ARITHMETIC DIFFERENTIAL EQUATIONS ON GL_n, II: ARITHMETIC LIE THEORY

ALEXANDRU BUIUM AND TAYLOR DUPUY

ABSTRACT. Motivated by the search of a concept of linearity in the theory of arithmetic differential equations [3] we introduce here an arithmetic analogue of Lie algebras and a concept of skew arithmetic differential cocycles. We will then construct such skew cocycles, based on certain remarkable lifts of Frobenius for the classical groups GL_n, SL_n, SO_n, Sp_n. The theory for GL_n, especially on the Galois side, will be further developed in a sequel to this paper [5].

1. INTRODUCTION AND MAIN RESULTS

This paper is, in principle, part of a series of papers [4, 5] but can be read independently of the other papers in the series. In this series of papers we seek answers to the question: what is the arithmetic analogue of linear differential equations? A general theory of arithmetic differential equations was introduced in [2, 3]; we will not assume here any familiarity with [2, 3] but let us recall that the idea in loc. cit. was to replace derivation operators with Fermat quotient operators. However the concept of linearity in this theory seems elusive and turns out to be subtle. A naive attempt, modeled on Kolchin's logarithmic derivative [8], would be to consider "classical differential cocycles" of GL_n into its Lie algebra $\mathfrak{gl}_n$; but it turns out [4] that, essentially, no such cocycles exist in the arithmetic context. To remedy the situation we will introduce here an arithmetic analogue of Lie algebras, skew versions of classical cocycles, and a notion of linearity for arithmetic differential equations. We will then construct such skew cocycles, based on certain special lifts of Frobenius for the classical groups GL_n, SL_n, SO_n, Sp_n. The existence results for these special lifts of Frobenius are the main results of the present paper. The "flows" attached to these lifts admit remarkable "prime integrals" and "symmetries" which will be used later in [5] when we discuss the Galois side of the theory.

To explain the main results of this paper let us quickly recall the δ-arithmetic setting of [2, 3]. We denote by R the unique complete discrete valuation ring with maximal ideal generated by an odd prime p and residue field $k = R/pR$ equal to the algebraic closure $\mathbb{F}_p^a$ of $\mathbb{F}_p$; then we denote by $\delta : R \to R$ the map

$$\delta x = \frac{\phi(x) - x^p}{p}$$

where $\phi : R \to R$ is the unique ring homomorphism lifting the p-power Frobenius on the residue field k. We refer to δ as a p-derivation; it is, of course, not a derivation. We denote by R^δ the monoid of constants $\{\lambda \in R; \delta\lambda = 0\}$; so R^δ consists of 0 and all roots of unity in R. Also we denote by K the fraction field of R. In this context we will consider smooth schemes of finite type X over R or, more generally, smooth p-formal schemes of finite type, by which we mean formal schemes locally

1

isomorphic to p-adic completions of smooth schemes of finite type; we denote by $X(R)$ the set of R-points of X; if there is no danger of confusion we often simply write X in place of $X(R)$. Groups in the category of smooth p-formal schemes will be called smooth group p-formal schemes.

A map $f : R^N \to R^M$ will be called a δ-map of order n if there exists an M-vector $F = (F_j)$, $F_j \in R[x_0, ..., x_n]\hat{}$ of restricted power series with coefficients in R in $n + 1$ N-tuples of variables $x_0, ..., x_n$, such that

$$(1.1) \qquad\qquad f(a) = F(a, \delta a, ..., \delta^n a), \quad a \in R^N.$$

One can then consider affine smooth schemes X, Y and define a map $f : X(R) \to Y(R)$ to be a δ-map of order n if there exist embeddings $X \subset \mathbb{A}^N$, $Y \subset \mathbb{A}^M$ such that f is induced by a δ-map $R^N \to R^M$ of order n; we simply write $f : X \to Y$. More generally if X is any smooth scheme and Y is an affine scheme a set theoretic map $X \to Y$ is called a δ-map of order n if there exists an affine cover $X = \bigcup X_i$ such that all the induced maps $X_i \to Y$ are δ-maps of order n. If G, H are smooth group schemes a δ-homomorphism $G \to H$ is, by definition, a δ-map which is also a homomorphism. An *arithmetic differential equation* (or simply a δ-*equation*) is an equation of the form $f(u) = 0$ where $f : X \to \mathbb{A}^N$ is a δ-map and $u \in X(R)$. We shall review these concepts, from a slightly different, but equivalent perspective, in section 2 following [2, 3].

In the present paper we will introduce the δ-*Lie algebra of an algebraic group, skew δ-cocycles, and δ-linear equations*. The theory will be introduced for arbitrary linear algebraic groups but here is how it looks in the case of GL_n and its subgroups. (The theory will be further pursued, especially from a Galois-theoretic viewpoint, in [5].)

The δ-Lie algebra of GL_n is defined as $\mathfrak{gl}_n$ equipped with the non-commutative group law $+_\delta : \mathfrak{gl}_n \times \mathfrak{gl}_n \to \mathfrak{gl}_n$ given by

$$a +_\delta b := a + b + pab,$$

where the addition and multiplication in the right hand side are those of $\mathfrak{gl}_n$, viewed as an associative ring. (This makes $\mathfrak{gl}_n$ a group p-formal scheme.) There is a natural "δ-adjoint" action $\star_\delta$ of GL_n on $\mathfrak{gl}_n$ given by

$$a \star_\delta b := \phi(a) \cdot b \cdot \phi(a)^{-1}.$$

In what follows, for a matrix $a = (a_{ij})$ with entries in R we set $a^{(p)} = (a_{ij}^p)$, $\phi(a) = (\phi(a_{ij}))$, $\delta a = (\delta a_{ij})$; so $\phi(a) = a^{(p)} + \delta a$. Consider the ring $\mathcal{O}(GL_n)\hat{} = R[x, \det(x)^{-1}]\hat{}$ where $x = (x_{ij})$ is a matrix of indeterminates, and $\hat{}$ denotes, as before, p-adic completion. Assume also that one is given a ring endomorphism ϕ_{GL_n} of $\mathcal{O}(GL_n)\hat{}$ lifting Frobenius, i.e. a ring endomorphism whose reduction mod p is the p-power Frobenius on $\mathcal{O}(GL_n)\hat{}/(p) = k[x, \det(x)^{-1}]$; we still denote by $\phi_{GL_n} : \widehat{GL_n} \to \widehat{GL_n}$ the induced morphism of p-formal schemes and we refer to it as a lift of Frobenius on $\widehat{GL_n}$. Consider the matrices $\Phi(x) = (\phi_{GL_n}(x_{ij}))$ and $x^{(p)} = (x_{ij}^p)$ with entries in $\mathcal{O}(GL_n)\hat{}$; then $\Phi(x) = x^{(p)} + p\Delta(x)$ where $\Delta(x)$ is some matrix with entries in $\mathcal{O}(GL_n)\hat{}$. Note that $\phi_{GL_n} : \widehat{GL_n} \to \widehat{GL_n}$ is not a morphism over R; nevertheless it induces naturally a map (still denoted by $\phi_{GL_n} : GL_n = GL_n(R) \to GL_n = GL_n(R)$) between the corresponding sets of points, via the formula $\phi_{GL_n}(a) = \phi^{-1}(\Phi(a))$, $a \in GL_n = GL_n(R)$. Furthermore given a lift

of Frobenius ϕ_{GL_n} as above one defines an operator

$$\delta_{GL_n} : \mathcal{O}(GL_n)\hat{\ } \to \mathcal{O}(GL_n)\hat{\ }, \quad \delta_{GL_n}(f) = \frac{\phi_{GL_n}(f) - f^p}{p},$$

referred to as the p-derivation associated to ϕ_{GL_n}.

Assume furthermore that we are given a smooth closed subgroup scheme $G \subset GL_n$. We say that G is ϕ_{GL_n}-horizontal if ϕ_{GL_n} sends the ideal of G into itself; in this case we have a lift of Frobenius endomorphism ϕ_G on $\widehat{G}$, equivalently on $\mathcal{O}(G)\hat{\ }$. (Note that given a smooth G there is always a lift of Frobenius ϕ_{GL_n} such that G is ϕ_{GL_n}-horizonal; this is a formal consequence of smoothness.) Furthermore δ_{GL_n} induces an operator $\delta_G : \mathcal{O}(G)\hat{\ } \to \mathcal{O}(G)\hat{\ }$ referred to as the p-derivation associated to ϕ_G.

Assume the ideal of G in $\mathcal{O}(GL_n)$ is generated by polynomials $f_i(x)$. Then recall that the Lie algebra $L(G)$ identifies, as an additive group, to the subgroup of the usual additive group $(\mathfrak{gl}_n, +)$ consisting of all matrices a satisfying

$$\text{``}\epsilon^{-1}\text{''} f_i(1 + \epsilon a) = 0,$$

where $\epsilon^2 = 0$. Let $f_i^{(\phi)}$ be the polynomials obtained from f_i by applying ϕ to the coefficients. Then we define the δ-Lie algebra $L_\delta(G)$ as the subgroup of $(\mathfrak{gl}_n, +_\delta)$ consisting of all the matrices $a \in \mathfrak{gl}_n$ satisfying

$$p^{-1} f_i^{(\phi)}(1 + pa) = 0;$$

in this formulation the factor p^{-1} is, of course, not necessary but scheme theoretically that factor will have to be there.

Note that $L_\delta(G)$ and $L(G)$ are not equal as subsets of $L(GL_n) = \mathfrak{gl}_n$. For instance if $G = SL_2 \subset GL_2$ then $L(SL_2) = \mathfrak{sl}_2$ consists of all $a \in \mathfrak{gl}_2$ with

$$\text{tr}(a) = 0$$

whereas $L_\delta(SL_2)$ consists of all $a \in \mathfrak{gl}_2$ such that

$$\text{tr}(a) + p \cdot \det(a) = 0.$$

Going back to the general situation, the analogue of Kolchin's logarithmic derivative will then be the map, referred to as the *arithmetic logarithmic derivative*,

$$l\delta : GL_n \to \mathfrak{gl}_n,$$

defined by

$$l\delta a := \frac{1}{p}\left(\phi(a)\Phi(a)^{-1} - 1\right) = (\delta a - \Delta(a))(a^{(p)} + p\Delta(a))^{-1}.$$

This is a δ-map of order 1. Note that $l\delta$ does not satisfy the cocycle condition but rather a condition which we shall call the *skew cocycle condition*; cf. the body of the paper. In particular $l\delta$ will satisfy the cocycle condition "modulo a term of order 0". For G a ϕ_{GL_n}-horizontal subgroup $l\delta$ above induces a δ-map of order 1

$$l\delta : G \to L_\delta(G).$$

Now any $\alpha \in L_\delta(G)$ defines an equation of the form

(1.2) $$l\delta u = \alpha,$$

with unknown $u \in G$; such an equation will be referred to as a δ_G-linear equation or a Δ-linear equation. A δ-equation on GL_n that is Δ-linear for some Δ will be simply called a δ-linear equation. Setting $\Delta^\alpha(x) = \alpha \cdot \Phi(x) + \Delta(x)$ and $\Phi^\alpha(x) =$

$x^{(p)} + p\Delta^\alpha(x) = \epsilon \cdot \Phi(x)$, where $\epsilon = 1 + p\alpha$, we see that Equation 1.2 is equivalent to the equation:

$$(1.3) \qquad\qquad\qquad \delta u = \Delta^\alpha(u)$$

and also to the equation

$$(1.4) \qquad\qquad\qquad \phi(u) = \Phi^\alpha(u).$$

Note that equation 1.4 is *not* a difference equation in the sense of [9]; indeed difference equations for ϕ have the form $\phi(u) = \alpha \cdot u$. Equations of the form 1.2 will be studied in some detail in [5]. Note that for any α as above one can attach a lift of Frobenius $\phi^\alpha_{GL_n}$ on $\widehat{GL_n}$ by the formula $\phi^\alpha_{GL_n}(x) = \Phi^\alpha(x)$; then its associated p-derivation $\delta^\alpha_{GL_n}$ satisfies $\delta^\alpha_{GL_n}(x) = \Delta^\alpha(x)$.

In order to implement the formalism above and obtain an interesting theory we need to construct lifts of Frobenius that satisfy certain compatibilities. We start by discussing compatibilities with subgroups. Let G be, as before, a smooth closed subgroup scheme of GL_n; let H be a smooth closed subgroup scheme of G. We say that ϕ_G is left compatible with H if H is ϕ_{GL_n}-horizontal and the following diagram is commutative:

$$(1.5) \qquad \begin{array}{ccc} \widehat{H} \times \widehat{G} & \to & \widehat{G} \\ \phi_H \times \phi_G \downarrow & & \downarrow \phi_G \\ \widehat{H} \times \widehat{G} & \to & \widehat{G} \end{array}$$

where $\phi_H : \widehat{H} \to \widehat{H}$ is induced by ϕ_G and the horizontal maps are given by multiplication. Similarly we say that ϕ_G is right compatible with H if H is ϕ_{GL_n}-horizontal and the right multiplication map fits into a commutative diagram

$$(1.6) \qquad \begin{array}{ccc} \widehat{G} \times \widehat{H} & \to & \widehat{G} \\ \phi_G \times \phi_H \downarrow & & \downarrow \phi_G \\ \widehat{G} \times \widehat{H} & \to & \widehat{G} \end{array}$$

We say ϕ_G is bicompatible with H if it is both left and right compatible with H.

Finally let us discuss compatibility of lifts of Frobenius with "quadratic maps". By an involution on G we understand a morphism of schemes $\dagger : G \to G$ over R, $x \mapsto x^\dagger$, such that $x^{\dagger\dagger} = x$ and $(xy)^\dagger = y^\dagger x^\dagger$. By a quadratic map on G we mean a morphism of schemes $\mathcal{H} : G \to G$ over R such that there exists an involution $\dagger : G \to G$ and an element $q \in G$ with the property that

$$\mathcal{H}(x) = x^\dagger q x.$$

Note that $\dagger$ and q are determined by $\mathcal{H}$; indeed we have $q = \mathcal{H}(1)$ and $x^\dagger = \mathcal{H}(x)x^{-1}\mathcal{H}(1)^{-1}$. Given a quadratic map $\mathcal{H}$ one can define a map

$$(1.7) \qquad \mathcal{H}_2 : G \times G \to G, \quad \mathcal{H}_2(x,y) = \mathcal{H}(x)x^{-1}y = x^\dagger q y.$$

One can also define a closed subgroup scheme S of G as the connected component $\mathcal{H}^{-1}(q)^\circ$ of the group scheme $\mathcal{H}^{-1}(q)$; we say that S is defined by $\mathcal{H}$.

Let us fix now a lift of Frobenius $\phi_{G,0}$ on $\widehat{G}$ such that q is $\phi_{G,0}$-horizontal (i.e. the ideal of q in $\mathcal{O}(G)\hat{}$ is sent by $\phi_{G,0}$ into itself); all the concepts below will depend on the choice of this $\phi_{G,0}$. We say that a lift of Frobenius ϕ_G on $\widehat{G}$ is horizontal

with respect to $\mathcal{H}$ if the following diagram is commutative:

$$(1.8) \qquad \begin{array}{ccc} \widehat{G} & \xrightarrow{\phi_G} & \widehat{G} \\ \mathcal{H} \downarrow & & \downarrow \mathcal{H} \\ \widehat{G} & \xrightarrow{\phi_{G,0}} & \widehat{G} \end{array}$$

We say that a lift of Frobenius ϕ_G on $\widehat{G}$ is symmetric with respect to $\mathcal{H}$ if the following diagram is commutative:

$$(1.9) \qquad \begin{array}{ccc} \widehat{G} & \xrightarrow{\phi_{G,0} \times \phi_G} & \widehat{G} \times \widehat{G} \\ \phi_G \times \phi_{G,0} \downarrow & & \downarrow \mathcal{H}_2 \\ \widehat{G} \times \widehat{G} & \xrightarrow{\mathcal{H}_2} & \widehat{G} \end{array}$$

Note that if ϕ_G is horizontal with respect to $\mathcal{H}$ and q is $\phi_{G,0}$-horizontal then the group S defined by $\mathcal{H}$ is ϕ_G-horizontal; in particular there is an induced lift of Frobenius ϕ_S on $\widehat{S}$. Also note that in the special case when $G = GL_n$ and $\phi_{GL_n,0}(x) = x^{(p)}$, viewing $\mathcal{H}$ as a matrix $\mathcal{H}(x)$ with entries in $R[x, \det(x)^{-1}]^{\wedge}$, we have that the commutativity of 1.8 is equivalent to the condition that

$$\delta_{GL_n} \mathcal{H} = 0,$$

which can be interpreted as saying that $\mathcal{H}$ is a *prime integral*.

The basic split classical groups GL_n, SO_n, Sp_n are defined by quadratic maps as follows. For all these groups we take $G = GL_n$ and $\phi_{G,0}(x) = x^{(p)}$. Now GL_n itself is defined by $\mathcal{H}(x) = 1$; in this case $x^{\dagger} = x^{-1}$, $q = 1$. We call $\mathcal{H}$ the canonical quadratic map defining GL_n.

The groups $Sp_{2r}, SO_{2r}, SO_{2r+1}$ are defined by $\mathcal{H}(x) = x^t q x$ where q is equal to

$$(1.10) \qquad \begin{pmatrix} 0 & 1_r \\ -1_r & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1_r \\ 1_r & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1_r \\ 0 & 1_r & 0 \end{pmatrix},$$

$n = 2r, 2r, 2r + 1$ respectively, $x^{\dagger} = x^t$ is the transpose, and 1_r is the $r \times r$ identity matrix. We call this $\mathcal{H}$ the canonical quadratic map defining $Sp_{2r}, SO_{2r}, SO_{2r+1}$ respectively. All these groups are smooth over R.

For SL_n we need to assume that $p \nmid n$ and we take

$$(1.11) \qquad G := GL_n^* := \{ \begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix} \in GL_{n+1}; \ x \in GL_n, \ t \in \mathbb{G}_m, \ \det(x)^2 = t^n \};$$

note that projection $\pi : G \to GL_n$ onto the a component is an étale homomorphism. In particular any lift of Frobenius on $\widehat{GL_n}$ can be extended uniquely to a lift of Frobenius on $\widehat{G}$. Consider the involution $\dagger = *$ on G defined by

$$(1.12) \qquad \begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix}^* = \begin{pmatrix} tx^{-1} & 0 \\ 0 & t \end{pmatrix}$$

and define the quadratic map

$$(1.13) \qquad \mathcal{H} \begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix}^* \begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} t \cdot 1 & 0 \\ 0 & t^2 \end{pmatrix}.$$

So the group $\mathcal{H}^{-1}(1)^{\circ}$ defined by $\mathcal{H}$ projects isomorphically onto SL_n via $\pi : G \to GL_n$. We will say, by abuse of terminology, that SL_n is defined by $\mathcal{H}$ and we call $\mathcal{H}$ the canonical quadratic map defining SL_n. Furthermore let us equip $\widehat{G}$ with the unique lift of Frobenius $\phi_{G,0}$ extending the lift of Frobenius $\phi_{GL_n,0}$ on $\widehat{GL_n}$. We

will say that a lift of Frobenius ϕ_{GL_n} on $\widehat{GL_n}$ is horizontal (respectively symmetric) with respect to $\mathcal{H}$ if the unique extension ϕ_G of ϕ_{GL_n} to $\widehat{G}$ is horizontal (respectively symmetric) with respect to $\mathcal{H}$.

In what follows we let $T \subset GL_n$ be the maximal torus of diagonal matrices and we let $W \subset GL_n$ be the Weyl subgroup of GL_n of all permutation matrices. Here is our main result.

Theorem 1.1. *Let $\mathcal{H}$ be the canonical quadratic map defining GL_n, SL_n, SO_n, Sp_n and let S be any of these groups. Then the following hold.*

1) There exists a unique lift of Frobenius $\phi_{GL_n} = \phi_{GL_n,\mathcal{H}}$ on $\widehat{GL_n}$ that is horizontal and symmetric with respect to $\mathcal{H}$.

2) ϕ_{GL_n} is right compatible with T and W; also ϕ_{GL_n} is left compatible with $T_S := T \cap S$ and $W_S := W \cap S$; in particular the lift of Frobenius ϕ_S on $\widehat{S}$ induced by ϕ_{GL_n} is bicompatible with T_S and W_S.

3) ϕ_{GL_n} and $\phi_{GL_n,0}$ coincide on the set $S \cap \phi_{GL_n,0}^{-1}(S)$.

4) If $l\delta : S \to L_\delta(S)$ is the arithmetic logarithmic derivative associated to ϕ_S then for all $a \in S$ and all $b \in T_S W_S$ we have

$$l\delta(ab) = a \star_\delta l\delta(b) +_\delta l\delta(a).$$

5) Let $\mathcal{H}^* = \mathcal{H}$ if $S = GL_n, SO_n, Sp_n$ and $\mathcal{H}^* = \det(x)$ if $S = SL_n$. Then, for any $\alpha \in L_\delta(S)$, we have

$$\delta_{GL_n}^\alpha (\mathcal{H}^*) = 0.$$

Cf. Propositions 4.5, 4.10, 4.13, where non-split versions of SO_n, Sp_n are also considered.

Remark 1.2. Assertion 5 above can be interpreted as implying that for $\alpha \in L_\delta(S)$, the components of $\mathcal{H}^*$ are *prime integrals* of the equation $\delta u = \Delta^\alpha(u)$. For more on this see Remark 2.4 below and [5]. Note also that $\mathcal{H}$ can be viewed as an analogue of classical Hamiltonian functions while the p-derivation $\delta_{GL_n,\mathcal{H}}$ associated to the lift of Frobenius $\phi_{GL_n} = \phi_{GL_n,\mathcal{H}}$ in our Theorem can be viewed as an analogue of the Hamiltonian vector field associated to a Hamiltonian function in classical mechanics. It would be interesting to pursue this analogy further, especially in terms of the formal "commutation" relations involved, in the style of a Poisson formalism.

Remark 1.3. Note also that assertion 3 in Theorem 1.1 trivially implies that for any $\phi_{GL_n,0}$-horizontal smooth closed subscheme $X \subset GL_n$ which is contained in S we have that X is also ϕ_{GL_n}-horizontal and the restrictions of $\phi_{GL_n,0}$ and ϕ_{GL_n} to $\widehat{X}$ coincide. On the other hand it turns out that (with the exception of $S = SO_n$ with n odd and χ a "shortest root" of that group) for any root χ of $S = GL_n, SL_n, SO_n, Sp_n$ the additive group U_χ attached to χ is $\phi_{GL_n,0}$-horizontal and there is an isomorphism $U_\chi \simeq \mathbb{G}_a$ such that the lift of Frobenius on $\widehat{\mathbb{G}_a} = Spf\ R[z]\hat{}$ induced by $\phi_{GL_n,0}$ is given by $z \mapsto z^p$. So by 3) above any such U_χ is also ϕ_{GL_n}-horizontal and for any such U_χ the lift of Frobenius on $\widehat{\mathbb{G}_a} = Spf\ R[z]\hat{}$ induced by ϕ_{GL_n} is given by $z \mapsto z^p$. Cf. the body of the paper for a review of terminology related to roots.

In [5] we will further investigate the case of $S = GL_n$. This is the only case among the classical groups we study for which the lift of Frobenius is defined by polynomials (rather than restricted power series). This makes the $S = GL_n$ case

amenable to usual algebraic geometric (rather than analytic) methods. Finally note that 4) in the theorem follows formally from 1) and 2); by the way 4) will be the starting point of the study of symmetries of solutions to δ-linear equations [5].

The present paper is organized as follows. Section 2 reviews some of the basic concepts in [2, 3] and adds some complements to them. In section 3 we introduce arithmetic Lie theory, i.e. δ-Lie algebras, skew δ-cocycles, and δ-linear equations for arbitrary groups. In section 4 we specialize to the classical groups and we prove Theorem 1.1.

2. REVIEW OF p-JETS

This section is devoted to reviewing some of the material in [2, 3, 7].

For any ring A we denote by $\widehat{A}$ the p-adic completion of A. Similarly for any scheme X of finite type over R we denote by $\widehat{X}$ the p-adic completion of X. A p-formal scheme (respectively a p-formal scheme of finite type over a base ring) is a formal scheme locally isomorphic to the p-adic completion of a Noetherian scheme (respectively of a scheme of finite type over the base ring). If $u : A \to B$ is a ring homomorphism we usually still denote by $u : Spec\ B \to Spec\ A$ the induced map; and conversely if $f : X \to Y$ is a morphism of schemes we still denote by $f : \mathcal{O}_Y \to f_*\mathcal{O}_X$ the induced morphism on functions.

A lift of Frobenius on a ring A will mean a ring homomorphism $\phi = \phi_A : A \to A$ whose reduction mod p is the p-power Frobenius $A/pA \to A/pA$; if A is p-torsion free we can attach to such a ϕ the operator

$$\delta = \delta_A : A \to A, \quad \delta a = \frac{\phi(a) - a^p}{p}$$

referred to as the *p-derivation* attached to ϕ; this was viewed in [2, 3] as an arithmetic analogue of a derivation.

A lift of Frobenius on a scheme (or p-formal scheme) X will mean a morphism of schemes (or p-formal schemes respectively) $\phi = \phi_X : X \to X$ whose reduction mod p is the p-power Frobenius; if X is a p-formal scheme and $\mathcal{O}_X$ is p-torsion free the above construction globalizes to yield an operator $\delta = \delta_X : \mathcal{O}_X \to \mathcal{O}_X$ referred to as the *p-derivation* attached to ϕ_X. If $f \in \mathcal{O}(X)$ is a global function then we say f is δ_X-constant if $\delta_X f = 0$; equivalently if $\phi_X(f) = f^p$. If X is a scheme and $\phi_{\widehat{X}}$ is a lift of Frobenius on $\widehat{X}$ we usually denote $\phi_{\widehat{X}}$ and $\delta_{\widehat{X}}$ simply by ϕ_X and δ_X respectively.

If $\pi : X \to Y$ is a morphism of schemes (or p-formal schemes) and X, Y are given lifts of Frobenius ϕ_X, ϕ_Y we say that π is horizontal (with respect to ϕ_X, ϕ_Y) if the following diagram commutes

$$\begin{array}{ccc} X & \xrightarrow{\pi} & Y \\ \phi_X \downarrow & & \downarrow \phi_Y \\ X & \xrightarrow{\pi} & Y \end{array}$$

If $Z \subset X$ is a closed subscheme (or closed p-formal subscheme) and we are given a lift of Frobenius ϕ_X we say Z is ϕ_X-horizontal if there exists a (necessarily unique)

lift of Frobenius ϕ_Z such that $Z \subset X$ is horizontal. If all the objects above are p-torsion free then we have at our disposal attached p-derivations and we sometimes say "δ_X-horizontal" instead of "ϕ_X-horizontal".

Recall from the introduction that R denotes, for us, the complete discrete valuation ring with maximal ideal generated by an odd prime p and algebraically closed residue field $k = \mathbb{F}_p^a$. Then R comes equipped with a unique lift of Frobenius $\phi = \phi_R : R \to R$. If X is a scheme (or a p-formal scheme) over R then lifts of Frobenius $\phi_X : X \to X$ will always be assumed to be such that $X \to Spec\, R$ is horizontal with respect to ϕ_X, ϕ_R; in particular ϕ_X in not a morphism of R-schemes. Nevertheless there is a naturally induced map between R-points, which we will still denote by $\phi_X : X(R) \to X(R)$, that sends a point $P : Spec\, R \to X$ into the R-point

$$\phi_X(P) := \phi_X \circ P \circ \phi_R^{-1} : Spec\, R \to Spec\, R \to X \to X;$$

the map $\phi_X : X(R) \to X(R)$ is, of course, not regular and it is not even a δ-map in the sense of [2, 3]; see below. Indeed, in case, say, $X = \mathbb{A}^1 = Spec\, R[x]$, if $\phi_X(x) = \Phi(x) \in R[x]\hat{\ }$ and $P \in \mathbb{A}^1(R) \simeq R$ corresponds to $a \in R$ then $\phi_X(P) \in \mathbb{A}^1(R) \simeq R$ corresponds to $\phi_R^{-1}(\Phi(a)) \in R$. Going back to the general case of a smooth scheme (or p-formal scheme) X recall from the Introduction that we usually continue to denote by X the set $X(R)$ of R-points of X. If $Y \subset X$ is a closed smooth subscheme (respectively p-formal scheme) then it is trivial to check that Y is ϕ_X-horizontal if and only if for all R-points $P \in Y$ one has $\phi_X(P) \in Y$. (The latter is an easy exercise using Nullstellensatz over k and the surjectivity of $Y(R) \to Y(k)$.) Also two lifts of Frobenius on a smooth $\widehat{X}$ coincide if and only if the corresponding maps on points coincide. We will later need the following trivial:

Lemma 2.1. *Let $Z \subset Y \subset X$ be closed embeddings of smooth schemes and let $\phi_{X,0}$ and $\phi_{X,1}$ be two lifts of Frobenius on $\widehat{X}$. Assume that Z is $\phi_{X,0}$-horizontal and that $\phi_{X,0}$ and $\phi_{X,1}$ coincide on the set $Y \cap \phi_{X,0}^{-1}(Y)$. Then Z is also $\phi_{X,1}$-horizontal and the restrictions of $\phi_{X,0}$ and $\phi_{X,1}$ to Z coincide.*

Proof. It is enough to show that for any point $P \in Z$ we have $\phi_{X,1}(P) \in Z$ and $\phi_{X,1}(P) = \phi_{X,0}(P)$. Since Z is $\phi_{X,0}$-horizontal we have $\phi_{X,0}(P) \in Z$. So $P \in Y \cap \phi_{X,0}^{-1}(Y)$. Hence $\phi_{X,1}(P) = \phi_{X,0}(P) \in Z$ and we are done. $\square$

Next we review p-jet spaces. We follow closely the discussion in [4]. For x a tuple of indeterminates over R and tuples of indeterminates $x', ..., x^{(n)}, ...$ we let $R\{x\} = R[x, x', x'', ...]$ and we still denote by $\phi : R\{x\} \to R\{x\}$ the unique lift of Frobenius extending ϕ on R such that $\phi(x) = x^p + px'$, $\phi(x') = x^p + px''$, etc. Then we consider the *total p-derivative* operator $\delta : R\{x\} \to R\{x\}$ defined by

$$\delta f = \frac{\phi(f) - f^p}{p}.$$

Now for any affine scheme of finite type

$$X = Spec\, \frac{R[x]}{(f)}$$

over R, where f is a tuple of polynomials, we define the p-jet spaces of X as being the p-formal schemes

$$(2.1) \qquad\qquad J^n(X) = Spf\, \frac{R[x, x', ..., x^{(n)}]\hat{\ }}{(f, \delta f, ..., \delta^n f)}$$

For X of finite type but not necessarily affine we define $J^n(X) = \bigcup J^n(X_i)$ where $X = \bigcup X_i$ is an affine cover and the gluing is an obvious one. The spaces $J^n(X)$ have an obvious universality property for which we refer to [2, 3] and can be defined for X a p-formal scheme of finite type as well. If X/R is smooth then $J^n(X)$ is locally the p-adic completion of a smooth scheme. The universality property yields natural maps on sets of R-points $\nabla^n : X(R) \to J^n(X)(R)$; for $X = \mathbb{A}^m$ (the affine space), $J^n(X) = \mathbb{A}^{m(n+1)}$ and $\nabla^n(a) = (a, \delta a, ..., \delta^n a)$. Let X, Y be schemes of finite type over R; by a δ-map (of order n) $f : X \to Y$ we understand a map of p-formal schemes $J^n(X) \to J^0(Y) = \widehat{Y}$. Two δ-maps $X \to Y$ and $Y \to Z$ of orders n and m respectively can be composed (using the universality property) to yield a δ-map of order $n + m$. Any δ-map $f : X \to Y$ induces a set theoretic map $f_* : X(R) \to Y(R)$ defined by $f_*(P) = f(\nabla^n(P))$; if X, Y are smooth the map f_* uniquely determines the map f and, in this case, we simply write f instead of f_* (and X, Y instead of $X(R), Y(R)$). A δ-map $X \to Y$ of order zero is nothing but a map of p-formal schemes $\widehat{X} \to \widehat{Y}$. The functors J^n commute with products and send groups into groups. By a δ-homomorphism $f : G \to H$ between two group schemes (or group p-formal schemes) we understand a group homomorphism $J^n(G) \to J^0(H) = \widehat{H}$.

We end by discussing the formalism of flows and prime integrals, following [7]. Let X be a an affine smooth scheme over R. A system of arithmetic differential equations of order r is simply a subset $\mathcal{E}$ of $\mathcal{O}(J^r(X))$. By a solution of $\mathcal{E}$ we mean an R-point $P \in X$ such that $f(P) = 0$ for all $f \in \mathcal{E}$. We denote by $Sol(\mathcal{E}) \subset X$ the set of solutions of $\mathcal{E}$. By a prime integral of $\mathcal{E}$ we mean a function $\mathcal{H} \in \mathcal{O}(X)\hat{\ }$ such that $\delta(\mathcal{H}(P)) = 0$ for all $P \in Sol(\mathcal{E})$. (Intuitively $\mathcal{H}$ is "constant along the solutions of $\mathcal{E}$".)

Let now δ_X be a p-derivation on $\mathcal{O}(X)\hat{\ }$. Then one can define a system of arithmetic differential equations of order 1, $\mathcal{E}(\delta_X) \subset \mathcal{O}(J^1(X))$, which we can refer to as the δ-*flow* associated to δ_X; by definition we take $\mathcal{E}(\delta_X)$ to be the ideal in $\mathcal{O}(J^1(X))$ generated by all elements of the form $\delta f - \delta_X f$ where $f \in \mathcal{O}(X)\hat{\ }$. (Here $\delta : \mathcal{O}(X)\hat{\ } \to \mathcal{O}(J^1(X))$ while $\delta_X : \mathcal{O}(X)\hat{\ } \to \mathcal{O}(X)\hat{\ } \subset \mathcal{O}(J^1(X))$.) By a δ-flow on X we wil understand an ideal in $\mathcal{O}(J^1(X))$ of the form $\mathcal{E}(\delta_X)$ where δ_X is some p-derivation on $\mathcal{O}(X)\hat{\ }$. We have natural bijections

$$\{\delta\text{-flows on } X\} \simeq \{p\text{-derivations on } \mathcal{O}(X)\hat{\ }\} \simeq \{\text{sections of } J^1(X) \to \widehat{X}\}.$$

If δ_X is a p-derivation on $\mathcal{O}(X)\hat{\ }$ and $\sigma : \widehat{X} \to J^1(X)$ is the corresponding section then the ideal $\mathcal{E}(\delta_X)$ equals the ideal of the image of σ.

Lemma 2.2. *Let $\mathcal{O}(X) = (R[x_1, ..., x_n]/I)_g$ for indeterminates $x_1, ..., x_n$ and some $g \in R[x_1, ..., x_n]$ and let us continue to denote by $x_i \in \mathcal{O}(X)\hat{\ }$ the images of x_i. Then the elements*

$$(2.2) \qquad\qquad \delta x_i - \delta_X x_i, \quad i = 1, ..., n$$

generate the ideal $\mathcal{E}(\delta_X)$. In particular

$$Sol(\mathcal{E}(\delta_X)) = Sol(\delta x_1 - \delta_X x_1, ..., \delta x_n - \delta_X x_n).$$

Proof. Denote by $\mathcal{F}$ the ideal of $\mathcal{O}(J^1(X))$ generated by the elements 2.2 and consider the set

$$\mathcal{A} = \{f \in \mathcal{O}(X)\hat{\ }; \delta f - \delta_X f \in \mathcal{F}\}.$$

Then $\mathcal{A}$ is easily checked to be a subring of $\mathcal{O}(X)\hat{\ }$ and it clearly contains R and $\tilde{x}_i$ for all i. It also contains the image of $1/g$ because

$$\delta\left(\frac{1}{g}\right) - \delta_X\left(\frac{1}{g}\right) = -\frac{\delta g - \delta_X g}{(g^p + p\delta g)(g^p + p\delta_X g)}.$$

By Noetherianity $\mathcal{F}$ is p-adically closed in $\mathcal{O}(J^1(X))$ so $\mathcal{A}$ is p-adically closed in $\mathcal{O}(X)$; so it must coincide with $\mathcal{O}(X)\hat{\ }$. $\square$

Lemma 2.3. *If $\mathcal{H} \in \mathcal{O}(X)\hat{\ }$ is such that $\delta_X \mathcal{H} = 0$ then $\mathcal{H}$ is a prime integral for $\mathcal{E}(\delta_X)$.*

Proof. Indeed if $P \in Sol(\mathcal{E}(\delta_X))$ then

$$0 = (\delta\mathcal{H} - \delta_X\mathcal{H})(P) = (\delta\mathcal{H})(P) - (\delta_X\mathcal{H})(P) = (\delta\mathcal{H})(P).$$

$\square$

Remark 2.4. In the terminology above, any Δ-linear equation $\delta u = \Delta^\alpha(u)$, cf. 1.3, may be identified with the system of arithmetic differential equations on GL_n,

(2.3) $\delta x_{ij} - \Delta_{ij}^\alpha(x), \quad i, j = 1, ..., n,$

where $(\Delta_{ij}^\alpha(x)) = \Delta^\alpha(x)$, and hence, by Lemma 2.2, it has the same solution set as the δ-flow $\mathcal{E}(\delta_{GL_n}^\alpha)$ on GL_n, where $\delta_{GL_n}^\alpha(x) = \Delta^\alpha(x)$. Moreover any δ-flow arises in this manner for some Δ and α (and indeed from a whole family of pairs (Δ, α)). If one fixes Δ and varies α then one gets a whole family of δ-flows corresponding to all possible Δ-linear equations. Also note that, by Lemma 2.3, for any $\mathcal{H} \in \mathcal{O}(GL_n)\hat{\ }$ with $\delta_X \mathcal{H} = 0$ we have that $\mathcal{H}$ is a prime integral of the system 2.3. This leads one to interpret assertion 5 in Theorem 1.1 as saying that $\mathcal{H}^*$ in that assertion is a prime integral for the equation $\delta u = \Delta^\alpha(u)$ in the sense that $\delta(\mathcal{H}^*(u)) = 0$ for any solution of that equation.

3. ARITHMETIC LIE THEORY

In this section we introduce δ-Lie algebras, skew δ-cocycles, and δ-linear equations for arbitrary group schemes. The case of classical groups will be analyzed in the next section.

Definition 3.1. Let G be a smooth group scheme over R (or more generally a group p-formal scheme). The δ-Lie algebra of G is the group p-formal scheme:

$$L_\delta(G) := Ker(J^1(G) \to J^0(G)).$$

Remark 3.2. This construction is obviously functorial in the following sense: if $u : G \to H$ is a homomorphism of group schemes (or group p-formal schemes) then we have an induced homomorphism of group p-formal schemes $L_\delta(u) : L_\delta(G) \to L_\delta(H)$.

Remark 3.3. If $L(G)$ is the Lie algebra of G (viewed as a vector group scheme) then we have a (non-canonical!) isomorphism of p-formal schemes

$$L_\delta(G) \simeq \widehat{L(G)};$$

cf. [2]. This is not an isomorphism of groups in general; indeed $L(G)$ is always commutative whereas $L_\delta(G)$ is commutative if and only if G is commutative.

Remark 3.4. One can introduce an analogue of the Lie bracket on $L_\delta(G)$; we will not need this concept in what follows so we will refrain from introducing it here.

In what follows we freely use our convention that if X is a scheme (or a p-formal scheme) of finite type we denote its set $X(R)$ of R-points simply by X; in particular we write $a \in X$ instead of $a \in X(R)$. We also identify, as usual, the δ-maps $X \to Y$ with the maps between the sets of R-points. Note that if X is a smooth R-scheme then $\widehat{X}(R) \simeq X(R)$; so, according to our conventions, both these sets will sometimes be denoted simply by X.

Consider in what follows the morphism $G \times G \to G$ which on R-points acts as $(g, h) \mapsto ghg^{-1}$, $g, h \in G$. We get an obvious induced morphism of p-formal schemes (i.e. δ-map of order 0) $J^1(G) \times J^1(G) \to J^1(G)$ which, by restriction, yields a δ-map of order 0

$$(3.1) \qquad \star : J^1(G) \times L_\delta(G) \to L_\delta(G),$$

which is, of course, an action that can be referred to as the adjoint action. Now the identity $J^1(G) \to J^1(G)$ defines a δ-homomorphism of order 1,

$$\nabla^1 : G \to J^1(G).$$

We get an induced δ-map of order 1,

$$(3.2) \qquad \nabla^1 \times id : G \times L_\delta(G) \to J^1(G) \times L_\delta(G).$$

Composing 3.2 with 3.1 we get a δ-map of order 1,

$$(3.3) \qquad \star_\delta : G \times L_\delta(G) \to L_\delta(G)$$

which is an action that we call the δ-adjoint action. (By the way one has a similar construction in the δ-algebraic setting; in this case the resulting action has order 0 and is the usual adjoint action; cf. [1].)

Here is another basic construction. Denote by $\mathcal{F}(G)$ the set of δ-flows on G; we identify δ-flows on G with sections $\sigma : \widehat{G} \to J^1(G)$ in the category of p-formal schemes of the projection $J^1(G) \to \widehat{G}$. (Here σ are not group homomorphisms in general!) Then $\mathcal{F}(G)$ is acted upon, via left multiplication, by the group $L_\delta(G)(G)$ of p-formal scheme maps $\widehat{G} \to L_\delta(G)$; of course $\mathcal{F}(G)$ is a principal homogeneous space for this action so it is either empty or in bijection with $L_\delta(G)(G)$. On the other hand the group $L_\delta(G) = L_\delta(G)(R)$ acts via left multiplication on $\mathcal{F}(G)$. So if one fixes, once and for all, a section $\sigma_G \in \mathcal{F}(G)$ then we have a natural identification

$$L_\delta(G) \backslash L_\delta(G)(G) \simeq L_\delta(G) \backslash \mathcal{F}(G).$$

The orbits of $L_\delta(G)$ on $L_\delta(G)(G)$ and $\mathcal{F}(G)$ respectively can be referred to as *linear equivalence classes*.

Assume now in addition that G is affine. Then, by smoothness, there exists a lift of Frobenius $\phi_G : \mathcal{O}(G)\hat{} \to \mathcal{O}(G)\hat{}$ extending $\phi : R \to R$ (and not necessarily compatible with the comultiplication); one can attach to ϕ_G the p-derivation $\delta_G : \mathcal{O}(G)\hat{} \to \mathcal{O}(G)\hat{}$ defined by

$$\delta_G(f) = p^{-1}(\phi_G(f) - f^p).$$

The latter induces (and is actually equivalent to giving) a section $\sigma_G : \widehat{G} \to J^1(G)$ of the projection $J^1(G) \to \widehat{G}$ in the category of p-formal schemes. Fix from now on ϕ_G (equivalently δ_G or σ_G.) We may then consider the δ-map of order 0,

$$\{\ ,\ \}_G : \widehat{G} \times \widehat{G} \to L_\delta(G)$$

which on R-points is given by:

$$\{\ ,\ \}_G : G \times G \to L_\delta(G), \quad \{a,b\}_G = \sigma_G(a)\sigma_G(b)\sigma_G(ab)^{-1}.$$

Recall that by a δ_G-horizontal (or ϕ_G-horizontal) subgroup scheme of G we understand a smooth closed subgroup scheme $H \subset G$ such that the ideal I_H of $\widehat{H}$ in $\mathcal{O}(G)\hat{}$ satisfies $\delta_G(I_H) \subset I_H$; the latter is equivalent to $\phi_G(I_H) \subset I_H$ (due to the flatness of H). The indices G in $\phi_G, \delta_G, \sigma_G, \{\ ,\ \}_G$ are not meant to indicate that these objects are attached in any natural way to G; rather the index is meant to suggest that these objects are to be considered as part of the data whenever G is being considered. Dropping the index G from ϕ_G, δ_G would create confusion even if the reference to G was clear, because ϕ and δ have other meanings; but we will often drop the index G from $\sigma_G, \{\ ,\ \}_G$ whenever the reference to G is clear.

Definition 3.5. A δ-map $f : G \to L_\delta(G)$ is called a skew δ-cocycle if it satisfies

$$f(ab) = (a \star_\delta f(b)) \cdot f(a) \cdot \{a,b\}$$

for all $a, b \in G$. We say f is δ-coherent if for any δ_G-horizontal closed subgroup scheme $H \subset G$ we have that $f(H) \subset L_\delta(H)$.

If f is a fixed skew δ-cocycle then we set

$$G^f = \{b \in G; f(b) = 1\}.$$

This is not a subgroup of G in general. For all $a \in G$ and all $b \in G^f$ with $\{a,b\} = 1$ we have $f(ab) = f(a)$. Consider the δ-map of order 1,

$$l\delta : G \to L_\delta(G)$$

given on R-points by

$$l\delta(a) = \nabla^1(a)\sigma(a)^{-1},\ a \in G$$

(operations performed in $J^1(G)$). This δ-map is easily seen to be a skew δ-coherent δ-cocycle and will be referred to as the *arithmetic logarithmic derivative* attached to ϕ_G. We view this as an analogue of Kolchin's logarithmic derivative. In view of the Remark above for any $b \in G^{l\delta}$ with $\{a,b\} = 1$ we have $l\delta(ab) = l\delta(a)$.

Definition 3.6. Let G be a smooth affine group scheme equipped with a lift of Frobenius ϕ_G and let $\alpha \in L_\delta(G)$. Then the equality

$$l\delta(u) = \alpha$$

will be referred to as a δ_G-linear equation with unknown $u \in G$.

Finally, let us discuss compatibility with subgroups. There are two types of compatibilities we would like to look at: compatibilities with left and right multiplication from subgroups; and compatibilities with quadratic maps. We start with the first type of compatibility. Recall from the Introduction the following:

Definition 3.7. Let $H \subset G$ be a smooth closed subgroup scheme. We say that ϕ_G (or, equivalenty δ_G) is left compatible with H if H is δ_G-horizontal and the diagram 1.5 is commutative. We say that ϕ_G (or, equivalenty δ_G) is right compatible with H if H is δ_G-horizontal and the diagram 1.6 is commutative. We say that ϕ_G is bicompatible with H if it is both left and right compatible with H. Note that the vertical maps in the diagrams 1.5 and 1.6 are morphisms of formal schemes over $\mathbb{Z}_p$ and not over R!

Remark 3.8. By a split torus over R we will understand a group scheme of the form $T = Spec\ R[t_1, t^{-1}, ..., t_n, t_n^{-1}]$ with t_i group like. There is exactly one lift of Frobenius ϕ_T on $\mathcal{O}(T)^{\hat{}}$ which is bicompatible with T itself. This ϕ_T acts as $\phi_T(t_i) = t_i^p$.

Remark 3.9. By a finite constant group scheme over R we will understand a group scheme which is a disjoint union W of schemes $Spec\ R$ indexed by some finite abstract group, with the obvious structure of group scheme. Any finite constant group scheme W has exactly one lift of Frobenius on $\mathcal{O}(W)^{\hat{}} = R \times ... \times R$ which is the identity on the topological space. Clearly this lift of Frobenius is bicompatible with W itself.

Lemma 3.10. *If ϕ_G is bicompatible with H then $\{a,b\}_G = 1$ whenever a and b are in G and either a or b is in H. In particular*

$$l\delta(ab) = (a \star_\delta l\delta(b)) \cdot l\delta(a)$$

for all $a \in G$ and $b \in H$.

Proof. Clear from the definitions. $\square$

Next we discuss compatibility with quadratic maps. Recall from the Introduction the following:

Definition 3.11. Let G be an affine smooth group scheme over R equipped with a lift of Frobenius $\phi_{G,0}$. By a quadratic map on G we mean a morphism of R-schemes $\mathcal{H} : G \to G$ of the form $\mathcal{H}(x) = x^\dagger q x$ where where $\dagger$ is an involution of G and $q \in G$ is a $\phi_{G,0}$-horizontal point. Given $\mathcal{H}$ one can consider the map $\mathcal{H}_2$ as in 1.7. One can also define a closed subgroup scheme S of G as the connected component of the group scheme $\mathcal{H}^{-1}(q)$; we say that S is defined by $\mathcal{H}$. We say that a lift of Frobenius ϕ_G on $\widehat{G}$ is horizontal with respect to $\mathcal{H}$ if the diagram 1.8 in the Introduction is commutative; we say ϕ_G is symmetric with respect to $\mathcal{H}$ if the diagram 1.9 in the Introduction is commutative. Diagram 1.8 simply says that $\mathcal{H}$ is horizontal with respect to ϕ_G and $\phi_{G,0}$. For the "moral" origin of these conditions (which is in the theory of usual differential equations) see Remark 4.17. Note that if ϕ_G is horizontal with respect to $\mathcal{H}$ and q is $\phi_{G,0}$-horizontal then S is ϕ_G-horizontal; in particular there is an induced lift of Frobenius ϕ_S on $\widehat{S}$. More generally for any $\phi_{G,0}$-horizontal point $\tilde{q} \in G$ the $\mathcal{H}^{-1}(q)$-torsor $\mathcal{H}^{-1}(\tilde{q})$ is ϕ_G-horizontal and hence has an induced lift of Frobenius. The connected components $\mathcal{H}^{-1}(\tilde{q})_i$ of $\mathcal{H}^{-1}(\tilde{q})$ are all S-torsors. So, in particular, the horizontality of $\mathcal{H}$ gives a way to compatibly give a lift of Frobenius structure to all S-torsors $\mathcal{H}^{-1}(\tilde{q})_i$ as $\tilde{q}$ varies in the set of $\phi_{G,0}$-horizontal points.

Remark 3.12. The arithmetic logarithmic derivatives $l\delta : G \to L_\delta(G)$ attached to various lifts of Frobenius ϕ_G all derive from a certain δ-map $l^1\delta : J^1(G) \to L_\delta(G)$ which we describe in what follows. This map was introduced in [6] and will not play any role later in the present paper; but it is conceptually tightly linked to our discussion so we present below a quick overview of its main features.

Let G be any smooth group scheme over R and denote by $\pi : J^1(G) \to G$ the canonical projection. One can consider the δ-map, of order 1, $l^1\delta : J^1(G) \to J^1(G)$ defined on points by $l^1\delta a := \nabla^1(\pi(a)) \cdot a^{-1}$, for $a \in J^1(G)$. Clearly this map takes values in $L_\delta(G)$ so it induces a δ-map of order 1

$$l^1\delta : J^1(G) \to L_\delta(G).$$

The following are trivial to check:

1) The map $l^1\delta : J^1(G) \to L_\delta(G)$ is a δ-cocycle for the $\star$-action in the sense that

$$l^1\delta(ab) = (l^1\delta a) \cdot (a \star (l^1\delta b)), \quad a, b \in J^1(G).$$

2) For $a, b \in J^1(G)$ one has $l^1\delta a = l^1\delta b$ if and only if there exists $c \in G$ such that $ab^{-1} = \nabla^1 c$. In particular the composition of $l^1\delta : J^1(G) \to L_\delta(G)$ with the map $\nabla^1 : G \to J^1(G)$ is the constant map with value $1 \in L_\delta(G)$.

3) The composition of $l^1\delta : J^1(G) \to L_\delta(G)$ with any section $s : G \to J^1(G)$ of the projection $\pi : J^1(G) \to G$ equals the arithmetic logarithmic derivative $l\delta : G \to L_\delta(G)$ attached to s.

4) The composition of $l^1\delta : J^1(G) \to L_\delta(G)$ with the inclusion $L_\delta(G) \subset J^1(G)$ is the antipode $L_\delta(G) \to L_\delta(G)$, $a \mapsto a^{-1}$.

5) The map of formal schemes $l^{11}\delta : J^1(J^1(G)) \to L_\delta(G)$ defining the δ-map $l^1\delta : J^1(G) \to L_\delta(G)$ (i.e. with the property that $l^1\delta = (l^{11}\delta)_*$) can be described as follows. Let $\pi_G^1 : J^1(G) \to J^0(G)$ denote the natural projection. Then one may consider the homomorphism

$$(3.4) \qquad \pi_G^{11} := \pi_{J^1(G)}^1 \times J^1(\pi_G^1) : J^1(J^1(G)) \to J^1(G) \times_{J^0(G)} J^1(G).$$

On the other hand the quotient map

$$J^1(G) \times J^1(G) \to J^1(G), \quad (a, b) \mapsto ba^{-1}$$

induces a morphism

$$q : J^1(G) \times_{J^0(G)} J^1(G) \to L_\delta(G).$$

Then the map $l^{11}\delta$ is obtained by composing q above with the morphism π_G^{11} defined in 3.4. It was checked in [6] that $l^{11}\delta^{-1}(1) = J^2(G)$. Moreover the restriction of $l^{11}\delta$ to $L_\delta(J^1(G))$ is obtained by composing the map $L_\delta(\pi_G^1) : L_\delta(J^1(G)) \to L_\delta(G)$ (induced by $J^1(\pi_G^1)$) with the antipode map $L_\delta(G) \to L_\delta(G)$.

4. Classical groups

In this section we specialize arithmetic Lie theory to classical groups and prove the main results of the paper.

Example 4.1. (GL_n). Consider the case

$$G = GL_n = Spec \ R[x, \det(x)^{-1}],$$

viewed as a group scheme over R, where $x = (x_{ij})$ is a matrix of indeterminates. Consider an arbitrary lift of Frobenius

$$\phi_G : R[x, \det(x)^{-1}]^\hat{} \to R[x, \det(x)^{-1}]^\hat{}.$$

Set

$$\phi_G(x_{ij}) = \Phi_{ij}(x) \in R[x, \det(x)^{-1}]^\hat{},$$
$$\delta_G(x_{ij}) = \Delta_{ij}(x) \in R[x, \det(x)^{-1}]^\hat{}.$$

So $\Phi_{ij}(x) = x_{ij}^p + p\Delta_{ij}(x)$. Write $\Phi(x)$ and $\Delta(x)$ for the matrices $(\Phi_{ij}(x))$ and $(\Delta_{ij}(x))$ respectively. (Conversely any choice of a matrix Δ defines a unique lift of Frobenius ϕ_G.) As usual, view the Lie algebra

$$L(G) = \mathfrak{g} = \mathfrak{gl}_n = Spec \ R[x']$$

as a vector group over R where x' is a matrix of indeterminates. We identify

$$J^1(G) = Spf \ R[x, x', \det(x)^{-1}]^\hat{}, \quad \delta x = x'.$$

If u, v are two matrices of indeterminates which are coordinates on $G \times G$ then the multiplication $G \times G \to G$ is given, of course, by the map $x \mapsto uv$. This map induces, by universality, a multiplication map on $J^1(G)$ induced by the map

$$\mu : R[x, x', \det(x)^{-1}]^\wedge \to R[u, v, u', v', \det(u)^{-1}, \det(v)^{-1}]^\wedge$$

with $\mu(x) = uv$ and $\mu(x') = \delta(uv)$. If $u = (u_{ij})$ then we set $u^{(p)} = (u_{ij}^p)$ the matrix whose entries are the p-th powers of the entries of u, we set $\phi(u) = (\phi(u_{ij}))$, and we set $\delta u = u' = (\delta u_{ij})$ the matrix whose entries are obtained from the entries of u by applying δ; hence we have

$$\phi(u) = u^{(p)} + p\delta u;$$

and similarly for v. Also, using the above notation we may write

(4.1) $$\Phi(x) = x^{(p)} + p\Delta(x).$$

In particular we have $\phi_G(x) = \Phi(x)$. Note however that in the latter equality x plays different roles in the left hand side and in the right hand side; in particular for $a \in G = GL_n(R)$ we have $\phi_G(a) = \phi(a) = a^{(p)} + p\delta a \neq a^{(p)} + p\Delta(a) = \Phi(a)$ in general. From the identity of matrices $\phi(uv) = \phi(u)\phi(v)$ we get:

(4.2) $$\delta(uv) = u^{(p)}v' + u'v^{(p)} + pu'v' + p^{-1}(u^{(p)}v^{(p)} - (uv)^{(p)}),$$

(4.3) $$\delta(u^{-1}) = -\phi(u)^{-1}(u'(u^{-1})^{(p)} + p^{-1}(u^{(p)}(u^{-1})^{(p)} - 1)).$$

We have

$$L_\delta(G) := Ker(J^1(G) \to \widehat{G}) = Spf \ R[x']^\wedge$$

and consequently we have (canonical !) identifications as p-formal schemes (but not as groups)

$$J^1(G) \simeq \widehat{G} \times \widehat{\mathfrak{g}}, \quad L_\delta(G) \simeq \widehat{\mathfrak{g}}.$$

(For groups other than GL_n there is still an identification as above but it is not canonical in general !) The set of points of $J^1(G)$ will be identified with pairs $(a_0, a_1) \in G \times \mathfrak{g}$; the set of R-points of $L_\delta(G)$ will be identified with the set of pairs $(1, a)$ with $a \in \mathfrak{g}$ and hence with $\mathfrak{g}$. Under these identifications:

• the group structure on $J^1(G)$ induces a group structure on the set $G \times \mathfrak{g}$; we denote the multiplication and inverse on $G \times \mathfrak{g}$ by $\circ$ and ι.

• the action $\star_\delta : G \times L_\delta(G) \to L_\delta(G)$ induces the action (still denoted by)

$$\star_\delta : G \times \mathfrak{g} \to \mathfrak{g}$$

• the group structure on $L_\delta(G)$ induces a group structure on $\mathfrak{g}$,

$$+_\delta : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

• $\nabla^1 : \widehat{G} \to J^1(G)$ induces a homomorphism (still denoted by)

$$\nabla^1 : G \to G \times \mathfrak{g}$$

• the map $\sigma : \widehat{G} \to J^1(G)$ induces a map (still denoted by)

$$\sigma : G \to G \times \mathfrak{g}$$

• for $\sigma : \widehat{G} \to J^1(G)$ as above, and $\alpha \in L_\delta(G) = \mathfrak{g}$, the map $\sigma^\alpha := \alpha \cdot \sigma : \widehat{G} \to J^1(G)$ induces a map (still denoted by)

$$\sigma^\alpha : G \to G \times \mathfrak{g}.$$

• the arithmetic logarithmic derivative $l\delta : G \to L_\delta(G)$ induces the map (still denoted by)
$$l\delta : G \to \mathfrak{g}$$
• the map $\{\ ,\ \} : G \times G \to L_\delta(G)$ induces a map (still denoted by)
$$\{\ ,\ \} : G \times G \to \mathfrak{g}$$

The following proposition provides a list of formulas computing the maps above. In the proposition below $+$ and $\cdot$ (or simply juxtaposition) in $\mathfrak{g}$ denote addition and multiplication in the associative ring $\mathfrak{g}$ of $n \times n$ matrices.

Proposition 4.2. *Let $G = GL_n$.*

1) The multiplication $\circ$ on $G \times \mathfrak{g}$ is given by:
$$(a_0, a_1) \circ (b_0, b_1) = (a_0 b_0, a_0^{(p)} b_1 + a_1 b_0^{(p)} + p a_1 b_1 + p^{-1}(a_0^{(p)} b_0^{(p)} - (a_0 b_0)^{(p)})).$$

2) The identity on $G \times \mathfrak{g}$ is the pair
$$(1, 0).$$

3) The inverse ι map on $G \times \mathfrak{g}$ is given by
$$\iota(a_0, a_1) = (a_0^{-1}, -(a_0^{(p)} + p a_1)^{-1}(a_1(a_0^{-1})^{(p)} + p^{-1}(a_0^{(p)}(a_0^{-1})^{(p)} - 1))).$$

4) The homomorphism $\nabla^1 : G \to G \times \mathfrak{g}$ is given by
$$\nabla^1(a) = (a, \delta a).$$

5) The multiplication $+_\delta$ on $\mathfrak{g}$ is given by
$$a +_\delta b := a + b + pab.$$

6) The action $\star_\delta : G \times \mathfrak{g} \to \mathfrak{g}$ is given by
$$a \star_\delta b = \phi(a) \cdot b \cdot \phi(a)^{-1}.$$

7) The arithmetic logarithmic derivative $l\delta : G \to \mathfrak{g}$ satisfies
$$l\delta(ab) = (\phi(a) \cdot l\delta(b) \cdot \phi(a)^{-1}) +_\delta l\delta(a) +_\delta \{a, b\}.$$

8) The map $\sigma : G \to G \times \mathfrak{g}$ is given by
$$\sigma(a) = (a, \Delta(a)).$$

9) The map $l\delta : G \to \mathfrak{g}$ is given by
$$l\delta a := \frac{1}{p}\left(\phi(a)\Phi(a)^{-1} - 1\right) = (\delta a - \Delta(a))(a^{(p)} + p\Delta(a))^{-1}.$$

10) The map $\{\ ,\ \} : G \times G \to \mathfrak{g}$ is given by
$$\{a, b\} = p^{-1}(\Phi(a)\Phi(b)\Phi(ab)^{-1} - 1).$$

11) If $\epsilon = 1 + p\alpha$ then the δ_G-linear equation $l\delta(u) = \alpha$ is equivalent to the equation

(4.4) $$\delta u = \Delta^\alpha(u)$$

and also to the equation

(4.5) $$\phi(u) = \Phi^\alpha(u),$$

where $\Delta^\alpha(x) := \alpha \cdot \Phi(x) + \Delta(x)$, $\Phi^\alpha(x) = \epsilon \cdot \Phi(x)$, $\epsilon = 1 + p\alpha$. (We shall refer to Equation 4.4 as a Δ-linear equation.)

12) For $\alpha \in \mathfrak{g}$ the map $\sigma^\alpha : G \to G \times \mathfrak{g}$ is given by

$$\sigma^\alpha(a) = (a, \Delta^\alpha(a)).$$

(So we can refer to $\{\Delta^\alpha(x); \alpha \in \mathfrak{g}\} \subset \mathfrak{g}(R[x, \det(x)^{-1}]\hat{\ })$ as the linear equivalence class of $\Delta(x)$.)

Proof. 1), 2), 3) follow directly from 4.2 and 4.3. 4) follows directly from definitions. 5) and 12) follow from 1). 7) follows from 6). 8) is clear. 12) is an easy exercise. 11) follows from 9). To prove the rest of the assertions one uses the following adaptation of a standard trick in Witt vector theory. Define the "ghost map"

$$w : G \times \mathfrak{g} \to G \times \mathfrak{g}, \quad w(a_0, a_1) = (a_0, a_0^{(p)} + p a_1).$$

Then w is a homomorphism of monoids with identity where the source $G \times \mathfrak{g}$ is the monoid (actually group) equipped with multiplication $\circ$ and the target $G \times \mathfrak{g}$ is equipped with the structure of direct product of multiplicative monoids (where $\mathfrak{g}$ is viewed as a monoid with respect to multiplication in the associative algebra $\mathfrak{g}$). The homomorphism w injective. So in order to prove the identities in 6), 9), 10) it is enough to prove them after composition with w; this however follows trivially using the equalities:

$$w(\nabla^1(a)) = (a, \phi(a)), \quad w(\sigma(a)) = (a, \Phi(a)).$$

$\square$

Definition 4.3. Denote by $T \subset GL_n$ the split torus of diagonal matrices and by $W \subset GL_n$ the Weyl group of permutation matrices. Let $N = WT = TW$; it is the normalizer of T in GL_n. In what follows we will view T and W either as abstract subgroups of the abstract group GL_n or as subgroup schemes of the group scheme GL_n. Finally one can consider the quadratic map $\mathcal{H}$ on GL_n defined by $\mathcal{H}(x) = x^{-1}1x = 1$; the group defined by $\mathcal{H}$ is, of course, GL_n itself and we refer to $\mathcal{H}$ as the canonical quadratic map defining GL_n. Note that the associated map $\mathcal{H}_2$ is given by

$$\mathcal{H}_2 : GL_n \times GL_n \to GL_n \to GL_n; \quad \mathcal{H}_2(x, y) = x^{-1}y,$$

We will always consider the lift of Frobenius $\phi_{GL_n,0}$ on $\widehat{GL_n}$ to be given by $\phi_{GL_n,0}(x) = x^{(p)}$.

Remark 4.4. For $G = GL_n$ we have

$$N = \{b \in G; (ab)^{(p)} = a^{(p)}b^{(p)} \ \text{ for all } \ a \in G\}$$

$$N = \{b \in G; (ba)^{(p)} = b^{(p)}a^{(p)} \ \text{ for all } \ a \in G\}$$

Also note that for any $w \in W$ we have $w^t = w^{-1}$, $w^{(p)} = w$, $\phi(w) = w$. Also, for any $d \in T$, $d^t = d$ and $d^{(p)} = d^p$.

Proposition 4.5.

i) The lift of Frobenius ϕ_{GL_n} on $\widehat{GL_n}$ defined by $\phi_{GL_n}(x) = \phi_{GL_n,0}(x) = x^{(p)}$ is the unique lift of Frobenius that is horizontal and symmetric with respect to $\mathcal{H}(x) = 1$.

ii) ϕ_{GL_n} is bicompatible with T and W.

iii) If $l\delta : GL_n \to L_\delta(GL_n) = \mathfrak{gl}_n$ is the arithmetic logarithmic derivative attached to ϕ_{GL_n} then for all $a \in GL_n$ and all $b \in TW$ we have

$$l\delta(ab) = (\phi(a) \cdot l\delta(b) \cdot \phi(a)^{-1}) +_\delta l\delta(a).$$

Proof. To check i) consider any lift of Frobenius ϕ_{GL_n} on $\mathcal{O}(GL_n)\hat{}$, $\phi_{GL_n}(x) = \Phi(x) := x^{(p)}\Lambda(x)$, $\Lambda \equiv 1 \mod p$. Clearly the diagram 1.8 is commutative. It is trivial to see that diagram 1.9 is commutative if and only if

$$\Phi(x)^{-1}x^{(p)} = (x^{(p)})^{-1}\Phi(x)$$

which is equivalent to $\Lambda^2 = 1$. We claim that this implies $\Lambda = 1$. Indeed it is enough to check by induction that $\Lambda \equiv 1 \mod p^m$ for all m. The case $m = 1$ is true by the above. Assume now $\Lambda = 1 + p^m M$. Then

$$1 = \Lambda^2 \equiv 1 + 2p^m M \mod p^{m+1}$$

which implies $M \equiv 0 \mod p$ and the induction step is proved. This ends the proof of i). ii) is an easy exercise. iii) follows from Lemma 3.10 $\square$

The following is a specialization of Proposition 4.2:

Proposition 4.6. *Let $G = GL_n$, $\phi_G(x) = x^{(p)}$, so $\Delta = 0$.*
1) The map $l\delta : G \to \mathfrak{g}$ is given by

$$l\delta a := \delta a \cdot (a^{(p)})^{-1}.$$

2) The map $\{\ ,\ \} : G \times G \to \mathfrak{g}$ is given by

$$\{a, b\} = p^{-1}(a^{(p)} \cdot b^{(p)} \cdot ((ab)^{(p)})^{-1} - 1).$$

3) If $\epsilon = 1 + p\alpha$ then the Δ-linear equation $l\delta(u) = \alpha$ is equivalent to either of the following equations:

$$\begin{aligned} \delta u &= \alpha \cdot u^{(p)}, \\ \phi(u) &= \epsilon \cdot u^{(p)}. \end{aligned}$$

The case $G = GL_n$, $\phi_G(x) = x^{(p)}$ in the above Propositions will be discussed in detail in [5]. On the other hand other choices of ϕ_G in the discussion above lead to appropriate variants of the theory for other groups; cf. the discussion below.

Remark 4.7. We will need to use, in what follows, various fractional powers of elements in the ring $A = \mathcal{O}(GL_n)\hat{} = R[x, \det(x)^{-1}]\hat{}$ where, as usual, x is an $n \times n$ matrix of variables. So we introduce the following convention. Let $U \in GL_M(A)$ with $U \equiv 1 = 1_M \mod p$, and let N be an integer not divisible by p. Then let $V = \frac{U-1}{p}$ and set

$$(4.6) \qquad U^{1/N} := (1 + pV)^{1/N} := \sum_{m=0}^{\infty} \binom{1/N}{m} p^m V^m \in GL_M(A).$$

Remark 4.8. Let $G \subset GL_n$ be a smooth closed subgroup scheme and let ϕ_{GL_n} be a lift of Frobenius on $\mathcal{O}(GL_n)\hat{} = R[x, \det(x)^{-1}]\hat{}$ such that G is δ_G-horizontal. (Such a ϕ_{GL_n} always exists by smoothness of G.) Let ϕ_G be the induced lift of Frobenius on $\mathcal{O}(G)\hat{}$. Then the embedding $G \subset GL_n$ induces a closed embedding $J^1(G) \subset J^1(GL_n)$ and hence a closed embedding $L_\delta(G) \subset L_\delta(GL_n)$. Composing the latter with the natural identification $L_\delta(GL_n) = \mathfrak{gl}_n$ we get a natural embedding of groups $L_\delta(G) \subset \mathfrak{gl}_n$ where $\mathfrak{gl}_n$ is viewed as a group with respect to $+_\delta$. Note that the usual Lie algebra $L(G)$ is also embedded as a subgroup into $L(GL_n) = \mathfrak{gl}_n$ where this time $\mathfrak{gl}_n$ is equipped with the usual addition $+$ of matrices; but note that, as subsets of $\mathfrak{gl}_n$ we have $L_\delta(G) \neq L(G)$ in general! Indeed it is trivial to check that if

$$G = Spec\ R[x, \det(x)^{-1}]\hat{}/(f_1(x), ..., f_m(x))$$

and if

$$\delta_1 f_i(x') = p^{-1} f_i^{(\phi)}(1 + px')$$

where $f_i^{(\phi)}$ is obtained from f_i by applying ϕ to the coefficients then

$$L_\delta(G) = Spf\ R[x']\hat{\ }/(\delta_1 f_1(x'), ..., \delta_1 f_m(x'))$$

hence the R-points of the latter are the zeroes in $\mathfrak{gl}_n$ of the polynomials $\delta_1 f_i(x')$. On the other hand the Lie algebra $L(G)$ is given by

$$L(G) = Spec\ R[x']/(d_1 f_1(x'), ..., d_1 f_m(x'))$$

where

$$d_1 f_i(x') = \text{``}\epsilon^{-1}\text{''} f_i(1 + \epsilon x').$$

So the set of R-points of $L(G)$ is the zero locus in $\mathfrak{gl}_n$ of the polynomials $d_1 f_i$. Cf. our discussion of examples below. Going back to our discussion it follows from horizontality that

$$l\delta : G \to L_\delta(G)$$

is the restriction of the map

$$l\delta : GL_n \to L_\delta(GL_n) = \mathfrak{gl}_n.$$

Similarly the map

$$\{\ ,\ \}_G : G \times G \to L_\delta(G)$$

is the restriction of the map

$$\{\ ,\ \}_{GL_n} : GL_n \times GL_n \to L_\delta(GL_n) = \mathfrak{gl}_n.$$

In particular the formulas in Proposition 4.2 continue to be valid if one replaces $G = GL_n$ by $G \subset GL_n$ an arbitrary smooth closed subgroup of GL_n, provided G is δ_{GL_n}-horizontal and provided we make the identifications explained above.

Example 4.9. (SL_n). Consider the group scheme

$$SL_n = Spec\ R[x]/(\det(x) - 1).$$

Embed SL_n as a closed subgroup scheme of GL_n in the natural way and equip GL_n with the lift of Frobenius $\phi_{GL_n,0}(x) = x^{(p)}$. Recall that T and W are the torus of diagonal matrices in GL_n and the Weyl group of GL_n consisting of the permutation matrices. In particular $T_{SL_n} = T \cap SL_n$ is a maximal torus in SL_n and $W_{SL_n} = W \cap SL_n$ is the group of even permutation matrices (which is smaller than the Weyl group of SL_n!). Also recall that the group of characters $Hom(T, \mathbb{G}_m)$ of T has a $\mathbb{Z}$-basis $\chi_1, ..., \chi_n$ where

$$\chi_i(diag(d_1, ..., d_n)) = d_i.$$

The restrictions of $\chi_1, ..., \chi_n$ to T_{SL_n}, which will still be denoted by $\chi_1, ..., \chi_n$ generate the group of characters of T_{SL_n} and satisfy one relation $\chi_1 + ... + \chi_n = 0$ (where we use, as usual, the additive notation for characters). The roots of SL_n are

$$\chi_i - \chi_j, \ \ i \neq j.$$

The additive group $U_{\chi_i - \chi_j}$ corresponding to the root $\chi_i - \chi_j$ comes from an embedding of $\mathbb{G}_a$ over R into SL_n and, as an abstract group

$$U_{\chi_i - \chi_j} = \{\mu E_{ij}\}$$

where $\mu \in R$ and E_{ij} is the matrix with 1s on the diagonal, 1 on position (i,j) and 0 everywhere else. Note that $U_{\chi_i - \chi_j}$ is $\phi_{GL_n,0}$-horizontal in GL_n and the lift of Frobenius induced by $\phi_{GL_n,0}$ on $\widehat{\mathbb{G}_a} = Spf\ R[z]\hat{}$ is given by $z \mapsto z^p$.

Finally recall from the Introduction that, in discussing SL_n, we need to require $p \nmid n$ and we need to consider the étale cover $\pi : G = GL_n^* \to GL_n$ defined in 1.11. We equip G with the quadratic map $\mathcal{H}$ as in 1.13. Then π induces an isomorphism $\mathcal{H}^{-1}(1)^\circ \simeq SL_n$; we call $\mathcal{H}$ the canonical quadratic map defining SL_n. Of course, SL_n is smooth over R. Let us equip $\widehat{G}$ with the unique lift of Frobenius $\phi_{G,0}$ extending the lift of Frobenius $\phi_{GL_n,0}$ on $\widehat{GL_n}$. We say that a lift of Frobenius ϕ_{GL_n} on $\widehat{GL_n}$ is compatible (respectively symmetric) with respect to $\mathcal{H}$ if the unique extension ϕ_G of ϕ_{GL_n} to $\widehat{G}$ is compatible (respectively symmetric) with respect to $\mathcal{H}$. For any such ϕ_{GL_n} the group SL_n is easily seen to be ϕ_{GL_n}-horizontal so there is an induced lift of Frobenius ϕ_{SL_n} on $\widehat{SL_n}$.

In the next statement we use the convention on fractional powers that we introduced in Equation 4.7.

Proposition 4.10. *Let $p \nmid n$ and let $\mathcal{H}$ be the canonical quadratic map on $G = GL_n^*$ defining SL_n.*

i) There is a unique lift of Frobenius ϕ_{GL_n} on $\widehat{GL_n}$ that is horizontal and symmetric with respect to $\mathcal{H}$. It is given by $\phi_{GL_n}(x) = \lambda(x) \cdot x^{(p)}$ where $\lambda(x) \in R[x, \det(x)^{-1}]\hat{}$,

$$\lambda(x) = \left(\frac{\det(x^{(p)})}{(\det(x))^p} \right)^{-1/n} .$$

ii) ϕ_{GL_n} is bicompatible with T and W; in particular the lift of Frobenius ϕ_{SL_n} on $\widehat{SL_n}$ induced by ϕ_{GL_n} is bicompatible with T_{SL_n} and W_{SL_n}.

iii) ϕ_{GL_n} and $\phi_{GL_n,0}$ coincide on the set $SL_n \cap \phi_{GL_n,0}^{-1}(SL_n)$; in particular the additive groups $U_{\chi_i - \chi_j}$ are ϕ_{GL_n}-horizontal and the lifts of Frobenius induced by ϕ_{GL_n} on $\widehat{\mathbb{G}_a} = Spf\ R[z]\hat{}$ are given by $z \mapsto z^p$.

iv) If $l\delta : SL_n \to L_\delta(SL_n)$ is the arithmetic logarithmic derivative attached to ϕ_{SL_n} then for all $a \in SL_n$ and all $b \in T_{SL_n}W_{SL_n}$ we have

$$l\delta(ab) = (\phi(a) \cdot l\delta(b) \cdot \phi(a)^{-1}) +_\delta l\delta(a).$$

v) Let $\alpha \in L_\delta(SL_n)$, let $\phi_{GL_n}^\alpha$ be the lift of Frobenius on $\widehat{GL_n}$ defined by $\phi_{GL_n}^\alpha(x) = \epsilon \cdot \phi_{GL_n}(x)$, $\epsilon = 1 + p\alpha$, and let $\delta_{GL_n}^\alpha$ be the p-derivation on $\mathcal{O}(GL_n)\hat{}$ associated to $\phi_{GL_n}^\alpha$. Let $\mathcal{H}^* \in \mathcal{O}(GL_n)\hat{}$ be defined as $\mathcal{H}^*(x) = \det(x)$. Then

$$\delta_{GL_n}^\alpha(\mathcal{H}^*) = 0.$$

Proof. We have

$$\mathcal{O}(G) = R[x, \det(x)^{-1}, T]/(T^n - \det(x)^2) = R[x, \det(x)^{-1}, t],$$

where t is the class of T. Denoting, as usual, by $*, \mathcal{H}, \mathcal{H}_2$ the ring maps induced by the corresponding scheme maps, we have $x^* = tx^{-1}$, $t^* = t$, $\mathcal{H}_2(x) = tx_1^{-1}x_2$, $\mathcal{H}(x) = t \cdot 1_n$. (Here x_1, x_2 are $x \otimes 1$ and $1 \otimes x$ respectively.) Now from $t^n = \det(x)^2$

we get

$$(4.7) \qquad \begin{aligned} \phi_{G,0}(t)^n &= \phi_{G,0}(\det(x))^2 \\ &= \det(x^{(p)})^2 \\ &= \lambda(x)^{-2n}\det(x)^{2p} \\ &= (\lambda(x)^{-2}t^p)^n \end{aligned}$$

where $\lambda(x)$ is defined as in assertion i). Since $\phi_{G,0}(t) \equiv \lambda(x)^{-2}t^p \bmod p$ it follows that

$$(4.8) \qquad \phi_{G,0}(t) = \lambda(x)^{-2}t^p.$$

Let $\phi_{GL_n}(x) = x^{(p)}\Lambda(x)$ be an arbitrary lift of Frobenius, where Λ is a matrix $\equiv 1 \bmod p$. Then

$$(4.9) \qquad \begin{aligned} \phi_G(t)^n &= \phi_G(\det(x))^2 \\ &= \det(x^{(p)}\Lambda(x))^2 \\ &= \det(x^{(p)})^2(\det(\Lambda(x))^2 \\ &= (\lambda(x)^{-2}t^p(\det(\Lambda(x))^2)^{1/n})^n. \end{aligned}$$

Since $\phi_G(t) \equiv \lambda(x)^{-2}t^p(\det(\Lambda(x))^2)^{1/n} \bmod p$ it follows that

$$(4.10) \qquad \phi_G(t) = \lambda(x)^{-2}t^p(\det(\Lambda(x))^2)^{1/n}.$$

Consequently

$$(4.11) \qquad \mathcal{H}(\phi_{G,0}(x)) = \mathcal{H}(x^{(p)}) = t^p \cdot 1$$

$$(4.12) \qquad \phi_G(\mathcal{H}(x)) = \phi_G(t \cdot 1) = \lambda(x)^{-2}t^p(\det(\Lambda(x))^2)^{1/n} \cdot 1$$

Hence the commutativity of 1.8 is equivalent to

$$(4.13) \qquad \lambda(x)^2 = (\det(\Lambda(x))^2)^{1/n}$$

Similarly, using the expression for $\mathcal{H}_2$ and using 4.8 and 4.10 again, we get that the commutativity of 1.9 is equivalent to

$$(\det(\Lambda(x))^{-1/n}\Lambda(x))^2 = 1.$$

Since $\det(\Lambda(x))^{-1/n}\Lambda(x) \equiv 1 \bmod p$ it follows that 1.9 is equivalent to

$$(4.14) \qquad \det(\Lambda(x))^{-1/n}\Lambda(x) = 1$$

Let us check assertion i). The existence part is clear because if we set $\Lambda(x) = \lambda(x) \cdot 1$ then 4.13 and 4.14 are clearly satisfied. The uniqueness follows because by 4.14 $\Lambda(x)$ must be a scalar matrix $\tilde{\lambda}(x) \cdot 1$ with $\tilde{\lambda} \equiv 1 \bmod p$; but then by 4.13 we must have $\tilde{\lambda} = \lambda$.

To check assertion ii) note first that if $a \in T$ or $a \in W$ then

$$\begin{aligned} \lambda(xa) &= \left(\frac{\det((xa)^{(p)})}{(\det(xa))^p}\right)^{-1/n} \\ &= \left(\frac{\det(x^{(p)}a^{(p)})}{\det(x)^p \cdot \det(a)^p}\right)^{-1/n} \\ &= \left(\frac{\det(x^{(p)}) \cdot \det(a)^p}{\det(x)^p \cdot \det(a)^p}\right)^{-1/n} \\ &= \lambda(x). \end{aligned}$$

Similarly $\lambda(ax) = \lambda(x)$. Hence

$$\phi_{GL_n}(xa) = \lambda(xa) \cdot (xa)^{(p)} = \lambda(x) \cdot x^{(p)} \cdot a^{(p)} = \phi_{GL_n}(x) \cdot a^{(p)}.$$

Similarly

$$\phi_{GL_n}(ax) = \lambda(ax) \cdot (ax)^{(p)} = \lambda(x) \cdot a^{(p)} \cdot x^{(p)} = a^{(p)} \cdot \phi_{GL_n}(x).$$

In particular $\phi_{GL_n}(a) = \lambda(a) \cdot a^{(p)} = a^{(p)}$ which is in T or W if a is in T or W respectively. So T and W are δ_{GL_n}-horizontal and ϕ_{GL_n} is bicompatible with T and W.

To check assertion iii) let $g \in SL_n \cap \phi_{GL_n,0}^{-1}(SL_n)$. So $\det(g) = 1$ and

$$1 = \det(\phi_{GL_n,0}(g)) = \det(\phi^{-1}(g^{(p)})) = \phi^{-1}(\det(g^{(p)}))$$

hence $\det(g^{(p)}) = 1$. So $\lambda(g) = 1$ and so

$$\phi_{GL_n}(g) = \phi^{-1}(\lambda(g))\phi^{-1}(x^{(p)}) = \phi^{-1}(\lambda(g))\phi_{GL_n,0}(g) = \phi_{GL_n,0}(g).$$

which ends the proof of the first assertion in iii). The second assertion in iii) follows from Lemma 2.1.

Assertion of iv) follows from Lemma 3.10.

To check assertion v) note that the equality $\delta_{GL_n}^\alpha(\det(x)) = 0$, which is equivalent to $\phi_{GL_n}^\alpha(\det(x)) = \det(x)^p$, follows from the following computation (where we use $\det(\epsilon) = 1$):

$$\begin{aligned}
\phi_{GL_n}^\alpha(\det(x)) &= \det(\phi_{GL_n}^\alpha(x)) \\
&= \det(\lambda(x) \cdot \epsilon \cdot x^{(p)}) \\
&= \lambda(x)^n \cdot \det(\epsilon) \cdot \det(x^{(p)}) \\
&= \det(x)^p.
\end{aligned}$$

$\square$

By Proposition 4.2 and with the conventions in Remark 4.8 we get:

Proposition 4.11. *Let $\phi_{SL_n}(x)$ be induced by $\phi_{GL_n}(x) = \lambda(x) \cdot x^{(p)}$ with λ as in Proposition 4.10.*

1) The map $l\delta : SL_n \to L_\delta(SL_n) \subset \mathfrak{gl}_n$ is given by

$$l\delta a = \delta a \cdot (\lambda(a) \cdot a^{(p)})^{-1} + \frac{\lambda(a)^{-1} - 1}{p} \cdot 1_n.$$

2) The map $\{ \ , \ \}_{SL_n} : SL_n \times SL_n \to L_\delta(SL_n) \subset \mathfrak{gl}_n$ is given by

$$\{a, b\}_{SL_n} = p^{-1}\left(\frac{\lambda(a)\lambda(b)}{\lambda(ab)}a^{(p)}b^{(p)}((ab)^{(p)})^{-1} - 1_n\right).$$

3) If $\epsilon = 1 + p\alpha$ then the Δ-linear equation $l\delta(u) = \alpha$ is equivalent to either of the following equations:

$$\delta u = \left(\lambda(u) \cdot \alpha + \frac{\lambda(u) - 1}{p} \cdot 1_n\right) \cdot u^{(p)},$$

$$\phi(u) = \epsilon \cdot \lambda(u) \cdot u^{(p)}.$$

Example 4.12. ($SO(q)$). Consider again $G = GL_n$ equipped with the lift of Frobenius $\phi_{GL_n,0}(x) = x^{(p)}$. Consider the quadratic map $\mathcal{H}$ on GL_n defined by $\mathcal{H}(x) = x^t q x$ where x^t is the transpose of x, and $q \in GL_n$ is either symmetric or antisymmetric; we express this by writing $q^t = \pm q$. We have $\mathcal{H}_2(x, y) = x^t q y$. Let $SO(q)$ be the group defined by $\mathcal{H}$; we refer to $\mathcal{H}$ as the canonical quadratic map defining $SO(q)$. The group $SO(q)$ is trivially seen to be formally smooth, and hence smooth, over R. If $T \subset GL_n$ is the torus of diagonal matrices in GL_n we set

$T_{SO(q)} = T \cap SO(q)$. If $W = W_n$ is the group of permutation matrices in GL_n we set $W_{SO(q)} = W \cap SO(q)$.

We say q (or $SO(q)$) is split if q is one of the matrices 1.10; in this case $qq^t = 1$. If $SO(q)$ is split it is denoted by Sp_{2r}, SO_{2r}, SO_{2r+1} respectively. These groups contain the following split (maximal) tori:

$$\begin{aligned}
T_{Sp_{2r}} &= \{d \in T; d = diag(d_1, ..., d_r, d_1^{-1}, ..., d_r^{-1})\} \\
T_{SO_{2r}} &= \{d \in T; d = diag(d_1, ..., d_r, d_1^{-1}, ..., d_r^{-1})\} \\
T_{SO_{2r+1}} &= \{d \in T; d = diag(1, d_1, ..., d_r, d_1^{-1}, ..., d_r^{-1})\}.
\end{aligned}$$

Also $W_{SO(q)}$ contains all the matrices of the form

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

respectively, where $w_r \in W_r$ is an arbitrary permutation matrix in GL_r. The groups of characters of $T_{Sp_{2r}}$ and $T_{SO_{2r}}$ have bases $\chi_1, ..., \chi_r$ where

$$\chi_i(diag(d_1, ..., d_r, d_1^{-1}, ..., d_r^{-1})) = d_i.$$

The group of characters of $T_{SO_{2r+1}}$ has basis $\chi_1, ..., \chi_r$ where

$$\chi_i(diag(1, d_1, ..., d_r, d_1^{-1}, ..., d_r^{-1})) = d_i.$$

The roots of Sp_{2r} are $\pm 2\chi_i$, $\pm \chi_i \pm \chi_j$, $i \neq j$. The roots of SO_{2r} are $\pm \chi_i \pm \chi_j$, $i \neq j$. The roots of SO_{2r+1} are $\pm \chi_i$, $\pm \chi_i \pm \chi_j$, $i \neq j$. Recall that if G is any of the groups $Sp_{2r}, SO_{2r}, SO_{2r+1}$ and if χ is a root of G then there is an attached additive group U_χ of G over K^a; it is the unique subgroup isomorphic to $\mathbb{G}_a$ over K^a normalized by the corresponding maximal torus on which this maximal torus acts via χ. In all these cases U_χ comes from an embedding of $\mathbb{G}_a$ into G over R and has the following explicit description which we need to review.

We consider $r \times r$ matrices as follows. For $i = 1, ..., r$ let F_{ii} be the matrix with 1 on position (i, i) and 0 everywhere else. Let now $i \neq j$ between 1 and r. Let E_{ij} be the matrix with 1s on the diagonal, 1 on position (i, j) and 0 everywhere else. Let $F_{ij} = E_{ij} + E_{ji}$ and $G_{ij} = E_{ij} - E_{ji}$. Finally let e_i be the $1 \times r$ matrix with 1 on position i and 0 everywhere else. Then the groups U_χ are given as follows (where $\mu \in R$). For Sp_{2r} we have:

$$U_{2\chi_i} = \{\begin{pmatrix} 1 & \mu F_{ii} \\ 0 & 1 \end{pmatrix}\}, \quad U_{-2\chi_i} = U_{2\chi_i}^t$$

$$U_{\chi_i - \chi_j} = \{\begin{pmatrix} 1 + \mu E_{ij} & 0 \\ 0 & 1 - \mu E_{ji} \end{pmatrix}\}$$

$$U_{\chi_i + \chi_j} = \{\begin{pmatrix} 1 & \mu F_{ij} \\ 0 & 1 \end{pmatrix}\}, \quad U_{-\chi_i - \chi_j} = U_{\chi_i + \chi_j}^t$$

For SO_{2r} we have:

$$U_{\chi_i + \chi_j} = \{\begin{pmatrix} 1 & \mu G_{ij} \\ 0 & 1 \end{pmatrix}\}, \quad U_{-\chi_i - \chi_j} = U_{\chi_i + \chi_j}^t$$

$$U_{\chi_i - \chi_j} = \{\begin{pmatrix} 1 + \mu E_{ij} & 0 \\ 0 & 1 - \mu E_{ji} \end{pmatrix}\}$$

For SO_{2r+1} we have:

$$U_{\pm\chi_i\pm\chi_j} \quad = \quad \{\begin{pmatrix} 1 & 0 \\ 0 & \star \end{pmatrix}\}, \quad \text{where } \star \text{ is as for } SO_{2r}$$

$$U_{\chi_i} \quad = \quad \{\begin{pmatrix} 1 & \mu e_i & 0 \\ 0 & 1 & 0 \\ -\mu e_i^t & -\frac{\mu^2}{2}e_i^t e_i & 1 \end{pmatrix}\}, \quad U_{-\chi_i} = U_{\chi_i}^t.$$

Remark that if G is Sp_{2r} and χ is any root or if G is SO_{2r} and χ is any root or if G is SO_{2r+1} and $\chi \neq \pm\chi_i$ we have that U_χ is $\phi_{GL_n,0}$-horizontal. On the other hand if $G = SO_{2r+1}$ and $\chi = \pm\chi_i$ then U_χ is not $\phi_{GL_n,0}$-horizontal (because it is not stable under the map $u \mapsto u^{(p)}$). For obvious reasons we shall refer to $\pm\chi_i$ as the short roots.

Let us consider again the general case when q is not necessarily split; in this general case $T_{SO(q)}$ is, of course, not necessarily a maximal torus in $SO(q)$. Note that the δ-Lie algebra $L_\delta(SO(q))$ identifies with the set of matrices $a \in \mathfrak{gl}_n$ satisfying

$$a^t\phi(q) + \phi(q)a + pa^t\phi(q)a = 0.$$

On the other hand the Lie algebra $L(SO(q))$ identifies with the set of matrices $a \in \mathfrak{gl}_n$ satisfying

$$a^t q + qa = 0.$$

In the next Proposition we are using, again, the convention on fractional powers that we introduced in Equation 4.7.

Proposition 4.13. *Let $q \in GL_n$, $q^t = \pm q$, and let $\mathcal{H}(x) = x^t qx$ be the canonical quadratic map on GL_n defining $SO(q)$.*

i) There exists a unique lift of Frobenius ϕ_{GL_n} on $\widehat{GL_n}$ which is horizontal and symmetric with respect to $\mathcal{H}$. It is given by $\phi_{GL_n}(x) = x^{(p)} \cdot \Lambda(x)$, where

$$\Lambda(x) = (((x^{(p)})^t\phi(q)x^{(p)})^{-1}(x^t qx)^{(p)})^{1/2}.$$

ii) If $q^{(p)} = q$ then ϕ_{GL_n} is right compatible with T and W and is left compatible with $T_{SO(q)}$ and $W_{SO(q)}$; in particular the lift of Frobenius $\phi_{SO(q)}$ on $\widehat{SO(q)}$ induced by ϕ_{GL_n} is bicompatible with $T_{SO(q)}$ and $W_{SO(q)}$.

iii) If $q^{(p)} = q$ then ϕ_{GL_n} and $\phi_{GL_n,0}$ coincide on the set $SO(q) \cap \phi_{GL_n,0}^{-1}(SO(q))$; in particular if $SO(q)$ is split and χ is not a short root then the additive group U_χ is ϕ_{GL_n}-horizontal and the lift of Frobenius on $\widehat{\mathbb{G}_a} = Spf\ R[z]\hat{}$ induced by ϕ_{GL_n} is given by $z \mapsto z^p$.

iv) If $q^{(p)} = q$ and if $l\delta : SO(q) \to L_\delta(SO(q))$ is the arithmetic logarithmic derivative attached to $\phi_{SO(q)}$ then for all $a \in SO(q)$ and all $b \in T_{SO(q)}W_{SO(q)}$ we have

$$l\delta(ab) = (\phi(a) \cdot l\delta(b) \cdot \phi(a)^{-1}) +_\delta l\delta(a).$$

v) Let $\alpha \in L_\delta(SO(q))$, let $\phi_{GL_n}^\alpha$ be the lift of Frobenius on $\mathcal{O}(GL_n)\hat{}$ defined by $\phi_{GL_n}^\alpha(x) = \epsilon \cdot \phi_{GL_n}(x)$, $\epsilon = 1 + p\alpha$, and let $\delta_{GL_n}^\alpha$ be the p-derivation on $\mathcal{O}(GL_n)\hat{}$ associated to $\phi_{GL_n}^\alpha$. Then

$$\delta_{GL_n}^\alpha(\mathcal{H}) = 0.$$

Proof. We start by constructing a certain matrix $\Lambda(x) \in GL_n(R[x, \det(x)^{-1}]\hat{\ })$. Consider the matrices

$$A := (x^{(p)})^t \phi(q) x^{(p)}, \qquad B := (x^t q x)^{(p)}.$$

Clearly $A^t = \pm A$, $B^t = \pm B$, according as $q^t = \pm q$. Note that $A \equiv B \bmod p$; set

$$C = p^{-1}(B - A).$$

Define the matrix

$$(4.15) \quad \Lambda = \Lambda(x) := (A^{-1}B)^{1/2} := (1 + pA^{-1}C)^{1/2} := \sum_{i=0}^{\infty} \binom{1/2}{i} p^i (A^{-1}C)^i.$$

Clearly $\Lambda \equiv 1 \bmod p$. Note that

$$(4.16) \qquad\qquad\qquad (A\Lambda)^t = \pm A\Lambda;$$

this follows because

$$(A(A^{-1}C)^i)^t = (C^t(A^t)^{-1})^i A^t = \pm (CA^{-1})^i A = \pm A(A^{-1}C)^i.$$

Also note that

$$(4.17) \qquad\qquad\qquad \Lambda^t A \Lambda = B.$$

This follows from the following computation:

$$
\begin{aligned}
\Lambda^t A \Lambda &= \left(\sum_{i=0}^{\infty} \binom{1/2}{i} p^i (CA^{-1})^i \right) A \left(\sum_{j=0}^{\infty} \binom{1/2}{j} p^j (A^{-1}C)^i \right) \\[2mm]
&= A + \sum_{n=1}^{\infty} p^n (CA^{-1})^{n-1} C \sum_{i+j=n} \binom{1/2}{i} \binom{1/2}{j} \\[2mm]
&= A + pC \\[2mm]
&= B.
\end{aligned}
$$

Let us consider next the right action of $SO(q)$ on $R[x, \det(x)^{-1}]\hat{\ }$

$$F(x) \bullet c := F(xc), \quad F \in R[x, \det(x)^{-1}]\hat{\ }, \quad c \in SO(q),$$

and the left action of $SO(q)$ on $R[x, \det(x)^{-1}]\hat{\ }$

$$c \bullet F(x) := F(cx), \quad F \in R[x, \det(x)^{-1}]\hat{\ }, \quad c \in SO(q).$$

Assume in addition that $q^{(p)} = q$ (hence $\phi(q) = q$). Let u be in T or W and let v be in $T_{SO(q)}$ or $W_{SO(q)}$. One checks that:

$$(4.18) \quad A \bullet u = (u^{(p)})^t A u^{(p)}, \quad v \bullet A = A, \quad B \bullet u = (u^{(p)})^t B u^{(p)}, \quad v \bullet B = B,$$

$$(4.19) \qquad\qquad\qquad A(u) = B(u).$$

Hence

$$(4.20) \qquad\qquad C \bullet u = (u^{(p)})^t C u^{(p)}, \quad v \bullet C = C, \quad C(u) = 0,$$

$$(4.21) \qquad\qquad \Lambda \bullet u = (u^{(p)})^{-1} \Lambda u^{(p)}, \quad v \bullet \Lambda = \Lambda, \quad \Lambda(u) = 1.$$

Let us prove i)

To prove the existence part in i) define the lift of Frobenius ϕ_{GL_n} by $\phi_{GL_n}(x) = \Phi(x) = x^{(p)} \cdot \Lambda(x)$. Then, using 4.17, we get:

$$
\begin{aligned}
\phi_{GL_n}(x^t q x) &= \Lambda^t (x^{(p)})^t \phi(q) x^{(p)} \Lambda \\
&= \Lambda^t A \Lambda \\
&= B \\
&= (x^t q x)^{(p)} \\
&= \phi_0(x^t q x).
\end{aligned}
$$

This implies the commutativity of 1.8. The commutativity of 1.9 is equivalent to

$$
(x^{(p)})^t \phi(q) \Phi(x) = \Phi(x)^t \phi(q) x^{(p)},
$$

which is just a reformulation of the equality 4.16. This ends, in particular, the proof of the existence claim in i).

To prove uniqueness in i) let ϕ_i, $i = 1, 2$ be lifts of Frobenius on $\mathcal{O}(GL_n)\hat{} = R[x, \det(x)^{-1}]\hat{}$. They are defined by $\phi_i(x) = x^{(p)} \cdot \Lambda_i(x)$, $i = 1, 2$, for two matrices $\Lambda_1 \equiv \Lambda_2 \equiv 1 \mod p$. Assume that both ϕ_1 and ϕ_2 are horizontal and symmetric with respect to $\mathcal{H}$; we need to show that $\phi_1 = \phi_2$. By the arguments in the existence part of i) the compatibility of Λ_1 and Λ_2 with $\mathcal{H}_2$ implies $\Lambda_i^t A \Lambda_i = B$ and $\Lambda_i^t A^t = (A\Lambda_i)^t = \pm A\Lambda_i$, $i = 1, 2$. We get

$$
B = \Lambda_i^t A \Lambda_i = \pm \Lambda_i^t A^t \Lambda_i = A \Lambda_i^2
$$

hence

(4.22) $$\Lambda_i^2 = A^{-1} B.$$

Let us prove by induction that $\Lambda_1 \equiv \Lambda_2 \mod p^m$ for all m. By hypothesis this true for $m = 1$. Assume

$$
\Lambda_2 = \Lambda_1 + p^m M.
$$

Then

$$
\Lambda_2^2 \equiv \Lambda_1^2 + p^m (\Lambda_1 M + M \Lambda_1) \ \ mod \ \ p^{m+1}
$$

hence, by 4.22, and by $\Lambda_1 \equiv 1 \mod p$ we get $2M \equiv 0 \mod p$. Hence $\Lambda_1 \equiv \Lambda_2 \mod p^{m+1}$ which ends the induction step, and hence the proof of i).

To check ii) we check first that T and W are ϕ_{GL_n}-horizontal. For this it is enough to show that $\phi_{GL_n}(u)$ is in T or W if u is in T or W respectively; but this follows from the fact that $\Lambda(u) = 1$ in 4.21.

In order to check compatibility of ϕ_{GL_n} with right multiplication by H (where H is T or W) and left multiplication by $H_{SO(q)}$ (where $H_{SO(q)}$ is $T_{SO(q)}$ or $W_{SO(q)}$) it is sufficient to notice that, by 4.21, we get

$$
\begin{aligned}
\phi_{GL_n}(xu) &= \phi_{GL_n}(x) \bullet u \\
&= (x^{(p)} \Lambda) \bullet u \\
&= (xu)^{(p)} (\Lambda \bullet u) \\
&= (x^{(p)} u^{(p)})((u^{(p)})^{-1} \Lambda u^{(p)}) \\
&= x^{(p)} \Lambda u^{(p)} \\
&= \phi_{GL_n}(x) \cdot \phi_H(u)
\end{aligned}
$$

and

$$\begin{aligned}
\phi_{GL_n}(vx) &= v \bullet \phi_{GL_n}(x) \\
&= v \bullet (x^{(p)}\Lambda) \\
&= (vx)^{(p)}(v \bullet \Lambda) \\
&= v^{(p)}x^{(p)}\Lambda \\
&= \phi_{H_{SO(q)}}(v) \cdot \phi_{GL_n}(x).
\end{aligned}$$

To check assertion iii) let $g \in SO(q) \cap \phi_{GL_n,0}^{-1}(SO(q))$. Then $g^t q g = q$ hence $B(g) = q^{(p)} = q$; and also $\phi_{GL_n,0}(g)^t q \phi_{GL_n,0}(g) = q$, hence

$$q = \phi(q) = \phi(\phi_{GL_n,0}(g)^t q \phi_{GL_n,0}(g)) = (g^{(p)})^t \phi(q) g^{(p)} = (g^{(p)})^t q g^{(p)},$$

so $A(g) = q$. Hence $C(g) = 0$, hence $\Lambda(g) = 1$, and hence

$$\phi_{GL_n}(g) = \phi^{-1}(x^{(p)})\phi^{-1}(\Lambda(g)) = \phi_{GL_n,0}(g).$$

This ends the proof of the first assertion in iii). The second assertion in iii) follows from Lemma 2.1.

Assertion iv) follows from Lemma 3.10.

To check assertion v) note that from the computation in the proof of i) we have

(4.23) $$\Phi(x)^t \phi(q) \Phi(x) = (x^t q x)^{(p)}.$$

Now assertion v) follows from the following computation (where we use $\epsilon \in SO(\phi(q))$):

$$\begin{aligned}
\phi_{GL_n}^\alpha(x^t q x) &= (\phi_{GL_n}^\alpha(x))^t \phi(q) \phi_{GL_n}^\alpha(x) \\
\\
&= (\epsilon\Phi(x))^t \phi(q)\epsilon\Phi(x) \\
\\
&= \Phi(x)^t \epsilon^t \phi(q)\epsilon\Phi(x) \\
\\
&= \Phi(x)^t \phi(q)\Phi(x) \\
\\
&= (x^t q x)^{(p)}.
\end{aligned}$$

$\square$

Remark 4.14. Note that in the above proof we have

$$C = -(x^{(p)})^t(\delta q)x^{(p)} + \frac{(x^t q x)^{(p)} - (x^{(p)})^t q^{(p)} x^{(p)}}{p}$$

hence $\Phi(x)$, viewed as a function of x, q, is a restricted power series in

$$x, q, \delta q, \det(x)^{-1}, \det(q).$$

Remark 4.15. In contrast with assertion 3 in the Proposition 4.13 above if $SO(q)$ is split and χ is a short root (i.e. $SO(q) = SO_{2r+1}$ and $\chi = \pm\chi_i$) then one can check (by direct computation involving the explicit formula for ϕ_{GL_n} in the above proof) that U_χ is not ϕ_{GL_n}-horizontal. This is a curious phenomenon that may deserve further attention.

Remark 4.16. Note that the lift of Frobenius $\phi_{GL_n}(x) = x^{(p)}$ in Corollary 4.6 (which is the one that is horizontal and symmetric with respect to the quadratic map $\mathcal{H} = 1$ defining GL_n itself) has polynomial components. In contrast to this case the lifts of Frobenius ϕ_{GL_n} in Propositions 4.10 and 4.13 (which are horizontal and symmetric with respect to the canonical quadratic maps defining SL_n, SO_n, Sp_n)

are not given by polynomials but, rather, by p-adic restricted power series. This makes the quadratic map defining GL_n more tractable (e.g. tractable by algebraic rather than analytic methods) than the quadratic maps defining the other classical groups; and it is this case that will be further investigated in [5].

Remark 4.17. It is interesting to see what the conditions 1.8 and 1.9 correspond to in the classical case of usual differential equations. So assume, in this remark, that we are in the framework of differential algebra [8] which we refer to as the δ-algebraic case (as opposed to the δ-arithmetic case studied so far). So we assume R is a δ-closed field equipped with a derivation δ. Let G be a linear algebraic group over R equipped with an involution $x \mapsto x^\dagger$ and let $q \in G = G(R)$. Let $A := \mathcal{O}(G)$ and fix a derivation $\delta_{A,0}$ of A whose restriction to R is δ. Let $\mathcal{H} : A \to A$ be the R-algebra map induced by the map $G \to G$, $x \mapsto x^\dagger q x$ and let $\mathcal{H}_2 : A \to A \otimes_R A$ be the R-algebra map defined by the map $G \times G \to G$, $(x_1, x_2) \mapsto x_1^\dagger q x_2$. Let δ_A be another derivation on A whose restriction to R is δ. Let us say that δ_A is horizontal with respect to $\mathcal{H}$ if the following diagram is commutative:

$$(4.24) \qquad \begin{array}{ccc} A & \xleftarrow{\delta_A} & A \\ \mathcal{H} \uparrow & & \uparrow \mathcal{H} \\ A & \xleftarrow{\delta_{A,0}} & A \end{array}$$

Let us say that δ_A is symmetric with respect to $\mathcal{H}$ if the following diagram is commutative:

$$(4.25) \qquad \begin{array}{ccc} A & \xleftarrow{\delta_A \otimes 1 + 1 \otimes \delta_{A,0}} & A \otimes_R A \\ \delta_{A,0} \otimes 1 + 1 \otimes \delta_A \uparrow & & \uparrow \mathcal{H}_2 \\ A \otimes_R A & \xleftarrow{\mathcal{H}_2} & A \end{array}$$

These diagrams can be viewed as δ-algebraic analogues of the diagrams 1.8 and 1.9 respectively. Then Proposition 4.13 should be viewed as an arithmetic analogue of the following easy fact in differential algebra. Let $G = GL_n$ be equipped with the involution be given by transposition $x^\dagger = x^t$ and let $q \in GL_n = GL_n(R)$ be such that $q^t = \pm q$. For $a \in \mathfrak{gl}_n(A)$ let δ_a be the unique derivation of $A = R[x, \det(x)^{-1}]$ whose restriction to R is δ and such that $\delta_a x = ax$. Let $\delta_{A,0} = \delta_0$ so $\delta_0 x = 0$.

Proposition 4.18. *With the above notation the following hold.*

1) The set of all $a \in \mathfrak{gl}_n(A)$ such that δ_a is horizontal with respect to $\mathcal{H}$ is a torsor for the Lie algebra $L(SO(q))(A)$. For any such a we have $\delta_a(x^t q x) = 0$; so if $a \in L(SO(q)) = L(SO(q))(R)$ then, for any solution $u \in GL_n$ of $\delta u = au$, we have $\delta(u^t q u) = 0$.

2) There is exactly one $a \in \mathfrak{gl}_n(A)$ such that δ_a is horizontal and symmetric with respect to $\mathcal{H}$; it belongs to $\mathfrak{gl}_n = \mathfrak{gl}_n(R)$ and it is given by

$$a = -\frac{1}{2} q^{-1} \delta q.$$

The second assertion of 1) morally says that $x^t q x$ is a "prime integral" for the equation $\delta u = au$.

Proof. The commutativity of the diagram 4.24 is equivalent to

$$(4.26) \qquad\qquad a^t q + qa = -\delta q,$$

while the commutativity of 4.25 is equivalent to

$$(4.27) \qquad a^t q - qa = 0.$$

Clearly if a_1 is a solution to 4.26, $b \in \mathfrak{gl}_n$, and $a_2 = a_1 + b$ then a_2 is a solution to 4.26 if and only if b is a solution to the equation $b^t q + qb = 0$ i.e. if and only if $b \in L(SO(q))(A)$. This proves the first assertion of 1). The second assertion of 1) then follows. To check assertion 2) note that $a = -\frac{1}{2}q^{-1}\delta q$ is a solution to both 4.26 and 4.27. Now if a_1 and a_2 are solutions to 4.26 and 4.27 then $b := a_2 - a_1$ is a solution to the equations $b^t q + qb = 0$ and $b^t q - qb = 0$. Hence $qb = 0$ hence $b = 0$. □

A δ-algebraic analogue of Proposition 4.10 is the following Proposition. Here we take G be group of all matrices in GL_{n+1} of the form $\begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix}$ with $x \in GL_n$, $t \in GL_1$, and either $t^n = \det(x)^2$ if n is odd or $t^{n/2} = \det(x)$ if n is even. So $A = R[x, \det(x)^{-1}, \det(x)^{2/n}]$, where $\det(x)^{2/n}$ is either the nth root of $\det(x)^2$ if n is odd or the $n/2$-th root of $\det(x)$ if n is even. For $a \in \mathfrak{gl}_n(A)$ we denote by δ_a the unique derivation of A whose restriction to R is δ and such that $\delta_a x = ax$. We let $\delta_{A,0} = \delta_0$ so $\delta_0 x = 0$. Finally let G be equipped with its natural involution 1.12 and let $q = 1 \in G$; so the map $\mathcal{H} : A \to A$ is defined by $\mathcal{H}(x) = \det(x)^{2/n} \cdot 1$.

Proposition 4.19. *With the above notation we have:*

1) Let $a \in \mathfrak{gl}_n(A)$; then δ_a is horizontal with respect to $\mathcal{H}$ if and only if $tr(a) = 0$, i.e. if and only if a belongs to the Lie algebra $L(SL_2)(A)$. For any such a we have $\delta_a(\det(x)) = 0$; hence if $a \in L(SL_2) = L(SL_2)(R)$ then, for any solution $u \in GL_n$ of the equation $\delta u = au$, we have $\delta(\det(u)) = 0$.

2) Let $a \in \mathfrak{gl}_n(A)$; then δ_a is horizontal and symmetric with respect to $\mathcal{H}$ if and only if $a = 0$.

The second assertion in 1) morally says that $\det(x)$ is a "prime integral" for the equation $\delta u = au$.

Proof. We have the formula $\delta_a(\det(x)) = tr(a) \cdot \det(x)$. The commutativity of 4.24 is equivalent to

$$(4.28) \qquad \delta_a(\det(x)^{2/n}) = 0$$

hence to $\delta_a(\det(x)) = 0$, hence to $tr(a) = 0$ which proves 1). To check 2) note that the commutativity of 4.25 is equivalent to

$$(4.29) \qquad (\delta_a(\det(x)^{2/n} \cdot x^{-1})) \cdot x = (\det(x)^{2/n}) \cdot x^{-1} \cdot (\delta_a x).$$

On the other hand one has $\delta_a x = -x^{-1}a$. So 4.28 and 4.29 imply $x^{-1}ax = -x^{-1}ax$ i.e. $a = 0$; this proves 2). □

REFERENCES

[1] A. Buium, *Geometry of differential polynomial functions I: algebraic groups*, Amer J. Math. 115, 6 (1993), 1385-1444.

[2] A. Buium, *Differential characters of Abelian varieties over p-adic fields*, Invent. Math., 122 (1995), pp. 309-340.

[3] A. Buium, *Arithmetic Differential Equations*, Math. Surveys and Monographs, 118, American Mathematical Society, Providence, RI, 2005. xxxii+310 pp.

[4] A. Buium, T. Dupuy, *Arithmetic differential equations on GL_n, I: differential cocycles*, preprint.

[5] A. Buium, T. Dupuy, *Arithmetic differential equations on GL_n, III: Galos groups*, preprint.

[6] A. Buium, A. Saha, *The first p-jet space of an elliptic curve: global functions and lifts of Frobenius*, preprint.
[7] A. Buium, Yu. I. Manin, *Arithmetic differential equations of Painlevé VI type*, preprint.
[8] E.R. Kolchin, *Differential algebra and algebraic groups*. Pure and Applied Mathematics, Vol. 54. Academic Press, New York-London, 1973. xviii+446 pp.
[9] M. Singer, M. van der Put, *Galois theory of difference equations*, LNM, Springer 1997.

University of New Mexico, Albuquerque, NM 87131
E-mail address: buium@math.unm.edu