Relative invariants, difference equations, and the Picard-Vessiot theory

Katsutoshi Amano
(Doctoral Program in Mathematics)

Submitted to the Graduate School of
Pure and Applied Sciences
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in
Science
at the
University of Tsukuba

Acknowledgements

First of all I would like to thank my supervisor Professor T. Kimura. He taught me how to learn mathematics from the beginning when I just started afresh my life. About four years ago he suggested to study on archimedean local zeta functions of several variables as my first research task for the Master's thesis. I can not give enough thanks to his heart-warming encouragement all over the period of this program.

I would like to express my thanks to Dr. Fujigami. A large extent of the hard calculations in [1] was due to him. Also he gave me a first opportunity to be interested in diffrence equations.

Professor Kogiso first invited me to join in the study of [1]. I thank him and Professor Sugiyama for being close advisers on prehomogeneous vector spaces.

I also would like to thank Professor M. Takeuchi and Professor A. Masuoka. In June or July 2003, I had a chance to know the existence of the Professor Takeuchi's paper [3] when I was trying to understand [2]. Since I once attended to an introductory part of his lecture on Hopf algebras at 2002 to obtain suitable descriptions of the ring of differntial/difference operators, the paper seemed like just what I wanted. Then I was absorbed in it and came to think that the results can be extended to involve [2]. But I could not have developed it in the presented form without the collaboration with Professor Masuoka. He suggested the viewpoint from relative Hopf modules as is described in Section 3.2, added many interesting results, and helped me to complete several proofs.

Finally I would like to thank my parents for supporting my decision to study mathematics as the lifework.

References

[1] K. Amano, M. Fujigami, T. Kogiso, *Construction of irreducible relative invariant of the prehomogeneous vector space* $(SL_5 \times GL_4, \Lambda^2(\mathbb{C}^5) \otimes \mathbb{C}^4)$, Linear Algebra Appl. 355 (2002), 215–222.

[2] M. van der Put, M. F. Singer, *"Galois theory of difference equations"*, Lecture Notes in Math. 1666, Springer, 1997.

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

This paper is the compilation of the three separate studies. See Introduction of each part.

CONTENTS

Part 1. An equivariant map from $(SL_5 \times GL_4, (\wedge^2\mathbb{C}^5) \otimes \mathbb{C}^4)$ to $(GL_4, \mathrm{Sym}^2(\mathbb{C}^4))$

Introduction of Part 1

The prehomogeneous vector space $(SL_5 \times GL_4, (\wedge^2\mathbb{C}^5) \otimes \mathbb{C}^4)$ of quadruples of quinary alternating forms is known as the classification number (11) in [7, Theorem 54 (I)]. In this part, we construct an equivariant polynomial map from $(SL_5 \times GL_4, (\wedge^2\mathbb{C}^5) \otimes \mathbb{C}^4)$ to the prehomogeneous vector space $(GL_4, \mathrm{Sym}^2(\mathbb{C}^4))$ of quaternary quadratic forms. The presented result was obtained by Kogiso, Fujigami, and the author [1] to get an expression of the irreducible relative invariant of the former space explicitly. Then I heard that the equivariant map had further importance as follows. For a field k in general, the structure of the space $(SL_5 \times GL_4, (\wedge^2 k^5) \otimes k^4)$ has an arithmetic significance by reason of the correspondence between its non-singular orbits and isomorphism classes of separable quintic k-algebras (see [8]). Kable [3, Theorem 5.7] listed all equivariant polynomial maps from this space to any other prehomogeneous vector space and showed those maps could be obtained from two maps; the map presented here is one of the two. Such equivariant maps seem to be used in [4, 5] for arithmetic purposes. (Though we consider the map over $\mathbb{C}$ conventionally, it is defined over $\mathbb{Z}$ by the construction.)

Let Alt_n be the set of all skew-symmetric $n \times n$ complex matrices (i.e. $\mathrm{Alt}_n = \{X \in M_n(\mathbb{C}) \mid {}^tX = -X\}$). One sees that the $\mathbb{C}$-vector space $(\wedge^2\mathbb{C}^5)\otimes\mathbb{C}^4$ is isomorphic to $\mathrm{Alt}_5^{\oplus 4}$. The space $(SL_5 \times GL_4, (\wedge^2\mathbb{C}^5) \otimes \mathbb{C}^4)$ is identified with $(SL_5 \times GL_4, \rho = \Lambda_2 \otimes \Lambda_1, \mathrm{Alt}_5^{\oplus 4})$ in which the representation ρ is defined by

$$\rho(A, B) : (X_1, X_2, X_3, X_4) \longmapsto (AX_1{}^tA, AX_2{}^tA, AX_3{}^tA, AX_4{}^tA)^tB$$

for $(X_1, X_2, X_3, X_4) \in \mathrm{Alt}_5^{\oplus 4}$ and $(A, B) \in SL_5 \times GL_4$. Our construction of the equivariant map is inspired by the method treated in [6, §3], constructing an equivariant map from $(SL_5 \times GL_3, (\wedge^2\mathbb{C}^5) \otimes \mathbb{C}^3)$ to $(GL_3, \mathrm{Sym}^2(\mathbb{C}^3))$. Especially a certain SL_5-equivariant bilinear form $\beta : \mathrm{Alt}_5 \times \mathrm{Alt}_5 \to \mathbb{C}^5$, which is introduced originally in [2], plays an important role. As in [2, 6], we define SL_5-invariant polynomials on $\mathrm{Alt}_5^{\oplus 4}$ by

$$[ijklm](X_1, X_2, X_3, X_4) := {}^t\beta(X_i, X_j)X_k\beta(X_l, X_m)$$

for $X_1, X_2, X_3, X_4 \in \mathrm{Alt}_5$ and $i, j, k, l, m \in \{1, 2, 3, 4\}$. Here each image of β is considered as a column vector. We identify $\mathrm{Sym}^2(\mathbb{C}^4)$ with the space of 4×4 symmetric matrices.

Then the equivariant map $\Phi : \mathrm{Alt}_5^{\oplus 4} \longrightarrow \mathrm{Sym}^2(\mathbb{C}^4)$, $X \mapsto (\varphi_{st}(X))$ will be defined like

$$\varphi_{st} = \sum_{i,j,k,l,m,i',j',k',l',m'} c_{stijklmi'j'k'l'm'}[ijklm][i'j'k'l'm'],$$

where the coefficients $c_{stijklmi'j'k'l'm'}$ are determined suitably.

In §1.1, we define the map β and the polynomials $[ijklm]$, and describe some properties of them which are used to obtain the result. The equivariant map Φ will be defined in §1.2 and we will show the equivariance and the surjectivity of Φ (Proposition 1.2.1 and Theorem 1.2.2).

Notations. For $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \varepsilon \in \mathbb{C}$, let $\mathrm{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and E_ε be the following matrices:

$$\mathrm{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) := \begin{pmatrix} \alpha_1 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 \\ 0 & 0 & \alpha_3 & 0 \\ 0 & 0 & 0 & \alpha_4 \end{pmatrix}, \quad E_\varepsilon := \begin{pmatrix} 1 & \varepsilon & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let $\mathfrak{S}_4$ be the fourth symmetric group. In $\mathfrak{S}_4$, a transposition between i and j is denoted by $(i\ j)$. One sees each permutation $\sigma \in \mathfrak{S}_4$ is considered as the 4×4 matrix such that its (i, j)-element is 1 or 0 with respect to $i = \sigma(j)$ or not. So we may apply for regarding one as the other.

1.1. SL_5-INVARIANT POLYNOMIALS ON $\mathrm{Alt}_5^{\oplus 4}$

In the beginning, we define a certain SL_5-equivariant map $\beta : \mathrm{Alt}_5 \times \mathrm{Alt}_5 \longrightarrow \mathbb{C}^5$ which is used in [2, 6]. Let Pf be the Pfaffian on Alt_4. For $X \in \mathrm{Alt}_5$ and $i = 1, \cdots, 5$, let $X^{(i)}$ denote the matrix in Alt_4 which is obtained by deleting i-th row and i-th column from X. For $X = (x_{ij}), Y = (y_{ij}) \in \mathrm{Alt}_5$, $\beta(X, Y)$ is defined by

$$\begin{aligned}
\beta(X,Y) &:= \begin{pmatrix} \mathrm{Pf}(X^{(1)} + Y^{(1)}) - \mathrm{Pf}(X^{(1)}) - \mathrm{Pf}(Y^{(1)}) \\ -(\mathrm{Pf}(X^{(2)} + Y^{(2)}) - \mathrm{Pf}(X^{(2)}) - \mathrm{Pf}(Y^{(2)})) \\ \mathrm{Pf}(X^{(3)} + Y^{(3)}) - \mathrm{Pf}(X^{(3)}) - \mathrm{Pf}(Y^{(3)}) \\ -(\mathrm{Pf}(X^{(4)} + Y^{(4)}) - \mathrm{Pf}(X^{(4)}) - \mathrm{Pf}(Y^{(4)})) \\ \mathrm{Pf}(X^{(5)} + Y^{(5)}) - \mathrm{Pf}(X^{(5)}) - \mathrm{Pf}(Y^{(5)}) \end{pmatrix} \\
&= \begin{pmatrix} x_{23}y_{45} - x_{24}y_{35} + x_{25}y_{34} + y_{23}x_{45} - y_{24}x_{35} + y_{25}x_{34} \\ x_{34}y_{51} - x_{35}y_{41} + x_{31}y_{45} + y_{34}x_{51} - y_{35}x_{41} + y_{31}x_{45} \\ x_{45}y_{12} - x_{41}y_{52} + x_{42}y_{51} + y_{45}x_{12} - y_{41}x_{52} + y_{42}x_{51} \\ x_{51}y_{23} - x_{52}y_{13} + x_{53}y_{12} + y_{51}x_{23} - y_{52}x_{13} + y_{53}x_{12} \\ x_{12}y_{34} - x_{13}y_{24} + x_{14}y_{23} + x_{12}y_{34} - x_{13}y_{24} + x_{14}y_{23} \end{pmatrix}.
\end{aligned}$$

Then, for $i, j, k, l, m \in \{1, 2, 3, 4\}$, we define a polynomial $[ijklm]$ on $\mathrm{Alt}_5^{\oplus 4}$ by

$$[ijklm](X_1, X_2, X_3, X_4) := {}^t\beta(X_i, X_j)X_k\beta(X_l, X_m)$$

for $X_1, X_2, X_3, X_4 \in \mathrm{Alt}_5$. They are fifth multilinear forms, and satisfy the following lemmas:

Lemma 1.1.1 ([2, §2, Lemma]). *For all $i, j, k, l, m \in \{1, 2, 3, 4\}$, the polynomial $[ijklm]$ is invariant with respect to SL_5, i.e.*

$$[ijklm](AX_1{}^tA, AX_2{}^tA, AX_3{}^tA, AX_4{}^tA) = [ijklm](X_1, X_2, X_3, X_4)$$

for all $A \in SL_5$.

Lemma 1.1.2 ([2, §2, (4)]). *If there are only one or two kinds of numbers among $\{i, j, k, l, m\}$, then $[ijklm] = 0$.*

Lemma 1.1.3 ([6, Lemma 3.1]). *For each $i, j, k, l, m \in \{1, 2, 3, 4\}$,*

$$\begin{array}{ll} \text{(i) } [ijklm] = [jiklm],\ [ijklm] = [ijkml], & \text{(ii) } [ijklm] = -[lmkij], \\ \text{(iii) } [ijklm] + [jkilm] + [kijlm] = 0, & \text{(iv) } [iiklm] = -2[kiilm], \\ \text{(v) } [iikli] = -[iilki] = [iklii] = -[ilkii], & \text{(vi) } [iiilm] = 0,\ [ijkij] = 0. \end{array}$$

Finally in this section, we consider the action of GL_4 on $[ijklm]$. GL_4 is generated by the following three types of matrices: $\mathrm{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, permutation matrices, and E_ε. Thus we only need to think on these types. For $B \in GL_4$ and P a polynomial on $\mathrm{Alt}_5^{\oplus 4}$, let P^B denote the polynomial such that $P^B(X) = P(X{}^tB)$. Diagonal matrices $D = \mathrm{diag}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ and $\sigma \in \mathfrak{S}_4$ act on $[ijklm]$ by

$$\begin{array}{rcl} [ijklm]^D & = & \alpha_i\alpha_j\alpha_k\alpha_l\alpha_m[jiklm], \\ [ijklm]^\sigma & = & [\sigma^{-1}(i)\sigma^{-1}(j)\sigma^{-1}(k)\sigma^{-1}(l)\sigma^{-1}(m)]. \end{array}$$

Since $[ijklm]$ are multilinear forms, we see, for $i, j, k, l, m \in \{2, 3, 4\}$,

$$\begin{array}{rcl} [ijklm]^{E_\varepsilon} & = & [ijklm], \\ [1ijkl]^{E_\varepsilon} & = & [1ijkl] + \varepsilon[2ijkl], \\ [11ijk]^{E_\varepsilon} & = & [11ijk] + 2\varepsilon[12ijk] + \varepsilon^2[22ijk], \\ [11ij1]^{E_\varepsilon} & = & [11ij1] + \varepsilon(2[12ij1] + [11ij2]) \\ & & +\varepsilon^2(2[12ij2] + [22ij1]) + \varepsilon^3[22ij2], \text{ etc.} \end{array}$$

1.2. Construction of the equivariant map

Our first objective is to define a map $\Phi : \mathrm{Alt}_5^{\oplus 4} \to \mathrm{Sym}^2(\mathbb{C}^4)$, $X \mapsto (\varphi_{st}(X))$, where each φ_{st} is written like

$$\varphi_{st} = \sum c_{stijklmi'j'k'l'm'}[ijklm][i'j'k'l'm'].$$

Then we will show the following lemma.

Proposition 1.2.1. *For $X \in \mathrm{Alt}_5^{\oplus 4}$ and $(A,B) \in SL_5 \times GL_4$,*

$$\Phi(\rho(A,B)X) = (\det B)^2 B\Phi(X)\,{}^tB.$$

First we observe that Φ should be determined uniquely from φ_{11} and φ_{12}, so that $\Phi(X)$ is equivariant with respect to the action of $\mathfrak{S}_4$:

$$(1.1) \qquad \varphi_{ss} = \varphi_{11}^{(1\ s)} \quad (s = 1, \ldots, 4), \qquad \varphi_{\sigma^{-1}(1)\sigma^{-1}(2)} = \varphi_{12}^{\sigma} \quad (\sigma \in \mathfrak{S}_4).$$

Furthermore, φ_{12} should also be determined from φ_{11}. To obtain $\Phi(\rho(A, E_\varepsilon)X) = E_\varepsilon \Phi(X)\,{}^tE_\varepsilon$ $(A \in SL_5)$, the polynomials φ_{st} should satisfy at least the following:

$$\begin{aligned}
&(1.2) & \varphi_{11}^{E_\varepsilon} &= \varphi_{11} + 2\varepsilon\varphi_{12} + \varepsilon^2\varphi_{22}, \\
&(1.3) & \varphi_{22}^{E_\varepsilon} &= \varphi_{22}, \\
&(1.4) & \varphi_{33}^{E_\varepsilon} &= \varphi_{33}, \\
&(1.5) & \varphi_{13}^{E_\varepsilon} &= \varphi_{13} + \varepsilon\varphi_{23}, \\
&(1.6) & \varphi_{34}^{E_\varepsilon} &= \varphi_{34}.
\end{aligned}$$

If we obtain φ_{11}, then $\varphi_{22} = \varphi_{11}^{(1\ 2)}$ and φ_{12} will be determined from (1.2).

Considering the action of diagonal matrices for $\Phi(X)$, we start by assuming that each term $[ijklm][i'j'k'l'm']$ in φ_{11} is constructed by the following numbers:

$$\{i, j, k, l, m, i', j', k', l', m'\} = \{1, 1, 1, 1, 2, 2, 3, 3, 4, 4\}.$$

But from Lemma 1.1.2 and Lemma 1.1.3, we need not to think on the all combinations of the above numbers. By choosing combinations and using the method of indeterminate coefficients, it is possible to determine the polynomial φ_{11} so that the equations from (1.2) to (1.6) are satisfied. Indeed, we conclude that the following definitions are suitable:

$$\begin{aligned}
\varphi_{11} \ := \ & 160[31114](3[24132] - 2[21342] - 2[23412]) \\
& +160[41112](3[32143] - 2[34213] - 2[31423]) \\
& +160[21113](3[43124] - 2[41234] - 2[42314]) \\
& +50([11233][11244] + [11322][11344] + [11422][11433]) \\
& -288([13241]^2 + [14321]^2 + [12431]^2) \\
& +224([13241][14321] + [14321][12431] + [12431][13241]),
\end{aligned}$$

$$\begin{aligned}
\varphi_{12} \;:=\; & 400[31114][32224] \\
& -100([21113][22344]+[21114][22433]) \\
& -100([12223][11344]+[12224][11433]) \\
& +20[11422](4[31423]-[34213]-[32143]) \\
& +20[11322](4[41324]-[43214]-[42134]) \\
& -25([22144][11233]+[11244][22133]) \\
& +368[13241][23142] \\
& +112([13241]([21342]+[23412])+[23142]([12341]+[13421])) \\
& +192([14321][23412]+[13421][24312]) \\
& -208([14321][21342]+[12431][23412]).
\end{aligned}$$

These polynomials satisfy the following properties:

(i) If $\sigma \in \mathfrak{S}_4$ and $\sigma(1)=1$, then $\varphi_{11}^{\sigma}=\varphi_{11}$,

(ii) If $\sigma \in \mathfrak{S}_4$ and $\{\sigma(1),\sigma(2)\}=\{1,2\}$, then $\varphi_{12}^{\sigma}=\varphi_{12}$.

Then we define the map $\Phi : \mathrm{Alt}_5^{\oplus 4} \to \mathrm{Sym}^2(\mathbb{C}^4)$, $X \mapsto (\varphi_{st}(X))$ so that (1.1) is satisfied; the well-definedness follows from (i), (ii). It is easily seen that $\varphi_{st}=\varphi_{ts}$ and $\varphi_{st}^{\sigma}=\varphi_{\sigma^{-1}(s)\sigma^{-1}(t)}$ for all $\sigma \in \mathfrak{S}_4$.

Proof of Proposition 1.2.1. Let $D=\mathrm{diag}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$ and let A be an arbitrary element of SL_5. Since $\varphi_{st}^{D}=(\alpha_1\alpha_2\alpha_3\alpha_4)^2\alpha_s\alpha_t\varphi_{st}$ for all $s,t\in\{1,2,3,4\}$, and each φ_{st} is invariant with respect to SL_5, we have

$$\Phi(\rho(A,D)X)=(\det D)^2 D\Phi(X)\,{}^tD.$$

By the definition, it follows

$$\Phi(\rho(A,\sigma)X)=(\varphi_{\sigma^{-1}(s)\sigma^{-1}(t)}(X))=\sigma\Phi(X)\,{}^t\sigma$$

for all $\sigma \in \mathfrak{S}_4$.

The rest of the proof is to show $\Phi(\rho(A,E_\varepsilon)X)=E_\varepsilon\Phi(X)\,{}^tE_\varepsilon$, i.e.

- $\varphi_{11}^{E_\varepsilon}=\varphi_{11}+2\varepsilon\varphi_{12}+\varepsilon^2\varphi_{22}$,
- $\varphi_{1t}^{E_\varepsilon}=\varphi_{t1}^{E_\varepsilon}=\varphi_{1t}+\varepsilon\varphi_{2t}$ for $t=2,3,4$,
- $\varphi_{st}^{E_\varepsilon}=\varphi_{ts}^{E_\varepsilon}=\varphi_{st}$ for $s,t=2,3,4$.

Recall that we defined φ_{st} to satisfy the equations from (1.2) to (1.6) (in fact, they are shown directly). By $E_\varepsilon^2 = E_{2\varepsilon}$ and (1.2), we have

$$\varphi_{11}^{E_\varepsilon^2} = \varphi_{11} + 4\varepsilon\varphi_{12} + 4\varepsilon^2\varphi_{22}.$$

On the other hand, by (1.2) and (1.3),

$$\begin{aligned} \varphi_{11}^{E_\varepsilon^2} &= (\varphi_{11} + 2\varepsilon\varphi_{12} + \varepsilon^2\varphi_{22})^{E_\varepsilon} \\ &= \varphi_{11}^{E_\varepsilon} + 2\varepsilon\varphi_{12}^{E_\varepsilon} + \varepsilon^2\varphi_{22}^{E_\varepsilon} \\ &= \varphi_{11} + 2\varepsilon\varphi_{12} + 2\varepsilon\varphi_{12}^{E_\varepsilon} + 2\varepsilon^2\varphi_{22}. \end{aligned}$$

Therefore $\varphi_{12}^{E_\varepsilon} = \varphi_{12} + \varepsilon\varphi_{22}$. Similarly by (1.5),

$$\begin{aligned} \varphi_{13}^{E_\varepsilon^2} &= \varphi_{13} + 2\varepsilon\varphi_{23} \\ &= \varphi_{13} + \varepsilon\varphi_{23} + \varepsilon\varphi_{23}^{E_\varepsilon}. \end{aligned}$$

Hence $\varphi_{23}^{E_\varepsilon} = \varphi_{23}$. By (1.5) and $E_\varepsilon(3\ 4) = (3\ 4)E_\varepsilon$, we have

$$\varphi_{14}^{E_\varepsilon} = \varphi_{13}^{(3\ 4)E_\varepsilon} = \varphi_{13}^{E_\varepsilon(3\ 4)} = (\varphi_{13}^{E_\varepsilon})^{(3\ 4)} = \varphi_{14} + \varepsilon\varphi_{24}.$$

Similarly by (1.4), we have

$$\varphi_{44}^{E_\varepsilon} = \varphi_{33}^{E_\varepsilon(3\ 4)} = \varphi_{33}^{(3\ 4)} = \varphi_{44}.$$

Now the proof is completed. $\square$

To prove that Φ is surjective, we only need to find five points in $\mathrm{Alt}_5^{\oplus 4}$ such that each image has rank $0, 1, 2, 3, 4$. For

$$X_{01} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad X_{02} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix},$$

$$X_{03} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \end{pmatrix}, \quad X_{04} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \end{pmatrix},$$

$$Y_{01} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad Y_{02} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix},$$

$$Y_{03} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \end{pmatrix},$$

we have

$$\begin{aligned}
\Phi(X_{01}, X_{02}, X_{03}, X_{04}) &= \begin{pmatrix} 0 & 0 & -720 & 0 \\ 0 & -480 & 0 & 0 \\ -720 & 0 & 0 & 0 \\ 0 & 0 & 0 & -288 \end{pmatrix} \quad \text{(rank 4)}, \\
\Phi(Y_{01}, X_{02}, X_{03}, X_{04}) &= \begin{pmatrix} -192 & 0 & -192 & -96 \\ 0 & -480 & 0 & 0 \\ -192 & 0 & -192 & -96 \\ -96 & 0 & -96 & -288 \end{pmatrix} \quad \text{(rank 3)}, \\
\Phi(Y_{01}, Y_{02}, X_{03}, X_{04}) &= \begin{pmatrix} -192 & 0 & -192 & -96 \\ 0 & 0 & 0 & 0 \\ -192 & 0 & -192 & -96 \\ -96 & 0 & -96 & -288 \end{pmatrix} \quad \text{(rank 2)}, \\
\Phi(Y_{01}, Y_{02}, Y_{03}, X_{04}) &= \begin{pmatrix} -192 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{(rank 1)}, \\
\Phi(0,0,0,0) &= 0 \quad \text{(rank 0)}.
\end{aligned}$$

Therefore Φ is surjective and especially $\det \Phi(X) \neq 0$. This fact and Proposition 1.2.1 implies that $\det \Phi(X)$ is the relative invariant in degree 40.

Theorem 1.2.2. (i) *The map* $\Phi : \mathrm{Alt}_5^{\oplus 4} \to \mathrm{Sym}^2(\mathbb{C}^4)$ *is surjective.*

(ii) $f(X) = \det \Phi(X)$ *is the irreducible relative invariant of the prehomogeneous vector space* $(SL_5 \times GL_4, \Lambda_2 \otimes \Lambda_1, \mathrm{Alt}_5^{\oplus 4})$ *in degree* 40 *corresponding to the rational character* $(\det B)^4$.

References

[1] K. Amano, M. Fujigami, T. Kogiso, *Construction of irreducible relative invariant of the prehomogeneous vector space* $(SL_5 \times GL_4, \Lambda^2(\mathbb{C}^5) \otimes \mathbb{C}^4)$, Linear Algebra Appl. 355 (2002), 215–222.

[2] A. Gyoja, *Construction of invariants*, Tsukuba J. Math. 14 (1990), 437–457.

[3] A.C. Kable, *The concomitants of a prehomogeneous vector space*, J. Algebra 271 (2004), 295–311.

[4] A.C. Kable, A. Yukie, *On the space of quadruples of quinary alternating forms*, J. Pure Appl. Algebra 186 (2004), 277–295.

[5] A.C. Kable, A. Yukie, *A construction of quintic rings*, Nagoya Math. J. 173 (2004), 163–203.

[6] H. Ochiai, *Quotients of some prehomogeneous vector spaces*, J. Algebra 192 (1997), 61–73.

[7] M. Sato, T. Kimura, *A classification of irreducible prehomogeneous vector spaces and their relative invariants*, Nagoya Math. J. 65 (1977), 1–155.

[8] D.J. Wright, A. Yukie, *Prehomogeneous vector spaces and field extensions*, Invent. math. 110 (1992), 283–314.

Part 2. Archimedean local zeta functions which satisfy $\mathbf{G}_{\mathrm{m}}$-primitive difference equations

Introduction of Part 2

Let K be the complex number field $\mathbb{C}$ or the real number field $\mathbb{R}$, (G, ρ, V) a reductive prehomogeneous vector space defined over K, and V_K the set of K-rational points of V. Let $P_1(x), \cdots, P_r(x)$ be the basic relative invariants of (G, ρ, V) over K. For a Schwartz function $\Phi(x)$ on V_K and $s = (s_1, \cdots, s_r) \in \mathbb{C}^r$, the integral

$$Z_K(s, \Phi) = \int_{V_K} \prod_{i=1}^{r} |P_i(x)|_K^{s_i} \Phi(x) dx$$

is called the *archimedean local zeta function* associated with (G, ρ, V). When we take $\Phi(x)$ as

$$\Phi(x) = \begin{cases} \exp(-2\pi\, x^t\bar{x}) & (K = \mathbb{C}) \\ \exp(-\pi\, x^t x) & (K = \mathbb{R}), \end{cases}$$

$Z_K(s, \Phi)$ will be denoted by $Z_K(s)$ simply.

In the case $r = 1$, Igusa suggested in [7, §3, Remark] and proved in [8, Chapter 6] the following theorem:

Theorem (Igusa). *Let P be the basic relative invariant of (G, ρ, V), assuming $r = 1$. Let $d = \deg P$ and $b(s) = c\prod_{j=1}^{d}(s + \alpha_j)$ the b-function of $P(x)$.*

(1) *When $K = \mathbb{C}$,*

$$Z_{\mathbb{C}}(s) = ((2\pi)^{-d}c)^s \prod_{j=1}^{d} \frac{\Gamma(s + \alpha_j)}{\Gamma(\alpha_j)}.$$

(2) *When $K = \mathbb{R}$ and when every term of $P(x)$ is a multilinear form,*

$$Z_{\mathbb{R}}(s) = (\pi^{-d}c)^{\frac{s}{2}} \prod_{j=1}^{d} \frac{\Gamma((s + \alpha_j)/2)}{\Gamma(\alpha_j/2)}.$$

In this part, we extend this theorem to several variables ($r \geq 1$). Though basically our proof presented here is an easy modification of the proof given in [8], a careful treatment of the Ore-Sato theorem (see Section 2.1) is needed. The most important point of the proof is the fact that $Z_{\mathbb{C}}(s)$ and $Z_{\mathbb{R}}(2s)$ satisfies a difference equation in a certain type, called *hypergeometric* (or $\mathbf{G}_{\mathrm{m}}$*-primitive*) which is written by the b-functions. The proof can be divided into two steps. The first step is to characterize a desired solution of such a difference equation, written as a product of an exponential function and gamma functions.

The next step is to prove that the characterization can be adapted to $Z_{\mathbb{C}}(s)$ and $Z_{\mathbb{R}}(2s)$. To obtain a suitable difference equation (especially for $Z_{\mathbb{R}}(2s)$), very delicate facts which are seen in the proof of the Ore-Sato theorem are needed. For this reason, we include a detailed proof of the theorem in Section 2.1. The main results will be described in Section 2.3, 2.4 (Theorem 2.3.1 and Theorem 2.4.3).

2.1. The Ore-Sato theorem

Let k be a field of zero characteristic and $k(s) = k(s_1, \ldots, s_r)$ the rational function field of r variables. Let Ξ be the free abelian group of rank r ($\Xi \simeq \mathbb{Z}^r$) and $\tau_1, \ldots, \tau_r$ a basis of Ξ. Then Ξ acts on $k(s)$ as k-algebra automorphisms by $\tau_i f(s) = f(s + e_i)$ ($f(s) \in k(s)$) where $e_1 = (1, 0, \ldots, 0), \ldots, e_r = (0, \ldots, 0, 1)$, the canonical basis of k^r. Consider the group algebra $k\Xi$ as a Hopf algebra in the usual sense, $k(s)$ a $k\Xi$-module algebra, and $k(s)\#k\Xi$ the smash product; i.e. $k(s)\#k\Xi$ is $k(s) \otimes_k k\Xi$ with the semi-direct product: $(f_1 \otimes g) \cdot (f_2 \otimes h) = f_1(gf_2) \otimes gh$ ($g, h \in \Xi$). We say that a $k(s)\#k\Xi$-module V is $\mathbf{G}_{\mathrm{m}}$*-primitive*, or *hypergeometric*, iff $\dim_{k(s)} V = 1$. (We will see in Part 3 that the Picard-Vessiot group scheme of such a $k(s)\#k\Xi$-module is a closed subgroup scheme of $\mathbf{G}_{\mathrm{m}}$.) Let $k(s)^\times = k(s) \backslash \{0\}$. For a fixed $k(s)$-basis v of a $\mathbf{G}_{\mathrm{m}}$-primitive $k(s)\#k\Xi$-module V, we have an associated map $b_v : \Xi \to k(s)^\times$, $g \mapsto b_{g,v}(s)$ defined by $gv = b_{g,v}(s)v$. Since $b_{1,v}(s) = 1$ and $b_{gh,v}(s) = (gb_{h,v}(s))b_{g,v}(s)$ for all $g, h \in \Xi$, b_v is in the set $Z^1(\Xi; k(s)^\times)$ of 1-cocycles. Let v' be another $k(s)$-basis of V. Then there exists an $f \in k(s)^\times$ such that $v' = f(s)v$. It follows $b_{g,v'}(s) = (gf(s))f(s)^{-1}b_{g,v}(s)$ for all $g \in \Xi$; this implies that both of $b_{v'}$ and b_v define the same cohomology class in $H^1(\Xi; k(s)^\times)$ since the map $g \mapsto (gf(s))f(s)^{-1}$ is in the set $B^1(\Xi; k(s)^\times)$ of 1-coboundaries. Thus $\mathbf{G}_{\mathrm{m}}$-primitive $k(s)\#k\Xi$-modules are classified by $H^1(\Xi; k(s)^\times)$.

An explicit description of $Z^1(\Xi; k(s)^\times)$ is given by a result called *the Ore-Sato theorem*, which was first obtained by Ore [13] for the case $r = 2$ and by Sato [16] for arbitrary r. Detailed proofs are also seen in [11, §1.1] and [5, §1]. The purpose of this section is to introduce the theorem for later use. Since some delicate facts such as Corollary 2.1.4 are important to us, we follow carefully the discussion given in [16, Appendix]. (Thus our statement of the theorem may be verbose according to the interest of the reader. For a more elegant description of $H^1(\Xi; \mathbb{C}(s)^\times)$, [11, Proposition 1.1.4] is recommended. See Remark 2.1.5.)

$k(s)^\times$ has a natural $\mathbb{Z}\Xi$-module structure as follows:

$$\left(\sum_i n_i g_i\right) f(s) = \prod_i (g_i f(s))^{n_i} \qquad (n_i \in \mathbb{Z}, \quad g_i \in \Xi).$$

We easily see $k(s)^\times \simeq k^\times \times k(s)^\times/k^\times$ as $\mathbb{Z}\Xi$-modules. Moreover, by decomposing to irreducible polynomials, it follows that $k(s)^\times/k^\times$ is a free $\mathbb{Z}\Xi$-module. We have the following $\mathbb{Z}\Xi$-module isomorphisms:

$$k(s)^\times \xrightarrow{\sim} k^\times \oplus \bigoplus_f \mathbb{Z}\Xi f \xrightarrow{\sim} k^\times \oplus \bigoplus_f \mathbb{Z}(\Xi/\Xi_f),$$

where f runs over a $\mathbb{Z}\Xi$-basis of $k(s)^\times/k^\times$ and $\Xi_f := \{g \in \Xi \mid gf = f\}$. We observe that we can take such a $\mathbb{Z}\Xi$-basis that each f is the image of an irreducible polynomial.

Since Ξ is a finitely generated group, we have

$$Z^1(\Xi; k(s)^\times) \simeq Z^1(\Xi; k^\times) \oplus \bigoplus_f Z^1(\Xi; \mathbb{Z}(\Xi/\Xi_f)).$$

One sees that $Z^1(\Xi; k^\times)$ is equal to the character group $\mathrm{Hom}(\Xi, k^\times)$. The structure of each $Z^1(\Xi; \mathbb{Z}(\Xi/\Xi_f))$ is described by the following two lemmas.

Lemma 2.1.1. *Let f be an irreducible polynomial in $k[s] = k[s_1, \ldots, s_r]$. Then $\Xi_f := \{g \in \Xi \mid gf = (\text{const.})f\} = \{g \in \Xi \mid gf = f\}$.*

(i) *Ξ/Ξ_f is a free abelian group of $\operatorname{rank} \Xi/\Xi_f > 0$.*

(ii) *Take an arbitrary $\alpha \in Z^1(\Xi; \mathbb{Z}(\Xi/\Xi_f))$. Then $\alpha(g) = 0$ for all $g \in \Xi_f$.*

(iii) *If $\operatorname{rank} \Xi/\Xi_f \geq 2$, then $H^1(\Xi; \mathbb{Z}(\Xi/\Xi_f)) = 0$.*

Proof. (i) Since f is not a constant, $\Xi_f \neq \Xi$. Suppose $g \in \Xi$ and $g^n \in \Xi_f$ for some positive integer n. There is an $m \in \mathbb{Z}^r$ such that $gf(s) = f(s+m)$. Consider $P(t) := f(s+tnm) - f(s)$ as a polynomial in $k(s)[t]$. Since $P(l) = g^{ln}f(s) - f(s) = 0$ for all $l \in \mathbb{Z}$ and since $k(s)$ is an infinite field, we have $P \equiv 0$. Hence $0 = P(1/n) = gf(s) - f(s)$, and so $g \in \Xi_f$.

(ii) Take a $g' \in \Xi$ which is not in Ξ_f. Let $\tilde{g}'$ be the image of g' in Ξ/Ξ_f. Then for all $g \in \Xi_f$, we have

$$\alpha(gg') = \alpha(g') + \alpha(g) = \tilde{g}'\alpha(g) + \alpha(g').$$

Thus $(\tilde{g}' - 1)\alpha(g) = 0$. Since $\mathbb{Z}(\Xi/\Xi_f)$ is an integral domain by part (i), we have $\alpha(g) = 0$.

(iii) By part (ii), we have $H^1(\Xi; \mathbb{Z}(\Xi/\Xi_f)) \simeq H^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f))$. Let $\lambda_1, \ldots, \lambda_l$ be a basis of Ξ/Ξ_f. For all $\alpha \in Z^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f))$, we have

$$\alpha(\lambda_i\lambda_j) = \lambda_i\alpha(\lambda_j) + \alpha(\lambda_i) = \lambda_j\alpha(\lambda_i) + \alpha(\lambda_j)$$

and hence $(\lambda_i - 1)\alpha(\lambda_j) = (\lambda_j - 1)\alpha(\lambda_i)$ for $i, j = 1, \ldots, l$. Since $\mathbb{Z}(\Xi/\Xi_f)$ is the Laurent polynomial ring, there exists an $a \in \mathbb{Z}(\Xi/\Xi_f)$ such that

$$\alpha(\lambda_i) = (\lambda_i - 1)a \qquad (i = 1, \ldots, l).$$

Moreover, since

$$0 = \alpha(1) = \alpha(\lambda_i^{-1}\lambda_i) = \lambda_i^{-1}\alpha(\lambda_i) + \alpha(\lambda_i^{-1}) = (1 - \lambda_i^{-1})a + \alpha(\lambda_i^{-1}),$$

we have $\alpha(\lambda_i^{-1}) = (\lambda_i^{-1} - 1)a$. Therefore

$$\alpha(g) = ga - a \quad (g \in \Xi/\Xi_f),$$

concluding $\alpha \in B^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f))$, follows by induction. Indeed, if $\alpha(g') = g'a - a$ for a $g' \in \Xi/\Xi_f$, then

$$\begin{aligned} \alpha(\lambda_i g') &= \lambda_i(g'a - a) + (\lambda_i - 1)a = \lambda_i g'a - a, \\ \alpha(\lambda_i^{-1} g') &= \lambda_i^{-1}(g'a - a) + (\lambda_i^{-1} - 1)a = \lambda_i^{-1} g'a - a \end{aligned}$$

for $i = 1, \ldots, l$. □

Lemma 2.1.2. *Let f be an irreducible polynomial in $k[s]$. Suppose that* $\operatorname{rank}\Xi/\Xi_f = 1$ *and let λ be a basis of Ξ/Ξ_f.*

(i) *There exist a linear form $\mu(s) = n_1 s_1 + \cdots + n_r s_r$ ($n_1, \ldots, n_r \in \mathbb{Z}$) and an irreducible polynomial $h(t) \in k[t]$ of one variable t, such that $f(s) = h(\mu(s))$ and $\lambda f(s) = h(\mu(s)+1)$. Moreover, there exists an $m \in \mathbb{Z}^r$ such that $\mu(m) = 1$, i.e. the greatest common divisor of non-zero coefficients of μ is* 1.

(ii) *For every $\alpha \in Z^1(\Xi; \mathbb{Z}(\Xi/\Xi_f))$, there is an $\eta \in \mathbb{Z}(\Xi/\Xi_f)$ such that*

$$\alpha(\tau_1^{m_1} \cdots \tau_r^{m_r}) = \begin{cases} \eta \displaystyle\sum_{\nu=0}^{\mu(m)-1} \lambda^\nu & (\mu(m) \geq 1), \\ 0 & (\mu(m) = 0), \\ -\eta \displaystyle\sum_{\nu=\mu(m)}^{-1} \lambda^\nu & (\mu(m) \leq -1), \end{cases}$$

for all $m = (m_1, \ldots, m_r) \in \mathbb{Z}^r$.

(iii) $H^1(\Xi; \mathbb{Z}(\Xi/\Xi_f)) \simeq \mathbb{Z}$.

Proof. (i) Let $\lambda_1, \ldots, \lambda_r$ be a basis of Ξ such that the image of λ_1 in Ξ/Ξ_f is λ and $\lambda_2, \ldots, \lambda_r \in \Xi_f$. Then there exists an invertible $r \times r$ matrix $(n_{ij})_{i,j}$ in $GL_r(\mathbb{Z})$ such that $\tau_i = \lambda_1^{n_{i1}} \cdots \lambda_r^{n_{ir}}$ for $i = 1, \ldots, r$. Put $\mu(s) := n_{11}s_1 + \cdots + n_{r1}s_r$ and take linear forms $s_1'(= \mu(s)), \ldots, s_r'$ by $(s_1', \ldots, s_r') = (s_1, \ldots, s_r)(n_{ij})_{i,j}$. Then we have $\lambda_j s_i' = s_i' + \delta_{ij}$, where

δ_{ij} denotes the Kronecker's delta. There exists an irreducible polynomial $h(t_1, \ldots, t_r) \in k[t_1, \ldots, t_r]$ such that $f(s) = h(s'_1, \ldots, s'_r)$. But

$$h(s'_1, s'_2 + m_2, \ldots, s'_r + m_r) = \lambda_2^{m_2} \cdots \lambda_r^{m_r} f(s) = f(s) = h(s'_1, \ldots, s'_r)$$

for all $m_2, \ldots, m_r \in \mathbb{Z}$, since $\lambda_2, \ldots, \lambda_r \in \Xi_f$. Thus it follows that h is actually a polynomial of one variable t_1. The second part obviously follows by the definition of μ.

(ii) By part (ii) of Lemma 2.1.1, we have $Z^1(\Xi; \mathbb{Z}(\Xi/\Xi_f)) \simeq Z^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f))$. For an arbitrary $\alpha \in Z^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f))$, set $\eta = \alpha(\lambda)$. Then the assertion follows by induction on $\mu(m)$, since the image of $\tau_1^{m_1} \cdots \tau_r^{m_r}$ in Ξ/Ξ_f is $\lambda^{\mu(m)}$.

(iii) We see that $Z^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f)) \to \mathbb{Z}(\Xi/\Xi_f)$, $\alpha \mapsto \alpha(\lambda)$ is a $\mathbb{Z}\Xi$-linear isomorphism. Then $B^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f))$ is isomorphic to $\mathbb{Z}(\Xi/\Xi_f)^+ = \mathbb{Z}(\Xi/\Xi_f)(\lambda - 1)$, the augmentation ideal, under this isomorphism. Hence $H^1(\Xi/\Xi_f; \mathbb{Z}(\Xi/\Xi_f)) \simeq \mathbb{Z}(\Xi/\Xi_f)/\mathbb{Z}(\Xi/\Xi_f)^+ \simeq \mathbb{Z}$; the last isomorphism is induced by the counit $\varepsilon : \mathbb{Z}(\Xi/\Xi_f) \to \mathbb{Z}$, $\sum_i z_i \lambda^i \mapsto \sum_i z_i$. $\square$

By translating the lemmas above, we have the following theorem.

Theorem 2.1.3 (Ore-Sato). *Let $\Xi \to k(s)^\times$, $g \mapsto b_g(s)$ be a 1-cocycle in $Z^1(\Xi; k(s)^\times)$. Write $\tau^m = \tau_1^{m_1} \cdots \tau_r^{m_r}$ for $m = (m_1, \ldots, m_r) \in \mathbb{Z}^r$. Then b is written as the following form:*

$$(2.1) \qquad b_{\tau^m}(s) = c(\tau^m) \prod_{j=1}^{N} \zeta_j \frac{f_j(s+m)}{f_j(s)} \prod_{i=1}^{l} \eta_i \cdot \begin{cases} \displaystyle\prod_{\nu=0}^{\mu_i(m)-1} h_i(\mu_i(s)+\nu) & (\mu_i(m) \geq 1) \\ 1 & (\mu_i(m) = 0) \\ \displaystyle\prod_{\nu=\mu_i(m)}^{-1} \frac{1}{h_i(\mu_i(s)+\nu)} & (\mu_i(m) \leq -1) \end{cases}$$

for all $m \in \mathbb{Z}^r$. Here, $c : \Xi \to k^\times$ is a character, $h_1, \ldots, h_l \in k[t]$ are irreducible polynomials of one variable, $\mu_1, \ldots, \mu_l \in \mathbb{Z}s_1 + \cdots + \mathbb{Z}s_r$ are non-zero linear forms whose each greatest common divisor of non-zero coefficients is 1, $\eta_i \in \mathbb{Z}(\Xi/\Xi_{\mu_i(s)})$ $(i = 1, \ldots, l)$, $f_1, \ldots, f_N$ are irreducible polynomials in $k[s]$ which satisfy that $\operatorname{rank} \Xi/\Xi_{f_j} > 1$ $(j = 1, \ldots, N)$ and $f_1(s), \ldots, f_N(s), h_1(\mu_1(s)), \ldots, h_l(\mu_l(s))$ are $\mathbb{Z}\Xi$-linearly independent, and $\zeta_j \in \mathbb{Z}(\Xi/\Xi_{f_j})$ $(j = 1, \ldots, N)$.

Let $\varepsilon : \mathbb{Z}(\Xi/\Xi_{\mu_i(s)}) \to \mathbb{Z}$ denote the counit (see the last sentence in the proof of Lemma 2.1.2). We normalize each η_i, μ_i, h_i in (2.1) so that $\varepsilon(\eta_i) > 0$ $(i = 1, \ldots, l)$ (when $\varepsilon(\eta_i) < 0$, replace $\eta_i, \mu_i, h_i(t)$ with $-\eta_i, -\mu_i, h_i(-t-1)$). Put $f(s) = \prod_{j=1}^{N} \zeta_j f_j(s)$.

Corollary 2.1.4. *In Theorem 2.1.3, assume $b_{\tau_1}(s), \dots, b_{\tau_r}(s)$ are polynomials. Take the expression (2.1) with $f(s) = 1$ (which necessarily holds) and η_i, μ_i, h_i normalized as above. Then they satisfy the following conditions* (1), (2).

(1) *All coefficients of each μ_i are non-negative integers.*

(2) *For each $i = 1, \dots, l$, let λ_i be the basis of $\Xi/\Xi_{\mu_i(s)}$ such that $\lambda_i \mu_i(s) = \mu_i(s) + 1$. Write $\eta_i = \sum_{j=n}^{n'} z_{ij} \lambda_i^j$ ($z_{ij} \in \mathbb{Z}$, $z_{in}, z_{in'} \neq 0$). Then $h_i(\mu_i(s) + n)^{z_{in}}$ and $h_i(\mu_i(s) + n' + \mu_i(m) - 1)^{z_{in'}}$ are not cancelled in the product $\prod_{j=n}^{n'} \prod_{\nu=0}^{\mu_i(m)-1} h_i(\mu_i(s) + j + \nu)^{z_{ij}}$ ($0 \neq m \in \mathbb{Z}_{\geq 0}^r$). Hence z_{in} and $z_{in'}$ are positive integers.*

Proof. (1) Necessarily $\mu_i(e_1)\varepsilon(\eta_i), \dots, \mu_i(e_r)\varepsilon(\eta_i)$ are non-negative integers for $i = 1, \dots, l$ by the assumption.

(2) This is easily seen. □

Remark 2.1.5. (i) The 1-cocycle given by (2.1) and the following one both define the same cohomology class in $H^1(\Xi; k(s)^\times)$:

$$\tau^m \mapsto c(\tau^m) \prod_{i=1}^{l} \begin{cases} \displaystyle\prod_{\nu=0}^{\mu_i(m)-1} h_i(\mu_i(s) + \nu)^{\varepsilon(\eta_i)} & (\mu_i(m) \geq 1) \\ 1 & (\mu_i(m) = 0) \\ \displaystyle\prod_{\nu=\mu_i(m)}^{-1} h_i(\mu_i(s) + \nu)^{-\varepsilon(\eta_i)} & (\mu_i(m) \leq -1). \end{cases}$$

In [5, §1], η_i, μ_i, h_i are normalized to be $\varepsilon(\eta_i) < 0$. Another normalization is given in [11, Proposition 1.1.4] with a restriction on μ_i instead of $\varepsilon(\eta_i)$. To describe the group structure of cohomology classes, such descriptions are more elegant. But, in this article, the Ore-Sato theorem should be introduced in the presented form for a reason which will arise later (especially in Lemma 2.4.2). Here we are interested in $Z^1(\Xi; k(s)^\times)$ rather than $H^1(\Xi; k(s)^\times)$.

(ii) The assumption in Corollary 2.1.4 does not imply that each $\eta_i h_i(\mu_i(s))$ is a polynomial; for example, let $r = 2$ and consider the 1-cocycle defined by (2.1) with $c = 1$, $f(s) = 1$, $l = 1$, $h_1(t) = t$, $\mu_1(s) = 2s_1 + 3s_2$, $\eta_1 = 1 - \lambda + \lambda^2$ (here λ is the basis of $\Xi/\Xi_{\mu_1(s)}$ represented by $\tau_1^{-1}\tau_2$). In addition, we observe that the conditions (1), (2) in the corollary are not sufficient for the assumption; consider the 1-cocycle where η_1 in the above example is replaced with $\eta_1 = 1 - \lambda - \lambda^2 + \lambda^3 + \lambda^4$. (But these two examples define the same cohomology class in $H^1(\Xi; k(s)^\times)$).

Let $k = \mathbb{C}$. Take a 1-cocycle $b \in Z^1(\Xi; \mathbb{C}(s)^\times)$ and keep the notation in Theorem 2.1.3. Write $h_i = t + \alpha_i$ ($\alpha_i \in \mathbb{C}$) and $c(\tau^m) = c_1^{m_1} \cdots c_r^{m_r}$ ($c_1, \ldots, c_r \in \mathbb{C}^\times$). Then the $\mathbf{G}_\mathrm{m}$-primitive difference equation associated with b has a solution

$$\gamma(s) = c_1^{s_1} \cdots c_r^{s_r} f(s) \prod_{i=1}^{l} \eta_i \Gamma(\mu_i(s) + \alpha_i).$$

Assume $b_{\tau_1}, \ldots, b_{\tau_r}$ are polynomials. In this case, $\gamma(s)$ has no zeros by Corollary 2.1.4. There are several methods to characterize $\gamma(s)$ among other solutions; by asymptotic behavior (see [1, §1], [11, §4.1], and [14, Ch. 11]) and by log convexity: M. Fujigami [4] gave a generalization of the Bohr-Mollerup theorem [2, Theorem 2.1]. Further methods may be suggested in [2, §6].

2.2. Reductive prehomogeneous vector spaces and its b-functions

Let V be an n-dimensional $\mathbb{C}$-vector space and G a connected reductive linear algebraic group over $\mathbb{C}$. Suppose (G, ρ, V) is a reductive prehomogeneous vector space. Then, by the definition, there exists a proper algebraic subset S of V such that $V \setminus S$ is a single G-orbit. Let S_0 denote the union of the irreducible components of S with codimension 1. We always assume that S_0 is not empty. Since $\rho(G)$ is connected reductive, it is self-adjoint with respect to a $\mathbb{C}$-basis of V by the theorem of Mostow [12]. By such a basis, we identify the coordinate ring $\mathbb{C}[V]$ of V with $\mathbb{C}[x] = \mathbb{C}[x_1, \ldots, x_n]$, the polynomial ring of n variables. Let $P_1, \ldots, P_r \in \mathbb{C}[x]$ be irreducible polynomials which define the irreducible components of S_0. These polynomials are relative invariants and every relative invariant is uniquely expressed in the form $cP_1(x)^{m_1} \cdots P_r(x)^{m_r}$ ($c \in \mathbb{C}^\times$, $(m_1, \ldots, m_r) \in \mathbb{Z}^r$). In this sense, $P_1, \ldots, P_r$ are called the *basic relative invariants* of (G, ρ, V) [10, Definition 2.10]. They are necessarily homogeneous polynomials [10, Corollary 2.7]. Let $\bar{P}_1, \ldots, \bar{P}_r$ be the polynomials obtained by complex conjugation of coefficients of $P_1, \ldots, P_r$ respectively. By the choice of the basis of V, those are the basic relative invariants of the dual prehomogeneous vector space (G, ρ^*, V^*), when we identify $\mathbb{C}[V^*]$ with $\mathbb{C}[x]$ by the dual basis (see [6, Lemma 1.5] or [10, Proposition 2.21]).

In the following, we consider $P_1(x)^{s_1} \cdots P_r(x)^{s_r}$ as a many-valued holomorphic function on $\mathbb{C}^r \times (V \setminus S_0)$. Write $\mathrm{grad}_x = (\partial/\partial x_1, \ldots, \partial/\partial x_r)$. For each $m = (m_1, \ldots, m_r) \in \mathbb{Z}^r_{\geq 0}$,

$$\frac{\bar{P}_1(\mathrm{grad}_x)^{m_1} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r} (P_1(x)^{s_1+m_1} \cdots P_r(x)^{s_r+m_r})}{P_1(x)^{s_1} \cdots P_r(x)^{s_r}} \in \mathbb{C}[s_1, \ldots, s_r; x_1, \ldots, x_n]$$

is (absolutely) invariant under the action of G. Since every absolute invariant in $\mathbb{C}[x]$ is a constant [10, Proposition 2.4], it is independent of x. Thus there exists a polynomial $b_m(s) \in \mathbb{C}[s_1, \dots, s_r]$ such that

$$\bar{P}_1(\mathrm{grad}_x)^{m_1} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r}(P_1(x)^{s_1+m_1} \cdots P_r(x)^{s_r+m_r}) = b_m(s)P_1(x)^{s_1} \cdots P_r(x)^{s_r}.$$

Moreover, it is known that the degree of $b_m(s)$ (on s) is equal to the degree of $\prod_{i=1}^{r} P_i(x)^{m_i}$ (on x); this follows from an easy modification of the proof given in [6, Lemma 1.7] or [10, Proposition 2.22].

Definition 2.2.1. The polynomials $b_m(s)$ are called the *b-functions* of $P_1, \dots, P_r$.

By calculating

$$\bar{P}_1(\mathrm{grad}_x)^{m_1+m_1'} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r+m_r'}(P_1(x)^{s_1+m_1+m_1'} \cdots P_r(x)^{s_r+m_r+m_r'})$$

in two ways, we have

$$b_{m+m'}(s) = b_{m'}(s+m)b_m(s)$$

for all $m = (m_1, \dots, m_r), m' = (m_1', \dots, m_r') \in \mathbb{Z}_{\geq 0}^r$. Hence the map $\mathbb{Z}_{\geq 0}^r \to \mathbb{C}(s)^\times$, $m \mapsto b_m(s)$ is uniquely extended to a 1-cocycle $b : \mathbb{Z}^r \to \mathbb{C}(s)^\times$. By the Ore-Sato theorem (Theorem 2.1.3), each $b_m(s)$ $(0 \neq m = (m_1, \dots, m_r) \in \mathbb{Z}_{\geq 0}^r)$ is written as

$$b_m(s) = c_1^{m_1} \cdots c_r^{m_r} \prod_{i=1}^{l} \prod_{j} \prod_{\nu=0}^{\mu_i(m)-1} (\mu_i(s) + \alpha_i + j + \nu)^{z_{ij}}, \tag{2.2}$$

where the notations are taken as in §2.1 and $\eta_i = \sum_j z_{ij}\lambda_i^j$ satisfying the conditions in Corollary 2.1.4. We take them so that $(\mu_1(s) + \alpha_1), \dots, (\mu_l(s) + \alpha_l)$ are $\mathbb{Z}\Xi$-linearly independent. It is known that each $\alpha_i + j$ (with $z_{ij} > 0$) is a positive rational number (due to M. Kashiwara [9]). Moreover, we have $c_1, \dots, c_r \in \mathbb{R}_{>0}$ since

$$b_m(0) = \bar{P}_1(\mathrm{grad}_x)^{m_1} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r}(P_1(x)^{m_1} \cdots P_r(x)^{m_r}) \in \mathbb{R}_{>0}$$

for all $m = (m_1, \dots, m_r) \in \mathbb{Z}_{\geq 0}^r$. Let d_k be the degree of $P_k(x)$ for $k = 1, \dots, r$. Then the observation just before Definition 2.2.1 implies that

$$d_k = \sum_{i=1}^{l} \mu_i(e_k)\varepsilon(\eta_i) \qquad (k = 1, \dots, r), \tag{2.3}$$

where $e_1 = (1, 0, \dots, 0), \dots, e_r = (0, \dots, 0, 1)$.

2.3. Local zeta functions over $\mathbb{C}$

We identify V with $\mathbb{C}^n$ by the basis fixed in §2.2. Let dx denote the Haar measure on V normalized to satisfy

$$\int_V \exp(-2\pi x^t\bar{x})dx = 1,$$

where $x = (x_1, \ldots, x_r) \in \mathbb{C}^n$ and ${}^t\bar{x}$ denotes the transposition of the complex conjugate of x. Let $|\cdot|_{\mathbb{C}}$ be the valuation of $\mathbb{C}$ defined by $|z|_{\mathbb{C}} = z\bar{z} = |z|^2$ for $z \in \mathbb{C}$. The integral

$$Z_{\mathbb{C}}(s) = \int_V |P_1(x)|_{\mathbb{C}}^{s_1} \cdots |P_r(x)|_{\mathbb{C}}^{s_r} \exp(-2\pi x^t\bar{x})dx$$

converges when $(s_1, \ldots, s_r) \in \{(s_1, \ldots, s_r) \in \mathbb{C}^r \mid \mathrm{Re}(s_1), \ldots, \mathrm{Re}(s_r) > 0\}$, and hence $Z_{\mathbb{C}}(s)$ is a holomorphic function on this region. Our purpose is to show that $Z_{\mathbb{C}}(s)$ is equal to

$$\gamma_{\mathbb{C}}(s) := \prod_{k=1}^{r}((2\pi)^{-d_k}c_k)^{s_k} \prod_{i=1}^{l}\prod_{j} \left(\frac{\Gamma(\mu_i(s) + \alpha_i + j)}{\Gamma(\alpha_i + j)}\right)^{z_{ij}}$$

with the notations in (2.2) (recall that $\gamma_{\mathbb{C}}(s)$ has no zeros in $\mathbb{C}^r$ by Corollary 2.1.4):

Theorem 2.3.1. *$Z_{\mathbb{C}}(s)$ has a meromorphic continuation to $\mathbb{C}^r$ and $Z_{\mathbb{C}}(s) = \gamma_{\mathbb{C}}(s)$.*

Actually, the first part of this theorem has been known (see [3]) and our aim is to obtain the second part. To prove this theorem, we need the following lemma:

Lemma 2.3.2. *For $s = (s_1, \ldots, s_r) \in \mathbb{C}^r$ and $m = (m_1, \ldots, m_r) \in \mathbb{Z}_{\geq 0}^r$, we have*

$$\begin{aligned} &\bar{P}_1(\mathrm{grad}_x)^{m_1} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r}(|P_1(x)|_{\mathbb{C}}^{s_1} \cdots |P_r(x)|_{\mathbb{C}}^{s_r} P_1(x)^{m_1} \cdots P_r(x)^{m_r}) \\ = \;& b_m(s)|P_1(x)|_{\mathbb{C}}^{s_1} \cdots |P_1(x)|_{\mathbb{C}}^{s_1} \end{aligned}$$

on $V \setminus S_0$.

Proof. Locally we choose the branching of the value of $\log P_i(x)$ and $\log \overline{P_i(x)} = \log \bar{P}_i(\bar{x})$ so that $|P_i(x)|_{\mathbb{C}}^{s_i} = \bar{P}_i(\bar{x})^{s_i}P_i(x)^{s_i}$ holds. Since $\bar{P}_j(\mathrm{grad}_x)$ and $\bar{P}_i(\bar{x})^{s_i}$ commute as differential operators for $i, j = 1, \cdots, r$, we have

$$\begin{aligned} &\bar{P}_1(\mathrm{grad}_x)^{m_1} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r}(|P_1(x)|_{\mathbb{C}}^{s_1} \cdots |P_r(x)|_{\mathbb{C}}^{s_r} P_1(x)^{m_1} \cdots P_r(x)^{m_r}) \\ = \;& \bar{P}_1(\mathrm{grad}_x)^{m_1} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r}(\bar{P}_1(\bar{x})^{s_1} \cdots \bar{P}_r(\bar{x})^{s_r} P_1(x)^{s_1+m_1} \cdots P_r(x)^{s_r+m_r}) \\ = \;& \bar{P}_1(\bar{x})^{s_1} \cdots \bar{P}_r(\bar{x})^{s_r} \bar{P}_1(\mathrm{grad}_x)^{m_1} \cdots \bar{P}_r(\mathrm{grad}_x)^{m_r}(P_1(x)^{s_1+m_1} \cdots P_r(x)^{s_r+m_r}) \\ = \;& \bar{P}_1(\bar{x})^{s_1} \cdots \bar{P}_r(\bar{x})^{s_r} b_m(s) P_1(x)^{s_1} \cdots P_r(x)^{s_r} \\ = \;& b_m(s)|P_1(x)|_{\mathbb{C}}^{s_1} \cdots |P_1(x)|_{\mathbb{C}}^{s_1}. \end{aligned}$$

□

Proof of Theorem 2.3.1. By Lemma 2.3.2, we have

$$\begin{aligned}
&b_m(s)Z_{\mathbb{C}}(s)\\
=\ & \int_V \left\{\left(\prod_{i=1}^r \bar{P}_i(\mathrm{grad}_x)^{m_i}\right)\left(\prod_{j=1}^r |P_j(x)|_{\mathbb{C}}^{s_j} P_j(x)^{m_j}\right)\right\}\exp(-2\pi x^t\bar{x})dx\\
=\ & \int_V \left(\prod_{j=1}^r |P_j(x)|_{\mathbb{C}}^{s_j} P_j(x)^{m_j}\right)\left(\prod_{i=1}^r \bar{P}_i(-\mathrm{grad}_x)^{m_i}\right)\exp(-2\pi x^t\bar{x})dx\\
=\ & (2\pi)^{\sum_{k=1}^r d_k m_k}\int_V \prod_{j=1}^r |P_j(x)|_{\mathbb{C}}^{s_j} P_j(x)^{m_j}\prod_{i=1}^r \bar{P}_i(\bar{x})^{m_i}\exp(-2\pi x^t\bar{x})dx\\
=\ & (2\pi)^{\sum_{k=1}^r d_k m_k}\int_V \prod_{j=1}^r |P_j(x)|_{\mathbb{C}}^{s_j+m_j}\exp(-2\pi x^t\bar{x})dx\\
=\ & (2\pi)^{\sum_{k=1}^r d_k m_k} Z_{\mathbb{C}}(s+m)
\end{aligned}$$

for $(s_1,\dots,s_r)\in\{(s_1,\dots,s_r)\in\mathbb{C}^r \mid \mathrm{Re}(s_1),\dots,\mathrm{Re}(s_r)>0\}$ and $m=(m_1,\dots,m_r)\in\mathbb{Z}_{\geq 0}^r$. Hence $Z_{\mathbb{C}}(s)$ satisfies the following equation:

$$Z_{\mathbb{C}}(s+m) = (2\pi)^{-\sum_{k=1}^r d_k m_k} b_m(s) Z_{\mathbb{C}}(s). \tag{2.4}$$

Then $Z_{\mathbb{C}}(s)$ has a meromorphic continuation to $\mathbb{C}^r$ by this equation (as in [3]). Furthermore, (2.4) implies that both $Z_{\mathbb{C}}(s)$ and $\gamma_{\mathbb{C}}(s)$ satisfy the same ($\mathbf{G}_{\mathrm{m}}$-primitive) difference equation. Therefore $C(s) := Z_{\mathbb{C}}(s)/\gamma_{\mathbb{C}}(s)$ is a holomorphic and periodic function with periods $e_1,\dots,e_r$. To show that $C(s)$ is a constant function, we investigate the asymptotic behavior of $C(s)$ on the strip $\mathcal{S}=\{(s_1,\dots,s_r)\in\mathbb{C}^r \mid 1\leq \mathrm{Re}(s_i)\leq 2 \quad (i=1,\cdots,r)\}$.

Put $S^{n-1}(\mathbb{C}) = \{x\in V \mid x^t\bar{x}=1\}$ ($\simeq SO(2n,\mathbb{R})/SO(2n-1,\mathbb{R})$ as real manifolds). We identify $V\setminus\{0\}$ with $\mathbb{R}_{>0}\times S^{n-1}(\mathbb{C})$ via $x\mapsto(\xi,u)=(\sqrt{x^t\bar{x}}, x/\sqrt{x^t\bar{x}})$. Take the $SO(2n,\mathbb{R})$-invariant measure du on $S^{n-1}(\mathbb{C})$ such that $dx = 2^n\xi^{2n-1}d\xi du$ on $V\setminus\{0\}$. Let

$$\psi(s) = 2^{n-1}\int_{S^{n-1}(\mathbb{C})} |P_1(u)|_{\mathbb{C}}^{s_1}\cdots|P_r(u)|_{\mathbb{C}}^{s_r}du.$$

Then we have

$$\begin{aligned}
Z_{\mathbb{C}}(s) &= \int_{V\setminus\{0\}} |P_1(x)|_{\mathbb{C}}^{s_1}\cdots|P_r(x)|_{\mathbb{C}}^{s_r}\exp(-2\pi x^t\bar{x})dx\\
&= 2\psi(s)\int_0^\infty \xi^{2(\sum_{k=1}^r d_k s_k+n)-1}\exp(-2\pi\xi^2)d\xi\\
&= (2\pi)^{-\sum_{k=1}^r d_k s_k - n}\psi(s)\Gamma(d_1s_1+\cdots+d_rs_r+n)
\end{aligned}$$

when $\mathrm{Re}(s_i) > 0$ $(i = 1, \cdots, r)$. Since

$$|(2\pi)^{-\sum_{k=1}^r d_k s_k - n}\psi(s)| \leq (2\pi)^{-\sum_{k=1}^r d_k \mathrm{Re}(s_k) - n} 2^{n-1} \int_{S^{n-1}(\mathbb{C})} |P_1(u)|_{\mathbb{C}}^{\mathrm{Re}(s_1)} \cdots |P_r(u)|_{\mathbb{C}}^{\mathrm{Re}(s_r)} du,$$

$|(2\pi)^{-\sum_{k=1}^r d_k s_k - n}\psi(s)|$ is bounded in $\mathcal{S}$. Let $a_1, \ldots, a_r$ be arbitrary positive real numbers and t_0 a real variable. Then the well-known asymptotic behavior of the gamma function and (2.3) imply that

$$C(1 + \sqrt{-1}a_1 t_0, \ldots, 1 + \sqrt{-1}a_r t_0) = o(\exp(|t_0|)) \qquad (|t_0| \to \infty).$$

Unless $C(s)$ is a constant function, this is impossible. Thus the proof is completed since $C(0) = 1$. □

2.4. Local zeta functions over $\mathbb{R}$

In this section, we assume that the prehomogeneous vector space (G, ρ, V) is *defined over* $\mathbb{R}$ (in the sense of [15, §1] or [10, §2.1]) and replace $P_1, \ldots, P_r$ and b as follows. Since S_0 is defined over $\mathbb{R}$ (see [15, Lemma 1.1]), we can take irreducible polynomials $P_1, \ldots, P_r \in \mathbb{R}[x]$ which define the $\mathbb{R}$-irreducible components of S_0 (possibly r becomes smaller). Here, we are assuming the basis of V is fixed so that the $\mathbb{R}$-rational points of $\rho(G)$ is self-adjoint with respect to the induced $\mathbb{R}$-basis of $V_{\mathbb{R}}$, the $\mathbb{R}$-rational points of V. Those $P_1, \ldots, P_r$ are often called *the basic relative invariants of* (G, ρ, V) *over* $\mathbb{R}$. They are also considered as the basic relative invariants of (G, ρ^*, V^*) over $\mathbb{R}$. Then there exist polynomials $b_m(s)$ such that

$$P_1(\mathrm{grad}_x)^{m_1} \cdots P_r(\mathrm{grad}_x)^{m_r}(P_1(x)^{s_1+m_1} \cdots P_r(x)^{s_r+m_r}) = b_m(s) P_1(x)^{s_1} \cdots P_r(x)^{s_r}$$

for $m = (m_1, \ldots, m_r) \in \mathbb{Z}_{\geq 0}^r$. All properties on $b_m(s)$ described in §2.2 also hold. Keep the notations in (2.2) and in (2.3).

Let dx denote the Lebesgue measure on $V_{\mathbb{R}}$ identified with $\mathbb{R}^r$. As in the previous section, the integral

$$Z_{\mathbb{R}}(s) = \int_{V_{\mathbb{R}}} |P_1(x)|^{s_1} \cdots |P_r(x)|^{s_r} \exp(-\pi x^t x) dx$$

converges when $(s_1, \ldots, s_r) \in \{(s_1, \ldots, s_r) \in \mathbb{C}^r \mid \mathrm{Re}(s_1), \ldots, \mathrm{Re}(s_r) > 0\}$, and hence $Z_{\mathbb{R}}(s)$ is a holomorphic function on this region. From now on, we assume the following:

Assumption 2.4.1. Every term of $P_i(x)$ is a multilinear form on x for $i = 1, \ldots, r$, i.e. each $P_i(x)$ is of the form:

$$P_i(x) = \sum_{1 \le j_1 < \cdots < j_{d_i} \le n} a_{j_1 \cdots j_{d_i}} x_{j_1} \cdots x_{j_{d_i}} \qquad (i = 1, \ldots, r).$$

We will see that $Z_{\mathbb{R}}(2s)$ satisfies a certain $\mathbf{G}_{\mathrm{m}}$-primitive difference equation in such a case. By the assumption above, we see

$$P_i(\mathrm{grad}_x) \exp(-\pi x^t x) = (-2\pi)^{d_i} P_i(x) \exp(-\pi x^t x) \qquad (i = 1, \cdots, r).$$

Thus

$$\begin{aligned}
b_{e_i}(s) Z_{\mathbb{R}}(s) &= \int_{V_{\mathbb{R}}} \{P_i(\mathrm{grad}_x)(|P_1(x)|^{s_1} \cdots |P_r(x)|^{s_r} P_i(x))\} \exp(-\pi x^t x) dx \\
&= (-1)^{d_i} \int_{V_{\mathbb{R}}} (|P_1(x)|^{s_1} \cdots |P_r(x)|^{s_r} P_i(x)) P_i(\mathrm{grad}_x) \exp(-\pi x^t x) dx \\
&= (2\pi)^{d_i} \int_{V_{\mathbb{R}}} |P_1(x)|^{s_1} \cdots |P_r(x)|^{s_r} P_i(x) P_i(x) \exp(-\pi x^t x) dx \\
&= (2\pi)^{d_i} \int_{V_{\mathbb{R}}} |P_1(x)|^{s_1} \cdots |P_i(x)|^{s_i+2} \cdots |P_r(x)|^{s_r} \exp(-\pi x^t x) dx \\
&= (2\pi)^{d_i} Z_{\mathbb{R}}(s + 2e_i),
\end{aligned}$$

for $i = 1, \ldots, r$. Hence $Z_{\mathbb{R}}(s)$ satisfies the equation

$$Z_{\mathbb{R}}(s + 2e_i) = (2\pi)^{-d_i} b_{e_i}(s) Z_{\mathbb{R}}(s) \qquad (i = 1, \ldots, r). \tag{2.5}$$

We can obtain a meromorphic continuation of $Z_{\mathbb{R}}(s)$ to $\mathbb{C}^r$. By considering $Z_{\mathbb{R}}(s + 2e_j + 2e_k)$ in two ways, we have

$$b_{e_j}(s) b_{e_k}(s + 2e_j) = b_{e_j}(s + 2e_k) b_{e_k}(s) \quad (j, k = 1, \cdots, r). \tag{2.6}$$

Lemma 2.4.2. *When Assumption 2.4.1 holds, $\mu_i(e_j)$ $(i = 1, \cdots, l,\ j = 1, \cdots, r)$ are equal to either 0 or 1 and hence each $\eta_i \cdot (\mu_i(s) + \alpha_i)$ is a polynomial.*

Proof. For each $i = 1, \cdots, l$, take any j, k such that $\mu_i(e_j), \mu_i(e_k) > 0$ and write $\eta_i = \sum_{u=\kappa}^{\kappa'} z_{iu} \lambda_i^u$ $(z_{i\kappa}, z_{i\kappa'} \neq 0)$. By (2.6), we have

$$\begin{aligned}
&\prod_{u=\kappa}^{\kappa'} \left(\prod_{v=0}^{\mu_i(e_j)-1} (\mu_i(s) + \alpha_i + u + v) \prod_{w=0}^{\mu_i(e_k)-1} (\mu_i(s) + 2\mu_i(e_j) + \alpha_i + u + w) \right)^{z_{iu}} \\
= &\prod_{u=\kappa}^{\kappa'} \left(\prod_{v=0}^{\mu_i(e_j)-1} (\mu_i(s) + 2\mu_i(e_k) + \alpha_i + u + v) \prod_{w=0}^{\mu_i(e_k)-1} (\mu_i(s) + \alpha_i + u + w) \right)^{z_{iu}}.
\end{aligned}$$

In each side, the constant terms of the factors

$$(\mu_i(s) + 2\mu_i(e_j) + \alpha_i + \kappa' + \mu_i(e_k) - 1),$$
$$(\mu_i(s) + 2\mu_i(e_k) + \alpha_i + \kappa' + \mu_i(e_j) - 1)$$

are maximal respectively; recall that these factors are not cancelled (Corollary 2.1.4). Hence the two factors coincide and we have $\mu_i(e_j) = \mu_i(e_k)$. Therefore the all non-zero numbers among $\mu_i(e_1), \ldots, \mu_i(e_r)$ coincide. This proves the lemma since the greatest common divisor of them is 1. $\square$

Theorem 2.4.3. *When Assumption 2.4.1 holds, we have*

$$Z_{\mathbb{R}}(s) = \prod_{k=1}^{r} (\pi^{-d_i} c_i)^{\frac{s_i}{2}} \prod_{i=1}^{l} \prod_{j} \left(\frac{\Gamma((\mu_i(s) + \alpha_i + j)/2)}{\Gamma((\alpha_i + j)/2)} \right)^{z_{ij}}.$$

Proof. Let $\beta : \mathbb{Z}^r \to \mathbb{C}(s)^\times$ be the map given by

$$\beta_m(s) = \prod_{k=1}^{r} (\pi^{-d_k} c_k)^{m_k} \prod_{i=1}^{l} \prod_{j} \begin{cases} \displaystyle\prod_{\nu=0}^{\mu_i(m)-1} (\mu_i(s) + \frac{\alpha_i + j}{2} + \nu)^{z_{ij}} & (\mu_i(m) \geq 1) \\ 1 & (\mu_i(m) = 0) \\ \displaystyle\prod_{\nu=\mu_i(m)}^{-1} (\mu_i(s) + \frac{\alpha_i + j}{2} + \nu)^{-z_{ij}} & (\mu_i(m) \leq -1). \end{cases}$$

We see that β is a 1-cocycle since $Z_{\mathbb{R}}(2s)$ satisfies the $\mathbf{G}_{\mathrm{m}}$-primitive difference equation

$$Z_{\mathbb{R}}(2(s+m)) = \beta_m(s) Z_{\mathbb{R}}(2s)$$

by (2.5) and Lemma 2.4.2. In addition, the second assertion of Lemma 2.4.2 implies that all z_{ij} is non-negative. Let

$$\gamma_{\mathbb{R}}(s) := \prod_{k=1}^{r} (\pi^{-d_i} c_i)^{\frac{s_i}{2}} \prod_{i=1}^{l} \prod_{j} \left(\frac{\Gamma((\mu_i(s) + \alpha_i + j)/2)}{\Gamma((\alpha_i + j)/2)} \right)^{z_{ij}}.$$

Then both $\gamma_{\mathbb{R}}(2s)$ and $Z_{\mathbb{R}}(2s)$ satisfy the same difference equation.

Put $S^{n-1}(\mathbb{R}) = \{x \in V_{\mathbb{R}} \mid x^t x = 1\}$ ($\simeq SO(n, \mathbb{R})/SO(n-1, \mathbb{R})$). We identify $V_{\mathbb{R}} \setminus \{0\}$ with $\mathbb{R}_{>0} \times S^{n-1}(\mathbb{R})$ via $x \mapsto (\xi, u) = (\sqrt{x^t x}, x/\sqrt{x^t x})$. Take the $SO(n, \mathbb{R})$-invariant measure du on $S^{n-1}(\mathbb{R})$ such that $dx = \xi^{n-1} d\xi du$ on $V_{\mathbb{R}} \setminus \{0\}$. Let

$$\psi(s) = \frac{1}{2} \int_{S^{n-1}(\mathbb{R})} |P_1(u)|^{s_1} \cdots |P_r(u)|^{s_r} du.$$

Then we have

$$\begin{aligned} Z_{\mathbb{R}}(s) &= \int_{V_{\mathbb{R}}\setminus\{0\}} |P_1(x)|^{s_1}\cdots|P_r(x)|^{s_r}\exp(-\pi x^t x)dx \\ &= 2\psi(s)\int_0^{\infty}\xi^{\sum_{k=1}^r d_k s_k+n-1}\exp(-\pi\xi^2)d\xi \\ &= \pi^{(-\sum_{k=1}^r d_k s_k-n)/2}\psi(s)\Gamma\left(\frac{d_1s_1+\cdots+d_rs_r+n}{2}\right) \end{aligned}$$

when $\mathrm{Re}(s_i) > 0$ $(i = 1,\cdots,r)$. Therefore, similarly to the proof of Theorem 2.3.1, we obtain that $Z_{\mathbb{R}}(2s)/\gamma_{\mathbb{R}}(2s) = 1$. □

REFERENCES

[1] K. Aomoto, *Les équations aux différences linéaires et les intérales des fonctions multiformes*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 22 (1975), 271–297.

[2] E. Artin, translated by M. Butler, *"The gamma function"*, Holt, Rinehart and Winston, Inc., 1964.

[3] I.N. Bernshtein, *The analytic continuation of generalized functions with respect to a parameter*, Funct. Anal. Appl. 6 (1972), 273–285.

[4] M. Fujigami, *A generalization of the Bohr-Mollerup theorem and the Γ-factors of local functional equations* (Japanese), Sūrikaisekikenkyūsho Kōkyūroku, Kyoto Univ., 1238 (2001), 20–29.

[5] I.M. Gel'fand, M.I. Graev, V.S. Retakh, *General hypergeometric systems of equations and series of hypergeometric type*, Russian Math. Surveys 47:4 (1992), 1–88.

[6] A. Gyoja, *Theory of prehomogeneous vector spaces without regularity condition*, Publ. Res. Inst. Math. Sci. 27 (1991), 861–922.

[7] J. Igusa, *On functional equations of complex powers*, Invent. math. 85 (1986), 1–29

[8] J. Igusa, *"An introduction to the theory of local zeta functions"*, AMS/IP Studies in Advanced Mathematics 14, AMS, 2000.

[9] M. Kashiwara, *B-functions and holonomic systems—rationality of roots of B-functions*, Invent. math. 38 (1976), 33–53.

[10] T. Kimura, translated by M. Nagura and T. Niitani, *"Introduction to prehomogeneous vector spaces"*, Translations of Mathematical Monographs 215, AMS, 2003.

[11] F. Loeser, C. Sabbah, *Equations aux différences finies et déterminants d'intégrales de fonctions multiformes*, Comment. Math. Helvetici 66 (1991), 458–503.

[12] G.D. Mostow, *Self-adjoint groups*, Ann. of Math. 62 (1955), 44–55.

[13] O. Ore, *Sur la forme des fonctions hypergéométriques de plusieures variables*, J. Math. Pures et Appl. 9 (1930), 311–327.

[14] M. van der Put, M.F. Singer, *"Galois theory of difference equations"*, Lecture Notes in Math. 1666, Springer, 1997.

[15] F. Sato, *Zeta functions in several variables associated with prehomogeneous vector spaces I: Functional equations*, Tôhoku Math. J. (2) 34 (1982), 437–483.

[16] M. Sato, note by T. Shintani, translated by M. Muro, *Theory of prehomogeneous vector spaces (algebraic part)—the English translation of Sato's lecture from Shintani's note*, Nagoya Math. J. 120 (1990), 1–34.

Part 3. Picard-Vessiot theories for artinian simple module algebras

Introduction of Part 3

The purpose of this part is to develop a unified Picard-Vessiot theory, including Picard-Vessiot theories for differential equations and for difference equations. The presented result was obtained by the author and Masuoka [1, 2].

In the usual sense, the "Picard-Vessiot theory" means a Galois theory for linear ordinary differential equations. See [21] for modern treatment. For example, consider the following differential equation over $\mathbb{C}$:

$$y''(x) - y'(x) - y(x) = 0. \tag{3.1}$$

Let $\mathbb{C}[\partial]$ ($\partial = d/dx$) be the ring of differential operators with constant coefficients. The differential module ($\mathbb{C}[\partial]$-module) associated with the equation (3.1) is

$$\mathbb{C}[\partial]/\langle \partial^2 - \partial - 1\rangle \simeq (\mathbb{C}[\partial]/\langle \partial - (1+\sqrt{5})/2\rangle) \oplus (\mathbb{C}[\partial]/\langle \partial - (1-\sqrt{5})/2\rangle).$$

Thus the space of solutions is given by the 2-dimensional $\mathbb{C}$-vector space $\mathbb{C}\alpha + \mathbb{C}\beta$ with $\alpha = e^{\frac{1+\sqrt{5}}{2}x}$, $\beta = e^{\frac{1-\sqrt{5}}{2}x}$. A differential field (i.e. a field given a derivation) L including this space is called a *splitting field* for the equation. If L is minimal with this property, it is called a *minimal splitting field.* For the equation above, $L = \mathbb{C}(\alpha, \beta)$ is a minimal splitting field. Like Galois extensions, $L/\mathbb{C}$ is then an extension of a special type, called a *Picard-Vessiot extension.* For such an extension, we can take a Galois group, called the *differential Galois group* (or the *Picard-Vessiot group*) as an algebraic group defined by $\mathrm{Aut}_{\mathbb{C}[\partial],\mathbb{C}\text{-alg}}(L) =: G(L/\mathbb{C})$, where $\mathrm{Aut}_{\mathbb{C}[\partial],\mathbb{C}\text{-alg}}$ denotes the $\mathbb{C}[\partial]$-linear and $\mathbb{C}$-algebra automorphisms. We have $G(L/\mathbb{C}) = \mathbf{G}_m \times \mathbf{G}_m$ in this case, and we can obtain the Galois correspondence between closed subgroups of $G(L/\mathbb{C})$ and intermediate differential fields of $L/\mathbb{C}$. For example, the differential field $\mathbb{C}(\alpha)$ corresponds to $\{1\} \times \mathbf{G}_m$ (or $\mathbf{G}_m \times \{1\}$ according to the choice of the group action).

An analogous theory for *difference* equations is also known. Białynicki-Birula [4] and Franke [8] first developed such a theory for inversive difference fields, i.e. fields given an automorphism (though the Białynicki-Birula's paper was intended for more general theory, not only for difference fields). A definition of Picard-Vessiot extensions of inversive difference fields and Galois correspondences were obtained there. But the theory had a difficulty on the existence of suitable solution fields. For example, consider the Fibonacci recurrence

$$a(n+2) - a(n+1) - a(n) = 0. \tag{3.2}$$

Let $\mathbb{C}[\tau, \tau^{-1}]$ ($\tau : n \mapsto n+1$) be the ring of difference operators with constant coefficients. The difference module ($\mathbb{C}[\tau, \tau^{-1}]$-module) associated with the equation (3.2) is

$$\mathbb{C}[\tau, \tau^{-1}]/\langle \tau^2 - \tau - 1 \rangle \simeq (\mathbb{C}[\tau]/\langle \tau - (1+\sqrt{5})/2 \rangle) \oplus (\mathbb{C}[\tau]/\langle \tau - (1-\sqrt{5})/2 \rangle).$$

Let $\mathcal{S}_\mathbb{C}$ denote the ring of complex sequences (see [20, Example 3]). The space of solutions in $\mathcal{S}_\mathbb{C}$ is given by the 2-dimensional $\mathbb{C}$-vector space $\mathbb{C}\alpha + \mathbb{C}\beta$ with $\alpha = \{(\frac{1+\sqrt{5}}{2})^n\}$, $\beta = \{(\frac{1-\sqrt{5}}{2})^n\} \in \mathcal{S}_\mathbb{C}$. But one can not take any splitting field which becomes a Picard-Vessiot extension for this equation. If a subring in $\mathcal{S}_\mathbb{C}$ contains α, β, then it has a zero divisor:

$$(\alpha\beta - 1)(\alpha\beta + 1) = 0.$$

On the other hand, if we take any inversive difference field which includes a 2-dimensional $\mathbb{C}$-vector space of solutions of (3.2), then it necessarily contains a new constant (see [20, p. 2]). However, overcoming this difficulty, the Picard-Vessiot theory for difference equations in modern sense was developed by van der Put and Singer [20] with the notion of *Picard-Vessiot rings*, as follows. Consider the Laurent polynomial ring $\mathbb{C}[x, y, (xy)^{-1}]$ as an inversive difference ring by

$$\tau x = \frac{1+\sqrt{5}}{2}x, \quad \tau y = \frac{1-\sqrt{5}}{2}y.$$

On sees that $\langle (xy-1)(xy+1) \rangle \subset \mathbb{C}[x, y, (xy)^{-1}]$ is a maximal difference ideal. Put

$$A = \mathbb{C}[x, y, (xy)^{-1}]/\langle (xy-1)(xy+1) \rangle.$$

Then A is a Picard-Vessiot ring for the equation (3.2) in their sense (see [20, Definition 1.4]). The total quotient ring of a Picard-Vessiot ring is called the *total Picard-Vessiot ring* [20, Definition 1.22]. For the equation (3.2), we have the following total Picard-Vessiot ring:

$$\begin{array}{rcl} Q(A) & \simeq & \mathbb{C}(\alpha) \times \mathbb{C}(\alpha) \\ x & \mapsto & (\alpha, \alpha) \\ y & \mapsto & (\alpha^{-1}, -\alpha^{-1}). \end{array} \tag{3.3}$$

Then the *difference Galois group* for the equation can be defined by $G(Q(A)/\mathbb{C}) := \mathrm{Aut}_{\mathbb{C}[\tau,\tau^{-1}],\mathbb{C}\text{-alg}}(Q(A))$. In this case, we have $G(Q(A)/\mathbb{C}) \simeq \mathrm{G_m} \times \mathbb{Z}/2\mathbb{Z}$. We obtain the Galois correspondence between closed subgroups of $G(Q(A)/\mathbb{C})$ and intermediate difference subrings of $Q(A)/\mathbb{C}$ such that every non-zero divisor is invertible (see [20, Theorem 1.29]). For example, $\mathbb{C}(\alpha)$ ($= \mathbb{C}(\alpha)(1,1)$) corresponds to $\{1\} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{C} \times \mathbb{C}$ corresponds to $\mathbf{G}_{\mathrm{m}} \times \{1\}$.

A unified approach to both differential and difference cases was first attempted by Białynicki-Birula [4], though it was a theory for field extensions. Including the case that the solution algebras can have zero divisors, André [3] gave such a unified approach from the viewpoint of non-commutative differential geometry with the theory of tannakian categories [5, 6]. Alternatively we develop a unified Picard-Vessiot theory by a different way based on the Takeuchi's Hopf algebraic approach: Takeuchi [27] beautifully clarified the heart of the Picard-Vessiot 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* [27] is a field given a unital, measuring action by C; the concept includes differential fields, Δ-fields [13], fields with higher derivations [18], and difference fields (even non-inversive ones are included). However, it was also a theory for field extensions and the assumption that the tensor bialgebra $T(C^+)$ [27, p. 485] is a Birkhoff-Witt coalgebra (see [27, p. 504] or Assumption 3.3.1), is required for the existence theorem of minimal splitting algebras.

In this article, we consider 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 a Birkhoff-Witt coalgebra. An inversive difference ring which includes R in its constants is precisely a D-module algebra when $D^1 = R$ 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. Precisely a differential ring which includes R (of zero characteristic) in its constants is a D-module algebra when $D^1 = R[\partial]$ with a primitive ∂ and G is trivial. Algebras with higher derivations of infinite length fit in the assumption, in arbitrary characteristic. 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 becomes a Birkhoff-Witt coalgebra in arbitrary characteristic.

Throughout this article, D-module algebras are all supposed to be commutative. A D-module algebra K is said to be *artinian simple* (AS) if it is artinian as a ring and simple as a D-module algebra. The last condition means that K has no non-trivial D-stable ideal. For example, the total Picard-Vessiot ring considered in (3.3) is an AS $\mathbb{C}[\tau, \tau^{-1}]$-module algebra. Of course differential fields over $\mathbb{C}$ are AS $\mathbb{C}[\partial]$-module algebras. In this sense we can generalize and unify the Picard-Vessiot theories for differential and difference equations, involving the theory of van der Put and Singer [20].

Let L be an AS D-module algebra. If $P \subset L$ is a maximal ideal, then one will see that $L_1 := L/P$ 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, L can recover from L_1, so as

$$L = D \otimes_{D(G_P)} L_1 = \bigoplus_{g \in G/G_P} g \otimes L_1,$$

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 3.3. (For example, when $D = \mathbb{C}[\tau, \tau^{-1}]$ and $L = Q(A) \simeq \mathbb{C}(\alpha) \times \mathbb{C}(\alpha)$ as above, take $P = \langle xy - 1 \rangle \subset Q(A)$. Then $G_P = \{g^2 \mid g \in G\} \xrightarrow{\sim} 2\mathbb{Z}$ under the group isomorphism $G \simeq \mathbb{Z}$.) The D-invariants $L^D = \{a \in L \mid da = \varepsilon(d)a \quad \text{for all} \quad d \in D\}$ (where ε denotes the counit of D) in L form a subfield, such that $L^D \simeq L_1^{D(G_P)}$. Following [27], we say that an inclusion $K \subset L$ of AS D-module algebras is a *Picard-Vessiot (PV) extension* iff $K^D = L^D$ and 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 3.5.2. (In the example (3.3), we have $H = \mathbb{C}[z_1, z_2]/\langle z_1^2 z_2^2 - 1 \rangle$ with grouplikes $z_1 = x \otimes x^{-1}$, $z_2 = y \otimes y^{-1}$.) 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 3.7.4 and Theorem 3.7.6.

As our main theorems we prove:

Galois Correspondence (Theorem 3.5.4): 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 (Proposition 3.5.7). This has the obvious interpretation in terms of the affine group scheme $\mathbf{G}(L/K) = \mathrm{Spec}H$ corresponding to H, and $\mathbf{G}(L/K)$ is isomorphic to the automorphism group scheme $\mathbf{Aut}_{D,K\text{-alg}}(A)$ (see Section 3.6).

Characterization (Theorem 3.8.7): An inclusion $K \subset L$ of AS D-module algebras with $K^D = L^D$ is a finitely generated (see Definition 3.8.6) PV extension iff L/K is a minimal splitting algebra for some $K\#D$-module V of finite K-free rank, say n; this means that $\dim_{L^D} \mathrm{Hom}_{K\#D}(V, L) = n$ and L is "minimal" with this property (see Proposition 3.8.3).

Tensor Equivalence (Theorem 3.8.13): If this is the case, the symmetric tensor category $\mathcal{M}^H_{\mathrm{fin}}$ of finite-dimensional right comodules over the associated Hopf algebra H (or equivalently that category $\mathrm{Rep}_{\mathbf{G}(L/K)}$ of finite-dimensional linear representations of $\mathbf{G}(L/K)$) 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. [21, Theorem 2.33].

Unique Existence (Theorem 3.8.11): 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 [27] by Takeuchi on this article of ours. Especially the main theorems above except the third are very parallel to results in [27], including their proofs. A C-ferential field is equivalent to a module field over the tensor bialgebra $T(C^+)$. We remark that even if K, L are fields, the first two theorems above do not imply the corresponding results in [27] since the notion of C-ferential fields is more general than D-module fields in the sense of ours. The last one only generalizes [27, Theorems 4.5, 4.6] in which $T(C^+)$ is supposed to be of Birkhoff-Witt type.

The last section (Section 3.9) treats the solvability theory for liouvillian extensions. The notion of liouvillian extensions of differential fields first appeared in the Kolchin's historical work on the Picard-Vessiot theory [12], to make clear the idea of linear differential equations being "solvable by quadratures" which was used by Picard and Vessiot not being stated clearly. An extension of differential fields (of zero characteristic) is called liouvillian iff it contains no new constants and it is obtained by iterating integrations, exponentiations, and algebraic extensions. It was shown that a Picard-Vessiot extension of differential fields is liouvillian iff the connected component of its differential Galois group is solvable. By the Lie-Kolchin triangularization theorem and others [12, Ch. I], we can characterize several types of liouvillian extensions in matrix theoretical way. For example, a liouvillian extension is obtained only by iterating integrations iff its differential Galois group is unipotent. For the case of an arbitrary characteristic, Okugawa [18] studied the Picard-Vessiot theory for fields with higher derivations of infinite length, and obtained similar results on liouvillian extensions.

Liouvillian extensions of difference fields were first studied by Franke [8]. In the context of [20], Hendriks and Singer [10] studied on liouvillian solutions of difference equations with rational function coefficients. They defined the notion of "Liouvillian sequences" and showed that a linear difference equation can be solved in terms of such sequences iff the difference Galois group is solvable. (Moreover, they gave an algorithm to find such liouvillian solutions, using the Petkovšek's algorithm [19].)

In the last section, we define the notion of liouvillian extensions of AS D-module algebras and prove a solvability theorem in the unified context.

When we study liouvillian extensions with affine group schemes, we will meet the following difficulty: the Lie-Kolchin triangularization theorem can not be extended generally to affine group schemes (see [29, Ch. 10]). Certainly there are gaps between the triangulability and the connected solvability, even if the base field is algebraically closed. So we need some intermediate notions and have to study how they are related each other. In Section 3.9.1, we define "liouvillian group schemes" so that it is suitable for liouvillian extensions defined later, and study how strong the definition is. An algebraic affine group scheme $\mathbf{G}$ over a field k is called *(k-)liouvillian* (cf. [13, p. 374]) iff there exists a normal chain of closed subgroup schemes $\mathbf{G} = \mathbf{G}_0 \rhd \mathbf{G}_1 \rhd \cdots \rhd \mathbf{G}_r = \{1\}$ such that each $\mathbf{G}_{i-1}/\mathbf{G}_i$ ($i = 1, \ldots, r$) is at least one of the following types: finite etale, a closed subgroup scheme of $\mathbf{G}_{\mathrm{a}}$, or a closed subgroup scheme of $\mathbf{G}_{\mathrm{m}}$. When k is algebraically closed, $\mathbf{G}$ is liouvillian iff the connected component $\mathbf{G}^{\circ}$ is solvable (Proposition 3.9.5). But in general it does not holds; we show this fact by examples. For connected affine group schemes, we will see the condition to be liouvillian is properly stronger than the solvability but weaker than the triangulability.

Let $L \supset K$ be an inclusion of AS D-module algebras. For finitely many elements $x_1, \ldots, x_n \in L$, let $K\langle x_1, \ldots, x_n\rangle$ denote the smallest AS D-module subalgebra in L

including both K and $x_1, \ldots, x_n$. L/K is called $\mathbf{G}_{\mathrm{a}}$*-primitive extension* (resp., $\mathbf{G}_{\mathrm{m}}$*-primitive extension*) iff there is an $x \in L$ such that $d(x) \in K$ for all $d \in D^+ = \operatorname{Ker} \varepsilon$ (resp., x is a non-zero divisor of L (which is necessarily invertible) and $d(x)x^{-1} \in K$ for all $d \in D$) and $L = K\langle x \rangle$. We say that L/K is a *finite etale extension* iff L is a separable K-algebra in the sense of [7], i.e. L is a projective $L \otimes_K L$-module. Then we define *liouvillian extension* as such a finitely generated extension L/K that $L^D = K^D$ and there exists a sequence of AS D-module algebras $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$ such that each L_i/L_{i-1} $(i = 1, \ldots, r)$ is at least one of the following types: $\mathbf{G}_{\mathrm{a}}$-primitive extension, $\mathbf{G}_{\mathrm{m}}$-primitive extension, or finite etale extension. As the last one of the main theorems, we will show the following:

Solvability (Theorem 3.9.17): Let L/K be a finitely generated PV extension. Then the following are equivalent:

(a) L/K is a liouvillian extension.
(b) There exists a liouvillian extension F/K such that $L \subset F$.
(c) $\mathbf{G}(L/K)$ is liouvillian.

When k is algebraically closed, these are equivalent to:

(d) $\mathbf{G}(L/K)^\circ$ is solvable.

Moreover we will characterize ten types of liouvillian extensions just being compatible with [12, §24–27]; see Definition 3.9.15, Corollary 3.9.19 and its following paragraph.

Conventions. Throughout this part, we always work over an arbitrarily fixed field R. All vector spaces, algebras and coalgebras are defined at least over R. All algebras are associative and have the identity element. All modules over an algebra are unital, left modules unless otherwise stated. All separable algebras are taken in the sense of [7]; see also [29, Ch. 6].

The notation $\operatorname{Hom}_{\mathcal{R}}$ (resp. $\operatorname{End}_{\mathcal{R}}$) with a ring $\mathcal{R}$ always denotes the set of all $\mathcal{R}$-linear maps (resp. $\mathcal{R}$-linear endomorphisms), but the unadorned Hom may indicate group homomorphisms or homomorphisms of group schemes. Algebra (resp. coalgebra) maps are always dentoed by Alg (resp. Coalg). The notation Aut indicates automorphisms in some sense; for example, $\operatorname{Aut}_{D,K\text{-alg}}$ means D-linear and K-algebra automorphisms. **Aut** in the bold style indicates an associated group functor as in [29, (7.6)]. Coalgebra structures are denoted by (Δ, ε). If we need to specify a coalgebra (or a coring) C, the notation $(\Delta_C, \varepsilon_C)$ is also used. For a coalgebra C, C^+ denotes $\operatorname{Ker} \varepsilon$. The antipode of a

Hopf algebra is denoted by S. We use the *sigma notation* (see [23, §1.2, pp. 10–11] or [16, §1.4, pp. 6–7]):

$$\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)} \qquad \text{etc.}$$

When (M, λ) is a right (resp. left) C-comodule, $\lambda(m)$ $(m \in M)$ is denoted by the sigma notation

$$\lambda(m) = \sum_{(m)} m_{(0)} \otimes m_{(1)} \in M \otimes_R C \quad (\text{resp. } \ \lambda(m) = \sum_{(m)} m_{(-1)} \otimes m_{(0)} \in C \otimes_R M).$$

By "a symmetric tensor category $(\mathfrak{A}, \otimes, I)$" we mean that $(\mathfrak{A}, \otimes)$ is a symmetric tensor (or monoidal) category [16, §10.4, p. 199] with a fixed unit object I. We can define algebras, coalgebras, etc., in $(\mathfrak{A}, \otimes, I)$ naturally by commutative diagrams. For an algebra A in $(\mathfrak{A}, \otimes, I)$, left A-modules (resp. right A-modules, resp. (A, A)-bimodules) in $(\mathfrak{A}, \otimes, I)$ can also be defined and the category of them is denoted by ${}_A\mathfrak{A}$ (resp. $\mathfrak{A}_A$, resp. ${}_A\mathfrak{A}_A$). For a ring $\mathcal{R}$, ${}_{\mathcal{R}}\mathcal{M}$ (resp. $\mathcal{M}_{\mathcal{R}}$) denotes the category of left (resp. right) $\mathcal{R}$-modules. For a coalgebra C, $\mathcal{M}^C$ (resp. ${}^C\mathcal{M}$) denotes the category of right (resp. left) C-comodules. Moreover, further notations, such as ${}_A\mathcal{M}^H$, ${}^H_A\mathcal{M}$, etc., which indicate categories of relative Hopf modules are used as in [16, §8.5].

3.1. Basic notions and results on D-module algebras

Let D be a cocommutative bialgebra. An algebra A is called a *D-module algebra* (see [23, §7.2, p. 153] or [16, §4.1]) iff A is a D-module and the action of D measures A to A. The last condition means that

$$\rho_A : A \to \mathrm{Hom}_R(D, A), \quad a \mapsto [d \mapsto da]$$

is an algebra map, where $\mathrm{Hom}_R(D, A)$ is considered as an algebra with the convolution product (see [23, pp. 69–70] or [16, §1.4]); or in other words, using the sigma notation,

$$d(ab) = \sum_{(d)} (d_{(1)}a)(d_{(2)}b), \qquad d(1) = \varepsilon(d)1$$

hold for all $d \in D$ and $a, b \in A$. Throughout this part, we assume D-module algebras are commutative unless otherwise stated. Note that the algebra $\mathrm{Hom}_R(D, A)$ is commutative in our situation, and it has a D-module algebra structure given by

$$(3.4) \qquad (d\varphi)(c) = \varphi(cd) \qquad (c, d \in D, \ \varphi \in \mathrm{Hom}_R(D, A)).$$

One sees ρ_A is an injective D-module algebra map. For a D-module algebra A, the *smash product* $A\#D$ means the algebra which is $A \otimes_R D$ with the semi-direct product:

$$(a\#c)(b\#d) = \sum_{(c)} a(c_{(1)}b)\#c_{(2)}d$$

(see [23, pp. 155–156] or [16, §4.1]). For $A\#D$-modules $V, W \in {}_{A\#D}\mathcal{M}$, we have an $A\#D$-module structure on $V \otimes_A W$ given by

$$(a\#d)(v \otimes w) = a\sum_{(d)} d_{(1)}v \otimes d_{(2)}w \qquad (a \in A,\ d \in D,\ v \in V,\ w \in W).$$

Thus we have an abelian symmetric tensor category [6, Definition 1.15] $({}_{A\#D}\mathcal{M}, \otimes_A, A)$ with the canonical symmetry $V \otimes_A W \to W \otimes_A V$, $v \otimes w \mapsto w \otimes v$. For a D-module V,

$$V^D := \{v \in V \mid dv = \varepsilon(d)v \quad \text{for all} \quad d \in D\}$$

is called the *constants* (or the *D-invariants*) of V. Especially A^D becomes an algebra. We see $\mathrm{Hom}_{A\#D}(A, V) \xrightarrow{\sim} V^D$, $\varphi \mapsto \varphi(1)$ is an A^D-module isomorphism and in particular $\mathrm{End}_{A\#D}(A) \simeq A^D$ as algebras. The functor $(-)^D : {}_{A\#D}\mathcal{M} \to {}_{A^D}\mathcal{M}$ is an exact functor since A is a projective $A\#D$-module (indeed, $A\#D \simeq A \oplus (A \otimes_R D^+)$ as $A\#D$-modules via $a\#d \mapsto (a\varepsilon(d), a \otimes (d - \varepsilon(d)))$). Let B be a D-module algebra including A as a D-module subalgebra, V an $A\#D$-module, and W a $B\#D$-module. If D is a Hopf algebra with the antipode S, then $\mathrm{Hom}_A(V, W)$ has a $B\#D$-module structure given by the D-conjugation:

$$((b\#d)\varphi)(v) = b\sum_{(d)} d_{(1)}(\varphi(S(d_{(2)})v) \qquad (v \in V) \tag{3.5}$$

for $b \in B$, $d \in D$, and $\varphi \in \mathrm{Hom}_A(V, W)$; see [27, Proposition 1.8]. We see $\mathrm{Hom}_A(V, W)^D = \mathrm{Hom}_{A\#D}(V, W)$. Especially Hom_A is an internal Hom [6, p. 109] of $({}_{A\#D}\mathcal{M}, \otimes_A, A)$ in such a case.

The following proposition, like the Schur's lemma, is very important:

Proposition 3.1.1. *Let $\mathfrak{A}$ be an abelian category. An object X in $\mathfrak{A}$ is simple iff*

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

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

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

is injective.

Proof. It suffices to show that the proposition holds for every small abelian full subcategory of $\mathfrak{A}$ containing X as an object. By the Freyd-Mitchell embedding theorem (see [9]), we may assume $\mathfrak{A} = {}_{\mathcal{R}}\mathcal{M}$ for a ring $\mathcal{R}$.

("If" part.) Let Y be an $\mathcal{R}$-submodule of X. Since $\mathrm{Hom}_{\mathcal{R}}(X, Y)$ is a right ideal of $E = \mathrm{End}_{\mathcal{R}}(X)$, $\mathrm{Hom}_{\mathcal{R}}(X, Y)$ equals 0 or E by (a). If $\mathrm{Hom}_{\mathcal{R}}(X, Y) = E$, we have $Y = X$ since $X \simeq E \otimes_E X \to Y$ is injective. If $\mathrm{Hom}_{\mathcal{R}}(X, Y) = 0$, then $E \to \mathrm{Hom}_{\mathcal{R}}(X, X/Y)$ is injective. Since all E-modules are flat, we have that $X \simeq E \otimes_E X \to \mathrm{Hom}_{\mathcal{R}}(X, X/Y) \otimes_E X \to X/Y$ is injective and hence $Y = 0$.

("Only if" part.) (a) For $0 \neq f \in E$, $\mathrm{Im}(f)$ is a non-zero $\mathcal{R}$-submodule of X and hence $\mathrm{Im}(f) = X$, $\mathrm{Ker}(f) = 0$. Thus f is invertible.

(b) Since X is simple, each $0 \neq f \in \mathrm{Hom}_{\mathcal{R}}(X, Y)$ is injective and hence $\mathrm{Im}(f)$ is simple. It suffices to prove that the sum $\sum_{i=1}^{r} \mathrm{Im}(f_i) \subset Y$ is direct if $f_1, \ldots, f_r$ are E-linearly independent in $\mathrm{Hom}_{\mathcal{R}}(X, Y)$. To prove this, we shall use induction on r. When $r = 1$, the assertion is clear. When $r > 1$, suppose that the assertion is true for $\{f_1, \ldots, f_{r-1}\}$. Seeking a contradiction, assume $\mathrm{Im}(f_r) \cap \sum_{i=1}^{r-1} \mathrm{Im}(f_i) \neq 0$. Since $\mathrm{Im}(f_r)$ is simple, we have $\mathrm{Im}(f_r) \subset \bigoplus_{i=1}^{r-1} \mathrm{Im}(f_i)$. Then there exist $\varphi_i \in E$ $(i = 1, \ldots, r-1)$ such that the diagram

$$\begin{tikzcd}
\mathrm{Im}(f_r) \arrow[r, "\text{inclusion}"] & \displaystyle\bigoplus_{i=1}^{r-1} \mathrm{Im}(f_i) \arrow[r, "\text{projection}"] & \mathrm{Im}(f_i) \\
X \arrow[u, "f_r"] \arrow[rr, "\varphi_i"] & & X \arrow[u, "f_i"']
\end{tikzcd}$$

commutes for $i = 1, \ldots, r-1$ since $f_i : X \to \mathrm{Im}(f_i)$ is invertible. Then $f_r = f_1 \circ \varphi_1 + \cdots + f_{r-1} \circ \varphi_{r-1}$. This contradicts that $f_1, \ldots, f_r$ are E-linearly independent. $\square$

Remark 3.1.2. I heard the above proposition from Professor A. Masuoka. Though it seems well-known, an explicit citation was not found as far as I searched. It is said that Professor Masuoka knew this by a comment from Professor T. Breziński on [15, Theorem 1.1 and the Theorem on p. 232]; see the proof of [2, Proposition 3.1].

Definition 3.1.3. A D-module algebra A is called *simple* iff it is simple in ${}_{A\#D}\mathcal{M}$, i.e. A has no non-trivial D-stable ideal.

The next corollary follows immediately from Propositoin 3.1.1.

Corollary 3.1.4. *A D-module algtebra A is simple iff*

(a) *A^D is a field, and*

(b) *for every $A\#D$-module Y, the map*

$$Y^D \otimes_{A^D} A \to Y, \quad y \otimes a \mapsto ay$$
$$(\textit{or} \quad A \otimes_{A^D} Y^D \to Y, \quad a \otimes y \mapsto ay)$$

is injective.

Proof. Recall that $\mathrm{End}_{A\#D}(A) \simeq A^D$ and $\mathrm{Hom}_{A\#D}(A, Y) \simeq Y^D$. The evaluation map is identified with the map in (b) above. □

Let A be a D-module algebra and $\rho_A : A \to \mathrm{Hom}_R(D, A)$ the associated algebra map. Then $\mathrm{Hom}_R(D, A)$ has two kind of A-module structures: $A \otimes_R \mathrm{Hom}_R(D, A) \to \mathrm{Hom}_R(D, A)$, given by (I) $a \otimes \varphi \mapsto \rho_A(a) * \varphi = \varphi * \rho_A(a)$, and (II) $a \otimes \varphi \mapsto a\varphi = [d \mapsto a\varphi(d)]$. The structure given by (II) can be considered through the following algebra isomorphism:

$$\sigma : A \xrightarrow{\sim} \mathrm{Hom}_R(D, A)^D, \quad a \mapsto a\varepsilon_D,$$

which has the inverse given by $\varphi \mapsto \varphi(1)$. Here we are taking the D-module structure on $\mathrm{Hom}_R(D, A)$ in the sense of (3.4). As in [27, Corollary 1.4], the next lemma follows from Corollary 3.1.4.

Lemma 3.1.5. *If A is simple, then the following map:*

$$\beta : A \otimes_{A^D} A \to \mathrm{Hom}_R(D, A), \quad a \otimes b \mapsto \rho_A(b) * (a\varepsilon_D) = a\rho_A(b)$$

is a two-sided A-linear (left through σ, right through ρ_A) injection.

Proof. Consider $Y = \mathrm{Hom}_R(D, A)$ as an $A\#D$-module by the A-module structure given by (I) and by the D-module structure in the sense of of (3.4):

$$(a\#d)\varphi = \rho_A(a) * (d\varphi) \qquad (a \in A,\ d \in D,\ \varphi \in Y).$$

This is well-defined:

$$\begin{aligned}
&(a'\#d')((a\#d)\varphi)) = \rho_A(a') * \sum_{(d')} (d'_{(1)}\rho_A(a)) * (d'_{(2)}d\varphi) \\
= \;& \rho_A(a') * \sum_{(d')} \rho_A(d'_{(1)}a) * (d'_{(2)}d\varphi) = \sum_{(d')} \rho_A(a'(d'_{(1)}a)) * (d'_{(2)}d\varphi) \\
= \;& ((a'\#d')(a\#d))\varphi.
\end{aligned}$$

Then β is injective since $A \simeq Y^D$ through σ. □

This lemma has an application when one needs to think of the A^D-linear dependence of elements in A. Takeuchi generalized the Wronskian (and Casoratian) criterion as follows:

Proposition 3.1.6. *([27, Proposition 1.5]) Let K be a D-module field. Then $a_1, \ldots, a_n \in K$ are K^D-linearly independent iff there exist $h_1, \ldots, h_n \in D$ such that* $\det(h_i(a_j))_{i,j} \neq 0$.

Proof. We include the proof for convenience.

("If" part.) If $\sum_{j=1}^n c_j a_j = 0$ $(c_1, \ldots, c_n \in K^D)$, then $\sum_{j=1}^n c_j h_i(a_j) = 0$ for $i = 1, \ldots, n$. Since the matrix $(h_i(a_j))_{i,j}$ is invertible, we have $c_1 = \cdots = c_n = 0$.

("Only if" part.) Put $W = K^D a_1 + \cdots + K^D a_n$, an n-dimensional K^D-vector subspace of K. Consider the K-linear injection

$$\beta : K \otimes_{K^D} W \to \mathrm{Hom}_R(D, K) \simeq \mathrm{Hom}_K(K \otimes_R D, K)$$

which is restricted by the map β in Lemma 3.1.5. Let $\{d_\alpha\}_{\alpha \in \Lambda}$ be an R-basis of D and $d_\alpha^\vee$ be the dual of d_α in $\mathrm{Hom}_R(D, K)$. Then $\mathrm{Hom}_K(K \otimes_R D, K) = \prod_{\alpha \in \Lambda} K d_\alpha^\vee$ as a K-vector space. Notice that $\rho_A(a) = \sum_{\alpha \in \Lambda} (d_\alpha a) d_\alpha^\vee$ $(a \in K)$. Since $\rho_A(a_1), \ldots, \rho_A(a_n)$ are K-linearly independent and since K is a field, we obtain a K-basis $v_1, \ldots, v_n$ of $K \otimes_{K^D} W$ such that

$$\begin{aligned}
\beta(v_1) &= h_1^\vee + \sum_{\substack{\alpha \in \Lambda \\ d_\alpha \neq h_1}} c_{1,\alpha} d_\alpha^\vee \\
\beta(v_2) &= h_2^\vee + \sum_{\substack{\alpha \in \Lambda \\ d_\alpha \neq h_1, h_2}} c_{2,\alpha} d_\alpha^\vee \\
&\vdots \\
\beta(v_n) &= h_n^\vee + \sum_{\substack{\alpha \in \Lambda \\ d_\alpha \neq h_1, \ldots, h_n}} c_{n,\alpha} d_\alpha^\vee
\end{aligned}$$

for some n elements $h_1, \ldots, h_n \in \{d_\alpha\}_{\alpha \in \Lambda}$ by sweeping-out. Consider the transposed K-linear map of β:

$$\gamma : K \otimes_R D \to \mathrm{Hom}_K(K \otimes_{K^D} W, K), \quad a \otimes d \mapsto [b \otimes w \mapsto ab(dw)].$$

Let $v_1^\vee, \ldots, v_n^\vee$ be the dual basis of $v_1, \ldots, v_n$. Then we have ${}^t(\gamma(h_1), \ldots, \gamma(h_n)) = T\,{}^t(v_1^\vee, \ldots, v_n^\vee)$ with a strictly lower triangular matrix $T \in GL_n(K)$. Thus $\gamma(h_1), \ldots, \gamma(h_n)$ form a K-basis for $\mathrm{Hom}_K(K \otimes_{K^D} W, K) \simeq \mathrm{Hom}_{K^D}(W, K)$. The K-isomorphism

$$\begin{array}{ccccc}
K^n & \xrightarrow{\sim} & \mathrm{Hom}_{K^D}(W, K) & \xrightarrow{\sim} & K^n \\
(c_i)_i & \mapsto & \displaystyle\sum_{i=1}^n c_i \gamma(h_i) & \mapsto & \displaystyle\left(\sum_{i=1}^n c_i h_i(a_j)\right)_j
\end{array}$$

is precisely the right multiplication of matrix $(h_i(a_j))_{i,j}$. It follows that the matrix has an inverse. $\square$

Remark 3.1.7. In the above proof, we see that $\operatorname{Ker}\gamma$ is a left ideal of $K\#D$. If $D = R[\partial]$ with one primitive ∂, then $\operatorname{Ker}\gamma$ is generated by a monic differential operator of order n. Thus we can take $h_1 = 1, h_2 = \partial, \ldots, h_n = \partial^{n-1}$ in such a case. Namely we have the Wronskian criterion in the usual sense. Similarly we also have the ordinary Casoratian criterion for difference fields.

3.2. Tensor equivalences associated to Hopf subalgebras

In what follows we assume that D is a cocommutative Hopf algebra. Let C be a Hopf subalgebra of D. A coalgebra in the tensor category $({}_D\mathcal{M}, \otimes_R, R)$ is called a *D-module coalgebra.* D is a D-module coalgebra, and $\bar{D} := D/DC^+$ is its quotient. The R-abelian category ${}^{\bar{D}}_{D}\mathcal{M}$ of left $(\bar{D}, D)$-Hopf modules is defined as follows (see [26, pp. 454–455] or [16, §8.5].):

Objects. An object of ${}^{\bar{D}}_{D}\mathcal{M}$ is a left D-module which is also a left $\bar{D}$-comodule with a structure λ_M, say, such that

$$\lambda_M(dm) = \Delta(d)\lambda_M(m) = \sum_{(d)}\sum_{(m)} d_{(1)}m_{(-1)} \otimes d_{(2)}m_{(0)} \in \bar{D} \otimes_R M$$

for all $d \in D$ and $m \in M$.

Morphisms. Morphisms of ${}^{\bar{D}}_{D}\mathcal{M}$ are D-module and $\bar{D}$-comodule maps.

Given objects M, N in ${}^{\bar{D}}_{D}\mathcal{M}$, let $M\square_{\bar{D}}N$ 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, or in other words,

$$M\square_{\bar{D}}N = \left\{ \sum_i x_i \otimes y_i \;\middle|\; \sum_i \sum_{(x_i)} (x_i)_{(-1)} \otimes (x_i)_{(0)} \otimes y_i = \sum_i \sum_{(y_i)} (y_i)_{(-1)} \otimes x_i \otimes (y_i)_{(0)} \right\}.$$

This is a D-submodule of $M \otimes N$, and is further an object in ${}^{\bar{D}}_{D}\mathcal{M}$. We see that ${}^{\bar{D}}_{D}\mathcal{M} = ({}^{\bar{D}}_{D}\mathcal{M}, \square_{\bar{D}}, \bar{D})$ is a symmetric tensor category. Indeed, the associativity $(M\square_{\bar{D}}N)\square_{\bar{D}}L \xrightarrow{\sim}$

$M\square_{\bar{D}}(N\square_{\bar{D}}L)$ and the symmetry $M\square_{\bar{D}}N \xrightarrow{\sim} N\square_{\bar{D}}M$ are induced by those of $({}_D\mathcal{M}, \otimes_R)$ naturally. We have isomorphisms

$$M\square_{\bar{D}}\bar{D} \xrightarrow{\sim} M, \quad \sum_i m_i \otimes a_i \mapsto \sum_i m_i\varepsilon(a_i),$$
$$\bar{D}\square_{\bar{D}}M \xrightarrow{\sim} M, \quad \sum_i a_i \otimes m_i \mapsto \sum_i \varepsilon(a_i)m_i,$$

whose inverses are obtained by λ_M. Thus $\bar{D}$ is a unit object.

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

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

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

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

Proposition 3.2.1. Φ *is an equivalence of symmetric tensor categories.*

Proof. By [26, Theorem 2 and 4], Φ is a category equivalence; its quasi-inverse $N \mapsto \Psi(N)$ is given by

$$\Psi(N) = {}^{\mathrm{co}\,\bar{D}}N = \{n \in N \mid \lambda_N(n) = \bar{1} \otimes n \ \text{ in } \ \bar{D} \otimes N\},$$

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

$$\Psi(M) \otimes \Psi(N) \to \Psi(M\square_{\bar{D}}N), \quad m \otimes n \mapsto m \otimes n,$$
$$R \to \Psi(\bar{D}), \quad 1 \mapsto \bar{1}$$

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

Let D^1 denote the irreducible component in D containing 1; this is the largest irreducible Hopf subalgebra. If the characteristic $\operatorname{ch} R$ 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 [23, Ch. XIII] or [16, §5.6]. Let $G = G(D)$ denote the group of all grouplikes in D.

In what follows we suppose:

Assumption 3.2.2. D is pointed, so that

$$D = D^1 \# RG,$$

the smash product with respect to the conjugate action by G on D^1; see [23, Theorem 8.1.5] or [16, Corollary 5.6.4].

In the following, we take as C a Hopf subalgebra of the form

$$C = D(G_1) := D^1 \# RG_1,$$

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

$$\Phi_{G_1} : {}_{D(G_1)}\mathcal{M} \xrightarrow{\approx} {}_D^{\bar{D}}\mathcal{M}, \tag{3.6}$$

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 $\bar{D} \xrightarrow{\simeq} R(G/G_1)$, left $\bar{D}$-comodules are identified with (G/G_1)-graded vector spaces: for $N \in {}^{\bar{D}}\mathcal{M}$,

$$N = \bigoplus_{s \in G/G_1} N_s \qquad (N_s = \{n \in N \mid \lambda_N(n) = s \otimes n\}).$$

An object in ${}_D^{\bar{D}}\mathcal{M}$ is a left D-module $N = \bigoplus_{s \in G/G_1} N_s$ which satisfy that $gN_s \subset N_{gs}$ ($g \in G$, $s \in G/G_1$). If $M = \bigoplus_{s \in G/G_1} M_s$ is another object in ${}_D^{\bar{D}}\mathcal{M}$, then

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

We have $D = \bigoplus_{g \in G/G_1} gD(G_1)$.

Notation 3.2.3. 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 $N_1 = \Psi(N)$ in N is a $D(G_1)$-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 $hg = g't$. Hence, by Proposition 3.2.1, we have an isomorphism $\Phi(N_1) = \bigoplus_{g \in G/G_1} g \otimes N_1 \xrightarrow{\simeq} N$ in ${}_D^{\bar{D}}\mathcal{M}$, given by $g \otimes n \mapsto gn$.

An algebra A in $({}^{\bar{D}}_{D}\mathcal{M}, \square_{\bar{D}}, \bar{D})$ 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. We observe that $e_g = g \otimes 1 \in \Phi(A_1)$ are orthogonal central idempotents.

Let $A = \Phi(A_1)$ be as above. An A_1-module V in ${}_{D(G_1)}\mathcal{M}$ is precisely a module over the algebra $A_1\#D(G_1)$ of smash product: ${}_{A_1}({}_{D(G_1)}\mathcal{M}) = {}_{A_1\#D(G_1)}\mathcal{M}$. $\Phi(V)$ is naturally an A-module in ${}^{\bar{D}}_{D}\mathcal{M}$; this is in particular an $A\#D$-module.

Proposition 3.2.4. *Let A_1 be a $D(G_1)$-module algebra and $A = \Phi(A_1)$. The functor*

$$\Phi : {}_{A_1\#D(G_1)}\mathcal{M} \to {}_{A\#D}\mathcal{M}$$

is an equivalence of R-abelian categories.

Proof. By Proposition 3.2.1, 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 $N_g = e_gN$ $(e_g = g \otimes 1 \in A = \Phi(A_1),\ g \in G/G_1)$. 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. □

This proposition can be extended as follows:

Proposition 3.2.5. *Let $A = \Phi(A_1)$ be as above. The functor*

$$\Phi : ({}_{A_1}({}_{D(G_1)}\mathcal{M})_{A_1}, \otimes_{A_1}, A_1) \to ({}_A({}^{\bar{D}}_{D}\mathcal{M})_A, \otimes_A, A)$$

is a tensor equivalence.

Proof. For $V, W \in {}_{A_1}({}_{D(G_1)}\mathcal{M})_{A_1}$, we easily see

$$\Phi(V) \otimes_A \Phi(W) \simeq \sum_{g\in G/G_1} g \otimes (V \otimes_{A_1} W) = \Phi(V \otimes_{A_1} W)$$

in $({}_A({}^{\bar{D}}_{D}\mathcal{M})_A, \otimes_A, A)$. □

We see that the functor Φ preserves constants and simple module algebras:

Lemma 3.2.6. (i) *Let V be a $D(G_1)$-module. Then an isomorphism $V^{D(G_1)} \xrightarrow{\sim} \Phi(V)^D$ is given by $v \mapsto \sum_{g\in G/G_1} g \otimes v$.*

(ii) *Let A_1 be a commutative $D(G_1)$-module algebra. Then A_1 is a simple $D(G_1)$-module algebra iff $\Phi(A_1)$ is a simple D-module algebra.*

Proof. (i) 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 $g \in G/G_1$.

(ii) This directly follows from Proposition 3.2.4. □

3.3. Artinian simple D-module algebras

Let $D = D^1 \# RG$ be a cocommutative pointed Hopf algebra as in the previous section. In what follows we further assume:

Assumption 3.3.1. The irreducible Hopf algebra D^1 is of Birkhoff-Witt type.

This means that every primitive element of D lies in a divided power sequence of infinite length; an infinite sequence $\{1 = d_0, d_1, \ldots, d_n, \ldots\}$ in D^1 is called a *divided power sequence* if $\Delta(d_n) = \sum_{i=0}^{n} d_i \otimes d_{n-i}$ (see [23, p. 268]). This assumption is necessarily satisfied if $\operatorname{ch} R = 0$ (for each primitive $\partial \in P(D)$, $\{1, \partial, \partial^2/2, \ldots, \partial^n/n!, \ldots\}$ is a divided power sequence of infinite length). If $\operatorname{ch} R = p > 0$, this is equivalent to the Verschiebung map $D^1 \to R^{1/p} \otimes D^1$ being surjective; see [11]. The assumption is also equivalent to saying that D is smooth as a cocommutative coalgebra.

Moreover this implies that, for a commutative algebra A, the A-algebra $\operatorname{Hom}_R(D^1, A)$ with the convolution product is the projective limit of power series A-algebras (see [23, p. 278]). Thus, if A is a domain (resp. reduced), then $\operatorname{Hom}_R(D^1, A)$ is also a domain (resp. reduced). Furthermore, $\operatorname{Hom}_R(D, A)$ is isomorphic to the direct product of A-algebras isomorphic to $\operatorname{Hom}_R(D^1, A)$ indexed by G:

$$\begin{array}{ccccc} \operatorname{Hom}_R(D, A) & \xrightarrow{\sim} & \operatorname{Hom}_R(RG, \operatorname{Hom}_R(D^1, A)) & \xrightarrow{\sim} & \prod_{g \in G} \operatorname{Hom}_R(D^1, A) \\ \varphi & \mapsto & [g \mapsto [d \mapsto \varphi(dg)]] & \mapsto & ([d \mapsto \varphi(dg)])_g. \end{array}$$

Hence, if A is reduced, then $\operatorname{Hom}_R(D, A)$ is also reduced. (These facts implies that D^1 and D are convolutionally reduced in the sense of [28, Definition 5.2].)

As in [27, p. 505], we have the following:

Lemma 3.3.2. *Let A be a D-module algebra and $\rho_A : A \to \operatorname{Hom}_R(D, A)$ the algebra map associated with the structure on A.*

(i) *If $J \subset A$ is an ideal, then $\rho_A^{-1}(\operatorname{Hom}_R(D, J))$ is a D-stable ideal, which is maximal among D-stable ideals included in J. Therefore J is a D-stable ideal iff $J = \rho_A^{-1}(\operatorname{Hom}_R(D, J))$.*

(ii) *If $I \subset A$ is a D-stable ideal, then also the radical $\sqrt{I}$ is a D-stable ideal.*

(iii) *If $P \subset A$ is a prime ideal, then $(\rho_A^1)^{-1}(\operatorname{Hom}_R(D^1, P))$ is a prime D^1-stable ideal. Here $\rho_A^1 : A \to \operatorname{Hom}_R(D^1, A)$ is the algebra map associated with the D^1-module algebra structure on A.*

Proof. (i) This is easily seen.

(ii) Since the algebra $\mathrm{Hom}_R(D, A/\sqrt{I}) \simeq \mathrm{Hom}_R(D, A)/\mathrm{Hom}_R(D, \sqrt{I})$ is reduced, we have $\mathrm{Hom}_R(D, \sqrt{I})$ is a radical ideal of $\mathrm{Hom}_R(D, A)$. Hence its pull-back $\rho_A^{-1}(\mathrm{Hom}_R(D, \sqrt{I}))$ is also a radical ideal. By part (i), it includes I. On the other hand, $\rho_A^{-1}(\mathrm{Hom}_R(D, \sqrt{I}))$ is included in $\sqrt{I}$. Therefore $\rho_A^{-1}(\mathrm{Hom}_R(D, \sqrt{I})) = \sqrt{I}$.

(iii) Since $\mathrm{Hom}_R(D^1, A/P) \simeq \mathrm{Hom}_R(D^1, A)/\mathrm{Hom}_R(D^1, P)$ is a domain, $\mathrm{Hom}_R(D^1, P)$ is a prime ideal. Thus its pull-back $(\rho_A^1)^{-1}(\mathrm{Hom}_R(D^1, P))$ is also prime. □

Let K be a D-module algebra and $\Omega(K)$ the 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 3.3.3. *Suppose that K is noetherian as a ring and simple as a D-module algebra. Then $\Omega(K)$ is a finite set.*

(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 $\rho : K \to \mathrm{Hom}_R(D^1, K)$ be the algebra map associated with the D^1-module algebra structure on K. Put $P' = \rho^{-1}(\mathrm{Hom}_R(D^1, P))$. By Lemma 3.3.2 (iii), P' is a D^1-stable prime ideal included in P. Then we have $P = P'$ by the minimality of P. Hence P is D^1-stable. (This also follows from [28, Theorem 5.9 (2)].)

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 $g^{-1}P$, we have $P = J$ $(= g^{-1}P)$. Thus K/P is a simple $D(G_{\Omega(K)})$-module algebra.

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

$$\bigcap_{g \in G} gP = \bigcap_{Q \in \Omega(K)} Q = 0, \tag{3.7}$$

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 $G/G_P \xrightarrow{\sim} \Omega(K)$. If Q and Q' in $\Omega(K)$ are distinct, then $(Q \subsetneq)\ Q + Q' = K$, by (ii). This together with (3.7) proves that the natural map gives an isomorphism,

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

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

For a commutative ring K in general, we say that K is *total* iff every non-zero divisor in K is invertible.

Corollary 3.3.4. *Let K be a noetherian simple D-module algebra as above. Then the following are equivalent.*

(a) *K is total;*

(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 3.2.4. □

Definition 3.3.5. A D-module algebra K is said to be *AS* iff it is artinian and simple. By the corollary above, this is equivalent to that K is total, noetherian and simple.

For later use we prove some results. The following lemma is a particular case of [28, Theorem 3.4].

Lemma 3.3.6. *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. Let $\rho : A \to \mathrm{Hom}_R(D, A) \subset \mathrm{Hom}_R(D, T^{-1}A)$ be the algebra map associated with the D-module algebra structure on A. For each $t \in T$, we see $\rho(t)(g) = g(t)$ are invertible in $T^{-1}A$ for all $g \in G$. Hence $\rho(t)$ $(t \in T)$ is invertible in $\mathrm{Hom}_R(D, T^{-1}A)$ by [23, Corollary 9.2.4]. This implies that ρ is uniquely extended to an algebra map $\tilde{\rho} : T^{-1}A \to \mathrm{Hom}(D, T^{-1}A)$ so that $\tilde{\rho}(1/t) * \rho(t) = \varepsilon$ $(t \in T)$; cf. the proof of [27, 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 $D \otimes D \to T^{-1}A$, given by $c \otimes d \mapsto cd(1/t)$ and $c \otimes d \mapsto c(d(1/t))$ coincide, being the convolution-inverse of $c \otimes d \mapsto cdt$.

For convenience, we describe how to extend the action of D explicitly. Let $t \in T$. The action of D on $1/t$ is given by:

$$\begin{aligned} g(1/t) &= 1/g(t) \qquad (g \in G), \\ d(1/t) &= \frac{\varepsilon(d)}{t} - \frac{dt - \varepsilon(d)t}{t^2} + \frac{1}{t^3}\sum_{(d)}(d_{(1)}t - \varepsilon(d_{(1)})t)(d_{(2)}t - \varepsilon(d_{(2)})t) \\ &\quad - \frac{1}{t^4}\sum_{(d)}(d_{(1)}t - \varepsilon(d_{(1)})t)(d_{(2)}t - \varepsilon(d_{(2)})t)(d_{(3)}t - \varepsilon(d_{(3)})t) + \cdots \qquad (d \in D^1). \end{aligned}$$

We observe that the right hand side of $d(1/t)$ $(d \in D^1)$ in the equation is a finite sum by the coradical filtration; see the proof of [23, Lemma 9.2.3] or [16, Lemma 5.2.10]. □

Lemma 3.3.7. *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

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

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

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 3.3.3 (i), we have those elements $x, g_1x, \dots, g_rx$ 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 $\mathrm{supp}(e) = \mathrm{supp}(x)$. By the minimality of the support, each non-zero element in eK has $\mathrm{supp}(x)$ as its support, and hence has an inverse in eK, just as x above. We have $K = \prod_{i=1}^r g_ieK$, the direct product of the fields g_ieK; this proves the lemma. □

Corollary 3.3.8. *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:* $\mathrm{supp}(x) = \Omega(L)$ *(see (3.8)).*

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

(ii) Let $\rho_L : L \to \mathrm{Hom}(D, L)$ be the algebra map associated to the D-module algebra structure on L. It restricts to $\rho : A \to \mathrm{Hom}(D, A)$ associated to A. If $t \in T$, $\rho_L(1/t)$ is the inverse of $\rho(t)$ in $\mathrm{Hom}(D, L)$, and hence is contained in $\mathrm{Hom}(D, T^{-1}A)$ by the proof of Lemma 3.3.6. This implies that K $(= T^{-1}A)$ is a D-module subalgebra of L. K is AS by Lemma 3.3.7. $\square$

3.4. The Sweedler's correspondence theorem

Let $K \subset A$ be an inclusion of D-module algebras. Then $A \otimes_K A$ has a coalgebra structure in the symmetric tensor category $({}_A({}_D\mathcal{M})_A, \otimes_A, A)$ given by

$$\Delta : A \otimes_K A \to (A \otimes_K A) \otimes_A (A \otimes_K A), \quad a \otimes b \mapsto (a \otimes 1) \otimes (1 \otimes b),$$
$$\varepsilon : A \otimes_K A \to A, \quad a \otimes b \mapsto ab.$$

In particular $A \otimes_K A$ is an *A-coring* (or a coalgebra in $({}_A\mathcal{M}_A, \otimes_A, A)$); see [24]. The next theorem is an analogy of the Sweedler's correspondence theorem [24, Theorem 2.1] on AS D-module algebras, which play a key role to obtain the Galois correspondence later.

Theorem 3.4.1. *Let $K \subset L$ be an inclusion of AS D-module algebras. Let $\mathcal{C}_{L/K}$ be the set of all D-stable coideals of $L \otimes_K L$ and $\mathcal{A}_{L/K}$ the set of all intermediate AS D-module algebras of L/K.*

(i) *For $M \in \mathcal{A}_{L/K}$, we have $J_M := \mathrm{Ker}(L \otimes_K L \twoheadrightarrow L \otimes_M L) \in \mathcal{C}_{L/K}$.*

(ii) *For $J \in \mathcal{C}_{L/K}$, let $\pi : L \otimes_K L \twoheadrightarrow L \otimes_K L/J$ be the canonical surjection. Then $M_J := \{a \in L \mid a\pi(1 \otimes 1) = \pi(1 \otimes 1)a\} \in \mathcal{A}_{L/K}$.*

(iii) *The correspondence*

$$\begin{array}{ccc} \mathcal{C}_{L/K} & \leftrightarrow & \mathcal{A}_{L/K} \\ J & \to & M_J \\ J_M & \leftarrow & M \end{array}$$

is bijective.

Proof. (i) Both $L \otimes_K L$ and $L \otimes_M L$ are coalgebras in $({}_L({}_D\mathcal{M})_L, \otimes_L, L)$ and obviously $L \otimes_K L \twoheadrightarrow L \otimes_M L$ is a D-linear L-coring map. Hence its kernel J_M is a D-stable coideal of $L \otimes_K L$.

(ii) We easily see that M_J is a subalgebra of L which contains K. For any $d \in D$ and $a \in M_J$, we have $d(a)\pi(1 \otimes 1) = d(a\pi(1 \otimes 1)) = d(\pi(1 \otimes 1)a) = \pi(1 \otimes 1)d(a)$. Thus M_J is a D-module subalgebra of L. Let t be a non-zero divisor in M_J. By Corollary 3.3.8 (i), t is invertible in L. We see $t^{-1}\pi(1 \otimes 1) = t^{-1}\pi(1 \otimes 1)tt^{-1} = t^{-1}t\pi(1 \otimes 1)t^{-1} = \pi(1 \otimes 1)t^{-1}$ and hence $t^{-1} \in M_J$. This implies that M_J is total. Therefore M_J is an intermediate AS D-module algebra of L/K by Lemma 3.3.7.

(iii) Take an $M \in \mathcal{A}_{L/K}$. For all $a \in M$, we have $a \otimes 1 - 1 \otimes a \in J_M$. Then $M \subset M_{J_M}$. By the definition of M_{J_M}, one sees $M_{J_M} \otimes_M M_{J_M} \simeq M_{J_M} \otimes_M M$. Since M_{J_M} is an $M\#D$-module, it is a free M-module (see Corollary 3.3.4). Hence $M_{J_M} = M$.

Conversely, take $J \in \mathcal{C}_{L/K}$. Let $\xi : L \otimes_{M_J} L \to L \otimes_K L/J$, $a \otimes b \mapsto a\pi(1 \otimes 1)b$, which is a surjective D-linear L-coring map. Then we have $J_{M_J} \subset J$ by chasing the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & J_{M_J} & \longrightarrow & L \otimes_K L & \longrightarrow & L \otimes_{M_J} L & \longrightarrow & 0 \qquad \text{(exact)} \\
 & & & & \| & & \downarrow{\scriptstyle \xi} & & \\
0 & \longrightarrow & J & \longrightarrow & L \otimes_K L & \longrightarrow & L \otimes_K L/J & \longrightarrow & 0 \qquad \text{(exact)}.
\end{array}$$

If we prove that ξ is injective, then $J = J_{M_J}$ follows.

For a fixed $P \in \Omega(M_J)$, put $M' = M_J/P$ $(= \Psi_{G_P}(M_J))$, $L' = L/PL$ $(= \Psi_{G_P}(L))$, and $C = \Psi_{G_P}(L \otimes_K L/J) = (L \otimes_K L/J)e_1 = e_1(L \otimes_K L/J)e_1$ (where $e_1 \in M_J$ is the primitive idempotent such that $M' = M_J e_1$). Then C is a coalgebra in $({}_{L'}({}_{D(G_P)}\mathcal{M})_{L'}, \otimes_{L'}, L')$ by Corollary 3.2.5. It suffices to prove that $\xi' = \Psi_{G_P}(\xi) : L' \otimes_{M'} L' \to C$ is injective.

Regarding C merely as an L'-coring, let $\mathfrak{A}$ be the category of right C-comodules in $({}_{L'}\mathcal{M}_{L'}, \otimes_{L'}, L')$. Then $\mathfrak{A}$ is an abelian category since C is a left free L'-module. L' has a natural C-comodule structure given by

$$\lambda : L' \to L' \otimes_{L'} C \simeq C, \quad a \mapsto \pi(1 \otimes 1)a \quad (= e_1\pi(1 \otimes 1)e_1 a).$$

We see $\mathrm{End}_{\mathfrak{A}}(L') \xrightarrow{\sim} M'$, $f \mapsto f(1)$ is an algebra isomorphism. ($f \in \mathrm{End}_{L'}(L')$ is a C-comodule map iff $f(1)\pi(1 \otimes 1) = \pi(1 \otimes 1)f(1)$.) On the other hand, $\mathrm{Hom}_{\mathfrak{A}}(L', C) \xrightarrow{\sim} L'$, $f \mapsto (\varepsilon \circ f)(1)$ is an M'-module isomorphism whose inverse is given by $a \mapsto [b \mapsto a\pi(1 \otimes 1)b]$. Indeed, for $f \in \mathrm{Hom}_{\mathfrak{A}}(L', C)$,

$$\begin{aligned}
&(\varepsilon \circ f)(1)\pi(1 \otimes 1)b = (\varepsilon \circ f)(1)\lambda(b) = (\varepsilon \circ f)(1)\sum_{(b)} b_{(0)} \otimes b_{(1)} \\
= &\sum_{(b)} (\varepsilon \circ f)(b_0) \otimes b_{(1)} = ((\varepsilon \otimes \mathrm{id}) \circ (f \otimes \mathrm{id}))(\lambda(b)) = (\varepsilon \otimes \mathrm{id})(\Delta_C(f(b))) = f(b).
\end{aligned}$$

We will show that L' is simple in $\mathfrak{A}$, concluding that ξ' is injective by Proposition 3.1.1. Every simple subobject of L' is of the form eL', where e is an idempotent of L'. Since λ is $D(G_P)$-linear, we see that $g(eL')$ is also a simple object for each $g \in G$. Each $g(eL')$ coincides or trivially intersects with eL' since $g(eL') \cap eL'$ is also a right C-comodule. It follows from Proposition 3.3.3 (i) that L' is semisimple in $\mathfrak{A}$. But the endomorphism ring $\mathrm{End}_{\mathfrak{A}}(L') \simeq M'$ is a field. This implies that L' is a simple object in $\mathfrak{A}$. $\square$

Example 3.4.2. Let $R = \mathbb{Q}$ and $D = \mathbb{Q}[\tau, \tau^{-1}]$, the ring of linear difference operators. Take $\alpha = \{(\frac{1+\sqrt{5}}{2})^n\} \in \mathcal{S}_{\mathbb{C}}$ as in Introduction. Then $\mathbb{Q} = \mathbb{Q}(1,1) \subset L = \mathbb{Q}(\sqrt{5}, \alpha) \times \mathbb{Q}(\sqrt{5}, \alpha)$ (where $\tau(1,0) = (0,1)$, $\tau(0,1) = (1,0)$, $L^D = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sqrt{5})(1,1))$ is an inclusion of AS D-module algebras. Write $e_1 = (1,0), e_2 = (0,1) \in L$. Then $\mathcal{A}_{L/\mathbb{Q}}$ and $\mathcal{C}_{L/\mathbb{Q}}$ correspond as the following:

$\mathcal{A}_{L/\mathbb{Q}}$	$\mathcal{C}_{L/\mathbb{Q}}$
L	$\mathrm{Span}_{L,L}\{\sqrt{5} \otimes 1 - 1 \otimes \sqrt{5},\ e_1 \otimes e_2,\ e_2 \otimes e_1,\ \alpha \otimes 1 - 1 \otimes \alpha\}$
$\mathbb{Q}(\sqrt{5}, \alpha)$	$\mathrm{Span}_{L,L}\{\sqrt{5} \otimes 1 - 1 \otimes \sqrt{5},\ \alpha \otimes 1 - 1 \otimes \alpha\}$
$\mathbb{Q}(\sqrt{5}) \times \mathbb{Q}(\sqrt{5})$	$\mathrm{Span}_{L,L}\{e_1 \otimes e_2,\ e_2 \otimes e_1,\ \sqrt{5} \otimes 1 - 1 \otimes \sqrt{5}\}$
$\mathbb{Q}(\alpha)$	$\mathrm{Span}_{L,L}\{\alpha \otimes 1 - 1 \otimes \alpha\}$
$\mathbb{Q}(\sqrt{5})$	$\mathrm{Span}_{L,L}\{\sqrt{5} \otimes 1 - 1 \otimes \sqrt{5}\}$
$\mathbb{Q} \times \mathbb{Q}$	$\mathrm{Span}_{L,L}\{e_1 \otimes e_2,\ e_2 \otimes e_1\}$
$\mathbb{Q}$	0

We will see that $L/\mathbb{Q}$ is not a Picard-Vessiot extension but $L/\mathbb{Q}(\sqrt{5})$ is.

3.5. Galois correspondence for Picard-Vessiot extensions

Let $K \subset A$ be an inclusion of D-module algebras. Then $A \otimes_K A$ has an algebra structure naturally and become a D-module algebra since D is cocommutative. Thus $(A \otimes_K A)^D$ is a K^D-subalgebra of $A \otimes_K A$.

Definition 3.5.1. Let $K \subset L$ be an inclusion of AS D-module algebras. 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 3.5.2. *Let L/K be a PV extension of AS D-module algebras and take A, H as in the 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* A*-coring structure maps* Δ, ε *of* $A \otimes_K A$ *induce* k*-algebra maps* $\Delta_H : H \to H \otimes_k H$, $\varepsilon_H : H \to k$. *Then* $(H, \Delta_H, \varepsilon_H)$ *becomes a commutative Hopf algebra over* k. *The antipode is induced from the twist map* $\mathrm{tw} : A \otimes_K A \to A \otimes_K A$, $a \otimes b \mapsto b \otimes a$.

(iii) *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* [16, 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. A Hopf algebra structure on H *with this property is unique.*

(iv) *Such an algebra* A *that satisfies the condition (b) above is unique.*

Proof. (i) By Corollary 3.1.4, the natural map $L \otimes_k (L \otimes_K A)^D \to L \otimes_K A$ is injective. Since the map μ is its restriction, it is injective. On the other hand, μ is surjective by the condition (b). Note that this can be uniquely extended to an isomorphism $L \otimes_k H \xrightarrow{\sim} L \otimes_K A$.

(ii) Since $A^D = k$ by the condition (a), ε maps H into k. The twofolds of μ:

$$ \varphi : A \otimes_k H \otimes_k H \xrightarrow{\mu \otimes \mathrm{id}} A \otimes_K A \otimes_k H \xrightarrow{\mathrm{id} \otimes \mu} A \otimes_K A \otimes_K A $$

is a D-linear isomorphism. This induces an algebra isomorphism $\varphi_1 := \mathrm{id} \otimes \mu|_{H \otimes_k H} : H \otimes_k H \xrightarrow{\sim} (A \otimes_K A \otimes_K A)^D$. Similarly the threefolds of μ induces an algebra isomorphism $\varphi_2 : H \otimes_k H \otimes_k H \xrightarrow{\sim} (A \otimes_K A \otimes_K A \otimes_K A)^D$. Since $\Delta : A \otimes_K A \to (A \otimes_K A) \otimes_A (A \otimes_K A) \simeq A \otimes_K A \otimes_K A$ maps H into $(A \otimes_K A \otimes_K A)^D$, a k-algebra map $\Delta_H : H \to H \otimes_k H$ is induced by $\Delta_H = \varphi_1^{-1} \circ \Delta|_H$. We see

$$ \begin{aligned} \varphi_2 \circ (\Delta_H \otimes \mathrm{id}_H) \circ \Delta_H &= (\Delta \otimes \mathrm{id}) \circ \varphi_1 \circ \Delta_H = (\Delta \otimes \mathrm{id}_A) \circ \Delta|_H, \\ \varphi_2 \circ (\mathrm{id}_H \otimes \Delta_H) \circ \Delta_H &= (\mathrm{id} \otimes \Delta) \circ \varphi_1 \circ \Delta_H = (\mathrm{id}_A \otimes \Delta) \circ \Delta|_H. \end{aligned} $$

Then we have $(\Delta_H \otimes \mathrm{id}) \circ \Delta_H = (\mathrm{id} \otimes \Delta_H) \circ \Delta_H$ by the coassociativity of Δ. The counitary property is easily seen. Therefore $(H, \Delta_H, \varepsilon_H)$ is a commutative bialgebra. Since D is cocommutative, tw maps H into H. Put $S = \mathrm{tw}|_H$. For $w = \sum_i (a_i \otimes a_i') \otimes (b_i' \otimes b_i) \in H \otimes_k H$, we see

$$ \varphi_1(w) = \sum_i a_i \otimes a_i' b_i' \otimes b_i, \quad m((\mathrm{id} \otimes S)(w)) = \sum_i a_i b_i \otimes a_i' b_i' $$

where m denotes the multiplication of H. Thus, for $h = \sum_i a_i \otimes b_i \in H$,

$$ m((\mathrm{id} \otimes S)(\Delta_H(h))) = m((\mathrm{id} \otimes S)(\varphi_1^{-1}(\sum_i a_i \otimes 1 \otimes b_i))) = \sum_i a_i b_i \otimes 1. $$

This implies $\mathrm{id} * S = m \circ (\mathrm{id} \otimes S) \circ \Delta_H = u\varepsilon$ where $u : k \to H$ is the unit map of H. We have $S * \mathrm{id} = u\varepsilon$ similarly. Therefore S is the antipode of H.

(iii) We see

$$(\varphi \circ (\theta \otimes \mathrm{id}) \circ \theta)(a) = 1 \otimes 1 \otimes a = (\Delta \circ \mu \circ \theta)(a) = (\varphi \circ (\mathrm{id} \otimes \Delta_H) \circ \theta)(a)$$

for all $a \in A$. Thus we have $(\theta \otimes \mathrm{id}) \circ \theta = (\mathrm{id} \otimes \Delta_H) \circ \theta$. On the other hand,

$$(\mathrm{id} \otimes \varepsilon_H) \circ \theta = \varepsilon \circ \mu \circ \theta = \mathrm{id}.$$

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

(iv) This follows in the same way as [27, Lemma 2.5]. We include the proof for convenience. If A, B satisfy the condition (b), then also AB satisfy it. Thus we may assume $A \subset B$. Put $H_A = (A \otimes_K A)^D$, $H_B = (B \otimes_K B)^D$, the corresponding Hopf algebras. Then H_A is a Hopf subalgebra of H_B. Hence H_B/H_A is a faithfully flat extension (see [25, Theorem 3.1] or [29, Ch. 14]). The extension $(L \otimes_K B)/(L \otimes_K A)$ is identified with $(L \otimes_k H_B)/(L \otimes_k H_A)$ through the μ-isomorphism. It follows that B/A is a faithfully flat extension since L is a free K-module. Hence $aA = aB \cap A$ for all $a \in A$ since the canonical map $A/aA \to B \otimes_A (A/aA) \simeq B/aB$ is injective. For any $b \in B$, there exists a non-zero divisor $a \in A$ such that $ab \in A$. Since $ab \in aB \cap A = aA$ and since a is a non-zero divisor, $b \in A$ follows. Therefore we have $A = B$. □

Definition 3.5.3. A (resp., H) is called *the principal algebra* (resp., *the Hopf algebra*) *for* L/K. To indicate these we say that $(L/K, A, H)$ is a PV extension. The associated affine group scheme $\mathbf{G}(L/K) := \mathrm{Spec}H$ is called *the PV group scheme for* L/K.

Theorem 3.5.4. *Let L/K be a PV extension of AS D-module algebras with the Hopf algebra H. Let $\mathcal{A}_{L/K}$ be the set of intermediate AS D-module algebras of L/K and $\mathcal{HI}_H$ the set of all Hopf ideals of H. Then $\mathcal{A}_{L/K}$ and $\mathcal{HI}_H$ correspond bijectively as follows:*

$$\mathcal{A}_{L/K} \to \mathcal{HI}_H, \quad M \mapsto H \cap \mathrm{Ker}(L \otimes_K L \to L \otimes_M L),$$
$$\mathcal{HI}_H \to \mathcal{A}_{L/K}, \quad I \mapsto \{x \in L \mid x \otimes 1 - 1 \otimes x \in I \cdot (L \otimes_K L)\}.$$

This theorem is obtained as the composite of 1-1 correspondences given by Theorem 3.4.1 and the next proposition. For a commutative algebra A (resp. a D-module algebra B), let $\mathcal{I}(A)$ (resp. $\mathcal{I}_D(B)$) denote the set of all ideals of A (resp. D-stable ideals of B).

Proposition 3.5.5. *Let $(L/K, A, H)$ be a PV extension.*

(i) $\mathcal{I}(H)$ *and* $\mathcal{I}_D(L \otimes_K L)$ *correspond bijectively as follows:*

$$\mathcal{I}(H) \to \mathcal{I}_D(L \otimes_K L), \quad I \mapsto I \cdot (L \otimes_K L),$$
$$\mathcal{I}_D(L \otimes_K L) \to \mathcal{I}(H), \quad J \mapsto J \cap H.$$

(ii) *Under the correspondence,* J *is a* D*-stable coideal iff* I *is a Hopf ideal.*

Proof. This follows in the same way as [27, Proposition 2.6]. We include the proof for convenience.

(i) Since L is the total quotient ring of A, we have $\mathcal{I}_D(L \otimes_K L) \subset \mathcal{I}_D(A \otimes_K A)$. Furthermore, $\mathcal{I}_D(L \otimes_K A) \cap \mathcal{I}_D(A \otimes_K L) = \mathcal{I}_D(L \otimes_K L)$ in $\mathcal{I}_D(A \otimes_K A)$. Considering the μ-isomorphism, we claim the map

$$\mathcal{I}(H) \to \mathcal{I}_D(A \otimes_k H) \xrightarrow{\sim} \mathcal{I}_D(A \otimes_K A), \quad I \mapsto A \otimes_k I \mapsto I \cdot (A \otimes_K A)$$

is injective with the image $\mathcal{I}_D(L \otimes_k H) \simeq \mathcal{I}_D(L \otimes_K A)$. The injectivity is clear. Since $A \otimes_k I = (L \otimes_k I) \cap (A \otimes_k H)$, the image is contained in $\mathcal{I}_D(L \otimes_k H)$. Then it suffices to prove that every D-stable ideal of $L \otimes_k H$ is written as $L \otimes_k I$ by some $I \in \mathcal{I}(H)$. Let $\mathfrak{a} \subset L \otimes_k H$ be a D-stable ideal and take the canonical map $\varphi : H \xrightarrow{\sim} (L \otimes_k H)^D \twoheadrightarrow ((L \otimes_k H)/\mathfrak{a})^D$. Put $I = \operatorname{Ker} \varphi = \mathfrak{a} \cap H$, an ideal of H. Since $L \otimes_k ((L \otimes_k H)/\mathfrak{a})^D \to (L \otimes_k H)/\mathfrak{a}$ is injective (Corollary 3.1.4), we have $\mathfrak{a} = L \otimes_k I$ by chasing the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & L \otimes_k I \arrow[r] & L \otimes_k H \arrow[r, "\mathrm{id}\otimes\varphi"] \arrow[d, equal] & L \otimes_k ((L \otimes_k H)/\mathfrak{a})^D \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathfrak{a} \arrow[r] & L \otimes_k H \arrow[r] & (L \otimes_k H)/\mathfrak{a} \arrow[r] & 0.
\end{tikzcd}$$

Then the claim is proved. By symmetry, we see the image of $\mathcal{I}(H) \to \mathcal{I}_D(A \otimes_K A)$ is also equal to $\mathcal{I}_D(A \otimes_K L)$. It follows $\mathcal{I}_D(L \otimes_K A) = \mathcal{I}_D(A \otimes_K L) = \mathcal{I}_D(L \otimes_K L)$ in $\mathcal{I}_D(A \otimes_K A)$, proving (i).

(ii) By the similar discussion to (i), we have that $\mathcal{I}(H \otimes_k H)$ and $\mathcal{I}_D(L \otimes_K L \otimes_K L)$ correspond bijectively. If $I \leftrightarrow J$ in (i), then $I \otimes_k H \leftrightarrow J \otimes_K L$ and $H \otimes_k I \leftrightarrow L \otimes_K J$. Therefore, $\Delta_H(I) \subset I \otimes_k H + H \otimes_k I$ iff $\Delta J \subset J \otimes_K L + L \otimes_K J$. On the other hand, $\operatorname{Ker}((L \otimes_K L) \otimes_L (L \otimes_K L) \to (L \otimes_K L/J) \otimes_L (L \otimes_K L/J)) = J \otimes_L (L \otimes_K L) + (L \otimes_K L) \otimes_L J = J \otimes_K L + L \otimes_K J$ holds since J, $L \otimes_K L$, and $J \otimes_K L/J$ are free L-modules. It follows that I is a biideal of H iff J is a D-stable coideal of $L \otimes_K L$. It is known that every biideal of a commutative Hopf algebra over a field is a Hopf ideal (see [17, Theorem 1 (iv)]). □

Example 3.5.6. In Example 3.4.2, if we put $K = \mathbb{Q}(\sqrt{5})$, then L/K is a PV extension. The principal algebra and the Hopf algebra are given by $A = K[\alpha, \alpha^{-1}] \times K[\alpha, \alpha^{-1}]$ and

$H = K[g_1, g_2]$ with grouplikes $g_1 = \alpha \otimes \alpha^{-1}$, $g_2 = (e_1 - e_2) \otimes (e_1 - e_2)$. In this case, $\mathcal{A}_{L/K}$, $\mathcal{C}_{L/K}$, $\mathcal{HI}_H$ correspond as follows:

$\mathcal{A}_{L/K}$	$\mathcal{C}_{L/K}$	$\mathcal{HI}_H$
L	$\mathrm{Span}_{L,L}\{e_1 \otimes e_2,\ e_2 \otimes e_1,\ \alpha \otimes 1 - 1 \otimes \alpha\}$	$H^+ = \langle g_1 - 1, g_2 - 1\rangle$
$K(\alpha)$	$\mathrm{Span}_{L,L}\{\alpha \otimes 1 - 1 \otimes \alpha\}$	$\langle g_1 - 1\rangle$
$K \times K$	$\mathrm{Span}_{L,L}\{e_1 \otimes e_2,\ e_2 \otimes e_1\}$	$\langle g_2 - 1\rangle$
K	0	0

Proposition 3.5.7. *Let $(L/K, A, H)$ be a PV extension. Suppose $\mathcal{A}_{L/K} \ni M \leftrightarrow I \in \mathcal{HI}_H$ in Theorem 3.5.4.*

(i) *$(L/M, AM, H/I)$ is a PV extension.*

(ii) *$A^{\mathrm{co}\,H/I} = \{a \in A \mid \theta(a) - a \otimes 1 \in A \otimes_k I\} = A \cap M$, and the μ-isomorphism $A \otimes_k H \xrightarrow{\sim} A \otimes_K A$ induces an isomorphism $A \otimes_k H^{\mathrm{co}\,H/I} \xrightarrow{\sim} A \otimes_K (A \cap M)$.*

(iii) *M is the total quotient ring of $A \cap M$.*

Proof. (i) We have an isomorphism $L \otimes_k H/I \xrightarrow{\bar{\mu}} L \otimes_M AM$ by considering the following diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L \otimes_k I & \longrightarrow & L \otimes_k H & \longrightarrow & L \otimes_k H/I & \longrightarrow & 0 \\
 & & \big\downarrow{\scriptstyle \mu} & & \big\downarrow{\scriptstyle \mu} & & \big\downarrow{\scriptstyle \bar{\mu}} & & \\
0 & \longrightarrow & I \cdot (L \otimes_K A) & \longrightarrow & L \otimes_K A & \longrightarrow & L \otimes_M AM & \longrightarrow & 0.
\end{array}$$

Restrict the diagram as

$$\begin{array}{ccccccccc}
0 & \longrightarrow & AM \otimes_k I & \longrightarrow & AM \otimes_k H & \longrightarrow & AM \otimes_k H/I & \longrightarrow & 0 \\
 & & \big\downarrow{\scriptstyle \mu} & & \big\downarrow{\scriptstyle \mu} & & \big\downarrow{\scriptstyle \bar{\mu}} & & \\
0 & \longrightarrow & I \cdot (AM \otimes_K A) & \longrightarrow & AM \otimes_K A & \longrightarrow & AM \otimes_M AM & \longrightarrow & 0.
\end{array}$$

Since $AM \otimes_K A = (AM \otimes_K K) \cdot H$, we have $AM \otimes_M AM = AM \cdot (AM \otimes_M AM)^D$ through the surjection $AM \otimes_K A \to AM \otimes_M AM$. On the other hand, $\bar{\mu}$ induces an isomorphism $H/I \xrightarrow{\sim} (AM \otimes_M AM)^D$ of Hopf algebras.

(ii) This follows by considering the next diagram:

$$\begin{array}{ccccccc}
0 & \longrightarrow & A \otimes_K (A \cap M) & \longrightarrow & A \otimes_K A & \rightrightarrows & A \otimes_K AM \otimes_M AM \\
 & & \uparrow & & \| & & \uparrow \\
0 & \longrightarrow & A \otimes_K A^{\mathrm{co}\,H/I} & \longrightarrow & A \otimes_K A & \rightrightarrows & A \otimes_K A \otimes_k H/I \\
 & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & A \otimes_k H^{\mathrm{co}\,H/I} & \longrightarrow & A \otimes_k H & \rightrightarrows & A \otimes_k H \otimes_k H/I.
\end{array}$$

(iii) Let M' be the total quotient ring of $A \cap M$ realized in L. Then M' is an intermediate AS D-module algebra of L/K which is included in M by Corollary 3.3.8. Let I' be the Hopf ideal of H corresponding to M'. Since $M' \cap A \supset M \cap A$, we have $H^{\mathrm{co}\, H/I'} \supset H^{\mathrm{co}\, H/I}$ by part (ii). Define the maps $\xi_1 : H \to H \otimes_k H/I'$ and $\xi_2 : H \to H \otimes_k H/I$ given by $h \mapsto \sum_{(h)} h_{(1)} \otimes \bar{h}_{(2)} - h \otimes \bar{1}$. Then we have a surjection $\operatorname{Im} \xi_2 \twoheadrightarrow \operatorname{Im} \xi_1$. Since this induces a surjection $(H/I)^+ \twoheadrightarrow (H/I')^+$, we have a Hopf algebra surjection $H/I \twoheadrightarrow H/I'$. Thus $I' \supset I$, which implies $M' \supset M$. $\square$

Let H be a commutative Hopf algebra over k. It is known that normal Hopf ideals I of H and Hopf subalgebras $H_1 \subset H$ correspond bijectively by $H_1 = H^{\mathrm{co}\, H/I} = {}^{\mathrm{co}\, H/I}H$ and $I = HH_1^+$ (see [25]). Let (V, λ) be a right H-comodule in general. If we put $V_1 = \lambda^{-1}(V \otimes_k H_1)$ $(= V^{\mathrm{co}\, H/I})$, then we have $\lambda(V_1) \subset V_1 \otimes_k H_1$. Indeed, write $\lambda(v) = \sum_i v_i \otimes h_i \in V \otimes_k H_1$ for $v \in V_1$, where h_i are k-linearly independent. Then

$$\sum_i \sum_{(v_i)} (v_i)_{(0)} \otimes (v_i)_{(1)} \otimes h_i = \sum_i \sum_{(h_i)} v_i \otimes (h_i)_{(1)} \otimes (h_i)_{(2)} \in V \otimes_k H_1 \otimes_k H_1.$$

This implies $v_i \in V_1$. As in [27, Theorem 2.9], we have the following proposition.

Proposition 3.5.8. *Let $(L/K, A, H)$ be a PV extension and $H_1 \subset H$ a Hopf subalgebra. Put $I = HH_1^+$ and $A_1 = \theta^{-1}(A \otimes_k H_1) = A^{\mathrm{co}\, H/I}$. Let L_1 be the total quotient ring of A_1 so that L_1 is an intermediate AS D-module algebra of L/K.*

(i) *$(L_1/K, A_1, H_1)$ is a PV extension.*

(ii) *I is the Hopf ideal of H which corresponds to L_1.*

(iii) *$H_1 \mapsto L_1$ gives a 1-1 correspondence between the Hopf subalgebras of H and the intermediate AS D-module algebras which are PV extensions over K.*

Proof. (i) Since $\theta(A_1) \subset A_1 \otimes_k H_1$, we have $\mu(A_1 \otimes_k H_1) \supset A_1 \otimes_K A_1$. Consider $A \otimes_K A$ as a right H-comodule by the structure map $\mathrm{id} \otimes \theta$. Then the inclusion $H \hookrightarrow A \otimes_K A$ is an H-comodule map; recall that, for $h = \sum_i a_i \otimes_K b_i \in H = (A \otimes_K A)^D$,

$$\Delta(h) = \sum_i a_i \otimes_K \mu^{-1}(1 \otimes_K b_i) = \sum_i a_i \otimes_K \theta(b_i).$$

Thus $H_1 \subset A \otimes_K \theta^{-1}(A \otimes_k H_1) = A \otimes_K A_1$. Also we have $H_1 = S(H_1) \subset \mathrm{tw}(A \otimes_K A_1) = A_1 \otimes_K A$. Hence $H_1 \subset A_1 \otimes_K A_1$ and so $\mu(A_1 \otimes_k H_1) \subset A_1 \otimes_K A_1$. This implies that $\mu : A \otimes_k H \xrightarrow{\sim} A \otimes_K A$ induces a D-linear isomorphism $A_1 \otimes_k H_1 \xrightarrow{\sim} A_1 \otimes_K A_1$. Therefore $H_1 = (A_1 \otimes_K A_1)^D$ and $A_1 \otimes_K A_1 = A_1 \cdot H_1$.

(ii) This follows from Proposition 3.5.7.

(iii) Let L_1 be an intermediate AS D-module algebra of L/K such that $(L_1/K, A_1, H_1)$ is a PV extension. Since $A \otimes_K A = A \cdot H$ and $A_1 \otimes_K A_1 = A_1 \cdot H_1$, we have $A_1A \otimes_K A_1A = A_1A \cdot H_1H$. This implies that A_1A is the principal algebra for L/K and hence $A_1A = A$ by Proposition 3.5.2 (iv). Thus $A_1 \subset A$ and $H_1 \subset H$, a Hopf subalgebra. Since the μ-isomorphism $A_1 \otimes_k H_1 \xrightarrow{\sim} A_1 \otimes_K A_1$ induces a left A-module isomorphism $A \otimes_k H_1 \xrightarrow{\sim} A \otimes_K A_1$, we have $A_1 = \theta^{-1}(A \otimes_k H_1)$. This proves (iii). □

Finally in this section, we prove two important properties on principal algebras which are used later.

Proposition 3.5.9. *Let $(L/K, A, H)$ be a PV extension.*

(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 [27, Theorem 2.11].

Let $0 \neq I \subset A$ be a D-stable ideal. Since $L \otimes_K I \in \mathcal{I}_D(L \otimes_K A)$, there exists an ideal $\mathfrak{a} \in \mathcal{I}(H)$ such that $L \otimes_K I = \mathfrak{a} \cdot (L \otimes_K A)$ by the proof of Proposition 3.5.5 (i). But $IL = L$ since L is simple and hence $L \otimes_K IL = L \otimes_K L$. This implies that the D-stable ideal of $L \otimes_K L$ which corresponds to $\mathfrak{a}$ is $L \otimes_K L$. Thus $\mathfrak{a} = H$. Therefore $L \otimes_K I = H \cdot (L \otimes_K A) = L \otimes_K A$, concluding $I = A$.

(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 $\bigcap_{g \in G/G_{\Omega(L)}} gJ$ is a D-stable ideal in A, and hence is zero by part (i). Since $P \cap A$ is prime, there exists g such that $gJ \subset P \cap A$, and so $P \cap A \subset J \subset g^{-1}P \cap A$. By the minimality of $g^{-1}P \cap A$, we have $P \cap A = J$ $(= g^{-1}P \cap A)$. Similarly we have $J = Q \cap A$, and so $P = Q$. □

3.6. Translation into affine group schemes

For an inclusion of D-module algebras $K \subset A$, let $\mathrm{Aut}_{D,K\text{-alg}}(A)$ denote the group of D-linear K-algebra automorphisms of A. Let $\mathbf{Aut}_{D,K\text{-alg}}(A)$ denote the associated group functor over $k = K^D$; it associates to each commutative k-algebra T the automorphism group $\mathrm{Aut}_{D,K \otimes_k T\text{-alg}}(A \otimes_k T)$, where T is considered as a D-module algebra by the trivial action $dt = \varepsilon(d)t$ $(d \in D,\ t \in T)$. As in [27, Appendix], we have the following:

Theorem 3.6.1. *Let $(L/K, A, H)$ be a PV extension and $\mathrm{G}(L/K) = \mathrm{Spec} H$ the PV group scheme. Then the linear representation $\phi : \mathrm{G}(L/K) \to \mathbf{GL}(A)$ arising from the*

H-comodule structure $\theta : A \to A \otimes_k H$ gives an isomorphism $\mathbf{G}(L/K) \xrightarrow{\sim} \mathbf{Aut}_{D,K\text{-alg}}(A)$ of affine k-group schemes. In particular, $\mathbf{G}(L/K)(k) \simeq \mathrm{Aut}_{D,\,K\text{-alg}}(A) = \mathrm{Aut}_{D,\,K\text{-alg}}(L)$.

Proof. Let T be a commutative k-algebra. For $\alpha \in \mathbf{G}(L/K)(T) = \mathrm{Alg}_k(H,T)$, $\phi_T(\alpha)$ is given by

$$\phi_T(\alpha) : A \otimes_k T \xrightarrow{\sim} A \otimes_k T, \quad a \otimes t \mapsto \sum_{(a)} a_{(0)} \otimes \alpha(a_{(1)})t.$$

We easily see $\phi_T(\alpha) \in \mathrm{Aut}_{D,\,K \otimes_k T\text{-alg}}(A \otimes_k T)$. We will construct the inverse $\psi : \mathbf{Aut}_{D,K\text{-alg}}(A) \to \mathbf{G}(L/K)$. For an element $\beta \in \mathrm{Aut}_{D,\,K \otimes_k T\text{-alg}}(A \otimes_k T)$, let ${}_A\beta$ denote the left A-linear extension of $\beta|_A : A \to A \otimes_k T$. Consider the D-linear A-algebra map

$$A \otimes_k H \xrightarrow{\mu} A \otimes_K A \xrightarrow{{}_A\beta} A \otimes_k T.$$

We see this maps the constants H into T. Then we have a k-algebra map $\psi_T(\beta) := ({}_A\beta \circ \mu)^D \in \mathrm{Alg}_k(H,T) = \mathbf{G}(L/K)(T)$ so that $(\mathrm{id}_A \otimes \psi_T(\beta)) \circ \theta = \beta|_A$. This gives a homomorphism $\psi : \mathbf{Aut}_{D,K\text{-alg}}(A) \to \mathbf{G}(L/K)$. Indeed, for $\beta, \gamma \in \mathrm{Aut}_{D,\,K \otimes_k T\text{-alg}}(A \otimes_k T)$,

$$(\gamma \circ \beta)(a \otimes 1) = \sum_{(a)} \gamma(a_{(0)} \otimes 1)\psi_T(\beta)(a_{(1)}) = \sum_{(a)} a_{(0)} \otimes \psi_T(\gamma)(a_{(1)})\psi_T(\beta)(a_{(2)}) \quad (a \in A).$$

One easily sees $\phi_T \circ \psi_T = \mathrm{id}$. For $\alpha \in \mathbf{G}(L/K)(T)$, we see ${}_A\phi_T(\alpha) = (\varepsilon \otimes \alpha) \circ (\mathrm{id} \otimes \theta)$ where $\varepsilon : A \otimes_K A \to A$, the counit, and hence ${}_A\phi_T(\alpha)|_H = (\varepsilon_H \otimes \alpha) \circ \Delta_H = \alpha$. This implies $\psi_T \circ \phi_T = \mathrm{id}$. □

Theorem 3.5.4 and Proposition 3.5.7, 3.5.8 can be translated as follows.

Theorem 3.6.2. *Let L/K be a PV extension of AS D-module algebras.*

(i) *If M is an intermediate AS D-module algebra of L/K, then L/M is also a PV extension and the PV group scheme $\mathbf{G}(L/M)$ is identified with a closed subgroup scheme of $\mathbf{G}(L/K)$. Then intermediate AS D-module algebras of L/K and closed subgroup schemes of $\mathbf{G}(L/K)$ correspond bijectively by $M \mapsto \mathbf{G}(L/M)$.*

(ii) *Under the correspondence above, M/K is a PV extension iff $\mathbf{G}(L/K) \rhd \mathbf{G}(L/M)$. If this is the case, we have an isomorphism $\mathbf{G}(M/K) \simeq \mathbf{G}(L/K)/\mathbf{G}(L/M)$ of affine group schemes.*

3.7. Copying and interlacing

In this section, we investigate how PV extensions change through the functor Φ and Ψ described in Section 3.2.

First we easily see the following:

Lemma 3.7.1. *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. Then $(L_1/K_1, A_1, H)$ is a PV extension iff $(\Phi(L_1)/\Phi(K_1), \Phi(A_1), H)$ is a PV extension of AS D-module algebras.*

Proof. This follows by Proposition 3.2.5 and Lemma 3.2.6. □

Remark 3.7.2. 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 $K_1 = K/\mathfrak{p}$, $L_1 = L/\mathfrak{p}L = \prod_{i=1}^{r} L/P_i$. 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 by Lemma 3.7.1.

Example 3.7.3. 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 3.2.6 (i). Moreover, $(L/K, L, H)$ is a PV extension with $H = k(G/G_1)^*$, 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 $L \otimes_K L$:

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

Proposition 3.7.4. *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) $A \simeq \Phi(A_1)$.

(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.* [20, 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 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_{p}, then $B \subset H$ is a Hopf subalgebra which is isomorphic to $k(G_{\mathrm{p}}/G_P)^*$, and we have an extension*

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

of Hopf algebras; cf. [20, Corollary 1.17].

Proof of Proposition 3.7.4 (i), (ii), (iii). (i) This follows from Proposition 3.5.9.

(ii) This is easy to see.

(iii) By Proposition 3.5.7 (i), 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 3.7.1. □

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

Lemma 3.7.5. *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. Recall that K can be considered as a D-module subalgebra of $\Phi(K)$ by $K \hookrightarrow \Phi(K)$, $x \mapsto \sum_{g \in G/G_1} g \otimes g^{-1}x$.*

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

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

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,*

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

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) It is easily seen that the map is D^1-linear. For $h \in G$ and $g \in G/G_1$, take $g' \in G/G_1$, $t \in G_1$ such that $hg = g't$. We see that the given map is D-linear by the computation

$$h(a \otimes_K (g \otimes x)) = (ha) \otimes_K (g' \otimes tx) \mapsto g' \otimes (g'^{-1} ha)tx = g' \otimes (tg^{-1}a)tx = h(g \otimes (g^{-1}a)x).$$

The inverse $\Phi(A) \to A \otimes_K \Phi(K)$ is given by $g \otimes a \mapsto (ga) \otimes_K (g \otimes 1)$ $(g \in G/G_1)$.

(ii) This follows from (i) and Lemma 3.2.6 (i).

(iii) Precisely N is the kernel of the natural group homomorphism $G \to \mathfrak{S}(G/G_1)$, where $\mathfrak{S}(G/G_1)$ is the permutation group of G/G_1. Hence the index $[G : N]$ is finite. 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 iff $\sum_{g \in O_i} g \otimes a_g$ is so for each $1 \leq i \leq t$. Fix a coset $g_i G_1$, and suppose that

$$g_i, s_2 g_i, \dots, s_l g_i \quad (s_j \in G_1)$$

represent the G_1-orbit O_i. Then, $\sum_{j=1}^{l} s_j g_i \otimes a_j$ $(s_1 = 1,\ a_j \in F)$ is G_1-invariant iff $s(g_i \otimes a_1) = s_j g_i \otimes a_j$ for every $s \in G_1$, where $s g_i G_1 = s_j g_i G_1$, or $s_j^{-1} s \in S_i$. (The "if" part of this is shown as follows: for each $s \in G_1$, write $s s_j g_i G_1 = s_{\sigma_s(j)} g_i G_1$ $(j = 1, \dots, l)$ where σ_s is a permutation of $\{1, \dots, l\}$. Then we have $s(\sum_{j=1}^{l} s_j g_i \otimes a_j) = \sum_{j=1}^{l} s s_j (g_i \otimes a_1) = \sum_{j=1}^{l} s_{\sigma_s(j)} g_i \otimes a_{\sigma_s(j)} = \sum_{j=1}^{l} s_j g_i \otimes a_j$. In addition, this condition implies $a_1 = \cdots = a_l$ since $s_j(g_i \otimes a_1) = s_j g_i \otimes a_1$.) This is further equivalent to that $a_1 = \cdots = a_l \in F^{g_i^{-1} S_i g_i}$, since we compute

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

□

Proof of Proposition 3.7.4 (iv), (v). By Remark 3.7.2 we may suppose that K is a field, and so $\mathfrak{p} = 0$, $G_\mathfrak{p} = G$.

(iv) By Proposition 3.5.7 (ii), we see that

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

and so

$$B = (A \otimes_K \Phi(K))^D. \tag{3.9}$$

By applying Lemma 3.7.5 to the present situation especially when $G_1 = G_P$, it follows that

$$(A \otimes_K \Phi(K))^D \simeq \sum_{i=1}^{t} (\sum_{g \in O_i} g) \otimes F^{g_i^{-1} S_i g_i}, \tag{3.10}$$

where $F = A_1^{D(N)}$ with $N = G_{\Omega(L)}$; see Proposition 3.3.3. 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 $F^{g_i^{-1} S_i g_i}$ now are finite separable field extensions over k. By (3.9), (3.10), B is a 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

$$\sigma : \Phi(A_1 \otimes_K A_1) = A \otimes_{\hat{K}} A \to A \otimes_K A \tag{3.11}$$

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 [16, Theorem 7.2.2] that

$$B \otimes_k \bar{H} \to H, \quad b \otimes x \mapsto b\sigma^D(x) \tag{3.12}$$

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

(v) If G_P is normal in G, then $G_P = N$, and hence $F = k$ in (3.10). We then see $B = (\Phi(K) \otimes_K \Phi(K))^D$. By Example 3.7.3, $B \subset H$ is a Hopf subalgebra which is isomorphic to $k(G/G_P)^*$. The isomorphism given in (3.12) induces the described extension of Hopf algebras. □

Theorem 3.7.6. *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 3.7.4 that if L/K is PV, the principal 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 (3.11) induces an $\bar{H}$-colinear k-algebra map $\sigma^D : \bar{H} \to (A \otimes_K A)^D$. Again by [16, 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 (3.12). It follows that L/K is a PV extension iff the natural injection

$$A \otimes_k (A \otimes_K \Phi(K))^D \to A \otimes_K \Phi(K) \tag{3.13}$$

is surjective. If G_P is normal in G, then this is surjective since by Example 3.7.3, $A \otimes_k (\Phi(K) \otimes_K \Phi(K))^D \to A \otimes_K \Phi(K)$ is already surjective.

To prove the converse, we may suppose (b) by Proposition 3.7.4 (iii), and that the map given in (3.13) is an isomorphism by the argument above. It follows that

$$\dim_k (A \otimes_K \Phi(K))^D = [G : G_P]. \tag{3.14}$$

If k is separably closed, then $F = k$ in (3.10). The equation (3.14) implies that $(t =)$ $|G_P \backslash G / G_P| = [G : G_P]$, or G_P is normal in G. $\square$

The first half of the theorem above seems new even in the standard PV theory for difference equations; especially this theorem together with Theorem 3.8.7 (and [20, Theorem 3.1]) implies that the conjecture in [20, Ch. 3] is true. As will be seen from the following, the second half does not necessarily hold true unless k is separably closed.

Example 3.7.7. Let $N \subset G_1 \subset G$ be as in Lemma 3.7.5. 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 (3.14) that L/K is a PV extension iff

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

The left-hand side equals

$$\sum_{i=1}^{t} \dim_k F^{g_i^{-1} S_i g_i} \tag{3.15}$$

with the notation in Lemma 3.7.5, 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 (3.15) 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.

For example, let $G = D_3 = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ ($\sigma^3 = 1$, $\tau^2 = 1$, $\sigma\tau = \tau\sigma^2$), $G_1 = \{1, \tau\} \subset G$, and $D = \mathbb{Q}G$. Put $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{-1})$, and consider $G_1 = \mathrm{Gal}(K/k)$. Then G acts on K so that $\sigma a = a$ for all $a \in K$. Take the system of representatives $\{1, \sigma, \sigma^2\}$ for G/G_1 and let $L = \Phi_{G_1}(K) = 1 \otimes K + \sigma \otimes K + \sigma^2 \otimes K$. Then L/K is a PV extension of AS D-module algebras with the Hopf algebra

$$H = \mathbb{Q}[z_1, z_2, z_3]/\langle z_1 + z_2 - 1, z_2^2 - z_2, z_3^2 + z_2, z_2 z_3 - z_3\rangle$$

where $\varepsilon(z_i) = \delta_{1i}$ ($i = 1, 2, 3$) and

$$\begin{aligned} \Delta(z_1) &= z_1 \otimes z_1 + \frac{1}{2} z_2 \otimes z_2 + \frac{1}{2} z_3 \otimes z_3, \\ \Delta(z_2) &= z_1 \otimes z_2 + z_2 \otimes (z_1 + \frac{1}{2} z_2) - \frac{1}{2} z_3 \otimes z_3, \\ \Delta(z_3) &= z_1 \otimes z_3 - \frac{1}{2} z_2 \otimes z_3 + z_3 \otimes (z_1 - \frac{1}{2} z_2). \end{aligned}$$

Indeed, the Hopf algebra isomorphism $H \xrightarrow{\sim} (L \otimes_K L)^D$ is given by

$$\begin{aligned} z_1 &\mapsto (1 \otimes 1) \otimes_K (1 \otimes 1) + (\sigma \otimes 1) \otimes_K (\sigma \otimes 1) + (\sigma^2 \otimes 1) \otimes_K (\sigma^2 \otimes 1), \\ z_2 &\mapsto (1 \otimes 1) \otimes_K (\sigma \otimes 1 + \sigma^2 \otimes 1) + (\sigma \otimes 1) \otimes_K (1 \otimes 1 + \sigma^2 \otimes 1) \\ &\quad + (\sigma^2 \otimes 1) \otimes_K (1 \otimes 1 + \sigma \otimes 1), \\ z_3 &\mapsto -\sqrt{-1}(1 \otimes 1) \otimes_K (\sigma \otimes 1 - \sigma^2 \otimes 1) + \sqrt{-1}(\sigma \otimes 1) \otimes_K (1 \otimes 1 - \sigma^2 \otimes 1) \\ &\quad - \sqrt{-1}(\sigma^2 \otimes 1) \otimes_K (1 \otimes 1 - \sigma \otimes 1). \end{aligned}$$

The PV group scheme $\mathbf{G}(L/K) = \mathrm{Spec} H$ is a twisted form of $\mathbb{Z}/3\mathbb{Z}$ (see [29, (6.4)]):

$$\begin{aligned} \mathbb{Q}(\sqrt{-1}) \otimes_{\mathbb{Q}} H &\xrightarrow{\sim} \mathbb{Q}(\sqrt{-1}) \times \mathbb{Q}(\sqrt{-1}) \times \mathbb{Q}(\sqrt{-1}) \simeq \mathbb{Q}(\sqrt{-1})(\mathbb{Z}/3\mathbb{Z})^* \\ z_1 &\mapsto (1, 0, 0) \\ \frac{1}{2}(z_2 + \sqrt{-1} z_3) &\mapsto (0, 1, 0) \\ \frac{1}{2}(z_2 - \sqrt{-1} z_3) &\mapsto (0, 0, 1). \end{aligned}$$

Let K be an AS D-module algebra and V a $K\#D$-module. The rank $\mathrm{rk}_K(V)$ of the free K-module V will be called the K-rank; see Corollary 3.3.4.

Definition 3.8.1. Let $K \subset L$ be an inclusion of AS D-module algebras and V a $K\#D$-module. We say that V *splits in* L/K, or L/K is a *splitting algebra for* V iff there is an $L\#D$-linear injection $L \otimes_K V \hookrightarrow L^\Lambda$ into some power L^Λ of L. $K\langle V\rangle$ denotes the smallest AS D-module subalgebra of L including K and $f(V)$ for all $f \in \mathrm{Hom}_{K\#D}(V, L)$. If $L = K\langle V\rangle$ and V splits in L/K, we say L/K is a *minimal splitting algebra for* V.

Similarly to [27, Proposition 3.1], we have the following:

Proposition 3.8.2. *Let $K \subset L$ be an inclusion of AS D-module algebras and V a $K\#D$-module.*

(i) *If V splits in L/K, every $K\#D$-submodule of V splits in L/K.*

(ii) *If V splits in L/K, it splits in $K\langle V\rangle/K$.*

(iii) *V splits in L/K iff the canonical L-module map*

$$L \otimes_{L^D} \mathrm{Hom}_{K\#D}(V, L) \to \mathrm{Hom}_K(V, L), \tag{3.16}$$

has a dense image; in other words, the dual L-module map

$$L \otimes_K V \to \mathrm{Hom}_{L^D}(\mathrm{Hom}_{K\#D}(V, L), L), \quad a \otimes v \mapsto [f \mapsto af(v)] \tag{3.17}$$

is injective.

Proof. (i) Since all $K\#D$-modules are free K-modules, this follows immediately by the definition.

(ii) If V splits in L/K, then the image of $L \otimes_K V \to L^\Lambda$ is in $K\langle V\rangle^\Lambda$ by the definition. Thus V splits in $K\langle V\rangle/K$.

(iii) Recall that $\mathrm{Hom}_K(V, L)$ has an $L\#D$-module structure by D-conjugation (3.5) and the map (3.16) is necessarily injective by Corollary 3.1.4.

("If" part.) Since L^D is a field, $\mathrm{Hom}_{K\#D}(V, L)$ is a free L^D-module. By taking a dual basis, we can identify $\mathrm{Hom}_{L^D}(\mathrm{Hom}_{K\#D}(V, L), L)$ with some power L^Λ of L. Then the injective L-module map $L \otimes_K V \to \mathrm{Hom}_{L^D}(\mathrm{Hom}_{K\#D}(V, L), L) \xrightarrow{\sim} L^\Lambda$ can be considered as an injective $L\#D$-module map.

("Only if" part.) By the definition, there is an $L\#D$-linear injection $\varphi : L \otimes_K V \to L^\Lambda$ for some power L^Λ. Let $\{f_i\}_{i\in\Lambda} \subset \mathrm{Hom}_{K\#D}(V, L)$ be the family of $K\#D$-module maps induced by $\varphi(1 \otimes v) = (f_i(v))_{i\in\Lambda}$ $(v \in V)$. Take an arbitrary element $w = \sum_j a_j \otimes v_j \in$

$L \otimes_K V$. If the image of w by the map (3.17) is 0, then we have $\sum_j a_j f_i(v_j) = 0$ for all $i \in \Lambda$ and so $\varphi(w) = 0$ ($\Leftrightarrow w = 0$). Thus the map (3.17) is injective. □

Proposition 3.8.3. *Let $K \subset L$ be an inclusion of AS D-module algebras and V a $K\#D$-module with finite K-rank $\mathrm{rk}_K(V) = r < \infty$. Then*

$$\dim_{L^D} \mathrm{Hom}_{K\#D}(V, L) \leq r \tag{3.18}$$

and the following are equivalent:

(a) *V splits in L/K;*
(b) $L \otimes_{L^D} \mathrm{Hom}_{K\#D}(V, L) \xrightarrow{\sim} \mathrm{Hom}_K(V, L)$;
(c) $\dim_{L^D} \mathrm{Hom}_{K\#D}(V, L) = r$;
(d) *There is an isomorphism $L \otimes_K V \xrightarrow{\sim} L^r$ as $L\#D$-modules;*
(e) $L \otimes_{L^D} (L \otimes_K V)^D \xrightarrow{\sim} L \otimes_K V$;
(f) $\dim_{L^D}(L \otimes_K V)^D = r$;
(g) *There is an injective $L\#D$-module map $L \otimes_K V \to L^n$ for some integer n.*

Proof. The inequality (3.18) follows since $L \otimes_{L^D} \mathrm{Hom}_{K\#D}(V, L) \to \mathrm{Hom}_K(V, L)$ is an injective $L\#D$-module map whose cokernel is a free L-module with finite rank. Then ((a) $\Leftrightarrow$ (b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d)) follows from (the proof of) Proposition 3.8.2 (iii). The equivalence between (d), (e), (f) is easily seen. ((d) $\Rightarrow$ (g) $\Rightarrow$ (a)) is trivial. □

Lemma 3.8.4. *Let $K \subset L$ be an inclusion of AS D-module algebras, V a $K\#D$-module, and W a $K\#D$-submodule of V with finite K-rank. If V splits in L/K, then the restriction* res. : $\mathrm{Hom}_{K\#D}(V, L) \to \mathrm{Hom}_{K\#D}(W, L)$ *is surjective.*

Proof. Consider the following $L\#D$-module map:

$$\varphi : L \otimes_{L^D} \mathrm{Hom}_{K\#D}(V, L) \to \mathrm{Hom}_K(W, L), \quad a \otimes f \mapsto af|_W.$$

Notice that $\mathrm{Im}\,\varphi$ is a direct summand of $\mathrm{Hom}_K(W, L)$ as an L-module. The transposed L-linear map of φ is given by

$$L \otimes_K W \hookrightarrow L \otimes_K V \to \mathrm{Hom}_{L^D}(\mathrm{Hom}_{K\#D}(V, L), L),$$

which is injective by Proposition 3.8.2 (iii). Thus φ is surjective. Since the functor $(-)^D$ is exact, we have that $\varphi^D =$ res. is surjective. □

We see that the functor Φ preserves splitting algebras:

Lemma 3.8.5. *Let $G_1 \subset G$, $K_1 \subset L_1$ be as in Lemma 3.7.1. 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, iff $\Phi(L_1)/\Phi(K_1)$ is a (minimal) splitting algebra for the $\Phi(K_1)\#D$-module $\Phi(V_1)$.*

Proof. This easily follows from Proposition 3.2.4 if one notices that

$$\Phi(K_1\langle V_1\rangle) = \Phi(K_1)\langle\Phi(V_1)\rangle$$

to see the equivalence on minimality. □

Let $K \subset L$ be an inclusion of AS D-module algebras. For finitely many elements $u_1, \dots, u_m$ in L, let $K\langle u_1, \dots, u_m\rangle$ denote the smallest AS D-module subalgebra in L including K and $u_1, \dots, u_m$.

Definition 3.8.6. L/K is said to be *finitely generated* iff L is of the form $K\langle u_1, \dots, u_m\rangle$. 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 3.8.7. *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* [13]*: $X \in GL_n(L)$, 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 3.7.1 and 3.8.5, we may assume that K is a field. Suppose that $(L/K, A, H)$ is a finitely generated PV extension. By Proposition 3.7.4, 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 [29, (3.3)] and [27, 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 $g_1, \ldots, g_s$ 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 an $i \in \{1, \ldots, s\}$, and let $\boldsymbol{w} = (w_1, \ldots, w_m) \in A_1^m$ 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, $w_1, \ldots, w_r$ $(r \le m)$, of the k-subspace in A_1 spanned by $w_1, \ldots, w_m$. There is a rank r matrix T with entries in k, such that $\boldsymbol{w} = \boldsymbol{w}'T$ with $\boldsymbol{w}' = (w_1, \ldots, w_r)$. 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 $g \in G$, $gu_1, \ldots, gu_m$ span an H-subcomodule in A since the comodule structure map $\theta : A \to A \otimes_k H$ is D-linear. It then follows that $w_1, \ldots, w_r$ form a k-basis of an $\bar{H}$-subcomodule in A_1. By applying Proposition 3.1.6 for $w_1, \ldots, w_r \in L_1$, there exist r elements $h_1, \ldots, h_r \in C$ such that $(h_i(w_j))_{i,j}$ is an invertible matrix. We claim that $(c\boldsymbol{w}')(h_i(w_j))_{i,j}^{-1} \in K^r$ for all $c \in C$. If it follows, then $W' = Kh_1(\boldsymbol{w}')+\cdots+Kh_r(\boldsymbol{w}')$ and hence we have $\dim_K W' < \infty$, as desired.

Let $\theta_1 : A_1 \to A_1 \otimes_k \bar{H}$ be the comodule structure map associated to the PV extension L_1/K. Write

$$\theta_1(w_j) = \sum_{s=1}^{r} w_s \otimes_k z_{sj} \quad (z_{sj} \in H,\ j = 1, \ldots, r).$$

By applying μ-isomorphism $A_1 \otimes_k H \xrightarrow{\sim} A_1 \otimes_K A_1$ in each side, we have

$$1 \otimes_K w_j = \sum_{s=1}^{r}(w_s \otimes_K 1)z_{sj} \quad \text{in } A_1 \otimes_K A_1. \tag{3.19}$$

Hence

$$1 \otimes_K h_i(w_j) = \sum_{s=1}^{r}(h_i(w_s) \otimes_K 1)z_{sj} \quad (i, j = 1, \ldots, r),$$

i.e. $1 \otimes_K (h_i(w_j))_{i,j} = ((h_i(w_j))_{i,j} \otimes_K 1)Z$ with $Z = (z_{ij})_{i,j}$. Since $(h_i(w_j))_{i,j}$ is invertible, we have

$$Z = ((h_i(w_j))_{i,j}^{-1} \otimes_K 1)(1 \otimes_K (h_i(w_j))_{i,j}) \in GL_r(L_1 \otimes_K L_1).$$

On the other hand, recalling (3.19) we have

$$1 \otimes_K (c\boldsymbol{w}') = ((c\boldsymbol{w}') \otimes_K 1)Z$$

for all $c \in C$. Thus, by multiplying $1 \otimes_K (h_i(w_j))^{-1}_{i,j} = Z^{-1}((h_i(w_j))^{-1}_{i,j} \otimes_K 1)$ from the left,

$$1 \otimes_K (cw')(h_i(w_j))^{-1}_{i,j} = ((cw') \otimes_K 1)ZZ^{-1}((h_i(w_j))^{-1}_{i,j} \otimes_K 1) = (cw')(h_i(w_j))^{-1}_{i,j} \otimes_K 1$$

for all $c \in C$. This implies the claim above.

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

(c) $\Rightarrow$ (d). Suppose that L/K is a minimal splitting algebra for V with finite K-free basis $v_1, \dots, v_n$. By Proposition 3.8.3 (c), we have a k-basis $f_1, \dots, f_n$ in $\mathrm{Hom}_{K\#D}(V, L)$. Define

$$X = (x_{ij})_{i,j} = (f_j(v_i))_{i,j}, \quad \boldsymbol{v} = {}^t(v_1, \dots, v_n). \tag{3.20}$$

Then we have $X \in GL_n(L)$ since there is an L-module isomorphism

$$L^n \simeq L \otimes_K V \xrightarrow{\sim} \mathrm{Hom}_k(\mathrm{Hom}_{K\#D}(V, L), L) \simeq L^n$$

which is precisely the multiplication of X (see the proof of Proposition 3.8.2, 3.8.3). If we write $dv_i = \sum_{s=1}^n c_{is}(d)v_s$ ($c_{is}(d) \in K$) for $d \in D$, then we have $dx_{ij} = f_j(dv_i) = \sum_{s=1}^n c_{is}(d)f_j(v_s) = \sum_{s=1}^n c_{is}(d)x_{sj}$. This implies that X is GL_n-primitive such that

$$(dX)X^{-1}\boldsymbol{v} = d\boldsymbol{v} \quad (d \in D), \tag{3.21}$$

i.e. $(dX)X^{-1} = (c_{ij}(d))_{i,j} \in M_n(K)$. By the definition, we have $L = K\langle V\rangle = K\langle x_{ij}\rangle$.

(d) $\Rightarrow$ (a). This is shown by modifying [27, Example 2.5c] as follows.

Put $Y = (y_{ij})_{i,j} = X^{-1}$ and $A = K[x_{ij}, y_{ij}]$. First we shall show that A is a D-module subalgebra of L. Define $\phi \in \mathrm{Hom}_R(D, M_n(K))$ by $\phi_d = d(X)X^{-1} = d(X)Y$ ($d \in D$). Since $\phi_g^{-1} = Xg(Y) = g(g^{-1}(X)X^{-1}) \in GL_n(K)$ for all $g \in G$, ϕ is convolution-invertible in $\mathrm{Hom}_R(D, M_n(K))$ by [23, Corollary 9.2.4]. We see that the $\psi \in \mathrm{Hom}_R(D, M_n(L))$ given by $\psi_d = Xd(Y)$, is the inverse of ϕ, and so $\psi \in \mathrm{Hom}_R(D, M_n(K))$. This implies that A is a D-module subalgebra of L. Since $Q(A)$, the total quotient ring of A, is an AS D-module subalgebra of L containing K and $x_{11}, \dots, x_{nn}$ (recall Corollary 3.3.8), we have $Q(A) = K\langle x_{ij}\rangle = L$.

Put

$$Z = (Y \otimes_K 1)(1 \otimes_K X), \;\; Z^{-1} = (1 \otimes_K Y)(X \otimes_K 1) \in GL_n(A \otimes_K A).$$

For all $d \in D$,

$$\begin{aligned}
d(Z) &= \sum_{(d)} (d_{(1)}(Y) \otimes_K 1)(1 \otimes_K d_{(2)}(X)) \\
&= \sum_{(d)} (Y\psi_{d_{(1)}} \otimes_K 1)(1 \otimes_K \phi_{d_{(2)}} X) \\
&= \sum_{(d)} (Y \otimes_K 1)(\psi_{d_{(1)}} \otimes_K 1)(1 \otimes_K \phi_{d_{(2)}})(1 \otimes_K X) \\
&= \sum_{(d)} (Y \otimes_K 1)(\psi_{d_{(1)}} \otimes_K 1)(\phi_{d_{(2)}} \otimes_K 1)(1 \otimes_K X) \\
&= \sum_{(d)} (Y \otimes_K 1)(\psi_{d_{(1)}}\phi_{d_{(2)}} \otimes_K 1)(1 \otimes_K X) \\
&= \varepsilon(d)Z.
\end{aligned}$$

Thus Z has entries in $H := (A \otimes_K A)^D$. Similarly we have that the entries in Z^{-1} are also in H and hence $Z \in GL_n(H)$. Then,

$$1 \otimes_K X = (X \otimes_K 1)Z, \ 1 \otimes_K Y = Z^{-1}(Y \otimes_K 1) \in GL_n(A \cdot H).$$

This implies $A \otimes_K A = A \cdot H$. Therefore $(L/K, A, H)$ is a PV extension. □

Remark 3.8.8. Keep the notation just as above.

(i) Write $Z = (z_{ij})$, $Z^{-1} = (w_{ij})$. Then $A \otimes_K A = A[z_{ij}, \det(z_{ij})^{-1}]$ and $H = k[z_{ij}, \det(z_{ij})^{-1}] = k[z_{ij}, w_{ij}]$. Taking μ, θ as in Proposition 3.5.2, we see

$$\begin{aligned}
\theta(X) &= \mu^{-1}(1 \otimes_K X) = \mu^{-1}((X \otimes_K 1)Z) = \mu^{-1}\left(\sum_{s=1}^{n}(x_{is} \otimes_K 1)z_{sj}\right)_{i,j} \\
&= \left(\sum_{s=1}^{n} x_{is} \otimes_k z_{sj}\right)_{i,j} = (X \otimes_k 1)(1 \otimes_k Z).
\end{aligned}$$

This is often written like

$$\theta(X) = X \otimes_k Z. \tag{3.22}$$

It follows that the Hopf algebra structure of H is given by

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

here I denotes the identity matrix; see [29, (3.2), Corollary]. We have a Hopf algebra surjection,

$$k[GL_n] = k[T_{ij}, \det(T_{ij})^{-1}] \twoheadrightarrow H, \quad T_{ij} \mapsto z_{ij},$$

which gives a closed embedding $\mathbf{G}(L/K) \to \mathbf{GL}_n$ of affine k-group schemes.

(ii) Suppose that $D = R[\tau, \tau^{-1}]$, the group algebra of the free abelian group of rank 1, and K is a field; K is then an inversive difference field. A difference system $\tau \boldsymbol{y} = B\boldsymbol{y}$ 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 (3.21) that the X in (3.20) is a fundamental matrix [20, Definition 1.4] for the difference system arising from the V and the $\boldsymbol{v}$ above, and so that A is the Picard-Vessiot ring [20, Definition 1.5] for the system. It will follow from Theorems 3.8.7, 3.8.11 that if k $(= K^D)$ is algebraically closed, a Picard-Vessiot ring for any difference system as above uniquely exists, and is given by such an A as above.

Corollary 3.8.9. *Let $(L/K, A, H)$ be a PV extension of AS D-module algebras. The following are equivalent:*

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

(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. ((a) $\Rightarrow$ (c) $\Rightarrow$ (b) $\Rightarrow$ (a)) and ((a) $\Rightarrow$ (d)) follow by the proof of Theorem 3.8.7. If H is a finitely generated k-algebra, then we have an ascending chain condition for Hopf ideals of H. Hence we have an ascending chain condition for intermediate AS D-module algebras of L/K, which implies (a). $\square$

Corollary 3.8.10. *Let $K \subset L$ be an inclusion of AS D-module algebras such that $K^D = L^D =: k$. Then L/K is a PV extension iff 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 [27, Corollary 3.5]. We include the proof for convenience.

("Only if" part.) Let $(L/K, A, H)$ be a PV extension. Then H is a directed union of Hopf subalgebras which are finitely generated k-algebras (see [29, (3.3)]). It follows by Proposition 3.5.8 and Corollary 3.8.9 that L is a directed union, say $L = \bigcup_\lambda L_\lambda$, of AS D-module subalgebras which are finitely generated PV extensions over K. By Theorem 3.8.7, each L_λ/K is a minimal splitting algebra for a $K\#D$-module V_λ of finite K-rank. Then L/K is a minimal splitting algebra for the direct sum $V = \bigoplus_\lambda V_\lambda$.

("If" part.) Suppose that L/K is a minimal splitting algebra for a $K\#D$-module $V = \bigcup_\lambda V_\lambda$, a directed union of $K\#D$-modules V_λ of finite K-rank. Since every V_λ splits in L/K, each $L_\lambda := K\langle V_\lambda \rangle$ is a minimal splitting algebra for V_λ and is a finitely generated PV extension over K by Theorem 3.8.7. By Lemma 3.8.4, the union $\bigcup_\lambda L_\lambda$ is a directed union of AS D-module subalgebras of L. Thus $\bigcup_\lambda L_\lambda$ is an AS D-module subalgebra of L by Lemma 3.3.7. For every $f \in \mathrm{Hom}_{K\#D}(V, L)$, we have $f(V) = \bigcup_\lambda f(V_\lambda) \subset \bigcup_\lambda L_\lambda$. Hence $L = K\langle V \rangle = \bigcup_\lambda L_\lambda$. Let A_λ (resp. H_λ) be the principal algebra (resp. the Hopf algebra) for L_λ/K. Then one sees that $(L/K, \bigcup_\lambda A_\lambda, \bigcup_\lambda H_\lambda)$ is a PV extension. $\square$

Theorem 3.8.11. *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 3.8.12. *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 3.3.6, 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 [14, 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 3.3.3, 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 $\varphi(T) = T^n + c_1 T^{n-1} + \cdots + c_n$ 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. $\square$

Proof of Theorem 3.8.11. Existence; this is proved by modifying the proof of [27, Theorem 4.5], as follows. Let $v_1, \ldots, v_r$ 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 3.3.6. 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 3.3.3 and Lemma 3.3.6. By Lemma 3.8.12, we have $L^D = K^D$. Let x_{ij} denote the image of X_{ij} in A, and define K-linear maps $f_j : V \to L$ $(j = 1, \ldots, r)$ 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 3.8.3 (c).

Uniqueness; also this proof is essentially the same as the proof given in [27, Theorem 4.6]. Let L_1/K and L_2/K are two minimal splitting algebra for V such that $L_1^D = L_2^D = K^D = k$. By Theorem 3.8.7, L_1/K and L_2/K are finitely generated PV extensions. Let A_i be the principal algebra for L_i/K $(i = 1, 2)$ respectively. Put $A = A_1 \otimes_K A_2$ and let I be a maximal D-stable ideal of A. We see A_1, A_2 are noetherian simple D-module algebras which are finitely generated K-algebras by the proof of Theorem 3.8.7 (d) $\Rightarrow$ (a), and by Proposition 3.5.9 (i). Thus $A_i \cap I = 0$ $(i = 1, 2)$ and hence A_1, A_2 are identified with D-module subalgebras of A/I. Let L be the total quotient ring of A/I. By Lemma 3.3.6 and Proposition 3.3.3, L is an AS D-module algebra since A/I is a noetherian simple D-module algebra. Furthermore, since A/I is a finitely generated K-algebra, we have $L^D = K^D = k$ by Lemma 3.8.12. Let $\chi_i : L_i \hookrightarrow L$ $(i = 1, 2)$ denote the induced inclusions of D-module algebras over K. The injective k-linear maps $\mathrm{Hom}_{K\#D}(V, L_i) \to \mathrm{Hom}_{K\#D}(V, L)$ $(i = 1, 2)$ are precisely isomorphisms by Proposition 3.8.3. Therefore $f(V) \subset \chi_1(L_1) \cap \chi_2(L_2)$ for all $f \in \mathrm{Hom}_{K\#D}(V, L)$. Since L_i are generated over K by the image of all $f \in \mathrm{Hom}_{K\#D}(V, L_i)$, we have $\chi_1(L_1) = \chi_2(L_2) = K\langle V\rangle$ in L. Thus we have $\chi_2^{-1} \circ \chi_1 : L_1 \xrightarrow{\sim} L_2$, a D-module algebra isomorphism over K. $\square$

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 a dual object under the D-conjugation; see (3.5). 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 [21, Theorem 2.33] also for comparing with the following.

Theorem 3.8.13. *Let $(L/K, A, H)$ be a finitely generated PV extension of AS D-module algebras. By Theorem 3.8.7, 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 $\mathrm{Rep}_{\mathbf{G}(L/K)}$ of the same kind, consisting of finite-dimensional linear representations of the PV group scheme $\mathbf{G}(L/K) = \mathrm{Spec}H$.

Proof. Put $D_k = D \otimes_R k$, a cocommutative Hopf algebra over k, and consider D_k as a right H-comodule algebra with the trivial structure map $d \mapsto d \otimes 1$. Regard naturally A as an algebra in the symmetric tensor category $({}_{D_k}\mathcal{M}^H, \otimes_k, k)$ of right (H, D_k^{op})-Hopf modules (see [16, §8.5]); its objects are D_k-modules N which has a D_k-linear, right H-comodule structure $\rho_N : N \to N \otimes_k H$. We then have the symmetric tensor category ${}_A({}_{D_k}\mathcal{M}^H)$ of A-modules in ${}_{D_k}\mathcal{M}^H$, which is denoted 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 [22], Θ_2 and Ξ_2 are quasi-inverses of each other, since A/K is H-Galois by Proposition 3.5.2 (iii). 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 3.5.9 (i), we see from Corollary 3.1.4 that the 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 $\mathcal{N}$ denote 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 (3.20). We see from (3.21) 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 (3.22), 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 3.8.7 (d) $\Rightarrow$ (a)), $\tilde{V}$ generates $\mathcal{M}^H_{\mathrm{fin}}$; see [29, 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). □

3.9. Liouvillian extensions

Finally we define the notion of liouvillian extensions and show the solvability theorem. As is described in Introduction, we should define *liouvillian group schemes* and study how strong the definition is.

3.9.1. **Liouvillian group schemes.**

Definition 3.9.1. Let $\mathbf{G}$ be an algebraic affine group scheme over a field k.

(1) We say $\mathbf{G}$ is *(k-)liouvillian* (cf. [13, p. 374]) iff there exists a normal chain of closed subgroup schemes

$$\mathbf{G} = \mathbf{G}_0 \rhd \mathbf{G}_1 \rhd \cdots \rhd \mathbf{G}_r = \{1\} \tag{3.23}$$

such that each $\mathbf{G}_{i-1}/\mathbf{G}_i$ ($i = 1, \dots, r$) is at least one of the following types: finite etale, a closed subgroup scheme of $\mathbf{G}_\mathrm{a}$, or a closed subgroup scheme of $\mathbf{G}_\mathrm{m}$. In this case, we call (3.23) a *liouvillian normal chain* (LNC).

(2) In (3.23), if each $\mathbf{G}_{i-1}/\mathbf{G}_i$ is merely a closed subgroup scheme of $\mathbf{G}_\mathrm{a}$ or a closed subgroup scheme of $\mathbf{G}_\mathrm{m}$, then we call it a *restricted liouvillian normal chain* (RLNC).

We use the following abbreviation of some types on group schemes which arise as factor group schemes in an LNC: we say $\mathbf{G}$ is of *$\mathbf{G}_\mathrm{a}$-type* (resp., *$\mathbf{G}_\mathrm{m}$-type*) iff it is a closed subgroup scheme of $\mathbf{G}_\mathrm{a}$ (resp., $\mathbf{G}_\mathrm{m}$), and a group scheme of *RL-type* (resp., *L-type*) means that it is of $\mathbf{G}_\mathrm{a}$-type or $\mathbf{G}_\mathrm{m}$-type (resp., RL-type or finite etale).

Lemma 3.9.2. (1) *If $\mathbf{G}$ is liouvillian (resp., has an RLNC), then every closed subgroup scheme of $\mathbf{G}$ is liouvillian (resp., has an RLNC). Especially $\mathbf{G}$ is liouvillian iff the connected component $\mathbf{G}^\circ$ is liouvillian.*

(2) *Let $\mathbf{H}$ be a normal closed subgroup scheme of $\mathbf{G}$. Then $\mathbf{G}$ is liouvillian (resp., has an RLNC) iff both $\mathbf{H}$ and $\mathbf{G}/\mathbf{H}$ are liouvillian (resp., have an RLNC).*

(3) *If $\mathbf{G}$ is connected liouvillian, then $\mathbf{G}$ is solvable.*

Proof. First we take an LNC (resp., an RLNC): $\mathbf{G} = \mathbf{G}_0 \rhd \mathbf{G}_1 \rhd \cdots \rhd \mathbf{G}_r = \{1\}$ in each proof of (1), "only if" part of (2), and (3).

(1) Let $\mathbf{H}$ be a closed subgroup scheme of $\mathbf{G}$ and put $\mathbf{H}_i := \mathbf{H} \cap \mathbf{G}_i$ ($i = 0, \dots, r$). Then we have $\mathbf{H}_0 = \mathbf{H}$ and $\mathbf{H}_i = \mathbf{H}_{i-1} \cap \mathbf{G}_i = \mathrm{Ker}(\mathbf{H}_{i-1} \to \mathbf{G}_{i-1}/\mathbf{G}_i)$ for $i = 1, \dots, r$. It follows that $\mathbf{H}_{i-1} \rhd \mathbf{H}_i$ and $\mathbf{H}_{i-1}/\mathbf{H}_i$ is a closed subgroup scheme of $\mathbf{G}_{i-1}/\mathbf{G}_i$ for $i = 1, \dots, r$. Therefore $\mathbf{H} = \mathbf{H}_0 \rhd \mathbf{H}_1 \rhd \cdots \rhd \mathbf{H}_r = \{1\}$ is an LNC (resp., an RLNC).

(2) ("Only if" part.) $\mathbf{H}$ is liouvillian (resp., has an RLNC) by (1). Put $\mathbf{F}_i := \mathbf{G}_i/\mathbf{H} \cap \mathbf{G}_i$ ($i = 0, \dots, r$). Since each $k[\mathbf{F}_{i-1}/\mathbf{F}_i]$ is a Hopf subalgebra of $k[\mathbf{G}_{i-1}/\mathbf{G}_i]$, each $\mathbf{F}_{i-1}/\mathbf{F}_i$ is of L-type (resp., RL-type) for $i = 1, \dots, r$. Then $\mathbf{G}/\mathbf{H} = \mathbf{F}_0 \rhd \mathbf{F}_1 \rhd \cdots \rhd \mathbf{F}_r = \{1\}$ is an LNC (resp., an RLNC).

("If" part.) Let $\mathbf{G}/\mathbf{H} = \mathbf{F}_0 \rhd \mathbf{F}_1 \rhd \cdots \rhd \mathbf{F}_r = \{1\}$ be an LNC (resp., an RLNC) and $(0) = I_0 \subset I_1 \subset \cdots \subset I_r$ the corresponding sequence of Hopf ideals of $k[\mathbf{G}/\mathbf{H}]$. If we put $I'_i := k[\mathrm{G}] \cdot I_i$ $(i = 0, \ldots, r)$, then each I'_i becomes a Hopf ideal of $k[\mathrm{G}]$. Let $\mathbf{G}_i$ be the closed subgroup scheme of $\mathbf{G}$ which corresponds to I'_i. Then we have a normal chain $\mathbf{G} = \mathbf{G}_0 \rhd \mathbf{G}_1 \rhd \cdots \rhd \mathbf{H}$ such that $\mathbf{G}_{i-1}/\mathbf{G}_i \simeq \mathbf{F}_{i-1}/\mathbf{F}_i$ $(i = 1, \ldots, r)$. Therefore $\mathbf{G}$ is liouvillian (resp., has an RLNC).

(3) We use induction on the least length r of LNC. The case $r = 0$ is clear. Let $r > 0$. Since $\mathbf{G}$ is connected, $\mathbf{G}/\mathbf{G}_1$ is also connected. Then $\mathbf{G}/\mathbf{G}_1$ is of RL-type and hence abelian. Therefore $\mathscr{D}\mathbf{G}$ (see [29, (10.1)]) is a connected closed subgroup scheme of $\mathbf{G}_1$. By (1) and its proof, $\mathscr{D}\mathbf{G}$ is connected liouvillian and has an LNC with length $\leq r - 1$. Then $\mathscr{D}\mathbf{G}$ is solvable by inductive assumption, concluding the proof. $\square$

The converse of (3) above does not hold in general; see the following example:

Example 3.9.3. (1) A nontrivial anisotropic torus $\mathbf{T}$ is connected solvable but not liouvillian since both $\mathrm{Hom}(\mathbf{T}, \mathbf{G}_{\mathrm{m}})$ and $\mathrm{Hom}(\mathbf{T}, \mathbf{G}_{\mathrm{a}})$ are trivial.

(2) Let k be the prime field of $\mathrm{ch}(k) = 2$ and $H = k[x]/\langle x^4 + x^2 + x \rangle$ with x primitive. Then H is a commutative Hopf algebra and $\mathbf{G} = \mathrm{Spec}H$ is abelian, finite etale, and unipotent. The Cartier dual $\mathbf{G}^*$ is finite connected of multiplicative type and then solvable. Since H^* does not have any nontrivial grouplike, $\mathrm{Hom}(\mathbf{G}^*, \mathbf{G}_{\mathrm{m}})$ is trivial. Therefore $\mathbf{G}^*$ is not liouvillian.

Proposition 3.9.4. *Let $\mathbf{G}$ be a connected algebraic affine group scheme over a field k. Then $\mathbf{G}$ is liouvillian iff $\mathbf{G}$ has an RLNC.*

Proof. The "if" part is clear. For the "only if" part, we use induction on the least length r of LNC $\mathbf{G} = \mathbf{G}_0 \rhd \mathbf{G}_1 \rhd \cdots \rhd \mathbf{G}_r = \{1\}$. The case $r = 0$ is clear. Let $r > 0$ and assume $\mathbf{G}_1^\circ$ has an RLNC. By the argument in the proof of Lemma 3.9.2 (3), we have $\mathbf{G} \rhd \mathbf{G}_1^\circ$ and $\mathbf{G}/\mathbf{G}_1^\circ$ is abelian. Thus the proof can be reduced to the case that $\mathbf{G}$ is connected abelian by Lemma 3.9.2 (2).

Let $\mathbf{G}$ be connected abelian and put $H = k[\mathbf{G}]$. Let H_{u} $(= H^1)$ be the irreducible component of H which contains 1 and $H_{\mathrm{s}} = H/HH_{\mathrm{u}}^+$. Then we have the exact sequence

$$H_{\mathrm{u}} \rightarrowtail H \twoheadrightarrow H_{\mathrm{s}}. \tag{3.24}$$

Let $\bar{k}$ denote the algebraic closure of k. It is known that $H_{\mathrm{u}} \otimes_k \bar{k}$ is also the irreducible component of $H \otimes_k \bar{k}$ containing 1. The exact sequence (3.24) splits over $\bar{k}$ (the Jordan decomposition of $\mathbf{G}_{\bar{k}}$ [29, (9.5)]), and $\mathbf{G}_{\mathrm{s}} := \mathrm{Spec}H_{\mathrm{s}}$ is connected of multiplicative type since $(\mathbf{G}_{\mathrm{s}})_{\bar{k}}$ is connected diagonalizable. Put $\mathbf{G}_{\mathrm{u}} := \mathrm{Spec}H_{\mathrm{u}}$ $(= \mathbf{G}/\mathbf{G}_{\mathrm{s}})$; this is unipotent. We see $\mathbf{G}_{\mathrm{u}}$ has an RLNC whose all factor group schemes are of $\mathbf{G}_{\mathrm{a}}$-type (see [29, Ch. 16, Ex. 5]). Then it suffices to show that $\mathbf{G}_{\mathrm{s}}$ has an RLNC. Let $\mathbf{T}$ be a maximal torus of $\mathbf{G}_{\mathrm{s}}$. $\mathbf{T}$ includes no nontrivial anisotropic subtorus since it is liouvillian. Hence, by [29, (7.4)], we see $\mathbf{T}$ is a split torus and has an RLNC. Put $\mathbf{H} = \mathbf{G}_{\mathrm{s}}/\mathbf{T}$; this is finite connected, liouvillian, and of multiplicative type. Let $\mathbf{H} \rhd \mathbf{H}_1 \rhd \cdots \rhd \mathbf{H}_r = \{1\}$ be an LNC. We see $\mathbf{H}/\mathbf{H}_1$ is of $\mathbf{G}_{\mathrm{m}}$-type. Since $\mathbf{H}$ is finite connected, $k[\mathbf{H}]$ is a local algebra of finite dimension. Then its quotient $k[\mathbf{H}_1]$ is also a local algebra of finite dimension and hence $\mathbf{H}_1$ is connected. By inductive assumption, $\mathbf{H}_1$ has an RLNC. Therefore $\mathbf{H}$ also has an RLNC, concluding the proof. □

Proposition 3.9.5. *Let k be an algebraically closed field and $\mathbf{G}$ an algebraic affine group scheme over k. Then $\mathbf{G}$ is liouvillian iff $\mathbf{G}^\circ$ is solvable.*

Proof. In fact we have proved the "only if" part in Lemma 3.9.2 over an arbitrary field. For the "if" part, we use induction on the least m such that $\mathscr{D}^m\mathbf{G}^\circ = \{1\}$. The case $m = 0$ is clear. Let $m > 0$ and assume that $\mathscr{D}\mathbf{G}^\circ$ has an RLNC. By Lemma 3.9.2 (2), it suffices to show that $\mathbf{G}^\circ/\mathscr{D}\mathbf{G}^\circ$ has an RLNC. Thus the proof can be reduced to the case that $\mathbf{G}$ is (connected) abelian.

Let $\mathbf{G}$ be abelian and take the Jordan decomposition $\mathbf{G} = \mathbf{G}_{\mathrm{s}} \times \mathbf{G}_{\mathrm{u}}$. $\mathbf{G}_{\mathrm{u}}$ has an RLNC. Since k is algebraically closed, $\mathbf{G}_{\mathrm{s}}$ is diagonalizable and hence has an RLNC. Therefore $\mathbf{G}$ has an RLNC. □

We observe that the triangulability is certainly stronger than the condition to have an RLNC, even if k is algebraically closed. For example, the group scheme in [29, Ch. 10, Ex. 3] has an RLNC but not triangulable.

It is known that $\mathbf{G}$ is unipotent iff $\mathbf{G}$ has an RLNC whose all factor group schemes are of $\mathbf{G}_{\mathrm{a}}$-type. We say that $\mathbf{G}$ is $\mathbf{G}_{\mathrm{m}}$*-composite* iff $\mathbf{G}$ has an RLNC whose all factor group schemes are of $\mathbf{G}_{\mathrm{m}}$-type. When $\mathbf{G}$ corresponds to the affine algebraic group $G(k)$ (in the sense of [29, (4.5)]), $\mathbf{G}$ is $\mathbf{G}_{\mathrm{m}}$-composite iff $G(k)$ is solvable and "quasicompact" in the Kolchin's terminology, which implies that each element of $G(k)$ is diagonalizable [12, §6, Theorem 2]. In general it is difficult to characterize the condition to be $\mathbf{G}_{\mathrm{m}}$-composite. As seen above, not all group schemes of multiplicative type are $\mathbf{G}_{\mathrm{m}}$-composite. On the other hand, non-diagonalizable group schemes can be $\mathbf{G}_{\mathrm{m}}$-composite; see the following example.

Example 3.9.6. Let k be the prime field with $\mathrm{ch}(k) = p > 0$ and take the commutative Hopf algebra $H = k[x,y]/\langle x^p - x, y^p - x - y\rangle$ with x, y primitive. One sees $\mathbf{G} = \mathrm{Spec}H$ is abelian, finite etale, and unipotent. Hence the Cartier dual $\mathbf{G}^*$ is of multiplicative type and connected. We have the RLNC of $\mathbf{G}$:

$$k[x]/\langle x^p - x\rangle \rightarrowtail H \twoheadrightarrow k[y]/\langle y^p - y\rangle.$$

By dualizing this we see that $\mathbf{G}^*$ is $\mathbf{G}_{\mathrm{m}}$-composite:

$$k[\mu_p] \twoheadleftarrow H^* \leftarrowtail k[\mu_p].$$

The grouplikes of H^* is given by

$$\mathrm{Coalg}_k(k, H^*) \simeq \mathrm{Alg}_k(H, k) = \{(a,b) \in k^2 \mid a^p - a = 0, \quad b^p - a - b = 0\}.$$

Thus we have $\mathbf{G}^*$ is not diagonalizable since $p^2 = \dim_k H^* \neq p = \#\mathrm{Alg}_k(H,k)$.

3.9.2. **Finite etale extensions.** In what follows, we always assume that L/K is an extension of AS D-module algebras such that $L^D = K^D =: k$.

Definition 3.9.7. We say that L/K is a *finite etale extension* iff L is a separable K-algebra in the sense of [7], i.e. L is a projective $L \otimes_K L$-module.

For a commutative K-algebra A, let $\pi_0(A)$ denote the union of all separable K-subalgebras. If we take a maximal ideal P of L and put $L' = L/P$ and $K' = K/P \cap K$, then the following are equivalent:

- L/K is a finite etale extension.
- L is a finitely generated K-algebra and $\pi_0(L) = L$.
- L'/K' is a finite separable field extension.

Take a maximal ideal $\mathfrak{p}$ of K. We say a finite etale extension L/K is *copied* (resp., *anticopied*) iff $L' = K'$ (resp., $\mathfrak{p}L$ is a maximal ideal of L); this condition is independent of the choice of P (resp., $\mathfrak{p}$).

Lemma 3.9.8. *Let $(L/K, A, H)$ be a PV extension. Then $(\pi_0(A)/K, \pi_0(A), \pi_0(H))$ is also a PV extension and hence $\pi_0(A)$ is the intermediate AS D-module algebra which corresponds to $\mathbf{G}(L/K)^\circ$. Especially L/K is a finite etale extension iff $\mathbf{G}(L/K)$ is finite etale.*

Proof. The μ-isomorphism $A \otimes_k H \xrightarrow{\sim} A \otimes_K A$ restricts to the algebra isomorphism $\pi_0(A) \otimes_k \pi_0(H) \xrightarrow{\sim} \pi_0(A) \otimes_K \pi_0(A)$. Hence $\theta^{-1}(A \otimes_k \pi_0(H)) = \pi_0(A)$; this implies that $(\pi_0(A)/K, \pi_0(A), \pi_0(H))$ is a PV extension by Proposition 3.5.8. □

Lemma 3.9.9. *Let $(L/K, A, H)$ be a finitely generated PV extension. Then $\pi_0(A)$ is maximal among those separable K-subalgebras of L which are D-module subalgebras.*

Proof. Let M be a separable K-subalgebra of L which is a D-module subalgebra. Then M is an intermediate AS D-module algebra of L/K. Let I be the Hopf ideal of H which corresponds to M. By Proposition 3.5.7 (ii), we have $A^{\mathrm{co}\,H/I} = A \cap M \subset \pi_0(A)$ and hence $H^{\mathrm{co}\,H/I} \subset \pi_0(H)$. This implies $I \subset H \cdot \pi_0(H)^+$ and so $M \subset \pi_0(A)$. $\square$

Definition 3.9.10. Let $\mathscr{G}$ be a finite group and put $H = (k\mathscr{G})^*$. Consider $D_k = D \otimes_R k$ as a right H-comodule algebra with the trivial structure map $d \mapsto d \otimes 1$. We say L/K is a *$\mathscr{G}$-primitive extension* iff

(i) L is an algebra in the symmetric tensor category $({}_{D_k}\mathcal{M}^H, \otimes_k, k)$, and
(ii) L/K is a right H-Galois extension.

Here ${}_{D_k}\mathcal{M}^H$ denotes the category of right (H, D_k^{op})-Hopf modules as in the proof of Theorem 3.8.13.

We easily see that L/K is a $\mathscr{G}$-primitive extension iff $(L/K, L, (k\mathscr{G})^*)$ is a PV extension. If L/K is an anticopied $\mathscr{G}$-primitive extension, then L'/K' is a Galois extension of fields in ordinary sense such that $\mathrm{Gal}(L'/K') = \mathscr{G}$. Conversely, when L/K is a finite Galois extension of fields, L/K is $\mathrm{Gal}(L/K)$-primitive iff every element of $\mathrm{Gal}(L/K)$ is D-linear.

3.9.3. $\mathbf{G}_{\mathrm{a}}$-primitive extensions and $\mathbf{G}_{\mathrm{m}}$-primitive extensions.

Definition 3.9.11. (1) An $x \in L$ is called *$\mathbf{G}_{\mathrm{a}}$-primitive* over K iff $d(x) \in K$ for all $d \in D^+$. In this case, we say that $K\langle x\rangle/K$ is a *$\mathbf{G}_{\mathrm{a}}$-primitive extension.*

(2) An $x \in L$ is called *$\mathbf{G}_{\mathrm{m}}$-primitive* over K iff x is a non-zero divisor of L and $d(x)x^{-1} \in K$ for all $d \in D$. In this case, we say that $K\langle x\rangle/K$ is a *$\mathbf{G}_{\mathrm{m}}$-primitive extension.*

As in [27, (2.5a), (2.5b)], we have the following lemmas:

Lemma 3.9.12. (1) *Let $K\langle x\rangle/K$ be a $\mathbf{G}_{\mathrm{a}}$-primitive extension. Put $A = K[x]$ and $l = 1 \otimes_K x - x \otimes_K 1 \in (A \otimes_K A)^D$. Then $(K\langle x\rangle/K, A, k[l])$ is a PV extension with l primitive and the PV group scheme $\mathbf{G}(K\langle x\rangle/K)$ of $\mathbf{G}_{\mathrm{a}}$-type.*

(2) *Let $K\langle x\rangle/K$ be a $\mathbf{G}_{\mathrm{m}}$-primitive extension. Put $A = K[x, x^{-1}]$ and $g = x^{-1} \otimes_K x \in (A \otimes_K A)^D$. Then $(K\langle x\rangle/K, A, k[g, g^{-1}])$ is a PV extension with g grouplike and the PV group scheme $\mathbf{G}(K\langle x\rangle/K)$ of $\mathbf{G}_{\mathrm{m}}$-type.*

Proof. (1) x is $\mathbf{G}_{\mathrm{a}}$-primitive iff there exists a $\varphi \in \mathrm{Hom}_R(D, K)$ such that $d(x) = \varepsilon(d)x + \varphi(d)$ for all $d \in D$. Then

$$X = \begin{pmatrix} 1 & 1 \\ x & x+1 \end{pmatrix} \in GL_2(K\langle x\rangle)$$

is GL_2-primitive over K. In fact,

$$dX = \begin{pmatrix} \varepsilon(d) & 0 \\ \varphi(d) & \varepsilon(d) \end{pmatrix} X \qquad (d \in D).$$

Recalling the proof of Theorem 3.8.7 (d) $\Rightarrow$ (a), we see

$$Z = (X^{-1} \otimes_K 1)(1 \otimes_K X) = \begin{pmatrix} 1-l & -l \\ l & 1+l \end{pmatrix},$$

which concludes the proof.

(2) This is equivalent to saying that x is GL_1-primitive over K. $\square$

Lemma 3.9.13. (1) *If $l \in (L \otimes_K L)^D$ and if l is primitive in the L-coring $L \otimes_K L$, then there exists an $x \in L$ such that $l = 1 \otimes_K x - x \otimes_K 1$ and x is $\mathrm{G_a}$-primitive over K.*

(2) *If $g \in (L \otimes_K L)^D$ and if g is grouplike in $L \otimes_K L$, then there exists a non-zero divisor $x \in L$ such that $g = x^{-1} \otimes_K x$ and x is $\mathrm{G_m}$-primitive over K.*

Proof. (1) Primitive elements in the L-coring $L \otimes_K L$ are precisely 1-cocycles in the Amitsur complex:

$$0 \to L \xrightarrow{\delta_0} L \otimes_K L \xrightarrow{\delta_1} L \otimes_K L \otimes_K L \xrightarrow{\delta_2} \cdots,$$
$$\delta_0(x) = 1 \otimes_K x - x \otimes_K 1,$$
$$\delta_1(\sum x_i \otimes_K y_i) = \sum 1 \otimes_K x_i \otimes_K y_i - \sum x_i \otimes_K 1 \otimes_K y_i + \sum x_i \otimes_K y_i \otimes_K 1, \quad \ldots,$$

whose n-th cohomology is $H^n(L/K, \mathrm{G_a})$. But $H^1(L/K, \mathrm{G_a}) = 0$ since L/K is a faithfully flat extension (see [29, Ch. 17, Ex. 10]). Then $l \in \mathrm{Ker}\,\delta_1 = \mathrm{Im}\,\delta_0$ and hence there exists some $x \in L$ such that $l = 1 \otimes_K x - x \otimes_K 1$. Since $dl = \varepsilon(d)l$ for all $d \in D$, we have $(dx) \otimes_K 1 = 1 \otimes_K (dx)$ for all $d \in D^+$. This implies $dx \in K$ for all $d \in D^+$.

(2) Grouplike elements in $L \otimes_K L$ are precisely 1-cocycles in the complex:

$$\{1\} \to \mathrm{G_m}(L) \xrightarrow{\delta_0} \mathrm{G_m}(L \otimes_K L) \xrightarrow{\delta_1} \mathrm{G_m}(L \otimes_K L \otimes_K L) \xrightarrow{\delta_2} \cdots,$$
$$\delta_0(x) = (1 \otimes_K x)(x \otimes_K 1)^{-1} = x^{-1} \otimes_K x,$$
$$\delta_1(\sum x_i \otimes_K y_i) = (\sum 1 \otimes_K x_i \otimes_K y_i)(\sum x_i \otimes_K 1 \otimes_K y_i)^{-1}(\sum x_i \otimes_K y_i \otimes_K 1), \quad \ldots,$$

whose n-th cohomology is $H^n(L/K, \mathrm{G_m})$. But $H^1(L/K, \mathrm{G_m}) = \mathrm{Pic}(L/K) \subset \mathrm{Pic}(K) = \{1\}$ since K is a finite product of fields. Then $g \in \mathrm{Ker}\,\delta_1 = \mathrm{Im}\,\delta_0$ and hence there exists some $x \in \mathrm{G_m}(L)$ such that $g = x^{-1} \otimes_K x$. Since $dg = \varepsilon(d)g$, we have

$$1 \otimes_K dx = d(1 \otimes_K x) = d((x \otimes_K 1)g) = d(x)x^{-1} \otimes_K x$$

for all $d \in D$. By multiplying $1 \otimes_K x^{-1}$, we have $1 \otimes_K d(x)x^{-1} = d(x)x^{-1} \otimes_K 1$ for all $d \in D$, which implies $d(x)x^{-1} \in K$ for all $d \in D$. $\square$

Proposition 3.9.14. *L/K is a $\mathrm{G_a}$-primitive (resp., $\mathrm{G_m}$-primitive) extension iff L/K is a PV extension and $\mathrm{G}(L/K)$ is of $\mathrm{G_a}$-type (resp., $\mathrm{G_m}$-type).*

Proof. ("Only if" part.) This has been proved in Lemma 3.9.12.

("If" part.) Let $k[l]$ (resp., $k[g, g^{-1}]$) be the Hopf algebra for L/K. By Lemma 3.9.13, there exists the corresponding $x \in L$. Then $K\langle x\rangle$ is an intermediate AS D-module algebra of L/K such that $K\langle x\rangle/K$ is a PV extension. Since the Hopf algebras of $K\langle x\rangle/K$ and L/K coincide, we have $L = K\langle x\rangle$. □

3.9.4. **The solvability theorem.**

Definition 3.9.15. Let F/K be a finitely generated extension of AS D-module algebras. We call F/K a *liouvillian extension* iff $F^D = K^D = k$ and there exists a sequence of AS D-module algebras

$$K = F_0 \subset F_1 \subset \cdots \subset F_r = F \tag{3.25}$$

such that each F_i/F_{i-1} ($i = 1, \ldots, r$) is at least one of the following types: $\mathrm{G_a}$-primitive extension, $\mathrm{G_m}$-primitive extension, or finite etale extension. In this case, the sequence (3.25) is called *liouvillian chain.* Moreover, F/K is called a *liouvillian extension of type (j)* ($j = 1, \ldots, 10$) iff F/K has a liouvillian chain (3.25) such that each extension F_i/F_{i-1} ($i = 1, \ldots, r$) is

(1) $\mathrm{G_a}$-primitive, $\mathrm{G_m}$-primitive, or finite etale,
(2) $\mathrm{G_a}$-primitive or $\mathrm{G_m}$-primitive,
(3) $\mathrm{G_m}$-primitive or finite etale,
(4) $\mathrm{G_a}$-primitive or finite etale,
(5) $\mathrm{G_a}$-primitive or $\mathscr{G}$-primitive for a finite solvable group $\mathscr{G}$,
(6) $\mathrm{G_m}$-primitive,
(7) $\mathrm{G_a}$-primitive,
(8) finite etale,
(9) $\mathscr{G}$-primitive for a finite solvable group $\mathscr{G}$,
(10) trivial (i.e. $F_i = F_{i-1}$),

respectively. Here we are taking priority of the compatibility with [12, §24]. We observe an anticopied $\mathscr{G}$-primitive extension for a finite solvable group $\mathscr{G}$ is identified with a Galois extension by radicals and is also a liouvillian extension of type (6).

To show the solvability theorem, we need the following lemma (cf. [12, §21]).

Lemma 3.9.16. *Let L/K be a finitely generated PV extension and F an AS D-module algebra including L such that $F^D = K^D = k$. Take one $t \in F$. Then $L\langle t\rangle/K\langle t\rangle$ is a finitely generated PV extension and $\mathbf{G}(L\langle t\rangle/K\langle t\rangle) \simeq \mathbf{G}(L/K\langle t\rangle \cap L)$.*

Proof. By Theorem 3.8.7, there exists a GL_n-primitive $X = (x_{ij}) \in GL_n(L)$ over K such that $L = K\langle x_{ij}\rangle$. Since $L\langle t\rangle = K\langle t, x_{ij}\rangle$, we have that $L\langle t\rangle/K\langle t\rangle$ is a finitely generated PV extension. Write $M = K\langle t\rangle \cap L$, $Z = (X^{-1} \otimes_M 1)(1 \otimes_M X) = (z_{ij})$, and $Z^{-1} = (w_{ij})$. Then $H = k[z_{ij}, w_{ij}]$ becomes the Hopf algebra for L/M. Similarly by writing $Z' = (X^{-1} \otimes_{K\langle t\rangle} 1)(1 \otimes_{K\langle t\rangle} X) = (z'_{ij})$, and $(Z')^{-1} = (w'_{ij})$, we obtain the Hopf algebra $H' = k[z'_{ij}, w'_{ij}]$ for $L\langle t\rangle/K\langle t\rangle$. It follows that there exists a surjective Hopf algebra map $\varphi : H \twoheadrightarrow H'$, $z_{ij} \mapsto z'_{ij}$. This implies that $\mathbf{G}(L\langle t\rangle/K\langle t\rangle)$ is a closed subgroup scheme of $\mathbf{G}(L/M)$. Let $I = \operatorname{Ker}\varphi$ be the corresponding Hopf ideal.

φ is the restriction (to H) of the natural map $\tilde{\varphi} : L \otimes_M L \to L\langle t\rangle \otimes_{K\langle t\rangle} L\langle t\rangle$. Since the coideal $I \cdot (L \otimes_M L)$ of $L \otimes_M L$, which corresponds to I, is included in $\operatorname{Ker}\tilde{\varphi}$, we have $\{a \in L \mid a \otimes_M 1 - 1 \otimes_M a \in I \cdot (L \otimes_M L)\} \subset \{a \in L \mid a \otimes_M 1 - 1 \otimes_M a \in \operatorname{Ker}\tilde{\varphi}\} = L \cap K\langle t\rangle = M$. This implies that the intermediate AS D-module algebra of L/M which corresponds to I is M. Thus $I = 0$. □

Theorem 3.9.17. *Let L/K be a finitely generated PV extension. Then the following are equivalent:*

(a) *L/K is a liouvillian extension.*

(b) *There exists a liouvillian extension F/K such that $L \subset F$.*

(c) *$\mathbf{G}(L/K)$ is liouvillian.*

When k is algebraically closed, these are equivalent to:

(d) *$\mathbf{G}(L/K)^\circ$ is solvable.*

Proof. ((a) $\Rightarrow$ (b)) This is clear.

((b) $\Rightarrow$ (c)) Take a liouvillian chain of F/K:

$$K = F_0 \subset F_1 \subset \cdots \subset F_r = F.$$

We use induction on r. The case $r = 0$ is obvious. Let $r > 0$. Since there are finite $t_1, \ldots, t_s \in F$ such that $F_1 = K\langle t_1, \ldots, t_s\rangle$, we have that $L\langle t_1, \ldots, t_s\rangle/F_1$ is a finitely generated PV extension and $\mathbf{G}(L\langle t_1, \ldots, t_s\rangle/F_1) \simeq \mathbf{G}(L/F_1 \cap L)$ by Lemma 3.9.16. By the inductive assumption, $\mathbf{G}(L/F_1 \cap L)$ is liouvillian.

Let A be the principal algebra for L/K. If F_1/K is a finite etale extension, then $F_1 \cap L \subset \pi_0(A)$ by Lemma 3.9.9. Hence we have $\mathrm{G}(L/F_1 \cap L) \supset \mathrm{G}(L/\pi_0(A)) = \mathrm{G}(L/K)^\circ$ (Lemma 3.9.8). Thus, $\mathrm{G}(L/F_1 \cap L)^\circ = \mathrm{G}(L/K)^\circ$ and hence (c) holds by Lemma 3.9.2 (1).

If F_1/K is a $\mathrm{G_a}$-primitive extension, then there exists a $\mathrm{G_a}$-primitive $x \in F_1$ such that $F_1 = K\langle x \rangle$. Write $L_1 = F_1 \cap L$. One sees that L_1/K is also a $\mathrm{G_a}$-primitive extension (see [27, (2.9a)]). Let A_1 be the principal algebra for L_1/K. By applying Lemma 3.9.8 to L_1/K, we have

$$\begin{aligned} &\mathrm{G}(L/K) \rhd \mathrm{G}(L/\pi_0(A_1)) \rhd \mathrm{G}(L/L_1), \\ &\mathrm{G}(L/K)/\mathrm{G}(L/\pi_0(A_1)) = \mathrm{G}(\pi_0(A_1)/K) \quad : \text{finite etale}, \\ &\mathrm{G}(L/\pi_0(A_1))/\mathrm{G}(L/L_1) = \mathrm{G}(L_1/\pi_0(A_1)) = \mathrm{G}(L_1/K)^\circ. \end{aligned}$$

Therefore $\mathrm{G}(L/K)$ is liouvillian.

If F_1/K is a $\mathrm{G_m}$-primitive extension, then there exists a $\mathrm{G_m}$-primitive $x \in F_1$ such that $F_1 = K\langle x \rangle$. Write $L_1 = F_1 \cap L$. One sees that L_1/K is also a $\mathrm{G_m}$-primitive extension (see [27, (2.9b)]). Then we obtain (c) in the same way to the above.

((c) $\Rightarrow$ (a)) Let $\mathrm{G}(L/K) = \mathrm{G}_0 \rhd \mathrm{G}_1 \rhd \cdots \rhd \mathrm{G}_r = \{1\}$ be an LNC and L_i $(i = 0, \ldots, r)$ the intermediate AS D-module algebra which corresponds to G_i. Then by Lemma 3.9.8 and by Proposition 3.9.14, $K = L_0 \subset L_1 \subset \cdots \subset L_r = L$ is a liouvillian chain. □

By Proposition 3.9.4, we have the following.

Corollary 3.9.18. *Let L/K be a finitely generated PV extension with the principal algebra A. If L/K is a liouvillian extension, then there exists a liouvillian chain*

$$K = L_0 \subset \pi_0(A) = L_1 \subset L_2 \subset \ldots \subset L_r = L$$

such that each L_i/L_{i-1} $(i = 2, \ldots, r)$ is $\mathrm{G_m}$-primitive or $\mathrm{G_a}$-primitive extension.

Corollary 3.9.19. *Let L/K be a finitely generated PV extension. Then L/K is (included in) a liouvillian extension of type (j) $(j = 1, \ldots, 10)$ iff*

(1) $\mathrm{G}(L/K)$ *is liouvillian,*
(2) $\mathrm{G}(L/K)$ *has an RLNC,*
(3) $\mathrm{G}(L/K)^\circ$ *is $\mathrm{G_m}$-composite,*
(4) $\mathrm{G}(L/K)^\circ$ *is unipotent,*
(5) $\pi_0\mathrm{G}(L/K)$ *is finite constant and solvable, and* $\mathrm{G}(L/K)^\circ$ *is unipotent,*
(6) $\mathrm{G}(L/K)$ *is $\mathrm{G_m}$-composite,*
(7) $\mathrm{G}(L/K)$ *is unipotent,*

(8) $\mathrm{G}(L/K)$ *is finite etale,*

(9) $\mathrm{G}(L/K)$ *is finite constant and solvable,*

(10) $\mathrm{G}(L/K)$ *is trivial,*

respectively.

This corollary can become more explicit when K is a perfect field and k is algebraically closed. In such a case, if $(L/K, A, H)$ is a finitely generated PV extension, then $A \otimes_K A$ is reduced (see [29, Ch. 6, Ex. 2]), and so H is reduced. Thus $\mathrm{G}(L/K)$ corresponds to the affine algebraic group $\mathrm{G}(L/K)(k) = \mathrm{Aut}_{D, K\text{-alg}}(L)$ in the sense of [29, (4.5)]. There we can do the following replacement on the condition about $\mathrm{G}(L/K)$:

(1) $\mathrm{G}(L/K)^\circ$ is solvable ($\Leftrightarrow$ $\mathrm{G}(L/K)^\circ$ is triangulable),

(2) $\mathrm{G}(L/K)$ is solvable,

(3) $\mathrm{G}(L/K)^\circ$ is diagonalizable,

(4) $\mathrm{G}(L/K)^\circ$ is unipotent,

(5) $\mathrm{G}(L/K)$ is solvable and $\mathrm{G}(L/K)^\circ$ is unipotent,

(6) $\mathrm{G}(L/K)(k)$ is solvable and quasicompact (in the Kolchin's sense),

(7) $\mathrm{G}(L/K)$ is unipotent,

(8) $\mathrm{G}(L/K)$ is finite constant,

(9) $\mathrm{G}(L/K)$ is finite constant and solvable,

(10) $\mathrm{G}(L/K)$ is trivial.

References

[1] K. Amano, *Liouvillian extensions of artinian simple module algebras*, preprint.

[2] K. Amano, A. Masuoka, *Picard-Vessiot extensions of artinian simple module algebras*, to appear in J. Algebra (2005).

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

[4] A. Białynicki-Birula, *On Galois theory of fields with operators*, Amer. J. Math. 84 (1962), 89–109.

[5] P. Deligne, *Catégories tannakiennes*, In P. Cartier et al., editor, "Grothendieck Festschrift", Vol. 2, Progress in Math. 87, Birkhäuser, 1990, pp. 111–195.

[6] P. Deligne, J.S. Milne, *Tannakian categories*, In P. Deligne et al., editor, "Hodge cycles, motives and Shimura varieties", Lecture Notes in Math. 900, Springer, 1982, pp. 101–228.

[7] F. DeMeyer, E. Ingraham, *"Separable algebras over commutative rings"*, Lecture Notes in Math. 181, Springer, 1971.

[8] C.H. Franke, *Picard-Vessiot Theory of Linear Homogeneous Difference Equations*, Trans. Amer. Math. Soc. 108 (1963), 491–515.

[9] P. Freyd, *"Abelian categories—an introduction to the theory of functors"*, Harper's Series in Modern Mathematics, Harper & Row, Publishers, New York, 1964.

[10] P.A. Hendriks, M.F. Singer, *Solving difference equations in finite terms*, J. Symbolic Computation 27 (1999), 239–259.

[11] R.G. Heyneman, M.E. Sweedler, *Affine Hopf algebras II*, J. Algebra 16 (1970), 271–297.
[12] E.R. Kolchin, *Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations*, Ann. of Math. 49 (1948), 1–42.
[13] E.R. Kolchin, *"Differential algebra and algebraic groups"*, Pure and Applied Mathematics 54, Academic Press, New York, 1973.
[14] A.H.M. Levelt, *Differential Galois theory and tensor products*, Indag. Mathem., N.S., 1(4) (1990), 439–450.
[15] A. Masuoka, T. Yanai, *Hopf module duality applied to X-outer Galois theory*, J. Algebra 265 (2003), 229–246.
[16] S. Montgomery, *"Hopf algebras and their actions on rings"*, CBMS Reg. Conf. Series 82, AMS, 1993.
[17] W.D. Nichols, *Quotients of Hopf algebras*, Comm. Algebra 6 (1978), 1789–1800.
[18] K. Okugawa, *Basic properties of differential fields of an arbitrary characteristic and the Picard-Vessiot theory*, J. Math. Kyoto Univ. 2–3 (1963), 295–322.
[19] M. Petkovšek, *Hypergeometric solutions of linear recurrences with polynomial coefficients*, J. Symbolic Computation 14 (1992), 243–264.
[20] M. van der Put, M.F. Singer, *"Galois theory of difference equations"*, Lecture Notes in Math. 1666, Springer, 1997.
[21] M. van der Put and M.F. Singer, *"Galois theory of linear differential equations"*, Grundlehren Math. Wiss. 328, Springer, 2003.
[22] H.-J. Schneider, *Principal homogeneous spaces for arbitrary Hopf algebras*, Israel J. Math. 72 (1990), 167–195.
[23] M.E. Sweedler, *"Hopf algebras"*, Benjamin, New York, 1969.
[24] M.E. Sweedler, *The predual theorem to the Jacobson-Bourbaki theorem*, Trans. Amer. Math. Soc. 213 (1975), 391–406.
[25] M. Takeuchi, *A correspondence between Hopf ideals and sub-Hopf algebras*, Manuscripta Math. 7 (1972), 251–270.
[26] M. Takeuchi, *Relative Hopf modules—equivalences and freeness criteria*, J. Algebra 60 (1979), 452–471.
[27] M. Takeuchi, *A Hopf algebraic approach to the Picard-Vessiot theory*, J. Algebra 122 (1989), 481–509.
[28] A. Tyc, P. Wiśniewski, *The Lasker-Noether theorem for commutative and noetherian module algebras over a pointed Hopf algebra*, J. Algebra 267 (2003), 58–95.
[29] W.C. Waterhouse, *"Introduction to affine group schemes"*, Grad. Texts in Math. 66, Springer, 1979.