Lecture Notes in Mathematics 1666

Marius van der Put Michael F. Singer

Galois Theory of Difference Equations

Springer

Marius van der Put
Michael F. Singer

Galois Theory of Difference Equations

Springer

Authors

Marius van der Put
Department of Mathematics
University of Groningen
P.O. Box
NL-9700 AV Groningen, The Netherlands
e-mail: M.van.der.Put@math.rug.nl

Michael F. Singer
Department of Mathematics
North Carolina State University
Box 8205, Raleigh, N.C. 27695-8205, USA
e-mail: singer@math.ncsu.edu

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Put, Marius van der:
Galois theory of difference equations / Marius van der Put ; Michael F. Singer. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Lecture notes in mathematics ; 1666)
ISBN 3-540-63243-3

Mathematics Subject Classification (1991): 12H10, 39A10

ISSN 0075-8434
ISBN 3-540-63243-3 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1997
Printed in Germany

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready $\TeX$ output by the authors
SPIN: 10553306 46/3142-543210 - Printed on acid-free paper

Contents

此为试读，需要完整PDF请访问：www.ertongbook.com

Algebraic Theory

We shall develop here a Galois theory for difference equations. In the Picard-Vessiot Galois theory for *differential* equations, the basic objects of study are the *Picard-Vessiot extension* of a field and its associated Galois group. Recall that a *Picard-Vessiot extension* of a differential field k is an extension K generated by a fundamental set of solutions of a linear differential equation and having the same field of constants as k. The automorphism group of K over k is an algebraic group and properties of this group reflect properties of the differential equation. When one tries to mimic this approach for difference equations one is confronted with the following example (recall that a difference field is a field k together with an automorphism ϕ of k):

Example 0.1 ([25]) *Let k be a difference field whose characteristic is not 2. If the field of constants $C_k = \{c \in k \mid \phi(c) = c\}$ is algebraically closed, then the equation $\phi x + x = 0$ has no nonzero solution in k. To see this note that if $y \in k$ satisfies $\phi y + y = 0$ then $\phi(y^2) = y^2$ so y^2 is a constant. Since C_k is algebraically closed, we have y is a constant, contradicting the fact that $\phi y = -y$.*

Therefore, if one restricts oneself to fields, the properties of having algebraically closed constants and having full sets of solutions of difference equations can be incompatible. A field theoretic Galois theory for difference equations was developed by Franke [25] who investigated its ramifications. The main deficiency of this theory is that one could not associate a Picard-Vessiot-type extension to every difference equation. We take a different approach. Fahim [23], Levelt [36], and van der Put [49] showed that a Galois theory of differential equations could be based on *rings*, in particular, simple differential rings. In the differential case, the rings are integral domains and so have quotient fields which are the Picard-Vessiot extensions. We shall follow this approach and develop a theory based on simple difference rings. These rings will be shown to be reduced but can have zero divisors. Nonetheless they are the natural analogue of Picard-Vessiot extensions.

In Chapter 1, we will develop the basic properties of the Picard-Vessiot theory of difference equations - their existence and unicity, and the existence of a Galois group that is a linear algebraic group. In Chapter 2, we discuss algorithms for determining the Galois group of difference equations of order 1 and difference equations in diagonal form. We also outline the algorithm of Hendriks [26] for determining the Galois group of second order difference equations. Chapter 3 is devoted to giving an algebraic (and constructive) proof of the fact that every connected linear algebraic group is the Galois group of a Picard-Vessiot difference ring over $C(z)$, where C is an arbitrary algebraically closed field of characteristic zero and the difference operator is defined by $\phi(z) = z + 1$. We return to this question in Chapter 8 where we show (using analytic tools) that a necessary and sufficient condition for a linear algebraic group to be the Galois group of a difference equation over $\mathbf{C}(\{z^{-1}\})$, ($\mathbf{C}$ being the complex numbers) is that G/G^0 is cyclic, where G^0 is the connected component of the identity in G. Chapter 4 applies the Galois theory of difference equations to the study of algebraic properties of linear recursive and differentially finite sequences, that is, sequences satisfying difference equations over C and $C(z)$ respectively. Chapter 5 considers difference equations over $\overline{\mathbf{F}}_p(x)$, where $\overline{\mathbf{F}}_p$ is the algebraic closure of the field with p elements. We show that there is a simple classification of difference modules M over this field. Furthermore, we show that the difference Galois group of M is the Zariski closure (over $\overline{\mathbf{F}}_p(x^p - x)$) of the cyclic group generated by the "p-curvature of M". We also compare the characteristic zero and characteristic p theories and show that the natural analogue of the Grothendieck conjecture is false for difference equations. In Chapter 6, we give the classification of difference modules over $\mathcal{P}$, the field of Puiseux series in $t = x^{-1}$, where $\phi(t^{1/m}) = t^{1/m}(1 + t)^{-1/m}$. The results here are similar to the formal local classification of differential modules and form the starting point for the study of analytic properties of difference modules.

We wish to thank Anne Duval for many discussions during the preliminary stages of writing and in particular for her help with the material in Chapters 6 and 7.

Chapter 1

Picard-Vessiot rings

We begin this section with several definitions.

Definition 1.1 *1. A* difference ring *is a commutative ring R, with 1, together with an automorphism $\phi : R \to R$. If, in addition, R is a field, we say that R is a* difference field.

2. The constants *of a difference ring R, denoted by C_R are the elements $c \in R$ satisfying $\phi(c) = c$.*

3. A difference ideal *of a difference ring is an ideal I such that $\phi(a) \in I$ for all $a \in I$. A* simple difference ring *is a difference ring R whose only difference ideals are (0) and R.*

Example 1.2 Let $\mathbf{C}$ be the field of complex numbers. Each of the fields

- $\mathbf{C}(z)$, the field of rational functions in z,
- $\mathbf{C}(\{z^{-1}\})$, the fraction field of convergent power series in z^{-1},
- $\mathbf{C}((z^{-1}))$, the fraction field of formal power series in z^{-1},

are all difference fields with ϕ given by $\phi(z) = z + 1$. For the last two fields this means that ϕ is given by $\phi(t) = \frac{t}{1+t}$ where $t = z^{-1}$. Note that this automorphism extends to

- $\mathcal{P}$, the algebraic closure of $\mathbf{C}((z^{-1}))$, which is also called the field of the formal Puiseux series,

by putting $\phi(t^{\frac{1}{m}}) = t^{\frac{1}{m}}(1 + t)^{-\frac{1}{m}}$. ∎

Example 1.3 Consider the set of sequences $\mathbf{a} = (a_0, a_1, \ldots)$ of elements of an algebraically closed field C. We define an equivalence relation on this set by saying that two sequences $\mathbf{a}, \mathbf{b}$ are equivalent if there exists an N such that $a_n = b_n$ for all $n > N$. Using coordinatewise addition and multiplication, one sees that the set of such equivalence classes forms a ring $\mathcal{S}$. The map $\phi_0((a_0, a_1, a_2, \ldots)) = (a_1, a_2, \ldots)$ is well defined on equivalence classes (one needs to work with equivalence classes to have the property that this map is injective). The ring $\mathcal{S}$ with the automorphism ϕ_0 is therefore a difference ring. To simplify notation we shall identify an element with its equivalence class. The field C may be identified with the subring of constant sequences $(c, c, c, \ldots)$ of $\mathcal{S}$. If the characteristic of C is zero then any element of $C(z)$ is defined for sufficiently large integers (note that in characteristic p, this is not true for $(z^p - 1)^{-1}$). Therefore the map $f \mapsto (f(0), f(1), \ldots)$ defines a difference embedding of $C(z)$ into $\mathcal{S}$. Note that the map the map $f \mapsto (f(0), f(1), \ldots)$ also defines a difference embedding of $\mathbf{C}(\{z^{-1}\})$ into $\mathcal{S}$.

We note that $\mathcal{S}$ is not a simple difference ring. To see this let $\mathbf{a}$ be any sequence whose support (i.e., those integers i such that $a_i \neq 0$) is an infinite set of density zero in the integers (e.g., $\mathbf{a} = (a_i)$ where $a_i = 1$ if i is a power of 2 and 0 otherwise). The ideal generated by $\mathbf{a}, \phi_0(\mathbf{a}), \phi_0^2(\mathbf{a}), \ldots$ is a nontrivial difference ideal in $\mathcal{S}$. ∎

Let R be a difference ring. For $A \in Mat_n(R)$

$$\phi Y = AY$$

denotes a first order linear difference system. We shall restrict ourselves to equations where $A \in Gl_n(R)$ (to guarantee that we get n independent solutions). Here Y denotes a column vector $(y_1, \ldots, y_n)^T$ and $\phi Y = (\phi y_1, \ldots, \phi y_n)^T$. Given an n^{th} order difference equation $L(y) = \phi^n y + \ldots + a_1 \phi Y + a_0 Y = 0$ we can consider the equivalent system

$$\begin{pmatrix} \phi y \\ \phi^2 y \\ \vdots \\ \phi^n y \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -a_0 & -a_1 & \ldots & -a_{n-2} & -a_{n-1} \end{pmatrix} \begin{pmatrix} y \\ \phi^1 y \\ \vdots \\ \phi^{n-1} y \end{pmatrix}$$

For this system, the condition that the matrix lies in Gl_n is that $a_0 \neq 0$.

Definition 1.4 *Let R be a difference ring and $A \in Gl_n(R)$. A* fundamental matrix with entries in R *for $\phi Y = AY$ is a matrix $U \in Gl_n(R)$ such that $\phi U = AU$. If U and V are fundamental matrices for $\phi Y = AY$, then $V = UM$ for some $M \in Gl_n(C_R)$ since $U^{-1}V$ is left fixed by ϕ.*

Definition 1.5 *Let k be a difference field and $\phi Y = AY$ a first order system $A \in Gl_n(k)$. We call a $k-$algebra R a* Picard-Vessiot ring *for $\phi Y = AY$ if:*

1. *An automorphism of R, also denoted by ϕ, which extends ϕ on k is given.*

此为试读，需要完整PDF请访问：www.ertongbook.com

2. *R is a simple difference ring.*

3. *There exists a fundamental matrix for $\phi Y = AY$ with coefficients in R.*

4. *R is minimal in the sense that no proper subalgebra of R satisfies the conditions 1,2 and 3.*

We will show in the next section that if C_k is algebraically closed then, for any system $\phi Y = AY$, there is a Picard-Vessiot ring for this system and that it is unique up to $k-$difference isomorphism.

Example 1.6 Let C be an algebraically closed field of characteristic not equal to 2. R be the difference subring of $\mathcal{S}$ generated by C and $\mathbf{j} = (1, -1, 1, -1, \ldots)$. Note that $R = C[(1, -1, 1, -1, \ldots)]$. The 1×1 matrix whose only entry is $(1, -1, 1, -1, \ldots)$ is the fundamental matrix of the equation $\phi_0 y = -y$. This ring is isomorphic to $\mathbf{C}[X]/(X^2 - 1)$ whose only non-trivial ideals are generated by the cosets of $X - 1$ and $X + 1$. Since the ideals generated in R by $\mathbf{j} + 1$ and $\mathbf{j} - 1$ are not difference ideals, R is a simple difference ring. Therefore R is a Picard-Vessiot extension of C. Note that R is reduced but not integral. ∎

In the following sections we will make use of the next elementary lemma.

Lemma 1.7 *a) The set of constants in a simple difference ring forms a field.*
b) If I is a maximal difference ideal of a difference ring R, then I is a radical ideal and for any $r \in R$, $\phi(r) \in I$ if and only if $r \in I$. Therefore R/I is a reduced difference ring.

Proof: a) If c is a constant, then $c \cdot R$ is a nonzero difference ideal so there is a $d \in R$ such that $c \cdot d = 1$. A computation shows that d is a constant.

b) To prove the first claim, one can easily show that the radical of a difference ideal is a difference ideal. To prove the second claim, note that $\{r \in R \mid \phi(r) \in I\}$ is a difference ideal that contains I but does not contain 1. ∎

The remainder of this section is organized as follows. In section 1.1 we show the existence and uniqueness of Picard-Vessiot rings assuming that the field of constants of k is algebraically closed. In section 1.2, we shall show that the group G of $k-$difference automorphisms of a Picard-Vessiot ring R that is a separable extension of k has the structure of an algebraic group over C_k and that R is the coordinate ring of variety which is a principal homogeneous space for G. In section 1.3 we consider the total quotient ring of a Picard-Vessiot ring and establish a Galois correspondence between certain difference subrings and closed subgroups of the Galois group. Finally in section 1.4, we consider the Tannakian category approach to defining the Galois group [20] and we will discuss the relation of our approach to this approach.

1.1 Existence and uniqueness of Picard-Vessiot rings

Let k be a difference field and let

$$\phi(Y) = AY \tag{1.1}$$

be a difference system with $A \in Gl(d)(k)$. To form a Picard-Vessiot ring for (1.1) we proceed as follows. Let (X_{ij}) denote a matrix of indeterminates over k and let det denote the determinant of this matrix. On the $k-$algebra $k[X_{ij}, \frac{1}{det}]$ one extends the automorphism ϕ be setting $(\phi X_{ij}) = A(X_{ij})$. If I is a maximal difference ideal of $k[X_{ij}, \frac{1}{det}]$ then Lemma 1.7 implies that $k[X_{ij}, \frac{1}{det}]/I$ is a simple difference ring. From the definition we see that $k[X_{ij}, \frac{1}{det}]/I$ is a Picard-Vessiot ring for (1.1) and any Picard-Vessiot ring will be of this form. To prove uniqueness of Picard-Vessiot rings, we need the following result. In this result we restrict ourselves to difference fields with algebraically closed fields of constants. This restriction excludes difference fields (k, ϕ) with ϕ of finite order. In particular, $(\overline{\mathbf{F}}_p(z), \phi(z) = z + 1)$ is excluded.

Lemma 1.8 *Let R be a finitely generated k-algebra having an automorphism, also called ϕ, extending ϕ on k. Let C be the constants of k and assume that C is algebraically closed and that R is a simple difference ring. Then the set of constants of R is C.*

Proof: Suppose that $b \notin C$ and $\phi(b) = b$. Consider the subring $C[b]$ of R. Since R is simple every nonzero element f of this subring has the property that $Rf = R$, i.e., there is an element $g \in R$ such that $fg = 1$. Since C is algebraically closed it follows that $C[b]$ is a polynomial ring over C. Let $\overline{k}$ denote the algebraic closure of k. One sees that any nonzero element $f \in C[b]$ defines a regular, nowhere zero map of the affine variety $spec(\overline{k} \otimes_k R)$ to $\overline{k}$ whose image is therefore a constructible subset of $\overline{k}$. Consider the map defined by the element b. If $c \in C$ is in the image of this map then the map defined by $b - c \in C[b]$ has a zero. Therefore the image of the map b has empty intersection with C. It follows that the image of this map is finite and so there is a polynomial $P = X^d + a_{d-1}X^{d-1} + ... + a_0 \in k[X]$ such that $k[b] = k[X]/(P)$. Since $\phi(b) = b$, one finds that b also satisfies the polynomial $X^d + \phi(a_{d-1})X^{d-1} + ... + \phi(a_0)$. The uniqueness of P implies that P lies in $C[X]$. This contradicts the fact that $C[b]$ is a polynomial ring over C. ▮

Proposition 1.9 *Let k be a difference field with algebraically closed field of constants and let R_1 and R_2 be Picard-Vessiot extensions of k for $\phi(Y) = AY$. Then there exists a $k-$difference isomorphism between R_1 and R_2.*

Proof: We consider $R_1 \otimes_k R_2$ a difference ring where $\phi(r_1 \otimes r_2) = \phi(r_1) \otimes \phi(r_2)$. Choose an ideal I in $R_1 \otimes_k R_2$ which is maximal in the collection of ϕ-invariant ideals and put $R_3 = R_1 \otimes_k R_2/I$. The canonical maps $R_1 \to R_3$ and $R_2 \to R_3$ are injective since the kernels are ϕ-invariant ideals. The image of the first map is generated over k by a fundamental matrix in R_3 and similarly for the second map. Two fundamental matrices differ by a matrix with coefficients in C_{R_3}, which according to Lemma 1.8 is C_k. It follows that the two images are the same. Hence R_1 is isomorphic to R_2. ∎

1.2 The Galois group

As an aid in understanding the structure of Picard-Vessiot rings, we will introduce a geometric point of view. As noted above, any Picard-Vessiot extension for (1.1) is of the form $k[X_{ij}, \frac{1}{det}]/I$ where I is a maximal $\phi-$invariant ideal of $k[X_{ij}, \frac{1}{det}]$. Lemma 1.7 implies that such an ideal is a radical ideal and so is the ideal of a reduced algebraic subset of $Gl(d)_k = spec(k[X_{ij}, \frac{1}{det}])$. Let $\overline{k}$ denote the algebraic closure of k. The automorphism ϕ extends to an automorphism of $\overline{k}$ which will also be denoted by ϕ. The automorphism ϕ of $D := \overline{k}[X_{ij}, \frac{1}{det}]$, extending ϕ on $\overline{k}$, is given (in matrix notation) by $(\phi X_{ij}) = A(X_{ij})$. For every maximal ideal M of D, $\phi(M)$ is also a maximal ideal. The maximal ideal M has the form $(X_{11} - b_{11}, X_{12} - b_{12}, \ldots, X_{dd} - b_{dd})$ and corresponds to the matrix $B = (b_{ij}) \in Gl(d)(\overline{k})$. A small calculation shows that the maximal ideal $\phi(M)$ corresponds to the matrix $A^{-1}\phi(B)$. The expression $\phi(B)$ for a matrix $B = (b_{ij})$ is defined as before as $(\phi(b_{ij}))$. Thus ϕ on D induces the map τ on $Gl(d)(\overline{k})$, given by the formula $\tau(B) = A^{-1}\phi(B)$. The elements $f \in D$ are seen as functions on $Gl(d)(\overline{k})$. The following formula holds

$$(\phi f)(\tau(B)) = \phi(f(B)) \text{ for } f \in D \text{ and } B \in Gl(d)(\overline{k}).$$

Indeed, one can easily verify the formula for $f \in \overline{k}$ and for the $f = X_{ij}$. This proves the formula for any $f \in D$.

For an ideal $J \subset k[X_{ij}, \frac{1}{det}]$ satisfying $\phi(J) \subset J$, one has $\phi(J) = J$. Indeed, if $\phi(J)$ is a proper subset of J then one finds an infinite chain of ideals $J \subset \phi^{-1}(J) \subset \phi^{-2}(J) \subset \ldots$ This contradicts the Noetherian property of $k[X_{ij}, \frac{1}{det}]$. Likewise for reduced algebraic subsets Z of $Gl(d)_k$ the condition $\tau(Z) \subset Z$ implies $\tau(Z) = Z$. The following lemma is an immediate consequence of the remarks above and the formula.

Lemma 1.10 *The ideal J of a reduced subset Z of $Gl(d)_k$ satisfies $\phi(J) = J$ if and only if $Z(\overline{k})$ satisfies $\tau Z(\overline{k}) = Z(\overline{k})$*

An ideal I maximal among the ϕ-invariant ideals corresponds then to a minimal (reduced) algebraic subset Z of $Gl(d)_k$ such that $\tau(Z(\overline{k})) = Z(\overline{k})$. We shall call such a set *a minimal $\tau-$invariant reduced set.*

Let Z be a minimal τ-invariant reduced subset of $Gl(d)_k$ with ideal $I \subset k[X_{i,j}, \frac{1}{det}]$ and let $O(Z) = k[X_{i,j}, \frac{1}{det}]/I$. Let $x_{i,j}$ denote the image of $X_{i,j}$ in $O(Z)$. One considers the rings

$$k[X_{i,j}, \frac{1}{det}] \subset O(Z) \otimes_k k[X_{i,j}, \frac{1}{det(X_{i,j})}] =$$

$$O(Z) \otimes_C C[Y_{i,j}, \frac{1}{det(Y_{i,j})}] \supset C[Y_{i,j}, \frac{1}{det(Y_{i,j})}] \qquad (1.2)$$

where the variables $Y_{i,j}$ are defined by $(X_{i,j}) = (x_{i,j})(Y_{i,j})$. Note that the action of ϕ on $C[Y_{i,j}, \frac{1}{det(Y_{i,j})}] \subset O(Z) \otimes_k k[X_{i,j}, \frac{1}{det(X_{i,j})}]$ is the identity. Let (I) be the ideal of $O(Z) \otimes_k k[X_{i,j}, \frac{1}{det}]$ generated by I and let J be the intersection of (I) with $C[Y_{i,j}, \frac{1}{det}]$. The ideal (I) is ϕ-invariant. Using that the set of constants of $O(Z)$ is C one can prove that J generates the ideal (I) in $O(Z) \otimes_k k[X_{i,j}, \frac{1}{det}]$. The proof follows from the next lemma.

Lemma 1.11 *Let R be a Picard-Vessiot ring over a field k and let A be a commutative algebra with unit over C_k. The action of ϕ on A is supposed to be the identity. Let N be an ideal of $R \otimes_C A$ which is invariant under ϕ. Then N is generated by the ideal $N \cap A$ of A.*

Proof: Dividing A by $N \cap A$ and $R \otimes_C A$ by the ideal generated by $N \cap A$, one reduces the lemma to proving that $N \neq 0$ implies that $N \cap A \neq 0$. Let $\{a_i\}_{i \in \mathcal{I}}$ be a basis of A over C. Consider a minimal subset $\mathcal{J}$ of $\mathcal{I}$ such that $N \cap \sum_{i \in \mathcal{J}} R \otimes a_i \neq 0$. Fix some $j \in \mathcal{J}$, then the set of the $b \in R$ such that there exists an element in $N \cap \sum_{i \in \mathcal{J}} R \otimes a_i$ with coordinate b at the place j, is a nonzero ideal of R which is invariant under ϕ. Hence there exists an element $f \in N \cap \sum_{i \in \mathcal{J}} R \otimes a_i$ with coordinate 1 at the place j. If $\mathcal{J}$ has only one element then $a_j \in N \cap A$. If $\mathcal{J}$ has more than one element, then $\phi(f) - f$ has a smaller support than $\mathcal{J}$. Hence $\phi(f) - f = 0$. It follows that all the coordinates of f are in the field of constants C of R. Hence $f \in N \cap A$. ∎

In particular, the above lemma shows that when we divide the rings in the sequence (1.2) by the ideals $I, (I)$, and J, we have

$$O(Z) \to O(Z) \otimes_k O(Z) = \qquad (1.3)$$

$$= O(Z) \otimes_C (C[Y_{i,j}, \frac{1}{det(Y_{i,j})}]/J) \leftarrow C[Y_{i,j}, \frac{1}{det(Y_{i,j})}]/J$$

We now assume that the ring $O(Z)$ is a *separable extension* of k ([15], §7, n^o. 5). In this case Corollaire 3 of ([15], §7, n^o. 5) and Corollaire 3 of ([15], §7, n^o. 6) imply that $O(Z) \otimes_k O(Z)$ is reduced. Therefore,

$C[Y_{i,j}, \frac{1}{det(Y_{i,j})}]/J$ is reduced and so J is a radical ideal. Note that our assumption on $O(Z)$ is always true if the characteristic of k is zero or more generally, if k is perfect. We will now show that J is the ideal of an algebraic subgroup of $Gl(d)(C)$.

Consider a matrix $A \in Gl(d)(C)$. Let σ_A denote the action on the three rings in the sequence (1.2) given by $(\sigma_A X_{i,j}) = (X_{i,j})A$ and $(\sigma_A Y_{i,j}) = (Y_{i,j})A$. Using Lemma 1.11 and the facts that I is maximal and Z is minimal, one can easily show that following conditions on A are equivalent:

1. $ZA = Z$.
2. $ZA \cap Z \neq \emptyset$.
3. $\sigma_A I = I$.
4. $I + \sigma I$ is not the unit ideal of $k[X_{i,j}, \frac{1}{det}]$.
5. $\sigma_A(I) = (I)$.
6. $(I) + \sigma_A(I)$ is not the unit ideal of $O(Z) \otimes_k k[X_{i,j}, \frac{1}{det}]$.
7. $\sigma_A J = J$.
8. $J + \sigma_A J$ is not the unit ideal of $C[Y_{i,j}, \frac{1}{det}]$.

The collection of the A satisfying the equivalent conditions form a group.

Lemma 1.12 *Let $O(Z)$ be a separable extension of k. Using the above notation, A satisfies the equivalent conditions if and only if A lies in the reduced subspace V of $Gl(d)_C$ defined by J. Therefore, the set of such A is an algebraic group.*

Proof: Assume that A satisfies the conditions. Condition 3. implies that A defines a difference automorphism on $O(Z)$. We again refer to this automorphism as σ_A. This in turn allows us to define a difference homomorphism $id \otimes \sigma_A : O(Z) \otimes_k O(Z) \to O(Z)$ given by $a \otimes b \mapsto a\sigma_A(b)$. Restricting this map to $C[Y_{i,j}, \frac{1}{det}]/J \subset O(Z) \otimes_k O(Z)$ we get a difference map from $C[Y_{i,j}, \frac{1}{det}]/J$ to $O(Z)$. Since the difference operator is the identity on $C[Y_{i,j}, \frac{1}{det}]/J$, the image of this map must lie in the constants of $O(Z)$, that is, in C. Therefore A corresponds to a map in $HOM_C(C[Y_{i,j}, \frac{1}{det}]/J, C)$ and so A is a point of V.

Conversely, let A lie in V. Then A yields a difference homomorphism from $O(V) \otimes_C C[Y_{i,j}, \frac{1}{det}]/J$ to $O(V)$ given by $a \otimes b \mapsto a \cdot b(A)$. If we restrict this map to $O(Z) = 1 \otimes O(Z) \subset O(Z) \otimes_k O(Z) = O(V) \otimes_C C[Y_{i,j}, \frac{1}{det}]/J$, we have a difference homomorphism from $O(Z)$ to $O(Z)$. One then sees that this yields $\sigma_A I = I$. ∎

Let G denote the group of the automorphisms of $O(Z)$ over k which commute with the action of ϕ. The group G is called the *(difference) Galois group* of the equation $\phi(Y) = AY$ over the field k. Each element σ of G must have the form $(\sigma x_{i,j}) = (x_{i,j})A$ where $A \in Gl(d)(C)$ is such that σ_A (as defined above) satisfies $\sigma_A I = I$. It follows that G coincides the points of the algebraic group V. In the sequel we will identify G and V and denote by $O(G)$ the ring $C[Y_{i,j}, \frac{1}{det}]/J$. Let $O(G_k) = O(G) \otimes_C k$ and $G_k = spec(O(G_k))$. From the sequence of rings (1.3), we have

$$O(Z) \to O(Z) \otimes_k O(Z) = O(Z) \otimes_C O(G) = O(Z) \otimes_k O(G_k) \tag{1.4}$$

The first embedding of rings corresponds to the morphism $Z \times G_k \to Z$ given by $(z, g) \mapsto zg$. The identification $O(Z) \otimes_k O(Z) = O(Z) \otimes_C O(G) = O(Z) \otimes_k O(G_k)$ corresponds to the fact that the morphism $Z \times G_k \to Z \times Z$ given by $(z, g) \mapsto (zg, z)$ is an isomorphism. In other words, Z is a $k-$homogeneous space for G_k or in the language of [20], Z/k is a G-torsor. The following theorem summarizes the above.

Theorem 1.13 *Let R be a separable Picard-Vessiot ring over k, a difference field with algebraically closed subfield of constants, and let G denote the group of the k-algebra automorphisms of R which commute with ϕ. Then G has a natural structure as reduced linear algebraic group over C and the affine scheme $Z = spec(B)$ over k has the structure of a G-torsor over k.*

Example 1.14 In the course of the proof of the above result, the assumption that R was separable over k was used to prove that the group G was a *reduced* space. We give here an example in characteristic p where this is not the case. Let k_0 be an algebraically closed field of characteristic $p > 0$ such that there is an $\alpha \in k_0^*$ which is not of finite order. Let $k = k_0((z))$ with automorphism ϕ given by $\phi(z) = \alpha z$ (and so $\phi(\sum a_n z^n) = \sum a_n \alpha^n z^n$). Let $\beta \in k_0$ satisfy $\beta^p = \alpha$. Consider the 1-dimensional difference equation $\phi(X) = \beta X$. A calculation shows that $L = k[X]/(X^p - z)$ is the Picard-Vessiot ring for the equation. It is in fact an inseparable extension of k and so $L \otimes_k L$ has nilpotents. Following the above development further, one finds that the difference Galois group for the equation above is the group μ_p in characteristic p. This group is given as $spec(k_0[t]/(t^p - 1))$ and the group structure is given by $t \mapsto t \otimes t$. ∎

The fact that a Picard-Vessiot ring is the coordinate ring of a torsor for its Galois group has several interesting consequences, which we now state.

Corollary 1.15 *Let R be a separable Picard-Vessiot ring over k, a difference field with algebraically closed subfield of constants, and let G denote the group of the k-algebra automorphisms of R which commute with ϕ. The set of $G-$invariant elements of R is k and R has no proper, nontrivial $G-$invariant ideals.*

Proof: Let $R = O(Z)$ for some $G-$torsor Z and let $\overline{k}$ be the algebraic closure of k. Any $G-$invariant element of R defines a regular function on $Z(\overline{k})$. Since

此为试读，需要完整PDF请访问：www.ertongbook.com