# A NOTE ABOUT INVARIANTS OF ALGEBRAIC CURVES 

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


#### Abstract

Let $G$ be the group generated by the transformations $x=\alpha \tilde{x}+$ $b, y=\tilde{y}, \alpha \neq 0, \alpha, b \in \mathbf{k}$, 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 $\mathbf{k}$, 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 $\phi\left(a_{0,0}, a_{1,0}, \ldots, a_{d, 0}\right) \in \mathbf{k}(C)$ is called $G$-invariant if $\phi\left(\tilde{a}_{0,0}, \tilde{a}_{1,0}, \ldots, \tilde{a}_{d, 0}\right)=$ $\phi\left(a_{0,0}, a_{1,0}, \ldots, a_{d, 0}\right)$ where $\tilde{a}_{0,0}, \tilde{a}_{1,0}, \ldots, \tilde{a}_{d, 0}$ are defined from the condition

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

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

[^0]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 $\sum_{i+j \leq d} b_{i, j} x^{d-(i+j)} y^{i} z^{j}$, $b_{i, j} \in \mathbf{k}$ endowed with the natural action of the group $G L_{3}:=G L_{3}(\mathbf{k})$. Given $G L_{3}$-invariant function $f$ of $\mathbf{k}\left(T_{d}\right)^{G L_{3}}$, 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 $S L_{3}$-invariants(thus and $G L_{3}$-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 $\mathbf{k}\left(T_{d}\right)^{G L_{3}}$ coincides with $\mathbf{k}\left(T_{d}\right)^{\mathfrak{g l}_{3}}$ it implies that the algebra of invariants is the intersection of kernels of some derivations of the algebra $\mathbf{k}\left(T_{d}\right)$. 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

$$
C_{3}: y^{2}+a_{0} x^{3}+3 a_{1} x^{2}+3 a_{2} x+a_{3}=0
$$

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):

$$
j\left(C_{3}\right)=6912 \frac{\left(a_{0} a_{2}-a_{1}^{2}\right)^{3}}{a_{0}^{2}\left(4 a_{1}^{3} a_{3}-6 a_{3} a_{0} a_{1} a_{2}-3 a_{1}^{2} a_{2}^{2}+a_{3}^{2} a_{0}^{2}+4 a_{0} a_{2}^{3}\right)}
$$

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

From another viewpoint a direct calculation yields that the following is true: $\mathcal{D}\left(j\left(C_{3}\right)\right)=0$ and $\mathcal{H}\left(j\left(C_{3}\right)\right)=0$ where $\mathcal{D}, \mathcal{H}$ denote the following derivations of the algebra of rational functions $\mathbf{k}\left(C_{3}\right)=\mathbf{k}\left(a_{0}, a_{1}, a_{2}, a_{3}\right)$ :

$$
\mathcal{D}\left(a_{i}\right)=i a_{i-1}, \mathcal{H}\left(a_{i}\right)=(3-i) a_{i}, i=0,1,2,3 .
$$

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

$$
\operatorname{ker} \mathcal{D}_{3} \cap \operatorname{ker} H_{3}=\mathbf{k}\left(\frac{\left(a_{0} a_{2}-a_{1}^{2}\right)^{3}}{a_{0}^{3}}, \frac{a_{3} a_{0}^{2}+2 a_{1}^{3}-3 a_{1} a_{2} a_{0}}{a_{0}^{2}}\right)
$$

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.

$$
\text { 2. Invariants of curves } y^{n}=f(x)
$$

Consider the curve

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

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 $\mathbf{k}\left(C_{n, d}\right)^{G}$ consists of functions $\phi\left(a_{0}, a_{1}, \ldots, a_{d}\right)$ that have the invariance property

$$
\phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)=\phi\left(a_{0}, a_{1}, \ldots, a_{d}\right)
$$

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

$$
\begin{equation*}
\tilde{a}_{i}=\alpha^{n-i} \sum_{k=0}^{i}\binom{i}{k} a_{i-k} b^{k} . \tag{1}
\end{equation*}
$$

The following statement holds
Theorem 2.1. We have

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

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

$$
\begin{equation*}
\mathcal{D}_{d}\left(a_{i}\right)=i a_{i-1}, \mathcal{E}_{d}\left(a_{i}\right)=(d-i) a_{i} . \tag{2}
\end{equation*}
$$

A linear map $D: \mathbf{k}\left(C_{n, d}\right) \rightarrow \mathbf{k}\left(C_{n, d}\right)$ is called a derivation of the algebra $\mathbf{k}\left(C_{n, d}\right)$ if $D(f g)=D(f) g+f D(g)$, for all $f, g \in \mathbf{k}\left(C_{n, d}\right)$. The subalgebra ker $D:=\{f \in$ $\left.\mathbf{k}\left(C_{n, d}\right) \mid D(f)=0\right\}$ 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

$$
\phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)=\phi\left(a_{0}, a_{1}, \ldots, a_{d}\right)
$$

and obtain in this way

$$
\frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{0}} \frac{\partial \tilde{a}_{0}}{\partial b}+\frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{1}} \frac{\partial \tilde{a}_{1}}{\partial b}+\cdots+\frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{d}} \frac{\partial \tilde{a}_{d}}{\partial b}=0 .
$$

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

$$
\tilde{a}_{0} \frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{1}}+2 \tilde{a}_{1} \frac{\partial \phi\left(\tilde{a}_{0}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{2}}+\cdots d \tilde{a}_{d-1} \frac{\partial \phi\left(\tilde{a}_{0}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{d}}=0
$$

Since the function $\phi\left(\tilde{a}_{0}, \ldots, \tilde{a}_{d}\right)$ depends on the variables $\tilde{a}_{i}$ in the exact same way as the function $\phi\left(a_{0}, a_{1}, \ldots, a_{d}\right)$ depends on the $a_{i}$ then it implies that $\phi\left(a_{0}, a_{1}, \ldots, a_{d}\right)$ satisfies the differential equation

$$
a_{0} \frac{\partial \phi\left(a_{0}, a_{1} \ldots, a_{d}\right)}{\partial a_{1}}+2 a_{1} \frac{\partial \phi\left(a_{0}, a_{1} \ldots, a_{d}\right)}{\partial a_{2}}+d a_{d-1} \frac{\partial \phi\left(a_{0}, a_{1} \ldots, a_{d}\right)}{\partial a_{d}}=0
$$

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

$$
\begin{gathered}
\phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)=\phi\left(a_{0}, a_{1}, \ldots, a_{d}\right) . \\
\frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{0}} \frac{\partial \tilde{a}_{0}}{\partial \alpha}+\frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{1}} \frac{\partial \tilde{a}_{1}}{\partial \alpha}+\cdots+\frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{d}} \frac{\partial \tilde{a}_{d}}{\partial \alpha}=0 .
\end{gathered}
$$

Substitute $\alpha=1, b=0$, to $\phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)$ and taking into account

$$
\left.\frac{\partial \tilde{a}_{i}}{\partial \alpha}\right|_{\alpha=1 b=0}=(d-i) a_{i},
$$

we get:

$$
\tilde{a}_{0} \frac{\partial \phi\left(\tilde{a}_{0}, \tilde{a}_{1}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{0}}+(d-1) \tilde{a}_{1} \frac{\partial \phi\left(\tilde{a}_{0}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{1}}+\cdots+\tilde{a}_{d-1} \frac{\partial \phi\left(\tilde{a}_{0}, \ldots, \tilde{a}_{d}\right)}{\partial \tilde{a}_{d-1}}=0
$$

It implies that $\mathcal{E}_{d}\left(\phi\left(a_{0}, a_{1} \ldots, a_{d}\right)\right)=0$.
The formulas (1) define a representation of two-parametric Lie group $G$ on the polynomial algebra $\mathbf{k}\left[a_{0}, a_{1}, \ldots, a_{d}\right]$. 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

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

The derivation $\mathcal{E}_{d}$ sends the monomial $a_{0}^{m_{0}} a_{1}^{m_{1}} \cdots a_{d}^{m_{d}}$ to the term

$$
\left(m_{0} d+m_{1}(d-1)+\cdots m_{d-1}\right) a_{0}^{m_{0}} a_{1}^{m_{1}} \cdots a_{d}^{m_{d}} .
$$

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 $\omega\left(a_{i}\right)=d-i$.

A homogeneous polynomial $f \in \mathbf{k}\left[C_{n, d}\right]$ 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 $\mathbf{k}\left[C_{n, d}\right]^{\mathcal{E}_{d}}=0$. It implies that $\mathbf{k}\left[C_{n, d}\right]^{G}=0$.

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 $k\left(C_{n, d}\right)^{\mathcal{E}_{d}}$ 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

$$
\operatorname{ker} \mathcal{D}_{d}=\mathbf{k}\left(a_{0}, z_{2}, \ldots, z_{d}\right)
$$

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 $\omega\left(z_{i}\right)=i(n-1)$. The following element $\frac{z_{i}^{d}}{a_{0}^{i(d-1)}}$ has the zero weight for any $i$. Therefore, the statement holds:

## Theorem 2.2.

$$
\mathbf{k}\left(C_{n, d}\right)^{G}=\mathbf{k}\left(\frac{z_{2}^{d}}{a_{0}^{2(d-1)}}, \frac{z_{3}^{d}}{a_{0}^{3(d-1)}}, \cdots, \frac{z_{d}^{d}}{a_{0}^{d(d-1)}}\right) .
$$

For the curve

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

and for the group $G_{0}$ generated by translations $x=\tilde{x}+b$, the algebra of invariants becomes simpler:

$$
\mathbf{k}\left(C_{d}^{0}\right)^{G_{0}}=\mathbf{k}\left(z_{2}, z_{3}, \ldots, z_{d}\right)
$$

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 $C^{\prime}$ the equalities $z_{i}(C)=z_{i}\left(C^{\prime}\right)$ hold for $2 \leq i \leq d$, if and only if these curves are $G_{0}$-isomorphic.

Proof. (i). Consider the system of equations

$$
\left\{\begin{array}{l}
a_{2}-a_{1}^{2}=j_{2} \\
a_{3}+2 a_{1}^{3}-3 a_{1} a_{2}=j_{3} \\
a_{4}-3 a_{1}^{4}+6 a_{1}^{2} a_{2}-4 a_{1} a_{3}=j_{4} \\
\cdots \\
a_{d}+\sum_{k=1}^{d-2}(-1)^{k}\binom{d}{k} a_{d-k} a_{1}^{k}+(d-1)(-1)^{d+1} a_{1}^{d}=j_{d}
\end{array}\right.
$$

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

$$
C^{\prime}: y^{2}=x^{d}+d a_{1} x^{d-1}+\cdots+a_{d}=x^{d}+\sum_{i=1}^{d} a_{d}\binom{d}{i} x^{d-i}
$$

holds $z_{i}\left(C^{\prime}\right)=z_{i}(C)=j_{i}$.
By solving the above system we obtain

$$
\begin{equation*}
a_{i}=j_{i}+a_{1}^{i}+\sum_{s=1}^{i-2}\binom{i}{s} a_{1}^{s} j_{i-s}, i=2,3, \ldots, d \tag{2}
\end{equation*}
$$

Comparing (3) with (1) we deduce that the curve $C^{\prime}$ 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, SpringerVerlag, 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.


[^0]:    2000 Mathematics Subject Classification. 14H99, 20F10, 30F10.

