Factorization of skew polynomials over k((u))

Jérémy Le Borgne

Factorization of skew polynomials over $k(\!(u)\!)$

Jérémy Le Borgne*

September 25, 2022

Abstract

Let k be a perfect field of characteristic $p > 0$, and let $K = k(\!(u)\!)$ be the field of Laurent series over K. We study the skew polynomial ring $K[T, \phi]$, where ϕ is an endomorphism of K that extends a Frobenius endomorphism of k. We give a description of the irreducible skew polynomials, develop an analogue of the theory of the Newton polygon in this context, and classify the similarity classes of irreducible elements.

Contents

*Univ Rennes, IRMAR - UMR 6625, F-35000 Rennes, France

Introduction

Let $p > 0$ be a prime number and let k be a perfect field of characteristic p. Let $K = k(\!(u)\!)$ be the field of formal power series with coefficients in k. We denote by v the valuation map on K. Let σ be a power of the Frobenius automorphism of k (possibly, $\sigma = \mathrm{id}$). Let $b \geq 2$ be an integer. The field K is endowed with the endomorphism $\phi : K \to K$ defined by:

$$\phi\left(\sum_{n \geq n_0} a_n u^n\right) = \sum_{n \geq n_0} \sigma(a_n) u^{bn}.$$

The ring of skew polynomials over K with endomorphism σ, denoted by $K[T, \phi]$, is the K-vector space $K[T]$ endowed with the multiplication rule defined by $Xa = \phi(a)X$ for $a \in K$. In the general setting, such rings were introduced and studied by Ore ([10] and have led to extensive literature both for their theoretical study ([8]), practical arithmetics (see [7], [3]), and applications ([6], [1]) .
The paper is divided in five main sections. In the second section, we give an overview of the classical and fundamental case where ϕ is the Frobenius endomorphism and $K = \mathbf{F}_p(\!(u)\!)$ using the classical theory of the Newton polygon and the relation between skew polynomials and Galois representations, which we classify in this case. In the third section, we introduce a theory of the Newton polygon for skew polynomials over K in the general case, where it is not possible use representation theory. In the fourth section, we give a description of irreducible skew polynomials. Namely, Theorem 4.4 shows that the irreducible skew polynomials are those whose Newton polygon has a single slope (which we call monoclinic) and whose corresponding reduction in $k[T, \sigma]$ is irreducible (in a slightly twisted way). In the fifht section, we give a classification of the similarity classes of irreducible polynomials, showing that each class can be described by the data of a slope and an irreducible element in $k[T, \sigma]$ and giving the conditions for similarity of these classes (see Proposition 5.8 and Proposition 5.9 for a detailed formulation).

1 Skew polynomials and ϕ-modules over K

Let $p > 0$ be a prime number and let k be a perfect field of characteristic p. Let $K = k(\!(u)\!)$ be the field of formal power series with coefficients in k. Let σ be a power of the Frobenius automorphism of k (possibly, $\sigma = \mathrm{id}$). Let

$b \geq 2$ be an integer. The field K is endowed with the endomorphism $\phi : K \to K$ defined by:

$$\phi\left(\sum_{n \geq n_0} a_n u^n\right) = \sum_{n \geq n_0} \sigma(a_n) u^{bn}.$$

One important example is the case when ϕ is the Frobenius endomorphism of K, $x \mapsto x^p$, for which we give a presentation in Section 2 which takes advantage of the links between ϕ-modules and Galois representations.

Definition 1.1. *The ring of skew polynomials over K with endomorphism ϕ is the ring $K[T, \phi]$. The elements of T are the same as elements of $K[T]$, and multiplication is determined by the formula $Ta = \phi(a)T$ for all $a \in K$.*

Example 1.2. *If $k = \mathbf{F}_{p^2} = \mathbf{F}_p(\alpha)$, endowed with the Frobenius endomorphism ϕ, then in $K[T, \phi]$ one has:*

$$(T^2 + uT + 1)(\alpha T + 1 + u) = \alpha T^3 + (1 + \alpha^p u + u^{p^2})T^2 + (\alpha + u + u^p)T + 1 + u.$$

The ring $K[T, \phi]$ is noncommutative, but shares some nice properties with $K[T]$. In particular, it is right-euclidean, and thus has a notion of irreducible elements and a factorization theorem.

Theorem 1.3 (Ore, [10])**.** *Let $P \in K[T, \phi]$, then there exist $P_1, \ldots, P_r \in K[T, \phi]$ irreducible elements such that $P = P_1 \cdots P_r$.*

Such a factorization is not unique in general, and describing how two given factorizations are related is easier to do in the language of ϕ-modules. As for $K[T]$-modules in linear algebra, a module over $K[T, \phi]$ corresponds to a vector space endowed with an endomorphism, but in this case the endomorphism is merely *semilinear* with respect to ϕ.

Definition 1.4. *A ϕ-module over K is a couple (D, ϕ_D) where D is a finite dimensional vector space over K, and $\phi_D : D \to D$ a ϕ-semilinear endomorphism.*

A morphism of ϕ-modules is a K-linear map $f : D_1 \to D_2$ such that the following diagram is commutative:

$$\begin{array}{ccc} D_1 & \xrightarrow{f} & D_2 \\ {\scriptstyle \phi_{D_1}}\downarrow & & \downarrow{\scriptstyle \phi_{D_2}} \\ D_1 & \xrightarrow{f} & D_2 \end{array}.$$

The set of ϕ-modules over K forms an abelian category which we denote by $\mathrm{Mod}^{\phi}_{/K}$. We aim to study the full subcategory $\mathrm{Mod}^{\phi}_{/K,\mathrm{et}}$ of étale ϕ-modules over K, whose objects are the ϕ-modules (D, ϕ_D) such that $\phi_D(D)$ spans the K-vector space D.
Alternatively, let $R = K[T, \phi]$ be the noncommutative K-algebra of skew polynomials. Then $\mathrm{Mod}^{\phi}_{/K}$ is equivalent to the category of Mod_R of left-R-modules that have finite dimension over K (the semilinear map ϕ_D corresponds to the map of left-multiplication by the indeterminate T). If $\mathcal{B} = (e_1, \dots, e_d)$ is a basis of the ϕ-module D, and $(e_1^*, \dots, e_d^*)$ is the dual basis, then the matrix of ϕ_D in the basis $\mathcal{B}$ is the matrix $M \in \mathcal{M}_d(K)$ whose coefficient in position (i, j) is $e_i^*(\phi_D(e_j))$. In the case, if $P \in GL_d(K)$, the matrix of ϕ_D in the basis given by the columns of P is $P^{-1}M\phi(P)$, where $\phi(P)$ is the matrix obtained from P by applying ϕ to each coefficient. In particular, since $b \geq 2$, there exists a basis $\mathcal{B}$ of D such that $k[\![u]\!]$ submodule generated by the basis is stable by ϕ_D, *i.e.* such that the matrix of ϕ_D is this basis has coefficients in $k[\![u]\!]$.
This point of view allows us to describe more precisely how two factorizations of $P \in K[T, \phi]$ (as in Theorem 1.3) are related.

Definition 1.5. *Let $A, B \in K[T, \phi]$, then A and B are similar if the corresponding ϕ-modules $K[T, \phi]/K[T, \phi]A$ and $K[T, \phi]/K[T, \phi]B$ are isomorphic.*

Then, the number of occurrences of each similarity class of irreducible skew polynomials that appear in a factorization of a given skew polynomial P does not depend on the factorization, but only on P itself.
The aim of this paper is to give a description of irreducible elements of $K[T, \phi]$, give a classification of similarity classes, and describe how the similarity classes of the irreducible factors of a skew polynomial can be determined.
On a broader scope, we also aim to set the theoretical foundations to give a factorization algorithm for elements of $K[T, \phi]$, which is planned in future work.

2 The classical case

The classical case for ϕ-modules is the case when ϕ is (a power of the) Frobenius morphism. For the sake of simplicity, we will assume that $\phi(x) = x^p$ for all $x \in K$. Let K^{sep} be a separable closure of K, then K^{sep}, which is endowed with the canonical Frobenius morphism $x \mapsto x^p$ that we also

denote by ϕ. Let us recall how the classical theories of ϕ-modules (see [9]) and Newton polygons (see [5] , Chap. 6) apply in this case.

2.1 Skew polynomials and ϕ-modules over K

Let (D, ϕ_D) be an étale ϕ-module over K. Then $\mathrm{Hom}_{K,\phi}(D, K^{\mathrm{sep}})$ is a $\mathbf{F}_p$-vector space. Moreover, the Galois group $\mathcal{G} = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts on $\mathrm{Hom}_{K,\phi}(D, K^{\mathrm{sep}})$, and V is invariant under this action. Therefore, V is naturally a $\mathbf{F}_p$-linear representation of $\mathcal{G}$. Conversely, if V is a $\mathbf{F}_p$-representation of $\mathcal{G}$, then $\mathrm{Hom}_{\mathcal{G}}(V, K^{\mathrm{sep}})$ is an étale ϕ-module over K, and these two constructions are converse of each other (thus, the corresponding functors are equivalences of categories between ϕ-modules over K and $\mathbf{F}_p$-representations of $\mathcal{G}$).

$$\begin{array}{rcl} \{\mathbf{F}_p - \text{representations of } \mathcal{G}_K & \longrightarrow & \{\text{Étale } \phi\text{-modules over } K\} \\ V & \mapsto & \mathrm{Hom}_{\mathcal{G}_K}(V, K^{\mathrm{sep}}) \\ \mathrm{Hom}_{K,\phi}(D, K^{\mathrm{sep}}) & \hookleftarrow & D \end{array}$$

Now, let $P \in K[T, \phi]$ and let $D_P = K[T, \phi]/K[T, \phi]P$. Then the corresponding Galois representation is the set V_P of roots of $P(\phi)$ in K^{sep} (more precisely, the map $D_P \to V_P$ defined by $f \mapsto f(t)$ is an isomorphism of $\mathbf{F}_p$-representations of $\mathcal{G}$ from V to V_P).

Proposition 2.1. *Let $V_P \subset K^{sep}$ be the $\mathbf{F}_q$-vector subspace of roots of $P(\phi)$. Then V has a nondecreasing filtration $(V_\mu)_{\mu \in \mathbf{R}}$ of V by subrepresentation. The jumps of the filtration are the opposite of the valuations of the elements of V.*

Proof. By the classical theory of the Newton polygon, the valuations of the roots of the linearized polynomial $P(\phi)$ can be recovered from its Newton polygon. Let $\mu \in \mathbf{R}$ and let $V_\mu = \{x \in V,\ v(x) \geq -\mu\}$. Then V_μ is a $\mathbf{F}_q$-subspace of V that is stable under the action of $\mathcal{G}$, *i.e.* a subrepresentations of V. Therefore, the family $(V_\mu)_{\mu \in \mathbf{R}}$ is an increasing filtration of V. Let $V_\mu^+ = \{x \in V,\ v(x) > -\mu\}$, then $V_\mu \neq V_\mu^+$ if and only if $P(\phi)$ has a root of valuation $-\mu$. Thus, the slope filtration has finitely many jumps that are the opposite of the valuations of the roots of $P(\phi)$. In general, a factor of $P(\phi)$ of given valuation does not correspond to a subrepresentation of V (only to a subquotient of V), but a right factor does.
If the polynomial $P \in K[T, \phi]$ is irreducible, then so is the representation V_P, and therefore the Newton polygon of $P(\phi)$ only has one slope. The corresponding filtration on the ϕ-module D_P yields a factorization of the skew polynomial D_P as a product of skew polynomials with a single slope, which may not be irreducible. □

These results are generalized in [2] to the case of a more general endomorphism ϕ, when k is algebraically closed. The first section of the present paper is to further generalize these results simultaneously in two directions: first, to the case of a perfect residue field, and second to the more general version of the endomorphism ϕ that has already been introduced.

2.2 Irreducible Galois representations

In order to highlight what type of result should be expected for the first generalization that we indend to give, we present an elementary version in the classical case (where ϕ is the Frobenius endomorphism) based on the classification of irreducible Galois representations and the equivalence of categories of the previous section.
In this subsection, we assume that $k = \mathbf{F}_p$. Let $K = k(\!(u)\!)$, K^{sep} be the separable closure of K and let $\mathcal{G}_K = \text{Gal}(K^{\text{sep}}/K)$ be the absolute Galois group of K. Recall that this group has a natural ramification filtration, which cuts out a filtration of K^{sep} by subextensions whose first steps are $K^{\text{sep}} \supset K^{\text{tr}} \supset K^{\text{ur}} \supset K$. Let $I_t = \text{Gal}(K^{\text{tr}}/K^{\text{ur}})$ be the tame inertia subgroup. It is an abelian group and for all $n \geq 1$, the fundamental character of level n is defined as:

$$\omega_n : \left| \begin{array}{ccc} I_t & \to & \bar{\mathbf{F}}_p^{\times} \\ g & \mapsto & \frac{gu_n}{u_n}, \end{array} \right.$$

where $u_n = u^{\frac{1}{p^n-1}}$. Further, let $\sigma \in \mathcal{H}_K$ such that the projection of σ in $\text{Gal}(K^{\text{ur}}/K) \simeq \text{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p)$ is the Frobenius map $x \mapsto x^p$.

Proposition 2.2. *The irreducible $\mathbf{F}_p$-representations of $\mathcal{G}_K$ are described by:*

- *a level δ and an integer $0 \leq s \leq p^\delta - 1$,*
- *an irreducible skew polynomial $P = T^m - \sum_{i=0}^{m-1} \lambda_i T^i \in \mathbf{F}_{p^\delta}[T, \sigma]$.*

The corresponding representation has a basis over $\mathbf{F}_{p^\delta}$ that is of the form $(x, \sigma x, \ldots, \sigma^{m-1}x)$ such that:

- *$\forall g \in I_t$, $gx = \omega_\delta^s(g)x$,*
- *$\sigma^m x = \sum_{i=0}^{m-1} \lambda_i \sigma^i x$, and V only depends up to isomorphism on the digits of s in base p and the similarity class of P.*

Proof. Let V be an irreducible representation of $\mathcal{G}_K$. Let $I_p \subset \mathcal{G}_K$ be the wild inertia sugroup: since V is irreducible, the action of $\mathcal{G}_K$ factors through I_p and yields an irreducible representation of $\mathcal{H}_K = \mathcal{G}_K/I_p$. Now, let $W \subset V$

be an irreducible representation of I_t. Then $E = \mathrm{End}_{I_t}(W)$ is a division algebra by Schur's lemma, hence a field by Wedderburn's theorem. This endows W with a natural structure of E-representation. Since I_t is abelian, the elements of I_t act as elements of E, so that W is has dimension 1 as a E-vector space. Let $\delta = \dim W$, then W can be identified with a character $\omega : I_t \to \mathbf{F}_{p^\delta}^\times$. Since I_t is a procyclic group, such characters are precisely the powers of the fundamental character of level δ, *i.e.* there exists an integer $0 \leq s \leq p^\delta - 1$ such that $\omega = \omega_\delta^s$. We may see as a $\mathbf{F}_p$-representation through the choice of a basis of $\mathbf{F}_{p^\delta}/\mathbf{F}_p$: any other choice of basis may lead to a different value of s, but the digits of s in base p does not depend on this choice. These digits are the tame inertia weights of the representation W.
It remains to see how the Frobenius acts on V. Assume $W \simeq \omega_\delta^s$, then σW is stable by I_t and, as a representation of I_t, is isomorphic to ω_δ^{ps} (because of the relation $\sigma g \sigma^{-1} = g^p$ for all $g \in I_t$). Let m be maximal such that the sum $W_m = W + \sigma W + \cdots + \sigma^{m-1} W$ is a direct sum of $\mathbf{F}_{p^\delta}$-vector spaces. Then by hypothesis, $\sigma^r W \cap W_r$ is nonzero, so that $\sigma^r W \subset W_r$. Therefore, W_m is stable under the action of I_t and σ, and thus $W_m = V$. One has:

$$V = \omega_\delta^s \oplus \omega_\delta^{ps} \oplus \cdots \oplus \omega_\delta^{p^{m-1}s}.$$

Let $x \in W$, then there exist $\lambda_0, \ldots, \lambda_{r_1}$ such that $\sigma^r x = \lambda_0 x + \lambda_1 \sigma x + \cdots + \lambda_{r-1}\sigma^{m-1}x$. The polynomial $T^m - \sum_{i=0}^{m-1} \lambda_i T^i$ depends on the choice of W and x, but its similarity class in $E[T, \sigma]$ does not. Indeed, the map σ^δ is E-linear and its minimal polynomial is the norm $\mathcal{N}(P)$, which does not depend on any choice and completely determines the similarity class of P (see [4], Prop. 2.1.17.). □

2.3 Irreducible skew polynomials in $K[T, \phi]$ (classical case)

We still assume that $K = \mathbf{F}_p(\!(u)\!)$. According to the previous subsections, an irreducible element $A \in K[T, \phi]$ corresponds to an irreducible representation of $\mathcal{G}_K$, and therefore its similarity class can be described by a level δ, a weight s, and an irreducible polynomial $Q \in \mathbf{F}_p[T^\delta]$. Let us now explain how these invariants may be computed directly from A. Let $s \in \mathbf{Z}$, let $\delta \in \mathbf{N}^*$ and let $m \in \mathbf{N}^*$. Let $v = -\frac{p^{m\delta}-1}{p^\delta - 1} \in \mathbf{N}$. Let $\lambda_1, \ldots, \lambda_{m-1} \in k$ and $\lambda_0 \in k^\times$.

Proposition 2.3. *Let $A = (T^{\delta m} - \lambda_{m-1} T^{\delta(m-1)} - \cdots - \lambda_0) u^{sv} \in K[T^\delta, \phi]$. Then there exists $x \in V$ such that for $g \in I_t$, $gx = \omega_\delta^s(g)x$ and such that $\sigma^{\delta m} x = \sum_{j=0}^{m-1} \lambda_j \sigma^{\delta j} x$.*

Proof. By definition, the corresponding representation of $\mathcal{G}_K$ is the set of roots of

$$L_A = u^{p^{\delta m} sv} x^{p^{\delta m}} - u^{p^{\delta(m-1)} sv} \lambda_{m-1} x^{p^{\delta(m-1)}} - \cdots - \lambda_0 u^{sv} x.$$

The Newton polygon of this polynomial has only one slope, equal to $-\frac{s}{p^\delta - 1}$, so that all the nonzero roots of this polynomial have the same valuation, equal to $\frac{s}{p^\delta - 1}$. More precisely, if ξ is a root of A, then $u^{-\frac{s}{p^\delta - 1}} \xi$ is a root of $x^{p^{\delta m}} - \sum_{j=0}^{m-1} \lambda_j x^{p^{\delta j}}$, so that $x^{\delta m} - \sum_{j=0}^{m-1} \lambda_i x^{\delta i}$ is the minimal polynomial of σ over $\mathbf{F}_p$. □

Corollary 2.4. *Every irreducible étale skew polynomial in $K[T, \phi]$ is of the form $\bar{A} u^{sv}$ where $\bar{A} \in k[T^\delta]$ is irreducible of degree m (for some m), $s \in \mathbf{Z}$ and $v = \frac{p^{m\delta} - 1}{p^\delta - 1}$.*

Proof. By Proposition 2.3, each such polynomial corresponds to an irreducible representation of $\mathcal{G}_K$ and by Proposition 2.2 every irreducible representation of $\mathcal{G}_K$ is of this form. □

3 The Newton polygon of a skew polynomial

From now on, we revert to the more general setting where k is perfect of characteristic $p > 0$, $K = k(\!(u)\!)$ and ϕ is such that $\phi(u) = u^b$ with $b \geq 2$ an integer, and the restriction of ϕ to K is a power of the Frobenius endomorphism. The goal of this section is to introduce a notion of Newton polygons for elements of $K[T, \phi]$ that is analogous to the classical theory.

3.1 Definitions

Definition 3.1. *Let $A \in K[T, \phi]$, $A = \sum_{i=0}^{d} a_i T^i$. The* Newton polygon of P *is the lower convex hull of the set of points $\{(b^i, v(a_i)),\ 0 \leq i \leq d\} \subset \mathbf{R}^2\}$.*

Definition 3.2. *The* slopes *of the skew polynomial $A \in K[T, \phi]$ are the slopes of its Newton polygon.*
The multiplicity *of a slope μ of A is m if the endpoints of the segment of slope μ in the Newton polygon of A are of the form $(b^i, v(a_i)), (b^{i+m}, v(a_{i+m}))$.*
The skew polynomial A is said to be monoclinic *if it has only one slope.*

Definition 3.3. *Let $A \in K[T, \phi]$ and let μ be a slope of A. Then there exists a unique $\nu \in \mathbf{Q}$ such that $u^\nu A u^{-\mu}$ has valuation zero. The reduction of $u^\nu A u^{-\mu}$ modulo the ideal of skew polynomials of positive valuation is called the* μ-reduction *of A.*

3.2 The slopes of a product of skew polynomials

Lemma 3.4. *Let $P, Q \in K[T, \phi]$, with $P = \sum_{i=0}^{n} p_i T^i$, and $Q = \sum_{j=0}^{d} q_j T^j$ such that:*

- $\min_{0 \leq i \leq n} v(p_i) = 0$*,*
- $q_d = 1$*, $v(q_0) = 0$, and $v(q_i) \geq 0$ for all $1 \leq i \leq d-1$.*

Let $i_0 = \min\{0 \leq i \leq n,\ v(p_i) = 0\}$ and $i_1 = \max\{0 \leq i \leq n,\ v(p_i) = 0\}$. Then the vertices of the Newton polygon of $A = PQ$ are:

- *$(b^i, v(p_i))$ if $i \leq i_0$ and $(b^i, v(p_i))$ is a vertex of the Newton polygon of P,*
- *$(b^{i+d}, v(p_i))$ if $i \geq i_1$ and $(b^i, v(p_i))$ is a vertex of the Newton polygon of P.*

In particular, the Newton polygon of PQ has an edge of slope 0 and multiplicity $i_1 - i_0 + d$.

Proof. Let $0 \leq i \leq i_0$. Then the coefficient of T^i in PQ is $c_i = \sum_{j=0}^{i} p_j \phi^j(q_{i-j})$. For $0 \leq j < i$, $v(p_j) \geq 0$, $v(q_{i-j}) \geq 0$, and since $v(q_0) = 0$, $v(c_i) \geq v(p_i)$. Moreover, assume that $(b^i, v(p_i))$ is a vertex of the Newton polygon of P. Then for all $0 \leq j \leq i$, $v(p_j) > v(p_i)$, so that $v(c_i) = v(p_i)$. Moreover, if $(b^i, v(p_i))$ and $(b^{i'}, v(p_{i'}))$ are two consecutive vertices of the Newton polygon of P, then for $i \leq j \leq i'$, $\frac{v(p_j) - v(p_{i'})}{b^j - b^{i'}} \geq \frac{v(p_i) - v(p_{i'})}{b^i - b^{i'}}$. Thus, $\frac{v(c_j) - v(c_{i'})}{b^j - b^{i'}} \geq \frac{v(c_i) - v(c_{i'})}{b^i - b^{i'}}$. This shows that, for $i \leq i_0$, the vertices of the Newton polygon of PQ are the same as the vertices of the Newton polygon of P. On the other hand, for $i \geq i_1$, $c_{i+d} = \sum_{j=i}^{i+d-j} p_j \phi^j(q_{i+d-j})$. This shows in particular that $v(c_{i_1+d}) = 0$, and more generally that $v(c_{i+d}) = v(p_i)$ whenever $(b^i, v(p_i))$ is a vertex of the Newton polygon of P. Then a calculation similar to the previous one shows that the $(b^{i+d}, v(p_i))$ for the $i \geq i_1$ such that $(b^i, v(p_i))$ is a vertex of the Newton polygon of P, are indeed vertices of the Newton polygon of PQ.
Finally, since $v(c_{i_0}) = v(c_{i_1+d}) = 0$, there are no other vertices in the Newton polygon of PQ. □

Proposition 3.5. *Let $P, Q \in K[T, \phi]$. Let $\mu_1 < \cdots < \mu_r$ be the slopes of P. Assume that Q is monic and monoclinic of slope μ and degree d, so that $\mu = -\frac{s}{b^d - 1}$. Let r_0 be such that $\mu_{r_0} \leq \mu < \mu_{r_0+1}$. Then the slopes of PQ are $\mu_1 + s < \cdots < \mu_{r_0} + s \leq \mu < b^{-d}\mu_{r_0+1} < \cdots < b^{-d}\mu_r$.*

Proof. Multiplying by $u^{-\mu}$ on the right translates the slopes by $-\mu$, so the result on the slopes follows from applying Lemma 3.4 to $Pu^{-b^d\mu}$ and $u^{b^d\mu}Qu^{-\mu}$ (note that slopes may be computed in any extension of K as they are defined by the Newton polygon).
Indeed, the lemma shows that the smallest slopes of $Pu^{-b^d\mu}(u^{b^d\mu}Qu^{-mu}$ are the $\mu_i - b^d\mu$, and its highest slopes are the $(\mu_i - b^d)/b^d$, with one middle slope equal to zero. Multiplying again on the right by u^μ allows us to recover the slopes of PQ, and since $(b^d-1)\mu = -s$, we get the prescribed slopes. □

4 Irreducible skew polynomials

In this section, we use the results about Newton polygons of skew polynomials to give a description of the irreducible elements of $K[T,\phi]$.

Definition 4.1. *Let $\mu \in \mathbf{Q}^\times$. Write $\mu = b^\alpha \frac{s}{t}$, with $\alpha \in \mathbf{Z}$, and the two integers $s \in \mathbf{Z}$ and $t \in \mathbf{Z}\setminus\{0\}$ coprime, and t coprime to b. Then the b-length of μ, denoted by $\ell_b(\mu)$, is the order of b modulo t (or 0 if $t = 1$).*

Remark 4.2. *By definition, when $\mu \in \mathbf{Z}_{(b)}$, $\ell_b(\mu)$ is the smallest integer ℓ such that $\mu(b^\ell - 1) \in \mathbf{Z}$. Every such integer is a multiple of $\ell_b(\mu)$.*

Lemma 4.3. *Let μ be the smallest slope of $A \in K[T,\phi]$. Let P_μ be the μ-reduction of A. Let P be a right divisor of P_μ in $k[T^{\ell_b(\mu)}, \sigma^{\ell_b(\mu)}]$. Then there exists $Q_\mu \in K[T,\phi]$ such that Q_μ has slope μ and μ-reduction P, and such that Q_μ is a right-divisor of A.*

Proof. We may assume that $\mu = 0$. We show that there are sequences of skew polynomials $(F_j)_{j\geq 0}$, $(G_j)_{j\geq 0}$, and a sequence v_j with $\lim v_j = +\infty$, such that the valuation of $A - F_jG_j$ is $\geq v_j$, and such that $v(G_j - P) > 0$.
By hypothesis, there exists $F \in k[T,\sigma]$, $R \in k[\![u]\!][T,\phi]$ and $\nu > 0$ such that $A - FP = u^\nu R > 0$. Then the induction hypothesis holds for $j = 0$ with $F_0 = F$, $G_0 = P$, and $\nu_0 = \nu$.
Now assume that such sequences have been constructed up to some value of $j \geq 0$. We may write $A - F_jG_j = u^{\nu_j}R_j$. Let $\bar{R}_j$ be the reduction modulo $u^{>0}$ of R_j. Let $\bar{R} = MG_0 + a_0N$ be the right euclidean division of $\bar{R}$ by G_0, where $a_0 \in k^\times$ is the constant coefficient of F (it is nonzero because μ is the smallest slope of A). Then we have $(F_j + u^{\nu_j}M)(G_j + u^{\nu_j}N) = F_jG_j + u^{\nu_j}MG_j + u^{\nu_j}a_0N + O(u^{\nu_j+1})$. Thus, if we let $F_{j+1} = F_j + u^{\nu_j}M$ and $G_{j+1} = G_j + u^{\nu_j}N$, then $v(A - F_{j+1}G_{j+1}) \geq \nu_j + 1$.
In particular, the sequences (F_j) and (G_j) are convergent, and their respective limits F and G are such that $A = FG$ and $v(Gu^{-\mu} - P) > 0$. In

particular, $Q_\mu = G$ is a right-divisor of A and has slope μ and μ-reduction P. □

Theorem 4.4. *Let $A \in K[T, \phi]$. Then A is irreducible if and only if:*

- *A is monoclinic of slope μ, with $\ell_b(\mu) = \ell$*
- *the μ-reduction of A is irreducible in $k[T^\ell, \sigma^\ell]$.*

Proof. By Lemma 4.3, if A has more than one slope or is monoclinic but has a μ-reduction that is reducible, then A is reducible. Conversely, assume that A is monoclinic of slope μ and that its μ-reduction is irreducible. Assume $A = A_1 A_2$, then $u^\nu A u^{-\mu} = (u^\nu A_1 u^{-\nu_2})(u^{\nu_2} A_2 u^{-\mu})$, where ν_2 is such that $(u^{\nu_2} A_2 u^{-\mu})$ is the reduction of A_2. Then the irreducibility of the μ-reduction of A shows that either A_1 or A_2 is constant, which proves the irreducibility of A. □

Since the irreducible factors appearing in the factorization of a skew polynomial $A \in K[T, \phi]$ are determined up to similarity, we want to describe the similarity classes of irreducible skew polynomials. In terms of ϕ-modules, this amounts to describing the isomorphism classes of simple objects in $\mathrm{Mod}^{\phi}_{/K}$, and giving the similarity classes of the irreducible factors of a skew polynomial amounts to giving the semi-simplification of the corresponding ϕ-module. Note that in general, the fact that P is irreducible and appears in a factorization of A does not guarantee that A has a right-factor similar to P (whereas this is indeed the case over a finite field, see [4], Lemma 2.1.18).

5 Similarity classes of irreducible skew polynomials

The aim of this section is to describe the similarity classes of irreducible elements in $K[T, \phi]$. The slopes of a skew polynomial are not invariant by similarity: indeed, if $P \in K[T, \phi]$, then left-multiplication by T followed by right-division by T yield a polynomial similar to P whose coefficients have had all their valuations mutiplied by b, so the same holds for its slopes. Similarly, multiplication by u^m turns P into a skew polynomial similar to P, and its slopes are the slopes of P translated by m. This leads to the following defintions.

Definition 5.1. *The rational numbers μ, μ' are equivalent if $\ell_b(\mu) = \ell_b(\mu') = \ell$ and there exists an integer $0 \leq i \leq \ell$ such that $\mu - b^i \mu' \in \mathbf{Z}$.*

Remark 5.2. *Alternatively, two rational numbers μ_1 and μ_2 are equivalent if and only if they have the same b-length ℓ, and $(b^\ell-1)\mu_1$ and $(b^\ell-1)\mu_1$ have the same digits when they are written in base b.*

Definition 5.3. *Let $\mu \in \mathbf{Q}^\times$ with $\ell_b(\mu) = \ell$ and let $P \in k[T^\ell, \sigma^\ell]$. Then $P^{[\mu]} = u^{-\mu} P u^\mu \in K[T, \phi]$.*

Lemma 5.4. *Let $\mu \in \mathbf{Q}^\times$ with $\ell_b(\mu) = \ell$ and $P \in k[T^\ell, \sigma^\ell]$, the skew polynomial $P^{[\mu]}$ has slope μ and μ-reduction P.*

Proof. The μ-reduction can be computed directly from the definition of $P^{[\mu]}$. □

Lemma 5.5. *Let $P \in K[T, \phi]$ be monic étale with integral coefficients. Let $v_0 \geq 0$ be the valuation of the constant coefficient of P. Let $Q \in K[T, \phi]$ monic and assume that $v(P - Q) > bv_0/(b-1)$. Then P and Q are similar.*

Proof. Let C_P (resp. C_Q) be the companion matrix of P (resp. of Q). Let $M_0 = I_d$ and define the sequence $(M_n)_{n\geq 0}$ inductively by $M_{n+1} = C_Q \phi(M) C_P^{-1}$. Since $v(\det C_P) = v_0$, the cofactor matrix formula shows that $v(C_Q C_P^{-1} - I_d) > v_0/(b-1)$, *i.e.* $v(M_1 - M_0) > v_0/(b-1)$. Now assume that for some $n \in \mathbf{N}^*$, $v(M_n - M_{n-1}) = v > \frac{v_0}{b-1}$. Then $M_{n+1} - M_n = C_Q \phi(M_n - M_{n-1}) C_P^{-1}$, and therefore $v(M_{n+1} - M_n) \geq bv - v_0 > v$. In particular, the sequence $(M_n)_{n\in\mathbf{N}}$ is convergent. Let M be the limit of this sequence, then M is nonsingular because it is equal to I_n modulo u, and $C_P = M^{-1} C_Q \phi(M)$. Thus, P and Q are similar. □

Lemma 5.6. *Let $P \in K[T, \phi]$ be monoclinic of slope μ. Let $\bar{P}$ be its μ-reduction. Then P is similar to $\bar{P}^{[\mu]}$.*

Proof. Let $Q = \bar{P}^{[\mu]} \in K[T, \phi]$ since P is monoclinic of slope μ. Up to left multiplication of P by a constant, we may assume that $v(P - \bar{P}) > 0$. Up to right mutliplication by a constant, we may assume that $\mu \leq 0$. By Lemma 5.5, we may assume that the constant coefficient of P is of the form $\lambda_0 u^s$, and in particular P and $\bar{P}^{[\mu]}$ have the same constant coefficient.
Now let $D = K[T, \phi]/PK[T, \phi]$. This ϕ-module is endowed with its canonical basis $(x, \phi(x), \ldots, \phi^{d-1}(x))$, so that $P(\phi)(x) = 0$. Let $x_0 = x$, and define by induction $x_{n+1} = \bar{P}^{[\mu]}(\phi)(x_n) + x_n$. For $n \in \mathbf{N}^*$, $x_{n+1} - x_n = (\bar{P}^{[\mu]} - P)(\phi)(x_n - x_{n-1})$. Since P and $\bar{P}^{[\mu]}$ have the same constant coefficient, this shows that the sequence $(x_n)_{n\in\mathbf{N}}$ is convergent. Its limit x_∞ is such that $x_\infty = \bar{P}^{[\mu]}(\phi)(x_\infty) + x_\infty$, so that $\bar{P}^{[\mu]}(\phi)(x_\infty) = 0$. Therefore, $\bar{P}^{[\mu]}$ is similar to P. □

Corollary 5.7. *The slopes of a product of skew polynomials, counted with multiplicities, are up to equivalence the slopes of the factors, counted with multiplicities.*

Proof. Let $P, Q \in K[T, \phi]$. Let us show induction on the number of slopes of Q that the slopes of PQ are, up to equivalence, the slopes of P and Q. Assume Q is monclinic, then the result follows from Proposition 3.5 (since $\mu_i + s$ and μ_i / b^d are equivalent to μ_i). Suppose the result holds when Q has m slopes, and suppose now that Q has $m+1$ slopes. Then Q may be factored as $Q = Q_1 Q_\mu$ with Q_μ monoclinic of slope μ. By induction hypothesis, Q_1 has m slopes, the slopes of Q are the slopes of Q_1 and μ, and the slopes of PQ_1 are the slopes of P and Q_1 (up to equivalence). Thus, the results holds again as consquence of the case of monoclinic Q. □

Proposition 5.8. *Every irreductible element of $K[T, \phi]$ is similar to an element of the form $P^{[\mu]}$ with $P \in k[T^\ell, \sigma^\ell]$ irreducible, with $\ell = \ell_b(\mu)$.*

Proof. Let $P \in k[T, \phi]$ be irreducible. By Theorem 4.4, P is monoclinic of slope μ with $\ell_b(\mu) = \ell$, and its μ-reduction $\bar{P}$ is irreducible in $k[T^\ell, \sigma^\ell]$.
By Lemma 5.6, P is similar to $\bar{P} u^\mu$. Since $\bar{P} \in k[T^\ell, \sigma^\ell]$, P is indeed of the prescribed form. □

Proposition 5.9. *The irreducible skew polynomials $P_1^{[\mu_1]}$ and $P_2^{[\mu_2]}$ are similar if and only if $\mu_1 \sim \mu_2$ and $P_1 \sim_{k[T^\ell, \sigma^\ell]} P_2$.*

Proof. Let P_1 be a monoclinic monic skew polynomial, and let C_1 be its companion matrix. Then the slope of P_1 is $\frac{v(\det(C_1))}{b^{\deg P} - 1}$. Assume P_2 is similar to P_1, then there exists $M \in GL_d(K)$ such that $MC_1 = C_2 \phi(M)$, so that $\mu_1 + \det M = \mu_2 + b \det M$. Thus, $\mu_1 - \mu_2 \in (b-1)\mathbf{Z}$, so that $(b^d - 1)\mu_1$ and $(b^d - 1)\mu_2$ have the same digits when written in base b. This shows that $\mu_1 \sim \mu_2$. Thus, we may assume that $\mu_1 = \mu_2$, and in this case, the μ-reductions of P_1 and P_2 are similar.
Conversely, if $\mu = \mu_1 \sim \mu_2$ and the μ-reductions of P_1 and P_2 are similar, then an explicit isomorphism between the corresponding σ-modules over k yields an isomorphism between the ϕ-modules associated to P_1 and P_2. □

Note that using Lemma 4.3 gives a theoretical way to recursively obtain the list of the invariants describing the similarity classes of the irreducible factors of P: if μ is the smallest slope of the Newton polygon of P, then the μ-reduction of P can be factored in $k[T^\ell, \sigma^\ell]$, an irreducible right-factor of this μ-reduction yields an irreducible right factor of P, and the data of μ and such a factor describe one class of irreducible polynomials in $K[T, \phi]$.

References

[1] Delphine Boucher and Felix Ulmer. Coding with skew polynomial rings. *J. Symb. Comput.*, 44(12):1644–1656, 2009.

[2] Xavier Caruso. On the classification of some simple ϕ-modules (Appendix to "On the structure of some moduli spaces of finite flat group schemes" of E. Hellmann). *Moscow Mathematical Journal*, 9, 01 2009.

[3] Xavier Caruso and Jérémy Le Borgne. Fast multiplication for skew polynomials. In *Proceedings of the 42nd international symposium on symbolic and algebraic computation, ISSAC 2017, Kaiserslautern, Germany, July 25–28, 2017*, pages 77–84. New York, NY: Association for Computing Machinery (ACM), 2017.

[4] Xavier Caruso and Jérémy Le Borgne. A new faster algorithm for factoring skew polynomials over finite fields. *J. Symb. Comput.*, 79:411–443, 2017.

[5] J. W. S. Cassels. *Local fields*, volume 3 of *Lond. Math. Soc. Stud. Texts*. Cambridge University Press, Cambridge, 1986.

[6] È. M. Gabidulin. Theory of codes with maximum rank distance. *Probl. Inf. Transm.*, 21:1–12, 1985.

[7] Mark Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. Symb. Comput.*, 26(4):463–486, 1998.

[8] Nathan Jacobson. *Finite-dimensional division algebras over fields*. Berlin: Springer, 1996.

[9] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. Modular Functions of one Variable III, Proc. internat. Summer School, Univ. Antwerp 1972, Lect. Notes Math. 350, 69-190 (1973)., 1973.

[10] Øystein Ore. Theory of non-commutative polynomials. *Ann. Math. (2)*, 34:480–508, 1933.