7-12-2014

Arithmetic Differential Subgroups of GL_{n}

Alfonso E. Heras-Llanos

Alfonso Enrique Heras Llanos

Candidate

Mathematics and Statistics

Department

This dissertation is approved, and it is acceptable in quality and form for publication:

Approved by the Dissertation Committee:

Alexandru Buium , Chairperson

Charles Boyer

Janet Vassilev

Lance Miller

ARITHMETIC DIFFERENTIAL SUBGROUPS OF GL_n

by

ALFONSO ENRIQUE HERAS LLANOS

B.S., Mathematics and Physics, Univ. del Atlantico, Colombia, 1997
M.S., Mathematics, University of Puerto Rico, 2003

DISSERTATION

Submitted in Partial Fulfillment of the
Requirements for the Degree of

Doctor of Philosophy
Mathematics

The University of New Mexico
Albuquerque, New Mexico

May 2014

Arithmetic Differential Subgroups of GL_n

by

Alfonso Enrique Heras Llanos

B.S., Mathematics and Physics, Univ. del Atlantico, Colombia, 1997
M.S., Mathematics, University of Puerto Rico, 2003
Ph.D., Mathematics, University of New Mexico, 2014

ABSTRACT

A remarkable and special Galois Theory appears from the study of the arithmetic analogue of ordinary differential equations; where functions are replaced by integers, the derivative operator replaced by the "Fermat quotient operator" and differential equations are replaced by arithmetic differential equations. The main result presented in the thesis will be the study of a very special class of arithmetic subgroups of $\mathrm{GL_n}$. We also introduce a set of functions, that we call Leibniz systems. These functions "generate" some examples of the differential subgroups of $\mathrm{GL_n}$. As a by-product we found more analogies between the ordinary differential operator and the Fermat quotient operator, such as the chain rule and the product rule.

Contents

1 Introduction

1.1 Overview

In [1], an arithmetic theory of differential equations was introduced, in which differentiable functions $x(t)$ are replaced by integers n, and the differential operator $x(t) \mapsto \frac{dx}{dt}$ is replaced by the Fermat quotient operator $\delta : n \mapsto \frac{n-n^p}{p}$, where p is a prime integer. In [2], this theory was used to prove results about differential invariants of some remarkable groups. The aim of this thesis is to extend those results to more general groups, that appear as "differential groups" or $\delta-$subgroups of $R^\times$. A $\delta-$subgroup of $GL_n(R)$ is a subgroup which is the common zero locus of finitely many functions of the form $f : GL_n(R) \longrightarrow R$, $f(a) = F(a, \delta(a), ..., \delta^m(a), det(a)^{-1})$ where F is a restricted power series in $(m+1)n^2+1$ variables. As a by-product we also find more analogies between the operators $\frac{dx}{dt}$ and δ such as, the chain rule, the product rule and the quotient rule.

In chapter 3 we define and study an interesting class of $\delta-$subgroups of $B_n(R)$, where $B_n(R)$ is the group of $n \times n$ invertible and upper triangular matrices with entries in R , by introducing the concept of Leibniz Systems. Chapter 3 will constitute a wide open source of study for future research. Our $\delta-$subgroups are an arithmetic analogue of the differential algebraic groups of E.R. Kolchin [3], and P. Cassidy [4]. Differential algebraic groups are themselves analogues of of differential groups classically considered by S. Lie and E. Cartan in [5].

1.2 Methodology

First we introduce some basic definitions, examples and notation. Most of them are taken from [2].

Definition 1. Let $\mathbb{Z}_p^{ur} = \cup_\varsigma \{\mathbb{Z}_p[\varsigma] : \varsigma^n = 1, (n,p) = 1\}$ be the maximum unramified extension of the ring $\mathbb{Z}_p$. Let $R = R_p := \hat{\mathbb{Z}_p^{ur}}$ be the $p-$adic completion of the ring $\mathbb{Z}_p^{ur}$. This is the unique complete discrete valuation ring of characteristic zero with maximal ideal generated by p. R has residue field $k := R/pR = \mathbb{F}_p^a$, the algebraic closure of $\mathbb{F}_p$. This ring has a unique automorphism $\phi : R \longrightarrow R$ lifting the p-power Frobenius automorphism of k. Define the map $\delta : R \longrightarrow R$ by

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

The elements $c \in R$ such that $\delta(c) = 0$ will be called the constants. And they are: zero together with the n^{th} roots of unity in $R^\times$.

In the following definition the symbols $x, x', x'', ...$ represent variables.

Definition 2. Let $R\{x\} := R[x, x', x'', ...]$ be the polynomial ring in the variables $x, x', x'', ...$ with coefficients in R. Consider the unique extension $\phi : R\{x\} \longrightarrow R\{x\}$, of the map $\phi : R \longrightarrow R$ such that

$$\phi(x^{(i-1)}) = (x^{(i-1)})^p + px^{(i)} \quad i = 1, 2, 3, ...$$

Define a map $\delta : R\{x\} \longrightarrow R\{x\}$ by the following formula

$$\delta F(x, x', x'', ...) = \frac{\phi(F(x, x', x'', ...)) - F(x, x', x'', ...)^p}{p}$$

Similarly, define $k\langle x\rangle := k(x, x', x'', \ldots)$, to be the field of rational functions in the variables $x, x', x'', ...$ with coefficients in k.

Let's define the order and the degree of an element in $R\{x\}$ as follows:

Definition 3. Let $F(x, x', x'', ...) \in R\{x\}$. The *order* of F will be

$$\min\{n : F \in R[x, x', x'', ..., x^{(n)}]\}$$

And the *degree* of F with respect to the variable $x^{(n)}$ will be $deg_{x^{(n)}}F$, the usual degree.

Example 1. The polynomial $F(x, x', x'', ...) = 2x^{(9)}(x^{(3)})^7 + x + 3 \in R\{x\}$, has order 9 and $deg_{x^{(3)}}F = 7$.

The following example shows the non-linearity of δ. It also illustrates the fact that the constants with respect to δ are: zero and the n^{th} roots of the unity in $R^\times$.

Example 2. Take $F(x, x', x'', ...) = x + 2$, then letting $2' = \delta(2)$, we have

$$\begin{aligned} \delta(x+2) &= \frac{\phi(x+2) - (x+2)^p}{p} \\ &= x' + 2' - \frac{(x+2)^p - x^p - 2^p}{p} \end{aligned}$$

and

$$2' = \frac{\phi(2) - (2)^p}{p} = \frac{2 - 2^p}{p}$$

Let's start the introduction of our "differential subgroups" of $R^\times$ by defining what we shall call the rule of exponents:

Definition 4. Let $\mathbb{Z}[\phi]$ be the ring of all the polynomials with integer coefficients in the variable ϕ. Let $f(\phi) = \sum_{i=0}^{t} a_i\phi^i \in \mathbb{Z}[\phi]$, then we set,

$$x^{f(\phi)} = x^{\left(\sum_{i=0}^{t} a_i\phi^i\right)} = \prod_{i=0}^{t} \phi^i(x^{a_i})$$

Notice that Definition 4 implies that, for any f and g in $\mathbb{Z}[\phi]$ we have

$$x^{fg} = (x^f)^g$$

Example 3. Let $f(\phi) = \phi^2 - \phi - 6 \in \mathbb{Z}[\phi]$, then by Definition 4 we have that

$$x^{f(\phi)} = x^{\phi^2-\phi-6} = \phi^2(x)\phi(x^{-1})x^{-6} = (x^{\phi-3})^{\phi+2}$$

Next we introduce our "differential groups" or $\delta-$subgroups of $R^\times$.

Definition 5. *Let $f \in \mathbb{Z}[\phi]$, then define the following subgroups of the multiplicative group $R^\times$:*

$$\Gamma_f := \{\lambda \in R^\times : \lambda^f = 1\}, \quad \textit{and} \quad \Gamma_f^{(n)} = (1 + p^n R) \cap \Gamma_f.$$

Example 4. When $f = 0$ or $f = r$ and $r \in \mathbb{Z}\backslash\{0\}$ then, $\Gamma_f = R^\times$ or $\mu_r \cap R^\times$ respectively. Here μ_r represents the set of all r^{th} roots of unity in an algebraic closure of $K = R[\frac{1}{p}]$.

Definition 6. We have a Γ_f-action on $R\{x\}$ defined by

$$(\lambda, x^{(i)}) \mapsto \delta^i(\lambda x) \qquad \lambda \in \Gamma_f$$

Let's denote this by $k\langle x\rangle^{\Gamma_f}$, the field of elements of $k\langle x\rangle$ fixed by the induced action on $k\langle x\rangle$. For any $v \in R\{x\}_{(p)}$ we denote by $\overline{v} \in k\langle x\rangle$ the image of v. For $u \in R\{x\}_{(p)}$ define

$$k\langle u\rangle := k(\overline{u}, \overline{\delta(u)}, \overline{\delta^2(u)}, ...) \subset k\langle x\rangle$$

Recall the following result from [2], Proposition 5.14 page 148.

Theorem 1. *Consider the element $x^{\phi-1}$ from the ring $R\{x\}_{(p)}$. Then the extension $k\langle x^{\phi-1)}\rangle \subseteq k\langle x\rangle$ is Galois with Galois group $\Gamma_{\phi-1}$. In particular we have that*

$$k\langle x^{\phi-1}\rangle = k\langle x\rangle^{\Gamma_{\phi-1}}, \quad \textit{and} \quad \Gamma_{\phi-1} \cong \mathbb{Z}_p^\times.$$

Our main theorem (Theorem 2) is an extension of Theorem 1 from the linear polynomial $\phi - 1$ to more general polynomials $f(\phi) \in \mathbb{Z}[\phi]$.

Theorem 2. *Let $f \in \mathbb{Z}[\phi]$ be such that p does not divide its leading coefficient. Consider the element $x^{f(\phi)}$ from the ring $R\{x\}_{(p)}$. Then the extension $k\langle x^{f(\phi)}\rangle \subseteq k\langle x\rangle$ is algebraic Galois with Galois group $\Gamma_{f(\phi)}$. In particular,*

$$k\langle x^{f(\phi)}\rangle = k\langle x\rangle^{\Gamma_{f(\phi)}}$$

In what follows we briefly explain the strategy of the proof of Theorem 2. We need to introduce some definitions and results.

Definition 7. *Let $f \in \mathbb{Z}[\phi]$, then define the map*

$$\theta_\lambda : k(x, x', ..., x^{(n-1)}) \longrightarrow k(x, x', ..., x^{(n-1)}), \quad by \quad \theta_\lambda(x^{(i)}) = (\lambda x)^{(i)}$$

And the map

$$\rho_n : \Gamma_f \longrightarrow Aut(k(x, x', ..., x^{(n-1)})/k), \quad by \quad \lambda \longmapsto \theta_\lambda.$$

In what follows set $y_n = \delta^n(x^{f(\phi)})$, and denote by $\eta_n \in k\langle x\rangle$ the image of y_n. Note that $\eta_0 = \overline{x^{f(p)}}$.

The strategy of the proof of Theorem 2 is as follows: The inclusion " $\subset$ " will be clear. To prove the inclusion " $\supset$ " it will be enough to show the following two statements.

1. $\left[k(x, x', x'', ..., x^{(n)}) : k(\eta_0, \eta_1, \eta_2, ..., \eta_n)\right] \leq |f(p)|\, p^{n \cdot deg(f)}$ and
2. The cardinality of the image I_n of ρ_n is greater than or equal to $|f(p)|\, p^{n \cdot deg(f)}$.

To prove Statement 1 we need to control the degree of the elements η_i with respect to $x^{(i)}$. We can achieve this goal using what we shall call the $\delta-$Pascal triangle technique, which is one of the main contributions of this research. We will prove that

$$deg_{x^{(i)}}(\eta_i) = p^{deg(f)}$$

To prove Statement 2 we first estimate the cardinality of the quotients $\frac{\Gamma_{f(\phi)}}{\Gamma_{f(\phi)}^{(n+1)}}$. We

actually found that

$$\left|\frac{\Gamma_{f(\phi)}}{\Gamma_{f(\phi)}^{(n+1)}}\right| = \left|\mu_{f(p)}\right| p^{n\cdot deg(f)} = \left|f(p)\right| p^{n\cdot deg(f)}$$

And second by proving the following:

- Let n, l be natural numbers, such that, $0 < l < n$. Suppose that $\lambda = x + p^n y_0$, y_0 in R. Then, for some $y_l \in R$, we have

$$\delta^l(\lambda) = \delta^l(x) + p^{n-l} y_l$$

- For $n \in \mathbb{N}$, and $\lambda \in (1 + p^n R)$, we also have,

$$\delta^{n-1}(x\lambda) \equiv \delta^{n-1}(x) \, mod \, p$$

With the last two claims plus some extra work, we are proving that $Ker(\rho_n) = \Gamma_{f(\phi)}^{(n)}$, which gives the connection between the map ρ_n and the subgroups $\Gamma_{f(\phi)}^{(n)}$.

In the following section we explain our definition and use of the $\delta-$*Pascal Triangle*. Proofs are relegated to chapter 2.

1.3 The $\delta-$Pascal Triangle Technique

Besides the proof of our main theorem, the $\delta-$Pascal Triangle technique will provide new analogies between the operators $\frac{dx}{dt}$ and δ such as the chain rule, the product rule and the quotient rule.

Definition 8. Let $n, k \in \mathbb{N}$, where $0 \leqslant k \leqslant n$. Define the $\delta-$*binomial coefficient* of order k and $deg_{\delta^k(x)} = p^{n-k}$, to be

$$\binom{n}{k}_x = \sum (\delta(\delta(...(\delta(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_{k-1}}})^{p^{a_k}}$$

where $\sum a_j = n - k$, and $a_j \geq 0$.

Notice that the degree and the order in this definition are taken in the sense of

Definition 3 but after we write each term $(\delta(\delta(...(\delta(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_{k-1}}})^{p^{a_k}}$ in terms of the variables $x, x', x'', ..., x^{(k)}$.

The following example shows how the formula in the Definition 8 keeps track of the order and the degree of all terms in $\phi^n(x)$, and encapsulates its complexity.

Example 5. In particular $\binom{n}{0}_x = x^{p^n}$, $\binom{n}{n}_x = \delta^n(x)$, and

$$\binom{3}{2}_x = \delta^2(x^p) + \delta(\delta(x))^p + (\delta^2(x))^p$$

The following definition and lemma show the "binomial" behavior of $\binom{n}{k}_x$.

Definition 9. *Define the following expressions:*

$$\binom{n}{k}_x^* = \sum_{\sum a_j = n-k} \delta(\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k}} \quad \textit{and} \quad \binom{n}{k}_x^{**} = \sum_{\sum a_j = n-k} (\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k+1}}$$

where $0 \leq j \leq k$.

This definition will be used to show the following statement, and claim:

$$\phi(\binom{n}{k}_x) = \binom{n}{k}_x^{**} + p\binom{n}{k}_x^*$$

Claim 1. Let $n \in \mathbb{N}$, and $0 \leqslant k \leqslant n+1$, then,

$$\binom{n+1}{k}_x = \binom{n}{k}_x^{**} + \binom{n}{k-1}_x^*$$

This result and the fact that the expression $\binom{n}{k}_x$ has exactly $\binom{n}{k}$ terms, justify the Pascal terminology.

In what follows, we will state without proof some results. These results will be proven in chapter 2.

Now we present a formula that will be useful in the proof of our results.

Theorem 3. *Let* $n \in \mathbb{Z}$ *and* $n \geqslant 0$, *then,*

$$\phi^n(x) = \sum_{k=0}^{n} p^k \binom{n}{k}_x$$

Now we will explain in the next generic example how we work with Theorem 3 to obtain our results.

Example 6. Let $A = BC$, then $\phi^n(A) = \phi^n(BC)$. Since ϕ^n is a ring homomorphism we obtain that

$$\phi^n(A) = \phi^n(B)\phi^n(C)$$

Next we apply Theorem 3 to the last equation and we obtain

$$\sum_{k=0}^{n} p^k \binom{n}{k}_A = \left(\sum_{k=0}^{n} p^k \binom{n}{k}_B\right)\left(\sum_{k=0}^{n} p^k \binom{n}{k}_C\right)$$

Then we multiply the two summations in the right hand side of the last equation and we separate the terms of "order n". From this example we can obtain the equivalent to the product rule in the theory of arithmetic differential equations. Using this approach we can also keep track of the degree of each term in the last equation.

Definition 10. Let $n \in \mathbb{N}$, and $u \in R\{x\}$. Let $\mathcal{O}_u(n)$ be the $R-$submodule of $R\{x\}$ defined as

$$\mathcal{O}_u(n) = \{T \in R\{u\} : order_u(T) \leq n\}$$

and if $u = x$ we write $\mathcal{O}(n)$ for short. We also define $\mathcal{O}_{u,v}(n)$ to be the set of all finite linear combinations over R of products of elements in $\mathcal{O}_u(n)$, $\mathcal{O}_v(n)$.

Theorem 3 implies the following theorem, where one can see the similarities between δ and the usual derivative $\frac{dx}{dt}$.

Theorem 4. *(The Chain Rule) Let $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ then,*

$$\delta^n(x^m) \equiv \left(m\,(x^{p^n})^{m-1}\delta^n(x) + T\right)\ mod(p)$$

where $T \in \mathcal{O}(n-1)$.

(The Product Rule) Let $u, v \in R\{x\}$, then,

$$\delta^n(uv) \equiv \left(u^{p^n}\delta^n(v) + v^{p^n}\delta^n(u) + T\right)\ mod(p)$$

where $T \in \mathcal{O}_{u,v}(n-1)$.

It is clear, from the chain rule and using the fact that δ and ϕ commute, that we have the following more general result:

Corollary 1. *For* $y = x^{m\phi^t} = (x^{\phi^t})^m$ *and* $t \in \mathbb{N}$ *we have*

$$\delta^n(x^{m\phi^t}) \equiv \left(m \left(x^{\phi^t} \right)^{p^n(m-1)} \delta^n(x)^{p^t} + T \right) \ mod(p)$$

where $T \in \mathcal{O}(n-1)$.

The next corollary explain one of the achievements of Theorem 3.

Corollary 2. *Let* $n \in \mathbb{N}$, $f \in \mathbb{Z}[\phi]$ *where* p *does not divide the leading coefficient of* f. *Assume that* $y = x^{f(\phi)}$ *then,*

$$deg_{\delta^n(x)}(\overline{\delta^n(y)}) = p^{deg(f)}$$

Example 7. Let $y = \frac{\phi(x)}{x^m} = x^{\phi - m}$. Using Theorem 4, Corollary 2, for $l = 1$ and the fact that ϕ commutes with δ, we obtain:

$$\overline{\delta^n(y)} \equiv \left(x^{-mp^n} (\delta^n(x))^p - x^{p^{n+1} - 2mp^n} (\delta^n(x^m)) + T \right) \ mod(p), \qquad T \in \mathcal{O}(n-1)$$

since $\overline{\delta^n(\phi^l(x))} = (\delta^n(x))^{p^l}$, and $deg_{\delta^n(x)}(\overline{\delta^n(y)}) = p$, for $n \in \mathbb{N}$. In the case where $m = 1$, we obtain that $deg_{\delta^n(x)}(\overline{\delta^n(y)}) = p$, which is and important part in the proof of Theorem 1.

2 The $\delta-$Pascal Triangle and The Proof of the Main Theorem

Besides the proof of our main theorem, in this chapter we found a formula for $\phi^n(x)$ using The $\delta-$Pascal Triangle Technique. This formula constitute an important part in the proof of our main theorem. As we also said in the introduction, this formula is important, not only for the porpoises of this thesis, but for other applications in the theory of arithmetic differential equations as well.

2.1 The $\delta-$Pascal Triangle

Recall from the introduction the following definitions

Definition 11. Let $n, k \in \mathbb{N}$, where $0 \leqslant k \leqslant n$. Define the $\delta-$*binomial coefficient* of order k and $deg_{\delta^k(x)} = p^{n-k}$, to be

$$\binom{n}{k}_x = \sum (\delta(\delta(...(\delta(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_{k-1}}})^{p^{a_k}}$$

where $\sum a_j = n - k$, and $a_j \geq 0$.

Also recall that the degree and the order in this definition are taken in the sense of Definition 3 but after we write each term $(\delta(\delta(...(\delta(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_{k-1}}})^{p^{a_k}}$ in terms of the variables $x, x', x'', ..., x^{(k)}$.

Definition 12. *Define the following expressions:*

$$\binom{n}{k}_x^{*} = \sum_{\sum a_j = n-k} \delta(\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k}} \quad \textit{and} \quad \binom{n}{k}_x^{**} = \sum_{\sum a_j = n-k} (\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k+1}} .$$

Lemma 1. *Let $n \in \mathbb{N}$, and $0 \leqslant k \leqslant n+1$, then, the following formula is an identity*

$$\phi(\binom{n}{k}_x) = \binom{n}{k}_x^{**} + p\binom{n}{k}_x^{*}$$

Proof. From the last definition we have that

$$\begin{aligned}
\phi(\binom{n}{k}_x) &= \sum \phi\left((\delta(\delta(...(\delta(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_{k-1}}})^{p^{a_k}}\right) \\
&= \sum \left((\delta(\delta(...(\delta(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_{k-1}}})^{p^{a_k+1}} + p\delta\left((\delta(\delta(...(\delta(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_{k-1}}})^{p^{a_k}}\right)\right) \\
&= \sum_{\sum a_j = n-k} (\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k+1}} + p \sum_{\sum a_j = n-k} \delta(\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k}} \\
&= \binom{n}{k}_x^{**} + p\binom{n}{k}_x^{*}
\end{aligned}$$

□

Lemma 2. *Let $n \in \mathbb{N}$, and $0 \leqslant k \leqslant n+1$, then,*

$$\binom{n+1}{k}_x = \binom{n}{k}_x^{**} + \binom{n}{k-1}_x^{*}$$

This result and the fact that the expression $\binom{n}{k}_x$ has exactly $\binom{n}{k}$ terms, justify the Pascal terminology.

Proof. The proof is by induction over n. For $n = 1$ in the statement, the possibilities for k in the left hand side are:

$$\begin{aligned}
\binom{2}{0}_x &= x^{p^2} \\
\binom{2}{1}_x &= \delta(x^p) + (\delta(x))^p \\
\binom{2}{2}_x &= \delta^2(x)
\end{aligned}$$

for $k = 0, 1, 2$ respectively.

For the right hand side we have:

$$\begin{aligned}
\binom{1}{0}_x^{**} + \binom{1}{-1}_x^{*} &= x^{p^2} \\
\binom{1}{1}_x^{**} + \binom{1}{0}_x^{*} &= (\delta(x))^p + \delta(x^p) \\
\binom{1}{2}_x^{**} + \binom{1}{1}_x^{*} &= \delta^2(x)
\end{aligned}$$

for $k = 0, 1, 2$ respectively. All of the above imply that

$$\binom{n+1}{k}_x = \binom{n}{k}_x^{**} + \binom{n}{k-1}_x^{*} \qquad n = 1$$

which is the first induction steep.

Now suppose the statement is true for all integers t, $0 \leqslant t \leqslant n$. We claim that

$$\binom{n+2}{k}_x = \binom{n+1}{k}_x^{**} + \binom{n+1}{k-1}_x^{*} \qquad 0 \leqslant t \leqslant n$$

In fact

$$\begin{aligned}
\binom{n+2}{k}_x &= \sum_{\sum a_j = n+2-k} (\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k}} \\
&= \sum_{\substack{\sum a_j = n+2-k \\ a_k \geqslant 1}} (\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k}} + \sum_{\substack{\sum a_j = n+2-k \\ a_k = 0}} (\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k}} \\
&= \sum_{\sum a_j = n+1-k} (\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k+1}} + \sum_{\sum a_j = n+2-k} \delta(\delta(\delta...(x^{p^{a_0}}))^{p^{a_1}}...)^{p^{a_k}} \\
&= \binom{n+1}{k}_x^{**} + \binom{n+1}{k-1}_x^{*}
\end{aligned}$$

□

Next we present our formula for $\phi^n(x)$. This formula is useful because it keeps track of the degree and order of all its terms.

Theorem 5. *Let $n \in \mathbb{Z}$ and $n \geqslant 0$, then,*

$$\phi^n(x) = \sum_{k=0}^{n} p^k \binom{n}{k}_x$$

Proof. Again by induction on n. For $n = 1$ the result is evident. Now suppose the statement is true for $0 \leqslant t \leqslant n$. Since ϕ is additive and fixes p, it follows

$$\begin{aligned}
\phi^{n+1}(x) &= \sum_{k=0}^{n} p^k \phi(\tbinom{n}{k}_x) \\
&= \sum_{k=0}^{n} p^k [\tbinom{n}{k}_x^{**} + p\tbinom{n}{k}_x^{*}] \\
&= [\tbinom{n}{0}_x^{**} + p\tbinom{n}{0}_x^{*}] + p[\tbinom{n}{1}_x^{**} + p\tbinom{n}{1}_x^{*}] + \ldots + p^{n-1}[\tbinom{n}{n-1}_x^{**} + p\tbinom{n}{n-1}_x^{*}] + p^n[\tbinom{n}{n}_x^{**} + p\tbinom{n}{n}_x^{*}] \\
&= \tbinom{n}{0}_x^{**} + p[\tbinom{n}{0}_x^{*} + \tbinom{n}{1}_x^{**}] + p^2[\tbinom{n}{1}_x^{*} + \tbinom{n}{2}_x^{**}] + \ldots + p^n[\tbinom{n}{n-1}_x^{*} + \tbinom{n}{n}_x^{**}] + p^{n+1}\tbinom{n}{n}_x^{*} \\
&= \sum_{k=0}^{n+1} p^k \tbinom{n+1}{k}_x
\end{aligned}$$

The last equality follows by the Lemma 2. □

Theorem 5 implies the following theorem, where one can see the similarities between δ and the usual derivative $\frac{dx}{dt}$.

Theorem 6. *(The Chain Rule) Let $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ then,*

$$\delta^n(x^m) \equiv \left(m\,(x^{p^n})^{m-1}\delta^n(x) + T \right) \; mod(p)$$

where $T \in \mathcal{O}(n-1)$.

(The Product Rule) Let $u, v \in R\{x\}$, then,

$$\delta^n(uv) \equiv \left(u^{p^n}\delta^n(v) + v^{p^n}\delta^n(u) + T \right) \; mod(p)$$

where $T \in \mathcal{O}_{u,v}(n-1)$.

Proof. For the chain rule, let $y = x^m$ then by Theorem 3 implies that $\phi^n(y) = \phi^n(x^m)$, and since ϕ is a ring homomorphism we obtain that

$$\sum_{k=0}^{n} p^k \binom{n}{k}_y = \left(\sum_{k=0}^{n} p^k \binom{n}{k}_x \right)^m .$$

Hence

$$p^n\binom{n}{n}_y + \sum_{k=0}^{n-1} p^k \binom{n}{k}_y = \left(p^n\binom{n}{n}_x + \sum_{k=0}^{n-1} p^k \binom{n}{k}_x \right)^m$$

If we set that $a_u = \sum_{k=0}^{n-1} p^k \binom{n}{k}_u$, then we get

$$p^n\binom{n}{n}_y + a_y = \left(p^n\binom{n}{n}_x + a_x\right)^m$$

but

$$\left(p^n\binom{n}{n}_x + a_x\right)^m = \left(p^n\binom{n}{n}_x\right)^m + m\left(p^n\binom{n}{n}_x\right)^{m-1} a_x + \cdots + mp^n\binom{n}{n}_x a_x^{m-1} + a_x^m$$

Grouping the elements of order n and using the fact that $a_y \in \mathcal{O}(n-1)$, we have that

$$p^n\binom{n}{n}_y = \left[\left(p^n\binom{n}{n}_x\right)^m + m\left(p^n\binom{n}{n}_x\right)^{m-1} a_x + \cdots + mp^n\binom{n}{n}_x a_x^{m-1}\right] + (a_x - a_y).$$

Dividing by p^n we obtain that

$$\binom{n}{n}_y = p^{n(m-1)}\binom{n}{n}_x^m + mp^{n(m-2)}\binom{n}{n}_x^{m-1} a_x + \cdots + m\binom{n}{n}_x a_x^{m-1} + \frac{(a_x - a_y)}{p^n}.$$

Since $a_x = \binom{n}{0}_x = x^{p^n}$ and $\binom{n}{n}_u = \delta^n(u)$ we get that

$$\delta^n(y) = p^{n(m-1)}\binom{n}{n}_x^m + mp^{n(m-2)}\binom{n}{n}_x^{m-1} a_x + \cdots + m\delta^n(x)_x a_x^{m-1} + \frac{(a_x - a_y)}{p^n}$$

Taking the last equation modulo p we obtain our desired result.

For the product rule let $y = uv$ where $u, v \in R\{x\}$. Then Theorem 3 implies that

$$\phi^n(y) = \phi^n(uv) = \phi^n(u)\phi^n(v)$$

and

$$\sum_{k=0}^{n} p^k \binom{n}{k}_y = \left(\sum_{k=0}^{n} p^k \binom{n}{k}_u\right)\left(\sum_{k=0}^{n} p^k \binom{n}{k}_v\right)$$

Take $b_w := \sum_{k=0}^{n-1} p^k \binom{n}{k}_w$. Then we have

$$\begin{aligned} p^n \binom{n}{n}_y + b_y &= \left(p^n \binom{n}{n}_u + b_u\right)\left(p^n \binom{n}{n}_v + b_v\right) \\ &= p^{2n} \binom{n}{n}_u \binom{n}{n}_v + p^n \binom{n}{n}_u b_v + p^n \binom{n}{n}_v b_u + b_u b_v \end{aligned}$$

Isolating $\binom{n}{n}_y$ we obtain the following

$$\binom{n}{n}_y = p^n \binom{n}{n}_u \binom{n}{n}_v + \binom{n}{n}_u b_v + \binom{n}{n}_v b_u + \frac{b_u b_v - b_y}{p^n}$$

Again projecting the last equation modulus p we obtain our desired result. □

It is clear, from the chain rule and using the fact that δ and ϕ commute, that we have the following more general result:

Corollary 3. *For $y = x^{m\phi^t} = (x^{\phi^t})^m$ and $t \in \mathbb{N}$ we have*

$$\delta^n(x^{m\phi^t}) \equiv \left(m\left(x^{\phi^t}\right)^{p^n(m-1)} \delta^n(x)^{p^t} + T\right) \; mod(p)$$

where $T \in \mathcal{O}(n-1)$.

The next corollary explain one of the achievements of Theorem 3.

Corollary 4. *Let $n \in \mathbb{N}$, $f \in \mathbb{Z}[\phi]$ where p does not divide the leading coefficient of f. Assume that $y = x^{f(\phi)}$ then,*

$$deg_{\delta^n(x)}(\overline{\delta^n(y)}) = p^{deg(f)}$$

Proof. Let $n \in \mathbb{N}$ and $f(\phi) = \sum_{i=0}^{t} a_i \phi^i \in \mathbb{Z}[\phi]$. Without loss of generality we can assume that all the coefficients of $f(\phi)$ are positive, otherwise we will have denominators but this fact does not change the result. Let $y = x^{f(\phi)}$ then

$$\delta^n(y) = \delta^n(x^{f(\phi)}) = \delta^n\left(\prod_{i=0}^{t} \phi^i(x^{a_i})\right)$$

Now using the product rule for $t+1$ factors we get

$$\begin{aligned}
\delta^n(y) &= \delta^n(x^{f(\phi)}) \\
&= \delta^n\left(\prod_{i=0}^{t}\phi^i(x^{a_i})\right) \\
&= \sum_{i=0}^{t}\left(\prod_{j\neq i}^{t}(x^{a_j\phi^j})^{p^n}\right)\delta^n(x^{a_i\phi^i}) + T + pA \\
&= \sum_{i=0}^{t}\left(x^{p^n[f(\phi)-a_i\phi^i]}\right)\delta^n(x^{a_i\phi^i}) + T + pA
\end{aligned}$$

where $T \in \mathcal{O}(n-1)$ and $A \in R$. Taking the last equation modulo p and using the chain rule, we obtain the following result:

$$\delta^n(y) \equiv \left(\sum_{i=0}^{t} a_i x^{p^n[f(p)-p^i]}\left(\delta^n(x)\right)^{p^i} + T\right) \; mod(p)$$

From the last equation and since $p \nmid a_t$ one can see that

$$deg_{\delta^n(x)}(\overline{\delta^n(y)}) = p^{deg(f)}.$$

□

2.2 Differential Groups

In this section we introduce and study some remarkable differential groups also referred to as $\delta-$subgroups of $R^{\times}$. These differential groups will be the Galois Groups in the invariant theory that we address in this thesis.

Before we provide the definition of our $\delta-$subgroups let's define first the rule of exponents.

Definition 13. Let $\mathbb{Z}[\phi]$ be the set of all the polynomials with integer coefficients in the variable ϕ. Suppose that $f(\phi) = \sum_{i=0}^{t} a_i\phi^i \in \mathbb{Z}[\phi]$, then,

$$x^{f(\phi)} = x^{\left(\sum_{i=0}^{t} a_i\phi^i\right)} = \prod_{i=0}^{t}\phi^i(x^{a_i})$$

Notice that Definition 13 implies composition. For any f and g in $\mathbb{Z}[\phi]$ we have

$$x^{fg} = (x^f)^g$$

Let's introduce now our differential subgroups.

Definition 14. *Let $f \in \mathbb{Z}[\phi]$, then define the sets*

$$\Gamma_f := \{\lambda \in R^\times : \lambda^f = 1\}, \quad \textit{and} \quad \Gamma_f^{(n)} = (1 + p^n R) \cap \Gamma_f.$$

Clearly Γ_f is a subgroup of $R^\times$ under multiplication.

The next result shows that the subgroups Γ_f are "sufficiently" nontrivial. It also illustrates, with the particular case when $f(\phi) = \phi - m$, the way how we will prove the more general case, where $f \in \mathbb{Z}[\phi]$.

Lemma 3. *For any $\zeta \in \mu_{p-m}$ there is a sequence $\{(\lambda_k, x_{k-1})\}_{k=1}^{\infty} \subset R^2$, defined recursively as follows: $\lambda_1 = \zeta$, $x_0 = 0$, and $\lambda_{k+1} = \lambda_k + p^k x_k$. This sequence has the following property:*

$$\phi(\lambda_k) \equiv \lambda_k^m \; mod(p^k) \qquad k \in \mathbb{N}$$

Proof. We construct this sequence by induction on k. For the first induction step, $k = 0$, it is clear, because $\phi(\lambda_1) = \lambda_1^m + p\delta(\lambda_1) = \lambda_1^m$. Then we have first pair (λ_1, x_0). For the induction hypothesis step: Assume (λ_k, x_{k-1}) has the following property,

$$\phi(\lambda_k) \equiv \lambda_k^m \; mod(p^k)$$

We need to find the next pair (λ_{k+1}, x_k).

We let $\lambda_{k+1} = \lambda_k + p^k y_k$, then,

$$\lambda_{k+1}^m = (\lambda_k + p^k y_k)^m = \lambda_k^m + m\lambda_k^{m-1}(p^k y_k) + p^{2k} A$$

where $A \in R$. On the other hand,

$$\phi(\lambda_{k+1}) = \phi(\lambda_k) + p^k \phi(y_k) = \lambda_k^m + p^k B + p^k \phi(y_k)$$

where $B \in R$. This second equality comes from the induction hypothesis. So we need x_k such that

$$x_k^p - m\lambda_k x_k + B \equiv 0 \, mod(p)$$

This equation has all its solutions in the algebraically closed field R/pR.

Next we take one of the pre-images of the projection $mod(p)$ and we call it y_k. This y_k satisfies the desired condition,

$$\lambda_{k+1} = \lambda_k + p^k y_k$$

Let $x_k = y_k$, this condition gives the next pair (λ_{k+1}, x_k), in our induction proof.

□

Lemma 3 prove the non triviality of the subgroup $\Gamma_{\phi-m}$ of $R^\times$. In the next theorem we extend Lemma 3 to more general polynomials.

Theorem 7. *Let p be a large enough prime number. Assume that the polynomial $f(\phi) = \sum_{i=0}^{l} a_i \phi^i \in \mathbb{Z}[\phi]$ with $p \nmid f(p)$ and $a_l > 0$. Then for any $\zeta \in \mu_{f(p)}$, there is a sequence $\{(\lambda_k, x_{k-1})\}_{k=1}^{\infty} \subset R^2$, such that $\lambda_1 = \zeta$, $x_0 = 0$, and $\lambda_{k+1} = \lambda_k + p^k x_k$, with the property that*

$$(\lambda_k)^{f^+} \equiv (\lambda_k)^{f^-} mod\left(p^k\right) \qquad k \in \mathbb{N}$$

where $f^+(\phi) = \sum_{i=0}^{l} a_i^+ \phi^i$ and $f^-(\phi) = \sum_{i=0}^{l-1} a_i^- \phi^i$ are the positive and the negative parts of f respectively, i.e. $f = f^+ - f^-$.

Proof. We construct this sequence by induction over k.

Step1. $(k = 1)$. Since the constants with respect to the derivation δ are the n^{th} roots of unity prime to p, we get that

$$\lambda_1^{f(\phi)} = \lambda_1^{f(p)} = 1$$

Step 2. Assume the statement for k, and prove it, for $k + 1$.

Let $\lambda_{k+1} = \lambda_k + p^k x_k$, with the property that

$$\lambda_k^{f^+(\phi)} \equiv \lambda_k^{f^-(\phi)} \quad mod(p^k)$$

From the recursion and from the rule of exponents, we have that

$$\begin{aligned}
\lambda_{k+1}^{f^+(\phi)} &= (\lambda_k + p^k x_k)^{f^+(\phi)} \\
&= \prod_{i=0}^{l} \phi^i(\lambda_k + p^k x_k)^{a_i^+} \\
&= \prod_{i=0}^{l} \phi^i(\lambda_k^{a_i^+} + p^k a_i^+ \lambda_k^{a_i^+ - 1} x_k) \\
&= \prod_{i=0}^{l} [\phi^i(\lambda_k^{a_i^+}) + p^k a_i^+ \phi^i(\lambda_k^{a_i^+ - 1}) \phi^i(x_k)] \\
&= \lambda_k^{f^+(\phi)} + p^k \sum_{i=0}^{l} a_i^+ \lambda_k^{f^+(\phi)} \lambda_k^{-\phi^i} x_k^{\phi^i} \\
&= \lambda_k^{f^-(\phi)} + p^{k+1} A + p^k \sum_{i=0}^{l} a_i^+ \lambda_k^{f^+(\phi)} \lambda_k^{-\phi^i} x_k^{\phi^i}
\end{aligned}$$

Then for $f^+(\phi)$ we have that

$$\lambda_{k+1}{}^{f^+(\phi)} = \lambda_k^{f^-(\phi)} + p^{k+1} A + p^k \sum_{i=0}^{l} a_i^+ \lambda_k^{f^+(\phi)} \lambda_k^{-\phi^i} x_k^{\phi^i}$$

where $A \in R$. Similarly for $f^-(\phi)$ we have

$$\lambda_{k+1}^{f^-(\phi)} = \lambda_k^{f^-(\phi)} + p^k \sum_{i=0}^{l-1} a_i^- \lambda_k^{f^-(\phi)} \lambda_k^{-\phi^i} x_k^{\phi^i}$$

For the equations to be congruent modulus p^{k+1} the following holds:

$$\sum_{i=0}^{l} a_i \lambda_1^{-p^i} x_k^{p^i} \equiv 0 \, mod(p), \qquad \lambda_1 \in \mu_{f(p)}$$

The reduction modulo p of the left hand side has all its roots in the algebraically closed field $k = R/pR = \mathbb{F}_p^a$. Next we take one of the pre-images of one of these roots and we call it x_k. This x_k satisfies the desired conditions,

$$\lambda_{k+1} = \lambda_k + p^k x_k, \quad and \quad \lambda_{k+1}^{f^+(\phi)} \equiv \lambda_{k+1}^{f^-(\phi)} \quad mod(p^{k+1})$$

This condition gives the next pair (λ_{k+1}, x_k), in our induction proof. □

Corollary 5. *Let* $f(\phi) = \sum_{i=0}^{l} a_i \phi^i$ *and* p *be such that* $p \nmid a_l, a_0$ *as in Theorem 7. Then,*

$$\left| \frac{\Gamma_{f(\phi)}}{\Gamma_{f(\phi)}^{(n+1)}} \right| \geq \left| \mu_{f(p)} \right| p^{n \cdot deg(f)} = |f(p)| \, p^{n \cdot deg(f)} \tag{2.2.1}$$

Proof. To prove this corollary we will use the construction from the proof of Theorem 7 to count all the possible choices for the roots of the polynomial $h_f(x) \in k[x]$. Since $\lambda_0 \neq 0$, and $p \nmid a_0$, then the polynomial

$$h_f(x) = \sum_{i=0}^{l} a_i \lambda_0^{(a_i - 1)(f(p) - a_i p^i)} x^{p^i} + B_n \in k[x]$$

doesn't have multiple roots. On the other hand, since $p \nmid a_l, a_0$ and $k = R/pR$ is an algebraically close field, then the set $\{x \in k = R/pR : h_f(x) = 0\}$ has p^l elements. From the proof of Theorem 7, one can see that all the elements $\lambda \in \frac{\Gamma_f}{\Gamma_f^{(n+1)}} = \Gamma_f \; mod \, (p^{n+1})$ have the form

$$\lambda = \lambda_0 + \sum_{i=0}^{n} p^i x_i \qquad \lambda_0 \in \mu_{f(p)}$$

and the x_i are such that $\overline{x}_i \in \{x \in k : h_f(x) = 0\}$. Since $p \nmid f(p)$ then we have that $\left| \frac{\Gamma_{f(\phi)}}{\Gamma_{f(\phi)}^{(n+1)}} \right| \geq \left| \mu_{f(p)} \right| p^{n \cdot deg(f)} = |f(p)| \, p^{n \cdot deg(f)}$ by direct counting. □

2.3 $\delta-$Galois Theory: The Proof of the Main Theorem

Now we have created the preamble to give the proof of our main theorem. This theorem, as we said in the overview, is a generalization of the following

Theorem 8. *[2] Consider the element* $x^{\phi-1}$ *from the ring* $R\{x\}_{(p)}$. *Then the extension* $k\langle x^{\phi-1} \rangle \subseteq k\langle x \rangle$ *is Galois with Galois group* $\Gamma_{\phi-1}$. *In particular we have that*

$$k\langle x^{\phi-1} \rangle = k\langle x \rangle^{\Gamma_{\phi-1}}, \quad and \quad \Gamma_{\phi-1} \cong \mathbb{Z}_p^{\times}$$

In our main theorem we extend Theorem 8 from the case of linear polynomial $\phi - 1$ to a rather general polynomials $f(\phi) \in \mathbb{Z}[\phi]$ as follows:

Theorem 9. *(Main Theorem) Let $f \in \mathbb{Z}[\phi]$ be such that p does not divide its leading coefficient and its constant term. Consider the element $x^{f(\phi)}$ from the ring $R\{x\}_{(p)}$. Then the extension $k\langle x^{f(\phi)}\rangle \subseteq k\langle x\rangle$ is Galois with Galois group $\Gamma_{f(\phi)}$. In particular,*

$$k\langle x^{f(\phi)}\rangle = k\langle x\rangle^{\Gamma_{f(\phi)}}$$

To prove Theorem 9 we need to introduce first some definitions and a lemma.

Definition 15. *Let $f \in \mathbb{Z}[\phi]$, then define the map*

$$\theta_\lambda : k(x, x', ..., x^{(n-1)}) \longrightarrow k(x, x', ..., x^{(n-1)}), \quad by \quad \theta_\lambda(x^{(i)}) = (\lambda x)^{(i)}.$$

And the map

$$\rho_n : \Gamma_f \longrightarrow Aut(k(x, x', ..., x^{(n-1)})/k), \quad by \quad \lambda \longmapsto \theta_\lambda.$$

Lemma 4. *Let n, l be natural numbers, such that, $0 < l < n$. Suppose that $\lambda = x + p^n y_0$, y_0 in R. Then, for some $y_l \in R$, we have*

$$\delta^l(\lambda) = \delta^l(x) + p^{n-l} y_l$$

And for $n \in \mathbb{N}$, and $\lambda \in (1 + p^n R)$, we also have that,

$$\delta^{n-1}(x\lambda) \equiv \delta^{n-1}(x) \, mod \, p$$

Proof. The proof will be by induction on l. The first induction step is clear. For the induction hypothesis step: Assume that the statement is true for l, i.e.,

$$\delta^l(\lambda) = \delta^l(x) + p^{n-l} y_l \qquad y_l \in R, \; 0 < l + 1 < n$$

then,

$$p\delta^{l+1}(\lambda) = p\delta^{l+1}(x) + p^{n-l}\phi(y_l) + (\delta^l(x))^p - (\delta^l(x) + p^{n-l}y_l)^p$$

Dividing the last equation by p we get,

$$\delta^{l+1}(\lambda) = \delta^{l+1}(x) + p^{n-l-1}\phi(y_l) - p^{n-l-1}\sum_{k=1}^{p}\binom{p}{k}(\delta^l(x))^{p-k}p^{(k-1)(n-l)}y_l^k$$

Then we obtain, $\delta^{l+1}(\lambda) = \delta^{l+1}(x) + p^{n-l-1}y_{l+1}$, where y_{l+1} is clearly in R. To prove the second part of the lemma we take $y_0 = \alpha x$ and $l = n-1$. □

Corollary 6. *Let $n \in \mathbb{N}$. Then we have that*

$$\Gamma^{(n)}_{f(\phi)} = Ker(\rho_n).$$

Proof. [$\subseteq$]: Let $\lambda \in \Gamma^{(n)}_{f(\phi)}$. Since $\Gamma^{(n)}_{f(\phi)} = \Gamma_{f(\phi)} \cap (1 + p^nR)$, we get that $\lambda \in \Gamma_{f(\phi)}$ and $\lambda \in (1 + p^nR)$. Then from Lemma 4 implies that

$$\delta^{n-1}(x\lambda) \equiv \delta^{n-1}(x)\, mod\, p$$

Hence

$$\Gamma^{(n)}_{f(\phi)} \subseteq Ker(\rho_n)$$

[$\supseteq$]: Let $\lambda \in Ker(\rho_n)$. Then

$$\delta^{i-1}(x\lambda) \equiv \delta^{i-1}(x)\, mod(p), \quad 0 < i+1 < n.$$

Then for $x = 1$ there is a sequence $\{r_i : i = 1, ..., n-1\}$ such that

$$\begin{aligned} \lambda &= 1 + pr_0 \\ \lambda' &= pr_1 \\ \lambda^{(n-1)} &= pr_{n-1} \end{aligned}$$

We claim that p^{n-1} divides r_0. If we compare the first two equations we obtain

the following:

$$(1 + r_0 p)' = p r_1$$

this implies that

$$1 + p\phi(r_0) - (1 + r_0 p)^p = p^2 r_1$$

Then we get that $p \mid \phi(r_0)$, then $p \mid r_0$. We can conclude that $\lambda = 1 + r_1 p^2$. If we do the same with the first three equations we obtain that $p^2 \mid r_0$. Following in the same fashion we obtain that p^{n-1} divides r_0, and then, $1 + r_0^n p \in (1 + p^n R)$. □

In what follows set $y_n = \delta^n(x^{f(\phi)})$, and denote by $\eta_n \in k\langle x \rangle$ the image of y_n. Note that $\eta_0 = \overline{x^{f(p)}}$.

The strategy of the proof of Theorem 9 is as follows: The inclusion " $\subset$ " will be clear. To prove the inclusion " $\supset$ " it will be enough to show the following two lemmas.

Lemma 5. $\left[k(x, x', x'', ..., x^{(n)}) : k(\eta_0, \eta_1, \eta_2, ..., \eta_n)\right] \leq |f(p)|\, p^{n \cdot deg(f)}$.

Proof. Using Corollary 4. □

Lemma 6. *The cardinality of the image I_n of ρ_n is greater than or equal to $|f(p)|\, p^{n \cdot deg(f)}$.*

Proof. The first isomorphism theorem implies that $I_n \cong \frac{\Gamma_{f(\phi)}}{Ker(\rho_n)}$. From Corollary 6 we obtain that

$$|I_n| = \left|\frac{\Gamma_{f(\phi)}}{Ker(\rho_n)}\right| = \left|\frac{\Gamma_{f(\phi)}}{\Gamma^{(n)}_{f(\phi)}}\right| \geq |f(p)|\, p^{n \cdot deg(f)}$$

□

Proof of the Main theorem

Proof. Consider the extensions

$$\begin{array}{ccccc} k(\eta_0, \eta_1, ..., \eta_{n-1}) & \subset & k(x, x', ..., x^{(n-1)})^{\Gamma_f} & \subset & k(x, x', ..., x^{(n-1)}) \\ & \alpha & & \beta & \end{array}$$

By the Lemma 6 the degree of β equals $|f(p)|\, p^{n \cdot deg(f)}$. From Lemma 5, we have that, the extension $\beta \circ \alpha$ has at most degree $|f(p)|\, p^{n \cdot deg(f)}$. This forces α to be an equality. □

3 Subgroups of $B_n(R)$

In this chapter we define and study an interesting class of subgroups of $B_n(R)$, the group of $n \times n$ invertible and upper triangular matrices with entries in R, by introducing the concept of Leibniz Systems. The present chapter will constitute a wide open source of study for future research.

3.1 Leibniz Systems

Definition 16. A *Leibniz system* of size n is a collection $f = (f_{ij})_{1\leq i,j\leq n}$, $f_{ij} : (R^{\times})^n \longrightarrow R[\frac{1}{p}]$ satisfying the following condition:

$$f_{ij}(x_1y_1, x_2y_2, ..., x_ny_n) = \begin{cases} f_{i1}(x_1, x_2, ..., x_n)f_{1j}(y_1, y_2, ..., y_n) + \ldots + f_{in}(x_1, x_2, ..., x_n)f_{nj}(y_1, y_2, ..., y_n), & j > i \\ x_iy_j & i = j \\ 0 & j < i \end{cases}$$

Denote by $\mathcal{L}$ the set of all Leibniz systems. Let S_i are subgroups of $R^{\times}$, then a *Leibniz group*, is a group of the form

$$G_f(R) = \{(f_{ij}(a)) \in B_n(R) : a \in \prod_{i=1}^{n} S_i\}$$

where $f \in \mathcal{L}$.

Obviously $G_f(R)$ is a subgroup of $B_n(R)$.

Example 8. For $n = 2$ let $f = (f_{ij})_{1\leq i,j\leq 2}$ be such that $f_{12}(x, y) = k(x - y)$,

$f_{11} = x$ and $f_{22} = y$, where $k \in R[\frac{1}{p}]$. It is easy to check that f form a Leibniz system.

Lemma 7. *The Leibniz system f from the last example is the only Leibniz system for $n = 2$.*

Proof. It is clear that the function $f_{12} = k(x-y)$ where $k \in R[\frac{1}{p}]$, has the property

$$f(aa', dd') = af(a', d') + d'f(a, d)$$

for all $a, a', d, d' \in R^{\times}$. On the other hand, let f be a function that has the property

$$f(xx', yy') = xf(x', y') + y'f(x, y)$$

then, $f(1,1) = f(1,1) + f(1,1)$, so $f(1,1) = 0$. Since

$$f(xx', 1) = xf(x', 1) + f(x, 1) = x'f(x, 1) + f(x', 1)$$

then, $f(x,1) = (x-1)\frac{f(x',1)}{x'-1}$, so fixing $\frac{f(x',1)}{x'-1} = k_1$, we obtain $f(x,1) = k_1(x-1)$. From the property we also have,

$$f(1, yy') = f(1, y') + y'f(1, y) = f(1, y) + yf(y', 1)$$

similarly we get, $f(1,y) = k_2(y-1)$, and since

$$f(x1, 1y) = xf(1, y) + f(x, 1) = k_2x(y-1) + k_1(x-1)$$

we obtain $k_1 = -k_2 = k$, and $f(x,y) = k(x-y)$ for some $k \in R[\frac{1}{p}]$. □

Theorem 10. *The set* $\{\begin{pmatrix} a & f(a,b) \\ 0 & b \end{pmatrix} \in B_2(R)\}$ *is a subgroup of $B_2(R)$, if and only if, $f(x,y) = k(x-y)$ for some $k \in R[\frac{1}{p}]$.*

Proof. Use Lemma 7. □

For the case $n = 3$, we have the following example:

Example 9. To have a Leibniz system $f = (f_{ij})_{1\leq i,j\leq 3}$, where $f_{11} = x$, $f_{22} = y$, $f_{33} = z$ and the $f_{ij}(x, y, z)$ $j > i$, we need the following conditions to hold:

$$\begin{aligned} f_{12}(xx', yy', zz') &= xf_{12}(x', y', z') + y'f_{12}(x, y, z) \\ f_{13}(xx', yy', zz') &= xf_{13}(x', y', z') + f_{12}(x, y, z)f_{21}(x', y', z') + z'f_{13}(x, y, z) \\ f_{21}(xx', yy', zz') &= yf_{21}(x', y', z') + z'f_{21}(x, y, z) \end{aligned}$$

Since the functions in a Leibniz system are functions that can be viewed as functions of diagonal matrices, one can see that they only produce Abelian subgroups of $B_n(R)$. Notice that they define homomorphisms from $R^\times$ to $B_n(R)$.

Definition 17. Let $\varphi : R \longrightarrow R$ be an additive map, i.e., $\varphi(x+y) = \varphi(x)+\varphi(y)$; and $\psi : R^\times \longrightarrow R$ be an homomorphism, i.e., $\psi(xy) = \psi(x) + \psi(y)$.

A concrete example of a function ψ from the last definition will be

$$\psi(t) = \frac{1}{p} log(1 + p\frac{\delta(t)}{t^p})$$

this function was introduced by A. Buium in [1].

Example 10. Let S be a subgroup of $R^\times$ and $x, z \in S$. Consider the subset $\mathcal{D}$ of $B_3(R)$ of matrices of the form

$$\begin{pmatrix} x & x\psi(xz) & 0 \\ 0 & x & 0 \\ 0 & 0 & z \end{pmatrix}$$

Then $\mathcal{D}$ is a Leibniz subgroup of $B_3(R)$.

Using the last example we can construct an example of a Leibniz group of $B_n(R)$ as follows:

Example 11. Let $A = \begin{pmatrix} x & x\psi(x) \\ 0 & x \end{pmatrix}$ or $A = \begin{pmatrix} x & x\psi(xz) & 0 \\ 0 & x & 0 \\ 0 & 0 & z \end{pmatrix}$, where $x, z \in$

$S < R^{\times}$, and $n \in 2\mathbb{N} \cup 3\mathbb{N}$. Then the subgroup

$$G(S) = \{(a_{ij}) \in B_n(R) : a_{ii} = A, a_{ij} = 0, i \neq j\}$$

is a Leibniz group of $B_n(R)$.

In particular if in the last two examples we take $\psi(t) = \frac{1}{p} log(1 + p\frac{\delta(t)}{t^p})$ the Leibniz group became a Leibniz $\delta-$subgroup of $B_n(R)$.

3.2 A $B_4(R)$ Example

In this section we will illustrate the differences in finding Borel subgroups in $B_n(R)$ when n is even or odd. One of these differences is the symmetry in the properties of the functions in the differential systems. This fact will be shown in the following example.

Example 12. Let $\varphi : R \longrightarrow R$ be an additive map, and f a function with the following property,

$$f(x + y) = f(x) + f(y) + x\varphi(y) + y\varphi(x)$$

then the set D of all the matrices of the form

$$\begin{pmatrix} 1 & \varphi(x) & x & f(x) \\ 0 & 1 & 0 & x \\ 0 & 0 & 1 & \varphi(x) \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

is a subgroup of $B_4(R)$. In particular if we take $f(x) = xh(\phi)(x)$, where $\varphi = h(\phi) \in \mathbb{Z}[\phi]$. It is clear that

$$\begin{aligned} f(x + y) &= (x + y)h(\phi)(x + y) \\ &= xh(\phi)(x) + yh(\phi)(y) + xh(\phi)(y) + yh(\phi)(x) \\ &= f(x) + f(y) + x\varphi(y) + y\varphi(x) \end{aligned}$$

and D will be also a $\delta-$subgroup of $B_4(R)$.

At this point we have produced several $\delta-$subgroups $B_n(R)$. Another example will be:

Example 13. Consider the subset of $B(R)$ of matrices of the form

$$\begin{pmatrix} x & x\psi(x) & k(x-1) \\ 0 & x & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Where $x \in G < R^{\times}$, then, it is also a commutative subgroup of $B_3(R)$.

Let $x \in S$ where S is a subgroup of $R^{\times}$. Assume that f is a function with the following property

$$f(xy) = xf(y) + yf(x) + xy\psi(x)\psi(y) \tag{3.2.1}$$

If such a function exists then, the subset of $B_3(R)$ of matrices of the form

$$\begin{pmatrix} x & x\psi(x) & f(x) \\ 0 & x & x\psi(x) \\ 0 & 0 & x \end{pmatrix}$$

then, it is also a commutative subgroup of $B_n(R)$. If we divide equation 3.2.1 by xy we obtain,

$$\frac{f(xy)}{xy} = \frac{f(y)}{y} + \frac{f(x)}{x} + \psi(x)\psi(y) \tag{3.2.2}$$

And if we take $h(x) = \frac{f(x)}{x}$, equation 3.2.2 becomes,

$$h(xy) = h(x) + h(y) + \psi(x)\psi(y) \tag{3.2.3}$$

In the following example we show a concrete function h with the property in equation 3.2.3:

Example 14. Le h be the the following function

$$h(x) = \phi(\psi(x)) + \frac{1}{2}\psi(x)^2$$

We can also see from equation 3.2.1 that,

$$f(x^n) = nx^{n-1}f(x) + nx^n\psi(x)^2, \quad and \quad h(x^n) = nh(x) + n\psi(x)^2,\ n > 1$$

3.3 More Subgroups of $B_n(R)$

Let's start this section by analyzing the next example:

Example 15. For $B_4(R)$, assume that the map $\psi : R^\times \longrightarrow R$ is a group homomorphism, then, the set of all matrices in $B_4(R)$ of the form

$$E_4(x) = \begin{pmatrix} 1 & \psi(x) & \frac{1}{2!}\psi(x)^2 & \frac{1}{3!}\psi(x)^3 \\ 0 & 1 & \psi(x) & \frac{1}{2!}\psi(x)^2 \\ 0 & 0 & 1 & \psi(x) \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

is a subgroup of $B_4(R)$.

In general for $B_n(R)$, we have,

Theorem 11. *The set of all matrices of the form*

$$E_n(x) = \begin{pmatrix} 1 & \psi(x) & \frac{1}{2!}\psi(x)^2 & \cdots & \frac{1}{(n-1)!}\psi(x)^{n-1} \\ 0 & 1 & \psi(x) & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & \frac{1}{2!}\psi(x)^2 \\ \vdots & \vdots & \vdots & \ddots & \psi(x) \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

is a subgroup of $B_n(R)$.

And the map $E_n^\psi : R^\times \longrightarrow B_n(R)$ defined by

$$E_n^\psi(x) = \begin{pmatrix} 1 & \psi(x) & \frac{1}{2!}\psi(x)^2 & \cdots & \frac{1}{(n-1)!}\psi(x)^{n-1} \\ 0 & 1 & \psi(x) & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & \frac{1}{2!}\psi(x)^2 \\ \vdots & \vdots & \vdots & \ddots & \psi(x) \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

is a group homomorphism.

Proof. By direct computation. □

Again if we take $\psi(t) = \frac{1}{p}log(1 + p\frac{\delta(t)}{t^p})$ the subgroup $\mathcal{H} = \{E_n(x) : x \in R^\times\}$ is a $\delta-$subgroup of $B_n(R)$. We can also replace $R^\times$ by any $\Gamma_{f(\phi)}$ from chapter 2 and obtain a variety of examples of $\delta-$subgroups of $B_n(R)$.

3.4 More Leibniz $\delta-$Subgroups of $B_n(R)$

In the present section we will discus more examples of Leibniz $\delta-$Subgroups of $B_n(R)$.

We can check easily that if make a "small" perturbation in the entry a_{1n} of $E_n(x)$, ($E_n(x)$ from the last section) we still obtain a subgroup of $B_n(R)$, as follows:

Example 16. Let $t \in \mathbb{N}$, and $x \in R^\times$, then set S of all the matrices of the form

$$S_n(x) = \begin{pmatrix} 1 & \psi(x) & \frac{1}{2!}\psi(x)^2 & \cdots & \frac{1}{(n-1)!}[\psi(x)^{n-1} + \sum_{i=1}^{t}\phi^i(\psi(x))] \\ 0 & 1 & \psi(x) & \ddots & \vdots \\ 0 & 0 & 1 & \ddots & \frac{1}{2!}\psi(x)^2 \\ \vdots & \vdots & \vdots & \ddots & \psi(x) \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

is a Leibniz $\delta-$subgroup of $B_n(R)$.

Another example will be:

Example 17. Let $x \in R^\times$, then set S of all the matrices of the form

$$S_4(x) = \begin{pmatrix} 1 & \psi(x) & \frac{1}{2!}[\psi(x)^2 + \phi(\psi(x))] & \frac{1}{3!}[\psi(x)^3 + 3\psi(x)\phi(\psi(x)) + \phi^2(\psi(x)] \\ 0 & 1 & \psi(x) & \frac{1}{2!}[\psi(x)^2 + \phi(\psi(x))] \\ 0 & 0 & 1 & \psi(x) \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

is a Leibniz $\delta-$subgroup of $B_4(R)$.

It is clear that the first row of $S_n(x)$ determines the matrix. Then we can define the matrix by knowing this row, for example:

Example 18. For the case when $n = 5$ we have that the functions in the first row are:

$$\begin{aligned}
L_0(x) &= 1 \\
L_1(x) &= \psi(x) \\
L_2(x) &= \frac{1}{2!}[\psi(x)^2 + \phi(\psi(x))] \\
L_3(x) &= \frac{1}{3!}[\psi(x)^3 + 3\psi(x)\phi(\psi(x)) + \phi^2(\psi(x))] \\
L_4(x) &= \frac{1}{4!}[\psi(x)^4 + 4\psi(x)\phi^2(\psi(x)) + 6\psi(x)^2\phi(\psi(x)) + 3\phi(\psi(x)^2) + \phi^3(\psi(x))]
\end{aligned}$$

and they form a Leibniz system.

In this fashion we can find more L_k function:

Example 19. For $n = 6, 7$ we have

$L_5(x) = \frac{1}{5!}[\psi(x)^5+5\psi(x)\phi^3(\psi(x))+10\psi(x)^2\phi^2(\psi(x))+10\psi(x)^3\phi(\psi(x))+15\psi(x)\phi(\psi(x)^2)+10\phi(\psi(x))\phi^2(\psi(x))+\phi^4(\psi(x))]$,

$L_6(x) = \frac{1}{6!}[\psi(x)^6+6\psi(x)\phi^4(\psi(x))+15\psi(x)^2\phi^3(\psi(x))+20\psi(x)^3\phi^2(\psi(x))+15\psi(x)^4\phi(\psi(x))+60\psi(x)\phi(\psi(x))\phi^2(\psi(x))+45\psi(x)^2\phi(\psi(x)^2)+15\phi(\psi(x)^3)+10\phi^2(\psi(x)^2)+15\phi(\psi(x))\phi^3(\psi(x))+\phi^5(\psi(x))]$.

3.5 Coboundaries

In this section we study coboundaries. Knowing the properties of these coboundaries, will make easier the study of the Leibniz systems.

Definition 18. A function $\partial A : R^\times \times R^\times \longrightarrow R$ is called *coboundary* if there exist an expression $A(x)$ such that

$$\partial A(x, y) = A(xy) - A(x) - A(y).$$

Example 20. The function $\partial A(x,y) = \psi(x)\psi(y)$ is a coboundary, by taking $A(x) = \frac{1}{2}\psi(x)^2$. Another more complex coboundary is

$$\partial A(x,y) = \psi(x)\phi(\psi(y)) + \psi(y)\phi(\psi(x))$$

In this case we can take $A(x) = \psi(x)\phi(\psi(x))$.

It is clear from the definition that these coboundaries are symmetric in the following sense:

$$\partial A(x,y) = \partial A(y,x).$$

Definition 19. Let $k \in \mathbb{Z}$ then we define the *truncated binomial coefficient* to be the number

$$\left(\overleftarrow{\tfrac{k}{i}}\right) = \begin{cases} \binom{k}{i} & if \quad 0 \leq i < k-1 \\ 1 & i = k-1 \\ 0 & i = k \end{cases}$$

Clearly k must be bigger that 1.

Example 21. Using the truncated binomial notation we obtain that:
$L_6(x) = \frac{1}{6!}[\sum_{i=0}^{6}\left(\overleftarrow{\tfrac{6}{i}}\right)\psi(x)^i\phi^{5-i}(\psi(x)) + 60\psi(x)\phi(\psi(x))\phi^2(\psi(x)) + 45\psi(x)^2\phi(\psi(x)^2) + 15\phi(\psi(x)^3) + 10\phi^2(\psi(x)^2) + 15\phi(\psi(x))\phi^3(\psi(x))]$.

Definition 20. Let $k \in \mathbb{N}$, define the functions $L_k : R^\times \longrightarrow R$ by:

$$\begin{aligned} L_0(x) &= 1 \\ L_1(x) &= \psi(x) \\ L_2(x) &= \frac{1}{2!}[\psi(x)^2 + \phi(\psi(x))] \\ L_3(x) &= \frac{1}{3!}[\psi(x)^3 + 3\psi(x)\phi(\psi(x)) + \phi^2(\psi(x))] \\ &\vdots \\ L_k(x) &= \frac{1}{k!}[\sum_{i=0}^{k}\left(\overleftarrow{\tfrac{k}{i}}\right)\psi(x)^i\phi^{k-1-i}(\psi(x)) + A_k(x)]. \end{aligned}$$

Theorem 12. *Let $k \in \mathbb{N}$, then*

$$\partial L_k(x,y) = \sum_{i=1}^{k-1} L_i(x)L_{k-i}(y) = L_k(xy) - L(x) - L(y).$$

Proof. By the definition of L_k. □

3.6 Functions of Matrices

In this section we extend the function ψ from $R^\times$ to the set of some special matrices in $GL_n(R)$.

Definition 21. Let $n \in \mathbb{N}$, define the following set

$$\mathcal{D}_n(R) = \{A \in GL_n(R) : A = PJP^{-1}, \sigma(A) \subseteq R^\times\}.$$

Here $\sigma(A)$, as usual, stands for the spectrum of the matrix A, i.e., the set of all eigenvalues of A, and $A = PJP^{-1}$ is the Jordan canonical form of the matrix A.

Now we define the extension of ψ, which will be also called ψ when the context is understood, as follows:

Definition 22. Let $A \in \mathcal{D}_n(R)$, and $E_n(x)$ as in Section 3.3, then we define the function $\psi : \mathcal{D}_n(R) \longrightarrow GL_n(R)$ as follows:

$$\psi(A) = Pdiag(\psi(J_k))P^{-1}$$

Where $A = PJP^{-1}$ is the Jordan canonical form of A, $J = diag(J_k)$,

$$J_k(\lambda_k) = \begin{pmatrix} \lambda_k & 1 & 0 & \cdots & 0 \\ 0 & \lambda_k & 1 & \vdots & \vdots \\ 0 & 0 & \ddots & 1 & 0 \\ \vdots & \cdots & 0 & \lambda_k & 1 \\ 0 & \cdots & \cdots & 0 & \lambda_k \end{pmatrix} \quad and \quad \psi\left(J_k(\lambda_k)\right) = E_n(x).$$

Notice that we can use also The other matrices defined in last section instead $E_n(x)$, and everything will be as in the last example.

Bibliography

[1] A. Buium, *Differential characters of Abelian Varieties over p-adic fields*, Invent. Math. 122, 1995, pp. 309-340.

[2] A. Buium, *Arithmetic Differential Equations*, Mathematical Surveys and Monographs Vol. 118, AMS 2005.

[3] Kolchin, E.R. (1985), *Differential Algebraic Groups*, Pure and Apply Mathematics 114, Boston, MA.

[4] Cassidy, Phyllis Joan (1972), *Differential Algebraic Groups*, Amer. J. Math. 94: 891-954.

[5] Geometry I: *Basic Ideas and Concepts of Differential Geometry*, Encyclopedia of Mathematical Sciences. Vol. 1.

Index