PRELIMINARIES ON DIXMIER CONJECTURE

YOSHIFUMI TSUCHIMOTO

ABSTRACT. We gather some basic facts concerning algebra endomorphisms of Weyl algebras $A_n(k)$ for fields k with positive characteristic p. These facts could lead some preliminary results on Dixmier conjecture.

CONTENTS

1. INTRODUCTION

Our aim in this paper is to gather some basic facts concerning algebra endomorphisms of Weyl algebras $A_n(k)$ for fields k with positive characteristic p.

1991 *Mathematics Subject Classification.* 14R15(16W20).

Key words and phrases. Jacobian conjecture, Dixmier conjecture, Noncommutative algebra.

A study of such object may lead (Lemma 2) to some progress in the Dixmier conjecture (conjecture 1) which states that any algebra endomorphism of Weyl algebra over a field of characteristic zero is actually invertible.

It turns out that $A_n(k)$ is a free module of rank p^{2n} over its center $Z(A_n(k))$ (Lemma 3) and that any k-algebra endomorphism ϕ of $A_n(k)$ sends central elements to central elements (Lemma4).

Thus the study of ϕ may be deeply related to the study of sheaves of matrix algebras over polynomial algebras $Z(A_n(k))$.

In particular, we may use traces to obtain a nice formula for candidate of inverse of ϕ (Proposition 1).

On the other hand, suppose we are given an algebra endomorphism ϕ of the Weyl algebra $A_n(\mathfrak{K})$ over an algebraic number field $\mathfrak{K}$. Then we have, for almost all (that is, for all except finite number of) prime ideal $\mathfrak{p}$ of $\mathfrak{K}$, an algebra endomorphism of $A_n(k(\mathfrak{p})$ over the residue field $k(\mathfrak{p})$. We prove that almost all such maps are injective and that geometric degree of these maps are bounded by a constant which is independent of $\mathfrak{p}$ (Proposition 2).

2. Notations

All rings are assumed to be unital, associative. All homomorphisms are assumed to be unital. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

For any ring R and for any positive integer l, we put

$$M_l(R) = (\text{the set of } l \times l\text{-matrix with coefficients in } R.)$$

For any ring k, we denote by $A_n(k)$ the Weyl algebra.

$$A_n(k) = k\langle \xi_1, \xi_2, \dots, x_n, \eta_1, \eta_2, \dots, \eta_n\rangle/(\eta_j\xi_i - \xi_i\eta_j - \delta_{ij}; 1 \leq i, j \leq n)$$

where δ_{ij} is the Kronecker's delta.

If k is a field with characteristic p, then we further employ the following notations.

$Z_n(k) = Z(A_n(k))$ the center of $A_n(k)$ (Later we prove that $Z_n(k)$ is actually equal to $k[\xi_1^p, \xi_2^p, \dots, \xi_n^p, \eta_1^p, \eta_2^p, \dots, \eta_i^p]$).

$T_i = (\xi_i^p)^{1/p}$

$U_i = (\eta_i^p)^{1/p}$

$S_n(k) = Z_n(k)^{1/p} = k^{1/p}[T_1, T_2, \dots, T_n, U_1, U_2, \dots, U_n]$. ($p$-th roots are taken in the usual sense of commutative algebra. $S_n(k)$ is a commutative algebra over $Z_n(k)$.)

$K_n(k) = Q(Z_n(k))$, the quotient field of $Z_n(k)$.

$D_n(k) = A_n(k) \otimes_{Z_n(k)} K_n(k)$

$L_n(k) = Q(S_n(k))$.

$B_n(k) = A_n(k) \otimes_{Z_n(k)} S_n(k)$ ($\cong M_{p^n}(S_n(k))$)

$\mathcal{V}_n(k) = \oplus_{i=1}^{p^n} S_n(k)$

$E_n(k) = A_n(k) \otimes_{Z_n(k)} L_n(k)$ ($\cong M_{p^n}(L_n(k))$)

$\alpha_i = \xi_i - T_i$

$\beta_i = \eta_i - U_i$

$\overline{A_n}$: a copy of A_n

(Identified with the image of ϕ when ϕ is injective).

$\overline{Z_n} = Z(\overline{A_n})$: a copy of Z_n

$\overline{S_n}$: a copy of S_n (extension of $\overline{Z_n}$)

Similarly we use a notation $\overline{\xi_i}, \overline{\eta_i}, \overline{T_i}, \overline{U_i}$ to indicate a copy of non-bar counterparts.

For a matrix x, we denote by $\lambda(x), \rho(x), \mathrm{ad}(x)$ the left action, the right action, and the adjoint action by x, respectively.

$$\lambda(x)y = xy, \quad \rho(x)y = yx, \quad ad(x)y = xy - yx$$

2.1. **A presentation of the full matrix algebra.**

Lemma 1. *Let k be a field of characteristic p. Then a k-algebra $\mathfrak{M}$ which is generated by $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_n$ with the relations*

$$[\beta_j, \alpha_i] = \delta_{ji}, \beta_j^p = 0, \alpha_i^p = 0 \qquad (i, j = 1, 2, \dots, n)$$

(where δ_{ij} is the Kronecker's delta) is isomorphic to the full matrix algebra $M_{p^n}(k)$.

Proof. Since $M_{p^n}(k)$ is isomorphic to a tensor product of n copies of the matrix algebra $M_p(k)$, we may assume that $n = 1$. We define elements $\mu, \nu \in M_p(k)$ as follows.

$$\mu = (\delta_{i+1,j}), \qquad \nu = ((p - j)\delta_{i,j+1}) \tag{1}$$

Then μ, ν satisfies the same relation as α_1, β_1. In other words, we have a k-algebra homomorphism ϕ from $\mathfrak{M}$ to $M_p(k)$ with $\phi(\alpha_1) = \mu, \phi(\beta_1) = \nu$.

On the other hand, it is easy to see that the algebra $\mathfrak{M}$ is linearly generated by $\{\alpha^i \beta^j; 0 \leq i, j \leq p - 1\}$ and hence that its dimension is not greater than p^2.

By a dimension argument we see that the algebra homomorphism ϕ is an isomorphism.

□

2.2. **light exponential function.** For an element L of an algebra over a field k of characteristic $p > 0$, we may define light exponential of L by

$$\mathrm{ex}(L) = \sum_{i=0}^{p-1} \frac{1}{i!} L^i.$$

(The ex is obtained by cut exponential function off the tail after p).

If L_1, L_2 commutes and $\underline{L_1^i L_2^j = 0 \text{ whenever } i + j \geq p}$, then we have

$$\mathrm{ex}(L_1 + L_2) = \mathrm{ex}(L_1)\,\mathrm{ex}(L_2)$$

In particular, if $L^p = 0$ then we have

$$\mathrm{ex}(L)\,\mathrm{ex}(-L) = 1$$

There is a differential equation for the light exponential function.

$$d/dT(\mathrm{ex}(T)) = \mathrm{ex}(T) + T^{p-1}$$

Furthermore, the following equations holds for any constant c_1, c_2.

$$\mathrm{ex}(c_1\mu)\,\mathrm{ex}(c_2\nu) = \mathrm{ex}(c_2(\nu - c_1 E - c_1^p \mu^{p-1}))\,\mathrm{ex}(c_1\mu)$$
$$\mathrm{ex}(c_1\mu)\,\mathrm{ex}(c_2\nu)\,\mathrm{ex}(-c_1\mu) = \mathrm{ex}(c_2(\nu - c_1 E - c_1^p \mu^{p-1}))$$

$$[\mathrm{ex}(c_1\nu), \mu] = c_1\,\mathrm{ex}(c_1\nu) + c_1^p \nu^{p-1}$$
$$[\mathrm{ex}(c_1\mu), \nu] = -c_1\,\mathrm{ex}(c_1\mu) - c_1^p \mu^{p-1}$$

$$\mathrm{ex}(c_1\mu)\nu\,\mathrm{ex}(-c_1\mu) = \nu - c_1 1_p - c_1^p \mu^{p-1}$$

$$\mathrm{ex}(c_1\nu)\mu\,\mathrm{ex}(-c_1\nu) = \mu + c_1 1_p + c_1^p\nu^{p-1}$$
$$\mathrm{ex}(-c_1\mu)\nu\,\mathrm{ex}(c_1\mu) = \nu + c_1 1_p + c_1^p\mu^{p-1}$$
$$\mathrm{ex}(-c_1\nu)\mu\,\mathrm{ex}(c_1\nu) = \mu - c_1 1_p - c_1^p\nu^{p-1}$$

3. First properties of Weyl algebras

For any ring k we denote by $A_n(k)$ the Weyl algebra:

$$A_n(k) = k\langle \xi_1, \xi_2, \ldots, \xi_n, \eta_1, \eta_2, \ldots, \eta_n\rangle/(\eta_j\xi_i - \xi_i\eta_j - \delta_{ij})$$

where δ_{ij} is the Kronecker's delta.

One of the good ways to compute multiplications of elements in $A_n(k)$ appears in [2, formula (11,4)]. For any variable η, ξ with the canonical commutation relation $\eta\xi - \xi\eta = 1$,and for any pair of "normally ordered" polynomials $f(\xi,\eta) = \sum f_{i,j}\xi^i\eta^j$ and $g(\xi,\eta) = \sum g_{i,j}\xi^i\eta^j$, one has the following formula

$$f(\xi,\eta)g(\xi,\eta) = \sum_{k=0}^{\infty} \frac{1}{k!}\partial_\eta^k f(\xi,\eta) * \partial_\xi^k g(\xi,\eta)$$

where $*$ stands for an 'multiplication as though ξ, η commutes'. This formula is valid and proved in the book cited above only if characteristic of the coefficient field is 0. If the characteristic p of the coefficient field is positive, then we replace ∞ in the above formula by $p-1$ and obtain a valid formula in this case. The proof is almost the same. It is well suited for computer calculation using commutative polynomials and differentiations.

Dixmier conjectures that

Conjecture 1. *Every $\mathbb{C}$-algebra endomorphism ϕ of $A_n(\mathbb{C})$ is invertible (that is, it is an automorphism).*

Since $A_n(\mathbb{C})$ is simple (has no nontrivial both-sided ideal), we know that ϕ above is injective. The question therefore is the surjectivity of ϕ.

3.1. reduction to characteristic p.

Suppose we are given a $\mathbb{C}$-algebra endomorphism ϕ of $A_n(\mathbb{C})$. Since the algebra $A_n(\mathbb{C})$ is finitely generated over $\mathbb{C}$, the endomorphism ϕ is actually defined over a ring R which is finitely generated algebra over $\mathbb{Q}$.

By a specialization argument we may assume $R = \mathfrak{O}(\mathfrak{K})[1/f]$, where $\mathfrak{K}$ is a finite extension field of $\mathbb{Q}$, $\mathfrak{O}(\mathfrak{K})$ is the ring of all algebraic integers in $\mathfrak{K}$, f is a non zero element of $\mathfrak{O}(\mathfrak{K})$.

For almost all (that is, all except finite number of) prime ideals $\mathfrak{p}$ of $\mathfrak{O}(\mathfrak{K})$, we obtain an algebra endomorphism $\phi_\mathfrak{p}$ of an algebra $A_n(k(\mathfrak{p}))$ over $k(\mathfrak{p})$ where $k(\mathfrak{p}) = \mathfrak{O}(\mathfrak{K})/\mathfrak{p}$ is a field of a positive characteristic p.

Lemma 2. *ϕ is invertible if and only if homomorphisms $\phi_\mathfrak{p}$ are invertible for all except finite number of primes $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}(\mathfrak{K}))$.*

Proof. The "only if" part is clear. To prove "if", we suppose on the contrary that ϕ is not invertible. This means, as we mentioned, that ϕ is not surjective. Then there exists a nonzero linear functional [1] χ such that $\chi \circ \phi = 0$. It is easy to see that χ defines a non zero linear functional $\chi_\mathfrak{p}$ on $A_n(k(\mathfrak{p}))$ for all except finite

[1] Note added in proof: The functional χ should be chosen more carefully. We will correct this in a forthcoming paper.

number of primes $\mathfrak{p}$, and that $\chi_p e \circ \phi_{\mathfrak{p}} = 0$. this is a contradiction, and the lemma is proved. □

It is thus worthwhile to study $A_n(k)$ and its automorphism when k has a positive characteristic.

3.2. Weyl algebras over fields of positive characteristics and their centers.

Lemma 3. *Let k be a field of characteristic p. We have the following facts.*

(1) *ξ_i^p, η_j^p belongs to the center of $A_n(k)$.*
(2) *More precisely, the center $Z_n(k) = Z(A_n(k))$ of the ring $A_n(k)$ is given by*
$$Z_n(k) = k[\xi_1^p, \ldots, \xi_n^p, \eta_1^p, \ldots, \eta_n^p].$$
(3) *$A_n(k)$ is a free $Z_n(k)$-module of rank p^{2n}.*
(4) *Let $a = (a_1, \ldots, a_n), b = (b_1, \ldots b_n)$ be elements of k^n. Let $I_{a,b}$ be an ideal of $A_n(k)$ generated by $(\xi_1 - a_1)^p, \ldots, (\xi_n - a_n)^p, (\eta_1 - b_1)^p, \ldots, (\eta_n - b_n)^p$. Then we have*
$$A_n(k)/I_{a,b} \overset{\pi_{a,b}}{\cong} M_{p^n}(k).$$
(5) *If the field k is algebraically closed, then any maximal (both-sided) ideal of $A_n(k)$ is of the form $I_{a,b}$ above.*

Proof. (1) easy.
(2) Write
$$f = \sum_{I,J} f_{IJ} \xi^I \eta^J$$
and compute $[\xi_i, f]$ and $[\eta_j, f]$ term by term.
(3)
$$A_n(k) = \bigoplus_{0 \le i_1, \ldots, i_n, j_1, \ldots, j_n \le p-1} Z_n(k) \xi_1^{i_1} \xi_2^{i_2} \xi_3^{i_3} \ldots \xi_n^{i_n} \eta_1^{i_1} \eta_2^{i_2} \eta_3^{i_3} \ldots \eta_n^{i_n}.$$
(4) is a direct consequence of Lemma 1. For the reference purposes, we record here another explanation. By considering a translation in ξ- and η-directions, we may well assume $a = b = 0$. Consider an action of $A_n(k)$ on $A = k[\xi_1, \ldots, \xi_n]/(\xi_1^p, \ldots, \xi_n^p)$ defined by the following formula.

$$P.f = P(\xi_1, \ldots, \xi_n, \partial_1, \ldots, \partial_n).f \tag{2}$$

We may then verify that this gives a well-defined action of $A_n(k)/I_{0,0}$ on the p^n-dimensional vector space A.

If an element P in $A_n(k)/I_{0,0}$ satisfy
$$P.1 = 0, P.\xi = 0, \ldots, P.\xi^{p-1} = 0$$
then we may easily see that $P = 0$. This means the homomorphism
$$\pi_{0,0} : A_n(k)/I_{0,0} \to \mathrm{End}_{\mathrm{k\text{-}module}}(A)$$
is injective. A dimension argument now shows that $\pi_{0,0}$ is a bijection.

(5) Let M be an ideal of $A_n(k)$. We consider a sheaf $(\widetilde{A_n(k)/M})$ of algebras on $\mathrm{Spec}(Z_n(k))$ which corresponds to the $Z_n(k)$-module $A_n(k)/M$. Since $A_n(k)$ is a finitely generated module over a polynomial ring $Z_n(k)$, There exists a closed point $\mathfrak{m}$ of $Z_n(k)$ such that fiber $((\widetilde{A_n(k)/M})|\mathfrak{m}) = A_n(k)/(M + \mathfrak{m}A_n(k))$ is nonzero. Since M is maximal, this implies that $\mathfrak{m} \subset M$. The rest of the proof is easy (Use Nullstellensatz.)

3.3. **Algebra endomorphisms and centers of Weyl algebras.**

Lemma 4. *Let k be a field of characteristic $p > 0$. For any k-algebra endomorphism ϕ of $A_n(k)$,*

1. *$\pi_{a,b} \circ \phi$ is a surjective homomorphism for all $(a, b) \in k^{2n}$.*
2. *$\phi(Z_n(k)) \subset Z_n(k)$.*

Proof. We may assume that k is an algebraically closed field.
(1) The kernel of $\pi_{a,b}\circ\phi$ is an ideal of $A_n(k)$ and therefore, by a dimension argument, is one of the maximal ideals of $A_n(k)$. It also follows that $\pi_{a,b} \circ \phi$ is surjective.
(2) The result (1) implies that for any $(a, b) \in k^{2n}$ we have

$$\phi(Z_n(k)) \subset I_{a,b} + k$$

Thus the claim deduces to the following sublemma.

Sublemma 1.

$$\bigcap_{(a,b)\in k^{2n}} (I_{a,b} + k) = Z_n(k)$$

[proof of sublemma]

The left hand side may be identified with a section of $\widetilde{A_n(k)}$ which reduces to 0 at each k-valued point when we regard it as a section of $(\widetilde{A_n(k)/Z_n}(k))$. Since k is an infinite field, this implies that $f \in Z_n(k)$.

Corollary 1. *$A_n(k)$ is generated by $\phi(A_n(k))$ and $Z(A_n(k))$.*

[proof] We may assume k is algebraically closed. Let B be the algebra generated by $\phi(A_n(k))$ and $Z(A_n(k))$. Then the claim (1) of the previous lemma shows that for any maximal ideal $\mathfrak{m}$ of $Z(A_n(k))$, we have an isomorphism

$$B/\mathfrak{m}B \cong A_n(k)/\mathfrak{m}A_n(k).$$

as $Z(A_n(k))$-modules. Since $A_n(k)$ is finitely generated module over $Z(A_n(k))$, we see immediately that $M = A_n(k)$ as required.

Corollary 2. *Let $\overline{A_n(k)}$ be a copy of $A_n(k)$. Let $\phi : \overline{A_n(k)} \to A_n(k)$ be a k-homomorphism. Let $Z_n(k) = Z(A_n(k))$, $\overline{Z_n(k)} = Z(\overline{A_n(k)})$ be the center of the algebras $A_n(k)$ $\overline{A_n(k)}$, respectively. Then the natural homomorphism*

$$\overline{A_n(k)} \otimes_{\overline{Z_n(k)}} Z_n(k) \to A_n(k)$$

is an isomorphism.

Proof. By the corollary above we already know that it is surjective. Since both hand sides are free $Z_n(k)$-modules of rank p^{2n}, and since $Z_n(k)$ is an integral domain, the map is a bijection. [The surjection admits a splitting. Then we consider determinants.]

□

Corollary 3. *An algebra homomorphism $\phi : A_n(k) \to A_n(k)$ is surjective if and only if its restriction to the center*

$$\phi|^{Z(A_n(k))}_{Z(A_n(k))} : Z(A_n(k)) \to Z(A_n(k))$$

is surjective.

By the birational case of the Jacobian conjecture (which is already known to be true), we conclude that

Corollary 4. *$\phi : A_n(k) \to A_n(k)$ is bijective if and only if the following three conditions hold.*

(1) *$\psi = \phi|_{Z(A_n(k))}^{Z(A_n(k))} : Z(A_n(k)) \to Z(A_n(k))$ is injective.*
(2) *ψ is birational.*
(3) *The Jacobian $\det D(\psi)$ is a nonzero constant.*

3.4. **A splitting algebra of A_n.** In this subsection we assume that k is a field of characteristic $p > 0$. Let $S_n(k) = Z_n(k)^{1/p} = k^{1/p}[T_1, \dots, T_n, U_1, \dots, U_n]$ where $T_i = (\xi_i^p)^{1/p}, U_i = ((\eta_i)^p)^{1/p})$. It is a splitting algebra of $A_n(k)$, as the following lemma tells.

Lemma 5. *The algebra $A_n(k)$ acts on $\mathcal{V} = \oplus_{i=1}^{p^n} S_n(k)$. In other words, there exists a representation Φ of $A_n(k)$ on $\mathcal{V}$.*

$$\Phi(\xi_i) = \mu_i + T_i, \qquad \Phi(\eta_i) = \nu_i + U_i,$$

where elements μ_i, ν_i of $M_{p^n}(k)$ are defined (using notation in Lemma 1) as follows.

$$\mu_i = 1_{p^{i-1}} \otimes \mu \otimes 1_{p^{n-i}}, \nu_i = 1_{p^{i-1}} \otimes \nu \otimes 1_{p^{n-i}}.$$

The representation Φ may be extended to the following isomorphism.

$$\Phi : A_n(k) \otimes_{Z_n(k)} S_n(k) \cong M_{p^n}(S_n(k))$$

Proof. Put $\alpha_i = \xi_i - T_i, \beta_i = \eta_i - U_i (i = 1, \dots, n)$. Then it is easy to show that elements $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ satisfy the relation of generators of the algebra $\mathfrak{M}$ as in Lemma 1.

□

3.5. **The quotient field of the Weyl algebra.** Let k be a field of characteristic $p > 0$. There is a nice "quotient field of the Weyl algebra $A_n(k)$.

Lemma 6. *Let $K_n(k)$ be the quotient field of the center $Z_n(k)$ of the Weyl algebra $Z_n(k)$. Then the following statements hold.*

(1) *$D_n(k) = A_n(k) \otimes_{Z_n(k)} K_n(k)$ is a skew field.*
(2) *$\dim_{K_n(k)} D = p^{2n}$.*
(3) *$M_{p^n}(L_n(k))$ may be regarded as a p^{2n}-dimensional vector space over D with a basis $\{T^I U^J; ||I||_{\ell^\infty} \le p-1, ||J||_{\ell^\infty} \le p-1\}$.*

Proof. (1) $D_n(k)$ is a simple algebra with no zero-divisor except for 0. Then we use Wedderburn's structure theorem.

(2),(3): we may easily see that

$$\dim_{K_n(k)} D_n(k) \le p^{2n}, \quad \dim_{D_n(k)} M_p(L_n(k)) \le p^{2n}.$$

On the other hand we have

$$\dim_{K_n(k)} M_p(L_n(k)) = p^{4n}$$

□

3.6. **definition of reduced trace and reduced norm.** From a general theory of central simple algebra, we have a notion of reduced traces and reduced norms. (See for example [1] for a theory of reduced norms and reduced traces.)

It may be defined as follows. $D_n(k)$ is a central simple algebra over $K_n(k)$. Let Ω be a splitting field Ω of $D_n(k)$. That means, we have an isomorphism of k-algebras

$$\iota : D_n \otimes_{K_n(k)} \Omega \cong M_{p^n}(\Omega).$$

Then for each element x of D_n, it is known that the trace $\operatorname{tr}(\iota(x))$ and the determinant $\det(\iota(x))$ actually belongs to K_n and that they do not actually depend on the choice of the splitting field Ω.

We call them reduced trace and reduced norm of x respectively.

As we already saw in the previous section, $S_n(k)$ is a splitting algebra of $A_n(k)$. Thus we see that the quotient field $L_n(k)$ of $S_n(k)$ is one of the splitting field of $D_n(k)$. We have thus proved that reduced norm and reduced determinant of $A_n(k)$ actually lie in $Z_n(k)$.

3.7. **Algebra endomorphism and splitting of Weyl algebra.**

Lemma 7. *Let k be a algebraically closed field with characteristic $p > 0$. Let $\phi : A_n(k) \to A_n(k)$ be a k-homomorphism, $\psi : Z_n(k) \to Z_n(k)$ its restriction to the center. Then we have the following.*

(1) *ψ extends uniquely to a homomorphism*

$$\hat{\psi} : S_n(k) \to S_n(k)$$

(2) *ϕ extends uniquely to a homomorphism*

$$\hat{\phi} : A_n(k) \otimes_{Z_n(k)} S_n(k) \to A_n(k) \otimes_{Z_n(k)} S_n(k)$$

(3) *Under the isomorphism Φ of lemma 5, $\hat{\phi}$ may be identified with a map*

$$M_p(S_n(k)) \ni M(T,U) \mapsto G(T,U)M(f(T,U))G(T,U)^{-1}$$

where $G(T,U)$ is an element of $\mathrm{GL}_p(S_n(k))$ and $f = {}^a\psi : \mathbb{A}^{2n} \to \mathbb{A}^{2n}$ is a polynomial map associated to the algebra homomorphism $\hat{\psi}$. In other words, we have

$$\Phi(\phi(x)) = Gf^*(\Phi(x))G^{-1}$$

Proof. (1): In any commutative integral domain of characteristic p, p-th root of an element is unique.

(2): For each k-valued point (t,u) of $\mathbb{A}^{2n}$ we obtain a homomorphism $\psi_{t,u} : M_{p^n}(k) \to M_{p^n}(k)$. In other words, we obtain a morphism

$$\check{G} : \mathbb{A}^{2n} \to \mathrm{PGL}_p .$$

But since the sheaf cohomology $H^1(\mathbb{A}^{2n}, \mathbb{G}_m)$ (in Zariski topology) is trivial, we have a lift G of $\check{G}$ and the claim is proved.

Corollary 5 (invariance of trace under algebra endomorphism)**.**

$$\operatorname{trd}(\phi(a)) = \phi(\operatorname{trd}(a))$$

Lemma 8. *The polynomial map f of the lemma above is determined by $G(T,U)$ uniquely up to an addition of an element of $k[T^p, U^p]$. That means, if we have two f's, namely f_1 and f_2, with the same $G(T,U)$, then we have*

$$f_1^*(T) - f_2^*(T) \in k[T^p, U^p], \quad f_1^*(U) - f_2^*(U) \in k[T^p, U^p]$$

Proof. Put $\alpha = \xi - T, \beta = \eta - U$. Then

$$\phi(\xi) - \phi(T) = \phi(\alpha) = G(T,U)\alpha G(T,U)^{-1}, \tag{3}$$

$$\phi(\eta) - \phi(U) = \phi(\beta) = G(T,U)\beta G(T,U)^{-1}. \tag{4}$$

$$\phi(\xi), \phi(\eta) \in k[\xi,\eta], \phi(T), \phi(U) \in k[T,U].$$

3.8. **the geometric degree.**

Definition 1. *Let k be a field of positive characteristic. Then for any k-algebra homomorphism. $\phi : \overline{A_n(k)} \to A_n(k)$, the geometric degree* geomdeg(ϕ) *of ϕ is defined to be the index $[Q(Z_n(k)) : Q(\phi(Z_n(k))]$ of the corresponding field extension.*

Note that if the geometric degree is finite, then by comparing the transcendent degree we see that ϕ is actually injective and the geometric degree is equal to $[K_n(k) : \overline{K_n(k)}]$.

3.9. **uniqueness of an operator p-th root for generators of $A_n(k)$.**

Lemma 9. *If $F \in A_n(k)$ satisfies an identity $F^p = \xi_1^p$, then $F = \xi_1$.*

Proof. See the principal symbol (highest degree part) of F. Then it should be ξ_1. Thus there exists a constant c such that $F = \xi_1 + c$. On the other hand, we have $(\xi_1 + c)^p = \xi_1^p + c^p$. □

3.10. **Algebra endomorphisms of Weyl algebras are determined by its restriction to the center.** In this subsection we assume that k is a field of positive char.

Lemma 10. *The natural group homomorphism* $\mathrm{Aut}_{k\text{-alg}}(A_n(k)) \to \mathrm{Aut}_{k\text{-alg}}(Z_n(k))$ *(restriction map) is injective.*

Proof. The uniqueness of operator p-th root for generators of Z_n. □
Note.

It is not surjective. For example, let k be a field of odd characteristic and consider an algebra automorphism ψ of $Z_1(k)$ given by

$$\psi(\xi^p) = \xi^p, \quad \psi(\eta^p) = -\eta^p.$$

Then by the uniqueness of the operator p-th root we see that the lift ϕ of ψ should satisfy

$$\phi(\xi) = \xi, \quad \phi(\eta) = -\eta.$$

But this ϕ is not an algebra homomorphism.

Lemma 11. *The restriction map*

$$\mathrm{End}_{k\text{-alg}}(A_n(k)) \to \mathrm{End}_{k\text{-alg}}(Z_n(k))$$

is injective.

Proof. Let $\overline{A_n(k)}$ be a copy of $A_n(k)$ and consider two k-algebra homomorphisms

$$\phi^{(1)}, \phi^{(2)} : \overline{A_n(k)} \to A_n(k).$$

Then we have k-algebra isomorphisms

$$\phi^{(1)} \otimes \mathrm{id}_{Z_n(k)} : \overline{A_n(k)} \otimes_{\overline{Z_n(k)}} Z_n(k) \to A_n(k)$$

where $\overline{Z_n(k)}$ is the center of $\overline{A_n(k)}$. Since these two isomorphisms coincide on the center, we deduce from the previous lemma that both maps coincide. □

4. Reduced trace and reduced norm

In this section we study some properties of reduced trace and reduced norm defined in subsection3.6.

4.1. calculation of reduced trace.

Lemma 12. *The trace of a differential operator* $\xi^k(d/d\xi)^l$ *on a vector space* $k[\xi]/(\xi^p)$ *is non zero if and only if* $k = l = p-1$.

[proof] If $k \neq l$ then $\xi^i(d/d\xi)^j$ is represented by a strictly triangular matrix and the trace is 0. If $k = l$, we have

$$(\xi^l(d/d\xi)^l).\xi^s = s(s-1)\dots(s-k+1)\xi^s.$$

Summing up this we obtain the result.

□

Corollary 6.

$$\mathrm{tr}((\mu+T)^k(\nu+U)^l) = \begin{cases} -T^{k_0 p}U^{l_0 p} & \text{if } k = k_0 p + (p-1), l = l_0 p + (p-1) \\ 0 & \text{otherwise} \end{cases}$$

Lemma 13. (1) *If* $0 \leq i, j \leq p-1$, *then* $\mathrm{trd}(\xi^i\eta^j)$ *is an element of* k.
(2)

$$\mathrm{trd}(\xi^i\eta^j) = \begin{cases} -1 & (\text{if } i = j = p-1) \\ 0 & \text{otherwise} \end{cases}$$

A formula for the reduced trace when $n > 1$ is easily obtained by noting that $A_n(k)$ is isomorphic to a tensor product $A_1(k) \otimes_k A_1(k) \otimes_k \cdots \otimes_k A_1(k)$ of $A_1(k)$'s.

Lemma 14. *Let* k *be a field of characteristic* p. *Let* ϕ *be a* k*-endomorphism of* $A_n(k)$. *Let* I, J *be an element of* $\{0, 1, 2, \dots, p-1\}^n$ *(multi-index). Then for any* $f \in Z(A_n(k))$, *we have*

$$\mathrm{trd}(\xi^I\eta^J f) = \begin{cases} -f & \text{if } I = J = (p-1, p-1, \dots, p-1) \\ 0 & \text{otherwise} \end{cases}$$

4.2. invariance of trace and inversion formula.

Lemma 15. *Let* k *be a field of characteristic* p. *Let* ϕ *be a* k*-endomorphism of* $A_n(k)$. *Let* I, J *be an element of* $\{0, 1, 2, \dots, p-1\}^n$ *(multi-index). Then for any* $f \in Z(A_n(k))$, *we have*

$$\mathrm{trd}(\phi(\xi^I\eta^J f)) = \begin{cases} -\phi(f) & \text{if } I = J = (p-1, p-1, \dots, p-1) \\ 0 & \text{otherwise} \end{cases}$$

Proof. This is the same as Corollary 5. One may also prove this by using Corollary 2.

□

For any index set $I \in \mathbb{N}^{2n}$, we denote by I^c the index set $(p-1, p-1, \dots, p-1) - I$.

Corollary 7. *Let k be a field of characteristic p. Let ϕ be a k-endomorphism of $A_n(k)$. Assume we are given a set of p^{2n} elements $\{f_{IJ} \in Z(A_n(k)); I, J \subset \{0, 1, 2, \ldots, p-1\}^n\}$. Let M be the maximum of total degree of $\phi(\xi_1), \ldots, \phi(\xi_n)$, $\phi(\eta_1), \ldots, \phi(\eta_n)$. Then for any set $\{f_{IJ}\}$ of p^{2n} elements of $Z(A_n(k))$, we have*

$$\mathrm{totaldeg}(\phi(\sum_{I,J} f_{IJ}\xi^I\eta^J)) \geq \max_{I,J}(\mathrm{totaldeg}\,\phi(f_{IJ})) - Mp^{2n}$$

Proof. Put $F = \phi(\sum_{I,J} f_{IJ}\xi^I\eta^J)$. Then

$$\mathrm{trd}\, F\phi(\eta)^{J^c}\phi(\xi)^{I^c} = f_{IJ}$$

Thus $\mathrm{totaldeg}(F\phi(\eta)^{J^c}\phi(\xi)^{I^c}) \geq \mathrm{totaldeg}(f_{IJ})$. Noting that total degree is additive ($\mathrm{totaldeg}(FG) = \mathrm{totaldeg}(F) + \mathrm{totaldeg}(G)$), we complete the proof.

□

Proposition 1 (inversion formula)**.** *Let k be a field of characteristic p. Assume we have an injective algebra endomorphism ϕ of $A_n(k)$. We use the notation $\overline{\xi_i} = \phi(\xi_i)$, $\overline{\eta_j} = \phi(\eta_j)$. Then for any element $x \in A_n(k)$, we have*

$$x = -\sum_{I,J} \mathrm{trd}(x\overline{\eta}^{J^c}\overline{\xi}^{I^c})\overline{\xi}^I\overline{\eta}^J$$

Corollary 8. *Under the assumption of the Lemma above, if elements* $\mathrm{trd}(\xi_i\overline{\eta}^{J^c}\overline{\xi}^{I^c})$, $\mathrm{trd}(\eta_i\overline{\eta}^{J^c}\overline{\xi}^{I^c})$ $(i = 1, \ldots, n)$ *are all constants, then ϕ is invertible.*

5. INJECTIVITY $(n = 1)$

5.1. **comments on this section.** When characteristic of a field k is 0, then we know that $A_n(k)$ is simple and that any algebra endomorphism is injective. Even if the characteristic of k is nonzero, all examples of algebra endomorphisms of $A_n(k)$ author knows are injective.

In this section we prove this is true for $n = 1$ case.

5.2. **injectivity($n = 1$).**

Lemma 16. *$\phi : A_n(k) \to A_n(k)$ be a k-homomorphism. Then trans.deg$(\phi(\xi_1^p), \ldots, \phi(\xi_n^p))$ is equal to n.*

[proof] We may assume that k is algebraically closed. The field $k(\xi_1, \ldots, \xi_n)$ has n linearly independent k-derivations $\{\mathrm{ad}(\eta_i)\}_{i=1}^n$. Since $k(\xi_1, \ldots, \xi_n)$ is separable over k, its transcendent degree is equal to the number of linear independent derivations [3, Theorem 4.4.2.]. Thus we conclude that transcendent degree of $k(\xi_1, \ldots, \xi_n)$ is no less than (hence is equal to) n. That means, $\xi_1, \ldots, \xi_n$ are algebraically independent over k.

Lemma 17 $(n = 1)$**.** *Any k-algebra endomorphism $\phi : A_1(k) \to A_1(k)$ is injective.*

[proof] We may assume that the base field k is algebraically closed. $\phi(A_1(k))$ has no zero-divisor except for 0. Thus

$$\phi(A_1(k)) \otimes_{\phi(Z(A_1(k))} Q(\phi(Z(A_1(k)))$$

is a skew field which is of finite rank over $Q(\phi(Z(A_1(k))))$. If the transcendent degree of the field K is 1, then it contradicts with Tsen's theorem. Thus $\phi(\xi^p), \phi(\eta^p)$ are algebraically independent over k.

□

6. MULTIDEGREE MONOIDS AND LATTICES

For any element $f = \sum_{I,J} f_{IJ}\xi^I\eta^J \in A_n(k)$, we denote by multideg$(f)$ the multidegree of f. That means,

$$\operatorname{multideg}(f) = \max\{(I,J) \in \mathbb{N}^{2n}; f_{IJ} \neq 0\},$$

where we employ the lexicographic order on $\mathbb{N}^{2n}$. For any subalgebra A of $A_n(k)$, we define its multidegree monoid multideg(A) as follows.

$$\operatorname{multideg}(A) = \{\operatorname{multideg}(f); f \in A\}.$$

It is a sub monoid of $\mathbb{N}^{2n}$. We use several norms for indices in $\mathbb{N}^{2n}$. Among them is the "ℓ^1-norm" $|t_1| + \cdots + |t_{2n}|$. of $(t_1, \ldots, t_{2n})$ The total degree totaldeg(f) of an element f of $A_n(k)$ is then defined to be the ℓ^1-norm of multideg(f). By a total degree of a derivation or an algebra endomorphism of $A_n(k)$ we mean the maximum of the total degree of the image of the standard generators $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n$.

Definition 2. *For any subset S of $\mathbb{N}^{2n}$, we denote by $S_{\leq d}$ the set of all elements of S whose ℓ^1-norms are less than or equal to d. We denote by ${}^{\mathrm{a}}\mathrm{HF}$ "the affine Hilbert function" of S, that is,*

$${}^{\mathrm{a}}\mathrm{HF}_S(i) = \#(S_{\leq i}) \qquad (i \in \mathbb{N})$$

For any subalgebra A of $A_n(k)$, we define its affine Hilbert function ${}^{\mathrm{a}}\mathrm{HF}_A$ as the affine Hilbert function ${}^{\mathrm{a}}\mathrm{HF}_{\operatorname{multideg} A}$ of multidegree of A.

Lemma 18. *Let m be a positive integer. Let S be a sub monoid of $\mathbb{N}^m$. Let $L = \mathbb{Z}S$ be the submodule of $\mathbb{Z}^n$ generated by S. Then the following conditions are equivalent.*

1. *There exists a positive real number ϵ such that ${}^{\mathrm{a}}\mathrm{HF}_S(i) \geq \epsilon i^m$ for all $i >> 0$.*
2. $\operatorname{rank}(L) = m$

Proof. (2) $\implies$ (1): Take $I_1, I_2, \ldots, I_m \in S$ which are linearly independent over $\mathbb{Q}$. Put $c = \max(||I_1||_{\ell^1}, ||I_2||_{\ell^1}, \ldots, ||I_n||_{\ell^1})$. Then a map α defined by

$$\alpha : \mathbb{N}^m \ni (a_1, \ldots, a_m) \mapsto a_1 I_1 + a_2 I_2 + \cdots + a_m I_m \in S$$

is injective and satisfies $\alpha(\mathbb{N}^m_{\leq d}) \subset S_{\leq cd}$ for every positive integer d. Thus we have

$${}^{\mathrm{a}}\mathrm{HF}_S(d) \geq \binom{m + [d/c]}{m} \geq \frac{d^m}{(c+1)^m m!}$$

when d is large enough. ([•] denotes the Gaussian symbol.)

(1) $\implies$ (2): Assume on the contrary that $r = \operatorname{rank}(L) < m$. Then the module L, being torsion free, is isomorphic to $\mathbb{Z}^r$. Let $I_1, \ldots, I_r$ be elements of S which forms a $\mathbb{Z}$-basis of L. Then a map

$$\beta : \mathbb{R}^r \ni (t_1, t_2, \ldots, t_r) \mapsto (t_1 I_1 + t_2 I_2 + \cdots + t_r I_r) \in \mathbb{R}^m$$

is an injective linear map from $\mathbb{R}^r$ to $\mathbb{R}^m$. Thus we may easily see that there exists a real number M such that

$$||\sum_{i=1}^{r} t_i I_i||_{\ell^1} < 1 \implies ||(t_1, \ldots, t_r)||_{\ell^1} < M$$

This implies that $\#S_{<d}$ is smaller than the number of elements of $\mathbb{Z}^r$ which are shorter (in ℓ^1-norm) than Md. □

6.1. **injectivity for almost all primes.**

Lemma 19. *Let k be a field. Assume $\phi : A_n(k) \to A_n(k)$ is injective (which is always the case if* $\operatorname{char} k = 0$*). Then* $\operatorname{rank}(\mathbb{Z}\operatorname{multideg}(\phi(A_n(k))) = 2n$.

Proof. Let N be the maximum of total degrees of elements $\phi(\xi_1), \dots, \phi(\xi_n), \phi(\eta_1), \dots, \phi(\eta_n)$. Then we see that

$$\phi(A_n(k)_{\leq i}) \subset A_n(k)_{\leq Ni}$$

holds for any $i > 0$. Thus for any $i > 0$, we have

$${}^{\mathrm{a}}\mathrm{HF}_{\phi(A_n(k))}(Ni) \geq {}^{\mathrm{a}}\mathrm{HF}_{A_n(k)}(i) = \binom{i+2n}{i}.$$

This together with Lemma 18 gives the result. □

Lemma 20. *Let A be a subalgebra of a polynomial algebra $P = k[X_1, X_2, \dots, X_m]$ over a field k. If there exists an positive integer c such that*

$$\dim(A_{\leq d}) \geq \frac{1}{cm!} d^m$$

holds for all integers $d > 0$, then we have

$$[Q(P) : Q(A)] \leq c$$

Proof. Suppose on the contrary that $[Q(P) : Q(A)] > c$. Take elements $f_1, \dots, f_{c+1} \in Q(P)$ which are linearly independent over $Q(A)$. By multiplying a "common denominator", we may assume that f_i are elements of P. Then it follows that the sum

$$f_1 A + f_2 A + \cdots + f_{c+1} A$$

is direct in P. Let M be the maximum of total degrees of $f_1, \dots, f_{c+1}$. Then the directness above implies that an inequality

$$\dim\left((f_1 A + f_2 A + \cdots + f_{c+1} A)_{\leq d}\right) \geq (c+1) \dim A_{\leq (d-M)}$$

holds for any integer $d > M$. Since the left hand side is not greater than $\dim P_{\leq d}$, we obtain the following inequation

$$\frac{d^m}{m!} + O(d^{m-1}) \geq (c+1) \frac{1}{cm!} (d-M)^m$$

which leads to a contradiction when d is large enough. □

Proposition 2 (injectivity for almost all primes)**.** *Let $\mathfrak{K}$ be an algebraic number field, $\mathfrak{O} = \mathfrak{O}(\mathfrak{K})$ be the ring of integers in $\mathfrak{K}$. suppose we are given an $\mathfrak{K}$-algebra endomorphism ϕ of $A_n(\mathfrak{K})$.*

Then the multidegree monoid of the image $\operatorname{Image}(\phi)$ *has rank $2n$. Furthermore, for almost all prime ideals $\mathfrak{p}$ of $\mathfrak{O}$, we have the following facts.*

1. *ϕ induces an $k(\mathfrak{p})$-algebra endomorphism $\phi_{\mathfrak{p}}$ of $A_n(k(\mathfrak{p}))$ (where $k(\mathfrak{p}) = \mathfrak{O}/\mathfrak{p}$ is the residue field of $\mathfrak{p}$).*
2. *The multidegree monoid of the image* $\operatorname{Image}(\phi_{\mathfrak{p}})$ *has rank $2n$.*
3. *$\phi_{\mathfrak{p}}$ is injective.*
4. *There exists a constant C such that* $\operatorname{geomdeg}(\phi_{\mathfrak{p}}) \leq C$ *for all $\mathfrak{p}$.*

Proof. The first statement is an easy consequence of Lemma 19. This in turn implies (2) (except for finite primes). In precise, let $x_1, x_2, \dots, x_n$ be elements in $A_n(\mathfrak{K})$ such that multi degrees of $\phi(x_1), \phi(x_2), \dots, \phi(x_{2n})$ are linearly independent. Then for almost all primes, their reductions $x_1, x_2, \dots, x_n$ are defined as elements of $A_n(k(\mathfrak{p}))$ and their multi degrees stays invariant under the reduction.

We apply Lemma 18 to see that there exists a positive real number ϵ which is independent of $\mathfrak{p}$ such that an inequality

$$\dim(\phi_{\mathfrak{p}}(A_n(k))_{\leq s}) \geq \epsilon s^{2n}$$

holds for any large integer s.

(1) is already proved in subsection 3.1. To prove (4), we denote by $k = k(\mathfrak{p})$ the quotient field with characteristic $p(> 0)$. Since $A_n(k)$ is a free $Z_n(k)$-module of rank $2n$ with generators $\{\xi^I \eta^J ; ||I||_{\ell^\infty}, ||J||_{\ell^\infty} \leq p-1\}$, we have

$$\phi_{\mathfrak{p}}(Z_n(k)) \cdot (\sum_{||I||_{\ell^\infty}, ||J||_{\ell^\infty} \leq p-1} k\phi_{\mathfrak{p}}(\xi)^I \phi_{\mathfrak{p}}(\eta)^J) = \phi_{\mathfrak{p}}(A_n(k)).$$

Then Corollary 7 gives us an relationship of total degrees of both hands sides. Namely, there exists a positive number N such that

$$\phi_{\mathfrak{p}}(Z_n(k))_{\leq s+N} \cdot (\sum_{||I||_{\ell^\infty}, ||J||_{\ell^\infty} \leq p-1} k\phi_{\mathfrak{p}}(\xi)^I \phi_{\mathfrak{p}}(\eta)^J) \supset \phi_{\mathfrak{p}}(A_n(k))_{\leq s}$$

holds for any positive integer s.

Combining these, we obtain

$$\dim(\phi_{\mathfrak{p}}(Z_n(k))_{\leq s+N}) p^{2n} \geq \epsilon s^{2n}$$

Then we use Lemma20 to see that (4) is true. (One should be very careful about grading of $Z_n(k)$ here. degrees of generators ξ_i^p, η_i^p of $Z_n(k)$ are all p. not 1.) (3) follows from (4) and a consideration on transcendence degrees.

□

References

[1] P. K. Draxl, *Skew fields (London mathematical society lecture note series*, Cambridge Univ. press, 1983.
[2] D. Mumford, *Tata lectures on theta II*, Birkhäuser, 1984.
[3] M. Nagata, *Field theory*, Marcel Dekker, 1977.

Kochi University
Department of Mathematics
Faculty of Science
Kochi, 780 Japan
E-mail: docky@math.kochi-u.ac.jp