equivalent to the inequality $A(\mu) \leq A(m\varepsilon_0)$. For this, one first proves an inequality

$$(7) \quad (\mu_i - i)^2 + (\mu_j - j)^2 < (\mu_i + 1 - i)^2 + (\mu_j - 1 - j)^2 \quad \text{for } 0 \leq i < j \leq r,$$

which easily follows from $\mu_i \geq \mu_j$. The desired $A(\mu) \leq A(m\varepsilon_0)$ follows from inductively applying the inequality (7) to modify the dominant integral weight μ until it reaches $m\varepsilon_0$. □

Proof of the Main Theorem. — Assume $H^k(X) \neq 0$ for some odd integer k. By Corollary 2.2, there exists at least one component $V_\mu \subset H^*_{\mathrm{odd}}(X)$ with $\mu_0 + \cdots + \mu_{r-1} + |\mu_r| \geq n - \frac{k}{2} + \frac{r}{2}$. Thus, under the condition (2), we get $r \leq k$, and, hence, $b_2 = (2r \text{ or } 2r+1) \leq 2k+1$.

Now assume $H^*_{\mathrm{odd}}(X) = 0$. Among the irreducible components V_μ of the LLV decomposition (1), we always have the Verbitsky component, which as a $\mathfrak{g}$-module is isomorphic to $V_{(n)}$. Thus, if we assume that the condition (2) holds for X, then combining Corollary 3.5 with Proposition 3.2 gives us

$$s(H^*(X)) \leq \max\{s(V_\mu) : \mu \text{ appearing in (1)}\} = s(V_{(n)}) = \frac{8n(b_2+n)}{(b_2+1)(b_2+2)}.$$

On the other hand, we have Salamon's relation $s(H^*(X)) = \frac{n}{3}$ in (6). We conclude

$$s(H^*(X)) = \frac{n}{3} \leq \frac{8n(b_2+n)}{(b_2+1)(b_2+2)},$$

giving the desired bound on b_2 in the main theorem. □

4. Computation of $s(W)$ for irreducible $\mathfrak{g}$-modules

In this section, we prove Theorem 3.4 by using standard representation theoretic methods.

Let us first fix the notation. Here, we simply write $b = b_2(X)$. Let (V, q) be a quadratic space of dimension $b+2$ and $\mathfrak{g} = \mathfrak{so}(V, q)$ be the associated simple Lie algebra of type B_{r+1} / D_{r+1}. We fix a Cartan and a Borel subalgebra of $\mathfrak{g}$, so that the positive and simple roots are well defined. We also use the following notation:

- $\mathfrak{W}$ is the Weyl group of $\mathfrak{g}$.
- R_+ is the set of positive roots of $\mathfrak{g}$.
- For $w \in \mathfrak{W}$, $\ell(w)$ is the length of w. That is, $\ell(w)$ is the minimum length of the decomposition of w into a product of simple reflections $w = s_{\alpha_1} \cdots s_{\alpha_\ell}$, where all α_i are simple roots of $\mathfrak{g}$;
- ρ is the half sum of all the positive roots

$$(8) \qquad \rho = \frac{1}{2} \sum_{\alpha \in R_+} \alpha.$$

Throughout, we consider an irreducible representation $W = V_\mu$ of highest weight μ.

Our proof is inspired by the proof of the Weyl dimension formula (following [4, §8.5]). The Weyl dimension formula is a closed formula computing $\dim V_\mu$, which can be derived from the Weyl character formula.

THEOREM 4.1 (Weyl character formula). — *The formal character of the irreducible $\mathfrak{g}$-module V_μ of highest weight μ can be computed from a formal power series expansion of the rational function*

$$\mathrm{ch}(V_\mu) = \frac{\sum_{w\in\mathfrak{W}}(-1)^{\ell(w)}e^{w.(\mu+\rho)}}{\prod_{\alpha\in R_+}(e^{\alpha/2}-e^{-\alpha/2})}.$$

Due to its importance to our proof of Theorem 3.4, let us review first the proof of Weyl dimension formula. To start with, recall the $\mathfrak{g}$-module V_μ has a weight decomposition $V_\mu = \bigoplus_{\theta\in\Lambda} V_\mu(\theta)$, where Λ is the weight lattice of $\mathfrak{g}$, θ runs through the weights of $\mathfrak{g}$, and $V_\mu(\theta)$ indicates the weight θ subspace of V_μ. The formal character of V_μ is an element in the group algebra $\mathbb{Q}[\Lambda]$ encoding dimensions of the weight subspaces $V_\mu(\theta)$:

$$\mathrm{ch}(V_\mu) = \sum_\theta \dim V_\mu(\theta)\cdot e^\theta \in \mathbb{Q}[\Lambda].$$

Let us introduce a ring homomorphism "projection to ρ-direction"

$$\mathrm{pr}_\rho : \mathbb{Q}[\Lambda] \to \mathbb{Q}[q^{\pm 1}], \qquad e^\theta \mapsto q^{4(\rho,\theta)},$$

where $(\,\cdot\,,\cdot\,)$ is the Killing form of $\mathfrak{g}$, and ρ is defined in (8). Set $f(q) = f_\mu(q) \in \mathbb{Q}[q^{\pm 1}]$ to be the image of the formal character $\mathrm{ch}(V_\mu)$ by the homomorphism pr_ρ:

$$f(q) = \mathrm{pr}_\rho(\mathrm{ch}(V_\mu)) = \sum_\theta \dim V_\mu(\theta)\, q^{4(\rho,\theta)}. \tag{9}$$

Since $\dim V_\mu = \sum_\theta \dim V_\mu(\theta)$, the dimension of V_μ can be recovered from $f(q)$ by

$$\dim V_\mu = f(1). \tag{10}$$

On the other hand, if we apply pr_ρ to the Weyl character formula above, then using Weyl denominator identity (e.g., [4, Thm 8.39]), the Weyl character formula is translated into

$$f(q) = \prod_{\alpha\in R_+} \frac{q^{2(\mu+\rho,\alpha)} - q^{-2(\mu+\rho,\alpha)}}{q^{2(\rho,\alpha)} - q^{-2(\rho,\alpha)}}. \tag{11}$$

The Weyl dimension formula is obtained by computing $f(1) = \lim_{q\to 1} f(q)$ with the aid of (11).

Now let us begin the proof of Theorem 3.4. First, note that for irreducible modules V_μ, we can ignore the sign terms $(-1)^k$ in the definition of $s(V_\mu)$ (i.e., V_μ is either even or odd). Thus, we have

$$s(V_\mu) = \frac{\sum_k k^2 \dim(V_\mu)_k}{\dim V_\mu}.$$

The following lemma expresses $s(V_\mu)$ in terms of $f(q)$, imitating (10) above.

LEMMA 4.2. — *Let $f = f(q)$ be as in (9). Then, $s(V_\mu) = \frac{6}{b(b+1)(b+2)}(\log f)''(1)$.*

Proof. — Consider the derivatives of f

$$f'(q) = \sum_\theta 4(\rho,\theta) \dim V_\mu(\theta)\, q^{4(\rho,\theta)-1},$$
$$f''(q) = \sum_\theta 4(\rho,\theta)(4(\rho,\theta)-1) \dim V_\mu(\theta)\, q^{4(\rho,\theta)-2}.$$

The Weyl symmetry gives us $\dim V_\mu(\theta) = \dim V_\mu(-\theta)$. From it, we obtain $f'(1) = 0$ and

$$f''(1) = 16 \sum_\theta (\rho,\theta)^2 \dim V_\mu(\theta).$$

Let us now specialize the discussion to $\mathfrak{g} = \mathfrak{so}(V,q)$ and use the precise value of ρ. For special orthogonal Lie algebras, one can compute all the positive roots explicitly in terms of our preferred basis ε_i and, hence, obtain the half sum of all the positive roots

$$\rho = \begin{cases} r\varepsilon_0 + (r-1)\varepsilon_1 + \cdots + \varepsilon_{r-1} & \text{when } b = 2r \text{ is even} \\ (r+\frac{1}{2})\varepsilon_0 + (r-\frac{1}{2})\varepsilon_1 + \cdots + \frac{1}{2}\varepsilon_r & \text{when } b = 2r+1 \text{ is odd} \end{cases}. \tag{12}$$

Assume that $b = 2r$ is even. Letting $\theta = \sum_{i=0}^r \theta_i \varepsilon_i$, we have $(\rho,\theta) = \sum_{i=0}^r (r-i)\theta_i$. This gives us

$$f''(1) = 16 \sum_\theta \Big(\sum_{i=0}^r (r-i)^2 \theta_i^2 + 2 \sum_{0 \le i < j \le r} (r-i)(r-j)\theta_i\theta_j \Big) \dim V_\mu(\theta).$$

Again by Weyl symmetry, we have $\dim V_\mu(\theta) = \dim V_\mu(w.\theta)$ for any $w \in \mathfrak{W}$. Note that the Weyl group $\mathfrak{W}$ is, in this case, isomorphic to an order 2 subgroup of $\mathfrak{S}_{r+1} \ltimes (\mathbb{Z}/2)^{\times(r+1)}$, consisting of the elements with an even number of $1 \in \mathbb{Z}/2$. The symmetric group part $\mathfrak{S}_{r+1}$ acts on a weight $\theta = (\theta_0, \ldots, \theta_r)$ by permuting coordinates, and the $(\mathbb{Z}/2)^{\times(r+1)}$ part acts on it by flipping the signs of θ_i's. With these symmetries in mind, one deduces

(1) $\sum_\theta \theta_i^2 \dim V_\mu(\theta) = \sum_\theta \theta_j^2 \dim V_\mu(\theta)$; and
(2) $\sum_\theta \theta_i\theta_j \dim V_\mu(\theta) = 0$ for $i \neq j$.

This finally leads us to the identity

$$\begin{aligned} f''(1) &= 16 \cdot \left(r^2 + (r-1)^2 + \cdots + 1^2\right) \sum_{\theta} \theta_0^2 \dim V_\mu(\theta) \\ &= 16 \cdot \frac{r(r+1)(2r+1)}{6} \sum_k \left(\frac{k}{2}\right)^2 \dim(V_\mu)_k \\ &= \frac{b(b+1)(b+2)}{6} \sum_k k^2 \dim(V_\mu)_k. \end{aligned}$$

Combining it with $f(1) = \dim V_\mu$ and $f'(1) = 0$, we have $(\log f)''(1) = \frac{f''(1)}{f(1)} = \frac{b(b+1)(b+2)}{6} s(V_\mu)$, as claimed.

Next, assume $b = 2r+1$ is odd. A similar argument gives us the computation

$$\begin{aligned} f''(1) &= \frac{(r+1)(2r+1)(2r+3)}{3} \sum_k k^2 \dim(V_\mu)_k \\ &= \frac{b(b+1)(b+2)}{6} \sum_k k^2 \dim(V_\mu)_k. \end{aligned}$$

Hence, the same result follows, regardless of the parity of b. □

The next step is to use the Weyl character formula (11) and compute the value $(\log f)''(1)$.

LEMMA 4.3. — *Let $f = f(q)$ be as in (9). If $\mu_r \geq 0$, then $(\log f)''(1) = \frac{4}{3} b \left[\left(\sum_{i=0}^r \mu_i\right) b + \left(\sum_{i=0}^r \mu_i^2 - 2i\mu_i\right) \right]$.*

Proof. — From the q-polynomial version of the Weyl character formula (11), we derive

$$\log f(q) = \sum_{\alpha \in R_+} \log\left(\frac{q^{2(\mu+\rho,\alpha)} - q^{-2(\mu+\rho,\alpha)}}{q-1}\right) - \log\left(\frac{q^{2(\rho,\alpha)} - q^{-2(\rho,\alpha)}}{q-1}\right).$$

Here, $q-1$ on the denominators are inserted to make each log terms well-defined in the neighborhood of $q = 1$. Note that $(\log f)''(1)$ is twice the coefficient of the term $(q-1)^2$ in the Taylor series of $\log f$. For a general *positive integer* a, the Taylor series expansion of $\log\left(\frac{q^a - q^{-a}}{q-1}\right)$ at $q = 1$ is

$$\log\left(\frac{q^a - q^{-a}}{q-1}\right) = \log(2a) - \frac{1}{2}(q-1) + \frac{1}{24}(4a^2+5)(q-1)^2 + \cdots,$$

which has a degree 2 coefficient $\frac{1}{24}(4a^2+5)$. Since $2(\mu+\rho,\alpha)$ and $2(\rho,\alpha)$ are both positive integers for any $\alpha \in R_+$ (N.B. Here we used the fact $\mu_r \geq 0$), we

conclude

$$(\log f)''(1) = 2\sum_{\alpha\in R_+}\frac{1}{24}\big(16(\mu+\rho,\alpha)^2+5\big) - \frac{1}{24}\big(16(\rho,\alpha)^2+5\big)$$
$$= \frac{4}{3}\sum_{\alpha\in R_+}(\mu+\rho,\alpha)^2-(\rho,\alpha)^2.$$

Recalling (12), let us get into an explicit computation for $\mathfrak{g} = \mathfrak{so}(V,q)$. Assume that $b = 2r$ is even. The positive roots are $R_+ = \{\varepsilon_i \pm \varepsilon_j : 0 \le i < j \le r\}$. We get

$$\sum_{\alpha\in R_+}(\mu+\rho,\alpha)^2-(\rho,\alpha)^2$$
$$= \sum_{0\le i<j\le r}(\mu_i-\mu_j)^2+2(\mu_i-\mu_j)(j-i)+(\mu_i+\mu_j)^2+2(\mu_i+\mu_j)(2r-i-j)$$
$$= \sum_{0\le i<j\le r}\Big[2(\mu_i^2+\mu_j^2)+4r(\mu_i+\mu_j)-(i\mu_i+j\mu_j)\Big]$$
$$= 2r\Big[2r\sum_{i=0}^r\mu_i+\sum_{i=0}^r(\mu_i^2-2i\mu_i)\Big] = b\Big[\Big(\sum_{i=0}^r\mu_i\Big)b+\Big(\sum_{i=0}^r\mu_i^2-2i\mu_i\Big)\Big].$$

This proves the result in this case.

Similarly, for $b = 2r+1$ odd, the positive roots are $R_+ = \{\varepsilon_i : 0 \le i \le r\} \cup \{\varepsilon_i \pm \varepsilon_j : 0 \le i < j \le r\}$, giving:

$$\sum_{\alpha\in R_+}(\mu+\rho,\alpha)^2-(\rho,\alpha)^2$$
$$= \sum_{0\le i<j\le r}(\mu_i-\mu_j)^2+2(\mu_i-\mu_j)(j-i)+(\mu_i+\mu_j)^2 + 2(\mu_i+\mu_j)(2r+1-i-j)$$
$$+\sum_{i=0}^r\mu_i^2+2\mu_i(r+\tfrac{1}{2}-i)$$
$$= \sum_{0\le i<j\le r}\Big[2(\mu_i^2+\mu_j^2)+(4r+2)(\mu_i+\mu_j)-(i\mu_i+j\mu_j)\Big]$$
$$+\sum_{i=0}^r\mu_i^2+(2r+1)\mu_i-2i\mu_i$$
$$= (2r+1)\Big[(2r+1)\sum_{i=0}^r\mu_i+\sum_{i=0}^r(\mu_i^2-2i\mu_i)\Big]$$
$$= b\Big[\Big(\sum_{i=0}^r\mu_i\Big)b+\Big(\sum_{i=0}^r\mu_i^2-2i\mu_i\Big)\Big].$$

This completes the proof of the lemma. □

Proof of Theorem 3.4. — Combining Lemma 4.2 and 4.3, the theorem follows for the case $\mu_r \geq 0$. Now assume that $b_2 = 2r$ is even and $\mu_r < 0$. In this case, ρ does not have the ε_r-coordinate by (12). Hence, the Weyl character formula (Theorem 4.1) implies that the weights associated to V_μ and $V_{\mu'}$ are bijective via the action $(\theta_0, \ldots, \theta_{r-1}, \theta_r) \mapsto (\theta_0, \ldots, \theta_{r-1}, -\theta_r)$. By definition, the constant $s(W)$ captures only the h-eigenspaces, i.e., only the ε_0-coordinates of the weights associated to W. This means that $s(V_\mu) = s(V_{\mu'})$. □

BIBLIOGRAPHY

[1] M. Green, Y. Kim, R. Laza & C. Robles – "The LLV decomposition of hyper-Kähler cohomology", arXiv:1906.03432, 2019.

[2] D. Guan – "On the Betti numbers of irreducible compact hyperkähler manifolds of complex dimension four", *Math. Res. Lett.* **8** (2001), no. 5-6, p. 663–669.

[3] D. Huybrechts – "Finiteness results for compact hyperkähler manifolds", *J. Reine Angew. Math.* **558** (2003), p. 15–22.

[4] A. A. Kirillov – *An introduction to Lie groups and Lie algebras*, vol. 113, Cambridge University Press, 2008.

[5] N. Kurnosov – "Boundness of b_2 for hyperkähler manifolds with vanishing odd-Betti numbers", arXiv:1511.02838, 2015.

[6] E. Looijenga & V. A. Lunts – "A Lie algebra attached to a projective variety", *Invent. Math.* **129** (1997), no. 2, p. 361–412.

[7] S. M. Salamon – "On the cohomology of Kähler and hyper-Kähler manifolds", *Topology* **35** (1996), no. 1, p. 137–155.

[8] J. Sawon – "A bound on the second Betti number of hyperkähler manifolds of complex dimension six", arXiv:1511.09105, 2015.

[9] M. Verbitsky – "Cohomology of compact hyperkähler manifolds", Ph.D. thesis, Harvard University, 1995.

Bull. Soc. Math. France
148 (3), 2020, p. 481-514

CHARACTERISATION OF THE POLES OF THE ℓ-MODULAR ASAI L-FACTOR

BY ROBERT KURINCZUK & NADIR MATRINGE

ABSTRACT. — Let $\mathrm{F}/\mathrm{F}_\mathfrak{o}$ be a quadratic extension of non-archimedean local fields of odd residual characteristic, set $\mathrm{G} = \mathrm{GL}_n(F)$, $\mathrm{G}_\mathfrak{o} = \mathrm{GL}_n(\mathrm{F}_\mathfrak{o})$ and let ℓ be a prime number different from the residual characteristic of F. For a complex cuspidal representation π of G, the Asai L-factor $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi)$ has a pole at $\mathrm{X} = 1$, if and only if π is $\mathrm{G}_\mathfrak{o}$-distinguished. In this paper, we solve the problem of characterising the occurrence of a pole at $\mathrm{X} = 1$ of $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi)$ when π is an ℓ-modular cuspidal representation of G; we show that $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi)$ has a pole at $\mathrm{X} = 1$, if and only if π is a *relatively banal* distinguished representation, namely π is $\mathrm{G}_\mathfrak{o}$-distinguished but not $|\det(\ )|_{\mathrm{F}_\mathfrak{o}}$-distinguished. This notion turns out to be an exact analogue for the symmetric space $\mathrm{G}/\mathrm{G}_\mathfrak{o}$ of Mínguez and Sécherre's notion of banal cuspidal $\overline{\mathbb{F}_\ell}$-representation of $\mathrm{G}_\mathfrak{o}$. Along the way, we compute the Asai L-factor of all cuspidal ℓ-modular representations of G in terms of type theory and prove new results concerning lifting and reduction modulo ℓ of distinguished cuspidal representations. Finally, we determine when the natural $\mathrm{G}_\mathfrak{o}$-period on the Whittaker model of a distinguished cuspidal representation of G is non-zero.

Texte reçu le 25 juillet 2018, accepté le 26 février 2020.

ROBERT KURINCZUK, Department of Mathematics, Imperial College, London, SW7 2AZ, United Kingdom • *E-mail :* robkurinczuk@gmail.com
NADIR MATRINGE, Université de Poitiers, Laboratoire de Mathématiques et Applications, Téléport 2 - BP 30179, Boulevard Marie et Pierre Curie, 86962, Futuroscope Chasseneuil Cedex. France • *E-mail :* nadir.matringe@math.univ-poitiers.fr

Mathematical subject classification (2010). — 22E50, 11F70, 11F66.

Key words and phrases. — Asai L-factor, Distinguished representations of p-adic groups, Modular representations of p-adic groups.

This work has benefited from support from GDRI *Representation Theory* 2016–2020 and the EPSRC grant EP/R009279/1, and the Heilbronn Institute for Mathematical Research.

© Société Mathématique de France
0037-9484/2020/481/$ 5.00
doi:10.24033/bsmf.2814

RÉSUMÉ (*Caractérisation des pôles du facteur d'Asai ℓ-modulaire*). — Soit $\mathrm{F}/\mathrm{F}_\mathfrak{o}$ une extension quadratique de corps locaux non archimédiens de caractéristique résiduelle impaire. Posons $\mathrm{G} = \mathrm{GL}_n(F)$, $\mathrm{G}_\mathfrak{o} = \mathrm{GL}_n(\mathrm{F}_\mathfrak{o})$ et soit ℓ un nombre premier différent de la caractéristique résiduelle de F. Pour une représentation cuspidale complexe π de G, le facteur L d'Asai $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi)$ admet un pôle en $\mathrm{X} = 1$ si et seulement si π est $\mathrm{G}_\mathfrak{o}$-distinguée. Dans cet article nous résolvons le problème de l'occurence d'un pôle en $\mathrm{X} = 1$ de $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi)$ quand π est une représentation cuspidale ℓ-modulaire de G: dans ce cas $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi)$ admet un pôle en $\mathrm{X} = 1$ si et seulement si π est *relativement banale* distinguée; autrement dit π est $\mathrm{G}_\mathfrak{o}$-distinguée mais pas $|\det(\ )|_{\mathrm{F}_\mathfrak{o}}$-distinguée. Cette notion est l'analogue pour l'espace symétrique $\mathrm{G}/\mathrm{G}_\mathfrak{o}$ de la notion de cuspidale banale introduite par Mínguez et Sécherre pour les $\overline{\mathbb{F}_\ell}$-représentations de $\mathrm{G}_\mathfrak{o}$. En cours de route, on calcule le facteur L d'Asai des représentations cuspidales ℓ-modulaires de G par la théorie des types, et on prouve de nouveaux résultats concernant le relèvement et la réduction modulo ℓ des représentations cuspidales distinguées. Finalement, on détermine quand la $\mathrm{G}_\mathfrak{o}$-période sur le modèle de Whittaker d'une représentation cuspidale distinguée de G est non nulle.

1. Introduction

Let $\mathrm{F}/\mathrm{F}_\mathfrak{o}$ be a quadratic extension of non-archimedean local fields of residual characteristic $p \neq 2$ and set $\mathrm{G} = \mathrm{GL}_n(\mathrm{F})$ and $\mathrm{G}_\mathfrak{o} = \mathrm{GL}_n(\mathrm{F}_\mathfrak{o})$. An irreducible representation of G is said to be *distinguished by* $\mathrm{G}_\mathfrak{o}$, if it possesses a non-zero $\mathrm{G}_\mathfrak{o}$-invariant linear form. In the case of complex representations, the equality of the Asai L-factor defined by the Rankin–Selberg method and its Galois avatar ([3], [21]) provides a bridge between functorial lifting from the quasi-split unitary group $\mathrm{U}_n(\mathrm{F}/\mathrm{F}_\mathfrak{o})$ and $\mathrm{G}_\mathfrak{o}$-distinction of discrete series representations of G; a discrete series of G is a (stable or unstable depending on the parity of n) lift of a (necessarily discrete series) representation of $\mathrm{U}_n(\mathrm{F}/\mathrm{F}_\mathfrak{o})$, if and only if the Asai L-factor of its Galois parameter has a pole at $\mathrm{X} = 1$ ([25], [10]), whereas it is $\mathrm{G}_\mathfrak{o}$-distinguished, if and only if its Asai L-factor obtained by the Rankin–Selberg method has a pole at $\mathrm{X} = 1$ ([14], [1]).

Recently, motivated by the study of congruences between automorphic representations, there has been great interest in studying representations of G on vector spaces over fields of positive characteristic ℓ. There are two very different cases: when $\ell = p$ and when $\ell \neq p$. This article focuses on the latter $\ell \neq p$ case, where there is a theory of Haar measure that allows us to define Asai L-factors via the Rankin–Selberg method as in the complex case (Section 7).

The aim of this article is to show that in this case, a connection remains between the poles of Asai L-factor and distinction; however, this connection no longer characterises distinction, but a more subtle notion, which we call a *relatively banal* distinction. The easiest way to state that a cuspidal distinguished ℓ-modular representation is relatively banal is to say that it is not $|\det(\ \cdot\ )|_{\mathrm{F}_\mathfrak{o}}$-distinguished, where $|\det(\ \cdot\ )|_{\mathrm{F}_\mathfrak{o}}$ is considered as an $\overline{\mathbb{F}_\ell}$-valued character, but other compact definitions can also be given in terms of type theory, as well as in terms of its supercuspidal lifts:

PROPOSITION 1.1 (Definition 6.2, Theorem 6.11 and Corollary 6.3). — *Let π be an ℓ-modular cuspidal distinguished representation of* G*. Then, the following are equivalent, and when they are satisfied, we say that π is* relatively banal*:*

(i) *π is not $|\det(\ \cdot\ )|_{\mathrm{F_o}}$-distinguished.*
(ii) *All supercuspidal lifts of π are distinguished by an unramified character of $\mathrm{G_o}$.*
(iii) *$q_{\mathrm{o}}^{n/e_{\mathrm{o}}(\pi)} \not\equiv 1[\ell]$, where $e_{\mathrm{o}}(\pi)$ denotes the invariant associated to π in* [4, Lemma 5.10] *(see Section 5.2).*

Relatively banal for $\mathrm{G_o}$-distinguished cuspidal representations turns out to be the exact analogue of the definition of *banal cuspidal representations* of $\mathrm{G_o}$ (see [24, Remark 8.15] and [23]) after one identifies the cuspidal (irreducible) representations of $\mathrm{G_o}$ with the $\Delta(\mathrm{G_o})$-distinguished cuspidal (irreducible) representations of $\mathrm{G_o} \times \mathrm{G_o}$, where $\Delta : \mathrm{G_o} \to \mathrm{G_o} \times \mathrm{G_o}$ is the diagonal embedding, as we explain in Section 8.3.

The main theorem of this paper characterises the poles of the Asai L-factor:

THEOREM 1.2 (Theorem 8.1). — *Let π be a cuspidal ℓ-modular representation, then $\mathrm{L_{As}}(\mathrm{X}, \pi)$ has a pole at $\mathrm{X} = 1$, if and only if π is relatively banal distinguished.*

Note that the proof of the above theorem is completely different from the proof of characterisation theorem in the complex case (see Remark 8.2 for more on the comparison of the proofs). Here, we show that the Asai L-factor of a cuspidal ℓ-modular representation is equal to 1 whenever π is not the unramified twist of a relatively banal representation using Theorem 6.11, which is the characterisation of relatively banal in terms of supercuspidal lifts. Then, when π is the unramified twist of relatively banal representation, following our paper [18], we get an explicit formula for $\mathrm{L_{As}}(\mathrm{X}, \pi)$ in Theorem 7.8 from the test vector computation of [4], which due to the relatively banal assumption (more precisely its type theory version) reduces modulo ℓ without vanishing. We then deduce Theorem 1.2 from this computation, together with the computation of the group of unramified characters μ of $\mathrm{G_o}$, such that π is μ-distinguished (Corollary 5.17).

Finally, denoting by N the unipotent radical of the group of upper triangular matrices in G, by $\mathrm{Z_o}$ the centre of $\mathrm{G_o}$ and by $\mathrm{N_o}$ the group $\mathrm{N} \cap \mathrm{G_o}$, the most natural $\mathrm{G_o}$-invariant linear form to consider on the Whittaker model of an ℓ-modular cuspidal representation π with respect to a distinguished non-degenerate character of N trivial on $\mathrm{N_o}$ is the local period

$$\mathcal{L}_\pi : \mathrm{W} \mapsto \int_{\mathrm{Z_o N_o} \backslash \mathrm{G_o}} \mathrm{W}(h) dh.$$

In fact, this period plays an essential role in the proof of Theorem 1.2 over the field of complex numbers (see Remark 8.2). One of the main differences in the

ℓ-modular setting is that $\mathcal{L}_\pi$ can be zero even when π is distinguished. Not only do we show that it can vanish but we say exactly when it vanishes:

THEOREM 1.3 (Theorem 8.3). — *Let π be a cuspidal distinguished ℓ-modular representation of $\mathrm{GL}_n(\mathrm{F})$. Then, the local period $\mathcal{L}_\pi$ is non-zero, if and only if the following two properties are satisfied:*

(i) *π is relatively banal.*
(ii) *ℓ does not divide $e_{\mathfrak{o}}(\pi)$; in other words, if $\widetilde{\pi}$ is a lift of π, the ℓ-adic valuation of n is the same as the ℓ-adic valuation of the number of ℓ-adic unramified characters $\widetilde{\mu}_{\mathfrak{o}}$ of $\mathrm{G}_{\mathfrak{o}}$, such that $\widetilde{\pi}$ is $\widetilde{\mu}_{\mathfrak{o}}$-distinguished.*

This theorem is related to the vanishing modulo ℓ of a rather interesting and subtle scalar related, after fixing an isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}_\ell}$, to a quotient of the formal degree of a complex cuspidal representation of a unitary group by the formal degree of its base change to $\mathrm{GL}_n(\mathrm{F})$, see Remark 8.4 for a precise statement.

In light of Theorem 1.2, the role of the Asai L-factor in the study of distinguished representations will be less important in the ℓ-modular setting, as some ℓ-modular distinguished representations have Asai L-factors equal to 1 in the cuspidal case already, and new ideas will be required already for non-relatively banal distinguished cuspidal representations. We will focus on the general case of distinguished irreducible ℓ-modular representations, restricting it to small rank in the paper [19].

Finally, we mention that this paper relies heavily on the results from [4] and [27] and can be seen as a natural continuation of the themes developed in these two papers. In particular, our section on lifting distinction for cuspidal representations of finite general linear groups uses the same techniques as [27], and the statements that we obtain here were known to the author of [27].

2. Notation

Let $\mathrm{F}/\mathrm{F}_{\mathfrak{o}}$ be a quadratic extension of non-archimedean local fields of odd residual characteristic p. For any finite extension $\mathrm{E}/\mathrm{F}_{\mathfrak{o}}$, we let $|\ |_{\mathrm{E}}$ be the absolute value, $\mathrm{val}_{\mathrm{E}}$ the additive valuation, $\mathscr{O}_{\mathrm{E}}$ denote the ring of integers of E, with maximal ideal $\mathscr{P}_{\mathrm{E}}$, residue field k_{E}, and put $q_{\mathrm{E}} = \#\mathrm{k}_{\mathrm{E}}$. We put $|\ | = |\ |_{\mathrm{F}}$, $\mathrm{val} = \mathrm{val}_{\mathrm{F}}$, $\mathscr{O} = \mathscr{O}_{\mathrm{F}}$, $\mathscr{P} = \mathscr{P}_{\mathrm{F}}$, $\mathrm{k} = \mathrm{k}_{\mathrm{F}}$, $q = q_{\mathrm{F}}$, $|\ |_{\mathfrak{o}} = |\ |_{\mathrm{F}_{\mathfrak{o}}}$, $\mathrm{val}_{\mathfrak{o}} = \mathrm{val}_{\mathrm{F}_{\mathfrak{o}}}$, $\mathscr{O}_{\mathfrak{o}} = \mathscr{O}_{\mathrm{F}_{\mathfrak{o}}}$, $\mathscr{P}_{\mathfrak{o}} = \mathscr{P}_{\mathrm{F}_{\mathfrak{o}}}$, $\mathrm{k}_{\mathfrak{o}} = \mathrm{k}_{\mathrm{F}_{\mathfrak{o}}}$ and $q_{\mathfrak{o}} = q_{\mathrm{F}_{\mathfrak{o}}}$.

We let ℓ denote a prime not equal to p. Set $\overline{\mathbb{Q}_\ell}$ to be an algebraic closure of the ℓ-adic numbers, $\overline{\mathbb{Z}_\ell}$ its ring of integers, and $\overline{\mathbb{F}_\ell}$ its residue field.

Let G be the F-points of a connected reductive group defined over F and $\mathcal{G}$ be the k-points of a connected reductive group defined over k.

All representations considered are assumed to be smooth. We consider representations of G and $\mathcal{G}$ and their subgroups on $\overline{\mathbb{Q}_\ell}$ and $\overline{\mathbb{F}_\ell}$-vector spaces and

the relations between them. We let R denote either $\overline{\mathbb{Q}_\ell}$ or $\overline{\mathbb{F}_\ell}$, so that we can make statements valid in both cases more briefly. By an R-representation we mean a representation on an R-vector space.

An R-representation of G or $\mathcal{G}$ is called *cuspidal*, if it is irreducible and does not appear as a quotient of any representation parabolically induced from an irreducible representation of a proper Levi subgroup. It is called *supercuspidal*, if it is irreducible and does not appear as a subquotient of any representation parabolically induced from an irreducible representation of a proper Levi subgroup. Over $\overline{\mathbb{Q}_\ell}$ a representation of G or $\mathcal{G}$ is cuspidal, if and only if it is supercuspidal; however, this is not the case over $\overline{\mathbb{F}_\ell}$, see [28, III] and [16] for examples of cuspidal non-supercuspidal representations.

3. Background on integral representations and distinction

DEFINITION 3.1. — Let G be a locally profinite group and H be a closed subgroup of G. Let π be an R-representation of G and $\chi : \mathrm{H} \to \mathrm{R}^\times$ be a character. We say that π is *χ-distinguished*, if $\mathrm{Hom}_\mathrm{H}(\pi, \chi) \neq 0$. We say that π is *distinguished*, if it is 1-distinguished where 1 denotes the trivial character of H.

We will mainly consider cases where H is the group of fixed points $\mathrm{G}^\sigma = \{g \in \mathrm{G} : \sigma(g) = g\}$ of an involution σ. In this case, for any subset $\mathrm{X} \subset \mathrm{G}$, we set $\mathrm{X}^\sigma = \mathrm{X} \cap \mathrm{G}^\sigma$.

DEFINITION 3.2. — We call a triple $(\mathrm{G}, \mathrm{H}, \sigma)$ *an* F*-symmetric pair* when

(i) $\mathrm{G} = \mathbb{G}(\mathrm{F})$ with $\mathbb{G}$ a connected reductive group defined over F, and σ is an involution of $\mathbb{G}$ defined over F.
(ii) H is an open subgroup of the group G^σ.

The main symmetric pair of interest in this note will be $(\mathrm{GL}_n(\mathrm{F}), \mathrm{GL}_n(\mathrm{F}_\mathrm{o}), \sigma)$, where σ is the involution induced from the non-trivial element of $\mathrm{Gal}(\mathrm{F}/\mathrm{F}_\mathrm{o})$. Two important basic results concerning this pair, which we shall use later, are the following ([9], [26] for $\overline{\mathbb{Q}_\ell}$-representations, extended to R-representations in [27, Theorem 3.1]):

PROPOSITION 3.3. — *Let π be an irreducible* R*-representation of* $\mathrm{GL}_n(\mathrm{F})$*, then*

$$\dim(\mathrm{Hom}_{\mathrm{GL}_n(\mathrm{F}_\mathrm{o})}(\pi, \mathrm{R})) \leqslant 1.$$

Moreover, if this dimension is equal to 1, then $\pi^\vee \simeq \pi^\sigma$.

Let K be a locally profinite group. An irreducible $\overline{\mathbb{Q}_\ell}$-representation π of K is called *integral*, if it stabilises a $\overline{\mathbb{Z}_\ell}$-lattice in its vector space. An integral irreducible $\overline{\mathbb{Q}_\ell}$-representation π that stabilises a lattice L induces an $\overline{\mathbb{F}_\ell}$-representation on the space $\mathrm{L} \otimes_{\overline{\mathbb{Z}_\ell}} \overline{\mathbb{F}_\ell}$. When K is either a profinite group or the F-points of a connected reductive F-group, the semi-simplification $r_\ell(\pi) =$ of

$L \otimes_{\overline{\mathbb{Z}_\ell}} \overline{\mathbb{F}_\ell}$ is independent of the choice of L and is called the *reduction modulo* ℓ of π ([28, 9.6] in the profinite setting, where all representations are automatically defined over a finite extension of $\overline{\mathbb{F}_\ell}$, or [30, Theorem 1] in the context of reductive groups). Given an irreducible $\overline{\mathbb{F}_\ell}$-representation $\overline{\pi}$ of K, we will call any integral irreducible $\overline{\mathbb{Q}_\ell}$-representation π of K that satisfies $r_\ell(\pi) = \overline{\pi}$ a *lift* of $\overline{\pi}$.

We shall see later that the distinction of cuspidal representations of G does not always lift, i.e. that an ℓ-modular cuspidal distinguished representation may have no distinguished lifts. However, we have the following general result, which shows that distinction reduces modulo ℓ:

THEOREM 3.4. — *Let* (G, H, σ) *be an* F*-symmetric pair. Let* π *be an integral* ℓ*-adic supercuspidal representation of* G *and let* χ *be an integral character of* H*. Then, if* π *is* χ*-distinguished, the representation* $r_\ell(\pi)$ *is* $r_\ell(\chi)$*-distinguished.*

Proof. — Note that χ coincides with the central character of π restricted to H, which is also integral on $Z_G \cap H$ (where Z_G is the centre of G), and, hence, we extend it to a character still denoted χ to $Z_G H$: $\chi(zh) = c_\pi(z)\chi(h)$. Note that $\mathrm{Hom}_H(\pi, \chi) = \mathrm{Hom}_{Z_G H}(\pi, \chi)$. By [15, Proposition 8.1] for $\chi = 1$, extended to general χ in [8, Theorem 4.4], for L a non-zero element of $\mathrm{Hom}_H(\pi, \chi)$, the map

$$v \mapsto (g \mapsto L(\pi(g)v))$$

embeds π as a submodule of $\mathrm{ind}_{Z_G H}^G(\chi)$. Now, by [30, Proposition II.3], $\mathrm{ind}_{Z_G H}^G(\chi, \overline{\mathbb{Z}_\ell})$ is an integral structure in $\mathrm{ind}_{Z_G H}^G(\chi)$, and, hence, its intersection π_e with π is an integral structure of π by [28, 9.3] (note that Vignéras works over a finite extension of $\overline{\mathbb{F}_\ell}$, but her results apply here because both π and χ, and, hence, both π and $\mathrm{ind}_{Z_G H}^G(\chi)$ have E-structures by [28, Section 4]). So, $\pi_e \subset \mathrm{ind}_{Z_G H}^G(\chi, \overline{\mathbb{Z}_\ell})$, but the map $\Lambda : f \mapsto f(1_G)$ is an element of $\mathrm{Hom}_H(\mathrm{ind}_{Z_G H}^G(\chi, \overline{\mathbb{Z}_\ell}), \chi)$, which is non-zero on any submodule of $\mathrm{ind}_{Z_G H}^G(\chi, \overline{\mathbb{Z}_\ell})$, in particular on π_e. Up to multiplying Λ by an appropriate non-zero scalar in $\overline{\mathbb{Q}_\ell}$, we can suppose that $\Lambda(\pi_e) = \overline{\mathbb{Z}_\ell}$, and Λ induces a non-zero element of $\mathrm{Hom}_H(\pi_e \otimes \overline{\mathbb{F}_\ell}, r_\ell(\chi))$. The result follows. □

REMARK 3.5. — If K′ is a closed subgroup of a profinite group K, (smooth) finite dimensional $\overline{\mathbb{Q}_\ell}$-representations of K are always integral and the image of a lattice by a non-zero linear form on such a representation is obviously a lattice of $\overline{\mathbb{Q}_\ell}$, so the reduction modulo ℓ of a (K', χ)-distinguished finite-dimensional $\overline{\mathbb{Q}_\ell}$-representation of K is $(K', r_\ell(\chi))$-distinguished.

REMARK 3.6. — The following observation sheds more light on Theorem 3.4 when $G = GL_n(F)$. Let π be an integral supercuspidal $\overline{\mathbb{Q}_\ell}$-representation of $GL_n(F)$, then its reduction modulo ℓ is (irreducible and) cuspidal, by [28,

III 4.25]. This, however, is not true in general, see [16] for an example of an integral supercuspidal $\overline{\mathbb{Q}_\ell}$-representation whose reduction modulo ℓ is reducible.

Let K be a locally profinite group and K′ a closed subgroup. While, in general, it appears to be a subtle question to ascertain when the distinction of $\overline{\mathbb{F}_\ell}$-representations of K lifts, there is, however, one elementary case where it does: when the subgroup for which we want to study distinction K′ is profinite of pro-order prime to ℓ. In this case, an ℓ-modular finite dimensional (smooth) representation of K′ is semi-simple, and reduction modulo ℓ defines a bijection between the set of isomorphism classes of integral irreducible $\overline{\mathbb{Q}_\ell}$-representations of K′ and the set of isomorphism classes irreducible $\overline{\mathbb{F}_\ell}$-representations of K′, and we have:

LEMMA 3.7. — *Let* K *be a locally profinite group and* K′ *be a compact subgroup of* K. *Suppose that the pro-order of* K′ *is prime to* ℓ. *Let* ρ *be an finite-dimensional integral* $\overline{\mathbb{Q}_\ell}$*-representation of* K *and* χ *be a character of* K′. *Then,* ρ *is* χ*-distinguished, if and only if* $r_\ell(\rho)$ *is* $r_\ell(\chi)$*-distinguished.*

REMARK 3.8. — If K is compact modulo centre, an irreducible $\overline{\mathbb{Q}_\ell}$-representation of K is always finite-dimensional and is integral, if and only if its central character is integral.

4. Distinction for finite GL_n

For the rest of this section, we set $\mathcal{G} = \mathrm{GL}_n(\mathrm{k})$, where (as before) k denotes a finite field of odd cardinality q. If $\mathrm{k}/\mathrm{k}_\mathfrak{o}$ is a quadratic extension of $\mathrm{k}_\mathfrak{o}$, we denote by σ the non-trivial element of $\mathrm{Gal}(\mathrm{k}/\mathrm{k}_\mathfrak{o})$ and set $\mathcal{G}_\mathfrak{o} = \mathrm{GL}_n(\mathrm{k}_\mathfrak{o})$.

We recall the definitions of self-dual and σ-self-dual representations of $\mathcal{G}$:

DEFINITION 4.1. — (i) Suppose $\mathrm{k}/\mathrm{k}_\mathfrak{o}$ is a quadratic extension of finite fields, then a representation ρ of $\mathcal{G}$, over $\overline{\mathbb{Q}_\ell}$ or $\overline{\mathbb{F}_\ell}$, is called *$\sigma$-self-dual*, if $\rho^\sigma \simeq \rho^\vee$.

(ii) A representation ρ of $\mathcal{G}$, over $\overline{\mathbb{Q}_\ell}$ or $\overline{\mathbb{F}_\ell}$, is called *self-dual* if $\rho \simeq \rho^\vee$.

4.1. Basic results on distinction. — The following multiplicity one results are [27, Remark 3.2 with the adhoc modification in the proof of Theorem 3.1, Proposition 6.10 and Remark 6.11]:

PROPOSITION 4.2. — *Let* ρ *be an irreducible* R*-representation of* $\mathcal{G}$*:*

(i) *If* $\mathrm{k}/\mathrm{k}_\mathfrak{o}$ *is a quadratic extension of finite fields, then or any character* χ *of* $\mathcal{G}_\mathfrak{o}$, $\dim(\mathrm{Hom}_{\mathcal{G}_\mathfrak{o}}(\rho, \chi)) \leq 1$.

(ii) *If* ρ *is cuspidal, and* r *and* s *are two non-negative integers such that* $r + s = n \geq 2$. *Then,* $\dim(\mathrm{Hom}_{(\mathrm{GL}_r \times \mathrm{GL}_s)(\mathrm{k})}(\rho, \chi)) \leq 1$ *for any character* χ *of* $\mathrm{GL}_r \times \mathrm{GL}_s$, *and this dimension is equal to zero if* r *and* s *are positive, and* $r \neq s$.

The final goal of this section is to understand when a cuspidal $\overline{\mathbb{F}_\ell}$-representation of a finite general linear group that is distinguished by a maximal Levi subgroup or by a Galois involution has a lift that does not share the same distinction property.

The connection between (σ)-self-dual representations and distinction comes from:

LEMMA 4.3. — (i) *A* $\mathrm{GL}_n(\mathrm{k}_\mathfrak{o})$*-distinguished irreducible* R*-representation of* $\mathrm{GL}_n(\mathrm{k})$ *is* σ*-self-dual. Moreover, if* ρ *is supercuspidal, we have an equivalence:* ρ *is* σ *self-dual, if and only if it is* $\mathrm{GL}_n(\mathrm{k}_\mathfrak{o})$*-distinguished.*

(ii) *A supercuspidal representation of* $\mathrm{GL}_n(\mathrm{k})$ *is self-dual, if and only if either* $n = 1$*, and it a quadratic character, or if* n *is even, and it is* $(\mathrm{GL}_{n/2} \times \mathrm{GL}_{n/2})(\mathrm{k})$*-distinguished.*

Proof. — The first assertion of (i) follows from [27, Remark 3.2] and the second from [27, Lemma 8.3]. The second assertion follows from [27, Lemmas 7.1 and 7.3]. □

4.2. Self-dual and σ-self-dual cuspidal representations via the Green–Dipper–James parametrisation. — In this subsection, either k is an arbitrary finite field, and we consider self-dual representations of $\mathrm{GL}_n(\mathrm{k})$, or $\mathrm{k}/\mathrm{k}_\mathfrak{o}$ is quadratic, and we consider σ-self-dual representations of $\mathrm{GL}_n(\mathrm{k})$ where $\langle\sigma\rangle = \mathrm{Gal}(\mathrm{k}/\mathrm{k}_\mathfrak{o})$.

Let l/k be a degree n extension of k. A character $\theta : \mathrm{l}^\times \to \overline{\mathbb{Q}_\ell}^\times$ is called k-*regular*, if $\#\{\theta^\tau : \tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})\} = n$, i.e. the orbit of θ under $\mathrm{Gal}(\mathrm{l}/\mathrm{k})$ has maximal size. According to [11], there is a surjective map

$$\begin{aligned}&\{\text{k-regular characters of } \mathrm{l}^\times \to \overline{\mathbb{Q}_\ell}^\times\}\\ &\quad\to \{\text{supercuspidal } \overline{\mathbb{Q}_\ell}\text{-representations of } \mathcal{G}\}/\simeq\\ &\theta \mapsto \rho(\theta).\end{aligned}$$

The character formula given in [11] also implies:

(i) Two such cuspidal representations $\rho(\theta)$ and $\rho(\theta')$ are isomorphic, if and only if there exists $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$ such that $\theta' = \theta^\tau$.
(ii) The dual $\rho(\theta)^\vee$ is isomorphic to $\rho(\theta^{-1})$.
(iii) If k/k' is a finite extension and $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k}')$, we have $\rho(\theta^\tau) \simeq \rho(\theta)^\tau$.

The following is well known, and a similar proof to ours can be found in [27, Lemmas 7.1 & 8.1]. In the greater generality of supercuspidal R-representations, we provide a proof as a warm-up:

LEMMA 4.4. — (i) *If there exists a* σ*-self-dual supercuspidal* $\overline{\mathbb{Q}_\ell}$*-representation of* $\mathcal{G}$*, then* n *is odd.*

(ii) *If there exists a self-dual supercuspidal* $\overline{\mathbb{Q}_\ell}$*-representation of* $\mathcal{G}$*, then* n *is either 1 or even.*

Proof. — (i) Suppose that ρ is a σ-self-dual cuspidal $\overline{\mathbb{Q}_\ell}$-representation and write $\rho = \rho(\theta)$ for a k-regular character θ. Choose an extension of σ to $\widetilde{\sigma} \in \mathrm{Gal}(\mathrm{l}/\mathrm{k}_\mathrm{o})$. Then, as $\rho(\theta^{-1}) \simeq \rho(\theta)^\vee \simeq \rho(\theta)^\sigma$, necessarily $\theta^{\widetilde{\sigma}} = (\theta^{-1})^\tau$, for some $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$. Hence, $(\tau^{-1} \circ \widetilde{\sigma})^2$ fixes θ, so it is 1, as θ is regular. This implies that $\tau^{-1} \circ \widetilde{\sigma}$ is a k_o-linear involution of l, which extends σ. However, the cyclic group $\mathrm{Gal}(\mathrm{l}/\mathrm{k}_\mathrm{o})$ contains a unique element of order 2. If n were even, $\tau^{-1} \circ \widetilde{\sigma}$ would belong to $\mathrm{Gal}(\mathrm{l}/\mathrm{k})$, and this is absurd, as it extends σ, which is not k-linear.

(ii) Suppose that ρ is a self-dual cuspidal $\overline{\mathbb{Q}_\ell}$-representation and write $\rho = \rho(\theta)$ for a k-regular character θ. In this case, reasoning as before, necessarily $\theta = \tau(\theta^{-1})$, for some $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$, and it follows that $\tau^2 = 1$. Either $\tau = 1$, hence, $\theta^2 = 1$, but there is a unique non-trivial quadratic character of $\mathrm{l}^\times$, which is, thus, fixed by all $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$, and the trivial character of $\mathrm{l}^\times$ is also $\mathrm{Gal}(\mathrm{l}/\mathrm{k})$-invariant, so we deduce that $n = 1$, as θ is regular. Or τ has order 2, and, hence, $n = \#\,\mathrm{Gal}(\mathrm{l}/\mathrm{k})$ is even. □

We now recall the classification of cuspidal $\overline{\mathbb{F}_\ell}$-representations of James [13]. We have a surjective map

$$\begin{aligned}\{&\text{supercuspidal } \overline{\mathbb{Q}_\ell}\text{-representations of } \mathcal{G}\}/\simeq \\ &\to \{\text{cuspidal } \overline{\mathbb{F}_\ell}\text{-representations of } \mathcal{G}\}/\simeq \\ \rho(\theta) &\mapsto \overline{\rho(\theta)}\end{aligned}$$

given by reduction modulo ℓ.

Given a character $\theta : \mathrm{l}^\times \to \overline{\mathbb{Q}_\ell}^\times$ we can uniquely write $\theta = \theta_r\theta_s$ with θ_r of order prime to ℓ and θ_s of order a power of ℓ. James' parametrisation enjoys the following properties:

(i) Two supercuspidal $\overline{\mathbb{Q}_\ell}$-representations $\rho(\theta), \rho(\theta')$ have isomorphic reductions modulo ℓ, if and only if there exists $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$, such that $\theta'_r = \theta_r^\tau$.

(ii) $\overline{\rho(\theta)}$ is supercuspidal, if and only if θ_r is regular.

4.3. σ-self-dual lifts of cuspidal $\overline{\mathbb{F}_\ell}$-representations. — We now specialise to the case $\mathrm{k}/\mathrm{k}_\mathrm{o}$ is quadratic. Write $\Gamma = \mathrm{Hom}(\mathrm{l}^\times, \overline{\mathbb{Q}_\ell}^\times)$, then $\Gamma = \Gamma_s \times \Gamma_r$, where Γ_s consists of the characters of ℓ-power order, and Γ_r consists of the characters with order prime to ℓ.

We study σ-self-dual lifts of cuspidal $\overline{\mathbb{F}_\ell}$-representations, and when n is even, there are no σ-self-dual supercuspidal $\overline{\mathbb{Q}_\ell}$-representations by Lemma 4.4. Hence, without loss of generality, we can assume that n is odd. Moreover, as reduction modulo ℓ commutes with taking contragredients and with the action of σ, this implies that when the cuspidal representation $\overline{\rho}$ of $\mathcal{G}$ is not σ-self-dual, it has no σ-self-dual lifts.

For $\gamma \in \Gamma$, we set $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_\gamma = \{\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k}) : \gamma^\tau = \gamma\}$. Letting $\theta \in \Gamma$ we can decompose $\theta = \theta_r\theta_s$ and we have $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_\theta = \mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_r} \cap \mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_s}$. In particular, θ is regular, if and only if $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_r} \cap \mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_s} = \{1\}$.

Let $\mathrm{l}_\circ$ be the unique subextension of $\mathrm{l}/\mathrm{k}_\circ$ of degree n as an extension of $\mathrm{k}_\circ$ and put $\Gamma_\circ = \mathrm{Hom}(\mathrm{l}_\circ^\times, \overline{\mathbb{Q}_\ell}^\times)$. We have an embedding

$$i : \Gamma_\circ \hookrightarrow \Gamma, \qquad i : \gamma \mapsto \gamma \circ \mathrm{N}_{\mathrm{l}/\mathrm{l}_\circ},$$

by surjectivity of the norm. Hence, $\Gamma^+ = i(\Gamma_\circ)$ is a unique subgroup of the cyclic group Γ of order $q_\circ^n - 1$. Write $\widetilde{\sigma}$ for the unique involution in $\mathrm{Gal}(\mathrm{l}/\mathrm{k}_\circ)$, which extends σ (as n is odd). By Hilbert's theorem 90, we have

$$\Gamma^+ = \{\gamma \in \Gamma : \gamma^{\widetilde{\sigma}} = \gamma\}.$$

On the other hand, the unique subgroup of the cyclic group Γ of order $q_\circ^n + 1$ is

$$\Gamma^- = \{\gamma \in \Gamma : \gamma \circ \mathrm{N}_{\mathrm{l}/\mathrm{l}_\circ} = 1\} = \{\gamma \in \Gamma : \gamma^{\widetilde{\sigma}} = \gamma^{-1}\},$$

as the norm map is surjective. Note that $(q_\circ^n + 1, q_\circ^n - 1) = 2$ because q is odd, so $\Gamma^+ \cap \Gamma^- = \{1, \eta\}$, where η denotes the unique quadratic character in Γ. Moreover, if ℓ is odd:

(i) If $\ell \mid q_\circ^n - 1$, then $\Gamma_s \subseteq \Gamma^+$.
(ii) If $\ell \mid q_\circ^n + 1$, then $\Gamma_s \subseteq \Gamma^-$.

Before giving the full solution of the lifting σ-self-duality for ℓ-modular cuspidal representations, we characterise ℓ-modular cuspidal σ-self-duality in terms of the Dipper and James parametrisation.

PROPOSITION 4.5. — *Let $\overline{\rho}$ be a cuspidal representation of $\mathcal{G}$ and suppose that n and ℓ are odd, then $\overline{\rho}$ is σ-self-dual, if and only if $\theta_r^{\widetilde{\sigma}} = \theta_r^{-1}$.*

Proof. — Write $\overline{\rho} = \overline{\rho(\theta)}$ for a k-regular character θ and let $\widetilde{\sigma} \in \mathrm{Gal}(\mathrm{l}/\mathrm{k}_\circ)$ be the unique involution extending σ. One implication is obvious; for the other, we thus suppose that $\overline{\rho(\theta)}$ is σ-self-dual. Then, there exists $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$, such that $\theta_r^{\widetilde{\sigma}\tau} = \theta_r^{-1}$. This implies that $\tau^2 = (\widetilde{\sigma}\tau)^2$ belongs to $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_r}$. On the other hand, the order of τ is odd because n is, and, hence, τ also belongs to $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_r}$, so $\theta_r^{\widetilde{\sigma}} = \theta_r^{-1}$. □

We have the following complete result when ℓ is odd.

PROPOSITION 4.6. — *Assume that n and ℓ are odd. Let $\overline{\rho}$ be a σ-self-dual cuspidal $\overline{\mathbb{F}_\ell}$-representation of $\mathcal{G}$.*

(i) *Suppose that ℓ is prime with $q^n - 1$. Then, the unique supercuspidal lift of $\overline{\rho}$ is σ-self-dual.*

(ii) *Suppose that* $\ell \mid q_{\mathrm{o}}^n - 1$.
   (a) *If* $\overline{\rho}$ *is supercuspidal, and* ℓ^a *is the highest power of* ℓ *dividing* $q^n - 1$*, then there is a unique* σ*-self-dual supercuspidal lift amongst the* ℓ^a *supercuspidal lifts of* $\overline{\rho}$*. In terms, of Green's parameterisation of supercuspidal* $\overline{\mathbb{Q}_\ell}$*-representations, if* $\rho(\theta)$ *is a lift of* $\overline{\rho}$*, then* $\rho(\theta_r)$ *is the unique* σ*-self-dual supercuspidal lift of* $\overline{\rho}$*.*
   (b) *If* $\overline{\rho}$ *is cuspidal non-supercuspidal, then none of its supercuspidal lifts are* σ*-self-dual.*

(iii) *Suppose that* $\ell \mid q_{\mathrm{o}}^n + 1$*. Then all supercuspidal lifts of* $\overline{\rho}$ *are* σ*-self-dual.*

Proof. — Write $\overline{\rho} = \overline{\rho(\theta)}$ for a k-regular character θ of $\mathrm{l}^\times$ and let $\widetilde{\sigma} \in \mathrm{Gal}(\mathrm{l}/\mathrm{k}_{\mathrm{o}})$ be the unique involution extending σ.

The set of isomorphism classes of supercuspidal $\overline{\mathbb{Q}_\ell}$-representations lifting $\overline{\rho}$ is then

$$\{\rho(\theta_r\mu) : \mu \in \Gamma_s, \theta_r\mu \text{ k-regular}\}/\simeq .$$

Such a representation $\rho(\theta_r\mu)$ is σ-self-dual, if and only if there exists $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$, such that $(\theta_r\mu)^{\widetilde{\sigma}} = (\theta_r^{-1}\mu^{-1})^\tau$. As $\theta_r\mu$ is regular, this condition implies that $\tau^2 = (\widetilde{\sigma}\tau)^2$ is the identity, so that $\tau = \mathrm{Id}$ as n is odd. So, $\rho(\theta_r\mu)$ is σ-self-dual, if and only if $\theta_r^{\widetilde{\sigma}} = \theta_r^{-1}$ and $\mu^{\widetilde{\sigma}} = \mu^{-1}$, and the set of σ-self-dual lifts of $\overline{\rho}$ is equal to

$$\{\rho(\theta_r\mu) : \mu \in \Gamma_s \cap \Gamma^-, \theta_r\mu \text{ k-regular}\}/\simeq$$

because the condition $\theta_r^{\widetilde{\sigma}} = \theta_r^{-1}$ is always satisfied due to Proposition 4.5. In particular, when θ_r is regular, then all $\theta_r\mu$ must be regular as well, and the cardinality of the set of σ-self-dual lifts of $\overline{\rho}$ is that of Γ_s, namely, the highest power of ℓ dividing $q^n - 1$.

In particular, if ℓ is prime to $q^n - 1$, then Γ_s is trivial, and this proves (i).

If $\ell \mid q_{\mathrm{o}}^n - 1$. Then $\Gamma_s \subseteq \Gamma^+$, and $\Gamma_s \cap \Gamma^- = \Gamma_s \cap \Gamma^- \cap \Gamma^+ = \{1\}$ because $\Gamma^+ \cap \Gamma^- = \{1, \eta\}$ and $\eta \notin \Gamma_s$. Hence, if $\overline{\rho}$ is supercuspidal, i.e. if θ_r is regular, then $\rho(\theta_r)$ is the unique σ-self-dual supercuspidal lift of $\overline{\rho}$, whereas if $\overline{\rho}$ is cuspidal non-supercuspidal, then it has no σ-self-dual supercuspidal lift, and we have shown (ii).

Finally, suppose that $\ell \mid q_{\mathrm{o}}^n + 1$, then $\Gamma_s \subseteq \Gamma^-$, so all supercuspidal lifts of $\overline{\rho}$ are σ-self-dual, and we have shown (iii). □

In the case $\ell = 2$, we have:

Proposition 4.7. — *Assume that* n *is odd and* $\ell = 2$*. Let* $\overline{\rho}$ *be a* σ*-self-dual cuspidal* $\overline{\mathbb{F}_\ell}$*-representation of* $\mathcal{G}$*, then it has a non-*σ*-self-dual lift.*

Proof. — Write $\overline{\rho} = \overline{\rho(\theta)}$ for a regular character θ and let $\widetilde{\sigma} \in \mathrm{Gal}(\mathrm{l}/\mathrm{k}_{\mathrm{o}})$ be the unique involution extending σ.

First note that $q^n-1=(q_\circ^n-1)(q_\circ^n+1)$, so the highest power of 2 dividing q^n-1, which is the order of Γ_s, does not divide $q_\circ^n+1$, as 2 also divides $q_\circ^n-1$. In particular, Γ_s is not a subgroup of Γ^-, so if μ_0 is a generator of Γ_s, then $\widetilde{\sigma}(\mu_0)\neq\mu_0^{-1}$. Now we claim that $\rho(\theta_r\mu_0)$ is a non-σ-self-dual lift of $\overline{\rho(\theta)}$. First, it is supercuspidal; indeed, $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\mu_0}\subset\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_s}$ because θ_s is a power of μ_0, and, hence, $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_r}\cap\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\mu_0}$ is trivial because $\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_r}\cap\mathrm{Gal}(\mathrm{l}/\mathrm{k})_{\theta_s}$ is trivial. Moreover, suppose that $\rho(\theta_r\mu_0)$ was σ-self-dual, then following the beginning of the proof of Proposition 4.6, this would imply that both θ_r and μ_0 belong to Γ^-, which is absurd. □

4.4. Self-dual lifts of self-dual cuspidal $\overline{\mathbb{F}_\ell}$-representations. — If there exists a self-dual supercuspidal $\overline{\mathbb{Q}_\ell}$-representation of $\mathcal{G}$, then n is 1 or even by Lemma 4.4. The case $n=1$ is straightforward; a character is self-dual, if and only if it is quadratic, and we treat it separately:

PROPOSITION 4.8. — *Suppose that $n=1$. Then $1,\eta$ are the unique self-dual supercuspidal $\overline{\mathbb{Q}_\ell}$-representations of $\mathrm{GL}_1(\mathrm{k})$. The reductions $\overline{1},\overline{\eta}$ of $1,\eta$, respectively, are the unique self-dual cuspidal $\overline{\mathbb{F}_\ell}$-representations of $\mathrm{GL}_1(\mathrm{k})$.*

(i) *Suppose that $\ell\nmid q-1$. Then $\overline{1},\overline{\eta}$ have $1,\eta$, respectively, as unique lift.*
(ii) *Suppose that $\ell\mid q-1$ and let ℓ^a be the highest power of ℓ dividing $q-1$. Then $\overline{1},\overline{\eta}$ each have ℓ^a-supercuspidal lifts of which $1,\eta$ (respectively) is the unique self-dual supercuspidal lift.*

Note that case (ii) contains the case $\ell=2$, in which case $\overline{1}=\overline{\eta}$. So, in particular in case (ii), non-trivial lifts of the trivial character of $\kappa^\times$ always exist.

Hence, for the rest of this section, we assume that n is even. Let σ' denote the unique involution in $\mathrm{Gal}(\mathrm{l}/\mathrm{k})$ and $\mathrm{l}'_\circ=\mathrm{l}^{\sigma'}$ denote the σ'-fixed subfield. Then we have an embedding

$$i':\mathrm{Hom}(\mathrm{Gal}(\mathrm{l}'_\circ/\mathrm{k}),\overline{\mathbb{Q}_\ell}^\times)\hookrightarrow\Gamma,\qquad i':\gamma\mapsto\gamma\circ\mathrm{N}_{\mathrm{l}/\mathrm{l}'_\circ},$$

by surjectivity of the norm, so its image is the unique subgroup of Γ of order $q^{n/2}-1$:

$$\Gamma_+=\{\gamma\in\Gamma:\gamma^{\sigma'}=\gamma\}.$$

The unique subgroup of Γ of order $q^{n/2}+1$ is, thus,

$$\Gamma_-=\{\gamma\in\Gamma:\gamma^{\sigma'}=\gamma^{-1}\},$$

their intersection is given by $\Gamma_+\cap\Gamma_-=\{1,\eta\}$, as q is odd. As $(q^{n/2}+1,q^{n/2}-1)=2$, we deduce that, if ℓ is odd:

(i) If $\ell\mid q^{n/2}-1$, then $\Gamma_s\subseteq\Gamma_+$.
(ii) If $\ell\mid q^{n/2}+1$, then $\Gamma_s\subseteq\Gamma_-$.

The results concerning self-duality look very similar to those concerning σ-self-duality; however, in one case, we only consider lifting of distinction.

PROPOSITION 4.9. — *Suppose that $n = 2m \geqslant 2$ is even and that ℓ is odd. Let $\overline{\rho}$ be a self-dual cuspidal $\overline{\mathbb{F}_\ell}$-representation of $\mathcal{G}$.*

(i) *Suppose that ℓ is prime with $q^n - 1$. Then the unique supercuspidal lift of $\overline{\rho}$ is self-dual.*
(ii) *Suppose that $\ell \mid q^{n/2} - 1$.*
  (a) *If $\overline{\rho}$ is supercuspidal, and ℓ^a is the highest power of ℓ dividing $q^n - 1$, then there is a unique self-dual lift of $\overline{\rho}$ amongst its ℓ^a supercuspidal lifts. In terms of Green's parameterisation of supercuspidal $\overline{\mathbb{Q}_\ell}$-representations, if $\rho(\theta)$ is a lift of $\overline{\rho}$, then $\rho(\theta_r)$ is the unique self-dual supercuspidal lift of $\overline{\rho}$.*
  (b) *If $\overline{\rho}$ is cuspidal non-supercuspidal, then none of its supercuspidal lifts are self-dual.*
(iii) *Suppose that $\ell \mid q^{n/2}+1$ and that $\overline{\rho}$ is $\mathrm{GL}_m(\mathrm{k}) \times \mathrm{GL}_m(\mathrm{k})$-distinguished. Then all supercuspidal lifts of $\overline{\rho}$ are self-dual.*

Proof. — A lift $\rho(\theta_r\mu)$ with $\mu \in \Gamma_s$ is self-dual, if and only if there exists $\tau \in \mathrm{Gal}(\mathrm{l}/\mathrm{k})$, such that $\theta_r\mu = (\theta_r^{-1}\mu^{-1})^\tau$, and, hence, $\tau^2 = \mathrm{Id}$, i.e. $\tau = \mathrm{Id}$ or σ'. The first case is impossible, as it would imply that $\theta_r\mu$ is the quadratic character in Γ, which would contradict its regularity. Hence, $\rho(\theta_r\mu)$ is self-dual, if and only if $\theta_r^{\sigma'} = \theta_r^{-1}$ and $\mu^{\sigma'} = \mu^{-1}$. Thus, if $\theta_r^{\sigma'} = \theta_r^{-1}$, then the set

$$\{\rho(\theta_r\mu) : \mu \in \Gamma_s \cap \Gamma_-, \theta_r\mu \text{ regular}\}/\simeq$$

is a full set of representatives for the isomorphism classes of self-dual lifts of $\overline{\rho}$ (and there are no self-dual lifts if $\theta_r^{\sigma'} \neq \theta_r^{-1}$).

For parts (i) and (ii)(a), as θ_r is regular, the self-duality of $\overline{\rho}$ implies that $\theta_r^{\sigma'} = \theta_r^{-1}$. Hence, parts (i) and (ii)(a) follow in the same way as their analogues in Proposition 4.6. Part (ii)(b) is obvious, as $\Gamma_s \cap \Gamma_-$ is trivial in this case. Finally, (iii) holds, because in this case, distinction lifts by Lemma 3.7. □

When $\ell = 2$, we have the exact analogue of Proposition 4.7 with the same proof, replacing q_o^n by $q^{n/2}$.

PROPOSITION 4.10. — *Assume that $n \geqslant 2$ is even and $\ell = 2$. Let $\overline{\rho}$ be a self-dual cuspidal $\overline{\mathbb{F}_\ell}$-representation of $\mathcal{G}$, then it has a non-self-dual lift.*

5. Type theory and distinction

From now on we set $\mathrm{G} = \mathrm{GL}_n(\mathrm{F})$, $\mathrm{G}_\mathrm{o} = \mathrm{GL}_n(\mathrm{F}_\mathrm{o})$ and σ, the Galois involution. We use the Bushnell–Kutzko construction of cuspidal representations of G [7], extended by Vignéras to the setting of cuspidal R-representations [28,

§III]. We summarise the properties that we will use and refer the reader to [7] and [28], for more details on this construction.

5.1. Properties of types. — Let π be a cuspidal R-representation of G. Then, associated to it is a family of explicitly constructed pairs $(\mathbf{J}, \boldsymbol{\lambda})$, called *extended maximal simple types*, where $\mathbf{J}$ is an open subgroup of G containing the centre $\mathrm{Z_G}$ of G with $\mathbf{J}/\mathrm{Z_G}$ compact, and $\boldsymbol{\lambda}$ is an irreducible (hence, finite-dimensional) representation of $\mathbf{J}$, such that

$$\pi \simeq \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda}).$$

We abbreviate extended maximal simple type to *type* for the rest of the paper and will say R-*type* when we wish to specify the field R considered.

Let $(\mathbf{J}, \boldsymbol{\lambda})$ be an R-type *in* π, i.e. associated to π as described above. Types enjoy the following key properties:

(T-1) Two types in π are conjugate in G, [7, 6.2.4] and [28, III 5.3]

(T-2) The group $\mathbf{J}$ has a unique maximal compact subgroup J, and J has a unique maximal normal pro-p-subgroup J^1, cf. [7, §3.1] for the definitions of these groups.

(T-3) There is a subfield E of $\mathcal{M}_n(\mathrm{F})$ containing F, the multiplicative group of which normalises J, and $\mathbf{J} = \mathrm{E}^\times \mathrm{J}$. (In fact, we have summarised this construction in reverse; the extension E/F is part of the original data used to construct the type.) The quotient J/J^1 is isomorphic to $\mathrm{GL}_m(\mathrm{k}_E)$ with $m = n/[\mathrm{E} : \mathrm{F}]$. Moreover, $\mathrm{E}^\times \cap \mathrm{J} = \mathscr{O}_{\mathrm{E}}^\times$, hence $\mathbf{J} = \langle \varpi_{\mathrm{E}} \rangle \mathrm{J}$ is the semi-direct product of J with the group generated by ϖ_{E}.

(T-4) Let $(\mathbf{J}, \boldsymbol{\lambda})$ be a type, let $\boldsymbol{\lambda}'$ be a representation of $\mathbf{J}$, set $\pi = \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda})$ and $\pi' = \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda}')$. If $\boldsymbol{\lambda}' \mid_{\mathrm{J}} \simeq \boldsymbol{\lambda} \mid_{\mathrm{J}}$, then $(\mathbf{J}, \boldsymbol{\lambda}')$ is a type, and the cuspidal representation π' is an unramified twist of π. Conversely, if $(\mathbf{J}, \boldsymbol{\lambda}')$ is a type, and the cuspidal representation π' is an unramified twist of π, then $\boldsymbol{\lambda}' \mid_{\mathrm{J}} \simeq \boldsymbol{\lambda} \mid_{\mathrm{J}}$.

(T-5) The representation $\boldsymbol{\lambda}$ (by construction) decomposes (non-uniquely) as a tensor product $\boldsymbol{\kappa} \otimes \boldsymbol{\tau}$, where:
- $\boldsymbol{\tau}$ is a representation of $\mathbf{J}$ trivial on J^1, which restricts irreducibly to J, and the representation of J/J^1 induced by $\boldsymbol{\tau}$ identifies with a cuspidal representation of $\mathrm{GL}_m(\mathrm{k_E})$.
- $\boldsymbol{\kappa}$ is a representation of $\mathbf{J}$, which restricts irreducibly to J^1.

(T-6) The representation π is supercuspidal, if and only if $\boldsymbol{\tau}$ induces a supercuspidal restriction on J/J^1, [28, III 5.14].

(T-7) The pair $(\mathbf{J}, \boldsymbol{\kappa} \otimes \boldsymbol{\tau}')$ is another type in π, if and only if $\boldsymbol{\tau} \simeq \boldsymbol{\tau}'$.

(T-8) When $\mathrm{R} = \overline{\mathbb{Q}_\ell}$, the representation π is integral, if and only if $\boldsymbol{\lambda}$ is integral.

(T-9) The construction is compatible with reduction modulo ℓ in the following sense: given a $\overline{\mathbb{Q}_\ell}$-type $(\mathbf{J}, \boldsymbol{\lambda})$ with $\boldsymbol{\lambda}$ integral, $(\mathbf{J}, r_\ell(\boldsymbol{\lambda}))$ is an $\overline{\mathbb{F}_\ell}$-type, and $r_\ell(\mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda})) = \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(r_\ell(\boldsymbol{\lambda}))$ is a cuspidal $\overline{\mathbb{F}_\ell}$-representation, [28, III 4.25].

(T-10) The construction lifts [28, III 4.29]: given an $\overline{\mathbb{F}_\ell}$-type $(\mathbf{J}, \boldsymbol{\kappa} \otimes \boldsymbol{\tau})$, there is a unique irreducible $\overline{\mathbb{Q}_\ell}$-representation $\widetilde{\eta}$ of J^1, which lifts $\boldsymbol{\kappa}\,|_{\mathrm{J}^1}$, and we can fix a extension $\widetilde{\boldsymbol{\kappa}}$ of $\widetilde{\eta}$ with $r_\ell(\widetilde{\boldsymbol{\kappa}}) = \boldsymbol{\kappa}$. As all of the extensions of $\widetilde{\eta}$ to $\mathbf{J}$ are related by twisting by a character trivial on J^1, Property (T-7) implies that the set of isomorphism classes of lifts of $\pi = \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\kappa} \otimes \boldsymbol{\tau})$ is in bijection with the set of isomorphism classes of lifts of $\boldsymbol{\tau}$ by $\widetilde{\boldsymbol{\tau}} \mapsto \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\widetilde{\boldsymbol{\kappa}} \otimes \widetilde{\boldsymbol{\tau}})$.

(T-11) We call a field extension E/F associated to a type in π as in (T- 3) a *parameter field* for π. While there are potentially many choices, the ramification index $e(\mathrm{E}/\mathrm{F})$, inertial degree $f(\mathrm{E}/\mathrm{F})$, and (hence) the degree $[\mathrm{E} : \mathrm{F}]$ are invariants of π as follows from [7, 3.5.1]. As such, we write $d(\pi) = [\mathrm{E} : \mathrm{F}]$, $e(\pi) = e(\mathrm{E}/\mathrm{F})$ and $f(\pi) = f(\mathrm{E}/\mathrm{F})$. We write $m(\pi)$ for $n/d(\pi)$. These invariants are compatible with reduction modulo ℓ; for π an integral cuspidal $\overline{\mathbb{Q}_\ell}$-representation we have

$$d(\pi) = d(r_\ell(\pi)),\ e(\pi) = e(r_\ell(\pi)),\ f(\pi) = f(r_\ell(\pi)),\ m(\pi) = m(r_\ell(\pi)).$$

5.2. Galois-self-dual types. — It was recently shown in [4] and [27] that the construction of types also enjoys good compatibility properties with σ-self-duality and distinction. Indeed, according to [4, §4], if π is a cuspidal R-representation of G which is σ-self-dual, then one can chose a type $(\mathbf{J}, \boldsymbol{\lambda})$ in π such that:

(SSDT-I) $\mathbf{J}$ (hence, J and J^1) and E are σ-stable, and $\boldsymbol{\lambda}^\vee \simeq \boldsymbol{\lambda}^\sigma$.

(SSDT-II) Set $\mathrm{E}_\mathrm{o} = \mathrm{E}^\sigma$, then $\mathrm{E}/\mathrm{E}_\mathrm{o}$ is a quadratic extension, and we can choose a uniformiser ϖ_E with $\sigma(\varpi_\mathrm{E}) = \varpi_\mathrm{E}$, if $\mathrm{E}/\mathrm{E}_\mathrm{o}$ is unramified, and $\sigma(\varpi_E) = -\varpi_E$, if $\mathrm{E}/\mathrm{E}_\mathrm{o}$ is ramified as in [27, (5.2)].

(SSDT-III) $\boldsymbol{\kappa}$, hence, $\boldsymbol{\tau}$, are σ-self-dual ([27, Lemma 8.9]).

The ramification index $e(\mathrm{E}/\mathrm{E}_\mathrm{o}) \in \{1, 2\}$ (and is equal to 1 if $\mathrm{F}/\mathrm{F}_\mathrm{o}$ is unramified) is an invariant of π, and we write

$$e_\sigma(\pi) = e(\mathrm{E}/\mathrm{E}_\mathrm{o}).$$

Remark 5.1. — This latter invariant is also equal to the ramification index of the extension $\mathrm{T}/\mathrm{T}^\sigma$, where T is the maximal tamely ramified extension of F contained in E due to [27, Remark 4.15 (2)]. We use this fact when referring to some results of [27].

In [4, §6.2], another invariant, a positive integer $e_\mathrm{o}(\pi)$ dividing n defined only in terms of the σ-stable group $\mathbf{J}$, is associated to π. By [4, Lemma 5.10], we have the following description:

$$e_\mathrm{o}(\pi) = \begin{cases} 2e(\mathrm{E}_\mathrm{o}/\mathrm{F}_\mathrm{o}) & \text{if } e_\sigma(\pi) = 2 \text{ and } m(\pi) \neq 1; \\ e(\mathrm{E}_\mathrm{o}/\mathrm{F}_\mathrm{o}) & \text{otherwise.} \end{cases}$$

Again, these invariants are compatible with reduction modulo ℓ; for π an integral σ-self-dual supercuspidal $\overline{\mathbb{Q}_\ell}$-representation we have

$$e_\sigma(\pi) = e_\sigma(r_\ell(\pi)),\ e_{\mathfrak{o}}(\pi) = e_{\mathfrak{o}}(r_\ell(\pi)).$$

Definition 5.2. — We call a type $\boldsymbol{\lambda} = \boldsymbol{\kappa} \otimes \boldsymbol{\tau}$ satisfying Conditions (SSDT-I) to (SSDT-III) a *σ-self-dual type.*

Note that an immediate consequence of the existence of a σ-self-dual cuspidal type in a σ-self-dual cuspidal representation is that in some cases, there are no σ-self-dual cuspidal representations, as follows from [27, Lemma 6.9 and Lemma 8.1]:

Lemma 5.3. — *Let π be a σ-self-dual cuspidal* R*-representation.*

(i) *If $e_\sigma(\pi) = 1$ and π is supercuspidal, then $m(\pi)$ is odd.*
(ii) *If $e_\sigma(\pi) = 2$, then $m(\pi)$ is either equal to 1 or even.*

A crucial property of σ-self-dual types is the following:

Proposition 5.4 ([27, Lemma 5.19]). — *Let $(\mathbf{J}, \boldsymbol{\lambda})$ be a σ-self-dual type. Then there exists a unique character $\chi_{\boldsymbol{\kappa}}$ of $\mathbf{J}^\sigma$ trivial on $(\mathrm{J}^1)^\sigma$, such that*

$$\mathrm{Hom}_{(\mathrm{J}^1)^\sigma}(\boldsymbol{\kappa}, \mathrm{R}) = \mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\kappa}, \chi_{\boldsymbol{\kappa}}),$$

and the canonical map

$$\mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\kappa}, \chi_{\boldsymbol{\kappa}}) \otimes \mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\tau}, \chi_{\boldsymbol{\kappa}}^{-1}) \to \mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\lambda}, \mathrm{R})$$

is an isomorphism.

In many cases, it is shown in [27] that one can choose $\chi_{\boldsymbol{\kappa}} = 1$ above, including the supercuspidal case:

Proposition 5.5. — *Let π be a σ-self-dual supercuspidal* R*-representation and $(\mathbf{J}, \boldsymbol{\lambda})$ be a σ-self-dual type of π, then one can choose $\boldsymbol{\kappa}$ such that $\chi_{\boldsymbol{\kappa}} = 1$.*

Proof. — The only cases to consider are those that are not ruled out by Lemma 5.3, and the assertion then follows from [27, Propositions 6.15 and 8.10]. □

Remark 5.6. — Note that if $\mathrm{R} = \overline{\mathbb{Q}_\ell}$ above, then π is an integral, and $(\mathbf{J}, r_\ell(\boldsymbol{\tau}))$ is a σ-self-dual type for $r_\ell(\pi)$. Moreover, $\chi_{r_\ell(\boldsymbol{\kappa})} = 1$ if $\chi_{\boldsymbol{\kappa}} = 1$. Indeed, dues to Remark 3.5 applied to $(\mathbf{J}/\mathrm{F}_{\mathfrak{o}}^\times, \boldsymbol{\kappa})$, the representation $r_\ell(\boldsymbol{\kappa})$ is distinguished, and, hence, $\chi_{r_\ell(\boldsymbol{\kappa})} = 1$ by the first part of Proposition 5.4.

5.3. Generic types and distinguished types. — There are, in general, more than one $\mathrm{G}_{\mathfrak{o}}$-conjugacy class of σ-self-dual types in a σ-self-dual cuspidal R-repre-

sentation (see [27, Section 1.11]). However, there is only one $\mathrm{G}_\mathfrak{o}$-conjugacy class among those that contain a generic type in the following sense.

We denote by N be the maximal unipotent subgroup of the subgroup of upper triangular matrices in G, and $\mathrm{N}_\mathfrak{o} = \mathrm{N}^\sigma$. Let ψ a non-degenerate character of N. Note that such a character is always integral with non-degenerate reduction modulo ℓ, as N is exhausted by its pro-p-subgroups.

Definition 5.7. — Let $(\mathbf{J}, \boldsymbol{\lambda})$ be an R-type; we say that $(\mathbf{J}, \boldsymbol{\lambda})$ is a *ψ-generic type*, if

$$\mathrm{Hom}_{\mathrm{N}\cap\mathbf{J}}(\boldsymbol{\lambda}, \psi) \neq \{0\}.$$

We say that it is *generic*, if it is ψ-generic for some non-degenerate character of N.

Remark 5.8. — Note that if μ is a character of G, and $(\mathbf{J}, \boldsymbol{\lambda})$ is a ψ-generic type, then $(\mathbf{J}, \mu\,|_{\mathbf{J}} \otimes \boldsymbol{\lambda})$ is also ψ-generic.

We will also use the following observation later.

Lemma 5.9. — *A $(\mathbf{J}, \boldsymbol{\lambda})$ is an integral $\overline{\mathbb{Q}_\ell}$-type, and ψ be a non-degenerate character of* N. *If $(r_\ell(\mathbf{J}), r_\ell(\boldsymbol{\lambda}))$ is $r_\ell(\psi)$-generic, then $(\mathbf{J}, \boldsymbol{\lambda})$ is ψ-generic.*

Proof. — It is a consequence of Lemma 3.7, once one observes that $\mathbf{J} \cap \mathrm{N}$ is a (compact) pro-p group. □

If the type we consider is, moreover, σ-self-dual, we will only consider distinguished non-degenerate characters ψ of N, i.e. those that are trivial on $\mathrm{N}_\mathfrak{o}$:

Definition 5.10. — A σ-self-dual R-type is called *generic*, if it is ψ-generic with respect to a distinguished non-degenerate character ψ of N.

Our definition of a *generic σ-self-dual type* coincides with the definition given in [27, Definition 9.1] (see the discussion after [4, Definition 5.7]). There are two fundamental facts about these types: first, they always occur in σ-self-dual cuspidal representations.

Proposition 5.11 ([4, Proposition 5.5]). — *Let π be a σ-self-dual cuspidal* R*-representation of* G *and let ψ be a distinguished non-degenerate character of* N*; then π has a ψ-generic σ-self-dual type, which is, moreover, unique up to $\mathrm{N}_\mathfrak{o}$-conjugacy.*

The second fact concerns distinguished representations, which are σ-self-dual due to Proposition 3.3.

Theorem 5.12 ([4, Corollary 6.6], [27, Theorem 9.3]). — *Let π be a σ-self-dual cuspidal* R*-representation and $(\mathbf{J}, \boldsymbol{\lambda})$ a generic σ-self-dual type of π. Then π is distinguished, if and only if $\boldsymbol{\lambda}$ is $\mathbf{J}^\sigma$-distinguished.*

DEFINITION 5.13. — We call a σ-self-dual type $(\mathbf{J},\boldsymbol{\lambda})$ a *distinguished type* if $\boldsymbol{\lambda}$ is $\mathbf{J}^\sigma$-distinguished.

We have the following surprising result, which completes Theorem 5.12 and is evidence of the interplay between genericity and Galois distinction for $\mathrm{GL}_n(\mathrm{F})$:

LEMMA 5.14. — *A distinguished* R*-type is automatically σ-self-dual generic.*

Proof. — Take a σ-self-dual type $(\mathbf{J},\boldsymbol{\lambda})$ such that $\boldsymbol{\lambda}$ is $\mathbf{J}^\sigma$-distinguished. Then, $\mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda})$ is distinguished by Mackey theory and Frobenius reciprocity. However, then by [4, Remark 6.7] (and the equivalence of our definition of generic type with that given in [27, Defintion 9.1]), the type $(\mathbf{J},\boldsymbol{\lambda})$ must be ψ-generic for some distinguished non-degenerate character ψ of N. □

We end this section with the following important corollary of Proposition 5.4:

COROLLARY 5.15. — *A σ-self-dual type $(\mathbf{J},\boldsymbol{\lambda})$ is a distinguished type, if and only if* $\mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\kappa},\chi_{\boldsymbol{\kappa}})$ *and* $\mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\tau},\chi_{\boldsymbol{\kappa}}^{-1})$ *are non-zero, in which case both are one-dimensional.*

5.4. The relative torsion group of a distinguished representation. — For the rest of this section, we fix π a distinguished cuspidal R-representation and $(\mathbf{J},\boldsymbol{\lambda})$ a distinguished type in π. We set $\varpi_{\mathrm{E}_\mathfrak{o}}=\varpi_{\mathrm{E}}^2$, if $\mathrm{E}/\mathrm{E}_\mathfrak{o}$ is ramified, and $\varpi_{\mathrm{E}_\mathfrak{o}}=\varpi_{\mathrm{E}}$, if $\mathrm{E}/\mathrm{E}_\mathfrak{o}$ is unramified. When $e_\sigma(\pi)=2$, and $m(\pi)=2r$ is even, we denote by w the element of $\mathbf{J}$ corresponding to $\left(\begin{smallmatrix}0 & 1_r\\ 1_r & 0\end{smallmatrix}\right)$ as in [27, Lemma 6.19]. We define the *relative torsion group of* π to be the following group:

$$\mathrm{X}_\mathfrak{o}(\pi)=\{\mu_\mathfrak{o}\in\mathrm{Hom}(\mathrm{G}_\mathfrak{o},\mathrm{R}^\times):\mu_\mathfrak{o}\text{ is unramified, }\mathrm{Hom}_{\mathrm{G}_\mathfrak{o}}(\pi,\mu_\mathfrak{o})\neq\{0\}\}.$$

THEOREM 5.16. — *Let π be a cuspidal distinguished* R*-representation of* G *and set $\varpi'=\varpi_E w$, if $e_\sigma(\pi)=2$, and $m(\pi)$ is even and $\varpi'=\varpi_{\mathrm{E}_\mathfrak{o}}$ otherwise. Then we have:*

(i) *Let $\mu_\mathfrak{o}$ be an unramified character of $\mathrm{G}_\mathfrak{o}$, then $\mu_\mathfrak{o}\in\mathrm{X}_\mathfrak{o}(\pi)$, if and only if $\mu_\mathfrak{o}(\varpi')=1$.*
(ii) *Let $\chi_\mathfrak{o}$ be an unramified character of $\mathrm{F}_\mathfrak{o}^\times$, then $\chi_\mathfrak{o}\circ\det\in\mathrm{X}_\mathfrak{o}(\pi)$, if and only if $\chi_\mathfrak{o}(\varpi_\mathfrak{o})^{n/e_\mathfrak{o}(\pi)}=1$.*

Proof. — Note that if $e_\sigma(\pi)=2$, then $m(\pi)$ is even or equal to 1 due to Lemma 5.3. Then, $\mathbf{J}^\sigma$ is generated by ϖ' and J^σ, due to [27, Lemmas 6.18, 6.19 and 8.7]. Let $\mu_\mathfrak{o}$ be an unramified character of $\mathrm{G}_\mathfrak{o}$ and denote by μ an unramified extension of it to G; hence, $\mu_\mathfrak{o}\in\mathrm{X}_\mathfrak{o}(\pi)$, if and only if $\mu\otimes\pi$ is distinguished. Suppose that $\mu\otimes\pi$ is distinguished, then $(\mathbf{J},\boldsymbol{\kappa}\otimes(\mu\otimes\boldsymbol{\tau}))$ is a σ-self-dual type, which is, in fact, a distinguished type due to Remark 5.8 and Theorem 5.12, and conversely, if $(\mathbf{J},\boldsymbol{\kappa}\otimes(\mu\otimes\boldsymbol{\tau}))$ is a distinguished type, then $\mu\otimes\pi$ is distinguished.

So, $\mu_{\mathrm{o}} \in \mathrm{X}_{\mathrm{o}}(\pi)$, if and only if $(\mathbf{J}, \boldsymbol{\kappa} \otimes (\mu \otimes \boldsymbol{\tau}))$ is a distinguished type, which is, if and only if $\mathrm{Hom}_{\mathbf{J}^\sigma}(\mu \otimes \boldsymbol{\tau}, \chi_{\boldsymbol{\kappa}}^{-1})$ has dimension 1 according to Corollary 5.15.

However, $\mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\tau}, \chi_{\boldsymbol{\kappa}}^{-1})$ has dimension 1 by the same corollary, but $\mathrm{Hom}_{\mathrm{J}^\sigma}(\boldsymbol{\tau}, \chi_{\boldsymbol{\kappa}}^{-1})$ is already at most one-dimensional due to Proposition 4.2, so from these multiplicity one statements, we deduce that $\mu_{\mathrm{o}} \in \mathrm{X}_{\mathrm{o}}(\pi)$, if and only if $\mathrm{Hom}_{\mathbf{J}^\sigma}(\mu \otimes \boldsymbol{\tau}, \chi_{\boldsymbol{\kappa}}^{-1}) = \mathrm{Hom}_{\mathbf{J}^\sigma}(\boldsymbol{\tau}, \chi_{\boldsymbol{\kappa}}^{-1})$. Finally, this translates as: $\mu_{\mathrm{o}} \in \mathrm{X}_{\mathrm{o}}(\pi)$, if and only if $\mu(\varpi') = 1$ and proves (i).

Now, let χ_{o} be an unramified character of $\mathrm{F}_{\mathrm{o}}^\times$ and let χ be an unramified character of $\mathrm{F}^\times$ extending it. If $e_\sigma(\pi) = 2$, then $\mathrm{F}/\mathrm{F}_{\mathrm{o}}$ is ramified according to [27, Lemma 4.14].

Suppose that $e_\sigma(\pi) = 2$ and $m(\pi)$ is even; we have:

$$\begin{aligned}\chi_{\mathrm{o}}(\det(w')) &= \chi(\det(\varpi_E)) = \chi(\mathrm{N}_{\mathrm{E}/\mathrm{F}}(\varpi_{\mathrm{E}}))^{m(\pi)} = \chi(\varpi)^{f(\mathrm{E}/F)m(\pi)} \\ &= \chi(\varpi)^{n/e(\mathrm{E}/\mathrm{F})} = \chi(\varpi)^{ne(\mathrm{F}/\mathrm{F}_{\mathrm{o}})/e_\sigma(\pi)e(\mathrm{E}_{\mathrm{o}}/\mathrm{F}_{\mathrm{o}})} \\ &= \chi(\varpi)^{n/e(\mathrm{E}_{\mathrm{o}}/\mathrm{F}_{\mathrm{o}})} = \chi(\varpi_{\mathrm{o}})^{n/2e(\mathrm{E}_{\mathrm{o}}/\mathrm{F}_{\mathrm{o}})} = \chi(\varpi_{\mathrm{o}})^{n/e_{\mathrm{o}}(\pi)}\end{aligned}$$

due to [4, Lemma 5.10]. Otherwise, we have:

$$\begin{aligned}\chi_{\mathrm{o}}(\det(w')) &= \chi_{\mathrm{o}}(\mathrm{N}_{\mathrm{E}/\mathrm{F}}(\varpi_{E_{\mathrm{o}}}))^{m(\pi)} = \chi_{\mathrm{o}}(\mathrm{N}_{\mathrm{E}_{\mathrm{o}}/\mathrm{F}_{\mathrm{o}}}(\varpi_{E_{\mathrm{o}}}))^{m(\pi)} \\ &= \chi_{\mathrm{o}}(\varpi_{\mathrm{o}})^{f(\mathrm{E}_{\mathrm{o}}/\mathrm{F}_{\mathrm{o}})m(\pi)} = \chi_{\mathrm{o}}(\varpi_{\mathrm{o}})^{n/e(\mathrm{E}_{\mathrm{o}}/\mathrm{F}_{\mathrm{o}})} = \chi(\varpi_{\mathrm{o}})^{n/e_{\mathrm{o}}(\pi)}\end{aligned}$$

due to [4, Lemma 5.10] again. □

It has the following two corollaries.

COROLLARY 5.17. — *Let π be a distinguished cuspidal* R*-representation of* G*. Write $n/e_{\mathrm{o}}(\pi) = a(\pi)\ell^r$ with $a(\pi)$ prime to ℓ. Then, $\mathrm{X}_{\mathrm{o}}(\pi)$ is a cyclic group, of order $n/e_{\mathrm{o}}(\pi)$, if $\mathrm{R} = \overline{\mathbb{Q}_\ell}$, and of order $a(\pi)$, if $\mathrm{R} = \overline{\mathbb{F}_\ell}$.*

COROLLARY 5.18. — *Let π be a distinguished cuspidal (hence, integral) $\overline{\mathbb{Q}_\ell}$-representation of* G*. Then, the homomorphism*

$$r_\ell : \mu_{\mathrm{o}} \mapsto r_\ell(\mu_{\mathrm{o}})$$

is surjective from $\mathrm{X}_{\mathrm{o}}(\pi)$ to $\mathrm{X}_{\mathrm{o}}(r_\ell(\pi))$, and its kernel is the ℓ-singular part of $\mathrm{X}_{\mathrm{o}}(\pi)$.

Proof. — It suffices to verify the assertion on the kernel. It is clear that the ℓ-singular part of $\mathrm{X}_{\mathrm{o}}(\pi)$ belongs to the kernel of r_ℓ. Conversely, if $r_\ell(\mu_{\mathrm{o}}) = 1$, write $\mu_{\mathrm{o}} = (\mu_{\mathrm{o}})_r(\mu_{\mathrm{o}})_s$ with $(\mu_{\mathrm{o}})_r$ of order prime to ℓ and $(\mu_{\mathrm{o}})_s$ of order a power of ℓ, then $r_\ell((\mu_{\mathrm{o}})_r) = r_\ell(\mu_{\mathrm{o}}) = 1$ so $(\mu_{\mathrm{o}})_r = 1$ because r_ℓ induces a bijection between the group of roots of unity of order prime to ℓ in $\overline{\mathbb{Q}_\ell}^\times$ and the group of roots of unity in $\overline{\mathbb{F}_\ell}^\times$. □

6. Relatively banal cuspidal representations of p-adic GL_n

In [24] and [23], Mínguez and Sécherre single out a class of irreducible representations called *banal*, for which the Zelevinski classification works particularly nicely. For cuspidal representations, the following definition can be given ([24, Remarque 8.15] and [24, Lemme 5.3]).

Definition 6.1. — A cuspidal $\overline{\mathbb{F}_\ell}$-representation π is called *banal*, if $q^{n/e(\pi)} \not\equiv 1[\ell]$.

The following definition is new and is motivated by our cuspidal L-factor computation later and an analogy with banal cuspidal representations and the Rankin–Selberg computation of [18]. We show in Section 8.3 how it is a natural analogue of banal for the symmetric pair $(\mathrm{G}, \mathrm{G}_\circ, \sigma)$.

Definition 6.2. — Let π be a distinguished cuspidal $\overline{\mathbb{F}_\ell}$-representation. We say that it is *relatively banal*, if $q_\circ^{n/e_\circ(\pi)} \not\equiv 1[\ell]$.

Theorem 5.16 (ii) has the following third consequence:

Corollary 6.3 (of Theorem 5.16). — *Let π be a distinguished cuspidal $\overline{\mathbb{F}_\ell}$-representation, it is relatively banal, if and only if it is not $|\det(\ )|_\circ$-distinguished.*

Before stating the next lemma, we make the following observation, which shows that the statement of the lemma in question (Lemma 6.6) is, indeed, complete.

Remark 6.4. — For any character χ of $\mathrm{G}_\circ$, there are no χ-distinguished cuspidal R-representations π of G with $e_\sigma(\pi) = 2$ when $m(\pi) \geqslant 3$ is odd, by Proposition 5.4 and [27, Lemma 6.9].

While we have defined relatively banal distinguished representations in terms of the invariant $e_\circ(\ )$, we will use the following equivalent formulation:

Lemma 6.5. — *Let π be a σ-self-dual cuspidal* R*-representation of* G*. Let* E *be a σ-self-dual parameter field for π. Then,*

(i) *If $e_\sigma(\pi) = 1$, then $q_\circ^{n/e_\circ(\pi)} = q_{\mathrm{E}_\circ}^{m(\pi)}$ (and is also equal to $q_\circ^{n/e(\pi)}$, if $\mathrm{F}/\mathrm{F}_\circ$ is unramified, and $q^{n/2e(\pi)}$, if $\mathrm{F}/\mathrm{F}_\circ$ is ramified).*
(ii) *If $e_\sigma(\pi) = 2$ and $m(\pi) = 1$, then $q_\circ^{n/e_\circ(\pi)} = q_{\mathrm{E}_\circ}$ (and is also equal to $q^{n/e(\pi)} = q_{\mathrm{E}}$).*
(iii) *If $e_\sigma(\pi) = 2$ and $m(\pi) \geqslant 2$ is even, then $q_\circ^{n/e_\circ(\pi)} = q_{\mathrm{E}_\circ}^{m(\pi)/2}$ (and is also equal to $q^{n/2e(\pi)} = q_{\mathrm{E}}^{m(\pi)/2}$).*

Proof. — In all cases, we have $q^{n/e(\pi)} = q_{\mathrm{E}}^{m(\pi)}$. In case (i), $q_{\mathrm{E}_\circ}^m$ is the positive square root of q_{E}^m. However, by [4, Lemma 5.10], we have

$$\begin{aligned} e_\circ(\pi) &= e(\mathrm{E}_\circ/\mathrm{F}_\circ) = e(\mathrm{E}/\mathrm{F}_\circ)/e_\sigma(\pi) = e(\mathrm{E}/\mathrm{F}_\circ) \\ &= e(\mathrm{E}/\mathrm{F})e(\mathrm{F}/\mathrm{F}_\circ) = e(\pi)e(\mathrm{F}/\mathrm{F}_\circ). \end{aligned}$$

If $\mathrm{F}/\mathrm{F}_\circ$ is unramified, then $q_\circ^{n/e_\circ(\pi)} = q_\circ^{n/e(\pi)}$ is the positive square root of $q^{n/e(\pi)}$. Now, if $\mathrm{F}/\mathrm{F}_\circ$ is ramified, then $q_\circ^{n/e_\circ(\pi)} = q_\circ^{n/2e(\pi)}$ and (i) is proved.

In case (ii) by [4, Lemma 5.10], again, we have

$$\begin{aligned} e_\circ(\pi) &= e(\mathrm{E}_\circ/\mathrm{F}_\circ) = e(\mathrm{E}/\mathrm{F}_\circ)/e_\sigma(\pi) = e(\mathrm{E}/\mathrm{F}_\circ)/2 \\ &= e(\mathrm{E}/\mathrm{F})e(\mathrm{F}/\mathrm{F}_\circ)/2 = e(\pi)e(\mathrm{F}/\mathrm{F}_\circ)/2. \end{aligned}$$

However, $e(\mathrm{F}/\mathrm{F}_\circ) = 2$ by [27, Lemma 4.14], so $e_\circ(\pi) = e(\pi)$ and $q = q_\circ$, which proves case (ii).

Finally, in case (iii) by [4, Lemma 5.10], again, we have

$$\begin{aligned} e_\circ(\pi) &= 2e(\mathrm{E}_\circ/\mathrm{F}_\circ) = 2e(\mathrm{E}/\mathrm{F}_\circ)/e_\sigma(\pi) = e(\mathrm{E}/\mathrm{F}_\circ) \\ &= e(\mathrm{E}/\mathrm{F})e(\mathrm{F}/\mathrm{F}_\circ) = e(\pi)e(\mathrm{F}/\mathrm{F}_\circ), \end{aligned}$$

and $e(\mathrm{F}/\mathrm{F}_\circ) = 2$ by [27, Lemma 4.14], so $e_\circ(\pi) = 2e(\pi)$ and $q = q_\circ$, which proves case (iii). □

Immediately, from Remark 6.4 and Lemma 6.5, we have:

COROLLARY 6.6. — *A banal distinguished cuspidal $\overline{\mathbb{F}_\ell}$-representation of* G *is relatively banal.*

REMARK 6.7. — A banal cuspidal $\overline{\mathbb{F}_\ell}$-representation is supercuspidal. However, there are relatively banal distinguished cuspidal non-supercuspidal $\overline{\mathbb{F}_\ell}$-representations. For example, when $n = 3$ and $\ell \neq 2$, the non-normalised parabolic induction of the trivial representation of the Borel subgroup has a cuspidal subquotient $\mathrm{St}(3)$ when $q_\circ^3 \equiv -1[\ell]$, and when $\mathrm{F}/\mathrm{F}_\circ$ is unramified, it is relatively banal distinguished (see [19]).

Before proving the main result of this section, it will be useful to know that there are no relatively banal distinguished cuspidal representations π when $e_\sigma(\pi) = 1$ and $m(\pi)$ is even:

LEMMA 6.8. — *Let π be a cuspidal $\overline{\mathbb{F}_\ell}$-representation of* G*, which is σ-self-dual. Suppose that $e_\sigma(\pi) = 1$, that $m(\pi)$ is even, and $q_\circ^{n/e_\circ(\pi)} \not\equiv 1[\ell]$, then π is not distinguished.*

Proof. — Let $(\mathbf{J}, \boldsymbol{\kappa} \otimes \boldsymbol{\tau})$ be a σ-self-dual generic $\overline{\mathbb{F}_\ell}$-type for π (Proposition 5.11) with σ-stable parameter field E. Suppose π is distinguished. Then, by Theorem 5.12, we can suppose that $\boldsymbol{\kappa} \otimes \boldsymbol{\tau}$ is distinguished as well. By Proposition 5.4, $\boldsymbol{\tau}$ is $\chi_{\boldsymbol{\kappa}}^{-1}$-distinguished, and, hence, $\rho = \boldsymbol{\tau}\,|_{\mathrm{J}}$ is seen as a representation of $\mathrm{GL}_{m(\pi)}(\mathrm{k}_\mathrm{E})$ is $\chi_{\boldsymbol{\kappa}}^{-1}$-distinguished by the group $\mathrm{GL}_{m(\pi)}(\mathrm{k}_{\mathrm{E}_\circ})$,

i.e. that $\rho' = \chi \otimes \rho$ is distinguished for an extension χ of $\chi_{\boldsymbol{\kappa}}$ to $\mathrm{k}_{\mathrm{E}}^{\times}$. Now, by Lemma 6.5 and Lemma 3.7, ρ' has a distinguished lift, which contradicts Lemma 4.4. □

Remark 6.9. — Note that the statement of Lemma 6.8 is not empty, as σ-self-dual representations π exist under the hypothesis $e_\sigma(\pi) = 1$ and $q_{\mathfrak{o}}^{n/e_{\mathfrak{o}}(\pi)} \not\equiv 1[\ell]$; for example, when $n = 2$ and $\mathrm{F}/\mathrm{F}_{\mathfrak{o}}$ is unramified, the non-normalised parabolic induction of the trivial representation of the Borel subgroup has a cuspidal subquotient $\mathrm{St}(2)$ when $q \equiv -1[\ell]$, which is σ-self-dual and $e_\sigma(\mathrm{St}(2)) = 1$, as $\mathrm{F}/\mathrm{F}_{\mathfrak{o}}$ is unramified.

Lemma 6.10. — *Let $(\mathbf{J}, \boldsymbol{\lambda})$ be an* R*-type, such that $\mathbf{J}$ is σ-stable and put $\pi = \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda})$. If $\boldsymbol{\lambda}\,|_{\mathrm{J}}$ is distinguished, then π is the unramified twist of a distinguished representation. Conversely, suppose that, moreover, $\boldsymbol{\lambda} = \boldsymbol{\kappa} \otimes \boldsymbol{\tau}$ is generic and that $\boldsymbol{\kappa}$ is distinguished and σ-self-dual, if π is the unramified twist of a distinguished representation, then $\boldsymbol{\tau}\,|_{\mathrm{J}}$ is distinguished.*

Proof. — If $\boldsymbol{\lambda}\,|_{\mathrm{J}}$ is distinguished, then we can extend $\boldsymbol{\lambda}$ to a distinguished representation $\boldsymbol{\lambda}_{\mathrm{F}}$ of $\mathrm{F}^{\times}\mathrm{J}$ by setting $\boldsymbol{\lambda}_{\mathrm{F}}(\varpi_{\mathrm{F}}) = 1$. The induced representation $\mathrm{ind}_{\mathrm{F}^{\times}\mathrm{J}}^{\mathrm{E}^{\times}\mathrm{J}}(\boldsymbol{\lambda}_{\mathrm{F}})$ is distinguished, and because $\mathbf{J}/\mathrm{F}^{\times}\mathrm{J} \simeq \langle \varpi_{\mathrm{E}} \rangle / \langle \varpi_{\mathrm{F}} \rangle$ is cyclic, all of its irreducible subquotients extend $\boldsymbol{\lambda}_{\mathrm{F}}$ by Clifford theory, so one extension $\boldsymbol{\lambda}_{\mathrm{E}}$ of $\boldsymbol{\lambda}_{\mathrm{F}}$ to $\mathbf{J}$ is distinguished. Hence, $\mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda}_{\mathrm{E}})$ is distinguished and an unramified twist of $\mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\boldsymbol{\lambda})$ by Property (T-4).

For the partial converse, by twisting by an unramified character without loss of generality we can suppose that π is distinguished (and $\boldsymbol{\kappa}$ is the same). Then, $\boldsymbol{\tau}$ is σ-self-dual due to Property (T-7), and, hence, $\boldsymbol{\lambda}$ as well, and it is distinguished because of Theorem 5.12. Then Proposition 5.4 implies that $\boldsymbol{\tau}$, and, hence, $\boldsymbol{\tau}\,|_{\mathrm{J}}$ is distinguished. □

Relatively banal distinguished cuspidal $\overline{\mathbb{F}_\ell}$-representations enjoy very nice lifting properties:

Theorem 6.11. — *Let π be a cuspidal and distinguished $\overline{\mathbb{F}_\ell}$-representation of* G.

(i) *Then π is relatively banal, if and only if all of its lifts are unramified twists of distinguished representations.*
(ii) *If it is relatively banal, then it has a distinguished lift.*

Proof. — Suppose that π is relatively banal distinguished. Choose a distinguished type $(\mathbf{J}, \boldsymbol{\lambda})$ in π and let $\widetilde{\pi}$ be a lift of π. We can choose a type in $\widetilde{\pi}$ of the form $(\mathbf{J}, \widetilde{\boldsymbol{\lambda}})$ with $r_\ell(\widetilde{\boldsymbol{\lambda}}) = \boldsymbol{\lambda}$ by property (T-10). As ℓ is coprime to J^{σ}, we can apply Lemma 3.7, and $\widetilde{\boldsymbol{\lambda}}\,|_{\mathrm{J}}$ is distinguished because so is $\boldsymbol{\lambda}\,|_{\mathrm{J}}$. Hence, $\widetilde{\pi}$ is a unramified twist of a distinguished representation by Lemma 6.10, and this proves one implication in (i).

We now prove (ii). Suppose that π is relatively banal. By the implication already proved in (i) we know that π has a lift $\widetilde{\pi}$, which is $\widetilde{\mu_{\mathsf{o}}}$-distinguished for $\widetilde{\mu_{\mathsf{o}}}$ an unramified character of G_{o}. Let $\widetilde{\mu}$ be an unramified character of G extending $\widetilde{\mu_{\mathsf{o}}}$; then $\widetilde{\mu}^{-1}\otimes\widetilde{\pi}$ is distinguished. However, because π is distinguished, setting $\mu = r_\ell(\widetilde{\mu})$, the representation $\mu^{-1}\otimes\pi$ is μ_{o}^{-1}-distinguished for $\mu_{\mathsf{o}} = r_\ell(\widetilde{\mu_{\mathsf{o}}}) = \mu\mid_{\mathrm{G}_{\mathsf{o}}}$. Due to Corollary 5.18, μ_{o} has a lift $\widetilde{\mu_{\mathsf{o}}}' \in \mathrm{X}_{\mathsf{o}}(\widetilde{\mu}^{-1}\otimes\widetilde{\pi})$. Writing $\mu = \chi\circ\det$, it is possible to extend $\widetilde{\mu_{\mathsf{o}}'}$ to an unramified character $\widetilde{\mu}'$ of G such that, if $\mu' = r_\ell(\mu) = \chi'\circ\det$, then $\chi'(\varpi) = \chi(\varpi)$; indeed, as μ and μ' both extend μ_{o}, this is automatic, if $\mathrm{F}/\mathrm{F}_{\mathsf{o}}$ is unramified, whereas, if $\mathrm{F}/\mathrm{F}_{\mathsf{o}}$ is ramified $\chi'(\varpi) = \pm\chi(\varpi)$ is automatic, and we can always change $\widetilde{\mu}'$ so that this sign is $+$. With such choices, the representation $\widetilde{\mu}'\widetilde{\mu}^{-1}\otimes\widetilde{\pi}$ is a distinguished lift of π.

It remains to prove the second implication of (i). Suppose that π is not relatively banal, i.e. $q_{\mathsf{o}}^{n/e_{\mathsf{o}}(\pi)} \equiv 1[\ell]$. Suppose, for the sake of contradiction, that all lifts of π are distinguished up to an unramified twist and let $\widetilde{\pi}$ be a lift of π. Under this assumption the argument used to prove (ii) shows that π has a distinguished supercuspidal lift $\widetilde{\pi}$. This lift has a distinguished type $(\mathbf{J}, \widetilde{\boldsymbol{\kappa}}\otimes\widetilde{\boldsymbol{\tau}})$ with $\chi_{\widetilde{\boldsymbol{\kappa}}} = 1$ due to Theorem 5.12 and Proposition 5.5, and we set $\boldsymbol{\kappa} = r_\ell(\widetilde{\boldsymbol{\kappa}})$ and $\boldsymbol{\tau} = r_\ell(\widetilde{\boldsymbol{\tau}})$, so in particular, $(\mathbf{J}, \boldsymbol{\kappa}\otimes\boldsymbol{\tau})$ is a distinguished type due to Remark 3.5 (and also Lemma 5.14). Proposition 5.4 together with Lemma 4.4 imply that if $e_\sigma(\pi) = 2$, then either $m(\pi) = 1$ or it is even, and if $e_\sigma(\pi) = 1$, then $m(\pi)$ is odd. Then, $\boldsymbol{\tau}\mid_{\mathrm{J}}$ is distinguished according to Remark 3.5, but the assumption $q_{\mathsf{o}}^{n/e_{\mathsf{o}}(\pi)} \equiv 1[\ell]$ translated in terms of $\mathrm{GL}_{m(\pi)}(\mathrm{k_E})$ due to Lemma 6.5 together with Propositions 4.6 (ii), 4.7, 4.8 (ii), 4.6 (ii) and 4.10 imply that $\boldsymbol{\tau}\mid_{\mathrm{J}}$ has a non-distinguished lift $\widetilde{\boldsymbol{\tau}}'$. This lift extends to $\langle\varpi_{\mathsf{o}}\rangle\mathrm{J}$ to a lift of $\boldsymbol{\tau}\mid_{\langle\varpi_{\mathsf{o}}\rangle\mathrm{J}}$ by setting $\widetilde{\boldsymbol{\tau}}'(\varpi_{\mathsf{o}}) = 1$. Then, by Clifford theory, because the quotient $\mathbf{J}/\langle\varpi_{\mathsf{o}}\rangle\mathrm{J} \simeq \langle\varpi_{\mathrm{E}}\rangle/\langle\varpi_{\mathsf{o}}\rangle$ is cyclic, the representation $\mathrm{ind}_{\langle\varpi_{\mathsf{o}}\rangle\mathrm{J}}^{\mathbf{J}}(\widetilde{\boldsymbol{\tau}}')$ contains a lift of $\boldsymbol{\tau}$ that extends $\widetilde{\boldsymbol{\tau}}'$, and we again denote it $\widetilde{\boldsymbol{\tau}}'$. Then, the representation $\pi' = \mathrm{ind}_{\mathbf{J}}^{\mathrm{G}}(\widetilde{\boldsymbol{\kappa}}\otimes\widetilde{\boldsymbol{\tau}}')$ is a supercuspidal lift of π. As $\widetilde{\boldsymbol{\kappa}}\otimes\widetilde{\boldsymbol{\tau}}'$ reduces to the generic type $\boldsymbol{\kappa}\otimes\boldsymbol{\tau}$, it is generic due to Lemma 5.9, and, hence, it cannot be an unramified twist of a distinguished representation according to the second part of Lemma 6.10. □

Remark 6.12. — Note that as an unramified character of G_{o} always has an unramified extension to G, Part (i) of Theorem 6.11 can also be stated as π is relatively banal, if and only if all its lifts are distinguished by an unramified character.

7. Asai L-factors of cuspidal representations

7.1. Asai L-factors. — Let N be the maximal unipotent subgroup of the subgroup of upper triangular matrices in G, and $\mathrm{N}_{\mathsf{o}} = \mathrm{N}^{\sigma}$. Let ψ be a non-degenerate R-valued character of N trivial on N_{o}. Let π be an R-representation

of G of *Whittaker type* (i.e. of finite length with a one-dimensional space of Whittaker functionals) with Whittaker model $\mathcal{W}(\pi,\psi)$. We refer to [17, Section 2] for more details as well as basic facts about Whittaker functions and their analytic behaviour. For $\mathrm{W}\in\mathcal{W}(\pi,\psi)$ and $\Phi\in\mathscr{C}_c^\infty(\mathrm{F}_\mathfrak{o}^n)$ and $l\in\mathbb{Z}$, we define the local *Asai coefficient* to be

$$\mathrm{I}^l_{\mathrm{As}}(\mathrm{X},\Phi,\mathrm{W})=\int_{\substack{\mathrm{N}_\mathfrak{o}\backslash\mathrm{G}_\mathfrak{o}\\ \mathrm{val}(\det(g))=l}}\mathrm{W}(g)\Phi(\eta_n g)\,dg, \tag{1}$$

where η_n denotes the row vector $(\,0\,\cdots\,0\,1\,)$, and dg denotes a right invariant measure on $\mathrm{N}_\mathfrak{o}\setminus\mathrm{G}_\mathfrak{o}$ with values in R. We refer the reader to [17, Section 2.2] for details on R-valued equivariant measures on homogeneous spaces and their properties. The integrand in the Asai coefficient has compact support, so it is well defined and it, moreover, vanishes for $l<<0$. We define the *Asai integral* of $\mathrm{W}\in\mathcal{W}(\pi,\psi)$ and $\Phi\in\mathscr{C}_c^\infty(\mathrm{F}_\mathfrak{o}^n)$ to be the formal Laurent series

$$\mathrm{I}_{\mathrm{As}}(\mathrm{X},\Phi,\mathrm{W})=\sum_{l\in\mathbb{Z}}\mathrm{I}^l_{\mathrm{As}}(\mathrm{X},\Phi,\mathrm{W})\mathrm{X}^l. \tag{2}$$

In exactly the same way as in [17, Theorem 3.5], we deduce the following lemma:

LEMMA 7.1. — *For* $\mathrm{W}\in\mathcal{W}(\pi,\psi)$ *and* $\Phi\in\mathscr{C}_c^\infty(\mathrm{F}_\mathfrak{o}^n)$, $\mathrm{I}_{\mathrm{As}}(\mathrm{X},\Phi,\mathrm{W})\in\mathrm{R}(\mathrm{X})$ *is a rational function. Moreover, as* W *varies in* $\mathcal{W}(\pi,\psi)$, *and* Φ *varies in* $\mathscr{C}_c^\infty(\mathrm{F}_\mathfrak{o}^n)$, *these functions generate a* $\mathrm{R}[\mathrm{X}^{\pm1}]$*-fractional ideal of* $\mathrm{R}(\mathrm{X})$ *independent of the choice of* ψ.

In the setting of the lemma, it follows that there is a unique generator $\mathrm{L}_{\mathrm{As}}(\mathrm{X},\pi)$, which is a Euler factor and is independent of the character ψ. We call $\mathrm{L}_{\mathrm{As}}(\mathrm{X},\pi)$ the *Asai* L*-factor* of π.

For $s(X)$ of the form $1/P(X)$ for $P(X)\in\in\overline{\mathbb{Z}_\ell}[X]$ with non-zero reduction modulo ℓ, we write $r_\ell(s(X))=1/r_\ell(P(X))$. If P and Q are two non-zero elements of $k[X]$ for any field k, we write

$$1/P(X)\mid 1/Q(X)\quad\text{if } P(X)\mid Q(X).$$

LEMMA 7.2. — *Let* π *be an integral cuspidal* $\overline{\mathbb{Q}_\ell}$*-representations of* G *and* $\overline{\pi}$ *its reduction modulo* ℓ.

(i) *Then,* $\mathrm{L}_{\mathrm{As}}(\mathrm{X},\pi)$ *is the inverse of a polynomial in* $\overline{\mathbb{Z}_\ell}[\mathrm{X}]$.
(ii) *Moreover,*

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X},\overline{\pi})\mid r_\ell(\mathrm{L}_{\mathrm{As}}(\mathrm{X},\pi))$$

with constant term equal to 1.

Proof. — The first part (i) follows from the asymptotic expansion of Whittaker functions as in [17, Corollary 3.6]. The second part (ii) follows by imitating the proof of [17, Theorem 3.13]. We recall the argument here: by definition, we can

write the L-factor $\mathrm{L}_{\mathrm{As}}(\mathrm{X},\overline{\pi})$ as a finite sum of Asai integrals; for $i\in\{1,\dots,r\}$, there are $\Phi_i\in\mathscr{C}_c^\infty(\mathrm{F}_{\mathrm{o}}^n)$ and $\mathrm{W}_i\in\mathcal{W}(\overline{\pi},\overline{\psi})$, such that

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X},\overline{\pi})=\sum_{i=1}^{r}\mathrm{I}_{\mathrm{As}}(\mathrm{X},\Phi_i,\mathrm{W}_i).$$

By [17, Lemma 2.23] there are Whittaker functions $\mathrm{W}_{i,e}\in\mathcal{W}(\pi,\psi)$ that take values in $\overline{\mathbb{Z}_\ell}$, such that $\mathrm{W}_i=r_\ell(\mathrm{W}_{i,e})$, and clearly there are Schwartz functions $\Phi_{i,e}\in\mathscr{C}_c^\infty(\mathrm{F}_{\mathrm{o}}^n)$ that take values in $\overline{\mathbb{Z}_\ell}$, such that $\Phi_i=r_\ell(\Phi_{i,e})$. Moreover,

$$\sum_{i=1}^{r}\mathrm{I}_{\mathrm{As}}(\mathrm{X},\Phi_{i,e},\mathrm{W}_{i,e})\in\mathrm{L}_{\mathrm{As}}(\mathrm{X},\pi)\overline{\mathbb{Q}_\ell}[\mathrm{X}^{\pm1}]\cap\overline{\mathbb{Z}_\ell}((\mathrm{X}))=\mathrm{L}_{\mathrm{As}}(\mathrm{X},\pi)\overline{\mathbb{Z}_\ell}[\mathrm{X}^{\pm1}],$$

and, hence, $\mathrm{L}_{\mathrm{As}}(\mathrm{X},\overline{\pi})=\sum_{i=1}^{r}\mathrm{I}_{\mathrm{As}}(\mathrm{X},\Phi_i,\mathrm{W}_i)\in r_\ell(\mathrm{L}_{\mathrm{As}}(\mathrm{X},\pi))\overline{\mathbb{F}_\ell}[\mathrm{X}^{\pm1}]$. □

As we shall see later, strict divisions occur.

7.2. Test vectors. — In [4], test vectors for the Asai integral of a distinguished supercuspidal $\overline{\mathbb{Q}_\ell}$-representation were given with the Asai integral computed explicitly. The pro-order of a compact open subgroup of G_{o} may be zero in $\overline{\mathbb{F}_\ell}$, and so one cannot normalise a right Haar measure with values in $\overline{\mathbb{F}_\ell}$ arbitrarily. So, for compatibility with reduction modulo ℓ, we need to be more careful with normalisation of measures over $\overline{\mathbb{Q}_\ell}$. We set $\mathrm{K}=\mathrm{GL}_n(\mathscr{O})$ and $\mathrm{K}_{\mathrm{o}}=\mathrm{K}^\sigma$, $\mathrm{K}_{\mathrm{o}}^1=\mathrm{I}_n+\mathcal{M}_n(\mathscr{O}_{\mathrm{o}})$, and P the σ-stable mirabolic subgroup of G of all elements with final row $(\,0\ \cdots\ 0\ 1\,)$.

Definition 7.3. — A triple $(\mathbf{J},\boldsymbol{\lambda},\psi)$ with $(\mathbf{J},\boldsymbol{\lambda})$ a σ-self-dual R-type, and ψ a distinguished non-degenerate character of N satisfying conditions (i) and (ii) of [4, Lemma 6.8] will be called an *adapted type*.

Remark 7.4. —
(i) In particular, if $(\mathbf{J},\boldsymbol{\lambda},\psi)$ is an adapted type, the type $(\mathbf{J},\boldsymbol{\lambda})$ is a σ-self-dual ψ-generic type (in particular, ψ is distinguished).
(ii) By the proof of [4, Lemma 6.8], if π is a σ-self-dual cuspidal R-representation, it contains an adapted type, the point of the remark being that the N of [4, Lemma 6.8] can be chosen to be our N: the group of unipotent upper triangular matrices in G.

Now let π be a σ-self-dual cuspidal R-representation and $(\mathbf{J},\boldsymbol{\lambda},\psi)$ be an adapted type of π. We associate to $(\mathbf{J},\boldsymbol{\lambda},\psi)$ the *Paskunas–Stevens Whittaker function* $\mathrm{W}_{\boldsymbol{\lambda}}\in\mathcal{W}(\pi,\psi)$ defined in [4, (6.3)]. Note that $\mathrm{W}_{\boldsymbol{\lambda}}$ takes values in $\overline{\mathbb{Z}_\ell}$ as soon as π is integral (see, for example, [18, Lemma 10.2]). One of the main results of [4] is that this Whittaker function is a test vector for the Asai L-factor:

Proposition 7.5 ([4, Theorem 7.14]). — *Let π be a distinguished supercuspidal $\overline{\mathbb{Q}_\ell}$-representation of* G *and* $\mathrm{W}_{\boldsymbol{\lambda}}$ *be the explicit Whittaker function defined*

above. There is a unique normalisation of the invariant measure on $\mathrm{N}_{\mathfrak{o}} \setminus \mathrm{G}_{\mathfrak{o}}$*, such that*

$$\mathrm{I}_{\mathrm{As}}(\mathrm{X}, \mathbf{1}_{\mathfrak{o}_{\mathrm{F}}^n}, \mathrm{W}_{\boldsymbol{\lambda}}) = (q_{\mathfrak{o}} - 1)(q_{\mathfrak{o}}^{n/e_{\mathfrak{o}}(\pi)} - 1)\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi).$$

The volume of $\mathrm{N}_{\mathfrak{o}} \cap \mathrm{K}_{\mathfrak{o}}^1 \setminus \mathrm{K}_{\mathfrak{o}}^1$ *is of the form* p^l *for* $l \in \mathbb{Z}$ *with this normalisation.*

Proof. — We start with Haar measures dg and dn on $\mathrm{G}_{\mathfrak{o}}$ with values in $\overline{\mathbb{Q}_\ell}$ normalised by $dg(\mathrm{K}_{\mathfrak{o}}^1) = 1$ and $dg(\mathrm{N}_{\mathfrak{o}} \cap \mathrm{K}_{\mathfrak{o}}^1) = 1$, which, in turn, normalises the measure (still denoted dg) on the quotient $\mathrm{N}_{\mathfrak{o}} \setminus \mathrm{G}_{\mathfrak{o}}$.

With this normalisation, which is the exact parallel of the normalisation used in [18] for the analogue Rankin–Selberg computation, first of all we get an extra factor of $(q_{\mathfrak{o}} - 1)$ on the top of the Tate factor defined before [4, Lemma 7.11]. Then there is a factor $dk((\mathrm{P}^\sigma \cap \mathrm{K}^\sigma) \setminus \mathrm{J}^\sigma)$, which appears in [4, Lemma 6.11], and we have

$$dk((\mathrm{P}^\sigma \cap \mathrm{J}^\sigma) \setminus \mathrm{J}^\sigma) = dk((\mathrm{P}^\sigma \cap (\mathrm{J}^1)^\sigma) \setminus (\mathrm{J}^1)^\sigma)|\mathrm{J}^\sigma/(\mathrm{P}^\sigma \cap \mathrm{J}^\sigma)(\mathrm{J}^1)^\sigma)|.$$

As $dk((\mathrm{P}^\sigma \cap (\mathrm{J}^1)^\sigma) \setminus (\mathrm{J}^1)^\sigma)$ is a (possibly negative) power of p, we can renormalise our measure to remove it. The image of $\mathrm{P} \cap \mathrm{J}$ modulo J^1 is a σ-stable mirabolic $\overline{\mathrm{P}}_m(\mathrm{k}_{\mathrm{E}})$ of J/J^1, and we thus have

$$|\mathrm{J}^\sigma/(\mathrm{P}^\sigma \cap \mathrm{J}^\sigma)(\mathrm{J}^1)^\sigma)| = |\,\mathrm{GL}_m(\mathrm{k}_{\mathrm{E}})^\sigma/\overline{\mathrm{P}}_m(\mathrm{k}_{\mathrm{E}})^\sigma| = q_0^{n/e_{\mathfrak{o}}(\pi)} - 1$$

due to Lemma 6.5. □

Corollary 7.6. — *Suppose that* π *is an unramified twist of a relatively banal distinguished cuspidal* $\overline{\mathbb{F}_\ell}$*-representation, and let* $\widetilde{\pi}$ *be a supercuspidal lift of* π*. Then,*

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) = r_\ell(\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \widetilde{\pi})).$$

Proof. — Let $\widetilde{\pi}$ be such a lift. Due to Theorem 6.11 there is an unramified character $\widetilde{\chi}$ of $\mathrm{F}^\times$, such that $\widetilde{\pi}_0 = (\widetilde{\chi} \circ \det)^{-1} \otimes \widetilde{\pi}$ is distinguished. Let $(\mathbf{J}, \widetilde{\boldsymbol{\lambda}}, \widetilde{\psi})$ be an adapted type of $\widetilde{\pi}_{\mathfrak{o}}$. Proposition 7.5 then implies that

$$\mathrm{I}_{\mathrm{As}}(\mathrm{X}, \mathbf{1}_{\mathfrak{o}_{\mathrm{F}}^n}, \mathrm{W}_{\boldsymbol{\lambda}}) = (q_{\mathfrak{o}} - 1)(q_{\mathfrak{o}}^{n/e_{\mathfrak{o}}(\pi)} - 1)\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi_{\mathfrak{o}}).$$

Then, setting $\pi_{\mathfrak{o}} = r_\ell(\widetilde{\pi}_{\mathfrak{o}})$, we deduce that

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi_{\mathfrak{o}}) = r_\ell(\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \widetilde{\pi}_{\mathfrak{o}}))$$

in the exact same way that [18, Corollary 10.1] follows from [18, Proposition 9.3]. We obtain the statement of the corollary by twisting $\widetilde{\pi}_{\mathfrak{o}}$ by $\widetilde{\chi} \circ \det$ in this equality, as it sends X to $\chi(\varpi_{\mathfrak{o}})\mathrm{X}$ on the left-hand side and to $\widetilde{\chi}(\varpi_{\mathfrak{o}})\mathrm{X}$ on the right-hand side. □

7.3. Asai L-factors of cuspidal representations. — We first recall the computation of the Asai L-function of a cuspidal $\overline{\mathbb{Q}_\ell}$-representation:

PROPOSITION 7.7 ([4, Corollary 7.6] and Remark 7.7). — *Let π be a cuspidal $\overline{\mathbb{Q}_\ell}$-representation. If no unramified twist of π is distinguished, then* $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) = 1$. *If π is distinguished, then*

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) = \frac{1}{1 - \mathrm{X}^{n/e_{\mathfrak{o}}(\pi)}}.$$

This gives a complete description in the cuspidal case; as for an unramified character $\chi : \mathrm{F}^\times \to \mathrm{K}^\times$, we have

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X}, (\chi \circ \det) \otimes \pi) = \mathrm{L}_{\mathrm{As}}(\chi(\varpi_{\mathfrak{o}})\mathrm{X}, \pi).$$

THEOREM 7.8. — *Let π be a cuspidal $\overline{\mathbb{F}_\ell}$-representation of* $\mathrm{GL}_n(\mathrm{F})$.

(i) *If π is an unramified twist $(\chi \circ \det) \otimes \pi_0$ of a relatively banal distinguished representation π_0, then*

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) = \frac{1}{1 - (\chi(\varpi_{\mathfrak{o}})\mathrm{X})^{n/e_{\mathfrak{o}}(\pi)}}.$$

(ii) *If π is not an unramified twist of a relatively banal distinguished representation, then*

$$\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) = 1.$$

Proof. — If π is an unramified twist of a relatively banal distinguished representation, the statement follows, for example, from Corollary 7.6 and Proposition 7.7.

If π is not an unramified twist of a relatively banal distinguished representation, it has a supercuspidal lift $\widetilde{\pi}$, which is not an unramified twist of a distinguished representation due to Theorem 6.11. By Proposition 7.7 we have $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \widetilde{\pi}) = 1$, and, hence, $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) = 1$ as $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) \mid r_\ell(\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \widetilde{\pi}))$ by Lemma 7.2. □

REMARK 7.9. — Note that when $\ell = 2$, we are in case (ii) of Theorem 7.8, and $\mathrm{L}_{\mathrm{As}}(\mathrm{X}, \pi) = 1$. This can also be seen directly from the asymptotics of Whittaker functions. Without entering the details as we do not need to, the asymptotic expansion of Whittaker functions on the diagonal torus allow one to express the Asai integrals in terms of Tate integrals for $\mathrm{F}_{\mathfrak{o}}^\times$, and these Tate integrals are all 1 because $q = 1[2]$, as shown in [22].

8. Distinction and poles of the Asai L-factor

8.1. Characterisation of the poles of the Asai L-factor. — We are now in position to prove the main results of this paper:

THEOREM 8.1. — *Let π be a cuspidal $\overline{\mathbb{F}_\ell}$-representation of* G*. Then,* $L_{As}(X,\pi)$ *has a pole at* $X=1$*, if and only if π is relatively banal distinguished. In this case, the pole is of order ℓ^r, where $n/e_{\mathfrak{o}}(\pi)=a\ell^r$ with a prime to ℓ.*

Proof. — If $L_{As}(X,\pi)$ has a pole at $X=1$, in particular $L_{As}(X,\pi)$ is not equal to 1, and, hence, the representation π is an unramified twist of a relatively banal distinguished cuspidal $\overline{\mathbb{F}_\ell}$-representation π_0, say $\pi=(\chi\circ\det)\otimes\pi_0$, with χ an unramified character of $F^\times$. Denote by $\chi_{\mathfrak{o}}$ the restriction of χ to $F_{\mathfrak{o}}^\times$, then by Theorem 7.8,

$$L_{As}(X,\pi)=\frac{1}{1-(\chi_{\mathfrak{o}}(\varpi_{\mathfrak{o}})X)^{n/e_{\mathfrak{o}}(\pi)}}=\frac{1}{(1-(\chi_{\mathfrak{o}}(\varpi_{\mathfrak{o}})X)^a)^{\ell^r}}$$

which has a pole at $X=1$, if and only if $\chi_{\mathfrak{o}}(\varpi_{\mathfrak{o}})^{n/e_{\mathfrak{o}}(\pi)}=1$. By Theorem 5.16 this implies that $\chi_{\mathfrak{o}}\circ\det$ belongs to $X_{\mathfrak{o}}(\pi)$, i.e. that $\pi=(\chi\circ\det)\otimes\pi_0$ is distinguished. The converse is just Theorem 7.8. □

REMARK 8.2. — Note that our proof of Theorem 8.1 is very different from the proof over the field of complex numbers. In the proof above, the direction π relatively banal distinguished implies $L_{As}(X,\pi)$ having a pole at 1 is an immediate consequence of Theorem 7.8 and works for complex representations as well (in which case, we consider all cuspidal distinguished $\mathbb{C}$-representations as "relatively banal") due to [4, Corollary 7.6]. Saying this is not enough to claim a proof in the case of complex cuspidal representations different from the original one given in [1, Theorem 1.4], as the way the equality of [4, Corollary 7.6] is obtained is a consequence of [20, Proposition 6.3], which itself follows either from [20, Theorem 3.1] or from [1, Theorem 1.4] and [14, Theorem 4], together with the fact that the poles of the Asai L-factor are simple in the cuspidal case. However, the first equality in [4, Theorem 7.14] is independent of the results cited above, and it in particular implies that, if π is a cuspidal distinguished $\mathbb{C}$-representation, its Asai L-factor has a pole at $X=1$. The proof of the other implication that we give also works in the complex case, and is again different from the original proof given in [14, Theorem 4]. Kable shows that, if $L_{As}(X,\pi)$ has a pole at $X=1$, the rational function $(1-X)I_{As}(X,W,\Phi)$ is regular at $X=1$ and that up to a non-zero constant independent of W and Φ its value at $X=1$ is given by

$$\Phi(0)\int_{Z^\sigma N^\sigma\backslash G^\sigma}W(h)dh.$$

As by assumption the Asai L-factor has a pole at $X=1$, the G^σ-invariant linear form

$$\mathcal{L}_\pi : W\mapsto\int_{Z^\sigma N^\sigma\backslash G^\sigma}W(h)dh$$

is non-zero. Note that to adapt this proof to the modular setting with $\mathrm{R} = \overline{\mathbb{F}_\ell}$ we would need to take $1-\mathrm{X}^{n/e_{\mathfrak{o}}(\pi)}$, where Kable takes $1-\mathrm{X}$ (this does not matter over $\mathbb{C}$, as both polynomials have a simple zero at $\mathrm{X} = 1$) to get the correct order of the pole, although from Kable's proof, one sees that the natural choice is, in fact, $1-\mathrm{X}^n$. However, we claim that this cannot be done in general, as we shall now see that the local period $\mathcal{L}_\pi$, although well defined for cuspidal $\overline{\mathbb{F}_\ell}$-representations, might vanish even for relatively banal distinguished cuspidal $\overline{\mathbb{F}_\ell}$-representations.

8.2. The $\mathrm{G}_{\mathfrak{o}}$-period of cuspidal distinguished representations. — Let π be a cuspidal distinguished R-representation; we still denote by ψ a distinguished non-degenerate character of N. There are two natural G^σ-invariant linear forms on $\mathcal{W}(\pi, \psi)$. The first is

$$\mathcal{P}_\pi : \mathrm{W} \mapsto \int_{\mathrm{N}^\sigma \backslash \mathrm{P}^\sigma} \mathrm{W}(p)dp$$

which is well-defined and non-zero due to [28, Chapter III, Theorem 1.1]. Although it does not look G^σ-invariant, it is so by [4, Proposition B.23]. Let $(\mathbf{J}, \boldsymbol{\lambda}, \psi)$ be an adapted type in π. A natural test vector for this linear form is the Paskunas–Stevens Whittaker function $\mathrm{W}_{\boldsymbol{\lambda}}$; we have $\mathcal{P}_\pi(\mathrm{W}_{\boldsymbol{\lambda}}) \neq 0$ according to the proof of [4, Proposition 6.5].

The second is

$$\mathcal{L}_\pi : \mathrm{W} \mapsto \int_{\mathrm{Z}^\sigma \mathrm{N}^\sigma \backslash \mathrm{G}^\sigma} \mathrm{W}(h)dh.$$

It is G^σ-invariant by definition, and well defined, as all $\mathrm{W} \in \mathcal{W}(\pi, \psi)$ have compact support on $\mathrm{N} \setminus \mathrm{P}$; they have compact support of $\mathrm{ZN} \setminus \mathrm{G}$ due to the Iwasawa decomposition $\mathrm{G} = \mathrm{PZK}$. By cuspidal multiplicity one for the pair $(\mathrm{P}, \mathrm{P}^\sigma)$ ([4, Proposition B.23]), $\mathcal{L}_\pi$ is a multiple of $\mathcal{P}_\pi$, and the proportionality constant between them turns out to be a very interesting quantity; this scalar is related to the formal degrees of complex discrete series representations of unitary groups (see [2] and Remark 8.4). When $\mathrm{R} = \overline{\mathbb{Q}_\ell}$ the linear form, $\mathcal{L}_\pi$ is non-zero (Remark 8.2); here, we solve the problem of understanding when $\mathcal{L}_\pi$ is non-zero when $\mathrm{R} = \overline{\mathbb{F}_\ell}$:

THEOREM 8.3. — *Let π be a cuspidal distinguished $\overline{\mathbb{F}_\ell}$-representation of* G*, then $\mathcal{L}_\pi$ is non-zero, if and only if:*

(i) *π is relatively banal.*
(ii) *ℓ does not divide $e_{\mathfrak{o}}(\pi)$.*

Proof. — Due to the Iwasawa decomposition $\mathrm{G} = \mathrm{PZK}$, we have the equality:

$$\int_{\mathrm{Z}^\sigma \mathrm{N}^\sigma \backslash \mathrm{G}^\sigma} \mathrm{W}(h)dh = \int_{\mathrm{K}^\sigma \cap \mathrm{P}^\sigma \backslash \mathrm{K}^\sigma} \int_{\mathrm{N}^\sigma \backslash \mathrm{P}^\sigma} \mathrm{W}(pk)|\det(pk)|_{\mathfrak{o}}^{-1} dpdk.$$

We introduce the power series

$$\mathrm{I}_{\mathrm{As},(0)}(\mathrm{X},\mathrm{W}) = \sum_{l\in\mathbb{Z}} \left(\int_{\mathrm{N}^\sigma\backslash \mathrm{P}^{\sigma\,(l)}} \mathrm{W}(p)|\det(p)|_{\mathfrak{o}}^{-1} dp \right) \mathrm{X}^l$$

where $\mathrm{P}^{\sigma\,(l)} = \{p \in \mathrm{P}^\sigma,\ \mathrm{val}_{\mathrm{F}_{\mathfrak{o}}}(\det(p)) = l\}$ which is, in fact, a Laurent polynomial, as π is cuspidal, so that

$$\mathcal{P}_\pi(\mathrm{W}) = \mathrm{I}_{\mathrm{As},(0)}(1,\mathrm{W}).$$

Now suppose that π is not relatively banal; then, π is $|\det(\,\cdot\,)|_{\mathfrak{o}}$-distinguished, and appealing to [4, Proposition B.23], it means that the linear form

$$\mathcal{P}_{\pi,|\det(\,\cdot\,)|_{\mathfrak{o}}} : \mathrm{W} \mapsto \int_{\mathrm{N}^\sigma\backslash \mathrm{P}^\sigma} \mathrm{W}(p)|\det(p)|_{\mathfrak{o}}^{-1} dp$$

is $|\det(\,\cdot\,)|_{\mathfrak{o}}$-equivariant under the action of $\mathrm{G}_{\mathfrak{o}}$. So, in particular, up to possible renormalisation of the invariant measure,

$$\begin{aligned}\int_{\mathrm{Z}^\sigma\mathrm{N}^\sigma\backslash \mathrm{G}^\sigma} \mathrm{W}(h)dh &= \mathrm{vol}(\mathrm{K}^\sigma \cap \mathrm{P}^\sigma \setminus \mathrm{K}^\sigma)\mathcal{P}_{\pi,|\det(\,\cdot\,)|_{\mathfrak{o}}}(\mathrm{W}) \\ &= (q_{\mathfrak{o}}^n - 1)\mathcal{P}_{\pi,|\det(\,\cdot\,)|_{\mathfrak{o}}}(\mathrm{W}) = 0\end{aligned}$$

as $q_{\mathfrak{o}}^{n/e_{\mathfrak{o}}(\pi)} = 1$.

So it remains to understand what happens when π is relatively banal. As we said, by multiplicity one we know that $\mathcal{L}_\pi = \lambda\mathcal{P}_\pi$ and we noticed that $\mathcal{P}_\pi(\mathrm{W}_{\boldsymbol{\lambda}}) \neq 0$. Hence, $\mathcal{L}_\pi = 0$, if and only if $\mathcal{L}_\pi(\mathrm{W}_{\boldsymbol{\lambda}}) = 0$. However, following the proof of [18, Theorem 9.1] at the end of [18, p. 19] or the proof of [4, Theorem 7.14], one gets up to a possible renormalisation of invariant measures:

$$\begin{aligned}\mathcal{L}_{\pi,\mathrm{X}}(\mathrm{W}_{\boldsymbol{\lambda}}) &:= \int_{\mathrm{K}^\sigma\cap\mathrm{P}^\sigma\backslash\mathrm{K}^\sigma} \mathrm{I}_{\mathrm{As},(0)}(\mathrm{X},\rho(k)\mathrm{W}_{\boldsymbol{\lambda}})dk \\ &= (q_{\mathfrak{o}}-1)(q_{\mathfrak{o}}^{n/e_{\mathfrak{o}}(\pi)}-1)\frac{1-\mathrm{X}^n}{1-\mathrm{X}^{n/e_{\mathfrak{o}}(\pi)}}.\end{aligned}$$

Now, the value at $\mathrm{X}=1$ of $\mathcal{L}_{\pi,\mathrm{X}}$ is $\mathcal{L}_\pi$, so $\mathcal{L}_\pi$ vanishes, if and only if $\frac{1-\mathrm{X}^n}{1-\mathrm{X}^{n/e_{\mathfrak{o}}(\pi)}}$ vanishes at $\mathrm{X}=1$. However, the order of the zero of $1-\mathrm{X}^n$ is the $\ell^{\mathrm{val}_\ell(n)}$, whereas that of the zero of $1-\mathrm{X}^{n/e_{\mathfrak{o}}(\pi)}$ is $\ell^{\mathrm{val}_\ell(n/e_{\mathfrak{o}}(\pi))}$. This means that, if π is relatively banal, $\mathcal{L}_\pi$ is non-zero, if and only if $\mathrm{val}_\ell(n) = \mathrm{val}_\ell(n/e_{\mathfrak{o}}(\pi))$, i.e., if and only if ℓ does not divide $e_{\mathfrak{o}}(\pi)$. □

Remark 8.4. — Here, we explain how this vanishing result modulo ℓ is related to the vanishing of the ℓ-adic proportionality constant between $\mathcal{L}$ and $\mathcal{P}$. For an algebraically closed field $\mathbf{C}$, write $\mathrm{Cusp}_{\mathbf{C},\mathrm{dist}}(\mathrm{G})$ for the set of isomorphism classes of distinguished cuspidal $\mathbf{C}$-representations. Fix an isomorphism $\mathbb{C} \simeq \overline{\mathbb{Q}_\ell}$; this induces a bijection $\mathrm{Cusp}_{\mathbb{C},\mathrm{dist}}(\mathrm{G}) \to \mathrm{Cusp}_{\overline{\mathbb{Q}_\ell},\mathrm{dist}}(\mathrm{G})$, depending on the choice of isomorphism.

Let $\pi \in \mathrm{Cusp}_{\overline{\mathbb{Q}_\ell},\mathrm{dist}}(\mathrm{G})$ and $\psi : \mathrm{N} \to \overline{\mathbb{Z}_\ell}^\times$ be an N^σ-distinguished non-degenerate character of N. Then, by [1, Corollary 1.2], there exists $\mu \in \overline{\mathbb{Q}_\ell}$, such that

$$\mathcal{L}_\pi = \mu \mathcal{P}_\pi, \tag{3}$$

Let c_π denote the central character of π and Res_P denote the restriction of Whittaker functions to P. Then,

$$\mathcal{W}(\pi,\psi) \subset \mathrm{ind}_{\mathrm{ZN}}^{\mathrm{G}}(c_\pi \otimes \psi) \text{ and } \mathrm{Res}_\mathrm{P}(\mathcal{W}(\pi,\psi)) \subset \mathrm{ind}_{\mathrm{N}}^{\mathrm{P}}(\psi),$$

the first fact being a consequence of the second, which has been known since [5]. Now let $\mathcal{W}(\pi,\psi)_e$ denote the $\overline{\mathbb{Z}_\ell}$-submodule of $\mathcal{W}(\pi,\psi)$ consisting of Whittaker functions with values in $\overline{\mathbb{Z}_\ell}$. It follows from [30, Theorem 2] and [29, Theorem 2] that $\mathcal{W}(\pi,\psi)_e$ is a lattice in $\mathcal{W}(\pi,\psi)$, and $\mathrm{Res}_\mathrm{P}(\mathcal{W}(\pi,\psi)_e) = \mathrm{ind}_{\mathrm{N}}^{\mathrm{P}}(\psi, \overline{\mathbb{Z}_\ell})$ is a lattice in $\mathrm{Res}_\mathrm{P}(\mathcal{W}(\pi,\psi))$, reducing to $\mathcal{W}(\pi,\psi)$ and $\mathrm{Res}_\mathrm{P}(\mathcal{W}(\pi,\psi))$, respectively.

Finally, from [17, Section 2.2], there are appropriate ℓ-adic and ℓ-modular invariant measures on $\mathrm{Z}^\sigma\mathrm{N}^\sigma \setminus \mathrm{G}^\sigma$ and $\mathrm{N}^\sigma \setminus \mathrm{P}^\sigma$, such that

$$r_\ell(\mathcal{L}_\pi(\mathrm{W}_e)) = \mathcal{L}_{r_\ell(\pi)}(r_\ell(\mathrm{W}_e)), \tag{4}$$

$$r_\ell(\mathcal{P}_\pi(\mathrm{W}_e)) = \mathcal{P}_{r_\ell(\pi)}(r_\ell(\mathrm{W}_e)) \tag{5}$$

for all $\mathrm{W}_e \in \mathrm{W}(\pi,\psi)_e$ and $\mathcal{P}_\pi(\mathrm{Res}_\mathrm{P}(\mathcal{W}(\pi,\psi)_e)) = \overline{\mathbb{Z}_\ell}$.

Evaluating Equation 3 on an element $\mathrm{W}_e \in \mathcal{W}(\pi,\psi)_e$, such that $\mathcal{P}_\pi(\mathrm{W}_e) = 1$, we deduce that $\mu \in \overline{\mathbb{Z}_\ell}$. Now, Theorem 8.3 and Equations 4 and 5 imply that ℓ divides μ, if and only if either $r_\ell(\pi)$ is not relatively banal or $\ell \mid e_\mathfrak{o}(\pi)$. Running over all $\ell \neq p$, we recover the radical of the p-regular part of μ (explicitly using the type theoretic definition of relatively banal, Definition 6.2).

As was mentioned already, this scalar μ is a very interesting and subtle quantity. By [2, Theorem 7.1], we have

$$\mathcal{L}_\pi = \lambda \frac{d(\rho)}{d(\pi)} \mathcal{P}_\pi,$$

where λ is a constant independent of π, ρ is the cuspidal $\overline{\mathbb{Q}_\ell}$-representation of the quasi-split unitary group in n-variables defined over $\mathrm{F}_\mathfrak{o}$ which base changes to π (stably or unstably depending on the parity of n), and $d(\rho)$ and $d(\pi)$ denote the formal degrees of ρ and π, respectively, under the normalisation of invariant measures of [12]. One could check that the formal degrees are rational for our well-chosen measures (and λ as well), and preserved under the bijection $\mathrm{Cusp}_{\mathbb{C},\mathrm{dist}}(\mathrm{G}) \to \mathrm{Cusp}_{\overline{\mathbb{Q}_\ell},\mathrm{dist}}(\mathrm{G})$.

While we have explained how Theorem 8.3 tells us exactly when μ vanishes modulo ℓ, we could also go in the other direction. By [12] and [6], the constant μ could be computed explicitly, and its explicit description would give a different proof of Theorem 8.3. It should be clear to the reader that the amount of work

required for such a proof is much more considerable than that of the proof given above.

8.3. Comparison of banal and relatively banal. — Finally, we compare our notion of relatively banal distinguished with the notion of banal representation introduced in [24] for cuspidal representations.

By [24, Remarque 8.15] a cuspidal $\overline{\mathbb{F}_\ell}$-representation π of $\mathrm{G}_\mathfrak{o}$ is banal, if and only if

$$|\det(\ )|_\mathfrak{o} \otimes \pi \not\simeq \pi.$$

However, the map

$$b : \pi \mapsto \pi \otimes \pi^\vee$$

is a bijection between the set of (isomorphism classes of) irreducible representations of $\mathrm{G}_\mathfrak{o}$ and the set of $\Delta(\mathrm{G}_\mathfrak{o})$-distinguished irreducible representations of $\mathrm{G}' = \mathrm{G}_\mathfrak{o} \times \mathrm{G}_\mathfrak{o}$, where Δ is the diagonal embedding of $\mathrm{G}_\mathfrak{o}$ into G'. In particular, π (seen as the distinguished representation $b(\pi)$ of G') is banal, if and only if $|\det(\ )|_\mathfrak{o} \otimes b(\pi) = (|\det(\ )|_\mathfrak{o} \otimes \pi) \otimes \pi^\vee$ is not distinguished. Note that $|\ |_\mathfrak{o}$ plays the same role for the split quadratic algebra $(\mathrm{F}_\mathfrak{o} \times \mathrm{F}_\mathfrak{o})/\mathrm{F}_\mathfrak{o}$ that $|\ |_\mathfrak{o}$ plays for $\mathrm{F}/\mathrm{F}_\mathfrak{o}$, i.e. it is a square root of the absolute value on the bigger algebra. So, this proves the exact analogy of banal cuspidal representations of $\mathrm{G}_\mathfrak{o}$ and relatively banal distinguished cuspidal representations of G according to Corollary 6.3.

The analogy can also be seen at the L-factor level; it follows from [18, Theorem 4.9] that, if $\pi \otimes \pi'$ is a cuspidal representation of G', then the Rankin–Selberg L-factor $\mathrm{L}(\mathrm{X}, \pi, \pi')$ (which can be thought of as the Asai L-factor of $\pi \otimes \pi'$) has a pole at $\mathrm{X} = 1$, if and only if $\pi \otimes \pi'$ is $\Delta(\mathrm{G}_\mathfrak{o})$-distinguished, and π is banal, which is the exact analogue of Theorem 8.1 replacing banal with relatively banal.

Finally, in terms of the type theory definition, a cuspidal representation π of $\mathrm{G}_\mathfrak{o}$ is banal, if and only if $q_\mathfrak{o}^{n/e(\pi)} \not\equiv 1[\ell]$, but tracking down how $e(\pi)$ is defined with respect to π in terms of type theory (more precisely lattice periods) shows that it plays the same role for the $\Delta(\mathrm{G}_\mathfrak{o})$-distinguished representation $b(\pi)$ of G' that $e_\mathfrak{o}(\tau)$ plays for a distinguished cuspidal representation τ of G.

Acknowledgements. — It is a pleasure to thank Vincent Sécherre for motivating discussions and very useful explanations concerning his paper [27]. We thank David Helm and Alberto Mínguez for their interest and useful conversations.

Parts of the paper were written while the second author was at the conferences "On the Langlands Program: Endoscopy and Beyond" held at the IMS of the National University of Singapore in 2018/2019 and "Automorphic Forms, Automorphic Representations and Related Topics" held at the RIMS of the University of Kyoto in 2019. He would like to thank the organisers of both conferences, especially Wee Teck Gan and Shunsuke Yamana, and both institutions for their hospitality. Finally, we thank the referee for useful comments.

BIBLIOGRAPHY

[1] U. K. Anandavardhanan, A. C. Kable & R. Tandon – "Distinguished representations and poles of twisted tensor L-functions", *Proc. Amer. Math. Soc.* **132** (2004), no. 10, p. 2875–2883.

[2] U. K. Anandavardhanan & N. Matringe – "Test vectors for finite periods and base change", *Adv. Math.* **360** (2020), p. 106915, 27.

[3] U. K. Anandavardhanan & C. S. Rajan – "Distinguished representations, base change, and reducibility for unitary groups", *Int. Math. Res. Not.* (2005), no. 14, p. 841–854.

[4] U. Anandavardhanan, R. Kurinczuk, N. Matringe, V. Sécherre & S. Stevens – "Galois self-dual cuspidal types and Asai local factors", arXiv:1807.07755. Accepted to appear in J. Eur. Math. Soc.

[5] I. N. Bernstein & A. V. Zelevinsky – "Representations of the group $\mathrm{GL}(n, F)$ where F is a non-Archimedean local field", *Russ. Math. Surv.* **31** (1976), no. 3, p. 1–68 (English).

[6] R. Beuzart-Plessis – "Plancherel formula for $\mathrm{GL}_n(\mathrm{F})\backslash\mathrm{GL}_n(\mathrm{E})$ and applications to the Ichino-Ikeda and formal degree conjectures for unitary groups", arXiv:1812.00047.

[7] C. J. Bushnell & P. C. Kutzko – *The admissible dual of* $\mathrm{GL}(N)$ *via compact open subgroups*, Annals of Mathematics Studies, vol. 129, Princeton University Press, Princeton, NJ, 1993.

[8] P. Delorme – "Constant term of smooth H_ψ-spherical functions on a reductive p-adic group", *Trans. Amer. Math. Soc.* **362** (2010), no. 2, p. 933–955.

[9] Y. Z. Flicker – "On distinguished representations", *J. Reine Angew. Math.* **418** (1991), p. 139–172.

[10] W. T. Gan, B. H. Gross & D. Prasad – "Symplectic local root numbers, central critical L values, and restriction problems in the representation theory of classical groups", *Astérisque* (2012), no. 346, p. 1–109, Sur les conjectures de Gross et Prasad. I.

[11] J. A. Green – "The characters of the finite general linear groups", *Trans. Amer. Math. Soc.* **80** (1955), p. 402–447.

[12] K. Hiraga, A. Ichino & T. Ikeda – "Formal degrees and adjoint γ-factors", *J. Amer. Math. Soc.* **21** (2008), no. 1, p. 283–304.

[13] G. James – "The irreducible representations of the finite general linear groups", *Proc. London Math. Soc. (3)* **52** (1986), no. 2, p. 236–268.

[14] A. C. Kable – "Asai L-functions and Jacquet's conjecture", *Amer. J. Math.* **126** (2004), no. 4, p. 789–820.

[15] S.-i. Kato & K. Takano – "Subrepresentation theorem for p-adic symmetric spaces", *Int. Math. Res. Not. IMRN* (2008), no. 11, p. Art. ID rnn028, 40.

[16] R. Kurinczuk – "ℓ-modular representations of unramified p-adic U$(2,1)$", *Algebra & Number Theory* **8** (2014), no. 8, p. 1801–1838.
[17] R. Kurinczuk & N. Matringe – "Rankin-Selberg local factors modulo ℓ", *Selecta Math. (N.S.)* **23** (2017), no. 1, p. 767–811.
[18] ———, "Test vectors for local cuspidal Rankin–Selberg integrals", *Nagoya Math. J.* (2017), p. 1–23.
[19] R. Kurinczuk, N. Matringe & V. Sécherre – "Galois distinguished ℓ-modular representations of p-adic GL$_n$", In preparation.
[20] N. Matringe – "Distinguished representations and exceptional poles of the Asai-L-function", *Manuscripta Math.* **131** (2010), no. 3-4, p. 415–426.
[21] ———, "Distinguished generic representations of GL(n) over p-adic fields", *Int. Math. Res. Not. IMRN* (2011), no. 1, p. 74–95.
[22] A. Mínguez – "Fonctions zêta ℓ-modulaires", *Nagoya Math. J.* **208** (2012), p. 39–65.
[23] A. Mínguez & V. Sécherre – "Représentations banales de GL$_m(D)$", *Compos. Math.* **149** (2013), no. 4, p. 679–704.
[24] ———, "Représentations lisses modulo ℓ de GL$_m(D)$", *Duke Math. J.* **163** (2014), no. 4, p. 795–887.
[25] C. P. Mok – "Endoscopic classification of representations of quasi-split unitary groups", *Mem. Amer. Math. Soc.* **235** (2015), no. 1108, p. vi+248.
[26] D. Prasad – "Trilinear forms for representations of GL(2) and local ϵ-factors", *Compositio Math.* **75** (1990), no. 1, p. 1–46.
[27] V. Sécherre – "Supercuspidal representations of GL$_n$(F) distinguished by a Galois involution", *Algebra Number Theory* **13** (2019), no. 7, p. 1677–1733.
[28] M.-F. Vignéras – *Représentations l-modulaires d'un groupe réductif p-adique avec $l \neq p$*, Progress in Mathematics, vol. 137, Birkhäuser Boston, Inc., Boston, MA, 1996.
[29] ———, "Integral Kirillov model", *C. R. Acad. Sci. Paris Sér. I Math.* **326** (1998), no. 4, p. 411–416.
[30] M.-F. Vignéras – "On highest Whittaker models and integral structures", in *Contributions to automorphic forms, geometry, and number theory*, Johns Hopkins Univ. Press, Baltimore, MD, 2004, p. 773–801.

Bull. Soc. Math. France
148 (3), 2020, p. 515-527

THE SCHUR MULTIPLIER OF FINITE SYMPLECTIC GROUPS

BY LOUIS FUNAR & WOLFGANG PITSCH

ABSTRACT. — We show that the Schur multiplier of $Sp(2g, \mathbb{Z}/D\mathbb{Z})$ is $\mathbb{Z}/2\mathbb{Z}$, when D is divisible by 4.

RÉSUMÉ (*Multiplicateur de Schur des groupes symplectiques finis*). — Nous montrons que le multiplicateur de Schur de $Sp(2g, \mathbb{Z}/D\mathbb{Z})$ est $\mathbb{Z}/2\mathbb{Z}$ quand D est divisible par 4.

1. Introduction and statements

Let $g \geq 1$ be an integer and denote by $Sp(2g, \mathbb{Z})$ the symplectic group of $2g \times 2g$ matrices with integer coefficients. Deligne's nonresidual finiteness theorem from [5] states that the *universal central extension* $\widetilde{Sp(2g, \mathbb{Z})}$ is not residually finite, since the image of its center under any homomorphism into a finite group has an order of at most 2 when $g \geq 3$. Our first motivation was to understand this result and give a sharp statement, namely to decide whether the

Texte reçu le 30 octobre 2013, modifié le 5 novembre 2019, accepté le 3 mars 2020.

LOUIS FUNAR, Institut Fourier BP 74, UMR 5582, Laboratoire de Mathématiques, Université Grenoble Alpes, CS 40700, 38058 Grenoble cedex 9, France • *E-mail :* `louis.funar@univ-grenoble-alpes.fr`

WOLFGANG PITSCH, Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra (Cerdanyola del Vallès), Spain • *E-mail :* `pitsch@mat.uab.es`

Mathematical subject classification (2010). — 57M50, 55N25, 19C09, 20F38.

Key words and phrases. — Symplectic groups, Group homology, Mapping class groups, Central extension, Residually finite group.

The first author was supported by the ANR 2011 BS 01 020 01 ModGroup and the second author by the FEDER/MEC grant MTM2016-80439-P.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037-9484/2020/515/$ 5.00
© Société Mathématique de France
doi:10.24033/bsmf.2815

image of the central $\mathbb{Z}$ might be of order 2. Since these symplectic groups have the congruence subgroup property, this boils down to understanding the second homology of symplectic groups with coefficients in finite cyclic groups. In the sequel, for simplicity and unless otherwise explicitly stated, all (co)homology groups will be understood to be with trivial integer coefficients. An old theorem of Stein (see [14], Thm. 2.13 and Prop. 3.3.a) is that $H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) = 0$, when D is not divisible by 4. The case $D \equiv 0 \pmod 4$ has remained open since then; this is explicitly mentioned, for instance, in [13] (Remarks after Thm. 3.8). Our main result settles this case.

THEOREM 1.1. — *The second homology group of finite principal congruence quotients of $Sp(2g, \mathbb{Z})$, $g \geq 3$ is*

$$H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}, \text{ if } D \equiv 0 \pmod 4.$$

In comparison, recall that Beyl (see [2]) showed that $H_2(SL(2, \mathbb{Z}/D\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}$, for $D \equiv 0 \pmod 4$, and Dennis and Stein proved using K-theoretic methods that for $n \geq 3$, we have $H_2(SL(n, \mathbb{Z}/D\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}$, for $D \equiv 0 \pmod 4$, while $H_2(SL(n, \mathbb{Z}/D\mathbb{Z})) = 0$, for $D \not\equiv 0 \pmod 4$ (see [6], Cor. 10.2 and [11], Section 12).

Our proof also relies on Deligne's nonresidual finiteness theorem from [5] and deep results of Putman in [13], and shows that we can detect this $\mathbb{Z}/2\mathbb{Z}$ factor on $H_2(Sp(2g, \mathbb{Z}/32\mathbb{Z}))$ for $g \geq 4$, providing an explicit extension that detects this homology class.

2. Preliminaries

2.1. Residual finiteness of universal central extensions. — In this section, we collect results about universal central extensions of perfect groups, for the sake of completeness of our arguments. Every perfect group Γ has a universal central extension $\widetilde{\Gamma}$; the kernel of the canonical projection map $\widetilde{\Gamma} \to \Gamma$ contains the center $Z(\widetilde{\Gamma})$ of $\widetilde{\Gamma}$ and is canonically isomorphic to the second integral homology group $H_2(\Gamma)$. We will recall now how the residual finiteness problem for the universal central $\widetilde{\Gamma}$ of a perfect and residually finite group Γ translates into an homological problem about $H_2(\Gamma)$. We start with a classical result for maps between universal central extensions of perfect groups.

LEMMA 2.1. — *Let Γ and F be perfect groups, $\widetilde{\Gamma}$ and $\widetilde{F}$ be their universal central extensions and $p : \Gamma \to F$ be a group homomorphism. Then, there exists a unique homomorphism $\widetilde{p} : \widetilde{\Gamma} \to \widetilde{F}$ lifting p such that the following*

diagram is commutative:

$$\begin{array}{ccccccc} 1 \to & H_2(\Gamma) & \to & \widetilde{\Gamma} & \to \Gamma & \to 1 \\ & p_* \downarrow & & \widetilde{p} \downarrow & \downarrow p & \\ 1 \to & H_2(F) & \to & \widetilde{F} & \to F & \to 1 \end{array}$$

For a proof we refer the interested reader to ([10], Chap. VIII) or ([4], Chap. IV, Ex. 1, 7). If Γ is a perfect residually finite group, to prove that its universal central extension $\widetilde{\Gamma}$ is also residually finite we only have to find enough finite quotients of $\widetilde{\Gamma}$ to detect the elements in its center $H_2(\Gamma)$. The following lemma analyzes the situation.

LEMMA 2.2. — *Let Γ be a perfect group and denote by $\widetilde{\Gamma}$ its universal central extension.*

1. *Let H be a finite index normal subgroup $H \subset \Gamma$ such that the image of $H_2(H)$ into $H_2(\Gamma)$ contains the subgroup $dH_2(\Gamma)$, for some $d \in \mathbb{Z}$. Let $F = \Gamma/H$ be the corresponding finite quotient of Γ and $p : \Gamma \to F$ the quotient map. Then, $d \cdot p_*(H_2(\Gamma)) = 0$, where $p_* : H_2(\Gamma) \to H_2(F)$ is the homomorphism induced by p. In particular, if $p_* : H_2(\Gamma) \to H_2(F)$ is surjective, then $d \cdot H_2(F) = 0$.*
2. *Assume that F is a finite quotient of Γ satisfying $d \cdot p_*(H_2(\Gamma)) = 0$. Let $\widetilde{F}$ denote the universal central extension of F. Then, the homomorphism $p : \Gamma \to F$ has a unique lift $\widetilde{p} : \widetilde{\Gamma} \to \widetilde{F}$, and the kernel of $\widetilde{p}$ contains $d \cdot H_2(\Gamma)$.*

Observe that in point 2. of Lemma 2.2 the group F being finite, $H_2(F)$ is also finite, and, hence, one can take $d = |H_2(F)|$.

Proof. — The image of H into F is trivial, and, thus, the image of $H_2(H)$ into $H_2(F)$ is trivial. This implies that $p_*(d \cdot H_2(\Gamma)) = 0$, which proves the first part of the lemma.

Further, by Lemma 2.1 there exists a unique lift $\widetilde{p} : \widetilde{\Gamma} \to \widetilde{F}$. If $d \cdot p_*(H_2(\Gamma)) = 0$, then Lemma 2.1 yields $d \cdot \widetilde{p}(c) = d \cdot p_*(c) = 0$, for any $c \in H_2(\Gamma)$. This settles the second part of the lemma. □

REMARK 2.3. — It might be possible that we have $d' \cdot p_*(H_2(\Gamma)) = 0$ for some proper divisor d' of d, so the first part of Lemma 2.2 can only give an upper bound of the orders of the image of the second cohomology. In order to find lower bounds we need additional information concerning the finite quotients F.

LEMMA 2.4. — *Let Γ be a perfect group, $\widetilde{\Gamma}$ its universal central extension, $p : \Gamma \to F$ a surjective homomorphism onto a finite group F, and $\widehat{p} : \widetilde{\Gamma} \to G$ be some lift of p to a central extension G of F by some finite abelian group C. Assume that the image of $H_2(\Gamma) \subset \widetilde{\Gamma}$ in G by $\widehat{p}$ contains an element of order q. Then there exists an element of $p_*(H_2(\Gamma)) \subset H_2(F)$ of order q.*

Proof. — By Lemma 2.1 there exists a lift $\widetilde{p} : \widetilde{\Gamma} \to \widetilde{F}$ of p into the universal central extension $\widetilde{F}$ of F. Then, by universality there exists a unique homomorphism $s : \widetilde{F} \to G$ of central extensions of F lifting the identity map of F. The homomorphisms $\widehat{p}$ and $s \circ \widetilde{p} : \widetilde{\Gamma} \to G$ are then both lifts of p. Using the centrality of C in G it follows that the map $\widetilde{\Gamma} \to C$ given by $x \mapsto \widehat{p}(x)^{-1} \cdot (s \circ \widetilde{p}(x))$ is a group homomorphism and is, hence, trivial, since $\widetilde{\Gamma}$ is perfect and C abelian. We conclude that $\widehat{p} = s \circ \widetilde{p}$.

Recall that the restriction of $\widetilde{p}$ to $H_2(\Gamma)$ coincides with the homomorphism $p_* : H_2(\Gamma) \to H_2(F)$ and that $H_2(F)$ is finite, since F is so. Then, if $z \in H_2(\Gamma)$ is such that $\widehat{p}(z)$ has order q in C, the element $p_*(z) \in p_*(H_2(\Gamma)) \subset \widetilde{F}$ is sent by s onto an element of order q, and, therefore, $p_*(z)$ has the order of a multiple of q, say aq. Then, $(p_*(z))^a = p_*(z^a) \in p_*(H_2(\Gamma)) \subset \widetilde{F}$ has order q. □

3. Proof of Theorem 1.1

3.1. Reducing the proof to $D = 2^k$. — Let $D = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ be the prime decomposition of an integer D. Then, according to ([12, Thm. 5]), we have $Sp(2g, \mathbb{Z}/D\mathbb{Z}) = \bigoplus_{i=1}^{s} Sp(2g, \mathbb{Z}/p_i^{n_i}\mathbb{Z})$. Since symplectic groups are perfect for $g \geq 3$ (see, e.g., [13], Thm. 5.1), from the Künneth formula, we derive:

$$H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) = \bigoplus_{i=1}^{s} H_2(Sp(2g, \mathbb{Z}/p_i^{n_i}\mathbb{Z})).$$

Stein (see [14, 16]) proved that for any odd prime p and $n \geq 2$, the Schur multipliers vanish:

$$H_2(Sp(2g, \mathbb{Z}/p^n\mathbb{Z})) = 0$$

while Steinberg showed that

$$H_2(Sp(2g, \mathbb{Z}/2\mathbb{Z})) = 0.$$

Then, Theorem 1.1 is equivalent to the statement:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}, \text{ for all } g \geq 3, k \geq 2.$$

In the following, we will freely use two classical results due to Stein. *Stein's isomorphism theorem* (see [14], Thm. 2.13 and Prop. 3.3.(a)) states that there is an isomorphism:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \simeq H_2(Sp(2g, \mathbb{Z}/2^{k+1}\mathbb{Z})), \text{ for all } g \geq 3, k \geq 2.$$

Further, *Stein's stability theorem* (see [14]) states that the stabilization homomorphism $Sp(2g, \mathbb{Z}/2^k\mathbb{Z}) \hookrightarrow Sp(2g+2, \mathbb{Z}/2^k\mathbb{Z})$ induces an isomorphism:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \simeq H_2(Sp(2g+2, \mathbb{Z}/2^k\mathbb{Z})), \text{ for all } g \geq 3, k \geq 1.$$

Therefore, to prove Theorem 1.1 it suffices to show that:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}, \text{ for some } g \geq 3 \text{ and some } k \geq 2.$$

3.2. An alternative for the order of $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$. — As our first step we prove, as a consequence of Deligne's theorem:

PROPOSITION 3.1. — *We have $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$, when $g \geq 4$.*

Proof of Proposition 3.1. — Let $p : Sp(2g, \mathbb{Z}) \to Sp(2g, \mathbb{Z}/2^k\mathbb{Z})$ be the reduction mod 2^k and $p_* : H_2(Sp(2g, \mathbb{Z})) \to H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ the induced homomorphism. The first ingredient in the proof is the following result, which seems well known, and that we isolate for later reference:

LEMMA 3.2. — *The homomorphism $p_* : H_2(Sp(2g, \mathbb{Z})) \to H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ is surjective, if $g \geq 4$.*

The rather technical proof of Lemma 3.2 is postponed to Section 3.5.

Now, it is a classical result that $H_1(Sp(2g, \mathbb{Z})) = 0$, for $g \geq 3$ and $H_2(Sp(2g, \mathbb{Z})) = \mathbb{Z}$, for $g \geq 4$ (see, e.g., [13], Thm. 5.1). Note, however, that for $g = 3$, we have that $H_2(Sp(6, \mathbb{Z})) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ according to [15]. This implies that $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ is cyclic when $g \geq 4$ (this was also shown by Stein in [14]), and we only have to bound the order of this cohomology group.

Lemma 2.1 provides a lift between the universal central extensions $\widetilde{p} : \widetilde{Sp(2g, \mathbb{Z})} \to \widetilde{Sp(2g, \mathbb{Z}/2^k\mathbb{Z})}$ of the mod 2^k reduction map, such that the restriction of $\widetilde{p}$ to the central subgroup $H_2(Sp(2g, \mathbb{Z}))$ of $\widetilde{Sp(2g, \mathbb{Z})}$ is the homomorphism $p_* : H_2(Sp(2g, \mathbb{Z})) \to H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$. From Deligne's theorem [5] every finite index subgroup of the universal central extension $\widetilde{Sp(2g, \mathbb{Z})}$, for $g \geq 4$, contains $2\mathbb{Z}$, where $\mathbb{Z}$ is the central kernel $\ker(\widetilde{Sp(2g, \mathbb{Z})} \to Sp(2g, \mathbb{Z}))$. If c is a generator of the central $\mathbb{Z} = H_2(Sp(2g, \mathbb{Z}))$, we have $2p_*(c) = \widetilde{p}(2c) = 0$. According to Lemma 3.2 p_* is surjective, and, thus, $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ is a quotient of $\mathbb{Z}/2\mathbb{Z}$, as claimed. □

3.3. Divisibility of the universal symplectic central extension when restricted to level subgroups. — The Siegel upper half-plane $\mathcal{H}_g$ is the space of $g \times g$ symmetric complex matrices with positive definite imaginary parts. Let $Sp(2g, L)$ denote the *level L congruence subgroup* of $Sp(2g, \mathbb{Z})$, namely the kernel of the mod L reduction map $Sp(2g, \mathbb{Z}) \to Sp(2g, \mathbb{Z}/L\mathbb{Z})$. The moduli space $\mathcal{A}_g(L)$ of principally polarized abelian varieties with level L structures (over $\mathbb{C}$ of dimension g) is defined as the quotient $\mathcal{H}_g/Sp(2g, L)$. This is a quasiprojective orbifold. As $Sp(2g, \mathbb{Z})$ has Kazhdan's property T for $g \geq 2$, we have $H^1(Sp(2g, L); \mathbb{Z}) = 0$, and there exists an injection of the Picard group $Pic(\mathcal{A}_g) \to H^2(Sp(2g, L); \mathbb{Z})$; Borel ([3]) proved that $H^2(Sp(2g, L); \mathbb{Z})$ has rank 1, for $g \geq 3$ and Putman ([13], Thm. D) showed that for $g \geq 4$ and

$4 \nmid L$ this injection is an isomorphism. There is a line bundle $\lambda_g \in Pic(\mathcal{A}_g)$ whose holomorphic sections are Siegel modular forms of weight 1 and level 1, also called the Hodge line bundle. Then, λ_g generates $Pic(\mathcal{A}_g)$ (see [7]), and its first Chern class $c_1(\lambda_g)$ generates $H^2(Sp(2g,\mathbb{Z});\mathbb{Z}) = \mathbb{Z}$, for $g \geq 3$. Denote by $\lambda_g(L) \in Pic(\mathcal{A}_g(L))$ the pullback of λ_g to the orbifold covering $\mathcal{A}_g(L)$.

Recall the (slightly corrected) version of Putman's lemma ([13], Lemma 5.5):

LEMMA 3.3. — *Let $L \geq 2$ be an even number. The pullback $\lambda_g(L)$ of the Hodge bundle $\lambda_g \in \mathcal{A}_g$ to $\mathcal{A}_g(L)$ is divisible by 2 if $4 \mid L$ and is divisible by 2 modulo torsion but not divisible by 2 if $4 \nmid L$.*

In view of the canonical injection $Pic(\mathcal{A}_g(L)) \hookrightarrow H^2(Sp(2g,L);\mathbb{Z})$, this result cohomologically translates as:

LEMMA 3.4. — *Let $L \geq 2$ be an even number. The pullback of the class of the universal central extension $c \in H^2(Sp(2g,\mathbb{Z});\mathbb{Z})$ to $Sp(2g,L)$ is divisible by 2 if $4 \mid L$ and divisible by 2 modulo torsion if $4 \nmid L$.*

Proof. — The transformation formulas for the theta nulls (see, e.g., [7]) provide a square root for the pullback; nevertheless, these computations do not see the torsion (i.e., flat) bundles. So, they provide for $L = 2$ and, hence, for every even L a square root for λ_g modulo torsion.

The universal coefficients exact sequence reads:

$$0 \to \mathrm{Hom}(H_1(Sp(2g,2);\mathbb{Z}),\mathbb{C}^*) \to H^2(Sp(2g,2);\mathbb{Z}) \\ \to \mathrm{Hom}(H_2(Sp(2g,2);\mathbb{Z}),\mathbb{Z}) \to 0$$

As $Sp(2g,\mathbb{Z})$ is perfect, the divisibility by 2 mod torsion of $\lambda_g(2)$ shows that the image of $H_2(Sp(2g,2);\mathbb{Z}) \to H_2(Sp(2g,\mathbb{Z});\mathbb{Z}) = \mathbb{Z}$ is contained in $2\mathbb{Z}$. By Deligne's theorem, the image must, in fact, be $2\mathbb{Z}$.

Further, torsion elements in $H^2(Sp(2g,2);\mathbb{Z})$ all come from the abelianization of $Sp(2g,2)$. It is proved in [9] that the commutator $[Sp(2g,2), Sp(2g,2)]$ coincides with the so-called Igusa subgroup $Sp(2g,4,8)$ of $Sp(2g,4)$ consisting of those symplectic matrices $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ with the property that the diagonal entries of $AB^\top$ and $CD^\top$ are multiples of 8. Since $Sp(2g,4,8) \supset Sp(2g,8)$ the pullback of the universal central extension on $Sp(2g,\mathbb{Z})$ to $Sp(2g,8)$ is genuinely divisible by 2.

We are only left with the proof that the pullback of the class c on $Sp(2g,4)$ is divisible by 2. This is a consequence of Stein's stability theorem. Indeed, the divisibility by 2 on $Sp(2g,8)$ implies that the mod 2 reduction of the universal central extension c is the pullback of the universal central extension of $Sp(2g,\mathbb{Z}/32\mathbb{Z})$, so by stability it is also the pullback of the universal central

extension of $Sp(2g,\mathbb{Z}/4\mathbb{Z})$, and we have a commutative diagram:

$$\begin{array}{ccccccc} 1 \to \mathbb{Z} & \to & \widetilde{Sp(2g,\mathbb{Z})} & \to & Sp(2g,\mathbb{Z}) & \to 1 \\ \downarrow \bmod 2 & & \downarrow F & & \downarrow & \\ 1 \to \mathbb{Z}/2\mathbb{Z} & \to & \widetilde{Sp(2g,\mathbb{Z}/4\mathbb{Z})} & \to & Sp(2g,\mathbb{Z}/4\mathbb{Z}) & \to 1. \end{array} \tag{1}$$

Let $H = \ker F$. Then, H is the preimage of $Sp(2g,4) \subset Sp(2g,\mathbb{Z})$ and $H \cap \mathbb{Z} = 2\mathbb{Z}$. By construction twice the class of the central extension

$$1 \to \mathbb{Z} \to H \to Sp(2g,4) \to 1$$

is c restricted to $Sp(2g,4)$. □

3.4. Nonsplit central extensions. — In order to show that $H_2(Sp(2g,\mathbb{Z}/2^k\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}$, when $k \geq 2$ and $g \geq 4$, it is enough to show that $H_2(Sp(2g,\mathbb{Z}/m\mathbb{Z})) \neq 0$, for some value of m. This will follow by exhibiting a nonsplit central extension of $Sp(2g,\mathbb{Z}/m\mathbb{Z})$. Let

$$1 \to \mathbb{Z} \to \widetilde{Sp(2g,\mathbb{Z})} \to Sp(2g,\mathbb{Z}) \to 1$$

be the universal central extension of $Sp(2g,\mathbb{Z})$ and let $c \in H^2(Sp(2g,\mathbb{Z})) = \mathbb{Z}$ be the generator. Let $Sp(2g,2)$ be the level 2 subgroup of $Sp(2g,\mathbb{Z})$, namely the kernel of the mod 2 reduction map $Sp(2g,\mathbb{Z}) \to Sp(2g,\mathbb{Z}/2\mathbb{Z})$, and $\iota : Sp(2g,2) \to Sp(2g,\mathbb{Z})$ the inclusion.

From Lemma 3.4 there exists some $d \in H^2(Sp(2g,4))$ such that $2d = \iota^*(c)$. Let

$$1 \to \mathbb{Z} \to \widetilde{G} \to Sp(2g,4) \to 1$$

be the central extension corresponding to the class d, so that we have a commutative diagram:

$$\begin{array}{ccccccc} 1 \to \mathbb{Z} & \to & \widetilde{G} & \to & Sp(2g,4) & \to 1 \\ \downarrow \times 2 & & \downarrow & & \downarrow \iota & \\ 1 \to \mathbb{Z} & \to & \widetilde{Sp(2g,\mathbb{Z})} & \to & Sp(2g,\mathbb{Z}) & \to 1. \end{array} \tag{2}$$

The group $\widetilde{G}$ is, thus, a finite-index subgroup of $\widetilde{Sp(2g,\mathbb{Z})}$. Let $\widetilde{K} \subset \widetilde{G}$ be a finite-index normal subgroup of $\widetilde{Sp(2g,\mathbb{Z})}$ and K be its image in $Sp(2g,4)$.

Using the congruence subgroup property, we can find some m such that $Sp(2g,m) \subset K$. Let $\widetilde{Sp(2g,m)}$ be the preimage of $Sp(2g,m)$ under the map $\widetilde{Sp(2g,\mathbb{Z})} \to Sp(2g,\mathbb{Z})$ and $\widetilde{H} = \widetilde{K} \cap \widetilde{Sp(2g,m)}$. Since it is the intersection of two finite-index normal subgroups, the group $\widetilde{H}$ is a finite-index normal subgroup of $\widetilde{Sp(2g,\mathbb{Z})}$ that is contained in $\widetilde{K}$. Its intersection with the central $\mathbb{Z}$ in $\widetilde{Sp(2g,\mathbb{Z})}$ is, thus, of the form $2n\mathbb{Z}$, for some $n \geq 1$. By Deligne's theorem

we derive that $n = 1$. We obtain the commutative diagram:

$$\begin{array}{ccccccc} 1 \to \mathbb{Z} & \to & \widetilde{H} & \to Sp(2g,m) & \to 1 \\ \downarrow \times 2 & & \downarrow & \downarrow \iota & \\ 1 \to \mathbb{Z} & \to \widetilde{Sp(2g,\mathbb{Z})} & \to Sp(2g,\mathbb{Z}) & \to 1. \end{array} \tag{3}$$

We have $Sp(2g,\mathbb{Z}/m\mathbb{Z}) = Sp(2g,\mathbb{Z})/Sp(2g,m)$. Define $\Gamma = \widetilde{Sp(2g,\mathbb{Z})}/\tilde{H}$. We thus have a central extension

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \Gamma \to Sp(2g,\mathbb{Z}/m\mathbb{Z}) \to 1$$

Since $\widetilde{Sp(2g,\mathbb{Z})}$ is the universal central extension of the perfect group $Sp(2g,\mathbb{Z})$, the group $\widetilde{Sp(2g,\mathbb{Z})}$ is perfect. This implies that Γ is also perfect, and, in particular, it has no nontrivial homomorphism to $\mathbb{Z}/2$. We conclude that this central extension of $Sp(2g,\mathbb{Z}/m\mathbb{Z})$ does not split, as desired.

Remark 3.5. — We can take for $\widetilde{K} = [\widetilde{Sp(2g,4)}, \widetilde{Sp(2g,4)}]$, which is a finite index normal subgroup of $\widetilde{Sp(2g,\mathbb{Z})}$. In this case, K is the Igusa subgroup $Sp(2g,16,32)$ consisting of those symplectic matrices $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ from $Sp(2g,16)$ with the property that the diagonal entries of $AB^\top$ and $CD^\top$ are multiples of 32. Therefore, we can take $m = 32$ in the argument above.

Remark 3.6. — As a consequence, Deligne's nonresidual finiteness theorem is sharp. Putman in ([13], Thm. F) previously obtained the existence of finite index subgroups of $\widetilde{Sp(2g,\mathbb{Z})}$ that contain $2\mathbb{Z}$ but not $\mathbb{Z}$. We make explicit his construction as the image of the center of the universal central extension $\widetilde{Sp(2g,\mathbb{Z})}$ into the universal central extension of $Sp(2g,\mathbb{Z}/D\mathbb{Z})$ is of order 2, when $D \equiv 0 \pmod 4$ and $g \geq 3$.

3.5. Proof of Lemma 3.2. — Let $\mathbb{K}$ be a *number field*, $\mathcal{R}$ be the set of inequivalent valuations of $\mathbb{K}$ and $S \subset \mathcal{R}$ be a finite set of valuations of $\mathbb{K}$ including all the Archimedean (infinite) ones. Let

$$O(S) = \{x \in \mathbb{K} \colon\ v(x) \leq 1, \text{ for all } v \in \mathcal{R} \setminus S\}$$

be the ring of S-integers in $\mathbb{K}$ and $\mathfrak{q} \subset O(S)$ be a nonzero ideal. By $\mathbb{K}_v$ we denote the completion of $\mathbb{K}$ with respect to $v \in \mathcal{R}$. Following [1], a domain $\mathfrak{A}$, which arises as $O(S)$ above, will be called a *Dedekind domain of arithmetic type*.

Let $\mathfrak{A} = O_S$ be a Dedekind domain of arithmetic type and $\mathfrak{q}$ be an ideal of $\mathfrak{A}$. Denote by $Sp(2g,\mathfrak{A},\mathfrak{q})$ the kernel of the surjective homomorphism $p : Sp(2g,\mathfrak{A}) \to Sp(2g,\mathfrak{A}/\mathfrak{q})$. The surjectivity is not a purely formal fact and follows from the fact that in these cases, the symplectic group coincides with the so-called "elementary symplectic group", and that it is trivial to lift elementary

generators of $Sp(2g, \mathfrak{A}/\mathfrak{q})$ to $Sp(2g, \mathfrak{A})$, for a proof of this fact when $\mathfrak{A} = \mathbb{Z}$ (see [8], Thm. 9.2.5).

The goal of this section is to give a self-contained proof of the following result, which contains Lemma 3.2 as a particular case:

PROPOSITION 3.7. — *Given an ideal $\mathfrak{q} \in \mathfrak{A}$, for any $g \geq 3$, the homomorphism $p_* : H_2(Sp(2g, \mathfrak{A})) \to H_2(Sp(2g, \mathfrak{A}/\mathfrak{q}))$ is surjective.*

Normal generators of the group $Sp(2g, \mathfrak{A}, \mathfrak{q})$ can be found in ([1], III.12), as follows. Fix a symplectic basis $\{a_i, b_i\}_{1 \leq i \leq g}$ and write the matrix by blocks according to the associated decomposition of $\mathfrak{A}^{2g}$ into maximal isotropic subspaces.

For each pair of distinct integers $i, j \in \{1, \ldots, g\}$ denote by $e_{ij} \in \mathfrak{M}_g(\mathbb{Z})$ the matrix whose only nonzero entry is a 1 at the place ij. Set also $\mathbf{1}_k$ for the k-by-k identity matrix.

Then following ([1], Lemma 13.1) $Sp(2g, \mathfrak{A}, \mathfrak{q})$ is the *normal subgroup* of $Sp(2g, \mathfrak{A})$ generated by the matrices:

$$U_{ij}(q) = \begin{pmatrix} \mathbf{1}_g & qe_{ij} + qe_{ji} \\ 0 & \mathbf{1}_g \end{pmatrix}, \quad U_{ii}(q) = \begin{pmatrix} \mathbf{1}_g & qe_{ii} \\ 0 & \mathbf{1}_g \end{pmatrix}, \tag{4}$$

and

$$L_{ij}(q) = \begin{pmatrix} \mathbf{1}_g & 0 \\ qe_{ij} + qe_{ji} & \mathbf{1}_g \end{pmatrix}, \quad L_{ii}(q) = \begin{pmatrix} \mathbf{1}_g & 0 \\ qe_{ii} & \mathbf{1}_g \end{pmatrix}, \tag{5}$$

where $q \in \mathfrak{q}$.

Denote by $E(2g, \mathfrak{A}, \mathfrak{q})$ the subgroup of $Sp(2g, \mathfrak{A}, \mathfrak{q})$ generated by the matrices $U_{ij}(q)$ and $L_{ij}(q)$.

LEMMA 3.8. — *The group $E(2g, \mathfrak{A}, \mathfrak{q})$ is the subgroup $Sp(2g, \mathfrak{A}, \mathfrak{q}|\mathfrak{q}^2)$ of $Sp(2g, \mathfrak{A})$ of those symplectic matrices $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, whose entries satisfy the conditions:*

$$B \equiv C \equiv 0 \pmod{\mathfrak{q}}, \quad \textit{and} \quad A \equiv D \equiv \mathbf{1}_g \pmod{\mathfrak{q}^2}. \tag{6}$$

Proof. — We follow closely the proof of Lemma 13.1 from [1]. One verifies easily that $Sp(2g, \mathfrak{A}, \mathfrak{q}|\mathfrak{q}^2)$ is, indeed, a subgroup of $Sp(2g, \mathfrak{A})$. It then suffices to show that all elements of the form $\left(\begin{smallmatrix} A & 0 \\ 0 & (A^{-1})^\top \end{smallmatrix}\right)$, with $A \in GL(g, \mathfrak{A})$ satisfying $A \equiv \mathbf{1}_g \pmod{\mathfrak{q}^2}$ belong to $E(2g, \mathfrak{A}, \mathfrak{q})$. Here, the notation $A^\top$ stands for the transpose of the matrix A. Next, it suffices to verify this claim when A is an elementary matrix, and hence when A is in $GL(2, \mathfrak{A})$ and $g = 2$. Taking, therefore, $A = \left(\begin{smallmatrix} 1 & 0 \\ q_1 q_2 & 1 \end{smallmatrix}\right)$, where $q_1, q_2 \in \mathfrak{q}$, we can write:

$$\begin{pmatrix} A & 0 \\ 0 & (A^{-1})^\top \end{pmatrix} = \begin{pmatrix} 1_2 & \sigma A^\top \\ 0 & 1_2 \end{pmatrix} \begin{pmatrix} 1_2 & 0 \\ -\tau & 1_2 \end{pmatrix} \begin{pmatrix} 1_2 & \sigma \\ 0 & 1_2 \end{pmatrix} \begin{pmatrix} 1_2 & 0 \\ \tau & 1_2 \end{pmatrix}, \tag{7}$$

where $\sigma = \left(\begin{smallmatrix} 0 & q_1 \\ q_1 & 0 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} q_2 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. □

Define now

$$R_{ij}(q) = \begin{pmatrix} \mathbf{1}_g + qe_{ij} & 0 \\ 0 & \mathbf{1}_g - qe_{ji} \end{pmatrix}, \quad \text{for } i \neq j, \tag{8}$$

and

$$N_{ii}(q) = \begin{pmatrix} \mathbf{1}_g + (q+q^2+q^3)e_{ii} & -q^2 e_{ii} \\ q^2 e_{ii} & \mathbf{1}_g - qe_{ii} \end{pmatrix}. \tag{9}$$

Proof of Proposition 3.7. — If M is endowed with a structure of G-module, we denote by M_G the quotient module of coinvariants, namely the quotient of M by the submodule generated by $\langle g \cdot x - x, g \in G, x \in M \rangle$.

It is known (see [4], VII. 6.4) that an exact sequence of groups

$$1 \to K \to G \to Q \to 1$$

induces the following five-term exact sequence in homology (with coefficients in an arbitrary G-module M):

$$H_2(G;M) \to H_2(Q;M_H) \to H_1(K)_Q \to H_1(G,M) \to H_1(Q,M_H) \to 0. \tag{10}$$

From the five-term exact sequence associated to the short exact sequence:

$$1 \to Sp(2g,\mathfrak{A},\mathfrak{q}) \to Sp(2g,\mathfrak{A}) \to Sp(2g,\mathfrak{A}/\mathfrak{q}) \to 1$$

we deduce that the surjectivity of p_* is equivalent to Lemma 3.9 hereafter.

LEMMA 3.9. — *For any ideal $\mathfrak{q}$, if $g \geq 3$, we have:*

$$H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))_{Sp(2g,\mathfrak{A}/\mathfrak{q})} = 0. \tag{11}$$

Proof of Lemma 3.9. — For each pair of distinct integers $i,j \in \{1,\dots,g\}$ denote by A_{ij} the symplectic matrix:

$$A_{ij} = \begin{pmatrix} \mathbf{1}_g - e_{ij} & 0 \\ 0 & \mathbf{1}_g + e_{ji} \end{pmatrix}. \tag{12}$$

Then, for each triple of distinct integers (i,j,k) and $q \in \mathfrak{q}$ the action of A_{ij} by conjugacy on the generating matrices of $Sp(2g,\mathfrak{A},\mathfrak{q})$ is given by:

$$\begin{aligned}
A_{ij} \cdot U_{jj}(q) &= U_{ii}(q)U_{jj}(q)U_{ij}(q)^{-1}, \\
A_{ki} \cdot U_{ij}(q) &= U_{ij}(q)U_{jk}(q)^{-1}, \\
A_{ji} \cdot U_{ij}(q) &= U_{ij}(q)U_{jj}(q)^{-2}, \\
A_{ij} \cdot L_{jj}(q) &= L_{ii}(q)L_{jj}(q)L_{ij}(q), \\
A_{ik} \cdot L_{ij}(q) &= L_{ij}(q), \\
A_{ij} \cdot L_{ij}(q) &= L_{ij}(q)L_{ii}(q)^2,
\end{aligned}$$

where we used the notation $A \cdot U = AUA^{-1}$. We also have:

$$A_{ij} \cdot R_{jk}(q) = R_{jk}(q)R_{ik}(q).$$

Further, the symplectic map $J = \left(\begin{smallmatrix} 0 & -\mathbf{1}_g \\ \mathbf{1}_g & 0 \end{smallmatrix}\right)$ acts as follows:

$$J \cdot U_{ij}(q) = -L_{ij}(q), \quad J \cdot U_{ii}(q) = -L_{ii}(q).$$

Denote by lower-case letters the classes of the maps $U_{ij}(q)$, $U_{ii}(q)$, $L_{ij}(q)$, $L_{ii}(q)$, $R_{ij}(q)$ and $N_{ii}(q)$ in the quotient $H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))_{Sp(2g,\mathfrak{A}/\mathfrak{q})}$ of the abelianization $H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))$. By definition, the action of $Sp(2g,\mathfrak{A}/\mathfrak{q})$ on $H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))_{Sp(2g,\mathfrak{A}/\mathfrak{q})}$ is trivial.

Using the action of J we obtain the equality $u_{ij}(q) + l_{ij}(q) = 0$ in $H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))_{Sp(2g,\mathfrak{A}/\mathfrak{q})}$, and, hence, we can discard the generators $l_{ij}(q)$. As $g \geq 3$, from the action of A_{ki} on $u_{ij}(q)$ we derive that $u_{jk}(q) = 0$, for every $j \neq k$. Using the action of A_{ij} on $u_{jj}(q)$ we obtain that $u_{jj}(q) = 0$ for every j. Further, the action of A_{ij} on $r_{jk}(q)$ yields $r_{ik}(q) = 0$, for all $i \neq k$.

Consider now the symplectic matrix $B_{ii} = \left(\begin{smallmatrix} \mathbf{1}_g & 0 \\ e_{ii} & \mathbf{1}_g \end{smallmatrix}\right)$. Then,

$$B_{ii} \cdot U_{ii}(q) = \begin{pmatrix} \mathbf{1}_g - qe_{ii} & qe_{ii} \\ -qe_{ii} & \mathbf{1}_g + qe_{ii} \end{pmatrix} \tag{13}$$

and hence

$$B_{ii} \cdot U_{ii}(q) \equiv U_{ii}(q) L_{ii}(q)^{-1} N_{ii}(q)^{-1} \pmod{\mathfrak{q}^2}.$$

Recall that the elements of $Sp(2g,\mathfrak{A},\mathfrak{q}^2) \subset Sp(2g,\mathfrak{A},\mathfrak{q}|\mathfrak{q}^2)$ can be written as products of the generators $U_{ij}(q)$ and $L_{ij}(q)$ according to Lemma 3.8, whose images in the quotient $H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))_{Sp(2g,\mathfrak{A}/\mathfrak{q})}$ vanish. Therefore, $B_{ii} \cdot u_{ii}(q) = u_{ii}(q) + l_{ii}(q) - n_{ii}(q)$. This proves that $n_{ii}(q) = 0$ in $H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))_{Sp(2g,\mathfrak{A}/\mathfrak{q})}$. Consequently, $H_1(Sp(2g,\mathfrak{A},\mathfrak{q}))_{Sp(2g,\mathfrak{A}/\mathfrak{q})} = 0$, as claimed. □

□

3.6. Nondivisibility of the universal symplectic central extension when restricted to level subgroups. — We will show that lemma 3.4 is sharp:

LEMMA 3.10. — *Let $L \geq 2$ be an even number. The pullback of the class of the universal central extension $c \in H^2(Sp(2g,\mathbb{Z});\mathbb{Z})$ to $Sp(2g,L)$ is not divisible by 2 if $4 \nmid L$.*

The proof is the result of discussions that the authors had with D. Benson about Lemma 3.4.

Proof. — Let $\iota : Sp(2g,2) \to Sp(2g,\mathbb{Z})$ be the inclusion. We will prove by contradiction that $\iota^*(c) \in H^2(Sp(2g,2);\mathbb{Z})$ is not divisible by 2. Suppose that there exists an extension $\widetilde{G}$ of $Sp(2g,2)$ whose class d in $H^2(Sp(2g,2);\mathbb{Z})$ satisfies $\iota^*(c) = 2d$. Then we have a commutative diagram:

$$\begin{array}{ccccccc} 1 \to \mathbb{Z} & \to & \widetilde{G} & \to & Sp(2g,2) & \to 1 \\ \downarrow \times 2 & & \downarrow & & \downarrow \iota & \\ 1 \to \mathbb{Z} & \to & \widetilde{Sp(2g,\mathbb{Z})} & \to & Sp(2g,\mathbb{Z}) & \to 1. \end{array}$$

Denote by $\widehat{Sp(2g,\mathbb{Z})}$ the quotient of the universal central extension $\widetilde{Sp(2g,\mathbb{Z})}$ by the square of the generator of the central $\mathbb{Z}$.

The composition of group homomorphisms $\widetilde{G} \to \widetilde{Sp(2g,\mathbb{Z})} \to \widehat{Sp(2g,\mathbb{Z})}$ lifts the inclusion ι and factors through $\widetilde{G}/\mathbb{Z} = Sp(2g,2)$. Therefore, the restriction of the extension $\widehat{Sp(2g,\mathbb{Z})}$ to $Sp(2g,2)$ is split.

The image H of $Sp(2g,2)$ within $\widehat{Sp(2g,\mathbb{Z})}$ under this section might not be a normal subgroup. However, the group generated by squares of elements in H is a normal subgroup $K \lhd \widehat{Sp(2g,\mathbb{Z})}$. Moreover, K is isomorphic to the group $Sp(2g,4)$, which is the group generated by the squares in $Sp(2g,2)$.

By taking the quotient by the normal subgroup K above we obtain a central extension:

$$1 \to \mathbb{Z}/2\mathbb{Z} \to \widehat{Sp(2g,\mathbb{Z}/4\mathbb{Z})} \to Sp(2g,\mathbb{Z}/4\mathbb{Z}) \to 1.$$

By the proof of Theorem 1.1 this exact sequence is nonsplit, and by construction it splits when restricted to the subgroup $Sp(2g,2)/Sp(2g,4) = \mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, the symplectic Lie algebra over the field of two elements.

We now compute $H^2(Sp(2g,\mathbb{Z}/4\mathbb{Z});\mathbb{Z}/2\mathbb{Z})$ using the Leray-Serre spectral sequence of the extension:

$$1 \to \mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z}) \to Sp(2g,\mathbb{Z}/4\mathbb{Z}) \to Sp(2g,\mathbb{Z}/2\mathbb{Z}) \to 1.$$

By Steinberg's computation [17] $H_2(Sp(2g,\mathbb{Z}/2\mathbb{Z}),\mathbb{Z}/2\mathbb{Z}) = 0$ for $g \geq 4$. Since symplectic groups are perfect, we derive $H^2(Sp(2g,\mathbb{Z}/2\mathbb{Z}),\mathbb{Z}/2\mathbb{Z}) = 0$. By Putman [13, Proof of Thm. G], $H^1(Sp(2g,\mathbb{Z}/2\mathbb{Z}),\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})) = 0$, so the only possibility is that

$$H^2(Sp(2g,\mathbb{Z}/4\mathbb{Z});\mathbb{Z}/2\mathbb{Z})) = H^0(Sp(2g,\mathbb{Z}/2\mathbb{Z});H^2(\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z});\mathbb{Z}/2\mathbb{Z})) \neq 0.$$

However, this means that the above nonsplit extension of $Sp(2g,\mathbb{Z}/4\mathbb{Z})$ can not split when restricted to $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$, which is a contradiction.

The proof for even L with $4 \nmid L$ is similar, and we skip the details. □

REMARK 3.11. — D. Benson informed us that the largest subgroup of $\mathfrak{sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ on which the above extension splits has index 2^{g+1}.

Acknowledgements. — We are thankful to Jean Barge, Nicolas Bergeron, Dave Benson, Will Cavendish, Florian Deloup, Philippe Elbaz-Vincent, Richard Hain, Greg McShane, Ivan Marin, Gregor Masbaum, Alexander Rahm, and Alan Reid for helpful discussions and suggestions. We are grateful to Pierre Lochak and Andy Putman for their help in clarifying a number of technical points and improving the presentation and the referee for cleaning and simplifying our proof.

BIBLIOGRAPHY

[1] H. Bass, J. Milnor & J.-P. Serre – "Solution of the congruence subgroup problem for $\mathrm{SL}_n\,(n \geq 3)$ and $\mathrm{Sp}_{2n}\,(n \geq 2)$", *Inst. Hautes Études Sci. Publ. Math.* **33** (1967), p. 59–137.

[2] R. Beyl – "The Schur multiplicator of $SL(2, \mathbb{Z}/m\mathbb{Z})$ and the congruence subgroup property", *Math.Z.* **91** (1986), p. 23–42.

[3] A. Borel – "Stable real cohomology of arithmetic groups", *Ann. Sci. École Norm. Sup. (4)* **7** (1974), p. 235–272.

[4] K. Brown – *Cohomology of groups*, Graduate Texts in Math., Springer-Verlag, 1994.

[5] P. Deligne – "Extensions centrales non résiduellement finies de groupes arithmétiques", *C. R. Acad. Sci. Paris Sér. A-B* **287** (1978), no. 4, p. A203–A208.

[6] R. K. Dennis & M. R. Stein – "Algebraic K-theory II", Lecture Notes in Math., no. 342, ch. The functor K: a survey of computations and problems, p. 243–280, Springer-Verlag, Berlin, New York, 1973.

[7] J. Freitag – *Theta functions*, Lect. Notes in Math., no. 1487, Springer Verlag, 1987.

[8] A. J. Hahn & O. T. O'Meara – *The classical groups and K-theory*, Grund. math. Wissenschaften, no. 291, Springer Verlag, 1989.

[9] J.-I. Igusa – *Theta functions*, Springer, New York, 1972.

[10] S. Lang – *Rapport sur la cohomologie des groupes*, W. A. Benjamin, Inc., 1967.

[11] J. Milnor – *Introduction to algebraic K-theory*, Annals Math. Studies, no. 72, Princeton Univ. Press, 1971.

[12] M. Newman & J. R. Smart – "Symplectic modulary groups", *Acta Arith.* **9** (1964), p. 83–89.

[13] A. Putman – "The Picard group of the moduli space of curves with level structures", *Duke Math. J.* **161** (2012), p. 623–674.

[14] M. R. Stein – "Surjective stability in dimension 0 for K_2 and related functors", *Trans. Amer. Math. Soc.* **178** (1973), p. 165–191.

[15] ———, "The Schur multipliers of $Sp_6(\mathbb{Z})$, $Spin_8(\mathbb{Z})$, $Spin_7(\mathbb{Z})$ and $F_4(\mathbb{Z})$", *Math. Annalen* **215** (1975), p. 165–172.

[16] ———, "Stability theorems for K_1, K_2 and related functors modeled on Chevalley groups", *Japan. J. Math. (N.S.)* **4** (1978), p. 77–108.

[17] R. Steinberg – "Generators, relations and coverings of algebraic groups. II", *J. Algebra* **71** (1981), no. 2, p. 527–543.

Bull. Soc. Math. France
148 (3), 2020, p. 529-595

CORPS DIFFÉRENTIELS ET FLOTS GÉODÉSIQUES I

ORTHOGONALITÉ AUX CONSTANTES POUR LES ÉQUATIONS DIFFÉRENTIELLES AUTONOMES

PAR RÉMI JAOUI

RÉSUMÉ. — L'orthogonalité aux constantes est une propriété issue de l'étude modèle-théorique des équations différentielles algébriques et qui traduit des propriétés d'indépendance algébrique remarquables pour ses solutions.

Dans cet article, on étudie la propriété d'orthogonalité aux constantes dans un langage algebro-différentiel pour les équations différentielles autonomes ainsi que des méthodes effectives pour établir cette propriété. Le résultat principal est un critère d'orthogonalité aux constantes (et sa version en famille) pour les D-variétés réelles absolument irréductibles (X, v) s'appuyant sur la dynamique du flot réel associé (M, ϕ). Plus précisément, on montre que s'il existe une partie compacte K de M, Zariski-dense dans X telle que la restriction du flot à K est topologiquement faiblement mélangeante, alors le type générique de (X, v) est orthogonal aux constantes.

Ce critère sera appliqué dans [18] à l'étude modèle-théorique du flot géodésique sur les variétés riemanniennes compactes à courbure strictement négative, présentées algébriquement.

Texte reçu le 5 février 2019, modifié le 19 février 2019, accepté le 6 avril 2020.

RÉMI JAOUI, Rémi Jaoui, Department of Mathematics – University of Notre Dame, 255 Hurley, Notre Dame, IN 46556, United States • *E-mail :* rjaoui@nd.edu

Classification mathématique par sujets (2010). — 03C98, 12H05.

Mots clefs. — Théorie des modèles, Algèbre différentielle, Théorie géométrique de la stabilité, Équations différentielles algébriques.

Recherche soutenue en partie par le contrat ANR-13-BS01-0006.

© Société Mathématique de France
0037-9484/2020/529/$ 5.00
doi:10.24033/bsmf.2816

Abstract (*Differential fields and geodesic flows I. Orthogonality to the constants for autonomous differential equations*). — Orthogonality to the constants is property of an algebraic differential equation that originated from the model-theoretic study of differential fields and that expresses remarkable independence properties for its solutions

In this article, we study the property of orthogonality to the constants in a differential algebraic language for autonomous differential equations and describe some effective methods to establish this property. The main result is a criterion for orthogonality to the constants (and its version for families) for real absolutely irrecucible D-varieties (X, v) based on the dynamical properties of the associated real analytic flow (M, ϕ). More precisely, we show that if there exists a compact region K of M, Zariski-dense in X and such that the restriction of the flow ϕ to K is topologically weakly mixing then the generic type of (X, v) is orthogonal to the constants.

This criterion will be applied in [18] to study from this model-theoretic point of view the geodesic flow of a compact Riemannian varieties (presented algebraically) with negative curvature.

L'étude des propriétés d'indépendance algébrique des solutions d'une équation différentielle algébrique est un thème majeur de la théorie des équations différentielles, qui se situe au coeur des travaux de nombreux illustres mathematiciens — notamment Newton, Leibniz, Picard, Painlevé et Poincaré. En particulier, à la fin du XIX^{eme} siecle, Drach étudie dans sa thèse [9], l'existence d'un cadre algébrique (désincarné de ses réalisations analytiques) où étudier les propriétés d'intégrabilité algébrique de ces équations différentielles, à la manière de Picard et Vessiot pour les équations différentielles linéaires (voir [2] pour un aperçu historique).

Néanmoins, les problèmes de formalisme rencontrés par Drach — comparables à ceux rencontrés en géométrie algébrique à la même époque — ont poussé les mathématiciens du début du XX$^{\text{ème}}$ siècle à privilégier un cadre analytique pour étudier les équations différentielles algébriques alors même que ces dernières vérifient (très vraisemblablement) des propriétés structurelles plus fortes que leurs analogues analytiques.

A la fin des années 1970, les développements conjoints de la théorie des modèles des théories stables et de l'algèbre différentielle ont permis de développer un cadre géométrique noethérien, propice à l'étude des équations différentielles algébriques. Une caractéristique essentielle est le recours à des corps différentiels « universels » appelés *corps differentiellement clos*.

L'étude de ces « compagnons de route de la théorie des modèles » (voir [27]) est une illustration remarquable de l'efficacité des méthodes de la théorie géométrique de la stabilité pour étudier certaines géometries noetheriennes, innaccessibles auparavant. Un résultat essentiel est le théorème de Hrushovski-Sokolovic [14] — une incarnation du théorème de trichotomie de Hrushovski et Zilber pour les corps differentiellement clos — qui décrit *les équations différentielles minimales*, dont la résolution ne peut être ramenée à la résolution

successive d'équations différentielles « plus simples ». L'article de Hrushovski et Sokolovic n'ayant jamais été publié, nous renvoyons à [26] et [24, Section 2.1] pour une présentation complète de la trichotomie.

L'objectif de cet article est de présenter quelques conséquences du théorème de Hrushovski-Sokolovic pour les équations différentielles autonomes (dans un langage géométrique) ainsi que d'établir des critères effectifs pour étudier les propriétés mises en jeu par ce théorème — *orthogonalité aux constantes et désintégration*. En s'appuyant sur des résultats d'Anosov [1] concernant la dynamique des champs de vecteurs hyperboliques, ces résultats seront appliqués dans [18] et [17] à l'étude de propriétés d'indépendance algébrique des solutions géodésiques d'une variété riemannienne compacte (présentée algébriquement) à courbure strictement négative.

Équations différentielles algébriques autonomes. — Dans ce texte, on travaille uniquement au dessus de corps k *de caractéristique* 0 et on considère des *équations différentielles algébriques autonomes* à paramètres dans k. Une telle equation peut être décrite « sous forme explicite » comme une paire (X, v) où X *est une variété algébrique au dessus d'un corps* k *de caractéristique* 0 — que l'on pourra toujours supposée lisse — *munie d'un champ de vecteurs* v.

Les relations algébriques entre n solutions de (X, v) sont représentées par certaines *sous-variétés fermées* de $(X, v)^n$ dites *invariantes*.

Ici, une sous-variété fermée (et plus généralement tout sous-schéma fermé) de (X, v) est *invariant* si le faisceau d'idéaux associé $\mathcal{I} \subset (\mathcal{O}_X, \delta_v)$ est stable par la dérivation δ_v induite par le champ de vecteurs v sur X. Géométriquement, une sous-variété fermée Z de (X, v) est invariante lorsque la sous-variété localement fermée Z_{reg} de X (constituée des points réguliers de Z) est tangente en tout point au champ de vecteurs v.

Les sous-variétés fermées invariantes de $(X, v)^n$ sont définies, tout simplement, comme les sous-variétés fermées de X^n invariante pour le champ de vecteurs produit $v \times \cdots \times v$ induit par v sur X^n. En notant $\mathcal{I}_n(X, v)$ la collection des sous-variétés fermées irréductibles invariantes de $(X, v)^n$, la suite des $\mathcal{I}_n(X, v)$ lorsque n parcourt $\mathbb{N}^*$ définit alors un langage $\mathcal{L}$ (au sens de la théorie des modèles).

L'ensemble des solutions analytiques de l'équation différentielle (X, v) est naturellement munie d'une $\mathcal{L}$-structure. Comme il est d'usage en théorie des modèles, il convient alors de compléter cette structure en *une structure existentiellement close* notée $(X, v)^{(\mathcal{U},\delta)}$ en adjoignant toutes les solutions de cette équation différentielle dans un corps différentiel universel $(\mathcal{U}, \delta)$.

La $\mathcal{L}$-structure $(X, v)^{(\mathcal{U},\delta_\mathcal{U})}$, produite par la construction précédente, jouit de propriétés particulièrement agréables : c'est une *structure ω-stable de rang fini* (borné par la dimension de X), interprétable dans un corps differentiellement clos, qui admet *l'élimination des quantificateurs dans le langage* $\mathcal{L}$. Les

méthodes de la théorie géométrique de la stabilité appliquées à la structure $(X, v)^{(\mathcal{U},\delta)}$ permettent alors d'obtenir :

(a) Une *classification des équations différentielles minimales*. Intuitivement ce sont celles dont la résolution ne peut être ramenée à la résolution d'équations différentielles plus simples.
(b) Un dévissage des équations différentielles de rang fini à partir d'équations différentielles minimales selon un procédé appelé *analyse semi-minimale des types*.

Dans le paragraphe qui suit, on décrit plus précisément ces deux procédés (en commençant par le second) dans le langage de *la théorie géométrique de la stabilité*.

Théorie géométrique de la stabilité. — Plutôt que la structure associée à l'équation différentielle (X, v), les résultats de décomposition dont il est question ici, concernent en réalité *les types* — qui sont les ultrafiltres sur l'algèbre booléenne des ensembles définissables — de cette structure. Lorsque la variété X est irréductible, il existe un type privilégié parmi ces derniers (par élimination des quantificateurs), appelé *type générique de* (X, v) dont les réalisations sont les solutions génériques de l'équation différentielle (X, v), c'est-à-dire, celles qui sont Zariski-dense dans X.

Commençons par décrire les deux situations extrêmes qui peuvent se produire pour les relations entre un type de rang fini q et un type minimal p dans une théorie stable T : soit il est possible de reconstruire (après une possible extension des paramètres) une réalisation du type q à partir de réalisations de p (et de ses conjugués). On dit alors que le type q *est interne à* p (et ses conjugués). A l'inverse, le *type* q *est orthogonal à* p lorsque p et q sont sans relation dans la théorie T et le demeurent après toute extension des paramètres, ou autrement dit après tout changement de base.

En général, on peut aussi observer des situations intermédiaires, où le type q est non-orthogonal au type minimal p sans pour autant lui être interne. Dans ce cas, il existe alors un *facteur non-trivial*[1] q_0 de q qui est interne à p (et ses conjugués). Quitte à remplacer le type q par un facteur non-trivial q_0, on peut donc toujours se ramener à une des deux situations extrêmes exposées ci-dessus.

De plus, on peut alors itérer ce processus pour obtenir un dévissage complet du type q en types semi-minimaux (c'est-à-dire interne à un type minimal et ses conjugués) appelé *analyse semi-minimale de* q. Appliqué aux équations différentielles algébriques, ce dévissage permet ainsi de décomposer toute equation différentielle algébrique (X, v), au voisinage de son point générique, en

1. Le type $q_0 \in S(\emptyset)$ est un facteur non-trivial de $q \in S(\emptyset)$ s'il existe des réalisations $a \models q$ et $b \models q_0$ telles que $b \in \mathrm{dcl}(a) \setminus \mathrm{acl}(\emptyset)$.

une suite de facteurs semi-minimaux. Décrivons maintenant la classification des équations différentielles minimales, mentionnée ci-dessus.

L'étude des types minimaux — pour toute théorie stable et donc dans un cadre bien plus général que celui des équations différentielles — a conduit Zilber à les classifier en trois différentes classes selon la nature de la notion de dimension qui leur est naturellement associée. De façon informelle, la notion de dimension se comporte ou bien comme le cardinal dans un ensemble infini sans structure, ou bien comme la dimension linéaire dans un espace vectoriel, ou bien comme le degré de transcendance dans un corps algébriquement clos. On dit alors respectivement que *le type minimal est désintégré, localement modulaire (non désintégré) ou non-localement modulaire.*

Pour les équations différentielles algébriques minimales, le cas désintégré correspond à celles dont les solutions (génériques) possèdent *les plus fortes propriétés d'indépendance algébrique* (voir le paragraphe suivant). Le théorème de Hrushovski-Sokolovic (voir [14]) est une classification complète des équations différentielles minimales (pas nécessairement autonomes) non-désintégrées.

Théorème (Hrushovski-Sokolovic). — *Soit $p \in S(A)$ un type minimal non-désintégré de la théorie des corps differentiellement clos. Alors :*

(i) *Ou bien le type p est non-localement modulaire. Dans ce cas, le type p est non-orthogonal au type générique du corps des constantes.*
(ii) *Ou bien le type p est localement modulaire. Il existe alors une variété abélienne simple A, qui ne descend pas au corps des constantes, tel que p est non-orthogonal au type générique du « noyau de Manin » $A^\sharp$ associé à A.*

Dans [12], Hrushovski et Itai étudient les conséquences de ce théorème pour les équations différentielles autonomes (X, v) de *dimension* 1 *où l'hypothèse de minimalité est automatiquement vérifiée.* En dimension supérieure, il est très difficile de formuler une description géométrique (raisonnable en pratique) de cette propriété (voir par exemple [16, Chapitre 3, Théorème 1.3.12] pour une formulation géométrique).

Désintégration et orthogonalité aux constantes. — Dans ce paragraphe, nous décrivons en termes géométriques quelques conséquences du théorème de Hrushovski-Sokolovic pour des équations différentielles autonomes (X, v) (de dimension supérieure et donc sans hypothèse de minimalité *a priori* pour leur type générique) à travers une analyse semi-minimale de leur type générique.

La propriété d'*orthogonalité aux constantes* pour (le type générique d') une équation différentielle (X, v) peut être formulée à l'aide de la notion d'intégrale première rationnelle dans (X, v) et ses puissances. Ici, *une intégrale première rationnelle* de (X, v) est simplement une fonction rationnelle $f \in k(X)$ sur X constante le long des orbites de v, c'est-a-dire vérifiant $v(f) = 0$. Le type

générique de (X, v) est alors orthogonal aux constantes si et seulement si :

$$(O) : \begin{cases} \text{Pour tout entier } n \geq 0, \ (X, v)^n \text{ n'admet pas d'intégrale} \\ \text{première rationnelle non constante.} \end{cases}$$

La propriété de *désintégration* (au point générique) de (X, v) concerne, quant à elle, les relations algébriques entre un nombre arbitraire de solutions génériques de (X, v). Intuitivement, elle exprime que l'ensemble des relations algébriques entre n solutions de l'équation différentielle (X, v) est aussi petit que possible dès que $n \geq 3$.

Formellement, notons $\mathcal{I}_n^{gen}(X, v)$ l'ensemble des sous-variétés fermées irréductibles invariantes *génériques* (c'est-à-dire celles se projetant génériquement sur chacun des facteurs) de $(X, v)^n$. L'équation différentielle (X, v) est *génériquement désintégrée* si et seulement si :

$$(D) : \begin{cases} \text{Pour tout } n \geq 3 \text{ et tout } Z \in \mathcal{I}_n^{gen}(X, v), \\ \text{il existe } (Z_{i,j})_{i \neq j \leq n} \in \mathcal{I}_2^{gen}(X, v) \text{ pour tout } i \neq j, \\ \text{telles que } Z \text{ est une composante irreductible de } \bigcap_{1 \leq i \neq j \leq n} \pi_{i,j}^{-1}(Z_{i,j}). \end{cases}$$

Pour toute équation différentielle algébrique autonome, *la propriété* (D) *implique la propriété* (O). En apparence, la propriété (D) — qui concerne des sous-variétés fermées invariantes de $(X, v)^n$ de dimension arbitraire — semble bien plus restrictive que la propriété (O). Néanmoins, nous montrons que la propriété (O) est suffisante pour garantir l'existence d'un facteur rationnel (non-trivial) génériquement désintégré.

THÉORÈME A. — *Soient k un corps de caractéristique 0 et (X, v) une variété absolument irréductible au dessus de k munie d'un champ de vecteurs v.*

Si le type générique de (X, v) est orthogonal aux constantes alors il existe une variété absolument irréductible Y au dessus de k de dimension > 0, un champ de vecteurs w sur Y et un morphisme rationnel dominant

$$\pi : (X, v) \dashrightarrow (Y, w)$$

tels que (Y, w) est génériquement désintégrée.

Le morphisme π apparaissant dans le théorème A est un morphisme de la catégorie des D-variétés (voir Appendice A), c'est-à-dire que le morphisme rationnel $\pi : X \dashrightarrow Y$ vérifie la règle de compatibilité évidente aux champs de vecteurs : $d\phi(v) = w$. Le théorème A est obtenu dans la première partie de ce texte, en appliquant le théorème de Hrushovski-Sokolovic à un facteur semi-minimal de l'équation différentielle (X, v).

Pour résumer, la propriété d'*orthogonalité aux constantes* pour une équation différentielle algébrique concerne donc aussi bien *l'absence d'intégrales premières rationnelles pour l'équation différentielle sous étude et ses puissances* que *l'existence d'un facteur rationnel génériquement désintégré.*

Un critère dynamique d'orthogonalité aux constantes. — Paradoxalement, on ne connait que très peu d'exemples explicites d'équations différentielles algébriques (en dimension > 1) ou cette propriété de désintégration a été établie. Mentionnons deux exemples récents : en dimension 2, les équations différentielles (non-autonomes) de Painlevé à parametres génériques étudiées par Pillay et Nagloo dans [23] et en dimension 3, l'équation différentielle satisfaite par la fonction j et ses $Gl_2(\mathbb{C})$-conjugués, étudiée par Freitag et Scanlon dans [10].

Dans ces deux cas, leurs démonstrations s'appuient sur des propriétés très spécifiques des solutions des équations différentielles considérées. Nous démontrons dans ce texte, *un critère dynamique d'orthogonalité aux constantes pour les équations différentielles réelles* au caractère bien plus général, permettant notamment de construire des familles non-limitées[2] d'équations différentielles algébriques dont le type générique est orthogonal aux constantes (voir aussi le paragraphe suivant concernant d'autres applications de ce critère).

Notre critère d'orthogonalité aux constantes concerne certaines équations différentielles algébriques (X, v) *définies sur le corps* $\mathbb{R}$ *des nombres réels* (munie de la dérivation triviale). Sous des hypothèses naturelles de lissité, on peut considérer l'espace analytique réel $X(\mathbb{R})^{an}$ *des conditions initiales réelles* ainsi que le flot analytique réel ϕ du champs de vecteurs v (défini sur un voisinage connexe U de $X(\mathbb{R})^{an} \times \{0\}$ dans $X(\mathbb{R})^{an} \times \mathbb{R}$)

$$\phi : U \subset X(\mathbb{R})^{an} \times \mathbb{R} \longrightarrow \mathbb{R}$$

décrivant pour tout $(t, x_0) \in U$, la position $\phi(x_0, t)$ de la condition initiale x_0 au temps t.

En général, le flot analytique réel ϕ ne peut être étendu à $X(\mathbb{R})^{an} \times \mathbb{R}$ tout entier — on parle alors d'explosion en temps fini des solutions — et il est nécessaire de se restreindre à un voisinage connexe de $X(\mathbb{R})^{an} \times \{0\}$ dans $X(\mathbb{R})^{an} \times \mathbb{R}$.

Lorsque c'est le cas et que le flot analytique réel ϕ peut être étendu à $X(\mathbb{R})^{an} \times \mathbb{R}$ tout entier, on dit alors que le flot ϕ est *complet*. Dans ce cas, on l'identifie à une action continue du groupe additif $(\mathbb{R}, +)$ par automorphismes analytiques sur $X(\mathbb{R})^{an}$ ou en d'autres termes à un $(\mathbb{R}, +)$-*système dynamique analytique réel*. Cette condition est automatique lorsque $X(\mathbb{R})^{an}$ est compact ou plus généralement lorsque l'on se restreint à travailler sur un à compact $K \subset X(\mathbb{R})^{an}$ invariant.

Le critère d'orthogonalité aux constantes, que nous démontrons ici, est extension modèle-théorique des arguments de non-intégrabilité *à la Poincaré*, reposant sur la complexité de la dynamique topologique réelle des équations différentielles considérées.

2. c'est-à-dire ne provenant pas toutes d'une même famille ne dépendant d'un nombre fini de paramètres.

THÉORÈME B. — *Soient X une variété absolument irréductible sur $\mathbb{R}$ et v un champ de vecteurs rationnel sur X. On note (M, ϕ) le flot régulier réel de (X, v_X). Supposons qu'il existe une partie compacte K de M, Zariski-dense dans X et invariante par le flot ϕ.*

Si $(K, (\phi_{t|K})_{t\in\mathbb{R}})$ est faiblement topologiquement mélangeant alors le type générique de (X, v) est orthogonal aux constantes.

Par définition, $M = X(\mathbb{R}) \setminus (\mathrm{Sing}(X) \cup \mathrm{Sing}(v))$ est ici la variété analytique réelle vérifiant les hypothèses de lissité nécessaires à l'intégration analytique du champ de vecteurs v. La restriction de ce flot à toute partie compacte invariante K de M définit alors un système dynamique réel. Ce système dynamique est dit *faiblement topologiquement mélangeant* si tous ses produits sont topologiquement transitifs (voir la partie 3.2 pour des formulations équivalentes de cette condition).

Le théorème B est prouvé dans la quatrième partie de ce texte à partir d'une étude consciencieuse (dans la troisième partie de ce texte) des compatibilités entre les notions d'invariance dans la catégorie « algébrique » des D-variétés et la catégorie « dynamique » des systèmes dynamiques analytiques.

Application aux équations de la mécanique classique. — Dans ce paragraphe, nous décrivons brièvement les applications du théorème B aux équations géodesiques à courbure negative qui sont l'objet de [18] et [17].

Nous considérons des équations différentielles modélisant des *systèmes autonomes conservatifs de la mécanique classique*, décrits de la façon suivante : Si (M, g) est une variété riemannienne présentée algébriquement et V une fonction algébrique sur M représentant l'énergie potentielle, ce sont les équations hamiltoniennes associé au hamiltonien :

$$H(x, p) = \frac{1}{2} g_x(p, p) + V(x)$$

(voir [18] pour une description du formalisme hamiltonien dans ce cadre algébrique).

Pour un tel système hamiltonien, les relations algébriques entre n solutions (resp. génériques) d'un même niveau d'énergie $H = E_0$ sont décrites par l'ensemble $\mathcal{I}_n(H; E_0)$ (resp. $\mathcal{I}_n^{gen}(H, E_0)$) des sous-variétés fermées $Z \subset T^n_{M/\mathbb{R}}$ qui s'écrivent

$$Z = \overline{\{(\gamma_1(t), \dot\gamma_1(t), \ldots, \gamma_n(t), \dot\gamma_n(t)) \mid t \in \mathbb{D}\}}.$$

comme la clôture de Zariski de n solutions analytiques (resp. génériques) $\gamma_1, \ldots, \gamma_n$ (définies sur un disque complexe $\mathbb{D}$), d'énergie E_0, de l'équation hamiltonienne sous étude.

Dans [18], nous étudions le cas des équations géodésiques d'une variété riemannienne compacte à courbure strictement négative — c'est-à-dire lorsque $V = 0$ et la variété riemannienne (M, g) est compacte a courbure strictement

négative. Dans ce cas, les résultats d'Anosov [1] mettent en évidence des propriétés hyperboliques globales pour la dynamique du flot analytique réél — regroupées sur le terme de *flot d'Anosov* — sur les niveaux d'énergie non nul du hamiltonien H. En utilisant conjointement ces résultats d'Anosov, le théorème A et le théorème B, nous obtenons dans [18], *l'existence d'un facteur désintégré pour le système de relations algébriques :*

$$\mathcal{L}^{gen}(H, E_0) = \{\mathcal{I}_n^{gen}(H, E_0) \mid n \geq 1\} \text{ lorsque } E_0 \neq 0.$$

Plus récemment et de façon complémentaire, j'ai étudié dans [17] les facteurs rationnels d'une équation différentielle réelle (X, v) dont le flot analytique est un flot d'Anosov mélangeant, lorsque la dimension de X est 3. Ces résultats impliquent que *pour une surface riemannienne (M, g) (présentée algébriquement) compacte à courbure strictement négative, le système de relations algébriques $\mathcal{L}^{gen}(H, E_0)$ de l'équation différentielle géodésique de (M, g) sur un niveau d'énergie non nul est lui-même désintégré.*

Familles d'équations différentielles algébriques. — Outre les équations différentielles « concrètes » évoquées ci-dessus, nous étudions aussi les propriétés d'orthogonalité aux constantes en famille pour les familles lisses d'équations différentielles algébriques.

En termes géométriques, une famille lisse d'équations différentielles algébriques $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ (à paramètres constants) est décrite par la donnée d'une famille lisse $f : \mathcal{X} \longrightarrow S$ de variétés algébriques paramétrée par S au dessus d'un corps k de caractéristique 0 et d'un champ de vecteurs v sur $\mathcal{X}$ tangent aux fibres de f.

Le champ de vecteurs v se restreint ainsi le long de chaque fibre et on pense au morphisme f comme à la famille $\{(X, v)_s \mid s \in S\}$ de ses fibres. Lorsque toutes les fibres de f sont absolument irréductibles (et donc que le type générique de chacune des fibres est stationnaire), on peut alors considérer

$$S^{\perp 0} = \{s \in S(\bar{l}) \mid \text{le type générique de } (X, v)_s \text{ est orthogonal aux constantes}\}.$$

où $\bar{l}$ est une extension algébriquement close fixée saturée de k.

Les exemples de dimension 1 de Hrushovski et Itai (voir [12]) montrent qu'en général, le sous-ensemble $S^{\perp 0} \subset S(\bar{l})$ n'est pas définissable. En revanche, des considérations très générale de théorie de la stabilité permettent de présenter $S^{\perp 0}$ comme un sous-ensemble $\mathrm{Aut}(\bar{l}/k)$-invariante de $S(\bar{l})$ — ou autrement dit, comme l'image inverse d'un sous-ensemble du schéma S.

Pour les familles d'équations différentielles algébriques complexes, cette propriété admet la conséquence suivante :

LEMME. — *Soit S une variété irréductible algébrique complexe et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille d'équations différentielles algébriques paramétrée par S dont les fibres sont toutes absolument irréductibles.*

Si la fibre générique de f est orthogonale aux constantes alors, il existe un ensemble dénombrable de sous-variétés algébriques fermées propres $\{Z_n \mid n \in \mathbb{N}\}$ de S tel que :

$$S(\mathbb{C}) \setminus \bigcup_{i\in\mathbb{N}} Z_i(\mathbb{C}) \subset S^{\perp 0}(\mathbb{C}).$$

Plus généralement, cet énoncé est valide si l'on remplace les nombres complexes par tout corps algébriquement clos. Dans le cas complexe qui est formulé ici, le théorème de Baire permet de garantir la non-vacuité de $S(\mathbb{C})\setminus\bigcup_{i\in\mathbb{N}} Z_i(\mathbb{C})$. Plus précisément, si la fibre générique de f est orthogonale aux constantes alors pour presque tout $s \in S(\mathbb{C})$ au sens de Baire, l'équation différentielle $(X, v)_s$ est orthogonale aux constantes.

Le lemme précédent sera appliqué conjointement avec le théorème de spécialisation suivant concernant la propriété de non-orthogonalité aux constantes pour les familles lisses d'équations différentielles algébriques.

Théorème C. — *Soient S une variété algébrique lisse et irréductible au dessus d'un corps k et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variétés à paramètres dans S.*

On suppose que toutes les fibres de f sont absolument irréductibles, on fixe $s \in S(k)$ et on dénote par η le point générique de S. Si le type générique de $(X, v)_\eta$ est non-orthogonal aux constantes alors le type générique de $(X, v)_s$ est non-orthogonal aux constantes.

Pour les familles d'équations différentielles complexes $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ vérifiant les hypothèses d'irréductibilité et de lissité du théorème C, le théorème C et le lemme ci-dessus impliquent donc que :

$$\text{ou bien } S^{\perp 0} = \emptyset, \text{ ou bien } S^{\perp 0} = S(\mathbb{C}) \setminus \bigcup_{i\in\mathbb{N}} Z_i(\mathbb{C})$$

pour un ensemble dénombrable de sous-variétés algébriques fermées propres $\{Z_n \mid n \in \mathbb{N}\}$ de S (voir le corollaire 2.24).

La preuve du théorème C repose sur l'équivalence entre la propriété d'orthogonalité aux constantes et sa formulation géométrique (la propriété (O)) Sous les hypothèses de lissité, les énoncés de spécialisation correspondant pour les intégrales premières rationnelles sont prouvés dans la seconde partie cet article.

Équations différentielles à paramètres très génériques. — Pour conclure, nous formulons maintenant deux applications du théorème C aux équations différentielles algébriques à paramètres très génériques.

Le premier résultat concerne les champs de vecteurs de degré d sur $\mathbb{A}^n_{\mathbb{C}}$ avec $n \geq 1$.

THÉORÈME D. — *Soit $d \geq 3$ et $n \geq 1$. Considérons un champs de vecteurs*

$$v(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n)\frac{d}{dx_1} + \cdots f_n(x_1, \ldots, x_n)\frac{d}{dx_n}.$$

sur l'espace affine complexe de dimension n, où $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]_{\leq d}$ sont des polynômes de degré $\leq d$.

Si les coefficients de $f_1, \ldots, f_n$ sont $\mathbb{Q}$-algébriquement indépendants[3] *alors le champ de vecteurs v est orthogonal aux constantes.*

Lorsque $n = 1$, le theoreme D est conséquence immédiate de résultats de Rosenlicht [28]. En dimension supérieure, notre démonstration (voir Section 2.4) s'appuie le cas de dimension 1 et sur le théorème C.

Pour conclure, formulons une seconde application du théorème C qui est une variante du critère dynamique d'orthogonalité aux constantes pour la fibre générique d'une famille d'équations différentielles algébriques. Cet énoncé obtenu en utilisant conjointement le théorème B et le théorème C.

THÉORÈME E. — *Soient k un sous-corps des nombres réels, S une variété algébrique lisse et irréductible au dessus de k et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variétés absolument irréductibles à paramètres dans S.*

Supposons qu'il existe un point $p \in S(\mathbb{R})$ et un compact $K \subset \mathcal{X}_p(\mathbb{R})^{an}$ Zariski-dense dans X et invariant par le flot ϕ du champ de vecteurs $v_{|X_p}$.

Si $(K, (\phi_{t|K})_{t\in\mathbb{R}})$ est faiblement topologiquement mélangeant alors il existe un ensemble dénombrable $\{Z_i : i \in \mathbb{N}\}$ de sous-variétés fermées algébriques strictes (sur le corps des nombres réels) Z_i de S tel que :

$$\forall s \in S(\mathbb{C}) \setminus \bigcup_{i\in\mathbb{N}} Z_i(\mathbb{C}),\ (\mathcal{X}, v)_s \text{ est orthogonal aux constantes.}$$

De façon similaire aux applications du théorème B à l'étude des équations géodésiques sur une variété riemannienne compacte à courbure strictement négative, le théorème D peut être appliqué à l'étude *des équations hamiltoniennes pour un potentiel V à paramètres très génériques sur une variété riemannienne compacte à courbure strictement négative.*

Plus précisément, considérons (M, g) est une variété riemannienne compacte à courbure strictement négative (présentée algébriquement) et $\mathcal{V} \in \mathrm{H}^0(S \times M, \mathcal{O}_{S\times M})$ une famille algébrique de potentiels sur M, paramétrée par une variété algébrique réelle S. Supposons de plus que pour un point $s_0 \in S(\mathbb{R})$, on ait $V(s_0, 0) = 0$.

On obtient alors une famille (au sens précédent) $f_{\mathcal{V}} : (T_{M/\mathbb{R}}, v_{\mathcal{V}}) \longrightarrow (S, 0)$ d'équations différentielles hamiltoniennes paramétrée par S dont la fibre au dessus de s_0 est l'équation différentielle géodésique de (M, g). Si la famille $f_{\mathcal{V}}$ vérifie les hypothèses du théorème D alors il existe un ensemble dénombrable

3. Cela implique, en particulier, que les f_i sont des polynômes de degré d dont tous les coefficients sont distincts et non nuls.

$\{Z_i : i \in \mathbb{N}\}$ de sous-variétés fermées algébriques strictes Z_i de S tel que *pour tout* $s \in S(\mathbb{C}) \setminus \bigcup_{i\in\mathbb{N}} Z_i(\mathbb{C})$, *le système hamiltonien avec potentiel* $V(s,-)$ *est orthogonal aux constantes.*

Organisation de l'article. — Cet article est organisé de la manière suivante :

La première partie est consacrée à l'étude des conséquences du théorème de Hrushovski-Sokolovic pour les équations différentielles autonomes. On étudie notamment la propriété de désintégration (propriété (D)) ainsi que le théorème A (corollaire 1.35 dans le texte).

La seconde partie concerne l'orthogonalité aux constantes, en tant que telle. On y démontre l'équivalence avec sa formulation géométrique (propriété (O)), puis on en déduit le théorème C de spécialisation (théorème 2.23 dans le texte) ainsi que ses conséquences concernant les champs de vecteurs génériques planaires (théorème D dans l'introduction et corollaire 2.25 dans le texte).

La troisième partie se concentrera l'aspect dynamique de l'étude des équations différentielles et jouera un rôle « d'intermédiaire » essentiel entre la catégorie des équations différentielles algébriques et la catégorie des systèmes dynamiques topologiques réels.

La quatrième et dernière partie est consacrée à la preuve du critère dynamique d'orthogonalité aux constantes (théorème B dans l'introduction et théorème 4.10 dans le texte) et de sa version en famille (théorème E dans l'introduction et théorème 4.10 dans le texte).

Enfin, cet article contient en appendice, des resultats formels concernant la catégorie des D-variétés, qui joue un rôle central dans les traductions entre les propriétés modèle-théoriques et leurs formulations géométriques.

1. Orthogonalité aux constantes

Dans cette partie, nous discutons la propriété d'orthogonalité aux constantes pour un type stationnaire de la théorie $\mathbf{DCF}_0$ défini sur un corps différentiel constant et sa relation avec la propriété de désintégration.

Il est bien connu que, dans toute théorie stable, un type stationnaire désintégré est orthogonal à tout type minimal non-localement modulaire (voir par exemple [25, Lemma 2.3 pp158]. En particulier, un type stationnaire désintégré est toujours orthogonal aux constantes. En revanche, des constructions élémentaires utilisant des noyaux de Manin illustrent simplement que la réciproque n'est pas toujours vérifiée (voir §14 de l'introduction et le théorème 4.24 du chapitre 3 de [16]).

Notre résultat principal concerne les équations différentielles autonomes : *Une équation différentielle autonome dont le type générique est orthogonal aux constantes admet toujours un facteur rationnel* (non-trivial, c'est-à-dire de dimension strictement positive) *désintégré.*

Ce résultat, propre à la théorie $\mathbf{DCF}_0$ — le corollaire 1.34 et sa formulation géométrique, le corollaire 1.35 — est obtenu à l'aide de méthodes pures de théorie géométrique de la stabilité et du théorème de trichotomie de Hrushovski-Sokolovic.

Nous supposerons une familiarité avec les résultats élémentaires de théories des modèles et de théorie de la stabilité. La lecture des chapitres 1-3 et 5-8 de [29] est suffisante à la compréhension de cette partie. La première section est consacrée la relation d'orthogonalité entre deux types d'une même théorie stable. Nous exposons brièvement dans la seconde, quelques résultats sur la théorie $\mathbf{DCF}_0$ dont nous nous servirons, dans la suite. Enfin, la troisième partie de cette section est consacrée à la preuve du théorème 1.35.

1.1. Orthogonalité dans une théorie stable. — Dans ce paragraphe, fixons T une théorie du premier ordre, stable, complète, dans un langage $\mathcal{L}$ ainsi que $\mathfrak{M} \models T$ un modèle monstre (relativement à un cardinal fixé κ) de la théorie T.

Un *(petit) ensemble de paramètres* désigne un sous-ensemble $A \subset M$ de cardinal strictement inférieur à κ. Si A est un ensemble de paramètres, on désigne par $S(A)$ l'ensemble des types (avec un nombre fini arbitraire de variables) au sens de la théorie T à paramètres dans A.

Si a, b des uplets de M, on rappelle que les deux uplets a et b sont dits *indépendants au dessus de* A si $\mathrm{tp}(a/A, b)$ est une extension non-déviante de $\mathrm{tp}(a/A)$. On notera alors $a \mathop{\smile\!\!\!\!\!\!|}_A b$ pour désigner que a et b sont indépendants au dessus de A. Cette relation vérifie les règles propriétés usuelles d'une relation d'indépendance [29, Théorème 8.5.5]. En particulier, elle est symétrique, i.e. $a \mathop{\smile\!\!\!\!\!\!|}_A b$ si et seulement si $b \mathop{\smile\!\!\!\!\!\!|}_A a$.

1.1.1. *Orthogonalité entre deux types stationnaires.* —

Notation 1.1. — Rappelons qu'un type $p \in S(A)$ est dit *stationnaire* lorsqu'il admet une unique extension non-déviante à toute extension des paramètres $A \subset B$. Si T est une théorie stable qui élimine les imaginaires alors tout type à paramètres dans un ensemble algébriquement clos est stationnaire.

Si p est un type stationnaire et $A \subset B$ une extension des paramètres, on note $p|B$ son unique extension non-déviante à B.

Définition 1.2. — Soient $p, q \in S(A)$ deux types stationnaires sur A. On dit que p et q sont *faiblement orthogonaux* et on note $p \perp^a q$ si deux réalisations quelconques $a, b \in M$ de p et q respectivement sont indépendantes au dessus de A i.e.

$$\text{Si } a \models p \text{ et } b \models q \text{ alors } a \mathop{\smile\!\!\!\!\!\!|}_A b.$$

Par symétrie de la relation d'indépendance dans une théorie ω-stable, la notion d'orthogonalité faible est une relation symétrique.

Remarque 1.3. — De façon équivalente, deux types stationnaires $p(x) \in S(A)$ et $q(y) \in S(A)$ sont faiblement orthogonaux si et seulement si le type partiel $\pi(x,y) = p(x) \cup q(y)$ admet une unique complétion en un type complet.

Définition 1.4. — Soient $A, B \subset M$ des ensembles, $p \in S(A)$ et $q \in S(B)$ deux types stationnaires. On dit que p et q sont *orthogonaux* et on note $p \perp q$ si pour tout ensemble de paramètres $C \supset A \cup B$, les extensions non-déviantes respectives $p|C$ et $q|C$ de p et q à C sont faiblement orthogonales.

1.1.2. *Principe de réflexivité de Shelah.* —

Définition 1.5. — Soient $p, q \in S(A)$ deux types stationnaires. On appelle *produit tensoriel de p et q*, le type complet à paramètres dans A

$$p \otimes q = \mathrm{tp}(a, b/A)$$

où a est une réalisation de p et b réalise l'unique extension non deviante de q à $q|A, a$. De même, pour tout $n \in \mathbb{N}$, on note $p^{\otimes n} = p \otimes \cdots \otimes p$ le produit tensoriel de p avec lui même n fois.

Nous utiliserons l'avatar suivant du principe de réflexivité de Shelah pour la notion d'orthogonalité.

Proposition 1.6 ([25, Chapitre 1, Lemme 4.3.1]). — *Soient $\mathfrak{M}$ un modèle de T, $A \subset M$ un ensemble de paramètres et $p, q \in S(A)$ deux types stationnaires. On a équivalence entre :*

(i) *Les types p et q sont orthogonaux.*
(ii) *Pour tout $n \in \mathbb{N}$ et tout $m \in \mathbb{N}$, les types $p^{\otimes n}$ et $q^{\otimes m}$ sont faiblement orthogonaux.*

1.1.3. *Analyse semi-minimale et non-orthogonalité.* — Rappelons qu'un type stationnaire $p \in S(A)$ dans une théorie stable T est *minimal* s'il est non-algébrique et toute extension déviante de p est algébrique.

Proposition 1.7 ([25, Chapitre 2, Remarque 2.10]). — *Soit $\mathfrak{M}$ un modèle κ-saturé de T. La relation « être non-orthogonal » est une relation d'équivalence sur l'ensemble des types minimaux à paramètres dans M.*

La relation de non-orthogonalité cesse d'être une relation d'équivalence lorsqu'on ne se restreint plus au types minimaux dès que la théorie T est multidimensionnelle — i.e. admet au moins deux types minimaux orthogonaux. Néanmoins, elle permet de définir un dévissage des types p de rang de Lascar fini en *types semi-minimaux*, que nous décrivons maintenant.

Lemme 1.8 ([25, Chapitre 2, Lemme 2.5.1]). — *Soient $\mathfrak{M}$ un modèle κ-saturé de T, $A \subset M$ un ensemble de paramètres petit et $p \in S_n(A)$ un type de rang* RU *fini. Il existe une extension $A \subset B$ de paramètres et un type stationnaire minimal $q \in S(B)$ non-orthogonal à p.*

PROPOSITION 1.9. — *Soient $\mathfrak{M}$ un modèle de T, $A \subset M$ un ensemble de paramètres et $p \in S_n(A)$ un type stationnaire de rang* RU *fini égal à $r \in \mathbb{N}$. Il existe une suite d'extensions de paramètres $A \subset A_1 \subset A_2 \subset \cdots \subset A_r$, une suite d'extension $p \subset p_1 \subset p_2 \subset \cdots \subset p_r$ où $p_i \in S(A_i)$ est un type stationnaire et des types minimaux stationnaires $q_i \in S(A_i)$ vérifiant*

(i) *Pour tout $i \leq r$, le rang de Lascar $RU(p_i)$ de p_i est $r+1-i$. En particulier, le type p_1 est une extension non déviante de p et p_r est un type minimal.*

(ii) *Pour $i = r$, on a $p_r = q_r$ et pour tout $1 \leq i < r$, il existe des réalisations $a_i \models p_i$ et $b_i \models q_i$ telles que $b_i \in \mathrm{acl}(A_i, a_i)$ et p_{i+1} est une extension stationnaire non déviante à A_{i+1} de $\mathrm{tp}(a_i/A_i, b_i)$.*

Démonstration. — On raisonne par récurrence sur le rang de Lacar $r = \mathrm{RU}(p) \in \mathbb{N}$ de p.

Pour $r = 1$, il suffit de poser $A_1 = A$ et $p_1 = q_1 = p$.

Supposons le résultat montré pour les types de rang de Lascar $r \in \mathbb{N}$. Considérons $p \in S(A)$ un type stationnaire de rang de Lascar $r+1$.

D'après le lemme 1.8, il existe un ensemble $B \subset M$ de paramètres et $q \in S(B)$ un type stationnaire minimal non orthogonal à p. Considérons $C \supset A \cup B$ un ensemble de paramètres et des réalisations $a \models p|C$ et $b \models q|C$ vérifiant $a \not\perp_C b$.

Le type $\mathrm{tp}(b/C)$ étant minimal, on en déduit que $b \in \mathrm{acl}(C, a)$. On pose alors $A_1 = C$, $q_1 = q|C$, $p_1 = p|C$. Par additivité du rang de Lascar, le type $p = \mathrm{tp}(a/b, C)$ est de rang de Lascar $r \in \mathbb{N}$. On applique alors l'hypothèse de récurrence à une extension stationnaire de $p = \mathrm{tp}(a/b, C)$. □

REMARQUE 1.10. — Les données $\mathcal{A} = ((A_i)_{i \leq r}, (p_i)_{i \leq r}, (q_i)_{i \leq r})$ où $A \subset A_1 \subset A_2 \subset \cdots \subset A_r$ est une extension de paramètres, et de types stationnaires $p_i, q_i \in S(A_i)$ dont l'existence est assurée par la proposition 1.9 est appelée *une analyse du type $p \in S(A)$ par les types minimaux $q_1, \cdots q_r$.*

On note alors $[p]_{\mathcal{A}} = \{[q_1], \cdots, [q_r]\}$ l'ensemble des classes de non-orthogonalité des types minimaux intervenant dans l'analyse de p.

PROPOSITION 1.11. — *Soient $\mathfrak{M}$ un modèle de T, $A \subset M$ un ensemble de paramètres et $p \in S_n(A)$ un type stationnaire de rang* RU *fini égal à $r \in \mathbb{N}$. Si $\mathcal{A}$ et $\mathcal{A}'$ sont deux analyses de p alors $[p]_{\mathcal{A}} = [p]_{\mathcal{A}'}$.*

Plus précisément, pour toute analyse $\mathcal{A}$ de p, on a

$$[p]_{\mathcal{A}} = \{[q] \mid q \text{ est un type minimal non orthogonal à une extension de } p\}.$$

Si $p \in S(A)$ est un type de rang de Lascar fini, on notera $[p] = [p]_{\mathcal{A}}$ pour toute analyse $\mathcal{A}$ de p dont l'existence est assurée par la proposition 1.9 et qui est bien défini d'après la proposition 1.11.

Démonstration. — La deuxième partie de la proposition implique la première. La condition (ii) de la proposition 1.9 montre que :

$$[p]_{\mathcal{A}} \subset \{[q] \mid q \text{ est un type minimal non orthogonal à une extension de } p\}.$$

Il suffit donc de montrer l'inclusion réciproque : Considérons $\mathcal{A}$ une analyse de p et un type $q \in S(B)$ minimal orthogonal à $[p]_{\mathcal{A}}$ (i.e. orthogonal à tous les éléments de $[p]_{\mathcal{A}}$). Soit $A \subset C$ une extension de paramètres et $\widehat{p} \in S(C)$ une extension de p. Montrons que q est orthogonal à $\widehat{p}$.

D'après [25, Chapitre 8, Lemme 1.2(i)], il existe une analyse $\widehat{\mathcal{A}}$ de $\widehat{p}$ avec

$$[\widehat{p}]_{\widehat{\mathcal{A}}} \subset [p]_{\mathcal{A}}.$$

Par hypothèse, le type q est orthogonal à tous les éléments de $[\widehat{p}]_{\widehat{\mathcal{A}}}$ et donc d'après [25, Chapitre 8, Lemme 1.2(iv)], le type q est orthogonal à tous les types analysables dans $[\widehat{p}]_{\widehat{\mathcal{A}}}$ et en particulier à $\widehat{p}$. □

Exemple 1.12. — Soient $\mathfrak{M}$ un modèle de T, $A \subset M$ un ensemble de paramètres et $p_1, \cdots, p_n \in S(A)$ des types minimaux stationnaires. On vérifie facilement que

$$[p_1 \otimes \cdots \otimes p_n] = \{[p_1], \cdots, [p_n]\}.$$

1.2. Corps différentiellement clos. — On rappelle qu'un corps différentiel (de caractéristique 0) est un couple (K, δ) où K est un corps de *caractéristique* 0 et $\delta : K \longrightarrow K$ une dérivation. Dans tout le texte, on travaillera en caractéristique 0, on parlera donc de corps différentiel pour désigner un corps différentiel de caractéristique 0.

1.2.1. *Définition.* — Du point de vue syntaxique, un corps différentiel est une $\mathcal{L}_\delta$-structure où $\mathcal{L}_\delta = \{0, 1, +, ., -, \delta\}$ est appelé *langage des corps différentiels* vérifiant les axiomes des corps différentiels (qui sont du premier ordre dans le langage $\mathcal{L}_\delta$).

Remarque 1.13. — Pour le langage $\mathcal{L}_\delta$ des corps différentiels, les formules sans quantificateurs à paramètres dans un corps différentiel (K, δ) sont les combinaisons booléennes d'équations différentielles algébriques, c'est-à-dire d'équations différentielles de la forme :

$$(E) : P(x_1, \cdots, x_r, \delta(x_1), \cdots, \delta(x_r), \cdots, \delta^k(x_1), \cdots, \delta^k(x_r)) = 0$$

où $P \in K[X_1^{(0)}, \cdots, X_r^{(0)}, \cdots, X_1^{(k)}, \cdots, X_r^{(k)}]$ est un polynôme.

Parmi les modèles de la théorie des corps différentiels, certains possèdent une importance particulière, ce sont les modèles existentiellement clos.

Définition 1.14. — Soient T une théorie dans un langage $\mathcal{L}$ et $\mathfrak{M}$ un modèle de T. On dit $\mathfrak{M}$ est *un modèle existentiellement clos de* T si pour toute extension

de modèles $\mathfrak{M} \subset \mathfrak{M}'$ de T, toute formule sans quantificateurs $\phi(\overline{x}, \overline{y})$ et tout $\overline{b} \in M^n$, on a :

$$\mathfrak{M}' \models \exists \overline{x} \phi(\overline{x}, \overline{b}) \Longleftrightarrow \mathfrak{M} \models \exists \overline{x} \phi(\overline{x}, \overline{b}).$$

DÉFINITION 1.15. — On appelle *corps différentiellement clos*, tout modèle existentiellement clos de la théorie des corps différentiels.

1.2.2. *Propriétés globales de la théorie* $\mathbf{DCF}_0$. —

THÉORÈME 1.16 (Blum, Poizat). — *La classe des corps différentiellement clos est axiomatisable dans le langage $\mathcal{L}_\delta$ des corps différentiels par une théorie du premier ordre notée $\mathbf{DCF}_0$ et appelée théorie des corps différentiellement clos. Une axiomatisation de cette théorie est donnée par :*

$\mathbf{DCF}_0^I$: *(K, δ) est un corps différentiel (de caractéristique 0).*

$\mathbf{DCF}_0^{II}$: *Pour tout $n \in \mathbb{N}$, et tous polynômes $P \in K[X_1^{(0)}, \cdots, X_1^{(n)}] \setminus K[X_1^{(0)}, \cdots, X_1^{(n-1)}]$ et $Q \in K[X_1^{(0)}, \cdots, X_1^{(n-1)}]$ non nul, il existe $y \in K$ tel que*

$$P(y, \delta(y), \cdots, \delta^n(y)) = 0 \wedge Q(y, \delta(y), \cdots, \delta^{n-1}(y)) \neq 0.$$

De plus, la théorie $\mathbf{DCF}_0$ est complète et élimine les quantificateurs et les imaginaires dans le langage $\mathcal{L}_\delta$ des corps différentiels.

COROLLAIRE 1.17 (Description des types). — *Soient $(\mathcal{U}, \delta_U)$ un corps différentiellement clos et $(K, \delta) \subset (\mathcal{U}, \delta_U)$ un sous-corps différentiel. L'application définie par*

$$I : \begin{cases} S_n(K) \longrightarrow \mathrm{Spec}_\delta(K\{X_1, \cdots X_n\}) \\ \qquad p \longmapsto \{P \in K\{X_1, \cdots X_n\} \mid \text{« } P(x) = 0 \text{ »} \in p\} \end{cases}$$

est une bijection, où $\mathrm{Spec}_\delta(K\{X_1, \cdots, X_n\})$ désigne l'ensemble des idéaux premiers différentiels de la (K, δ)-algèbre différentielle libre $K\{X_1, \cdots, X_n\}$ avec variables $X_1, \ldots X_n$.

COROLLAIRE 1.18. — *La théorie $\mathbf{DCF}_0$ est ω-stable.*

Démonstration. — D'après le théorème de Ritt-Raudenbush (voir [21, Partie 2, Théorème 1.16]), on peut choisir pour tout idéal premier différentiel $I \subset K\{X_1, \cdots, X_n\}$, un système générateur $S(I)$ de l'idéal I en tant qu'idéal différentiel radical. La description précédente de l'ensemble $S_n(A)$ des types à paramètres dans A montre que l'application

$$\begin{cases} S_n(A) \longrightarrow \mathbb{Q}\langle A \rangle\{X_1, \cdots, X_n\}^{(\mathbb{N})} \\ \qquad p \longmapsto S(I(p)) \end{cases}$$

est une injection. On en déduit que $S_n(A)$ est dénombrable dès que A est dénombrable et donc que la théorie $\mathbf{DCF}_0$ est ω-stable. □

1.2.3. *Structure induite sur le corps des constantes.* —

Définition 1.19. — Soit (K, δ) un corps différentiel. Le *corps des constantes* de (K, δ) est le sous-corps de K noté K^δ et défini par :

$$K^\delta = \{x \in K \mid \delta(x) = 0\}.$$

Corollaire 1.20 ([21, Partie 2, Lemme 5.10]). — *Soit $(\mathcal{U}, \delta_\mathcal{U})$ un corps différentiellement clos. Le corps des constantes $\mathcal{C}$ de $(\mathcal{U}, \delta_U)$ est un corps algébriquement clos et la structure induite par $\mathcal{U}$ sur le sous-corps définissable $\mathcal{C}$ est celle d'un pur corps algébriquement clos*[4].

En particulier, comme pour un pur corps algébriquement clos, les sous-ensembles definissables du corps des constantes d'un corps différentiellement clos sont toujours finis ou cofinis. Autrement dit, le corps des constantes d'un corps différentiellement clos est un ensemble definissable fortement minimal.

Définition 1.21. — Soient $(\mathcal{U}, \delta_\mathcal{U})$ un corps différentiellement clos et $p \in S(A)$ un type à paramètres dans un sous-ensemble $A \subset \mathcal{U}$. On dit que le type p est *orthogonal aux constantes* si p est orthogonal au type générique de l'ensemble fortement minimal

$$\mathcal{U}^\delta = \{x \in \mathcal{U} \mid \delta(x) = 0\}.$$

1.3. Orthogonalité aux constantes et désintégration. —

1.3.1. *Propriété de désintégration.* — On fixe k un corps de caractéristique 0.

Remarque 1.22. — On travaille dans ce qui suit dans la catégorie des D-schémas (X, δ_X) au dessus de $(k, 0)$ au sens de l'appendice A — c'est-à-dire des schémas X au dessus de k munis d'une dérivation $\delta_X : \mathcal{O}_X \longrightarrow \mathcal{O}_X$ sur le faisceau structurel de X.

Lorsque X est un schéma intègre lisse, le k-espace vectoriel $\mathrm{Der}_k(\mathcal{O}_X)$ des dérivations de X triviales sur k peut être identifié avec l'ensemble $\mathcal{X}(X)$ des champs de vecteurs sur X (c'est à dire des sections globales du fibré tangent $T_{X/k}$ de X) par :

$$\begin{cases} \mathcal{X}(X) \longrightarrow \mathrm{Der}_k(\mathcal{O}_X) \\ \qquad v \longrightarrow \delta_v : f \mapsto df(v). \end{cases}$$

Lorsque X est un schéma intègre lisse, on idenfiera le champ de vecteurs v et la derivation δ_v qu'il induit sur $\mathcal{O}_X$ et on notera (X, v) la D-variété associée au champ de vecteurs v.

4. Autrement dit, pour tout sous-ensemble de paramètres petit $B \subset \mathcal{U}$, les sous-ensembles B-définissables de $\mathcal{C}$ sont les sous-ensembles $\mathrm{dcl}(B) \cap \mathcal{C}$-définissables de $\mathcal{C}$ dans le langage des anneaux.

NOTATION 1.23. — Soit (X, v) une D-variété absolument irréductible au dessus de $(k, 0)$. Pour tout $n > 0$, on note $\mathcal{I}_n^{gen}(X, v)$, *l'ensemble des sous-schémas fermés intègres invariants de* $(X, v)^n$ *qui se projettent génériquement sur tous les facteurs.*

Notons que d'après la proposition A.13, un sous-schéma fermé réduit $Y \subset (X, v)^n$ est invariant si et seulement si ses composantes irréductibles le sont.

DÉFINITION 1.24. — Soit (X, v) une variété absolument irréductible X munie d'un champ de vecteurs v au dessus de k. On dit que (X, v) est *génériquement désintégrée* si pour tout $n \geq 3$, tout élément $Z \in \mathcal{I}_n^{gen}(X, v)$ s'écrit comme une composante irréductible (se projetant génériquement sur tous les facteurs) de :

$$\bigcap_{1 \leq i < j \leq n} \pi_{i,j}^{-1}(Z_{i,j}). \tag{1}$$

où $\pi_{i,j} : X^n \longrightarrow X^2$ est la projection sur les i^{eme} et j^{eme} coordonnées et $Z_{i,j} \in \mathcal{I}_2^{gen}$ pour tout $i \neq j$.

REMARQUE 1.25. — Les propriétés suivantes sont des conséquences immédiate de la définition précédente :

(1) Dans la définition 1.24, on peut remplacer l'identité (1) par :

$$\bigcap_{1 \leq i \neq j \leq n} \pi_{i,j}^{-1}(Z_{i,j}).$$

Cette forme est particulièrement agréable lorsque l'on travaille avec des notations multi-indices (par exemple lemme 1.27).

(2) Si (X, v) est génériquement désintégrée, alors pour tout $n \geq 3$, tout $Z \in \mathcal{I}_n^{gen}(X, v)$ s'écrit comme une composante irréductible de

$$\bigcap_{1 \leq i < j \leq n} \pi_{i,j}^{-1}(\overline{\pi_{i,j}(Z)}).$$

(3) Dans la définition 1.24, il n'est pas nécessaire de supposer que les $Z_{i,j}$ sont irréductibles. En effet, si $Z_{1,2}$ se décompose en une union de sous-variétés fermés stricts $Z_{1,2} = F \cup G$ alors ces dernières sont invariantes (voir Appendice A) et :

$$\bigcap_{1 \leq i < j \leq n} \pi_{i,j}^{-1}(Z_{i,j}) = \Big(\pi_{1,2}^{-1}(F) \cap \bigcap_{(i,j) \neq (1,2)} \pi_{i,j}^{-1}(Z_{i,j})\Big) \cup \Big(\pi_{1,2}^{-1}(G) \cap \bigcap_{(i,j) \neq (1,2)} \pi_{i,j}^{-1}(Z_{i,j})\Big).$$

En particulier, les composantes irréductibles du membre de droite sont les composantes irréductibles des deux facteurs du membre de gauche.

LEMME 1.26. — *Soit (X, v) une variété absolument irréductible X munie d'un champ de vecteurs v au dessus de k. Si le type générique de (X, v) est minimal et désintégré alors (X, v) est génériquement désintégrée.*

Cet énoncé est une variante des résultats bien connus de théorie des modèles. Par manque de référence, nous formulons une preuve rapide.

Démonstration. — Considérons $Z \in \mathcal{I}_n^{gen}(X, v)$ une sous-variété fermée invariante de $(X, v)^n$ se projetant génériquement sur tous les facteurs.

Considérons $n_0 \in \mathbb{N}$ maximal tel que Z se projette génériquement sur X^{n_0} via les projections coordonnées. Sans perte de généralité, on peut supposer que Z se projette génériquement sur les n_0 premières coordonnées.

Fixons maintenant un corps differentiellement clos $(\mathcal{U}, \delta_{\mathcal{U}})$ et considérons $(a_1, \ldots, a_n)$ une réalisation du type générique de Z (comme Z se projette génériquement sur chacun des facteurs, chaque a_i réalise le type générique de (X, v)).

Comme le type générique de X est minimal et désintégré, on en deduit que pour tout $k > n_0$,

$$a_k \in \operatorname{acl}(a_1, \ldots, a_{n_0}) = \operatorname{acl}(a_1) \cup \cdots \cup \operatorname{acl}(a_{n_0}).$$

Pour tout $k > n_0$, il existe donc $i(k) \leq n_0$ et une correspondance génériquement finie $Y_k \subset X^2$ telle que $(a_k, a_{i(k)}) \in Y_k$. Posons alors

$$Y = \bigcap_{k > n_0} \pi_{k,i(k)}^{-1}(Z_k).$$

Par construction, la fibre générique de Y par la projection sur les n_0 premières coordonnées est finie (bornée par le produit des fibres des Y_k pour $k > n_0$). De plus, on a $(a_1, \ldots, a_n) \in Y$ et donc $Z \subset Y$. On en déduit que :

$$\dim(Z) = \dim(Y) = n_0.\dim(X)$$

et donc que Z est une composante irréductible de Y. □

1.3.2. *Quelques propriétés structurelles de la désintégration.* —

LEMME 1.27. — *Soit (X, v) une variété absolument irréductible X munie d'un champ de vecteurs v au dessus de k. Si (X, v) est génériquement désintégrée et $n \geq 1$ alors $(X, v)^n$ l'est aussi.*

Démonstration. — Considérons $Z \in \mathcal{I}_m^{gen}((X, v)^n)$ une sous-variété fermée invariante de $((X, v)^n)^m$ se projetant génériquement sur tous les facteurs. On utilise une notation double-indice : pour tout $1 \leq i \leq n$ et $1 \leq k \leq m$, (i, k) désigne la i-ème coordonne du k-ème facteur $(X, v)^n$.

Puisque (X,v) est désintégrée, il existe $Z_{i,j,k,l} \in \mathcal{I}_2^{gen}(X,v)$ pour tout $(i,k) \neq (j,l)$ telles que Z est une composante irréductible de

$$Y = \bigcap_{(i,k)\neq(j,l)} \pi_{i,k,j,l}^{-1}(Z_{i,j,k,l}).$$

Comme Z se projette génériquement sur tous les facteurs on peut supposer $Z_{i,j,k,k} = X^2$ pour $i \neq j$. On peut donc réécrire :

$$Y = \bigcap_{k\neq l} \Big(\bigcap_{i,j} \pi_{i,k,j,l}^{-1}(Z_{i,j,k,l}) \Big) = \bigcap_{k\neq l} Y_{k.l}.$$

Fixons $k \neq l$. En notant $\pi_{k,l}$ la projection sur le k-ème et l-ème facteur et $\pi_{i,j}$ la projection de $(X,v)^n \times (X,v)^n$ sur la i-ème coordonnée du premier facteur et la j-ème du second, on a $\pi_{i,j,k,l} = \pi_{i,j} \circ \pi_{k,l}$. On en déduit que :

$$Y_{k,l} = \bigcap_{i,j} \pi_{k,l}^{-1}(\pi_{i,j}^{-1}(Z_{i,j,k,l})) = \pi_{k,l}^{-1}\Big(\bigcap_{i,j} \pi_{i,j}^{-1}(Z_{i,j,k,l}) \Big).$$

Posons alors $Z_{k,l} = \bigcap_{i,j} \pi_{i,j}^{-1}(Z_{i,j,k,l})$ qui est une sous-variété fermée invariante de $(X,v)^n \times (X,v)^n$ se projetant génériquement sur les deux facteurs. On conclut que Z est une composante irréductible de Y qui s'écrit :

$$Y = \bigcap_{k\neq l} Y_{k,l} = \bigcap_{k\neq l} \pi_{k,l}^{-1}(Z_{k,l}). \qquad \square$$

PROPOSITION 1.28. — *Soient (X,v) et (Y,w) deux variétés absolument irréductibles munies respectivement de champs de vecteurs v et w au dessus de k et $f : (X,v) \dashrightarrow (Y,w)$ un morphisme rationnel génériquement fini de D-variétés au dessus de k.*

L'équation différentielle (X,v) est génériquement désintégrée si et seulement si (Y,w) est génériquement désintégrée.

La preuve de la proposition précédente est construire a partir du lemme de géométrie algébrique pure (non différentielle) suivant :

LEMME 1.29. — *Soit $f : X \longrightarrow Y$ est un morphisme étale au dessus d'un corps k de caractéristique 0, Z_Y une sous-variété fermée irréductible de Y et Z_X une composante irréductible de $f^{-1}(Z_Y)$. Pour toute sous-variété fermée Z de Y les propriétés suivantes sont équivalentes :*

(i) *Z_X est une composante irréductible de $f^{-1}(Z)$.*
(ii) *Z_Y est une composante irréductible de Z.*

Démonstration. — Supposons (i). Il suffit de montrer que Z_Y est une sous-variété fermée irréductible maximale de Z.

Considérons une sous-variété fermée irréductible T de Y telle que $Z_Y \subset T \subset Z$. On en déduit que Z_X est inclus dans une composante irréductible T_1 de $f^{-1}(T)$. Par maximalité de Z_X, on a $Z_X = T_1$. On en déduit que :

$$Z_Y = \overline{f(Z_X)} = \overline{f(T_1)} = T.$$

Réciproquement supposons (ii) et considérons une sous-variété fermée irréductible T de X telle que $Z_X \subset T \subset f^{-1}(Z)$

En appliquant f, on obtient $Z_Y \subset \overline{p(T)} \subset \overline{Z}$ et donc $Z_Y = \overline{p(T)}$ (par maximalité de Z_Y). Il suit que T est une composante irreductible de $f^{-1}(\overline{p(T)}) = f^{-1}(Z_Y)$ qui contient Z_X et donc $T = Z_X$. □

Demonstration de la proposition 1.28. — La propriété de désintégration est préservée en replaçant X et Y par des ouverts non vides, on peut donc supposer que $f : (X, v) \longrightarrow (Y, w)$ est un morphisme étale surjectif.

Pour tout $n \geq 1$, on note $f_n = f \times \cdots \times f : X^n \longrightarrow Y^n$ qui est aussi un morphisme étale. On a un diagramme commutatif :

$$\begin{array}{ccc} X^n & \xrightarrow{f_n} & Y^n \\ {\scriptstyle \pi^X_{i,j}}\downarrow & & \downarrow{\scriptstyle \pi^Y_{i,j}} \\ X^2 & \xrightarrow{f_2} & Y^2 \end{array}$$

Considérons $Z_Y \in \mathcal{I}_n^{gen}(Y, v)$ et considérons Z_X une composante irréductible de $f^{-1}(Z_Y)$. Nous montrons que les propriétés de désintégration pour Z_X et Z_Y sont équivalentes :

Posons $X_{i,j} = \overline{\pi^X_{i,j}(Z_X)} \in \mathcal{I}_2^{gen}(X, v)$ et $Y_{i,j} = \overline{f_2(X_{i,j})} \in \mathcal{I}_2^{gen}(Y, w)$. Comme le morphisme f_2 est étale, $X_{i,j}$ est une composante irréductible $f_2^{-1}(\overline{f_2(X_{i,j})})$.

Comme le morphisme f_2 est étale, $X_{i,j}$ est une composante irréductible $f_2^{-1}(\overline{f_2(X_{i,j})})$. En utilisant le point (3) de la remarque après la définition 1.24, on en deduit que l'ensemble des composantes irréductibles de

$$\bigcap_{1 \leq i \neq j \leq n} (\pi^X_{i,j})^{-1}(X_{i,j})$$

est inclus dans l'ensemble des composantes irréductibles de :

$$\bigcap_{1 \leq i \neq j \leq n} (\pi^X_{i,j})^{-1}(f_2^{-1}(Y_{i,j})) = f_n^{-1}\Big(\bigcap_{1 \leq i \neq j \leq n} (\pi^Y_{i,j})^{-1}(Y_{i,j})\Big).$$

Ainsi Z_X vérifie la propriété de désintégration si et seulement si c'est une composante irréductible du membre de droite si et seulement Z_Y est une composante irréductible de

$$\bigcap_{1 \leq i \neq j \leq n} (\pi^Y_{i,j})^{-1}(Y_{i,j}).$$ □

1.3.3. *De la minimalité à la semi-minimalité.* — Dans cette section, on étend le lemme 1.26 au cas où le type générique de l'équation différentielle (X, v) est seulement semi-minimal et désintégré. Ce raffinement sera necessaire pour la preuve du corollaire 1.35.

Définition 1.30. — Soient T une théorie stable, A un ensemble de paramètres et $p \in S(A)$ un type à paramètres dans A.

On dit que p est *semi-minimal* s'il existe une extension des paramètres $A \subset B$ et $q \in S(B)$ un type minimal tels que le type p est presque-interne à l'ensemble des $\mathrm{acl}(A)$-conjugués de q. On dit que le type p est *semi-minimal et désintégré* si, de plus, le type minimal $q \in S(B)$ est désintégré.

On a une description particulièrement simple des types semi-minimaux désintégrés si l'on s'autorise à remplacer le type q par un autre type minimal qui lui est non-orthogonal :

Proposition 1.31. — *Soient T une théorie stable, A un ensemble de paramètres et $p \in S(A)$ un type semi-minimal et désintégré à paramètres dans A.*

Il existe un type minimal désintégré $r \in S(A)$ (non-orthogonal à q) et des réalisations A-indépendantes $a_1, \ldots, a_j$ de r et une réalisation b de p telles que :

$$\mathrm{acl}_A(b) = \mathrm{acl}_A(a_1, \ldots a_j).$$

Démonstration. — On travaille dans un modèle saturé $\mathcal{U}$. Le type q est un type minimal et désintégré et donc en particulier localement modulaire. Cela implique que tout type analysable dans des conjugués de q est monobasé. En particulier, le type p est un type monobasé.

Soit b une réalisation de p. Considérons e tel que $\mathrm{RU}(b/eA) = \mathrm{RU}(b/A) - 1$ et tel que $e = \mathrm{Cb}(b/e)$. Comme le type p est monobasé, on a donc $e \in \mathrm{acl}(A, b)$. On en déduit facilement que :

$$\mathrm{RU}(e/A) = \mathrm{RU}(be/A) - \mathrm{RU}(b/Ae) = 1.$$

On en déduit que $r = \mathrm{tp}(e/A)$ est un type minimal non-orthogonal à p et donc à q (car le type p est q-semi minimal). On a donc construit un type minimal et désintégré $r \in S(A)$ tel que p est presque interne à r. Quitte a remplacer p par un type interalgebrique, on peut donc supposer que p est interne à r.

Montrons maintenant que $b \in \mathrm{acl}_A(e_1, \ldots, e_n)$ pour des réalisations $e_1, \ldots, e_n$ de r, c'est-à-dire que b a une orbite finie sous l'action du groupe $\mathrm{Aut}(\mathcal{U}/\mathcal{R})$ des automorphismes de $\mathcal{U}$ fixant point par point l'ensemble $\mathcal{R}$ des réalisations de r.

Comme le type p est interne à r, le groupe de liaison $\mathrm{Aut}_A(\mathcal{P}/\mathcal{R})$ des permutations de $\mathcal{P}$ provenant d'un automorphisme de $\mathcal{U}$ fixant $\mathcal{R}$ est isomorphe à un groupe définissable dans $\mathcal{R}^{eq}$ (voir [13, Theorem 3]). La propriété de désintégration de r garantit la finitude du groupe G et donc de l'orbite de b.

On a donc obtenu $b \in \mathrm{acl}_A(e_1, \ldots, e_n)$ pour des réalisations $e_1, \ldots, e_n$ de r et donc que $\mathrm{acl}_A(b) \subset \mathrm{acl}_A(e_1, \ldots, e_n)$. Par minimalité de r, cet ensemble acl-clos admet une base de transcendance de réalisations de r : il existe des réalisations A-indépendantes $a_1, \ldots a_j$ de r telles que

$$\mathrm{acl}_A(b) = \mathrm{acl}_A(a_1, \ldots a_j). \qquad \square$$

COROLLAIRE 1.32. — *Soit Y variété absolument irréductible au dessus d'un corps k munie d'un champ de vecteurs w. Si le type générique de (Y, w) est semi-minimal et désintégré alors (Y, w) est génériquement désintégrée.*

Démonstration. — Considérons un corps différentiellement clos $(\mathcal{U}, \delta_{\mathcal{U}})$ et b réalisant le type générique de (X, v). D'après la proposition 1.31, il existe un type minimal et désintégré $q \in S(k)$ et des réalisations k-indépendantes $(a_1, \ldots, a_j)$ de q telles que :

$$(*) \qquad \mathrm{acl}_k(b) = \mathrm{acl}_k(a_1, \ldots a_j).$$

Comme le type q est un type de rang fini à paramètres dans k, il existe une variété absolument irréductible Y et champ de vecteurs w sur Y tel que q est le type générique de (Y, w).

Comme les a_i sont des réalisations k-indépendantes de q, on en déduit que $a_1, \ldots, a_j$ réalise le type générique de $(Y, w)^j$. La propriété $(*)$ exprime donc que les types génériques de $(Y, w)^j$ et (X, v) sont interalgebriques, c'est-à-dire qu'il existe une correspondance génériquement finie entre (X, v) et $(Y, w)^j$. On conclut à l'aide du lemme 1.27 et de la proposition 1.28. $\square$

1.3.4. *Désintégration et orthogonalité aux constantes.* — Le théorème de trichotomie dans les corps différentiellement clos accorde une place toute particulière au corps des constantes d'un corps differentiellement clos : il s'agit d'un représentant « canonique » de l'unique classe de non-orthogonalité non-localement modulaire dans un corps differentiellement clos.

THÉORÈME 1.33 (Théorème de trichotomie pour $\mathbf{DCF}_0$, [14]). — *Pour la théorie $\mathbf{DCF}_0$, on a la description suivante des classes d'équivalence de non-orthogonalité pour les types minimaux :*

(i) *Il existe une unique classe d'équivalence non-localement modulaire représentée par le type générique du corps des constantes.*
(ii) *Les classes de non-orthogonalité, localement modulaires non-désintégrées sont en correspondance biunivoque avec les variétés abéliennes simples définies sur $\mathcal{U}$ modulo isogénie, qui ne descendent pas aux constantes.*
(iii) *Il existe une infinité non bornée de classes de non-orthogonalité désintégrées.*

COROLLAIRE 1.34. — *Soient $(k, 0)$ un corps différentiel constant et $p \in S(k)$ un type non-algébrique et de rang fini.*

On suppose que le type p est orthogonal aux constantes. Alors il existe un type semi-minimal désintégré $q \in S(k)$ et des réalisations $a \models p$ and $b \models q$ tels que :

$$b \in \mathrm{dcl}(k, a) \setminus \mathrm{acl}(k).$$

Démonstration. — En effet, puisque le type p est non-algébrique, il existe une extension des paramètres $(k, 0) \subset (L, \delta)$ et un type minimal $r \in S(L)$ non-orthogonal à p.

Considérons $a \models p$, une réalisation de p. D'après le lemme de décomposition (voir, par exemple, [25, Chapter 7, Lemma 4.5], il existe $b \in \mathrm{dcl}(k, a) \setminus \mathrm{acl}(k)$ tel que $\mathrm{tp}(b/k)$ est (non-algébrique) et interne a l'ensemble des $\mathrm{acl}(k)$-conjugues de r.

On en déduit que le type $q = \mathrm{tp}(b/k)$ est r-semi-minimal. Il suffit alors de montrer que le type r est un type minimal désintégré :

On sait que le type p est orthogonal aux constantes. Comme r est un type minimal non-orthogonal à p, on en déduit que r est orthogonal aux constantes. D'après le théorème de Hrushovski-Sokolovic (voir [26] pour une version publiée), le type r est *localement modulaire*.

Supposons par l'absurde que r est localement modulaire et non désintégré. La classification fine des types minimaux localement modulaires non désintégrés obtenue par Hrushovski et Sokolovic implique que r est orthogonal à tout type défini sur un corps différentiel constant (voir [14, Theorem 2.8] et [6, Proposition 5.8]).

Or, on sait que le type p est défini sur un corps différentiel constant et que r est un type minimal non-orthogonal à p, ce qui est une contradiction. On en déduit que r est un *type minimal désintégré*. □

Comme expliqué dans l'introduction, le corollaire 1.34 permet d'obtenir l'existence de facteurs rationnels désintégrés pour les équations différentielles autonomes (définies sur un corps différentiel constant) :

Corollaire 1.35. — *Soient k un corps de caractéristique 0 et (X, v) une variété absolument irréductible au dessus de k munie d'un champ de vecteurs v.*

Si le type générique de (X, v) est orthogonal aux constantes alors il existe une variété absolument irréductible Y au dessus de k de dimension > 0, un champ de vecteurs $w \in \mathrm{H}^0(Y, \Theta_{Y/k})$ et un morphisme rationnel dominant

$$\pi : (X, v) \dashrightarrow (Y, w)$$

tels que (Y, w) est génériquement désintégrée.

Quand les conclusions du corollaire 1.35 sont vérifiées, on dit que (X, v) admet *un facteur rationnel désintégré*.

Démonstration. — On note p le type générique de (X, v) et on travaille dans un corps differentiellement clos $(\mathcal{U}, \delta)$.

D'après le corollaire 1.34, il existe un type $q \in S(k)$ semi-minimal et désintégré et des réalisations $a \models p$ and $b \models q$ tels que :

$$b \in \mathrm{dcl}(k, a) \setminus \mathrm{acl}(k).$$

Maintenant, il existe une D-variété (Y, w) au dessus de $(k, 0)$ tel que q est (interdéfinissable avec) le type générique de (Y, w). Le corollaire 1.32 assure que la D-variété (Y, w) est génériquement désintégrée.

En utilisant que $b \in \mathrm{dcl}(a, k)$, on obtient, à l'aide du lemme A.27, un morphisme rationnel dominant $\pi : (X, v) \dashrightarrow (Y, w)$. Enfin, puisque $a \notin \mathrm{acl}(k)$, la variété Y est de dimension > 0. □

2. Intégrale première rationnelle et orthogonalité aux constantes

Dans cette partie, on étudie la relation entre la propriété d'orthogonalité aux constantes pour le type générique d'une équation différentielle autonome et les propriétés classiques de « non-intégrabilité algébrique » qui concernent l'absence de quantités algébriques conservées le long du mouvement (*intégrales premières rationnelles*).

Étant donnée une équation différentielle algébrique (absolument irréductible) (X, v), une des caractéristiques nouvelles des méthodes issues de la théorie des modèles est de considérer l'équation différentielle (X, v) et toutes ses puissances $(X, v)^n$ sur le même plan. Le critère d'orthogonalité aux constantes (théorème 2.4) que nous démontrons dans la première section est une illustration parfaite de ce phénomène : *Le type générique de* (X, v) *est orthogonal aux constantes si et seulement si pour tout* $n > 0$*, toute intégrale première rationnelle de* $(X, v)^n$ *est constante.*

La suite de cette partie est alors consacrée à l'étude des conséquences de ce premier résultat pour les familles lisses d'équations différentielles autonomes absolument irréductibles. Plutôt qu'une équation différentielle autonome, on considère alors une famille lisse $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ d'équations différentielles algébriques à paramètres constants au dessus d'un corps différentiel constant $(k, 0)$ — ou, en d'autres termes, une famille lisse de variétés algébriques $f : \mathcal{X} \longrightarrow S$ munie d'un champ de vecteurs $v \in \mathrm{H}^0(\mathcal{X}, \Theta_{X/S})$, tangent au fibres de f.

Si s est un point de S, le champ de vecteurs v sur $\mathcal{X}$ induit alors un champ de vecteurs sur la fibre $\mathcal{X}_s$. Autrement dit, la fibre $(\mathcal{X}, v)_s$ est une D-variété au dessus du corps différentiel (constant) $(k(s), 0)$ que l'on supposera absolument irréductible. On étudie l'ensemble :

$$S^{\not\perp 0} = \{s \in S(\bar{l}) \mid \text{le type générique de } (X, v)_s \text{ est non-orthogonal aux constantes}\}$$

où $\bar{l}$ est une extension algébriquement close de k. A ce sujet, il est bien connu que $S^{\not\perp 0}$ est, en général, plus complexe qu'un simple sous-ensemble définissable

de $S(\overline{l})$. En revanche, des considérations très générales permettent de décrire $S^{\not 0}$ comme l'image inverse d'un sous ensemble de S par l'application :

$$\pi : S(\overline{k}) \longrightarrow S$$

qui envoie un point de $S(\overline{k})$ sur son image dans le schéma S.

Dans la section 2.3, nous démontrons que, sous des hypothèses nécessaires de lissité, l'ensemble $S^{\not 0}$ est stable par spécialisation : si $s_*, s \in S(\overline{l})$ sont deux points et $\mathrm{tp}(s_*/k)$ se spécialise (au sens usuel de la théorie $\mathbf{ACF}_0$) en $\mathrm{tp}(s/k)$ alors :

$$s_* \in S^{\not 0} \Longrightarrow s \in S^{\not 0}.$$

En outre, nos résultats s'appuient sur des énoncés classiques de spécialisation pour les intégrales premières rationnelles que nous rappelons (faute de référence appropriée) dans la deuxième sous-section de cette partie.

2.1. Un premier critère d'orthogonalité aux constantes. — On donne une caractérisation des D-variétés absolument irréductibles dont le type générique est orthogonal aux constantes.

Définition 2.1. — Soient (K, δ) un corps différentiel et (X, δ_X) une D-variété irréductible sur (K, δ). On appelle *intégrale première rationnelle de* (X, δ_X), toute fonction rationnelle $f \in K(X)$ telle que $\delta_X(f) = 0$.

Remarque 2.2. — Soient (K, δ) un corps différentiel et (X, δ_X) une D-variété irréductible sur (K, δ). L'ensemble des intégrales premières rationnelles de X s'identifie au corps des constantes du corps différentiel $(K(X), \delta_X)$.

Nous dirons que (X, δ_X) est *sans intégrale première non constante* si $K(X)^\delta = K^\delta$.

Lemme 2.3. — *Soient (K, δ) un corps différentiel et (X, δ_X) une D-variété irréductible au-dessus de (K, δ). On a équivalence entre :*

(i) *La D-variété irréductible (X, δ_X) est sans intégrale première rationnelle.*
(ii) *Pour toute variété Y de dimension > 0 au dessus du corps des constantes $k = K^\delta$ de (K, δ), il n'existe pas de morphisme rationnel dominant de D-schémas au dessus de (K, δ)*

$$f : (X, \delta_X) \dashrightarrow (Y, 0) \times_{(k,0)} (K, \delta).$$

Démonstration. — On raisonne par contraposition. Soit $f \in (K(X), \delta_X)$ une intégrale première rationnelle non constante. La fonction f détermine un morphisme rationnel dominant de D-schémas au dessus de (K, δ)

$$f : (X, \delta_X) \longrightarrow (\mathbb{A}^1, 0) \times_{(k,0)} (K, \delta)$$

On en déduit que (ii) $\Longrightarrow$ (i).

Réciproquement, supposons qu'il existe un morphisme $(X,\delta_X) \dashrightarrow (Y,0)\times_{(k,0)} (K,\delta)$ rationnel dominant. Considérons $f \in k(Y)$ une fonction rationnelle non constante. Le morphisme rationnel dominant obtenu par composition

$$(X,\delta_X) \dashrightarrow (Y,0) \times_{(k,0)} (K,\delta) \dashrightarrow (\mathbb{A}^1,0) \times_{(k,0)} (K,\delta)$$

est un morphisme de D-schémas. On en déduit qu'il correspond à une intégrale première rationnelle non constante de (X,δ_X). □

THÉORÈME 2.4. — *Soient (K,δ) un corps différentiel et (X,δ_X) une D-variété absolument irréductible au dessus de (K,δ). On a équivalence entre :*

(i) *Le type générique de (X,δ_X) est orthogonal aux constantes.*
(ii) *Pour toute extension de corps différentiels $(K,\delta) \subset (L,\delta_L)$, le changement de base $(X,\delta_X)_{(L,\delta_L)}$ est sans intégrale rationnelle non constante.*
(iii) *Pour tout $n \in \mathbb{N}$, la D-variété produit $(X,\delta_X)^n$ est sans intégrale première rationnelle non constante.*

Démonstration. — (i) $\Longrightarrow$ (ii) : Supposons qu'il existe une extension de corps différentiels $(K,\delta) \subset (L,\delta_L)$ telle que le changement de base $(X,\delta_X)_{(L,\delta_L)}$ admette une intégrale première non constante $f \in (L(X),\delta_X)$. On obtient un morphisme rationnel dominant de D-schémas au dessus de (L,δ_L) :

$$f : (X,\delta_X)_{(L,\delta_L)} \dashrightarrow (\mathbb{A}^1,0) \times_{(L^\delta,0)} (L,\delta_L)$$

Les types génériques de $(X,\delta_X)_{(L,\delta_L)}$ et de $(\mathbb{A}^1,0) \times_{(L^\delta,0)} (L,\delta)$ ne sont pas faiblement orthogonaux d'après le lemme A.27.

De plus, d'après la propriété (ii) du lemme A.25, le type générique de $(X,\delta_X)_{(L,\delta_L)}$ est l'unique extension non-déviante à L du type générique de (X,δ_X) et le type générique de $(\mathbb{A}^1,0) \times_{(L^\delta,0)} (L,\delta)$ est l'unique extension non déviante à L du type générique des constantes. On en déduit que $p_{(X,\delta_X)}$ est non-orthogonal au type générique des constantes.

(ii) $\Longrightarrow$ (iii) Considérons f une intégrale première rationnelle de $(X,\delta_X)^n$ avec $n \geq 1$ minimal :

$$f : (X,\delta_X)^n \dashrightarrow (\mathbb{A}^1,0) \times_{(k,0)} (K,\delta)$$

On note (L,δ_L) le corps des fractions de la D-variété irréductible $(X,\delta_X)^{n-1}$. Par minimalité de $n \in \mathbb{N}$, la D-variété $(X,\delta_X)^{n-1}$ n'admet pas d'intégrales premières rationnelles non constantes et donc $L^{\delta_L} = k$. Par changement de base, f induit une intégrale première

$$\tilde{f} : (X,\delta_X)_{(L,\delta_L)} \dashrightarrow (\mathbb{A}^1,0) \times_{(k,0)} (L,\delta_L)$$

qui est non constante car $f \notin k$ et $L^{\delta_L} = k$.

(iii) $\Longrightarrow$ (i) : On note q le type générique des constantes.

LEMME 2.5. — *Soit (K,δ) un corps différentiel et $p \in S(K)$ un type non-orthogonal aux constantes. Il existe un entier $n \in \mathbb{N}$, une réalisation a de $p^{\otimes n}$ et une réalisation b de $q|K$ telle que $b \in \mathrm{dcl}(a,K)$.*

Démonstration. — D'après le lemme 1.6, il existe des entiers $n, m \in \mathbb{N}$ tels que les types $p^{\otimes m}$ et $q^{\otimes n}$ ne sont pas faiblement orthogonaux. Considérons des réalisations $a \models p^{\otimes m}$ et $b \models q^{\otimes n}$ telles que $a \not\perp_K b$. Il existe donc une formule $\phi(x,y)$ à paramètres dans K telle que

$$b \in \phi(\mathcal{U},a) \subset \mathcal{C}^n \text{ et } \mathrm{RM}(\phi(\mathcal{U},a)) < n.$$

Le sous-ensemble $\phi(\mathcal{U},a) \subset \mathcal{C}^n$ est un sous-ensemble définissable à paramètres dans $(\mathcal{U},\delta_U)$. D'après le corollaire 1.20, le corps des constantes est un pur corps algébriquement clos stablement plongé (et donc en particulier élimine les imaginaires dans le langage des anneaux). Il existe donc un paramètre canonique $c \in \mathcal{C}^l$ pour la formule $\phi(\mathcal{U},a)$, c'est-à-dire que pour tout automorphisme de corps $\sigma \in \mathrm{Aut}(\mathcal{U},\delta_{\mathcal{U}})$, on a

$$\sigma(c) = c \text{ si et seulement si } \sigma(\phi(\mathcal{U},a)) = \phi(\mathcal{U},a).$$

En particulier, on a $c \in \mathrm{dcl}(K,a)$. Montrons que $\mathrm{RU}(c/K) > 0$. En effet, le rang de Lascar et le rang de Morley coïncident dans un corps algébriquement clos. On a alors :

$$n = \mathrm{RU}(b/K) > \mathrm{RM}(\phi(x,a)) \geq \mathrm{RM}(b/K,c) = \mathrm{RU}(b/K,c).$$

On en déduit que $c \not\perp_K b$ et donc que le rang de Lascar de c sur K est ≥ 1. Il suffit alors de remplacer c par une coordonnée non algébrique de c. □

Supposons que $p = p_{(X,\delta_X)}$ est non-orthogonal aux constantes. D'après le lemme précédent, il existe un entier $n \in \mathbb{N}$, une réalisation a de $p^{\otimes n}$ et une réalisation b de $q|K$ telle que $b \in \mathrm{dcl}(a,K)$.

Comme $p^{\otimes n}$ est le type générique de $(X,\delta_X)^n$, il suffit d'appliquer le lemme A.27 pour obtenir une intégrale première non constante de $(X,\delta_X)^n$, ce qui montre par contraposition que (iii) $\Longrightarrow$ (i). □

REMARQUE 2.6. — Modulo la proposition A.27, l'équivalence entre (i) et (iii) se réduit à l'énoncé suivant (valable dans toute théorie stable) : Soient T une théorie stable éliminant les imaginaires et $\mathfrak{M}$ un modèle de T κ-saturé.

Considérons A un ensemble de paramètres petit, D un ensemble fortement minimal A-définissable éliminant les imaginaires et $p \in S(A)$ un type stationnaire. Alors le type p est non-orthogonal au type générique de D si et seulement s'il existe $\overline{a} \in M^n$ réalisant $p^{(n)}$ tel que $\mathrm{dcl}(K) \cap D \subsetneq \mathrm{dcl}(K\overline{a}) \cap D$.

2.2. Spécialisation pour les intégrales premières rationnelles. — Dans cette sous-section, on fixe k un corps de caractéristique 0.

Définition 2.7. — Soit S un schéma au dessus de k. On appelle *famille de D-schémas paramétrée par S*, tout morphisme de D-schémas $f : (\mathcal{X}, v) \longrightarrow (S, 0)$.

On dira que f est *une famille lisse de D-variétés paramétrée par S* lorsque S et $\mathcal{X}$ sont des schémas intègres lisses, de type fini au dessus de k et le morphisme f est lisse.

Remarque 2.8. — De façon équivalente, une famille lisse de D-variétés au dessus de k est la donnée d'une famille lisse $f : \mathcal{X} \longrightarrow S$ de variétés au dessus de k et d'un champ de vecteurs $v \in \mathrm{H}^0(\mathcal{X}, \Theta_{X/S})$ sur $\mathcal{X}$, tangent aux fibres de f.

Notation 2.9. — Soit $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variétés paramétrée par S et $s \in S$. On note $(\mathcal{X}, v)_s$, *la fibre de* $(\mathcal{X}, v)$ *en* s.

Le champ de vecteurs v étant une section du fibré tangent relatif de f, il se restreint un champ de vecteurs sur chacune des fibres de f. La fibre $(\mathcal{X}, v)_s$ est une variété lisse X_s au dessus de k munie d'un champ de vecteurs v_s.

Les fibres de f seront toujours munies de cette structure de D-variétés. Le corps des intégrales premières rationnelles de $(\mathcal{X}, v)_s$ sera alors noté $k(\mathcal{X}_s)^\delta$ (et donc sans référence explicite au champ de vecteurs sur $\mathcal{X}_s$).

Théorème 2.10. — *Soit $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variétés paramétrées par une variété lisse et irréductible S au dessus de k.*

Supposons, de plus, que toutes les fibres de f soient absolument irréductibles. Pour tout point $s \in S(k)$, on a :

$$\mathrm{degtr}(k(\mathcal{X})^\delta / k(S)) \geq 1 \Longrightarrow \mathrm{degtr}(k(\mathcal{X}_s)^\delta / k) \geq 1.$$

Remarque 2.11. — Il est vraisemblable qu'une inégalité plus forte que l'implication du théorème 2.10 soit en fait valide et que sous les hypothèses du théorème 2.10, on ait en réalité :

$$(*) \qquad \mathrm{degtr}(k(\mathcal{X}_s)^\delta / k) \geq \mathrm{degtr}(k(\mathcal{X})^\delta / k(S))$$

Il semble en effet que les résultats de [19] — dans le cas hamiltonien — s'appuyant sur le lemme de Ziglin puisse être adaptés ici en une preuve de l'inégalité $(*)$.

La suite de cette sous-section est consacrée à une preuve du théorème 2.10.

2.2.1. *Terme initial.* — Dans le cas où $S = \mathbb{A}^1$, la notion essentielle est celle de terme initial qui permet de restreindre une fonction rationnelle f à un diviseur irréductible (possiblement inclus dans le lieu d'indétermination de f).

Construction 2.12. — Soit $f : \mathcal{X} \longrightarrow \mathbb{A}^1$ une famille lisse de variétés paramétrée par $\mathbb{A}^1$ telle que $\mathcal{X}_0$ soit absolument irréductible.

Par hypothèse, la fibre $\mathcal{X}_0 = f^{-1}(0)$ est un diviseur irréductible de $\mathcal{X}$ et correspond à un anneau de valuation discrète $\mathcal{O}_0$ sur le corps $k(\mathcal{X})$. On note ord_0 la valuation discrète associée. Par hypothèse, la fonction f est lisse et donc :

$$\mathrm{ord}_0(f) = 1.$$

Considérons maintenant une fonction rationnelle $g \in k(\mathcal{X})$ sur $\mathcal{X}$ et notons $n_g = \mathrm{ord}_0(g)$. La fonction rationnelle

$$g_0 = g.f^{-n_g} \in k(\mathcal{X}) \text{ vérifie donc } \mathrm{ord}_0(g_0) = 0.$$

On en déduit que la fonction g_0 vérifie $g_0 \in \mathcal{O}_Z \setminus m_Z$ et se restreint donc en une fonction rationnelle non identiquement nulle sur $\mathcal{X}_0$.

DÉFINITION 2.13. — Soient $f : \mathcal{X} \longrightarrow \mathbb{A}^1$ une famille lisse de variétés paramétrée par $\mathbb{A}^1$. Pour toute fonction rationnelle $g \in k(\mathcal{X})$ non identiquement nulle sur $\mathcal{X}$, on appelle *terme initial de g le long de $\mathcal{X}_0$*, la fonction $g_0 \in k(\mathcal{X})$ associée à g par la construction 2.12.

REMARQUE 2.14. — Les deux remarques suivantes découlent de la construction 2.12 :

- Le terme initial g_0 de g se restreint en une fonction non-identiquement nulle sur $\mathcal{X}_0$.
- Si $f : (\mathcal{X}, v) \longrightarrow (\mathbb{A}^1, 0)$ une famille lisse de D-variétés à paramètres dans $\mathbb{A}^1$ et g est une intégrale première de $(\mathcal{X}, v)$ alors son terme initial $g_0 \in k(\mathcal{X})$ est aussi une intégrale première de $(\mathcal{X}, v)$.

2.2.2. *Familles de D-variétés paramétrée par $\mathbb{A}^1_k$.* — Pour les fonctions rationnelles, l'indépendance algébrique et fonctionnelle coïncident :

REMARQUE 2.15 (voir, par exemple, [4, Appendice III.6]). — Soit X une variété algébrique au dessus de k $f_1, \ldots, f_p \in k(X)$ des fonctions rationnelles. Les propriétés suivantes sont équivalentes :

(i) Les fonctions $f_1, \ldots, f_p$ sont k-algébriquement indépendantes (indépendance algébrique).
(ii) La p-forme $df_1 \wedge \cdots df_p \neq 0$ est non nulle dans $\mathrm{H}^0(X, \Lambda^p \Omega^1_{X/k} \otimes k(X))$ (indépendance fonctionnelle).

LEMME 2.16. — *Soient k un corps de caractéristique 0 et $f : (\mathcal{X}, v) \longrightarrow (\mathbb{A}^1_k, 0)$ une famille lisse de D-variétés à paramètres dans $\mathbb{A}^1_k$.*

On suppose que les variétés algébriques $\mathcal{X}$ et $\mathcal{X}_0$ (la fibre en 0) sont absolument irréductibles. Alors :

$$\mathrm{degtr}(k(\mathcal{X})^\delta / k(\mathbb{A}^1)) \geq 1 \Longrightarrow \mathrm{degtr}(k(\mathcal{X}_0)^\delta / k) \geq 1.$$

Démonstration. — Considérons $g \in k(\mathcal{X})^\delta$ une intégrale première rationnelle algébriquement indépendante de f. Notons que :

- Quitte à remplacer g par son terme initial le long de $\mathcal{X}_0$ (en passant éventuellement à un nouvel ouvert affine), on peut supposer que g est bien définie sur $\mathcal{X}$ et non-identiquement nulle sur $\mathcal{X}_0$.
- Quitte à réduire $\mathcal{X}$ par un ouvert affine rencontrant $\mathcal{X}_0$, on peut de plus supposer que $\mathcal{X} = \mathrm{Spec}(A)$ est affine et que les fonctions rationnelles f et g sont régulières sur $\mathcal{X}$.

Par hypothèse, f est lisse et donc l'idéal I définissant le sous-schéma fermé $\mathcal{X}_0$ s'écrit $I = (f)$.

On raisonne par l'absurde et on suppose que $\mathrm{degtr}(k(\mathcal{X}_0)^\delta/k) = 0$. Puisque $\mathcal{X}_0$ est absolument irréductible, cela implique que $k(\mathcal{X}_0)^\delta = k$ et donc que toute intégrale première rationnelle de $(\mathcal{X}_0, v)$ est constante.

Assertion. — *Pour tout $n \geq 1$, il existe $c_0, \ldots, c_{n-1} \in k$ tels que :*

$$g - \sum_{i=0}^{n-1} c_k.f^k \in I^n.$$

Preuve de l'assertion. — On raisonne par récurrence sur $n \in \mathbb{N}$:

- Pour $n = 1$, on sait que $g_{|\mathcal{X}_0}$ est une intégrale première de $(\mathcal{X}_0, v)$ et que $k(\mathcal{X}_0)^\delta = k$. Il existe donc une constante $c_0 \in k$ telle que $g - c_0 \in I$.
- Supposons qu'il existe $c_0, \ldots, c_{n-1} \in k$ tel que $g = \sum_{k=0}^{n-1} c_k.f^k + h.f^n$ avec $h \in A$.

  Puisque $h \in k(g, f)$, c'est une intégrale première de $\mathcal{X}$ et en appliquant le cas $n = 1$, il existe $c_n \in k$ tel que $h = c_n + f.h_2$ avec $h_2 \in A$. On en déduit que $g - \sum_{k=0}^{n} c_k.f^k = f^{n+1}.h_2 \in I^{n+1}$. □

Considérons maintenant l'élément $df \wedge dg$ du A-module $\Lambda^2\Omega^1_{A/k}$. Pour tout $n \geq 1$, on a

$$df \wedge dg = df \wedge d(g - \sum_{k=0}^{n-1} c_k.f^k) \in \Omega^1_{A/k} \wedge d(I^n) \subset I^{n-1}.\Lambda^2\Omega^1_{A/k}.$$

Cela implique donc que :

$$df \wedge dg \in \bigcap_{n\in\mathbb{N}} I^n.\Omega^1_{A/k} = \{0\}.$$

En utilisant la remarque 2.15, cela implique que f et g ne sont pas algébriquement indépendantes, ce qui contredit le choix de g. □

2.2.3. *Preuve du théorème 2.10.* — On commence par étendre le lemme 2.16 au cas des familles paramétrées par $\mathbb{A}^n_k$ en raisonnant par induction. Pour cela on considère le drapeau :

$$\{0\} \subset \{0\} \times \mathbb{A}^1_k \subset \cdots \subset \{0\} \times \mathbb{A}^{n-1}_k \subset \mathbb{A}^n_k.$$

LEMME 2.17. — *Soient k un corps de caractéristique 0 et $f : (\mathcal{X}, v) \longrightarrow (\mathbb{A}^n_k, 0)$ une famille lisse de D-variétés paramétrée par $\mathbb{A}^n$ avec $n > 0$.*

Pour $r \leq n$, on note η_r le point générique de $\{0\} \times \mathbb{A}^r_k$ et on suppose que les fibres de f en $0 = \eta_0, \ldots, \eta_n$ sont absolument irréductibles (et donc, en particulier, non vides). Alors :

$$\mathrm{degtr}(k(\mathcal{X})^\delta / k(\mathbb{A}^n) \geq 1 \Longrightarrow \mathrm{degtr}(k(\mathcal{X}_0)^\delta / k) \geq 1.$$

Démonstration. — On raisonne par récurrence sur $n \in \mathbb{N}^*$

- Pour $n = 1$, c'est le contenu du lemme 2.16.
- Supposons maintenant le résultat établi pour un $n > 0$ et considérons $f : (\mathcal{X}, v) \longrightarrow (\mathbb{A}^{n+1}, 0)$ une famille lisse de D-variétés à paramètres dans $\mathbb{A}^{n+1}$ dont toutes les fibres sont absolument irréductibles.

Considérons l'hyperplan $H = \{0\} \times \mathbb{A}^n$ et la restriction de la famille

$$f_H : f^{-1}(H) \longrightarrow H$$

à cet hyperplan. La famille f_H paramétrée par H vérifie les hypothèses du lemme 2.17. En appliquant l'hypothèse de récurrence à cette famille, il suffit de vérifier que :

$$\mathrm{degtr}(k(\mathcal{X})^\delta / k(\mathbb{A}^{n+1}) \geq 1 \Longrightarrow \mathrm{degtr}(k(f^{-1}(H))^\delta / k(\mathbb{A}^n)) \geq 1. \tag{2}$$

Preuve de l'implication (2) : Notons $\pi : \mathbb{A}^{n+1} \longrightarrow \mathbb{A}^n$ la projection sur les n dernières coordonnées et considérons

$$(\mathcal{X}, v) \xrightarrow{f} (\mathbb{A}^{n+1}, 0) \xrightarrow{\pi} (\mathbb{A}^n, 0).$$

Posons $K = k(x_1, \ldots, x_n)$. Après changement de base par le point générique de $\mathbb{A}^n$, on obtient une famille de D-variétés à paramètres dans $\mathbb{A}^1$ au dessus de K

$$f_K : (X, v)_{(K,0)} \longrightarrow (\mathbb{A}^1_K, 0).$$

L'implication (2) est alors conséquence de la proposition 2.16 appliquée à cette famille de D-variétés à paramètres dans $\mathbb{A}^1$ au dessus de K. □

Preuve du théorème 2.10. — On se ramène au cas des familles de D-variétés paramétrée par $\mathbb{A}^n_k$ à l'aide de coordonnées étales.

Soient S une variété algébrique lisse et irréductible au dessus d'un corps k et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variétés à paramètres dans S dont toutes les fibres sont absolument irréductibles.

Notons $n = \dim(S)$ et fixons $s \in S(k)$. Puisque S est supposée lisse, il existe un voisinage U de s dans S et un morphisme étale $g : U \longrightarrow \mathbb{A}^n$ tel $g(s) = 0$. On considère la composition

$$\tilde{f} : (f^{-1}(V), v) \xrightarrow{f} (V, 0) \xrightarrow{g} (\mathbb{A}^n, 0).$$

qui est une famille lisse de D-variétés paramétrée par $\mathbb{A}^n$.

On modifie maintenant la famille $\tilde{f}$ de sorte que les fibres au dessus de $0 = \eta_0, \ldots, \eta_n$ soient absolument irreductible.

Considérons l'hyperplan $H = \{0\} \times \mathbb{A}^{n-1}$. On peut alors écrire une décomposition en composantes irréductibles :

$$g^{-1}(H) = Z_1 \cup \ldots \cup Z_n.$$

Comme le morphisme g est étale, toutes les composantes irréductibles de $g^{-1}(H)$ ont même dimension et pour tout point $p \in H$ tel que $g^{-1}(p) \in H$, il existe une unique composante irréductible de H contenant p. En particulier :

- Il existe une unique composante irréductible qui contient s. Sans perte de généralité, on peut supposer que $s \in Z_1$.
- Pour tout $r \leq n$, le point η_r admet un unique antécédent noté γ_r dans Z_1.

On pose alors $V = U \setminus \{Z_2 \ldots Z_n\}$ et on considère la composition :

$$\tilde{f}_V : (f^{-1}(V), v) \xrightarrow{f} (V, 0) \xrightarrow{g} (\mathbb{A}^n, 0).$$

Avec les notations précédentes, le morphisme $\tilde{f}_V$ satisfait :

(i) Le morphisme $\tilde{f}_V$ définit une famille lisse de D-variétés paramétrée par $\mathbb{A}^n_k$.

(ii) La fibre $(\tilde{f}^{-1}_{|V}(\eta_r), v_{|\tilde{f}^{-1}_{|V}(\eta_r)})$ est isomorphe (en tant que D-variété) à $(\mathcal{X}, v)_{\gamma_r}$. En particulier, cette fibre est absolument irréductible.

Il suffit alors d'appliquer le lemme 2.16 à la famille $\tilde{f}_V$ à paramètres dans $\mathbb{A}^n_k$. □

2.3. Spécialisation et non-orthogonalité aux constantes. —

2.3.1. *Orthogonalité aux constantes en famille.* — Fixons T une theorie stable avec l'élimination des imaginaires.

Définition 2.18. — Soit $r(\overline{y})$ un type partiel à paramètres dans A. On appelle *famille de types stationnaires à paramètres dans* $r(\overline{y})$, tout type partiel $\pi(\overline{x}, \overline{y})$ à paramètres dans A vérifiant : pour tout $\overline{a} \models r(\overline{y})$, le type $\pi(\overline{x}, \overline{a}) \in S(A\overline{a})$ est un type (complet) stationnaire.

Remarque 2.19. — Soit $f : (X, v) \longrightarrow (S, 0)$ une famille de D-variétés absolument irréductibles au dessus d'un corps différentiel constant $(k, 0)$. Le type partiel (à paramètres dans k) :

$$\pi(x, y) := \{y \in S\} \cup \{x \text{ réalise le type générique de } (X, v)_y \text{ au dessus de } k(y)\}$$

est une famille de types stationnaires à paramètres dans $\{y \in S\}$.

COROLLAIRE 2.20. — *Soient $r(\overline{y}) \in S(A)$ un type partiel et $\pi_1(\overline{x},\overline{y}), \pi_2(\overline{x},\overline{y}) \in S(A)$ deux familles de types stationnaires à paramètres dans $r(\overline{y})$. Pour toute réalisation $\overline{a} \models r(y)$, la propriété :*

$$\mathcal{P}(\overline{a}) : \pi_1(\overline{x},\overline{a}) \text{ et } \pi_2(\overline{x},\overline{a}) \text{ sont orthogonaux}$$

ne dépend que du type $\mathrm{tp}(\overline{a}/A)$ *de $\overline{a}$ sur A.*

Démonstration. — En utilisant la proposition 1.6, il suffit de démontrer que la propriété :

$$\mathcal{P}'(a) : \pi_1(\overline{x},\overline{a}) \text{ et } \pi_2(\overline{x},\overline{a}) \text{ sont faiblement orthogonaux}$$

ne dépend que du type $\mathrm{tp}(\overline{a}/A)$.

Soient $\overline{a}$ et $\overline{a}'$ deux réalisations du type $\mathrm{tp}(\overline{a}/A)$.

Supposons que la propriété $\mathcal{P}(\overline{a})$ ne soit pas vérifiée. Il existe une formule $\phi(x,y,\overline{a})$ qui dévie au dessus de A et telle que :

$$\pi(x,y,\overline{a}) = p(x,\overline{a}) \cup q(y,\overline{a}) \cup \phi(x,y,\overline{a}) \text{ est coherent.}$$

Par invariance par automorphisme de la déviation, on en déduit que $\pi(x,y,\overline{a}')$ est cohérent et que $\phi(x,y,\overline{a}')$ dévie au dessus de A. Il suit que $\mathcal{P}(\overline{a}')$ n'est pas vérifiée. □

REMARQUE 2.21. — Soit $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille de D-variétés absolument irréductibles au dessus d'un corps différentiel constant $(k, 0)$. Considérons l'ensemble :

$$S^{\not\perp 0} = \{s \in S(\overline{l}) \mid \text{le type générique de } (\mathcal{X}, v)_s \text{ est non-orthogonal aux constantes}\}$$

où $\overline{l}$ est une extension algébriquement close saturée, fixée de k.

Le corollaire 2.20 implique ici que $S^{\not\perp 0}$ s'écrit comme l'image inverse d'un sous-ensemble du schéma S par l'application

$$\pi : S(\overline{k}) \longrightarrow S$$

qui envoie un point de $S(\overline{k})$ sur son image dans le schéma S.

En revanche, on sait que en général l'ensemble $S^{\not\perp 0}$ n'est pas un sous-ensemble constructible (ni même un sous ensemble ∞-definissable de $S(\overline{l})$). Cela découle de l'étude de Hrushovski et Itai des champs de vecteurs sur $\mathbb{A}^1$ orthgonaux aux constantes (voir [12], Exemple 2.20).

De même, on note $S^{\perp 0}$, le complémentaire de $S^{\not\perp 0}$ dans $S(\overline{l})$ dont les éléments sont les points $s \in S(\overline{l})$ tels que $(\mathcal{X}, v)_s$ est orthogonal aux constantes.

LEMME 2.22. — *Soit S une variété irréductible algébrique complexe et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille d'équations différentielles algébriques paramétrée par S dont les fibres sont toutes absolument irréductibles.*

Si la fibre générique de f est orthogonale aux constantes alors, il existe un ensemble dénombrable de sous-variétés algébriques fermées propres $\{Z_n \mid n \in \mathbb{N}\}$ de S tel que :

$$S(\mathbb{C}) \setminus \bigcup_{i\in\mathbb{N}} Z_i(\mathbb{C}) \subset S^{\perp 0}(\mathbb{C}).$$

Démonstration. — Il existe un corps k finement engendré sur $\mathbb{Q}$ (donc dénombrable) sur lequel la variété S, le morphisme f et le champ de vecteurs v sont définis. Le morphisme f est donc obtenu par changement de base à partir d'un morphisme $f_k : (\mathcal{X}_k, v_k) \longrightarrow S_k$ défini au dessus de k. Par hypothèse, il existe une réalisation s du point générique de S_k telle que $(\mathcal{X}, v)_s$ est orthogonal aux constantes.

Le corollaire 2.20 assure que c'est le cas pour toutes les réalisations dans $S(\mathbb{C})$ du point générique de S_k. Il suffit donc de choisir pour $\{Z_n \mid n \in \mathbb{N}\}$, l'ensemble des sous-variétés fermées propres de S définies sur k. Comme k est dénombrable, cet ensemble est bien dénombrable. □

2.3.2. *Un énoncé de spécialisation.* — A l'aide du premier critère d'orthogonalité aux constantes (théorème 2.4), nous montrons maintenant que $S^{\perp 0}$ est stable par spécialisation pour les familles lisses de D-variétés dont les fibres sont absolument irréductibles.

Théorème 2.23 (Spécialisation et non-orthogonalité aux constantes). — *Soient S une variété algébrique lisse et irréductible au dessus d'un corps k et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variétés à paramètres dans S.*

On suppose que toutes les fibres de f sont absolument irréductibles et on dénote par η le point générique de S. Si le type générique de $(\mathcal{X}, v)_\eta$ est non-orthogonal aux constantes alors le type générique de $(\mathcal{X}, v)_s$ est non-orthogonal aux constantes pour tout $s \in S(k)$.

Démonstration. — Considérons $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variété à paramètres dans S dont les fibres sont absolument irréductibles. Posons :

$$(\mathcal{X}_n, v_n) = (X, v) \times_{(S,0)} \cdots \times_{(S,0)} (X, v) \text{ and } f_n : (\mathcal{X}_n, v_n) \longrightarrow (S, 0).$$

Les hypothèses sur la famille f impliquent que $f_n : \mathcal{X}_n \longrightarrow S$ est une famille lisse de D-variétés à paramètres dans S dont les fibres sont absolument irréductibles. De plus, si $s \in S$, la fibre de f_n au dessus de s est la puissance n-ieme $(\mathcal{X}, v)_s^n$ de la fibre de f en s.

Supposons maintenant que le type générique de $(\mathcal{X}, v)_\eta$ est non-orthogonal aux constantes. D'après le théorème 2.4, il existe un entier $n > 0$ telle que $(\mathcal{X}, v)_\eta^n$ admet une intégrale première rationnelle non constante. On en déduit que :

$$\operatorname{degtr}(k(\mathcal{X}_n)^\delta / k) \geq \dim(S) + 1.$$

Pour tout $s \in S$, la proposition 2.16 implique alors que

$$\mathrm{degtr}(k(\mathcal{X}_{n,s})^{\delta}/k) \geq 1.$$

Cela implique que $(\mathcal{X}, v)_s^n$ admet une intégrale première non-constante et donc que le type générique de $(\mathcal{X}, v)_s$ est non-orthogonal aux constantes. □

COROLLAIRE 2.24. — *Soient S une variété algébrique lisse et irréductible au dessus du corps $\mathbb{C}$ des nombres complexes et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variété à paramètres dans S.*

On suppose que toutes les fibres de f sont absolument irréductibles. Exactement un des deux cas suivants est réalisé :

(i) *$\forall s \in S(\mathbb{C})$, le type générique de $(X, v)_s$ est non-orthogonal aux constantes.*

(ii) *Le sous-ensemble $S^{\not\perp 0}(\mathbb{C}) \subset S(\mathbb{C})$ des paramètres complexes $s \in S(\mathbb{C})$ tels que $(X, v)_s$ est non-orthogonal aux constantes s'écrit :*

$$S^{\not\perp 0}(\mathbb{C}) = \bigcup_{n \in \mathbb{N}} Z_n(\mathbb{C})$$

où $\{Z_n \mid n \in \mathbb{N}\}$ est un ensemble dénombrable de sous-varietés fermées (irréductibles) propres de S.

Démonstration. — On peut toujours supposer que la famille $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ est définie au dessus d'un sous-corps dénombrable k du corps des nombres complexes. Pour toute sous-variété fermée irréductible Z de S, note η_Z, le point générique de Z (au dessus de k).

Considérons l'ensemble dénombrable $\mathcal{E}$ des sous-variétés fermées irréductibles Z de S (au dessus de k) telles que l'équation différentielle $(X, v)_{\eta_Z}$ est non-orthogonal aux constantes.

Supposons que le cas (i) n'est pas réalisé. D'après le théorème 2.23, l'équation différentielle $(X, v)_{\eta_S}$ est orthogonale aux constantes et donc $S \notin \mathcal{E}$. Montrons que :

$$S^{\not\perp 0}(\mathbb{C}) = \bigcup_{Z \in \mathcal{E}} Z(\mathbb{C}).$$

Considérons $Z \in \mathcal{E}$ et $\pi : \widehat{Z} \longrightarrow Z$ une désingularisation de Z (qui existe car k est un corps de caractéristique 0). Notons de plus $\widehat{f_Z} : \mathcal{X}_Z \longrightarrow \widehat{Z}$ la famille d'équations différentielles induite par changement de base de la restriction $f_{|f^{-1}(Z)}$ par π.

Puisque la lissité et l'irréductibilité des fibres d'un morphisme $f : X \longrightarrow S$ sont deux propriétés invariantes par restriction et par changement de base, on en déduit que $\widehat{f_Z} : \mathcal{X}_Z \longrightarrow \widehat{Z}$ vérifie les hypothèses du théorème 2.23.

De plus, comme $\pi^{-1}(\eta_Z) = \eta_{\widehat{Z}}$, la fibre générique de $f_{\widehat{Z}}$ est isomorphe à $(\mathcal{X}, v)_{\eta_Z}$ et donc non-orthogonale aux constantes. D'après le théorème 2.23, pour tout point $s \in \widehat{Z}(\mathbb{C})$, l'équation différentielle $(\mathcal{X}_Z, v)_s$ est orthogonale

aux constantes. On en déduit que pour tout $z \in Z(\mathbb{C})$, l'équation différentielle $(\mathcal{X}, v)_z$ est orthogonale aux constantes et donc que :

$$\bigcup_{Z \in \mathcal{E}} Z(\mathbb{C}) \subset S^{\not\downarrow 0}(\mathbb{C}).$$

Réciproquement, si $s \in S^{\not\downarrow 0}(\mathbb{C})$ alors $Z = \mathrm{loc}_k(s)$ est une sous-variété fermée de S au dessus de k et l'équation différentielle $(\mathcal{X}, v)_{\eta_Z}$ est orthogonale aux constantes (car $(X, v)_s$ est orthogonale aux constantes et s réalise le point générique de Z). On conclut que $Z \in \mathcal{E}$ et donc que $s \in \bigcup_{Z \in \mathcal{E}} Z(\mathbb{C})$. □

2.4. Champ de vecteurs polynomiaux très génériques. — On applique maintenant les résultats précédents a l'étude des champs de vecteurs polynomiaux complexes sur l'espace affine complexe $\mathbb{A}^n_{\mathbb{C}}$ dimension n. Le résultat principal de cette section concerne le cas très générique où les coefficients du champs de vecteurs sont $\mathbb{Q}$-algébriquement indépendants.

Corollaire 2.25. — *Soit $d \geq 3$ et $n \geq 1$. Considérons un champs de vecteurs*

$$v(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n)\frac{d}{dx_1} + \cdots f_n(x_1, \ldots, x_n)\frac{d}{dx_n}.$$

sur l'espace affine complexe de dimension n, où $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]_{\leq d}$ sont des polynômes de degré $\leq d$.

Si les coefficients de $f_1, \ldots, f_n$ sont $\mathbb{Q}$-algébriquement indépendants[5] *alors le champ de vecteurs v est orthogonal aux constantes.*

Formulons aussi la version géométrique suivante qui se déduit immédiatement à l'aide du lemme 2.22.

Corollaire 2.26. — *Soit $d \geq 3$ et $n \geq 1$. Notons $\mathcal{A}_{n,d}$ l'ensemble des champs de vecteurs complexes de degré d sur $\mathbb{A}^n_{\mathbb{C}}$, qui est un $\mathbb{C}$-espace vectoriel de dimension n^{d+1}.*

Il existe un ensemble dénombrable $\{Z_n \mid n \in \mathbb{N}\}$ de sous-variétés fermées propres de $\mathcal{A}_{n,d}$ tel que :

$$\forall v \in \mathcal{A}_{n,d} \setminus \bigcup_{i \in \mathbb{N}} Z_i(\mathbb{C}),\ \textit{le type générique de } (\mathbb{A}^n_{\mathbb{C}}, v) \textit{ est orthogonal aux constantes.}$$

2.4.1. *Cas de la droite affine.* — En dimension 1, des travaux de Rosenlicht (voir [28]) décrivent très precisement les champs de vecteurs polynomiaux orthogonaux aux constantes. Le corollaire 2.25 est donc en dimension 1, une conséquence directe [28]. La formulation que nous donnons ici est celle de [12] (voir Exemple 2.20).

5. Cela implique, en particulier, que les f_i sont des polynômes de degré d dont tous les coefficients sont distincts et non nuls.

THÉORÈME 2.27 (Rosenlicht). — *Soit $v(x) = P(x)\frac{d}{dx}$ un champ de vecteurs polynomial sur la droite affine. Le type générique de $(\mathbb{A}^1, v)$ est orthogonal aux constantes si et seulement si l'un des deux cas suivants est réalisé :*

(i) *soit le polynôme $P(x)$ admet au moins une racine multiple et une racine simple.*

(ii) *soit toutes les racines de $P(x)$ sont simples et il existe deux racines x_1 et x_2 de $P(x)$ telles que les résidus de $\frac{1}{P(x)}$ sont $\mathbb{Q}$-linéairement indépendants.*

EXEMPLE 2.28. — Considérons la famille $\mathcal{A}^*_{1,d}$ des champs de vecteurs polynomiaux unitaires de degré d complexes, de dimension 1. On a donc $\mathcal{A}^*_{1,d} \simeq \mathbb{C}^d$.

A l'aide du théorème de Rosenlicht, on peut décrire ici explicitement les sous-variétés fermées $\{Z_n \mid n \in \mathbb{N}\}$ apparaissant dans le corollaire 2.26 :

- Le premier cas est contenu dans la sous-variété fermée propre $Z \subset \mathcal{A}^*_{1,d}$ décrite par l'équation
$$\mathrm{Res}(P, P') = 0.$$
- Notons $\Delta \subset \mathbb{C}^d$ l'ensemble des diagonales de $\mathbb{C}^d$. Le complémentaire $\mathcal{A}^*_{1,d} \setminus Z$ peut alors être identifié au quotient $(\mathbb{C}^d \setminus \Delta)/\Sigma_d$ via :
$$\pi : \begin{cases} \mathbb{C}^d \setminus \Delta \longrightarrow \mathcal{A}^*_{1,d} \setminus Z \\ (x_1, \ldots, x_d) \longmapsto (x - x_1) \cdots (x - x_d)\frac{d}{dx} \end{cases}$$

Notons que en particulier π est fermée. Pour tout choix $i \neq j \leq n$ et $q \in \mathbb{Q}$, l'équation
$$\mathrm{Res}_{x_i}(1/P(x)) = q.\mathrm{Res}_{x_j}(1/P(x))$$
définit une sous-variété algébrique fermée $Y_{i,j,q}$ (au dessus de $\mathbb{Q}$) de $\mathbb{C}^n \setminus \Delta$. Un calcul immédiat montre que cette sous-variété fermée est une *sous-variété propre* dès que le degré $d \geq 3$.

Supposons donc $d \geq 3$. En posant $Z_{i,j,q} = \pi(Y_{i,j,q})$ (qui est une sous-variété fermée propre de $\mathcal{A}^*_{1,d} \setminus Z$), le théorème de Rosenlicht implique donc que :

$$\forall v \in \mathcal{A}^*_{1,d} \setminus \Big(\bigcup_{i \neq j, q \in \mathbb{Q}} Z_{i,j,q}(\mathbb{C}) \cup Z(\mathbb{C}) \Big), \text{ le type générique de } (\mathbb{A}^1_{\mathbb{C}}, v) \text{ est orthogonal aux constantes.}$$

2.4.2. *Démonstration du corollaire 2.25.* — La démonstration du corollaire 2.25 s'appuie sur le théorème 2.23 plutôt que sur le théorème de Rosenlicht (valable uniquement sur $\mathbb{A}^1$).

ASSERTION. — *Il existe un champ de vecteurs v_d « universel de degré d » sur $\mathcal{X} = \mathbb{A}^n_{\mathbb{C}} \times \mathcal{A}_{n,d}$ défini sur $\mathbb{Q}$ et tangent à la seconde projection $\pi : (\mathcal{X}, v_d) \longrightarrow (\mathcal{A}_{n,d}, 0)$ tel que pour tout champ de vecteurs w de degré d sur $\mathbb{A}^n$, on ait :*
$$(\mathcal{X}, v_d)_w \simeq (\mathbb{A}^n, w).$$

Démonstration. — Il suffit de poser $\mathcal{X} = \mathbb{A}^n_{\mathbb{C}} \times \mathcal{A}_{n,d}$ et de considérer la section v_d du faisceau coherent $\pi_1^*\Theta_{\mathbb{A}^n/k}$ définie par $v_d(x, v) = v(x)$. □

ASSERTION. — *Il existe un champ de vecteurs w de degré 3 sur $\mathbb{A}^n$ tel que le type générique de $(\mathbb{A}^n, w)$ est orthogonal aux constantes.*

Démonstration. — Considérons le champ de vecteurs $v(x) = x^2(x-1)\frac{d}{dx}$ de degré 3 sur $\mathbb{A}^1$.

Le théorème de Rosenlicht implique que le type générique de $(\mathbb{A}^1, v)$ est orthogonal aux constantes. Cela implique que pour tout $n \in \mathbb{N}$, le type générique de $(\mathbb{A}^1, v)^n = (\mathbb{A}^n, v \times v \ldots \times v)$ est orthogonal aux constantes.

Le champ de vecteurs

$$w = (v \times v \ldots \times v)(x_1, \ldots, x_n) = x_1^2(x_1 - 1)\frac{\partial}{\partial x_1} + \cdots + x_n^2(x_n - 1)\frac{\partial}{\partial x_n}$$

est donc un champ de vecteurs de degré 3 sur $\mathbb{A}^n$ vérifiant les conclusions de l'assertion. □

Démonstration du corollaire 2.25 : La famille $\pi : (\mathcal{X}, v_d) \longrightarrow (\mathcal{A}_{n,d}, 0)$ vérifie les hypothèses du théorème 2.23. En effet, le morphisme π est clairement lisse et les fibres de π sont absolument irréductibles (car isomorphes à $\mathbb{A}^n$).

De plus, l'assertion précédente assure que le type générique de la fibre de π au dessus de w

$$(\mathcal{X}, v_d)_w \simeq (\mathbb{A}^n, w)$$

est orthogonal aux constantes.

D'après le théorème 2.23, la fibre générique de π est orthogonal aux constantes. On en déduit qu'un champ de vecteurs dont les coefficients réalisent le type générique de $\mathcal{A}_{n,d}$ — c'est à dire dont les coefficients sont $\mathbb{Q}$-algébriquement indépendants — est orthogonal aux constantes. □

3. Propriétés dynamiques du flot réel analytique d'une D-variété réelle

On s'intéresse désormais aux D-variétés (X, v_X) définies sur le corps $\mathbb{R}$ des nombres réels muni de la dérivation triviale. On dispose d'un foncteur d'analytification réel vers la catégorie des espaces analytiques réels munis de champs de vecteurs. Sous des hypothèses de lissité, on peut alors, par les théorèmes classiques d'existence et d'unicité des solutions d'équations différentielles analytiques, intégrer ce champ de vecteur et obtenir un flot réel analytique. Lorsque ce flot est complet (ce qui est automatique sous des hypothèses de compacité), il définit une action continue du groupe additif $(\mathbb{R}, +)$ sur l'espace topologique métrisable $X(\mathbb{R})^{an}$.

Dans le première section, on étudie le foncteur d'analytification réel (ainsi que son analogue complexe) et son effet sur les sous-variétés fermées invariantes. Dans la deuxième section, on donne une présentation auto-contenue des résultats de dynamique topologique que nous utiliserons, et en particulier la notion de *flot faiblement topologiquement mélangeant*.

3.1. Des D-variétés réelles aux flots réels. — On présente les foncteurs d'analytification réel (resp. complexe) pour les D-variétés réelles (resp. complexe). Sous des hypothèses de lissité, on construit alors le flot réel associé (resp. le flot complexe associé). On supposera que le lecteur est familier avec les résultats élémentaires de la théorie des équations différentielles (voir [3] pour le cas réel et la partie 1 du chapitre 1 de [15] pour le cas complexe).

Contrairement au cas algébrique, on suivra la terminologie analytique usuelle c'est-à-dire que les variétés analytiques seront toujours supposées lisses et on parlera d'espaces analytiques (réels ou complexes) lorsque l'on travaillera sans hypothèse de lissité.

3.1.1. *Flot réel d'une D-variété réelle.* — On présente d'abord le foncteur d'analytification pour les D-variétés réelles.

Définition 3.1. — On appellera *D-espace analytique réel*, tout couple (M, v_M) où M est un espace analytique réel et v_M un champ de vecteurs analytique sur M. Si l'espace analytique réel sous-jacent M est lisse, on dit que (M, v_M) est *une D-variété analytique réelle*.

Si (M, v_M) et (N, v_N) sont deux espaces analytiques réels, on définira les morphismes de (M, v_M) vers (N, v_N) comme les applications analytiques $f : M \longrightarrow N$ vérifiant $df(v_M) = f^* v_N$.

Construction 3.2. — Soit (X, v_X) une D-variété au dessus de $(\mathbb{R}, 0)$. On munit l'ensemble des points réels $M = X(\mathbb{R})$ de X de sa structure analytique $(M, \mathcal{O}_M)$, i.e. de la topologie métrisable d'espace analytique et du faisceau des fonctions analytiques $\mathcal{O}_M$.

Remarque 3.3. — L'espace analytique réel $(M, \mathcal{O}_M)$ est lisse si et seulement si $X(\mathbb{R})$ est contenu dans l'ouvert X_{reg} des points régulier de X.

Le champ de vecteurs v_X induit alors un champ de vecteurs analytique sur M noté v_M. On a ainsi construit un D-espace analytique réel (M, v_M).

La correspondance $(X, v_X) \mapsto (M, v_M)$ détermine un foncteur appelé *foncteur d'analytification réel* de la catégorie des D-variétés au dessus de $(\mathbb{R}, 0)$ vers la catégorie des D-espaces analytiques réels.

Construction 3.4. — Soit (M, v_M) une D-variété réelle analytique. Le théorème d'existence et d'unicité de solutions pour les équations différentielles analytiques (voir [3, §35]) assure l'existence pour tout $x \in M$, d'un unique ouvert connexe $U_x \subset \mathbb{R}$ maximal et d'une application analytique $\phi_x : U_x \longrightarrow M$ telle que

$$\begin{cases} \phi_x(0) = x \\ \forall t \in U_x,\ \frac{d}{dt}\phi_x(t) = v_M(\phi_x(t)). \end{cases}$$

De plus, l'ensemble $U = \bigsqcup_{x\in M} U_x \subset \mathbb{R}\times M$ est un voisinage connexe de $\{0\}\times M$ et la collection des $(\phi_x)_{x\in M}$ définit une application analytique $\phi : U \longrightarrow M$ vérifiant :

$$\begin{cases} \forall x \in M,\ \phi(0,x) = x \\ \forall t \in U_x,\ \frac{d}{dt}\phi(t,x) = v_M(\phi(t,x)). \end{cases}$$

Définition 3.5. — Soit (M, v_M) une D-variété analytique réelle. On appelle *flot réel (maximal) de* (M, v_M), le couple (U, ϕ) maximal associé par la construction 3.4.

On dira de plus que le flot (U, ϕ) est *complet* si $U = \mathbb{R} \times M$.

Lemme 3.6 ([3, §35]). — *Soit (M, v_M) une D-variété analytique réelle compacte. Le flot réel de (M, v_M) est complet.*

Remarque 3.7. — Soit (M, v_M) une D-variété analytique réelle et (U, ϕ) le flot réel associé. On appelle *courbe intégrale ou orbite au point* $x \in X$, le sous-ensemble

$$\mathcal{O}_x = \{\phi(t,x) \mid (t,x) \in U\}.$$

On observera que la partition de M selon les courbes intégrales du champ de vecteurs v_M définit un feuilletage analytique en courbes sur M dont les singularités sont les zéros du champ de vecteur v_M.

Définition 3.8. — Soit (M, v_M) une D-variété analytique réelle et $A \subset M$ un sous-ensemble. On note (U, ϕ) le flot associé à (M, v_M). On dit que $A \subset M$ est *ϕ-invariant* si

$$\phi((\mathbb{R} \times A) \cap U) \subset A.$$

Autrement dit, le sous-ensemble $A \subset M$ est invariant si et seulement si pour tout $a \in A$ et tout $t \in \mathbb{R}$ tel que $(t, a) \in U$, on a $\phi(t, a) \in A$.

On montre maintenant que la propriété d'invariance est de nature locale.

Notation 3.9. — Soient M une variété analytique réelle et $a \in M$. On note (M, a) le germe de l'espace analytique M en a. Si $A \subset M$ est un sous-ensemble de M, on note $[A]_a$ le germe de A en a, c'est-à-dire la classe d'équivalence de A modulo la relation d'équivalence définie par :

> $A \sim_a B$ si et seulement s'il existe un voisinage $V \subset M$ de a tel que $A \cap V = B \cap V$.

La relation d'inclusion entre les sous-ensembles de M induit une relation d'inclusion sur les germes donnée pour $A, B \subset M$ par :

> $[A]_a \subset [B]_a$ si et seulement s'il existe un voisinage V de a dans M tels que $A \cap V \subset B$.

LEMME 3.10. — *Soient (M, v_M) une D-variété analytique réelle et $A \subset M$ un sous-ensemble fermé. On note (U, ϕ) le flot réel associé. On a équivalence entre :*

(i) *Le sous-ensemble $A \subset M$ est ϕ-invariant.*
(ii) *Pour tout $a \in A$, le germe du flot ϕ en $(0, a)$ noté $\phi_a : (\mathbb{R} \times M, (0, a)) \longrightarrow (M, a)$ vérifie*

$$\phi_a([\mathbb{R} \times A]_{(0,a)}) \subset [A]_a.$$

Démonstration. — L'implication (i) $\Longrightarrow$ (ii) est tautologique. Montrons que (ii) $\Longrightarrow$ (i). Considérons $a \in A$ et notons $U_a = \{t \in \mathbb{R} \mid (t, a) \in U\}$ qui est un ouvert connexe de $\mathbb{R}$.

L'ensemble $G = \{t \in U_a \mid \phi(t, a) \in A\} \subset U_a$ est fermé non vide car $A \subset M$ est un sous-ensemble fermé. Pour tout $t \in G$, la propriété (ii) appliquée en $a' = \phi_t(a)$ montre que G est un voisinage de t. On en déduit que G est ouvert.

Par connexité de U_a, on en déduit que $G = U_a$ et donc que A est ϕ-invariant. □

DÉFINITION 3.11. — Soient X une variété algébrique sur $(\mathbb{R}, 0)$ et v_X un champ de vecteurs rationnel sur X. On appelle *flot réel régulier de* (X, v_X), le flot réel associé à l'analytifié de la D-variété lisse $(U, v_{|U})$ où $U = X \setminus (\mathrm{Sing}(X) \cup \mathrm{Sing}(v_X))$[6].

REMARQUE 3.12. — Soit (X, v_X) une D-variété réelle. La connaissance du flot réel régulier de (X, v_X) n'est pas suffisante pour étudier les sous-variétés invariantes de (X, v_X) et de ses produits : Les sous-variétés invariantes $W \subset (X, v_X)$ sans points réels n'auront aucune trace dans $X(\mathbb{R})$. Il suffit par exemple que $X(\mathbb{R}) = \emptyset$ et on ne peut rien dire du tout.

3.1.2. *Flot complexe d'une D-variété complexe.* — En travaillant avec un flot complexe, plutôt qu'avec le flot réel, on résout complètement la difficulté précédente. Néanmoins, contrairement au cas réel, le flot complexe n'admet pas d'ouvert maximal de définition et il faut travailler localement avec des germes de flots.

DÉFINITION 3.13. — On appelle *D-espace analytique complexe*, tout couple (M, v_M) où M est un espace analytique complexe et v_M un champ de vecteurs analytique sur M.

CONSTRUCTION 3.14. — Soit (X, v_X) une D-variété au dessus de $(\mathbb{C}, 0)$.

On munit l'ensemble $M = X(\mathbb{C})$ de sa structure analytique complexe. Le champ de vecteurs v_X induit un champ de vecteurs analytique v_M sur M. On obtient ainsi un D-espace analytique complexe (M, v_M).

6. Ici, $\mathrm{Sing}(v_X)$ désigne le complémentaire du plus grand ouvert de définition de v_X.

Comme dans le cas réel, la construction précédente détermine un foncteur de la catégorie des D-variétés au dessus de $(\mathbb{C},0)$ vers la catégorie des D-espaces analytiques complexes appelé *foncteur d'analytification complexe*. Contrairement au cas réel, ce foncteur est fidèle et réalise donc la catégorie des D-variétés au dessus de $(\mathbb{C},0)$ comme une sous-catégorie de la catégorie des D-espaces analytiques complexes.

Définition 3.15. — Soit (M,v_M) un D-espace analytique complexe. Le champ de vecteurs v_M induit une dérivation $\delta_M : \mathcal{O}_M \longrightarrow \mathcal{O}_M$ sur le faisceau $\mathcal{O}_M$ des fonctions analytiques sur M. Un sous-espace analytique fermé $Z \subset (M,v_M)$ est appelée *δ_M-invariant* si le faisceau d'idéaux $I_Z \subset \mathcal{O}_M$ définissant Z est stable par la dérivation δ_M.

Remarque 3.16. — Dans le cas où le D-espace analytique complexe (M,v_M) est l'analytifié d'une D-variété au dessus de $(\mathbb{C},0)$ et où la sous-variété analytique $Z \subset (M,v_M)$ est l'analytifié d'une sous-variété algébrique, les deux notions d'invariance (analytique et algébrique) coïncident.

Construction 3.17. — Soit (M,v_M) une D-variété analytique complexe. Le théorème d'existence et d'unicité locale de solutions pour les équations différentielles analytiques complexes [15, Théorème 1.1] assure que pour tout point $y \in M$, il existe un voisinage connexe $U_y \subset \mathbb{C}\times M$ de $(0,y)$ et d'une application analytique $\phi : U_y \longrightarrow M$ tels que

$$\begin{cases} \forall (0,x) \in U_y,\ \phi(0,x) = x \\ \forall (t,x) \in U_y,\ \frac{d}{dt}\phi(t,x) = v_M(\phi(t,x)). \end{cases}$$

De plus, le germe de (U_y,ϕ) en $(y,0)$ est unique.

Définition 3.18. — Soient (M,v_M) une D-variété analytique complexe et $y \in M$. On appelle *germe de flot de v_M en $y \in M$*, le germe $\phi_y : (\mathbb{C}\times M,(y,0)) \longrightarrow (M,y)$ associé par la construction 3.17.

Définition 3.19. — Soient (M,v_M) une D-variété analytique complexe et $A \subset M$ un sous-ensemble. On dit que $A \subset M$ est *ϕ-invariant* si pour tout $a \in A$, le germe du flot ϕ en $(0,a)$ noté $\phi_a : (\mathbb{C}\times M,(0,a)) \longrightarrow (M,a)$ vérifie

$$\phi_a([\mathbb{C}\times A]_{(0,a)}) \subset [A]_a.$$

Proposition 3.20. — *Soient (M,v_M) une D-variété analytique complexe et $Z \subset M$ un sous-espace analytique complexe. On a équivalence entre :*

(i) *La sous-variété analytique $Z \subset (M,v_M)$ est un sous-espace analytique δ_M-invariant.*
(ii) *Le sous-ensemble $Z \subset M$ est ϕ-invariant.*

Soit $a \in Z$. On note $\mathcal{O}_{M,a}$ l'anneau local des germes de fonctions analytiques sur M en a. Le champ de vecteurs v_M munit l'anneau $\mathcal{O}_{M,a}$ d'une dérivation notée $\delta_a : \mathcal{O}_{M,a} \longrightarrow \mathcal{O}_{M,a}$. En notant $\mathcal{O}_{M,a}\{t\}$ l'anneau local des germes de fonctions analytiques sur $\mathbb{C} \times M$ en $(0, a)$, le germe du flot ϕ en a induit un morphisme d'anneaux :

$$\phi_a^\sharp : \begin{cases} \mathcal{O}_{M,a} \longrightarrow \mathcal{O}_{M,a}\{t\} \\ f \longmapsto f \circ \phi_a \end{cases}$$

Nous noterons encore $\delta_a : \mathcal{O}_{M,a}\{t\} \longrightarrow \mathcal{O}_{M,a}\{t\}$ la dérivation déduite de δ_a définie par :

$$\delta_a\Big(\sum_{n\in\mathbb{N}} f_n.t^n\Big) = \sum_{n\in\mathbb{N}} \delta_a(f_n).t^n.$$

Remarquons que le morphisme d'anneaux $.|_{t=0} : \mathcal{O}_{M,a}\{t\} \longrightarrow \mathcal{O}_{M,a}$ est alors un morphisme d'anneaux différentiels.

LEMME 3.21. — *Avec les notations précédentes, on a pour tout $f \in \mathcal{O}_{M,a}$,*

$$(*) \qquad \begin{cases} \phi_a^\sharp(f)_{|t=0} = f \\ \frac{d}{dt}\phi_a^\sharp(f) = \delta_a(\phi_a^\sharp(f)) \end{cases}$$

où $\frac{d}{dt}$ désigne la dérivation usuelle sur $\mathcal{O}_{M,a}\{t\}$. De plus, on a :

$$(**) \qquad \phi_a^\sharp(f) = \sum_{n=0}^{\infty} \frac{\delta_a^n(f)}{n!} t^n.$$

Les identités $(*)$ découlent aussitôt de la définition du flot ϕ (construction 3.17). La formule $(**)$ est une conséquence immédiate de $(*)$. Des formules du type $(**)$ apparaissent déjà chez Cauchy.

Preuve de la proposition 3.20. — Montrons que (ii) $\Longrightarrow$ (i). Il suffit de montrer que pour tout $a \in Z$, le faisceau d'idéaux $I_{Z,a} \subset \mathcal{O}_{M,a}$ est stable par la dérivation δ_a.

Fixons $a \in Z$. Par définition, on a $\phi_a([\mathbb{C} \times Z]_{(0,a)}) \subset [Z]_a$. On en déduit que pour tout $f \in I_{Z,a}$, on a :

$$\phi_a^\sharp(f) \in I_{\mathbb{C}\times Z,(0,a)} = I_{Z,a}.\mathcal{O}_{M,a}\{t\}$$

Le lemme 3.21 permet de conclure que $\delta_a(f) = \frac{d}{dt}\phi_a^\sharp(f)_{|t=0} \in I_{Z,a}$, ce qui montre que $Z \subset (M, v_M)$ est bien une sous-variété analytique invariante.

Réciproquement, supposons que $Z \subset (M, v_M)$ est une sous-variété invariante. Fixons $a \in Z$. On a donc pour tout $f \in I_{Z,a} \subset \mathcal{O}_{M,a}$ et tout entier $n \geq 1$, $\frac{1}{n!}\delta_a^n(f) \in I_{Z,a}$. Le lemme 3.21 permet d'affirmer que

$$f \in I_{Z,a} \Longrightarrow \phi_a^\sharp(f) \in I_{Z,a}.\mathcal{O}_{M,a}\{t\} = I_{\mathbb{C}\times Z,(0,a)}.$$

On en déduit que $\phi_a([\mathbb{C} \times Z]_{(0,a)}) \subset [Z]_a$, ce qu'il fallait démontrer. □

3.1.3. *Compatibilité des différentes notions d'invariances.* —

PROPOSITION 3.22. — *Soient (X, v_X) une D-variété lisse au dessus de $(\mathbb{R}, 0)$ et $Z \subset X$ une sous-variété fermée invariante (définie sur $\mathbb{R}$). On note (M, ϕ) le flot réel de (X, v_X). L'ensemble $Z(\mathbb{R}) \subset M$ est un fermé ϕ-invariant.*

Autrement dit, si $Z \subset X$ est une sous-variété fermée invariante alors pour tout $x \in Z(\mathbb{R})$, l'orbite $\mathcal{O}_x$ de x est contenue dans Z.

Démonstration. — Soit $Z \subset X$ une sous-variété fermée invariante. D'après la remarque 3.16, la sous-variété fermée analytique $Z(\mathbb{C})^{an} \subset M_{\mathbb{C}} = X(\mathbb{C})^{an}$ est $\delta_{M_{\mathbb{C}}}$-invariante. D'après la proposition 3.20, on en déduit que, en notant ϕ_a le germe du flot complexe en $a \in M_{\mathbb{C}}$, on a :

$$\phi_a([\mathbb{C} \times Z(\mathbb{C})]_{(0,a)}) \subset [Z(\mathbb{C})]_a$$

Si $a \in M \subset M_{\mathbb{C}}$, le germe du flot réel en a est la restriction du germe du flot complexe aux nombres réels et vérifie :

$$\phi_a([\mathbb{R} \times M]_{(0,a)}) \subset [M]_a.$$

En prenant les intersections, on obtient que pour tout $a \in X(\mathbb{R})$:

$$\phi_a([\mathbb{R} \times Z(\mathbb{R})]_{(0,a)}) \subset [Z(\mathbb{R})]_a.$$

Le lemme 3.10 permet de conclure que $Z(\mathbb{R})$ est ϕ-invariant. □

Voici une réciproque partielle au résultat précédent. Elle ne sera pas utilisée dans la preuve du critère d'orthogonalité aux constantes.

PROPOSITION 3.23. — *Soit (X, v_X) une D-variété lisse au-dessus de $(\mathbb{R}, 0)$. On note (M, ϕ) le flot réel de (X, v_X). Si $A \subset X(\mathbb{R})$ est un sous-ensemble ϕ-invariant alors la clôture de Zariski $\overline{A}$ de A est une sous-variété fermée invariante de (X, v_X).*

Démonstration. — Remarquons d'abord que d'après le lemme A.12, on peut supposer que X est affine. On note $Z = \overline{A}$ la clôture de Zariski de A dans X.

Il suffit de vérifier que l'idéal $I \subset \mathcal{O}_M(M)$ des fonctions analytiques qui s'annulent sur A est stable par la dérivation $\delta_v : \mathcal{O}_M \longrightarrow \mathcal{O}_M$ induite par le champ de vecteurs v_M sur M. En effet, en utilisant l'inclusion $\mathbb{R}[X] \subset \mathcal{O}_M(M)$, l'idéal $I_Z \subset \mathbb{R}[X]$ définissant Z est donné par

$$I_Z = I \cap \mathbb{R}[X] \subset \mathcal{O}_M(M).$$

Ces deux sous-ensembles sont stables par la dérivation δ_v, et donc Z est une sous-variété invariante de (X, v_X).

Montrons donc que le faisceau d'idéaux $\mathcal{I} \subset \mathcal{O}_M$ des fonctions analytiques s'annulant sur A est invariant par la dérivation δ_v.

Soient $f \in \mathcal{I}$ et $x \in M$. En notant $\phi_x : (\mathbb{R} \times M, (0,x)) \longrightarrow (M,x)$ le germe du flot ϕ en x, le germe de $\delta_v(f)$ en x est donné par :

$$\delta_v(f)_x = \frac{d}{dt}[f \circ \phi_x]_{|t=0}.$$

Comme A est un sous-ensemble ϕ-invariant, on a $f \circ \phi_x([\mathbb{R} \times A]_{(0,x)}) = 0$ et donc

$$\delta_v(f)_x([A]_x) = \frac{d}{dt}[f \circ \phi_x]_{|t=0}([A]_x) = 0.$$

On en déduit que le germe $\delta_v(f)_x$ de $\delta_v(f)$ en x appartient à $\mathcal{I}_x$ pour tout $x \in M$ et donc que $\delta_v(f) \in I$. □

COROLLAIRE 3.24. — *Soit (X, v_X) une D-variété au dessus de $(\mathbb{R}, 0)$. La clôture de Zariski de $X(\mathbb{R})$ dans X est une sous-variété fermée invariante.*

Il suffit d'appliquer successivement les deux proposition 3.22 et 3.23. Cet énoncé a la forme d'un énoncé d'algèbre différentielle mais il est propre à l'extension de corps $\mathbb{R} \subset \mathbb{C}$. Il n'est pas difficile de construire des exemples de D-variétés (X, v_X) définie sur le corps $\mathbb{Q}$ des nombres rationnels telles que la clôture de Zariski de $X(\mathbb{Q})$ ne soit pas invariante.

Par exemple, si C est une courbe affine sur le corps $\mathbb{Q}$ admettant un nombre fini de points rationnels et si v_C est un champ de vecteurs régulier sur C qui ne s'annule pas en tous les points de $C(\mathbb{Q})$ alors la sous-variété fermée $\overline{C(\mathbb{Q})} = C(\mathbb{Q}) \subset (C, v_C)$ n'est pas invariante.

3.2. Flots topologiquement transitifs et topologiquement mélangeants. — Dans cette partie, on se restreint à l'étude de flots réels complets $(M, (\phi_t)_{t\in\mathbb{R}})$. De plus, au lieu de considérer des flots analytiques réels, on considère plus généralement des flots continus sur un espace métrisable, ce qui est le cadre naturel pour les résultats de cette partie.

Un flot réel continu s'identifie alors à une action du groupe additif $(\mathbb{R}, +)$ des nombres réels sur un espace métrisable M et donc à un système dynamique pour le groupe additif des nombres réels.

On renvoie aux trois premières sections du chapitre 1 de [11] pour des résultats et notions analogues dans le cadre plus général des systèmes dynamiques sur un groupe topologique localement compact et de cardinal $\leq 2^{\aleph_0}$. Dans les prochains paragraphes, on donne une présentation autonome des résultats qui nous seront utiles dans la suite.

3.2.1. *Flot topologiquement transitif.* — On fixe M un espace topologique métrisable.

Définition 3.25. — Soit $(M,(\phi_t)_{t\in\mathbb{R}})$ un flot continu complet. On dit que $(M,(\phi_t)_{t\in\mathbb{R}})$ est *un flot topologiquement transitif* si pour tout couple d'ouverts non vides $U,V\subset M$, il existe $t\in\mathbb{R}$ tel que $\phi_t(U)\cap V\neq\emptyset$.

Notation 3.26. — Soit $(M,(\phi_t)_{t\in\mathbb{R}})$ un flot continu complet. Pour tout couple d'ouverts non vides $U,V\subset X$, on note

$$N(U,V)=\{t\in\mathbb{R}\mid \phi_t(U)\cap V\neq\emptyset\}\subset\mathbb{R}$$

Un flot complet $(M,(\phi_t)_{t\in\mathbb{R}})$ est topologiquement transitif si et seulement si pour tout couple d'ouverts non vides $U,V\subset M$, le sous-ensemble $N(U,V)\subset\mathbb{R}$ est non vide.

Remarque 3.27. — Pour tout couple d'ouverts non vides $U,V\subset\mathbb{R}$, le sous-ensemble $N(U,V)\subset\mathbb{R}$ est un ouvert de $\mathbb{R}$. On en déduit que $N(U,V)$ s'écrit comme une union (au plus) dénombrable et éventuellement vide d'intervalles ouverts disjoints de $\mathbb{R}$.

De plus, remarquons que $N(U,V)=-N(V,U)\subset\mathbb{R}$.

Exemple 3.28. — Si $(M,(\phi_t)_{t\in\mathbb{R}})$ est le flot continu complet sur le disque unité $\mathbb{S}^1=\mathbb{R}/2\pi\mathbb{Z}$ induit par le champ de vecteurs unitaire sur $\mathbb{S}^1$ alors pour tout couple d'intervalles ouverts non vides $U,V\subset\mathbb{S}^1$, il existe $a<b\in\mathbb{R}$ tels que

$$N(U,V)=\bigcup_{k\in\mathbb{Z}}]a+2.\pi k\mathbb{Z};b+2.\pi k\mathbb{Z}[.$$

Si $(M,(\phi_t)_{t\in\mathbb{R}})$ est le flot continu complet sur la droite réelle induit par le champ de vecteurs constant $\frac{d}{dt}$ alors pour tout couple d'intervalles ouverts bornés non vides $U,V\subset\mathbb{R}$, il existe $a<b\in\mathbb{R}$ tels que

$$N(U,V)=]a,b[.$$

En particulier, les deux flots précédents sont topologiquement transitifs.

Avec des hypothèses topologiques raisonnables, on a la caractérisation suivante des flots complets continus topologiquement transitifs.

Proposition 3.29. — *Soit $(M,(\phi_t)_{t\in\mathbb{R}})$ un flot complet continu. Supposons que M soit localement compact et séparable. Les propriétés suivantes sont alors équivalentes :*

(i) *Le flot $(M,(\phi_t)_{t\in\mathbb{R}})$ est topologiquement transitif.*
(ii) *Il existe une orbite dense dans $(M,(\phi_t)_{t\in\mathbb{R}})$.*

Démonstration. — (ii) $\Rightarrow$ (i) Soient $U,V\subset M$ un couple d'ouverts non vide de M. Considérons $x\in M$ dont l'orbite est dense dans M.

Comme l'orbite de x est dense dans M, il existe un réel $t \in \mathbb{R}$ tel que $\phi_t(x) \in U$ et un entier $s \in \mathbb{R}$ tel que $\phi_s(x) \in V$. On en déduit que

$$\phi_{-s}(V) \cap \phi_{-t}(U) \neq \emptyset \text{ et donc } \phi_{s-t}(U) \cap V \neq \emptyset.$$

(i) $\Rightarrow$ (ii) Considérons une base dénombrable d'ouverts $(U_k)_{k\in\mathbb{N}}$ de l'espace métrique séparable M. Remarquons qu'un sous-ensemble de M est dense si et seulement s'il rencontre tous les $(U_k)_{k\in\mathbb{N}}$.

On construit par récurrence sur $k \in \mathbb{N}^*$ une suite de compacts d'intérieur non vide

$$V_k \subset V_{k-1} \subset \cdots \subset V_1$$

tels que l'orbite de tout point de V_i rencontre les ouverts $U_1, \cdots, U_i$.

- Pour $n = 1$, comme M est localement compact, il existe un compact $V_1 \subset U_1$ d'intérieur non vide.
- Supposons $V_k \subset V_{k-1} \subset \cdots \subset V_1$ construits. Par hypothèse, $\overset{\circ}{V_k}$ est un ouvert non vide. Comme le flot est topologiquement transitif, il existe $t \in \mathbb{R}$ tel que $\overset{\circ}{V_k} \cap \phi_t(U_{k+1}) \neq \emptyset$. L'ensemble $\overset{\circ}{V_k} \cap \phi_t(U_{k+1})$ est un ouvert non vide de M et par construction, l'orbite de chacun de ses points rencontre $U_1, \cdots, U_{k+1}$. Comme M est localement compact, il suffit de choisir un compact V_{k+1} d'intérieur non vide tel que $V_{k+1} \subset \overset{\circ}{V_k} \cap \phi_t(U_k)$.

Une intersection de compacts non vides emboités étant toujours non vide, considérons $x \in \bigcap_{k\in\mathbb{N}} V_k$. Par construction, l'orbite de x rencontre tous les $(U_k)_{k\in\mathbb{N}}$ et est donc dense dans M. □

Exemple 3.30. — Considérons le tore $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ et le flot $(\phi_t)_{t\in\mathbb{R}}$ défini sur $\mathbb{T}^n$ par le système d'équations différentielles linéaires

$$\begin{cases} \frac{dy_1}{dt} = \omega_1 \\ \quad \vdots \\ \frac{dy_n}{dt} = \omega_n \end{cases}$$

où $\omega = (\omega_1, \cdots, \omega_n) \in \mathbb{T}^n$. Le flot complet $(\mathbb{T}^n, (\phi_t)_{t\in\mathbb{R}})$ défini par le système d'équations différentielles précédent est appelé *le flot constant sur le tore* $\mathbb{T}^n$ *de fréquences* $\omega_1, \cdots, \omega_n$.

Le flot $(\mathbb{T}^n, (\phi_t)_{t\in\mathbb{R}})$ est topologiquement transitif si et seulement si les fréquences $\omega_1, \cdots, \omega_n$ sont $\mathbb{Z}$-indépendantes [20, Proposition 1.5.1].

Remarque 3.31. — Un produit de deux flots complets topologiquement transitifs n'est pas toujours topologiquement transitif :

Considérons les flots constants sur $\mathbb{T}^n$ de fréquences respectives $(\omega_1, \ldots, \omega_n)$ et $(\tau_1, \ldots, \tau_n)$. Le flot produit est le flot constant sur $\mathbb{T}^{2n}$ de fréquences $(\omega_1, \ldots, \omega_n, \tau_1, \ldots, \tau_n)$. D'après l'exemple 3.30, le flot produit est topologi-

quement transitif si et seulement si $(\omega_1, \dots, \omega_n, \tau_1, \dots, \tau_n)$ sont $\mathbb{Z}$-linéairement indépendants. En particulier le produit d'un flot constant sur le tore avec lui-même n'est jamais topologiquement transitif.

3.2.2. *Flots faiblement topologiquement mélangeants.* — La condition « être topologiquement transitif » n'est donc pas stable par produit. On s'intéresse donc désormais à la classe des flots complets continus $(M, (\phi_t)_{t\in\mathbb{R}})$ tel que pour tout $n \in \mathbb{N}$, le flot produit $(M, (\phi_t)_{t\in\mathbb{R}})^n$ est topologiquement transitif.

PROPOSITION 3.32. — *Soit $(M, (\phi_t)_{t\in\mathbb{R}})$ un flot continu. Les propriétés suivantes sont équivalentes*

(i) *Le flot $(M, (\phi_t)_{t\in\mathbb{R}}) \times (M, (\phi_t)_{t\in\mathbb{R}})$ est topologiquement transitif.*
(ii) *Pour tout $n \in \mathbb{N}$, le flot $(M, (\phi_t)_{t\in\mathbb{R}}) \times \cdots \times (M, (\phi_t)_{t\in\mathbb{R}})$ est topologiquement transitif.*
(iii) *La famille des $N(U, V)$ où U et V parcourent l'ensemble des ouverts non vides de M est une famille filtrante de $\mathcal{P}(\mathbb{R})$.*

Rappelons que si E est un ensemble, une partie filtrante de $\mathcal{P}(E)$ est une partie $\mathcal{F} \subset \mathcal{P}(E) \setminus \{\emptyset\}$ vérifiant : pour tout $A, B \in \mathcal{F}$ il existe $C \in \mathcal{F}$ tel que $C \subset A \cap B$.

Démonstration. — (ii) $\Rightarrow$ (i) est immédiat. Montrons que (iii) $\Rightarrow$ (ii). Soit $n \in \mathbb{N}$. Pour vérifier que $(M, (\phi_t)_{t\in\mathbb{R}})^n$ est topologiquement transitif, il suffit de vérifier que $N(U, V) \neq \emptyset$ pour U et V parcourant une base d'ouverts de M^n.

Les ouverts de la forme $U_1 \times \cdots \times U_n$, où $U_1, \cdots, U_n \subset M$ sont des ouverts de M, engendrent la topologie produit sur M^n. On en déduit que $(M, (\phi_t)_{t\in\mathbb{R}})^n$ est topologiquement transitif si et seulement si

$$N(U_1 \times \cdots \times U_n) \cap N(V_1 \times \cdots \times V_n) = N(U_1, V_1) \cap \cdots \cap N(U_n, V_n) \neq \emptyset$$

lorsque $U_1, \cdots, U_n, V_1 \cdots, V_n$ parcourent les ouverts non vides de M.

Soient $U_1, \cdots, U_n, V_1 \cdots, V_n$ des ouverts non vides de M. D'après la propriété (iii), il existe des ouverts non vides $A, B \subset M$ tels que $N(A, B) \subset N(U_{n-1}, V_{n-1}) \cap N(U_n, V_n)$. On en déduit que :

$$\begin{aligned} N(U_1, V_1) \cap \cdots \cap N(U_{n-2}, V_{n-2}) \cap N(A, B) \subset \\ \subset N(U_1 \times \cdots \times U_n) \cap N(V_1 \times \cdots \times V_n). \end{aligned}$$

Par induction, il existe des ouverts non vides $\tilde{A}, \tilde{B} \subset M$ tels que :

$$N(\tilde{A}, \tilde{B}) \subset N(U_1 \times \cdots \times U_n) \cap N(V_1 \times \cdots \times V_n).$$

En particulier, on obtient que $N(U_1 \times \cdots \times U_n) \cap N(V_1 \times \cdots \times V_n) \neq \emptyset$ car $N(\tilde{A}, \tilde{B}) \neq \emptyset$.

Montrons que (i) $\Rightarrow$ (iii). Soient U_1, V_1, U_2, V_2 des ouverts non vides de M. Le système dynamique $(M, (\phi_t)_{t\in\mathbb{R}}) \times (M, (\phi_t)_{t\in\mathbb{R}})$ étant topologiquement transitif, on a

$$N(U_1, V_1) \cap N(U_2, V_2) \neq \emptyset.$$

En particulier, $N(U_1, V_1)$ est toujours non vide.

De plus, considérons $t \in N(U_1, V_1) \cap N(U_2, V_2)$ et posons $A = \phi_t(U_1) \cap U_2$ et $B = \phi_t(V_1) \cap V_2$. Par hypothèse sur t, A et B sont des ouverts non vides de M et on vérifie facilement que

$$N(A, B) \subset N(U_1, V_1) \cap N(U_2, V_2). \qquad \square$$

DÉFINITION 3.33. — Soit $(M, (\phi_t)_{t\in\mathbb{R}})$ un flot complet continu. On dit que $(M, (\phi_t)_{t\in\mathbb{R}})$ est *un flot faiblement topologiquement mélangeant* si l'une des trois conditions équivalentes de la proposition 3.32 est vérifiée.

EXEMPLE 3.34. — Le calcul direct des $N(U, V)$ pour les exemples 3.28 montrent que ces deux flots ne sont pas faiblement topologiquement mélangeants.

De même, la remarque 3.31 montre que les flots constants sur le tore (exemple 3.30) ne sont pas faiblement topologiquement mélangeants non plus.

L'exemple fondamental de flot faiblement topologiquement mélangeant est le flot géodésique unitaire sur une variété réelle compacte munie d'une métrique à courbure strictement négative (voir [1], [7], [8]). Cet exemple sera le point de départ des applications pour le critère d'orthogonalité aux constantes présenté dans ce texte et sera discuté dans une suite de cet article.

4. Un critère dynamique d'orthogonalité aux constantes

Dans cette section, on établit le critère annoncé d'orthogonalité aux constantes pour les D-variétés réelles ainsi que sa version en familles annoncées dans l'introduction.

Le critère d'orthogonalité aux constantes que nous présentons (théorème 4.8) consiste en *une obstruction topologique à la présence d'intégrale première rationnelle* pour ce flot complet et tous ses produits. L'argument essentiel est donné par une notion élémentaire de la théorie des systèmes dynamiques topologiques : les flots faiblement topologiquement mélangeants.

En s'appuyant sur les résultats de spécialisation de la deuxième partie de ce texte, nous démontrons ensuite une variante de ce critère d'orthogonalité aux constantes (théorème 4.10) pour *les membres « très génériques » de familles lisses de D-variétés absolument irréductibles a partir de l'étude dynamique d'une des fibres réelles.*

4.1. Indétermination et intégrale première rationnelle. — On étudie plus généralement les conséquences de l'existence d'une intégrale première rationnelle pour les D-variétés définies sur des corps de constantes. On fixe k un corps de caractéristique 0.

NOTATION 4.1. — Soient X une variété algébrique irréductible sur le corps k et $f \in k(X)$ une fonction rationnelle. Alors f définit un morphisme rationnel de variétés $f : X \dashrightarrow \mathbb{P}^1$ qui admet un plus grand ouvert de définition $U \subset X$.

Le graphe $G_f \subset U \times \mathbb{P}^1$ de f s'identifie à une sous-variété fermée irréductible de $U \times \mathbb{P}^1$. Sa clôture de Zariski dans $X \times \mathbb{P}^1$ sera notée $\overline{G_f}$.

LEMME 4.2. — *Soient (X, v_X) une D-variété irréductible au dessus de $(k, 0)$ et $f \in k(X)$ une fonction rationnelle. On a équivalence entre :*

(i) *La fonction rationnelle f est une intégrale première rationnelle de (X, v_X).*
(ii) *La sous-variété fermée $\overline{G_f} \subset (X, v_X) \times (\mathbb{P}^1, 0)$ est une sous-variété fermée invariante.*

Démonstration. — Considérons $U \subset X$ un ouvert affine tel que $f_{|U} : U \longrightarrow \mathbb{A}^1$ est une fonction régulière. D'après les lemmes A.12 et A.7, il suffit de vérifier l'équivalence pour $f_{|U}$. On peut donc supposer que $U = X$, c'est à dire que X est affine et que $f \in k[X]$.

Le graphe $G_f \subset X \times \mathbb{A}^1$ de f est alors l'hypersurface de $X \times \mathbb{A}^1$ d'équation $Y - f = 0$.

On en déduit que G_f est une sous-variété invariante de $(X, v_X) \times (\mathbb{A}^1, 0)$ si et seulement s'il existe $h(Y) \in k[X][Y]$ tel que

$$\delta_X(f) = h(Y)(Y - f) \in k[X][Y].$$

En comparant les dégrés en Y, on voit que nécessairement $h(Y) = 0$ et donc que la seconde condition est équivalente à $\delta_X(f) = 0$, autrement dit que f est une intégrale première rationnelle de (X, v_X). □

DÉFINITION 4.3. — Soient X une variété algébrique irréductible et $f \in k(X)$ une fonction rationnelle. On appelle *lieu d'indétermination de f* et on note $\mathrm{Ind}(f)$, le complémentaire du plus grand ouvert de définition de $f : X \dashrightarrow \mathbb{P}^1$. Le lieu d'indétermination de f est donc une sous-variété fermée de X.

REMARQUE 4.4. — Soient X une variété algébrique irréductible et lisse et $f : X \dashrightarrow \mathbb{P}^1$ une fonction rationnelle sur X. En notant $\pi_f : \overline{G_f} \longrightarrow X$ la restriction de la première projection à $\overline{G_f}$, d'après le Main Theorem de Zariski [22, Théorème 3.20], on a la description suivante de $\mathrm{Ind}(f)$:

$$\mathrm{Ind}(f) = \{x \in X \mid \pi_f^{-1}(x) \text{ admet une composante irréductible de dimension} > 0\}$$

Comme $\overline{G_f} \subset X \times \mathbb{P}^1$, la condition précédente se réécrit :

$$\mathrm{Ind}(f) = \{x \in X \mid \{x\} \times \mathbb{P}^1 \subset \overline{G_f}\}.$$

LEMME 4.5. — *Soient (X, v_X) une D-variété irréductible et lisse au-dessus de $(k, 0)$ et $f \in k(X)$ une intégrale première rationnelle. Le lieu d'indétermination de f, $\mathrm{Ind}(f) \subset (X, v_X)$ est une sous-variété fermée invariante.*

Démonstration. — On note $Z = \mathrm{Ind}(f) \subset X$ le lieu d'indétermination de f qui est donc une sous-variété fermée de X. On commence par décrire le faisceau d'idéaux associé à Z avant de vérifier qu'il est invariant.

Considérons $U \subset X$ un ouvert affine. La sous-variété fermée irréductible $G_U := \overline{G_f} \cap (U \times \mathbb{A}^1) \subset U \times \mathbb{A}^1$ est une hypersurface. Comme $U \times \mathbb{A}^1$ est lisse, il existe $F \in k[U][T]$ tel que $G_U \subset U \times \mathbb{A}^1$ est l'hypersurface d'équation $F(X, T) = 0$. Fixons $t_0 \in k$. D'après la remarque 4.4, on a alors

$$Z = \{x \in X \mid F(x, .) = 0\} = \{x \in X \mid \forall n \in \mathbb{N},\ \frac{\partial}{\partial t^n} F(x, t_0) = 0\}.$$

On en déduit que $I_Z(U) \subset \mathcal{O}_X(U)$ est l'idéal engendré par $\frac{\partial}{\partial t^n} F(X, t_0)$ où n parcourt $\mathbb{N}$.

D'après le lemme 4.2, la sous-variété fermée $G_U \subset (U, v_X) \times (\mathbb{A}^1, 0)$ est une sous-variété invariante, donc il existe $h(X, Y) \in k[U][T]$ tel que

$$\delta_{X \times \mathbb{A}^1}(F(X, T)) = h(X, T) F(X, T).$$

Les dérivations $\delta_{X \times \mathbb{A}^1}$ et $\frac{\partial}{\partial t}$ commutent (car $\delta_{X \times \mathbb{A}^1}(T) = 0$) et donc pour tout $n \in \mathbb{N}$,

$$\left[\delta_{X \times \mathbb{A}^1} \frac{\partial}{\partial t^n} F\right](X, t_0) = \left[\frac{\partial}{\partial t^n} \delta_{X \times \mathbb{A}^1}(F)\right](X, t_0) = \left[\frac{\partial}{\partial t^n}(h.F)\right](X, t_0)$$

Comme $I_Z(U)$ est l'idéal engendré par $\frac{\partial}{\partial t^n} F(X, t_0)$ où n parcourt $\mathbb{N}$, la règle de Leibniz pour les dérivations supérieures d'un produit permet alors de conclure que $I_Z(U) \subset \mathcal{O}_X(U)$ est un idéal invariant et donc que $\mathrm{Ind}(f)$ est une sous-variété fermée invariante. □

PROPOSITION 4.6. — *Soit (X, v_X) une D-variété irréductible et lisse au dessus de $(k, 0)$ admettant une intégrale première rationnelle non constante. En notant* Inv *l'ensemble des sous-variétés fermées invariantes strictes de (X, v_X), on a :*

$$X(k) = \bigcup_{Z \in \mathrm{Inv}} Z(k).$$

Démonstration. — Considérons $f : X \dashrightarrow \mathbb{P}^1$ une intégrale première rationnelle non constante et notons U son plus grand ouvert de définition.

Considérons $x \in X(k)$. On a deux cas :

- Si $x \in U(k)$ alors en notant $a = f(x)$, $f^{-1}(a)$ est une sous-variété fermée invariante de (U, v_X) contenant x et de codimension 1. Sa clôture de

Zariski dans X est une sous-variété fermée invariante (d'après le lemme A.12) et stricte de (X, v_X).
- Si $x \notin U(k)$ alors $x \in \mathrm{Ind}(f)$ qui est une sous-variété fermée invariante stricte d'après le lemme 4.5. □

4.2. Critère d'orthogonalité aux constantes pour les D-varietes reelles. —

LEMME 4.7. — *Soient (M, v_M) une D-variété analytique réelle et $K \subset M$ un compact ϕ-invariant. On note (U, ϕ) le flot réel associé. La restriction du flot ϕ au sous-ensemble K est un flot complet.*

Démonstration. — Pour tout $x \in M$, notons $U_x =]t^-(x); t^+(x)[$ où $t^-(x) < 0 < t^+(x)$, le plus grand ouvert de définition de la courbe intégrale ϕ_x de v_M en $x \in M$ vérifiant $\phi_x(0) = x$.

Les fonctions $t^+ : M \longrightarrow \mathbb{R} \cup \{-\infty; \infty\}$ et $t^- : M \longrightarrow \mathbb{R} \cup \{-\infty; \infty\}$ sont des fonctions continues. Comme K est compact, le réel $\epsilon = \inf_{x \in K} t^+(x)$ est strictement positif.

On raisonne par l'absurde en considérant $x_0 \in K$ tel que, par exemple, $t_0 = t^+(x) < \infty$. Posons $x_1 = \phi_{t_0 - \frac{\epsilon}{2}}(x) \in K$ car K est ϕ-invariant.

La courbe définie par :

$$\overline{\phi_x} : \begin{cases}]t^-(x); t^+(x) + \frac{\epsilon}{2}[\longrightarrow M \\ \qquad\qquad t \longmapsto \begin{cases} \phi_{x_0}(t) & \text{si } t \leq t_0 \\ \phi_{x_1}(t - t_0 - \frac{\epsilon}{2}) & \text{si } t \geq t_0 - \frac{\epsilon}{2} \end{cases} \end{cases}$$

est bien définie par la propriété de semi-groupe du flot associé au champ de vecteurs v_M. On vérifie aisément que $\overline{\phi_x}$ est une courbe intégrale de v_M vérifiant $\overline{\phi}_x(0) = x$, ce qui contredit la maximalité de U_x.

De même, on obtient que $t^-(x) = -\infty$ pour tout $x \in K$ et donc que la restriction du flot ϕ au compact K est complet. □

THÉORÈME 4.8. — *Soient X une variété absolument irréductible sur $\mathbb{R}$ et v un champ de vecteurs rationnel sur X. On note (M, ϕ) le flot régulier réel de (X, v_X). Supposons qu'il existe un compact $K \subset M$ Zariski-dense dans X et invariant par le flot ϕ. La restriction du flot ϕ à K est alors un flot métrisable complet.*

Si $(K, (\phi_{t|K})_{t \in \mathbb{R}})$ est faiblement topologiquement mélangeant alors le type générique de (X, v) est orthogonal aux constantes.

Démonstration. — La conclusion reste inchangée lorsque l'on remplace X par $U = X \setminus (\mathrm{Sing}(X) \cup \mathrm{Sing}(v))$. On peut donc supposer que (X, v) est une D-variété absolument irréductible et lisse au dessus de $(\mathbb{R}, 0)$.

LEMME 4.9. — *Soit (X, v) une D-variété irréductible lisse au dessus de $(\mathbb{R}, 0)$. Si le flot réel associé (M, ϕ) admet une orbite Zariski-dense dans X alors (X, v) est sans intégrale première rationnelle non constante.*

Démonstration. — Considérons $x \in M = X(\mathbb{R})$ dont l'orbite est Zariski-dense dans X et $Z \subset X$ une sous-variété fermée invariante contenant x. D'après la proposition 3.22, l'orbite $\mathcal{O}_x$ de $x \in M$ est contenue dans $Z(\mathbb{R})$ et comme cette orbite est Zariski-dense dans X, on en déduit que $Z = X$. On en déduit que $x \notin \bigcup_{Z \in \mathrm{Inv}} Z(\mathbb{R})$. La proposition 4.6 permet de conclure que (X, v) est sans intégrale première rationnelle. □

La fin de la démonstration est alors formelle : Puisque $(K, (\phi_{t|K})_{t\in\mathbb{R}})$ est faiblement topologiquement mélangeant, pour tout $n \in \mathbb{N}$, le flot $(K, (\phi_{t|K})_{t\in\mathbb{R}})^n$ est topologiquement transitif et admet donc une orbite $\mathcal{O}_n \subset K^n$ dense pour la topologie analytique (proposition 3.29).

De plus, $K \subset X$ est Zariski-dense et donc $K^n \subset X^n$ aussi pour tout $n \in \mathbb{N}$. La topologie analytique étant plus fine que la topologie de Zariski, on en déduit que pour tout $n \in \mathbb{N}$, $(X, v)^n$ admet $\mathcal{O}_n$ pour orbite Zariski-dense.

D'après le lemme précédent, la D-variété $(X, v)^n$ est sans intégrale première rationnelle non constante pour tout $n \in \mathbb{N}$. Son type générique est donc orthogonal aux constantes d'après le théorème 2.4. □

4.3. Critère d'orthogonalité aux constantes pour les familles de D-variétés. —

THÉORÈME 4.10. — *Soient k un sous-corps des nombres réels, S une variété algébrique lisse et irréductible au dessus de k et $f : (\mathcal{X}, v) \longrightarrow (S, 0)$ une famille lisse de D-variétés absolument irréductibles à paramètres dans S.*

Supposons qu'il existe un point $p \in S(\mathbb{R})$ et un compact $K \subset \mathcal{X}_p(\mathbb{R})^{an}$ Zariski-dense dans X et invariant par le flot ϕ du champ de vecteurs $v_{|X_p}$.

Si $(K, (\phi_{t|K})_{t\in\mathbb{R}})$ est faiblement topologiquement mélangeant alors il existe un ensemble dénombrable $\{Z_i : i \in \mathbb{N}\}$ de sous-variétés fermées algébriques strictes (sur le corps des nombres réels) Z_i de S tel que :

$$\forall s \in S(\mathbb{C}) \setminus \bigcup_{i\in\mathbb{N}} Z_i(\mathbb{C}),\ (\mathcal{X}, v)_s \text{ est orthogonal aux constantes.}$$

Démonstration. — Notons d'abord qu'on peut toujours supposer que k est finiment engendré et donc un corps dénombrable.

Sous les hypothèses du théorème 4.10, le théorème 4.8 implique que le type générique de la fibre $(\mathcal{X}, v)_p$ est orthogonal aux constantes.

Notons η le point générique de S. Le théorème 2.23 (ou plus précisément sa contraposée) implique alors que le type générique de $(\mathcal{X}, v)_\eta$ est orthogonal aux constantes.

En utilisant le lemme 2.20, pour toutes les realisations

Considérons maintenant l'ensemble $\mathcal{S}$ des sous-variétés fermées strictes de S (au dessus de k). Puisque k est dénombrable, l'ensemble $\mathcal{S}$ est dénombrable.

Soit $s \in S(\mathbb{C}) \setminus \bigcup_{Z\in\mathcal{S}} Z(\mathbb{C})$. Par construction, s réalise le type générique de S (au sens de $\mathbf{ACF}_0$) et donc le type générique de $(S, 0)$ (au sens de $\mathbf{DCF}_0$)

puisque le corps des constantes est un pur corps algébriquement clos stablement plongé. Le corollaire 2.20 implique donc que $(X, v)_s$ est orthogonal aux constantes. □

Annexe A. *D*-variétés et ensembles définissables associés

Dans cette partie, nous étudions les interactions entre les ensembles définissables dans un corps différentiellement clos et la notion de D-variété, introduite par A. Buium dans [5]. L'utilisation des D-variétés pour l'étude des corps différentiellement clos est fréquente en théorie des modèles ([12], [26]). La relation entre la catégorie des D-schémas et les ensembles définissables (et les types) dans un corps différentiellement clos est analogue à la relation entre les schémas et les ensembles définissables dans un corps algébriquement clos.

Dans la première section, nous rappelons la définition et les propriétés structurelles des D-schémas ainsi que de la notion associée de sous-schéma invariant. Dans la deuxième section, nous nous concentrons sur la relation entre D-variété et ensemble définissable dans la théorie $\mathbf{DCF}_0$.

A.1. *D*-schémas. —

A.1.1. *Catégorie des D-schémas.* —

Définition A.1. — On appelle *D-schéma* tout couple (X, δ_X) où X est un schéma et $\delta_X : \mathcal{O}_X \longrightarrow \mathcal{O}_X$ est une dérivation sur le faisceau structural $\mathcal{O}_X$ de X, c'est-à-dire un morphisme de faisceaux en groupes abéliens satisfaisant à la règle de Leibniz :

$$\delta_X(s.t) = \delta_X(s).t + s.\delta_X(t) \text{ pour tout ouvert } U \subset X \text{ et tous } s, t \in \mathcal{O}_X(U).$$

Si (X, δ_X) et (Y, δ_Y) sont deux D-schémas, on appelle *morphisme de D-schémas de* (X, δ_X) *vers* (Y, δ_Y), tout morphisme de schémas $f = (|f|, f^\sharp) : (X, \mathcal{O}_X) \longrightarrow (Y, \mathcal{O}_Y)$ faisant commuter le diagramme suivant :

$$\begin{array}{ccc} \mathcal{O}_X & \xrightarrow{\delta_X} & \mathcal{O}_X \\ {\scriptstyle f^\sharp}\uparrow & & \uparrow{\scriptstyle f^\sharp} \\ f^{-1}\mathcal{O}_Y & \xrightarrow[f^{-1}\delta_Y]{} & f^{-1}\mathcal{O}_Y \end{array} \tag{3}$$

On a ainsi défini une catégorie appelée *catégorie des D-schémas* et notée **D-Sch**.

Exemple A.2. — Soit (A, δ_A) un anneau (commutatif) différentiel. La dérivation δ_A se prolonge uniquement aux localisations de A et induit une dérivation sur le faisceau structural $\mathcal{O}_{\mathrm{Spec}(A)}$. On obtient ainsi un D-schéma noté $(\mathrm{Spec}(A), \delta_A)$.

REMARQUE A.3. — Plus généralement, on peut définir la catégorie **C** des D-espaces localement annelés dont :

- les objets sont les espaces localement annelés $(X, \mathcal{O}_X)$ muni d'une dérivation $\delta_X : \mathcal{O}_X \longrightarrow \mathcal{O}_X$ du faisceau structural $\mathcal{O}_X$.
- les flèches sont les morphismes d'espaces localement annelés faisant commuter le diagramme (3).

La catégorie des D-schémas s'identifie alors à la sous-catégorie pleine de la catégorie **C** dont les objets sont les D-espaces localement annelés $(X, \mathcal{O}_X, \delta_X)$ localement représentable sous la forme $(\mathrm{Spec}(A), \delta_A)$ où (A, δ) est un anneau différentiel.

La catégorie **D-Sch** admet un foncteur d'oubli naturel vers la catégorie des schémas obtenu en oubliant la dérivation sur le faisceau structural F_{oub} : **D-Sch** $\longrightarrow$ **Sch**.

NOTATION A.4. — Pour toute propriété (P) des schémas (resp. des morphismes de schémas), nous dirons qu'un D-schéma (resp. un morphisme de D-schémas) possède la propriété (P) si le schéma sous-jacent (resp. le morphisme de schémas sous-jacent) possède la propriété (P).

Par exemple, on dira qu'un D-schéma (X, δ_X) est de type fini (resp. séparé, réduit, irréductible) si le schéma sous-jacent X a la même propriété.

PROPOSITION A.5. — *La catégorie* **D-Sch** *admet des produits fibrés et un élément terminal. De plus, la formation des produits fibrés commute au foncteur d'oubli vers la catégorie des schémas.*

Démonstration. — En effet, si (C, δ_C) est un anneau différentiel et (A, δ_A) et (B, δ_B) sont deux (C, δ_C)-algèbres différentielles, on définit la (C, δ)-algèbre différentielle

$$(A, \delta_A) \otimes_{(C,\delta_C)} (B, \delta_B) = (A \otimes_C B, \delta_A \otimes_C \mathrm{Id}_B + \mathrm{Id}_A \otimes_C \delta_B).$$

On vérifie alors qu'on a ainsi défini le produit de $(\mathrm{Spec}(A), \delta_A)$ avec $(\mathrm{Spec}(B), \delta_B)$ au dessus de $(\mathrm{Spec}(C), \delta_C)$. Pour les D-schémas généraux, on procède par recollement à partir d'un recouvrement affine. Cette construction montre que la formation des produits commute au foncteur d'oubli vers la catégorie des schémas. □

REMARQUE A.6. — Soit (K, δ) un corps différentiel. Le couple $(\mathrm{Spec}(K), \delta)$ est un D-schéma. On note **D-Sch**$/(K, \delta)$, la catégorie des objets au dessus de $(\mathrm{Spec}(K), \delta)$.

La catégorie **D-Sch**$/(K, \delta)$ admet un élément terminal ainsi que des produits fibrés d'après la proposition A.5. Cette proposition montre aussi que, si $(K, \delta) \subset (L, \delta_L)$ est une extension de corps différentiels alors, on a un foncteur

de changement de base noté

$$- \times_{(K,\delta)} (L, \delta_L) : \begin{cases} \mathbf{D\text{-}Sch}/(K,\delta) \longrightarrow \mathbf{D\text{-}Sch}/(L,\delta_L) \\ (X,\delta_X) \longmapsto (X,\delta_X)_{(L,\delta_L)}. \end{cases}$$

Si (X, δ_X) est un D-schéma alors tout ouvert $U \subset X$ est naturellement muni d'une structure de D-schéma notée (U, δ_U) qui fait de l'immersion ouverte un morphisme de D-schémas.

Lemme A.7. — *Soient (X, δ_X) et (Y, δ_Y) deux D-schémas, $f : X \longrightarrow Y$ un morphisme de schémas et $U \subset X$ un ouvert schématiquement dense. Si $f_{|U} : (U, \delta_U) \longrightarrow (Y, \delta_Y)$ est un morphisme de D-schémas alors $f : (X, \delta_X) \longrightarrow (Y, \delta_Y)$ est un morphisme de D-schémas.*

La réciproque du lemme A.7 est bien-sûr toujours vérifiée même lorsqu'on ne suppose plus que $U \subset X$ est schématiquement dense.

Démonstration. — On veut montrer que le diagramme (3) est commutatif. Comme l'inclusion $i : (U, \delta_U) \longrightarrow (X, \delta_X)$ est un morphisme de D-schémas, et par adjonction entre les foncteurs i^{-1} et i_*, on a le diagramme commutatif :

$$\begin{array}{ccc} i_*\mathcal{O}_U & \xrightarrow{i_*\delta_U} & i_*\mathcal{O}_U \\ \uparrow & & \uparrow \\ \mathcal{O}_X & \xrightarrow[\delta_X]{} & \mathcal{O}_X \end{array} \tag{4}$$

De plus, puisque $U \subset X$ est schématiquement dense, les deux flèches verticales sont injectives. Ainsi, pour vérifier la commutativité du diagramme (3), il suffit de vérifier que le diagramme suivant est commutatif :

$$\begin{array}{ccc} i_*\mathcal{O}_U & \xrightarrow{i_*\delta_U} & i_*\mathcal{O}_U \\ \uparrow & & \uparrow \\ f^{-1}\mathcal{O}_Y & \xrightarrow[f^{-1}\delta_Y]{} & f^{-1}\mathcal{O}_Y \end{array}$$

La commutativité du dernier diagramme est conséquence du fait que $f_{|U} : (U, \delta_U) \longrightarrow (Y, \delta_Y)$ est un morphisme de D-schémas et de l'adjonction entre les foncteurs i^{-1} et i_*. □

Définition A.8. — Soient (X, δ_X) et (Y, δ_Y) deux D-schémas intègres et $f : X \dashrightarrow Y$ un morphisme rationnel. On dit que $f : (X, \delta_X) \dashrightarrow (Y, \delta_Y)$ est *un morphisme rationnel de D-schémas* si sa restriction à un ouvert non vide de X est un morphisme de D-schémas.

D'après le lemme A.7, si $f : (X, \delta_X) \dashrightarrow (Y, \delta_Y)$ est un morphisme rationnel de D-schémas alors f définit un morphisme de D-schémas sur son ouvert de définition.

A.1.2. *Sous-schémas invariants.* —

DÉFINITION A.9. — Soit (X, δ_X) un D-schéma. On dit qu'un sous-schéma fermé $Y \subset X$ est un *sous-schéma fermé invariant* de (X, δ_X), si le faisceau d'idéaux $\mathcal{I}_Y \subset \mathcal{O}_X$ définissant Y est stable par la dérivation δ_X, c'est-à-dire si pour tout ouvert $U \subset X$,

$$\mathcal{I}_Y(U) \subset (\mathcal{O}_X(U), \delta_X) \text{ est un idéal différentiel.}$$

REMARQUE A.10. — Soit (X, δ_X) un D-schéma et $i : Y \longrightarrow X$ un sous-schéma fermé invariant. La dérivation δ_X passe au quotient en une dérivation $\delta_Y : \mathcal{O}_Y \longrightarrow \mathcal{O}_Y$ sur le faisceau structural de Y qui fait de (Y, δ_Y) un D-schéma tel que l'immersion fermée $i : (Y, \delta_Y) \longrightarrow (X, \delta_X)$ est un morphisme de D-schémas.

Réciproquement, toute immersion fermée $i : (Y, \delta_Y) \longrightarrow (X, \delta_X)$ de D-schémas définit un sous-schéma fermé invariant de (X, δ_X).

LEMME A.11. — *Soient $f : (X, \delta_X) \longrightarrow (S, \delta_S)$ un morphisme de D-schémas et $(T, \delta_T) \longrightarrow (S, \delta_S)$ un changement de base.*

Si $Y \subset X$ un sous-schéma fermé invariant de (X, δ_X) alors $Y \times_S T$ est un sous-schéma fermé invariant de $(X, \delta_X) \times_{(S,\delta_S)} (T, \delta_T)$.

Démonstration. — L'immersion fermée $i : (Y, \delta_Y) \longrightarrow (X, \delta_X)$ induit après changement de base, un morphisme de D-schémas :

$$i_B : (Y, \delta_Y) \times_{(S,\delta_S)} (T, \delta_T) \longrightarrow (X, \delta_X) \times_{(S,\delta_S)} (T, \delta_T)$$

La notion d'immersion fermée étant invariante par changement de base, on conclut à l'aide de la remarque A.10. □

En particulier, si (X, δ_X) est un D-schéma, $U \subset X$ un ouvert et $Y \subset X$ un sous-schéma fermé invariant alors $Y \cap U$ est un sous-schéma fermé invariant de (U, δ_U). Réciproquement, on a le résultat suivant.

LEMME A.12. — *Soient (X, δ_X) un D-schéma et $Y \subset X$ un sous-schéma fermé. Considérons $U \subset X$ un ouvert tel que $Y \cap U$ est schématiquement dense dans Y.*

Si $Y \cap U$ est un sous-schéma fermé invariant de (U, δ_U) alors Y est un sous-schéma fermé invariant de (X, δ_X).

Démonstration. — On note $\mathcal{I} \subset \mathcal{O}_X$, le faisceau d'idéaux définissant Y. L'immersion ouverte $U \subset X$ induit un diagramme commutatif :

$$\begin{array}{ccc} \mathcal{O}_X/\mathcal{I} & \xrightarrow{j} & i_*(\mathcal{O}_X/I)_{|U} \\ \uparrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \pi_U} \\ \mathcal{O}_X & \longrightarrow & i_*\mathcal{O}_{X|U} \end{array}$$

où la première flèche horizontale j est injective car $Y \cap U$ est schématiquement dense dans Y.

Montrons que le faisceau d'idéaux $\mathcal{I} \subset \mathcal{O}_X$ est stable par la dérivation δ_X.

Soit $V \subset X$ un ouvert et $f \in I(V)$. On a alors $\pi_U(\delta_X(f)_{|U}) = \pi_U[\delta_U(f_{|U})] = 0$ car $Y \cap U$ est un sous-schéma fermé invariant de U. On en déduit que $(j \circ \pi)(\delta_X(f)) = 0$ donc que $\pi(\delta_X(f)) = 0$ car j est injective, c'est-à-dire $\delta_X(f) \in I(V)$. □

Proposition A.13. — *Soit (X, δ_X) un D-schéma noethérien au dessus de $(\mathbb{Q}, 0)$ et $Y \subset X$ un sous-schéma fermé invariant. Alors :*

(i) *Le sous-schéma fermé invariant réduit $Y_{red} \subset Y \subset (X, \delta_X)$ est un sous-schéma fermé invariant.*
(ii) *Les composantes irréductibles $Y_1, \cdots, Y_n \subset (X, \delta_X)$ de Y_{red} sont des sous-schémas fermés invariants.*

Démonstration. — Si (A, δ) est un anneau différentiel de caractéristique 0 alors le radical de tout idéal différentiel est un idéal différentiel [21, Chapitre 2, Lemme 1.15]. On en déduit que la propriété (i) est vérifiée.

Pour (ii), considérons Y_i une composante irréductible de Y_{red}. Considérons un ouvert $U \subset X$ tel que

$$Y_{red} \cap U = Y_i \cap U \neq \emptyset$$

(Il suffit de considérer l'ouvert $U = X \setminus \bigcup_{j \neq i} Y_j$).

Le schéma $Y_i \cap U = Y_{red} \cap U$ est un sous-schéma fermé invariant de (U, δ_U). Comme de plus $Y_i \cap U \subset Y_i$ est schématiquement dense dans Y_i (car Y_i est irréductible et $U \cap Y_i$ est non vide), le sous-schéma fermé $Y_i \subset (X, \delta_X)$ est invariant d'après le lemme A.12. □

A.2. Ensemble définissable associé à une D-variété. — On fixe $(\mathcal{U}, \delta_U)$ un modèle saturé de la théorie des corps différentiellement clos. Tous les corps différentiels considérés seront des sous-corps différentiels de $(\mathcal{U}, \delta_U)$.

Notation A.14. — Soit (K, δ) un corps différentiel. On appelle *D-variété au dessus de (K, δ)*, tout D-schéma au dessus de (K, δ) séparé, de type fini et réduit.

En particulier, les D-variétés au dessus de (K,δ) ne sont pas supposées irréductibles et on parlera de D-variétés irréductibles (resp. absolument irréductibles) au dessus de (K,δ) pour désigner les D-variétés au dessus de (K,δ) dont le K-schéma sous-jacent est irréductible (resp. absolument irréductible).

REMARQUE A.15. — La notion de D-variété est préservée par changement de base par un corps différentiel puisque les corps différentiels sont de caractéristique 0, c'est-à-dire si $(K,\delta)\subset(L,\delta_L)$ est une extension de corps différentiels et (X,δ_X) est une D-variété au dessus de (K,δ), alors $(X,\delta_X)_{(L,\delta_L)}$ est une D-variété au dessus de (L,δ_L).

A.2.1. *Interprétation d'une D-variété dans* $\mathbf{DCF}_0$. — Soit (K,δ) un corps différentiel.

NOTATION A.16. — Soient $(K,\delta)\subset(L,\delta_L)$ une extension de corps différentiels et (X,δ_X) un D-schéma au dessus de (K,δ). On appelle *ensemble des (L,δ_L)-points différentiels de (X,δ_X)*, l'ensemble

$$(X,\delta_X)^{(L,\delta_L)}=\mathrm{Hom}_{D-Sch/(K,\delta)}[(\mathrm{Spec}\,L,\delta_L);(X,\delta_X)].$$

On montre dans la suite de cette partie que l'ensemble $(X,\delta_X)^{(U,\delta_U)}$ peut être muni d'une structure d'ensemble définissable dans $\mathbf{DCF}_0$.

EXEMPLE A.17. — Soit (S) un système d'équations différentielles algébriques à paramètres dans (K,δ), c'est-à-dire un système d'équations différentielles algébriques de la forme :

$$(S):\begin{cases}P_1(x_1,\cdots,x_r,\delta(x_1),&\cdots,\delta^k(x_1),\cdots\delta^k(x_r))=0\\&\vdots\\P_r(x_1,\cdots,x_r,\delta(x_1),&\cdots,\delta^k(x_1),\cdots\delta^k(x_r))=0\end{cases}$$

où les $P_i\in K[X_1^{(0)},\cdots,X_r^{(0)},\cdots,X_1^{(k)},\cdots,X_r^{(k)}]$ sont des polynômes.

Le foncteur $\mathcal{S}$ « solutions de (S) » de la catégorie des (K,δ)-algèbres différentielles vers la catégorie des ensembles est représentable par un D-schéma affine (X,δ_X) au dessus de (K,δ).

En effet, considérons $K\{X_1,\cdots,X_r\}$ la (K,δ)-algèbre différentielle libre engendrée par les indéterminées $X_1,\cdots,X_r$. Pour tout $i\leq r$, on a

$$P_i(X_1,\cdots,X_r,\delta(X_1),\cdots,\delta^k(X_1),\cdots\delta^k(X_r))\in K\{X_1,\cdots,X_r\}.$$

Notons $I\subset K\{X_1,\cdots X_r\}$ l'idéal différentiel engendré par ces éléments. Le foncteur $\mathcal{S}$ est alors représentable par le D-schéma affine associé à la (K,δ)-algèbre différentielle $K\{X_1,\cdots,X_n\}/I$. En général, ce D-schéma n'est ni réduit ni de type fini.

REMARQUE A.18. — On en déduit que si (X, δ_X) représente le foncteur solutions d'un système d'équations différentielles algébriques (S) à paramètres dans (K, δ) alors $(X, \delta_X)^{(\mathcal{U}, \delta_\mathcal{U})} = \mathcal{S}(\mathcal{U}, \delta_U)$ s'identifie à un ensemble K-définissable de $(\mathcal{U}, \delta_\mathcal{U})$.

CONSTRUCTION A.19. — Soit (X, δ_X) une D-variété au dessus de (K, δ). Considérons $\mathcal{V} = (V_i, f_i)_{i=1,\cdots,n}$ où (V_i) est un recouvrement ouvert affine de X et où les $f_i : V_i \longrightarrow \mathbb{A}^n$ sont des immersions fermées.

On peut construire une formule $\phi_\mathcal{V}(x)$ sans quantificateurs à paramètres dans K telle que pour toute extension de corps différentiels $(K, \delta) \subset (L, \delta_L)$, on a l'identification suivante :

$$(X, \delta_X)^{(L, \delta_L)} = \phi_\mathcal{V}(L, \delta_L).$$

Démonstration. — Pour toute extension de corps différentiels $(K, \delta) \subset (L, \delta_L)$, puisque $(V_i)_{i=1}^n$ est un recouvrement ouvert de X, on a une application surjective :

$$\pi : \bigsqcup_{i=1}^{n} (V_i, \delta_{V_i})^{(L, \delta_L)} \longrightarrow (X, \delta_X)^{(L, \delta_L)}.$$

qui identifie $(X, \delta_X)^{(L, \delta_L)}$ au quotient de $\bigsqcup_{i=1}^n (V_i, \delta_{V_i})^{(L, \delta_L)}$ par une relation d'équivalence E.

Pour tout $i \leq n$, les immersions fermées $f_i : V_i \longrightarrow \mathbb{A}^n$ permettent d'identifier $(V_i, \delta_i)^{(L, \delta_L)}$ à l'ensemble des solutions d'un système d'équations différentielles algébriques (S_i) à n indéterminées et donc à un ensemble K-définissable sans quantificateurs dans (L, δ_L).

On en déduit que $\bigsqcup_{i=1}^n (V_i, \delta_{V_i})^{(L, \delta_L)}$ s'identifie à un ensemble K-définissable de (L, δ_L) sans quantificateurs.

ASSERTION. — *La relation d'équivalence E est K-définissable sans quantificateurs dans le langage des anneaux.*

En effet, sa définition est donnée par les fonctions de transitions du recouvrement ouvert $(U_i)_{i \leq n}$ et donc définissable sans quantificateurs dans le langage des anneaux (et donc dans le langage des anneaux différentiels).

Par élimination des imaginaires dans la théorie des corps algébriquement clos, il existe une formule sans quantificateurs $\phi_\mathcal{V}(\overline{x})$ telle que pour toute extension de corps différentiels $(K, \delta) \subset (L, \delta_L)$:

$$(X, \delta_X)^{(L, \delta_L)} = \bigsqcup_{i=1}^{n} (V_i, \delta_{V_i})^{(L, \delta_L)} / E = \phi_\mathcal{V}(L, \delta_L). \qquad \square$$

Le lemme suivant montre que la structure définissable induite ne dépend pas du recouvrement ouvert choisi.

LEMME A.20. — *Soit $\mathcal{E}$ l'ensemble des données $\mathcal{V} = (V_i, f_i)_{i=1,\cdots,n}$ où (V_i) est un recouvrement ouvert affine de V et où les $f_i : V_i \longrightarrow \mathbb{A}^n$ sont des immersions fermées.*

Si $\mathcal{V}, \mathcal{V}' \in \mathcal{E}$ alors pour toute extension de corps différentiels $(K, \delta) \subset (L, \delta_L)$, les ensembles $\phi_{\mathcal{V}}(L, \delta_L)$ et $\phi_{\mathcal{V}'}(L, \delta_L)$ sont en bijection définissable sans quantificateurs à paramètres dans (K, δ).

Démonstration. — Deux recouvrement ouverts admettent toujours un raffinement commun. On peut donc supposer que $\mathcal{V}'$ est un recouvrement plus fin que $\mathcal{V}$. Il suffit alors de vérifier que si X est un D-schéma affine et $(V_i)_{i\leq n}$ un recouvrement affine de X alors l'application

$$\pi : \coprod_{i=1}^{n} (V_i, \delta_{V_i})^{(L,\delta_L)} \longrightarrow (X, \delta_X)^{(L,\delta_L)}$$

est K-définissable sans quantificateurs, ce qui est immédiat. □

Suivant l'usage en théorie des modèles, si $(K, \delta) \subset (\mathcal{U}, \delta_{\mathcal{U}})$ est une extension différentiellement close, on identifiera $(X, \delta_X)^{(\mathcal{U},\delta_{\mathcal{U}})}$ à un ensemble K-définissable dans $(\mathcal{U}, \delta_{\mathcal{U}})$ sans préciser le recouvrement affine choisi. On a la description intrinsèque suivante de la structure induite par $(\mathcal{U}, \delta_U)$ sur $(X, \delta_X)^{(\mathcal{U},\delta_{\mathcal{U}})}$.

COROLLAIRE A.21. — *Soient (K, δ) un corps différentiel et (X, δ_X) une D-variété au-dessus de (K, δ). Les sous-ensembles K-définissables de $(X, \delta_X)^{(\mathcal{U},\delta_{\mathcal{U}})}$ sont les combinaisons booléennes d'ensembles de la forme $(Y, \delta_Y)^{(\mathcal{U},\delta_{\mathcal{U}})}$ où $Y \subset (X, \delta_X)$ est une sous-variété invariante.*

Démonstration. — Supposons que le D-schéma (X, δ_X) est affine et considérons une immersion fermée $X \subset \mathbb{A}^n$. Par élimination des quantificateurs, les sous-ensembles K-définissables de $\mathcal{U}^n$ sont les combinaisons booléennes de sous-ensembles de la forme :

$$V(I) = \{x \in \mathcal{U}^n \mid f(x) = 0, \forall f \in I\} \subset \mathcal{U}^n.$$

où $I \subset K\{X_1, \cdots, X_n\}$ est un idéal différentiel de la (K, δ)-algèbre libre d'indéterminées $X_1, \cdots X_n$. On en déduit que les sous-ensemble définissables de $(X, \delta_X)^{(\mathcal{U},\delta_{\mathcal{U}})}$ sont les combinaisons booléennes des ensembles $V(I)$ où $I \subset K\{X_1, \cdots, X_n\}$ est un idéal différentiel contenant l'idéal I_X définissant X. Ces derniers sont en correspondance avec les sous-schémas fermés invariants de (X, δ_X). La proposition A.13 permet alors de conclure.

On en déduit le cas général à l'aide du lemme A.12 et de la construction précédente. □

NOTATION A.22. — Soient (X, δ_X) une D-variété au dessus d'un corps différentiel (K, δ) et $\Sigma = (X, \delta_X)^{(\mathcal{U},\delta_{\mathcal{U}})}$. On note $S_\Sigma(K)$ l'ensemble des types vivants sur Σ (c'est-à-dire vérifiant $p_\Sigma(x) \models x \in \Sigma$) à paramètres dans K.

COROLLAIRE A.23. — *Soient (K,δ) un corps différentiel et (X,δ_X) une D-variété au dessus de (K,δ). On pose $\Sigma=(X,\delta_X)^{(\mathcal{U},\delta_\mathcal{U})}$. Pour toute sous-variété fermée invariante $Y\subset(X,\delta_X)$, il existe un unique type complet $p_{(Y,\delta_Y)}(x)$ vivant sur Σ vérifiant :*

$$p_{(Y,\delta_Y)}(x)\models\begin{cases}x\in(Y,\delta_Y)^{(\mathcal{U},\delta_\mathcal{U})}\\ x\notin(Y',\delta'_Y)^{(\mathcal{U},\delta_\mathcal{U})} & \text{pour } Y'\nsubseteq Y \text{ une sous-variété}\\ & \text{invariante stricte}\end{cases}$$

De plus, en notant $\mathrm{Inv}_\delta(X,\delta_X)$ l'ensemble des sous-variétés fermées irréductibles et invariantes de (X,δ_X), l'application $\mathrm{Inv}_\delta(X,\delta_X)\longrightarrow S_\Sigma(K)$ ainsi définie est une bijection.

Le cas affine est donné par le corollaire 1.17 et la cas général s'en déduit aisément à l'aide du lemme A.12.

A.2.2. *Type générique d'une D-variété irréductible.* — Soit (X,δ_X) une D-variété irréductible au dessus de (K,δ). Le corollaire précédent montre qu'il existe un type $p\in S(K)$ à paramètres dans K et vivant sur $(X,\delta_X)^{(\mathcal{U},\delta_\mathcal{U})}$ dont les réalisations coïncident avec les réalisations du point générique (au sens de la géométrie algébrique) de (X,δ_X).

DÉFINITION A.24. — Soient (K,δ) un corps différentiel et (X,δ_X) une D-variété irréductible au dessus de (K,δ). On appelle *type générique de* (X,δ_X), le type $p_{(X,\delta_X)}\in S(K)$ correspondant à la variété X elle-même dans le corollaire A.23.

LEMME A.25. — *Soient (K,δ) un corps différentiel et (X,δ_X) une D-variété irréductible au dessus de (K,δ). Posons $\Sigma=(X,\delta_X)^{(\mathcal{U},\delta_\mathcal{U})}$.*

(i) *Le type $p_{(X,\delta_X)}$ est l'unique type d'ordre maximal vivant sur Σ. De plus, il vérifie*

$$\mathrm{ord}(p_{(X,\delta_X)})=\dim(X).$$

(ii) *Le type $p_{(X,\delta_X)}$ est stationnaire si et seulement si la D-variété (X,δ_X) est absolument irréductible. Dans ce cas, son unique extension non-déviante à une extension $(K,\delta)\subset(L,\delta_L)$ est le type générique de $(X,\delta_X)_{(L,\delta_L)}$.*

Démonstration. — Soit $a\models p_{(X,\delta_X)}$ une réalisation du type $p_{(X,\delta_X)}$. Par définition du type $p_{(X,\delta_X)}$, ses réalisations sont les réalisations du point générique de (X,δ_X) et donc le sous-corps différentiel $K\langle a\rangle$ engendré par a dans $(\mathcal{U},\delta_U)$ est isomorphe au corps différentiel $(K(X),\delta_X)$. On en déduit que :

$$\mathrm{ord}(p)=\mathrm{tr}(K\langle a\rangle/K)=\mathrm{tr}(K(X)/K)=\dim(X).$$

La propriété (i) est donc vérifiée. Montrons la propriété (ii). Soit $(K,\delta)\subset(L,\delta_L)$ une extension de corps différentiels.

Le corollaire A.23 montre que les extensions de $p_{(X,\delta_X)}$ à (L,δ_L) correspondent aux sous-variétés irréductibles invariantes de $(X,\delta_X)_{(L,\delta_L)}$ dont la projection vers X est dominante. Comme l'ordre d'un type témoigne de la déviation, la propriété (i) implique que les extensions non déviantes de $p_{(X,\delta_X)}$ à (L,δ_L) correspondent aux sous-variétés irréductibles invariantes de $(X,\delta_X)_{(L,\delta_L)}$ de dimension $\dim(X)$ et dont la projection vers X est dominante.

On en déduit que les extension non-déviantes de $p_{(X,\delta_X)}$ à (L,δ_L) correspondent aux composantes irréductibles de $(X,\delta_X)_{(L,\delta_L)}$. □

Remarque A.26. — La propriété (i) du lemme précédent montre qu'il est facile de calculer l'ordre du type générique $p_{(X,\delta_X)}$ si l'on connait la D-variété (X,δ_X). En particulier l'ordre de $p_{(X,\delta_X)}$ ne dépend que de la variété X et non de la structure de D-variété sur X considérée.

Cependant, on ne sait en général pas déterminer $\mathrm{RM}(p_{(X,\delta_X)})$ et $\mathrm{RU}(p_{(X,\delta_X)})$. De plus, ces deux quantités dépendent de la structure de D-variété sur X.

Lemme A.27. — *Soient (K,δ) un corps différentiel, (X,δ_X) et (Y,δ_Y) des D-variétés irréductibles au dessus de (K,δ). Considérons $a \models p_{(X,\delta_X)}$, $b \models p_{(Y,\delta_Y)}$ des réalisations des types génériques de (X,δ_X) et (Y,δ_Y) respectivement. Les propriétés suivantes sont équivalentes :*

(i) $b \in \mathrm{dcl}(K,a)$

(ii) *Il existe un morphisme rationnel de D-variétés*

$$\phi : (X,\delta_X) \dashrightarrow (Y,\delta_Y) \text{ tel que } \phi^{\mathcal{U}}(a) = b.$$

où $\phi^{\mathcal{U}}$ désigne le morphisme induit par ϕ après passage au points différentiels dans $(\mathcal{U},\delta_{\mathcal{U}})$.

Démonstration. — (ii) $\Longrightarrow$ (i) est immédiat puisque l'application $\phi^{\mathcal{U}}$ est K-définissable et $\phi^{\mathcal{U}}(a) = b$. Montrons que (i) $\longrightarrow$ (ii). Comme $b \in \mathrm{dcl}(K,a)$, on en déduit que :

$$K\langle b\rangle = \mathrm{dcl}(K,b) \subset K\langle a\rangle = \mathrm{dcl}(K,a) \subset (\mathcal{U},\delta_U).$$

Les isomorphismes de corps différentiels au dessus de (K,δ), $(K(X),\delta_X) \simeq K\langle a\rangle$ et $(K(Y),\delta_Y) \simeq K\langle b\rangle$ définissent alors une injection de corps différentiels $i : (K(Y),\delta_Y) \longrightarrow (K(X),\delta_X)$ et donc un morphisme rationnel de D-variétés $\phi : (X,\delta_X) \dashrightarrow (Y,\delta_Y)$ tel que $\phi^{\mathcal{U}}(a) = b$. □

Remerciements. — Les théorèmes A et B constituent une partie de ma thèse de doctorat, réalisée sous la direction de Jean-Benoît Bost (Orsay) et de Martin Hils (Paris VII – Münster) tandis que les théorèmes C, D et E ont été écrit lors de mon postdoc à l'université de Waterloo. Outre mes directeurs de thèse, je tiens à remercier Elisabeth Bouscaren et Zoe Chatzidakis pour leurs précieuses remarques sur le contenu présenté dans ce texte, lors des exposés que j'ai donnés à Paris VII et à Orsay. Je tiens aussi à remercier Rahim Moosa (Waterloo) pour de nombreuses discussions au sujet de cet article.

BIBLIOGRAPHIE

[1] D. V. Anosov – *Geodesic flows on closed Riemann manifolds with negative curvature*, Proceedings of the Steklov Institute of Mathematics, No. 90 (1967). Translated from the Russian by S. Feder, American Mathematical Society, Providence, R.I., 1969.

[2] T. Archibald – « Differential equations and algebraic transcendents : French efforts at the creation of a Galois theory of differential equations 1880–1910 », *Rev. Histoire Math.* **17** (2011), no. 2, p. 373–401.

[3] V. I. Arnol'd – *Ordinary differential equations*, Universitext, Springer-Verlag, Berlin, 2006, Translated from the Russian by Roger Cooke, Second printing of the 1992 edition.

[4] M. Audin – *Les systèmes hamiltoniens et leur intégrabilité*, Cours Spécialisés [Specialized Courses], vol. 8, Société Mathématique de France, Paris ; EDP Sciences, Les Ulis, 2001.

[5] A. Buium – « Geometry of differential polynomial functions. I. Algebraic groups », *Amer. J. Math.* **115** (1993), no. 6, p. 1385–1444.

[6] G. Casale, J. Freitag & J. Nagloo – « Ax-Lindemann-Weierstrass with derivatives and the genus 0 Fuchsian groups », *arXiv :1811.06583* (2019).

[7] Y. Coudene – « Topological dynamics and local product structure », *J. London Math. Soc. (2)* **69** (2004), no. 2, p. 441–456.

[8] F. Dal'bo – « Remarques sur le spectre des longueurs d'une surface et comptages », *Bol. Soc. Brasil. Mat. (N.S.)* **30** (1999), no. 2, p. 199–221.

[9] J. Drach – « Essai sur la théorie générale de l'itération et sur la classification des transcendantes », *Ann. Sci. École Norm. Sup. (3)* **15** (1898), p. 243–384.

[10] J. Freitag & T. Scanlon – « Strong minimality and the j-function », *J. Eur. Math. Soc. (JEMS)* **20** (2018), no. 1, p. 119–136.

[11] E. Glasner – *Ergodic theory via joinings*, Mathematical Surveys and Monographs, vol. 101, American Mathematical Society, Providence, RI, 2003.

[12] E. Hrushovski & M. Itai – « On model complete differential fields », *Trans. Amer. Math. Soc.* **355** (2003), no. 11, p. 4267–4296.

[13] E. Hrushovski – « Unidimensional theories are superstable », *Ann. Pure Appl. Logic* **50** (1990), no. 2, p. 117–138.

[14] E. Hrushovski & Z. Sokolovic – « Minimal subsets of differentially closed fields », *Preprint* (1996).

[15] Y. Ilyashenko & S. Yakovenko – *Lectures on analytic differential equations*, Graduate Studies in Mathematics, vol. 86, American Mathematical Society, Providence, RI, 2008.

[16] R. Jaoui – « Geodesic Flows and Model Theory of Differential Fields », Thèses, Université Paris-Saclay, 2017.

[17] ———, « Rational factors of D-varieties of dimension 3 with real Anosov flow », *arXiv :1803.08811* (2018).
[18] ———, « Differential fields and geodesic flows II : Geodesic flows of pseudo-Riemannian algebraic varieties », *Israel J. Math.* **230** (2019), no. 2, p. 527–561.
[19] E. Julliard Tosel – « Meromorphic parametric non-integrability ; the inverse square potential », *Arch. Ration. Mech. Anal.* **152** (2000), no. 3, p. 187–205.
[20] A. Katok & B. Hasselblatt – *Introduction to the modern theory of dynamical systems*, Encyclopedia of Mathematics and its Applications, vol. 54, Cambridge University Press, Cambridge, 1995, With a supplementary chapter by Katok and Leonardo Mendoza.
[21] D. Marker, M. Messmer & A. Pillay – *Model theory of fields*, second éd., Lecture Notes in Logic, vol. 5, Association for Symbolic Logic, La Jolla, CA ; A K Peters, Ltd., Wellesley, MA, 2006.
[22] D. Mumford – *Algebraic geometry. I*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, Complex projective varieties, Reprint of the 1976 edition.
[23] J. Nagloo & A. Pillay – « On the algebraic independence of generic Painlevé transcendents », *Compos. Math.* **150** (2014), no. 4, p. 668–678.
[24] ———, « On algebraic relations between solutions of a generic Painlevé equation », *J. Reine Angew. Math.* **726** (2017), p. 1–27.
[25] A. Pillay – *Geometric stability theory*, Oxford Logic Guides, vol. 32, The Clarendon Press, Oxford University Press, New York, 1996, Oxford Science Publications.
[26] A. Pillay & M. Ziegler – « Jet spaces of varieties over differential and difference fields », *Selecta Math. (N.S.)* **9** (2003), no. 4, p. 579–599.
[27] B. Poizat – « Les corps différentiellement clos, compagnons de route de la théorie des modèles », *Math. Japon.* **42** (1995), no. 3, p. 575–585.
[28] M. Rosenlicht – « The nonminimality of the differential closure », *Pacific J. Math.* **52** (1974), p. 529–537.
[29] K. Tent & M. Ziegler – *A course in model theory*, Lecture Notes in Logic, vol. 40, Association for Symbolic Logic, La Jolla, CA ; Cambridge University Press, Cambridge, 2012.