PICARD-VESSIOT EXTENSIONS OF ARTINIAN SIMPLE MODULE ALGEBRAS

KATSUTOSHI AMANO AND AKIRA MASUOKA

ABSTRACT. This paper pursues Takeuchi's Hopf algebraic approach [T] to the Picard-Vessiot (PV) theory for differential equations, to involve the PV extensions of difference equations. Differential fields and total difference rings in the standard PV theory are unified here by artinian simple (AS) module algebras over a cocommutative, pointed smooth Hopf algebra.

INTRODUCTION

The Picard-Vessiot (PV) theory is a Galois theory for extensions of differential fields; see van der Put and Singer [vPS2] for modern treatment. A *differential field* is a field given a differential operator (or derivation). Let K be such a field of characteristic zero, in which the field $k := K_0$ of constants is algebraically closed. Suppose that a linear differential equation, $\boldsymbol{v}' = Z\boldsymbol{v}$, is given, where Z is an $n \times n$ matrix with entries in K. This is equivalent to saying that a differential K-module of K-dimension n is given. There is a unique (up to isomorphism) extension L/K, called the PV extension, of differential fields with $(K_0 =)\ k = L_0$ that is a *minimal splitting field* for $\boldsymbol{v}' = Z\boldsymbol{v}$ in the sense that L^n includes an n-dimensional (many enough!) k-subspace of solutions $\boldsymbol{v}$ for $\boldsymbol{v}' = Z\boldsymbol{v}$, and their entries generate L over K. The group $G(L/K)$ of differential automorphisms of L/K naturally forms a linear algebraic group over k. There is a 1-1 correspondence between the intermediate differential fields $K \subset M \subset L$ and the closed subgroups $G(L/M) \subset G(L/K)$.

By the beautiful, Hopf-algebraic approach, M. Takeuchi [T] clarified the heart of the theory in the generalized context of C-ferential fields, intrinsically defining PV extensions and the minimal splitting fields of C-ferential modules. By replacing linear algebraic groups with affine group schemes (or equivalently commutative Hopf algebras), he succeeded in removing from many of the results the assumptions of finite generation, zero characteristic and algebraic closedness. For a cocommutative coalgebra C with a specific grouplike 1_C, a *C-ferential field* [T] is a field given a unital, measuring action by C; the concept includes differential fields, Δ-fields [K] and fields with higher derivations.

A *difference field* [vPS1] is a field given an automorphism. A linear difference equation has coefficients in such a field. To amend a failure which arises when one develops, restricting oneself to fields, a PV theory for difference equations, van der Put and Singer [vPS1] introduced the notion of the PV ring for such an equation, and established the desired theory.

From the viewpoint of non-commutative differential geometry, André [A] gave a unified approach to the PV theories for differential and difference equations. Alternatively following Takeuchi's line, this paper will give such an approach in the context of artinian simple (AS) module algebras over a cocommutative, pointed smooth Hopf algebra D. Thus D is of the form $D = D^1 \# RG$ over a fixed field, say R, where G is the group of grouplikes in D, and the irreducible component D^1 containing 1 is of Birkhoff-Witt type; see Assumption 2.3. A difference ring which includes R in its constants is precisely a D-module algebra, where $D^1 = R$, and G is the free group with one generator. Differential rings are also within our scope, though only in characteristic zero because of the smoothness assumption. Algebras with higher derivations of infinite length fit in the assumption, in arbitrary characteristic.

D-module algebras are all supposed to be commutative, at least in this Introduction. A D-module algebra K is said to be *AS* if it is artinian as a ring and simple as a D-module algebra. Let K be an AS D-module algebra. If $P \subset K$ is a maximal ideal, then one will see that $K_1 := K/P$ is a module field over the Hopf subalgebra $D(G_P) := D^1 \# RG_P$, where G_P denotes the subgroup (necessarily of finite index) of the stabilizers of P. Moreover, K can recover from K_1, so as

$$K = D \otimes_{D(G_P)} K_1 = \bigoplus_{g \in G/G_P} g \otimes K_1,$$

where the product in K recovers from the component-wise product $(g \otimes a)(g \otimes b) = g \otimes ab$ in the last direct sum; see Section 2 below. The D-invariants K^D in K form a subfield, such that $K^D \simeq K_1^{D(G_P)}$. Following [T], we say that an inclusion $K \subset L$ of AS D-module algebras is a *PV extension*, if $K^D = L^D$ and if there exists a (necessarily unique) D-module algebra $K \subset A \subset L$ such that the total quotient ring $Q(A)$ equals L, and $H := (A \otimes_K A)^D$ generates the left (or right) A-module $A \otimes_K A$. Then H has a natural structure of a commutative Hopf algebra over K^D $(= L^D)$, with which A/K is a right

H-Galois extension; see Proposition 3.4. If an inclusion $K \subset L$ of AS D-module algebras is a PV extension, then the induced inclusion $K/P \cap K \subset L/P$ of $D(G_P)$-module fields is a PV extension, where P is an arbitrary maximal ideal of L. The converse holds true if G_P is normal in $G_{P\cap K}$; see Proposition 3.13 and Theorem 3.15.

As our main theorems we prove:

Galois Correspondence (Theorem 3.9): Given a PV extension L/K of AS D-module algebras, there is a 1-1 correspondence between the intermediate AS D-module algebras $K \subset M \subset L$ and the Hopf ideals I in the associated Hopf algebra H; L/M is then a PV extension with the associated Hopf algebra H/I. This has the obvious interpretation in terms of the affine group scheme $\boldsymbol{G}(L/K) = \operatorname{Spec} H$ corresponding to H.

Characterization (Theorem 4.6): An inclusion $K \subset L$ of AS D-module algebras with $K^D = L^D$ is a finitely generated PV extension if and only if L/K is a minimal splitting algebra for some $K\#D$-module V of finite K-free rank, say n; this means that $L \otimes_K V \simeq L^n$ as $L\#D$-modules, and L is "minimal" with this property.

Tensor Equivalence (Theorem 4.10): If this is the case, the symmetric tensor category $\mathcal{M}^H_{\text{fin}}$ of finite-dimensional right comodules over the associated Hopf algebra H (or equivalently that category $\operatorname{Rep}_{\boldsymbol{G}(L/K)}$ of finite-dimensional linear representations of $\boldsymbol{G}(L/K)$) is equivalent to the abelian, rigid tensor full subcategory $\{\{V\}\}$ "generated" by V, in the tensor category $({}_{K\#D}\mathcal{M}, \otimes_K, K)$ of $K\#D$-modules; cf. [vPS2, Theorem 2.33].

Unique Existence (Theorem 4.11): Suppose that K^D is an algebraically closed field. For every $K\#D$-module V of finite K-free rank, there is a unique (up to isomorphism) minimal splitting algebra L/K which is a (finitely generated) PV extension.

One cannot overestimate the influence of the article [T] by Takeuchi on this paper of ours. Especially the main theorems above except the third are very parallel to results in [T], including their proofs. A C-ferential field is equivalent to a module field over the tensor bialgebra $T(C^+)$ [T, p. 485]. We remark that even if K, L are fields, the first two theorems above do not imply the corresponding results in [T]. The last one only generalizes [T, Theorems 4.5, 4.6] in which $T(C^+)$ is supposed to be of Birkhoff-Witt type.

1. Tensor equivalences associated to an inclusion of cocommutative Hopf algebras

Throughout we work over a fixed field R. In particular the unadorned $\otimes$ means $\otimes_R$. Modules mean left modules unless otherwise stated.

Let C be a cocommutative Hopf algebra. The structure maps (for any Hopf algebra as well) will be denoted by

$$\Delta : C \to C \otimes C, \quad \varepsilon : C \to R, \quad S : C \to C,$$

as usual. The C-modules form an R-abelian tensor category ${}_C\mathcal{M} = ({}_C\mathcal{M}, \otimes, R)$ with the obvious tensor product $V \otimes W$ and the unit object R. This is symmetric by the trivial symmetry $V \otimes W \to W \otimes V$, $v \otimes w \mapsto w \otimes v$.

Let D be a cocommutative Hopf algebra including C as a Hopf subalgebra. A coalgebra in the tensor category ${}_D\mathcal{M}$ is called a *D-module coalgebra*. Define $\bar{D} = D/DC^+$, where $C^+ = \mathrm{Ker}(\varepsilon : C \to R)$. D is a D-module coalgebra, and $\bar{D}$ is its quotient. Let ${}^{\bar{D}}_D\mathcal{M}$ denote the R-abelian category of $(\bar{D}, D)$-Hopf modules such as defined in [T2, pp. 454–455]. Given objects M, N in ${}^{\bar{D}}_D\mathcal{M}$, let $M \Box_{\bar{D}} N$ denote the cotensor product; this is by definition the equalizer of the two $\bar{D}$-colinear maps $M \otimes N \rightrightarrows \bar{D} \otimes M \otimes N$ given by the structure maps of M, N. This is a D-submodule of $M \otimes N$, and is further an object in ${}^{\bar{D}}_D\mathcal{M}$. We see that ${}^{\bar{D}}_D\mathcal{M} = ({}^{\bar{D}}_D\mathcal{M}, \Box_{\bar{D}}, \bar{D})$ is a symmetric tensor category, in which the associativity constraint $(M \Box_{\bar{D}} N) \Box_{\bar{D}} L \xrightarrow{\simeq} M \Box_{\bar{D}} (N \Box_{\bar{D}} L)$, the unit constraint $\bar{D} \Box_{\bar{D}} N \xrightarrow{\simeq} N$ and the symmetry $M \Box_{\bar{D}} N \xrightarrow{\simeq} N \Box_{\bar{D}} M$ are the obvious ones.

For an object V in ${}_C\mathcal{M}$, define

$$\Phi(V) = D \otimes_C V.$$

This is naturally an object in ${}^{\bar{D}}_D\mathcal{M}$. We thus have an R-linear functor

$$\Phi : {}_C\mathcal{M} \to {}^{\bar{D}}_D\mathcal{M}.$$

Proposition 1.1. *Φ is an equivalence of symmetric tensor categories.*

Proof. By [T2, Theorem 2 and 4], Φ is a category equivalence; its quasi-inverse $N \mapsto \Psi(N)$ is given by

$$\Psi(N) = \{n \in N \mid \lambda(n) = \bar{1} \otimes n \ \text{ in } \ \bar{D} \otimes N\},$$

where $\lambda : N \to \bar{D} \otimes N$ is the structure map on N. It is easy to see that

$$\begin{array}{l} \Psi(M) \otimes \Psi(N) \to \Psi(M \Box_{\bar{D}} N), \quad m \otimes n \mapsto m \otimes n, \\ R \to \Psi(\bar{D}), \quad 1 \mapsto \bar{1} \end{array}$$

are isomorphisms in ${}_C\mathcal{M}$. We see that the isomorphisms, as tensor structures, make Ψ an equivalence of symmetric tensor categories. □

Let D^1 denote the irreducible component in D containing 1; this is the largest irreducible Hopf subalgebra. If the characteristic $\mathrm{ch}\, R$ of R is zero, then $D^1 = U(\mathfrak{g})$, the universal envelope of the Lie algebra $\mathfrak{g} = P(D)$ of all primitives in D; see [Mo, Sect. 5.6]. Let $G = G(D)$ denote the group of all grouplikes in D.

In what follows we suppose:

Assumption 1.2. D is pointed, so that

$$D = D^1 \# RG, \tag{1}$$

the smash product with respect to the conjugate action by G on D^1; see [Mo, Cor. 5.6.4].

In what follows we also take as C a Hopf subalgebra of the form

$$C = D^1 \# RG_1,$$

where $G_1 \subset G$ is a subgroup *of finite index*. This will be denoted by

$$C = D(G_1). \tag{2}$$

The equivalence Φ will be denoted by

$$\Phi_{G_1} : {}_{D(G_1)}\mathcal{M} \xrightarrow{\approx} {}^{\bar{D}}_{D}\mathcal{M}, \tag{3}$$

if one needs to specify G_1.

The vector space $R(G/G_1)$ freely spanned by the set G/G_1 of left cosets is a quotient left D-module coalgebra of D along the map $D = D^1 \# RG \to R(G/G_1)$ which is given by the counit $\varepsilon : D^1 \to R$ and the natural projection $G \to G/G_1$. Since the map induces an isomorphism $\bar{D} \xrightarrow{\simeq} R(G/G_1)$, an object in ${}^{\bar{D}}_{D}\mathcal{M}$ is such a left D-module N that is the direct sum $\bigoplus_{s \in G/G_1} N_s$ of those D^1-submodules N_s ($s \in G/G_1$) which satisfy that $gN_s \subset N_{gs}$, where $g \in G$, $s \in G/G_1$. If $M = \bigoplus_{s \in G/G_1} M_s$ is another object in ${}^{\bar{D}}_{D}\mathcal{M}$, then

$$M \Box_{\bar{D}} N = \bigoplus_{s \in G/G_1} M_s \otimes N_s.$$

We have $D = \bigoplus_{g \in G/G_1} gC$.

Notation 1.3. Here and in what follows, $g \in G/G_1$ means that g lies in a fixed system of those representatives in G for the left cosets G/G_1 which include the neutral element 1 in G.

The neutral component N_1 in N is a C-submodule. We have the identification

$$\Phi(N_1) = \bigoplus_{g \in G/G_1} g \otimes N_1.$$

Here D acts on the right-hand side so that if $d \in D^1$,

$$d(g \otimes n) = g \otimes (g^{-1} dg)n \quad (n \in N_1),$$

and if $h \in G$,

$$h(g \otimes n) = g' \otimes tn \quad (n \in N_1),$$

where g' is a representative and $t \in G_1$ such that $hg = g't$. Notice that $\Psi(N) = N_1$. Hence, by Proposition 1.1, we have a natural isomorphism $\Phi(N_1) = \bigoplus_{g \in G/G_1} g \otimes N_1 \xrightarrow{\simeq} N$ in ${}^{\bar{D}}_{D}\mathcal{M}$, given by $g \otimes n \mapsto gn$.

An algebra A in ${}^{\bar{D}}_{D}\mathcal{M}$ is precisely such a D-module algebra that is the direct product $\prod_{s \in G/G_1} A_s$ of D^1-module algebras A_s $(s \in G/G_1)$, satisfying $gA_s \subset A_{gs}$ $(g \in G)$. It is identified with $\Phi(A_1) = \bigoplus_{g \in G/G_1} g \otimes A_1$, which is endowed with the component-wise product.

Let $A = \Phi(A_1)$ be as above. An A_1-module V in ${}_C\mathcal{M}$ is precisely a module over the algebra $A_1 \# C$ of smash product. $\Phi(V)$ is naturally an A-module in ${}^{\bar{D}}_{D}\mathcal{M}$; this is in particular an $A\#D$-module.

Proposition 1.4. *The functor*

$$\Phi : {}_{A_1 \# C}\mathcal{M} \to {}_{A \# D}\mathcal{M}$$

gives an equivalence between the R-abelian categories of modules.

Proof. By Proposition 1.1, it suffices to prove that the category ${}_A({}^{\bar{D}}_{D}\mathcal{M})$ of A-modules in ${}^{\bar{D}}_{D}\mathcal{M}$ is isomorphic to ${}_A({}_D\mathcal{M}) = {}_{A\#D}\mathcal{M}$. Given N in ${}_{A\#D}\mathcal{M}$, define $N_g = (g \otimes 1)N$ $(g \in G/G_1)$, where $g \otimes 1$ denote the canonical, orthogonal central idempotents in $\Phi(A_1)$. Then $N = \bigoplus_{g \in G/G_1} N_g$ so that N is in ${}_A({}^{\bar{D}}_{D}\mathcal{M})$. This gives the desired isomorphism. $\square$

The proposition can be extended to bimodule categories. As is easily seen, the equivalence preserves the tensor structure:

Proposition 1.5. *Let $A = \Phi(A_1)$ be as above. The functor*

$$\Phi : ({}_{A_1}({}_C\mathcal{M})_{A_1}, \otimes_{A_1}, A_1) \to ({}_A({}_D\mathcal{M})_A, \otimes_A, A)$$

gives a tensor equivalence between the categories of bimodules.

For a C-module V, let

$$V^C = \{v \in V \mid cv = \varepsilon(c)v \quad (c \in C)\}$$

denote the vector space of C-invariants. Similarly, let N^D denote the vector space of D-invariants in a D-module N.

Lemma 1.6. *A natural isomorphism $V^C \xrightarrow{\simeq} \Phi(V)^D$ is given by $v \mapsto \sum_{g \in G/G_1} g \otimes v$.*

Proof. If $\sum_g g \otimes v_g \in \Phi(V)^D$, one sees first $v_1 \in V^C$, and then $v_g = v_1$ for all $g \in G/G_1$. □

To prepare for discussions in Section 3, let $K \subset A$ be an inclusion of D-module algebras. Then $A \otimes_K A$ is in ${}_A({}_D\mathcal{M})_A$. This has the natural coalgebra structure

$$A \xleftarrow{\boldsymbol{\varepsilon}} A \otimes_K A \xrightarrow{\boldsymbol{\Delta}} (A \otimes_K A) \otimes_A (A \otimes_K A) \tag{4}$$

in the tensor category $({}_A({}_D\mathcal{M})_A, \otimes_A, A)$, given by

$$\boldsymbol{\varepsilon}(a \otimes b) = ab, \quad \boldsymbol{\Delta}(a \otimes b) = (a \otimes 1) \otimes (1 \otimes b).$$

See [Sw].

2. Simple module algebras

In what follows algebras (in any symmetric tensor category) are supposed to be commutative and non-zero, unless otherwise stated.

Let $D = D^1 \# RG$ be a cocommutative pointed Hopf algebra, as in (1); this, as an exception, can be non-commutative.

Definition 2.1. A D-module algebra K is said to be *simple* if it is simple as a $K\#D$-module, or in other words if it includes no non-trivial D-stable ideal.

Lemma 2.2. *Let $G_1 \subset G$ be a subgroup of finite index. A module algebra K_1 over $D(G_1)$ (see (2)) is simple if and only if the D-module algebra $\Phi_{G_1}(K_1)$ is simple.*

Proof. This follows from Proposition 1.4. □

In what follows we suppose in addition:

Assumption 2.3. The irreducible Hopf algebra D^1 is of Birkhoff-Witt type.

This means that as a coalgebra, D^1 is spanned by (possibly infinitely many) divided power sequences of infinite length. This is necessarily satisfied if $\mathrm{ch}\, R = 0$. If $\mathrm{ch}\, R = p > 0$, this is equivalent to the Verschiebung map $D^1 \to R^{1/p} \otimes D^1$ being surjective. The assumption implies that if A is an algebra, the A-algebra $\mathrm{Hom}(D^1, A)$ of all R-linear maps $D^1 \to A$, whose product is given by the convolution-product, is the projective limit of A-algebras, $A[[x_1, \ldots, x_n]]$, of power series. The assumption is equivalent to saying that D is smooth as a cocommutative coalgebra.

A differential ring which includes R in its constants is precisely a module algebra over the polynomial Hopf algebra $R[d]$, in which d is primitive, and hence acts as a derivation. The Hopf algebra $R[d]$ $(= R[d]^1)$ satisfies Assumption 2.3 if and only if $\mathrm{ch}\, R = 0$. A difference ring which includes R in its constants is precisely a module algebra over the group algebra $R[g, g^{-1}]$ of the free group with one generator g, which is grouplike, and hence acts as an automorphism. An algebra (over R) with R-linear higher derivations $d_0 = \mathrm{id}, d_1, d_2, \ldots$ of infinite length is precisely a module algebra over the Hopf algebra $R\langle d_1, d_2, \ldots \rangle$, which denotes the (non-commutative) free algebra generated by $d_1, d_2, \ldots$, and in which $1, d_1, d_2, \ldots$ form a divided power sequence. This Hopf algebra satisfies Assumption 2.3, in arbitrary characteristic; see [T, p. 504].

Let K be a D-module algebra in general. Suppose that K is noetherian as a ring. Let $\Omega(K)$ denote the (finite) set of all minimal prime ideals in K. Then G acts on $\Omega(K)$. Let $G_{\Omega(K)}$ denote the normal subgroup consisting of those elements in G which stabilize every $P \in \Omega(K)$.

Proposition 2.4. *Suppose that K is simple.*

(i) *The action of G on $\Omega(K)$ is transitive, so that the subgroups G_P of stabilizers of $P \in \Omega(K)$ are conjugate to each other.*

(ii) *Every $P \in \Omega(K)$ is D^1-stable, so that K/P is a $D(G_P)$-module domain. This is simple as a $D(G_{\Omega(K)})$-module algebra.*

(iii) *Let $P \in \Omega(K)$, and set $K_1 = K/P$. Then we have a natural isomorphism of D-module algebras,*

$$K \simeq \Phi_{G_P}(K_1).$$

Proof. (ii) Let

$$\rho : K \to \mathrm{Hom}(D^1, K), \quad x \mapsto [d \mapsto dx] \tag{5}$$

denote the algebra map associated to the D^1-module algebra structure on K. This is D^1-linear, where $(d\varphi)(c) = \varphi(cd)$ $(c, d \in D^1,\ \varphi \in \mathrm{Hom}(D^1, K))$. Since $\mathrm{Hom}(D^1, K/P)$ is a domain, $\mathrm{Hom}(D^1, P)$ is a prime ideal in $\mathrm{Hom}(D^1, K)$, so that its pull-back P', say, along ρ is a D^1-stable prime ideal; see the proof of [T, Lemma 4.2]. We see that $P' \subset P$, and so $P = P'$ by the minimality of P. Hence P is D^1-stable.

For the second statement, let $P \subset J \subsetneq K$ be a $D(G_{\Omega(K)})$-stable ideal. Then, $\bigcap_{g \in G/G_{\Omega(K)}} gJ$ is D-stable, and hence is zero. Since P is prime, there exists g such that $gJ \subset P$, and so $P \subset J \subset g^{-1}P$. By the minimality of $g^{-1}P$, $P = J$ $(= g^{-1}P)$.

(i) Let $P \in \Omega(K)$. We see

$$\bigcap_{g \in G} gP = \bigcap_{Q \in \Omega(K)} Q = 0, \tag{6}$$

since the intersections are both D-stable. The first equality implies $\{gP \mid g \in G\} = \Omega(K)$; this proves (i).

(iii) By (i), $g \mapsto gP$ gives a bijection $G/G_P \xrightarrow{\simeq} \Omega(K)$. If Q and Q' in $\Omega(K)$ are distinct, then $(Q \subsetneq)\ Q + Q' = K$, by (ii). This together with (6) proves that the natural map gives an isomorphism,

$$K \xrightarrow{\simeq} \prod_{Q \in \Omega(K)} K/Q = \prod_{g \in G/G_P} K/gP.$$

Obviously, $\Phi_{G_P}(K_1)$ is isomorphic to the last direct product. □

Corollary 2.5. *For K as above the following are equivalent.*

(a) *K is total in the sense that any non-zero divisor in K is invertible;*
(b) *K is artinian as a ring;*
(c) *The Krull dimension* $\mathrm{Kdim}(K) = 0$*, or in other words $\Omega(K)$ equals the set of all maximal ideals in K.*

If these conditions are satisfied, every $K\#D$-module is free as a K-module.

Proof. Each condition is equivalent to that for any/some $P \in \Omega(K)$, K/P is a field. The last assertion holds true by Part (iii) of the last proposition and by Proposition 1.4. □

Definition 2.6. A D-module algebra K is said to be *AS*, if it is artinian and simple. By the corollary above, this is equivalent to that K is total, noetherian and simple.

A D-module field is obviously AS. The total PV ring [vPS1, Definition 1.22] of a difference equation is an AS $R[g, g^{-1}]$-module algebra over the field R of constants. Therefore the standard PV theories for differential equations in characteristic zero, and for difference equations in arbitrary characteristic is within our scope.

For later use we prove some results.

Lemma 2.7. *Let A be a D-module algebra, and let $T \subset A$ be a G-stable multiplicative subset. The D-module algebra structure on A can be uniquely extended to the localization $T^{-1}A$ of A by T. (D^1 may not be of Birkhoff-Witt type.)*

Proof. The algebra map $\rho : A \to \mathrm{Hom}(D, A)$ associated to A (see (5)) is uniquely extended to an algebra map $\tilde{\rho} : T^{-1}A \to \mathrm{Hom}(D, T^{-1}A)$, since each $\rho(t)$, $t \in T$, is invertible on RG, and so on the whole D; cf. the proof of [T, Proposition 1.9]. We have thus obtained the measuring action

$$d(a/t) = \tilde{\rho}(a/t)(d) \qquad (d \in D, \quad a \in A, \quad t \in T)$$

by D on $T^{-1}A$. It remains to prove that this makes $T^{-1}A$ a D-module. We have only to see that

$$cd(1/t) = c(d(1/t)) \qquad (c, d \in D, \quad t \in T).$$

This holds since the two maps $D \otimes D \to T^{-1}A$, $c \otimes d \mapsto cd(1/t)$ and $c \otimes d \mapsto c(d(1/t))$ coincide, because both of them are the convolution-inverse of $c \otimes d \mapsto cdt$. □

As the referee kindly informed us, the preceding lemma is proved by Tyc and Wiśniewski [TyW, Theorem 3.4], in which the pointed Hopf algebra is not supposed to be cocommutative. Also, the first part of our Proposition 2.4 (ii) follows from [TyW, Theorem 5.9 (2)].

Lemma 2.8. *Let L be an AS D-module algebra, and let $K \subset L$ be a D-module subalgebra. If K is total, then K is AS.*

Proof. Given an element $x \neq 0$ in $L = \prod_{P \in \Omega(L)} L/P$, define the support of x by

$$\mathrm{supp}(x) = \{P \in \Omega(L) \mid x \notin P\}. \tag{7}$$

One sees that x is a non-zero divisor if and only if $\mathrm{supp}(x) = \Omega(L)$.

Choose an element $x \neq 0$ in K with minimal support. Then for $g \in G$, the supports $\mathrm{supp}(x)$ and $\mathrm{supp}(gx)$ are either equal or disjoint, according to $x(gx)$ being non-zero or zero. By Proposition 2.4 (i), we have those elements $x, g_1x, \ldots, g_rx$ in K with disjoint supports, whose sum is a non-zero divisor. Let y be the inverse of the sum; this is indeed in K, since K is total. We see that $e := xy$ is a (primitive) idempotent in K

with $\operatorname{supp}(e) = \operatorname{supp}(x)$. By the minimality of the support, each non-zero element in eK has $\operatorname{supp}(x)$ as its support, and hence has an inverse in eK, just as x above. We have $K = \prod_{i=1}^{r} g_i eK$, the direct product of the fields $g_i eK$; this proves the lemma. □

Corollary 2.9. *Let A be a D-module subalgebra in an AS D-module algebra L.*

(i) *Every non-zero divisor x in A has full support:* $\operatorname{supp}(x) = \Omega(L)$ *(see (7)).*

(ii) *Let $K = Q(A)$ denote the total quotient ring of A; this is realized in L by* (i). *Then K is an AS D-module subalgebra of L.*

Proof. Let T be the set of all non-zero divisors in A. Then, $K = T^{-1}A$.

(i) Choose an $x \in T$ such that $\operatorname{supp}(x)$ is minimal in $\{\operatorname{supp}(t) \mid t \in T\}$. If $\operatorname{supp}(x) \neq \Omega(L)$, there is a $g \in G$ such that $\operatorname{supp}(gx) \cap \operatorname{supp}(x) = \emptyset$, which implies $x(gx) = 0$, a contradiction.

(ii) Let $\rho_L : L \to \operatorname{Hom}(D, L)$ be the algebra map associated to the D-module algebra structure on L. It restricts to $\rho : A \to \operatorname{Hom}(D, A)$ associated to A. If $t \in T$, $\rho_L(1/t)$ is the inverse of $\rho(t)$ in $\operatorname{Hom}(D, L)$, and hence is contained in $\operatorname{Hom}(D, T^{-1}A)$ by the proof of Lemma 2.7. This implies that K $(= T^{-1}A)$ is a D-module subalgebra of L. K is AS by Lemma 2.8. □

3. Picard-Vessiot extensions of AS module algebras

Proposition 3.1. *In general an object X in an abelian category $\mathfrak{A}$ is simple if and only if*

(a) *the endomorphism ring $E := \mathfrak{A}(X, X)$ is a division ring, and*

(b) *for every object Y in $\mathfrak{A}$, the evaluation map*

$$\mathrm{ev} : \mathfrak{A}(X, Y) \otimes_E X \to Y$$

is injective.

Proof. This seems well known, though we could not find an explicit citation in the literatures. The proposition is specialized by [MY, Theorem 1.1 and the Theorem on p. 232], and the proof given there works in the generalized context, as was suggested by T. Brzeziński. □

Corollary 3.2. *Let L be a simple D-module algebra. Then L^D is a field, and for every $Y \in {}_{L\#D}\mathcal{M}$, the natural map*

$$L \otimes_{L^D} Y^D \to Y, \quad x \otimes y \mapsto xy$$

is injective.

Proof. This follows by applying the proposition for X in $\mathfrak{A}$ to L in ${}_{L\#D}\mathcal{M}$. Notice that $L^D \simeq \mathrm{End}_{L\#D}(L)$, and the natural map above is identified with the evaluation map. □

Let $K \subset L$ be an inclusion of AS D-module algebras. By the corollary we have an inclusion of fields, $K^D \subset L^D$.

Definition 3.3. We say that L/K is a *Picard-Vessiot*, or *PV*, *extension* if the following conditions are satisfied:

(a) $K^D = L^D$; this will be denoted by k.

(b) There exists a D-module subalgebra $A \subset L$ including K, such that the total quotient ring $Q(A)$ of A equals L, and the k-subalgebra $H := (A \otimes_K A)^D$ generates the left (or equivalently right) A-module $A \otimes_K A$: $A \cdot H = A \otimes_K A$ (or $H \cdot A = A \otimes_K A$).

Proposition 3.4. *Suppose that L/K is a PV extension. Let A, H be as in Condition (b) above.*

(i) *The product map $\mu : A \otimes_k H \to A \otimes_K A$, $\mu(a \otimes h) = a \cdot h$ is a D-linear isomorphism.*

(ii) *The k-algebra H has a unique Hopf algebra structure such that the k-algebra map $\theta : A \to A \otimes_k H$, $\theta(a) = \mu^{-1}(1 \otimes a)$ makes A a right H-comodule. A/K is necessarily a right H-Galois extension* [Mo, Sect. 8.1] *in the sense that*

$$ {}_A\theta : A \otimes_K A \to A \otimes_k H, \quad {}_A\theta(a \otimes b) = a\theta(b) $$

is an isomorphism.

(iii) *Such an algebra A that satisfies Condition (b) above is unique.*

Proof. (i) Since by Corollary 3.2, the natural map $L \otimes_k (L \otimes_K A)^D \to L \otimes_K A$ is injective, the map μ is injective; it is surjective by Condition (b).

(ii) Notice that $A^D = k$ by Condition (a). The twofolds $A \otimes_k H \otimes_k H \xrightarrow{\simeq} A \otimes_K A \otimes_K A$ of μ, being a D-linear isomorphism, induces an isomorphism $H \otimes_k H \xrightarrow{\simeq} (A \otimes_K A \otimes_K A)^D$. Similarly the threefolds of μ induces $H \otimes_k H \otimes_k H \xrightarrow{\simeq} (A \otimes_K A \otimes_K A \otimes_K A)^D$. It follows by [T, Proposition 2.2] that the coalgebra structure (4) on $A \otimes_K A$ in ${}_A({}_D\mathcal{M})_A$ induces a Hopf algebra structure on H,

$$ k \xleftarrow{\varepsilon} H \xrightarrow{\Delta} H \otimes_k H. $$

The antipode is induced from the twist map $a \otimes b \mapsto b \otimes a$, $A \otimes_K A \to A \otimes_K A$. The map ${}_A\theta$, being μ^{-1}, is an isomorphism. Since this interprets θ into the natural right $A \otimes_K A$-comodule structure $a \mapsto 1 \otimes a$, $A \to A \otimes_K A = A \otimes_A (A \otimes_K A)$ on A, we see the described uniqueness of the structure on H.

(iii) This follows in the same ways as [T, Lemma 2.5], but by using the fact that L is a free K-module; see Corollary 2.5. □

Definition 3.5. A (resp., H) is called *the principal D-module algebra* (resp., *the Hopf algebra*) *for L/K*. To indicate these we say that $(L/K, A, H)$ is a PV extension.

Example 3.6. Let $G_1 \subset G$ be a *normal* subgroup of finite index. Let K be a D-module field. Regarding this as a $D(G_1)$-module algebra, define $L = \Phi_{G_1}(K)$. We then have the inclusion

$$K \hookrightarrow L = \bigoplus_{g \in G/G_1} g \otimes K, \quad x \mapsto \sum_g g \otimes g^{-1}x$$

of AS D-module algebras. If $K^{D(G_1)} = K^D$, then $K^D = L^D$ $(=: k)$ by Lemma 1.6. Moreover, $(L/K, L, H)$ is a PV extension, where $H = k(G/G_1)^*$, the dual of the group algebra $k(G/G_1)$. In fact, we see that the elements

$$e_g := \sum_{h \in G/G_1} (h \otimes 1) \otimes_K (hg \otimes 1) \quad (g \in G/G_1)$$

in $L \otimes_K L$ are D-invariant, and behave as the dual basis in H of the group elements g $(\in G/G_1)$ in $k(G/G_1)$. Thus, $\Delta(e_g) = \sum_h e_{gh^{-1}} \otimes e_h$, $\varepsilon(e_g) = \delta_{1,g}$, $S(e_g) = e_{g^{-1}}$. The H-comodule structure $\theta : L \to L \otimes_k H$ is given by

$$\theta(h \otimes x) = \sum_g (hg^{-1} \otimes gx) \otimes_k e_g,$$

as is seen from following computation in $L \otimes_K L$:

$$1 \otimes_K (h \otimes x) = \sum_f (f \otimes f^{-1}hx) \otimes_K (h \otimes 1) = \sum_g (hg^{-1} \otimes gx) \otimes_K (h \otimes 1) = \sum_g (hg^{-1} \otimes gx) \cdot e_g.$$

Lemma 3.7. *Let $G_1 \subset G$ be a subgroup of finite index. Write $\Phi = \Phi_{G_1}$. Let $K_1 \subset L_1$ be an inclusion of AS $D(G_1)$-module algebras. $(L_1/K_1, A_1, H)$ is a PV extension if and only if $(\Phi(L_1)/\Phi(K_1), \Phi(A_1), H)$ is a PV extension of AS D-module algebras.*

Proof. The natural coalgebra isomorphism $\Phi(A_1 \otimes_{K_1} A_1) \simeq \Phi(A_1) \otimes_{\Phi(K_1)} \Phi(A_1)$ (see Proposition 1.5) together with Lemma 1.6 prove the lemma. □

Remark 3.8. Let $K \subset L$ be an inclusion of AS D-module algebras. Choose $\mathfrak{p} \in \Omega(K)$, and let $P_1, \dots, P_r$ be all those elements in $\Omega(L)$ that lie over $\mathfrak{p}$. Define $K_1 = K/\mathfrak{p}$, $L_1 = \prod_{i=1}^{r} L/P_i$. Then we have an inclusion $K_1 \subset L_1$ of AS $D(G_\mathfrak{p})$-module algebras such that the induced inclusion $\Phi_{G_\mathfrak{p}}(K_1) \subset \Phi_{G_\mathfrak{p}}(L_1)$ is identified with $K \subset L$. We can thus reduce to the case where K is a field, especially to discuss PV extensions; see Lemma 3.7.

Theorem 3.9. *Let $(L/K, A, H)$ be a PV extension of AS D-module algebras.*

(i) *There is a 1-1 correspondence between the Hopf ideals $I \subset H$ and the intermediate AS D-module algebras $K \subset M \subset L$, given by*

$$M = \{x \in L \mid 1 \otimes x \equiv x \otimes 1 \mod I \cdot (L \otimes_K L)\},$$
$$I = H \cap \mathrm{Ker}(L \otimes_K L \to L \otimes_M L).$$

(ii) *If $I \leftrightarrow M$ under the correspondence, $(L/M, AM, H/I)$ is a PV extension.*

(iii) *Suppose $I \leftrightarrow M$ under the correspondence. I is a normal Hopf ideal* [T1] *if and only if M/K is a PV extension.*

The 1-1 correspondence in Part (i) is obtained as the composite of the 1-1 correspondences given below.

Proposition 3.10. *Let $K \subset L$ be an inclusion of AS D-module algebras.*

(i) *Suppose that $(L/K, A, H)$ is a PV extension. Then, $I \mapsto I \cdot (L \otimes_K L)$ gives a 1-1 correspondence between the Hopf ideals $I \subset H$ and the coideals $\mathcal{I}$ of the coalgebra $L \otimes_K L$ in $({}_L({}_D\mathcal{M})_L, \otimes_L, L)$; see (4).*

(ii) *$M \mapsto \mathrm{Ker}(L \otimes_K L \to L \otimes_M L)$ gives a 1-1 correspondence between the intermediate AS D-module algebras $K \subset M \subset L$ and the coideals $\mathcal{I}$ as above.*

Proof. (i) This follows in the same way as [T, Proposition 2.6], but by using Corollary 3.2. In fact the correspondence is extended to a 1-1 correspondence between the ideals $I \subset H$ and the D-stable ideals $\mathcal{I} \subset L \otimes_K L$.

(ii) Suppose that $K \subset M \subset L$ is given. Since L, being an $M\#D$-module, is M-free, M can recover from $\mathcal{I} := \mathrm{Ker}(L \otimes_K L \to L \otimes_M L)$ so as

$$M = \{x \in L \mid 1 \otimes x \equiv x \otimes 1 \mod \mathcal{I} \text{ in } L \otimes_K L\}. \tag{8}$$

Suppose that $\mathcal{I} \subset L \otimes_K L$ is a coideal, and define M by (8); this is obviously an intermediate D-module algebra. By Corollary 2.9 (i), every non-zero divisor x in M has full support, and we easily see $x^{-1} \in M$. Then M is AS by Lemma 2.8.

Let $\mathcal{C} = L \otimes_K L/\mathcal{I}$. One sees that the canonical $L \otimes_K L \to \mathcal{C}$ factors through a coalgebra surjection,

$$\alpha : L \otimes_M L \to \mathcal{C}.$$

To prove the injectivity we may suppose by Proposition 1.5 that M is a field; replace $M \subset L$ with $M_1 \subset L_1$ so as in Remark 3.8. To apply Proposition 3.1, regard $\mathcal{C}$ merely as an L-coring, or a coalgebra in $({}_L\mathcal{M}_L, \otimes_L, L)$, and suppose $\mathfrak{A}$ is the category of right $\mathcal{C}$-comodules; an object Y in $\mathfrak{A}$ is thus a *right* L-module with a right L-linear structure map $Y \to Y \otimes_L \mathcal{C}$. Notice that the category is abelian since $\mathcal{C}$ is left L-free. Take L as the X in the proposition; it has the natural $\mathcal{C}$-comodule structure

$$\lambda : L \to L \otimes_L \mathcal{C} = \mathcal{C}, \quad \lambda(x) \equiv 1 \otimes_K x \mod \mathcal{I}.$$

Since $E = \mathfrak{A}(L, L) \simeq M$, $\mathfrak{A}(L, \mathcal{C}) \simeq L$, we identify α with the evaluation map for $Y = \mathcal{C}$. Therefore it suffices to see that L is simple in $\mathfrak{A}$. L includes a simple subobject of the form eL, where e is an idempotent. Since λ is D-linear, we see that for $g \in G$, $g(eL)$ is also a simple subobject, which coincides or trivially intersects with eL. It follows from Proposition 2.4 (i) that L is semisimple; this implies that L is simple since the endomorphism ring E is a field. □

Part (ii) of Theorem 3.9 follows in the same way as [T, Proposition 2.8]. Part (iii) follows as [T, Theorem 2.9], but by using Lemma 2.7. Suppose $I \leftrightarrow M$ is as in Part (iii). The Hopf algebra H' and the principal module algebra A' associated to M/K is given by

$$H' = \{h \in H \mid \Delta(h) \equiv h \otimes 1 \mod H \otimes_k I\},$$
$$A' = \theta^{-1}(A \otimes_k H'),$$

where $\theta : A \to A \otimes_k H$ denotes the natural H-comodule structure. For a right comodule V over a k-Hopf algebra $\mathcal{H}$ in general, let

$$V^{\mathrm{co}\mathcal{H}} = \{v \in V \mid \rho_V(v) = v \otimes 1\}$$

denote the k-subspace of $\mathcal{H}$-coinvariants, where $\rho_V : V \to V \otimes_k \mathcal{H}$ is the structure on V. We remark that

$$H' = H^{\mathrm{co}\bar{H}}, \quad A' = A^{\mathrm{co}\bar{H}} \qquad (\bar{H} = H/I).$$

Remark 3.11. Let $(L/K, A, H)$ be a PV extension of AS D-module algebras. The affine k-group scheme $\boldsymbol{G}(L/K) = \mathrm{Spec}_k H$ corresponding to H is called *the PV group scheme for* L/K. As in [T, Appendix], one sees that this is isomorphic to the automorphism group scheme $\mathbf{Aut}_{D,K-\mathrm{alg}}(A)$ of A; this associates to each k-algebra T the group $\mathrm{Aut}_{D,K\otimes_k T-\mathrm{alg}}$

$(A \otimes_k T)$ of D-linear $K \otimes_k T$-algebra automorphisms of $A \otimes_k T$. In fact the linear representation $\boldsymbol{G}(L/K) \to \boldsymbol{GL}(A)$ arising from the H-comodule structure $\theta : A \to A \otimes_k H$ gives an isomorphism $\boldsymbol{G}(L/K) \simeq \mathbf{Aut}_{D,K-\mathrm{alg}}(A)$. Since $L = Q(A)$, the group $\boldsymbol{G}(L/K)(k)$ with values in k is isomorphic to the group $\mathrm{Aut}_{D,K-\mathrm{alg}}(L)$ of automorphisms of L. Theorem 3.9 allows the obvious interpretation in terms of $\boldsymbol{G}(L/K)$; see [T, Theorem 2.10].

Corollary 3.12. *Let $(L/K, A, H)$ be a PV extension of AS D-module algebras.*

(i) *A is simple as a D-module algebra.*

(ii) *A contains all primitive idempotents in L.*

Proof. (i) The following proof is essentially the same as that of [T, Theorem 2.11]; we contain this for the importance of the result.

Let $0 \neq \mathfrak{a} \subset A$ be a D-stable ideal. Then $L \otimes_K (A/\mathfrak{a})$ is a quotient D-module algebra of $L \otimes_K A$ $(\simeq L \otimes_k H)$. We see from Corollary 3.2 that $L \otimes_k (H/I) \simeq L \otimes_K (A/\mathfrak{a})$, and so $L \otimes_k I \simeq L \otimes_K \mathfrak{a}$, where $I \subset H$ is an ideal. Since $L\mathfrak{a} = L$ by the simplicity of L, it follows that $I \cdot (L \otimes_K L) = L \otimes_K L$. This implies that $I = H$, and so $\mathfrak{a} = A$, by the fact stated in the proof of Proposition 3.10 (i).

(ii) Since L is a localization of A, we have $\Omega(L) \subset \Omega(A)$ via $P \mapsto P \cap A$. We see $A \subset \prod_{P \in \Omega(L)} A/P \cap A$. It remains to prove that if $P \neq Q$ in $\Omega(L)$, then the sum $J := P \cap A + Q \cap A$ equals A. If $J \subsetneq A$ on the contrary, one sees as in the proof of Proposition 2.4 (ii) that $J = P \cap A = Q \cap A$ by Part (i), and so $P = Q$. □

Proposition 3.13. *Let $(L/K, A, H)$ be a PV extension of AS D-module algebras. Choose arbitrarily $P \in \Omega(L)$, and write $\Phi = \Phi_{G_P}$. Let $\mathfrak{p} = P \cap K$ $(\in \Omega(K))$. Define*

$$K_1 = K/\mathfrak{p}, \quad A_1 = A/P \cap A, \quad L_1 = L/P.$$

Then, (i) *We have $A \simeq \Phi(A_1)$.*

(ii) *$\Phi(K_1)$ is identified with the K-subalgebra $\hat{K}$ of L which is spanned over K by the primitive idempotents in L.*

(iii) *$(L_1/K_1, A_1, \bar{H} = H/I)$ is a PV extension of $D(G_P)$-module fields, where $I = H \cap \mathrm{Ker}(L \otimes_K L \to L \otimes_{\hat{K}} L)$; cf.* [vPS1, Corollary 1.16].

(iv) *The subalgebra of H*

$$B = \{h \in H \mid \Delta(h) \equiv h \otimes 1 \mod H \otimes_k I\} \quad (= H^{\mathrm{co}\bar{H}})$$

is a finite-dimensional separable k-algebra. We have a right $\bar{H}$-colinear B-algebra isomorphism $H \simeq B \otimes_k \bar{H}$.

(v) *If G_P is normal in $G_{\mathfrak{p}}$, then $B \subset H$ is a Hopf subalgebra which is isomorphic to $k(G_{\mathfrak{p}}/G_P)^*$, and we have an extension*

$$k(G_{\mathfrak{p}}/G_P)^* \rightarrowtail H \twoheadrightarrow \bar{H}$$

of Hopf algebras; cf. [vPS1, Corollary 1.17].

Proof. (i) This follows from Corollary 3.12 (ii).

(ii) This is easy to see.

(iii) By Theorem 3.9 (ii), we have a PV extension $(L/\hat{K}, A, \bar{H}) = (\Phi(L_1)/\Phi(K_1), \Phi(A_1), \bar{H})$. Part (iii) now follows by Lemma 3.7. □

For the remaining (iv), (v) we prove:

Lemma 3.14. *Let $G_1 \subset G$ be a subgroup of finite index. Write $\Phi = \Phi_{G_1}$. Let $K \subset A$ be an inclusion of D-module algebras.*

(i) *We have an isomorphism of D-module algebras over $\Phi(K)$,*

$$A \otimes_K \Phi(K) \xrightarrow{\simeq} \Phi(A),$$

given by $a \otimes_K (g \otimes x) \mapsto g \otimes (g^{-1}a)x$ $(g \in G/G_1)$.

(ii) *We have an isomorphism of K^D-algebras,*

$$A^{D(G_1)} \xrightarrow{\simeq} (A \otimes_K \Phi(K))^D,$$

given by $a \mapsto \sum_{g \in G/G_1} ga \otimes_K (g \otimes 1)$.

(iii) *Suppose $\Phi(K) \subset A$, so that $A = \Phi(A_1)$, where A_1 is a $D(G_1)$-module algebra. Let $N \subset G$ denote the largest normal subgroup (necessarily of finite index) that is included in G_1. Define $F = A_1^{D(N)}$; this is G_1-stable. Choose a system of representatives $g_1, \dots, g_t$ $(\in G)$ for the double cosets $G_1 \backslash G/G_1$. Then,*

$$A^{D(G_1)} = \sum_{i=1}^{t} (\sum_{g \in O_i} g) \otimes F^{g_i^{-1} S_i g_i},$$

where O_i denotes the orbit containing the coset $g_i G_1$ in the left G_1-set G/G_1, and $S_i \subset G_1$ denotes the subgroup of stabilizers of $g_i G_1$.

Proof. (i) This is easily seen.

(ii) This follows from (i) and Lemma 1.6.

(iii) We see

$$A^{D(G_1)} = (A^{D(N)})^{G_1} = (\bigoplus_{g\in G/G_1} g \otimes F)^{G_1}.$$

An element $\sum_{g\in G/G_1} g\otimes a_g$ ($a_g \in F$) is G_1-invariant if and only if $\sum_{g\in O_i} g\otimes a_g$ is so for each $1 \le i \le t$. Fix a coset g_iG_1, and suppose that

$$g_i, s_2g_i, \ldots, s_lg_i \quad (s_j \in G_1)$$

represent the G_1-orbit O_i. Then, $\sum_{j=1}^{l} s_jg_i \otimes a_j$ ($s_1 = 1$, $a_j \in F$) is G_1-invariant if and only if $s(g_i \otimes a_1) = s_jg_i \otimes a_j$ for every $s \in G_1$, where $sg_iG_1 = s_jg_iG_1$, or $s_j^{-1}s \in S_i$. This is further equivalent to that $a_1 = \cdots = a_l \in F^{g_i^{-1}S_ig_i}$, since we compute

$$s(g_i \otimes a_1) = s_jg_i \otimes (g_i^{-1}s_j^{-1}sg_i)a_1.$$

□

Proof of Proposition 3.13 (iv), (v). By Remark 3.8 we may suppose that K is a field, and so $\mathfrak{p} = 0$, $G_{\mathfrak{p}} = G$.

(iv) The obvious equalizer diagram

$$0 \to A \otimes_K \hat{K} \to A \otimes_K A \rightrightarrows A \otimes_K A \otimes_{\hat{K}} A$$

of D-module algebras is naturally identified with

$$0 \to A \otimes_k B \to A \otimes_k H \rightrightarrows A \otimes_k H \otimes_k \bar{H}.$$

In particular we see that

$$A \otimes_k B \simeq A \otimes_K \hat{K} = A \otimes_K \Phi(K)$$

and so

$$B = (A \otimes_K \Phi(K))^D. \tag{9}$$

By applying Lemma 3.14 to the present situation especially when $G_1 = G_P$, it follows that

$$(A \otimes_K \Phi(K))^D \simeq \sum_{i=1}^{t}(\sum_{g\in O_i} g) \otimes F^{g_i^{-1}S_ig_i}, \tag{10}$$

where $F = A_1^{D(N)}$ with $N = G_{\Omega(L)}$; see Proposition 2.4. Since $(L_1^{D(N)})^{G/N} = k$ with G/N finite, $L_1^{D(N)}/k$ is a finite Galois extension of fields. Therefore F and hence $F^{g_i^{-1}S_ig_i}$ now are finite separable field extensions over k. By (9), (10), B is a finite-dimensional separable k-algebra.

Recall that A has the natural, right $\bar{H}$-comodule k-algebra structure $A \xrightarrow{1\otimes -} A \otimes_{\hat{K}} A \simeq A \otimes_k \bar{H}$; in fact, A is also a left $\bar{H}$-comodule k-algebra. We see that the map

$$\sigma : \Phi(A_1 \otimes_K A_1) = A \otimes_{\hat{K}} A \to A \otimes_K A \tag{11}$$

given by $g \otimes (a \otimes_K b) \mapsto (g \otimes a) \otimes_K (g \otimes b)$ $(g \in G/G_P)$ is a D-linear, two-sided $\bar{H}$-colinear k-algebra splitting of $A \otimes_K A \to A \otimes_{\hat{K}} A$. The induced $\sigma^D : \bar{H} \to H$ is a two-sided $\bar{H}$-colinear k-algebra splitting of $H \to \bar{H}$. It follows by [Mo, Theorem 7.2.2] (due to Doi and Takeuchi) that

$$B \otimes_k \bar{H} \to H, \quad b \otimes x \mapsto b\sigma^D(x) \tag{12}$$

gives a right $\bar{H}$-colinear B-algebra isomorphism.

(iv) If G_P is normal in G, then $G_P = N$, and hence $F = k$ in (10). We then see $B = (\Phi(K) \otimes_K \Phi(K))^D$. By Example 3.6, $B \subset H$ is a Hopf subalgebra which is isomorphic to $k(G/G_P)^*$. The isomorphism given in (12) induces the described extension of Hopf algebras. □

Theorem 3.15. *Let $K \subset L$ be an inclusion of AS D-module algebras. Choose arbitrarily $P \in \Omega(L)$, and let $\mathfrak{p} = P \cap K$ $(\in \Omega(K))$. Then L/K is a PV extension if*

(a) *G_P is normal in $G_{\mathfrak{p}}$, and*

(b) *the inclusion $K_1 := K/\mathfrak{p} \subset L_1 := L/P$ of $D(G_P)$-module fields is a PV extension.*

The converse holds true if the field K^D $(= L^D)$ of D-invariants is separably closed.

Proof. This follows by slightly modifying the last proof, as follows. We may suppose that K is a field.

Suppose that $(L_1/K_1, A_1, \bar{H})$ is a PV extension. Define $A = \Phi(A_1)$ with $\Phi = \Phi_{G_P}$. Recall from Proposition 3.13 that if L/K is PV, the principal module algebra must be A. As was seen in the last proof, $A \otimes_K A$ is a right $\bar{H}$-comodule k-algebra and the map σ given in (11) induces an $\bar{H}$-colinear k-algebra map $\sigma^D : \bar{H} \to (A \otimes_K A)^D$. Again by [Mo, Theorem 7.2.2], we have a D-linear and $\bar{H}$-colinear isomorphism

$$A \otimes_K \Phi(K) \otimes_k \bar{H} \simeq A \otimes_K A$$

of algebras over $A \otimes_K \Phi(K)$; see (12). It follows that L/K is a PV extension if and only if the natural injection

$$A \otimes_k (A \otimes_K \Phi(K))^D \to A \otimes_K \Phi(K) \tag{13}$$

is surjective. If G_P is normal in G, then this is surjective since by Example 3.6, $A \otimes_k (\Phi(K) \otimes_K \Phi(K))^D \to A \otimes_K \Phi(K)$ is already surjective.

To prove the converse, we may suppose (b), and that the map given in (13) is an isomorphism. It follows that

$$\dim_k (A \otimes_K \Phi(K))^D = [G : G_P]. \tag{14}$$

If k is separably closed, then $F = k$ in (10). The equation (14) implies that ($t =$) $|G_P \backslash G / G_P| = [G : G_P]$, or G_P is normal in G. □

The first half of the theorem above seems new even in the standard PV theory for difference equations. As will be seen from the following, the second half does not necessarily hold true unless k is separably closed.

Example 3.16. Let $N \subset G_1 \subset G$ be as in Lemma 3.14. Suppose that K is a D-module field such that $K^{D(G_1)} = K^D$ $(=: k)$. Let $L = \Phi_{G_1}(K)$. One sees from the argument for (14) that L/K is a PV extension if and only if

$$\dim_k (L \otimes_K L)^D = [G : G_1].$$

The left-hand side equals

$$\sum_{i=1}^{t} \dim_k F^{g_i^{-1} S_i g_i} \tag{15}$$

with the notation in Lemma 3.14, including $F = K^{D(N)}$.

Suppose that N is trivial, and K/k is a Galois extension with $G_1 = \mathrm{Gal}(K/k)$. If $G_1 \subset G$ has a splitting $\pi : G \to G_1$ through which G acts on K, then L/K is a PV extension since one sees that the quantity (15) equals $\sum_{i=1}^{t} [G_1 : S_i] = \sum_{i=1}^{t} |O_i| = [G : G_1]$. We have a non-trivial example of such PV extension, for which $G = D_n$ is the dihedral group of order $2n \geq 6$ and G_1 is a cyclic subgroup of order 2.

4. Splitting algebras

Let $K \subset L$ be an inclusion of AS D-module algebras. Let V be a $K\#D$-module. The rank $\mathrm{rk}_K(V)$ of the free K-module V will be called the K-rank; see Corollary 2.5.

Definition 4.1. We say that V *splits in* L/K, or L/K is a *splitting algebra for* V, if there is an $L\#D$-linear injection $L \otimes_K V \hookrightarrow L^I$ into some power L^I of L.

Any $K\#D$-submodule $W \subset V$ splits in L/K, if V does.

Lemma 4.2. *If V has a finite K-rank, say, $n = \mathrm{rk}_K(V)$, then the following are equivalent:*

(a) *V splits in L/K;*

(b) *There is an $L\#D$-linear isomorphism $L \otimes_K V \xrightarrow{\simeq} L^n$;*

(c) *The canonical L-linear map*

$$L \otimes_{L^D} \mathrm{Hom}_{K\#D}(V, L) \to \mathrm{Hom}_K(V, L)$$

is an isomorphism.

Proof. See [T, Proposition 3.1] also for other equivalent conditions. We only remark that by Corollary 3.2, the map in (c) is necessarily injective, since $Y := \mathrm{Hom}_K(V, L)$ is an $L\#D$-module with $Y^D = \mathrm{Hom}_{K\#D}(V, L)$, under the D-conjugation:

$$(d\varphi)(v) = \sum d_1(\varphi(S(d_2)v)) \quad (d \in D, \quad \varphi \in Y, \quad v \in V). \tag{16}$$

Here, $\Delta(d) = \sum d_1 \otimes d_2$. □

Let $K\langle V\rangle$ denote the smallest AS D-module subalgebra in L that includes K and all $f(V)$, where $f \in \mathrm{Hom}_{K\#D}(V, L)$. This equals the quotient ring of the K-subalgebra in L generated by all $f(V)$. Obviously, V splits in $K\langle V\rangle/K$ if it does in L/K.

Definition 4.3. A splitting algebra L/K for V is said to be *minimal* if $L = K\langle V\rangle$.

Lemma 4.4. *Let $G_1 \subset G$, $K_1 \subset L_1$ be as in Lemma 3.7. Write $\Phi = \Phi_{G_1}$. Then, L_1/K_1 is a (minimal) splitting algebra for a $K_1\#D(G_1)$-module V_1, if and only if $\Phi(L_1)/\Phi(K_1)$ is a (minimal) splitting algebra for the $\Phi(K_1)\#D$-module $\Phi(V_1)$.*

Proof. This easily follows from Proposition 1.4 if one notices that $\Phi(K_1\langle V_1\rangle) = \Phi(K_1)\langle\Phi(V_1)\rangle$, in particular. □

For finitely many elements $u_1, \ldots, u_m$ in L, let $K\langle u_1, \ldots, u_m\rangle$ denote the smallest AS D-module subalgebra in L including K and $u_1, \ldots, u_m$.

Definition 4.5. L/K is said to be *finitely generated* if L is of the form $K\langle u_1, \ldots, u_m\rangle$. This is equivalent to that L_1/K_1 is finitely generated, where $K_1 = K/P \cap K$, $L_1 = L/P$ for an arbitrarily chosen $P \in \Omega(L)$.

Theorem 4.6. *Let $K \subset L$ be as above. Suppose $K^D = L^D$. Then the following are equivalent:*

(a) *L/K is a finitely generated PV extension;*

(b) *L/K is a minimal splitting algebra for a cyclic $K\#D$-module of finite K-rank;*

(c) *L/K is a minimal splitting algebra for a $K\#D$-module of finite K-rank;*

(d) *$L = K\langle x_{ij}\rangle$, where $X = (x_{ij})_{i,j}$ is a GL_n-primitive in Kolchin's sense* [K]*: $X \in GL_n(L)$, and for every $d \in D$, $(dX)X^{-1} \in M_n(K)$ with $dX = (dx_{ij})_{i,j}$.*

Proof. We write $k = K^D$ $(= L^D)$.

(a) $\Rightarrow$ (b). By Lemmas 3.7 and 4.4, we may suppose that K is a field. Suppose that $(L/K, A, H)$ is a finitely generated PV extension. By Proposition 3.13 (iii), we have a finitely generated PV extension $(L_1/K, A_1, \bar{H})$ of module fields over $C := D(G_P)$ with $P \in \Omega(L)$, such that $L = \Phi(L_1)$, $A = \Phi(A_1)$.

There exist those finitely many elements $u_1, \dots, u_m$ in A which span an H-subcomodule over k, and satisfy $L = K\langle u_1, \dots, u_m\rangle$; see [T, p. 501] (but, we do not suppose here the k-linear independence of these elements). Set an element $\boldsymbol{u} = (u_1, \dots, u_m)$ in A^m, and let $V = (K\#D)\boldsymbol{u}$, the cyclic $K\#D$-submodule generated by $\boldsymbol{u}$. Since $L \otimes_K A \simeq L \otimes_k H$, we see that L/K is a minimal splitting algebra for A^m, and hence for V.

It remains to prove that the K-dimension $\dim_K(V)$ is finite. It suffices to prove that the natural image $V(P)$, say, of V under the projection $A^m \to A_1^m$ has a finite K-dimension, since V is naturally embedded into $\prod_{P\in\Omega(L)} V(P)$. Let $g_1, \dots, g_s$ be a system of representatives of the right cosets $G_P\backslash G$. Then we have

$$V = \sum_{i=1}^{s} (K\#C) g_i \boldsymbol{u}.$$

Fix $1 \le i \le s$, and let $\boldsymbol{w} = (w_1, \dots, w_m) \in A_1^m$ denote the natural image of $g_i\boldsymbol{u}$. It suffices to prove that $W := (K\#C)\boldsymbol{w}$ has a finite K-dimension. By re-numbering we have a k-basis, $w_1, \dots, w_r$ $(r \le m)$, of the k-subspace in A_1 spanned by $w_1, \dots, w_m$. There is a rank r matrix T with entries in k, such that $\boldsymbol{w} = \boldsymbol{w}'T$ with $\boldsymbol{w}' = (w_1, \dots, w_r)$. It suffices to prove that $W' := (K\#C)\boldsymbol{w}'$ has a finite K-dimension, since $W' \simeq W$ under the right multiplication by T.

Notice that for any $g \in G$, $gu_1, \dots, gu_m$ span an H-subcomodule in A. It then follows that $w_1, \dots, w_r$ form a k-basis of an $\bar{H}$-subcomodule in A_1. We see from proof of [T, Theorem 3.3, (a) $\Rightarrow$ (b)] that $\dim_K(W')$ is finite, as desired.

(b) $\Rightarrow$ (c). This is trivial.

(c) $\Rightarrow$ (d). This follows in the same way as [T, Theorem 3.3, (c) $\Rightarrow$ (d)]. For later use we follow the outline.

Suppose that L/K is a minimal splitting algebra for V with finite K-free basis $v_1, \dots, v_n$. By Lemma 4.2, we have a k-basis $f_1, \dots, f_n$ in $\mathrm{Hom}_{K\#D}(V, L)$. Define

$$X = (f_j(v_i)), \quad \boldsymbol{v} = {}^t(v_1, \dots, v_n). \tag{17}$$

Then, X is GL_n-primitive, such that

$$(dX)X^{-1}\boldsymbol{v} = d\boldsymbol{v} \quad (d \in D). \tag{18}$$

(d) $\Rightarrow$ (a). Let $X = (x_{ij})$ be GL_n-primitive, and suppose $X^{-1} = (y_{ij})$. As in [T, Example 2.5c], one sees that the K-subalgebra

$$A = K[x_{ij}, y_{ij}] \subset L$$

and the k-subalgebra

$$H = k[z_{ij}, w_{ij}] \subset L \otimes_K L$$

generated by the entries in

$$Z = (z_{ij}) = (X^{-1} \otimes_K 1)(1 \otimes_K X), \quad Z^{-1} = (w_{ij}) = (1 \otimes_K X^{-1})(X \otimes_K 1) \tag{19}$$

make $(L/K, A, H)$ a PV extension. We only need to be careful to see that $\phi : D \to M_n(K)$, $\phi_d = (dX)X^{-1}$ $(d \in D)$ is convolution-invertible since each ϕ_g $(g \in G)$ is; cf. [T, p. 494, line -11]. □

Remark 4.7. Keep the notation just as above.

(i) As is noted in [T, p. 495], one sees from (19) that the natural right H-comodule structure $\theta : A \to A \otimes_k H$ is given by

$$\theta(X) = X \otimes_k Z \; (= (X \otimes_k 1)(1 \otimes_k Z)). \tag{20}$$

It follows that the structure of H is given by

$$\Delta(Z) = Z \otimes_k Z, \quad \varepsilon(Z) = I, \quad S(Z) = Z^{-1}.$$

We have a Hopf algebra surjection,

$$O(\boldsymbol{GL}_n) = k[T_{ij}, \det(T_{ij})^{-1}] \to H, \quad T_{ij} \mapsto z_{ij},$$

which gives a closed embedding $\boldsymbol{G}(L/K) \to \boldsymbol{GL}_n$ of affine k-group schemes; see [T, Example A.3].

(ii) Suppose that $D = R[g, g^{-1}]$ with g grouplike, and K is a field; K is then a difference field [vPS1, Definition 1.1], given an automorphism, say, $\varphi : K \to K$. A difference system $\varphi \boldsymbol{y} = B\boldsymbol{y}$ with $B \in GL_n(K)$ arises uniquely from a $K\#D$-module of K-dimension n, together with its K-basis. We see from (18) that the X in (17) is a fundamental matrix [vPS1, Definition 1.4] for the difference system arising from the V and the $\boldsymbol{v}$ above, and so that A is the PV ring [vPS1, Definition 1.5] for the system. It will follow from Theorems 4.6, 4.11 that if k $(= K^D)$ is algebraically closed, a PV ring for any difference system as above uniquely exists, and is given by such an A as above.

Corollary 4.8. *Let $(L/K, A, H)$ be a PV extension of AS D-module algebras. The following are equivalent:*

(a) *L/K is finitely generated (Definition 4.5);*
(b) *L is the total quotient ring of a finitely generated K-subalgebra in L;*
(c) *A is finitely generated as a K-algebra;*
(d) *H is finitely generated as a k-algebra.*

Proof. When $K \subset L$ are D-module fields, the result is proved in [T, Corollary 3.4 and the following paragraph]. The proof works in our generalized situation. Alternatively, the result easily reduces to the special case above; use Proposition 3.13 (iv) for the reduction of (d). □

Corollary 4.9. *Let $K \subset L$ be an inclusion of AS D-module algebras such that $K^D = L^D$. Then L/K is a PV extension if and only if it is a minimal splitting algebra for such a $K\#D$-module V that is a directed union, $V = \bigcup_\lambda V_\lambda$, of $K\#D$-submodules V_λ of finite K-rank.*

Proof. This follows in the same way as [T, Corollary 3.5], but by using Theorems 3.9 (iii) and 4.6, together with Corollary 4.8. □

Let K be an AS D-module algebra. We have the K^D-abelian symmetric tensor category $({}_{K\#D}\mathcal{M}, \otimes_K, K)$. Let V be an object in ${}_{K\#D}\mathcal{M}$ of finite K-rank. Then the K-linear dual $V^* := \mathrm{Hom}_K(V, K)$ is an dual object under the D-conjugation; see (16). Thus the tensor full subcategory ${}_{K\#D}\mathcal{M}_{\mathrm{fin}}$ consisting of the finite K-rank objects is rigid. Let $\{\{V\}\}$ denote the abelian, rigid tensor full subcategory of ${}_{K\#D}\mathcal{M}$ generated by V, that is, the smallest full subcategory containing V that is closed under subquotients, finite direct sums, tensor products and duals. Thus an object in $\{\{V\}\}$ is precisely a subquotient of some finite direct sum $W_1 \oplus \cdots \oplus W_r$, where each W_i is the tensor product of some copies of V, V^*; see [vPS2, Theorem 2.33] also for comparing with the following.

Theorem 4.10. *Let $(L/K, A, H)$ be a finitely generated PV extension of AS D-module algebras. By Theorem 4.6, we have such a $K\#D$-module V of finite K-rank for which L/K is a minimal splitting algebra.*

(i) *Let $W \in \{\{V\}\}$. Regard the $A \otimes_K W$ as a right H-comodule with the structure induced by A. Then $(A \otimes_K W)^D$ is an H-subcomodule with k-dimension $\mathrm{rk}_K(W)$.*

(ii) *$W \mapsto (A \otimes_K W)^D$ gives a k-linear equivalence*

$$\{\{V\}\} \approx \mathcal{M}^H_{\mathrm{fin}}$$

of symmetric tensor categories, where $\mathcal{M}^H_{\mathrm{fin}} = (\mathcal{M}^H_{\mathrm{fin}}, \otimes_k, k)$ denotes the rigid symmetric tensor category of finite-dimensional right H-comodules; notice that this is isomorphic to the category $\mathrm{Rep}_{\boldsymbol{G}(L/K)}$ of the same kind, consisting of finite-dimensional linear representations of the PV group scheme $\boldsymbol{G}(L/K) = \mathrm{Spec}_k H$.

Proof. Regard naturally A as an algebra in the symmetric tensor category $({}_D\mathcal{M}^H, \otimes_k, k)$ of those D-modules N which has a D-linear, right H-comodule structure $\rho_N : N \to N \otimes_k H$; D acts on N in $N \otimes_k H$. We then have the symmetric tensor category ${}_A({}_D\mathcal{M}^H)$ of A-modules in ${}_D\mathcal{M}^H$, which we denote by $({}_{A\#D}\mathcal{M}^H, \otimes_A, A)$; this is k-abelian. Define k-linear functors

$$\mathcal{M}^H \underset{\Xi_1}{\overset{\Theta_1}{\rightleftarrows}} {}_{A\#D}\mathcal{M}^H \underset{\Xi_2}{\overset{\Theta_2}{\rightleftarrows}} {}_{K\#D}\mathcal{M}$$

by

$$\begin{aligned} \Theta_1(U) &= A \otimes_k U; \quad H \text{ coacts codiagonally}, \\ \Xi_1(N) &= N^D, \\ \Theta_2(N) &= N^{\mathrm{co}H} \quad (= \{n \in N \mid \rho_N(n) = n \otimes_k 1\}), \\ \Xi_2(W) &= A \otimes_K W; \quad H \text{ coacts on } A. \end{aligned}$$

We see that Θ_1 and Ξ_2 are symmetric tensor functors with the obvious tensor structures. Moreover by [Mo, Theorem 8.5.6] (due to Schneider), Θ_2 and Ξ_2 are quasi-inverses of each other, since A/K is H-Galois by Proposition 3.4 (ii). Since $A^D = k$, $\Xi_1 \circ \Theta_1$ is isomorphic to the identity functor. Suppose $N \in {}_{A\#D}\mathcal{M}^H$. Since A is simple by Corollary 3.12 (i), we see from Corollary 3.2 that the natural morphism in ${}_{A\#D}\mathcal{M}^H$

$$\mu_N : \Theta_1 \circ \Xi_1(N) = A \otimes_k N^D \to N$$

is an injection. Let $\mathcal{N}$ denotes the full subcategory of ${}_{A\#D}\mathcal{M}^H$ consisting of those N for which μ_N is an isomorphism. Since each $\Theta_1(U)$ is in $\mathcal{N}$, Θ_1 gives an equivalence

$$\mathcal{M}^H \approx \mathcal{N}.$$

Necessarily, $\mathcal{N}$ is closed under tensor products, and this is an equivalence of symmetric tensor categories.

Since $A \otimes_K V \simeq A^n$ $(n = \mathrm{rk}_K(V))$ in ${}_{A\#D}\mathcal{M}$, $\Xi_2(V) = A \otimes_K V \in \mathcal{N}$. We see that Θ_1 is exact, and $\mathcal{N}$ is closed under subquotients. Therefore for (ii), it suffices to prove that

$$\tilde{V} := \Xi_1 \circ \Xi_2(V) = (A \otimes_K V)^D$$

generates $\mathcal{M}^H_{\mathrm{fin}}$. Let $v_1, \ldots, v_n$ be a K-free basis of V, and define $X, \boldsymbol{v}$ as in (17). We see from (18) that the entries in $\tilde{\boldsymbol{v}} := X^{-1} \otimes_K \boldsymbol{v}$ $(\in (A \otimes_K V)^n)$ are D-invariant, and hence form a k-basis in $\tilde{V}$. By (20), the H-comodule structure $\rho_{\tilde{V}} : \tilde{V} \to \tilde{V} \otimes_k H$ on $\tilde{V}$ is given by

$$\rho_{\tilde{V}}({}^t\tilde{\boldsymbol{v}}) = {}^t\tilde{\boldsymbol{v}} \otimes_k {}^tZ^{-1},$$

where ^{t} denotes the transpose of matrices. This means that the coefficient k-space of $\tilde{V}$ is the subcoalgebra in H spanned by the entries w_{ij} in ${}^tZ^{-1}$. Since w_{ij} together with the entries $S(w_{ij})$ in Z generate the k-algebra H (see the proof of Theorem 4.6 (d) $\Rightarrow$ (a)), $\tilde{V}$ generates $\mathcal{M}^H_{\mathrm{fin}}$; see [W, Theorem 3.5]. This proves Part (ii).

If $W \in \{\{V\}\}$, then $\Xi_2(W) \in \mathcal{N}$, and so

$$\dim_k(A \otimes_K W)^D = \mathrm{rk}_A(A \otimes_K W) = \mathrm{rk}_K(W).$$

This proves Part (i). □

Theorem 4.11. *Let K be an AS D-module algebra such that the field K^D of D-invariants is algebraically closed. Let V be a $K\#D$-module of finite K-rank. Then there exists an AS D-module algebra L including K such that $K^D = L^D$, and L/K is a (necessarily finitely generated) minimal splitting algebra for V. Such an algebra is unique up to D-linear isomorphism of K-algebras.*

To prove this, we need the following:

Lemma 4.12. *Let K be an AS D-module algebra. Let A be a simple D-module algebra, and let $L = Q(A)$ be the total quotient ring of A; by Lemma 2.7, L is uniquely a D-module algebra. If A is finitely generated as a K-algebra, then L^D/K^D is an algebraic extension of fields.*

Proof. We follow Levelt [L, Appendix] for this proof. If $x \in L^D$, then $(A : x) = \{a \in A \mid ax \in A\}$ is a D-stable ideal. Since this contains a non-zero divisor, we have that $(A : x) = A$, and so $A^D = L^D$.

If A is finitely generated, then it is noetherian. By Proposition 2.4, we may suppose that K is a field (and A is a domain). If $P \subset A$ is a maximal ideal, then the field A^D is included in the field A/P, which is algebraic over K. Therefore if $x \in A^D$, it is algebraic over K. Let $\varphi(T) = T^n + c_1T^{n-1} + \cdots + c_n$ denote the minimal polynomial of x over K. Since for any $d \in D$, $\varepsilon(d)T^n + (dc_1)T^{n-1} + \cdots + dc_n$ has x as a root, each $c_i \in K^D$ by the minimality of $\varphi(T)$. Thus x is algebraic over K^D. □

Proof of Theorem 4.11. Existence; this is proved by modifying the proof of [T, Theorem 4.5], as follows. Let $v_1, \dots, v_r$ be a K-basis for V. For $d \in D$, write

$$dv_i = \sum_{s=1}^{r} c_{is}(d)v_s$$

with $c_{is}(d) \in K$. Define a D-module algebra structure on $K[X_{ij}]$, the polynomial K-algebra in r^2 indeterminates, by

$$d(X_{ij}) = \sum_{s=1}^{r} c_{is}(d)X_{sj} \qquad (d \in D).$$

Since $\det(c_{ij}(g))$ is invertible in K for each $g \in G$, the D-module algebra structure of $K[X_{ij}]$ is uniquely extended to $F = K[X_{ij}, \det(X_{ij})^{-1}]$ by Lemma 2.7. Let I be a maximal D-stable ideal of F, and put $A = F/I$. Since K is simple, $I \cap K = 0$. Hence A is a noetherian simple D-module algebra including K. Let L be the total quotient ring of A; this is an AS D-module algebra by Proposition 2.4 and Lemma 2.7. By Lemma 4.12, we have $L^D = K^D$. Let x_{ij} denote the image of X_{ij} in A, and define K-linear maps $f_j : V \to L$ $(j = 1, \dots, r)$ by $f_j(v_i) = x_{ij}$. Then these maps are in $\mathrm{Hom}_{K\#D}(V, L)$, and are linearly independent over L^D, since $(x_{ij})_{i,j} \in GL_r(L)$. Therefore, L/K is a minimal splitting algebra for V by Lemma 4.2 (c).

Uniqueness; this follows by modifying the proof of [T, Theorem 4.6]. □

Acknowledgements

We thank the referee who gave to us helpful comments, informing us of the interesting article [TyW].

References

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

[K] E. R. Kolchin, *"Differential Algebra and Algebraic Groups"*, Pure and Applied Mathematics 54, Academic Press, New York, 1973.

[L] A.H.M. Levelt, *Differential Galois theory and tensor products*, Indag. Mathem., N.S., 1(4) (1990), 439–450.

[MY] A. Masuoka and T. Yanai, *Hopf module duality applied to X-outer Galois theory*, J. Algebra 265 (2003), 229–246.

[Mo] S. Montgomery, *"Hopf Algebras and Their Actions on Rings"*, CBMS Reg. Conf. Series 82, Amer. Math. Soc., Providence, 1993.

[vPS1] M. van der Put and M. F. Singer, *"Galois Theory of Difference Equations"*, Lec. Notes in Math. 1666, Springer, 1997.

[vPS2] M. van der Put and M. F. Singer, *"Galois Theory of Linear Differential Equations"*, Grundlehren Math. Wiss. 328, Springer, 2003.

[Sw] M. Sweedler, *The predual theorem to the Jacobson-Bourbaki theorem*, Trans. Amer. Math. Soc. 213 (1975), 391–406.

[T1] M. Takeuchi, *A correspondence between Hopf ideals and sub-Hopf algebras*, Manuscripta Math. 7 (1972), 251–270.

[T2] M. Takeuchi, *Relative Hopf modules—equivalences and freeness criteria*, J. Algebra 60 (1979), 452–471.

[T] M. Takeuchi, *A Hopf algebraic approach to the Picard-Vessiot theory*, J. Algebra 122 (1989), 481–509.

[TyW] A. Tyc and P. Wiśniewski, *The Lasker-Noether theorem for commutative and noetherian module algebras over a pointed Hopf algebra*, J. Algebra 267 (2003), 58–95.

[W] W. C. Waterhouse, *"Introduction to Affine Group Schemes"*, GTM 66, Springer, 1979.

Institute of Mathematics, University of Tsukuba, Ibaraki 305-8571, Japan
E-mail address: amano@math.tsukuba.ac.jp

Institute of Mathematics, University of Tsukuba, Ibaraki 305-8571, Japan
E-mail address: akira@math.tsukuba.ac.jp