Algebraic and Algorithmic Aspects of Linear Difference Equations

Michael F. Singer*

Abstract

These are an extended version of lecture notes from a series of talks given at the CIMPA Research School *Galois Theory of Difference Equations* held in Santa Marta, Columbia, July 23-August 1, 2012.In this course, I gave an elementary introduction to the Galois theory of linear difference equations from an algebraic and algorithmic perspective. This theory shows how to associate a group of matrices with a linear difference equation and shows how group theory can be used to determine properties of the solutions of the equations.

These notes begin by giving an introduction to the theory of linear algebraic groups, those groups that occur as Galois groups. I then present the basic features of the Galois theory and show how this theory can be used to determine algebraic properties of sequences of numbers determined by linear recurrences. In particular I show how the Galois theory leads to algorithms to determine algebraic relations among such solutions (such as the relation $F(n)F(n+2)-F(n+1)^2=(-1)^n$ among the Fibonacci numbers $F(n)$) and algorithms to express such solutions in "finite terms".

The goal of my course and of these notes is to give an overview of algebraic and algorithmic results in the Galois theory of linear difference equations, give a taste of the various ingredients that are used to build this theory and describe some of the applications. Therefore I focus on explaining definitions and statements of results rather than giving complete proofs. I will assume that the reader has a basic knowledge of abstract algebra (groups, rings, fields, ideals, ...). I hope that these notes give enough knowledge and evoke enough interest that you will go to the sources mentioned and delve further into the subject.

*North Carolina State University, Department of Mathematics, Box 8205, Raleigh, North Carolina 27695-8205, USA, singer@math.ncsu.edu. The author was partially supported by NSF Grant CCF-1017217.

Contents

1 Introduction

The goal of these lectures is to develop theory and algorithms that will allow us to understand the algebraic behavior of sequences defined by linear recurrences. Examples of the issues we will address are:

1. (cf. Example 6.3) The Fibonacci numbers $F(n)$ are defined by

$$F(n+2) - F(n+1) - F(n) = 0, \quad F(0) = 0, F(1) = 1.$$

   This sequence satisfies

$$F(n)F(n+2) - F(n+1)^2 = (-1)^n.$$

   In Section 6.1, I will describe a method to discover such identities.

2. (cf. Example 6.11) Solutions of the equation

$$y(n+2) - (2n+5)y(n+1) + (2n+2)y(n) = 0$$

   have a nice "closed form"

$$y(n) = c_1 2^n n! + c_2 2^n n! \sum_{m=0}^{n} \frac{1}{2^m m!}.$$

   In Section 6.2, I will give a formal definition of a notion of closed form solution and discuss an algorithm to find such solutions.

3. (cf. Proposition 4.22) Let $\{u(n)\}$ be a sequence of numbers satisfying, for large enough n, both a recurrence relation

$$a_t(n)u(n+t) + a_{t-1}(n)u(n+t-1) + \ldots + a_0(n)u(n) = 0$$

   and an algebraic equation

$$b_s(n)u(n)^s + b_{s-1}(n)u(n)^{s-1} + \ldots + b_0(n) = 0,$$

   where the $a_i(n)$ and $b_i(n)$ are polynomials in n. In Section 4.3, I will discuss why such a sequence must be of the form

$$u(n) = \begin{cases} f_0(n) & \text{if } n \equiv 0 \pmod{r} \\ f_1(n) & \text{if } n \equiv 1 \pmod{r} \\ \vdots & \vdots \\ f_{r-1}(n) & \text{if } n \equiv r-1 \pmod{r}, \end{cases}$$

   for large enough n, where r is a positive integer and the $f_i(n)$ are rational functions of n.

These results can be derived using a Galois theory of such recurrences. The usual Galois theory of algebraic equations associates to a polynomial equation $p(x) = 0$ a finite group. Properties of the equation and its solutions are reflected in properties of the group and one can use group theory to understand these properties and develop algorithms to determine them as well. We will develop a Galois theory of linear recurrences (or more generally, of what we will call difference equations). This will associate to any difference equation a group of matrices. The group will furthermore be a *linear algebraic group*, that is a group of matrices whose entries satisfy some fixed set of polynomial equations. An example of this is the group of matrices whose determinant is 1. Properties of the difference equation and its solutions will be mirrored in properties of the group and, in analogy with the case of polynomial equations, the theory of linear algebraic groups will give us the tools to understand and develop algorithms to determine these properties.

Linear algebraic groups are examples of algebraic varieties and I will start by giving an introduction to the theory of algebraic varieties in Section 2. In Section 3, I develop a little of the theory of linear algebraic groups. In Section 4, I will discuss the notion of a Picard-Vessiot extension which is the analogue of a splitting field in the usual Galois theory. In Section 5, I will finally develop the Galois theory of linear difference equations and in Section 6, I will discuss the problem of calculating the Galois groups and determining their properties and related properties of the linear difference equations.

Proofs of several of the results are left as exercises or, when these proofs involve concepts not introduced in the notes or are a little too long to include in these notes, references are given. Despite the fact that some of the results hold in positive characteristic, throughout these notes **all fields are assumed to be of characteristic 0**. The symbols $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$ will denote the nonnegative integers, all integers, the rational numbers and the complex numbers.

2 Algebraic Varieties

Let k be a field and $\bar{k}$ some fixed algebraically closed field containing k. For example, we could have $k = \mathbb{Q}$ and $\bar{k} = \mathbb{C}$ or $k = \mathbb{Q}$ and $\bar{k} = \bar{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. If R is a ring, we denote by $R[X_1, \ldots, X_m]$ the ring of polynomials with coefficients in R. In this section, we will give a brief and rapid introduction to the concepts of algebraic geometry that we will need in the succeeding sections. If this topic interests you, more information can be found in [5, 11, 18].

2.1 Varieties and Ideals

Definition 2.1 *A subset $V \subset \bar{k}^m$ is a* **k-variety** *if there exists a set of polynomials $\{f_i\}_{i\in\mathcal{I}} \subset k[X_1, \ldots, X_m]$ such that $V = \{v \in \bar{k}^m \mid f_i(v) = 0 \text{ for all } f_i,\ i \in \mathcal{I}\}$. We denote this by $V = V(\{f_i\}_{i\in\mathcal{I}})$.*

Example 2.2 *Let $k = \mathbb{Q}, \bar{k} = \bar{\mathbb{Q}}, m = 1$. The set $V = \{\pm\sqrt{2}\} = \{v \in \bar{k} \mid v^2 - 2 = 0\}$ is a k-variety. Note that $\{\sqrt{2}\}$ is not a k-variety since any polynomial in $\mathbb{Q}[X]$ that vanishes at $\sqrt{2}$ also vanishes at $-\sqrt{2}$. The set $\{\sqrt{2}\}$ is a $\bar{k}$-variety.*

We need to note that the above definition of a **k-variety** is not intrinsic but depends on a choice of $\bar{k}$-basis of $\bar{k}^m$. A more intrinsic definition is given, for example, in ([35], Sec. 1.3.7). When one changes bases, one can get a new k-variety that is not isomorphic to the original one (see Example 2.21). We shall be careful to keep track of this subtlety.

Definition 2.3 *Let V be a k-variety defined by $\{f_i\}_{i\in\mathcal{I}} \subset k[X_1, \ldots, X_m]$ and E a field with $k \subset E$. We define $V(E) = \{v \in E^m \mid f_i(v) = 0$ for all $i \in \mathcal{I}\}$.*

Note that we always have $V(\bar{k}) = V$. In the previous example, $V(\mathbb{Q}) = \emptyset$ while $V(\overline{\mathbb{Q}}) = \{\pm\sqrt{2}\}$.

Example 2.4 *The k-varieties of $\bar{k}$. These are: the empty set $\emptyset$ (the zero set of the polynomial 1), all of $\bar{k}$ (the zero set of the polynomial 0), and roots in $\bar{k}$ of polynomials defined over k. Therefore aside from $\bar{k}$ itself, the k-varieties are finite sets. The previous example shows that not all finite sets are k-varieties unless k is itself algebraically closed.*

Lemma 2.5 *(i) If $\{V_j\}_{j\in\mathcal{J}}$ is a family of k-varieties, then $\cap_{j\in\mathcal{J}} V_j$ is a k-variety*
(ii) If V and W are k-varieties, then $V \cup W$ is a k-variety.

Lemma 2.5 (whose proof is left as an exercise) implies that the k-varieties form the set of closed sets of a topology. This topology is called the **Zariski k-topology**. We will frequently refer to k-varieties as k-closed sets to underline the topological nature of this concept.

Let V be a k-closed set defined by $\{f_i\}_{i\in\mathcal{I}} \subset k[X_1, \ldots, X_m]$ and let $I = \langle\{f_i\}_{i\in\mathcal{I}}\rangle \subset k[X_1, \ldots, X_m]$ be the ideal generated by this set. Clearly, $V = \{v \in \bar{k}^m \mid g(v) = 0$ for all $g \in I\}$. Therefore we can assume that k-closed sets are defined by ideals in $k[X_1, \ldots, X_m]$, that is $V = V(I)$ where I is an ideal in $k[X_1, \ldots, X_m]$.

Definition 2.6 *Let $Z \subset \bar{k}^m$. We define*

$$\mathbf{I_k(Z)} = \{f \in k[X_1, \ldots, X_m] \mid f(v) = 0 \text{ for all } v \in Z\}.$$

Note that $I_k(Z)$ is an ideal and that if $Z_1 \subset Z_2$ then $I_k(Z_2) \subset I_k(Z_1)$. $I_k(Z)$ has an additional property.

Definition 2.7 *(i) An ideal I is* **radical** *if $f^t \in I$ for some positive integer t implies that $f \in I$.*
(ii) If I is an ideal, the **radical $\sqrt{\mathbf{I}}$** *of I is*

$$\sqrt{I} = \{f \mid f^t \in I \text{ for some positive integer } t\}.$$

Example 2.8 *The ideal $I = \langle (x-1)(x-2) \rangle \subset \mathbb{Q}[X]$ is a radical ideal but $\langle (x-1)^2 \rangle$ is not radical. The radical of $\langle (x-1)^2 \rangle$ is $\langle x-1 \rangle$.*

Lemma 2.9 *(i) For $Z \subset \bar{k}^m$, $I_k(Z)$ is a radical ideal.*
(ii) If I is an ideal then $\sqrt{I}$ is also an ideal.
(iii) If I is a radical ideal, then $\sqrt{I} = I$.

Proof. (i) Easy. (ii) The only thing to prove that is not totally obvious is: $f, g \in \sqrt{I} \Rightarrow f + g \in \sqrt{I}$. Assume $f^s \in I$, $g^t \in I$. We then have

$$(f+g)^{s+t-1} = \sum_{i=0}^{s+t-1} \binom{s+t-1}{i} f^i g^{s+t-1-i}.$$

Note than in any product $f^i g^{s+t-1-i}$ either the exponent of f is at least s or the exponent of g is at least t. Therefore each product lies in I and so $(f+g)^{s+t-1}$ is in I. (iii) Clear. ∎

We can now give a correspondence between k-varieties in $\bar{k}^m$ and radical ideals in $k[X_1, \ldots, X_m]$:

$$\begin{array}{rcl} k\text{-varieties } V & \Leftrightarrow & \text{Radical Ideals in } k[X_1, \ldots, X_m] \\ V & \Rightarrow & I_k(V) \\ V(I) & \Leftarrow & I \end{array}$$

It is not hard to show that $V(I_k(V)) = V$ for any k-variety V (this is an exercise!) The relation between an ideal I and $I_k(V(I))$ is given by

Theorem 2.10 *(Hilbert Nullstellensatz; Chapter I.3 [18]) If I is an ideal of $k[X_1, \ldots, X_m]$ then*

$$I_k(V(I)) = \sqrt{I}.$$

Therefore we have a bijection between k-varieties and radical ideals. We will need some more concepts and facts concerning the Zariski k-topology.

2.2 Irreducible Varieties

Definition 2.11 *A k-variety V is* **k-reducible** *if $V = V_1 \cup V_2$ where V_1, V_2 are k-varieties and $V \not\subset V_1, V \not\subset V_2$. If V is not k-reducible then it is* **k-irreducible**.

Example 2.12 *Let $k = \mathbb{Q}$. $V = \{1, 0\}$ is k-reducible but $W = \{\pm\sqrt{2}\}$ is k-irreducible.*

Lemma 2.13 *V is k-irreducible if and only if $I_k(V)$ is a prime ideal.*

Proof. Assume V is k-irreducible and let $fg \in I_k(V)$. Let $V_1 = V(\{f\} \cup I_k(V))$ and $V_2 = V(\{g\} \cup I_k(V))$. We have $V \subset V_1 \cup V_2$ so V must be a subset of one of these. Say $V \subset V_1$ and so $V = V_1$. Therefore f vanishes on V and so $f \in I_k(V)$.

Now assume V is k-reducible, so $V = V_1 \cup V_2$ where V_1, V_2 are k-varieties and $V \not\subset V_1, V \not\subset V_2$. We then have that $I_k(V) \subsetneq I_k(V_1)$ and $I_k(V) \subsetneq I_k(V_2)$. Let $p_1 \in I_k(V_1) \backslash I_k(V)$ and $p_2 \in I_k(V_2) \backslash I_k(V)$. We then have $p_1 p_2 \in I_k(V)$ so $I_k(V)$ is not prime. ∎

Theorem 2.14 *(Hilbert Basis Theorem) Any ideal I in $k[X_1, \ldots, X_m]$ is finitely generated, that is, there exist $f_1, \ldots, f_t \in k[X_1, \ldots, X_m]$ such that $I = \langle f_1, \ldots, f_t \rangle$.*

Proof. I reproduce the very short proof, due to Sarges [32], that is given in (Proposition 2.3, [18]). I will show that if R is a commutative ring and if there exists an ideal of $R[X]$ that is not finitely generated then there is an ideal of R that is not finitely generated. Using induction, this fact will yield a proof of the Theorem. Let I be an ideal of $R[X]$ that is not finitely generated and let f_1 be a nonzero element of I of least degree. Since I is not finitely generated we can produce an infinite sequence of distinct polynomials $f_i \in R[X]$ where each f is a element of least degree in $I \backslash \langle f_1, \ldots, f_{i-1} \rangle$. Let n_i be the degree of f_i and a_i be the leading coefficient of f_i. We have $n_1 \leq n_2 \leq \ldots$. I claim that the ideal $(a_1, \ldots, a_n, \ldots)$ is not finitely generated. If it were, then for some s we would have $(a_1, \ldots, a_s) = (a_1, \ldots, a_s, a_{s+1}) = \ldots$. We would then have that $a_{s+1} = \sum_{i=1}^{s} b_i a_i$ for some $b_i \in R$. Let $g := f_{s+1} - \sum_{i=1}^{s} b_i X^{n_{s+1} - n_i} f_i$. The element g has lower degree than f_{s+1} and lies in $I \backslash (f_1, \ldots, f_s)$, contradicting the choice of f_{s+1}. ∎

Corollary 2.15 *(i) Let $I_1 \subset I_2 \subset \ldots \subset I_r \subset \ldots$ be an ascending chain of ideals of $k[X_1, \ldots, X_m]$. Then there exists an s such that $I_s = I_{s+1} = \ldots$.*
(ii) If $V_1 \supset V_2 \supset \ldots \supset V_t \supset \ldots$ is a decreasing sequence of k-closed sets, then there exists an s such that $V_s = V_{s+1} = \ldots$.
(iii) Any nonempty collection $\{V_i\}_{i \in \mathcal{I}}$ of k-closed sets has an element V_t minimal with respect to containment.

Proof. (i) Let $J = \cup_{i \in \mathcal{I}} I_i$. It is easy to see that J is an ideal so, by Theorem 2.14, $J = \langle f_1, \ldots, f_r \rangle$. There exists an s such that $f_1, \ldots, f_r \in I_s$. Therefore $J \subset I_s$, Since $I_s \subset I_{s+1} \subset \ldots \subset J \subset I_s$ we have $I_s = I_{s+1} = \ldots$.
The proofs of (ii) and (iii) are left as an exercise. ∎

Corollary 2.16 *Any k-closed set V is uniquely expressible as the union of k-irreducible closed sets $\{V_1, \ldots, V_n\}$ such that $V_i \not\subset V_j$ if $i \neq j$.*

Proof. Let

$\mathcal{S} = \{V \mid V$ is k-closed and cannot be expressed as a finite union of k-irreducible closed sets$\}$.

If $\mathcal{S} \neq \emptyset$, Corollary 2.15(iii) implies that $\mathcal{S}$ has a minimal element W, which must be k-reducible. Therefore $W = W_1 \cup W_2$ where W_1, W_2 are k-closed. We must have $W_1 \subsetneq W, W_2 \subsetneq W$ so $W_1, W_2 \notin \mathcal{S}$. Therefore, $W_1 = \cup W_{1,i}, W_2 = \cup W_{2,i}$ with $W_{i,j}$ k-closed and k-irreducible. This leads to $W = (\cup W_{1,i}) \cup (\cup W_{2,i})$, a contradiction.

We now write any $V = \cup_{i=1}^{r} V_i$ with the V_i k-closed and k-irreducible. If one throws away any V_i properly containing any other, we arrive at the sets claimed to exist in the Corollary. To prove uniqueness, let $V = \cup_{i=1}^{s} V_i = \cup_{j=1}^{t} W_j$. For each $i, V_i \subset \cup_{j=1}^{t} W_j$ so there exists a j such that $V_i \subset W_j$. Similarly for each W_j there is a V_ℓ such that $W_j \subset V_\ell$. Therefore $V_i \subset V_\ell$, so $i = \ell$ and $V_i = W_j$. This implies that $s = t$ and, after a possible renumbering, $V_i = W_i$ ∎

Definition 2.17 *The V_i of Corollary 2.16 are called the* **irreducible components of V**.

Corollary 2.18 *(i) For any radical ideal $I \subset k[X_1, \ldots, X_m]$, there exist prime ideals $P_1, \ldots P_s \subset k[X_1, \ldots, X_m]$ such that $P_i \not\subset P_j$ for $i \neq j$ and $I = \cap_{i=1}^s P_i$.*
(ii) If R is a ring, finitely generated over a field k, then for any radical ideal $I \subset R$, there exist prime ideals $P_1, \ldots, P_s \subset R$ such that $P_i \not\subset P_j$ for $i \neq j$ and $I = \cap_{i=1}^s P_i$.

Proof. Left as an exercise. ∎

2.3 Morphisms and Coordinate Rings

Definition 2.19 *Let $V \subset \bar{k}^m$ and $W \subset \bar{k}^n$ be k-closed sets. A function $F : V \to W$ is a* **k-morphism** *if there exist polynomials $f_1, \ldots, f_n \in k[X_1, \ldots, X_m]$ such that*

$$F(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots, f_n(a_1, \ldots, a_m))$$

for all $(a_1, \ldots, a_m) \in V$. A **k-morphism** *$F : V \to W$ is a* **k-isomorphism** *if there is a k-morphism $G : W \to V$ such that $G \circ F = id_V$ and $F \circ G = id_W$.*

Example 2.20 *Let gl_n be the set of $n \times n$ matrices. We can identify this with $\bar{k}^{n^2}$ so this is a k-variety. Identifying $\mathrm{gl}_n \times \mathrm{gl}_n$ with $\bar{k}^{2n^2}$, one sees that the map $M : \mathrm{gl}_n \times \mathrm{gl}_n \to \mathrm{gl}_n$ defined by $M(A, B) = A \cdot B$ is a k-morphism.*

Example 2.21 *The sets $\{1, -1\}$ and $\{\sqrt{2}, -\sqrt{2}\}$ are not isomorphic as $\mathbb{Q}$-varieties but are isomorphic as $\mathbb{C}$-varieties (via the isomorphism $x \mapsto \sqrt{2}x$). This is an example of how a change of $\bar{k}$-bases yields distinct k-varieties.*

Lemma 2.22 *k-morphisms are continuous in the Zariski k-topology.*

Proof. Left as an exercise. ∎

Of course it is too much to expect that morphisms take k-closed sets to k-closed sets. For example, let $V = V(xy - 1) \subset \bar{k}^2$, $W = k$ and $F : V \to W$, $F(x, y) = x$. The image of F is $\{x \in \bar{k} \mid x \neq 0\}$. Nonetheless, the image of a morphism is "large" in its Zariski k-closure.

Theorem 2.23 *(Chevalley's Theorem; [14], Chapter 4.4) Let V and W be as above and $F : V \to W$ a k-morphism. Then $F(V)$ contains a set that is dense and open in $\overline{F(V)}$, the k-closure of $F(V)$.*

Let us now consider k-morphisms F from a k-closed set V to $\bar{k}$. The set of such morphisms forms a ring under operations $(F + G)(a_1, \ldots, a_m) := F(a_1, \ldots, a_m) + G(a_1, \ldots, a_m)$ and $(F \cdot G)(a_1, \ldots, a_m) := F(a_1, \ldots, a_m)G(a_1, \ldots, a_m)$. We denote this ring by $\mathcal{O}_k(V)$; it is called the **coordinate ring of V**. Consider the map

$$\Phi : k[X_1, \ldots, X_n] \to \mathcal{O}_k(V)$$

give by $\Phi(f(X_1,\ldots,X_n)) =$ the k-morphism defined by $(a_1,\ldots,a_n) \mapsto f(a_1,\ldots,a_n)$. One can check that Φ is a ring homomorphism and that the kernel of Φ is $I_k(V)$. Therefore

$$\mathcal{O}_k(V) \simeq k[X_1,\ldots,X_n]/I_k(V).$$

One sometimes sees the notation $k[V]$ for $\mathcal{O}_k(V)$.

Example 2.24 *(i)* $\mathcal{O}_k(\bar{k}) = k[X]$
(ii) Let $k = \mathbb{Q}, V = \{\pm\sqrt{2}\}, I_k(V) = \langle X^2 - 2\rangle$ *so* $\mathcal{O}_k(V) = \mathbb{Q}(\sqrt{2})$.

Lemma 2.25 *$\mathcal{O}_k(V)$ is an integral domain if and only if V is k-irreducible.*

Proof. Left as an exercise. ∎

If $F : V \to W$ is a k-morphism and $g \in \mathcal{O}_k(W)$, then $g \circ F : V \to \bar{k}$ and furthermore $g \circ F \in \mathcal{O}_k(V)$. We define $F^* : \mathcal{O}_k(W) \to \mathcal{O}_k(V)$ to be the map $F^*(g) = g \circ F$. We then have

Lemma 2.26 *(i) The map $F^* : \mathcal{O}_k(W) \to \mathcal{O}_k(V)$ is a k-algebra homomorphism (i.e., a ring homomorphism that is the identity on k).*
(ii) If $G : \mathcal{O}_k(W) \to \mathcal{O}_k(V)$ is a k-algebra homomorphism, then there exists a unique k-morphism $F : V \to W$ such that $G = F^*$.

Proof. (i) This follows from a straightforward verification of the definition.

(ii) Write

$$\begin{aligned} \mathcal{O}_k(W) &= k[Y_1,\ldots,Y_n]/I_k(W) = k[y_1,\ldots,y_n] \\ \mathcal{O}_k(V) &= k[X_1,\ldots,X_m]/I_k(V) = k[x_1,\ldots,x_m]. \end{aligned}$$

Since $G : \mathcal{O}_k(W) \to \mathcal{O}_k(V)$ we have $G(y_i) = p_i(x_1,\ldots,x_m)$ for some $p_i \in k[X_1,\ldots,X_m]$. Define $F : \bar{k}^m \to \bar{k}^n$ via

$$F(a_1,\ldots,a_m) = (p_1(a_1,\ldots,a_m),\ldots,p_n(a_1,\ldots,a_m)).$$

This is a k-morphism from $\bar{k}^m$ to $\bar{k}^n$. I will now show that $F(V) \subset W$.

I first claim that for any polynomial $h \in k[Y_1,\ldots,Y_n]$,

$$G(h(y_1,\ldots,y_n)) = h(p_1(x_1,\ldots,x_m),\ldots,p_n(x_1,\ldots,x_m)).$$

This is because G is a k-algebra homomorphism and so acts in the natural way on polynomial combinations of the y_i. Now let $(a_1,\ldots,a_m) \in V$. We wish to show that $F(a_1,\ldots,a_m) \in W$. Recall that for any k-variety, Z, we have $V(I_k(Z)) = Z$, so to show that $F(a_1,\ldots,a_m) \in W$ we need to show that for any $h \in I_k(W)$, we have $h(p_1(a_1,\ldots,a_m),\ldots,p_n(a_1,\ldots,a_m)) = 0$. Note that for $h \in I_k(W)$ we have that $h(y_1,\ldots,y_n) = 0$ so $G(h(y_1,\ldots,y_n)) = 0$. This

means that $h(p_1(x_1,\ldots,x_m),\ldots,p_n(x_1,\ldots,x_m)) = 0$ and so $h(p_1(X_1,\ldots,X_m),\ldots,p_n(X_1,\ldots,X_m))$ $\in I_k(V)$. Therefore $h(p_1(a_1,\ldots,a_m),\ldots,p_n(a_1,\ldots,a_m)) = 0$.

To show uniqueness, let $G = F_1^* = F_2^*$ where

$$\begin{aligned} F_1(a_1,\ldots,a_m) &= (p_1(a_1,\ldots,a_m),\ldots,p_n(a_1,\ldots,a_m)), \text{ and} \\ F_2(a_1,\ldots,a_m) &= (q_1(a_1,\ldots,a_m),\ldots,q_n(a_1,\ldots,a_m)). \end{aligned}$$

We have $G(y_i) = p_i(x_1,\ldots,x_m) = q_i(x_1,\ldots,x_m)$ so $p_i(X_1,\ldots,X_m) - q_i(X_1,\ldots,X_m) \in I_k(V)$. Therefore $p_i(a_1,\ldots,a_m) = q_i(a_1,\ldots,a_m)$ for all $(a_1,\ldots,a_m) \in V$. This yields $F_1 = F_2$ on V. ∎

A simple application of the previous lemma yields

Corollary 2.27 *Aa k-algebra homomorphism $F : V \to W$ is an isomorphism if and only if the map $F^* : \mathcal{O}_k(W) \to \mathcal{O}_k(V)$ is a k-algebra isomomorphism.*

In later sections, we shall run into the following situation. Let V be a k-irreducible k-variety and let K be a field containing k. What can be said about V as a K-variety? V need not be K-irreducible. For example the $\mathbb{Q}$-variety $\{\pm\sqrt{2}\}$ is $\mathbb{Q}$-irreducible but is $\mathbb{C}$-reducible. Nonetheless, when k is algebraically closed this loss of irreducibility does not happen. We have the following proposition.

Proposition 2.28 *Let k_0 be an algebraically closed field and k_1 a field containing k_0. Let V be a k_0-irreducible k_0-variety.*

1. *$I_{k_1}(V) = k_1 \cdot I_{k_0}(V)$ that is, $I_{k_1}(V)$ is the k_1-span of $I_{k_0}(V)$.*
2. *$I_{k_1}(V)$ is prime and $\mathcal{O}_{k_1}(V) = k_1 \otimes_{k_0} \mathcal{O}_{k_0}(V)$.*

Proof. We will prove item 1. and refer the reader to [19], Corollary 4.15, Corollary 4.16, p. 368 or [16] Ch. 0, Sec. 12, esp. Proposition 7, p. 25 for the proof of item 2.

Let $f \in I_{k_1}(V)$ and let $\{\alpha_j\}_{j\in J}$ be a k_0-basis of k_1. We may write $f = \sum_{j\in J} f_j\alpha_j$ where f_j is a polynomial with coefficients in k_0. For any $v \in V(k_0)$ we have $f(v) = 0$ so each $f_j(v) = 0$. Since k_0 is algebraically closed, the Hilbert Nullstellensatz, Theorem 2.10, implies that each $f_j \in I_{k_0}(V)$. Therefore $I_{k_1}(V) \subset k_1 \cdot I_{k_0}(V)$. The reverse inclusion is clear. ∎

2.4 Problems

2.1 Prove Lemma 2.5. Is the union of an infinite set of k-varieties a k-variety?

2.2 Show that any two non-empty k-open sets have a nonempty intersection.

2.3 Show that if V is a k-variety then $V(I_k(V)) = V$.

2.4 Prove parts (ii) and (iii) of Corollary 2.15.

2.5 Prove Corollary 2.18.

2.6 Prove Lemma 2.22.

2.7 Prove Lemma 2.25.

3 Linear Algebraic Groups

In this section, we give an introduction to the theory of linear algebraic groups and give a flavor for some of the basic proofs. If this subject interests you, a good introduction is [31]. For a more complete treatment, see [14] or [35].

3.1 Linear Algebraic Groups

In this section and Section 3.2, we will assume that all varieties are defined over an algebraically closed field which we denote by C. As in the rest of the paper, we restrict ourselves to fields of characteristic 0. We will use the terms open, closed, etc. to refer to C-open, C-closed, etc. in the Zariski C-topology.

Let us consider the group GL_n of $n \times n$ invertible matrices with entries in C. We can identify the n^2 entries of a matrix $g \in \mathrm{GL}_n(C)$ with a vector in C^{n^2}. In this way $\mathrm{GL}_n(C)$ can naturally be identified with the open set $\{g \in C^{n^2} \mid \det(g) \neq 0\}$. We would like to think of $\mathrm{GL}_n(C)$ as a *closed* set and we do this in the following way. For $g \in \mathrm{GL}_n(C)$, consider the matrix

$$\hat{g} = \begin{pmatrix} & & & 0 \\ & g & & \vdots \\ & & & 0 \\ 0 & \dots & 0 & \det(g)^{-1} \end{pmatrix}.$$

The set of such matrices $\hat{g} = (\hat{g}_{i,j})$ is a closed set in $C^{(n+1)^2}$ defined by $\hat{g}_{1,n+1} = \ldots = \hat{g}_{n,n+1} = 0$, $\hat{g}_{n+1,1} = \ldots = \hat{g}_{n+1,n} = 0, \det(\hat{g}_{i,j})_{1 \leq i,j \leq n} \cdot \hat{g}_{n+1,n+1} = 1$. Let $I(\mathrm{GL}_n)$ be the ideal of this closed set. The coordinate ring of GL_n therefore is

$$\mathcal{O}_C(\mathrm{GL}_n) = C[Y_{1,1}, \ldots, Y_{n+1,n+1}]/I(\mathrm{GL}_n) = C[y_{1,1}, \ldots, y_{n,n}, 1/\det(y_{i,j})].$$

Although we are identifying elements g of GL_n with the matrices $\hat{g}$ above, we will be casual and just refer to the original matrix g. $\mathrm{GL}_n(C)$ is the main example of the following

Definition 3.1 *A* **linear algebraic group** *is a closed subgroup of* GL_n.

Example 3.2 *(i)* $\mathrm{SL}_n = \{g \in \mathrm{GL}_n \mid \det(g) = 1\}$
(ii) $\mathrm{T}_n = \{g \in \mathrm{GL}_n \mid g_{i,j} = 0 \text{ if } i > j\}$
(iii) $\mathbf{G_a} = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in C\}$ *= the additive group*
(iv) $\mathbf{G_m} = \mathrm{GL}_1 = \{a \mid a \in C, a \neq 0\}$ *= the multiplicative group*

From example 2.20 we see that multiplication is a morphism from $\mathrm{GL}_n \times \mathrm{GL}_n \subset C^{2n^2}$ to GL_n. Furthermore, the inverse of an element $(g_{i,j})$ of GL_n has entries that are polynomials in the $g_{i,j}$ and $1/\det(g_{i,j})$. Therefore the map $g \mapsto g^{-1}$ is a morphism as well.

Definition 3.3 *A morphism (isomorphism) of linear algebraic groups that preserves the group operations is called a* **group morphism (group isomorphism)**.

We now turn to some elementary properties of linear algebraic groups. One sees from Corollary 2.16 that a linear algebraic group G may be written as an irredundant union of irreducible varieties $G = V_1 \cup \ldots \cup V_t$. I claim that any element $g \in G$ belongs to exactly one component. To see this let $h \in V_1, h \notin V_2 \cup \ldots \cup V_t$. For any $y \in G$ the map $m_y : G \to G$ defined by $m_y(g) = yg$ is an isomorphism (in the sense of varieties, not in the sense of groups). Therefore, m_y permutes the components of G. For any $g \in G$, $m_{gh^{-1}}(h) = g$ so g belongs to a unique component of G and our claim is proved. In particular, the irreducible components of G are disjoint. One usually refers to a linear algebraic group that is irreducible as a variety as a *connected* linear algebraic group. In group theory the word *irreducible* has other meanings.

Definition 3.4 *Let G be a linear algebraic group. The unique component containing the identity is denoted by* $\mathbf{G^0}$ *and is called the* **identity component of G**.

Lemma 3.5 *(i) G^0 is a normal subgroup of G of finite index whose cosets are the components of G.*
(ii) If H is a closed subgroup of finite index in G, then $G^0 \subset H$.

Proof. (i) Note that multiplication by an element of G is an isomorphism of G to itself. Therefore, for any $g \in G^0$, $g^{-1}G^0$ is an irreducible component of G. Since $e \in g^{-1}G^0 \cap G^0$, we have $g^{-1}G^0 = G^0$. Therefore $(G^0)^{-1} \subset G^0$. For any $g \in G^0$, we have $e \in gG^0 \cap G^0$ so $G^0 \cdot G^0 \subset G^0$. Therefore G^0 is a subgroup of G. For any $g \in G$ the map $y \mapsto gyg^{-1}$ is an isomorphism from G to G. Since $e \in gG^0g^{-1} \cap G^0$ we have $gG^0g^{-1} \subset G^0$ so G^0 is normal in G. Finally, if $V_1, \ldots, V_t$ are the components of G, then for any $g_i \in V_i$ we have $g_i \in g_iG^0 \cap V_i$ so $g_iG^0 = V_i$.

(ii) Let H be a closed subgroup of G of finite index. Each coset of H is also closed. We have $G = g_1H \cup \ldots \cup g_sH$ with $g_iH \cap g_jH = \emptyset$ for $i \neq j$. Since G^0 is irreducible, we must have $G^0 \subset g_iH$ for some i. Since $e \in G^0$, we have $e \in g_iH = eH = H$ so $G^0 \subset H$. ∎

Many facts about linear algebraic groups can be proven using simple topological arguments. For example, let X and Y be topological spaces, $Z \subset X$ and $\phi : X \to Y$ a continuous map. Denote by $\overline{Z}$ the closure of the set Z. We then have that $\phi(\overline{Z}) \subset \overline{\phi(Z)}$. Several facts about linear algebraic groups can be deduced from this simple fact.

Lemma 3.6 *If G is a linear algebraic group and H is a subgroup, then $\overline{H}$ is a linear algebraic group.*

Proof. Using the above observation for $\phi(x) = x^{-1}$ we have $(\overline{H})^{-1} \subset \overline{H^{-1}} = \overline{H}$. Using the same observation for $\phi(x) = gx$ for $g \in H$, on sees that $g\overline{H} \subset \overline{gH} = \overline{H}$ and so $H\overline{H} \subset \overline{H}$. If $x \in \overline{H}$ then $Hx \subset \overline{H}$ so $\overline{H} \cdot \overline{H} \subset \overline{H}$. ∎

Recall that the image of a variety does not need to be closed in general. Nonetheless, we will show that the image of a linear algebraic group under a group morphism is closed.

Lemma 3.7 *(i) If U and V are two dense open subsets of a linear algebraic group G, then $G = U \cdot V$.*
(ii) If H is a subgroup of a linear algebraic group G and H contains a dense open set of its closure, the $H = \overline{H}$.
(iii) If $\phi : G \to G'$ is a group morphism of linear algebraic groups, then $\phi(G)$ is a closed subgroup of G'. Furthermore, $\phi(G^0) = (\phi(G))^0$.

Proof. (i) Since $\phi(x) = x^{-1}$ is a homeomorphism of G, we have that V^{-1} is again a dense open set. Furthermore, for $g \in G$, gV^{-1} is also a dense open subset of G. Since both gV^{-1} and U are dense and open, we have $gV^{-1} \cap U \neq \emptyset$. Therefore $gv^{-1} = u$ or $g = uv$ for some $u \in U, v \in V$.
(ii) Let $U \subset H$ be a dense open subset of $\overline{H}$. From (i), we know $\overline{H} = U \cdot U \subset H$. Therefore $\overline{H} = H$.
(iii) By Theorem 2.23, we know that $\phi(G)$ contains a dense open subset of $\overline{\phi(G)}$. Therefore (ii) implies that $\overline{\phi(G)} = \phi(G)$. To prove the second statement, note that $\phi(G^0)$ is closed and $\phi(G^0)$ is of finite index in $\phi(G)$. Therefore Lemma 3.5 implies that $\phi(G)^0 \subset \phi(G^0)$. Since ϕ is continuous, $\phi(G^0)$ is irreducible so $\phi(G^0) \subset \phi(G)^0$. ∎

We state the following theorem without proof. It is a key result for the further study of linear algebraic groups and a proof can be found in (Chapter 11.5, [14]).

Theorem 3.8 *Let N be a normal closed subgroup of a linear algebraic group G. There exists an integer m and a group morphism $\phi : G \to \mathrm{GL}_m$ such that $\ker \phi = N$.*

Since Lemma 3.7 implies that $\phi(G)$ in the above theorem is closed and $G/N \simeq \phi(G)$, the above theorem allows us to say that G/N "is" a linear algebraic group as well.

3.2 Lie-Kolchin Theorem

The following result comes from the existence of Jordan Normal Forms of matrices.

Theorem 3.9 *If A is an $n \times n$ matrix with entries in C then there exists an invertible matrix B with entries in C such that BAB^{-1} is an upper triangular matrix.*

One would like to generalize this result to show that certain *sets* of matrices can be simultaneously put in upper triangular form. Obviously one cannot do this for all sets of matrices but it is not hard to generalize the above result to show that if $\{A_i\}_{i \in \mathcal{I}}$ is a set of commuting matrices, then there exists an invertible matrix B with entries in C such that BA_iB^{-1} is an upper triangular matrix for all $i \in \mathcal{I}$. One can generalize this further.

Definition 3.10 *A group G is* solvable *if there is a tower of subgroups $G = G_0 \supset G_1 \supset \ldots \supset G_t = \{e\}$ such that G_{i+1} is normal in G_i and G_i/G_{i+1} is abelian.*

Example 3.11 *(i) Any commutative group is solvable.*
(ii) Another example is given by T_n, the group of upper triangular matrices. As Rosenlicht points out in (p.18,[31]), the following chain of subgroups satisfies the conditions of the definition for T_4

$$\left\{\begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix}\right\} \supset \left\{\begin{pmatrix} 1 & * & * & * \\ 0 & 1 & * & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\} \supset \left\{\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\}$$
$$\supset \left\{\begin{pmatrix} 1 & 0 & 0 & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\} \supset \left\{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\right\}$$

The following can be thought of as a global version of the above theorem.

Theorem 3.12 *(Lie-Kolchin) If $G \subset \mathrm{GL}_n$ is a connected, solvable linear algebraic group then there exists a $B \in GL_n$ such that $BGB^{-1} \subset \mathrm{T}_n$.*

Direct proofs of Theorems 3.9 and 3.12 are given in 18 pages in [31]. One of the exercises in this section shows that the Lie-Kolchin Theorem is not necessarily true without the connectedness asumption.

3.3 Torsors

In this section, k is an arbitrary field and $\bar{k}$ is again an algebraically closed field containing k.

Definition 3.13 *Let $G \subset \mathrm{GL}_n$ be a linear algebraic group defined over k and V be a k-closed subset of GL_n. V is a* **k-torsor for G** *(also called a principal homogeneous space) if for any $v, w \in V$ there exists a $g \in G$ such that $v \cdot g = w$, where $v \cdot g$ denotes the usual matrix multiplication.*

The above is not the usual definition of a torsor (cf. [35] §2.3, [33] §5.2) but rather a special case of the general definition that suffices for our needs. Note that since $v, w \in \mathrm{GL}_n$, the g in the definition is unique.

Example 3.14 *G is itself a k-torsor. Given $u, v \in G$, let $g = v^{-1}u$.*

Definition 3.15 *G is called the* **trivial torsor** *for G.*

Lemma 3.16 *A k-torsor for G is k-isomorphic to the trivial torsor for G if and only if $V(k) \neq \emptyset$.*

Proof. Note that $e \in G(\mathbb{Q})$ so G has a k-point for any k. If $\phi : G \to V$ is a k-morphism, then $\phi(e)$ is a k-point of V. Now assume $v \in V(k)$. The map $\phi : G \to V$ defined by $g \mapsto vg$ is defined over k and from the definition of k-torsor, one sees that it is an isomorphism of k-torsors. ∎

Example 3.17 *Let $k = \mathbb{Q}$, $G = \mathbb{Z}/2\mathbb{Z} = \{(\pm 1)\} \subset \mathrm{GL}_1(\bar{\mathbb{Q}})$. Let $V = \{(\pm\sqrt{2})\}$. V is a k-irreducible, k-torsor for G. Note that V is not k-isomorphic to the trivial torsor for G.*

If V is a k-torsor for G and $g \in G(k)$, then the map $\rho_g : v \mapsto vg$ is a k-isomorphism of V to itself and so induces a k-algebra isomorphism $\rho_g^* : \mathcal{O}_k(V) \to \mathcal{O}_k(V)$. Explicitly, if $\mathcal{O}_k(V) = k[x_{1,1}, \ldots, x_{n,n}, 1/\det(x_{i,j})]/I$ for some ideal I, then for $g = (g_{i,j})$ the map ρ_g^* is given by $\rho_g^*(x_{i,j}) = y_{i,j}$ where $(y_{i,j}) = (x_{i,j})(g_{i,j})$.

Example 3.18 (Example 3.17 bis) *$V = \{\sqrt{2}, -\sqrt{2}\}$ and $\mathcal{O}_{\mathbb{Q}}(V) = \mathbb{Q}(\sqrt{2})$. $\rho_{(1)}^*(\sqrt{2}) = \sqrt{2}$ and $\rho_{(-1)}^*(\sqrt{2}) = -\sqrt{2}$. In this example $G = \{\pm 1\}$ is also the Galois group of $\mathbb{Q}(\sqrt{2})$. So $g \in G$ acts on $\mathcal{O}_{\mathbb{Q}}(V) = \mathbb{Q}(\sqrt{2})$ in two ways: first as ρ_g^* and second as an element of the Galois group. One easily sees that these actions are the same.*

Theorem 3.19 *Let G be a linear algebraic group defined over k.*
(i) If k is algebraically closed, then any k-torsor for G is trivial.
(ii) If $G = \mathbf{G_a}, \mathbf{G_m}$ or a connected solvable linear algebraic group, the any k-torsor for G is trivial.
(iii) If G is a connected linear algebraic group defined over an algebraically closed field C and $k = C(x)$, then any k-torsor for G is trivial.

Proof. (i) follows from Lemma 3.16. For (ii) and (iii) see ([33], p. 150; (iii) is originally due to T.A.Springer). ∎

3.4 Problems

In problems [3.1]-[3.4], the algebraic groups are defined over an algebraically closed field C.

3.1 Let X be a closed subset of GL_n such that $e \in X$ and X is closed under products. Show that X is a linear algebraic group. (Hint: recall that any descending chain of closed sets $X_1 \supset X_2 \supset \ldots$ must stabilize.). Show the same result without assuming that $e \in X$ (but assume X is nonempty).

3.2 Let G be a connected linear algebraic group and let N be a finite normal subgroup. Show that $N \subset Z(G) = \{g \in G \mid hg = gh \text{ for all } g \in G\}$.

3.3 Prove that the sets in example 3.11(ii) show that T_4 is solvable.

3.4 The aim of this exercise is to show that the Lie-Kolchin Theorem is not true without the connectedness assumption. We will show that a finite subgroup of T_n is abelian and that there are solvable nonabelian finite subgroups of GL_4.
(a) Let A be an $n \times n$ matrix such that $A^m = e$. Show that if 1 is the only eigenvalue of A, then $A = e$. Hint: The minimal polynomial of A divides $X^m - 1$ and also $(X-1)^t$ for some $t > 0$.
(b) If G is a finite subgroup of T_n then G must be abelian. Hint: Let $g_1, g_2 \in G$ and consider the element $g_1 g_2 g_1^{-1} g_2^{-1} \in G$.
(c) The alternating group $\mathcal{A}_4$ on 4 elements can be represented as 4×4 permutation matrices. It is solvable but nonabelian.

3.5 Let k be any field and $G = \mathbb{Z}/2\mathbb{Z} = \{(\pm 1)\} \subset \mathrm{GL}_1$. The aim of this exercise is to classify the irreducible k-torsors of G in $\mathrm{GL}_1(k)$. In particular, we will show that there is a bijection between the k-isomorphism classes of irreducible k-torsors for this group and the group $k^*/(k^*)^2$, where $k^* = k \backslash \{0\}$. Let V be an irreducible k-torsor in $\mathrm{GL}_1(k)$.
(a) Show that $\mathcal{O}(V) = k(\sqrt{a})$ for some $a \in k^*$.
(b) Show that $k(\sqrt{a})$, a not a square in k, is isomorphic to $k(\sqrt{b})$ as k-algebras if and only if $a = bc^2$, for some $c \in k$.
(c) Show that the map $V \mapsto a$ is a well defined bijection from irreducible k-torsors to the set $k^*/(k^*)^2$.

4 Picard-Vessiot Extensions

Many authors (Malgrange, Umemura, Chatzidakis/Hrushovsky, André, Franke, Etingof, Casale, Blázquez-Sanz, Wibmer,...) have developed Galois theories of linear difference equations and even extensions to nonlinear equations. Here, we will develop an algebraic approach that is particularly successful in dealing with properties of sequences satisfying recurrence relations. The general reference for Sections 4, 5 and 6 is [27] and the rough notes [34].

4.1 Difference Rings and Fields

Definition 4.1 *A* **difference ring** (R, σ) *is a ring together with an automorphism* $\sigma : R \to R$. *If* R *is in addition a field, we say that* R *is a* **difference field**. *If* (R, σ) *is a difference ring, the set* $R^\sigma = \{c \in R \mid \sigma(c) = c\}$ *is called the* **ring of constants of R**. *If* (R, σ) *and* (S, τ) *are difference rings, a* **difference homomorphism** *of* R *to* S *is a homomorphism* $\phi : R \to S$ *such that* $\phi \circ \sigma = \tau \circ \phi$. **Difference isomorphism** *and* **difference automorphism** *are defined in a similar way.*

One can develop a Galois theory where one only assumes that σ is injective (see the papers of P. Nguyen[23] or M. Wibmer[36]) but the above definition will suffice for our present purposes.

Example 4.2 *(i) Any ring with $\sigma =$ identity.*
(ii) $(\mathbb{Q}(\sqrt{2}, \sigma)$ where $\sigma(\sqrt{2}) = -\sqrt{2}$.
(iii) $(\mathbb{C}[x], \sigma)$ where $\sigma(x) = x + 1$.
(iv) $(\mathbb{C}[x], \sigma)$ where $\sigma(x) = qx, q \in \mathbb{C}\backslash\{0\}$ (linear difference equations over this difference field are studied in the paper of Sauloy in this volume).

Example 4.3 The Ring of Germs at Infinity of Sequences *Let C be a field and let SEQ_C be the ring of sequences $\{a = (a(0), a(1), \ldots,) \mid a(i) \in C\}$ where multiplication and addition are defined componentwise. Define a ring homomorphism $\sigma : \mathrm{SEQ}_C \to \mathrm{SEQ}_C$ as $\sigma((a(0), a(1), \ldots)) = (a(1), a(2), \ldots)$. Note that σ is surjective but not injective since $\sigma((1, 0, 0, \ldots) = (0, 0, \ldots)$. To ameliorate this, define an equivalence relation on SEQ_C as follows: $a \sim b$ if there is an $N \in \mathbb{N}$ such that $a(j) = b(j)$ for all $j > N$. One can show that addition, multiplication and σ are well defined on equivalence classes. Furthermore, σ is now a bijection on equivalence classes. The ring $\mathcal{S}_C = \mathrm{SEQ}_C/\sim$ of equivalence classes with automorphism induced by σ is called the* **ring of germs at infinity of sequences**. *We will frequently abuse notation and identify a sequence a with its equivalence class. Therefore equations such as $a = b$ must be interpreted as $a(i) = b(i)$ for $i >> 0$.*

One can embed C into $\mathcal{S}_C$ by mapping c to the sequence $(c, c, c, \ldots)$. One can also embed $C(x)$ into $\mathcal{S}_C$ by mapping the rational function $f(x)$ to $(0, 0, \ldots, 0, f(N), f(N+1), \ldots)$ where N is an integer larger than any integer roots of the denominator of f.

Definition 4.4 *Let (R, σ) be a difference ring. An ideal $I \subset R$ is called a* **σ-ideal** *if $\sigma(I) \subset I$. (R, σ) is said to be a* **simple difference ring** *if the only σ-ideals are (0) and R.*

4.2 Linear Difference Equations and Picard-Vessiot Extensions

Let (R, σ) be a difference ring and y an variable. An equation of the form

$$L(y) = c_n\sigma^n(y) + c_{n-1}\sigma^{n-1}(y) + \ldots + c_0 y \tag{1}$$

with $c_i \in R$ and $c_n \neq 0$ is called **an $\mathbf{n^{th}}$ order scalar difference equation.** An element $z \in R$ such that $L(z) = 0$ is called a solution of $L(y) = 0$.

Example 4.5 *In $\mathcal{S}_{\mathbb{C}}$, the sequence of Fibonacci numbers $F = (F(0), F(1), \ldots)$ is a solution of $\sigma^2(y) - \sigma(y) - y = 0$.*

Example 4.6 *Let p be an integer greater than 1. The map $\sigma(x) = x^p$ is an injective homomorphism for $\mathbb{C}(x)$ to itself. If is not surjective but this can be remedied in the following way. Let*

$$K_{p^n} = \mathbb{C}(x^{\frac{1}{p^n}}).$$

One can identify K_{p_n} with a subfield of $K_{p^{n+1}}$ and form

$$K_{p^\infty} = \cup_{n=0}^{\infty} K_{p^n}.$$

The map given by $\sigma(x^{\frac{1}{p^n}}) = (x^{\frac{1}{p^n}})^p$ is an isomorphism of K_{p^∞} to itself. Linear difference equations over K_{p^∞} are called Mahler equations and arise when studying generating functions of automatic sequences and other sequences arising from combinatorics (see [8, 23, 24, 29]).

Example 4.7 *Let $\mathcal{E}$ be an elliptic curve defined over $\mathbb{C}$ and $K = \mathbb{C}(x, y)$ its associated function field. The curve $\mathcal{E}$ has a natural structure of an abelian group. Letting $\oplus$ denote the group operation and P a point on $\mathcal{E}$, we have a map $\rho_P : \mathcal{E} \to \mathcal{E}$ given by $\rho_P(Q) = Q \oplus P$. This map induces an automorphism $\sigma : K \to K$ giving (K, σ) the structure of a difference field. Linear difference equation over this field and their Galois theory have been studied in [9].*

We will always assume that $c_0 \neq 0$ in a scalar difference equation. This is not a restriction as far as solutions are concerned. If $c_i \neq 0, c_{i+1} = \ldots = c_0 = 0$, then we may write

$$\begin{aligned} L(y) &= c_n\sigma^n(y) + \ldots + c_i\sigma^i(y) \\ &= \sigma^i(\sigma^{-i}(c_n)\sigma^{n-i}(y) + \ldots + \sigma^{-i}(c_i)y) \\ &= \sigma^i(\hat{L}(y)) \end{aligned}$$

Since σ is an automorphism, the solutions of $L(y) = 0$ and $\hat{L}(y) = 0$ coincide.

In fact it is more convenient to deal with **first order matrix difference equations**

$$\sigma(Y) = AY \text{ where } A \in \mathrm{GL}_n(R)$$

where $\mathrm{GL}_n(R)$ denotes the group of invertible matrices with entries in R. Given a scalar difference equation with $c_0 \neq 0$, we associate to it a first order matrix difference equation $\sigma(Y) = A_L Y$ where

$$A_L = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & & 0 & \ldots & 1 & 0 \\ 0 & & 0 & \ldots & 0 & 1 \\ -\frac{c_0}{c_n} & -\frac{c_1}{c_n} & -\frac{c_2}{c_n} & \ldots & -\frac{c_{n-2}}{c_n} & -\frac{c_{n-1}}{c_n} \end{pmatrix}.$$

If z is a solution of $L(y) = 0$, then $(z, \sigma(z), \ldots, \sigma^{n-1}(z))^T$ is a solution of $\sigma(Y) = A_L Y$. In many cases, first order matrix equations can be reduced to scalar equations. See Appendix B of [13] for more details concerning the relation between scalar and matrix difference

equations.

If R is a difference ring and $\sigma(Y) = AY$ is a matrix difference equation with $A \in \mathrm{GL}_n(R)$ the set of solutions of this difference equation in R^n forms a vector space over R^σ. In general one cannot bound the dimension of this space but when one puts restrictions on R there is a natural bound.

Lemma 4.8 *Let (R, σ) be a simple difference ring and $A \in \mathrm{GL}_n(R)$. Let $z_1, \ldots, z_r \in R^n$ satisfy $\sigma(Y) = AY$. If $z_1, \ldots, z_r$ are linearly dependent over R then they are linearly dependent over R^σ.*

Proof. Assume there is a relation $\sum_{i=1}^r c_i z_i = 0$ with $c_i \in R$ and $c_1 \neq 0$. We can assume that no proper subset of $\{z_1, \ldots . z_r\}$ is linearly dependent over R. The set $I = \{c \in R \mid \text{there exist } d_2, \ldots, d_r \in R \text{ such that } cz_1 + \sum_{i=2}^r d_i z_i = 0\}$ is a σ-ideal and so contains 1. Therefore we can assume that there is a relation of the form $z_1 + \sum_{i=2}^r c_i z_i = 0$. Applying σ to $z_1 + \sum_{i=2}^r c_i z_i = 0$, we have $A(z_1 + \sum_{i=2}^r \sigma(c_i) z_i) = 0$ so $z_1 + \sum_{i=2}^r \sigma(c_i) z_i = 0$. Subtracting the original relation, we get $\sum_{i=2}^r (\sigma(c_i) - c_i) z_i = 0$. By minimality we must have $\sigma(c_i) = c_i$. ∎

Corollary 4.9 *Let (R, σ) be a simple difference ring and $A \in \mathrm{GL}_n(R)$. If $V = \{v \in R^n \mid \sigma(v) = AV\}$ then $\dim_{R^\sigma} V \leq n$.*

In the Galois theory of polynomial equation, it is convenient to have a field containing all the roots of a given polynomial. If $p(X) \in \mathbb{Q}[X]$ one can either use the fundamental theorem of algebra to see that $\mathbb{C}$ is such a field or one can synthetically construct a "splitting field". For difference equations with coefficients in $\mathbb{C}(x)$, the ring $\mathcal{S}_{\mathbb{C}}$ will play a role similar to the role $\mathbb{C}$ plays for the polynomial $p(x)$ and we will see below how a synthetic approach also allows us to find solutions. Since we would like the synthetic approach to agree with what we see when we look at solutions in $\mathcal{S}_C$, we start by considering the following example.

Example 4.10 *Consider the difference ring $\mathbb{C}$ with automorphism $\sigma =$ identity and the difference equation*

$$\sigma(y) = (-1)y, \ (-1) \in \mathrm{GL}_1(\mathbb{C}).$$

This equation has $z = (1, -1, 1, -1, \ldots) \in \mathcal{S}_C$ as a solution and the ring $R = \mathbb{C}[z]$ contains all solutions in $\mathcal{S}_{\mathbb{C}}$ of this equation. Note that for

$$\begin{aligned} w_1 &= z^2 + z = (2, 0, 2, 0, 2, 0, \ldots) \\ w_2 &= z^2 - z = (0, 2, 0, 2, 0, 2, \ldots) \end{aligned}$$

we have $w_1 \cdot w_2 = 0$. Therefore the ring R has zero divisor and cannot be embedded in a field. The ring R seems to be a natural analogue of a splitting field for the equation $\sigma(y) = (-1)y$ so we should not expect our synthetic approach to yield fields.

Let us recall a method for constructing a splitting field for a polynomial $p(X) \in k[X]$ with k a field, p having no repeated roots and $\deg p = n$. To construct an object that contains n roots of p, we could consider the ring

$$R_1 = k[X_1, \ldots, X_n]/\langle p(X_1), \ldots, p(X_n)\rangle \ .$$

Although p has n distinct roots in R_1, this ring does not take into account possible algebraic relations among the roots. For example, when $p(X) = X^3 - 2, k = \mathbb{Q}$, one sees that $R_1 = \mathbb{Q}(\alpha_1) \oplus \mathbb{Q}(\alpha_2) \oplus \mathbb{Q}(\alpha_3)$ where $\alpha_i^3 - 2 = 0$ but we do not have $\alpha_1 + \alpha_2 + \alpha_3 = 0$. To try to fix this, let I be a maximal ideal in $k[X_1, \ldots, X_n]$ containing $\langle p(X_1), \ldots, p(X_n)\rangle$. Intuitively, I is a maximal set of relations among the X_i consistent with the X_i being roots of $p(X)$. Let

$$R_2 = k[X_1, \ldots, X_n]/I.$$

When $p(X) = x^3 - 2$, we may select $I = \langle X_1^3 - 2, X_2^3 - 2, X_3^3 - 2, X_1 - X_2, X_1 - X_3\rangle$. In this case $R_2 = \mathbb{Q}(\alpha_1)$ where $\alpha_1^3 - 2 = 0$. R_2 therefore does not contain 3 distinct roots. The final solution is the following. Let J be a maximal ideal containing $\langle p(X_1), \ldots, p(X_n)\rangle$ in the ring $k[X_1, \ldots, X_n, 1/\prod_{i\neq j}(X_i - X_j)]$. The added term $1/\prod_{i\neq j}(X_i - X_j)$ is to insure that the roots stay distinct. We then let

$$R = k[X_1, \ldots, X_n, 1/\prod_{i\neq j}(X_i - X_j)]/J.$$

One sees that R is a field generated over k by n distinct roots of $p(X)$ and so must be the usual splitting field of this polynomial. Therefore, up to isomorphism, R will be independent of the choice of J.

We now turn to constructing an object that contains as large a set as possible of solutions of a difference equation $\sigma(Y) = AY$. From now on we will assume that $A \in \mathrm{GL}_n(k)$ where k is a difference *field*. We shall follow the path we described for constructing a splitting field of a polynomial. We wish to construct an object containing n linearly independent solutions of $\sigma(Y) = AY$. For this it will suffice to construct an $n \times n$ invertible matrix Z with $\det Z \neq 0$ that satisfies $\sigma(Z) = AZ$. The columns of Z then will span the solution space of the equation and have dimension n. Let $X = (X_{i,j})$ be an $n \times n$ matrix of variables. We consider the ring $k[X, 1/\det X] = k[X_{1,1}, \ldots, X_{n,n}, 1/\det X]$ and extend the automorphism σ by letting $\sigma(X) = AX$. Let I be a maximal σ-ideal in $k[X, 1/\det X]$ and let $R = k[X, 1/\det X]/I$. Note that since I is a maximal σ-ideal, R is a simple difference ring. From the construction and Corollary 4.9, the solution space of $\sigma(Y) = AY$ has dimension n over the field of constants R^σ.

Example 4.11 *Let $k = \mathbb{C}$ and σ = identity. Let $A = (-1) \in \mathrm{GL}_1(\mathbb{C})$ so our equation is $\sigma(y) = -y$. Following the construction above, we consider the difference ring $\mathbb{C}[y, 1/y]$ where $\sigma(y) = -y$. Let $I = \langle y^2 - 1\rangle$. I is a σ-ideal. There are only two ideals that contain I: $P_1 = \langle y - 1\rangle$ and $P_2 = \langle y + 1\rangle$. Neither is a σ-ideal, in fact, $\sigma(P_1) = P_2$. Therefore I is a maximal σ-ideal. Therefore the above construction yields $R = \mathbb{C}[y, 1/y]/\langle y^2 - 1\rangle$.*

Note that the map $y \mapsto (1,-1,1,-1,\ldots)$ *yields a* σ*-isomorphism of* R *with* $\mathbb{C}[(1,-1,1,-1,\ldots)] \subset \mathcal{S}_{\mathbb{C}}$.

The ring R that we have constructed is an example of

Definition 4.12 *Let* (k,σ) *be a difference field and* $A \in \mathrm{GL}_n(k)$. *A difference ring* (R,σ) *is a* **Picard-Vessiot ring (PV ring)** *for* $\sigma(Y) = AY$ *if*

1. $k \subset R$,
2. $R = k[Z, 1/\det Z]$ *where* $Z \in \mathrm{GL}_n(R)$ *and* $\sigma(Z) = AZ$, *and*
3. R *is a simple difference ring.*

Our construction above shows that PV rings exist. We note that one can define PV rings over rings that are more general than fields (see [1] and [36]). Regrettably, without further assumptions, a PV ring for a difference equation need not be unique but we do have the following result

Proposition 4.13 *Let* (k,σ) *be a difference field with* k^σ *algebraically closed. Let* R *be a PV ring for* $\sigma(Y) = AY, A \in GL_n(k)$. *Then*

1. $R^\sigma = k^\sigma$, *and*
2. *If* S *is another PV ring for* $\sigma(Y) = AY$, *then there exists a* k*-difference isomorphism of* R *and* S.

For the proof of the above proposition, see Lemma 1.8 and Proposition 1.9 of [27].

We now consider the finer structure of PV rings. We start with the following elementary lemma whose proof we leave as an exercise.

Lemma 4.14 *Let* (R,σ) *be a difference ring and* I *a* σ*-ideal of* R. *Then* $\sqrt{I}$ *is a* σ*-ideal and so every maximal* σ*-ideal is radical.*

Note that example 4.11 shows that a maximal σ-deal need not be prime.

Let R be a PV-ring for $\sigma Y = AY$. Since R is a simple difference ring we may write

$$R = k[Y, \frac{1}{\det Y}]/I$$

where Y is a set of n^2 variables and I is a maximal σ-ideal. Since I is radical, we have that $I = \cap_{i=0}^{t-1} P_i$ for some prime ideals P_i in $k[Y, \frac{1}{\det Y}]$. Since I is invariant under σ the P_i are permuted by σ. If a subset $\{P_{i_1}, \ldots, P_{i_r}\}$ is left invariant by σ, then $P_{i_1} \cap \ldots \cap P_{i_r}$ is a proper σ-ideal containing I. Since I is a maximal σ-ideal, we have that $r = t$ and so, after a possible renumbering, we may assume that $\sigma(P_i) = P_{i+1 \mod t}$. This furthermore implies that $\sigma^t(P_i) = P_i$ for all i.

I claim that each P_i is a maximal σ^t-ideal. If not, let Q_i be a σ^t-ideal containing P_i. We then have that $\cap_{j=0}^{t-1}\sigma^j(Q_i)$ is a proper σ-invariant ideal containing I and so must equal $I \subset P_i$. We can conclude that for some j, $\sigma^j(P_i) \subset \sigma^j(Q_i) \subset P_i$ for some $j \leq t-1$. This in turn implies that $j = 0$ and so $Q_i = P_i$.

Let $R_i = k[Y, \frac{1}{\det Y}]/P_i$. From the previous paragraph, we know that R_i is a simple σ^t-difference ring. We leave it as an exercise to find a difference equation for which it is a σ^t-PV extension. Let $\pi : k[Y, \frac{1}{\det Y}] \to R$ be the canonical projection with kernel I. For each pair $i \neq j$, the ideal $P_i + P_j$ is a σ^t-ideal containing both P_i and P_j and so, by the previous paragraph, must be all of $k[Y, \frac{1}{\det Y}]$. Therefore the Chinese Remainder Theorem implies that

$$R \simeq \oplus_{i=0}^{t-1} R_i.$$

Taken together, these facts imply the following

Proposition 4.15 *(Corollary 1.16, [27]) Let R be a PV extension of k for $\sigma(Y) = AY, A \in \mathrm{GL}_n(k)$. Then there exist $e_0, \ldots, e_{t-1} \in R$ such that*

1. $e_0 + \ldots + e_{t-1} = 1,\ e_i^2 = e_i, e_i e_j = 0$ *for* $i \neq j$, *and* $\sigma(e_i) = e_{i+1} \mod t$.
2. $R = R_0 \oplus \ldots \oplus R_{t-1},\ R_i = e_i R,$ *and* $\sigma(R_i) = R_{i+1} \mod t$.
3. *R_i is an integral domain and R_i is a PV extension of (k, σ^t) for some equation $\sigma^t(Y) = A_i Y, A_i \in \mathrm{GL}_n(k)$.*

Example 4.16 *Let us return to example 4.11: $R = \mathbb{C}[y, 1/y]/\langle y^2 - 1\rangle$. We have $P_1 = \langle y - 1\rangle, P_2 = \langle y+1\rangle$. We have $R = \mathbb{C}[y, 1/y]/P_1 \oplus \mathbb{C}[y, 1/y]/P_2 = R_0 \oplus R_1$. Letting $e_0 = \frac{1}{2}(y^2+y)$ and $e_1 = \frac{1}{2}(y^2 - y)$, we have $R_0 = e_0 R$ and $R_1 = e_1 R$ as in the above proposition. Note that $R \simeq \mathbb{C}[(1, -1, 1, -1, \ldots)]$ and $\mathbb{C}[(1, -1, 1, -1, \ldots)] \simeq \mathbb{C}[(1, 0, 1, 0, \ldots)] \oplus \mathbb{C}[(0, 1, 0, 1, \ldots)]$ and e_0 corresponds to $(1, 0, 1, 0, \ldots)$ and e_1 corresponds to $(0, 1, 0, 1, \ldots)$. They satisfy $\sigma^2(y) = y$.*

This completes our discussion of a synthetic approach to constructing solutions of linear difference equations. We had claimed that $\mathcal{S}_C$ is an analogue of the complex numbers. This is supported by the following result

Proposition 4.17 *(c.f., Proposition 4.1 of [27], Proposition 2.1 of [34]) Let C be an algebraically closed field and k a difference field with $C \subset k \subset \mathcal{S}_C$. If R is a PV extension of k for $\sigma(Y) = AY, A \in \mathrm{GL}_n(k)$ then there exists a k-difference isomorphism from R into $\mathcal{S}_C$. Furthermore, if $v \in \mathcal{S}_C^n$ satisfies $\sigma(v) = Av$, then, $v \in \phi(R)^n$.*

Corollary 4.18 *Let $C \subset k \subset \mathcal{S}_C$ be as above. Let $A \in \mathrm{GL}_n(k)$ and $Z \in \mathrm{GL}_n(\mathcal{S}_C)$ be such that $\sigma(Z) = AZ$. Then $k[Z, 1/\det(Z)]$ is a PV extension of k.*

Note that these results imply that there is a unique PV extension in $\mathcal{S}_C$ for any such equation.

Corollary 4.19 *Let $C \subset k \subset \mathcal{S}_C$ be as above. Assume that for $i = 1, \ldots, \ell, z_i \in \mathcal{S}_C^{n_i}$ and satisfies a difference equation $\sigma(z_i) = A_i z_i, A_i \in \mathrm{GL}_{n_1}(k)$. Then there exists a PV extension $R \subset \mathcal{S}_C$ of k with each $z_i \in R^{n_i}$.*

Proof. Let R be a PV extension of k for the difference equation $\sigma(Y) = AY$ where A is the block diagonal matrix $\mathrm{diag}(A_1, \ldots, A_\ell)$. Proposition 4.17 implies that we can assume that $R \subset \mathcal{S}_C$ and, since $\sigma(z) = Az$ for $z = (z_1, \ldots, z_\ell)^T$, we have each entry of the $z_i's$ is in R. ∎

Note that the proposition and its corollaries apply to C and $C(x)$ for any algebraically closed field C.

4.3 Applications

Definition 4.20 *Let C be a field. The* **interlacing** *$u = (u(0), u(1), \ldots)$ of sequences $v_0 = (v_0(0), v_0(0), \ldots), v_1 = (v_1(0), v_1(1), \ldots), \ldots, v_{t-1} = (v_{t-1}(0), v_{t-1}(1), \ldots) \in \mathcal{S}_C$ is the sequence*

$$(v_0(0), v_1(0), \ldots, v_{t-1}(0), v_0(1), v_1(1), \ldots, v_{t-1}(1), \ldots),$$

that is,

$$u(n) = \begin{cases} v_0(\frac{n}{t}) & \text{if } n \equiv 0 \mod t \\ v_1(\frac{n-1}{t}) & \text{if } n \equiv 1 \mod t \\ \quad \vdots & \quad \vdots \\ v_{t-1}(\frac{n-t+1}{t}) & \text{if } n \equiv t-1 \mod t \end{cases}$$

Proposition 4.21 *(Larson/Taft, [20] for the case $k = C$) Let C be an algebraically closed field and k a difference field with $C \subset k \subset \mathcal{S}_C$. Let $u, v \in \mathcal{S}_C$ each satisfy a linear difference equation over k and assume that $uv = 0$. Then there exist sequences $u_0, \ldots, u_{t-1}, v_0, \ldots, v_{t-1} \in \mathcal{S}_C$ such that*

1. *u is the interlacing of the u_i and v is the interlacing of the v_i, and*
2. *for each i either $u_i = 0$ or $v_i = 0$.*

Proof. By Corollary 4.19, we can assume that u and v belong to a PV extension R of k with $R \subset \mathcal{S}_C$. By Proposition 4.15, $R = R_0 \oplus \ldots \oplus R_{t-1}$ where $R_i = e_i R$ as in Proposition 4.15. Let $\tilde{u}_i = e_i u$ and $\tilde{v}_i = e_i v$. Note that $\tilde{u}_i \tilde{v}_i = 0$. Since R_i is an integral domain, we must have either $\tilde{u}_i = 0$ or $\tilde{v}_i = 0$. From Problem 4.2 below, we know that we can assume that each e_i is of the form $e_i(n) = 1$ if $n \equiv i \mod t$ and 0 if not . Define a sequence u_i and v_i by $u_i(j) = \tilde{u}_i(tj + i)$ and $v_i(j) = \tilde{v}_i(tj + i)$. The conclusion follows. ∎

Proposition 4.22 *(Benzaghou/Bézivin [3]) Let C be an algebraically closed field and k a difference field with $C \subset k \subset \mathcal{S}_C$. Let $u \in \mathcal{S}_C$ satisfy a linear difference equation over k and also satisfy a nonzero polynomial equation over k. Then u is the interlacing of sequences, each of which lies in a finite algebraic difference field extension of k. If $k = C(x), \sigma(x) = x + 1$, then these elements lie in $C(x)$.*

Proof. Let $R \subset \mathcal{S}_C$ be a PV extension of k containing u and let $R = \oplus_{i=0}^{t-1} R_i$ be a decomposition as in Proposition 4.15. Let $p(X) \in k[X]$ be a polynomial such that $p(u) = 0$ and let $p_i(X) = e_i p(X)$.We then have that $\tilde{u}_i = e_i u$ lies in R_i and satisfies $p_i(u_i) = 0$. Since R_i is a domain, finitely generated over k, the set of elements of R_i algebraic over k is a finite algebraic extension. Arguing as in the proof of Proposition 4.21, we create from the $\tilde{u}_i$ sequences u_i that lie in a finite algebraic extensions of k and whose interlacing yields u. The final claim follows from the fact that there are no finite algebraic difference extension fields of $(C(x), \sigma), \sigma(x) = x + 1$ (this nontrivial fact is proven in Lemma 1.19 of [27]; for a more detailed proof see Lemma A.2 of [4]). ∎

4.4 Problems

4.1 Let (k, σ) be a difference field with k^σ algebraically closed. Show that either σ is trivial or it has infinite order (i.e., $\sigma^n \neq \mathit{identity}$ for any positive integer n).

4.2 Let (R, σ) be a difference ring. Show that R^σ is a ring. If R is a simple difference ring, show that R^σ is a field.

4.2 Let $e_0, \ldots, e_{t-1} \in \mathcal{S}_C$ be elements such that $1 = e_0 + \ldots + e_{t-1}, \sigma(e_i) = e_{i+1} \mod t$ and $e_i^2 = e_i, e_i e_j = 0$ if $i \neq j$. Show that, after a possible renumbering, $e_i(n) = 1$ if $n \equiv i \mod t$ and $e_i(n) = 0$ if not .

4.4 In Proposition 4.15, each R_i is said to be a PV extension of (k, σ^t). Can you find a difference equation $\sigma^t(Y) = A_i Y$ such that R_i is the PV extension for this equation?

5 Picard-Vessiot Groups

In this section, (k, σ) is a difference field with $C = k^\sigma$ algebraically closed.

5.1 Galois Groups of PV Extensions

Definition 5.1 *Let R be a PV extension of k. The* **PV group** $\mathrm{Gal}_\sigma(R/k)$ *of R over k is*

$$\mathrm{Gal}_\sigma(R/k) = \{\phi : R \to R \mid \phi \text{ is a difference automorphism of } R \text{ and } \phi|_k = \text{ identity.}\}$$

We wish to identify a PV group with a group of matrices and show that this latter group is a linear algebraic group. We start with the following lemma.

Lemma 5.2 *Let (R, σ) be a difference ring and $A \in \mathrm{GL}_n(R)$, Let $Z_1, Z_2 \in \mathrm{GL}_n(R)$ satisfy $\sigma(Z_i) = AZ_i$ for $i = 1, 2$. Then there exists a $U \in \mathrm{GL}_n(R^\sigma)$ such that $Z_1 = Z_2 U$.*

Proof. $\sigma(Z_2^{-1} Z_1) = \sigma(Z_2)^{-1} \sigma(Z_1) = (Z_2^{-1} A^{-1})(AZ_1) = Z_2^{-1} Z_1$. Therefore, $Z_2^{-1} Z_1 = U \in \mathrm{GL}_n(R^\sigma)$. ∎

Let $R = k[Z, 1/\det(Z)]$ be a PV extension of k for $\sigma(Y) = AY$. If $\phi \in \mathrm{Gal}_\sigma(R/k)$, the PV group of R, then $\phi(Z) \in \mathrm{GL}_n(R)$ also satisfies $\sigma(Y) = AY$, so Lemma 5.2 implies that there is a matrix $[\phi]_Z \in \mathrm{GL}_n(R^\sigma) = \mathrm{GL}_n(C)$ such that

$$\phi(Z) = Z[\phi]_Z.$$

The map $\phi \mapsto [\phi]_Z$ is a group isomorphism of $\mathrm{Gal}_\sigma(R/k)$ into $\mathrm{GL}_n(C)$. Note that this map depends on our choice of Z. If W is another matrix in $\mathrm{GL}_n(R)$ such that $\sigma(W) = AW$, then $Z = WU$ for some $U \in \mathrm{GL}_n(C)$. A simple calculation shows that $[\phi]_Z = U^{-1}[\phi]_W U$. Therefore, the embedding of the PV group into $\mathrm{GL}_n(C)$ depends on a choice of basis of the solution space in R and changing the basis results in conjugating this image. Except when otherwise stated, we fix a basis of this solution space throughout, suppress the subscript in our notation and use $[\phi]$ to represent the matrix of ϕ.

Proposition 5.3 *Let R be a PV extension of k with PV group $\mathrm{Gal}_\sigma(R/k)$. The group $G = \{[\phi] \mid \phi \in \mathrm{Gal}_\sigma(R/k)\}$ is C-closed and therefore a linear algebraic group defined over C.*

Proof. For simplicity, I will assume that $n = 2$ and follow Kovacic's proof for a similar result in the differential case (c.f., [17]). Let

$$Z = \begin{pmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{pmatrix}$$

and let $R_0 = k[z_{1,1}, z_{1,2}, z_{2,1}, z_{2,2}]$. Note that $\mathrm{Gal}_\sigma(R/k)$ leaves R_0 stable. We may write $R_0 = k[Z_{1,1}, Z_{1,2}Z_{2,1}, Z_{2,2}]/I$ where the $Z_{i,j}$ are variables and I is as ideal in $k[Z_{1,1}, Z_{1,2}Z_{2,1}, Z_{2,2}]$. Any

$$g \;=\; \begin{pmatrix} a & b \\ c & c \end{pmatrix} \in \mathrm{GL}_n(C) \tag{2}$$

acts on the $Z_{i,j}$ via

$$\begin{pmatrix} Z_{1,1} & Z_{1,2} \\ Z_{2,1} & Z_{2,2} \end{pmatrix} \mapsto \begin{pmatrix} Z_{1,1} & Z_{1,2} \\ Z_{2,1} & Z_{2,2} \end{pmatrix} \begin{pmatrix} a & b \\ c & c \end{pmatrix}.$$

This matrix induces a σ-automorphism of R_0 if and only if the action takes I to itself. Let $I = \langle q_1, \ldots, q_r \rangle$ and let m be the maximum of the degrees of the p_i. Let W be the k-vector space of polynomials in $k[Z_{1,1}, Z_{1,2}Z_{2,1}, Z_{2,2}]$ of degree at most m and and let $\{p_i\}_{i\in\mathcal{I}}$ be a k-basis of $W \cap I$. Extend $\{p_i\}_{i\in\mathcal{I}}$ to a k-basis $\{p_i\}_{i\in\mathcal{J}}$ of W. For any $g \in \mathrm{GL}_n(C)$ as in equation (2) and $i \in \mathcal{J}$, we have

$$p_i(aZ_{1,1} + cZ_{1,2}, \ldots, bZ_{2,1} + dZ_{2,2}) = \sum_{j\in\mathcal{J}} P_{i,j}(a, b, c, d)p_j$$

where the $P_{i,j}$ are polynomials with coefficients in k. Therefore $g \in \mathrm{GL}_n(C)$ leaves I invariant if and only if $P_{i,j}(a, b, c, d) = 0$ for all $i \in \mathcal{I}$ and $j \in \mathcal{J}\backslash\mathcal{I}$. If $\{a_\alpha\}_{\alpha\in\mathcal{A}}$ is a C basis of k, we may write each $P_{i,j} = \sum_{i\in\mathcal{A}} a_\alpha P_{i,j,\alpha}$ for some polynomials $P_{i,j,\alpha}$ with coefficients in C. Therefore the polynomials $\{P_{i,j,\alpha} \mid i \in \mathcal{I}, j \in \mathcal{J}\backslash\mathcal{I}, \alpha \in \mathcal{A}\}$ define G. ∎

Example 5.4 *Let us once again return to example 4.11:* $\sigma(y) = (-1)y$, $R = \mathbb{C}[y, 1/y]/\langle y^2 - 1\rangle = \mathbb{C}[y]/\langle y^2 - 1\rangle$. *The PV group may be identified with a subgroup of* $\mathrm{GL}_1(\mathbb{C})$. *It is the set of* $a \in \mathbb{C}\backslash\{0\}$ *such that* $y \mapsto ay$ *leaves* $\langle y^2 - 1\rangle$ *stable. The* m *in the above proof is* 2 *and* $y^2 - 1, y, 1$ *is a basis of the space* W *polynomials of degree at most* 2 *with* $W \cap I = \{\mathbb{C} \cdot (y^2 - 1)\}$. *If* $g = (a) \in \mathrm{GL}_1(\mathbb{C})$, *then* g *takes* $Y^2 - 1$ *to* $a^2(Y^2 - 1) + (a^2 - 1) \cdot 1$, *so* $g \in G$ *if and only if* $a^2 - 1 = 0$. *Therefore* $G = \{(\pm 1)\} = \mathbb{Z}/2\mathbb{Z}$.

5.2 PV Extensions and Torsors

In Example 3.17, we showed that the Galois extension $\mathbb{Q}(\sqrt{2})$ is coordinate ring of a torsor of the Galois group $G = \{\pm 1\}$ and that the Galois action is the same as the action induced by G acting on the torsor. In general, a finite Galois extension can be shown to be the coordinate ring of a torsor of the Galois group (see Exercise A.50, p. 370 of [28]). In this section we shall discuss the fact that PV extensions are also the coordinate rings of torsors of their Galois groups.

Let k be a σ-field with constants $k^\sigma = C$ algebraically closed and let R be a PV extension of k with PV group $\mathrm{Gal}_\sigma(R/k)$. We have shown above that the map $\phi \in \mathrm{Gal}_\sigma(R/k) \mapsto [\phi] \in G \subset \mathrm{GL}_n(C)$ identifies $\mathrm{Gal}_\sigma(R/k)$ with a linear algebraic group defined over C. We will need to consider points of G from extension fields of C so we emphasize the fact that the PV group of R corresponds to the C-points of G, that is, $G(C)$.

Since $R = k[X, 1/\det X]/I$ for some ideal I, R is the k-coordinate ring of a k-closed subset V of $\mathrm{GL}_n(\bar{k})$. The linear algebraic group $G(C)$ is defined over C and acts on R as k-algebra automorphisms via the Galois action of $\mathrm{Gal}_\sigma(R/k)$. It is not hard to show that this action is induced by the action of $G(C)$ on V by right multiplication $\rho_g : v \mapsto v[g]$, that is,

$$\text{For } \phi \in \mathrm{Gal}_\sigma(R/k) \text{ and } r \in R,\ \phi(r) \ = \ \rho^*_{[\phi]}(r) \tag{3}$$

(see Section 2.3 to recall the meaning of the notation F^* for a morphism F). Since $C \subset \bar{k}$, we can speak of $G(\bar{k})$ and think of G as being defined over k. Furthermore, one can show that $\rho_g : V \to V$ even for $g \in G(\bar{k})$ and that this action turns V into a k-torsor for G. We sumarize these statements in the following result (whose statement and complete proof can be found in (p.11, [27])).

Theorem 5.5 *Let* R *be a PV extension of* k *with PV group* $\mathrm{Gal}_\sigma(R/k) \simeq G(C) \subset \mathrm{GL}_n(C)$. *Then* R *is the coordinate ring of a* k*-torsor* V *for* G. *Furthermore the Galois action of* $\phi \in \mathrm{Gal}_\sigma(R/k)$ *on* R *is given by action* $\rho^*_{[\phi]}$ *on* R *induced by the action of* $[\phi] \in G(C)$ *on* V *via right multiplication as in (3).*

When $k = C$ or $k = C(x)$, C algebraically closed and G is a connected linear algebraic group, we have already stated in Theorem 3.19 that a k-torsor for G is trivial. Using this and further arguments one can show (see Proposition 1.2 of [27]) the following (note G is not necessarily connected).

Proposition 5.6 *Let $k = C, \sigma =$ identity or $k = C(x), \sigma(x) = x + 1$ and let $R = k[Z, 1/\det(Z)]$ be a PV extension of k with PV group $\mathrm{Gal}_\sigma(R/k) = G$. Then there exists a $B \in \mathrm{GL}_n(k)$ such that $BZ \in G(k)$ and the map $Z \mapsto BZ$ yields an isomorphism of R onto $\mathcal{O}_k(G)$. Furthermore, G/G^0 is cyclic and if we write $R = \oplus_{i=0}^{t-1} R_i$ as in Proposition 4.15, then $t = |G/G^0|$ and $R_i \simeq \mathcal{O}_k(G^0)$.*

When $k = C$, we shall give a direct proof of this proposition in Section 6.1.

Example 5.7 *We continue with example 4.11: $\sigma(y) = (-1)y$, $R = \mathbb{C}[y, 1/y]/\langle y^2 - 1\rangle = \mathbb{C}[y]/\langle y^2 - 1\rangle, \mathrm{Gal}_\sigma(R/k) = \{(\pm 1)\} \simeq \mathbb{Z}/2\mathbb{Z}$. In this case $\mathcal{O}_k(G) = C[X, X^{-1}]/\langle X^2 - 1\rangle \simeq R$. Furthermore, $R = R_0 \oplus R_1$ where $R_i \simeq \mathbb{C} \simeq \mathcal{O}_{\mathbb{C}}(G^0)$, since $G^0 = \{(1)\}$.*

The previous proposition allows us to give another characterization of the PV group which we state in the following corollary. This corollary says that, under the stated hypotheses on the difference field k, the PV group of a difference equation $\sigma Y = AY, A \in \mathrm{GL}_n(k)$ is the smallest linear algebraic group H such that one can "transform" A to be in $H(k)$. An allowable transformation is of the form $A \mapsto \sigma(B)AB^{-1}$ for some $\sigma(B)AB^{-1}$. and this latter transformation corresponds to a transformation $Z \mapsto BZ$ for a fundamental solution matrix.

Corollary 5.8 *Let $k = C, \sigma =$ identity or $k = C(x), \sigma(x) = x+1$ and let $R = k[Z, 1/\det(Z)]$ be a PV extension of k for $\sigma(Y) = AY, A \in \mathrm{GL}_n(k)$ with PV group $\mathrm{Gal}_\sigma(R/k) \simeq G \in \mathrm{GL}_n(C)$. Let H be a linear algebraic group defined over C.*

1. *If $G \subset H$, then there exists a $B \in \mathrm{GL}_n(k)$ such that $\sigma(B)AB^{-1} \in H$.*
2. *If there exists a $B \in \mathrm{GL}_n(k)$ such that $\sigma(B)AB^{-1} \in H$, then $G \subset H$.*

Therefore $G \subset \mathrm{GL}_n(C)$ is the PV group of $\sigma(Z) = AZ$ if and only if for any $B \in GL_n(k)$ and any proper C-subgroup H of G, one has that $\sigma(B)AB^{-1} \notin H$

Proof. 1. From Proposition 5.6, we know there exists an element $B \in \mathrm{GL}_n(k)$ such that $BZ \in G \subset H$. Since H is defined over C and $BZ \in H$ we must have $\sigma(BZ) \in H$. Therefore $\sigma(BZ) = \sigma(B)\sigma(Z) = \sigma(B)AZ \in H$ and so $\sigma(B)AZ(BZ)^{-1} = \sigma(B)AB^{-1} \in H$

2. I start by showing that if $\sigma(Y) = \tilde{A}Y$ is a difference equation with $\tilde{A} \in H(k)$, then the PV group of this equation can be embedded in $\mathrm{GL}_n(C)$ as a subgroup of H. To see this let $J = I_k(H)$ be the ideal in $S = k[Y, 1/\det(Y)]$ of elements that vanish on H. Note that Proposition 2.28.1 implies that $J = I_C(H) \cdot k$. Extend σ to S by letting $\sigma(Y) = \tilde{A}Y$. Since $\tilde{A} \in H$, J is stable under the action of σ. Therefore there exists a maximal σ-ideal J' containing $I_C(H)$. The difference ring $S' = S/J'$ is a PV ring for $\sigma(Y) = \tilde{A}Y$ and the image U of X in this ring lies in $H(S')$. Any difference automorphism $\phi \in \mathrm{Gal}_\sigma(S')$ comes from an automorphism of S that leaves J' stable. Therefore $\phi(U) = U[\phi] \in H(S')$ and so $[\phi] = U^{-1}\phi(U) \in H(C)$.

We now return to the original equation $\sigma(Y) = AY, A \in \mathrm{GL}_n(k)$. Assume there exists

$B \in \mathrm{GL}_n(k)$ such that $\sigma(B)AB^{-1} \in H$. Let $R = k[Z, 1/\det(Z)]$ be a PV extension for $\sigma(Y) = AY$. Let $\tilde{Z} = BZ$. A calculation shows that $\tilde{Z}$ satisfies the equation $\sigma(\tilde{Z}) = (\sigma(B)AB^{-1})\tilde{Z}$. By the discussion in the previous paragraph, we have that the PV group of this equation is a subgroup of H. Clearly $k[\tilde{Z}, 1/\det(\tilde{Z})] = k[Z, 1/\det(Z)]$. For any $\phi \in \mathrm{Gal}_\sigma(R/k)$ we have that $\tilde{Z}[\phi]_{\tilde{Z}} = \phi(\tilde{Z}) = \phi(BZ) = B\phi(Z) = BZ[\phi]_Z = \tilde{Z}[\phi]_Z$. Therefore the matrix representations of an element of the PV group with respect Z and $\tilde{Z}$ are the same so $G \subset H$. ∎

5.3 Applications

We give an application of Proposition 5.6 and an application of Corollary 5.8 in this section. The following result was conjectured in [3] and proven, when $k = C$, an algebraically closed field in [2] and [20]. The result and proof appear as Proposition 3.5 of [27]. We will need the following simple lemma.

Lemma 5.9 *Let k be a difference field and T a difference ring containing k. If $u \in T$ satisfies $L(u) = a_n\sigma^n(u) + a_{n-1}\sigma^{n-1}(u) + \ldots + a_0u = 0$ with $a_i \in k$ and $a_n \neq 0$, then the set $\{\sigma^i(u) \mid i = 0, 1, \ldots\}$ spans a k-vector space of dimension at most n.*

Proof. Use the linear difference equation and induction on m to show that $\sigma^m(u)$ lies in the k-span of $u, \sigma(u), \ldots, \sigma^{n-1}(u)$ for all m. ∎

Proposition 5.10 *Let C be an algebraically closed field and $k = C, \sigma =$ identity or $k = C(x), \sigma(x) = x + 1$.If $u \in \mathcal{S}_C$ is invertible in $\mathcal{S}_C$ and u and $1/u$ satisfy linear difference equations over k, then u is the interlacing of sequences u_i such that for each i, $\sigma(u_i)/u_i \in k$.*

Proof. Corollary 4.19 implies that u and $1/u$ belong to a PV extension $R \subset \mathcal{S}_C$ of k. Let $R = \oplus_{i=0}^{t-1} R_i$ as in Proposition 4.15 and let $w_i = u \cdot e_i$. Note that each w_i is invertible in R_i. Fix a value of i, say $i = 0$. We shall show that $\sigma^t(w_0)/w_0 \in ke_0$. We shall do this in three steps.

The first step is to show that for any $\phi \in \mathrm{Gal}_{\sigma^t}(R_0/k)$, $\phi(w_0) = a_\phi w_0$. for some $a_\phi \in k$. To do this we invoke a theorem of Rosenlicht ([30], [21]): *Let G be a connected linear algebraic group defined over an algebraically closed field $\bar{k}$ and $y \in \mathcal{O}_{\bar{k}}(G)$ with $1/y \in \mathcal{O}_{\bar{k}}(G)$, then y is a $\bar{k}$ multiple of a character* (a character of a linear algebraic group is a morphism $\chi : G \to \bar{k}^*$ such that $\chi(gh) = \chi(g)\chi(h)$). Proposition 5.6 implies that $R_i \simeq \mathcal{O}_k(G^0)$, where G^0 is the identity component of the PV group of R over k. The group G^0 is defined over the algebraically closed field C and is C-irreducible. Proposition 2.28 implies that G^0 is still $\bar{k}$-irreducible and we can apply Rosenlicht's Theorem to w_0. Therefore $w_0 = r\chi$ where $r \in \bar{k}$ and $\chi \in \mathcal{O}_{\bar{k}}(G^0)$ is a character. Both r and χ have coefficients that lie in a finite normal algebraic extension $\tilde{k}$ of k. Taking the norm with respect to this extension we have $w_0 = \frac{1}{m}\mathrm{Norm}_{\tilde{k}/k}(r)\mathrm{Norm}_{\tilde{k}/k}(\chi)$ for some integer m. Note that $\mathrm{Norm}_{\tilde{k}/k}(\chi)$ is again a character. Therefore, we may abuse notation and write $w_0 = r\chi$ where $r \in k$ and $\chi \in R_0$ is a character. Recall that the action of the PV group of $R_0 = \mathcal{O}_k(G^0)$ over k is induced by

the action of the group on itself by right multiplication. Therefore for any $\phi \in \mathrm{Gal}_{\sigma^t}(R_0/k)$ and $h \in G^0$, $\phi(\chi)(h) = \chi(h \cdot [\phi]) = \chi(h)\chi([\phi]) = a_\phi \chi(h)$ where $a_\phi = \chi([\phi])$. This implies that for any $\phi \in \mathrm{Gal}_{\sigma^t}(R_0/k)$, $\phi(w_0) = a_\phi w_0$. for some $a_\phi \in k$.

The second step is to show that each of the a_ϕ are in C. Lemma 5.9 implies that for some $r \geq 0$ we have a minimal nontrivial relation of the form

$$L(w_0) = a_r \sigma^{rt}(w_0) + a_s \sigma^{st}(w_0) + \ldots + a_0 w_0 = 0$$

with $a_i \in k$ and $a_r a_s \neq 0$. Applying ϕ we have

$$\begin{aligned} L(\phi(w_0)) &= a_r \sigma^{rt}(\phi(w_0)) + a_s \sigma^{st}(\phi(w_0)) + \ldots + a_0 \phi(w_0) \\ &= a_r \sigma^{rt}(a_\phi w_0) + a_s \sigma^{st}(a_\phi w_0) + \ldots + a_0 a_\phi w_0 \\ &= a_r \sigma^{rt}(a_\phi)\sigma^{rt}(w_0) + a_s \sigma^{st}(a_\phi)\sigma^{st}(w_0) + \ldots + a_0 a_\phi w_0 \\ &= 0 \end{aligned}$$

By minimality, we must have that $\sigma^{rt}(a_\phi) = \sigma^{st}(a_\phi)$ so $\sigma^{(r-s)t}(a_\phi) = a_\phi$. This implies that a_ϕ is algebraic over $k^\sigma = C$ (see Problem 5.2 below) and, since C is algebraically closed, we have $a_\phi \in C$.

The third step is to finish by showing that $\sigma^t(w_0)/w_0 \in k$. To do this we will use Corollary 5.15 which states that an element $y \in R_0$ is in k if and only if $\phi(y) = y$ for all $\phi \in \mathrm{Gal}_{\sigma^t}(R_0/k)$. Let $\phi \in \mathrm{Gal}_{\sigma^t}(R_0/k)$. Applying ϕ to $\sigma^t(w_0)/w_0 \in k$ and using the fact that $a_\phi \in C$, a calculation shows that $\phi(\sigma^t(w_0)/w_0) = \sigma^t(w_0)/w_0$.

A similar argument shows that for each i, we have $\sigma^t(w_i)/w_i = f_i \in ke_i$. Let u_i be the sequence defined by $u_i(n) = w_i(tn + i)$. One sees that $\sigma(u_i)/u_i = v_i$ where $v_i(n) = f(tn + i) \in k$ and that u is an interlacing of $u_0, \ldots, u_{t-1}$. ∎

As another application we will discuss first order difference equations over $C(x), \sigma(x) = x + 1$, that is, difference equations of the form

$$y(x + 1) = a(x)y(x). \tag{4}$$

The PV group of such an equation must be $\mathrm{GL}_1(C)$ or $\{(a) \mid a^n - 1 = 0\} \simeq \mathbb{Z}/n\mathbb{Z}$. Corollary 5.8 implies that if the PV group is a subgroup of $\mathbb{Z}/n\mathbb{Z}$ then there exists an $f \in C(x)^*$ such that $f(x + 1)a(x)(f(x))^{-1} = \omega$ where $\omega^n = 1$, that is

$$a(x) = \omega \frac{f(x)}{f(x + 1)}.$$

Example 5.11 *Consider the equation $y(x + 1) = xy(x)$. I will show that the PV group of this equation is $\mathrm{GL}_1(C)$. To do this I will show that we cannot write x as $\omega f(x)/f(x + 1)$*

for any $f(x) \in C(x)$. Assume we could. We then would have

$$\begin{aligned} \frac{1}{x} &= \frac{x'}{x} \\ &= \frac{(\omega \frac{f(x)}{f(x+1)})'}{\omega \frac{f(x)}{f(x+1)}} \\ &= \frac{f'(x)}{f(x)} - \frac{f'(x+1)}{f(x+1)} \end{aligned}$$

where $'$ denotes the derivative with respect x. We would therefore have

$$\frac{1}{x} = g(x) - g(x+1) \text{ for some } g(x) \in C(x).$$

Since $\frac{1}{x}$ has a pole at 0, we must have that g has at least one pole. Let $\alpha_1, \ldots, \alpha_r$ be the poles of g ordered so that g has no poles of the form $\alpha_1 - n$ or $\alpha_r + n$ for any positive integer n. The function $g(x+1)$ therefore has a pole at $\alpha_1 - 1$ and at $\alpha_r - 1$ but no pole at α_r (otherwise g would have a pole at $\alpha_r + 1$). Therefore the pole of g at α_r and the pole of $g(x+1)$ at $\alpha_1 - 1$ persist in the expression $g(x) - g(x+1)$. Since $\frac{1}{x}$ has only one pole this is a contradiction.

One can use this fact to show that the Gamma Function $\Gamma(x)$ is not algebraic over $\mathbb{C}(x)$. If the Gamma Function were algebraic over $\mathbb{C}(x)$, the sequence $\Gamma = (\Gamma(1), \ldots, \Gamma(n), \ldots) = (1, 1, \ldots, (n-1)!, \ldots) \in \mathcal{S}_{\mathbb{C}}$ whould be algebraic over $\mathbb{C}(x) \subset \mathcal{S}_{\mathbb{C}}$. $y = \Gamma$ satisfies $y(x+1) = xy(x)$ so Corollary 4.19 implies that $R = \mathbb{C}(x)[\Gamma, 1/\Gamma]$ is a PV extension for this equation. Since the PV group of this equation is $\mathrm{GL}_1(\mathbb{C})$ we have $R = \mathcal{O}_{\mathbb{C}(x)}(\mathrm{GL}_1) = \mathbb{C}(x)[Y, 1/Y]$, where Y is a variable. It is clear that any element of this latter ring algebraic over $\mathbb{C}(x)$ is in $\mathbb{C}(x)$.

A complete analysis of first order difference equations is given in Section 2.1 of [27].

5.4 Galois Correspondence

In the proof of Proposition 5.10, we used the fact that an element of a PV extension that is left fixed by the Galois group must lie in the base field. This is a key feature of the Galois correspondence and will be used again in Section 6.1. In this section we will describe the full Galois correspondence.

In the usual Galois theory of polynomial equations, there is a correspondence between subgroups of the Galois group and subfields of the splitting field. We shall derive the corresponding result in our context. One would hope for a correspondence between subgroups of the PV group and difference subrings of the associated PV ring but this is not true even when one restricts to *closed* subgroups of the PV group (see p.16 of [27]). Such a correspondence does exist if we replace R by a suitable "quotient field".

Definition 5.12 *Let R be a commutative ring and let $S = \{s \in R \,|\, s \text{ is not a zero divisor in } R\}$. On $R \times S$ define an equivalence relation $(r_1, s_1) \sim (r_2, s_2)$ if $r_1 s_2 - r_2 s_1 = 0$. Let $Q(R)$ denote the ring of equivalence classes where the ring operations are defined by $(r_1, s_1) + (r_2, s_2) := (r_1 s_2 + r_2 s_1, s_1 s_2)$ and $(r_1, s_1)(r_2, s_2) := (r_1 r_2, s_1, s_2)$. The ring* $\mathbf{Q(R)}$ *is called the* **total quotient ring** *of R*

Several properties of $Q(R)$ are developed in the Problems. If (R, σ) is a difference ring then we can make $Q(R)$ into a difference ring by defining $\sigma((r, s)) = (\sigma(r), \sigma(s))$.

Definition 5.13 *Let (k, σ) be a difference field. A* **total PV ring** *of k is the total quotient ring $Q(R)$ of a PV extension R of k.*

Note that if G is the PV group of a PV ring R then G acts as difference automorphisms of $Q(R)$.

Theorem 5.14 *(Fundamental Theorem of PV Theory) Let (k, σ) be a difference field with $k^\sigma = C$ algebraically closed. Let R be a PV extension of k and $K = Q(R)$ the associated total PV ring. Let G be the PV group of R over k and let*

$\mathcal{F} = \{F \mid F \text{ is a difference ring, } k \subset F \subset K, \text{ and every non-zerodivisor of } F \text{ is invertible.}\}$

$\mathcal{G} = \{H \mid H \text{ is a } C\text{-closed subgroup of } G\}$

For any $F \in \mathcal{F}$, let $G(K/F) = \{\phi \in G \mid \phi|_F = \text{identity}\}$ and for any $H \in \mathcal{G}$, let $K^H = \{a \in K \,|\phi(a) = a \text{ for all } \phi \in H\}$. Then

1. *for an $F \in \mathcal{F}$, $G(K/F) \in \mathcal{G}$,*
2. *for an $H \in \mathcal{G}$, $K^H \in \mathcal{F}$, and*
3. *the maps $\alpha : \mathcal{F} \to \mathcal{G}, \alpha(F) = G(K/F)$ and $\beta : \mathcal{G} \to \mathcal{F}, \beta(H) = K^H$ are inverses of each other.*

Furthermore, if $H \in \mathcal{G}$ is a normal subgroup of G then $\mathrm{Gal}_\sigma(K^H/k) \simeq G/H$.

Proof. The proof is given in Section 1.3 of [27] and uses the fact that a PV ring is the coordinate ring for a k-torsor of its PV group. ∎

Corollary 5.15 *Let k, R, K, G be as above. If $a \in K$ is left fixed by all elements of G, then $a \in k$.*

Proof. Since α and β are inverses of each other and $\alpha(k) = G$, we have $\beta(G) = L^G = k$. ∎

In the following examples, k is a difference field with k^σ algebraically closed.

Example 5.16 *Let $\sigma(u) = ay,\ a \in k$ be a first order equation with PV group $\mathbf{G_m}$ (eg, Example 5.11). In this case the PV ring is $k[z, 1/z]$ where z is transcendental over k and $\sigma(z) = az$. The total quotient ring is $k(z)$. The proper algebraic subgroups of $\mathbf{G_m}$ are of the form $H_n = \{\zeta \in k^\sigma \mid \zeta^n = 1\}$. The fixed field of H_n is $k(z^n)$. Since $\mathbf{G_m}$ is commutative all subgroups are normal so the Galois group of $k(z^n)$ over k is isomorphic to $\mathbf{G_m}/H_n$ which is isomorphic to $\mathbf{G_m}$.*

Example 5.17 *Let ζ be a primitive n^{th} root of unity and consider the equation $\sigma(y) = \zeta y$. As in Example 4.11, one can show that the ring $R = k[y, 1/y]/(y^n - 1)$ is the PV ring for this equation. We have that $R = \oplus_{i=0}^{n-1} R_i$ where $R_i \simeq k$. Furthermore, simple calculations show*

1. *The PV Galois group G of R over k is $\mathbb{Z}/n\mathbb{Z} \subset \mathbf{G_m}$.*
2. *If we write $R_i = Re_i$ as in Proposition 4.15, then*

$$z = e_0 + \zeta e_1 + \ldots + \zeta^{n-1} e_{n-1}$$

   satisfies $\sigma(z) = \zeta z$.

3. *If ϕ is an automorphism that generates of G, the $\phi(z) = \zeta z$ so we must have $\phi(e_i) = e_{i+1 \mod n}$.*
4. *The total quotient ring K of R is R.*
5. *If H is a subgroup of G, then H is again cyclic and generated by ϕ^m for some m dividing n. In this case*

$$K^H = \oplus_{i=0}^{n/m-1} Rf_i \quad \textit{where} \quad f_i = \sum_{j=0}^{m-1} e_{i+j}.$$

6. *Since G is abelian each K^H is again a total PV ring. In fact K^H is the total PV ring for $\sigma(y) = \zeta^{n/m}$ and*

$$u = f_0 + \zeta^{n/m} f_1 + \ldots + \zeta^{(m-1)n/m} f_{m-1} \in K^H$$

   is a solution of this equation.

5.5 Problems

5.1 Let R be a PV extension of a difference field k and $e_0, \ldots, e_{t-1} \in R$ as in Proposition 4.15. Let $\phi \in \mathrm{Gal}_\sigma(R/k)$. Show that ϕ permutes the $e_0, \ldots, e_{t-1}$.

5.2 Let (k, σ) be a difference field and $u \in k$. Show that if $\sigma^s(u) = u$ for some $s \geq 1$, then u is algebraic over k^σ. Hint: The orbit of u under σ is finite. What can you say about the symmetric functions of this orbit?

5.3 Let R be a commutative ring.
(i) Show that any non-zerodivisor is invertible in $Q(R)$.
(ii) Show that the map $r \mapsto (r, 1)$ is an embedding of R into $Q(R)$.

5.4 Let (R, σ) be a simple difference ring and $Q(R)$ its total quotient ring. Show that $Q(R)^\sigma \subset R$ and so $Q(R)^\sigma = R^\sigma$.

5.5 Let R be a PV extension of a difference field k and write $R = \oplus_{i=1}^{t-1} R_i$ as in Proposition 4.15. Show that $Q(R) = \oplus_{i=0}^{t-1} Q(R_i)$.

6 Computational Questions

6.1 Calculating PV groups and Algebraic Relations Among Solutions of Linear Difference Equations

In this section, we consider two questions:

- Given a linear difference equation, can one calculate its PV group?
- Given a linear difference equation, can one calculate the algebraic relations among its solutions?

We note that the first question has been recently answered positively for linear difference equations over $\overline{\mathbb{Q}}(x)$ by Ruyong Feng [10]. I will not discuss his solution but rather discuss these questions for linear difference equations over a constant difference field and then discuss how these questions are algorithmically related.

We begin by considering these questions for equations with constant coefficients, that is, linear difference equations over the difference field (C, σ) where C is an algebraically closed field (in which we can effectively do the algebraic operations and factor polynomials) and $\sigma =$ identity.

Let

$$\sigma(Y) \;=\; AY \tag{5}$$

be a linear difference equation over C, where $A \in \mathrm{GL}_n(C)$. We shall construct a matrix $Z \in \mathrm{GL}_n(\mathcal{S}_C)$ such that $\sigma(Z) = AZ$ but before we do, we will make some remarks about matrices with entries in $\mathcal{S}_C$. We can identify such a matrix with a sequence of matrices $((z_{i,j}(0)), (z_{i,j}(1)), \ldots, (z_{i,j}(m)), \ldots)$. Conversely, one can identify a sequence of matrices with entries in C with a matrix with entries in $\mathcal{S}_C$, that is the matrix whose i, j entry is the sequence of i, j entries of the sequence of matrices. It will be convenient to frequently go back and forth between these two representations. Note that $(z_{i,j}) \in \mathrm{GL}_n(\mathcal{S}_C)$ if and only if $\det(z_{i,j}(m)) \neq 0$ for $m >> 0$.

Let I_n be the $n \times n$ identity matrix. I now claim that the sequence of matrices

$$Z = (I_n, A, A^2, \ldots)$$

(or the matrix of sequences associated to this) satisfies $\sigma(Z) = AZ$. This follows from the fact that $\sigma((I_n, A, A^2, \ldots)) = (A, A^2, \ldots) = A(I_n, A, A^2, \ldots)$. Corollary 4.19 implies that $R = C[Z, 1/\det(Z)]$ is the PV extension of C for equation (5).

I now describe the PV group G of this equation. First note that the automorphism σ of R is in G. This is because σ is an automorphism that is the identity on C (here we use the assumption from the beginning that σ is trivial on C) and σ obviously commutes with σ.

Now let us compute $[\sigma]_Z$. We have

$$\sigma(Z) = AZ = A(I_n, A, A^2, A^3, \cdots) = (A, A^2, A^3, \ldots) = ZA$$

so

$$[\sigma]_Z = A.$$

I now claim that G is the Zariski closure of the group generated by A, that is, $G = \overline{\langle A \rangle}$. First note that the set of elements in $Q(R)$ left fixed by A is precisely the constants C. The same therefore holds for $\langle A \rangle$ and therefore for $\overline{\langle A \rangle}$. Therefore the Galois correspondence tells us that $G = \overline{\langle A \rangle}$.

The PV ring $R = C[Z, 1/\det(Z)]$ may be written as $R = C[Y, 1/\det(Y)]/J$ where Y is an $n \times n$ matrix of variables and J is a maximal σ-ideal. We now describe J. We have

$$\begin{aligned} J &= \{P \in C[Y, 1/\det(Y)] \mid P(Z, 1/\det(Z)) = 0\} \\ &= \{P \in C[Y, 1/\det(Y)] \mid P((I_n, A, A^2, \ldots)) = 0\} \\ &= \{P \in C[Y, 1/\det(Y)] \mid (P(I_n), P(A), P(A^2), \ldots)) = 0\} \\ &= \{P \in C[Y, 1/\det(Y)] \mid P(A^m) = 0 \text{ for } m \geq 0\} \end{aligned}$$

Therefore $V(J)$ is the Zariski closure of $\{A^m \mid m \geq 0\}$. Since this latter set is closed under multiplication and contains I_n, $V(J)$ is a linear algebraic group (cf. Problem 3.4). It therefore is the Zariski closure of $\langle A \rangle$. Since J is radical, we have that J is the defining ideal of G. Note that J is the ideal of relations among the entries of Z and $1/\det(Z)$ so $J \cap C[Y]$ is the ideal of relations among the entries of Z. We therefore have

Proposition 6.1 *Let C be an algebraically closed field and $A \in \mathrm{GL}_n(C)$. Let $Z \in \mathrm{GL}_n(\mathcal{S}_C)$ satisfy $Z(0) = I_n$ and $\sigma(Z) = AZ$. Let R be the associated PV extension of C and G be the image of $\mathrm{Gal}_\sigma(R/C)$ in $\mathrm{GL}_n(C)$ with respect to Z.*

1. *G is the Zariski closure of the group generated by A.*
2. *If $R = C[Z, 1/det(Z)] = C[Y, 1/\det(Y)/J$, then $J = I_C(G)$.*

In particular, the ideal of algebraic relations among the entries of Z comes from $I_C(G)$. This leads to the following algorithm. Note that any $U(0) \in \mathrm{GL}_n(C)$ determines a unique solution $U = (U(0), AU(0), A^2U(0), \ldots) \in \mathrm{GL}_n(\mathcal{C}_S)$ of $\sigma(Y) = AY$.

Input: $A, U(0) \in \mathrm{GL}_n(C)$.
Output: A basis of $I = \{P \in C[X, 1/\det(X) \mid P(U) = 0\}$.

Step1: Use the algorithm of [7] to find a basis of $J = I_C(\overline{\langle A \rangle})$. This later algorithm will find the defining ideal of the Zariski closure of a group generated by a finite set of matrices.

Step 2: Let I be the ideal one gets when one replaces $X = (X_{i,j})$ with $XU(0)^{-1}$ in the polynomials in J.

Since J is the defining ideal of Z, one sees that I is the defining ideal of J.

Example 6.2 *Let us find the ideal of relations among the Fibonacci numbers $F = (0, 1, 1, 2, 3, 5, \ldots)$. We let $C = \mathbb{C}$. Note that F satisfies $\sigma^2(F) - \sigma(F) - F = 0$. The associated matrix equation is*

$$\sigma \begin{pmatrix} F \\ \sigma(F) \end{pmatrix} = A \begin{pmatrix} F \\ \sigma(F) \end{pmatrix} \text{ where } A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

For our matrix U we will take

$$U = \begin{pmatrix} F & \sigma(F) \\ \sigma(F) & \sigma^2(F) \end{pmatrix} \text{ where } U(0) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

The fact that $A = U(0)$ in this example is a coincidence. We now wish to find the Zariski closure of the group generated by A. We note that $A = QBQ^{-1}$ where

$$Q = \begin{pmatrix} \frac{1}{2} + \frac{1}{10}\sqrt{5} & \frac{1}{2} - \frac{1}{10}\sqrt{5} \\ -\frac{\sqrt{5}}{5} & \frac{\sqrt{5}}{5} \end{pmatrix} \text{ and } B = \begin{pmatrix} \frac{1}{2} - \frac{1}{2}\sqrt{5} & 0 \\ 0 & \frac{1}{2} + \frac{1}{2}\sqrt{5} \end{pmatrix}.$$

Therefore, to find the defining ideal J of $\overline{\langle A \rangle}$, it suffices to find the defining ideal of $\overline{\langle B \rangle}$ and then make a change of variables. The entries of B satisfy $X_{2,1} = X_{1,2} = (X_{1,1}X_{2,2})^2 - 1 = 0$. The algorithm of [7] verifies that these are the only relations among the entries of the elements of $\overline{\langle B \rangle}$ and so form a basis for the defining ideal of this group . The substitution $(Y_{i,j}) := Q^{-1}(X_{i,j})Q$ yields a basis of the ideal J of $\overline{\langle A \rangle}$ (you can use MAPLE *to find these equations; they are not complicated, just unpleasant to view).*

One now makes the substitution $(X_{i,j}) := (Y_{i,j})U(0)^{-1}$ to find the ideal I above. The result is

$$I = \langle Y_{1,2} - Y_{2,1}, Y_{2,2} - Y_{1,2} - Y_{1,1}, (Y_{1,1}Y_{2,2} - Y_{1,2}^2)^2 - 1 \rangle.$$

This gives a basis of the algebraic relations among the entries of U and implies that ALL algebraic relations among $F(n), F(n+1), F(n+2)$ are a result of

$$F(n+2) - F(n+1) - F(n) = 0 \text{ and } (F(n)F(n+2) - F(n+1)^2)^2 = 1.$$

Example 6.3 *We can also calculate the relations among solutions of several difference equations. For example, consider the sequence of Fibonacci numbers $F = (F(n))$ and the sequence $S(n) = (-1)^n$. In matrix terms, one has the following difference equation*

$$\sigma \begin{pmatrix} F \\ \sigma(F) \\ S \end{pmatrix} = A \begin{pmatrix} F \\ \sigma(F) \\ S \end{pmatrix} \text{ where } A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

For our matrix U we take

$$U = \begin{pmatrix} F & \sigma(F) & 0 \\ \sigma(F) & \sigma^2(F) & 0 \\ 0 & 0 & S \end{pmatrix} \text{ and } U(0) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

The matrix A is conjugate to B, where

$$B = \begin{pmatrix} \frac{1}{2} - \frac{1}{2}\sqrt{5} & 0 & 0 \\ 0 & \frac{1}{2} + \frac{1}{2}\sqrt{5} & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

and the defining ideal of $\overline{\langle B \rangle}$ is generated by

$$\{X_{1,2}, X_{1,3}, X_{2,1}, X_{2,3}, X_{3,1}, X_{3,2}, (X_{1,1}X_{2,2})^2 - 1, X_{3,3}^2 - 1\}.$$

Proceeding as above we get that the ideal of relations among $F(n), F(n+1), F(n+2)$ and $(-1)^n$ is generated by

$$F(n+1) - F(n+1) - F(n) \text{ and } F(n)F(n+2) - F(n+1)^2 - (-1)^n.$$

The equation $F(n)F(n+2) - F(n+1)^2 = (-1)^n$ is known as Cassini's Identity.

We note that Kauers and Zimmerman [15] also gave an algorithm to calculate the ideal of relations among the solutions of a linear difference equation with constant coefficients. Their algorithm is based on the fact that one can explicitly write down solutions of such an equation. The calculations involved in their algorithm and the algorithm for computing the Zariski closure of finitely generated matrix groups in [7] are very similar. The advantage of the above algorithm is that the general philosophy can possibly yield an algorithm for linear difference equations over other fields. We describe this approach now. We begin by formally restating the two questions posed at the beginning of this section and will show how they are related.

Let C be as above and $(C(x), \sigma)$ be a difference field with C as above and $\sigma(x) = x + 1$. Let $A \in \mathrm{GL}_n(C(x))$ and assume the entries of A are defined and $\det(A) \neq 0$ for all $x \geq N$. Given some $Z_N \in \mathrm{GL}_n(C)$, on can define a solution $Z \in \mathrm{GL}_n(\mathcal{S}_C)$ of $\sigma(Y) = AY$ as follows. Let $Z(i) = 0$ for $i < N$, $Z(N) = Z_N$ and for $i > 0$ define $Z(N + i)$ inductively as

$Z(N+i) = A(N+i-1)Z(N+i-1)$. Note that any other solutions of $\sigma(Y) = AY$ such that $Y(N) = Z_N$ satisfies $Y(N+i) = Z(N+i)$ for all $i > 0$. Consider the following two problems:

Problem 1: Given $Z_N \in \mathrm{GL}_n(C)$, let Z be the solution of $\sigma Y = AY$ with $Z(N) = Z_N$. Find the defining ideal I of the matrix representation (with respect to Z) of the PV group of this equation.

Problem 2: For Z as in Problem 1, find a basis of the ideal J of algebraic relations among the entries of Z.

Proposition 6.4 *There is a recursive procedure to reduce Problem 1 to Problem 2 and vice versa.*

Proof. Assume we can solve Problem 2. The PV group of the difference equation is represented by the group

$$G = \{g \in \mathrm{GL}_n(C) \mid \text{ the map } X \mapsto Xg \text{ leaves the ideal } J \text{ stable.}\}$$

Elimination (using Gröbner basis techniques [5] for example) allows one to find a basis for the ideal I defining G.

Assume we can solve Problem 1 and can find a basis of $I \subset C(x)[X, 1/\det(X)]$. We know there exists a $B \in \mathrm{GL}_n(C(x))$ such that $\sigma(B)AB^{-1} \in G(C(x)) = V(I)$. Since $C(x)$ is countable we can find such a B by, at worst listing all possibilities and checking the condition $\sigma(B)AB^{-1} \in G(C(x))$. Once we have found one B, replacing X in the polynomials of I by BY will yield the ideal J. ∎

The effective method that allows one to go from a solution of Problem 1 to Problem 2 is certainly not efficient but at least one sees the connection between the two problems; it would be interesting to find a more efficient method. For difference equations of order at most 2, Problem 1 has been solved by Hendriks in [12] and, as mentioned above, in general by Feng [10].

6.2 Liouvillian Sequences

In this section we will discuss the problem of expressing sequences in "closed form". Recall that we call a polynomial equation solvable if the roots can be expressed in terms of radicals. To be more precise, let $p(X) \in k[X], k$ a field. One says that $p(X)$ is *solvable in terms of radicals* if its splitting field K lies in a tower of fields $k = K_0 \subset K_1 \subset \ldots \subset K_m, K \subset K_m$ where for each i, $K_{i+1} = K_i(\zeta_i), \zeta_i^{n_i} \in K_i$. A classical result is that $p(X)$ is solvable in terms of radicals if and only if its Galois group is solvable.

One has a corresponding result for linear differential equations. If k is a differential field and $L(y) = 0$ is a linear differential equation of order n with coefficients in k, one says that

$L(y) = 0$ *is solvable in terms of liouvillian functions* if $L(y) = 0$ has n solutions, linearly independent over constants, that lie in a tower of differential fields $k = K_0 \subset K_1 \subset \ldots \subset K_n$ where for each i, $K_{i+1} = K_i(\zeta_i)$ and either

1. $\zeta_i' \in K_i$ (*i.e.* $\zeta_i = \int \eta_i, \eta_i \in K_i$), or
2. $\zeta_i'/\zeta_i \in K_i$ (*i.e.* $\zeta_i = exp(\int \eta_i), \eta_i \in K_i$), or
3. ζ_i is algebraic over K_i.

There is a Galois theory for linear differential equations that associates a linear algebraic group to such an equation [6],[16],[22],[28]. One knows that $L(y) = 0$ is solvable if and only the identity component if its Galois group is solvable.

Turning to linear difference equations, what corresponds to integrals and exponentiation? The following table gives an answer

Differential Equations	Difference Equations
meromorphic functions $y(x)$	sequences $y = (y(0), y(1), \ldots)$
integrals $z = \int y(x) \Leftrightarrow z' = a$	sums $z(n) = \sum_{i=0}^{n-1} y(i) \Leftrightarrow \sigma(z) - z = y$
exponentials $z = \exp(\int y(x)) \Leftrightarrow z' = yz$	products $z(n) = \prod_{i=0}^{n-1} y(i) \Leftrightarrow \sigma(z) = yz$
algebraic functions	interlacing

All of this motivates the following definition

Definition 6.5 *The* **Ring of Liouvillian Sequences** $\mathcal{LS}$ *in* $\mathcal{S}$ *is the smallest subring of* $\mathcal{S}_C$ *satisfying*

1. $C(x) \subset \mathcal{LS}$,
2. $a \in \mathcal{LS} \Leftrightarrow \sigma(a) \in \mathcal{LS}$,
3. *if* $a \in C(x)$ *and* $b \in \mathcal{S}$ *satisfies* $\sigma(b) = ab$ *then* $b \in \mathcal{LS}$,
4. *if* $a \in \mathcal{LS}$ *and* $b \in \mathcal{S}$ *satisfies* $\sigma(b) - b = a$, *then* $b \in \mathcal{LS}$, *and*
5. *if* $a_1, \ldots, a_m \in \mathcal{LS}$ *then the interlacing of these sequences is in* $\mathcal{LS}$.

Examples 6.6 *1) Example 2 of the introduction is an example of a linear difference equation all of whose solutions lie in* $\mathcal{LS}$

2) The solution

$$u(n) = \begin{cases} n & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}.$$

of

$$(n^2+n-1)u(n+2)+2u(n+1)-(n^2+3n+1)u(n)=0$$

is an example of an interlacing of rational sequences and lies in $\mathcal{LS}$.

3) (Example 1, p. 457, [12]) The solutions of

$$a(n+2)+na(n+1)+na(n)=0.$$

are of the form

$$\begin{aligned} a(n) &= c_1u(n)+c_2v(n),\ \textit{where } c_1 \textit{ and } c_2 \textit{ are constants and} \\ u(n) &= (-1)^n(n-2) \\ v(n) &= (-1)^n\left(\frac{-(n-1)!}{n-2}+(n-2)\sum_{k=3}^{n-1}(k-1)!\frac{k^3-6k^2+9k-3}{(k-1)^2(k-2)^2}\right) \end{aligned}$$

and so lie in $\mathcal{LS}$.

This definition is the definition given in [13]. One would like to replace the phrase "$a \in C(x)$" in condition 3 of the above definition with the phrase "$a \in \mathcal{LS}$". This former phrase was needed because the Galois theory used to prove the results below in [13] (and the one developed in [27]) is a Galois theory of difference equations *over difference fields*. Presumably the Galois theory of difference equations over difference rings developed in [1] and [36] allows one to use the stronger phrase. Nonetheless, one has the following results.

Theorem 6.7 *[13] Let* $a \in \mathcal{S}_C$. *The element* $a \in \mathcal{LS}$ *if and only if* a *satisfies a linear difference equation over* $C(x)$ *whose PV group is solvable.*

Note that Proposition 5.6 states that if G is a PV group over $C(x)$, then G/G^0 is cyclic so G is solvable if and only if G^0 is solvable. For the next result we need a definition

Definition 6.8 *An invertible sequence* $y \in \mathcal{S}_C$ *is said to be* **hypergeometric** *if* $\sigma(y)=ay$ *for some* $a \in C(x)$

Theorem 6.9 *[13] Let* $L(y)=0$ *be a linear difference equation of order* n *with coefficients in* $C(x)$. *Then* $L(y)=0$ *has a solution in* $\mathcal{LS}$ *if and only if* $L(y)=0$ *has a solution in* $\mathcal{S}$ *that is the interlacing of* m *hypergeometric sequences, where* $1 \leq m \leq n$.

Proof. I will only give a brief outline of the proof of this result; just enough to show where the Lie-Kolchin Theorem is used. Assume that $L(y)=0$ has a solution a in $\mathcal{LS}$. By Theorem 6.7 one knows that a satisfies a linear difference equation whose PV group is solvable. As a first step, it can be shown that one can reduce to the case where the PV group G of $L(y)$ is solvable. Next, let R be the associated PV extension and write $R=\oplus_{i=0}^{t-1}R_i=e_iR$ as in Proposition 5.6. Let $K=Q(R)=\oplus_{i=0}^{t-1}Q(R_i)$. One can show that $K^{G^0}=\oplus_{i=0}^{t-1}e_iC(x)$.

We now apply the Lie-Kolchin Theorem, Theorem 3.12. This theorem asserts that one can conjugate the group G^0 so that all its elements are in upper triangular form. In particular, there exists a solution v of $L(y) = 0$ such that for each $\phi \in G^0$ there exists a $c_\phi \in C$ such that $\phi(v) = c_\phi v$. Let $v_i = e_i v$. I will show that each v_i is hypergeometric with respect to σ^t. If $v_i = 0$, v_i is clearly hypergeometric. Assume $v_i \neq 0$. Since R_i is a domain, v_i is invertible in $Q(R_i)$. A calculation shows that $\sigma^t(v_i)/v_i$ is left fixed by every element of G^0 and so lies in $e_i C(x)$.

Define new sequences u_i by $u_i(n) = v_i(tn + i)$. For each v_i there exists an $f_i \in C(x)$ such that $\sigma^t(v_i) = f_i v_i$. Let $g_i(x) = f_i(tx+i)$. We then have $\sigma(u_i) = g_i u_i$ and v is the interlacing of the t hypergeometric u_i.

The value of t we have found in the above argument may be large and lie outside the bounds claimed by the Theorem. Nonetheless, a refinement of the above argument allows one to produce m hypergeometric sequences, where $1 \leq m \leq n$ such that v is the interlacing of these sequences. I refer to [13] for the details. ∎

The above theorem allows us to give a procedure to decide if a linear difference equation $L(y) = 0$ of order n has solutions in $\mathcal{LS}$. For each $m, 1 \leq m \leq n$ one proceeds as follows.

1. Construct linear difference equations $L_{m,i}(y) = 0, i = 0, \ldots, m-1$, with the property that if z is a solution of $L(y) = 0$ and is an interlacing of m sequences $z_0, \ldots, z_{m-1}$ then each z_i satisfies $L_{m,i}(z_i) = 0$. One does this by using $L(y) = 0$ to write each $\sigma^{im}(y)$, $i = 0, \ldots n$ as a $C(x)$-linear combination of $\sigma^j(y), j = 0, \ldots, n-1$ and then using elimination to get a $C(x)$-linear combination of the $\sigma^{im}(y)$, $i = 0, \ldots n$ that equals zero. One then has an operator $P(\sigma)$ of order at most n such that $P(\sigma^m)(y) = 0$ for any solution y of $L(y) = 0$. For each $i = 0, \ldots, m$, replace x by $mx + i$ in the coefficients of $P(\sigma)$ yielding an operator $L_{m,i}(\sigma)$. The equations $L_{m,i}(\sigma)(y) = 0$ have the desired properties.

   Example 6.10 *Let $L(y) = \sigma^2(y) - (x+1)y$ and $m = 2$. In this case the first step is rather trivial since the original equation already gives a relation between $\sigma^2(y)$ and y. Therefore $P(\sigma) = \sigma - (x+1)$. One then has that*

$$\begin{aligned} L_{2,0}(y) &= \sigma(y) - (2x+1)y \\ L_{2,1}(y) &= \sigma(y) - (2x+2)y. \end{aligned}$$

   Note that the sequence $(1, 1, 1, 2, 3, 4 \cdot 2, 5 \cdot 3, 6 \cdot 4 \cdot 3, \ldots)$ satisfies $L(y) = 0$ while the sequence $(1, 1, 3, 3 \cdot 5, \ldots)$ satisfies $L_{2,0}(y) = 0$ and the sequence $(1, 2, 4 \cdot 2, 6 \cdot 4 \cdot 2, \ldots)$ satisfies $L_{2,1}(y) = 0$.

2. Use the algorithm of Petkovsek ([25, 26]) to find all hypergeometric solutions of the $L_{m,i}(y) = 0$ and test whether interlacings of m of these satisfy $L(y) = 0$.

Using this and a variation of parameters argument, one can find a C-basis of $L(y) = 0$ (see Lemma 5.4, [13]).

I will not describe more fully the above algorithm here but refer the reader to [13]. Suffice it to say that it depends heavily on a procedure originally due to Petkovsek ([25, 26]) which, given a linear differential equation $L(y)$ over $C(x)$, finds all hypergeometric solutions of $L(y) = 0$. I will describe this latter algorithm in the context of second order equations and closely follow the presentation given in [12] and sketched in ([27], Chapter 2.3). A key idea in this algorithm is to reduce this question to questions of a local nature, that is, behavior at a point. When considering the field $C(x)$, the function field of the sphere $\mathbb{P}^1(C)$, with the shift $\sigma(x) = x + 1$, the only point that is left fixed is the point at infinity. We will therefore consider the field of Laurent series $C((z))$ where $z = 1/x$. Note that σ acts on this field via $\sigma(z) = \frac{z}{1+z}$.

Consider a second order linear difference equation

$$\sigma^2(y) + a\sigma(y) + by \;\; = \;\; 0, \;\; a, b \in C(x). \tag{6}$$

If y is a putative hypergeometric solution satisfying $\sigma(y) = uy$, then substitution shows that u satisfies the associated Riccati equation

$$u\sigma(u) + au + b \;\; = \;\; 0. \tag{7}$$

We wish to determine possible $u \in C(x)$ that satisfy this latter equation. Our first step is to determine the possible initial terms of the expansion of u in $C((z))$, where $z = \frac{1}{x}$. In [12], the author shows that the first two terms will suffice for later computations and that there are only finitely many possibilities for these.

Example 6.11 *We will consider the equation presented in the second example of the Introduction.*

$$L(y) = y(x+2) - (2x+5)y(x+1) + (2x+2)y(x) \;\; = \;\; 0 \tag{8}$$

whose associated Riccati equation is

$$u\sigma(u) - (2x+5)u + 2x + 2 = 0.$$

If we write $u = a_n z^n + a_{n+1} z^{n+1} + \text{h.o.t}$, *were* h.o.t *means "higher order terms", we then have*

$$\begin{aligned} &(a_n z^n + a_{n+1} z^{n+1} + \text{h.o.t})(a_n z^n + (a_{n+1} - n a_n) z^{n+1} + \text{h.o.t}) \\ &-(\frac{2}{z} + 5)(a_n z^n + a_{n+1} z^{n+1} + \text{h.o.t}) + \frac{2}{z} + 2 = 0 \end{aligned}$$

The terms of lowest order must cancel so either $n - 1 = -1$ *or* $n - 1 = 2n$. *Collecting terms corresponding to the two lowest powers of* z *and equating these to zero, one sees that assuming* $n - 1 = -1$ *leads to a contradiction while the assumption* $n - 1 = 2n$ *implies that* $n = -1, a_{-1} = 2, a_0 = 2$.

For the next step, clear denominators in equation (6) and write it as

$$F\sigma^2(y) + G\sigma(y) + Hy \;=\; 0, \quad F, G, H \in C[x],\ \gcd(F, G, H) = 1. \tag{9}$$

For a putative hypergeometric solution y with $\sigma(y) = uy$, we write $u = \frac{A}{B}$ with $A, B \in C[x],\ \gcd(A, B) = 1$. Let $R = \gcd(\sigma^{-1}(A), B)$. We then can write

$$u = c\frac{\sigma(R)}{R}\frac{p}{q}$$

where $c \in C$, R, p, q are monic polynomials, $\gcd(p, \sigma(q)) = 1$ and $\gcd(\sigma(R)p, Rq) = 1$. Substituting into the Riccati equation associated with equation (9), we have

$$c^2F\sigma^2(R)\sigma(p)p + cG\sigma(R)\sigma(q)p + HR\sigma(q)q \;=\; 0. \tag{10}$$

One sees that p divides H and q divides $\sigma^{-1}(F)$. Therefore there are only a finite number of possible choices for these polynomials. Fix some p, q satisfying these conditions. We shall now determine possible polynomials R.

If $R = x^e + b_{e-1}x^{e-1} + \ldots + b_0$, we then have that $\frac{\sigma(R)}{R} = 1 + ez + \text{h.o.t}$. In addition

$$1 + ez + \text{h.o.t} = \frac{\sigma(R)}{R} = \frac{uq}{cp}.$$

This allows us to determine a value of e. If this value of e is nonnegative, we let $R = x^e + b_{e-1}x^{e-1} + \ldots + b_0$, with the b_i variables. Equating powers of x in equation (10), yields a system of linear equations for the b_i that give possible solutions of the Riccati equation for this particular choice of p, q. Doing this for all possible choices, yields all possible u.

Example 6.11 (continued) *In this case,* $F = 1, G = -(2x+5)$ *and* $H = 2x+2$. *Therefore* $q = 1$ *and* p *divides* $2x + 2$ *and so* $p = 1$ *or* $p = x + 1$.

Case 1: $p = 1$. *In this case we have*

$$1 + ez + \text{h.o.t} = \frac{\sigma(R)}{R} = \frac{uq}{cp} = \frac{1}{c}(\frac{2}{z} + 2 + \text{h.o.t}).$$

This leads to a contradiction.

Case 2: $p = x + 1$. *In this case we have*

$$1 + ez + \text{h.o.t} = \frac{\sigma(R)}{R} = \frac{uq}{cp} = \frac{1}{c}(\frac{\frac{2}{z} + 2 + \text{h.o.t}}{\frac{1}{z} + 1}) = \frac{2}{c}(1 - 0z + \text{h.o.t})$$

Therefore, $c = 2$ *and* $e = 0$. *We then have that* $R = 1$ *so* $u = 2(x + 1)$.

We can conclude that the only hypergeometric solutions of equation (8) are solutions of

$$\sigma(y) = 2(x+1)y,$$

that is, constant multiples of

$$y(n) = 2^n n!.$$

For second order linear equations, when we know a hypergeometric solution, we can find another solution using " variation of parameters".

Example 6.11 (continued) *Consider the noncommutative ring of difference operators $C(x)[\sigma]$ where $\sigma \cdot f = \sigma(f) \cdot \sigma$. We may write the operator associated with equation (8) as*

$$\sigma^2 - (2x+5)\sigma + (2x+2) = (\sigma - 1) \cdot (\sigma - 2(x+1)).$$

Note that $y = 1$ is a solution of $\sigma(y) - y = 0$. Therefore to find another solution of equation (8), we must find a solution of $\sigma(y) - 2(x+1)y = 1$. Let $y = zy_1$ where y_1 satisfies $\sigma(y_1) - 2(x+1)y_1 = 0$. We then have

$$\sigma(z) - z = \frac{1}{2(x+1)y_1},$$

that is,

$$z(n+1) - z(n) = \frac{1}{2(n+1)2^n n!} = \frac{1}{2^{n+1}(n+1)!}.$$

Therefore,

$$z(n) = \sum_{m=0}^{n} \frac{1}{2^m m!} \quad \text{and so} \quad y = 2^n n! \sum_{m=0}^{n} \frac{1}{2^m m!}.$$

This verifies the form of solutions given in example 2 of the introduction.

7 Hints and Answers to Problems

7.1 Problems for Chapter 2

2.1 Let $k = \mathbb{Q}$ and for each $i \in \mathbb{Z}$, let $V_i = \{i\}$, Each V_i is k-closed, but $\cup_{i\in\mathbb{Z}} V_i = \mathbb{Z}$ is not k-closed. The reason for this is that if a polynomial $p(x) \in \mathbb{Q}[x]$ vanishes on all V_i then it must be identically 0 and so would vanish everywhere.

2.2 From the definition of k-closed, one sees that a set $O \subset \bar{k}^m$ is open if there exists a set of polynomials $\{f_i\}_{i\in\mathcal{I}} \subset k[X_1, \ldots, x_m]$ such that $O = \{v \in \bar{k}^m \mid f_i(v) \neq 0 \text{ for some } i \in \mathcal{I}\}$. We say the $\{f_i\}_{i\in\mathcal{I}}$ defines O. Let O_1 be defined by $\{f_i\}_{i\in\mathcal{I}}$ and O_2 be defined by $\{g_j\}_{j\in\mathcal{J}}$. Since they are both nonempty, some f_i and some g_j are not the zero polynomial. Since $\bar{k}$ is infinite, there is an element $v \in \bar{k}^m$ such that $f_i \cdot g_j(v) \neq 0$. This v belongs to $O_1 \cap O_2$.

2.3 Let V be a k-variety, so $V = V(I)$ for some ideal $I \subset k[X_1, \ldots, X_m]$. We begin by showing $V \subset V(I_k(V))$. If $v \in V$, then all the elements of $I_k(V)$ vanish at v (by the definition of $I_k(V)$.). Therefore $V \subset V(I_k(V))$. Now assume that $v \in V(I_k(V))$. Then any polynomial that vanishes on all of V must vanish at v. But the elements of I vanish on the elements of V (this is how V is defined), so the elements of I vanish at v. So $v \in V(I) = V$.

2.4 (ii) Let $V_1 \supset V_2 \supset \ldots$. We then have $I_k(V_1) \subset I_k(V_2) \subset \ldots$. Therefore by part (i), we have $I_k(V_s) = I_k(V_{s+1}) = \ldots$ for some s. From Problem 2.3, we then have that $V_s = V(I_k(V_s)) = V_{s+1} = V(I_k(V_{s+1})) = \ldots$
(iii) Let $V_1 \in \{V_i\}_{i\in\mathcal{I}}$. If V_1 is not minimal there is a $V_2 \in \{V_i\}_{i\in\mathcal{I}}$ such that $V_1 \supsetneq V_2$. By part (ii) we cannot continue indefinitely so after a finite number of steps we find a $V_j \in \{V_i\}_{i\in\mathcal{I}}$ which is minimal.

2.5 (i) This part of Corollary 2.18 follows from Corollary 2.16 in the following way. We have

$$V(I) = V_1 \cup \ldots \cup V_n$$

as in Corollary 2.16. We than have that $I_k(V(I)) = I_k(V_1) \cap \ldots \cap I_k(V_n)$. Since I is already radical, $I_k(V(I)) = I$ by the Hilbert Nullstellensatz. Lemma 2.13 implies that each of the $I_k(V_j)$ are prime. The rest of (i) follows in a similar way.
(ii) Let R be a ring finitely generated over a field k. We may write $R = k[x_1, \ldots, x_m]$. Let $k[X_1, \ldots, X_m]$ be the polynomial ring in m variables and $\Phi : k[X_1, \ldots, X_m] \to k[x_1, \ldots, x_m]$ be the homomorphism defined by $\Phi(X_i) = x_i$. If I is a radical ideal of R, then $\Phi^{-1}(I)$ is a radical ideal of $k[X_1, \ldots, X_m]$. Apply part (i) to this ideal and write $\Phi^{-1}(I) = P_1 \cap \ldots \cap P_n$. We then have $I = \Phi(P_1) \cap \cdots \cap \Phi(P_n)$.

2.6 As mentioned above, k-open sets in $\bar{k}^m$ are of the form $\cup_{i\in\mathcal{I}}\{v \in \bar{k}^m \mid p_i(v) \neq 0\}$ where $\{p_i\}_{i\in\mathcal{I}}$ is a set of polynomials in $k[X_1, \ldots, X_m]$. Therefore it is enough to show that if $F : V \to W$ is a morphism, then $F^{-1}(W \cap \{w \in \bar{k}^m \mid p(w) \neq 0\})$ is an open subset of V. Let $F := (f_1, \ldots, f_m)$. We then have that

$$F^{-1}(W \cap \{w \in \bar{k}^m \mid p(w) \neq 0\}) = \{v \in \bar{k}^n \mid p(f_1(v), \ldots, f_m(v)) \neq 0\}.$$

2.7 The coordinate ring of V is $k[X_1, \ldots, X_m]/I_k(V)$. This is an integral domain if and only if $I_k(V)$ is a prime ideal. On the other hand, $I_k(V)$ is a prime ideal if and only if V is k-irreducible by Lemma 2.13.

7.2 Problems for Chapter 3

3.1 Let $g \in X$ and assume $e \in X$. The map $x \mapsto gx$ is a homeomorphism of G to G that takes X into X. Therefore gX is a closed subset of X. Iterating the map, we have $X \supset gX \supset g^2X \supset \ldots$. We cannot have an infinite descending chain of such subsets, so for some s, we have $g^sX = g^{s+1}X$. Since $e \in X$, we have $g^se = g^{s+1}a$ for some

$a \in X$. Since G is a group, this implies that $e = ga$, so X is closed under inverse and must be a group.
One can modify this argument when we do not assume $e \in X$. As above one can show $g^s X = g^{s+1} X$ for some s. This implies that there is an $a \in X$ such that $g^{s+1}a = g^s g$. Therefore $a = e \in X$. Now use the first part of this problem.

3.2 Let $h \in N$. the map $c_h : G \to N$ defined by $g \mapsto gxg^{-1}$ is a continuous map from a connected set to a finite set. Each point of a finite set is closed ($v = (v_1, \ldots, v_m)$ is the unique zero of $\{X_1 - v_1, \ldots, X_m - v_m\}$) so each element of a finite set is one of the components of that set. The image of G under the map c_h is irreducible so must equal one of these points. Since $c_h(e) = e$, we have $c_h(G) = e$. This means $ghg^{-1} = h$ for all $g \in G$ so $h \in Z(G)$.

3.3 This is a long computation. One must show each of these sets is a group, normal in the previous set such that the quotients are abelian. To show the quotients are abelian, one should show that if g, h are in one set then $ghg^{-1}h^{-1}$ is in the next set. Again this is a computation.

3.4 (a) If $A^m = e$ then A satisfies $X^m - 1 = 0$. If 1 is the only eigenvalue, then the minimal polynomial must be of the form $(X-1)^t$ for some t. The minimal polynomial will divide $X^m - 1$ and this can only happen if $t = 1$, so A is the identity matrix.
(b) If $g_1, g_2 \in T_n$, the group of upper triangular matrices with nonzero elements on the diagonal, then the diagonal elements of $g_1 g_2 g_1^{-1} g_2^{-1}$ must all equal 1. If g_1 and g_2 are furthermore in a finite group then $g_1 g_2 g_1^{-1} g_2^{-1}$ has finite order. Therefore by (a), we have g_1 and g_2 commute.
(c) Think of each element of $\mathcal{A}_4$ as permuting the basis elements $\{e_1, \ldots, e_4\}$ of a four-dimensional vector space. This gives a representation of $\mathcal{A}_4$ as 4×4 matrices. The subgroup $H = \{e, (123)(4), (132)(4)\}$ of $\mathcal{A}_4$ is abelian and $\mathcal{A}_4/H$ has order 4 and so must be abelian as well. Therefore $\mathcal{A}_4$ is solvable but nonabelian (check).

3.5 (a) Let $V \in \mathrm{GL}_1(\bar{k}) = \bar{k}^*$ be a k-torsor. Since G has two elements, the definition of k-torsor implies that V has two elements. It is irreducible and the zero set of polynomials in one variable so we an conclude that $V = V(X^2 + bX + c)$ where $X^2 + bX + c$ is irreducible over k. The ring $\mathcal{O}_k(V) = k[X]/\langle X^2 + bX + c\rangle = k(\sqrt{a})$ for some a. Since $X^2 + bX + c$ is irreducible over k, a is not a square.
(b) If $a = bc^2$, then b is not a square and $k(\sqrt{b}) = k(\sqrt{a})$. Conversely if $k(\sqrt{b}) = k(\sqrt{a})$, then there exist $c, d \in k$ such that $\sqrt{a} = c + d\sqrt{b}$. This implies that $a = c^2 + d^2 b + 2cd\sqrt{b}$ and so $cd = 0$. If $d = 0$, then a would be a square, so $c = 0$ and $a = d^2 b$.
(c) The torsors V_1 and V_2 are isomorphic if and only if their coordinate rings are isomorphic (in such a way that the isomorphism commutes with the action of G on these rings). The rest follows from (b).

7.3 Problems for Chapter 4

4.1 If $\sigma^n = identity$, then for any $a \in k$, the coefficients of the polynomial

$$P_a(X) = \prod_{i=0}^{n-1}(X - \sigma^i(a))$$

are constant. Now use the fact that the field of constants is algebraically closed.

4.2 One easily checks that R^σ is a ring. Assume R is simple and let $c \in R^\sigma, c \neq 0$. One shows that the ideal $\langle c \rangle$ is a σ-ideal. Since $c \neq 0$, we must have $1 \in \langle c \rangle$ and so there exists an element $b \in R$ such that $bc = 1$ Since $\sigma(b)\sigma(c) = \sigma(b)c = 1 = bc$, we have $\sigma(b) = b$.

4.3 Since $e_0 + \ldots + e_{t-1} = 1$ some e_i has a 1 in the first place. After renumbering, assume this is e_0. Let j be the smallest positive integer such that $e_0(j) = 1$ (such an integer exists since $\sigma^t(e_0) = e_0$ so $e_0(t) = 1$). If $j < t$, then $e_j = \sigma^j(e_0)$ has 1 in the j^{th} place. This would contradict the fact that $e_0 e_j = 0$. Therefore $e_0(0) = 1$ and $e_0(i) = 0$ for $1 < i < t$. Since $e_0 = \sigma^t(e_0)$, we see that e_0 satisfies the conclusion of the problem. Since $e_i = \sigma^i(e_0)$, the other e_i satisfy the conclusion as well.

4.4 Let $R = k[Z, 1/\det(Z)]$. Since $\sigma(Z) = AZ$, we have

$$\sigma^t(Z) = BZ \text{ where } B = A\sigma(A)\cdots\sigma^{t-1}(Z).$$

We have $R_i = k[e_i Z, 1/\det(e_i Z)]$ and $\sigma^t(e_i Z) = B(e_i Z)$.

7.4 Problems for Chapter 5

5.1 Let $R = R_0 \oplus \ldots \oplus R_{t-1}$ where $R_i = e_i R$ is an integral domain. For any $r \in R$ we can write $r = (r_0, \ldots, r_{t-1}), r_i \in R_i$. Note that if r satisfies $r^2 = r$, then each r_i must be either 0 or $1 \in R_i$, since these rings are domains. Let $f_i = \phi(r_i)$. We therefore have the only entries of f_i are 0 or 1.

For $r \in R$, define $\text{supp}(r) = \{i \mid r_i \neq 0\}$. Note that $\text{supp}(e_i) = \{i\}$. We have the following observations

(i) If $r \neq 0$ then $\text{supp}(r) \neq \emptyset$.

(ii) If $r, s \in R$ and $rs = 0$ then $\text{supp}(r) \cap \text{supp}(s) = \emptyset$.

Since $e_i e_j = 0$, we have $f_i f_j = 0$. Therefore $\{\text{supp}(f_i)\}_{i=0}^{t-1}$ is a partition of $\{0, \ldots, t-1\}$ into n disjoint nonempty sets. This implies that each $\text{supp}(f_i)$ is a singleton. We have already seen that the nonzero entry must be 1 so the f_i are just a permutation of the e_i.

5.2 Let $u_i = \sigma^i(u), i = 0, \ldots, s-1$. The set $\{u_i\}_{i=0}^{s-1}$ is stable under the action of σ. Therefore any symmetric function of these elements is left fixed by σ. This means that the coefficients of

$$p(X) = \prod_{i=0}^{s-1}(X - u_i) = X^s - (u_0 + \ldots + u_{s-1})X^{s-1} + \ldots + (-1)^s(\prod u_i)$$

are left fixed by σ and so lie in k^σ. Therefore u is algebraic over k^σ.

5.3 (i) Note that $(r, s)(u, v) = (ru, sv) = (0, 1)$ if and only if $ru = 0$. therefore, (r, s) is a non-zerodivisor if and only if r is a non-zerodivisor. This implies that if (r, s) is not a zerodivisor, then $(s, r) \in Q(R)$.
(ii) It is enough to show that if $(r, 1) \sim (0, 1)$ then $r = 0$. This follows from $r \cdot 1 - 1 \cdot 0 = 0$.

5.4 Let $(r, s) \in Q(R)$ and assume that $\sigma((r, s)) = (r, s)$. Let $I = \{u \in R \mid (u, 1)(r, s) \in R\}$ where we identify R as in 5.3(ii). One sees that I is a difference ideal containing s so must be all of R. Therefore $1 \in I$ and this implies that $(r, s) \in R$.

5.5 Note that since each R_i is a domain, $Q(R_i)$ is the usual quotient field. An element $s = (s_0, \ldots, s_{t-1}) \in R$ is a non-zerodivisor if and only if all the s_i are nonzero. Therefore we may make the following identification:

$$\begin{aligned} Q(R) &= \{(r, s) \mid r = (r_0, \ldots, r_{t-1}), s = (s_0, \ldots, s_{t-1}), \text{ all the } s_i \neq 0\} \\ &= \{((r_0, s_0), \ldots, (r_{t-1}, s_{t-1})) \mid \text{all the } s_i \neq 0\} \\ &= \oplus_{i=0}^{t-1} Q(R_i) \end{aligned}$$

References

[1] Yves André. Différentielles non commutatives et théorie de Galois différentielle ou aux différences. *Ann. Sci. École Norm. Sup. (4)*, 34(5):685–739, 2001.

[2] Benali Benzaghou. Algèbres de Hadamard. *Bull. Soc. Math. France*, 98:209–252, 1970.

[3] Benali Benzaghou and Jean-Paul Bézivin. Propriétés algébriques de suites différentiellement finies. *Bull. Soc. Math. France*, 120(3):327–346, 1992.

[4] Shaoshi Chen and Michael F. Singer. Residues and Telescopers for Bivariate Rational Functions. *Advances in Applied Mathematics*, 49:111–133, 2012. arXiv:1203.4200.

[5] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.

[6] Teresa Crespo and Zbigniew Hajto. *Algebraic groups and differential Galois theory*, volume 122 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2011.

[7] Harm Derksen, Emmanuel Jaendel, and Pascal Koiran. Quantum automata and algebraic groups. *Journal of Symbolic Computation*, 39:357–371, 2005.

[8] Thomas Dreyfus, Charlotte Hardouin, and Julien Roques. Hypertranscendence of solutions of Mahler equations. preprint, `arXiv:1507.03361`, 2015.

[9] Thomas Dreyfus and Julien Roques. Galois groups of difference equations of order two on elliptic curves. *SIGMA Symmetry Integrability Geom. Methods Appl.*, 11:Paper 003, 23, 2015.

[10] Ruyong Feng. On the computation of the galois group of linear difference equations. preprint, `arXiv:1503.02239`, 2015.

[11] Brendan Hassett. *Introduction to algebraic geometry*. Cambridge University Press, Cambridge, 2007.

[12] Peter A. Hendriks. An algorithm for determining the difference Galois groups of second order linear difference equations. *Journal of Symbolic Computation*, 26(4):445–461, 1998.

[13] Peter A. Hendriks and Michael F. Singer. Solving difference equations in finite terms. *J. Symbolic Comput.*, 27(3):239–259, 1999.

[14] James E. Humphreys. *Linear Algebraic Groups*. Graduate Texts in Mathematics. Springer-Verlag, New York, 1975.

[15] Manuel Kauers and Burkhard Zimmermann. Computing the algebraic relations of C-finite sequences and multisequences. *J. Symbolic Comput.*, 43(11):787–803, 2008.

[16] Ellis R. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1976.

[17] Jerald J. Kovacic. An algorithm for solving second order linear homogeneous differential equations. *J. Symbolic Comput.*, 2(1):3–43, 1986.

[18] Ernst Kunz. *Introduction to commutative algebra and algebraic geometry*. Birkhäuser Boston Inc., Boston, MA, 1985. Translated from the German by Michael Ackerman, With a preface by David Mumford.

[19] Serge Lang. *Algebra*. Addison Wesley, New York, 3rd edition, 1993.

[20] Richard G. Larson and Earl J. Taft. The algebraic structure of linearly recursive sequences under Hadamard product. *Israel J. Math.*, 72(1-2):118–132, 1990. Hopf algebras.

[21] Andy R. Magid. Finite generation of class groups of rings of invariants. *Proc. Amer. Math. Soc.*, 60:45–48 (1977), 1976.

[22] Andy R. Magid. *Lectures on Differential Galois Theory*. University Lecture Series. American Mathematical Society, 1994. Second Edition.

[23] Pierre Nguyen. Hypertranscedance de fonctions de Mahler du premier ordre. *C. R. Math. Acad. Sci. Paris*, 349(17-18):943–946, 2011.

[24] Pierre Nguyen. *Équations de Mahler et hypertranscendance*. PhD thesis, Institut de Mathématiques de Jussieu, 2012.

[25] Marko Petkovsek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation*, 14:243–264, 1992.

[26] Marko Petkovsek, Herbert Wilf, and Doron Zeilberger. *A=B*. A. K. Peters, Wellsely, Massachusets, 1996.

[27] Marius van der Put and Michael F. Singer. *Galois Theory of Difference Equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Heidelberg, 1997.

[28] Marius van der Put and Michael F. Singer. *Galois Theory of Linear Differential Equations*, volume 328 of *Grundlehren der mathematischen Wissenshaften*. Springer, Heidelberg, 2003.

[29] Julien Roques. Algebraic relations between Mahler functions. Preprint available on https://www-fourier.ujf-grenoble.fr/ jroques/mahler.pdf, 2015.

[30] Maxwell Rosenlicht. Toroidal algebraic groups. *Proc. Amer. Math. Soc.*, 12:984–988, 1961.

[31] Maxwell Rosenlicht. Initial results in the theory of linear algebraic groups. In A. Seidenberg, editor, *Studies in Algebraic Geometry*, volume 20 of *MAA Studies in Mathematics*, pages 1–18. Mathematical Association of America, Washington, D.C., 1980.

[32] Heidrun Sarges. Ein Beweis des Hilbertschen Basissatzes. *J. Reine Angew. Math.*, 283/284:436–437, 1976.

[33] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[34] Michael F. Singer. Notes on Difference Equations. Technical report, NC State University, 1994.

[35] Tonny A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, second edition, 1998.

[36] Michael Wibmer. *Geometric difference Galois theory*. PhD thesis, Heidelberg, 2010.