REAL DIFFERENCE GALOIS THEORY

THOMAS DREYFUS

(Communicated by Matthew A. Papanikolas)

ABSTRACT. In this paper, we develop a difference Galois theory in the setting of real fields. After proving the existence and uniqueness of the real Picard-Vessiot extension, we define the real difference Galois group and prove a Galois correspondence.

INTRODUCTION

Let us consider an equation of the form:

$$(1) \qquad\qquad \phi Y = AY,$$

where A is an invertible matrix having coefficients in a convenient field $\mathbf{k}^*$ and ϕ is an automorphism of $\mathbf{k}$. A typical example is $\mathbf{k} := \mathbb{C}(x)$ and $\phi y(x) := y(x+1)$. The aim of the difference Galois theory is to study (1) from an algebraic point of view. See [vdPS97] for details on this theory. See also [BB62, Fra63, HS08, Mor09, MU09]. The classical framework for difference Galois theory is to assume that C, the subfield of $\mathbf{k}$ of elements invariant under ϕ, is algebraically closed. The goal of the present paper is to present a descent result. We explain what happens if we take instead a smaller field $\mathbf{k}$, such that $\mathbf{k}$ is a real field and C is real closed; see §2 for the definitions.

Assume that C is algebraically closed and let us make a brief summary of the difference Galois theory. An important object attached to (1) is the Picard-Vessiot extension. Roughly speaking, a Picard-Vessiot extension is a ring extension of $\mathbf{k}$ containing a basis of solutions of (1). The Picard-Vessiot extension always exists, but the uniqueness is proved in [vdPS97] only in the case where C is algebraically closed. To the Picard-Vessiot extension, we attach a group, the difference Galois group, that measures the algebraic relations between solutions belonging to the Picard-Vessiot extension. This group may be seen as a linear algebraic subgroup of invertible matrices in coefficients in C. We also have a Galois correspondence. Note that several definitions of the difference Galois group have been made and the comparison between different Galois groups can be found in [CHS08].

From now, we drop the assumption that C is algebraically closed, and we make the assumptions that $\mathbf{k}$ is a real field and C is real closed. Our approach will follow [CHS13, CHvdP16], which prove similar results in the framework of differential

Galois theory. Let us present a rough statement of our main result, Theorem 7. We prove that in this setting, a real Picard-Vessiot exists, i.e., a Picard-Vessiot extension that is additionally a real ring. Then, we also show a uniqueness result: given R_1 and R_2 two real Picard-Vessiot extensions, then R_1 and R_2 are isomorphic over $\mathbf{k}$ if and only if $R_1 \otimes_{\mathbf{k}} R_2$ has no elements x satisfying $x^2 + 1 = 0$. We define a real difference Galois group, which may be seen as a linear algebraic subgroup of invertible matrices in coefficients in the algebraic closure of C, and that is defined over C. See Proposition 11. This allows us to prove a Galois correspondence; see Theorem 12. See also [CH15, Dyc05] for similar results in the framework of differential Galois theory.

The paper is presented as follows. In §1, we make some reminders of difference algebra. In §2, we state and prove our main result, Theorem 7, about the existence and uniqueness of real Picard-Vessiot extensions. In §3, we define the real difference Galois group, and prove a Galois correspondence.

1. Reminders of difference algebra

For more details on what follows, we refer to [Coh65]. A difference ring (R, ϕ) is a ring R together with a ring automorphism $\phi : R \to R$. An ideal of R stabilized by ϕ is called a difference ideal of (R, ϕ). A simple difference ring (R, ϕ) is a difference ring with only difference ideals (0) and R. If R is a field, then (R, ϕ) is called a difference field.

Let (R, ϕ) be a difference ring and $m \in \mathbb{N}^*$. The difference ring $R\{X_1, \ldots, X_m\}_\phi$ of difference polynomials in m indeterminacies over R is the usual polynomial ring in the infinite set of variables

$$\{\phi^\nu(X_j)\}_{j \leq m}^{\nu \in \mathbb{Z}},$$

and with automorphism extending the one on R defined by:

$$\phi\left(\phi^\nu(X_j)\right) = \phi^{\nu+1}(X_j).$$

The ring of constants R^ϕ of the difference ring (R, ϕ) is defined by

$$R^\phi := \{f \in R \mid \phi(f) = f\}.$$

If R^ϕ is a field, the ring of constants will be called a field of constants.

A difference ring morphism from the difference ring (R, ϕ) to the difference ring $(\widetilde{R}, \widetilde{\phi})$ is a ring morphism $\varphi : R \to \widetilde{R}$ such that $\varphi \circ \phi = \widetilde{\phi} \circ \varphi$.

A difference ring $(\widetilde{R}, \widetilde{\phi})$ is a difference ring extension of a difference ring (R, ϕ) if $\widetilde{R}$ is a ring extension of R and $\widetilde{\phi}_{|R} = \phi$; in this case, we will often denote $\widetilde{\phi}$ by ϕ. Two difference ring extensions $(\widetilde{R}_1, \widetilde{\phi}_1)$ and $(\widetilde{R}_2, \widetilde{\phi}_2)$ of a difference ring (R, ϕ) are isomorphic over (R, ϕ) if there exists a difference ring isomorphism φ from $(\widetilde{R}_1, \widetilde{\phi}_1)$ to $(\widetilde{R}_2, \widetilde{\phi}_2)$ such that $\varphi_{|R} = \mathrm{Id}$.

Let (R, ϕ) be a difference ring such that $X^2 + 1 \in R[X]$ is irreducible, i.e., there is no $x \in R$ such that $x^2 + 1 = 0$. We define, $R[i]$, to be the ring $R[i] := R[X]/(X^2 + 1)$. We equip $R[i]$ with a structure of difference ring with $\phi(i) = i$. If (R, ϕ) is a difference ring with an element $x \in R$ satisfying $x^2 + 1 = 0$, we make the convention that $R[i] = R$.

2. Existence and uniqueness of Picard-Vessiot extensions over real fields

Let $(\mathbf{k}, \phi)$ be a difference field of characteristic zero. Consider a linear difference system

$$(2) \qquad \phi Y = AY \text{ with } A \in \mathrm{GL}_n(\mathbf{k}),$$

where GL_n denotes the group of invertible $n \times n$ square matrices with entries in $\mathbf{k}$.

Definition 1. A Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$ is a difference ring extension (R, ϕ) of $(\mathbf{k}, \phi)$ such that

(1) there exists $U \in \mathrm{GL}_n(R)$ such that $\phi(U) = AU$ (such a U is called a fundamental matrix of solutions of (2));

(2) R is generated, as a $\mathbf{k}$-algebra, by the entries of U and $\det(U)^{-1}$;

(3) (R, ϕ) is a simple difference ring.

We may always construct a Picard-Vessiot extension as follows. Take an indeterminate $n \times n$ square matrix $X := X_{j,k}$ and consider $\mathbf{k}\{X, \det(X)^{-1}\}_\phi$ which is equipped with a structure of difference ring with $\phi X = AX$. Then, for any I, maximal difference ideal of $\mathbf{k}\{X, \det(X)^{-1}\}_\phi$, the ring $\mathbf{k}\{X, \det(X)^{-1}\}_\phi/I$ is a simple difference ring and therefore, is a Picard-Vessiot extension.

According to [vdPS97, §1.1], when the field of constants $C := \mathbf{k}^\phi$ is algebraically closed, we also have the uniqueness of the Picard-Vessiot extension, up to a difference ring isomorphism. Furthermore, in this case we have $C = R^\phi$ and, see [vdPS97, Corollary 1.16], there exist an idempotent $e \in R$, and $t \in \mathbb{N}^*$, such that $\phi^t(e) = e$, $R = \bigoplus_{j=0}^{t-1} \phi^j(e)R$, and for all $0 \le j \le t - 1$, $\phi^j(e)R$ is an integral domain.

In [CHS08], the notion of weak Picard-Vessiot extension is defined. We will need this in the next section.

Definition 2. A weak Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$ is a difference ring extension (R, ϕ) of $(\mathbf{k}, \phi)$ such that

(1) there exists $U \in \mathrm{GL}_n(R)$ such that $\phi(U) = AU$;

(2) R is generated, as a $\mathbf{k}$-algebra, by the entries of U and $\det(U)^{-1}$;

(3) $R^\phi = \mathbf{k}^\phi = C$.

From what is above, we deduce that when the field of constants is algebraically closed, a Picard-Vessiot extension is a weak Picard-Vessiot extension. Note that the converse is not true as shown in [vdPS97, Example 1.25].

We say that a field $\mathbf{k}$ is real when 0 is not a sum of squares in $\mathbf{k} \setminus \{0\}$. We say that a field $\mathbf{k}$ is real closed when $\mathbf{k}$ does not admit an algebraic extension that is real. In particular, $\mathbf{k}$ is real closed if and only if $\mathbf{k}[i]$ is algebraically closed and satisfies $\mathbf{k}[i] \ne \mathbf{k}$.

Example 3. The field $\mathbb{R}((x))$ of formal Laurent series with real coefficients is real. The field $\mathbb{Q}(x)$ is real. The field of real numbers is real closed.

From now on we assume that $\mathbf{k}$ is a real field and its field of constants $C := \mathbf{k}^\phi$ is real closed.

Recall that we have seen that we have the existence of (R, ϕ), Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$.

Lemma 4. *Let (R, ϕ) be a Picard-Vessiot extension for* (2) *over* $(\mathbf{k}, \phi)$ *and assume that $R \neq R[i]$. Then, $(R[i], \phi)$, is a Picard-Vessiot extension for* (2) *over* $(\mathbf{k}[i], \phi)$.

Proof. Let $(0) \neq I$ be a difference ideal of $(R[i], \phi)$. Note that $I \cap R$ is a difference ideal of (R, ϕ). We claim that $I \cap R \neq (0)$. Let $a, b \in R$ with $0 \neq a + ib \in I$. Then, $\phi(a) + i\phi(b) \in I$ and for all $c \in R$, $ac + ibc \in I$. Let J be the smallest difference ideal of R that contains a. From what is above, we may deduce that for all $a_1 \in J$, there exists $b_1 \in R$ such that $a_1 + ib_1 \in I$. Since (R, ϕ) is a simple difference ring, we have two possibilities: $J = (0)$ and $J = R$. We are going to treat separately the two cases. Assume that $J = (0)$. Then $a = 0$ and $ib \in I$. But $ib \times (-i) = b \in I \cap R \setminus \{0\}$ which proves our claim when $J = (0)$. Assume that $J = R$. Then, there exists $b_1 \in R$ such that $1 + ib_1 \in I$. But $(1 + ib_1)(1 - ib_1) = 1 + b_1^2 \in I \cap R$. Since $R \neq R[i]$ we find that $1 + b_1^2 \neq 0$ which proves our claim when $J = R$.

Since $I \cap R \neq (0)$ and (R, ϕ) is a simple difference ring, $I \cap R = R$. We now remark that I is stable by multiplication by $\mathbf{k}[i]$, which shows that $I = R[i]$. This proves the lemma. $\qquad\square$

Proposition 5. *Let (R, ϕ) be a Picard-Vessiot extension for* (2) *over* $(\mathbf{k}, \phi)$. *Then, there exist an idempotent $e \in R$, and $t \in \mathbb{N}^*$, such that $\phi^t(e) = e$, $R = \bigoplus_{j=0}^{t-1} \phi^j(e)R$, and for all $0 \leq j \leq t-1$, $\phi^j(e)R$ is an integral domain.*

Proof. Let us separately treat the two cases. Assume that $R \neq R[i]$. Due to Lemma 4, $(R[i], \phi)$, is a Picard-Vessiot extension for (2) over $(\mathbf{k}[i], \phi)$. We recall that by definition, if $R \neq R[i]$, we extend ϕ to $R[i]$ by $\phi(i) = i$. Then, the field of constants of $R[i]$ is $C[i]$, which is algebraically closed. From [vdPS97, Corollary 1.16], we obtain that there exist $a, b \in R$, with $a + ib$ idempotent, $t \in \mathbb{N}^*$, such that $\phi^t(a + ib) = a + ib$,

$$(3) \qquad\qquad R[i] = \bigoplus_{j=0}^{t-1} \phi^j(a + ib)R[i],$$

and for all $0 \leq j \leq t-1$, $\phi^j(a + ib)R[i]$ is an integral domain. Let $e := a^2 + b^2 \in R$. A straightforward computation shows that $a - ib$ is idempotent. Since $e = (a + ib)(a - ib)$ is the product of two idempotent elements it is also idempotent. Using $\phi^t(a - ib) = a - ib$, we find $\phi^t(e) = e$.

Let us prove that for all $0 \leq j \leq t-1$, $\phi^j(a - ib)R[i]$ is an integral domain. Let $0 \leq j \leq t-1$, $c + id \in R[i]$ with $c, d \in R$, such that $\phi^j(a - ib)(c + id) = 0$. It follows that $\phi^j(a + ib)(c - id) = 0$ and therefore, $c - id = 0 = c + id$ since for all $0 \leq j \leq t-1$, $\phi^j(a + ib)R[i]$ is an integral domain. We have proved that for all $0 \leq j \leq t-1$, $\phi^j(a - ib)R[i]$ is an integral domain. Let us prove that for all $0 \leq j \leq t-1$, $\phi^j(e)R[i]$ is an integral domain. Let $0 \leq j \leq t-1$, $c \in R[i]$, such that $c\phi^j(e) = c\phi^j(a + ib)\phi^j(a - ib) = 0$. We use successively the fact that $\phi^j(a + ib)R[i]$ and $\phi^j(a - ib)R[i]$ are integral domains to deduce that $c = 0$, which shows that $\phi^j(e)R[i]$ is an integral domain. Therefore, for all $0 \leq j \leq t-1$, $\phi^j(e)R$ is an integral domain.

We claim that $\{\phi^j(e), 0 \leq j \leq t-1\}$ are linearly independent over $R[i]$. Let us consider $c_0, \ldots, c_{t-1} \in R[i]$ such that $\sum_{j=0}^{t-1} c_j\phi^j(e) = 0$. We have $\sum_{j=0}^{t-1} c_j\phi^j(a - ib)\phi^j(a + ib) = 0$. We use (3) to deduce that for all $0 \leq j \leq t-1$, $c_j\phi^j(a - ib) = 0$. We recall that for all $0 \leq j \leq t-1$, $\phi^j(a - ib)R[i]$ is an integral domain. This shows that for all $0 \leq j \leq t-1$, $c_j = 0$. This proves our claim.

Using (3), to prove the proposition, it is now sufficient to prove the equality

$$(4) \qquad \bigoplus_{j=0}^{t-1} \phi^j(a+ib)R[i] = \bigoplus_{j=0}^{t-1} \phi^j(e)R[i].$$

The inclusion $\bigoplus_{j=0}^{t-1} \phi^j(e)R[i] \subset \bigoplus_{j=0}^{t-1} \phi^j(a+ib)R[i]$ is a direct consequence of the fact that $e = (a-ib)(a+ib) \in (a+ib)R[i]$. Let us prove the other inclusion. Let $\alpha \in \bigoplus_{j=0}^{t-1} \phi^j(a+ib)R[i]$, and define $f := \prod_{j=0}^{t-1} \phi^j(e)$ which is invariant under ϕ. Therefore, $fR[i]$ is a difference ideal of $R[i]$. We use $e = (a+ib)(a-ib)$ and the fact that $(a+ib)R[i]$ is an integral domain to obtain that $f \neq 0$ and $fR[i] \neq (0)$. Since $R[i]$ is a simple difference ring, the difference ideal $fR[i]$ equals $R[i]$. This means that the ideal of $R[i]$ generated by the $\phi^j(f)$, $j \in \mathbb{Z}$, is $R[i]$. Since $\phi(f) = f$, there exists $\beta \in R[i]$ such that $f\beta = \alpha$. We again use (3) to find that $\alpha = f \sum_{j=0}^{t-1} c_j \phi^j(a+ib)$ for some $c_j \in R[i]$. Since $e = (a-ib)(a+ib)$, we may define for all $0 \leq j \leq t-1$, $d_j := f/\phi^j(a-ib) \in R[i]$. A straightforward computation shows that $\alpha = \sum_{j=0}^{t-1} c_j d_j \phi^j(e)$, which implies $\alpha \in \bigoplus_{j=0}^{t-1} \phi^j(e)R[i]$. We have proved $\bigoplus_{j=0}^{t-1} \phi^j(a+ib)R[i] \subset \bigoplus_{j=0}^{t-1} \phi^j(e)R[i]$. If we combine this with the other inclusion, we obtain (4). This completes the proof in the case $R \neq R[i]$.

Assume that $R = R[i]$. Since $i^2 = -1$, we have $\phi(i) = \pm i$ and then $\phi^2(i) = i$. Hence, (R, ϕ^2) is a ring extension of $(\mathbf{k}[i], \phi^2)$, whose field of constants is $C[i]$, which is algebraically closed. Furthermore, by construction, it is also a Picard-Vessiot extension for $\phi^2 Y = \phi(A)AY$ over $(\mathbf{k}[i], \phi^2)$. From [vdPS97, Corollary 1.16], we obtain that there exist an idempotent $e \in R$, $t \in \mathbb{N}^*$, such that $\phi^{2t}(e) = e$,

$$R = \bigoplus_{j=0}^{t-1} \phi^{2j}(e)R,$$

and for all $0 \leq j \leq t-1$, $\phi^{2j}(e)R$ is an integral domain. If $t = 1$, $R = eR$ is an integral domain, and we may take $e = 1$ to have the desired decomposition of R. Assume that $t > 1$. Using the fact that ϕ is an automorphism we find that for all $j \in \mathbb{Z}$, $\phi^j(e)R$ is an integral domain and $\phi^j(e)$ is idempotent. Let $t' \in \mathbb{N}^*$ maximal such that $eR, \ldots, \phi^{t'-1}(e)R$ are in direct sum. This implies that there exists $r \in R$ with $r\phi^{t'}(e) \neq 0$, such that $r\phi^{t'}(e) \in \bigoplus_{j=0}^{t'-1} \phi^j(e)R$. We claim that $r\phi^{t'}(e) \in eR$. If $t' = 1$ the claim is clear. Assume that $t' > 1$. Then, for all $0 < j < t'$, we have $e\phi^j(e) = 0$ and, since ϕ is an automorphism, $\phi^{t'}(e)\phi^j(e) = 0$. It follows that $\bigoplus_{j=0}^{t'-1} \phi^j(e)R\phi^{t'}(e) \subset eR$ and therefore, $r\phi^{t'}(e) = r(\phi^{t'}(e))^2 \in eR$, which proves the claim in the $t' > 1$ case. In particular, there exists $r' \in R$ such that $r\phi^{t'}(e) = r'e \neq 0$. We use the fact that $\phi^{t'}$ is an automorphism, to find $\phi^{t'}(r)\phi^{2t'}(e) = \phi^{t'}(r')\phi^{t'}(e) \neq 0$. Since $\phi^{t'}(e)R$ is an integral domain and $\phi^{t'}(e)$ is idempotent, we have $\phi^{t'}(r')r\phi^{t'}(e) = \phi^{t'}(r')\phi^{t'}(e)r\phi^{t'}(e) \neq 0$. But the latter inequality implies $\phi^{t'}(r)\phi^{2t'}(e)r'e \neq 0$. This shows that $\phi^{2t'}(e)e \neq 0$. Since $R = \bigoplus_{j=0}^{t-1} \phi^{2j}(e)R$, $\phi^{2t}(e) = e$, and $\bigoplus_{j=0}^{t'-1} \phi^j(e)R$, we find $t = t'$. With $R = \bigoplus_{j=0}^{t-1} \phi^{2j}(e)R$, we obtain $\phi^t(e) \in \bigoplus_{j=0}^{t-1} \phi^{2j}(e)R$. We recall that for all $0 < j < t$, we have $e\phi^j(e) = 0$. Using the fact that ϕ is an automorphism, we obtain that for all $0 < j < t$, we have $\phi^t(e)\phi^{2j}(e) = 0$. It follows that $\bigoplus_{j=0}^{t-1} \phi^{2j}(e)R\phi^t(e) \subset eR$ and therefore, $\phi^t(e) = (\phi^t(e))^2 \in eR$. So there exists $r' \in R$ such that $\phi^t(e) = er'$. But an integral domain may have only one non-zero idempotent element. Since

$e, \phi^t(e)$ are non-zero idempotent and eR is an integral domain we find that $e = \phi^t(e)$. In particular, $\bigoplus_{j=0}^{t-1} \phi^j(e)R$ is a difference ideal of the simple difference ring (R, ϕ). Since $e \neq 0$, we find that the difference ideal is not (0), proving that $R = \bigoplus_{j=0}^{t-1} \phi^j(e)R$. This completes the proof in the case $R = R[i]$. □

Let R be a difference ring that is the direct sum of integral domains $R := \bigoplus_{j=0}^{t-1} R_j$. We define K, the total ring of fractions of R, by $K := \bigoplus_{j=0}^{t-1} K_j$, where for all $0 \leq j \leq t-1$, K_j is the fraction field of R_j.

We say that R is a real ring if for all $0 \leq j \leq t-1$, K_j is a real field. Note that by [Lam84, Theorem 2.8], this is equivalent to the usual definition of a real ring, that is, that 0 is not a sum of squares in $R \setminus \{0\}$; see [Lam84, Definition 2.1].

The notion of Picard-Vessiot extension is not well suited in the real case. Following [CHvdP16], let us define:

Definition 6. A real Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$ is a difference ring extension (R, ϕ) of $(\mathbf{k}, \phi)$ such that

   (1) (R, ϕ) is a Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$;
   (2) (R, ϕ) is a real difference ring.

Let us recall that if (R, ϕ) is a difference ring such that $X^2 + 1 \in R[X]$ is irreducible, then $R[i]$ is the ring $R[i] := R[X]/(X^2 + 1)$. If (R, ϕ) is a difference ring with $x \in R$ satisfying $x^2 + 1 = 0$, we make the convention that $R[i] = R$.

We are now able to state our main result:

Theorem 7. *Let us consider equation* (2) *which has coefficients in* $(\mathbf{k}, \phi)$.

   (1) *There exists a real Picard-Vessiot extension for* (2) *over* $(\mathbf{k}, \phi)$.
   (2) *Let* (R, ϕ) *be a real Picard-Vessiot extension for* (2) *over* $(\mathbf{k}, \phi)$. *Then,* (R, ϕ) *is a weak Picard-Vessiot extension for* (2) *over* $(\mathbf{k}, \phi)$, *i.e., the ring of constants of* R *is* C.
   (3) *Let* (R_1, ϕ_1) *and* (R_2, ϕ_2) *be two real Picard-Vessiot extensions for* (2) *over* $(\mathbf{k}, \phi)$. *Let us equip the ring* $R_1 \otimes_{\mathbf{k}} R_2$ *with a structure of difference ring as follows:* $\phi(r_1 \otimes_{\mathbf{k}} r_2) = \phi_1(r_1) \otimes_{\mathbf{k}} \phi_2(r_2)$ *for* $r_j \in R_j$. *Then,* (R_1, ϕ_1) *is isomorphic to* (R_2, ϕ_2) *over* $(\mathbf{k}, \phi)$ *if and only if* $R_1 \otimes_{\mathbf{k}} R_2 \neq R_1 \otimes_{\mathbf{k}} R_2[i]$.

Before proving the theorem, we are going to state and prove a lemma which is inspired by a lemma of [Sei58].

Lemma 8. *Consider a difference field* $(\mathbf{K}, \phi)$ *of characteristic zero that is finitely generated over* $\mathbb{Q}$ *by the elements* $u_1, \ldots, u_m$ *and let* $(\mathbf{K}_R, \phi)$ *be a real difference subfield of* $(\mathbf{K}, \phi)$. *Then, there exists* $h : \mathbf{K} \to \mathbb{C}$, *injective morphism of fields that induces an injective morphism from* $\mathbf{K}_R$ *to* $\mathbb{R}$.

For every $1 \leq j \leq m$, $k \in \mathbb{Z}$, *let us write* $c_{j,k} := h(\phi^k(u_j)) \in \mathbb{C}$. *Then, the assignment* $u_j \mapsto \widetilde{u}_j := (c_{j,k})_{k \in \mathbb{Z}}$ *defines (resp. induces) an injective morphism of difference fields between* $(\mathbf{K}, \phi)$ *(resp.* $(\mathbf{K}_R, \phi)$) *and* $(\mathbb{C}^{\mathbb{Z}}, \phi_s)$ *(resp.* $(\mathbb{R}^{\mathbb{Z}}, \phi_s)$), *where* ϕ_s *denotes the shift.*

Proof of Lemma 8. Let us prove that there exists $h : \mathbf{K} \to \mathbb{C}$, injective morphism of fields. Let t_j be a transcendental basis of $\mathbf{K}|\mathbb{Q}$. Since $\mathbf{K}|\mathbb{Q}$ is generated as a field by a countable number of elements, the number of elements in the transcendental basis is countable. Using the fact that $\mathbb{R}$ is not countable, we find that there exists $h : \mathbb{Q}(t_j) \to \mathbb{R}$, injective morphism of fields. Let us extend h to $\mathbf{K}$. The elements of $\mathbf{K}|\mathbb{Q}(t_j)$, satisfy a list of algebraic equations, which have a solution in an extension

of $\mathbb{C}$. Since $\mathbb{C}$ is algebraically closed, we find that the equations have a solution in $\mathbb{C}$. In other words, we have the existence of an embedding of $\mathbf{K}$ into $\mathbb{C}$.

Let us prove that $\mathbb{K}_R := h(\mathbf{K}_R) \subset \mathbb{R}$. Let t_j be a transcendental basis of $\mathbf{K}_R | \mathbb{Q}$. We have $h(\mathbb{Q}(t_j)) \subset \mathbb{K}_R \subset \mathbb{C}$. Since h is an injective morphism of fields and $\mathbf{K}_R$ is a real field, we find that $\mathbb{K}_R$ is a real field. Then, we obtain that the real closure of $h(\mathbb{Q}(t_j))$ contains $\mathbb{K}_R$. Since by construction $h(\mathbb{Q}(t_j)) \subset \mathbb{R}$ we find that the real closure of $h(\mathbb{Q}(t_j))$ is contained in $\mathbb{R}$. Then, we conclude that $\mathbb{K}_R \subset \mathbb{R} \subset \mathbb{C}$.

Let $P \in \mathbb{Q}\{X_1, \ldots, X_m\}_\phi$. We have the following equality $P(\widetilde{u}_1, \ldots, \widetilde{u}_m) = P((c_{1,k})_{k \in \mathbb{Z}}, \ldots, (c_{m,k})_{k \in \mathbb{Z}})$. Therefore, $P(u_1, \ldots, u_m) = 0$ if and only if $P(\widetilde{u}_1, \ldots, \widetilde{u}_m) = 0$. This shows that the assignment $u_j \mapsto \widetilde{u}_j := (c_{j,k})_{k \in \mathbb{Z}}$ defines (resp. induces) an injective morphism of difference fields between $(\mathbf{K}, \phi)$ (resp. $(\mathbf{K}_R, \phi)$) and $(\mathbb{C}^{\mathbb{Z}}, \phi_s)$ (resp. $(\mathbb{R}^{\mathbb{Z}}, \phi_s)$). $\qquad\square$

Proof of Theorem 7. (1) Let us prove the existence of a real Picard-Vessiot extension. We have seen how to construct (R, ϕ), Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$. Let $U \in \mathrm{GL}_n(R)$ be a fundamental solution. As we can see in Proposition 5, R is a direct sum of integral domains and we may define K, the total ring of fractions of R. The ring K is a direct sum of fields $K := \bigoplus_{j=0}^{t-1} K_j$ satisfying $\phi(K_j) = K_{j+1}$, $K_t := K_0$. Therefore, for all $0 \le j \le t-1$, (K_j, ϕ^t) is a difference field. Let $(\mathcal{K}, \phi)$ be the difference subring of (K, ϕ) generated over $\mathbb{Q}$ by the components on the K_j, $0 \le j \le t-1$, of the entries of U, $\det(U)^{-1}$, and the elements in $\mathbf{k}$ involved in the algebraic difference relations between the entries of U and $\det(U)^{-1}$. In particular, the entries of the matrix A of (2) belong to $\mathcal{K}$. As we can see from Lemma 8, for all $0 \le j \le t-1$, there exists $\widetilde{h}_j$, an embedding of $(\mathcal{K} \cap K_j, \phi^t)$ into $(\mathbb{C}^{\mathbb{Z}}, \phi_s)$. If $t > 1$, without loss of generality, we may assume that for all $0 \le j \le t-2$, (resp. for $j = t-1$), for all $u \in \mathcal{K} \cap K_j$, $\widetilde{h}_j(u) = \widetilde{h}_{j+1}(\phi(u))$ (resp. $\phi_s\left(\widetilde{h}_0(\phi(u))\right) = \widetilde{h}_{t-1}(u)$). We may define $\widetilde{h}$, an embedding of the difference ring $(\mathcal{K}, \phi)$ into the difference ring $(\mathbb{C}^{\mathbb{Z}}, \phi_s)$ as follows. Let $k = \sum_{j=0}^{t-1} k_j$ with $k \in \mathcal{K}$, $k_j \in K_j$ and let us define $\widetilde{h}(k) \in \mathbb{C}^{\mathbb{Z}}$ as the sequence which term number $c + dt$, with $0 \le c \le t-1$, $d \in \mathbb{Z}$, equals the term number d of $\widetilde{h}_c(k_c)$. Furthermore, since $\mathbf{k}$ is a real field, we find, see Lemma 8, that for all $k \in (\mathcal{K} \cap \mathbf{k}, \phi)$, $\widetilde{h}(k) \in \mathbb{R}^{\mathbb{Z}}$.

Let $C_{r,1}, \ldots, C_{r,n}$, (resp. $C_{i,1}, \ldots, C_{i,n}$) be the real parts (resp. the imaginary parts) of the columns of the term number zero of $\widetilde{h}(U)$. We recall that U is invertible. Therefore, the term number zero of $\widetilde{h}(U)$ is invertible. Then, we may extract n columns $C_1, \ldots, C_n \in \{C_{r,1}, \ldots, C_{r,n}, C_{i,1}, \ldots, C_{i,n}\}$, that are linearly independent. Therefore, there exists B a matrix with entries in $\mathbb{Q}[i]$, such that the term number zero of $\widetilde{h}(U)B$ has columns $C_1, \ldots, C_n$, and is consequently real and invertible. Then, the term number zero of $\widetilde{h}(U)B$ is invertible. Since the term number zero of $\widetilde{h}(U)$ is also invertible, we find that $B \in \mathrm{GL}_n(\mathbb{Q}[i])$. Let $V := UB$ be a fundamental solution, which belongs to $\mathrm{GL}_n(\mathcal{K}[i])$. The map $\widetilde{h}$ extends to a morphism of difference rings between $(\mathcal{K}[i], \phi)$ and $(\mathbb{C}^{\mathbb{Z}}, \phi_s)$. Consequently, we have $\widetilde{V} := \widetilde{h}(V) = \widetilde{h}(U)\widetilde{h}(B)$.

Let $(\widetilde{\mathbb{Q}}, \phi_s)$ be the difference subring of $(\mathbb{Q}^{\mathbb{Z}}, \phi_s)$ of constant sequences. Note that $(\widetilde{\mathbb{Q}}, \phi_s)$ is a difference field. Let $(\widetilde{\mathbf{k}}, \phi_s)$ be the difference subring of $(\mathbb{R}^{\mathbb{Z}}, \phi_s)$ generated over $(\widetilde{\mathbb{Q}}, \phi_s)$, by the elements $\widetilde{h}(k)$, $k \in (\mathcal{K} \cap \mathbf{k}, \phi)$. Note that $(\widetilde{\mathbf{k}}, \phi_s)$ is a difference field. We recall that since $\mathbf{k}$ is a real field, Lemma 8 tells us that

$\widetilde{h}(A) \in (\mathrm{GL}_n(\mathbb{R}))^{\mathbb{Z}}$. Since the term number zero of $\widetilde{V}$ belongs to $\mathrm{GL}_n(\mathbb{R})$, and $\phi_s(\widetilde{V}) = \widetilde{h}(A)\widetilde{V}$, we obtain that $\widetilde{V} \in (\mathrm{GL}_n(\mathbb{R}))^{\mathbb{Z}}$. Let $(\widetilde{R}, \phi_s)$ be the difference subring of $(\mathbb{R}^{\mathbb{Z}}, \phi_s)$ generated over $(\widetilde{\mathbf{k}}, \phi_s)$ by the entries of $\widetilde{V}$, and $\det(\widetilde{V})^{-1}$.

We claim that $(\widetilde{R}, \phi_s)$ is a simple difference ring. To the contrary, assume that there exists I, a difference ideal of $\widetilde{R}$ different from (0) and $\widetilde{R}$. It follows that $I(\widetilde{R}[i])$ is different from (0) and $\widetilde{R}[i]$. We have a natural embedding from $(\widetilde{R}, \phi_s)$ into $(R[i], \phi)$. Then, $I(\widetilde{R}[i])$ induces a difference ideal of $(R[i], \phi)$, which is different from (0) and $R[i]$. Let us separately treat the two cases. If $R = R[i]$, then we use the fact that the Picard-Vessiot extension $(R[i], \phi)$ is a simple difference ring to conclude that we have a contradiction and $(\widetilde{R}, \phi_s)$ is a simple difference ring. If $R \neq R[i]$, we use Lemma 4, to deduce that $(R[i], \phi)$ is a Picard-Vessiot extension for (2) over $(\mathbf{k}[i], \phi)$ and therefore, is a simple difference ring. We find a contradiction and we have proved our claim, that is, that $(\widetilde{R}, \phi_s)$ is a simple difference ring. We additionally use the fact that by construction $\widetilde{R}$ is a real ring to prove that $(\widetilde{R}, \phi_s)$ is a real Picard-Vessiot extension for $\phi\widetilde{Y} = \widetilde{h}(A)\widetilde{Y}$, over $(\widetilde{\mathbf{k}}, \phi_s)$.

Let R_1, be the difference ring generated over $\mathcal{K} \cap \mathbf{k}$ by the entries of the fundamental solution V and $\det(V)^{-1}$. Using the fact that $(\widetilde{\mathbf{k}}, \phi_s)$ is isomorphic to $(\mathcal{K} \cap \mathbf{k}, \phi)$, and $(\widetilde{R}, \phi_s)$ is a real Picard-Vessiot extension for $\phi\widetilde{Y} = \widetilde{h}(A)\widetilde{Y}$, over $(\widetilde{\mathbf{k}}, \phi_s)$, we obtain that R_1 is a real Picard-Vessiot extension for (2) over $(\mathcal{K} \cap \mathbf{k}, \phi)$.

Let us prove that $R_2 := R_1 \otimes_{\mathcal{K} \cap \mathbf{k}} \mathbf{k}$ is a real Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$. By construction, R_2 is generated over $\mathbf{k}$ by the entries of V and $\det(V)^{-1}$. It is sufficient to prove that R_2 is a simple difference ring which is real.

We claim that R_2 is a real ring. Let $a_j \in R_2$ such that $\sum_j (a_j)^2 = 0$. Let us write $a_j = \sum_\ell r_{j,\ell} \otimes_{\mathcal{K} \cap \mathbf{k}} k_{j,\ell}$, with $r_{j,\ell} \in R_1$, $k_{j,\ell} \in \mathbf{k}$. With $\sum_j (a_j)^2 = 0$, we obtain an algebraic relation over $\mathbb{Q}$ between the $r_{j,\ell}$ and the $k_{j,\ell}$. Note that $R_1 \subset R_2 \subset K[i]$. Then, as a consequence of the definition of $\mathcal{K}$, we find that $\mathcal{K}[i]$ is the difference subring of $(K[i], \phi)$ generated over $\mathbb{Q}$ by i, the components on the $K_j[i]$, $0 \le j \le t-1$, of the entries of V, $\det(V)^{-1}$, and the elements in $\mathbf{k}$ involved in the algebraic difference relations between the entries of V and $\det(V)^{-1}$. Furthermore, since i in an algebraic number that does not belong to the real field $\mathbf{k}$, and $V = UB$, with $U \in \mathrm{GL}_n(\mathcal{K})$, $B \in \mathrm{GL}_n(\mathbb{Q}[i])$, we find that the elements in $\mathbf{k}$ involved in the latter relations are in fact involved in algebraic difference relations between the entries of U and $\det(U)^{-1}$, proving that they belong to $\mathcal{K}$. Hence, we find that for all j, ℓ, $r_{j,\ell} \in R_1 \cap \mathcal{K}[i]$ and $k_{j,\ell} \in \mathbf{k} \cap \mathcal{K}$. Therefore, for all j, $a_j \in R_1$. Since R_1 is a real ring, we find that for all j, $a_j = 0$, proving that R_2 is a real ring.

It is now sufficient to prove that (R_2, ϕ) is a simple difference ring. Let $I \neq (0)$ be a difference ideal of (R_2, ϕ). Since $V = UB$, with $V \in \mathrm{GL}_n(R_2)$, $U \in \mathrm{GL}_n(R)$, and $B \in \mathrm{GL}_n(\mathbb{Q}[i])$, we find that $R_2[i] = R[i]$. The difference ideal I induces the difference ideal $I[i]$ of $(R[i], \phi)$. Let us separately treat the two cases. If $R[i] = R$, then $(R[i], \phi)$ is a simple difference ring since it is a Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$, proving that $I[i] = R[i]$ and $I = R_2$. Therefore, (R_2, ϕ) is a simple difference ring and a real Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$. Assume that $R[i] \neq R$. With Lemma 4, $(R[i], \phi)$ is a Picard-Vessiot extension for (2) over $(\mathbf{k}[i], \phi)$. Then, $(R[i], \phi)$ is a simple difference ring and $I[i] = R_2[i]$, proving that $I = R_2$. This shows that (R_2, ϕ) is a simple difference ring and a real Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$.

(2) With Lemma 4 we find that $(R[i], \phi)$ is a Picard-Vessiot extension for (2) over $(\mathbf{k}[i], \phi)$. Recall that by assumption, $C[i]$ is algebraically closed. As we can deduce from [vdPS97, Lemma 1.8], $R[i]^\phi = C[i]$. It follows that $R^\phi \subset C[i]$. By assumption, R is a real ring. This implies that $i \notin R$. Therefore, $C = \mathbf{k}^\phi \subset R^\phi$. Hence, the field of constants of R is C.

(3) Let us assume that, $R_1 \otimes_{\mathbf{k}} R_2 \neq R_1 \otimes_{\mathbf{k}} R_2[i]$ and let us prove that (R_1, ϕ_1) is isomorphic to (R_2, ϕ_2) over $(\mathbf{k}, \phi)$. We recall, see Lemma 4, that for $j \in \{1, 2\}$, $(R_j[i], \phi_j)$, is a Picard-Vessiot extension for (2) over $(\mathbf{k}[i], \phi)$. We also recall that the field of constants of $\mathbf{k}[i]$ is $C[i]$. Due to [vdPS97, Proposition 1.9], we find that $(R_1[i], \phi_1)$ is isomorphic to $(R_2[i], \phi_2)$ over $(\mathbf{k}[i], \phi)$. Let $\varphi : R_1 \to R_2[i]$ be the restriction of the morphism. Then, we may define a morphism of difference rings

$$\Psi : \quad \begin{aligned} R_1 \otimes_{\mathbf{k}} R_2 &\to R_2[i] \\ x \otimes y &\mapsto \varphi(x)y. \end{aligned}$$

The morphism Ψ is an R_2-linear map, and the image of $R_1 \otimes_{\mathbf{k}} R_2$ under Ψ is an R_2-submodule of $R_2[i]$, called V.

The assumption $R_1 \otimes_{\mathbf{k}} R_2 \neq R_1 \otimes_{\mathbf{k}} R_2[i]$ implies that there are no $f \in R_1 \otimes_{\mathbf{k}} R_2$ such that $f^2 + 1 = 0$. Since Ψ is a morphism of difference ring, there are no $g \in V$ such that $g^2 + 1 = 0$, which proves $i \notin V$. Combining this fact with the inclusion $R_2 \subset V$, we obtain that $V = R_2$ (we recall that V is an R_2-submodule of $R_2[i]$). In other words, the image of R_1 under φ is included in R_2. This implies that (R_1, ϕ_1) is isomorphic to (R_2, ϕ_2) over $(\mathbf{k}, \phi)$.

Conversely, if (R_1, ϕ_1) is isomorphic to (R_2, ϕ_2) over $(\mathbf{k}, \phi)$, then there exists a morphism of difference rings $\varphi : R_1 \to R_2$. As above, let us define Ψ, morphism of difference rings between $R_1 \otimes_{\mathbf{k}} R_2$ and R_2 defined by $\Psi(x \otimes y) = \varphi(x)y$. Since R_2 is a real ring, we find that $R_2 \neq R_2[i]$. Since Ψ is a morphism of difference rings, we obtain that $R_1 \otimes_{\mathbf{k}} R_2 \neq R_1 \otimes_{\mathbf{k}} R_2[i]$. □

The following example, who is inspired by [CHS13], illustrates a situation where two Picard-Vessiot extensions are not isomorphic.

Example 9. Let $\phi := f(z) \mapsto f(2z)$ and consider $\phi Y = \sqrt{2}Y$ which has coefficients in $\mathbb{R}(x)$. Let us consider the following fundamental solutions $(\sqrt{x})$ and $(i\sqrt{x})$. Consider the corresponding difference ring extensions $R_1|\mathbb{R}(x) := \mathbb{R}\left[\sqrt{x}, \sqrt{x}^{-1}\right]|\mathbb{R}(x)$ and $R_2|\mathbb{R}(x) := \mathbb{R}\left[i\sqrt{x}, (i\sqrt{x})^{-1}\right]$. Let us prove that (R_1, ϕ) is a simple difference ring. The proof for (R_2, ϕ) is similar. Let $I \neq (0)$ be a difference ideal of R_1 and let $P \in \mathbb{R}[X]$ with minimal degree such that $P(\sqrt{x}) \in I$. Let $k \in \mathbb{N}$ be the degree of P. Assume that $k \neq 0$. We have $\phi(P(\sqrt{x})) = P(\sqrt{2}\sqrt{x}) \in I$, which shows that $\phi(P(\sqrt{x})) - \sqrt{2}^k P(\sqrt{x}) = Q(\sqrt{x}) \in I$ where $Q \in \mathbb{R}[X]$ has degree less than k. This is in contradiction with the minimality of k, and shows that $k = 0$. This implies that $I = R_1$, which proves that (R_1, ϕ) is a simple difference ring. Since R_1 and R_2 are real rings, $R_1|\mathbb{R}(x)$ and $R_2|\mathbb{R}(x)$ are two real Picard-Vessiot extensions for $\phi Y = \sqrt{2}Y$ over $(\mathbb{R}(x), \phi)$. Note that there are no difference ring isomorphisms between (R_1, ϕ) and (R_2, ϕ) over $\mathbb{R}(x)$ because $X^2 = x$ has a solution in R_1 and no solutions in R_2. This is not in contradiction with Theorem 7 since $R_1 \otimes_{\mathbb{R}(x)} R_2 = R_1 \otimes_{\mathbb{R}(x)} R_2[i]$, because

$$\left(\sqrt{x} \otimes_{\mathbb{R}(x)} \frac{1}{i\sqrt{x}}\right)^2 = -1.$$

3. Real difference Galois group

In this section, we still consider (2). Let (R, ϕ) be a real Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$ with fundamental solution $U \in \mathrm{GL}_n(R)$. Consider the difference ring $(R[i], \phi)$, which is different from (R, ϕ), since R is a real ring. From [CHS13], let us define the real difference Galois group as follows:

Definition 10. We define $G_{R[i]}$, as the group of difference ring automorphisms of $R[i]$ letting $\mathbf{k}[i]$ be invariant. We define G, the real difference Galois group of (2), as the group $\{\varphi_{|R}, \varphi \in G_{R[i]}\}$.

Note that elements of G are maps from R to $R[i]$. Due to Theorem 7, (2), we have an injective group morphism

$$
\rho_U : \quad \begin{array}{ccc} G & \longrightarrow & \mathrm{GL}_n(C[i]) \\ \varphi & \longmapsto & U^{-1}\varphi(U), \end{array}
$$

which depends on the choice of the fundamental solution U in R. Another choice of a fundamental solution in R will gives a representation that is conjugated to the first one.

Recall, see Proposition 5, that there exist an idempotent $e \in R$, and $t \in \mathbb{N}^*$, such that $\phi^t(e) = e$, $R = \bigoplus_{j=0}^{t-1} \phi^j(e)R$, and for all $0 \leq j \leq t-1$, $\phi^j(e)R$ is an integral domain. Due to Lemma 4, $(R[i], \phi)$ is a Picard-Vessiot extension for (2) over $(\mathbf{k}[i], \phi)$. Furthermore, $R[i] = \bigoplus_{j=0}^{t-1} \phi^j(e)R[i]$ and the total ring of fractions of $R[i]$ equals $K[i]$, where K is the total ring of fractions of R. Then, we call $G_{K[i]}$, the classical difference Galois group of (2), the group of difference ring automorphisms of $K[i]$ letting $\mathbf{k}[i]$ be invariant. See [vdPS97] for more details. The difference Galois group of (2) may also be seen as a subgroup of $\mathrm{GL}_n(C[i])$. Furthermore, its image in $\mathrm{GL}_n(C[i])$ is a linear algebraic subgroup of $\mathrm{GL}_n(C[i])$. We have the following result in the real case.

Proposition 11. *Let (R, ϕ) be a real Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$ with fundamental solution $U \in \mathrm{GL}_n(R)$. Let G be the real difference Galois group of (2) and $G_{K[i]}$ be the difference Galois group of (2). We have the following equality:*
$$
Im\ \rho_U = \left\{U^{-1}\varphi(U), \varphi \in G\right\} = \left\{U^{-1}\varphi(U), \varphi \in G_{K[i]}\right\}.
$$
Furthermore, $Im\ \rho_U$ is a linear algebraic subgroup of $\mathrm{GL}_n(C[i])$ defined over C. We will identify G with a linear algebraic subgroup of $\mathrm{GL}_n(C[i])$ defined over C for a chosen fundamental solution.

Proof. Let us prove the equality $\left\{U^{-1}\varphi(U), \varphi \in G\right\} = \left\{U^{-1}\varphi(U), \varphi \in G_{K[i]}\right\}$. Recall that $U \in \mathrm{GL}_n(R)$. Since an element of $G_{K[i]}$ induces an element of G, we obtain the inclusion $\left\{U^{-1}\varphi(U), \varphi \in G_{K[i]}\right\} \subset \left\{U^{-1}\varphi(U), \varphi \in G\right\}$. Let $\varphi \in G$. We may extend φ as an element $\varphi_{K[i]} \in G_{K[i]}$ by putting $\varphi_{K[i]}(i) = i$ and for all $0 \leq j \leq t-1$, $a, b \in \phi^j(e)R[i]$, $\varphi_{K[i]}(\frac{a}{b}) = \frac{\varphi_{K[i]}(a)}{\varphi_{K[i]}(b)}$. Since $U \in \mathrm{GL}_n(R)$, we find that $U^{-1}\varphi(U) = U^{-1}\varphi_{K[i]}(U)$. Therefore, we obtain the other inclusion $\left\{U^{-1}\varphi(U), \varphi \in G\right\} \subset \left\{U^{-1}\varphi(U), \varphi \in G_{K[i]}\right\}$ and the equality $\left\{U^{-1}\varphi(U), \varphi \in G\right\} = \left\{U^{-1}\varphi(U), \varphi \in G_{K[i]}\right\}$.

With a similar reasoning to what is above, we obtain the equalities:
$$
\left\{U^{-1}\varphi(U), \varphi \in G\right\} = \left\{U^{-1}\varphi(U), \varphi \in G_{K[i]}\right\} = \left\{U^{-1}\varphi(U), \varphi \in G_{R[i]}\right\}.
$$

We define G_R, as the group of difference ring automorphisms of R letting $\mathbf{k}$ be invariant. Due to Theorem 7, (2), (R, ϕ) is a weak Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$. Applying [CHS08, Proposition 2.2], we find that $\{U^{-1}\varphi(U), \varphi \in G_R\}$ is a linear algebraic subgroup of $\mathrm{GL}_n(C)$. Then, we may use [CHS08, Corollary 2.5], to find that the latter group, viewed as a linear algebraic subgroup of $\mathrm{GL}_n(C[i])$, equals $\{U^{-1}\varphi(U), \varphi \in G_{R[i]}\}$. We conclude the proof using the equality

$$\{U^{-1}\varphi(U), \varphi \in G\} = \{U^{-1}\varphi(U), \varphi \in G_{R[i]}\}.$$

$\square$

We finish this section by giving the Galois correspondence. See [vdPS97, Theorem 1.29] for the analogous statement in the case where C is algebraically closed.

Theorem 12. *Let (R, ϕ) be a real Picard-Vessiot extension for (2) over $(\mathbf{k}, \phi)$ with total ring of fractions K, $\mathcal{F}$ be the set of difference rings $\mathbf{k} \subset F \subset K$, and such that every non-zero divisor is a unit of F. Let G, be the real difference Galois group of (2), $\mathcal{G}$ be the set of linear algebraic subgroups of G.*

    (1) *For any $F \in \mathcal{F}$, the group $G(K/F)$ of elements of G letting F be invariant belongs to $\mathcal{G}$.*

    (2) *For any $H \in \mathcal{G}$, the ring $K^H := \{k \in K | \forall \varphi \in H, \varphi(k) = k\}$ belongs to $\mathcal{F}$.*

    (3) *Let $\alpha : \mathcal{F} \to \mathcal{G}$ and $\beta : \mathcal{G} \to \mathcal{F}$ denote the maps $F \mapsto G(K/F)$ and $H \mapsto K^H$. Then, α and β are each other's inverses.*

Remark 13. If we replace G by G_R, see the proof of Proposition 11, which is a more natural candidate for the definition of the real difference Galois group, we lose the Galois correspondence. Take for example $\phi Y(x) := Y(x + 1) = \exp(1)Y(x)$, which has solution $\exp(x)$. A real Picard-Vessiot extension for $Y(x + 1) = \exp(1)Y(x)$ over $(\mathbb{R}, \phi)$ is $(\mathbb{R}[\exp(x), \exp(-x)], \phi)$. Let $K := \mathbb{R}(\exp(x))$ be the total ring of fractions. We have $G \simeq \mathbb{C}^*$ and $G_R \simeq \mathbb{R}^*$. Note that $G_R \subset \mathrm{GL}_1(\mathbb{R})$, viewed as a linear algebraic subgroup of $\mathrm{GL}_1(\mathbb{C})$, equals G. On the other hand, we have no bijection with the linear algebraic subgroups of G_R, which are $\{1\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{R}^*$, and the difference subfields of K, which are $\mathbb{R}(\exp(kx))$, $k \in \mathbb{N}$.

Proof of Theorem 12. Let $\mathcal{F}_{[i]}$ be the set of difference rings $\mathbf{k}[i] \subset F \subset K[i]$, such that every non-zero divisor is a unit of F. Let $\mathcal{G}_{[i]}$ be the set of linear algebraic subgroups of $G_{K[i]}$. Recall that the field of constants of $\mathbf{k}[i]$ is algebraically closed. By virtue of the Galois correspondence in difference Galois theory, see [vdPS97, Theorem 1.29], we find that

(a) For any $F \in \mathcal{F}_{[i]}$, the group $G_{K[i]}(K[i]/F)$ of elements of $G_{K[i]}$ letting F invariant belongs to $\mathcal{G}_{[i]}$.

(b) For any $H \in \mathcal{G}_{[i]}$, the ring $K[i]^H$ belongs to $\mathcal{F}_{[i]}$.

(c) Let $\alpha_{[i]} : \mathcal{F}_{[i]} \to \mathcal{G}_{[i]}$ and $\beta_{[i]} : \mathcal{G}_{[i]} \to \mathcal{F}_{[i]}$ denote the maps $F_{[i]} \mapsto G_{K[i]}(K[i]/F)$ and $H \mapsto K[i]^H$. Then, $\alpha_{[i]}$ and $\beta_{[i]}$ are each other's inverses.

We use Proposition 5 to find that we have a bijection $\gamma : \mathcal{F} \to \mathcal{F}_{[i]}$ given by $\gamma(F) := F[i]$. The inverse is $\gamma^{-1}(F) = F \cap K$. Now, let us remark that since the fundamental solution has coefficients in R, for all $F \in \mathcal{F}$, $G(K/F) = G_{K[i]}(K[i]/\gamma(F))$. If we combine this fact with (a) and Proposition 11, we find (1).

Proposition 11 tells us that we may identify the groups in $\mathcal{G}$ with the corresponding groups in $\mathcal{G}_{[i]}$. To prove the point (2), we remark that for all $H \in \mathcal{G}$, $K[i]^H = K^H[i]$. Combined with (b), this shows the point (2) since $K^H = \gamma^{-1}(K[i]^H) \in \mathcal{F}$.

The point (3) follows from (c) and the fact that for all $F \in \mathcal{F}$ (resp. $H \in \mathcal{G}$) we have $G(K/F) = G_{K[i]}(K[i]/\gamma(F))$ (resp. $K[i]^H = \gamma(K^H)$). $\qquad\square$

ACKNOWLEDGMENT

REFERENCES

[BB62]   A. Białynicki-Birula, *On Galois theory of fields with operators*, Amer. J. Math. **84** (1962), 89–109, DOI 10.2307/2372805. MR0141663

[CH15]   Teresa Crespo and Zbigniew Hajto, *Real Liouville extensions*, Comm. Algebra **43** (2015), no. 5, 2089–2093, DOI 10.1080/00927872.2014.888561. MR3316840

[CHS08]   Zoé Chatzidakis, Charlotte Hardouin, and Michael F. Singer, *On the definitions of difference Galois groups*, Model theory with applications to algebra and analysis. Vol. 1, London Math. Soc. Lecture Note Ser., vol. 349, Cambridge Univ. Press, Cambridge, 2008, pp. 73–109, DOI 10.1017/CBO9780511735226.006. MR2441376

[CHS13]   Teresa Crespo, Zbigniew Hajto, and Elżbieta Sowa, *Picard-Vessiot theory for real fields*, Israel J. Math. **198** (2013), no. 1, 75–89, DOI 10.1007/s11856-013-0015-x. MR3096631

[CHvdP16] Teresa Crespo, Zbigniew Hajto, and Marius van der Put, *Real and p-adic Picard-Vessiot fields*, Math. Ann. **365** (2016), no. 1-2, 93–103, DOI 10.1007/s00208-015-1272-2. MR3498905

[Coh65]   Richard M. Cohn, *Difference algebra*, Interscience Publishers John Wiley & Sons, New York-London-Sydeny, 1965. MR0205987

[Dyc05]   Tobias Dyckerhoff, *Picard-vessiot extensions over number fields.*, Fakultat fur Mathematik und Informatik der Universitat Heidelberg, diplomarbeit, 2005.

[Fra63]   Charles H. Franke, *Picard-Vessiot theory of linear homogeneous difference equations*, Trans. Amer. Math. Soc. **108** (1963), 491–515, DOI 10.2307/1993595. MR0155819

[HS08]   Charlotte Hardouin and Michael F. Singer, *Differential Galois theory of linear difference equations*, Math. Ann. **342** (2008), no. 2, 333–377, DOI 10.1007/s00208-008-0238-z. MR2425146

[Lam84]   T. Y. Lam, *An introduction to real algebra*, Rocky Mountain J. Math. **14** (1984), no. 4, 767–814, DOI 10.1216/RMJ-1984-14-4-767. Ordered fields and real algebraic geometry (Boulder, Colo., 1983). MR773114

[Mor09]   Shuji Morikawa, *On a general difference Galois theory. I* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **59** (2009), no. 7, 2709–2732. MR2649331

[MU09]   Shuji Morikawa and Hiroshi Umemura, *On a general difference Galois theory. II* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **59** (2009), no. 7, 2733–2771. MR2649332

[Sei58]   A. Seidenberg, *Abstract differential algebra and the analytic case*, Proc. Amer. Math. Soc. **9** (1958), 159–164, DOI 10.2307/2033416. MR0093655

[vdPS97]   Marius van der Put and Michael F. Singer, *Galois theory of difference equations*, Lecture Notes in Mathematics, vol. 1666, Springer-Verlag, Berlin, 1997. MR1480919

UNIVERSITÉ CLAUDE BERNARD LYON 1, INSTITUT CAMILLE JORDAN, 43 BOULEVARD DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE, FRANCE

E-mail address: `dreyfus@math.univ-lyon1.fr`