ALBANIAN JOURNAL OF MATHEMATICS
Volume 6, Number 1, Pages 3–8
ISSN: 1930-1235; (**2012**)

A NOTE ABOUT INVARIANTS OF ALGEBRAIC CURVES

Leonid Bedratyuk
Department of Applied Mathematics,
Khmelnitskiy National University,
Khmelnitskiy, Ukraine.
Email: *leonid.uk@gmail.com*
Webpage: *http://sites.google.com/site/bedratyuklp/*

Abstract. Let G be the group generated by the transformations $x = \alpha\tilde{x} + b, y = \tilde{y}, \alpha \neq 0, \alpha, b \in \mathbf{k}$, $\operatorname{char}\mathbf{k}$ of the affine plane $\mathbf{k}^2$. For affine algebraic plane curves of the form $y^n = f(x)$ we reduce a calculation of its G-invariants to calculation of the intersection of kernels of some locally nilpotent derivations. We compute a complete set of independent invariants and then reconstruct a curve from given values of these invariants.

1. Introduction

Consider an affine algebraic curve

$$C : F(x, y) = \sum_{i+j\leq d} a_{i,j}x^i y^j = 0, a_{i,j} \in \mathbf{k},$$

defined over field $\mathbf{k}$, $\operatorname{char}\mathbf{k} = 0$. Let $\mathbf{k}[C]$ and $\mathbf{k}(C)$ be the algebras of polynomial and rational functions of coefficients of the curve C. Those affine transformations of plane which preserve the algebraic form of equation $F(x, y)$ generate a group G which is a subgroup of the group of affine plane transformations. A function $\phi(a_{0,0}, a_{1,0}, \ldots, a_{d,0}) \in \mathbf{k}(C)$ is called G-invariant if $\phi(\tilde{a}_{0,0}, \tilde{a}_{1,0}, \ldots, \tilde{a}_{d,0}) = \phi(a_{0,0}, a_{1,0}, \ldots, a_{d,0})$ where $\tilde{a}_{0,0}$, $\tilde{a}_{1,0}, \ldots$, $\tilde{a}_{d,0}$ are defined from the condition

$$F(gx, gy) = \sum_{i+j\leq d} a_{i,j}(gx)^i(gy)^j = \sum_{i+j\leq d} \tilde{a}_{i,j}x^i y^j,$$

for all $g \in G$. The curves C and C' are said to be G-isomorphic if they lies on the same G-orbit.

2000 *Mathematics Subject Classification.* 14H99, 20F10, 30F10.
Key words and phrases. algebraic curves, automorphisms, invariants.

The algebras of all G-invariant polynomials and rational functions we denote by $\mathbf{k}[C]^G$ and by $\mathbf{k}(C)^G$, respectively. One way to find elements of the algebra $\mathbf{k}[C]^G$ is the specification of invariants of associated ternary form of order d. In fact, consider a vector space T_d generated by the ternary forms $\sum_{i+j\leq d} b_{i,j}x^{d-(i+j)}y^iz^j$, $b_{i,j} \in \mathbf{k}$ endowed with the natural action of the group $GL_3 := GL_3(\mathbf{k})$. Given GL_3-invariant function f of $\mathbf{k}(T_d)^{GL_3}$, a specification f of the form $b_{i,j} \mapsto a_{i,j}$ or $b_{i,j} \mapsto 0$ in the case when $a_{i,j} \notin \mathbf{k}(C)$, gives us an element of $\mathbf{k}(C)^G$.

But SL_3-invariants(thus and GL_3-invariants) of ternary forms are known only for the cases $d \leq 4$, see [1]. Furthermore, analyzing of the Poincare series of the algebra of invariants of ternary forms, [2], we see that the algebras are very complicated and there is no chance to find theirs minimal generating set.

Since $\mathbf{k}(T_d)^{GL_3}$ coincides with $\mathbf{k}(T_d)^{\mathfrak{gl}_3}$ it implies that the algebra of invariants is the intersection of kernels of some derivations of the algebra $\mathbf{k}(T_d)$. Then in place of the specification of coefficients of the form we may use a "specification" of those derivations.

First, consider a motivating example. Let

$$C_3 : y^2 + a_0x^3 + 3a_1x^2 + 3a_2x + a_3 = 0,$$

and let G_0 be the group generated by the translations $x \mapsto \alpha\tilde{x} + b$. It is easy to show that j-invariant of the curve C_3 equals ([3], p. 46):

$$j(C_3) = 6912\,\frac{\left(a_0a_2 - {a_1}^2\right)^3}{{a_0}^2\left(4\,{a_1}^3a_3 - 6\,a_3a_0a_1a_2 - 3\,{a_1}^2{a_2}^2 + {a_3}^2{a_0}^2 + 4\,a_0{a_2}^3\right)}.$$

Up to constant factor $j(C_3)$ equal to $\dfrac{S^3}{T}$ where S and T are the specification of two SL_3-invariants of ternary cubic, see [4], p.173.

From another viewpoint a direct calculation yields that the following is true: $\mathcal{D}\left(j(C_3)\right) = 0$ and $\mathcal{H}\left(j(C_3)\right) = 0$ where $\mathcal{D}$, $\mathcal{H}$ denote the following derivations of the algebra of rational functions $\mathbf{k}(C_3) = \mathbf{k}(a_0, a_1, a_2, a_3)$:

$$\mathcal{D}(a_i) = ia_{i-1}, \mathcal{H}(a_i) = (3-i)a_i, i = 0,1,2,3.$$

From the computational point of view, the calculation of $\ker\mathcal{D} \cap \ker\mathcal{H}$ is more effective than the calculating of the algebra of invariants of the ternary cubic. We will derive further that

$$\ker\mathcal{D}_3 \cap \ker H_3 = \mathbf{k}\left(\frac{\left(a_0a_2 - {a_1}^2\right)^3}{a_0^3}, \frac{a_3\,a_0^2 + 2\,{a_1}^3 - 3\,a_1\,a_2\,a_0}{a_0^2}\right).$$

In section 2, we give a full description of the algebras of polynomial and rational invariants for the curve $y^n = f(x)$. We compute a complete set of independent invariants and then reconstruct a curve from given values of these invariants.

2. Invariants of curves $y^n = f(x)$.

Consider the curve

$$C_{n,d} : y^n = a_0x^d + da_1x^{d-1} + \cdots + a_d = \sum_{i=0}^{d} a_d\binom{d}{i}x^{d-i}, n \geq 1,$$

and let G be the group generated by the following transformations

$$x = \alpha\tilde{x} + b, y = \tilde{y}, \alpha \neq 0.$$

It is clear that G is isomorphic to the group of the affine transformations of the complex line $\mathbf{k}^1$.

The algebra $\mathbf{k}(C_{n,d})^G$ consists of functions $\phi(a_0, a_1, \dots, a_d)$ that have the invariance property

$$\phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d) = \phi(a_0, a_1, \dots, a_d).$$

Here $\tilde{a}_i$ denote the coefficients of the curve $\tilde{C}_{n,d}$:

$$\tilde{C}_{n,d} : \sum_{i=0}^{d} a_d \binom{d}{i} (\alpha \tilde{x} + b)^{d-i} = \sum_{i=0}^{d} \tilde{a}_d \binom{d}{i} \tilde{x}^{d-i}.$$

The coefficients $\tilde{a}_i$ are given by the formulas

$$\tilde{a}_i = \alpha^{n-i} \sum_{k=0}^{i} \binom{i}{k} a_{i-k} b^k. \tag{1}$$

The following statement holds

Theorem 2.1. *We have*

$$\mathbf{k}(C_{n,d})^G = \ker \mathcal{D}_d \cap \ker \mathcal{E}_d,$$

where $\mathcal{D}_d$, $\mathcal{E}_d$ denote the following derivations of the algebra $\mathbf{k}(C_{n,d})$:

$$\mathcal{D}_d(a_i) = i a_{i-1}, \mathcal{E}_d(a_i) = (d-i) a_i. \tag{2}$$

A linear map $D : \mathbf{k}(C_{n,d}) \to \mathbf{k}(C_{n,d})$ is called a derivation of the algebra $\mathbf{k}(C_{n,d})$ if $D(fg) = D(f)g + fD(g)$, for all $f, g \in \mathbf{k}(C_{n,d})$. The subalgebra $\ker D := \{f \in \mathbf{k}(C_{n,d}) \mid D(f) = 0\}$ is called the kernel of the derivation D. The above derivation $\mathcal{D}_d$ is called the basic Weitzenböck derivation.

Proof. Following the arguments of Hilbert [7],page 26, we differentiate with respect to b both sides of the equality

$$\phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d) = \phi(a_0, a_1, \dots, a_d),$$

and obtain in this way

$$\frac{\partial \phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)}{\partial \tilde{a}_0} \frac{\partial \tilde{a}_0}{\partial b} + \frac{\partial \phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)}{\partial \tilde{a}_1} \frac{\partial \tilde{a}_1}{\partial b} + \dots + \frac{\partial \phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)}{\partial \tilde{a}_d} \frac{\partial \tilde{a}_d}{\partial b} = 0.$$

Substitute $\alpha = 1$, $b = 0$ to $\phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)$ and taking into account that $\left.\frac{\partial \tilde{a}_i}{\partial b}\right|_{b=0} = i a_{i-1}$, we get:

$$\tilde{a}_0 \frac{\partial \phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)}{\partial \tilde{a}_1} + 2\tilde{a}_1 \frac{\partial \phi(\tilde{a}_0, \dots, \tilde{a}_d)}{\partial \tilde{a}_2} + \cdots d\tilde{a}_{d-1} \frac{\partial \phi(\tilde{a}_0, \dots, \tilde{a}_d)}{\partial \tilde{a}_d} = 0$$

Since the function $\phi(\tilde{a}_0, \dots, \tilde{a}_d)$ depends on the variables $\tilde{a}_i$ in the exact same way as the function $\phi(a_0, a_1, \dots, a_d)$ depends on the a_i then it implies that $\phi(a_0, a_1, \dots, a_d)$ satisfies the differential equation

$$a_0 \frac{\partial \phi(a_0, a_1 \dots, a_d)}{\partial a_1} + 2a_1 \frac{\partial \phi(a_0, a_1 \dots, a_d)}{\partial a_2} + d a_{d-1} \frac{\partial \phi(a_0, a_1 \dots, a_d)}{\partial a_d} = 0.$$

Thus, $\mathcal{D}_d(\phi) = 0$. Now we differentiate with respect to α both sides of the same equality

$$\phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d) = \phi(a_0, a_1, \dots, a_d).$$

$$\frac{\partial \phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)}{\partial \tilde{a}_0} \frac{\partial \tilde{a}_0}{\partial \alpha} + \frac{\partial \phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)}{\partial \tilde{a}_1} \frac{\partial \tilde{a}_1}{\partial \alpha} + \dots + \frac{\partial \phi(\tilde{a}_0, \tilde{a}_1, \dots, \tilde{a}_d)}{\partial \tilde{a}_d} \frac{\partial \tilde{a}_d}{\partial \alpha} = 0.$$

Substitute $\alpha=1, b=0$, to $\phi(\tilde a_0,\tilde a_1,\ldots,\tilde a_d)$ and taking into account

$$\frac{\partial \tilde a_i}{\partial \alpha}\Big|_{\alpha=1\, b=0}=(d-i)a_i,$$

we get:

$$\tilde a_0\frac{\partial\phi(\tilde a_0,\tilde a_1,\ldots,\tilde a_d)}{\partial \tilde a_0}+(d-1)\tilde a_1\frac{\partial\phi(\tilde a_0,\ldots,\tilde a_d)}{\partial \tilde a_1}+\cdots+\tilde a_{d-1}\frac{\partial\phi(\tilde a_0,\ldots,\tilde a_d)}{\partial \tilde a_{d-1}}=0$$

It implies that $\mathcal{E}_d(\phi(a_0,a_1\ldots,a_d))=0$.

The formulas (1) define a representation of two-parametric Lie group G on the polynomial algebra $\mathbf{k}[a_0,a_1,\ldots,a_d]$. By construction of the operators $\mathcal{D}_d$ and $\ker\mathcal{E}_d$ the formulas (2) define a representation of the corresponding Lie algebra of the group G. It is well-known fact of the representation theory that algebras of invariants of Lie group coincide with the algebra of invariant of its Lie algebra, see [8]. Thus

$$\mathbf{k}(C_{n,d})^G=\ker\mathcal{D}_d\cap\ker\mathcal{E}_d.$$

□

The derivation $\mathcal{E}_d$ sends the monomial $a_0^{m_0}a_1^{m_1}\cdots a_d^{m_d}$ to the term

$$(m_0 d+m_1(d-1)+\cdots m_{d-1})a_0^{m_0}a_1^{m_1}\cdots a_d^{m_d}.$$

Let the number $\omega\left(a_0^{m_0}a_1^{m_1}\cdots a_d^{m_d}\right):=m_0 d+m_1(d-1)+\cdots m_{d-1}$ be called the weight of the monomial $a_0^{m_0}a_1^{m_1}\cdots a_d^{m_d}$. In particular $\omega(a_i)=d-i$.

A homogeneous polynomial $f\in\mathbf{k}[C_{n,d}]$ be called *isobaric* if all their monomial have equal weights. A weight $\omega(f)$ of an isobaric polynomial f is called a weight of its monomials. Since $\omega(f)>0$, then $\mathbf{k}[C_{n,d}]^{\mathcal{E}_d}=0$. It implies that $\mathbf{k}[C_{n,d}]^G=0$.

If f,g are two isobaric polynomials then

$$\mathcal{E}_d\left(\frac{f}{g}\right)=(\omega(f)-\omega(g))\frac{f}{g}.$$

Therefore the algebra $k(C_{n,d})^{\mathcal{E}_d}$ is generated by rational functions which both denominator and numerator has equal weight.

The kernel of the derivation $\mathcal{D}_d$ also is well-known, see [5], [6]. It is given by

$$\ker\mathcal{D}_d=\mathbf{k}(a_0,z_2,\ldots,z_d),$$

where

$$z_i:=\sum_{k=0}^{i-2}(-1)^k\binom{i}{k}a_{i-k}a_1^k a_0^{i-k-1}+(i-1)(-1)^{i+1}a_1^i, i=2,\ldots,d.$$

In particular, for $d=5$ we get

$$\begin{aligned}
z_2&=a_2\,a_0-{a_1}^2\\
z_3&=a_3\,a_0^2+2\,{a_1}^3-3\,a_1\,a_2\,a_0\\
z_4&=a_4\,a_0^3-3\,{a_1}^4+6\,{a_1}^2\,a_2\,a_0-4\,a_1\,a_3\,a_0^2\\
z_5&=a_5\,a_0^4+4\,{a_1}^5-10\,{a_1}^3\,a_2\,a_0+10\,{a_1}^2\,a_3\,a_0^2-5\,a_1\,a_4\,a_0^3.
\end{aligned}$$

It is easy to see that $\omega(z_i)=i(n-1)$. The following element $\dfrac{z_i^d}{a_0^{i(d-1)}}$ has the zero weight for any i. Therefore, the statement holds:

Theorem 2.2.

$$\mathbf{k}(C_{n,d})^G = \mathbf{k}\left(\frac{z_2^d}{a_0^{2(d-1)}}, \frac{z_3^d}{a_0^{3(d-1)}}, \cdots, \frac{z_d^d}{a_0^{d(d-1)}}\right).$$

For the curve

$$C_{n,d}^0 : y^n = x^d + da_1x^{d-1} + \cdots + a_d = x^d + \sum_{i=1}^{d} a_d \binom{d}{i} x^{d-i}.$$

and for the group G_0 generated by translations $x = \tilde{x} + b$, the algebra of invariants becomes simpler:

$$\mathbf{k}\left(C_d^0\right)^{G_0} = \mathbf{k}(z_2, z_3, \ldots, z_d).$$

Theorem 2.3. *(i) For arbitrary set of $d-1$ numbers $j_2,j_3,\ldots,j_d$ there exists a curve C such that $z_i(C) = j_i$.*

(ii) For two curves C and C' the equalities $z_i(C) = z_i(C')$ hold for $2 \leq i \leq d$, if and only if these curves are G_0-isomorphic.

Proof. (i). Consider the system of equations

$$\begin{cases} a_2 - {a_1}^2 = j_2 \\ a_3 + 2\,{a_1}^3 - 3\,a_1\,a_2 = j_3 \\ a_4 - 3\,{a_1}^4 + 6\,{a_1}^2\,a_2 - 4\,a_1\,a_3 = j_4 \\ \ldots \\ a_d + \displaystyle\sum_{k=1}^{d-2} (-1)^k \binom{d}{k} a_{d-k} a_1^k + (d-1)(-1)^{d+1} a_1^d = j_d \end{cases}$$

Put $a_1 = 0$ we get $a_n = j_n$, i.e., the curve

$$C : y^n = x^d + \binom{d}{2} j_2 x^{d-2} + \cdots + j_d,$$

has the required property $z_i(C) = j_i$.

(ii). We may assume, without loss of generality, that the curve C has the form

$$C : y^2 = x^d + \binom{d}{2} j_2 x^{d-2} + \cdots + j_d.$$

Suppose that for a curve

$$C' : y^2 = x^d + da_1x^{d-1} + \cdots + a_d = x^d + \sum_{i=1}^{d} a_d \binom{d}{i} x^{d-i}.$$

holds $z_i(C') = z_i(C) = j_i$.

By solving the above system we obtain

$$a_i = j_i + a_1^i + \sum_{s=1}^{i-2} \binom{i}{s} a_1^s j_{i-s}, i = 2, 3, \ldots, d. \tag{2}$$

Comparing (3) with (1) we deduce that the curve C' is obtained from the curve C by the translation $x + a_1$. ∎

3. Acknowledgments

The author would like to thank the referee for many valuable suggestions that improved the paper.

References

[1] A. Brower, Invariants of the ternary quartic, http://www.win.tue.nl/∼aeb/math/ternary_quartic.html
[2] L. Bedratyuk, G.Xin, MacMahon Partition Analysis and the Poincaré series of the algebras of invariants of ternary and quaternary forms, *Linear and Multilinear Algebra*, V.59. No 7, (2011), 789–799
[3] J. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, 106, Springer-Verlag, 1986.
[4] B. Sturmfels, Algorithms in invariant theory, Texts and Monographs in Symbolic Computation. Wien: Springer, 2008.
[5] A. Nowicki, Polynomial derivation and their Ring of Constants.–UMK: Torun,–1994.
[6] L. Bedratyuk, On complete system of invariants for the binary form of degree 7, *J. Symb. Comput.*, **42**, (2007), 935-947.
[7] D. Hilbert, *Theory of Algebraic Invariants*,Cambridge University Press,1993.
[8] W. Fulton, J. Harris. Representation theory: a first course, 1991.

