Contemporary Mathematics

Algebras of p-symbols, noncommutative p-residue, and the Brauer group

Mariusz Wodzicki

Dedicated to Henri Moscovici on the occasion of his sixty-fifth birthday.

ABSTRACT. Importance of the pseudodifferential symbol calculus extends far beyond the fundamental role it is known to play in Global and Microlocal Analysis. In this article, we demonstrate that algebras of symbols contribute to subtle phenomena in characteristic $p > 0$.

A perfect fit between Smooth Geometry and de Rham Theory in characteristic zero leads many to interpret the situation in characteristic $p > 0$ as an apparent *failure* of de Rham Theory in positive characteristic. Smoothness, equated with the existence of local coordinates, i.e., of an étale map from a neighborhood of an arbitrary point to the affine space $\mathbb{A}^n$, is a concept independent of the ground ring. What however is very much dependent on the ground ring k and its characteristic is the geometry of the affine space itself which provides a local model for Smooth Geometry after all.

Local calculations in Smooth Geometry rely on the fact that the affine spaces are objects of the category of commutative unipotent algebraic groups. When the ground ring is a field of characteristic zero, this category is equivalent to the category of finite-dimensional vector spaces, all objects are semisimple, and the additive group $\mathbb{G}_a$, which corresponds to the one-dimensional affine space $\mathbb{A}^1$, is the sole simple object.

In contrast, over a ring of characteristic $p > 0$, the *line* is not even semisimple: $\mathbb{G}_a$ fits for example into the nontrivial extension of algebraic group schemes

$$\mathbb{G}_a \xtwoheadleftarrow{F} \mathbb{G}_a \longleftarrow \mathbb{G}_{a,1} \tag{0.1}$$

where $F : \mathbb{G}_a \to \mathbb{G}_a$, the Frobenius morphism, corresponds to the k-algebra endomorphism of $\mathcal{O}(\mathbb{G}_a) = k[z]$ which sends z to z^p.

1991 *Mathematics Subject Classification.* Primary 58J42, 16H05, 16K50; Secondary 14G17, 47L80, 58B34.

Key words and phrases. Pseudifferential symbols, Azumaya algebras, Brauer group, noncommutative residue.

The author was supported in part by NSF Grants DMS-0503401 and DMS-1001846.

The kernel of the Frobenius morphism $\mathbb{G}_{a,1}$, on the other hand, is a simple object. It resembles, however, a *circle* rather than a line even though, formally speaking, is neither smooth nor of dimension one.

Note the similarities: its module of Kähler differentials $\Omega^1_{\mathbb{G}_{a,1}/k}$ is a *free* module of rank 1 over $\mathcal{O}_{\mathbb{G}_{a,1}}$, its zeroth and first de Rham cohomology groups are free modules of rank 1 over k, and the Lie algebra of vector fields on $\mathbb{G}_{a,1}$ is the Witt algebra

$$W_p(k) = \bigoplus_{i\in\mathbb{Z}/p\mathbb{Z}} k\, e_i, \qquad [e_i, e_j] = (j-i)e_{i+j} \qquad (i, j \in \mathbb{Z}/p\mathbb{Z}),$$

considered to be a counterpart in positive characteristic to the Lie algebra of vector fields on a circle. In particular, $W_p(k)$ possesses a universal central extension with one-dimensional kernel for $p > 3$.

Note that the Witt algebra is a simple Lie algebra of rank 1 if $p > 2$, the only other simple Lie algebra of rank 1 over an algebraically closed field in positive characteristic being $\mathfrak{sl}_2(k)$.

An important structure associated with circle is its algebra of pseudodifferential symbols $\mathrm{CS}(S^1)$ together with the *noncommutative residue* trace. In present article we will demonstrate that its counterpart in positive characteristic is equally deserving of attention.

In Chapter 1 we introduce *algebras of p-symbols*, $\mathcal{S}_{ab}(k)$, parametrized by pairs of elements a and b of a commutative $\mathbb{F}_p$-algebra k. If $k = k^p$, then all $\mathcal{S}_{ab}(k)$ are isomorphic to the algebra of differential operators on the kernel of Frobenius $\mathbb{G}_{a,1}$.

We show that each $\mathcal{S}_{ab}(k)$ is equipped with a unique trace, a close relative of the noncommutative residue in characteristic zero. Appropriately, we call it the *noncommutative p-residue*.

In Chapter 2 we establish a number of useful tensor identities involving the algebras of p-symbols and we use these identities in Chapter 3 to prove that each $\mathcal{S}_{ab}(k)$ is an Azumaya algebra. We achieve this by providing an explicit isomorphism between $\mathcal{S}_{ab}(k)^{\otimes p}$ and a certain algebra of differential operators, cf. (2.13) below, which shows that the similarity class of $\mathcal{S}_{ab}(k)$ in the Brauer group $\mathrm{Br}(k)$, which is duly introduced in Chapter 3, is of order p when nontrivial.

In Chapter 3 we also characterize the algebras of p-symbols as being precisely the *central* quotients of the Weyl algebra[1]

$$A_1(k) := \frac{k\langle z, \zeta\rangle}{([\zeta, z] - 1)}. \tag{0.2}$$

In the next chapter we show that the Weyl algebra itself is a nontrivial Azumaya algebra over its center,

$$Z(A_1(k)) = k\,[z^p, \zeta^p]\,,$$

by identifying $A_1(k)$ with the algebra of p-symbols

$$\mathcal{S}_{z^p\zeta^p}\left(k\,[z^p, \zeta^p]\right).$$

[1]The term *Weyl algebra*, first introduced by Dixmier [**4**] in 1968 (cf. [**5**], p. 46), may be yet another example of wrong apellation: algebra of the Canonical Commutation Relations (CCR) was studied by Dirac in 1926 [**3**], i.e., two years before CCR appear in Weyl's book [**14**]. Apparently the first thorough investigation of $A_1(\mathbb{C})$ was carried by Littlewood in 1930–1931 [**8**], but see also [**6**].

As a corollary, we obtain a recent theorem of Bezrukavnikov, Mirković and Rumynin [**2**] stating that the algebra of PD-differential operators on a smooth scheme X/S, introduced by Berthelot [**1**] and studied by himself, Ogus, Vologodsky, among others, is an Azumaya algebra over the algebra of functions on the cotangent space of the Frobenius twist $X^{(p)}/S$. Our proof is totally explicit and elementary.[2]

An *adelic* noncommutative residue trace on the Weyl algebra over an arbitrary ring of coefficients k is presented in Chapter 5.

In Chapter 6 we collect a number of identities for powers of certain elements in general associative rings and in $\mathbb{F}_p$-algebras. With help of these identities we establish a sufficient condition for triviality of the class of $\mathcal{S}_{ab}$ in $\mathrm{Br}(k)$. These identities are also used in an essential way in the final two chapters.

Tensor identities of Chapter 2 are special cases of general identities associated with certain actions of the symplectic groups $\mathrm{Sp}_n(k)$, $n \geq 2$: these are the subject of Chapter 7. The orbits of the aforementioned actions correspond to elements in

$$ {}_p\mathrm{Br}(k) := \{\beta \in \mathrm{Br}(k) \mid p\beta = 0\} \tag{0.3}$$

whereas the elements of $\mathrm{Sp}_n(k)$ provide nontrivial relations in ${}_p\mathrm{Br}(k)$.

In the final chapter we represent *cyclic p-algebras*, which are defined as crossed products $k' \rtimes_b \mathbb{Z}/p\mathbb{Z}$ of Artin-Schreier extensions k'/k and $\mathrm{Gal}(k'/k) = \mathbb{Z}/p\mathbb{Z}$, as algebras of p-symbols. By combining this with a classical result of Teichmüller we deduce that any element of order p in the Brauer group of a field of characteristic p is represented by a suitable algebra of p-symbols.

Originally we encountered the noncommutative p-residue and the algebras of pseudodifferential p-symbols in our study of the structure of differential operators on the algebra of *divided-power polynomials*, $\Gamma_k[x]$, as documented in [**15**].

We would like to conclude this introduction by saying that the noncommutative residue, nontrivial extension (0.1), and the *Cartier operations*, are so intimately connected—they can be thought of as being manifestations of a single phenomenon.

1. The algebras of p-symbols $\mathcal{S}_{ab}(k)$

Let a and b be a pair of elements of a unital commutative ring k of prime characteristic $p > 0$. The latter means that $pk = 0$ or, equivalently, that k is an $\mathbb{F}_p$-algebra.

We shall denote by $\mathcal{S}_{ab}(k)$ the quotient of the free k-algebra

$$k\langle z, \zeta\rangle = T_k\left(W_{z\zeta}\right),$$

generated by the free k-module of rank 2 with basis $\{z, \zeta\}$,

$$W_{z\zeta} = kz \oplus k\zeta,$$

by the ideal $I_{ab} = I_{ab}(k)$ generated by the following three relations

$$[\zeta, z] = 1, \qquad z^p = a, \qquad \text{and} \qquad \zeta^p = b, \tag{1.1}$$

[2]In [**10**], Théorème 2, Philippe Revoy proves that $A_1(k)$ is a central and separable algebra over $k\left[z^p, \zeta^p\right]$. This is equivalent to $A_1(k)$ being an Azumaya $k\left[z^p, \zeta^p\right]$-algebra (cf. [**7**], Théorème 5.1). Revoy's article escaped our notice until the present work has been completed. There is no reference to Revoy in [**2**].

and call it the *algebra of p-symbols* defined by the pair of elements a and b of ground ring k. We shall omit k from notation when the ground ring is clear from the context.

The composition law. As a k-module, $\mathcal{S}_{ab}(k)$ is free of rank p^2 with the monomial basis $\{z^l\zeta^m\}_{0\leq l,m<p}$ where we identify $z^l\zeta^m$, for $0 \leq l, m < p$, with their images in $\mathcal{S}_{ab}(k)$.

If we identify $\mathcal{S}_{ab}(k)$ as a k-module with the commutative k-algebra

$$\mathcal{O}_{ab} := \mathcal{O}_a \otimes \mathcal{O}_b,$$

where

$$\mathcal{O}_c := k[t]/(t^p - c) \qquad (c \in k), \tag{1.2}$$

by sending z to $t \otimes 1$ and ζ to $1 \otimes t$, then multiplication in $\mathcal{S}_{ab}$ is given by the familiar law for composition of pseudofifferential symbols.

More precisely, for polynomial symbols $\alpha, \beta \in k[z, \zeta]$, where k denotes an arbitrary commutative ring of coefficients, their composition is given by the formula

$$\alpha \circ \beta = \sum_{j=0}^{\infty} \partial_\zeta^j \alpha \, \partial_z^{[j]} \beta. \tag{1.3}$$

Here $\partial_z^{[j]}$ denotes the j-th divided-power of ∂:

$$\partial^{[j]}(z^l) = \begin{cases} \binom{l}{j} z^{l-j} & \text{if } l \geq j \\ 0 & \text{otherwise} \end{cases}$$

which is a differential operator of order j on $k[z]$. If $j!$ is invertible in k, then

$$\partial^{[j]} = \frac{1}{j!}\partial^j.$$

Since we are assuming $pk = 0$ the operator ∂_ζ^j is identically zero for $j \geq p$. Thus, the composition law for polynomial symbols in characteristic p is in fact given by the finite expression

$$\alpha \circ \beta = \sum_{j=0}^{p-1} \frac{1}{j!} \partial_\zeta^j \alpha \, \partial_z^j \beta\,. \tag{1.4}$$

Note that the ideal $(t^p - c) \subset k[t]$ defining $\mathcal{O}_c$ is ∂-invariant, hence the right-hand side of (1.4) is well defined for $\alpha, \beta \in \mathcal{O}_{ab}$, and (1.4) is precisely the formula for multiplication in $\mathcal{S}_{ab}$.

We shall henceforth refer to elements of $\mathcal{S}_{ab}$, represented as elements of $\mathcal{O}_{ab}$ but multiplied according to (1.4), as *p-symbols*.

Noncommutative p-residue. In view of the remark made in the previous paragraph, the standard Poisson bracket on the algebra of polynomials $k[z, \zeta]$,

$$\{f, g\} = \partial_\zeta f \, \partial_z g - \partial_z f \, \partial_\zeta g,$$

passes to the quotient algebra $\mathcal{O}_{ab}$ thus making it a Poisson algebra. Similarly, the associated symplectic form on $\mathbf{A}^2$,

$$\omega = d\zeta \wedge dz,$$

passes to a differential 2-form on the quotient algebra.

The algebra of differential forms on $\mathcal{O}_{ab}$ is a free graded-commutative algebra over $\mathcal{O}_{ab}$ generated by the free $\mathcal{O}_{ab}$-module with basis $\{d\zeta, dz\}$ of degree 1,

$$\Omega^*_{\mathcal{O}_{ab}/k} \simeq \Omega^*_{\mathcal{O}_a/k} \otimes_k \Omega^*_{\mathcal{O}_b/k} \simeq \mathcal{O}_{ab} \otimes_k \Lambda^*_k(d\zeta, dz). \tag{1.5}$$

PROPOSITION 1.1. *The correspondence*

$$\tau \colon \alpha \mapsto [\alpha\omega] \in H^2_{dR}(\mathcal{O}_{ab}) \tag{1.6}$$

which sends a symbol α to the cohomology class of the 2-form $\alpha\omega$, is a trace on the algebra of symbols $\mathcal{S}_{ab}$.

This trace is unique, in the sense that (1.6) *induces an isomorphism*

$$\frac{S_{ab}}{[S_{ab}, S_{ab}]} \simeq H^2_{dR}(\mathcal{O}_{ab}) \tag{1.7}$$

and $H^2_{dR}(\mathcal{O}_{ab})$ is a free k-module of rank 1 generated by the class of the 2*-form*

$$z^{p-1}\zeta^{p-1}\omega. \tag{1.8}$$

PROOF. The commutator formula

$$[\alpha, \beta]\omega = d\big(\rho(\alpha, \beta)dz + \sigma(\alpha, \beta)d\zeta\big), \tag{1.9}$$

where

$$\rho(\alpha, \beta) := \sum_{j=1}^{p-1} \frac{1}{j!} \sum_{i=0}^{j-1} \partial_\zeta^{j-i-1}\alpha\, (-\partial_\zeta)^i \partial_z^j \beta \tag{1.10}$$

and

$$\sigma(\alpha, \beta) := \sum_{j=1}^{p-1} \frac{1}{j!} \sum_{i=0}^{j-1} \partial_z^{j-i-1}\alpha\, \partial_\zeta^j (-\partial_z)^i \beta, \tag{1.11}$$

shows that (1.6) is a k-linear trace on $\mathcal{S}_{ab}$ with values in $H^2_{\mathrm{dR}}(\mathcal{O}_{ab})$.

The de Rham cohomology algebra $H^*_{\mathrm{dR}}(\mathcal{O}_{ab})$ is free graded-commutative, and generated by the classes of the differential 1-forms

$$z^{p-1}dz \qquad \text{and} \qquad \zeta^{p-1}d\zeta.$$

In particular, $H^2_{\mathrm{dR}}(\mathcal{O}_{ab})$ is a free k-module generated by the class of (1.8), and thus map (1.6) is surjective.

The kernel of (1.6) is a free k-module of rank $p^2 - 1$ with the monomial basis

$$\{z^l \zeta^m\}_{0 \le l, m \le p-1;\, l+m \le 2p-3}. \tag{1.12}$$

Each basic monomial in (1.12) is a single commutator:

$$z^l \zeta^m = \begin{cases} \frac{1}{l+1}[\zeta, z^{l+1}\zeta^m] & \text{if } l \neq p-1 \\ -\frac{1}{m+1}[z, z^l \zeta^{m+1}] & \text{if } m \neq p-1 \end{cases} \tag{1.13}$$

which demonstrates that the kernel of (1.6) coincides with $[\mathcal{S}_{ab}, \mathcal{S}_{ab}]$ and thus correspondence (1.6) induces a k-module isomorphism (1.7). □

By identifying $H^2_{\mathrm{dR}}(\mathcal{O}_{ab})$ with k, we can also describe τ as the k-linear functional $\tau\colon \mathcal{O}_{ab} \to k$ which sends

$$\alpha = \sum_{0\leq l,m\leq p-1} c_{lm} z^l \zeta^m \ \in \mathcal{O}_{ab}, \qquad (c_{lm} \in k),$$

to

$$\tau(\alpha) := c_{p-1,p-1}. \tag{1.14}$$

When both a and b are invertible in k, then $\tau(\alpha)$ is the classical double Cauchy Residue in z and ζ variables:

$$\frac{1}{ab} \times \text{the coefficient of } \alpha \text{ at } z^{-1}\zeta^{-1}.$$

We shall be refering to τ as the *noncommuattive p-residue*.

2. Symplectic isomorphisms

Below we establish a number of special k-algebra isomorphisms

$$\mathcal{S}_{a_1b_1} \otimes \cdots \otimes \mathcal{S}_{a_nb_n} \simeq \mathcal{S}_{a'_1b'_1} \otimes \cdots \otimes \mathcal{S}_{a'_nb'_n} \qquad (n \geq 1). \tag{2.1}$$

The left-hand-side of (2.1) is a quotient of the tensor algebra

$$T_k(W_{z_1\zeta_1} \oplus \cdots \oplus W_{z_n\zeta_n}) \tag{2.2}$$

and, similarly, the right-hand-side is a quotient of the tensor algebra

$$T_k(W_{z'_1\zeta'_1} \oplus \cdots \oplus W_{z'_n\zeta'_n}). \tag{2.3}$$

If the k-algebra isomorphism, (2.1), is induced by an isomorphism of k-modules,

$$W_{z_1\zeta_1} \oplus \cdots \oplus W_{z_n\zeta_n} \simeq W_{z'_1\zeta'_1} \oplus \cdots \oplus W_{z'_n\zeta'_n}, \tag{2.4}$$

the latter preserves the symplectic form

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^{\oplus n}$$

that both sides of (2.4) are equipped with, and we propose to call (2.1) a *symplectic* isomorphism.

We shall signal symplectic isomorphisms by employing notation

$$\cong \qquad \text{instead of usual} \qquad \simeq .$$

Elementary observations. In the following proposition we collect preliminary observations about algebras $\mathcal{S}_{ab}$.

PROPOSITION 2.1. (a) *For any $a, b \in k$, one has*

$$\mathcal{S}_{ab} \cong \mathcal{S}_{-a,-b} \cong \mathcal{S}_{b,-a}. \tag{2.5}$$

(b) *The opposite algebra,$(\mathcal{S}_{ab})^{\mathrm{op}}$, is canonically isomorphic to $\mathcal{S}_{ba}$,*

$$(\mathcal{S}_{ab})^{\mathrm{op}} \cong \mathcal{S}_{ba}. \tag{2.6}$$

(c) *Algebra $\mathcal{S}_{a0}$ is canonically isomorphic to the algebra of differential operators, $\mathscr{D}_k(\mathcal{O}_a)$. The latter coincides with the algebra of all k-module endomorphisms,*

$$\mathscr{D}_k(\mathcal{O}_a) = \mathrm{End}_{k\text{-mod}}(\mathcal{O}_a), \tag{2.7}$$

and thus is isomorphic to the algebra of $p \times p$ matrices $M_p(k)$ with coefficients in k. Under this isomorphism, the noncommutative p-residue trace corresponds to the matrix trace with the reverse sign:

$$\tau = -\operatorname{Tr}.$$

(d) *If $b \in k^p \subset k$, then*

$$\mathcal{S}_{ab} \cong \mathcal{S}_{a0}. \tag{2.8}$$

□

If $b = c^p$, then the isomorphism in (2.8),

$$\frac{k\langle z, \zeta\rangle}{(z^p = a, \zeta^p = b, [\zeta, z] = 1)} \cong \frac{k\langle z, \zeta'\rangle}{(z^p = a, \zeta'^p = 0, [\zeta', z] = 1)},$$

is induced by the substitution

$$\zeta \mapsto \zeta' + c.$$

Tensor identities.

PROPOSITION 2.2. *One has the following canonical symplectic isomorphisms:*

$$\mathcal{S}_{ab} \otimes \mathcal{S}_{a'b'} \cong \mathcal{S}_{a,b-a'} \otimes \mathcal{S}_{a',b'-a} \tag{2.9}$$

$$\mathcal{S}_{ab} \otimes \mathcal{S}_{bc} \cong \mathcal{S}_{a0} \otimes \mathcal{S}_{b,c-a} \tag{2.10}$$

$$\begin{aligned} \mathcal{S}_{ab} \otimes \mathcal{S}_{ab}^{\mathrm{op}} &\cong \mathcal{S}_{ab} \otimes \mathcal{S}_{ba} \cong \mathcal{S}_{a0} \otimes \mathcal{S}_{b0} \\ &\simeq \mathscr{D}_k(\mathcal{O}_a) \otimes \mathscr{D}_k(\mathcal{O}_b) \simeq M_p(k)^{\otimes 2} \end{aligned} \tag{2.11}$$

$$\begin{aligned} \mathcal{S}_{ab}^{\otimes l} &\cong \mathcal{S}_{a0}^{\otimes(l-1)} \otimes \mathcal{S}_{b,-la} \simeq \mathscr{D}_k(\mathcal{O}_a)^{\otimes(l-1)} \otimes \mathcal{S}_{b,-la} \\ &\simeq M_p(k)^{\otimes(l-1)} \otimes \mathcal{S}_{b,-la} \end{aligned} \tag{2.12}$$

$$\mathcal{S}_{ab}^{\otimes p} \cong \mathcal{S}_{a0}^{\otimes(p-1)} \otimes \mathcal{S}_{b0} \simeq \mathscr{D}_k(\mathcal{O}_a)^{\otimes(p-1)} \otimes \mathscr{D}_k(\mathcal{O}_b) \simeq M_p(k)^{\otimes p}. \tag{2.13}$$

PROOF. The k-module map

$$\varphi\colon W_{z\zeta} \oplus W_{z'\zeta'} \to W_{z\theta} \oplus W_{z'\theta'} \tag{2.14}$$

which sends z and z' to themselves, and

$$\zeta \mapsto \theta + z', \qquad \zeta' \mapsto \theta' + z, \tag{2.15}$$

induces k-algebra homomorphisms

$$\varphi_{aba'b'}\colon \mathcal{S}_{ab} \otimes \mathcal{S}_{a'b'} \to \mathcal{S}_{a,b-a'} \otimes \mathcal{S}_{a',b'-a}, \tag{2.16}$$

while the map inverse to (2.14),

$$\psi\colon W_{z\theta} \oplus W_{z'\theta'} \to W_{z\zeta} \oplus W_{z'\zeta'},$$

which sends

$$\theta \mapsto \zeta - z', \qquad \theta' \mapsto \zeta' - z, \tag{2.17}$$

induces the inverse k-algebra homomorphisms

$$\psi_{a,b-a',a',b'-a}\colon \mathcal{S}_{a,b-a'} \otimes \mathcal{S}_{a',b'-a} \to \mathcal{S}_{ab} \otimes \mathcal{S}_{a'b'}. \tag{2.18}$$

Indeed, if

$$z^p = a, \quad \zeta^p = b, \quad z'^p = a', \quad \zeta'^p = b'$$

and

$$[\zeta, z] = 1 = [\zeta', z'],$$

then

$$(\zeta - z')^p = b - a', \qquad (\zeta' - z)^p = b' - a, \tag{2.19}$$

$$[\zeta - z', z] = 1 = [\zeta' - z, z'] \tag{2.20}$$

and

$$0 = [\zeta - z', \zeta' - z] = [\zeta - z', z'] = [\zeta' - z, z]. \tag{2.21}$$

This establishes the existence of a canonical symplectic isomorphism in (2.9).

Isomorphism (2.10) is a special case of (2.9), and (2.11) is a special case of (2.10) if one takes into account parts (b) and (c) of Proposition 2.1.

Isomorphism (2.12) is proven by induction on l by using (2.9) again:

$$\begin{aligned} \mathcal{S}_{ab}^{\otimes(l+1)} \cong \mathcal{S}_{ab} \otimes \mathcal{S}_{ab}^{\otimes l} &\cong \mathcal{S}_{ab} \otimes \mathcal{S}_{a0}^{\otimes(l-1)} \otimes \mathcal{S}_{b,-la} \\ &\cong \mathcal{S}_{a0}^{\otimes(l-1)} \otimes \mathcal{S}_{ab} \otimes \mathcal{S}_{b,-la} \cong \mathcal{S}_{a0}^{\otimes l} \otimes \mathcal{S}_{b,-(l+1)a}. \end{aligned}$$

Finally, isomorphism (2.13) is a special case of (2.12) combined with part (c) of Proposition 2.1. ◻

REMARK 2.3. If algebras $\mathcal{S}_{ab}$ are thought of as "1-dimensional," then the tensor products

$$\mathcal{S}_{a_1,\ldots,a_n;b_1,\ldots,b_n} = \mathcal{S}_{a_1b_1} \otimes \cdots \otimes \mathcal{S}_{a_nb_n} \tag{2.22}$$

should be considered "n-dimensional" algebras of p-symbols.

REMARK 2.4. Tensor identities (2.9)–(2.13) are special cases of a general identity established in Section 6, cf. Theorem 7.1.

3. The Brauer group $\mathbf{Br}(k)$.

Azumaya algebras. Let us recall that a unital algebra A is said to be an *Azumaya algebra* over k if there exist: a unital k-algebra B and a faithfully projective k-module P such that

$$A \otimes B^{\text{op}} \simeq \text{End}_{k\text{-mod}}(P).$$

Since $A \otimes B^{\text{op}}$ possesses an identity, k-module P must be finitely generated.

In this case we say that algebras A and B are *similar*, and denote this fact by

$$A \sim B.$$

Similarity is an equivalence relation on the class of Azumaya algebras over a given ground ring k, and the set of similarity classes of such algebras, equipped with the multiplication induced by tensor product, forms a group, denoted $\text{Br}(k)$, which is called the *Brauer group* of ring k. The inverse of $[A]$ in $\text{Br}(k)$ is the similarity class of the opposite algebra, $[A^{\text{op}}]$.

Several characterisations of Azumaya algebras are provided in Chapter III, Section 5, of **[7]** (cf. Théorème 5.1 *ibid.*)

The following is an immediate corollary of the existence of symplectic isomorphisms (2.11) and (2.13) in Proposition 2.2.

COROLLARY 3.1. *For any a and b in k, the algebra of symbols, $\mathcal{S}_{ab}(k)$, is an Azumaya k-algebra and defines an element in*

$$_p\mathrm{Br}(k) = \{\beta \in \mathrm{Br}(k) \mid p\beta = 0\}.$$

REMARK 3.2. For any $n \geq 1$, the correspondence

$$(a_1, \ldots, a_n;\, b_1, \ldots, b_n) \mapsto \left[\mathcal{S}_{a_1,\ldots,a_n;\, b_1,\ldots,b_n}\right] \tag{3.1}$$

produces a map

$$k^{2n} \to {}_p\mathrm{Br}(k),$$

whose fibers are invariant under the action of the group $\mathrm{Sp}_{2n}(k)$ of symplectic matrices with coefficients in k. We discuss this in detail in Section 7.

In the final Section we prove that the cumulative map

$$\bigcup_{n\geq 1} k^{2n} \to {}_p\mathrm{Br}(k)$$

is surjective when k is a field, cf. Theorem 8.3.

A characterisation of the algebras of p-symbols. We shall say that a k-algebra is a *central* quotient of a k-algebra B, if it is of the form $A = B/J$ for a certain twosided ideal $J \subseteq B$ and the structural homomorphism $k \to A$ identifies k with the center of A.

PROPOSITION 3.3. *Every k-algebra $\mathcal{S}_{ab}$ is a central quotient of the Weyl k-algebra $A_1(k)$, cf.* (0.2)*, and vice-versa: every central quotient of $A_1(k)$ is of the form $\mathcal{S}_{ab}$ for a suitable pair of $a, b \in k$.*

PROOF. If we consider $\mathcal{S}_{ab}$ as a free $k[z]$-module of rank p,

$$\mathcal{S}_{ab} = \bigoplus_{0\leq m\leq p-1} k[z]\zeta^m,$$

then the inner derivation $\mathrm{ad}_z = [z,\ ]$ identifies $k[z]\zeta^m$ with $k[z]\zeta^{m-1}$, for $m > 0$, and annihilates $k[z]\zeta^0$. In particular, $\ker \mathrm{ad}_z = k[z]$. Similarly, $\ker \mathrm{ad}_\zeta = k[\zeta]$. It follows that

$$k \subseteq Z(\mathcal{S}_{ab}) \subseteq \ker \mathrm{ad}_z \cap \ker \mathrm{ad}_\zeta = k$$

where $Z\,(\mathcal{S}_{ab})$ denotes the center of $\mathcal{S}_{ab}$.

Assume now that a k-algebra A is a central quotient of $A_1(k)$. We shall identify z and ζ with their images in A. The commutator identity

$$(\mathrm{ad}_z)^p = \mathrm{ad}_{z^p}$$

combined with

$$[z, [z, \zeta]] = 0$$

shows that $z^p \in Z(A) = k$. Similarly for ζ^p. Thus, A is a quotient of $\mathcal{S}_{ab}$ for $a = z^p$ and $b = \zeta^p$.

Above we demonstrated that $\mathcal{S}_{ab}$ is an Azumaya k-algebra, cf. Corollary 3.1. It remains to apply the following lemma.

LEMMA 3.4. *If $A = B/J$ is a central quotient of an Azumaya algebra, then $J = 0$ and $A = B$.*

Indeed, any twosided ideal in an Azumaya k-algebra is of the form $J = IB$ for some ideal $I \subseteq k$ (cf. [**7**], Chapter III, Cor. 5.2). The structural homomorphism $k \to A$ is a monorphism in view of the hypothesis that A is a central quotient of B. Since it factors through the quotient map $k \to k/I$, the latter is injective and thus $I = 0$. $\square$

4. The Weyl algebra in positive characteristic

The center of the (1-dimensional) Weyl algebra $A_1(k) = k\langle z, \zeta\rangle/([\zeta, z] - 1)$ with coefficients in an $\mathbb{F}_p$-algebra k contains

$$K = k[z^p, \zeta^p]. \tag{4.1}$$

Viewed as an algebra over K, the Weyl algebra is nothing but the following K-algebra of p-symbols

$$A_1(k) = \mathcal{S}_{z^p\zeta^p}(K).$$

In particular, $Z(A_1(k)) = K$, and the Weyl algebra is an Azumaya over its center.

Aided by tensor identity (2.13) we obtain a very precise form of that last statement.

PROPOSITION 4.1. *There exists a canonical isomorphism of K-algebras*

$$A_1(k)^{\otimes_K p} \simeq \mathscr{D}_K(\mathcal{O}_a)^{\otimes_K (p-1)} \otimes_K \mathscr{D}_K(\mathcal{O}_b) \simeq M_p(K)^{\otimes_K p}.$$

where $a = z^p$, $b = \zeta^p$, and K is given by (4.1).

$\square$

PROPOSITION 4.2. *The n-dimensional Weyl algebra, $A_n(k) \simeq A_1(k)^{\otimes_k n}$, is an Azumaya algebra over its center*

$$K_n = k\left[z_1^p, \dots, z_n^p; \zeta_1^p, \dots, \zeta_n^p\right],$$

and its similarity class in the Brauer group $\mathrm{Br}(K_n)$ *has exactly order p.*

PROOF. In view of Proposition 4.1, it remains only to prove that $[A_n(K_n)] \neq 0$ in $\mathrm{Br}(K_n)$.

Let us consider the homomorphism

$$K_n = k\left[z_1^p, \dots, z_n^p; \zeta_1^p, \dots, \zeta_n^p\right] \to k\left[z_1^p, \zeta_1^p\right] = K_1$$

which sends z_j and ζ_j to zero for $j > 1$. The associated base-change functor sends K_n-algebra $A_n(k)$ to the K_1-algebra

$$K_1 \otimes_{K_n} A_n(k) \simeq A_1(k) \otimes_k M_p(k)^{\otimes(p-1)},$$

and $[A_n(k)] \in \mathrm{Br}(K_n)$ is sent to $[A_1(k)] \in \mathrm{Br}(K_1)$.

Let $\bar{k}$ be the residue field of k at any maximal ideal. The base change functor associated with the quotient homomorphism $k \to \bar{k}$ sends K_1-algebra $A_1(k)$ to the $\bar{K}_1$-algebra $A_1(\bar{k})$, where

$$\bar{K}_1 = \bar{k}\left[z_1^p, \zeta_1^p\right].$$

The latter is a domain. Let F be the field of fractions of $\bar{K}_1$. The base change functor associated with the inclusion $\bar{K}_1 \hookrightarrow F$ sends $\bar{K}_1$-algebra $A_1(\bar{k})$ to

$$F \otimes_{\bar{K}_1} A_1(\bar{k}) \simeq \mathcal{S}_{z_1^p\zeta_1^p}(F). \tag{4.2}$$

The right hand side of (4.2) is an Azumaya F-algebra of dimension p^2 over F. Thus, it is either a central division F-algebra or is isomorphic to $M_p(F)$. It also contains $A_1(\bar{k})$, and the latter satisfies the left and the right Ore conditions. This was first noted in print perhaps by Dudley Ernest Littlewood[3] ([**8**], Thm. XIX, pp. 219-220; Littlewood considers there only the case of real or complex numbers but his proof of Thm. XIX applies to any field of coefficients).[4]

Algebra $A_1\left(\bar{k}\right)$ is a domain. Thus, the ring of fractions

$$\operatorname{Frac} A_1\left(\bar{k}\right) = \{DE^{-1} \mid D, E \in A_1\left(\bar{k}\right),\ E \neq 0\}$$

is a division ring. Since it contains $S_{z_1^p\zeta_1^p}(F)$, the latter cannot be isomorphic to a matrix algebra.

This proves that the class of $S_{z_1^p\zeta_1^p}(F)$ in $\mathrm{Br}(F)$ is not zero and as a consequence also the class of $A_n(K_n)$ in $\mathrm{Br}(K_n)$. It also demonstrates that $S_{z_1^p\zeta_1^p}(F)$, being a division algebra itself, must coincide with the total algebra of fractions of $A_1\left(\bar{k}\right)$,

$$S_{z_1^p\zeta_1^p}(F) = \operatorname{Frac} A_1\left(\bar{k}\right). \tag{4.3}$$

Equality in (4.3) is equivalent to the following property of Weyl algebra $A = A_1(k)$:

> *if k is a field of positive characteristic, then for any $\alpha \in A$, there exists $\alpha' \in A$ such that $\alpha\alpha'$ is a nonzero element of the center of A.*

Wedderburn in [**13**] calls these algebras *Hamiltonian* since the algebra of quaternions at that time was the best known example of such algebras. □

REMARK 4.3. Proposition 4.2 implies that the algebra of the so called *PD-differential operators*, introduced by Berthelot [**1**], is an Azumaya algebra over its center. This fact seems to have been first noted in print in [**2**] where it was also proved (Theorem 2.2.3 *ibidem*).

REMARK 4.4. In Section 6 of the present article we establish a sufficient condition for the triviality of class $\left[\mathcal{S}_{ab}\right]$ in $\mathrm{Br}(k)$ and, when k is a field, we prove it to be also necessary, cf. Corollary 6.10 and Proposition 6.11 below.

5. A trace on the Weyl algebra

Let k be an arbitrary comutative ring with identity. For any prime p, the composition of the *reduction modulo p* map

$$A_1(k) \twoheadrightarrow \mathbb{F}_p \otimes_{\mathbb{Z}} A_1(k)$$

with the trace map introduced in Section 1,

$$\mathbb{F}_p \otimes_{\mathbb{Z}} A_1(k) \simeq \mathcal{S}_{z^p\zeta^p}\left(\mathbb{F}_p \otimes_{\mathbb{Z}} k\left[z^p, \zeta^p\right]\right) \twoheadrightarrow \mathbb{F}_p \otimes_{\mathbb{Z}} k\left[z^p, \zeta^p\right] =: \mathbb{F}_p \otimes_{\mathbb{Z}} k\left[z_p, \zeta_p\right],$$

[3] Dudley Ernest Littlewood (1903–1979), not to be confused with Hardy's friend and collaborator, John Edensor Littlewood (1885–1977).

[4] In the same year 1933 appeared article [**9**] in which Öystein Ore introduced and thoroughly investigated a very general type rings of polynomials of one variable with multiplication twisted by a certain endomorphism α and a derivation δ acting on the "coefficients"; in particular, Ore proved for such rings the noncommutative versions of the Euclid Division Algorithm, from which he derived that such rings of twisted polynomials satisfy the conditions that today bear his name—if and only if α is an automorphism. Ore's article was submitted in December 1932, Littlewood's—in June 1931.

cf. (1.14), defines a trace on $A_1(k)$:

$$\operatorname{res}_p : A_1(k) \twoheadrightarrow \mathbb{F}_p \otimes_{\mathbb{Z}} k\left[z_p, \zeta_p\right]. \tag{5.1}$$

One has

$$\operatorname{res}_p\left(z^l\zeta^m\right) = \begin{cases} z_p^{\frac{l+1}{p}-1}\zeta_p^{\frac{m+1}{p}-1} & \text{if } l = m = -1 \mod p \\ 0 & \text{otherwise} \end{cases}. \tag{5.2}$$

Note that

$$\operatorname{res}_p\left(z^l\zeta^m\right) \neq 0$$

only for primes dividing the greatest common divisor of $l+1$ and $m+1$. It follows that the k-linear map

$$\operatorname{res} : A_1(k) \to \bigoplus_p \mathbb{F}_p \otimes_{\mathbb{Z}} k\left[z_p, \zeta_p\right], \qquad \operatorname{res}(\alpha) := \sum_p \operatorname{res}_p(\alpha), \tag{5.3}$$

where summation extends over all primes, is well defined and annihilates the commutator k-module $[A_1(k), A_1(k)]$.

Map (5.3) is surjective. Indeed, for $i, j \in \mathbb{N}$ and a prime p, let π be the product of all primes different from p which divide the greatest common divisor of $i+1$ and $j+1$,

$$\pi := \prod_{\substack{q|\gcd(i+1,j+1)\\ q\neq p}} q.$$

If $\pi' \in \mathbb{Z}$ satisfies

$$\pi\pi' = 1 \mod p,$$

then, for any prime q,

$$\operatorname{res}_q\left(\pi\pi' z^{(i+1)p-1}\zeta^{(j+1)p-1}\right) = \begin{cases} z_p^i\zeta_p^j & \text{if } q = p \\ 0 & \text{otherwise} \end{cases}.$$

By taking the n-th tensor power of (5.3) we obtain the corresponding trace on the n-dimensional Weyl algebra

$$\operatorname{res}^{\otimes_k n} : A_n(k) = A_1(k)^{\otimes_k n} \twoheadrightarrow \bigoplus_p \mathbb{F}_p \otimes_{\mathbb{Z}} k\left[z_p, \zeta_p\right]^{\otimes_k n}.$$

6. Power identities

Two power-of-the-product identities. Let R be a unital ring. Below we adopt the convention that $x^0 = 1$ for any $x \in R$.

PROPOSITION 6.1. *Let r and s be a pair of elements of R satisfying*

$$[[r,s],r] = 0 = [[r,s]s]. \tag{6.1}$$

Then

$$(rs)^n = \sum_{i=0}^{n} a_{nl}[r,s]^{n-l}s^l r^l \qquad (n \geq 0) \tag{6.2}$$

and

$$(rs)^n = \sum_{i=1}^{n} b_{nl}[s,r]^{n-l}r^l s^l \qquad (n \geq 1) \tag{6.3}$$

where

$$a_{nl} = \phi^{n-l}_{(l+1)}(1, 2, \ldots, l+1) \qquad (n \geq 0) \tag{6.4}$$

and

$$b_{nl} = \phi^{(n-l)}_{l}(1, 2, \ldots, l) \qquad (n \geq 1) \tag{6.5}$$

Here $\phi^{(d)}_m \in \mathbb{Z}[X_1, \ldots, X_m]$ *is the symmetric form of degree* d *in* m *variables*

$$\phi^{(d)}_m(X_1, \ldots, X_m) = \sum_{\substack{d, \ldots, d_m \geq 0 \\ d_1 + \cdots + d_m = d}} X_1^{d_1} \cdots X_m^{d_m}. \tag{6.6}$$

PROOF. Formulae (6.2) and (6.4) are obviously valid for $n = 0$. By multiplying both sides of (6.2) on the left by rs, we obtain the following expression for $(rs)^{n+1}$,

$$\begin{aligned}(rs)^{n+1} &= \sum_{l=0}^{n} a_{nl}[r,s]^{n-l}(rs)s^l r^l \\ &= \sum_{l=0}^{n} a_{nl}[r,s]^{n-l}s^{l+1}r^{l+1} + \sum_{l=0}^{n} a_{nl}[r,s]^{n-l} \sum_{m=0}^{l+1} s^l [r,s] s^{l-m} r^l \\ &= \sum_{l=1}^{n+1} a_{n,l-1}[r,s]^{n+1-l}s^l r^l + \sum_{l=0}^{n} a_{nl}[r,s]^{n+1-l}s^l r^l\end{aligned} \tag{6.7}$$

which can be re-written as

$$(rs)^{n+1} = \sum_{l=0}^{n+1} (a_{n,l-1} + (l+1)a_{nl})[r,s]^{n+1-l}s^l r^l, \tag{6.8}$$

if we adopt the convention

$$a_{nl} = 0 \qquad \text{for either } l < 0 \text{ or } l > n. \tag{6.9}$$

The latter is compatible with the fact that

$$a_{0l} = \begin{cases} 1 & \text{if } \ l = 0 \\ 0 & \text{otherwise} \end{cases}. \tag{6.10}$$

Induction on n with help of (6.8) demonstrates that formula (6.2) holds for certain integral coefficients a_{nl} satisfying the "boundary" conditions

$$a_{n0} = a_{nn} = 1 \tag{6.11}$$

and the recurrence formula

$$a_{n+1,l} = a_{n,l-1} + (l+1)a_{nl} \qquad (0 < l < n). \tag{6.12}$$

Note that the coefficients

$$a'_{nl} := \phi^{(n-l)}_{l+1}(1, \ldots, l+1)$$

obviously satisfy boundary conditions (6.11),

$$\phi^{(n)}_1(1) = 1^n = 1, \qquad \phi^{(0)}_{n+1}(1, \ldots, l+1) = 1^0 \cdots (l+1)^0 = 1,$$

while formula (6.12), for a'_{nl}, is a consequence of the identity

$$\phi_{l+1}^{((n+1)-l))}(X_1,\dots,X_{l+1}) = \phi_l^{(n-(l-1))}(X_1,\dots,X_l) + X_{l+1}\phi_{l+1}^{(n-l)}(X_1,\dots,X_{l+1}) \tag{6.13}$$

which holds in $\mathbb{Z}[X_1,\dots,X_{l+1}]$.

Induction on n shows that

$$a_{nl} = a'_{nl} \qquad (0 \le l \le n).$$

This yields equality (6.4).

Multiplication of both sides of (6.2) on the left by s and, on the right, by r, produces equalities (6.3) and (6.5), respectively. □

Arithmetic of the form $\phi_l^{(p-l)}$. For a given prime p, let us consider the functions $\mathbb{F}_p^l \to \mathbb{F}_p$ associated with forms $\phi_l^{(p-l)}$ for $0 \le l \le p$,

$$(x_1,\dots,x_l) \mapsto \phi_l^{(p-l)}(x_1,\dots,x_l). \tag{6.14}$$

PROPOSITION 6.2. *One has*

$$\phi_l^{(p-l)}(\nu_1,\dots,\nu_l) = 0, \tag{6.15}$$

for any $1 < l < p$ and any l-tuple $(\nu_1,\dots,\nu_l) \in (\mathbb{F}_p^*)^l$ such that

$$\nu_i \neq \nu_j \qquad (1 \le i \neq j \le l). \tag{6.16}$$

PROOF. Note the identity

$$\phi_{l-1}^{(n+1-l)}(X_1,\dots,\hat{X}_i,\dots,X_l) - \phi_{l-1}^{(n+1-l)}(X_1,\dots,\hat{X}_j,\dots,X_l) = (X_i - X_j)\phi_l^{(n-l)}(X_1,\dots,X_l) \tag{6.17}$$

in $\mathbb{Z}[X_1,\dots,X_l]$.

It follows that when $\nu_i - \nu_j \in \mathbb{F}_p^*$, then $\phi_l^{(p-l)}(\nu_1,\dots,\nu_l)$ vanishes if and only if

$$\phi_{l-1}^{(p+1-l)}(\nu_1,\dots,\hat{\nu}_i,\dots,\nu_l) = \phi_{l-1}^{(p+1-l)}(\nu_1,\dots,\hat{\nu}_j,\dots,\nu_l). \tag{6.18}$$

Since

$$\phi_1^{(p-1)}(\nu) = \nu^{p-1} = 1 \qquad (\nu \in \mathbb{F}_p^*),$$

we observe that both sides of (6.18) are equal to 1 for $l = 2$ and any $\nu_i, \nu_j \in \mathbb{F}_p^*$. Induction on l in the range $2 \le l \le p-1$ proves that both sides of (6.18) are equal and, indeed, for $3 \le l \le p-1$, both vanish, provided condition (6.16) is satisfied. □

In the rest of this Section we assume that $pR = 0$, i.e., that R is an $\mathbb{F}_p$-algebra. Under suitable hypotheses relevant to the study of algebras of p-symbols, we present two formulae for the p-th power of the product and of the sum of two elements in R.

A p^{th}-power-of-the-product identity for an $\mathbb{F}_p$-algebra. We begin from the formula for the p-th power of the product.

PROPOSITION 6.3. *Let p be a prime. For any pair r and s of elements of an $\mathbb{F}_p$-algebra R, satisfying condition* (6.1)*, one has*

$$(rs)^p = [s,r]^{p-1} rs + r^p s^p. \tag{6.19}$$

This is a corollary of formulae (6.3) and (6.5) combined with the congruences

$$\phi_l^{(p-l)}(1,\dots,l) = 0 \mod p \qquad (2 \le l \le p-1) \tag{6.20}$$

which form a special case of Proposition 6.2.

A p^{th}-power-of-the-sum identity. The following formula is well known even though probably not in the form presented below.

LEMMA 6.4. *Let r_0 and r_1 be a pair of elements in an $\mathbb{F}_p$-algebra R. One has the following formula*

$$(r_0+r_1)^p - (r_0^p + r_1^p) = \sum_{\iota\colon \{1,\dots,p-2\}\to\{0,1\}} \frac{1}{1+ |\operatorname{supp}\iota|} [r_{\iota_1}, \dots [r_{\iota_{p-2}}, [r_0, r_1]] \dots] \tag{6.21}$$

where $|\operatorname{supp}\iota|$ *is the cardinality of the support of* ι,

$$\operatorname{supp}\iota = \{1 \le j \le p-2 \mid \iota_j = 1\}.$$

$\square$

Summation in (6.21) extends over all functions from $\{1,\dots,p-2\}$ to $\{0,1\}$, including the case $p=2$ when the domain is the empty set.

COROLLARY 6.5. *Let r and s be a pair of elements in an $\mathbb{F}_p$-algebra R, satisfying the commutation relations*

$$\left[\operatorname{ad}_r^l(s), s\right] = [[\underbrace{r, \dots [r, [r}_{l \text{ times}}, s]] \dots], s] = 0 \qquad (0 < l < p).$$

Then

$$(r+s)^p - (r^p + s^p) = [\underbrace{r, \dots [r, [r}_{p-1 \text{ times}}, s]] \dots].$$

$\square$

DEFINITION 6.6. We shall call a $2n$-tuple of elements $(z_1,\dots,z_n;\, \zeta_1,\dots,\zeta_n)$ in an arbitrary unital ring R, a *CCR-system* (of length n), if it satisfies the Canonical Commutation Relations

$$[z_i, z_j] = [\zeta_i, \zeta_j] = 0 \qquad \text{and} \qquad [\zeta_i, z_j] = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}. \tag{6.22}$$

If $n = 1$ we shall call it a *CCR-pair*.

COROLLARY 6.7. *Suppose that $(z_1,\dots,z_n;\, \zeta_1,\dots,\zeta_n)$ is a CCR-system in an algebra A over an $\mathbb{F}_p$-algebra k. Then the p-th power of any linear combination of elements of the system*

$$(c_1^+\zeta_1 + \dots + c_n^+\zeta_n + c_1^- z_1 + \dots c_b^- z_n)^p \qquad (c_i^\pm \in k;\ 1 \le i \le n) \tag{6.23}$$

equals

$$(c_1^+)^p\,\zeta_1^p + \cdots + (c_n^+)^p\,\zeta_n^p + (c_1^-)^p\,z_1^p + \cdots + (c_n^-)^p\,z_n^p \tag{6.24}$$

if $p > 2$, and

$$(c_1^+)^2\,\zeta_1^2 + \cdots + (c_n^+)^2\,\zeta_n^2 + (c_1^-)^2\,z_1^2 + \cdots + (c_n^-)^2\,z_n^2 + (c_1^+c_1^- + \cdots + c_n^+c_n^-) \tag{6.25}$$

if $p = 2$. In particular, the p-th power of any linear combination with coefficients in k belongs to k if all z_i^p and ζ_j^p belong to k. □

The following proposition follows easily from Corollary 6.5 and the congruence

$$(p-1)! = -1 \mod p \qquad \text{(Wilson's Theorem)}.$$

PROPOSITION 6.8. *Let $f \in k[X]$ be a polynomial,*

$$f(X) = c_0 + c_1X + \cdots + c_{p-1}X^{p-1}, \tag{6.26}$$

over a commutative $\mathbb{F}_p$-algebra k. For any CCR-pair z and ζ in an arbitrary k-algebra A, one has

$$(\zeta + f(z))^p = \zeta^p + f^{(p)}(z^p) - c_{p-1} \tag{6.27}$$

where $f^{(p)}$ denotes the Frobenius-twist of f:

$$f^{(p)}(X) = c_0^p + c_1^pX + \cdots + c_{p-1}^pX^{p-1}. \tag{6.28}$$

As a corollary we obtain some important non-symplectic isomorphisms between the algebras of p-symbols.

COROLLARY 6.9. *Given a polynomial* (6.26), *the correspondence*

$$z \mapsto z', \qquad \zeta \mapsto \zeta' + f(z'), \tag{6.29}$$

induces an isomorphism of k-algebras

$$\mathcal{S}_{ab}(k) \simeq \mathcal{S}_{a,b-f^{(p)}(a)+c_{p-1}}(k). \tag{6.30}$$

PROOF. The homomorphism of free k-algebras $k\langle z,\zeta\rangle \to k\langle z',\zeta'\rangle$ induced by correspondence (6.29) sends the three generators of ideal I_{ab}, cf. (1.1), to elements of ideal $I_{ab'}$ where $b' = b - f^{(p)}(a) + c_{p-1}$. Thus, it induces a homomorphism from $\mathcal{S}_{ab}$ to $\mathcal{S}_{ab'}$. The inverse is induced by the correspondence

$$z' \mapsto z, \qquad \zeta' \mapsto \zeta - f(z).$$

□

Consider the following *Dependency Condition* connecting exponents a and b:

there exists a polynomial (6.26) *such that*

$$b = f^{(p)}(a) - c_{p-1}. \tag{D}$$

COROLLARY 6.10. *If the pair of exponents $a, b \in k$ satisfies Dependency Condition* (D)*, then*

$$\mathcal{S}_{ab} \simeq \mathscr{D}_k(\mathcal{O}_a) \simeq M_p(k).$$

□

When the ground ring is a field, this condition is not only sufficient but also necessary.

PROPOSITION 6.11. *If k is a field, then $[\mathcal{S}_{ab}] = 0$ in $\mathrm{Br}(k)$ if and only if the exponents satisfy Dependency Condition* (D) *introduced above.*

The necessity of Condition (D) is an immediate consequence of the following fact.

PROPOSITION 6.12. *Let z and ζ be any CCR-pair in the matrix algebra $M_p(k)$ over an arbitrary field of characteristic p. Then*

$$z^p \in k \qquad \text{and} \qquad \zeta^p \in k, \tag{6.31}$$

the set $\{z, \zeta\}$ generates $M_p(k)$ as a k-algebra, and the exponents $a = z^p$ and $b = \zeta^p$ satisfy Condition (D).

Vice-versa, for any pair $a, b \in k$ which satisfies Condition (D)*, there exists a CCR-pair $z, \zeta \in M_p(k)$ with $z^p = a$ and $\zeta^p = b$.*

PROOF. Suppose z and ζ form a CCR-pair in $M_p(k)$, and let ϕ and ψ be their respective minimal polynomials. Since $\phi(z) = \psi(\zeta) = 0$, we have

$$0 = [\zeta, \phi(z)] = \phi'(z) \qquad \text{and} \qquad 0 = [\psi(\zeta), z] = \psi'(\zeta),$$

which implies that $\phi' = \psi' = 0$. Since the degrees of ϕ and ψ do not exceed p, we infer that

$$\phi(X) = X^p - a \qquad \text{and} \qquad \psi(X) = X^p - b$$

for certain $a, b \in k$. This proves (6.31).

Thus the subalgebra $A \subseteq M_p(k)$ generated by z and ζ is isomorphic to a quotient of the algebra of p-symbols, $\mathcal{S}_{ab}$. In view of simplicity of the latter, A is isomorphic to $\mathcal{S}_{ab}$. Both S_{ab} and $M_p(k)$ have the same dimension as vector spaces over k, hence $A = M_p(k)$.

If $a \in k^p$, then exponents a and b satisfy Condition (D) with the polynomial

$$f(X) = -bX^{p-1} + b\left(\sqrt[p]{a}\right)^{p-1}.$$

If $a \in k \setminus k^p$, then the polynomial $X^p - a$ is irreducible and thus coincides with the minimal polynomial of z. In particular, z is similar to the companion matrix of $X^p - a$

$$Z = \begin{pmatrix} 0 & & & a \\ 1 & \ddots & & \\ & \ddots & 0 & \\ & & 1 & 0 \end{pmatrix} \tag{6.32}$$

and the latter forms with the matrix

$$\Xi = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 2 & & \\ & & \ddots & \ddots & \\ & & & 0 & p-1 \\ & & & & \end{pmatrix} \tag{6.33}$$

a CCR-pair. This shows that there exists $\xi \in M_p(k)$ such that $[\xi, z] = 1$ and $\xi^p = 0$. In particular, $\zeta - \xi$ belongs to the centralizer of z in $M_p(k)$ which coincides with $k[z] \subset M_p(k)$ since the centralizer of matrix Z coincides with $k[Z] \subset M_p(k)$. It follows that $\xi = \zeta - f(z)$ for some polynomial $f \in k[X]$ of degree less than p, whence

$$0 = \xi^p = b - f^{(p)}(a) + c_{p-1},$$

in view of identity (6.27). This completes the proof of the first part of Proposition 6.12

In order to show that any pair of exponents satisfying Condition (D) is realized by some CCR-pair in $M_p(k)$, note that for a given $a \in k$, matrices Z and Ξ, cf. (6.32)–(6.33) above, form a CCR-pair with exponents a and 0, respectively.

If $b = f^{(p)}(a) - c_{p-1}$, then by replacing Ξ with $\Xi + f(Z)$, we obtain a CCR-pair satisfying $z^p = a$ and $\zeta^p = b$. □

7. The general form of a symplectic isomorphism between n-dimensional algebras of p-symbols

A $2n \times 2n$-matrix with coefficients in k

$$C = \begin{pmatrix} D^+ & E^+ \\ E^- & D^- \end{pmatrix},$$

where $D^\pm, E^\pm \in M_n(k)$, induces a homomorphism of free algebras

$$k\langle z_1', \dots, z_n'; \zeta_1', \dots, \zeta_n' \rangle \to k\langle z_1, \dots, z_n; \zeta_1, \dots, \zeta_n \rangle \tag{7.1}$$

by sending z_j' to

$$d_{1j}^+ z_1 + \cdots + d_{nj}^+ z_n + e_{1j}^- \zeta_1 + \cdots + e_{nj}^- \zeta_n$$

and ζ_j' to

$$e_{1j}^+ z_1 + \cdots + e_{nj}^+ z_n + d_{1j}^- \zeta_1 + \cdots + d_{nj}^- \zeta_n.$$

If $C \in \mathrm{Sp}_{2n}(k)$, then homomorphism (7.1) induces an isomorphism of the corresponding n-dimensional Weyl algebras

(7.2)
$$A_n' = k\langle z_1', \dots, z_n'; \zeta_1', \dots, \zeta_n' \rangle / \mathrm{CCR}_n' \xrightarrow{\sim} A_n = k\langle z_1, \dots, z_n; \zeta_1, \dots, \zeta_n \rangle / \mathrm{CCR}_n$$

where CCR_n' and CCR_n denote the ideals generated by the Canonical Commutation Relations, cf. (6.22).

For a given $2n$-tuple

$$\pi = (a_1, \dots, a_n; b_1, \dots, b_n) \in k^{2n}$$

define

$$\rho_C(\pi) = (a_1', \dots, a_n'; b_1', \dots, b_n') \in k^{2n} \tag{7.3}$$

where

(7.4)
$$a_j' := \begin{cases} \left(d_{1j}^+\right)^p a_1 + \cdots + \left(d_{nj}^+\right)^p a_n + \left(e_{1j}^-\right)^p b_1 + \cdots + \left(e_{nj}^-\right)^p b_n & p > 2 \\ \left(d_{1j}^+\right)^2 a_1 + \cdots + \left(d_{nj}^+\right)^2 a_n + \left(e_{1j}^-\right)^2 b_1 + \cdots + \left(e_{nj}^-\right)^2 b_n + d_{1j}^+ e_{1j}^- + \cdots + d_{nj}^+ e_{nj}^- & p = 2 \end{cases}$$

and

(7.5)
$$b'_j := \begin{cases} \left(e^+_{1j}\right)^p a_1 + \cdots + \left(e^+_{nj}\right)^p a_n + \left(d^-_{1j}\right)^p b_1 + \cdots + \left(d^-_{nj}\right)^p b_n & p > 2 \\ \left(e^+_{1j}\right)^2 a_1 + \cdots + \left(e^+_{nj}\right)^2 a_n + \left(d^-_{1j}\right)^2 b_1 + \cdots + \left(d^-_{nj}\right)^2 b_n + d^-_{1j}e^+_{1j} + \cdots + d^-_{nj}e^+_{nj} & p = 2 \end{cases}.$$

Equalities (7.4)–(7.5) can be expressed in a more compact form as follows

$$\rho_C(\pi) := \begin{cases} \pi C^{(p)} & \text{if } p > 2 \\ \pi C^{(2)} + C^+ \cdot C^- & \text{if } p = 2 \end{cases} \tag{7.6}$$

where $C^{(p)} = \left(c^p_{ij}\right)$ denotes the *Frobenius twist* of C, and $C^+, C^- \in M_{n,2n}(k)$ are $n \times 2n$ matrices representing the top n, and the bottom n rows of C, respectively. Finally, $C^+ \cdot C^-$ is the row $2n$-vector formed by the dot products of columns of C^+ with the corresponding columns of C^-,

$$C^+ \cdot C^- = \left(C^+_1 \cdot C^-_1, \ldots, C^+_{2n} \cdot C^-_{2n}\right).$$

It follows from Corollary 6.7 that the ideal in A'_n, generated by the elements

$$(z'_1)^p - a'_1, \ldots, (z'_n)^p - a'_n, (\zeta'_1)^p - b'_1, \ldots, (\zeta'_n)^p - b'_n,$$

is being sent by isomorphism (7.2) to the ideal in A_n generated by the elements

$$z^p_1 - a_1, \ldots, z^p_n - a_n, \zeta^p_1 - b_1, \ldots, \zeta^p_n - b_n.$$

Thus (7.2) descends to a homomorphism of the corresponding n-dimensional k-algebras of p-symbols

$$\mathcal{S}_{a'_1,\ldots,a'_n;\, b'_1,\ldots,b'_n} \longrightarrow \mathcal{S}_{a_1,\ldots,a_n;\, b_1,\ldots,b_n}. \tag{7.7}$$

The inverse matrix C^{-1} induces a homomorphism that is inverse to (7.7).

We arrive at the following theorem that describes a general symplectic isomorphism between algebras of p-symbols.

THEOREM 7.1. *For any*

$$\pi = (a_1, \ldots, a_n;\, b_1, \ldots, b_n) \in k^{2n},$$

and any symplectic matrix $C \in \mathrm{Sp}_{2n}(k)$, one has the following canonical isomorphisms

$$\mathcal{S}_{a'_1 b'_1} \otimes \cdots \otimes \mathcal{S}_{a'_n b'_n} \simeq \mathcal{S}_{a'_1,\ldots,a'_n;\, b'_1,\ldots,b'_n} \cong \mathcal{S}_{a_1,\ldots,a_n;\, b_1,\ldots,b_n} \simeq \mathcal{S}_{a_1 b_1} \otimes \cdots \otimes \mathcal{S}_{a_n b_n} \tag{7.8}$$

where

$$(a'_1, \ldots, a'_n;\, b'_1, \ldots, b'_n) = \rho_C(\pi)$$

is given by equalities (7.3)–(7.5).

In a compact form, (7.8) *can be expressed as*

$$\left.\begin{array}{ll} (p > 2) & \mathcal{S}_{\pi C^{(p)}} \\ (p = 2) & \mathcal{S}_{\pi C^{(2)} + C^+ \cdot C^-} \end{array}\right\} = \mathcal{S}_{\rho_C(\pi)} \cong \mathcal{S}_\pi. \tag{7.9}$$

□

As mentioned in Remark 2.4, tensor identities (2.9)–(2.13) of Section 2 are nothing but special cases of identity (7.8) for suitably chosen symplectic matrices C.

8. Cyclic p-algebras as algebras of p-symbols

For $b \in k^*$ and $c \in k$, let us denote by $(b, c]_k$ the quotient of the free k-algebra $k\langle \zeta, \eta \rangle$ by the ideal $J_{bc} = J_{bc}(k)$ generated by the following three relations

$$\zeta^p = b, \qquad \eta^p = \eta + c \qquad \text{and} \qquad \zeta\eta = (\eta + 1)\zeta. \tag{8.1}$$

We shall omit subscript k if the ground ring is clear from the context.

Algebra $(b, c]$ is the crossed product

$$(b, c] = \frac{k[\eta]}{(\eta^p - \eta - c)} \rtimes_b (\mathbb{Z}/p\mathbb{Z}) \tag{8.2}$$

with the twisting cocyle

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to k^*, \qquad (i, j) \mapsto \begin{cases} 1 & \text{if } i + j < p \\ b & \text{if } i + j \geq p \end{cases},$$

where $0 \leq i, j < p$.

These algebras were perhaps first introduced by Hermann Ludwig Schmid in his 1934 Ph.D Thesis at Mahrburg ([**11**], §2) with Helmut Hasse acting as his advisor. They were studied also by Teichmüller and Witt. Notation adopted here is the one used by Teichmüller in [**12**], and is a slight modification of the notation employed for symbol pairings in Algebraic Number Theory. Algebras $(b, c]$ form a special class of the so called *cyclic p-algebras*.

PROPOSITION 8.1. *The correspondence*

$$\eta \mapsto z\zeta, \qquad \zeta \mapsto \zeta, \tag{8.3}$$

induces an isomorphism of algebras

$$(b, c] \simeq \mathcal{S}_{cb^{-1}, b}. \tag{8.4}$$

PROOF. Proposition 6.3 guarantees that the homomorphism $k\langle \zeta, \eta \rangle \to \mathcal{S}_{cb^{-1}, b}$ induced by correspondence (8.3) descends to a homomorphism of k-algebras

$$(b, c] \to \mathcal{S}_{cb^{-1}, b}. \tag{8.5}$$

In order to show that (8.5) is an isomorphism, let us consider the homomorphism $k\langle z, \zeta \rangle \to (b, c]$ induced by the correspondence

$$z \mapsto z' := b^{-1}\eta\zeta^{p-1}, \qquad \zeta \mapsto \zeta.$$

Note, that (z', ζ) is a CCR-pair in $(b, c]$,

$$[\zeta, z'] = b^{-1}((\eta + 1)\zeta^p - \eta\zeta^p) = 1.$$

Identity (6.19) is thus applicable and yields

$$\eta^p = \eta + (z')^p \zeta^p$$

which combined with (8.1) implies that $(z')^p b = c$. It follows that the homomorphism $k\langle z, \zeta \rangle \to (b, c]$ descends to a homomorphism of k-algebras $S_{cb^{-1}, b} \to (b, c]$ which supplies the inverse to homomorphism (8.5). □

Tensor identities of Proposition 2.2 yield several canonical isomorphisms involving cyclic algebras. We would like to record just one.

COROLLARY 8.2. *For any pair $b \in k^*$, and $c \in k$, there exists a canonical isomorphism*

$$(b,c]^{\otimes p} \simeq \mathscr{D}_k(\mathcal{O}_{cb^{-1}})^{\otimes(p-1)} \otimes \mathscr{D}_k(\mathcal{O}_b) \simeq M_p(k)^{\otimes p}.$$

In the case when the ground ring, k, is a field, we can say more.

THEOREM 8.3. *Any element of order p in the Brauer group,* $\mathrm{Br}(k)$*, is represented by an algebra of p-symbols*

$$\mathcal{S}_\pi = \mathcal{S}_{a_1,\dots,a_n;\,b_1,\dots,b_n}\ ,$$

cf. (2.22)*, for some $\pi = (a_1,\dots,a_n;\, b_1,\dots,b_n) \in k^{2n}$ and $n \geq 1$.*

PROOF. Let us invoke a few known facts about central simple algebras over a field k of characteristic $p > 0$. The absolute Frobenius map

$$F\colon k \to k, \qquad c \mapsto c^p, \tag{8.6}$$

induces on $\mathrm{Br}(k)$ the endomorphism of multiplication by p. Map (8.6) can be represented as the canonical inclusion $k \hookrightarrow k^{1/p}$ followed by the isomorphism $k^{1/p} \simeq k$. This means that if the similarity class $[A] \in \mathrm{Br}(k)$ of an algebra A has order p in $\mathrm{Br}(k)$, then A is split by a finitely generated subfield $k(u_1,\dots,u_n) \subset k^{1/p}$.

A theorem of Teichmüller ([T], Satz 29) implies existence of $b, c \in k^*$ such that $A \otimes (b,c]$ splits over $k(u_1,\dots,u_{n-1})$. By applying this factorization argument repetitively we find that there exists

$$(b_1,\dots,b_n,c_1,\dots,c_n) \in (k^*)^{2n}$$

such that

$$A \otimes (b_1,c_1] \otimes \cdots \otimes (b_n,c_n]$$

splits over k, and this means that the opposite algebra, A^{op}, is similar to

$$(b_1,c_1] \otimes \cdots \otimes (b_n,c_n].$$

It remains now to invoke Proposition 8.1. $\square$

References

[1] Pierre Berthelot, *Cohomologie cristalline des schémas de caractéristique $p > 0$*, Lecture Notes in Mathematics **451**, Springer-Verlag, 1974.

[2] Roman Bezrukavnikov, Ivan Mirković, Dmitriy Rumynin, *Localization of modules for a semisimple Lie algebra in prime characteristic*, Annals of Mathematics **167** (2008), 945–991.

[3] Paul Adrien Dirac, *On Quantum Algebra*, Proc. Cambridge Philos. Soc. **23** (1926), 412–418.

[4] Jacques Dixmier, *Sur les algèbres de Weyl*, Bull. Soc. Math. France **96** (1968), 209–242.

[5] Kenneth G. Goodearl, Robert B. Warfield, Jr., *An Introduction to Noncommutative Noetherian Rings*, Second Edition, London Mathematical Society Student Texts **61**, Cambridge University Press, 2004.

[6] William Ogilvy Kermack, William H McCrea, On Professor Whittaker's solution of differential equations by definite integrals. Part II. Applications of the methods of non-commutative algebra, Proc. Edin. Math. Soc. (2), **2** (1931), 220–239.

[7] Max-Albert Knus, Manuel Ojanguren, *Théorie de la Descente at Algèbres d'Azumaya*, Lecture Notes in Mathematics **389**, Springer-Verlag, 1974.

[8] Dudley Ernest Littlewood, *On the Classification of Algebras*, Proc. London Math. Soc. (2) **35** (1933), 200–240.

[9] Öystein Ore, *Theory of Noncommutative Polynomials*, Annals of Mathematics **34** (1933), 480–508.

[10] Philippe Revoy, *Algèbres de Weyl en caracteristique p*, C. R. Acad. Sci. Paris *Sér.* A **276** (1973), 225–228.

[11] Hermann Ludwig Schmid, *Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper*, Math. Z. **40** (1935/6), 94–119.

[12] Oswald Teichmüller, *p-Algebren*, Deutsche Mathematik **1** (1936), 362–388 (*reprinted in*: Oswald Teichmüller, *Gesammelte Anhandlungen*, herausgegeben von L. V. Ahlfors and F. W. Gehring, Springer-Verlag, 1982, pp. 120–146).
[13] Joseph Henry Maclagan Wedderburn, *Non-commutative domains of integrity*, J. f. d. reine u. angewandte Mathematik **167** (1932), 129–141.
[14] Hermann Weyl, *Gruppentheorie und Quantenmechanik*, S. Hirzel, Leipzig 1928.
[15] Mariusz Wodzicki, *Notes on Differential Operators*, Fall 2007, 66p.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720-3840

E-mail address: `wodzicki@math.berkeley.edu`