Publications mathématiques de Besançon
Algèbre et théorie des nombres

Florent Ulpat Rovetta

A strategy and a new operator to generate covariants in small characteristic

2018, p. 85-99.

<http://pmb.cedram.org/item?id=PMB_2018____85_0>

Publication éditée par le laboratoire de mathématiques de Besançon, UMR 6623 CNRS/UFC

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Publications mathématiques de Besançon – 2018, 85-99

A STRATEGY AND A NEW OPERATOR TO GENERATE COVARIANTS IN SMALL CHARACTERISTIC

by

Florent Ulpat Rovetta

Abstract. — We present some new results about covariants in small characteristic. In Section 1, we give a method to construct covariants using an approach similar to Sturmfels. We apply our method to find a separating system of covariants for binary quartics in characteristic 3. In Section 2, we construct a new operator on covariants when the characteristic is small compared to the degree of the form.

Résumé. — (*Une stratégie et un nouvel opérateur pour générer des covariants en petite caractéristique*) Nous présentons quelques résultats nouveaux sur les covariants en petite caractéristique. Dans la section 1, nous expliquons une méthode pour construire des covariants en utilisant une approche similaire à celle de Sturmfels. Nous appliquons notre méthode pour obtenir un système séparant pour les covariants des formes quartiques binaires en caractéristique 3. Dans la section 2, nous construisons un nouvel opérateur sur les covariants lorsque la caractéristique est petite par rapport au degré des formes.

Introduction

We are interested in the computation of covariants of binary forms in small characteristic with a similar point of view to [1] and in association with the moduli space of hyperelliptic curves. Although in characteristic 0 or in large characteristic it is a classic problem (but still formidable in practice when the degree of the form is higher than 10), in small characteristic the approach based on transvections (which are di□erential operators) collapses. In this context, we wanted to test the e□ectiveness of an alternative method following [4] and [9]. The idea is to consider the algebra of covariants of n-points of P^1 under the action of $\mathsf{GL}_2(k)$ (cf. Definition 1.1). The main advantage of this algebra is that it admits a generating system of covariants which are explicit and *independent* of the characteristic. The covariants for the binary forms are then obtained as the subalgebra symmetrised by S_n, the symmetric group.

2010 ***Mathematics Subject Classification.*** — 13A50, 14H45.
Key words and phrases. — Positive and small characteristic, syzygies, generating system of covariants, separating system of covariants.

Although attractive in theory, our current implementation is extremely limited. Indeed the computation of the action of the group S_n, in the modular case (i.e when the characteristic divides the order of the group), under the covariants of n points fails with generic algorithms of Magma as soon as $n = 6$ (cf. [10, Sec. 5.2.6]). However, this method was used to determine a separating set (a weaker condition than being a generating system, see Definition 1.10) in the characteristic 3 binary quartic case. Along the way, we realized that some of the invariants/covariants appearing in small characteristic could be derived from classical covariants by a new easy differential operation (cf. Section 2.2) under certain conditions that we clarify. For octavics, we get the new invariant of degree 1 found by [1] and new covariants in degree 4 and 6 (cf. page 96). This operation, while it enriches the algebra of covariants obtained by reduction of those in characteristic zero, is not sufficient to get all the covariants (as we will see in an example in degree 4 at the end of this paper). The question of efficient generation in small characteristic remains wide open.

Notation. — Let p be a prime number or 0, k be an algebraically closed field of characteristic p and C_n the algebra of binary covariants defined over k.

1. A strategy to construct covariants in small characteristic

Except for quartics (cf. [1, Sec. 2.10.2]) and Igusa invariants for sextics, we do not know a generating system of invariants in every characteristic. Thanks to clever reductions and many computations, Basson exhibited in his thesis a "separating" system[1]. He conjectures that it is generator in characteristic 3 and 7 for octavics. For characteristic $p \geq 11$, generating systems are known thanks to the results of [8]. To get new results for covariants, we will establish a totally different computation method following [4] and [9]. We obtain new results for covariants of binary quartics in characteristic 3.

1.1. Strategy. — The study of covariants of n-points of $\mathrm{P}^1(k)$ under the action of $\mathrm{GL}_2(k)$ is a classical framework and we recall here the principal results. The main advantage of this work is that there exists an explicit generating system of covariants *independent* of the characteristic. Then the covariants for binary forms come from the subalgebra symmetrised by S_n.
We slightly modify the results of Sturmfels [9, Chap 3. Sec. 6] in order to be valid in every characteristic. In the case of invariants, this is exactly Geyer's method [4]. Let $n > 1$ be a positive integer. Consider the binary form:

$$\begin{aligned} f(x,z) &= \sum_{k=0}^{n} a_k x^k z^{n-k} \\ &= (\mu_1 x - \nu_1 z)(\mu_2 x - \nu_2 z)\dots(\mu_n x - \nu_n z). \end{aligned}$$

The "roots" (μ_i, ν_i) can be seen as points (μ_i, ν_i) P^1.

Definition 1.1. — Let M be a monomial in $k[\mu_1, \nu_1, \mu_2, \nu_2, \dots, \mu_n, \nu_n, x, z]$ such that:

$$M = \mu_1^{u_1}\mu_2^{u_2}\cdots\mu_n^{u_n}\nu_1^{v_1}\nu_2^{v_2}\cdots\nu_n^{v_n}x^{w_1}z^{w_2}$$

and P be a polynomial in $k[\mu_1, \nu_1, \mu_2, \nu_2, \dots, \mu_n, \nu_n, x, z]$. We say that:

[1] i.e. separating the orbits (cf. Definition 1.10)

– M is *regular of degree* d if $u_1 + v_1 = u_2 + v_2 = \cdots = u_n + v_n = d$. The integer d is called the *regularity degree* of M.

– P is *regular of degree* d if all of its monomials are regular of degree d. When P is regular for a degree d, we say that P is *regular*.

– P is *symmetric* if, for all permutation $\sigma \quad S_n$:

$$P(\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n, x, z) = P(\mu_{\sigma(1)}, \nu_{\sigma(1)}, \mu_{\sigma(2)}, \nu_{\sigma(2)}, \ldots, \mu_{\sigma(n)}, \nu_{\sigma(n)}, x, z).$$

A regular monomial is *reducible* if it can be expressed as the product of two regular monomials of regularity degree greater than or equal to 1.

We define the action of $\mathrm{GL}_2(k)$ on $k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n, x, z]$ in the following way: let $M \quad \mathrm{GL}_2(k)$,

$$\begin{pmatrix} \nu_i \\ \mu_i \end{pmatrix} \to \begin{pmatrix} \overline{\nu}_i \\ \overline{\mu}_i \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} \nu_i \\ \mu_i \end{pmatrix}$$
$$\begin{pmatrix} x \\ z \end{pmatrix} \to \begin{pmatrix} \overline{x}_i \\ \overline{z}_i \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} x \\ z \end{pmatrix}.$$

A regular polynomial P is a *covariant (of n points)* if there exists $w \quad \mathbb{Z}$ such that:

$$P(\overline{\mu}_1, \overline{\nu}_1, \overline{\mu}_2, \overline{\nu}_2, \ldots, \overline{\mu}_n, \overline{\nu}_n, \overline{x}, \overline{z}) = \det(M)^w P(\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n, x, z).$$

The polynomial P is called an *invariant (of n points)* if it does not depend on x and z. It is easy to define covariants quantities thanks to the brackets. Let $1 \leq i < j \leq n$, we call *bracket* the following quantities:

$$[ij] := \mu_i \nu_j - \nu_i \mu_j,$$
$$[iu] := \mu_i x - \nu_i z.$$

The subring $B(n)$ generated by these brackets in $k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n, x, z]$ is called *the bracket ring*. We also denote $B_{reg}(n)$ the subring of $B(n)$ of polynomials in the brackets which are regular of degree d for $d \geq 0$. The latter is generated by the monomials of the form:

$$\prod_{i<j} [ij]^{m_{ij}},$$

where the integers m_{ij} verify $d = \sum_{j=1}^{i-1} m_{ji} + \sum_{j=i+1}^{n+1} m_{ij}$ (the value $j = n + 1$ represents a bracket $[iu]$). The polynomial ring of regular covariants is equal to $B_{reg}(n)$ (consequence of the first fundamental theorem, cf. [11]). When the acting group is $\mathrm{GL}_2(\mathbb{C})$, Theorem 3.2.1 and Lemma 3.6.5 of [9] provide a demonstration. When the group is arbitrary, the proof is in [2]. Note also that [4, Satz 5] gives an elementary proof in the case of $\mathrm{GL}_2(k)$.
In Section 1.2, we present an example of computation of generators of $B_{reg}(n)$. What remains to describe is the final stage to get the of binary forms. Let:

$$\Psi : k[a_0, a_1, \ldots, a_n, x, z] \to k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n, x, z]$$
$$a_{n-k} \to (-1)^n \mu_1 \cdots \mu_n \cdot \sigma_k \left(\frac{\nu_1}{\mu_1}, \ldots, \frac{\nu_n}{\mu_n} \right).$$

Here σ_k represents the k-th elementary symmetric polynomial function in n variables. The following theorem (from [9, Th. 3.6.6]) is an elementary consequence of the previous theorem. Let $B_{reg}(n)^{S_n}$ be the subring of $B_{reg}(n)$ of polynomials in the brackets which are symmetric.

Theorem 1.2. — *The mapping* Ψ *is an isomorphism between the ring* C_n *of covariants of binary forms on* $k[a_0, \ldots, a_n, x, z]$ *and the subring* $B_{reg}(n)^{S_n}$ *of symmetric and regular polynomial brackets functions of* $k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n, x, z]$. *If* $C(a_0, \ldots, a_n)$ *is a covariant of degree* d *and order* r *then* $\Psi(C)$ *is a symmetric polynomial bracket function such that:*

1. *in every monomial of* $\Psi(C)$, *the index* 1, 2, ..., n *appears* d *times,*

2. *in every monomial of* $\Psi(C)$, *the letter* u *appears* r *times.*

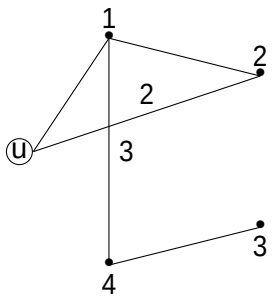
1.2. Computation of $B_{reg}(n)$. — In order to have a clearer view of a generating system of $B_{reg}(n)$, the monomials will be represented by weighted graphs such that the vertices form a regular polygon. We represent:

– a monomial of $B(n)$ by a graph with n vertices numbered from 1 to n and a vertex called ⓤ,

– the bracket $[ij]$ by an edge connecting the vertex i to the vertex j with $i < j \quad \{1, \ldots, n\}$,

– the bracket $[iu]$ by an edge connecting the vertex ⓤ to the vertex i.

For example, the bracket product $[12][14]^3[34][1u][2u]^2 \quad B(4)$ is represented by the following weighted graph:



Previous comments allow us to formulate five remarks which are very useful to construct a generating system for $B_{reg}(n)$. The next point follows from the definition of $B_{reg}(n)$.

Point 1.3. — *Every regular monomial of order* m *and of regularity degree* d *is represented by a graph with* m *connexions with* ⓤ *and every numbered vertex has a valence* d.

Moreover, by Kempe's lemma ([9, Th. 3.7.3 p. 132]), the covariant algebra of n points is generated by elements of regularity degree at most 2. Also, by [6, Th. 2.3, p. 7], the invariants of n points are generated by the regularity degree 1, hence the following point:

Point 1.4. — *The numbered vertices have a valence at most* 2. *The graph corresponding to invariants has a valence* 1.

By its definition, if a graph is expressed as a union of subgraphs corresponding to graphs of smaller degree and smaller order already computed, the associated covariant is reducible.

Point 1.5. — *The graphs having a subgraph already calculated are excluded.*

Proposition 1.6. — *Let* $1 \leq i < j < k < l \leq n$*, we have:*

$$[ik][jl] = [ij][kl] + [il][jk],$$

$$[ik][ju] = [ij][ku] + [iu][jk].$$

These relations are called the syzygies*.*

When the vertices are in a regular polygon, Proposition 1.6 causes the following point (see [7, Th. 6.2 p. 73] for a proof):

Point 1.7. — *The graphs of our generating system have no edges crossing.*

Thanks to Point 1.4, the number of adjacent edges of ⓤ is bounded. Moreover, when n is even, Point 1.3 imposes another condition on the edges adjacent to ⓤ.

Point 1.8. — *The vertex* ⓤ *has at most* $2n$ *adjacent edges. When* n *is even,* ⓤ *has an even number of adjacent edges.*

Example 1.9. — Using the five points above and considering increasing orders, we get the following generators of $B_{reg}(n)$ when $n = 4$, called t_0, t_1, u_0, u_1, u_2 and f.

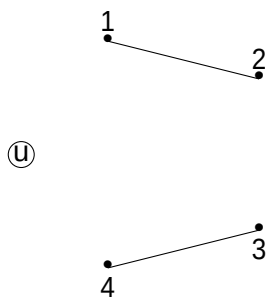


FIGURE 1. t_0

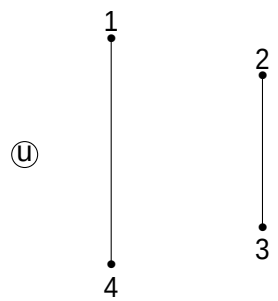


FIGURE 2. t_1

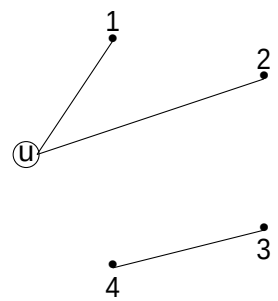


FIGURE 3. u_0

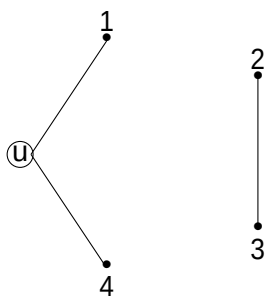


FIGURE 4. u_1

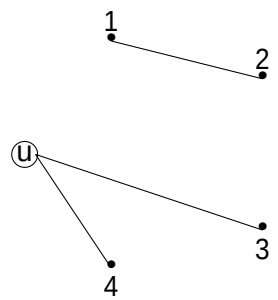


FIGURE 5. u_2

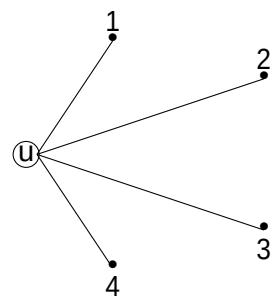


FIGURE 6. f

1.3. Symmetrization. — We wish to compute C_n as $B_{reg}(n)^{S_n}$. If $b_1, \dots, b_t$ is a generating system of bracket monomials for $B_{reg}(n)$, then we have a surjective morphism:

$$\begin{array}{ccc} k[x_1, \dots, x_t] & \to & B_{reg}(n). \\ x_i & \to & b_i \end{array}$$

The kernel I of this morphism is obviously generated by the syzygies which are pulled back by this morphism. The action of S_n on the b_i induces a representation G_n of S_n in $\mathrm{GL}_t(k)$. There are algorithms for computing $k[x_1, \dots, x_t]^{G_n} = R_n$ (cf. [3]). They are also valid in the modular case (i.e when $p \mid |G_n|$), we use them "naively" through their `Magma` implementations. However this process generates a limitation when $n \geq 6$. What remains to clarify is the link between R_n and C_n.
When p does not divide $|S_n|$, S_n is a linearly reductive group (cf. [3, Def. 2.2.1]) and the existence of Reynolds operators (cf. [3, Th. 2.2.5]) preserves the surjectivity of the morphism $k[x_1, \dots, x_t] \to B_{reg}(n)$ in the symmetrization process. Thanks to [9, Lem. 3.7.2], the image of a generating system of R_n by the canonical surjection $k[x_1, \dots, x_t] \to k[x_1, \dots, x_t]/I = B_{reg}(n)$ is a generating system of $C_n = B_{reg}(n)^{S_n}$. In particular, if $p > n$, we get a generalization of the result of Geyer: the covariant ring C_n is the reduction modulo p of the covariant ring in characteristic 0. In particular, the bigraduate Poincaré series are identical.
When $p \mid |S_n|$, S_n is only a reductive group (cf. [3, Sec. 2.2.2]) and the previous result is no longer valid in the general case. To overcome this, we recall the following concept:

Definition 1.10. — Let X be an affine variety and G an automorphism group of $k[X]$. A subset $S \quad k[X]^G$ is called *separating* if, for every pair of points (x, y) of X, we have the following property: if there exists an element $f \quad k[X]^G$ such that $f(x) = f(y)$, there exists an element g in S such that $g(x) = g(y)$.

The relation with the invariant ring is the following (cf. [3, Prop. 2.3.10]):

Proposition 1.11. — *Suppose that X is irreducible and $k[X]^G$ is finitely generated. Let $A \quad k[X]^G$ be a finitely generated and separating subalgebra. Then* $\mathrm{Frac}(k[X]^G)$ *is a purely inseparable finite extension of* $\mathrm{Frac}(A)$*. In particular, if the characteristic of k is zero then:*

$$\mathrm{Frac}(A) = \mathrm{Frac}(k[X]^G).$$

Definition 1.10 has the advantage to preserve the surjectivity on transition to invariants. Let G be a linear algebraic group. Thanks to [3, p. 59], if G is reductive, G acts regularly on an affine variety X and $Y \quad X$ is a G-stable subvariety, then the restriction map $k[X] \to k[Y]$ sends a separating subset of $k[X]^G$ to a separating subset of $k[Y]^G$. So with $G = G_n$ (see the beginning of this section), R_n is generated by separating system of C_n but we do not necessarily have an equality between R_n and C_n (we only have $R_n \quad C_n$). We will see, in the following case of quartics in characteristic 3, when the inclusion is strict.

Example 1.12. — In Example 1.9, we have seen that the covariant algebra of 4 points is generated by t_0, t_1, u_0, u_1, u_2 and f. We will make the group S_4 act and, using the function `InvariantRing` of `Magma`, we will compute a separating system of the covariant algebra C_4. Knowing that S_4 is generated by $\sigma = (1234)$ and $\tau = (12)$, the action of S_4 on t_0, t_1, u_0, u_1,

u_2 and f is given by the following equalities:

$$\begin{array}{lll} t_0^\tau = -t_0 & \text{and} & t_0^\sigma = -t_1, \\ t_1^\tau = t_1 + t_0 & \text{and} & t_1^\sigma = -t_0, \\ u_0^\tau = u_0 & \text{and} & u_0^\sigma = -(u_0 + u_1 + u_2), \\ u_1^\tau = u_1 + u_2 & \text{and} & u_1^\sigma = u_0, \\ u_2^\tau = -u_2 & \text{and} & u_2^\sigma = u_1, \\ f^\tau = f & \text{and} & f^\sigma = f. \end{array}$$

Using the `Magma` code of Appendix 2.2, we get the following generating system of covariants in characteristic 0 which is also generating in characteristic ≥ 5:

$$\begin{aligned} c_{0,2} &= -3a_1a_3 + a_2^2 + 12a_4a_0, \\ c_{0,3} &= -27/2a_1^2a_4 + 9/2a_1a_2a_3 - a_2^3 + 36a_2a_4a_0 - 27/2a_3^2a_0, \\ c_{4,1} &= a_0z^4 + a_1xz^3 + a_2x^2z^2 + a_3x^3z + a_4x^4, \\ c_{4,2} &= (a_1^2 - 8/3a_2a_0)z^4 + (4/3a_1a_2 - 8a_3a_0)xz^3 + (4/3a_2^2 - 2a_1a_3 - 16a_4a_0)x^2z^2 \\ &\quad + (4/3a_2a_3 - 8a_1a_4)x^3z + (a_3^2 - 8/3a_2a_4)x^4, \\ c_{6,3} &= (a_1^3 - 4a_1a_0a_2 + 8a_0a_3)z^6 + (2a_1^2a_2 + 4a_0a_1a_3 - 8a_0a_2^2 + 32a_0^2a_4)xz^5 \\ &\quad + (5a_1^2a_3 + 40a_0a_1a_4 - 20a_0a_2a_3)x^2z^4 + (20a_1^2a_4 - 20a_0a_3^2)x^3z^3 \\ &\quad + (20a_1a_2a_4 - 5a_1a_3^2 - 40a_0a_3a_4)x^4z^2 + (8a_2^2a_4 - 4a_1a_3a_4 - 2a_2a_3^2 - 32a_0a_4^2)x^5z \\ &\quad + (4a_2a_3a_4 - 8a_1a_4^2 - a_3^3)x^6. \end{aligned}$$

We recover the classic covariants of characteristic zero.
We apply the same process in characteristic 3 (we change `FF:= Rationals();` in the `Magma` code by `FF:= GF(3);`) and we get

$$\begin{aligned} c_{0,1} &= a_2, \\ c_{0,6} &= a_0^3a_4^3 + a_0^2a_2^2a_4^2 + a_0a_1a_2^2a_3a_4 + a_0a_2^4a_4 + 2a_0a_2^3a_3^2 + 2a_1^3a_3^3 + 2a_1^2a_2^3a_4 + a_1^2a_2^2a_3^2, \\ c_{4,1} &= a_0z^4 + a_1xz^3 + a_2x^2z^2 + a_3x^3z + a_4x^4, \\ c_{4,4} &= a_2c_{4,3}, \\ c_{6,3} &= (2a_0^2a_3 + 2a_0a_1a_2 + a_1^3) + (2a_0^2a_4 + a_0a_1a_3 + a_0a_2^2 + 2a_1^2a_2)x \\ &\quad + (a_0a_1a_4 + a_0a_2a_3 + 2a_1^2a_3)x^2 + (a_0a_3^2 + 2a_1^2a_4)x^3 + (2a_0a_3a_4 + 2a_1a_2a_4 + a_1a_3^2)x^4 \\ &\quad + (a_0a_4^2 + 2a_1a_3a_4 + 2a_2^2a_4 + a_2a_3^2)x^5 + (a_1a_4^2 + a_2a_3a_4 + 2a_3^3)x^6, \\ c_{8,4} &= c_{4,1}(c_{4,3} - a_2^2c_{4,1}), \\ c_{8,6} &= (c_{4,3} - a_2^2c_{4,1})c_{4,3} \end{aligned}$$

where

$$\begin{aligned} c_{4,3} &= (a_0a_4^2 + 2a_1a_3a_4 + 2a_2^2a_4 + a_2a_3^2)x^4 + (a_0a_3a_4 + a_1a_2a_4 + 2a_1a_3^2)x^3z \\ &\quad + (a_0a_1a_4 + a_0a_2a_3 + 2a_1^2a_3)xz^3 + (a_0^2a_4 + 2a_0a_1a_3 + 2a_0a_2^2 + a_1^2a_2)z^4. \end{aligned}$$

The quantity $c_{4,3}$ is a covariant of degree 3 and order 4 in characteristic 3. This system does not generate the algebra of covariants because we cannot find $c_{4,3}$ as polynomial in the $c_{2i,j}$. This case provides an example of a separating subset which is not a generating system of the

covariant algebra. We point out that $\{c_{0,1}, c_{0,6}, c_{4,1}, c_{4,3}, c_{6,3}\}$ is a separating system of C_4 and one wonders if it is also a generating system. Theorem [3, Th. 2.3.12] would in theory lead to an algorithm to test this hypothesis but the algorithm is not efficient enough to run in practice.

2. A new way to generate covariants in small characteristic

Here we introduce a new way to build covariants in small characteristic. To show the validity of our approach, our first idea was to use the differential characterization of covariants, as in [5, p. 43]. It turns out however that the result of Hilbert (Theorem 2.1), originally shown in characteristic 0, admits counterexamples in small characteristic, as discussed in Section 2.1. So we approach the proof of Theorem 2.3 directly. First we recall the result of Hilbert and then we give our proof. In the following, f is a binary form defined over the field k :

$$f = \sum_{i=0}^{n} a_i x^i z^{n-i}.$$

2.1. Hilbert's differential characterization of covariants. — Let :

- $k[a_0, \ldots, a_n]_d$ be the homogeneous polynomial algebra of degree d,
- T be the subgroup of diagonal matrices of $\mathrm{SL}_2(k)$,
- Γ be the subgroup of upper triangular matrices and diagonal equal to 1 of $\mathrm{SL}_2(k)$,
- Γ' be the subgroup of lower triangular matrices and diagonal equal to 1 of $\mathrm{SL}_2(k)$.

These three subgroups are important because they generate $\mathrm{SL}_2(k)$ and thus permit to break down the issues of invariance under the action of these groups. Let $M = a_0^{\rho_0} a_1^{\rho_1} \ldots a_n^{\rho_n}$ be a monomial of $k[a_0, \ldots, a_n]$. We define the *weight* of M by $w = \sum_{i=0}^{n} i\rho_i$. We say that a non zero element I of $k[a_0, \ldots, a_n]$ is *isobaric* if all of its monomials have the same weight. We define two differential operators on I that preserve the degree. The operators $\mathbf{\Delta}$ and $\mathbf{D}$ are given by:

$$\mathbf{\Delta} = \sum_{i=1}^{n} i a_i \frac{\partial}{\partial a_{i-1}},$$
$$\mathbf{D} = \sum_{i=0}^{n-1} (n-i) a_i \frac{\partial}{\partial a_{i+1}}.$$

Theorem 2.1. — *Suppose $p = 0$ or $p > nd + m$. The polynomial $C = \sum_{i=0}^{m} C_i x^i z^{m-i}$ is a covariant of the binary form f under the action of $\mathrm{SL}_2(k)$ if and only if the following conditions are satisfied:*

1. *$C_0, \ldots, C_m$ are homogeneous functions of degree d and isobaric of weight $w, w+1, \ldots, w+m$ with $nd - 2w = m$,*
2. *$\boldsymbol{D}C = x\frac{\partial C}{\partial z}$,*

3. $\mathbf{\Delta}C = z\frac{\partial C}{\partial x}$.

This result is not available in every characteristic. Let $f = \sum_{i=0}^{16} a_i x^i z^{16-i}$ be a binary form of degree $n = 16$ in characteristic 3. Note $C = a_{11}x^6$ a homogeneous polynomial of degree $m = 6$. The polynomial C is not a covariant of f because for $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\mathrm{SL}_2(k)$ we have

$$C(M.f, M.(x,z)) = (x + 2z)^6(a_{11} + a_{14}) = C.$$

Nonetheless

1. $C_0, \ldots, C_m$ are homogeneous functions of degree $d = 1$ and isobaric of weight $w = 5, 6, \ldots, 11$ with $nd - 2w = 16 \cdot 1 - 2 \cdot 5 = 6 = m$,
2. $\mathbf{D}C = 6a_{10}x^6 = 0 = x\frac{\partial C}{\partial z}$,
3. $\mathbf{\Delta}C = 12a_6x^6 = 0 = z\frac{\partial C}{\partial x}$.

Hence, Hilbert's theorem cannot be used to prove our next result. However we will revise some elements of the proof using the three subgroups Γ, Γ and T.

2.2. A new way to build covariants in positive characteristic. — Before showing our theorem, we set some notations. Let M $\mathrm{SL}_2(k)$. We have

$$f(M.(x,z)) = \sum_{i=0}^{n} a_i x^i z^{n-i}.$$

In the following, we note $X = (x,z)$, $X = M^{-1}(x,z)$, $a = (a_0, \ldots, a_n)$ and $a = (a_0, \ldots, a_n)$. We start with a lemma.

Lemma 2.2. — *An homogenous polynomial* C $k[a_0, \ldots, a_n]_d[x,z]$ *is a covariant under the action of* T *if and only if the* C_i *are isobaric of weight* $w + i$ *and* $nd - 2w = m$.

Proof. — Write

$$C = \sum_{i=0}^{m} C_i x^i z^{m-i}.$$

If $M = \left(\begin{smallmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ T, then $a_i = \lambda^{n-2i} a_i$ and $C_l(a) = \sum_{i=1}^{l} \prod_{j=0}^{n} {a_j}^{\epsilon_{i,j,l}}$ (resp. $C_l(a) = \sum_{i=1}^{l} \prod_{j=0}^{n} {a_j}^{\epsilon_{i,j,l}}$) with l $\{0, \ldots, m\}$ and $\epsilon_{i,j,l}$ N. We have

$$C_l(a) = \sum_{i=1}^{l} \prod_{j=0}^{n} \lambda^{(n-2j)\epsilon_{i,j,l}} {a_j}^{\epsilon_{i,j,l}} = \sum_{i=1}^{l} \lambda^{\sum_{j=0}^{n}(n-2j)\epsilon_{i,j,l}} \prod_{j=0}^{n} {a_j}^{\epsilon_{i,j,l}}$$
$$= \sum_{i=1}^{l} \lambda^{nd - 2\sum_{j=0}^{n} j\epsilon_{i,j,l}} \prod_{j=0}^{n} {a_j}^{\epsilon_{i,j,l}}.$$

Since M also acts on (x,z) by $M^{-1}.(x,z)$, we get

$$M.C(a,X) = C(a_0, \ldots, a_n, \lambda x, \lambda^{-1} z) = \sum_{l=0}^{m} \lambda^{2l-m} C_l(a) x^l z^{m-l}.$$

Suppose that C is a covariant. — Then $M.C = C$, so for all $l \quad \{0, \dots, m\}$

$$C_l(a) = \lambda^{2l-m} C_l(a\,).$$

This implies that for all l and for all i

$$nd - 2\sum_{j=0}^{n} j\epsilon_{i,j,l} + 2l - m = 0.$$

In particular, $\sum_{j=0}^{n} j\epsilon_{i,j,l} - l$ does not depend on the l or i. So, we can define w by putting $w = \sum_{j=0}^{n} j\epsilon_{i,j,l} - l$. We get then $nd - 2w = m$. Moreover, the integer w is the weight of C_0. The weight of C_l is $\sum_{j=0}^{n} j\epsilon_{i,j,l} = w + l$.

Conversely we want to prove that $C_l(a) = \lambda^{2l-m} C_l(a\,)$. — Since the weight of C_l is $\sum_{j=0}^{n} j\epsilon_{i,j,l}$, we have $w = \sum_{j=0}^{n} j\epsilon_{i,j,l} - l$. Moreover, $nd - 2w = m$, hence :

$$nd - 2\sum_{j=0}^{n} j\epsilon_{i,j,l} + 2l - m = 0.$$

This implies that:

$$C_l(a) = \lambda^{2l-m} C_l(a\,).$$

So, C is a covariant under the action of T.

Since, starting from C_0, we get the weight of C_i of the covariant C, we can say that w is the weight of C.

Theorem 2.3. — *Let $Q = \sum_{i=0}^{m_0} Q_i x^i z^{m_0-i}$ be a covariant of f of order m_0, degree d_0 and weight ω_0. Let l be an integer smaller than $m_0/2$ and p. The polynomial*

$$C = \frac{1}{z^l}\frac{\partial^l Q}{\partial x^l}$$

is a covariant of f if and only if $m_0 - l + 1$ is congruent to 0 modulo p. When C is a non zero covariant, its order is $m_0 - 2l$ and its degree is d_0.

Remark 2.4. — The operator was already known by Hilbert (cf. [5, Th. p. 103]). But the way to use it in small characteristic with the previous condition is new.

To show that C is a covariant under the action of $\mathrm{SL}_2(k)$, we consider the action of T, Γ and Γ . First we analyse the action of this three subgroups on C and then we give the proof of Theorem 2.3. Write again

$$C = \sum_{i=0}^{m} C_i x^i z^{m-i}.$$

Lemma 2.5 **(Action of T.)** — *C is covariant under the action of* T *if and only if* $p \mid (m_0 - l + 1)$.

Proof. — By definition of C, the polynomials $C_0, \dots, C_m$ are homogeneous functions of degree d_0 and isobaric of weight $l + \omega_0, l + \omega_0 + 1, \dots, l + \omega_0 + m$. We express C according to the coe□cients of Q

$$C = \sum_{i=l}^{m_0} \frac{i!}{l!} Q_i x^{i-l} z^{m_0-i-l}.$$

If $p \mid (m_0 - l + 1)$, then for all $i \quad \{m_0 - l + 1, \ldots, m_0\}$,

$$p \mid \frac{i!}{l!}.$$

In this case, if C is non zero, C is a homogeneous polynomial of degree $m = m_0 - 2l$. Moreover, Q being a covariant, Lemma 2.2 ensures that $m_0 = nd_0 - 2w_0$. The order of C can be written $m = nd_0 - 2(\omega_0 + l)$. So, by Lemma 2.2, C is a covariant under the action of T. The converse is also given by Lemma 2.2. The condition $p \mid (m_0 - l + 1)$ is then a necessary and su□cient condition for C to be a covariant under the action of T.

Lemma 2.6 **(Action of Γ).** — *C is covariant under the action of Γ.*

Proof. — We set $g : (a, X) \to (a\ , (x + \mu z, z))$, were $\mu \quad k$. We aim at showing that $C \circ g = C$, meaning that:

$$\left(\frac{1}{z^l}\frac{\partial^l Q}{\partial x^l}\right) \circ g = \frac{1}{z^l}\frac{\partial^l Q}{\partial x^l}.$$

This is equivalent to

$$\frac{\partial^l Q}{\partial x^l} \circ g = \frac{\partial^l Q}{\partial x^l}.$$

However, Q being a covariant under the action of Γ, we have

$$\frac{\partial Q}{\partial x} = \frac{\partial Q \circ g}{\partial x}.$$

Moreover,

$$\frac{\partial Q \circ g}{\partial x} = \frac{\partial Q}{\partial x} \circ g.$$

By immediate induction, we obtain the desired result. So, C is covariant under the action of Γ.

Lemma 2.7 **(Action of Γ).** — *If $p \mid (m_0 - l + 1)$ then C is invariant under the action of Γ .*

We set $g : (a, X) \to (a\ , (x, \mu x + z))$, where $\mu \quad k$. We want to prove that $C \circ g = C$, meaning that:

$$\left(\frac{1}{z^l}\frac{\partial^l Q}{\partial x^l}\right) \circ g = \frac{1}{z^l}\frac{\partial^l Q}{\partial x^l}.$$

This is equivalent to

$$z^l \left(\frac{\partial^l Q}{\partial x^l}\right) \circ g = (\mu x + z)^l \frac{\partial^l Q}{\partial x^l}.$$

Using the fact that $\dfrac{\partial^l Q}{\partial x^l} \circ g = \displaystyle\sum_{i=0}^{l} \binom{l}{i} \cdot (-\mu)^{l-i} \cdot \frac{\partial^l Q}{\partial x^i \partial^{l-i} z}$, this amounts to show

$$z^l \sum_{i=0}^{l} \binom{l}{i} \frac{\partial^l Q}{\partial x^i \partial z^{l-i}} (-\mu)^{l-i} = \sum_{i=0}^{l} \binom{l}{i} \frac{\partial^l Q}{\partial x^l} \mu^{l-i} x^{l-i} z^i.$$

This is still equivalent to

$$\sum_{i=0}^{l} \binom{l}{i} \mu^{l-i} \Big[\frac{\partial^l Q}{\partial x^l} x^{l-i} z^i + (-1)^{l-i+1} \frac{\partial^l Q}{\partial x^i \partial z^{l-i}} z^l\Big] = 0$$

i.e. for all $i \quad \{0, \dots, l\}$

$$\frac{\partial^l Q}{\partial x^l} x^{l-i} z^i + (-1)^{l-i+1} \frac{\partial^l Q}{\partial x^i \partial z^{l-i}} z^l = 0.$$

Proof of Lemma 2.7. — Assume that $p \mid (m_0 - l + 1)$. We develop the left-hand side of the expression and we get

$$0 = \sum_{j=l}^{m_0} Q_j j(j-1)\dots(j-l+1) x^{j-i} z^{m_0+i-j} + (-1)^{l-i+1} \sum_{j=i}^{m_0-l+i} Q_j j(j-1)\dots(j-i+1) x^{j-i} (m_0-j)(m_0-j-1)\dots \dots(m_0-j-l+i+1) z^{m_0-j+i}.$$

For all $j \quad \{m_0 - l, \dots, m\}$, p divides $j(j-1)\dots(j-l+1)$. In the same way, for all $j \quad \{m_0 - l, \dots, m_0 - l + i\}$, p divides $j(j-1)\dots(j-i+1)$. So the sums shall stop at $m_0 - l$. For all $j \quad \{i, \dots, l-1\}$, p divides $(m_0-j)(m_0-j-1)\dots(m_0-j-l+i+1)$. Therefore the two sums begin at l. Finally, since p divides $(m_0 - l + 1)$, we have

$$(m_0-j)(m_0-j-1)\dots(m_0-j-l+i+1) \equiv (l-1-j)(l-2-j)\dots(-j+i) \equiv (-1)^{l-i}(j-i)\dots(j-l+1) \pmod{p}.$$

This proves the vanishing of the expression. So it has been shown that if $p \mid (m_0 - l + 1)$ then C is invariant under the action of Γ'.

Proof of Theorem 2.3. — According to Lemma 2.5 (Action of T), C is a covariant under the action of T if and only if $p \mid (m_0 - l + 1)$. According to Lemma 2.6 (Action of Γ), C is a covariant under the action of Γ. According to Lemma 2.7 (Action of Γ'), if $p \mid (m_0 - l + 1)$ then C is a covariant under the action of Γ'. Since $\mathrm{SL}_2(k)$ is generated by T, Γ and Γ', if $p \mid (m_0 - l + 1)$ then C is a covariant under the action of $\mathrm{SL}_2(k)$.
Conversely, assume that C is a covariant under the action of $\mathrm{SL}_2(k)$. The invariance under the action of T (Lemma 2.5) shows that $p \mid (m_0 - l + 1)$.
Finally C is a covariant under the action of $\mathrm{SL}_2(k)$ if and only if $p \mid (m_0 - l + 1)$.

Thanks to this theorem, we can construct new covariants which do not appear in characteristic zero.

- For binary quartics in characteristic 3 (cf. Example 1.12), we find $c_{0,1}$ ($Q = f$ and $l = 2$) and $c_{4,3}$ ($Q = c_{6,3}$ and $l = 1$) ;
- For binary sextics in characteristic 3 (cf. [10, Sec. 5.2.6]), we find the covariant q ($Q = f$ and $l = 1$) of degree 1 and order 4 ;
- For binary sextics in characteristic 5 (cf. [10, Sec. 5.2.6] and [10, Sec. 6.6.2.3]), we find the covariant c ($Q = f$ and $l = 2$) of degree 1 and order 2 ;
- For binary octavics in characteristic 5, we find the same invariants, $C = a_4$ ($Q = f$ and $l = 4$) of degree 1 identified by Basson and Lercier.

It is tempting to wonder whether it is possible, in small characteristic, to get a generating system of covariants by adding this new operation. A first difficulty is the following. Let $Q_1, \dots, Q_r$ be covariants, $l_1, \dots, l_r$ be integers such that

$$C_i = \frac{1}{z^{l_i}} \frac{\partial^{l_i} Q_i}{\partial x^{l_i}}$$

are the covariants obtained by this new operation starting from Q_i. Let Q be an element of $k[Q_1, \dots, Q_r, C_1, \dots, C_r]$. The expression $\frac{1}{z^l} \frac{\partial^l Q}{\partial x^l}$ is not necessarily in $k[Q_1, \dots, Q_r, C_1, \dots, C_r]$. For instance, over $k = \mathbb{F}_5$, for $r = 1$ consider only the sextic binary form $Q_1 = f$. The covariant of f

$$\frac{1}{z^3} \frac{\partial^3 f^2}{\partial x^3} = (a_3a_6 + a_4a_5)x^6 + (4a_2a_6 + 4a_3a_5 + 2a_4^2)x^5z + (a_0a_4 + a_1a_3 + 3a_2^2)xz^5 + (4a_0a_3 + 4a_1a_2)z^6$$

is not in the algebra generated by f and $C_1 = \frac{1}{z^2} \frac{\partial^2 f}{\partial x^2}$. Indeed, if it was in this algebra, it would be a linear combination of f^2, fC_1 and C_1^2 since these are the only terms of degree 2 in a_i. However the terms that do not depend on x in these three covariants are a_0^2, $2a_0a_2$ and $4a_2^2$. We cannot generate the coefficient $(4a_0a_3 + 4a_1a_2)$. So, it is difficult to see when the new operation will saturate the algebra. Actually we even have an example where it does not. Consider the invariant $c_{0,6}$ I_4 in characteristic 3 of Example 1.12. It cannot be obtained using our new operator. To get it by our operation, it would have to be the l-th derivative starting from a certain covariant of order m and degree 6. The integers m and l have to verify $l < m/2$, $m - 2l = 0$ and $m - l + 1$ is a multiple of 3. So we get this invariant by taking the second derivative of a certain covariant $c_{4,6}$ of order 4 and degree 6. However by performing the computations, we find that the algebra of covariant of degree less than 6 generated by our operator on the reduction of covariants of characteristic zero is generated by $c_{0,1}$, $f = c_{4,1}$, $c_{4,3}$ and $c_{6,3}$. The only two options for $c_{4,6}$ are $c_{0,1}^5 c_{4,1}$ and $c_{0,1}^3 c_{4,3}$. These two options do not give $c_{0,6}$.

Acknowledgement. — It is a pleasure to thank Christelle Klein Scholz for her proofreading.

Appendix

```
symmetrisation:=function(C,P4)
P:=Parent(C);
F:=BaseRing(P);
r:=Rank(P);
P2:=PolynomialRing(F,r-1);
P3:=PolynomialRing(F,r-1);
f:=hom<P -> P2 | [P2.i : i in [1..r-1]] cat [1]>;
x:=P.r;
L:=f(Coefficients(C,x));
L2:=[];
for s in L do
b,t:=IsSymmetric(s,P3);
if b then
```

```
L2:=L2 cat [t];
else
return "not symmetric";
end if;
end for;
f2:=hom< P3 -> P4 | [P4.i : i in [1..r-1]]>;
return &+[f2(L2[i])*(-P4.r)^(i-1) : i in [1..#L2]];
end function;

FF:= Rationals();
// FF:= GF(3);
A<x1,x2,x3,x4,x>:= PolynomialRing(FF,5);
// Order 0
t0 := (x2-x1)*(x4-x3);
t1 := (x4-x1)*(x3-x2);
//Order 2
u0 := (x-x1)*(x-x2)*(x4-x3);
u1 := (x-x1)*(x-x4)*(x3-x2);
u2 := (x-x3)*(x-x4)*(x2-x1);
//Order 4
f := (x-x1)*(x-x2)*(x-x3)*(x-x4);
M1:= Matrix(FF,[
[0,-1,0,0,0,0],
[-1,0,0,0,0,0],
[0,0,-1,-1,-1,0],
[0,0,1,0,0,0],
[0,0,0,1,0,0],
[0,0,0,0,0,1]
]);
// representation of the action of the cycle (123456)

M2:=Matrix(FF,[
[-1,0,0,0,0,0],
[1,1,0,0,0,0],
[0,0,1,0,0,0],
[0,0,0,1,1,0],
[0,0,0,0,-1,0],
[0,0,0,0,0,1]
]);
// representation of the action of the cycle (12)

GT := MatrixGroup<6, FF| [M1,M2]>;
// Group generated by the matrices M1 and M2

R:=InvariantRing(GT);
// Invariant ring of the group G on a set of 6 points
```

```
F:=FundamentalInvariants(R);
// Invariants who generate the ring R

L:=[Evaluate(g,[t0,t1,u0,u1,u2,f]) : g in F];
L2:=MinimalAlgebraGenerators(L);
P4<a1,a2,a3,a4,z>:=PolynomialRing(FF,5);
L3:=[symmetrisation(C,P4) : C in L2];
// L3 is the list of elements of B_{reg,sym} expressed with the
// coefficients of ai f

[Factorization(C): C in L3];
```

References

[1] R. Basson, "Arithmétique des espaces de modules des courbes hyperelliptiques de genre 3 en caractéristique positive", PhD Thesis, Université de Rennes 1 (France), 2015, 187 pages.

[2] C. de Concini & C. Procesi, "A characteristic free approach to invariant theory", *Adv. Math.* **21** (1976), no. 3, p. 330-354.

[3] H. Derksen & G. Kemper, *Computational invariant theory*, Encyclopaedia of Mathematical Sciences, vol. 130, Springer, 2002, x+268 pages.

[4] W.-D. Geyer, "Invarianten binärer Formen", in *Classification of algebraic varieties and compact complex manifolds*, Lecture Notes in Math., vol. 412, Springer, 1974, p. 36-69.

[5] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, 1993, Translated from the German and with a preface by Reinhard C. Laubenbacher, Edited and with an introduction by Bernd Sturmfels, xiv+191 pages.

[6] B. Howard, J. Millson, A. Snowden & R. Vakil, "The equations for the moduli space of n points on the line", *Duke Math. J.* **146** (2009), no. 2, p. 175-226.

[7] J. P. S. Kung & G.-C. Rota, "The invariant theory of binary forms", *Bull. Am. Math. Soc.* **10** (1984), no. 1, p. 27-85.

[8] R. Lercier & C. Ritzenthaler, "Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects", *J. Algebra* **372** (2012), p. 595-636.

[9] B. Sturmfels, *Algorithms in invariant theory*, second ed., Texts and Monographs in Symbolic Computation, Springer, 2008, vi+197 pages.

[10] F. Ulpat Rovetta, "Étude algorithmique et arithmétique de courbes de petit genre", PhD Thesis, Aix Marseille Université (France), 2015, 199 pages.

[11] H. Weyl, *The Classical Groups. Their Invariants and Representations*, Princeton University Press, 1939, xii+302 pages.

Florent Ulpat Rovetta, Institut de Mathématiques de Marseille, UMR 6206 du CNRS, Luminy, Case 907, 13288 Marseille • *E-mail :* florent.rovetta@gmail.com