



HAL
open science

Infinitesimal behaviour of groups and beyond

Marion Jeannin

► **To cite this version:**

| Marion Jeannin. Infinitesimal behaviour of groups and beyond. 2023. hal-04132150

HAL Id: hal-04132150

<https://hal.science/hal-04132150v1>

Preprint submitted on 18 Jun 2023

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

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

INFINITESIMAL BEHAVIOUR OF GROUPS AND BEYOND

MARION JEANNIN

ABSTRACT. Linearisation often allows one to get a satisfactory local approximation of a complicated equation of motion. In the same spirit, algebraic tools have been developed to locally approximate affine group schemes: their Lie algebras. In this document, we will introduce these algebraic objects and describe how good the local approximation they provide can be.

1. MOTIVATION FROM PHYSICS

1.1. A mechanical starting point: linearise the pendulum oscillations : a mechanical starting point: linearise the pendulum oscillations. Before going any further, let us motivate the formalism that is to come with a simple situation: the simple gravity pendulum¹. A small bob viewed as a point mass is located at the end of a massless inextensible thread of length L . The latter is itself attached to a pivot. Here frictions are neglected. The bob is pushed out of its equilibrium position so that it oscillates back and forth.

Let θ be the angle between the (imaginary) vertical line and the thread. As θ varies through time it is a function of t . The motion of the bob is described by the variations of θ (where g is the local acceleration of gravity ²):

$$\frac{d^2\theta}{dt^2} + \frac{g}{L} \sin(\theta) = 0. \tag{1}$$

The main obstacle to solve this differential equation is posed by the sine term. One way to tackle this issue is to linearise the sine function. This follows from the observation that near 0 (when θ is small) the value of $\sin(\theta)$ is almost that of θ itself. Equation 1 is then approximated by that of simple harmonic motion:

$$\frac{d^2\theta}{dt^2} + \frac{g}{L} \theta = 0. \tag{2}$$

What precedes is based on the fact that any “reasonably painful” function f^3 can be approximated near a point by a polynomial function whose coefficients are determined by the successive derivatives of f^4 .

1.2. Symmetries as motions to study. A physical system is the data of an object together with its environment. To better understand some of its properties, one might want to have a look at its invariance under some transformations.

Those that leave the system invariant are called *symmetries*. Their study deeply simplifies one’s task: according to P. Curie’s principle, if a system is invariant under some symmetries so are its properties. Consider for instance a charged particle assimilated to a single point charge located at a point O in the 3-dimensional space. The frame of reference is located at O . In order to determine the induced electric field, first remark that the whole system is invariant under any rotation around O . By Curie’s

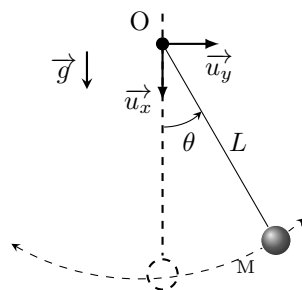


FIGURE 1. Simple gravity pendulum model with the corresponding variables.

¹This mathematical model provides a simplified version of the real pendulum.

²A constant that encodes the earth gravity $g \sim 9.80665m.s^{-2}$.

³Namely those that can be differentiated several times.

⁴This is known as Taylor’s theorem.

principle the electric field only depends on the distance to the particle, and is directed along the radial component in a spherical expression of the coordinates.

Symmetries of a physical system form a set \mathcal{S} . They can be seen as functions whose variables parametrise the system and satisfy some very specific properties:

- (1) the composition of two symmetries, denoted \circ , is a symmetry (\mathcal{S} is *stable under composition*);
- (2) let σ_1 , σ_2 and σ_3 belong to \mathcal{S} , then $(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3)$ (the composition is *associative*);
- (3) the identity Id , that is the transformation that fixes each parameter of the system, is a (trivial) symmetry ((\mathcal{S}, \circ) has a *neutral element*);
- (4) for any $\sigma \in \mathcal{S}$, the inverse function $\sigma^{-1} \in \mathcal{S}$. Note that σ^{-1} is the symmetry such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \text{Id}$ ⁵ (any $\sigma \in \mathcal{S}$ has an *inverse* in \mathcal{S} for \circ).

This makes the set of symmetries into a group. A *group* is the data of a pair $(G, *)$ where G is a set stable under a group law $*$ that satisfies the properties in parentheses in the above list (replace \mathcal{S} by G and \circ by $*$). In general $*$ need not be commutative: given $g_1, g_2 \in G$ the expressions $g_1 * g_2$ and $g_2 * g_1$ might differ. If they are equal for any $g_1, g_2 \in G$, the group is *abelian*.

The most natural example of group is $(\mathbb{Z}, +)$; here the neutral element is 0, and it is an abelian group. On the other hand (\mathbb{Z}, \cdot) , where \cdot denotes the usual multiplication, is not a group: in this case 1 is the neutral element and the issue is that for any $n \in \mathbb{Z} \setminus \{\pm 1\}$ there is no $m \in \mathbb{Z}$ such that $nm = 1$. The real numbers \mathbb{R} endowed with the multiplication are not a group either, as $0 \in \mathbb{R}$ has no inverse; although the set \mathbb{R}^* of non-zero real numbers is a group for the multiplication.

When symmetries of the physical system are defined by parameters that are continuous transformations⁶, one speaks about continuous symmetries. Rotations for instance are continuous functions of their defining angles. This enriches the group of continuous symmetries with an additional structure: that of a *Lie group*. These are groups G that locally look like $(\mathbb{R}^n, +)$ as a group for a given $n \in \mathbb{N}^*$

and where both the group law and the inverse map are continuous and smooth⁷. Intuitively, continuous symmetries can themselves be seen as motions. In the next section we will introduce algebraic tools that mimic the techniques used to study mechanical problems.

Another example of a Lie group is given by the set of square matrices of size n with real or complex entries and with non-zero determinant⁸, denoted GL_n .

1.3. Lie algebras. A *field* K is a set endowed with an addition $+$ and a multiplication \cdot , that admit respectively 0 and 1 as neutral elements; such that both $(K, +)$ and $(K \setminus \{0\}, \cdot)$ are abelian groups. Moreover, the multiplication distributes over the addition: namely, for any $a, b, c \in K$ one has $a \cdot (b + c) = a \cdot b + a \cdot c$. Classical examples of fields are the set of rational numbers \mathbb{Q} , that of real numbers \mathbb{R} and that of complex numbers \mathbb{C} with the usual addition $+$ and multiplication \cdot . However $(\mathbb{Z}, +, \cdot)$ is not a field as (\mathbb{Z}^*, \cdot) is not a group. All the fields mentioned so far have infinitely many elements. Later on we will see examples of finite fields.

A *ring* R is an algebraic object obtained by relaxing assumptions on fields: non-commutative multiplication and non-zero elements with no inverse in R are now allowed. Obviously, any field is a ring but there are rings that are not fields, for instance $(\mathbb{Z}, +, \cdot)$. The set of square matrices with entries in a ring is another example – indeed it is not commutative for matrix multiplication, and has non-invertible matrices: for instance those whose determinant is equal to 0.

⁵If σ_1, σ_2 are two symmetries it is not always true that $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

⁶Roughly speaking: functions whose values vary continuously (without jumps or breaks) under continuous variation of their arguments.

⁷Smooth functions are those who have “enough continuous derivatives” (this makes sense because of the local resemblance of G with \mathbb{R}^n).

⁸The determinant of a square matrix M is a polynomial whose variables are the entries of M . Such a matrix is invertible if and only if its determinant is invertible.

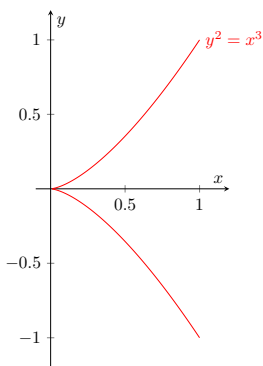


FIGURE 2. An example of a non smooth curve.

Lie algebras are abstract mathematical structures that help to study a Lie group near a point. They are defined with respect to a ring R . A *Lie algebra* L is a set which is:

- L1) an abelian group for an additive law $+$,
- L2) endowed with an external multiplication coming from R , called the scalar multiplication: for any $\alpha, \beta \in R$ and any $x, y \in L$ one has:
 - (a) $\alpha x \in L$, in particular if $\alpha = 1$ one has $1x = x$,
 - (b) $\alpha(x + y) = \alpha x + \alpha y$ and $(\alpha + \beta)x = \alpha x + \beta x$;
- L3) endowed with a so-called *Lie bracket* $[\cdot, \cdot] : L \times L \rightarrow L$ (that takes two elements of L to give back an element of L) and such that for any $\alpha \in K$ and any $x, y, z \in L$, the following identities are satisfied:
 - (a) $[\alpha x + z, y] = \alpha[x, y] + [z, y]$ and $[x, \alpha y + z] = \alpha[x, y] + [x, z]$ (*bilinearity*),
 - (b) $[x, x] = 0$,
 - (c) $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ (this is the Jacobi identity).

Note that conditions L3)a) and b) imply that $[x, y] = -[y, x]$ for any $x, y \in L$. To check this, start from $[x + y, x + y] = 0$ and use the bilinearity of the Lie bracket.

If R is a field and L satisfies assumptions L1) and L2), then L is an R -vector space. As for examples, a field K is itself a Lie algebra over K with the trivial Lie bracket, that is given by $[x, y] = 0$ for any $x, y \in K$. Similarly, the trivial Lie bracket endows any vector space with a Lie algebra structure. The set of square matrices of size $n \in \mathbb{N}^*$ with entries in R , denoted by $M_n(R)$, is a Lie algebra over R : it is an abelian group for the matrix addition, and for all $M, N \in M_n(R)$, the Lie bracket $[M, N]$ is given by *the commutator* $MN - NM$.

1.4. Infinitesimal behaviour: from Lie groups to Lie algebras. For the rest of this section we set $R = \mathbb{R}$ or \mathbb{C} . Let G be a Lie group so G locally looks like \mathbb{R}^n for some $n \in \mathbb{N}$. Intuitively if $g \in G$ is close to $h \in G$ (if it belongs to a neighbourhood of h) one can imagine that g is attained by moving away from h by a small amount in a given direction (this is a small variation around h). The study of small variations is that of the derivatives. The derivative of a real function f at $x \in \mathbb{R}$ is nothing but the slope of the tangent line to the graph of f at x . This gives the intuition behind the definition of *the Lie algebra of G* , denoted $\text{Lie}(G)$, as the tangent space to G at the neutral element e .

We are interested in studying elements of G located in the neighbourhood of another point of G , and that, for any point of G . This sounds quite tedious, as G is likely to be infinite. Things actually nicely arrange thanks to the presence of a group law on the whole G : this allows us to go continuously from one point to another, and neighbourhoods will be moved according to the same transformation. In other words, understanding G locally around a given $h \in G$ is enough to understand G locally around any $g \in G$. As we have the choice of the point near which we want to study G , we choose the only element that can be found, in substance, in any (Lie) group: the neutral element e . The idea is therefore to look at elements of G that are close to e , its so-called “infinitesimal elements”. These elements form the Lie algebra of G .

To make things clearer, G can locally be seen as \mathbb{R}^n and any $g \in G$ that is close to e is obtained by moving away from e in the direction u_g , namely $g = e + u_g$ with $u_g \in \text{Lie}(G)$. Any element of $\text{Lie}(G)$ occurs in this way. As we are interested only in infinitesimal behaviour, only the low order expression of u is kept (this sounds a bit mysterious now but should be clarified by what follows next). Let us check that $\text{Lie}(G)$ indeed satisfies L1), L2) and L3) and hence is a Lie algebra over R . To keep in mind the example of GL_n that rules a lot of things here, we write Id for e :

- L1) Let $u, v \in \text{Lie}(G)$, so there are $g, h \in G$ such that $g = \text{Id} + u$ and $h = \text{Id} + v$. As G is a group $gh = (\text{Id} + u)(\text{Id} + v) = \text{Id} + u + v + uv \in G$. We only keep the terms with the simplest expression in u and v : the idea is that if u and v are small uv is so small it is negligible. The multiplication of g by h therefore gives $u + v \in \text{Lie}(G)$, whence the additive law. Moreover Id belongs to its own neighbourhood and $\text{Id} = \text{Id} + 0 \in G$ so that $0 \in \text{Lie}(G)$ is the point that corresponds to $\text{Id} \in G$. As for the additive inverse of any $u \in \text{Lie}(G)$ defined by $g = \text{Id} + u \in G$, it comes from $g^{-1} \in G$. Locally $g^{-1} = \text{Id} + v$, and $gg^{-1} = \text{Id} + 0 \in G$ gives $u + v = 0 \in \text{Lie}(G)$.
- L2) Recall that G locally looks like \mathbb{R}^n for a given $n \in \mathbb{N}^*$. Moving away from Id in the direction u or αu , with $\alpha \in K = \mathbb{R}$ or \mathbb{C} , one follows the same line. Therefore $\text{Id} + \alpha u$ is an element of G in the neighbourhood of Id .

- L3) The Lie bracket is also induced by the group structure: let $g, h \in G$ and consider the commutator $ghg^{-1}h^{-1}$. Let g and h belong to the neighbourhood of Id so that $g = \text{Id} + u$ and $h = \text{Id} + v$, then

$$\begin{aligned} (\text{Id} + u)(\text{Id} + v)(\text{Id} - u)(\text{Id} - v) &= (\text{Id} + u)(\text{Id} + v)(\text{Id} - v - u + uv) \\ &= (\text{Id} + u)(\text{Id} - v - u + uv + v - v^2 - vu + vuv) \\ &= (\text{Id} - u + uv - vu + u + u^2 + u^2v - uvu) \\ &= (\text{Id} + uv - vu). \end{aligned}$$

To understand the successive equalities, remember that only the first-order expression in each variable are kept, so that v^2, vuv, u^2, u^2v, uvu are neglected. The commutator in G induces the Lie bracket on $\text{Lie}(G)$: namely $[u, v] = uv - vu$. Let us check that it satisfies L3a), b) and c): let $\alpha \in R$, and $u, v, w \in \text{Lie}(G)$, then

$$\begin{aligned} [\alpha u + w, v] &= (\alpha u + w)v - v(\alpha u + w) = (\alpha u + w)v - v(\alpha u + w) \\ &= \alpha uv + wv - \alpha vu + vw = \alpha(uv - vu) + wv - vw \\ &= \alpha[u, v] + [w, v], \end{aligned}$$

hence the left linearity of the bracket. Proceed on the same way to show the linearity from the right side. Finally one indeed has $[u, u] = 0$ for any $u \in \text{Lie}(G)$ and the Jacobi identity holds true, namely for any $u, v, w \in \text{Lie}(G)$:

$$\begin{aligned} [u, [v, w]] + [v, [w, u]] + [w, [u, v]] &= [u, vw - wv] + [v, wu - uw] + [w, uv - vu] \\ &= [u, vw] - [u, wv] + [v, wu] - [v, uw] + [w, uv] - [w, vu] \\ &= uvw - vwu - (uvw - wvu) + vwu - wuv - (vuw - uvw) \\ &\quad + wuv - uvw - (wvu - vuw) \\ &= 0. \end{aligned}$$

1.5. Exponential map: from Lie algebras to Lie groups. Lie algebras were introduced to facilitate the study of Lie groups by providing a good understanding of their local behaviour. Locally the datum of an element of the Lie algebra of the Lie group G should be “the same” as that of an element of G . This is formalised thanks to the exponential map. The idea is the following: on the one hand elements of $\text{Lie}(G)$ can be seen as derivatives of elements of G at the identity (locally they are derivatives at 0 of transformations of \mathbb{R}^n). On the other hand elements of G (that locally can be seen as transformations of \mathbb{R}^n) should locally look like those of $\text{Lie}(G)$. Therefore, roughly speaking, elements of G locally appear as fixed points of the operation consisting in taking the derivative. Hence they might look like the exponential of elements of the Lie algebra: we mimic what happens in \mathbb{R}^n . When $n = 1$ one has $\frac{d}{dx}(\exp(x)) = \exp(x)$, hence the use of the exponential.

When G appears as a matrix group¹⁰, for instance when $G = \text{GL}_n(K)$ with $K = \mathbb{R}$ or \mathbb{C} , the exponential of an element of $\text{Lie}(G)$ is well defined. Namely, if $A \in \text{Lie}(G)$ is a square matrix of size n we have:

$$\exp(A) = 1 + A + \frac{A^2}{2!} + \dots = \sum_{i=0}^{\infty} \frac{A^i}{i!}.$$

and then $\text{Lie}(G)$ is characterised as $\{M \in M_n(K) \mid \exp(tM) \in G \text{ for all } t \in K\}$. As taking the derivatives locally makes sense, one can check that the derivative at 0 of the exponential is indeed the same as the element we started with :

$$\left. \frac{d}{dt} \right|_{t=0} \exp(tX) = (X \exp(tX)) \Big|_{t=0} = X.$$

⁹This expresses the lack of commutativity of the group law: if g and h were to commute this product would be trivial as then $ghg^{-1}h^{-1} = hgg^{-1}h^{-1} = h \text{Id} h^{-1} = hh^{-1} = \text{Id}$.

¹⁰that is when elements of G are in particular invertible matrices.

2. FROM DIFFERENTIAL TO ALGEBRAIC GEOMETRY: A FIELD OF POSSIBILITIES

2.1. **Algebraic groups.** Let us focus on GL_n , the group of invertible square matrices of size n (characterised by a condition of invertible determinant). For any ring R , elements of $GL_n(R)$ can be thought of as zeros of polynomials in the matrix entries (those defined by the determinant minus an invertible element of R). Sets of solutions of polynomial equations define algebro-geometric objects called *affine schemes*.

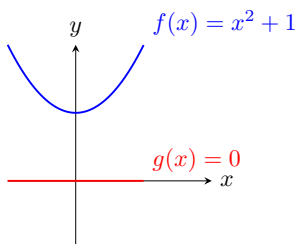


FIGURE 3. A graphic resolution of $x^2 + 1 = 0$ in \mathbb{R} .

That polynomial equations define geometric objects which are instructive to study the equation they derive from, is a frequent observation in mathematics. Consider for instance the affine scheme X defined by the polynomial equation $x^2 + 1 = 0$. Real solutions of this equation can be found by looking at the intersection of the graphs of two functions: on the one hand $f(x) = x^2 + 1$ (which defines a parabola), and on the other hand $g(x) = 0$. As these graphs don't intersect in \mathbb{R}^2 , the set of solutions, denoted by $X(\mathbb{R})$ is the empty set. Nevertheless, the set of complex solutions of $x^2 + 1 = 0$ is given by $X(\mathbb{C}) = \{i, -i\}$ ¹¹.

Let R be a ring and X be an affine scheme defined by polynomials with coefficients in R . Let A be a ring such that there exists a ring homomorphism $R \rightarrow A$ (that is a map from R to A that respects the ring structures). Henceforth such rings A are denoted $R \rightarrow A$. Polynomials that define X are sent to another set of polynomials, this time with coefficients in A , via the map $R \rightarrow A$. We denote by $X(A)$ the zeros of this new set of polynomials. If for any $R \rightarrow A$ these sets $X(A)$ can be endowed with a group structure, the affine scheme is a *group scheme*. For instance GL_n , is an affine scheme, defined by the polynomial equations given by the non-vanishing condition of the determinant. As for any ring A the set $GL_n(A)$ of square matrices of size n with entries and R with invertible determinant is a group, GL_n is a group scheme.

When $K = \mathbb{R}$ or \mathbb{C} we have seen that GL_n is a Lie group. Because of their local resemblance with \mathbb{R}^m , for a given $m \in \mathbb{N}^*$, Lie groups are of more analytic nature. On the other hand GL_n seen as an affine group scheme is of a more algebraic nature. Note that the affine group scheme structure of GL_n makes sense even if one looks at solutions in other rings than \mathbb{R} or \mathbb{C} . One can then wonder whether the analytic description can “extend” to other rings. The following paragraphs introduce the Lie algebra of an affine group scheme but also detail why the resulting approximation is no longer that precise in general.

2.2. **The Lie algebra associated to an algebraic group.** For the rest of this section G is an affine group scheme defined by a set of polynomial equations with coefficients in a ring R . Let A be a ring such that there is a ring homomorphism $R \rightarrow A$. We denote by $A[\epsilon]$ the ring of all polynomial with ϵ as a variable such that $\epsilon^2 = 0$ (the reader can check this is indeed a ring). For instance $1 + \epsilon = 1 + \epsilon + 15\epsilon^2$ in $A[\epsilon]$.

We proceed in the same way as before: for any $R \rightarrow A$ we are looking at first order variations around an element of $G(A)$ (as any greater power of ϵ equals zero). Thanks to the group structure the neutral element Id_A is again the canonical choice for the element near which one considers the variations. Elements of $\text{Lie}(G)(A)$ are those that can be written as $\text{Id}_A + \epsilon x$ in $G(A[\epsilon])$. Note that ϵ precisely encodes this idea of first order approximation. The Lie algebra structure is defined in the same way as before: the addition in $\text{Lie}(G)(A)$ is induced by the (multiplicative) group law on $G(A[\epsilon])$ and the Lie bracket is obtained by writing the commutator in $G(A[\epsilon])$ of two elements of the Lie algebra $\text{Lie}(G)(A)$ (with $\text{Id} + \epsilon g$ in $G(A[\epsilon])$ for some $g \in G(A)$). This defines a *Lie algebra scheme* $\text{Lie}(G)$: namely an affine scheme for which $\text{Lie}(G)(A)$ is a Lie algebra for any $R \rightarrow A$. If G is defined by some polynomial equations with coefficients in R , the *Lie algebra of G* is given by $\text{Lie}(G)(R)$.

As the formalism is quite heavy, let's illustrate what precedes with an example. As we want to get rid of any technical considerations, let's consider the special linear group SL_n whose elements are

¹¹Remember that $i \in \mathbb{C}$ is such that $i^2 = -1$.

matrices with determinant equal to 1. It is an affine subgroup scheme of GL_n (for any $R \rightarrow A$, the subset $\mathrm{SL}_n(A) \subset \mathrm{GL}_n(A)$ inherits of the group law of $\mathrm{GL}_n(A)$ by restriction). It is defined by the polynomial equation $\det(x_{i,j}) - 1 = 0$, where the $x_{i,j}$'s enumerate the matrix' entries. This equation has coefficients in \mathbb{Z} . Solutions in \mathbb{R} are given by the set of $n \times n$ matrices with entries in \mathbb{R} and determinant 1, whereas those in \mathbb{C} are square n matrices with determinant 1 and entries in \mathbb{C} . The affine group scheme SL_n defined by $\det(x_{i,j}) - 1 = 0$ is actually completely determined by the data of $\mathrm{SL}_n(A)$ for any ring $\mathbb{Z} \rightarrow A$. As any ring A actually comes with a ring homomorphism $\mathbb{Z} \rightarrow A$, the condition " $\mathbb{Z} \rightarrow A$ " in the preceding sentence can be replaced by "for any ring A ". Let us determine the associated Lie algebras $\mathrm{Lie}(\mathrm{SL}_n)(A)$. Their elements are $n \times n$ matrices M with entries in A such that $\mathrm{Id}_A + \epsilon M \in \mathrm{SL}_n(A[\epsilon])$, namely, matrices M such that $\mathrm{Id}_A + \epsilon M$ is a square matrix with entries in $A[\epsilon]$ and determinant 1. This is equivalent to M having trace zero¹² (so this scheme is defined by the equation $\sum x_{i,i} = 0$ where the $x_{i,i}$'s are the diagonal entries of a square matrix of size n).

2.3. The limits of the exponential. So far we have introduced a bunch of notions, the newest adapting the previously introduced ones to a slightly different context. Nevertheless this doesn't go without difficulties. This is particularly well illustrated by the question of the existence of the exponential map. Remember that this map is the tool that allows us to compare locally the Lie algebra of a matrix group with the matrix group itself. It is defined by the power series:

$$\exp(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}$$

where x is an indeterminate, and is evaluated at elements of the given Lie algebra to provide an element of the corresponding Lie group. As Lie algebras of affine group schemes are well defined objects, one can wonder whether the exponential can be used to better understand the local structure of affine group schemes. Note that the above power series has coefficients in \mathbb{Q} and thus can also be considered as a power series with coefficients in \mathbb{R} or \mathbb{C} . But there are fields for which the situation gets more complicated.

Let G be a group scheme defined by polynomial equations with coefficients in a ring R . Remember that there is always a morphism of rings $\mathbb{Z} \rightarrow R$. If one seeks a generalisation of the exponential, the image of any integer in R should at least be invertible (otherwise the denominators in the power series won't be well defined). This is ensured for instance when R is a field and no non zero integer is sent to 0 (as any non-zero element of a field is invertible).

The *characteristic* of a ring R is the smallest positive integer m such that for any $a \in R$ one has $ma = \underbrace{a + \dots + a}_{m \text{ times}} = 0$; if no such m exists, it is 0. For instance \mathbb{Z} , or \mathbb{R} or \mathbb{C} are of characteristic

0 as $m \cdot 1 \neq 0$ if $m \neq 0$. Let $m \in \mathbb{N}^*$, the set of integers modulo m , denoted $\mathbb{Z}/m\mathbb{Z}$ is a ring of positive characteristic. Two integers are *congruent modulo m* if they have the same remainder in their euclidean division by m . To build $\mathbb{Z}/m\mathbb{Z}$, start with \mathbb{Z} and cut it into several parts, the *classes*, each of them being filled by all integers that are pairwise congruent modulo m . To enumerate these classes it is enough to enumerate the set of all possible remainders for the euclidean division by m :

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \dots, [m-1]_m\}$$

where for any $x \in \mathbb{Z}$, we denote by $[x]_m$ the class of x modulo m . It can be checked that $\mathbb{Z}/m\mathbb{Z}$ is a ring¹³ of characteristic m : for any $[x]_m \in \mathbb{Z}/m\mathbb{Z}$ one indeed has $m[x]_m = \underbrace{[x]_m + \dots + [x]_m}_{m \text{ times}} = [mx]_m = [0]_m$

as the remainder of the euclidean division of mx by m is zero.

There exist fields of positive characteristic. For instance, when $m = p > 0$ is a prime number¹⁴, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field. Other examples can be built for example by enriching $\mathbb{Z}/p\mathbb{Z}$ with solutions of polynomial equations with coefficients in $\mathbb{Z}/p\mathbb{Z}$.

Let K be a field of positive characteristic $p > 0$ and consider an affine group scheme G which is a matrix group defined by a set of polynomial equations with coefficients in K (for instance $G = \mathrm{SL}_n$ or

¹²The trace of a matrix is the sum of its diagonal entries.

¹³In particular $[0]_m$ and $[1]_m$ are the neutral elements respectively for addition and multiplication.

¹⁴an integer which is strictly greater than 1 and that is only divisible by 1 and itself.

GL_n). Note that any matrix $M \in \mathrm{Lie}(G)(K)$ such that $M^p = 0$ has a well defined exponential:

$$\exp(M) = \sum_{i=0}^{p-1} \frac{M^i}{i!} \in G(K).$$

Matrices that give the null matrix when being raised at a certain power are *nilpotent* and this power is the *order of nilpotency*. From the previous discussion the reader can expect that, if the characteristic $p > 0$ is not too small (if it is greater than the maximal order of nilpotency), the exponential will integrate nilpotent matrices. Note the presence of $M^0 = \mathrm{Id}$ in the developed expression $\exp(M)$. As there exists $n \in \mathbb{N}$ such that $M^n = 0$ there actually exists an integer u such that the matrix $(\exp(M) - \mathrm{Id})^u = 0$ in G . This means that the matrix $\exp(M)$ is *unipotent*. The exponential, when it is defined, sends nilpotent elements of the Lie algebra on unipotent elements of the group.

This reasoning applies to other affine group schemes, when there is a well defined “power” map on the Lie algebra (when raising $x \in \mathrm{Lie}(G)(R)$ actually means something). For instance, it generalises to reductive groups G that are “nice enough groups” and can be thought as matrix groups for reasonably high bounds on the characteristic. In this case, G. McNinch provided an upper bound that depends on an intrinsic numerical value of G for the order of nilpotency of nilpotent elements of $\mathrm{Lie}(G)$ ([McN02]). This has been refined for some specific subsets of nilpotent elements of the Lie algebra of such groups by G. Seitz ([Sei00]).

Let us focus on what happens for a reductive group G . To summarise the last paragraph: for some reasonably high bounds on the characteristic, the exponential is well defined for nilpotent elements of $\mathrm{Lie}(G)$ and builds a dictionary between them and unipotent elements of G . This bound is determined by conditions of existence of the exponential. One can therefore wonder whether there exist other maps, that are well defined for smaller characteristics, that share some properties with the exponential and that integrate nilpotent elements of $\mathrm{Lie}(G)$ into unipotent elements of G . The answer is known: such maps exist for not too small characteristics and are called Springer isomorphisms. They are named after T. A. Springer who introduced them in [Spr69]. Springer’s results have been widely studied and refined by many mathematicians, e.g. P. Bardsley and R. W. Richardson ([BR85]); J.-P. Serre with in particular an enlightening appendix in G. McNinch’s paper [McN05], G. McNinch for instance in a common paper with D. Testerman ([MT09]); S. Herpel ([Her13]) and P. Sobaje ([Sob15], [Sob18])¹⁵. These works have contributed to eventually determining optimal conditions for the existence of Springer isomorphisms. They also raise many questions, in particular that of the properties of the set of nilpotent elements of $\mathrm{Lie}(G)$.

3. CAN WE APPROXIMATE THE STRUCTURES?

Let us conclude with another question which is naturally raised here. So far this article has focused on analysing whether elements of affine group schemes G can be recovered from the local approximation that $\mathrm{Lie}(G)$ provides. But elements of both $\mathrm{Lie}(G)$ and G are not only isolated points: they interact with one another, respectively by means of the Lie algebra and the group laws. One can therefore ask whether the integration is compatible with these structures, namely, is the image of a Lie subalgebra¹⁶ of $\mathrm{Lie}(G)$ via a map that goes from (a Lie subalgebra of) $\mathrm{Lie}(G)$ ¹⁷ to G , a subgroup of G ?

In characteristic 0 this is well known for Lie subalgebras of G made of nilpotent elements. This comes from the fact that the exponential map allows to endow these Lie subalgebras with a multiplicative group law. Unfortunately, the situation is no longer that simple (neither well understood) if for instance one considers subalgebras made of diagonal matrices (as explained in a very recent preprint of H. Kraft and M. Zaidenberg [KZ22, §3]). In positive characteristic on the other hand, the situation gets even trickier and Lie subalgebras made of nilpotent elements don’t always correspond to unipotent subgroups of G . This was expected for really small characteristics when Springer isomorphisms are not defined, but even when the situation is more favourable integrating the structure is not always possible. This in particular comes from the fact that not any Springer isomorphism endows the Lie subalgebra one wants to integrate with a multiplicative group law. Moreover, characteristic $p > 0$ also

¹⁵The list of contributors and contributions is not exhaustive but this should give the reader a better idea of the richness of the literature on the subject.

¹⁶A subset of $\mathrm{Lie}(G)$ that inherits a Lie algebra structure from restricting that of $\mathrm{Lie}(G)$

¹⁷It might be defined only for nilpotent elements.

raises a geometric issue: smoothness questions that have been ignored in this article actually play a crucial role here. However, when the exponential map is well defined the situation “almost” looks like characteristic 0^{18} , as explained by J.-P. Serre ([Ser96])¹⁹. As for the remaining cases, the question has been studied for some very specific Lie algebras, but a lot is still to be done.

REFERENCES

- [BDP17] V. Balaji, P. Deligne, and A. J. Parameswaran. On complete reducibility in characteristic p . *Épjournal de Géométrie Algébrique*, Volume 1, 2017.
- [BR85] P. Bardsley and R. W. Richardson. Étale slices for algebraic transformation groups in characteristic p . *Proc. London Math. Soc. (3)*, 51(2):295–317, 1985.
- [Her13] S. Herpel. On the smoothness of centralizers in reductive groups. *Trans. Amer. Math. Soc.*, 365(7):3753–3774, 2013.
- [Jea21] M. Jeannin. Integration questions in separably good characteristics, 2021.
- [KZ22] H. Kraft and M. Zaidenberg. Algebraically generated groups and their lie algebras, 2022.
- [McN02] G. J. McNinch. Abelian unipotent subgroups of reductive groups. *J. Pure Appl. Algebra*, 167(2-3):269–300, 2002.
- [McN05] G. J. McNinch. Optimal $SL(2)$ -homomorphisms. *Comment. Math. Helv.*, 80(2):391–426, 2005.
- [MT09] G. J. McNinch and D. M. Testerman. Nilpotent centralizers and Springer isomorphisms. *J. Pure Appl. Algebra*, 213(7):1346–1363, 2009.
- [Sei00] G. M. Seitz. Unipotent elements, tilting modules, and saturation. *Inv. Math.*, 141(3):467–502, Sep 2000.
- [Ser96] J.-P. Serre. Exemples de plongements des groupes $PSL_2(\mathbb{F}_p)$ dans des groupes de Lie simples. *Invent. Math.*, 124(1-3):525–562, 1996.
- [Sob15] P. Sobaje. Springer isomorphisms in characteristic p . *Transform. Groups*, 20(4):1141–1153, 2015.
- [Sob18] P. Sobaje. Unipotent elements and generalized exponential maps. *Adv. Math.*, 333:463–496, 2018.
- [Spr69] T. A. Springer. The unipotent variety of a semi-simple group. In *Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968)*, pages 373–391. Oxford Univ. Press, London, 1969.

¹⁸In characteristic $p > 0$ only some subgroups made of unipotent elements can be obtained by integration of the Lie algebras consisting of nilpotent elements ([Jea21, Remarks 3.8]).

¹⁹One should also quote G. Seitz’s work [Sei00] as well as V. Balaji, P. Deligne and A. J. Parameswaran’s paper [BDP17].