TOPICS IN NON COMMUTATIVE ALGEBRAIC GEOMETRY AND CONGRUENT ZETA FUNCTIONS (PART I).

YOSHIFUMI TSUCHIMOTO

1. Introduction

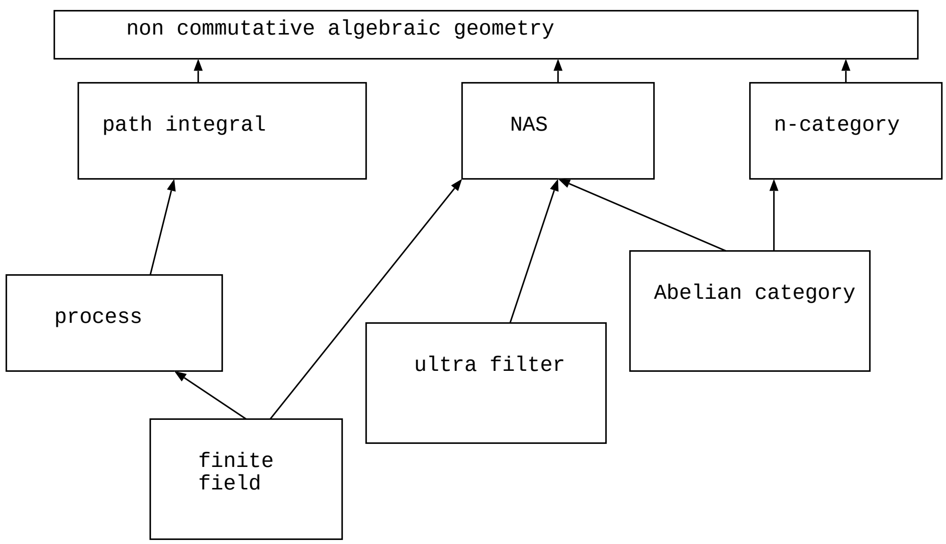
This is a note of lectures held at Kochi University from 2006.04.26.

2. Plan

...and I will show you how deep the rabbit hole goes.

Morpheus, 1999

The author is going to talk what he knows about non commutative algebraic geometry. The plan is summarized as the following diagram.



3. Notations and conventions

We include 0 as a “natural number”.

$$\mathbb{N} = \{0, 1, 2, \ldots, \}.$$

$$\#S = \text{number of elements in S}$$

All the rings and algebras (and homomorphism among them) here are assumed to be unital and associative unless otherwise stated.

4. Guiding problems

The following two conjectures are highly related to each other and appear frequently in our theory.

- The Jacobian conjecture.
- The Dixmier conjecture.

The following hypothesis is likely to be related.

- The Riemann hypothesis.

5. Finite fields

In this section we summarize some results on field theory, especially on finite fields. We omit the proofs. See for example [4] ([5] if the reader prefers a Japanese book).

All the rings and fields in this section is assumed to be commutative.

The following lemma is well-known.

Lemma 5.1. *For any prime number p, $\mathbb{Z}/p\mathbb{Z}$ is a field. (We denote it by $\mathbb{F}_p$.)*

Funny things about this field are:

Lemma 5.2. *Let p be a prime number. Let R be a commutative ring which contains $\mathbb{F}_p$ as a subring. Then:*

(1)
$$\underbrace{1+1+\cdots+1}_{p\text{-times}} = 0$$
holds in R.

(2) *For any $x, y \in R$, we have*
$$(x+y)^p = x^p + y^p$$

We would like to show existence of "finite fields". A first thing to do is to know their basic properties.

Lemma 5.3. *Let F be a finite field (that means, a field which has only a finite number of elements.) Then:*

(1) *There exists a prime number p such that $p = 0$ holds in F.*
(2) *F contains $\mathbb{F}_p$ as a subfield.*
(3) *$q = \#(F)$ is a power of p.*
(4) *For any $x \in F$, we have $x^q - x = 0$.*
(5) *The multiplicative group $F^\times$ is a cyclic group of order $q-1$.*

PROOF. (4): Use Euler-Lagrange theorem for $F^\times$.
(5): we prove the following Lemma which gives more general result. □

LEMMA 5.4. *Let K be a field. Let G be a finite subgroup of $K^\times$ (=multiplicative group of K). Then G is cyclic.*

PROOF. We first prove the lemma when $|G| = \ell^k$ for some prime number ℓ. In such a case Euler-Lagrange theorem implies that any element g of G has an order ℓ^s for some $s \in \mathbb{N}$, $s \leq k$. Let $g_0 \in G$ be an element which has the largest order m. Then we see that any element of G satisfies the equation

$$x^m = 1.$$

Since K is a field, there is at most m solutions to the equation. Thus $|G| \leq m$. So we conclude that the order m of g_0 is equal to $|G|$ and that G is generated by g_0.

Let us proceed now to the general case. Let us factorize the order.

$$|G| = \ell_1^{k_1} \ell_2^{k_2} \dots \ell_t^{k_t} \qquad (\ell_1, \ell_2, \dots, \ell_t : \text{ prime number}, k_1, k_2, \dots, k_t \in \mathbb{Z}_{>0}).$$

Then G may be decomposed into product of p-subgroups

$$G = G_1 \times G_2 \times \cdots \times G_t \qquad (|G_j| = \ell_j^{k_j} \quad (j = 1, 2, 3, \dots, t)).$$

By using the first step of this proof we see that each G_j is cyclic. Thus we conclude that G is also a cyclic group. □

The next task is to construct such field. An important tool is the following

LEMMA 5.5. *For any field K and for any non zero polynomial $f \in K[X]$, there exists a field L containing L such that f is decomposed into polynomials of degree 1.*

To prove it we use the following lemma.

LEMMA 5.6. *For any field K and for any irreducible polynomial $f \in K[X]$ of degree $d > 0$, we have the following.*

(1) *$L = K[X]/(f(X))$ is a field.*
(2) *Let a be the class of X in L. Then a satisfies $f(a) = 0$.*

LEMMA 5.7. *Let p be a prime number. Let $q = p^r$ be a power of p. Let L be a field extension of $\mathbb{F}_p$ such that $X^q - X$ is decomposed into polynomials of degree 1 in L. Then:*

(1)
$$L_1 = \{x \in L; x^q = x\}$$
is a subfield of L containing $\mathbb{F}_p$.
(2) *L_1 has exactly q elements.*

LEMMA 5.8. *Let p be a prime number. Let r be a positive integer. Let $q = p^r$. Then:*

1. *There exists a field which has exactly q elements.*
2. *There exists an irreducible polynomial f of degree r over $\mathbb{F}_p$.*
3. *$X^q - X$ is divisible by f.*
4. *For any field K which has exactly q-elements, there exists an element $a \in K$ such that $f(a) = 0$.*

THEOREM 5.9. *For any power q of p, there exists a field which has exactly q elements. It is unique up to an isomorphism. (We denote it by $\mathbb{F}_q$.)*

The relation between various $\mathbb{F}_q$'s is described in the following lemma.

LEMMA 5.10. *There exists a homomorphism from $\mathbb{F}_q$ to $\mathbb{F}_{q'}$ if and only if q' is a power of q.*

Note: The argument given in previous versions of this note was not good enough – inductive limits were taken for non-cofinal arrows. So we modified it to a corrected version(2006/11/29).

Suppose we are given a power q of a prime number p.

For each positive integer n, we put

$$K_n = \mathbb{F}_{q^{n!}} \qquad \text{(a field with } q^{n!} \text{ elements)}$$

which is unique up to an isomorphism. Then let us choose for each n a field homomorphism

$$\phi_n : K_n \hookrightarrow K_{n+1}.$$

Then we take an inductive limit to define

$$\overline{\mathbb{F}_q} = \varinjlim_n (K_n)$$

It is easy to check that the following theorem holds.

THEOREM 5.11. *$\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$.*

Thus, a fortiori the isomorphism class of the field $\overline{\mathbb{F}_q}$ does not depend of the choice of $\{K_n\}$ or $\{\phi_n\}$.

5.1. **Definition of congruent Zeta function.** In this section we define the congruent Zeta function $Z(V/\mathbb{F}_q, T)$. To avoid assuming too much knowledge on algebraic geometry, we only define it for "affine schemes of finite type" (although we do not use that terminology) for now. For a considerably good account of the theory of the congruent Zeta functions, see [3]. We also recommend [1] which also has a brief explanation on the topic.

DEFINITION 5.12. Let $V = \{f_1, f_2, \dots, f_m\}$ be a set of polynomial equations in n-variables over $\mathbb{F}_q$. We denote by $V(\mathbb{F}_{q^s})$ the set of solutions of V in $(\mathbb{F}_{q^s})^n$. That means,

$$V(\mathbb{F}_{q^s}) = \{x \in (\mathbb{F}_{q^s})^n; f_1(x) = 0, f_2(x) = 0, \dots, f_m(x) = 0\}.$$

Then we define

$$Z(V/\mathbb{F}_q, T) = \exp(\sum_{s=1}^{\infty}(\frac{1}{s}\#V(\mathbb{F}_{q^s})T^s)).$$

6. UNCERTAINTY PRINCIPLE

6.1. **A crush course in quantum physics.** Let us oversimplify the story and summarize the (earliest stage of) quantum physics in the following way. (For precise and physically more correct arguments, see for example [2])

(1) A system is described by a Hilbert space H.
(2) Each physical quantity A corresponds to an operator O_A on H.
(3) A state corresponds to a vector $v \in H$ of length 1.
(4) The expectation value $E_v(A)$ of A when the system is in the state v is given by

$$E_v(A) = \langle v, O_A v\rangle \qquad \text{(inner product)}$$

(Note for mathematicians: when we use "inner products" in this Lecture, we usually mean a biadditive forms which are linear in the second variable and conjugate-linear in the first variable. That means,

$$\langle c_1 f, c_2 g\rangle = \overline{c_1} c_2 \langle f, g\rangle \qquad (c_1, c_2 \in \mathbb{C}).$$

Please pay attention.)

One important example is a position $(q_1, q_2, q_3, \dots, q_n)$ and a momentum $(p_1, p_2, p_3, \dots, q_n)$ of a particle P.

$$H = L^2(\mathbb{R}^n), \quad O_{q_j} = x_j, \quad O_{p_j} = i\partial/\partial x_j \qquad (j = 1, 2, 3, \dots, n)$$

(Note for physicists: we employ a "system of units" such that the Planck's constant (divided by 2π) $\hbar$ is equal to 1.)

Then the expectation of a function $f(x) \in C(\mathbb{R}^n)$ (say) when the state corresponds to a L^2 function $\phi \in H$ is given by

$$E_\phi(f) = \int \overline{\phi(x)} f(x)\phi(x)dx = \int f(x)|\phi(x)|^2 dx.$$

One may then regard $|\phi(x)|^2$ as a "probability density" of the particle P on $\mathbb{R}^n$. $\phi(x)$ is called the wave function of the particle. We should note:

(1) $\phi(x)$ is complex valued. (It is not always positive nor real.)
(2) the square of the absolute value of $\phi(x)$ (rather than $\phi(x)$ itself) is the probability.

In this sense, we sometimes use the term "probability amplitude". The square of the absolute value of the probability amplitude is the probability.

On the other hand, the expectation of a function $g(i\partial/\partial x) \in C(\mathbb{R}^n)$ should be:

$$E_\phi(g) = \int \overline{\phi(x)} g(i\partial/\partial x)\phi(x)dx.$$

The computation becomes easier when we take a Fourier transform F of g.

$$\mathcal{F}[g](\xi) = (2\pi)^{-n/2} \int f(x)e^{ix\xi}dx$$

or its inverse

$$\bar{\mathcal{F}}[g](\xi) = (2\pi)^{-n/2} \int f(x)e^{-ix\xi}dx (= \mathcal{F}[g](-\xi)).$$

The Fourier transform is known to preserve the L^2-inner product. That means,

$$\langle \mathcal{F}[g_1], \mathcal{F}[g_2] \rangle = \langle g_1, g_2 \rangle$$

One of the most useful properties of the Fourier transform is that it transforms derivations into multiplication by coordinates. That means,

$$\mathcal{F}[(\partial/\partial x_j)g] = i\xi_j \mathcal{F}[g].$$

Using the Fourier transform we compute as follows.

$$E_\phi(g) = \int \overline{\mathcal{F}[\phi]} g(-\xi)\mathcal{F}[\phi]dx. = \int (\phi) g(-\xi)|\mathcal{F}[\phi]|^2 dx. = \int g(\xi)|\bar{\mathcal{F}}(\phi)|^2 dx.$$

We then realize that $|\bar{\mathcal{F}}[\phi]|^2$ plays the role of the probability density in this case.

Thus we come to conclude:

The probability amplitude of the momentum is the Fourier transform of the probability amplitude of the position.

The Fourier transform, then, is a way to know the behavior of quantum phenomena.

One may regard a table of Fourier transform (which appears for example in a text book of mathematics) as a vivid example of position and momentum amplitudes of a particle.

To illustrate the idea, let us know concentrate on the case where $n = 1$ and assume that ϕ is a square root of the normal(=Gaussian) distribution $N(m, \sigma)$ of mean value m and standard deviation σ.

$$\phi(x) = \sqrt{N(m,\sigma)} = \sqrt{\frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-m)^2}{2\cdot 2\sigma^2}}}.$$

By using a formula

$$\mathfrak{F}[e^{-x^2/a}] = \sqrt{\frac{a}{2}} e^{-a\xi^2/4},$$

we see that the Fourier transform of ϕ is given by

$$\mathfrak{F}[\phi] = \sqrt{\frac{1}{\sqrt{2\pi}\sigma^{-1}/\sqrt{2}}} e^{i\xi m} e^{-\frac{\xi^2}{2(\sigma^{-1}/\sqrt{2})^2}} = e^{i\xi m}\sqrt{N(0, \frac{1}{\sqrt{2}\sigma})},$$

so that the inverse Fourier transform is given as follows.

$$\bar{\mathfrak{F}}[\phi] = e^{-i\xi m}\sqrt{N(0, \frac{1}{\sqrt{2}\sigma})}.$$

We observe that both $|\phi|^2$ and $|\bar{\mathfrak{F}}[\phi]|^2$ are normal distribution, and that the standard deviation of them are inverse proportional to each other.

In easier terms, the narrower the $|\phi|^2$ distributes, the wider the transform $||\bar{\mathfrak{F}}|[\phi]|^2$ does.

It is a primitive form of the fact known as "the uncertainty principle".

6.2. **Eigen vectors.** Suppose we created a physical state ϕ (in the Laboratory, say) so that "each time we observe the physical quality A, we always obtain the same value λ. In such a case, we have

$$E_\phi(p(A)) = p(E_\phi(A)) = p(\lambda)$$

for any polynomial p. In other words, E_ϕ gives an representation of an algebra generated by A.

Let us now assume that O_A is a Hermitian operator. We put $m = E_\phi(A)$. The variance of A is given by

$$E_\phi(A^2) - E_\phi(A)^2 = E_\phi((A-m)^2) = ||(O_A - m)\phi||^2.$$

When A always takes the same value, then as we have explained above, the variance should be zero. In that case, we have

$$O_A\phi = m\phi.$$

This means that ϕ is an eigen vector of O_A which belongs to an eigen value m.

Thus we come to a situation where term “spectrum” is used. Terms like “spectrum of an operator”, “spectrum of a commutative ring” are thus related. We may study in several directions. Namely, theory in C^*-algebras, commutative algebras, operator theory, algebraic geometry, etc.

But we choose to continue a primitive approach where minimal knowledge is needed.

6.3. **Representations.** In abstract algebra, we may find another way of describing the uncertainty principle. We first define the algebra generated by the operators appeared in the preceding subsection.

$$A_n(k) = k\langle x_1, x_2, \dots, x_n, \partial_1, \partial_2, \dots, \partial_n \rangle$$

We call it the Weyl algebra over k. Here, k is the field $\mathbb{C}$ of complex numbers in the physics context, but may well be a domain of characteristic 0.

In general, including the case where the characteristic of the ground field k is non zero (or even the case where k is an arbitrary ring), we define as follows.

Definition 6.1. Let n be a positive integer. A Weyl algebra $A_n(k)$ over a commutative ring k is an algebra over k generated by $2n$ elements $\{\gamma_1, \gamma_2, \dots, \gamma_{2n}\}$ with the “canonical commutation relations” (CCR)

$$[\gamma_i \gamma_j] = h_{ij} \qquad (1 \le i, j \le 2n).$$

Where h is a non-degenerate anti-Hermitian $2n \times 2n$ matrix of the following form.

$$(h) = \begin{pmatrix} 0 & -1_n \\ 1_n & 0 \end{pmatrix}.$$

In what follows, h will always mean the matrix above. we denote by $\bar{h}$ the inverse matrix of h.

Lemma 6.2. *Any element a of $A_n(k)$ is written uniquely as*

$$\sum_{i_1, i_2, i_3, \dots, i_{2n}} a_{i_1, i_2, i_3, \dots, i_{2n}} \gamma_1^{i_1} \gamma_2^{i_2} \gamma_3^{i_3} \dots \gamma_{2n}^{i_n}$$

Then the fact is:

Lemma 6.3. *Assume k is a field of characteristic zero. Then the Weyl algebra $A_n(k)$ is simple (that means, has no proper two-sided ideals). There exists no finite dimensional representation of $A_n(k)$*

PROOF. Let $\mathfrak{a}$ be a non trivial two-sided ideal of $A_n(k)$. We take a non zero element $x \in \mathfrak{a}$ with the lowest degree when expressed as a polynomial of γ.

$$x = \sum_I x_I \gamma^I$$

Then it is easy to see that the commutator $[\gamma_i, x]$ has the degree lower than x, and that one of the commutators is non zero unless x is a constant.

From the manner we choose the element x, we deduce that x should be a non zero constant in $\mathfrak{a}$. That means,

$$\mathfrak{a} = A_n(k).$$

This is contrary to the assumption that $\mathfrak{a}$ is non trivial.

□

When the characteristic of the base field k is not zero, things are different. We shall see this in the next section.

Before that, we make an easy explanation for the latter part of the Lemma above. Let

$$\alpha : A_n(k) \to M_d(k)$$

be a finite dimensional representation. Then taking a trace of the CCR relations we obtain

$$0 = \operatorname{tr}[\alpha(\gamma_{n+i})\alpha(\gamma_i)] = \operatorname{tr}\alpha([\gamma_{n+i}\gamma_i]) = \operatorname{tr}(\alpha(1)) = d$$

which is absurd.

7. Representations of Weyl algebras of positive characteristics

> The matrix is everywhere. It is all around us. Even in this very room.

In this section we explain a theory described in [6] and [7].

7.1. differential operators in positive characteristics.

We begin by noting the following easy fact.

LEMMA 7.1. *Let k be a field of characteristic $p \neq 0$. Let n be a positive integer. Then we have*

$$(\frac{\partial}{\partial x_i})^p f(x) = 0 \quad (i = 1, 2, \dots, n).$$

for any polynomial $f \in k[x_1, x_2, \dots, x_n]$

In short, we have $\partial_i^p = 0$. This explains why we defined $A_n(k)$ by a generator and relation rather than a ring of differential operators.

Of course, differential operations give important examples of representation of the Weyl algebras.

LEMMA 7.2. *Let k be a field of characteristic $p \neq 0$. Let n be a positive integer. There is a finite dimensional representation Φ of $A_n(k)$ on $k[x_1, x_2, \dots, x_n]/(x_1^p, x_2^p, \dots, x_n^p)$ defined as follows.*

$$\Phi(\gamma_i)f = x_i f, \qquad \Phi(\gamma_{n+i})f = \partial_i \cdot f \qquad (i = 1, 2, \dots, n)$$

LEMMA 7.3. *Let k be a field of characteristic p . We have the following facts.*

(1) *γ_j^p belongs to the center of $A_n(k)$ for any $j \in \{1, 2, 3, \dots, 2n\}$.*
(2) *More precisely, the center $Z_n(k) = Z(A_n(k))$ of the ring $A_n(k)$ is given by*
$$Z_n(k) = k[\gamma_1^p, \gamma_2^p, \gamma_3^p, \dots, \gamma_{2n}^p].$$
(3) *$A_n(k)$ is a free $Z_n(k)$ -module of rank p^{2n} .*
(4) *Let $\mathfrak{a}_0$ be an ideal of $A_n(k)$ defined as*
$$\mathfrak{a}_0 = (\gamma_1^p, \gamma_2^p, \dots, \gamma_{2n}^p).$$
Then we have
$$\mathfrak{a}_0 = \sum_{j=0}^{2n} A_n(k)\gamma_j^p$$
(5) *Any element of $A_n(k)/\mathfrak{a}_0$ is written uniquely as*
$$\sum_{j_1, j_2, j_3, \dots, j_n = 0}^{p-1} a_{j_1 j_2 j_3 \dots j_{2n}} \gamma_1^{j_1} \gamma_2^{j_2} \gamma_3^{j_3} \dots \gamma_{2n-1}^{j_{2n-1}} \gamma_{2n}^{j_{2n}}$$
for some $a_\bullet \in k$.

LEMMA 7.4. *Let Φ be the representation given above. The kernel of Φ is equal to*
$$\mathfrak{a}_0 = (\gamma_1^p, \gamma_2^p, \dots, \gamma_n^p)$$
Φ gives rise to an algebra isomorphism
$$\overline{\Phi} : A_n(k)/\mathfrak{a}_0 \cong M_{p^n}(k).$$

PROOF. That $\mathfrak{a}_0$ is contained in $\mathrm{Ker}(\Phi)$ is obvious. Thus we obtain an well-defined algebra homomorphism $\overline{\Phi}$.

To see the injectivity of $\overline{\Phi}$, we employ a lexicographic order on multi index sets and see that

$$\partial^I x^J = \begin{cases} 0 & \text{if } I > J \\ I! & \text{if } I = J \end{cases}$$

holds for any multi-indices $I, J \subset \{0, 1, 2, 3, \dots, p-1\}^n$. Then by using the previous sublemma we see that $\overline{\Phi}$ is indeed injective.

The surjectivity of $\overline{\Phi}$ is verified by counting dimensions.

□

7.2. irreducible representations of the Weyl algebras.

By translating the irreducible representation Φ in the previous section, we obtain a family of irreducible representations.

LEMMA 7.5. *Let k be a field of characteristic $p \neq 0$. Let n be a positive integer. Let $c \in k^{2n}$. Then there is a finite dimensional representation Φ_c of $A_n(k)$ on $k[x_1, x_2, \dots, x_n]/(x_1^p, x_2^p, \dots, x_n^p)$ defined as follows.*

$$\Phi(\gamma_i)f = (x_i + c_i)f, \qquad \Phi(\gamma_{n+i})f = (\partial_i + c_{n+i}) \cdot f \qquad (i = 1, 2, \dots, n)$$

Then from what we have shown in the previous section, we obtain the following results.

LEMMA 7.6. *Let k, c, Φ_c as in Lemma above. Then:*

(1) *The kernel of Φ_c is given as*

$$\operatorname{Ker}(\Phi_c) = \mathfrak{a}_c = (\gamma_1^p - c_1^p, \gamma_2^p - c_2^p, \gamma_3^p - c_3^p, \dots, \gamma_{2n}^p - c_{2n}^p).$$

(2) *Φ_c gives rise to a k-algebra isomorphism*

$$\overline{\Phi_c} : A_n(k)/\mathfrak{a}_c \cong M_{p^n}(k).$$

(3) *Φ_c is an irreducible representation of $A_n(k)$.*

7.3. Schur's lemma.

LEMMA 7.7. *Let k be an algebraically closed field. Let V be a finite dimensional representation of a k-algebra A. That means, V is a finite dimensional vector space over k, and we have a k-algebra homomorphism*

$$\alpha : A \to \operatorname{End}_k(V).$$

V may be regarded as an A-module. We assume further that V is irreducible representation of A. That means, V admits no non trivial A-module.

Then for each element z the center $Z(A)$ of A, $\alpha(z)$ is equal to a constant.

PROOF. Let $c \in k$ be an eigen value of $\alpha(z)$. Then $\alpha(z - c)$ has a non trivial kernel. That means,

$$V_c = \{v \in V; \alpha(z - c).v = 0\}$$

is a non zero vector subspace of V. It is easy to verify that V_c is a A-submodule of V. From the irreducibility assumption, we have

$$V = V_c,$$

which in turn means that $\alpha(z) = c$.

□

COROLLARY 7.8. *Let k be an algebraically closed field of characteristic $p \neq 0$. Then every finite dimensional irreducible representation $\alpha : A_n(k) \to \mathrm{End}_k(V)$ of $A_n(k)$ is equivalent to a representation Φ_c for some $c \in k^{2n}$.*

PROOF. It is easy to see that γ_j^p is in the center $Z(A_n(k))$ of the Weyl algebra $A_n(k)$ for $j = 1, 2, 3, \ldots, 2n$.

From the Lemma above, we have

$$\alpha(\gamma_j^p) = a_j$$

for some $a_j \in k$. Let c_j be the p-th root of a_j in k (which exists uniquely). Then we see that

$$\mathfrak{a}_c \subset \mathrm{Ker}(\alpha).$$

Thus α is essentially a representation of $A_n(k)/\mathfrak{a}_c \cong M_{p^n}(k)$. □

For completeness's sake, we record here the following easy lemma.

LEMMA 7.9. *Let k be a field. Then any finite dimensional representation $M_n(k)$ is written as a direct sum of copies of the standard representation k^n.*

PROOF. Let us denote by e_{ij} the i, j-elementary matrix. That means,

$$(e_{ij})_{kl} = \begin{cases} 1 & \text{when } (i,j) = (k,l) \\ 0 & \text{otherwise.} \end{cases}$$

Let V be the representation vector space. We first note that $p_i = e_{ii}$ form a complete system of mutually orthogonal projections. That means,

$$p_i^2 = p_i, \qquad p_i p_j = 0 \quad (\text{if } i \neq j), \qquad \sum_{i=1}^n p_i = 1$$

Let us thus put $V_i = p_i V$. Then we have

$$V = \bigoplus_{i=1}^n V_n.$$

Furthermore,

$$e_{ij}. : V_j \to V_i$$

is an isomorphism of vector space whose inverse is equal to e_{ji}.

Let us take a linear basis $\{v_l\}_{l=1}^{d}$ of V_1 over k. Then

$$\{e_{i1}v_l; i = 1, 2, 3, \ldots, n, l = 1, 2, 3, \ldots, d\}$$

is a basis of V. It is now easy to see that for each l, the vector space

$$W_l = \text{linear span}(\{e_{i1}v_l; i = 1, 2, 3, \ldots, n\})$$

is isomorphic to the standard representation of $M_n(k)$.

□

We also notice the following

COROLLARY 7.10. *Let k be a field of characteristic $p \neq 0$. Then $M_{p^n}(k)$ is generated by $\{\mu_i\}_{i=1}^{2n}$ such that*

$$[\mu_i \mu_j] = h_{ij} \quad (\forall i, j), \quad \mu_i^p = 0 (\forall i)$$

PROOF. We take the representation Φ_0 above and

$$\mu_i = \Phi_0(\gamma_i) \qquad (i = 1, 2, 3, \ldots, 2n).$$

□

8. "Universal representation" of Weyl algebras and derivations

LEMMA 8.1. *Let k be a field of characteristic $p \neq 0$. Let $t_1, t_2, \ldots, t_{2n}$ be indeterminates over k. Then we have an injection*

$$\Phi : A_n(k) \to M_{p^n}(k[t_1, t_2, \ldots, t_{2n}])$$

such that

$$\Phi(\gamma_i) = \mu_i + t_i.$$

PROOF. We first note that $\Phi(\gamma_i^p) = t_i^p$ holds for all i. Thus for any element $x \in A_n(k)$, we write

$$x = \sum_I \gamma^I p_I(\gamma_1^p, \gamma_2^p, \gamma_3^p, \ldots, \gamma_{2n}^p)$$

where sum is taken over multi-indices $I \subset \{0, 1, 2, 3, \ldots, p-1\}^n$. Then we obtain

$$\Phi(x) = \sum_I (\mu + t)^I p_I(t_1^p, t_2^p, t_3^p, \ldots, t_{2n}^p)$$

Now, let I_0 be the greatest index among I such that $p_I \neq 0$ (in lexicographical order). Then we have

$$\partial_{I_0}\Phi(x) = (I_0!) p_I(t^p) \neq 0.$$

This is contrary to the assumption that $\Phi(x) = 0$. Thus we have $p_I = 0$ for all I. □

The representation is "universal". It contains all the information of $A_n(k)$ and also carries all the irreducible finite-dimensional representations as specializations.

Via this representation, any element of $A_n(k)$ may be viewed as a matrix-valued polynomial function on the affine space $\mathbb{A}^{2n}$.

8.1. **What is the image of Φ?** The answer is obtained by considering derivations.

LEMMA 8.2. *Let k be a field of characteristic p. For each $i = 1, 2, 3, \dots, 2n$, let $\nabla_i^{(0)}$ be a derivation on $M_{p^n}(k[t_1, t_2, t_3, \dots, t_{2n}])$ defined by*

$$\frac{\partial}{\partial t_i} - \sum_j \overline{h}_{ij} \operatorname{ad}(\mu_j).$$

Then:

(1) *We have*

$$\nabla_i^{(0)}(x) = 0 \quad (i = 1, 2, 3, \dots, 2n) \tag{*}$$

for any element $x \in \operatorname{Image}(\Phi)$.

(2) *Conversely, any element x of $M_p^n(k[t_1, t_2, t_3, \dots, t_{2n}])$ which satisfy the equations (*) belongs to the image* $\operatorname{Image}(\Phi)$.

PROOF. (1) Since $\nabla_i^{(0)}$ is a derivation, we see that the set of elements in $M_p^n(k[t_1, t_2, t_3, \dots, t_{2n}])$ which satisfy the equations (*) above form a k-algebra. It is also easy that $\nabla_i^{(0)}(\Phi(\gamma_j)) = 0$ for all i, j.
(2) Any element x of $M_p^n(k[t_1, t_2, t_3, \dots, t_{2n}])$ may be written uniquely as

$$\sum_I t^I f_I(\Phi(\gamma))$$

(where sum is taken over indices $I \subset \{0, 1, 2, 3, \dots, p-1\}^n$) for some polynomial f_I.

$$\sum_I \partial_i(t^I) f_I(\Phi(\gamma)) = 0$$

We may easily deduce that this happens only when $f_I = 0$ for all $I \neq 0$. □

DEFINITION 8.3. For any vector field $v = \sum_j v_j(t)\partial_j$ on $\mathbb{A}^{2n}$, We define

$$\nabla_v^{(0)} = \sum_j v_j \nabla_j^{(0)}$$

LEMMA 8.4. $\nabla^{(0)}$ *is a connection. That means,*

(1) $\nabla^{(0)}$ *is bi-additive*

$$\nabla^{(0)}_{v_1+v_2} = \nabla^{(0)}_{v_1} + \nabla^{(0)}_{v_2}, \quad \nabla^{(0)}_v(f+g) = \nabla^{(0)}_v(f) + \nabla^{(0)}_v(g).$$

(2) *For each v, $\nabla^{(0)}_v$ is a first order differential operator. Namely, we have*

$$\nabla^{(0)}_v(fm) = (v.f)m + f\nabla^{(0)}_v.m \qquad (\forall f \in k[t], \quad \forall m \in M_{p^n}(k[t])).$$

PROOF. Easy. □

LEMMA 8.5. *$\nabla^{(0)}_v$ is the only first order differential operator on $M_{p^n}(k[t])$ such that its principal symbol is v and*

$$\nabla^{(0)}_v(\mathrm{Image}(\Phi)) = 0$$

holds.

PROOF. Let D be another first order differential operator with the same property. Then we see that the difference

$$P = \nabla^{(0)}_v - D$$

is a $k[t]$-linear map from $M_{p^n}(k[t])$ to itself, and that P is zero when restricted to the image Image(Φ) of Φ. Since Image(Φ) generates $M_{p^n}(k[t])$ as a $k[t]$-module, we see immediately that P is equal to zero. □

We could go further and describe fully the result obtained in the author's papers in terms of algebras (that means, "global" things.)

But the author thinks it unnatural to do so without even mentioning geometric interpretation.

So let us close the part I of this talk and proceed to a more sophisticated world of schemes.

REFERENCES

[1] R. Hartshorne, *Algebraic geometry*, Springer Verlag, 1977.
[2] A. Messiah, *Quantum mechanics (two volumes bound as one)*, Dover, 1999.
[3] J. S. Milne, *Étale cohomology*, Princeton University Press, 1980.
[4] M. Nagata, *Field theory*, Marcel Dekker, 1977.
[5] ———, *Kakan tai ron(new edition)*, Shokabo, 1985.
[6] Y. Tsuchimoto, *Preliminaries on Dixmier conjecture*, Mem. Fac. Sci. Kochi Univ. Ser.A Math.. **24** (2003), 43–59.
[7] ———, *Endomorphisms of Weyl algebra and p-curvatures*, Osaka Journal of mathtematics **42** (2005), no. 2, 435–452.