DIFFERENTIAL GALOIS CORRESPONDENCE

PEDRO NÚÑEZ

Abstract. Script for a talk on differential Galois correspondence following [PS03, §1]. I would like to thank Annette Huber-Klavitter for useful discussions while preparing this talk.

Contents

—parts in gray will be omitted during the talk—

1. Introduction

Let k be a differential field of characteristic zero with algebraically closed subfield of constants C, $n \in \mathbb{N}$ and $A \in \mathrm{M}_n(k)$ an $n \times n$ matrix with entries in k. We consider a matrix differential equation over k of dimension n of the form

$$\begin{pmatrix} y_1' \\ \vdots \\ y_n' \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}, \tag{1}$$

which we will also write as $y' = Ay$ using the convention that the derivation acts entry-wise. We would like to find n solution vectors linearly independent over C, but this may not be possible in k^n. This motivates passing to a Picard-Vessiot extension $k \subseteq L$, in which some $F \in \mathrm{GL}_n(L)$ such that $F' = AF$ exists. Fixing such a *fundamental matrix* F we obtain an embedding of the group $\mathrm{Gal}(L/k)$ of differential k-automorphisms of L into $\mathrm{GL}_n(C)$ which expresses $\mathrm{Gal}(L/k)$ as a linear algebraic algebraic group, i.e., a Zariski-closed subgroup of $\mathrm{GL}_n(C)$. Our goal is to prove the Galois correspondence in this context:

Date: 1st June 2022.

The author gratefully acknowledges support by the DFG-Graduiertenkolleg GK1821 "Cohomological Methods in Geometry" at the University of Freiburg.

Theorem 1. *In the setting above, there is an inclusion reversing bijection between closed subgroups of* $\mathrm{Gal}(L/k)$ *and intermediate differential fields of* $k \subseteq L$ *given by sending a subgroup* H *to the fixed field* L^H *and a subfield* M *to the Galois group* $\mathrm{Gal}(L/M)$.

2. Recollections from previous talks

Most of the necessary results have already been discussed in earlier talks, so today's talk is more about putting the various ingredients together. In particular, it is a good opportunity to recall the things that we have seen so far. So let us recall all the objects involved in the statement through a couple of concrete examples.

2.1. **The differential field.** We are working over a differential field k of characteristic zero. This means that k is a field of characteristic zero together with a *derivation* on k, i.e., a function $(-)' \colon k \to k$ such that

$$(a+b)' = a' + b' \text{ and } (ab)' = a'b + ab'$$

for all $a, b \in k$. Inside k we have the subset of *constants*

$$C := \{a \in k \mid a' = 0\},$$

which is a subfield of k [PS03, Exercises 1.5.2]. We work under the assumption that C is an algebraically closed field. We will consider the fields $\mathbb{C}(t)$ and $\mathbb{C}(e^{3t})$ with the usual derivation. In both cases the field of constants is $\mathbb{C}$.

2.2. **The differential equation.** Throughout the recollection we will focus on the 1-dimensional equation $y' = y$. In this case, a fundamental matrix over some extension of differential rings $k \subseteq R$ consists of an invertible element $u \in R^\times$ such that $u' = u$. Neither in $k = \mathbb{C}(t)$ nor in $k = \mathbb{C}(e^{3t})$ we have such an element u, so in both cases we need to consider non-trivial extensions to find non-zero solutions to the equation.

2.3. **The Picard-Vessiot ring.** The *Picard-Vessiot ring* of Equation (1) over k is defined as a differential ring R over k satisfying the following properties:

(1) The differential ring R is a simple differential ring, i.e., its only differential ideals are 0 and R.
(2) There exists a fundamental matrix $F \in \mathrm{GL}_n(R)$, i.e., a matrix $F \in \mathrm{GL}_n(R)$ such that $F' = AF$.
(3) The k-algebra R is generated by the entries of a fundamental matrix F and the inverse of the determinant of F.

As we pointed out earlier, the Picard-Vessiot ring for $y' = y$ over k will be a non-trivial extension both in the case of $k = \mathbb{C}(t)$ and in the case of $k = \mathbb{C}(e^{3t})$. In order to write it down explicitly we start by adding a formal solution, i.e., we consider $k[X, X^{-1}]$ with the derivation extending the one on k such that $X' = X$, cf. [PS03, Exercises 1.5.1]. In this ring we have now

a fundamental matrix given by X itself, because X is a unit and $X' = X$. So conditions (2) and (3) in the definition of the Picard-Vessiot ring are satisfied. But we still need to study condition (1).

Let us first deal with the case $k = \mathbb{C}(t)$. In this case the claim is that $R = k[X, X^{-1}]$ is already a simple differential ring, hence a Picard-Vessiot ring for the equation $y' = y$ over k. Indeed, let (P) be a non-zero differential ideal for some $P = X^m + \cdots + a_1X + a_0$. Multiplying by the appropriate power of X^{-1} we may assume that $a_0 \neq 0$, and our goal is to show that $m = 0$, i.e., that $P = a_0$ is a unit and thus $(P) = R$. Assume that $m > 0$. Since (P) is a differential ideal, $P' = mX^m + \cdots + a_1X \in (P)$, so $P' - mP \in (P)$ and from degree comparison we deduce that $P' = mP$. But this would imply that $a_0 = 0$, a contradiction. Hence $m = 0$ and $(P) = R$.

Let us now consider the case $k = \mathbb{C}(e^{3t})$. In the previous case we needed the full transcendental extension $k[X, X^{-1}]$, but in this case it will sufice to find a third root of e^{3t}, so we should expect to find some maximal differential ideal such that the quotient gives the desired algebraic extension of k. We look at the ideal $I = (X^3 - e^{3t})$ in $k[X, X^{-1}]$. Since $(X^3 - e^{3t})' = 3(X^3 - e^{3t}) \in I$, this is a non-zero differential ideal. We let $R = k[X, X^{-1}]/I$ be the quotient, which is then a differential ring [PS03, Exercises 1.5.1]. We can also regard R as the localization of $k[X]/(X^3 - e^{3t})$ at the set of powers of the image of X, because localization is exact. But $X^3 - e^{3t}$ is irreducible in $k[X]$, because it is of degree 3 and has no root, so $k[X]/(X^3 - e^{3t})$ is a field already and therefore so is R. This shows that R is a Picard-Vessiot ring in this case.

2.4. **The Picard-Vessiot field.** A Picard-Vessiot ring for Equation (1) over k always exists, and any two Picard-Vessiot rings for this equation are isomorphic [PS03, Proposition 1.20]. Moreover, Picard-Vessiot rings are integral domains [PS03, Lemma 1.17] and their quotient fields still have C as field of constants [PS03, Proposition 1.20]. The quotient field of a Picard-Vessiot ring for Equation (1) is called a *Picard-Vessiot field* for this equation, and by [PS03, Proposition 1.22] it can also be characterized as an extension of differential fields $L \supseteq k$ such that the following properties hold:

(1) The field of constants of L is C.
(2) There exists a fundamental matrix $F \in \mathrm{GL}_n(L)$.
(3) The field L is generated by the entries of F over k.

A Picard-Vessiot field for $y' = y$ over $k = \mathbb{C}(t)$ is then the quotient field of $k[X, X^{-1}]$, i.e., the ring $k(X) = \mathbb{C}(t, X)$. On the other hand, the Picard-Vessiot ring for $y' = y$ over $k = \mathbb{C}(e^{3t})$ discussed above is already a Picard-Vessiot field for $y' = y$ over $\mathbb{C}(e^{3t})$, because it is a field and hence isomorphic to its quotient field.

2.5. **The differential Galois group.** Given an equation $y' = Ay$ over k of dimension n, we are looking for its *differential Galois group*. By definition this is the group $\mathrm{Gal}(R/k)$ of differential k-algebra automorphisms of

a Picard-Vessiot ring R for the equation, i.e., the group of k-algebra automorphisms $\sigma\colon R \to R$ such that $\sigma(f') = \sigma(f)'$ for all $f \in R$.

We start by computing the differential Galois group of $y' = y$ over $\mathbb{C}(t)$. In this case we have $R = \mathbb{C}(t)[X, X^{-1}]$ with $X' = X$, and a $\mathbb{C}(t)$-algebra automorphism $\sigma\colon R \to R$ is uniquely determined by $\sigma(X)$. Since $\sigma(X)' = \sigma(X') = \sigma(X)$, $\sigma(X)$ has to be a solution of $y' = y$ in R, hence of the form $c_\sigma X$ for some $c_\sigma \in \mathbb{C}^\times$. This shows that $\mathrm{Gal}(R/\mathbb{C}(t)) \cong (\mathbb{C}^\times, \cdot)$.

We compute now the Galois group of the same equation $y' = y$ over $\mathbb{C}(e^{3t})$. In this case $R = L \cong \mathbb{C}(e^{3t})[X]/(X^3 - e^{3t})$ is an algebraic extension obtained by taking the 3-rd root of an element in $\mathbb{C}(e^{3t})$, and this field already contains all 3-rd roots of unity, so this is a Kummer extension with Galois group $\mathbb{Z}/3\mathbb{Z}$ [Bos18, §4.9]. Explicitly, writing $L = k(\alpha)$ for an $\alpha \in L$ such that $\alpha^3 = e^{3t}$ and $\alpha' = \alpha$ and $\zeta_3 \in \mathbb{C}(e^{3t})$ for a primitive 3-rd root of unity, we have automorphisms $\sigma_i\colon \alpha \mapsto \zeta_3^i \alpha$ for $i \in \{0, 1, 2\}$. The isomorphism is given by $\sigma_i \mapsto i + 3\mathbb{Z}$ for each $i \in \{0, 1, 2\}$. We check that each of these σ_i is a differential automorphism, i.e., that it commutes with the derivation on L. By construction we have $\alpha' = \alpha$, hence

$$(\sigma_i(\alpha))' = \zeta_3^i \alpha' = \zeta_3^i \alpha = \sigma_i(\alpha) = \sigma_i(\alpha')$$

for all $i \in \{0, 1, 2\}$ and $\mathrm{Gal}(L/\mathbb{C}(e^{3t})) \cong \mathbb{Z}/3\mathbb{Z}$.

Let us also recall some useful results concerning differential Galois groups from previous talks:

Lemma 2 ([PS03, p. 19])**.** *If we fix a fundamental matrix $F \in \mathrm{M}_n(R)$, then we may regard $\mathrm{Gal}(R/k)$ as a subgroup of $\mathrm{GL}_n(C)$ by sending an automorphism σ to the uniquely determined constant matrix C_σ such that $\sigma(F) = FC_\sigma$. This gives us a faithful representation $\rho\colon \mathrm{Gal}(R/k) \to \mathrm{GL}(V)$, where $V := \{v \in R^n \mid v' = Av\}$ is the solution space of our equation, which is an n-dimensional C-vector space.*

Proof. Suppose such a matrix C_σ existed. Then we would have $C_\sigma = F^{-1}\sigma(F) \in \mathrm{GL}_n(R)$, so it is uniquely determined by F and σ. To show the existence we need to check that $C_\sigma' = 0$. For this we first observe that $\sigma(F)' = A\sigma(F)$, because σ is the identity on k and thus $\sigma(A) = A$. Therefore we have

$$AFC_\sigma = A\sigma(F) = \sigma(F)' = (FC_\sigma)' = F'C_\sigma + FC_\sigma' = AFC_\sigma + FC_\sigma',$$

hence $FC_\sigma' = 0$ and $C_\sigma' = 0$ because F is invertible. Thus we have a well-defined function $\mathrm{Gal}(R/k) \to \mathrm{GL}_n(C)$.

We check next that this is a group homomorphism. By the formula above we have

$$C_{\sigma_1 \circ \sigma_2} = F^{-1}\sigma_1\sigma_2(F) = F^{-1}\sigma_1(FF^{-1}\sigma_2(F)) = F^{-1}\sigma_1(FC_{\sigma_2}) = F^{-1}\sigma_1(F)C_{\sigma_2},$$

where in the last inequality we have used that $\sigma_1(C_{\sigma_2}) = C_{\sigma_2}$ because σ_1 is the identity on k. But we also have $F^{-1}\sigma_1(F) = C_{\sigma_1}$, hence $C_{\sigma_1 \circ \sigma_2} = C_{\sigma_1}C_{\sigma_2}$ as claimed. This shows that we have a group homomorphism.

We check next that this is an injective group homomorphism. Suppose $F^{-1}\sigma(F) = 1_n$ is the identitiy matrix. Then $\sigma(F) = F$. Since the entries and the inverse of the determinant of F generate R as a k-algebra, this implies that $\sigma(f) = f$ for all $f \in R$, hence $\sigma = \mathrm{id}_R$ and the group homomorphism is injective.

For the last statement, note that the columns of F form a C-basis of V. This fixes an isomorphism $\mathrm{GL}_n(C) \cong \mathrm{GL}(V)$. Hence this injective group homomorphism translates into a faithful representation $\rho\colon \mathrm{Gal}(R/k) \to \mathrm{GL}(V)$. □

Lemma 3 ([PS03, p. 19])**.** *Let L denote the quotient field of R, which is then by definition a Picard-Vessiot field for the equation. Let $\mathrm{Gal}(L/k)$ denote the group of k-linear automorphisms of L which commute with the derivation on L. Then there is a group isomorphism $\mathrm{Gal}(R/k) \to \mathrm{Gal}(L/k)$.*

Proof. Let $\sigma\colon R \to R$ be an automorphism in $\mathrm{Gal}(R/k)$. Since σ is bijective it extends to a k-linear automorphism $\tilde{\sigma}\colon L \to L$ given by

$$\tilde{\sigma}\left(\frac{f}{g}\right) = \frac{\sigma(f)}{\sigma(g)}.$$

We check that $\tilde{\sigma}$ commutes with the derivation on L:

$$\tilde{\sigma}\left(\left(\frac{f}{g}\right)'\right) = \frac{\sigma(f'g - fg')}{\sigma(g^2)} = \frac{\sigma(f)'\sigma(g) - \sigma(f)\sigma(g)'}{\sigma(g)^2} = \left(\frac{\sigma(f)}{\sigma(g)}\right)'.$$

Hence $\tilde{\sigma} \in \mathrm{Gal}(L/k)$. Moreover, the above formula for $\tilde{\sigma}$ shows that $\sigma_1 \tilde{\circ} \sigma_2 = \tilde{\sigma_1} \circ \tilde{\sigma_2}$, so $\sigma \mapsto \tilde{\sigma}$ is a group homomorphism. Since σ is determined by $\tilde{\sigma}$, this group homomorphism is injective. Let us show that it is also surjective.

Let $\tau \in \mathrm{Gal}(L/k)$. We want to show that the restriction of τ to R has image equal to R, i.e., that $\tau(R) = R$ when we identify R with a subring of L as usual. Let $F \in \mathrm{M}_n(R)$ be a fundamental matrix for our equation, so that the columns of F form a C-basis of the solution space $V = \{v \in R^n \mid v' = Av\}$. We regard F as a matrix with coefficients in L, and the same arguments as in the proof of Lemma 2 show that we can write $\tau(F) = FC_\tau$ for some $C_\tau \in \mathrm{GL}_n(C)$. Since the entries of F are all in R and $C \subseteq k$, the entries of $FC_\tau = \tau(F)$ are in R as well. Moreover, since

$$\frac{1}{\det(\tau(F))} = \frac{1}{\det(F)\det C_\tau}$$

and the right hand side is in R, so is the left hand side, which implies that $\tau(R) \in \mathrm{GL}_n(R)$. Since the k-algebra R is generated by the entries and the inverse of the determinant of F and τ is a k-algebra isomorphism, the k-algebra $\tau(R)$ is generated by the entries and the inverse of the determinant of $\tau(F)$, hence $\tau(R) \subseteq R$. Applying the same arguments to $\tau^{-1} \in \mathrm{Gal}(L/k)$ we deduce that $\tau^{-1}(R) \subseteq R$, hence $R \subseteq \tau(R)$ as well and $\tau(R) = R$. □

Let us denote $G := \mathrm{Gal}(L/k)$. We have seen in previous talks that G is an algebraic subgroup of $\mathrm{GL}_n(C)$, that the Lie algebra of G coincides with

the Lie algebra of the derivations of L/k that commute with the derivation on L and that the field L^G of G-invariant elements of L is equal to k [PS03, Theorem 1.27].

Moreover, we have also talked about torsors and seen that $Z := \mathrm{Spec}(R)$ is a G-torsor over k, i.e., there is a right G-action of G on Z such that for any $v, w \in Z(\bar{k})$ there exists a unique $g \in G(\bar{k})$ such that $v = wg$. Recall that a G-torsor was called trivial if there is a k-scheme isomorphism $Z \cong G$ which identifies $Z \times G \to G$ with the multiplication morphism. A G-torsor is trivial if and only if it has a k-rational point. One can think of torsors as principal G-bundles over a point, and this last statement corresponds to the topological statement that a principal G-bundle is trivial if and only if it admits a section. Intuitively, the difference between a G-torsor and G itself is that on a G-torsor we don't have a distinguished neutral element. A rational point or a seciton defines a notion of neutral element and this allows us to find the desired isomorphism. See [PS03, Appendix A.2.3] for more details.

3. Proof of the correspondence

We consider an equation $y' = Ay$ over k of dimension n and we let R be a Picard-Vessiot ring, L the quotient field of R, which is then a Picard-Vessiot field, and $G := \mathrm{Gal}(L/k)$ the differential Galois group, which is then isomorphic via restriction to the differential Galois group $\mathrm{Gal}(R/k)$. We denote by $\mathcal{S}$ the set of closed subgroups of G and by $\mathcal{L}$ the set of differential subfields of L containing k. The reference throughout this section is [PS03, Proposition 1.34]. We will use the following result from Christoph's talk:

Theorem 4 ([PS03, Theorem 1.27])**.** *Let $y' = Ay$ be a differential equation of degree n over k, having Picard-Vessiot field $L \supseteq k$ and differential Galois group $G = \mathrm{Gal}(L/k)$. Then*

1. *The group G, considered as a subgroup of $\mathrm{GL}_n(C)$, is an algebraic group.*
2. *The Lie algebra of G coincides with the Lie algebra of the derivations of L/k that commute with the derivation on L.*
3. *The field L^G of G-invariant elements of L is equal to k.*

We will also use the following result from Johan's talk:

Corollary 5 ([PS03, Corollary 1.30])**.** *Let R be a Picard-Vessiot ring for the equation $y' = Ay$ over k. Let L be the field of fractions of R. Put $Z = \mathrm{Spec}(R)$. Let G denote the differential Galois group and $C[G]$ the coordinate ring of G and let $\mathfrak{g}$ denote the Lie algebra of G. Then:*

1. *There is a finite extension $\tilde{k} \supseteq k$ such that $Z_{\tilde{k}} \cong G_{\tilde{k}}$.*
2. *The scheme Z is smooth and connected.*
3. *The transcendence degree of L/k is equal to the dimension of G.*
4. *Let H be a subgroup of G with Zariski closure $\overline{H}$. Then $L^H = k$ if and only if $\overline{H} = G$.*

Particularly relevant will be the last statements of both results, i.e., that $L^G = k$ and that $L^H = k$ implies that $\overline{H} = G$ for subgroups $H \subseteq G$.

Lemma 6. *If H is a closed subgroup of G, then L^H is a differential subfield of L containing k. Hence we have a well-defined map $\alpha\colon \mathcal{S} \to \mathcal{L}$ given by $\alpha(H) = L^H$.*

Proof. Since every $\sigma \in G$ restricts to the identity on k, $k \subseteq L^H$ is a subfield. And a direct computation shows that $L^H \subseteq L$ is a subfield as well. Hence it suffices to show that L^H is a differential subfield of L. So let $a \in L^H$ and let $\sigma \in H \subseteq G$. Then $\sigma(a') = \sigma(a)' = a'$. Hence $a' \in L^H$ as well and L^H is a differential subfield. □

Lemma 7. *If M is a differential subfield of L containing k, then the set of M-linear differential automorphisms $\mathrm{Gal}(L/M)$ is a closed subgroup of G. Hence we have a well-defined map $\beta\colon \mathcal{L} \to \mathcal{S}$ given by $\beta(M) = \mathrm{Gal}(L/M)$.*

Proof. Since $\mathrm{Gal}(L/M) \subseteq G$ is the subset of elements that restrict to the identity on M, it is a subgroup of G. Let $F \in \mathrm{GL}_n(L)$ be a fundamental matrix for the equation $y' = Ay$ over k. Since L is a Picard-Vessiot field of this equation, the field of constants of L is C and L is generated as a field extension over k by the entries of F. In particular, L is generated as a field extension over M by the entries of F, and $A \in \mathrm{M}_n(M)$ as well under the inclusion $k \subseteq M$. Hence L is a Picard-Vessiot field for the equation $y' = Ay$ over M by [PS03, Proposition 1.22] and $\mathrm{Gal}(L/M)$ is a closed subgroup of $\mathrm{GL}_n(C)$ by [PS03, Theorem 1.27]. This implies that $\mathrm{Gal}(L/M) \subseteq G$ is closed as well. □

Lemma 8. *The maps $\alpha\colon \mathcal{S} \to \mathcal{L}$ and $\beta\colon \mathcal{L} \to \mathcal{S}$ from Lemma 6 and Lemma 7 are mutually inverse.*

Proof. Let $M \in \mathcal{L}$ be an intermediate differential field. Then $\alpha\beta(M) = L^{\mathrm{Gal}(L/M)}$. We regard $y' = Ay$ as an equation over M again and apply [PS03, Theorem 1.27] regarding L as the Picard-Vessiot field of $y' = Ay$ over M to deduce that $\alpha\beta(M) = M$.

Let $H \in \mathcal{S}$ be a closed subgroup. Then we have $H \subseteq \beta\alpha(H)$, because every $\sigma \in H$ has the property that $\sigma(a) = a$ for all $a \in \beta(H) = L^H$, hence $\sigma \in \mathrm{Gal}(L/L^H)$. We now regard $y' = Ay$ as an equation over L^H and apply [PS03, Corollary 1.30] to deduce that the closed subgroup $H \subseteq \mathrm{Gal}(L/L^H)$ is in fact the whole Galois group $\mathrm{Gal}(L/L^H)$. □

Example 9. Let $n \in \mathbb{N}_{>1}$ and let $L = \mathbb{C}(t)(X)$ be the Picard-Vessiot field of $y' = y$ over $\mathbb{C}(t)$. We've seen earlier that its differentail Galois group is $\mathrm{Gal}(L/k) \cong \mathbb{C}^\times$, and the group μ_n of n-th roots of unity is a closed subgroup of $\mathbb{C}^\times$. The corresponding inermediate differential field is $\mathbb{C}(t)(X^n)$. Indeed, this is a differential field as well, because $(X^n)' = nX^n \in \mathbb{C}(t)(X^n)$. On the other hand, there are no intermediate differential fields for the equation $y' = y$ over $\mathbb{C}(e^{3t})$, because in this case the Picard-Vessiot field extension has degree 3 and the Galois group is of order 3.

Lemma 10. *Let $H \in \mathcal{S}$ be a closed subgroup of G. If $\sigma(L^H) = L^H$ for all $\sigma \in G$, then the restriction morphism $G \to \mathrm{Gal}(L^H/k)$ is surjective and has kernel H. In particular, H is a normal subgroup of G in this case.*

Proof. If the assumption is true, then the restriction morphism is a well-defined group homomorphism. The kernel is by definition $\beta\alpha(H) = H$, so it remains to show the surjectivity assertion.

Let $\sigma \in \mathrm{Gal}(L^H/k)$ be a differential automorphism of L^H over k, which we can regard as a k-linear homomorphism of differential fields $\sigma\colon L^H \to L$. Our goal is to extend this to a k-linear differential isomorphism $\sigma\colon L \to L$. Since L is a Picard-Vessiot field for the equation $y' = Ay$ over k, its subfield of constants is C and there exists a fundamental matrix $F \in \mathrm{GL}_n(L)$ whose entries generate L as a field extension over k, hence also as a field extension over L^H. This implies that L is a Picard-Vessiot field for the equation $y' = Ay$ over L^H [PS03, Proposition 1.22]. Let us denote by $\iota\colon L^H \to L$ the inclusion. The matrix F is still a fundamental matrix for $y' = \sigma(A)y = Ay$, and its entries generate L as a field extension over $\sigma(L^H)$ because they already generate L as a field extension over k. Hence $\sigma\colon L^H \to L$ is also a Picard-Vessiot field for the equation $y' = Ay$ over L^H and we have the following situation:

$$\begin{array}{ccc} L & \overset{\cong}{\dashrightarrow} & L \\ {\scriptstyle\iota}\uparrow & \nearrow_{\sigma} & \\ L^H & & \end{array}$$

The uniqueness of the Picard-Vessiot field implies that we can find the dashed isomorphism $L \cong L$ extending $\sigma\colon L^H \to L$. □

Lemma 11. *The converse of Lemma 10 holds as well, i.e., if $H \in \mathcal{S}$ is a normal subgroup of G, then $\sigma(L^H) = L^H$ for all $\sigma \in G$ and the restriction morphism $G \to \mathrm{Gal}(L^H/k)$ is surjective with kernel H.*

Proof. The second part of the statement follows as in Lemma 10, so let us show that $\sigma(L^H) = L^H$ for all $\sigma \in G$. Let $\sigma \in G$ be an arbitrary element and let $a \in L^H$. We want to show that $\sigma(a) \in L^H$, so let also $\tau \in H$. The equation $\tau\sigma(a) = \sigma(a)$ is equivalent to $\sigma^{-1}\tau\sigma(a) = a$. Since H is a normal subgroup of G, $\sigma^{-1}\tau\sigma \in H$ again, so $\sigma^{-1}\tau\sigma(a) = a$ as we wanted to show. Hence $\sigma(L^H) \subseteq L^H$ for all $\sigma \in G$. Conversely, applying what we have just proven to $\sigma^{-1} \in G$ we deduce that $\sigma^{-1}(L^H) \subseteq L^H$. Therefore

$$L^H = \sigma\sigma^{-1}(L^H) \subseteq \sigma(L^H) \subseteq L^H$$

and the desired equality follows. □

Combining Lemma 6, Lemma 7, Lemma 8, Lemma 10 and Lemma 11 we obtain the differential analogue of the usual Galois corresopndence [Bos18, Theorem 4.1/6]. One can also show using some theory of linear algebraic groups that if $H \in \mathcal{S}$ is a normal subgroup of G, then L^H is a Picard-Vessiot field for some linear differential equation over k [PS03, Corollary 1.40].

Let us also mention the following:

Lemma 12. *Let G^0 denote the identity component of G. Then $L^{G^0} \supset k$ is a finite Galois extension with Galois group G/G^0. Moreover, it is the algebraic closure of k in L.*

Proof. Since G has only finitely many irreducible components, G/G^0 is a finite group. We have $(L^{G^0})^{G/G^0} = k$, because $L^G = k$. Hence $k \subseteq L^{G^0}$ is a finite Galois extension with Galois group G/G^0 [Bos18, Proposition 4.1/4].

To show that L^{G^0} is the algebraic closure of k in L, let $\alpha \in L$ be algebraic over k. We want to show that $k(\alpha) \subseteq L^{G^0}$. An element $\sigma \in G$ will only send α to some other root of its minimal polynomial, so the G-orbit of α is finite. Therefore $\mathrm{Aut}(L/k(\alpha)) = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$ is an algebraic subgroup of G of finite index and $G^0 \subseteq \mathrm{Aut}(L/k(\alpha))$, so $k(\alpha) \subseteq L^{G^0}$ as we wanted to show. □

4. Another example

We consider now the equation $y' = 8$ instead, still working over the two fields $\mathbb{C}(t)$ and $\mathbb{C}(e^{3t})$. We can reduce this equation to the matrix equation

$$\begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = \begin{pmatrix} 0 & 8 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix},$$

so that $y_2 = \lambda \in \mathbb{C}$ is forced to be a constant and $y_1' = 8\lambda$. If $F \in \mathrm{GL}_2(R)$ is a fundamental matrix in some differential ring extension R, then we have

$$\begin{pmatrix} F_{11}' & F_{12}' \\ F_{21}' & F_{22}' \end{pmatrix} = \begin{pmatrix} 0 & 8 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} F_{11} & F_{12} \\ F_{21} & F_{22} \end{pmatrix} = \begin{pmatrix} 8F_{21} & 8F_{22} \\ 0 & 0 \end{pmatrix}.$$

Therefore $F_{21}, F_{22} \in \mathbb{C}$ are constants. But they cannot both be zero, because we want the matrix to be invertible. So let's say $F_{21} = 0$ and $F_{22} = 1$. Then we need $F_{11}' = 0$ and $F_{12}' = 8$. But F_{11} cannot be zero, because we want the matrix to be invertible, so we take $F_{11} = 1$ and the fundamental matrix becomes

$$F = \begin{pmatrix} 1 & F_{12} \\ 0 & 1 \end{pmatrix}$$

with F_{12} a solution of our original equation $y' = 8$. If we are working over $\mathbb{C}(t)$, then a solution already exists in the base field, namely $F_{12} = 8t$. So in this case $\mathbb{C}(t)$ is its own Picard-Vessiot field extension and the differential Galois group is trivial. On the other hand, there is no solution in $\mathbb{C}(e^{3t})$, so in this case we need to pass to a non-trivial extension. We add a formal solution by considering the polynomial ring $R := \mathbb{C}(e^{3t})[X]$ with $X' = 8$. A fundamental matrix $F \in \mathrm{GL}_2(R)$ is given by

$$F = \begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix},$$

so R is generated as a $\mathbb{C}(e^{3t})$-algebra by the entries of the fundamental matrix and the inverse of its determinant. It remains to show that R is a

simple differential ring in order to conclude that it is the Picard-Vessiot ring of the equation $y' = 8$ over $\mathbb{C}(e^{3t})$. Let $I = (P)$ be a differential ideal of $\mathbb{C}(e^{3t})$ with $P = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in R$. If $m = 0$, then $I = (0)$ or $I = R$. So assume $m > 0$. Then $P' = (8m + a'_{m-1})X^{m-1} + \cdots \in (P)$, hence $P' = 0$ for degree reasons. In particular we have $8m + a'_{m-1} = 0$, i.e.,

$$\left(\frac{-1}{m}a_{m-1}\right)' = 8.$$

This would imply that $\frac{-1}{m}a_{m-1} \in \mathbb{C}(e^{3t})$ was already a non-zero solution of the equation in $\mathbb{C}(e^{3t})$. But no such solution exists, so $m = 0$ and R is a simple differential ring. Let now $\sigma \in \mathrm{Gal}(R/\mathbb{C}(e^{3t}))$ be an automorphism in the differential Galois group. Then σ is uniquely determined by $\sigma(X)$, and we need

$$\sigma(X)' = \sigma(X') = \sigma(8) = 8,$$

hence $\sigma(X)$ is another solution of the equation $y' = 8$ over $\mathbb{C}(e^{3t})$. If we write $\sigma(X) = a_m X^m + \cdots + a_0 \in R$, then $\sigma(X)' = 8ma_m X^{m-1} + \cdots + 8a_1$, so for degree reasons we must have $\sigma(X) = X + a_\sigma$ for some $a_\sigma \in \mathbb{C}(e^{3t})$ which depends on σ. We have then another fundamental matrix ggiven by

$$\tilde{F} = \begin{pmatrix} 1 & X + a_\sigma \\ 0 & 1 \end{pmatrix}.$$

We compute $F^{-1}\tilde{F}$ in order to find the matrix $C_\sigma \in \mathrm{GL}_2(\mathbb{C})$ corresponding to σ:

$$C_\sigma = \begin{pmatrix} 1 & -X \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & X + a_\sigma \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_\sigma \\ 0 & 1 \end{pmatrix}.$$

Therefore $\mathrm{Gal}(L/\mathbb{C}(e^{3t})) \cong \mathrm{Gal}(R/\mathbb{C}(e^{3t})) \cong (\mathbb{C}, +)$.

Appendix A. Solutions to exercises

The exercises below are taken from [PS03, Exercises 1.5].

Exercise 1 (Constructions with rings and derivations). Let R be any differential ring with derivation ∂.

(a) Let $t, n \in R$ and assume that n is invertible. Prove the formula

$$\partial\left(\frac{t}{n}\right) = \frac{\partial(t)n - t\partial(n)}{n^2}.$$

Solution. Assume first that $t = 1$. The Leibniz rule implies that

$$\partial(1) = \partial(1) + \partial(1) = 2\partial(1),$$

and since $\mathbb{Q} \subseteq R$ we deduce that $\partial(1) = 0$. So in this case we need to show that

$$\partial(n^{-1}) = -\frac{\partial n}{n^2}.$$

Again by the Leibniz rule we have

$$0 = \partial(1) = \partial(nn^{-1}) = \frac{\partial n}{n} + n\partial(n^{-1}),$$

hence the claim. Now for any $t \in R$ we can apply again the Leibniz rule to the product tn^{-1} to deduce the desired equality. ∎

(b) Let $I \subseteq R$ be an ideal. Prove that ∂ induces a derivation on R/I if and only if $\partial(I) \subseteq I$.

Remark 13. It may happen that R/I is no longer of characteristic zero.

Solution. It follows from the Leibniz rule that $\partial(0) = 0$ on any differential ring, even if it does not contain $\mathbb{Q}$. If ∂ induces a derivation on R/I, then $\partial(0 + I) = 0 + I$, i.e., $\partial(a) \in I$ for all $a \in I$. Conversely, if $\partial(a) \in I$ for all $a \in I$, then ∂ induces a well-defined derivation on R/I. Indeed, since $\partial(0) = 0$ and $\partial(a + b) = \partial(a) + \partial(b)$, ∂ is a group homomorphism. Therefore

$$a - b \in I \Rightarrow \partial(a - b) = \partial(a) - \partial(b) \in I,$$

so $\partial\colon R/I \to R/I$ is a well-defined function. We have also

$$\partial(a + b + I) = \partial(a + b) + I = \partial(a) + \partial(b) + I = \partial(a + I) + \partial(b + I),$$

so $\partial\colon R/I \to R/I$ is additive. And finally

$$\partial(ab + I) = \partial(ab) + I = a\partial(b) + b\partial(a) + I = (a + I)\partial(b + I) + (b + I)\partial(a + I),$$

so $\partial\colon R/I \to R/I$ is a derivation. ∎

(c) Let the ideal $I \subseteq R$ be generated by $\{a_j\}_{j\in J}$. Prove that $\partial(I) \subseteq I$ if $\partial(a_j) \in I$ for all $j \in J$.

Solution. Since ∂ is a group homomorphism and I is a subgroup, it suffices to show that $\partial(aa_j) \in I$ for all $j \in J$ and all $a \in R$. Since $a_j, \partial(a_j) \in I$ and I is an ideal, we have $a\partial(a_j) \in I$ and $a_j\partial(a) \in I$, hence

$$\partial(aa_j) = a\partial(a_j) + a_j\partial(a) \in I.$$

∎

(d) Let $S \subseteq R$ be a multiplicative subset. Prove that there exists a unique derivation ∂ on RS^{-1} such that the canonical map $R \to RS^{-1}$ commutes with ∂. Hint: Use the fact that $tr = 0$ implies $t^2\partial(r) = 0$.

Solution. Suppose such a derivation existed and let $a \in R$ and $s \in S$. Since (the equivalence class of) s is invertible in RS^{-1}, part (a) of this exercise implies that

$$\partial\left(\frac{a}{s}\right) = \frac{s\partial(a) - a\partial(s)}{s^2}.$$

This proves uniqueness. For the existence we need to check that the previous expression is a well-defined derivation on RS^{-1}. Let $a, b \in R$ and $s, t \in S$ such that $a/s = b/t$, i.e., suppose there exists some $u \in S$ such that $u(at - bs) = 0$. We need to show that there eixsts some $v \in S$ such that

$$v(t^2(s\partial(a) - a\partial(s)) - s^2(t\partial(b) - b\partial(t))) = 0.$$

Taking the hint for granted and using that $uat = ubs$ we deduce

$$\begin{aligned}
0 = stu^2\partial(at - bs) &= stu^2(t\partial(a) + a\partial(t) - s\partial(b) - b\partial(s)) \\
&= u^2(st^2\partial(a) + sta\partial(t) - s^2t\partial(b) - stb\partial(s)) \\
&= u^2t^2s\partial(a) - u^2stb\partial(s) - u^2s^2t\partial(b) + u^2sta\partial(t) \\
&= u^2t^2s\partial(a) - u^2t^2a\partial(s) - u^2s^2t\partial(b) + u^2s^2b\partial(t) \\
&= u^2(t^2(s\partial(a) - a\partial(s)) - s^2(t\partial(b) - b\partial(t))
\end{aligned}$$

So taking $v = u^2 \in S$ works. We prove the hint now. From $tr = 0$ we deduce

$$\partial(tr) = 0 = t\partial(r) + r\partial(t).$$

Multiplying the equality by t and using again that $tr = 0$ we obtain the claim. Therefore the formula above yields a well-defined function $\partial\colon RS^{-1} \to RS^{-1}$.

We check finally that it is a derivation. On the one hand we have

$$\begin{aligned}
\partial\left(\frac{a}{s} + \frac{b}{t}\right) &= \partial\left(\frac{at + bs}{st}\right) \\
&= \frac{st(a\partial(t) + t\partial(a) + b\partial(s) + s\partial(b)) - (at + bs)(t\partial(s) + s\partial(t))}{s^2t^2} \\
&= \frac{t^2(s\partial(a) - a\partial(s))}{s^2t^2} + \frac{s^2(t\partial(b) - b\partial(t))}{s^2t^2} + 0 \\
&= \partial\left(\frac{a}{s}\right) + \partial\left(\frac{b}{t}\right),
\end{aligned}$$

so $\partial\colon RS^{-1} \to RS^{-1}$ is additive. On the other hand we have

$$\begin{aligned}
\partial\left(\frac{a}{s}\frac{b}{t}\right) &= \partial\left(\frac{ab}{st}\right) \\
&= \frac{st\partial(ab) - ab\partial(st)}{s^2t^2} \\
&= \frac{sta\partial(b) + stb\partial(a) - abs\partial(t) - abt\partial(s)}{s^2t^2} \\
&= \frac{sta\partial(b) + stb\partial(a) - abs\partial(t) - abt\partial(s)}{s^2t^2} \\
&= \frac{as}{s^2}\left(\frac{t\partial(b) - b\partial(t)}{t^2}\right) + \frac{bt}{t^2}\left(\frac{s\partial(a) - a\partial(s)}{s^2}\right) \\
&= \frac{a}{s}\partial\left(\frac{b}{t}\right) + \frac{b}{t}\partial\left(\frac{a}{s}\right),
\end{aligned}$$

so $\partial\colon RS^{-1} \to RS^{-1}$ is a derivation. ■

(e) Consider the polynomial ring $R[X_1, \ldots, X_n]$ and a multiplicative subset $S \subseteq R[X_1, \ldots, X_n]$. Let $a_1, \ldots, a_n \in R[X_1, \ldots, X_n]S^{-1}$

be given. Prove that there exists a unique derivation ∂ on $R[X_1, \ldots, X_n]S^{-1}$ such that the canonical map $R \to R[X_1, \ldots, X_n]S^{-1}$ commutes with ∂ and $\partial(X_i) = a_i$ for all i.

Solution. Suppose first that all a_i are in $R[X_1, \ldots, X_n]$. In that case, by part (d) of this exercise, it suffices to find a compatible derivation on $R[X_1, \ldots, X_n]$. Suppose that we have such a compatible derivation ∂ on $R[X_1, \ldots, X_n]$. Induction on m_i shows that

$$\partial(X_i^{m_i}) = m_i a_i X_i^{m_i - 1}$$

for all $m_i \geq 1$. With the convention that $X_i^{-1} = 0$, the same formula holds for $m_i = 0$ as well. The Leibniz rule implies then that

$$\partial(X_1^{m_1} \cdots X_n^{m_n}) = \sum_{i=1}^{n} m_i a_i X_1^{m_1} \cdots X_i^{m_i - 1} \cdots X_n^{m_n}$$

for all such monomials, again with the convention that $X_i^{-1} = 0$. We keep this convention throughout the rest of the solution. For an element $b \in R$ we have

$$\partial(bX_1^{m_1} \cdots X_n^{m_n}) = \partial(b)X_1^{m_1} \cdots X_n^{m_n} + b\left(\sum_{i=1}^{n} m_i a_i X_1^{m_1} \cdots X_i^{m_i - 1} \cdots X_n^{m_n}\right). \tag{2}$$

Any polynomial $P \in R[X_1, \ldots, X_n]$ is a finite sum of such monomials, so such a ∂ is already uniquely determined by Equation (2). This shows uniqueness. For the existence part, it remains to show that ∂ determines a well-defined derivation. Additivity holds by construction and by definition of addition of polynomials. So we only need to check the Leibniz rule. We check it first for the product of two monomials as in Equation (2), say $bX_1^{m_1} \cdots X_n^{m_n}$ and $cX_1^{l_1} \cdots X_n^{l_n}$. On one hand we have

$$\begin{aligned}\partial(bcX_1^{m_1+l_1} \cdots X_n^{m_n+l_n}) = {} & (c\partial(b) + b\partial(c))X_1^{m_1+l_1} \cdots X_n^{m_n+l_n} \\ & + bc\left(\sum_{i=1}^{n} (m_i + l_i) a_i X_1^{m_1+l_1} \cdots X_i^{m_i+l_i-1} \cdots X_n^{m_n}\right)\end{aligned}$$

On the other hand we have

$$\begin{aligned}& cX_1^{l_1} \cdots X_n^{l_n} \partial(bX_1^{m_1} \cdots X_n^{m_n}) = \\ & \quad c\partial(b)X_1^{m_1+l_1} \cdots X_n^{m_n+l_n} + bc\left(\sum_{i=1}^{n} m_i a_i X_1^{m_1+l_1} \cdots X_i^{m_i+l_i-1} \cdots X_n^{m_n+l_n}\right).\end{aligned}$$

Adding the analogous term we deduce that the Leibniz rule holds in this case. Let now M_1, M_2 and M_3 be monomials. Since $\partial(M_j M_k) = M_k \partial(M_j) + M_j \partial(M_k)$ and ∂ is additive, we have

$$\partial((M_1 + M_2)M_3) = M_3(\partial(M_1) + \partial(M_2)) + (M_1 + M_2)\partial(M_3).$$

By induction, the Leibniz rule is satisfied for the product of an arbitrary polynomial with a monomial. And if M_1 and M_2 are monomials and P is an arbitrary polynomial, then using additivity and the Leibniz rule for the product of a polynomial with a monomial we deduce that

$$\partial(P(M_1 + M_2)) = (M_1 + M_2)\partial(P) + P\partial(M_1 + M_2),$$

so by induction we conclude that the Leibniz rule holds in general. This proves the existence and hence finishes the proof when $a_i \in R[X_1, \dots, X_n]$ for all $i \in \{1, \dots, n\}$.

Now write each $a_i = P_i/Q_i$, where $P_i, Q_i \in R[X_1, \dots, X_n]$ for all $i \in \{1, \dots, n\}$. Consider the ring $A = R[X_1, \dots, X_n, T_1, \dots, T_n]$ and its ideal $I = (1 - T_1Q_1, \dots, 1 - T_nQ_n)$. In the quotient ring A/I we can think of T_i as Q_i^{-1}, so we first extend $\partial\colon R \to R$ to a derivation $\partial\colon A \to A$ such that $\partial(X_i) = P_iT_i$ and $\partial(T_i) = -T_i^2\partial(Q_i)$. For example, if $P_1 = 2X_1$ and $Q_1 = 3X_1^2 + 2$, then we would have $\partial(X_1) = 2X_1T_1$ and

$$\partial(T_1) = -6T_1^2X_1\partial(X_1) = -12T_1^3X_1^2.$$

Now we check that the (uniquely determined) derivation $\partial\colon A \to A$ extends to a uniquely determined derivation $\partial\colon A/I \to A/I$ using parts (b) and (c) of this exercise. For each $i \in \{1, \dots, n\}$ we have

$$\partial(1 - T_iQ_i) = -Q_i(-T_i^2\partial(Q_i)) - T_i\partial(Q_i) = -\partial(Q_i)T_i(1 - T_iQ_i),$$

so we can indeed apply part (b) of this exercise to obtain the uniquely determined $\partial\colon A/I \to A/I$ with the specified properties. The localization of A/I at (the image of) S is the same as the localization of $R[X_1, \dots, X_n]$ at S and a_i is the image of $P_iT_i + I$ for all $i \in \{1, \dots, n\}$; this follows from the universal property of the localization. Part (d) of this exercise allows us to conclude the solution. ■

Exercise 2 (Constants). Let R be any differential ring with derivation ∂.

(a) Prove that the set of constants C of R is a subring containing 1.

Solution. We have seen in the previous exercise that $\partial(1) = 0$ as a consequence of $\mathbb{Q} \subseteq R$, so 1 is always a constant. We have also seen in the previous exercise that $\partial(0) = 0$ in any case, so 0 is a constant as well. If c and d are constants, then $\partial(c + d) = \partial(c) + \partial(d) = 0$, so $c + d$ is a constant as well. And $\partial(cd) = c\partial(d) + d\partial(c) = 0$, so cd is a constant as well. Therefore C is a subring containing 1. ■

(b) Prove that C is a field if R is a field.

Solution. After part (a) of this exercise, it remains only to show that c^{-1} is a constant for any non-zero constant c. But we have seen in the previous exercise that $\partial(c^{-1}) = -\partial(c)c^{-2}$, so c^{-1} is a constant as well. ■

Assume that $K \supseteq R$ is an extension of differential fields.

(c) Assume that $c \in K$ is algebraic over the constants C of R. Prove that $\partial(c) = 0$. Hint: Let $P(X)$ be the minimal monic polynomial of c over C. Differentiate the expression $P(c) = 0$ and use the fact that $\mathbb{Q} \subseteq R$.

Solution. We consider the derivation on $R[X]$ which is compatible with the derivation on R and such that $\partial(X) = 1$, which is unique and well-defined by the previous exercise. Then we consider the polynomial $\partial(P) \in R[X]$. If $c = 0$, then $\partial(c) = 0$. So we may assume that $\deg(P) \geq 1$. We have $\deg(\partial P) = \deg(P) - 1$, because $\mathbb{Q} \subseteq R$. Explicitly, if $P = \sum_{i=0}^{m} a_i X^i$, then it follows from the solution to the previous exercise that

$$\partial(P) = \sum_{i=0}^{m} (i a_i X^{i-1} + \partial(a_i) X^i),$$

with the convention again that $X^{-1} = 0$. Since $a_i \in C$ for all i, we have

$$\partial(P) = \sum_{i=1}^{m} i a_i X^{i-1}.$$

We may regard c like a variable and extend the derivation to $R[X, c]$ so that $\partial(X) = 1$ and $\partial(c)$ is the value taht we want to determine. The solution to the previous exericse shows again that

$$\partial(P(c)) = \left(\sum_{i=1}^{m} i a_i \partial(c) c^{i-1} \right) + 0 = \partial(c) \left(\sum_{i=1}^{m} i a_i c^{i-1} \right) = \partial(c)(\partial(P)(c)),$$

where we are using that $P \in C[X]$ one more time in the first equality above. Since $P(c) = 0$, we have

$$\partial(c)(\partial(P)(c)) = 0.$$

But P is the minimal polynomial of c over C and $\deg(P) > \deg(\partial(P)) \geq 0$, so $\partial(P)(c) \neq 0$. Since R is a field, we deduce that $\partial(c) = 0$ and c is a constant. ■

(d) Show that $c \in K$, $\partial(c) = 0$ and c is algebraic over R, implies that c is algebraic over the field of constants C of R. Hint: Let $P(X)$ be the minimal monic polynomial of c over R. Differentiate the expression $P(c) = 0$ and use $\mathbb{Q} \subseteq R$.

Solution. Let $c \in K$ be such a constant. We may again assume that $c \neq 0$. We need to find a non-zero polynomial $Q \in C[X]$ such that $Q(c) = 0$. Let $P \in R[X]$ be the minimal monic polynomial of c over R as in the hint, say $P = \sum_{i=0}^{m} a_i X^i$ with $a_i \in R$. We consider again the induced derivaton on $R[X]$ with the property that $\partial(X) = 1$. Using again the formulas in the solution to the previous exercise

and the assumption that $\partial(c) = 0$ we have

$$\partial(P(c)) = 0 + \left(\sum_{i=0}^{m} \partial(a_i) X^i \right) = 0.$$

This implies that $\partial(a_i) = 0$ for all i, so $P \in C[X]$. Since $c \neq 0$, $P \neq 0$. Hence c is algebraic over C. ■

Exercise 3 (Derivations on field extensions). Let F be a field (of characteristic 0) and let ∂ be a derivation on F. Prove the following statements.

(a) Let $F \subseteq F(X)$ be a transcendental extension of F. Choose an $a \in F(X)$. There is a unique derivation $\tilde{\partial}$ of $F(X)$, extending ∂, such that $\tilde{\partial}(X) = a$.

Solution. By definition, $F(X)$ is the smallest field containing F and X. Therefore $F(X)$ is also the field of fractions of the polynomial ring $F[X]$. The claim follows then from part (e) of the first exercise. ■

(b) Let $F \subseteq \tilde{F}$ be a finite extension, then ∂ has a unique extension to a derivation of $\tilde{F}$. Hint: $\tilde{F} = F(a)$, where a satisfies some irreducible polynomial over F. Use the first exercise and $\mathbb{Q} \subseteq F$.

Solution. Let us show uniqueness first. Since $\mathbb{Q} \subseteq F$, the extension is separable. By the primitive element theorem there exists some $a \in \tilde{F}$ such that $\tilde{F} = F(a)$ and such that there exists some monic irreducible polynomial $P = \sum_{i=0}^{m} a_i X^i \in F[X]$ such that $P(a) = 0$ in $\tilde{F}$. Therefore we must have

$$0 = \partial(P(a)) = \partial(a) \left(\sum_{i=1}^{m} i a_i a^{i-1} \right) + \sum_{i=0}^{m} \partial(a_i) a^i,$$

and since $\mathbb{Q} \subseteq F$ and P is the minimal polynomial of a we must also have $\sum_{i=1}^{m} i a_i a^{i-1} \neq 0$. The value of $\partial(a)$ is therefore uniquely determined as

$$\partial(a) = -\frac{\sum_{i=0}^{m} \partial(a_i) a^i}{\sum_{i=1}^{m} i a_i a^{i-1}}.$$

This proves the uniqueness.

For the existence, we use part (e) of the first exercise with $S \subseteq F[X]$ the set of powers of the non-zero polynomial $Q := \sum_{i=1}^{m} i a_i X^{i-1}$. We can then define a derivation on $S^{-1}F[X]$ with the property that

$$\partial(X) = -\frac{\sum_{i=0}^{m} \partial(a_i) X^i}{Q}.$$

We have $\tilde{F} = F[X]/(P)$ and the image of Q is invertible in $\tilde{F}$, so we have

$$S^{-1}F[X]/S^{-1}(P) = S^{-1}\tilde{F} = \tilde{F}.$$

By parts (b) and (c) of the first exercise, it suffices to show that $\partial(P) \in S^{-1}(P)$ in $S^{-1}F[X]$. But replacing a by X in the formula above shows that $\partial(P) = 0$, thus we have a well-defined derivation on $\tilde{F}$ extending the given derivation on F. ■

(c) Prove that ∂ has a unique extension to any field $\tilde{F}$ that is algebraic over F (and, in particular, to the algebraic closure of F).

Solution. We can write any algebraic extension as the union of all finite subextensions. The uniqueness in part (b) of this exercise allows us to extend ∂ to each such finite subextension in a way that glues together to a well-defined ∂ on their union. ■

(d) Show that (b) and (c) are, in general, false if F has characteristic $p > 0$. Hint: Let $\mathbb{F}_p$ be the field with p elements and consider the field extension $\mathbb{F}_p(x^p) \subseteq \mathbb{F}_p(x)$, where x is transcendental over $\mathbb{F}_p$.

Solution. We consdier $\partial = 0$ on $\mathbb{F}_p$ and use part (a) of this exercise to extend ∂ to $\mathbb{F}_p(x)$ in two different ways: $\partial_0 = 0$ and ∂_1 such that $\partial_1(x) = 1$. For all $j \in \{1, 2\}$, all $a \in \mathbb{F}_p$ and all $i \in \mathbb{N}_{>0}$ we have

$$\partial_j(ax^{ip}) = piax^{ip-1}\partial_j(x) = 0,$$

so both ∂_0 and ∂_1 are extensions of $\partial = 0$ on $\mathbb{F}_p(x^p)$ to $\mathbb{F}_p(x)$. But $\partial_0 \neq \partial_1$, so the uniqueness in part (b) fails. ■

(e) Let F be a perfect field of characteristic $p > 0$ (i.e., $F^p =: \{a^p | a \in F\}$ is equal to F). Show that the only derivation on F is the zero derivation.

Solution. Let ∂ be a derivation on F and let $a \in F$. We want to show that $\partial(a) = 0$. Since Frobenius is surjective, we can write $a = b^p$ for some $b \in F$. Then we have

$$\partial(a) = \partial(b^p) = pb^{p-1}\partial(b) = 0,$$

hence $\partial = 0$. ■

(f) Suppose that F is a field of characteristic $p > 0$ such that $[F : F^p] = p$. Give a construction of all derivations on F. Hint: Compare with the beginning of [PS03, Sect. 13.1].

Solution. Let $\partial\colon F \to F$ be a derivation. Let $a = b^p$ be an element in F^p. Then $\partial(a) = pb^{p-1}\partial(b) = 0$. So $\partial\colon F \to F$ is F^p-linear, and in particular it is uniquely determined by the values of ∂ at the elements of a basis of F over F^p. Since $[F : F^p] = p$ is prime, every $x \in F \setminus F^p$ generates the field extension $F^p \subseteq F$. We consider the basis $1, x, \ldots, x^{p-1}$ of F over F^p. Since $1 \in F^p$, we must have $\partial(1) = 0$. We have

$$\partial(x^j) = jx^{j-1}\partial(x)$$

for all $j \in \{1, \dots, p-1\}$, so ∂ is uniquely deterined by the value $\partial(x) \in F$. So every derivation $\partial\colon F \to F$ has the form

$$\partial\left(\sum_{i=0}^{p-1} a_i x^i\right) = \partial(x)\left(\sum_{i=1}^{p-1} i a_i x^{i-1}\right)$$

for some $\partial(x) \in F$, where $a_i \in F^p$ for all $i \in \{0, \dots, p-1\}$. Conversely, given any $f \in F$, we can define an F^p-linear derivation $\partial\colon F \to F$ by setting $\partial(x) = f$. Such a derivation is by definition additive, so we only need to check that the Leibniz rule holds. We start by checking the Leibniz rule on temrs of the form ax with $a \in F^p$. In that case we have

$$\partial(axbx) = 2abx\partial(x) = bx\partial(ax) + ax\partial(bx).$$

In general we can use induction on the number of terms and the additivity of ∂ to conclude that the Leibniz rule holds in general as in part (e) of the first exercise. ■

Exercise 4 (Lie algebras and derivations). A *Lie algebra* over a field C is a C-vector space V equipped with a C-bilinear map $[\ ,\ ]\colon V \times V \to V$ that satisfies $[u, u] = 0$ for all $u \in V$ and satisfies the Jacobi identity.

(a) Let F be any field and let $C \subseteq F$ be a subfield. Let $\mathrm{Der}(F/C)$ denote the set of all derivations ∂ on F such that ∂ is the zero map on C. Prove that $\mathrm{Der}(F/C)$ is a vector space over F. Prove that for any two elements $\partial_1, \partial_2 \in \mathrm{Der}(F/C)$, the map $\partial_1\partial_2 - \partial_2\partial_1$ is again in $\mathrm{Der}(F/C)$. Conclude that $\mathrm{Der}(F/C)$ is a Lie algebra over C.

Solution. The Leibniz rule and the assumption that $\mathbb{Q} \subseteq F$ imply that $\partial|_C = 0$ if and only if $\partial\colon F \to F$ is C-linear. So $\mathrm{Der}(F/C)$ is the set of C-linear derivations on F. The zero derivation is C-linear, so this set is non-empty. Let ∂_1 and ∂_2 be two C-linear derivations. We check that $\partial_1 + \partial_2$ is a C-linear derivation. For any $a, b \in F$ we have

$$(\partial_1 + \partial_2)(a+b) = \partial_1(a) + \partial_1(b) + \partial_2(a) + \partial_2(b) = (\partial_1 + \partial_2)(a) + (\partial_1 + \partial_2)(b),$$

so $\partial_1 + \partial_2$ is additive. Moreover, we also have

$$\begin{aligned}(\partial_1 + \partial_2)(ab) &= \partial_1(ab) + \partial_2(ab)\\ &= b\partial_1(a) + a\partial_1(b) + b\partial_2(a) + a\partial_2(b)\\ &= b((\partial_1 + \partial_2)(a)) + a((\partial_1 + \partial_2)(b)),\end{aligned}$$

so the Leibniz rule is also satisfied by $\partial_1 + \partial_2$. And for $c \in C$ we have $(\partial_1 + \partial_2)(c) = \partial_1(c) + \partial_2(c) = 0$, so $\partial_1 + \partial_2$ is C-linear as well. If ∂ is a C-linear derivation, then so is $-\partial$. Pointwise addition of functions is associative and commutative, so $\mathrm{Der}(F/C)$ is an abelian group. We define a scalar multiplication pointwise as well, i.e., $(\lambda\partial)(a) := \lambda(\partial(a))$ for $\partial \in \mathrm{Der}(F/C)$, $\lambda, a \in F$. This defines again a C-linear derivation on F and endows $\mathrm{Der}(F/C)$ with the structure of a vector space over F.

For $\partial_1, \partial_2 \in \mathrm{Der}(F/C)$ we define

$$[\partial_1, \partial_2] := \partial_1 \circ \partial_2 - \partial_2 \circ \partial_1.$$

We check that $[\partial_1, \partial_2]$ is again a C-linear derivation on F. For $a, b \in F$ we have

$$\begin{aligned}[\partial_1, \partial_2](a+b) &= \partial_1 \circ \partial_2(a+b) - \partial_2 \circ \partial_1(a+b) \\ &= \partial_1 \circ \partial_2(a) + \partial_1 \circ \partial_2(b) - \partial_2 \circ \partial_1(a) - \partial_2 \circ \partial_1(b) \\ &= [\partial_1, \partial_2](a) + [\partial_1, \partial_2](b)\end{aligned}$$

and also

$$\begin{aligned}[\partial_1, \partial_2](ab) &= \partial_1 \circ \partial_2(ab) - \partial_2 \circ \partial_1(ab) \\ &= \partial_1(b\partial_2(a) + a\partial_2(b)) - \partial_2(b\partial_1(a) + a\partial_1(b)) \\ &= \partial_2(a)\partial_1(b) + b(\partial_1 \circ \partial_2(a)) + \partial_2(b)\partial_1(a) + a(\partial_1 \circ \partial_2(b)) \\ &\quad - \partial_1(a)\partial_2(b) - b(\partial_2 \circ \partial_1(a)) - \partial_1(b)\partial_2(a) - a(\partial_2 \circ \partial_1(b)) \\ &= b(\partial_1 \circ \partial_2(a)) + a(\partial_1 \circ \partial_2(b)) - b(\partial_2 \circ \partial_1(a)) - a(\partial_2 \circ \partial_1(b)) \\ &= b[\partial_1, \partial_2](a) + a[\partial_1, \partial_2](b),\end{aligned}$$

so $[\partial_1, \partial_2]$ is a derivation. If ∂_1 and ∂_2 vanish on C, then so does $[\partial_1, \partial_2]$, so it is a C-linear derivation, as we wanted to show. Since derivations are group homomorphisms, the bracket $[-,-]$ is $\mathbb{Z}$-bilinear. If $\partial_1, \partial_2 \in \mathrm{Der}(F/C)$, $c \in C$ and $a \in F$, then

$$[c\partial_1, \partial_2](a) = c(\partial_1(\partial_2(a))) - \partial_2(c(\partial_1(a))) = c[\partial_1, \partial_2](a) = [\partial_1, c\partial_2](a),$$

so the bracket is in fact C-bilinear. For any derivation ∂ we have $\partial \circ \partial - \partial \circ \partial = 0$, so it is also antisymmetric. It remains to show the Jacobi identity. So let $x, y, z \in \mathrm{Der}(F/C)$. We have

$$\begin{aligned}[[xy]z] + [[yz]x] + [[zx]y] &= (xy - yx)z - z(xy - yx) + (yz - zy)x \\ &\quad - x(yz - zy) + (zx - xz)y - y(zx - xz) \\ &= 0,\end{aligned}$$

because composition of group homomorphisms is associative and $\mathbb{Z}$-bilinear. Therefore $\mathrm{Der}(F/C)$ is a Lie algebra over C. ∎

(b) Assume now that the field C has characteristic 0 and that F/C is a finitely generated field extension. One can show that there is an intermediate field $M = C(z_1, \ldots, z_d)$ with M/C purely transcendental and F/M finite. Prove, with the help of the third exercise, that the dimension of the F-vector space $\mathrm{Der}(F/C)$ is equal to d.

Solution. We argue by induction on d. For $d = 0$ we have $\mathrm{Der}(F/C) = 0$ by the second exercise, because the elements of C are constants and finite extensions are algebraic. Suppose the result is true for some $d \in \mathbb{N}$ and assume F/C is such that there exists an intermediate field $M = C(z_1, \ldots, z_d, z_{d+1})$ with M/C purely transcendental and F/M finite. Let $N := C(z_1, \ldots, z_d)$, so that

$M = N(z_{d+1})$ is a transcendental extension. From the third exercise we know that

$$\dim_F(\mathrm{Der}(F/C)) = \dim_M(\mathrm{Der}(M/C)).$$

From the third exercise we also know that

$$\dim_M(\mathrm{Der}(M/C)) = \dim_N(\mathrm{Der}(N/C)) + 1,$$

because every derivation on $M = N(z_{d+1})$ is uniquely determined by a derivation on N and an element $f \in M$. By induction hypothesis we have $\dim_N(\mathrm{Der}(N/C)) = d$, therefore $\dim_F(\mathrm{Der}(F/C)) = d + 1$. ∎

References

[Bos18] Siegfried Bosch. *Algebra—from the viewpoint of Galois theory*. German. Birkhäuser Advanced Texts: Basler Lehrbücher. [Birkhäuser Advanced Texts: Basel Textbooks]. Birkhäuser/Springer, Cham, 2018, pp. viii+367. ISBN: 978-3-319-95176-8; 978-3-319-95177-5. DOI: 10.1007/978-3-319-95177-5. URL: https://doi.org/10.1007/978-3-319-95177-5.

[PS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*. Vol. 328. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2003, pp. xviii+438. ISBN: 3-540-44228-6. DOI: 10.1007/978-3-642-55750-7. URL: https://doi.org/10.1007/978-3-642-55750-7.

Pedro Núñez
Albert-Ludwigs-Universität Freiburg, Mathematisches Institut
Ernst-Zermelo-Strasse 1, 79104 Freiburg im Breisgau (Germany)
Email address: pedro.nunez@math.uni-freiburg.de
Homepage: https://home.mathematik.uni-freiburg.de/nunez