ARITHMETIC DIFFERENTIAL EQUATIONS ON GL_n, III GALOIS GROUPS

ALEXANDRU BUIUM AND TAYLOR DUPUY

ABSTRACT. Differential equations have arithmetic analogues [3] in which derivatives are replaced by Fermat quotients; these analogues are called arithmetic differential equations and the present paper is concerned with the "linear" ones. The equations themselves were introduced in a previous paper [5]. In the present paper we deal with the solutions of these equations as well as with the δ-Galois groups attached to the solutions.

1. Introduction, main definitions, and main results

In a series of papers beginning with [2] an arithmetic analogue of differential equations was introduced in which derivations are replaced by Fermat quotient operators. Cf. [3] for an overview. It is then natural to ask for an arithmetic analogue of linear differential equations. Classically a linear differential equation has the form

$$\frac{d}{dz}U = A \cdot U \tag{1.1}$$

where A is, say, a matrix of meromorphic functions on a domain in the complex plane $\mathbb{C}$ with complex variable z, and U is a matrix of unknown meromorphic functions (on a smaller domain). A basic object attached to 1.1 is its differential Galois group which is an algebraic subgroup of $GL_n(\mathbb{C})$. This concept is classical, going back to Picard and Vessiot. A modern version of the theory was developed by Kolchin [8] in the framework of differential algebra. In the present paper we ask for arithmetic analogues, in the spirit of [2, 3], of all of these concepts. The beginnings of such a theory were sketched in [5], where a concept of arithmetic linear differential equation on an algebraic group was introduced; the present paper deals with the solutions of these equations. Our paper is, in principle, a sequel to [4, 5] but it is entirely independent of [5]. Indeed very little of the theory in [2, 3, 4, 5] will be needed here and everything that will be needed will be reviewed in this Introduction. Our main purpose here will be to attach a Galois group to each given solution of a given linear arithmetic differential equation and to study some basic properties of this group; morally the Galois groups of such equations should (and in some sense will) appear as subgroups of "$GL_n(\mathbb{F}_1^a)$" where $\mathbb{F}_1^a$ is the "algebraic closure of the field with one element".

1.1. **Main definitions.** We denote by R the unique complete discrete valuation ring with maximal ideal generated by an odd prime p and with residue field $k = R/pR = \mathbb{F}_p^a$, the algebraic closure of $\mathbb{F}_p$. So R can be identified with the ring $W(k)$ of p-typical vectors on k. We denote by $\phi : R \to R$ the unique ring homomorphism lifting the p-power Frobenius on the residue field k and we denote by $\delta : R \to R$ the map $\delta a = \frac{\phi(a)-a^p}{p}$. We morally view δ as an arithmetic analogue of a derivation [2, 3]. 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. Recall that the reduction mod p map $R^\delta \to k$ is an isomorphism of monoids. Also we denote by K the fraction field of R. As usual we denote by $\mathfrak{gl}_n(A)$ the ring of $n \times n$ matrices with coefficients in a ring A and we denote by $GL_n(A)$ the group of invertible elements of that ring. If $A = R$ we will often write GL_n, $\mathfrak{gl}_n$ instead of $GL_n(R)$, $\mathfrak{gl}_n(R)$; more generally for a smooth scheme X over R we will often write X instead of $X(R)$. If $u = (u_{ij}) \in \mathfrak{gl}_n(A)$ then we set $\phi(u) = (\phi(u_{ij}))$, $\delta u = (\delta u_{ij})$, $u^{(p)} = (u_{ij}^p)$; hence $\phi(u) = u^{(p)} + p\delta u$. In what follows we fix a matrix $\Delta(x) \in \mathfrak{gl}_n(A)$ with entries in the ring $A = \mathcal{O}(GL_n)\hat{} = R[x, \det(x)^{-1}]\hat{}$ where x is an $n \times n$ matrix of indeterminates and $\hat{}$ means p-adic completion. (This matrix is usually canonically associated to the problem at hand and is uniquely determined by natural symmetry conditions that come with the problem; see [5]. We will not be concerned with explaining these conditions here but rather we will concentrate on the abstract case when Δ is arbitrary or on specific Examples, cf. 1.1, 1.2, 1.3 below). Set $\Phi(x) = x^{(p)} + p\Delta(x)$. Moreover for $\alpha \in \mathfrak{gl}_n = \mathfrak{gl}_n(R)$ set $\Delta^\alpha(x) = \alpha \cdot \Phi(x) + \Delta(x) = \alpha x^{(p)} + (1 + p\alpha)\Delta(x)$. By a Δ-*linear equation* we will then understand an equation of the form

$$\delta u = \Delta^\alpha(u) \tag{1.2}$$

where $u \in GL_n = GL_n(R)$; u is a referred to as a solution to the equation 1.4 and the set G^α of all $u \in GL_n$ such that 1.2 holds is referred to as the solution set of 1.2. If we set $\epsilon = 1 + p\alpha$ and $\Phi^\alpha(x) = \epsilon \cdot \Phi(x)$ then 1.2 is equivalent to

$$\phi(u) = \Phi^\alpha(u). \tag{1.3}$$

This concept of linearity is always relative to a given Δ. On the other hand one can define a δ-linear equation to be an equation which is Δ-linear for some Δ. Note by the way that there is a natural concept of equivalence on $\mathfrak{gl}_n(A)$ which lies in the background of our discussion; two matrices Δ_1 and Δ_2 in $\mathfrak{gl}_n(A)$ are equivalent if and only if there exists $\alpha \in \mathfrak{gl}_n(R)$ such that $\Delta_1 = \Delta_2^\alpha$. We have that $\delta u = \Delta_1(u)$ is Δ_2-linear if and only if Δ_1 and Δ_2 are equivalent.

A function $\mathcal{H} \in R[x, \det(x)^{-1}]\hat{}$ will be called a *prime integral* for the Δ-linear equation 1.2 if for any solution u of 1.2 we have

$$\delta(\mathcal{H}(u)) = 0.$$

(Intuitively $\mathcal{H}$ is "constant" along the solutions of 1.2.) More generally an m-tuple of functions $\mathcal{H} \in (R[x, \det(x)^{-1}]\hat{})^m$ is called a prime integral of our equation if each of the components of $\mathcal{H}$ is a prime integral.

The basic examples we have in mind are those in [5] and are going to be reviewed below; they are related to the classical groups and for their basic properties we refer to [5]. For the purpose of the present article we will not need to review these properties.

Example 1.1. We say that Δ is of type GL_n if $\Delta = 0$. So in this case $\Phi(x) = x^{(p)}$ and 1.2 and 1.3 become

$$\delta u = \alpha \cdot u^{(p)} \tag{1.4}$$

and

$$\phi(u) = \epsilon \cdot u^{(p)} \tag{1.5}$$

respectively. It is worth noting that 1.5 is *not* an instance of a linear difference equation in the sense of [11]. Indeed a linear difference equation for ϕ has the form

$$\phi(u) = \epsilon \cdot u \tag{1.6}$$

rather than the form 1.5.

Example 1.2. We say that Δ is of type SL_n if

$$\Delta(x) = \frac{\lambda(x) - 1}{p} \cdot x^{(p)}$$

where $p \not| n$ and

$$\lambda(x) := \left(\frac{\det(x^{(p)})}{\det(x)^p} \right)^{-1/n}. \tag{1.7}$$

Here the $-1/n$ power is computed using the usual series $(1 + pt)^a \in \mathbb{Z}_p[[t]]$ for $a \in \mathbb{Z}_p$. In this case $\Phi(x) = \lambda(x) \cdot x^{(p)}$ and the equations 1.2 and 1.3 become

$$\delta u = \left(\lambda(u) \cdot \alpha + \frac{\lambda(u) - 1}{p} \right) \cdot u^{(p)} \tag{1.8}$$

and

$$\phi(u) = \lambda(u) \cdot \epsilon \cdot u^{(p)} \tag{1.9}$$

respectively. Note that, in this case, $\Phi(u) \in SL_n$ for any $u \in SL_n$. In this context, following [5], it is useful to introduce the δ-Lie algebra $\mathfrak{sl}_{n,\delta}$ of SL_n as being the set of all $\alpha \in \mathfrak{gl}_n$ such that $1 + p\alpha \in SL_n$, in other words

$$\mathfrak{sl}_{n,\delta} = \{\alpha \in \mathfrak{gl}_n; tr(\alpha) + ... + p^{n-1} \det(\alpha) = 0\}.$$

This is not a subgroup of $(\mathfrak{gl}_n, +)$ where $+$ is the usual addition of matrices but rather a subgroup of $(\mathfrak{gl}_n, +_\delta)$ where $a +_\delta b := a + b + pab$; the latter group is the group of R-points of a group in the category of p-adic formal schemes; cf. [5].) This is in analogy with the Lie algebra $\mathfrak{sl}_n$ of SL_n which is given by

$$\mathfrak{sl}_n = \{\alpha \in \mathfrak{gl}_n; tr(\alpha) = 0\}.$$

Note also that if $\alpha \in \mathfrak{sl}_{n,\delta}$ then $\mathcal{H}(x) := \det(x)$ is a prime integral for the Δ-linear equation $\delta u = \Delta^\alpha(u)$. Indeed if u is a solution if this equation and $\epsilon = 1 + p\alpha$ then

$$\begin{aligned} \phi(\det(u)) &= \det(\phi(u)) \\ &= \det\left(\lambda(u) \cdot \epsilon \cdot u^{(p)}\right) \\ &= \lambda(u)^n \cdot \det(\epsilon) \cdot \det(u^{(p)}) \\ &= \det(u)^p, \end{aligned}$$

hence $\delta(\det(u)) = 0$.

Example 1.3. Let $q \in GL_n$ be defined as

$$\begin{pmatrix} 0 & 1_r \\ -1_r & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1_r \\ 1_r & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1_r \\ 0 & 1_r & 0 \end{pmatrix}, \tag{1.10}$$

where $n = 2r, 2r, 2r + 1$ respectively. Let $SO(q) \subset SL_n$ be the subgroup defined by the equations $x^t qx = q$; for q as above $SO(q)$ is denoted by $Sp_{2r}, SO_{2r}, SO_{2r+1}$ respectively. We say that Δ is of type $SO(q)$ if

$$\Delta(x) = x^{(p)} \cdot \frac{1}{p}(\Lambda(x) - 1),$$

where

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

Here, again, the $1/2$ power is computed using the usual series $(1+pT)^a \in \mathfrak{gl}_n(\mathbb{Z}_p[[T]])$ for $a \in \mathbb{Z}_p$, $T = (t_{ij})$. In this case we have $\Phi(x) = x^{(p)} \cdot \Lambda(x)$. Recall from [5] that $\Phi(x)^t q \Phi(x) = (x^t q x)^{(p)}$. Note also that, in this case, $\Phi(u) \in SO(q)$ for any $u \in SO(q)$; cf. [5]. In this context, following [5], it is useful to introduce the δ-Lie algebra $\mathfrak{so}(q)_\delta$ of $SO(q)$ as being the set of all $\alpha \in \mathfrak{gl}_n$ such that $1 + p\alpha \in SO(q)$, in other words

$$\mathfrak{so}(q)_\delta = \{\alpha \in \mathfrak{gl}_n; \alpha^t q + q\alpha + p\alpha^t q \alpha = 0\}.$$

This is, again, a subgroup of $(\mathfrak{gl}_n, +_\delta)$; and this is, again, in analogy with the Lie algebra $\mathfrak{so}(q)$ of $SO(q)$ which is given by

$$\mathfrak{so}(q) = \{\alpha \in \mathfrak{gl}_n; \alpha^t q + q\alpha = 0\}.$$

Note also that if $\alpha \in \mathfrak{so}(q)_\delta$ then $\mathcal{H}(x) := x^t q x$ is a prime integral for the Δ-linear equation $\delta u = \Delta^\alpha(u)$. Indeed, if u is a solution of this equation and $\epsilon = 1 + p\alpha$ then, using the identity $\Phi(x)^t q \Phi(x) = (x^t q x)^{(p)}$, we get

$$\begin{array}{rcl} \phi(u^t q u) & = & \phi(u)^t q \phi(u) \\ & = & \Phi(u)^t \epsilon^t q \epsilon \Phi(u) \\ & = & \Phi(u)^t q \Phi(u) \\ & = & (u^t q u)^{(p)}, \end{array}$$

which implies $\delta(u^t q u) = 0$.

1.2. **Main results.** One has an existence and uniqueness result for our equations 1.2; cf. Propositions 2.1, 2.5, 2.6, and Remark 2.3 in the body of the paper:

Theorem 1.4. *Let $u_0 \in GL_n$ and $\alpha \in \mathfrak{gl}_n$ and let Δ be arbitrary. Then the following hold:*

1) There is a unique $u \in GL_n$ satisfying 1.2 such that $u \equiv u_0$ mod p.

2) If Δ, u_0, and α have entries in a complete valuation subring $\mathcal{O}$ of R then u also has entries in $\mathcal{O}$.

3) If $u_0 \in SL_n$, $\alpha \in \mathfrak{sl}_{n,\delta}$, and Δ is of type SL_n then $u \in SL_n$.

4) If $u_0 \in SO(q)$, $\alpha \in \mathfrak{so}(q)_\delta$, and Δ is of type $SO(q)$ then $u \in SO(q)$.

5) If u_0 and α have entries in a valuation δ-subring $\mathcal{O}$ of R with finite residue field and either Δ is of type GL_n (i.e. $\Delta = 0$) or Δ is of type SL_n and $u \in SL_n$ then u has entries in a δ-subring of R which is generically finite over $\mathcal{O}$.

Here by a δ-subring $\mathcal{O}$ of R we understand a subring with $\delta\mathcal{O} \subset \mathcal{O}$. By a valuation subring of R we mean the intersection of R with a subfield of the field of fractions K of R. Also an extension of integral domains is called generically finite if the induced extension between fraction fields is finite.

The above theorem allows us to introduce the first steps in a δ-Galois theory attached to Δ-linear equations 1.4. In particular we will attach δ-Galois groups to such equations and prove results about their form in "generic" cases. Here are some details. Start with a δ-subring $\mathcal{O} \subset R$, let $\alpha \in \mathfrak{gl}_n(\mathcal{O})$ and let $u \in GL_n(R)$ be a solution of 1.2. Let $x', x'', ...$ be new matrices of indeterminates and consider the polynomial ring

$$\mathcal{O}\{x\} := \mathcal{O}[x, x', x'', ...].$$

There is a unique ring endomorphism ϕ of $\mathcal{O}\{x\}$ whose restriction to $\mathcal{O}$ is ϕ and such that $\phi(x) = x^{(p)} + px'$, $\phi(x') = (x')^{(p)} + px''$, etc. Define the map $\delta : \mathcal{O}\{x\} \to \mathcal{O}\{x\}$

by $\delta f = p^{-1}(\phi(f) - f^p)$. We let $I_{u/\mathcal{O}}$ be the kernel of the unique $\mathcal{O}$-algebra map $\mathcal{O}\{x\} \to R$, sending $x \mapsto u$, $x' \to \delta u$, $x'' \mapsto \delta^2 u$, etc. (the ideal of δ-algebraic relations among the entries of u) and we let $\Sigma_{u/\mathcal{O}}$ be the subgroup of $GL_n(\mathcal{O})$ consisting of all matrices c such that the $\mathcal{O}$-automorphism $\sigma_c : \mathcal{O}\{x\} \to \mathcal{O}\{x\}$ defined by $\sigma_c(x) = xc$, $\sigma(x') = \delta(xc)$, $\sigma(x'') = \delta^2(xc)$, etc. satisfies $\sigma_c(I_{u/\mathcal{O}}) = I_{u/\mathcal{O}}$. We also consider the matrix

$$\Phi_u(x) = \Phi(u)^{-1}\Phi(ux),$$

and the subset G_u of $G = GL_n(R)$ consisting of the solutions v to the equation

$$\phi(v) = \Phi_u(v). \tag{1.11}$$

Finally we define the δ-Galois set of $u/\mathcal{O}$ as the following subset of G:

$$G_{u/\mathcal{O}} = \Sigma_{u/\mathcal{O}} \cap G_u.$$

Note that equation 1.11 is equivalent to yet another equation namely to

$$\delta v = \Delta_u(v)$$

where $\Delta_u(x) := \frac{1}{p}(\Phi_u(x) - x^{(p)})$. (This equation is not Δ-linear but rather Δ_u-linear.)

Example 1.5. It is easy to see that if Δ is of type GL_n, SL_n, or $SO(q)$ and $\mathcal{H}(x)$ equals 1, $\det(x)$, $x^t qx$ respectively then for any u in $GL_n, SL_n, SO(q)$ respectively we have that $\mathcal{H}(x)$ is a prime integral of the Δ_u-linear equation $\delta v = \Delta_u(v)$; in other words $\delta(\mathcal{H}(v)) = 0$ for all $v \in G_u$. Cf. Proposition 3.8.

The subset $G_{u/\mathcal{O}}$ of G is not a priori a subgroup; but it is a subgroup in case $\Delta(x)$ has entries in $\mathcal{O}[x]$, e.g. if $\Delta(x) = 0$. We will mainly be interested below in the case $\Delta = 0$.

To state our result below we let $W \subset G$ be the Weyl group of all matrices obtained from the identity matrix by permuting its columns. Let $T \subset G$ be the maximal torus of diagonal matrices with entries in R and consider the normalizer $N = WT = TW$ of T in G. We denote by $1 \in G$ the identity matrix. Also consider the subset (not a subgroup!) G^δ of G consisting of all elements of G with entries in the monoid of constants R^δ. Let $N^\delta = N \cap G^\delta$ and $T^\delta = T \cap G^\delta$. Then N^δ and T^δ are subgroups (not just subsets!) of G. Also $N^\delta = WT^\delta = T^\delta W$. We also use below the notation K^a for the algebraic closure of the fraction field K of R; the Zariski closed sets of $GL_n(K^a)$ are then viewed as (possibly reducible) varieties over K^a. A subgroup of $GL_n(K^a)$ is called diagonalizable if it is conjugate in $GL_n(K^a)$ to a subgroup of the group of diagonal matrices. The next result illustrates some "generic" features of our δ-Galois groups in case $\Delta = 0$; assertion 1) shows that the δ-Galois group is generically "not too large". Assertions 2) and 3) show that the δ-Galois group are generically "as large as possible". As we shall see presently, the meaning of the word *generic* is different in each of the 3 situations: in situation 1) *generic* means *outside a Zariski closed set*; in situation 2) *generic* means *outside a thin set* (in the sense of [10]); in situation 3) *generic* means *outside a set of the first category* (in the sense of Baire category).

Theorem 1.6. *Assume* $\Delta(x) = 0$.

1) There exists a Zariski closed subset $\Omega \subset GL_n(K^a)$ *not containing* 1 *such that for any* $u \in GL_n(R)\backslash\Omega$ *the following holds. Let* $\alpha = \delta u \cdot (u^{(p)})^{-1}$ *and let* $\mathcal{O}$ *be a* *valuation δ-subring of R containing α. Then $G_{u/\mathcal{O}}$ contains a normal subgroup of finite index which is diagonalizable.*

2) Let $\mathcal{O} = \mathbb{Z}_{(p)}$. There exists a thin set $\Omega \subset \mathbb{Q}^{n^2}$ such that for any $\alpha \in \mathbb{Z}^{n^2} \backslash \Omega$ there exists a solution u of the equation $\delta u = \alpha u^{(p)}$ with the property that $G_{u/\mathcal{O}}$ is a finite group containing the Weyl group W.

3) There exists a subset Ω of the first category in the metric space

$$X = \{u \in GL_n(R); u \equiv 1 \mod p\}$$

such that for any $u \in X \backslash \Omega$ the following holds. Let $\alpha = \delta u \cdot (u^{(p)})^{-1}$. Then there exists a valuation δ-subring $\mathcal{O}$ of R containing R^δ such that $\alpha \in \mathfrak{gl}_n(\mathcal{O})$ and such that $G_{u/\mathcal{O}} = N^\delta$.

Cf. Propositions 3.17, 3.13, 3.14, in the body of the paper.

The groups W and N^δ should be morally viewed as "incarnations" of "$GL_n(\mathbb{F}_1)$" and "$GL_n(\mathbb{F}_1^a)$" where "$\mathbb{F}_1$" and "$\mathbb{F}_1^a$" are the "field with element" and "its algebraic closure" respectively. This suggests that the δ-Galois theory we are proposing here should be viewed as a Galois theory over "$\mathbb{F}_1$"; this is consistent, for instance, with ideas put forward in [3, 1]. By the way Theorem 1.6 suggests the following question: *Is the δ-Galois group $G_{u/\mathcal{O}}$ always a subgroup of N?* The answer to this turns out to be negative in general (cf. Remark 3.11) but something close to an affirmative answer may still be true.

We end with a couple of remarks comparing the theory above with some familiar situations.

Remark 1.7. It is worth comparing Equation 1.5 with the familiar linear equations in analysis in the case $n = 1$; in case $n = 1$ Equation 1.5 is, of course,

$$\phi(u) = \epsilon \cdot u^p \tag{1.12}$$

where $\epsilon = 1 + p\alpha$, $\alpha \in R$, $u \in R^\times$. This equation can be solved as follows. Write $\epsilon = \exp(p\beta)$, where $\exp : pR \to 1 + pR$ is the group isomorphism given by the p-dic exponential and $\beta \in R$. Then the set of solutions to 1.12 consists of all $u \in R^\times$ of the form

$$u = \zeta \cdot \exp\left(\sum_{n=1}^{\infty} p^n \phi^{-n}(\beta)\right) \tag{1.13}$$

where $\zeta \in R^\times$, $\delta\zeta = 0$. On the other hand consider the group homomorphism $\psi : R^\times \to R$ defined by

$$u \mapsto \psi(u) = \frac{1}{p} \log\left(\frac{\phi(u)}{u^p}\right) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{p^{n-1}}{n} \left(\frac{\delta u}{u^p}\right)^n \tag{1.14}$$

where log is the p-adic logarithm. Then Equation 1.12 is equivalent to the equation

$$\psi(u) = \beta \tag{1.15}$$

Now the homomorphism ψ above should be viewed as an analogue of the logarithmic derivative map $\mathcal{M}(D)^\times \to \mathcal{M}(D)$,

$$u \mapsto u'/u,$$

where $\mathcal{M}(D)$ is the field of meromorphic functions on a disk $D \subset \mathbb{C}$, say, and $u' = \frac{du}{dz}$, where z is a complex variable. So the analogue, in analysis, of Equation

1.15 is the equation

$$\frac{u'}{u} = \beta, \tag{1.16}$$

where $\beta \in \mathcal{M}(D)$. For β holomorphic in D the solutions to Equation 1.16 are of the form

$$u = c \cdot \exp\left(\int \beta dz\right) \tag{1.17}$$

where exp is the complex exponential and $c \in \mathbb{C}$. Hence the elements 1.13 in $R^\times$ should be viewed as arithmetic analogues of the functions 1.17 in $\mathcal{M}(D)$.

Remark 1.8. It is worth comparing the Δ-linear equations 1.4 with Lang's framework in [9]. Indeed in [9] Lang considers the map

$$GL_n(k) \to GL_n(k), \quad a \mapsto a^{(p)} \cdot a^{-1}, \tag{1.18}$$

where k is an algebraically closed field of characteristic p. This is a non-abelian cocycle for the adjoint action of $GL_n(k)$ on itself. A natural lift of 1.18 to characteristic zero is the map

$$GL_n(R) \to GL_n(R), \quad a \mapsto \phi(a) \cdot a^{-1}. \tag{1.19}$$

The fiber of 1.19 over $\alpha \in \mathfrak{gl}_n(R)$ consists of the solutions $u \in GL_n(R)$ to the *linear difference equation* 1.6 which, as already noted, is quite different from the equation 1.5. By the way the equation 1.6 can be studied in at least two ways leading to two rather different theories: one way is from the viewpoint of difference algebra [11]; the other way is from the δ-arithmetic viewpoint [3]. The δ-arithmetic viewpoint on equations 1.6 tends to lead to profinite groups; our δ-arithmetic study of the equations 1.5 will lead to torsion groups (hence to inductive, rather than projective, limits of finite groups). This makes the δ-arithmetic study of equations 1.5 and the δ-arithmetic study of equations 1.6 quite different in nature. Neverthless there are cases (such as that of abelian varieties [2]) where one encounters combinations of profinite and torsion groups; so it is conceivable that the δ-arithmetic theories of 1.5 and 1.6 can be unified.

On the other hand 1.18 has another natural lift to characteristic zero which is

$$GL_n(R) \to GL_n(R), \quad a \mapsto a^{(p)} \cdot a^{-1}. \tag{1.20}$$

Composing this with inversion $b \mapsto b^{-1}$ one gets a map

$$GL_n(R) \to GL_n(R), \quad a \mapsto a \cdot (a^{(p)})^{-1}. \tag{1.21}$$

Note now that the set of solutions to any of the equations 1.5 is a fiber of the map

$$GL_n(R) \to GL_n(R), \quad a \mapsto \phi(a) \cdot (a^{(p)})^{-1} \tag{1.22}$$

But 1.21 and 1.22 induce by restriction the same map $GL_n(\mathbb{Z}_p) \to GL_n(\mathbb{Z}_p)$. This connection points towards a link between the arithmetic of usual coverings such as 1.21 and the "δ-Galois theory" of Δ-linear equations such as 1.5; this will be seen in the proof of assertion 2 in Theorem 1.6.

The paper is organized as follows. In section 2 we provide the proof of Theorem 1.4. In section 3 we amplify our definitions and foundational discussion and we prove, in particular, Theorem 1.6.

1.3. **Acknowledgement.** The authors are indebted to P. Cartier for inspiring discussions. Also the first author would like to acknowledge partial support from the Hausdorff Institute of Mathematics in Bonn and from the NSF through grant DMS 0852591.

2. Existence, uniqueness, and rationality of solutions

The following proposition is an existence and uniqueness result for solutions of Δ-linear equations. In the Propositions below $\Delta(x)$ is arbitrary unless otherwise stated and, as usual, $\Phi(x) = x^{(p)} + p\Delta(x)$.

Proposition 2.1. *Let $u_0 \in GL_n(R)$, and $\alpha \in \mathfrak{gl}_n(R)$. Then the Δ-linear equation $\delta u = \alpha \cdot \Phi(u) + \Delta(u)$ has a unique solution $u \in GL_n(R)$ such that $u \equiv u_0$ mod p.*

Proof. Recall that the equation above is equivalent to $\phi(u) = \epsilon \cdot \Phi(u)$ where $\epsilon = 1 + p\alpha$. To check the uniqueness of the solution assume $\phi(u) = \epsilon \cdot \Phi(u)$ and $\phi(v) = \epsilon \cdot \Phi(v)$ with $u, v \in GL_n(R)$, $u \equiv v$ mod p. Then we prove by induction that $u \equiv v$ mod p^n. Indeed if the latter is the case then $u^{(p)} \equiv v^{(p)}$ mod p^{n+1} and $\Delta(u) \equiv \Delta(v)$ mod p^{n+1} hence $\Phi(u) \equiv \Phi(v)$ mod p^{n+1}. Hence $\phi(u) \equiv \phi(v)$ mod p^{n+1}. Hence $u \equiv v$ mod p^{n+1}.

To check the existence of a solution u such that $u \equiv u_0$ mod p we define a sequence of matrices $u_n \in GL_n(R)$ by the formula

$$u_{n+1} = \phi^{-1}(\epsilon \cdot \Phi(u_n)), \quad n \geq 0.$$

We claim that for all $n \geq 0$ we have

$$\phi(u_n) \equiv \epsilon \cdot \Phi(u_n) \mod p^{n+1}.$$

Assuming the claim we get $u_{n+1} \equiv u_n$ mod p^{n+1} hence u_n converges p-adically to some $u \in GL_n(R)$. Also $\phi(u) = \epsilon \cdot \Phi(u)$ which ends our proof. We are left with checking the claim. We proceed by induction. The case $n = 0$ is clear. Assume now $\phi(u_n) \equiv \epsilon \cdot \Phi(u_n)$ mod p^{n+1}. Hence

$$\phi^{-1}(\epsilon \cdot \Phi(u_n)) \equiv u_n \quad mod \quad p^{n+1},$$

hence

$$\Phi(\phi^{-1}(\epsilon \cdot \Phi(u_n))) \equiv \Phi(u_n) \quad mod \quad p^{n+2}.$$

Hence

$$\begin{aligned} \epsilon \cdot \Phi(u_{n+1}) &= \epsilon \cdot \Phi(\phi^{-1}(\phi(u_{n+1}))) \\ &= \epsilon \cdot \Phi(\phi^{-1}(\epsilon \cdot \Phi(u_n))) \\ &\equiv \epsilon \cdot \Phi(u_n) \mod p^{n+2} \\ &= \phi(u_{n+1}), \end{aligned}$$

and the induction step follows. □

Remark 2.2. If, in Proposition 2.1, $\Delta = 0$, $n = 1$, and $u_0 \equiv \zeta$ mod p where $\zeta \in R$ is a root of unity, the solution u has a closed form:

$$u = \zeta \cdot \epsilon_{-1} \cdot \epsilon_{-2}^{p} \cdot \epsilon_{-3}^{p^2} \cdot \ldots \quad \text{(convergent product)}$$

where $\epsilon_i = \phi^i(\epsilon)$ for $i \in \mathbb{Z}$. This computation implies the formula in Remark 1.7.

Remark 2.3. If in Proposition 2.1 we have Δ of type SL_n, $u_0 \in SL_n(R)$, and $\alpha \in \mathfrak{sl}_{n,\delta}$ then $u \in SL_n(R)$. Indeed this follows because $\Phi(a) \in SL_n(R)$ and $\phi^{-1}(a) \in SL_n(R)$ for all $a \in SL_n(R)$; hence if u_n is as in the proof of that Proposition then $u_n \in SL_n(R)$. Similarly if Δ is of type $SO(q)$, $u_0 \in SO(q)$, and $\alpha \in \mathfrak{so}(q)_\delta$ then $u \in SO(q)$. The above proves assertions 3 and 4 in Theorem 1.4.

Remark 2.4. In notation of Propositon 2.1 the natural reduction map $G^\alpha \to GL_n(k)$ is a bijection. So each solution set G^α has a natural structure of group; but of course with this structure G^α is not a subgroup of $GL_n(R)$.

Let us address the question of "rationality" of solutions of Δ-linear equations.

Let $\mathcal{O} \subset R$ be a subring. Recall that $\mathcal{O}$ is called a δ-subring if $\delta\mathcal{O} \subset \mathcal{O}$. Also we say $\mathcal{O}$ is a a valuation subring of R if $\mathcal{O}$ is the intersection of R with a subfield of K. Any valuation subring of R is a discrete valuation ring with maximal ideal generated by p. Note that if $\mathcal{O}$ is a valuation subring which is complete then either $\mathcal{O} = R$ or there exists $\nu \geq 1$ such that $\mathcal{O} = R^{\phi^\nu}$, the fixed ring of ϕ^ν; in particular such an $\mathcal{O}$ is automatically a δ-subring. An extension $\mathcal{O} \subset \mathcal{O}'$ of subrings of R will be called generically finite if the extension of their fraction fields is finite; if in addition $\mathcal{O}$ is a valuation subring then $\mathcal{O}'$ is a localization of a finite extension of $\mathcal{O}$; if, in addition $\mathcal{O}$ is complete then any generically finite extension of $\mathcal{O}$ in R is finite.

Proposition 2.5. *Assume $\mathcal{O}$ is a complete valuation subring of R (hence also a δ-subring). If in Proposition 2.1 we have*

$$\Delta \in \mathfrak{gl}_n(\mathcal{O}[x, \det(x)]\hat{\ }), \quad u_0 \in GL_n(\mathcal{O}), \quad \alpha \in \mathfrak{gl}_n(\mathcal{O})$$

then $u \in GL_n(\mathcal{O})$.

Proof. Let $\mathcal{O} = R^{\phi^\nu}$. Then $\phi^\nu(u_0) = u_0$ and $\phi^\nu(\alpha) = \alpha$ hence $\phi^\nu(\epsilon) = \epsilon$, where $\epsilon = 1 + p\alpha$. Also $\phi^\nu(\Delta(a)) = \Delta(\phi^\nu(a))$, and hence $\phi^\nu(\Phi(a)) = \Phi(\phi^\nu(a))$, for all $a \in GL_n(R)$. Since $\phi(u) = \epsilon \cdot \Phi(u)$ and $u \equiv u_0$ mod p it follows that

$$\phi^{\nu+1}(u) = \phi^\nu(\epsilon)(\phi^\nu(\Phi(u))) = \epsilon \cdot \Phi((\phi^\nu(u)))$$

and $\phi^\nu(u) \equiv \phi^\nu(u_0) \equiv u_0$ mod p. By the uniqueness in Proposition 2.1 it follows that $\phi^\nu(u) = u$ hence $u \in GL_n(\mathcal{O})$. □

Proposition 2.6. *Assume $\mathcal{O}$ is a valuation δ-subring of R with finite residue field. Assume in Proposition 2.1 that one of the following holds:*

1) Δ is of type GL_n (i.e. $\Delta = 0$), $u_0 \in GL_n(\mathcal{O})$, and $\alpha \in \mathfrak{gl}_n(\mathcal{O})$.

2) Δ is of type SL_n, $u_0 \in SL_n(\mathcal{O})$, and $\alpha \in \mathfrak{sl}_{n,\delta} \cap \mathfrak{gl}_n(\mathcal{O})$.

Then there exists a generically finite extension of δ-subrings $\mathcal{O} \subset \mathcal{O}'$ of R such that $u \in GL_n(\mathcal{O}')$.

Proof. Assume we are in case 2; case 1 is similar (and indeed slightly easier).

By Proposition 2.5 if $\widehat{\mathcal{O}}$ is the completion of $\mathcal{O}$ then $u \in GL_n(\widehat{\mathcal{O}})$ hence there exists $\nu \geq 0$ such that $\phi^{\nu+1}(u) = u$. Let $N = n^2$ and identify the points of $\mathbb{A}^N$ with $n \times n$ matrices. Let

$$\lambda_\nu(u) = \phi^\nu(\lambda(u)) \cdot \phi^{\nu-1}(\lambda(u))^p \cdot \ldots \cdot \lambda(u)^{p^\nu}.$$

Using $\phi(u) = \lambda(u) \cdot \epsilon \cdot u^{(p)}$, and setting $\epsilon_j = \phi^j(\epsilon)$, we get

$$u = \phi^{\nu+1}(u) = \lambda_\nu(u) \cdot \varphi(u), \tag{2.1}$$

where $\varphi : \mathbb{A}^N \to \mathbb{A}^N$ is the morphism of schemes over $\mathcal{O}$ defined on points by

$$\varphi(v) = \epsilon_\nu(\epsilon_{\nu-1}(\epsilon_{\nu-2}(...(\epsilon v^{(p)})^{(p)})^{(p)}...)^{(p)}.$$

Let K^a be an algebraic closure of K, let F be the fraction field of $\mathcal{O}$, and let F^a be the algebraic closure of F in K^a. Note that $\varphi : \mathbb{A}^N(K^a) \to \mathbb{A}^N(K^a)$ is obtained by composing maps $\eta \mapsto \epsilon_j \eta$ with copies of the map $\eta \mapsto \eta^{(p)}$; both these types of maps are given by homogeneous polynomials (of degree 1 and p respectively) and have the property that the pre-image of 0 is 0. Hence φ is given by

$$\varphi(\eta) = (\Phi_1(\eta), ..., \Phi_N(\eta))$$

where $\Phi_1, ..., \Phi_N \in F[x_1, ..., x_N]$ are homogeneous polynomials of degree $p^{\nu+1} > 1$ and $\varphi^{-1}(0) = \{0\}$; hence $\Phi_1, ..., \Phi_N$ have no common zero in $\mathbb{A}^N(K^a)$ except at the origin. Consider an extra variable x_0 and consider the projective variety $V \subset \mathbb{P}^N$ defined by the equations

$$\Phi_j(x_1, ..., x_N) - x_0^{p^{\nu+1}-1} x_j = 0. \tag{2.2}$$

Clearly the intersection of V with the hyperplane $x_0 = 0$ is empty. So V has dimension zero hence $V(K^a)$ is finite. Since V is defined over F we have $V(K^a) = V(F^a)$. By equation 2.1 the point

$$(\lambda_\nu(u)^{-1/(p^\nu-1)} : u) \in \mathbb{P}^N(K)$$

belongs to $V(K)$ hence it belongs to $V(F^a)$. (Here the $1/(p^\nu-1)$-power is computed, again, using the series $(1 + pt)^a \in \mathbb{Z}_p[[t]]$ for $a \in \mathbb{Z}_p^\times$). It follows that

$$\lambda_\nu(u)^{1/(p^\nu-1)} \cdot u \in \mathbb{A}^N(F^a) = \mathfrak{gl}_n(F^a) \tag{2.3}$$

hence

$$\det(\lambda_\nu(u)^{1/(p^\nu-1)} \cdot u) \in F^a.$$

Since, by Remark 2.3, $\det(u) = 1$ we get $(\lambda_\nu(u)^{1/(p^\nu-1)})^n \in F^a$ hence

$$\lambda_\nu(u)^{1/(p^\nu-1)} \in F^a.$$

By 2.3 again we get $u \in GL_n(F^a)$ which ends the proof. □

Note that the Propositions in this section imply Theorem 1.4 in the Introduction. The consideration of the variety cut out by equations 2.2 is a trick from [6] and is an indication of an interesting link between the paradigm of the present paper and the arithmetic of dynamical systems on projective space.

3. δ-Galois groups

Recall that δ-Galois groups were defined in the Introduction. We will review here their definition and also define some related concepts. Then we will prove a series of Propositions amounting to Theorem 1.6.

As usual we often denote by G the group $GL_n(R)$ and by $\mathfrak{gl}_n$ the Lie algebra $\mathfrak{gl}_n(R)$. Let $\Delta(x) \in \mathfrak{gl}_n(R[x, \det(x)^{-1}]\hat{\ })$, x an $n \times n$ matrix of indeterminates, and let $\Phi(x) = x^{(p)} + p\Delta(x)$. Let $\alpha \in \mathfrak{gl}_n$, $\Delta^\alpha(x) = \alpha \cdot \Phi(x) + \Delta(x)$, and consider the Δ-linear equation

$$\delta u = \Delta^\alpha(u). \tag{3.1}$$

Recall that if $\Phi^\alpha(x) = \epsilon \cdot \Phi(x)$, $\epsilon = 1 + p\alpha$, then this equation is equivalent to the equation

$$\phi(u) = \Phi^\alpha(u). \tag{3.2}$$

Let G^α be the set of solutions to Equation 3.1, let $u \in G^\alpha$ be a fixed solution, let $\Phi_u(x) = \Phi(u)^{-1}\Phi(ux)$, $\Delta_u(x) = \frac{1}{p}(\Phi_u(v) - v^{(p)})$, and let G_u be the set of solutions $v \in G$ to the Δ_u-linear equation

$$\delta v = \Delta_u(v), \tag{3.3}$$

equivalently to the equation

$$\phi(v) = \Phi_u(v). \tag{3.4}$$

Let now $\mathcal{O}$ be a δ-subring of R. Assume $\alpha \in \mathfrak{gl}_n(\mathcal{O})$ and let $u \in GL_n(R)$ be a solution of Equation 3.1. Recall from the Introduction the ring $\mathcal{O}\{x\}$ and the operator δ on this ring. We let $I_{u/\mathcal{O}}$ be the kernel of the natural map $\mathcal{O}\{x\} \to R$, $x \mapsto u$, $x' \mapsto \delta u$, etc. We also denote by $\mathcal{O}\{u\} = \mathcal{O}[u, \delta u, \delta^2 u, ...]$ the image of $\mathcal{O}\{x\} \to R$. For any $c \in GL_n(\mathcal{O})$ we denote by σ_c the unique $\mathcal{O}$-algebra automorphism of $\mathcal{O}\{x\}$, commuting with δ, such that $\sigma_c(x) = xc$. We let $\Sigma_{u/\mathcal{O}}$ be the subgroup of $GL_n(\mathcal{O})$ consisting of all matrices c such that $\sigma_c(I_{u/\mathcal{O}}) = I_{u/\mathcal{O}}$. On the other hand we consider the subset G_u of $G = GL_n(R)$ consisting of the solutions v to the equation 3.4. Note that

$$uG_u \subset G^\alpha.$$

Indeed if $c \in G_u$ we have

$$\phi(uc) = \phi(u) \cdot \phi(c) = \epsilon \cdot \Phi(u) \cdot \phi(c) = \epsilon \cdot \Phi(uc)$$

so $uc \in G^\alpha$.

Definition 3.1. The δ-Galois set of $u/\mathcal{O}$ is the subset $G_{u/\mathcal{O}}$ of G defined by

$$G_{u/\mathcal{O}} = \Sigma_{u/\mathcal{O}} \cap G_u.$$

This is a priori a subset rather than a subgroup of G. Below we present a case in which $G_{u/\mathcal{O}}$ is a priori a subgroup; this case is also a motivation for our definition of $G_{u/\mathcal{O}}$ given above.

Before explaining this let us introduce the group $Aut_\delta(\mathcal{O}\{u\}/\mathcal{O})$ of all $\mathcal{O}$-algebra automorphisms σ of $\mathcal{O}\{u\}$ such that $\sigma \circ \delta = \delta \circ \sigma$ on $\mathcal{O}\{u\}$. Note that there is a natural injective group homomorphism $\Sigma_{u/\mathcal{O}} \to Aut_\delta(\mathcal{O}\{u\}/\mathcal{O})$. Hence there is a natural injection of sets

$$G_{u/\mathcal{O}} \to Aut_\delta(\mathcal{O}\{u\}/\mathcal{O}). \tag{3.5}$$

Assume now Δ has entries in the polynomial ring $\mathcal{O}[x]$; note that this is the case if Δ is of type GL_n (i.e. $\Delta = 0$) but this is not the case for Δ of type SL_n or $SO(q)$. Then $\mathcal{O}\{u\} = \mathcal{O}[u]$. Moreover $\sigma_c : \mathcal{O}\{x\} \to \mathcal{O}\{x\}$ preserves $I_{u/\mathcal{O}}$ if and only if the induced map $\sigma_c : \mathcal{O}[x] \to \mathcal{O}[x]$ preserves the kernel of $\mathcal{O}[x] \to \mathcal{O}[u]$, $x \mapsto u$. So if $\mathcal{O}[x] \to \mathcal{O}[u]$ is an isomorphism we have $\Sigma_{u/\mathcal{O}} = GL_n(\mathcal{O})$.

Lemma 3.2. *If Δ has entries in $\mathcal{O}[x]$ the set*

$$\tilde{G}_{u/\mathcal{O}} := \{\sigma \in Aut_\delta(\mathcal{O}[u]/\mathcal{O});\ u^{-1} \cdot \sigma(u) \in GL_n(\mathcal{O})\} \tag{3.6}$$

is a subgroup of $Aut_\delta(\mathcal{O}[u]/\mathcal{O})$ and the map $\tilde{G}_{u/\mathcal{O}} \to GL_n(\mathcal{O})$ sending any σ into $c_\sigma := u^{-1} \cdot \sigma(u)$ is an injective group homomorphism with image $G_{u/\mathcal{O}}$; in particular

$G_{u/\mathcal{O}}$ is a subgroup of $GL_n(\mathcal{O})$ and the injection 3.5 is a group homomorphism whose image is $\tilde{G}_{u/\mathcal{O}}$.

Proof. The fact that 3.6 is a subgroup and its map to $GL_n(\mathcal{O})$ is an injective group homomorphism is trivial.

Now let $\sigma \in Aut_\delta(\mathcal{O}[u]/\mathcal{O})$ be such that $c = c_\sigma := u^{-1} \cdot \sigma(u) \in GL_n(\mathcal{O})$ and let $\epsilon = 1 + p\alpha$. We have

$$\phi(\sigma(u)) = \phi(uc) = \phi(u) \cdot \phi(c) = \epsilon \cdot \Phi(u) \cdot \phi(c), \tag{3.7}$$

$$\sigma(\phi(u)) = \sigma(\epsilon \cdot \Phi(u)) = \epsilon \cdot \sigma(\Phi(u)) = \epsilon \cdot \Phi(\sigma(u)) = \epsilon \cdot \Phi(uc). \tag{3.8}$$

Here we used the fact that $\sigma(\Phi(u)) = \Phi(\sigma(u))$ which is true because Δ and hence Φ has polynomial entries. Since $\sigma \circ \delta = \delta \circ \sigma$ it follows that $\sigma \circ \phi = \phi \circ \sigma$ so, by 3.7 and 3.8, $\Phi(uc) = \Phi(u) \cdot \phi(c)$ hence $c \in G_u$. Also $c \in \Sigma_{u/\mathcal{O}}$ by the commutativity of the diagram

$$\begin{array}{ccc} \mathcal{O}\{x\} & \stackrel{\sigma_c}{\to} & \mathcal{O}\{x\} \\ \downarrow & & \downarrow \\ \mathcal{O}[u] & \stackrel{\sigma}{\to} & \mathcal{O}[u] \end{array} \tag{3.9}$$

Hence $c \in G_{u/\mathcal{O}}$.

Conversely if we start with $c \in G_{u/\mathcal{O}}$ then, since $\sigma_c(I_{u/\mathcal{O}}) = I_{u/\mathcal{O}}$, it follows that $\sigma_c : \mathcal{O}\{x\} \to \mathcal{O}\{x\}$ induces an automorphism $\sigma : \mathcal{O}[u] \to \mathcal{O}[u]$ with $\sigma(u) = uc$. On the other hand since $c \in G_u$ we have $\Phi(uc) = \Phi(u) \cdot \phi(c)$ hence, by 3.7 and 3.8, $\phi(\sigma(u)) = \sigma(\phi(u))$. It follows that $\sigma \circ \phi = \phi \circ \sigma$ on $\mathcal{O}[u]$ and hence $\sigma \circ \delta = \delta \circ \sigma$ on $\mathcal{O}[u]$. So $c = c_\sigma$ and we are done. $\square$

For our discussion below we recall from the Introduction that we denote by T, W, N the torus of diagonal matrices in G, the Weyl group of permutation matrices in G and the normalizer of T in G respectively; so $N = TW = WT$. Also if $G^\delta = \{a \in G; \delta a = 0\}$ we set $T^\delta = T \cap G^\delta$, $N^\delta = N \cap G^\delta = T^\delta W = WT^\delta$; G^δ is a subset of G while T^δ and N^δ are subgroups of G.

Definition 3.3. We say that Φ is right compatible with N if $\Phi(ac) = \Phi(a) \cdot c^{(p)}$ for all $a \in G$ and all $c \in N$.

Example 3.4. If Δ is if type $GL_n, SL_n, SO(q)$ then Φ is right compatible with N. By the way if Δ is of type GL_n (i.e. in case $\Delta = 0$) right compatibility of $\Phi(x) = x^{(p)}$ with N simply means that $(ac)^{(p)} = a^{(p)}c^{(p)}$ for $a \in G$ and $c \in N$.

Definition 3.5. We define the set

$$N_{u/\mathcal{O}} = N^\delta \cap G_{u/\mathcal{O}}.$$

Lemma 3.6. *If Φ is right compatible with N then*

1) $N_{u/\mathcal{O}}$ is a subgroup of G;

2) $N^\delta \subset G_u$.

Proof. Trivial. $\square$

Lemma 3.7. *Assume $\Delta = 0$.*

1) Assume the entries of one of the rows of u are algebraically independent over $\mathcal{O}$. Then $G_{u/\mathcal{O}} \subset N^\delta$ hence

$$G_{u/\mathcal{O}} = N_{u/\mathcal{O}}.$$

2) Assume the entries of u are algebraically independent over $\mathcal{O}$; then

$$G_{u/\mathcal{O}} = N^{\delta} \cap GL_n(\mathcal{O}).$$

3) Assume σ is an $\mathcal{O}$-automorphism of $\mathcal{O}[u]$ such that $\sigma(u) = uc$ with $c \in GL_n(\mathcal{O}) \cap G_u$. Then $c \in G_{u/\mathcal{O}}$.

4) Assume $n = 1$. Then $G_{u/\mathcal{O}} \subset N^{\delta} = G^{\delta}$.

5) We have an equality

$$\bigcap_{u \in G} G_u = N^{\delta}.$$

Proof. To prove 1 let $c \in G_{u/\mathcal{O}}$, hence $c \in G_u$, i.e. $(uc)^{(p)} = u^{(p)}\phi(c)$. If $c = (c_{ij})$ then for all m and j

$$\sum_{i=1}^{n} u_{mi}^{p}\phi(c_{ij}) = (\sum_{i=1}^{n} u_{mi}c_{ij})^{p}.$$

Let m be such that $u_{m1}, ..., u_{mn}$ are algebraically independent over $\mathcal{O}$. Identifying the coefficients of the monomials in $u_{m1}, ..., u_{mn}$ in the latter equality we get that for each j there exists an index $\tau(j)$ such that $c_{ij} = 0$ for all $i \neq \tau(j)$ and such that $c_{\tau(j)j}^{p} = \phi(c_{\tau(j)j})$. Since c is non-singular we must have that τ is a permutation and $c \in N^{\delta}$.

To prove assertion 2 note that $G_{u/\mathcal{O}} \subset N^{\delta} \cap GL_n(\mathcal{O})$ by assertion 1. Also $N^{\delta} \subset G_u$ by Lemma 3.6 and, since $\mathcal{O}[x] \to \mathcal{O}[u]$ is a isomorphism, we also have $\Sigma_{u/\mathcal{O}} = GL_n(\mathcal{O})$; hence $N^{\delta} \cap GL_n(\mathcal{O}) \subset G_u \cap \Sigma_{u/\mathcal{O}} = G_{u/\mathcal{O}}$.

To prove assertion 3 let $\sigma_c : \mathcal{O}\{x\} \to \mathcal{O}\{x\}$ be the unique $\mathcal{O}$-algebra homomorphism commuting with δ such that $\sigma_c(x) = xc$. Then $\sigma_c(I_{u/\mathcal{O}}) = I_{u/\mathcal{O}}$ by the commutativity of the diagram 3.9; hence $c \in \Sigma_{u/\mathcal{O}}$, hence $c \in G_{u/\mathcal{O}}$.

To prove assertion 4 let $c \in G_{u/\mathcal{O}}$; then $uc \in G^{\alpha}$ hence $\phi(u)\phi(c) = \epsilon u^p c^p$ where $\epsilon = 1 + p\alpha$. Since $\phi(u) = \epsilon u^p$ we get $\phi(c) = c^p$ hence $c \in G^{\delta} = N^{\delta}$.

To prove 5 note that the inclusion $\supset$ follows from Lemma 3.6. To prove the inclusion $\subset$ let c be in the intersection. Since R is uncountable one can find u with entries algebraically independent over the ring generated by the entries of $c, \delta c, \delta^2 c, ...$ Then one concludes that $c \in N^{\delta}$ by using the same argument as in the proof of assertion 1. □

Proposition 3.8.

1) Assume Δ is of type SL_n and let $u \in GL_n$. Then $\mathcal{H}(x) = \det(x)$ is a prime integral for the Δ_u-linear equation $\delta v = \Delta_u(v)$; in other words for any $v \in G_u$ we have $\delta(\det(v)) = 0$.

2) Assume Δ is of type $SO(q)$ and let $u \in SO(q)$. Then $\mathcal{H}(x) = x^t q x$ is a prime integral for the Δ_u-linear equation $\delta v = \Delta_u(v)$; in other words for any $v \in G_u$ we have $\delta(v^t q v) = 0$.

Proof. To check 1) note that since $v \in G_u$ we have

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

Taking determinants we get

$$\lambda(uv)^n \cdot \det((uv)^{(p)}) = \lambda(u)^n \cdot \det(u^{(p)}) \cdot \det(\phi(v)).$$

Taking into account the definition of $\lambda(x)$ we get

$$(\det(uv))^p = \det(u)^p \cdot \det(\phi(v))$$

hence $\det(v)^p = \det(\phi(v)) = \phi(\det(v))$ which implies $\delta(\det(v)) = 0$.

To check 2) note that by Equation 3.4 we have

$$\phi(v) = \Phi(u)^{-1}\Phi(uv).$$

On the other hand recall that we have an identity $\Phi(x)^t q\Phi(x) = (x^t qx)^{(p)}$. We get that

$$\Phi(u)^t q\Phi(u) = (u^t qu)^{(p)} = q^{(p)} = q,$$

hence

$$(\Phi(u)^t)^{-1} q\Phi(u)^{-1} = q,$$

hence

$$\begin{aligned}
\phi(v^t qv) &= \phi(v)^t q\phi(v) \\
&= \Phi(uv)^t(\Phi(u)^t)^{-1} q\Phi(u)^{-1}\Phi(uv) \\
&= \Phi(uv)^t q\Phi(uv) \\
&= (v^t u^t quv)^{(p)} \\
&= (v^t qv)^{(p)},
\end{aligned}$$

which implies that $\delta(v^t qv) = 0$. $\square$

Corollary 3.9.

1) Assume Δ is of type SL_n and let $\alpha \in \mathfrak{gl}_n(\mathcal{O})$, $u \in G^\alpha$. Then for any $c \in G_{u/\mathcal{O}}$ we have $\delta(\det(c)) = 0$.

2) Assume Δ is of type $SO(q)$ and let $\alpha \in \mathfrak{gl}_n(\mathcal{O})$, $u \in SO(q) \cap G^\alpha$. Then for any $c \in G_{u/\mathcal{O}}$ we have $\delta(c^t qc) = 0$.

Remark 3.10. The above Corollary shows that if Δ is of type SL_n or $SO(q)$ the δ-Galois set $G_{u/\mathcal{O}}$ is "close to being contained" in SL_n and $SO(q)$ respectively (provided u is in these groups respectively). Indeed $G_{u/\mathcal{O}}$ being contained in SL_n or $SO(q)$ respectively means $\det(c) = 1$ or $c^t qc = q$ for $c \in G_{u/\mathcal{O}}$. The Corollary however merely guarantees that $\delta(\det(c)) = 0$ or $\delta(c^t qc) = 0$, which is a "slightly" weaker property.

Remark 3.11. The δ-Galois group $G_{u/\mathcal{O}}$ in case $\Delta = 0$ is not always contained in the group N. Here is a simple example. Let $\mathcal{O} = \mathbb{Z}_{(p)}$, $n = 2$, and assume $p \equiv 1$ mod 3. Consider the matrices

$$u = \begin{pmatrix} 1 & \zeta \\ 1 & \zeta^2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & \text{-1} \\ 0 & \text{-1} \end{pmatrix}, \quad uc = \begin{pmatrix} 1 & \zeta^2 \\ 1 & \zeta \end{pmatrix},$$

where $\zeta \in \mathbb{Z}_p \subset R$ is a cubic root of unity. Note that $\det u = \zeta^2 - \zeta \not\equiv 0$ mod p so $u, c, uc \in GL_2(R)$. Then u is a solution to the equation

$$\delta u = 0.$$

Now $u, c, uc \in G^\delta \backslash N$ and $u^{(p)} = u$, $c^{(p)} = c$, $(uc)^{(p)} = uc$ so $c \in G_u$. Also we have $\mathcal{O}[u] = \mathbb{Z}_{(p)}[\zeta]$ and the unique non-trivial automorphism σ of $\mathbb{Z}_{(p)}[\zeta]$ sending $\sigma(\zeta) = \zeta^2$ satisfies $\sigma(u) = uc$. By assertion 3 in Lemma 3.7 we have $c \in G_{u/\mathcal{O}}$. By the way in this case $G_{u/\mathcal{O}} = \langle c \rangle$ is cyclic of order 2.

Proposition 3.12. *Assume $\Delta = 0$ and $\mathcal{O}$ is a valuation δ-subring of R with finite residue field. Then $G_{u/\mathcal{O}}$ is a finite group.*

Proof. Let $u_0 \in G^\delta$ be the unique element such that $u \equiv u_0 \bmod p$. Let F be the field of fractions of $\mathcal{O}$, let F' be the field generated by F and the roots of unity appearing as entries in u_0, and let $\mathcal{O}' = R \cap F'$. Then $\mathcal{O}'$ is a valuation δ-subring of R generically finite over $\mathcal{O}$ and $u_0 \in GL_n(\mathcal{O}')$. In particular $\mathcal{O}'$ has a finite residue field. Since $\alpha \in GL_n(\mathcal{O}')$, by Proposition 2.6, we get $u \in GL_n(\mathcal{O}'')$ for some generically finite extension $\mathcal{O}''$ of $\mathcal{O}'$. Then, by the injectivity of 3.5, and by the equality $\mathcal{O}\{u\} = \mathcal{O}[u]$, $G_{u/\mathcal{O}}$ is finite. $\square$

Using the theory around the Hilbert irreducibility theorem one can easily come up with infinitely many examples of Δ-linear equations with "big" group $G_{u/\mathcal{O}}$ over rings such as $\mathcal{O} = \mathbb{Z}_{(p)}$. Recall from [10] the notion of *thin set* in $\mathbb{Q}^N$; also note that by [10], Theorem 1, p. 177, it follows that for any thin set Ω in $\mathbb{Q}^N$ the set $\mathbb{Z}^N \backslash \Omega$ is infinite.

Proposition 3.13. *Let $\Delta = 0$ and $\mathcal{O} = \mathbb{Z}_{(p)}$. There exists a thin set $\Omega \subset \mathbb{Q}^{n^2}$ such that for any $\alpha \in \mathbb{Z}^{n^2} \backslash \Omega$ there exists $u \in G^\alpha$ with the property that $G_{u/\mathcal{O}}$ is a finite group containing the Weyl group W.*

Proof. Consider $n \times n$ matrices x and y of indeterminates, consider the affine space $\mathbb{A}^{n^2} = \mathit{Spec}\ \mathcal{O}[y]$, view $Y = \mathit{Spec}\ \mathcal{O}[y, \det(y)^{-1}]$ as a Zariski open subset in $\mathbb{A}^{n^2}$, and let $X = \mathit{Spec}\ \mathcal{O}[x, \det(x)^{-1}]$. Consider the finite étale morphism of schemes $X \to Y$ over $\mathcal{O}$ defined by $y = x \cdot (x^{(p)})^{-1}$ and consider the induced morphism

$$\pi : X \to Y \subset \mathbb{A}^{n^2}.$$

Clearly the Weyl group W acts on the covering $X \to Y$ via $x \mapsto xw$ for $w \in W$. By [10], Proposition 1, p. 122, there exists a thin set $\Omega' \subset \mathbb{A}^{n^2}(\mathbb{Q})$ such that for all $\epsilon_{\mathbb{Q}} \in \mathbb{A}^{n^2}(\mathbb{Q}) \backslash \Omega'$ the finite $\mathbb{Q}$-scheme $\pi^{-1}(\epsilon_{\mathbb{Q}})$ is irreducible and reduced, hence is the spectrum of a field. Let $\Omega = \mathbb{Z}^{n^2} \cap \frac{\Omega' - 1}{p}$ which is, of course, thin. Let $\alpha \in \mathbb{Z}^{n^2} \backslash \Omega$, let $\epsilon = 1 + p\alpha \in GL_n(\mathcal{O})$, and let $\epsilon_{\mathbb{Q}} \in \mathbb{A}^{n^2}(\mathbb{Q})$ be the point induced by ϵ; then $\epsilon_{\mathbb{Q}} \notin \Omega'$. Clearly the $\mathcal{O}$-scheme $\pi^{-1}(\epsilon)$ is finite étale over $\mathcal{O}$ so it is regular; so its connected components are integral and flat over $\mathcal{O}$. Since $\pi^{-1}(\epsilon) \otimes \mathbb{Q} = \pi^{-1}(\epsilon_{\mathbb{Q}})$ is connected it follows that $\pi^{-1}(\epsilon)$ itself is connected hence it is the spectrum of a Dedekind domain D. Since D is étale over $\mathcal{O}$ it can be embedded into R; fix such an embedding $D \subset R$. Let $u \in GL_n(D) \subset GL_n(R)$ be the point corresponding to the map $\mathit{Spec}\ D = \pi^{-1}(\epsilon) \to X = GL_n$; hence $D = \mathcal{O}[u]$. Moreover $\phi(u) = u = \epsilon u^{(p)}$. Finally W acts on both $\mathcal{O}[x]$ and D and the map $\mathcal{O}[x] \to D$ is equivariant; so W preserves the kernel of the map $\mathcal{O}[x] \to D$, so one gets $W \subset G_{u/\mathcal{O}}$. Finiteness of $G_{u/\mathcal{O}}$ follows from Proposition 3.12. $\square$

In what follows we view R as a complete metric space with respect to the p-adic metric. So we can talk about open balls in R. Any open ball has the form $X = b + p^N R$ for some $b \in R$ and $N \in \mathbb{Z}_{\geq 0}$; any such X is also closed and is, again, a complete metric space with respect to the induced metric. Now recall that a subset of a metric space is called *of the first category* if it is a countable union of subsets each of which has the property that its closure has an empty interior. By the Baire-Hausdorff theorem [12], p. 11, any subset of the first category in a non-empty complete metric space X is different from X. This applies then to any open ball X in R.

Proposition 3.14. *Assume $\Delta = 0$. There exists a subset Ω of the first category in the metric space*

$$X = \{u \in GL_n(R); u \equiv 1 \mod p\}$$

such that for any $u \in X \backslash \Omega$ the following holds. Let $\alpha = \delta u \cdot (u^{(p)})^{-1}$. Then there exists a valuation δ-subring $\mathcal{O}$ of R containing R^δ such that $\alpha \in \mathfrak{gl}_n(\mathcal{O})$ and such that $G_{u/\mathcal{O}} = N^\delta$.

Lemma 3.15. *Let $x, x', ..., x^{(r)}$ are a m-tuples of indeterminates and let $f \in R[x, x', ..., x^{(r)}]\hat{}$. Assume the map $f_* : R^m \to R$ defined by*

$$f_*(a) = f(a, \delta a, ..., \delta^m a)$$

vanishes on a product of open balls. Then f vanishes on the whole of R^m.

Proof. By [2], Remark 1.6, $f = 0$ if and only if $f_* = 0$. So it is enough to show that for any $b_j \in R$, $1 \leq j \leq m$, the R-algebra homomorphism

$$R[x, x', ..., x^{(r)}]\hat{} \to R[x, x', ..., x^{(r)}]\hat{}, \quad x_j^{(i)} \mapsto \delta^i(b_j + p^N x_j),$$

is injective. To check this we may assume $b_j = 0$ for all j. But then the assertion follows from the fact that

$$R[x, x', ..., x^{(r)}]\hat{} \subset K[[x, x', ..., x^{(r)}]] = K[[x, \phi(x), ..., \phi^r(x)]]$$

and from the fact that the endomorphism of $K[[x, \phi(x), ..., \phi^r(x)]]$ defined by $\phi^i(x) \mapsto p^N \phi^i(x)$ is injective. $\square$

Lemma 3.16. *Let E be a countable subfield of K and let $X_1, ..., X_m \subset R$ be open balls. Then one can find a subset Ω of the first category in the metric space $X = X_1 \times ... \times X_m$ such that for all $u = (u_1, ..., u_m) \in X \backslash \Omega$ the family*

$$(\delta^i u_j)_{i \geq 0, 1 \leq j \leq m}$$

is algebraically independent over E.

Proof. Let $\mathcal{F} = E[x, x', x'', ...]$ be the polynomial ring where each of $x, x', x'', ...$ is an m-tuple of indeterminates . Hence $\mathcal{F}$ is countable. Then for each $f \in \mathcal{F}$ with $f \neq 0$ set

$$X_f := \{u \in X; f(u, \delta u, \delta^2 u, ...) = 0\}.$$

Now we claim that each X_f is closed in the metric space X and has empty interior; indeed X_f is the zero locus in X of $f_* : R^m \to R$ and our claim follows from Lemma 3.15. The present Lemma follows now by taking

$$\Omega = \bigcup_{0 \neq f \in \mathcal{F}} X_f.$$

$\square$

Proof of Proposition 3.14. Let E be the subfield of K generated over $\mathbb{Q}$ by all the roots of unity in K; i.e. $E = \mathbb{Q}(R^\delta)$. Now X in the Proposition is a product of balls so by Lemma 3.16 there exists a subset of the first category $\Omega \subset X$ such that for all $u \in X \backslash \Omega$ the family $(\delta^r u_{ij})_{r \geq 0, 1 \leq i,j \leq n}$ is algebraically independent over E. Let $\epsilon = \phi(u) \cdot (u^{(p)})^{-1}$, $\alpha = (\epsilon - 1)/p$ and consider the fields

$$F_s = E(\delta^r \alpha_{ij}; 0 \leq r \leq s, \ 1 \leq i, j \leq n) = E(\phi^r(\epsilon_{ij}); 0 \leq r \leq s, \ 1 \leq i, j \leq n)$$

and $F = \cup_s F_s$. Let $\mathcal{O}$ be a valuation δ-subring of $R \cap F$ containing R^δ and the entries of α (e.g. one can take the "maximal" choice" $\mathcal{O} = R \cap F$). Note that for $s \geq 1$ we have equalities of fields

$$E(\delta^r u_{ij}; 0 \leq r \leq s,\ 1 \leq i,j \leq n) = F_{s-1}(u_{ij}; 1 \leq i,j \leq n). \tag{3.10}$$

Now the field in the left hand side of the 3.10 has transcendence degree $(s+1)n^2$ over E. Since F_{s-1} has transcendence degree at most sn^2 over E it follows from 3.10 that $(u_{ij})_{ij}$ are algebraically independent over F_{s-1}. Since this is true for all s it follows that $(u_{ij})_{ij}$ are algebraically independent over F. By assertion 2 in Lemma 3.7, $G_{u/\mathcal{O}} = N^\delta$. □

The next Proposition shows that the δ-Galois group cannot be "too large" at least if we take our data in a Zariski open set of the set of all data. In the statement below by a Zariski K-closed set in $GL_n(R)$ we understand the intersection of $GL_n(R)$ with a Zariski K-closed set of $GL_n(K^a)$; in other words a K-closed set of $GL_n(R)$ is the zero set in $GL_n(R)$ of a collection of polynomials with coefficients in K in n^2 variables. A subgroup Γ of $GL_n(R)$ is called diagonalizable if there exists $g \in GL_n(K^a)$ such that $g^{-1}\Gamma g$ consists of diagonal matrices.

Proposition 3.17. *There exists a Zariski K-closed set Ω in $G = GL_n(R)$ not containing 1 such that for any $u \in G \backslash \Omega$ the following holds. Let $\alpha = \delta u \cdot (u^{(p)})^{-1}$ and let $\mathcal{O}$ be a valuation δ-subring of R containing the entries of α. Then $G_{u/\mathcal{O}}$ contains a normal subgroup of finite index which is diagonalizable.*

In order to prove Proposition 3.17 we need a series of Lemmas: 3.18, 3.22, 3.23. In the discussion below (pertaining to these Lemmas only!) it is convenient to temporarily change some of the notation used so far. Indeed we let $\mathcal{C}$ be an uncountable algebraically closed field of characteristic zero (such as K^a or $\mathbb{C}$) and all schemes will be schemes over $\mathcal{C}$. By a variety we will understand a reduced (not necessarily irreducible) scheme of finite type over $\mathcal{C}$. We use the same letter X to denote a variety X over $\mathcal{C}$ and its set $X(\mathcal{C})$ of $\mathcal{C}$-points. In particular we denote by G the group scheme GL_n over $\mathcal{C}$ and also the "abstract" group $GL_n(\mathcal{C})$; we denote by T the group scheme of diagonal matrices over $\mathcal{C}$ and also the "abstract" group $T(\mathcal{C})$ of diagonal matrices with entries in $\mathcal{C}$. If X is a variety and $x \in X$ is a point we always understand x is a $\mathcal{C}$-point and we denote by $\dim_x X$ the maximum of the dimensions of the irreducible components of X passing through x. Also, in what follows, we let p be any integer ≥ 2 (not necessarily prime).

Lemma 3.18. *Let $X \subset G$ be the Zariski closed subset consisting of all $v \in G$ satisfying the following properties:*

1) $(v^m)^{(p)} = (v^{(p)})^m$ for all $m \geq 0$,

2) $(v^m)^{(p)}(v^{-m})^{(p)} = 1$ for all $m \geq 0$.

Then X has exactly one irreducible component passing through 1 and that component is T.

Remark 3.19. The equalities 1) and 2) are viewed as equalities in $\mathfrak{g} = \mathfrak{gl}_n(\mathcal{C})$; note however that, by 1) and 2), for any $v \in X$ we have that $(v^m)^{(p)} \in G$ for all $m \in \mathbb{Z}$ and hence 1) holds for all $m \in \mathbb{Z}$ as an equality in G.

Remark 3.20. The set X contains the group $N = WT = TW$ generated by the Weyl group W and the group T of diagonal matrices with entries in $\mathcal{C}$. It is not clear whether X actually coincides with the group N.

Remark 3.21. Let $\mathbb{X}$ be the closed subscheme of G defined by the equations 1) and 2) in the statement of Lemma 3.18; hence the variety $\mathbb{X}_{red}$ coincides with X. It is interesting to note that tangent space of $\mathbb{X}$ at 1 is the whole of the tangent space of G i.e. the Lie algebra $L(G)$ of G; indeed, equations 1) and 2) are easily seen to hold when v is replaced by $1+\epsilon\xi$, where $\epsilon^2=0$ and ξ is an arbitrary element of $\mathfrak{gl}_n(\mathcal{C})$. In particular $\mathbb{X}$ is not reduced.

Proof of Lemma 3.18. Let $v \in X$, let $\langle v\rangle \subset G$ be the group generated by v, let $H_v \subset G$ be the Zariski closure of $\langle v\rangle$ in G (which is an algebraic subgroup of G, cf. [7], p. 54), and let H_v° be the identity component of H_v. Clearly H_v is commutative.

Claim. For all $v \in X$ we have $H_v^\circ \subset T$.

To check the claim note first that $\langle v\rangle \subset X$ hence $H_v \subset X$. Denote by $\Phi : G \to G$ the map $\Phi(v) = v^{(p)}$ (which, of course, is not a homomorphism). Clearly we have $\Phi(v^r v^s) = \Phi(v^r)\Phi(v^s)$ for all $r, s \in \mathbb{Z}$ hence we have $\Phi(gh) = \Phi(g)\Phi(h)$ for all $g, h \in H_v$. Let $\varphi : H_v \to G$ be the restriction of Φ; then the regular map φ is a group homomorphism hence its image $H'_v := \varphi(H_v) \subset G$ is a subgroup which is constructible. Hence H'_v is a closed subgroup of G (cf. [7], p. 54) and hence φ is an algebraic group homomorphism. Consider the commutative diagram of (possibly reducible) varieties

$$\begin{array}{ccc} H_v & \subset & G \\ \varphi\downarrow & & \downarrow\Phi \\ H'_v & \subset & G \end{array}$$

and the induced tangent maps between the corresponding tangent spaces at the identity

$$\begin{array}{ccc} L(H_v) & \subset & L(G) \\ d_1\varphi\downarrow & & \downarrow d_1\Phi \\ L(H'_v) & \subset & L(G) \end{array}$$

(Here $L(\ )$ denotes the Lie algebra functor. The linear map $d_1\Phi$ is not a Lie algebra map. The map $d_1\varphi$, on the other hand, is, of course, a Lie algebra map because its source and target are abelian.) One can compute $d_1\Phi$ explicitly: letting $v = 1+\epsilon\xi \in GL_n(\mathcal{C}[\epsilon])$, $\epsilon^2=0$, we have

$$\Phi(v) = (1+\epsilon\xi)^{(p)} = diag(1+\epsilon p\xi_{11}, ..., 1+\epsilon p\xi_{nn}).$$

Hence the image of $d_1\Phi$ is contained in the Lie algebra $L(T)$ of the torus T. Since $d_1\varphi$ is surjective (because we are in characteristic zero) it follows that $L(H'_v) \subset L(T)$. Hence the identity component $(H'_v)^\circ$ of H'_v is contained in T. Now, clearly, $\Phi^{-1}(T) = T$. Hence $H_v^\circ \subset \Phi^{-1}((H'_v)^\circ) \subset \Phi^{-1}(T) = T$ and our claim is proved.

For any subtorus $S \subset T$ let us denote by $C(S)$ the centralizer of S in G; moreover, for any integer $e \geq 1$ denote by $S^{1/e}$ the set of all $v \in G$ such that $v^e \in S$. By the above Claim and by the commutativity of H_v it follows that for any $v \in X$ we have that H_v° is a subtorus of T and there exists $e \geq 1$ such that $v \in C(H_v^\circ) \cap H_v^{\circ 1/e}$. In particular we have

$$X = \bigcup_{S,e} (C(S) \cap S^{1/e} \cap X)$$

where S runs through the (countable!) set of subtori of T and e runs through the set of positive integers. Since $\mathcal{C}$ is uncountable no irreducible variety over $\mathcal{C}$ is a countable union of proper closed subvarieties; in particular, applying this to the irreducible components of X it follows that there exists $e \geq 1$ and finitely many subtori $S_1, ..., S_q \subset T$ such that

$$X = \bigcup_{i=1}^{q} (C(S_i) \cap S_i^{1/e} \cap X). \tag{3.11}$$

To conclude the proof of the Lemma we assume (as we always can) that $\mathcal{C} = \mathbb{C}$. Let V be an irreducible component of X passing through 1. We will prove that $V = T$ and this will end the proof. Assume $V \neq T$ and seek a contradiction. Since $V \neq T$ it follows that $V \not\subset T$ hence $V \backslash T$ is Zariski open in V hence dense in V in the complex topology. So there exists a sequence $x_n \to 1$ (in the complex topology) with $x_n \in X \backslash T$. By 3.11 and by replacing x_n with a subsequence we may assume $x_n \in C(S_i) \cap S_i^{1/e} \cap X$ for some i. Let $[x_n] \in C(S_i)/S_i$ be the class of x_n and choose an embedding $\rho : C(S_i)/S_i \to GL_\nu(\mathcal{C})$ for some ν. Then $\rho([x_n]) \to 1$ hence the eigenvalues of $\rho([x_n])$ tend to 1. But $[x_n]^e = 1$, hence $\rho([x_n])^e = 1$, for all n. So the eigenvalues of $\rho([x_n])$ are e-th roots of unity so they form a discrete set. We get that for n sufficiently big the eigenvalues of $\rho([x_n])$ are equal to 1. But a matrix of finite order with all eigenvalues equal to 1 must be the identity. Hence $\rho([x_n]) = 1$ hence $[x_n] = 1$ hence $x_n \in S_i \subset T$ for some n, a contradiction. This ends the proof of the Lemma. □

The next lemma is completely standard; we just include it for convenience.

Lemma 3.22. *Let $\pi : Z \to Y$ be a morphism of varieties over $\mathcal{C}$ and assume $\sigma : Y \to Z$ is a section of π. Assume Y is irreducible and for $y \in Y$ consider the variety $\pi^{-1}(y)$. Let $y_0 \in Y$ and assume the point $\sigma(y_0)$ is a connected component of $\pi^{-1}(y_0)$. Then there exists a Zariski open set $U \subset Y$ containing y_0 such that for all $y \in U$ the point $\sigma(y)$ is a connected component of $\pi^{-1}(y)$.*

Proof. This is a standard consequence of the semicontuinty theorem for the local dimension of fibers. Indeed let $Z^1, ..., Z^m$ be the irreducible components of Z, let $S = \sigma(Y)$ and assume $\sigma(y_0) \in Z^i$ for $1 \leq i \leq r$ and $\sigma(y_0) \notin Z^j$ for $r < j \leq m$. Let $U_0 = \pi(S \backslash \bigcup_{j>r} Z^j)$. Also let $Y^i \subset Y$ be the closure of $\pi(Z^i)$ and let $\pi_i : Z^i \to Y^i$ for $i \leq r$ be induced by π. By the semicontinuity theorem in [7], p.33, for $i \leq r$, there exist closed sets $T^i \subset Z^i$ not containing $\sigma(y_0)$ such that

$$\dim_x \pi_i^{-1}(\pi(x)) \leq \dim_{\sigma(y_0)} \pi_i^{-1}(y_0) \quad \text{for all} \quad x \in Z^i \backslash T^i. \tag{3.12}$$

Consider the closed set $T := T^1 \cup ... \cup T^r \cup Z^{r+1} \cup ... \cup Z^m$ in Z and the open subset $U = \pi(S \backslash T) = Y \backslash \pi(S \cap T)$ of Y. Then $y_0 \in U$. Let $y \in U$ and let F be an irreducible component of $\pi^{-1}(y)$ passing through $\sigma(y)$. Then $F \not\subset Z^j$ for $j > r$ (because if one assumes the contrary then $\sigma(y) \in S \cap Z^j \subset S \cap T$ hence $y \in \pi(S \cap T)$, a contradiction). So $F \subset Z^i$ for some $i \leq r$ and hence $F \subset \pi_i^{-1}(y)$. Since $y \notin \pi(S \cap T)$ we have $\sigma(y) \notin T$ hence $\sigma(y) \notin T^i$; on the other hand $\sigma(y) \in F \subset Z^i$, hence $\sigma(y) \in Z^i \backslash T^i$. So by 3.12 we get

$$\dim_{\sigma(y)} F \leq \dim_{\sigma(y)} \pi_i^{-1}(y) \leq \dim_{\sigma(y_0)} \pi_i^{-1}(y_0) \leq \dim_{\sigma(y_0)} \pi^{-1}(y_0) = 0.$$

So $\dim_{\sigma(y)} F = 0$ hence $F = \{\sigma(y)\}$ and we are done. □

Lemma 3.23. *Let Y be the Zariski open set of $G = GL_n(\mathcal{C})$ consisting of all $u \in G$ such that $u^{(p)}$ is invertible. Let $\Psi : Y \times G \to \mathfrak{g}$ be the morphism defined by*

$$\Psi(u, v) = (u^{(p)})^{-1}(uv)^{(p)}.$$

For each $u \in Y$ let $X_u \subset G$ be the Zariski closed set consisting of all $v \in G$ such that

1) $\Psi(u, v^m) = \Psi(u, v)^m$ for all $m \geq 0$,

2) $\Psi(u, v^m)\Psi(u, v^{-m}) = 1$ for all $m \geq 0$.

Then there exists a Zariski open set $U \subset Y$ containing 1 with the property that for any $u \in U$ and for any connected closed subgroup $S \subset G$ contained in X_u we have that S is a torus.

Proof. Let $Z \subset Y \times G$ be the closed set defined by the equations 1) and 2) together with the equation $(v-1)^n = 0$. Note that this latter equation is equivalent to asking that v be unipotent. Let $\pi : Z \to Y$, $\pi(u, v) = u$, and let $pr_G : Y \times G \to G$ be the second projection. Then $pr_G(\pi^{-1}(u))$ coincides with the set of unipotent matrices in X_u. Also note that X_1 coincides with X in Lemma 3.18. Now, by Lemma 3.18, there is exactly one irreducible component of X_1 passing through 1 and that component is a torus so it does not contain unipotent matrices with the exception of 1 itself. In particular 1 is a connected component of $pr_G(\pi^{-1}(1))$. Now π has a section $\sigma : Y \to Z$, $\sigma(u) = (u, 1)$. By Lemma 3.22 there exists a Zariski open set U of Y containing 1 such that for all $u \in U$ we have that $(u, 1)$ is a connected component of $\pi^{-1}(u)$. So 1 is a connected component of the set of unipotent matrices in X_u. Now let $S \subset G$ be a closed connected subgroup contained in X_u. Then 1 is a connected component of the set of unipotent matrices in S. This implies that S contains no unipotent matrix except 1 (because any unipotent matrix $\neq 1$ is contained in a subgroup isomorphic to the additive group). So the unipotent radical of S is trivial, hence a torus by [7], p. 161. □

Remark 3.24. Exactly as in Remark 3.21, if $\mathbb{X}_u$ is the subscheme of G defined by equations 1) and 2) in Lemma 3.23 then $(\mathbb{X}_u)_{red} = X_u$ and the tangent space to $\mathbb{X}_u$ at 1 is, again, the whole of the Lie algebra $L(G) = \mathfrak{gl}_n(\mathcal{C})$.

Proof of Proposition 3.17. Consider the situation and notation in Lemma 3.23 with $\mathcal{C} = K^a$. Choose a polynomial $F \in K^a[x]$ such that

$$1 \in D(F) := \{v \in GL_n(K^a); F(v) \neq 0\} \subset U.$$

Replacing F by the product of its conjugates over K we may assume $F \in K[x]$ and hence that $F \in R[x]$. Now let $u \in D(F) \cap GL_n(R)$, $\alpha = \delta u \cdot (u^{(p)})^{-1}$, and let $\mathcal{O} \subset R$ be a valuation δ-subring containing the entries of α. Let $\overline{G_{u/\mathcal{O}}}$ be the Zariski closure of $G_{u/\mathcal{O}}$ in $GL_n(K^a)$. We want to show that the connected component $\overline{G_{u/\mathcal{O}}}^{\circ}$ of $\overline{G_{u/\mathcal{O}}}$ is a torus in $GL_n(K^a)$. Note that $u^{(p)}$ is invertible so $u \in Y$. Let $c \in G_{u/\mathcal{O}}$ hence $c^m \in G_{u/\mathcal{O}} \subset G_u$ for all $m \in \mathbb{Z}$. Hence $(uc^m)^{(p)} = u^{(p)}\phi(c^m)$, hence $\Psi(u, c^m) = \phi(c^m)$. We claim that $c \in X_u$; indeed for $m \geq 0$ we have

$$\Psi(u, c^m) = \phi(c^m) = \phi(c)^m = \Psi(u, c)^m$$

and also

$$\Psi(u, c^m)\Psi(u, c^{-m}) = \phi(c^m)\phi(c^{-m}) = \phi(1) = 1.$$

Since c was arbitrary in $G_{u/\mathcal{O}}$ we conclude that $G_{u/\mathcal{O}} \subset X_u$ hence $\overline{G_{u/\mathcal{O}}} \subset X_u$. By Lemma 3.23, $\overline{G_{u/\mathcal{O}}}^{\circ}$ is a torus. Then clearly

$$G_{u/\mathcal{O}} \cap \overline{G_{u/\mathcal{O}}}^{\circ}$$

is a normal subgroup of finite index in $G_{u/\mathcal{O}}$ which is diagonalizable. □

References

[1] J. Borger, *Λ-rings and the field with one element*, arXiv:0906.3146 [math.NT]

[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, II: arithmetic Lie theory*, preprint.

[6] J.K. Fornaes, N. Sibony, Complex dynamics in higher dimensions, in: Several Complex Variables, MSRI Publ. 37, Cambridge Univ. Press, Cambridge (1999), 273-296.

[7] J. E. Humphreys, *Linear algebraic groups*, GTM 21, Springer, New York, 1995.

[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] S. Lang, *Algebraic groups over finite fields*, Amer J. Math. 78 (1956), 555-563.

[10] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Vieweg, 1997.

[11] M. Singer, M. van der Put, *Galois theory of difference equaltions*, LNM, Springer 1997.

[12] K. Yoshida, *Functional Analysis*, Springer, New York, 1995.

University of New Mexico, Albuquerque, NM 87131

E-mail address: buium@math.unm.edu