

Appendix a

The Skew Polynomial Ring $K[\sigma]$

All statements in this chapter are relative to a field K of characteristic p and some power σ of the Frobenius endomorphism of K . They remain valid without any modification for *any* field K equipped with *any* endomorphism τ , provided that the occurrences of ' K is perfect' are read ' τ is invertible'.

a.1 The Ring $K[\sigma]$

a.1.1. Let K be a field containing the finite field k of q elements. The ring $K[\sigma]$ consists of polynomial expressions

$$x_0 + x_1\sigma + \cdots + x_n\sigma^n$$

with $x_i \in K$. Addition is defined in the usual way, multiplication is defined by the commutation rule

$$\sigma x = \tau(x)\sigma$$

where $\tau : K \rightarrow K$ is the q -th power Frobenius endomorphism. The centre of this ring is k . The left Euclidean algorithm holds, relative to the usual degree map $\deg : K[\sigma] \rightarrow \mathbf{N} \cup \{\infty\}$, therefore all left ideals in $K[\sigma]$ are principal.

If K is perfect then one can invert the roles of left and right using the formula $x\sigma = \sigma\tau^{-1}(x)$. One obtains that $K[\sigma]$ is also right Euclidean and that all right ideals are principal.

a.1.2. Since $K[\sigma]$ is left Euclidean, it has a unique skew field of fractions⁽¹⁾ which we denote by $K(\sigma)$. It consists of expressions of the form r/s with $s \neq 0$ and $r/s = r'/s'$ if and only if there exist non-zero u, u' in $K[\sigma]$ with $ur = u'r'$ and $us = u's'$.

The degree map $\deg : K(\sigma) \rightarrow \mathbf{Z} \cup \{\infty\} : r/s \mapsto \deg(r) - \deg(s)$ is well-defined and satisfies

$$\deg(tu) = \deg(t) + \deg(u).$$

It factors over $K(\sigma) \rightarrow K(\sigma)^{\text{ab}} \stackrel{\text{def}}{=} K(\sigma)^\times / [K(\sigma)^\times, K(\sigma)^\times] \cup \{0\}$.

a.2 Determinants over $K[\sigma]$

a.2.1. Denote the subring of diagonal matrices in $M(n, -)$ by $D(n, -)$. Write $E(n, -)$ for the subgroup of $GL(n, -)$ generated by the elementary matrices (corresponding to the elementary row and column operations).

The Dieudonné determinant⁽²⁾ defines a multiplicative function

$$\det : M(n, K(\sigma)) \rightarrow K(\sigma)^{\text{ab}}$$

and a short exact sequence of groups

$$1 \rightarrow E(n, K(\sigma)) \rightarrow GL(n, K(\sigma)) \rightarrow (K(\sigma)^{\text{ab}})^\times \rightarrow 1.$$

Furthermore, the subgroup $E(n, K(\sigma))$ coincides with the commutator subgroup of $GL(n, K(\sigma))$.⁽³⁾

a.2.2. As the function \det is rational in the entries of the matrix, we cannot hope for a restriction to $M(n, K[\sigma])$ with the same properties as its polynomial counterpart over commutative rings. However, consider the map

$$\deg \det : M(n, K(\sigma)) \rightarrow \mathbf{Z} \cup \{\infty\}.$$

⁽¹⁾See [COHN 1977].

⁽²⁾See [DIEUDONNÉ 1943].

⁽³⁾Over *every* skew field, E is the kernel of \det . It equals the commutator subgroup of GL unless $n = 2$ and the skew field is the finite field of two elements.

It is surjective and satisfies $\deg \det(AB) = \deg \det(A) + \deg \det(B)$. We make a little observation⁽⁴⁾ on its restriction to $M(n, K[\sigma])$.

Theorem. *The restriction of the map $\deg \det$ to $M(n, K[\sigma])$ induces an exact sequence of unitary semigroups*

$$1 \rightarrow \mathrm{GL}(n, K[\sigma]) \rightarrow M(n, K[\sigma]) \rightarrow \mathbf{N} \cup \{\infty\} \rightarrow 0.$$

Moreover, $\deg \det$ is unique in the sense that every semigroup homomorphism $f : M(n, K[\sigma]) \rightarrow \mathbf{Z} \cup \{\infty\}$ that coincides with $\deg \det$ on $D(n, K[\sigma])$ equals $\deg \det$.

Proof. We first prove the uniqueness claim and then use it to deduce the first part of the theorem.

Uniqueness. Assume that $f : M(n, K[\sigma]) \rightarrow \mathbf{Z} \cup \{\infty\}$ extends to $M(n, K(\sigma))$. As \deg has a unique extension from $K[\sigma]$ to $K(\sigma)$, we find that $f = \deg \det$ on $D(n, K(\sigma))$. Since every matrix $A \in M(n, K(\sigma))$ can be written as a product $A = ED$, with $E \in E(n, K(\sigma))$ and $D \in D(n, K(\sigma))$, and since f is necessarily zero on the commutator subgroup $E(n, K(\sigma))$ of $\mathrm{GL}(n, K(\sigma))$, we find for every $A = ED \in M(n, K(\sigma))$ that

$$f(A) = f(E) + f(D) = f(D) = \deg \det(D) = \deg \det(A).$$

The exact sequence. Given a matrix $A \in M(n, K[\sigma])$, consider the quotient of left $K[\sigma]$ -modules $K[\sigma]^n / K[\sigma]^n A$. It is a vector space over K . Now define

$$f : M(n, K[\sigma]) \rightarrow \mathbf{N} \cup \{\infty\} : A \mapsto \dim_K K[\sigma]^n / K[\sigma]^n A.$$

The third isomorphism theorem gives $f(AB) = f(A) + f(B)$ and because $f(D) = \deg \det(D)$ for diagonal matrices D , we conclude that $f = \deg \det$ on all of $M(n, K[\sigma])$. But f takes values in $\mathbf{N} \cup \{\infty\}$ and $\ker f = \mathrm{GL}(n, K[\sigma])$. This finishes the proof. \square

⁽⁴⁾See [TAEELMAN 2006].

a.3 The Non-Commutative Projective Line

In a letter⁽⁵⁾ to STUHLER, DRINFELD suggested the notion of (a vector bundle on) the non-commutative projective line. We give a brief overview, following [LAUMON *et al.* 1993], §3.

a.3.1. Rather than defining the non-commutative projective line as a geometric object, one defines the category of vector bundles on it. Assume that K is perfect.

Definition. A vector bundle of rank r on $\mathbf{P}_K^1(\sigma)$ is a pair (M, W) of

- a free $K[\sigma]$ -module M of rank r ;
- a free $K[[\sigma^{-1}]]$ -submodule $W \subset M \otimes K((\sigma^{-1}))$ that contains a $K((\sigma^{-1}))$ -basis.

A morphism of vector bundles is a homomorphism $M_1 \rightarrow M_2$ such that the induced

$$M_1 \otimes K((\sigma^{-1})) \rightarrow M_2 \otimes K((\sigma^{-1}))$$

maps W_1 into W_2 .

a.3.2. Instead of splitting a vector bundle in an ‘affine part’ M and a ‘local part at infinity’ W , one can use a standard ‘covering’ of $\mathbf{P}_K^1(\sigma)$. Then a rank r vector bundle becomes a triple (M, M', γ) with

- M a free $K[\sigma]$ -module of rank r ;
- M' a free $K[\sigma^{-1}]$ -module of rank r ;
- γ an isomorphism from $M \otimes K[\sigma, \sigma^{-1}]$ to $M' \otimes K[\sigma, \sigma^{-1}]$.

The two descriptions compare through

$$W = M' \otimes K[[\sigma^{-1}]] \subset M' \otimes K((\sigma^{-1})) \rightarrow M \otimes K((\sigma^{-1})),$$

where the arrow is the isomorphism induced from γ^{-1} , and

$$M' = W \cap M \otimes K[\sigma, \sigma^{-1}]$$

with the obvious γ .

⁽⁵⁾September 17th, 1985. See [LAUMON *et al.* 1993].

When $K[\sigma]$ is commutative, a vector bundle on $\mathbf{P}_K^1(\sigma)$ is nothing but a vector bundle on the ordinary projective line over K .

a.3.3. Denote by $\mathcal{O}(n)$ the vector bundle $(K[\sigma], \sigma^n K[[\sigma^{-1}]])$. In [LAUMON *et al.* 1993] the following classification is shown:

Theorem. *All vector bundles on $\mathbf{P}_K^1(\sigma)$ are direct sums of vector bundles of the type $\mathcal{O}(n)$.* \square

If $K[\sigma]$ is commutative then this specialises to the well-known classification of vector bundles on the commutative projective line.

Appendix b

Hilbert 90 and Other Vanishing Theorems

b.1 Galois Cohomology of $\mathrm{GL}(n)$

b.1.1. Let R be a commutative ring, S an étale R -algebra and G a finite group of R -linear automorphisms of S such that

$$S \otimes_R S \rightarrow \prod_{g \in G} S : (x, y) \mapsto \{g(x) y\}_g$$

is an isomorphism of R -algebras. This is the case, for example, when S/R is a Galois extension of fields with Galois group G . A consequence of faithfully flat descent is the following generalisation⁽¹⁾ of HILBERT'S Theorem 90.

Theorem. *Under the above hypothesis, the following are equivalent:*

- $M \otimes_R S \approx S^n$ implies $M \approx R^n$, for all projective R -modules M ;
- $H^1(G, \mathrm{GL}(n, S)) = 1$;
- if $V \approx S^n$ and $G \times V \rightarrow V$ an action of G on the abelian group V , satisfying $g(xv) = g(x)g(v)$ for all $g \in G$, $x \in S$, $v \in V$ then V has an invariant basis.

⁽¹⁾Satz 90 of HILBERT'S *Zahlbericht* [HILBERT 1897] treats the case where R is a number field, S/R a cyclic extension of prime degree, and $\mathrm{GL}(n) = \mathrm{GL}(1)$.

It may of course happen that over R all projective and finitely generated modules are free, say, for example, when R is a field or a polynomial ring over a field.⁽²⁾

Proof of the Theorem. By GROTHENDIECK'S Theorem of faithfully flat descent⁽³⁾ there is an equivalence between

- projective and finitely generated modules M on R , and,
- projective and finitely generated modules N on S , together with an action of $G \times N \rightarrow N$ satisfying $g(xv) = g(x)g(v)$,

given by the functor $M \rightsquigarrow N \stackrel{\text{def}}{=} M \otimes_R S$. This implies the Theorem as follows.

One \Rightarrow Two. Let $g \mapsto \gamma(g)$ be a 1-cocycle. The map

$$(g, (x_1, \dots, x_n)) \mapsto (g(x_1), \dots, g(x_n))\gamma(g)^t$$

defines an action of G on S^n that satisfies

$$g((xx_1, \dots, xx_n)) = g(x)g((x_1, \dots, x_n)).$$

By faithfully flat descent, these data correspond to a projective and finitely generated R -module M , such that S^n with its G -action is nothing but $M \otimes_R S$. But since M is free by the hypothesis, S^n has an invariant basis. Therefore there is an invertible matrix $\mu \in \text{GL}(n, S)$ with $\gamma(g) = \mu^{-1}g(\mu)$.

Two \Rightarrow Three. Choose an S -basis $e = (e_i)$ of V . Then for every $g \in G$ there exists a unique $\gamma(g) \in \text{GL}(n, S)$ such that $g(e) = \gamma(g)e$. It follows from the relation $g(xv) = g(x)g(v)$ that

$$h(g(e)) = \gamma(h)h(\gamma(g))e,$$

where $h(\gamma(g))$ is the matrix obtained from $\gamma(g)$ by applying $h \in G$ to all its entries. Thus, $g \mapsto \gamma(g)$ is a cocycle in $H^1(G, \text{GL}(n, S))$. Trivial by

⁽²⁾The latter by the Quillen-Suslin Theorem ('Serre's conjecture'). See [SUSLIN 1976] and [QUILLEN 1976].

⁽³⁾[GROTHENDIECK 1962], reprinted in [GROTHENDIECK 1995].

the hypothesis, it is of the form $\gamma(g) = \mu^{-1}g(\mu)$ for some $\mu \in \mathrm{GL}(n, S)$, independent of g . One checks that $\mu^{-1}e$ is an invariant basis of V .

Three \Rightarrow One. Assume that M is projective over R and that $M \otimes_R S$ is free of rank n over S . Then necessarily, M is projective of rank n over R . By the hypothesis, $M \otimes_R S$ has an invariant basis under the natural action of G and therefore there is an equivariant isomorphism

$$M \otimes_R S \rightarrow R^n \otimes_R S.$$

It remains to apply faithfully flat descent to obtain $M \approx R^n$. □

b.2 Some Variants in Positive Characteristic

b.2.1. Let K be field containing a finite field k of q elements. Denote by τ the q -th power endomorphism of K . Denote, abusively, also by τ the endomorphism of $\mathrm{GL}(n, K)$ obtained by applying τ to all the entries of elements of $\mathrm{GL}(n, K)$.

Proposition. *If K is separably closed then*

- *the map $\mathrm{GL}(n, K) \rightarrow \mathrm{GL}(n, K) : g \mapsto \tau(g)g^{-1}$ is surjective and*
- *if V is a finite dimensional vector space over K and σ a semi-linear automorphism of V , then V contains a (pointwise) σ -invariant basis.*

If K is moreover perfect then \mathbf{Z} acts on $\mathrm{GL}(n, K)$ via powers of τ . The Proposition then asserts that

$$H^1(\mathbf{Z}, \mathrm{GL}(n, K)) = 1.$$

Proof of the Proposition. First, assume that $K = k^a$. Pick a $g \in \mathrm{GL}(n, K)$. The entries of g generate a finite field $l \subset k^a$. Since $\mathrm{GL}(n, l)$ is a finite group, there is a d such that

$$g\tau(g) \cdots \tau^{d-1}(g) = 1.$$

Let l' be the subfield of K of degree d over l , then g determines a cocycle for $H^1(\mathrm{Gal}(l'/k), \mathrm{GL}(n, l'))$ and thus by b.1.1 there is an $h \in \mathrm{GL}(n, l')$ such that $g = h^{-1}\tau(h)$.

Now let K be an arbitrary separably closed field containing k^a . The map $\mathrm{GL}(n) \rightarrow \mathrm{GL}(n) : g \mapsto g^{-1}\tau(g)$ is an étale morphism of algebraic varieties over k . It is surjective on k^a -points, hence also on K -points. This proves the first part of the proposition.

The second statement is a consequence of the first, the proof being precisely the same as the ‘Two \Rightarrow Three’ part of Theorem b.1.1. \square

The proposition still holds with $\mathrm{GL}(n)$ replaced by any connected algebraic group defined over k , as was shown in [LANG 1956].

b.2.2. As a corollary we get the existence of solutions for Artin-Schreier type equations on a vector space.

Corollary. *Let K be separably closed and V a finite dimensional vector space over K . Given a semi-linear non-degenerate map $\sigma : V \rightarrow V$ as in the Proposition, a linear automorphism α of V and a constant $\beta \in V$, the equation*

$$\sigma(v) + \alpha(v) + \beta = 0$$

has a solution $v \in V$.

Proof. By the preceding Proposition, V has a σ -invariant basis. Let x_1, \dots, x_n be coordinates with respect to such a basis. Then the equation $\sigma(v) + \alpha(v) + \beta = 0$ transcribes to a system

$$\left\{ \begin{array}{l} x_1^q + \text{lower degree terms} = 0 \\ \dots \\ x_n^q + \text{lower degree terms} = 0 \end{array} \right.$$

of n equations in n variables. Make the system homogeneous to obtain n hyperplanes in \mathbf{P}_K^n . Since their intersection at infinity is visibly empty, they have, at least over an algebraic closure K^a , a common point in the standard affine chart. Since α is invertible, it follows from the above explicit form that this point is defined over $K = K^s$. \square

b.2.3. If g is an element in $\mathrm{GL}(n, K[[t]])$, denote by $\tau(g)$ the matrix obtained by raising every coefficient of every entry to the q -th power. Thus $\mathrm{GL}(n, K[[t]])^\tau = \mathrm{GL}(n, k[[t]])$.

Proposition. *Let K be a separably closed field containing k , then the map*

$$\mathrm{GL}(n, K[[t]]) \rightarrow \mathrm{GL}(n, K[[t]]) : g \mapsto g^{-1}\tau(g)$$

is surjective.

Proof. An element $g \in \mathrm{GL}(n, K[[t]])$ is a formal power series

$$g = g_0 + g_1t + g_2t^2 + \cdots$$

with $g_0 \in \mathrm{GL}(n, K)$ and $g_i \in \mathrm{M}(n, K)$. The proposition asserts that there is an $h = h_0 + h_1t + \cdots \in \mathrm{GL}(n, K[[t]])$ such that $hg = \tau(h)$, or, comparing the coefficients of t^m ,

$$\sum_{i \leq m} h_i g_{m-i} = \tau(h_m). \quad (\text{b.1})$$

One can find an h recursively. An invertible h_0 with the property that $h_0g_0 = \tau(h_0)$ exists by the previous proposition. Assume now that the coefficients h_0, h_1, \dots, h_{m-1} have been determined. Then h_m must be a solution of the Artin-Schreier type equation

$$\tau(h_m) - g_0h_m = \sum_{i < m} h_i g_{m-i}.$$

A solution h_m exists by Corollary 5.2.2 and it follows that $g = h^{-1}\tau(h)$. □

b.2.4. Now we assume that K is not only separably closed but also a valued field. Denote by $K\langle t \rangle$ the subring of $K[[t]]$ consisting of those power series $f = f_0 + f_1t + \cdots$ that satisfy

$$\text{there exists a } \rho > 1 \text{ such that } \|f_i\| \leq \rho^i \text{ for all } i.$$

Thus, $K\langle t \rangle$ is the ring of power series with positive radius of convergence. If the power series f is in $K\langle t \rangle$ then also $\tau(f)$ is in $K\langle t \rangle$.

Proposition. $g \mapsto g^{-1}\tau(g)$ is surjective on $\mathrm{GL}(n, K\langle t \rangle)$.

Proof. Let $g = g_0 + g_1t + \dots$. By the previous proposition there is an $h = h_0 + h_1t + \dots \in \text{GL}(n, K[[t]])$ with $hg = \tau(h)$. It suffices to show that $h \in \text{GL}(n, K\langle t \rangle)$. Denote the matrix norm (the maximum of the norm of the entries) by $\|\cdot\|$ and pick a $\rho > 1$ such that $\|g_i\| \leq \rho^i$. In particular $\|g_0\| \leq \rho$. From the equation (b.1) one obtains the following estimates:

$$\begin{aligned} \|h_m\| &\leq \max(\rho, \|h_m^\sigma - g_0h_m\|^{1/q}) \\ &\leq \max(\rho, \max_{i < m} \|h_i g_{m-i}\|^{1/q}) \\ &\leq \max(\rho, \rho^m \max_{i < m} \|h_i\|^{1/q}). \end{aligned}$$

Induction on m yields the bound

$$\|h_m\| \leq \rho^{2m} \max(\rho, \|h_0\|)$$

which implies $h \in \text{GL}(n, K\langle t \rangle)$. □

Appendix c

Tensor Categories

In this appendix we have summarised the vocabulary on \otimes -categories used in the thesis. For more details, we refer the reader to [DELIGNE AND MILNE 1982].

c.1 Linear Categories

c.1.1. Let R be a unitary commutative ring. A category \mathcal{C} is said to be *R -linear* if it is enriched in R -modules, has a zero object, and has finite direct sums.

The category of R -modules is R -linear, as is its full subcategory of projective and finitely generated modules.

c.1.2. An R -linear category \mathcal{C} is *R -linear pre-abelian* if every morphism has a kernel and a cokernel.

If R is a Dedekind domain, then the projective and finitely generated R -modules form an R -linear pre-abelian category.

Note that kernel and cokernel need not coincide with kernel and cokernel in larger categories. The doubling map $\mathbf{Z} \rightarrow \mathbf{Z} : n \mapsto 2n$ for example, has trivial cokernel in the \mathbf{Z} -linear pre-abelian category of finitely generated free abelian groups.

c.1.3. An R -linear pre-abelian category \mathcal{C} that is also abelian is said to be *R -linear abelian*.

The category of finite-dimensional vector spaces over a field R is an example of an R -linear abelian category.

c.2 Linear Tensor Categories

c.2.1. An R -linear tensor category is an R -linear category \mathcal{C} equipped with a bilinear bifunctor $- \otimes -$ from $\mathcal{C} \times \mathcal{C}$ to \mathcal{C} and with a collection of ACU⁽¹⁾ constraints. That is, there is a distinguished object $\mathbf{1} \in \mathcal{C}$ and a collection of isomorphisms

$$\begin{aligned} \mathbf{1} \otimes X &\rightarrow X \\ X \otimes Y &\rightarrow Y \otimes X \\ (X \otimes Y) \otimes Z &\rightarrow X \otimes (Y \otimes Z) \end{aligned}$$

functorial in X , Y , and Z , that satisfy a list of compatibility axioms. The collection of ACU constraints on a given bifunctor \otimes is *not* unique and should be considered part of the data defining an R -linear tensor category.

The category of projective R -modules with the usual tensor product and the natural constraints is an example of an R -linear tensor category.

c.2.2. An *internal hom* on an R -linear tensor category is a bilinear bifunctor $\mathcal{H}om(-, -)$ that is right adjoint to \otimes . This means that there exist functorial isomorphisms of R -modules

$$\mathcal{H}om(X \otimes Y, Z) \rightarrow \mathcal{H}om(X, \mathcal{H}om(Y, Z)).$$

Duals are defined using internal hom: $X^\vee \stackrel{\text{def}}{=} \mathcal{H}om(X, \mathbf{1})$.

c.2.3. A *rigid R -linear tensor category* is an R -linear tensor category with internal hom and so that the natural maps

$$\mathcal{H}om(X_1, Y_1) \otimes \mathcal{H}om(X_2, Y_2) \rightarrow \mathcal{H}om(X_1 \otimes X_2, Y_1 \otimes Y_2)$$

and

$$X \rightarrow (X^\vee)^\vee$$

⁽¹⁾Associativité, Commutativité, Unité. Cf. [SAAVEDRA RIVANO 1972].

are isomorphisms.

The category of finitely generated projective R -modules is rigid, its internal hom is the usual $\text{Hom}(-, -)$.

c.3 Tannakian Categories

c.3.1. Let \mathcal{C} be an R -linear rigid abelian tensor category. A functor ω from \mathcal{C} to the category of finitely generated projective R -modules is said to be a *neutral fibre functor* if it is faithful, exact and respects the tensor product on source and target categories.

c.3.2. If R and \mathcal{C} as above then one says that \mathcal{C} is *neutral Tannakian* if a neutral fibre functor ω on \mathcal{C} exists. Such a functor is in general not unique. One says that \mathcal{C} is *neutralised Tannakian* if a preferred fibre functor ω has been fixed.

Let Γ be an affine group scheme over a field L . Then the category of finite dimensional linear representations of Γ is a linear rigid abelian tensor category. The forgetful functor that associates with a representation the underlying vector space is a neutral fibre functor. This is the most general neutral Tannakian category.⁽²⁾

Theorem. *If (\mathcal{C}, ω) is a neutralised Tannakian category over L then there exists an affine group scheme Γ over L and an equivalence ϑ of \mathcal{C} to the category of representations of Γ so that ω coincides with the composition of the forgetful functor with ϑ . \square*

⁽²⁾See [DELIGNE AND MILNE 1982] or [SAAVEDRA RIVANO 1972].

