Classic and special Lie Groups structures on some plane cubic curves with singularities. II

$\boxed{\text{A. Constantinescu}}$, C. Udrişte, S. Pricopie

Abstract. The singular points of an irreducible plane cubic curve are quite limited: one knot/node, or one cusp. Our research starts originally with the Descartes Folium, which has a knot/node, and is able to have many group structures. The original results are concentrated in six directions: (i) special structures on affine algebraic varieties, (ii) theory of $\mathbb{K}$-groups, (iii) isomorphisms of $\mathbb{K}$-groups, (iv) canonic $\mathbb{K}$-groups structures on subsets $U \subset \mathbb{P}^1_{\mathbb{K}}$, (v) canonic $\mathbb{K}$-groups structures on the subset $\overline{DF}_{\mathbb{K}} \setminus \{O\}$ of the projective Descartes Folium $\overline{DF}_{\mathbb{K}}$, (vi) geometric interpretations.

M.S.C. 2010: 14H45, 14L10, 14A10.
Key words: $\mathbb{K}$-groups; algebraic groups; Lie groups; isomorphisms; Descartes Folium.

1 Motivation of problem

As in [2], we consider a field $\mathbb{K}$ with char. $\mathbb{K} \neq 3$ and *the projective Descartes Folium* $\overline{DF} = \overline{DF}_{\mathbb{K}} \subset \mathbb{P}^2_{\mathbb{K}}$ over $\mathbb{K}$, given by the homogeneous algebraic equation

$$\overline{DF} = \overline{DF}_{\mathbb{K}} : x^3 + y^3 - 3axyz = 0, \quad a \in \mathbb{K} \setminus \{0\},$$

where (x, y, z) are the natural homogeneous coordinates on $\mathbb{P}^2_{\mathbb{K}}$. This curve having a non-smooth point, namely $O = (0, 0, 1)$ (see [2], Section 1, Comments 2), iii)), is of interest in applied mathematics (code theory/cryptography).

We will address the following

Question. Are there "good" group composition laws on "nice" subsets $U \subseteq \overline{DF}$ (as $U = \overline{DF} \setminus \{0\}$, $U = \overline{DF}$ and *other ones*)?

In [2] we treated this Question in the case when $\mathbb{K}$ is algebraically closed with char. $\mathbb{K} \neq 3$ and $U = \overline{DF} \setminus \{0\}$.

In the following we will present some extensions of these results when $\mathbb{K}$ is an arbitrary field (not necessarily algebraically closed) (see Sections 4 and 5).

Balkan Journal of Geometry and Its Applications, Vol.22, No.1, 2017, pp. 18-32.

The main part of this exposition is the presentation of the notion of $\mathbb{K} - group$ and some of its properties (Sections 2 and 3). The results from Sections 4 and 5 concerning some "good" group composition laws on $\overline{DF} \setminus \{0\}$ over an arbitrary base field $\mathbb{K}$ with char. $\mathbb{K} \neq 3$, represent mainly applications of the given properties of $\mathbb{K}$-groups. In a further paper ([2], III), we intend to present other such applications of $\mathbb{K}$-groups to "good" group composition laws on other subsets $U \subseteq \overline{DF}$.

2 $\mathbb{K}$-structures on affine algebraic $\overline{\mathbb{K}}$-varieties

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}} \supseteq \mathbb{K}$ an algebraic closure of $\mathbb{K}$ and $\overline{C}$ an (irreducible) affine algebraic $\overline{\mathbb{K}}$-variety.

We will use throughout this paper the notions of $\mathbb{K}$-structure on $\overline{C}$, $\mathbb{K}$-rational points of $\overline{C}$ and morphism of affine algebraic $\overline{\mathbb{K}}$-varieties with $\mathbb{K}$-structure. The definitions of all these notions can be found in [1], §11 and §12.

Recall only the first from these definitions: a $\mathbb{K}$-*structure* on the affine (irreducible) algebraic $\overline{\mathbb{K}}$-variety is a finitely generated $\mathbb{K}$-subalgebra A of the affine $\overline{\mathbb{K}}$-algebra $\overline{\mathbb{K}}$ $[\overline{C}]$ of $\overline{C}$ such that $\overline{\mathbb{K}}[\overline{C}] = \overline{\mathbb{K}} \otimes_{\mathbb{K}} A$; in this situation we say that the algebraic $\mathbb{K}$-variety $\overline{C}$ is *defined over* $\mathbb{K}$ (see [1], 12.1).

We can adopt an equivalent point of view for the definitions of the notions above of $\mathbb{K}$-structure, rational $\mathbb{K}$-points and morphism of affine algebraic $\overline{\mathbb{K}}$-varieties with $\mathbb{K}$-structures, as follows.

a) The (irreducible) affine algebraic $\overline{\mathbb{K}}$-variety $\overline{C}$ is *defined over* $\mathbb{K}$ if there exists a closed immersion $\overline{C} \subseteq \mathbb{A}^n_{\overline{\mathbb{K}}}$ of algebraic $\overline{\mathbb{K}}$-varieties such that the ideal of definition $\mathbf{I}(\overline{C})$ of $\overline{C}$ in $\mathbb{A}^n_{\overline{\mathbb{K}}}$ is generated by $\mathbb{K}$-polynomials.

Then for the affine $\overline{\mathbb{K}}$-algebra $\overline{\mathbb{K}}[\overline{C}]$ of $\overline{C}$ we have $\overline{\mathbb{K}}[\overline{C}] = \overline{\mathbb{K}}[X_1, \ldots, X_n]/\mathbf{I}(\overline{C})$ $= \{f : V \to \overline{\mathbb{K}} | f$ defined by a $\overline{\mathbb{K}}$-polynomial $\}$. Let $\mathbf{I}_{\mathbb{K}}(\overline{C}) = \mathbb{K}[X_1, \ldots, X_n] \cap \mathbf{I}(\overline{C})$ and $A = \mathbb{K}[X_1, \ldots, X_n]/\mathbf{I}_{\mathbb{K}}(\overline{C})$. Then $A = \{f : V \to \overline{\mathbb{K}} | f$ defined by a $\mathbb{K}$-polynomial$\}$ and A is the *canonic* $\mathbb{K}$-*structure* of the algebraic $\overline{\mathbb{K}}$-variety $\overline{C}$ defined over $\mathbb{K}$; it is a $\mathbb{K}$-structure on $\overline{C}$ in the meaning of [1].

If $\overline{C}, \overline{C}'$ are algebraic $\overline{\mathbb{K}}$-varieties defined over $\mathbb{K}$ having A, resp. A', as $\mathbb{K}$-structures then $\overline{C} \times \overline{C}\,'$ is also defined over $\mathbb{K}$ with $A \otimes_{\mathbb{K}} A'$ as $\mathbb{K}$-structure.

b) If $\overline{C}$ is an (irreducible) affine algebraic $\overline{\mathbb{K}}$-variety defined over $\mathbb{K}$ and $\overline{C} \subseteq \mathbb{A}^n_{\overline{\mathbb{K}}}$ is a closed immersion as in a), we can define the subset $\overline{C}(\mathbb{K}) \subseteq \overline{C}$ of all $\mathbb{K}$-*rational points* of $\overline{C}$ by

$$\overline{C}(\mathbb{K}) = \mathbb{A}^n_{\mathbb{K}} \cap \overline{C} \subseteq \mathbb{A}^n_{\overline{\mathbb{K}}}$$

Then $\overline{C}(\mathbb{K}) = \{x = (x_1, \ldots, x_n) \in \overline{C} \,|\, x_1, \ldots, x_n \in \mathbb{K}\}$. We have a canonic bijection

$$\overline{C}(\mathbb{K}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{K}-alg}(A, \mathbb{K})$$

$$x \longrightarrow [f \longrightarrow f(x)].$$

If $\mathbb{K} = \overline{\mathbb{K}}$, then $\overline{C}(\mathbb{K}) = \overline{C}$.

c) Suppose $\overline{C} \subseteq \mathbb{A}^n_{\overline{\mathbb{K}}} = \overline{\mathbb{K}}^n$, $\overline{C}\,' \subseteq \mathbb{A}^m_{\overline{\mathbb{K}}} = \overline{\mathbb{K}}^m$ two (irreducible) affine algebraic $\overline{\mathbb{K}}$-varieties over $\mathbb{K}$ such that the ideals $\mathbf{I}(\overline{C})$, $\mathbf{I}(\overline{C}\,')$ defining $\overline{C}$, resp. $\overline{C}\,'$, are generated by $\mathbb{K}$-polynomials and let $f = (f_1, \ldots, f_m) : \overline{C} \to \overline{C}\,'$ be a morphism of algebraic $\overline{\mathbb{K}}$-varieties. We say that f is *defined over* $\mathbb{K}$ if its scalar components $f_1, \ldots, f_m : \overline{C} \to \overline{\mathbb{K}}$ are all defined by $\mathbb{K}$-polynomials.

In this situation, $f(\overline{C}(\mathbb{K})) \subseteq \overline{C'}(\mathbb{K})$. Moreover, if $f^* : \overline{\mathbb{K}}[\overline{C'}] \to \overline{\mathbb{K}}[\overline{C}]$ is the dual $\overline{\mathbb{K}}$-algebras morphism and $A \subseteq \overline{\mathbb{K}}[\overline{C}]$, $A' \subseteq \overline{\mathbb{K}}[\overline{C'}]$ are the $\mathbb{K}$-structures on $\overline{C}$, resp. $\overline{C'}'$, then $f^*(A') \subseteq A$. Now we will recall the notion of *algebraic (Lie)* $\overline{\mathbb{K}}$*-group defined over* $\mathbb{K}$, used throughout this exposition.

According to [1], Ch. I, 1.1, an *algebraic (Lie)* $\overline{\mathbb{K}}$*-group* is a pair $(G, \cdot)$ such that

i) G is an algebraic $\overline{\mathbb{K}}$-variety,

ii) $(G, \cdot)$ is a group,

iii) the maps $m : G \times G \to G$, where $m(x, y) = x \cdot y$, and $inv : G \to G$, where $inv(x) = x^{-1}$, are morphisms of algebraic $\overline{\mathbb{K}}$-varieties.

Moreover, if *G, m and inv* are all defined over $\mathbb{K}$, then $(G, \cdot)$ is called an algebraic (Lie) $\overline{\mathbb{K}}$-group *defined over* $\mathbb{K}$ (or an algebraic $\mathbb{K}$-group).

In this last situation, m induces a group structure $(G(\mathbb{K}), \cdot)$ on the subset of all $\mathbb{K}$-rational points $G(\mathbb{K}) \subseteq G$.

If $(G, \cdot)$, $(G', \cdot)$ are algebraic $\overline{\mathbb{K}}$-groups, resp. defined over $\mathbb{K}$, a map $f : G \to G'$ is called a *morphism* of algebraic $\overline{\mathbb{K}}$*-groups*, resp. *defined over* $\mathbb{K}$, if

i) $f : G \to G'$ is a morphism of algebraic $\overline{\mathbb{K}}$-varieties, resp. defined over $\mathbb{K}$,

ii) $f : (G, \cdot) \to (G', \cdot)$ is a group morphism.

(see [1], Ch.I, 1.1)

3 $\mathbb{K}$-groups

Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}} \supseteq K$ an algebraic closure of $\mathbb{K}$.

We will introduce a notion, useful throughout this paper:

Definition 2.1 Let $\overline{C}$ be an (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curve defined over $\mathbb{K}$. Suppose that the subset of all its $\mathbb{K}$-rational points $\overline{C}(\mathbb{K}) \neq \varnothing$ and it is endowed with a group structure $(\overline{C}(\mathbb{K}), \cdot)$.

We say that $(\overline{C}(\mathbb{K}), \cdot)$ is a $\mathbb{K}$*-group (w.r.t.* $\overline{C}$*)* if one of the following equivalent conditions is fulfilled:

i) the group composition law $\cdot$ on $\overline{C}(\mathbb{K})$ can be extended to a group composition law $\cdot$ on $\overline{C}$ such that $(\overline{C}, \cdot)$ is an algebraic $\overline{\mathbb{K}}$-group defined over $\mathbb{K}$,

ii) $(\overline{C}(\mathbb{K}), \cdot)$ is a subgroup of an algebraic $\overline{\mathbb{K}}$-group $(\overline{C}, \cdot)$ defined over $\mathbb{K}$.

Remarks 1) In Definition 2.1, if $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed then $\overline{C}(\mathbb{K}) = \overline{C}$ and $(\overline{C}(\mathbb{K}), \cdot)$ is a $\mathbb{K}$-group iff $(\overline{C}(\mathbb{K}), \cdot = (\overline{C}, \cdot)$ is an algebraic $\mathbb{K}$-group.

2) The above notion of $\mathbb{K}$-group can be formulated in more general conditions, for an (irreducible) smooth algebraic $\overline{\mathbb{K}}$-variety $\overline{C}$ defined over $\mathbb{K}$, of arbitrary dimension. A near idea of $\mathbb{K}$-group is evoked in [7, 9.4].

We have the following

Examples.

1) $\mathbb{G}_{m,\mathbb{K}} = (\mathbb{K} \setminus \{0\}, \cdot)$ is a $\mathbb{K}$-group (w.r.t. $\mathbb{A}^1_{\overline{\mathbb{K}}} \setminus \{0\}$)

2) $\mathbb{G}_{a,\mathbb{K}} = (\mathbb{K}, +)$ is a $\mathbb{K}$-group (w.r.t. $\mathbb{A}^1_{\overline{\mathbb{K}}}$).

In fact, for $\overline{C} = \mathbb{A}^1_{\overline{\mathbb{K}}} \setminus \{0\}$, resp. $\overline{C} = \mathbb{A}^1_{\overline{\mathbb{K}}}$, we have $\overline{C}(\mathbb{K}) = \mathbb{K} \setminus \{0\}$, resp. $\overline{C}(\mathbb{K}) = \mathbb{K}$, and $\mathbb{G}_{m,\mathbb{K}}$, $\mathbb{G}_{a,\mathbb{K}}$ are subgroups of $(\overline{C}, \cdot) = \mathbb{G}_{m,\overline{\mathbb{K}}}$, resp. $(\overline{C}, +) = \mathbb{G}_{a,\overline{\mathbb{K}}}$, with $\mathbb{G}_{m,\overline{\mathbb{K}}}$, $\mathbb{G}_{a,\overline{\mathbb{K}}}$ algebraic $\overline{\mathbb{K}}$-groups defined over $\mathbb{K}$.

We will call such a $\mathbb{K}$-group structure on $\mathbb{K} \setminus \{0\}$, resp. $\mathbb{K}$, the *canonic* $\mathbb{K}$-group structure on $\mathbb{K} \setminus \{0\}$, resp. $\mathbb{K}$.

The following fact is a direct consequence of the Structure Theorem for 1-dimensional connected affine algebraic $\mathbb{K}$-groups ([1, Ch. II, Th. 10.9]).

Lemma 2.1 a) In the previous Definition 2.1, if $(\overline{C}(\mathbb{K}), \cdot)$ is a $\mathbb{K}$-group (w.r.t. $\overline{C}$), then $(\overline{C}, \cdot) \backsimeq \mathbb{G}_{m,\overline{\mathbb{K}}}$ or $(\overline{C}, \cdot) \backsimeq \mathbb{G}_{a,\overline{\mathbb{K}}}$, as algebraic $\overline{\mathbb{K}}$-groups.

b) Each $\mathbb{K}$-group is commutative.

In particular, from a) of the Lemma 2.1 it follows that $\overline{C} \backsimeq \mathbb{A}^1_{\overline{\mathbb{K}}} \setminus \{0\}$ or $\overline{C} \backsimeq \mathbb{A}^1_{\overline{\mathbb{K}}}$ as algebraic $\overline{\mathbb{K}}$-varieties if $(\overline{C}(\mathbb{K}), \cdot)$ is a $\mathbb{K}$-group (w.r.t. $\overline{C}$).

Definition 2.2 In the previous Definition 2.1, let us assume that $(\overline{C}(\mathbb{K}), \cdot)$ is a $\mathbb{K}$-group (w.r.t. $\overline{C}$). Then $(\overline{C}(\mathbb{K}), \cdot)$ is called *of type* $\mathbb{G}_{m,\overline{\mathbb{K}}}$, resp. $\mathbb{G}_{a,\overline{\mathbb{K}}}$, if $\overline{C}$ is isomorphic with $\mathbb{A}^1_{\overline{\mathbb{K}}} \setminus \{0\}$, resp. $\mathbb{A}^1_{\overline{\mathbb{K}}}$, as algebraic $\overline{\mathbb{K}}$-variety.

We will give more

Examples. 3) Denote $U = \mathbb{P}^1_{\mathbb{K}} \setminus \{P_1, \dots, P_n\} \neq \varnothing$ and $\overline{C} = \mathbb{P}^1_{\overline{\mathbb{K}}} \setminus \{P_1, \dots, P_n\}$. $\overline{C}$ is an (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curve with $\overline{C}(\mathbb{K}) = U$. According to the definition, $(U, \cdot)$ is a $\mathbb{K}$-group (w.r.t. $\overline{C}$) if the composition law $\cdot$ on U can be extended to a group composition law $\cdot$ on $\overline{C}$ such that $(\overline{C}, \cdot)$ is an algebraic $\overline{\mathbb{K}}$-group defined over $\mathbb{K}$.

We will call such a $\mathbb{K}$-group structure on $U = \mathbb{P}^1_{\mathbb{K}} \setminus \{P_1, \dots, P_n\}$, a *canonic* $\mathbb{K}$-group structure on U.

Particular cases.

a) $n = 2$, $P_1 = \infty$, $P_2 = 0$.

Then $U = \mathbb{A}^1_{\mathbb{K}} \setminus \{0\} = \mathbb{K} \setminus \{0\}$ and we have the canonic $\mathbb{K}$-group $(U, \cdot) = \mathbb{G}_{m,\overline{\mathbb{K}}}$, with $\cdot$ the underlying multiplication of the field $\mathbb{K}$.

b) $n = 1$, $P_1 = \infty$.

Then $U = \mathbb{A}^1_{\mathbb{K}} = \mathbb{K}$ and we have the canonic $\mathbb{K}$-group $(U, +) = \mathbb{G}_{a,\mathbb{K}}$, with $+$ the underlying addition of the field $\mathbb{K}$.

4) Suppose char. $\mathbb{K} \neq 3$ and $F(X, Y, Z) = X^3 + Y^3 - 3aXYZ \in \mathbb{K}[X, Y, Z]$. Consider the projective *Descartes Folium* $\overline{DF} = \overline{DF}_{\mathbb{K}} \subset \mathbb{P}^2_{\mathbb{K}}$ defined by the equation $F(x, y, z) = 0$. Recall that the polynomial $F(X, Y, Z)$is irreducible (see, [2], Section 1, Prop. 1); then $\overline{DF}_{\overline{\mathbb{K}}} \subset \mathbb{P}^2_{\overline{\mathbb{K}}}$ is an (irreducible) algebraic $\overline{\mathbb{K}}$-curve defined on $\mathbb{K}$.

Let $\overline{C} = \overline{DF}_{\overline{\mathbb{K}}} \setminus \{P_1 = O, P_2, ..., P_n\}$ with $O = (0, 0, 1)$ the unique non-singular point of $\overline{C}$ and $P_2, ..., P_n \in \overline{DF}_{\mathbb{K}}$. Then $\overline{C}$ is an (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curve defined on $\mathbb{K}$ and $\overline{C}(\mathbb{K}) = \overline{DF}_{\mathbb{K}} \setminus \{P_1 = O, P_2, ..., P_n\}$. Then the group $(\overline{C}(\mathbb{K}), \cdot)$ is a $\mathbb{K}$-group (w.r.t. $\overline{C}$) if the composition law $\cdot$ on $\overline{C}(\mathbb{K})$ can be extended to a group composition law $\cdot$ on $\overline{C}$ such that $(\overline{C}, \cdot)$ is an algebraic $\overline{\mathbb{K}}$-group defined over $\mathbb{K}$.

We call such a $\mathbb{K}$-group structure a *canonic* $\mathbb{K}$-group structure on $\overline{C}(\mathbb{K}) = \overline{DF}_{\mathbb{K}} \setminus \{P_1 = O, P_2, ..., P_n\}$. We will see that only for $n = 1$, the set $\overline{C}(\mathbb{K})$ admits a canonic $\mathbb{K}$-structure (see the following Proposition 5.1)

Comment. The previous Definition 2.1 of $\mathbb{K}$-groups uses the notion of algebraic $\overline{\mathbb{K}}$-group. Now we will give a characterization of $\mathbb{K}$-groups in terms of group $\mathbb{K}$-scheme (see [5]) as follows.

Firstly we will make a short remark. Let $\overline{C}$ be an (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curve defined over $\mathbb{K}$ and $A \subseteq \overline{\mathbb{K}}[\overline{C}]$ the $\mathbb{K}$-subalgebra defining its $\mathbb{K}$-structure. Denote by $G = \operatorname{Spec} A$ the algebraic $\mathbb{K}$-scheme associated to A and by $G(\mathbb{K}) = \{\underline{m} \subset A \,|\, \underline{m}$ maximal ideal with $A/\underline{m} = \mathbb{K}\} \subset G$ the subset of all $\mathbb{K}$-points of G. Then we have the following canonical bijection

$$\overline{C}(\mathbb{K}) \xrightarrow{\sim} G(\mathbb{K})$$

defined as follows:

a) if we consider $\overline{C} \subseteq \mathbb{A}^n_{\overline{\mathbb{K}}}$ as a closed algebraic $\overline{\mathbb{K}}$-subvariety such that the defining ideal $\mathbf{I} \subset \overline{\mathbb{K}}[x_1, ..., x_n]$ is generated by $\mathbb{K}$-polynomials, according to Section 1 we have then

$$\overline{C}(\mathbb{K}) = \mathbb{A}^n_{\mathbb{K}} \cap \overline{C} = \mathbb{K}^n \cap \overline{C} = \{x = (x_1, ..., x_n) \in \overline{C} \,|\, x_1, ..., x_n \in \mathbb{K}\}$$

and $A = \{f : \overline{C} \to \mathbb{K} \,|\, f \text{ defined by a } \mathbb{K} - \textit{polynomial}\}$; then the bijection is

$$\overline{C}(\mathbb{K}) \xrightarrow{\sim} G(\mathbb{K})$$

$$x \longrightarrow \{f \in A \,|\, f(x) = 0\} = \ker[A \to \mathbb{K}, \text{ defined by } f \to f(x)]$$

(see also the canonic bijection from b) of Section 2).

b) For an alternative definition, we consider $\overline{C}(\mathbb{K}) \subseteq \overline{C} = \text{Spec.max.}\, \overline{\mathbb{K}}[\overline{C}]$ and the integral faithful flat ring extension $A \subseteq \overline{\mathbb{K}}[\overline{C}]$. Then the bijection is defined by

$$\begin{array}{ccc} \overline{C}(\mathbb{K}) & \xrightarrow{\sim} & G(\mathbb{K}) \subset G \\ \underline{n} & \longrightarrow & \underline{n} \cap A \\ & & \\ \underline{n}\overline{K}[\overline{C}] & \longleftarrow & \underline{n} \end{array}$$

Therefore, we can identify $\overline{C}(\mathbb{K}) = G(\mathbb{K})$ via this canonical bijective correspondence.

We have the following restatement of Definition 2.1:

Theorem 2.1′ Under the conditions and notations of Definition 2.1, let $(\overline{C}(\mathbb{K}), \cdot) = (G(\mathbb{K}), \cdot)$ be a group. Then the following assertions are equivalent: (i) the pair $(\overline{C}(\mathbb{K}), \cdot)$ is a $\mathbb{K}$-group (w.r.t. $\overline{C}$); (ii) there exists a group $\mathbb{K}$-scheme structure $(G, \underline{m})$ on G inducing the group composition law $\cdot$ on the subset $G(\mathbb{K}) \subset G$.

Remark Theorem 2.1′ and the preparatory remark are also valid if we work with the more general definition of $\mathbb{K}$-group (according to the previous Remark 2), i.e., with $\overline{C}$ an (irreducible)affine smooth algebraic $\overline{\mathbb{K}}$-variety defined over $\mathbb{K}$, of arbitrary dimension.

In the following we will state two basic properties for $\mathbb{K}$-groups.

Theorem 2.1 Let $\overline{C}$ be an (irreducible) smooth affine algebraic $\mathbb{K}$-curve defined over $\mathbb{K}$. Then the canonic map

$$\begin{array}{ccc} \{\text{algebraic}\, \overline{\mathbb{K}} - \text{group}\, (\overline{C}, \cdot)\, \text{over}\, \mathbb{K}\} & \xrightarrow{\sim} & \{\mathbb{K} - \text{group}\, (\overline{C}(\mathbb{K}), \cdot)\, (w.r.t.\ \overline{C})\} \\ (\overline{C}, \cdot) & \longrightarrow & (\overline{C}(\mathbb{K}), \cdot) \end{array}$$

is bijective.

Definition 2.3 In the bijective correspondence from Theorem 2.1, we say that the algebraic $\overline{\mathbb{K}}$-group $(\overline{C}, \cdot)$ defined over $\mathbb{K}$ is induced by the $\mathbb{K}$-group $(\overline{C}(\mathbb{K}), \cdot)$ and conversely.

Comment. Using the groups $\mathbb{K}$-schemes frame for the characterization of $\mathbb{K}$-groups (Theorem 2.1$'$), then Theorem 2.1 above can be easily restated in terms of group $\mathbb{K}$-scheme ([5]) as follows:

Corollary 2.1$'$ Let $\overline{C}$ be an (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curve defined over $\mathbb{K}$ and $G = \mathit{Spec}\ A$, with $A \subset \overline{\mathbb{K}}[\overline{C}]$ its structural $\mathbb{K}$-subalgebra. Then the canonic map

$$\begin{array}{ccc} \{\text{group}\,\mathbb{K}-\text{scheme}\,(G,m)\} & \xrightarrow{\sim} & \{\mathbb{K}-\text{group}\,(\overline{C}(\mathbb{K}),\cdot) = (G(\mathbb{K}),\cdot)\,w.r.t.\ \overline{C}\} \\ (G,m) & \longrightarrow & \text{induced group } (G(\mathbb{K}),m) \end{array}$$

is bijective.

Theorem 2.2 Let $\overline{C}$ be an (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curve defined over $\mathbb{K}$, let $(\overline{C}(\mathbb{K}), \cdot)$ be a $\mathbb{K}$-group (w.r.t $\overline{C}$) and $E \in \overline{C}(\mathbb{K})$. Then: (i) there exists a unique $\mathbb{K}$-group $(\overline{C}(\mathbb{K}), \cdot_E)$ (w.r.t. $\overline{C}$) having the neutral element E; (ii) for each $P, Q \in \overline{C}(\mathbb{K})$, we have $P \cdot Q = P \cdot Q \cdot E^{-1}$, with E^{-1} the inverse of E in the group $(\overline{C}(\mathbb{K}), \cdot)$.

Remark If $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed, then $\overline{C}(\mathbb{K}) = \overline{C}$ and in Theorem 2.2 above we can replace the condition "$\mathbb{K}$-group" with "algebraic $\mathbb{K}$-group".

There exists a similarity of Theorem 2.2 above with the following one. For this, let us firstly recall that for any smooth algebraic $\mathbb{C}$-variety $\overline{C}$ one associates a natural analytic $\mathbb{C}$-manifold $\overline{C}^{\,an}$ on the set $\overline{C}$; if $(\overline{C}, \cdot)$ is an algebraic $\mathbb{C}$-group then $(\overline{C}^{\,an}, \cdot)$ is a Lie $\mathbb{C}$-group, denoted also by $(\overline{C}, \cdot)^{an}$ and called the *associated* $\mathbb{C}$*-group*.

Theorem 2.3 Let $\mathbb{K} = \mathbb{C}$, let $\overline{C}$ be an (irreducible) affine smooth $\mathbb{C}$-curve, let $(\overline{C}, \cdot)$ be an algebraic $\mathbb{C}$-group and $E \in \overline{C}$. Denote by $(\overline{C}, \cdot_E)$ the unique algebraic $\mathbb{C}$-group having the neutral element E. Then: (i) there exists a unique Lie $\mathbb{C}$-group on $\overline{C}$ having the neutral element E; it is the associated Lie $\mathbb{C}$-group $(\overline{C}, \cdot_E)^{\,an} = (\overline{C}^{\,an}, \cdot_E)$; (ii) for each $P, Q \in \overline{C}^{\,an} = \overline{C}$, we have $P \cdot_E Q = P \cdot Q \cdot E^{-1}$, with E^{-1} the inverse/opposite of E in the group $(\overline{C}^{\,an}, \cdot_E) = (\overline{C}, \cdot_E)$.

It follows

Corollary 2.2 Let $\mathbb{K} = \mathbb{C}$, let $\overline{C}$ be an (irreducible) affine algebraic $\mathbb{C}$-curve, let $(\overline{C}, \cdot)$ be an algebraic $\mathbb{C}$-group. Then for each Lie $\mathbb{C}$-group $(\overline{C}^{\,an}, \odot)$, the group $(\overline{C}, \odot)$ is an algebraic $\mathbb{C}$-group.

Indeed, we apply Theorem 2.3 for $E \in \overline{C}$ the neutral element of the group $(\overline{C}^{\,an}, \odot)$; then $(\overline{C}^{\,an}, \odot) = (\overline{C}, \cdot_E)^{\,an}$, i.e., $(\overline{C}^{\,an}, \odot)$ is the associated Lie $\mathbb{C}$-group with the algebraic $\mathbb{C}$-group $(\overline{C}, \cdot_E)$. It follows $(\overline{C}, \odot) = (\overline{C}, \cdot_E)$.

Corollary 2.2 above extends Corollary 4.1 from the paper [2].

4 Isomorphisms of $\mathbb{K}$-groups

Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}} \supseteq \mathbb{K}$ an algebraic closure of $\mathbb{K}$.

Definition 3.1 Let $\overline{C}, \overline{C}\,'$ be two (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curves defined over $\mathbb{K}$ and $(\overline{C}(\mathbb{K}), \cdot)$, $(\overline{C}\,'(\mathbb{K}), \cdot)$ two $\mathbb{K}$-groups (w.r.t. $\overline{C}$, resp. $\overline{C}\,'$).

A map $f : \overline{C}(\mathbb{K}) \to \overline{C}\,'(\mathbb{K})$ is called *isomorphism of* $\mathbb{K}$*-groups* if (i) the function $f : (\overline{C}(\mathbb{K}), \cdot) \to (\overline{C}\,'(\mathbb{K}, \cdot)$ is a group isomorphism and (ii) the function f can be extended to an isomorphism $f : \overline{C} \xrightarrow{\sim} \overline{C}\,'$ of algebraic $\mathbb{K}$-curves defined over $\mathbb{K}$.

Then the extended $f : (\overline{C}, \cdot) \xrightarrow{\sim} (\overline{C}\,', \cdot)$ is even an isomorphism of algebraic $\overline{\mathbb{K}}$-groups defined over $\mathbb{K}$, according to the following

Proposition 3.1 Let $f : \overline{C} \xrightarrow{\sim} \overline{C}\,'$ be an isomorphism of (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curves defined over $\mathbb{K}$, let $(\overline{C}, \cdot)$ and $(\overline{C}\,', \cdot)$ two algebraic $\overline{\mathbb{K}}$-groups defined over $\mathbb{K}$ and $(\overline{C}(\mathbb{K}), \cdot)$, $(\overline{C}\,'(\mathbb{K}, \cdot)$ the induced $\mathbb{K}$-groups. Denote by $E \in \overline{C}(\mathbb{K})$, $E' \in \overline{C}\,'(\mathbb{K})$ the neutral elements of the groups above. Then the following assertions are equivalent: (i) the induced map $f : (\overline{C}(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}), \cdot)$ is a group isomorphism; (i') the function $f : (\overline{C}, \cdot) \xrightarrow{\sim} (\overline{C}\,', \cdot)$ is a group isomorphism; (i'') $f(E) = E'$.

Remarks. 1) If $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed, then $(\overline{C}(\mathbb{K}), \cdot) = (\overline{C}, \cdot)$, $(\overline{C}\,'(\mathbb{K}), \cdot) = (\overline{C}\,', \cdot)$ and $f : (\overline{C}(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}), \cdot)$ is a $\mathbb{K}$-group isomorphism iff $f : (\overline{C}, \cdot) \xrightarrow{\sim} (\overline{C}\,', \cdot)$ is an isomorphism of algebraic $\overline{\mathbb{K}}$-groups (see also Section 2, Remarks, 1)).

2) If $f : (\overline{C}(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}), \cdot)$ and $g : (\overline{C}\,'(\mathbb{K}), \cdot) \to (\overline{C}\,''(\mathbb{K}), \cdot)$ are $\mathbb{K}$-groups isomorphisms, then $g \circ f$ and f^{-1}, as $1_{\overline{C}(\mathbb{K})}$, are also $\mathbb{K}$-groups isomorphisms.

3) Using the group $\mathbb{K}$-schemes frame for characterization of $\mathbb{K}$-groups (Theorem 2.1′), we can state easily the following equivalence:

Theorem 3.1′ Let $\overline{C}$ and $\overline{C}\,'$ be two (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curves defined over $\mathbb{K}$, let $(\overline{C}(\mathbb{K}), \cdot)$ and $(\overline{C}\,'(\mathbb{K}), \cdot)$ be two $\mathbb{K}$-groups (w.r.t. $\overline{C}$, resp. $\overline{C}\,'$). Let $A \subseteq \overline{\mathbb{K}}[\overline{C}]$ and $A' \subseteq \overline{\mathbb{K}}[\overline{C}\,']$ be the $\mathbb{K}$-structures on $\overline{C}$ and $\overline{C}\,'$, and let $G = \operatorname{Spec} A$, $G' = \operatorname{Spec} A'$. Then the following assertions are equivalent: (a) the map $f : (\overline{C}(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}), \cdot)$ is an isomorphism of $\mathbb{K}$-groups; (b) the map $f : (\overline{C}(\mathbb{K}), \cdot) = (G(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}), \cdot) = (G'(\mathbb{K}), \cdot)$ is a group isomorphism and it can be extended to an isomorphism $f : G \xrightarrow{\sim} G'$ of $\mathbb{K}$-schemes.

The Definition 3.1 of the isomorphism between $\mathbb{K}$-groups is based on extensions to isomorphisms between their induced algebraic $\overline{\mathbb{K}}$-groups (see Proposition 3.1).

To formulate the next Theorem we recall that the cardinal of the set $\overline{C}(\mathbb{K})$ is usually denoted by $|\overline{C}(\mathbb{K})|$.

Theorem 3.1 Let $\overline{C}$, $\overline{C}\,'$ be two (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curves defined over $\mathbb{K}$. Let $f : (\overline{C}, \cdot) \xrightarrow{\sim} (\overline{C}\,', \cdot)$ be an isomorphism of algebraic $\overline{\mathbb{K}}$-groups defined over $\mathbb{K}$ and $\overline{f} : (\overline{C}(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}), \cdot)$ be an isomorphism of $\mathbb{K}$-groups. Then the (surjective) canonic map $\{f\} \longrightarrow \{\overline{f}\}$ is bijective if (a) the group $(\overline{C}(\mathbb{K}), \cdot)$ is of type $\mathbb{G}_{m,\mathbb{K}}$ and $|\overline{C}(\mathbb{K}| \geq 3$ or (b) the group $(\overline{C}(\mathbb{K}), \cdot)$ is of type $\mathbb{G}_{a,\mathbb{K}}$ and $|\overline{C}(\mathbb{K}| \geq 2$.

Remark. The condition $|\overline{C}(\mathbb{K}| \geq 3$ in the case (a) of the previous Theorem 3.1 is necessary, according to the following

Example. Let $\mathbb{K} = \mathbb{Z}_2$ or $\mathbb{Z}_3$ and $\overline{C} = \mathbb{A}^1_{\overline{\mathbb{K}}} \setminus \{O\} = \overline{\mathbb{K}} \setminus \{0\}$. Then $\overline{C}(\mathbb{K}) = \mathbb{K} \setminus \{0\}$. Now, we consider the $\mathbb{K}$-group $(\overline{C}(\mathbb{K}), \cdot) = (\mathbb{K} \setminus \{0\}, \cdot) = \mathbb{G}_{m,\mathbb{K}}$ and the map

$f = 1_{\overline{C}(\mathbb{K})} : (\overline{C}(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}(\mathbb{K}), \cdot)$. The induced algebraic $\overline{\mathbb{K}}$-group of the group $(\overline{C}(\mathbb{K}), \cdot)$ is $(\overline{C}, \cdot) = (\overline{\mathbb{K}} \setminus \{0\}, \cdot) = \mathbb{G}_{m,\overline{\mathbb{K}}}$. Then there exists two different isomorphisms $(\overline{C}, \cdot) \rightrightarrows (\overline{C}, \cdot)$ of algebraic $\overline{\mathbb{K}}$-groups defined over $\mathbb{K}$ inducing the previous map f, namely $t \to t$ and $t \to t^{-1}$.

Corollary 3.1 In the previous Theorem 3.1 assume that (a) $\mathbb{K}$ is separably closed field and $(\overline{C}(\mathbb{K}), \cdot)$ is of type $\mathbb{G}_{m,\overline{\mathbb{K}}}$ or (b) $\mathbb{K}$ is a perfect field and $(\overline{C}(\mathbb{K}), \cdot)$ is of type $\mathbb{G}_{a,\overline{\mathbb{K}}}$. Then the canonic map of Theorem 3.1 is bijective.

For the proof of Corollary 3.1 we can use the Structure Theorem of connected 1-dimensional affine algebraic $\overline{\mathbb{K}}$-groups from [1] (Ch. III, Th. 10.9) and its subsequent Remark: there exists an isomorphism $\overline{C} \xrightarrow{\sim} \mathbb{G}_{m,\overline{\mathbb{K}}} = (\overline{\mathbb{K}} \setminus \{0\}, \cdot)$ resp. $\overline{C} \xrightarrow{\sim} \mathbb{G}_{a,\overline{\mathbb{K}}} = (\overline{\mathbb{K}}, +)$ of algebraic $\overline{\mathbb{K}}$-groups defined over $\mathbb{K}$ and then $|\overline{C}(\mathbb{K})| = |\mathbb{K} \setminus \{0\}| \geq 3$, resp. $|\overline{C}(\mathbb{K})| = |\mathbb{K}| \geq 2$.

Definition 3.2 In Theorem 3.1 above, if the canonic map is bijective, we say that the map $f : (\overline{C}, \cdot) \xrightarrow{\sim} (\overline{C}\,', \cdot)$ is induced by $f : (\overline{C}(\mathbb{K}), \cdot) \xrightarrow{\sim} (\overline{C}(\mathbb{K}), \cdot)$ and conversely.

Comment. In terms of group $\mathbb{K}$-schemes, according Theorem $2.1'$, it is easy to establish the following equivalent form of the previous Theorem 3.1

Corollary 3.1′ Let $\overline{C}$, $\overline{C}\,'$ be two (irreducible) affine smooth algebraic $\overline{\mathbb{K}}$-curves defined over $\mathbb{K}$, let $A \subseteq \overline{\mathbb{K}}[\overline{C}]$ and $A' \subseteq \overline{\mathbb{K}}[\overline{C}\,']$ be their $\mathbb{K}$-structures and $G = \operatorname{Spec} A$, $G' = \operatorname{Spec} A'$. Let $f : (G, m) \xrightarrow{\sim} (G', m)$ be an isomorphism of group $\mathbb{K}$-schemes and let the map $\overline{f} : (\overline{C}(\mathbb{K}) \cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}), \cdot)$ be an isomorphism of $\mathbb{K}$-groups. Then the (surjective) canonic map

$$\{f\} \longrightarrow \{\overline{f}\},\ f \longrightarrow [f : (G(\mathbb{K}), m) \xrightarrow{\sim} (G'(\mathbb{K}), m)]$$

is bijective if (a) $G \otimes_{\mathbb{K}} \overline{\mathbb{K}} \simeq \overline{\mathbb{K}} \setminus \{0\}$ as $\overline{\mathbb{K}}$-schemes and $|G(\mathbb{K})| \geq 3$, or
(b) $G \otimes_{\mathbb{K}} \overline{\mathbb{K}} \simeq \overline{\mathbb{K}}$ as $\overline{\mathbb{K}}$-schemes and $|G(\mathbb{K})| \geq 2$.

In fact $\overline{C}(\mathbb{K}) = G(\mathbb{K})$, $\overline{C}\,'(\mathbb{K}) = G'(\mathbb{K})$ and $G \otimes_{\mathbb{K}} \overline{\mathbb{K}}$ is the $\overline{\mathbb{K}}$-scheme associated to the algebraic $\overline{\mathbb{K}}$-variety $\overline{C}$, because $\overline{\mathbb{K}} \otimes_{\mathbb{K}} A = \overline{\mathbb{K}}[\overline{C}]$.

Examples. 1) The group isomorphisms

$$(\mathbb{K} \setminus \{0\}, \cdot) \xrightarrow{\sim} (\mathbb{K} \setminus \{0\}, \cdot)$$

$$t \longrightarrow t^{\epsilon}$$

with $\epsilon \in \{-1, 1\}$ are automorphisms of the $\mathbb{K}$-group $\mathbb{G}_{m,\mathbb{K}} = (\mathbb{K} \setminus \{0\}, \cdot)$ (w.r.t. $\mathbb{A}^1_{\mathbb{K}} \setminus \{0\} = \mathbb{K} \setminus \{0\}$).

These represent all automorphisms of the $\mathbb{K}$-group $\mathbb{G}_{m,\mathbb{K}}$.

2) The group isomorphisms

$$(\mathbb{K}, +) \xrightarrow{\sim} (\mathbb{K}, +)$$

$$t \longrightarrow at,$$

with $a \in \mathbb{K} \setminus \{0\}$, are automorphisms of the $\mathbb{K}$-group $\mathbb{G}_{a,\mathbb{K}} = (\mathbb{K}, +)$ (w.r.t. $\mathbb{A}^1_{\mathbb{K}}$). These represent all automorphisms of the $\mathbb{K}$-group $\mathbb{G}_{a,\mathbb{K}}$.

3) Let $(\overline{C}(\mathbb{K},\cdot)$ be a $\mathbb{K}$-group, (w.r.t. $\overline{C}$). Let $E \in \overline{C}(\mathbb{K})$ and $(\overline{C}(\mathbb{K},\cdot_E)$ the unique $\mathbb{K}$-group (w.r.t. $\overline{C}$), with neutral element E (Theorem 2.2). Then the group isomorphism

$$t_E : (\overline{C}(\mathbb{K}),\cdot) \xrightarrow{\sim} (\overline{C}(\mathbb{K}),\cdot_E),\ A \longrightarrow E \cdot A$$

is an isomorphism of $\mathbb{K}$-groups (w.r.t. $\overline{C}$).

4) Let $\mathbb{K}$ be a *separably closed field* and $(\overline{C}(\mathbb{K}),\cdot)$ a $\mathbb{K}$-group (w.r.t $\overline{C}$) of type $\mathbb{G}_{m,\overline{\mathbb{K}}}$. Then there exists an isomorphism of $\mathbb{K}$-groups $(\overline{C}(\mathbb{K}),\cdot) \xrightarrow{\sim} \mathbb{G}_{m,\mathbb{K}} = (\mathbb{K}\setminus\{0\},\cdot)$.

5) Let $\mathbb{K}$ be a *perfect field* and $(\overline{C}(\mathbb{K}),\cdot)$ a $\mathbb{K}$-group (w.r.t. $\overline{C}$) of type $\mathbb{G}_{a,\overline{\mathbb{K}}}$. Then there exists an isomorphism of $\mathbb{K}$-groups $(\overline{C}(\mathbb{K},\cdot) \xrightarrow{\sim} \mathbb{G}_{a,\mathbb{K}} = (\mathbb{K},+)$.

In Examples 4) and 5) above, we can use the Structure Theorem of connected affine 1-dimensional algebraic $\mathbb{K}$-groups from [1, Ch. III, Th. 10.9] and its subsequent Remark.

Now we can state some properties of isomorphisms of $\mathbb{K}$-groups.

Theorem 3.2 Let $\overline{C}$, $\overline{C}\,'$ be two (irreducible) affine smooth $\overline{\mathbb{K}}$-curves defined over $\mathbb{K}$ and $(\overline{C}(\mathbb{K}),\cdot)$, $(\overline{C}\,'(\mathbb{K}),\cdot)$ two $\mathbb{K}$-groups (w.r.t. $\overline{C}$, resp. $\overline{C}\,'$). Then: (i) if $(\overline{C}(\mathbb{K}),\cdot)$, $(\overline{C}\,'(\mathbb{K},\cdot)$ are isomorphic $\mathbb{K}$-groups of type $\mathbb{G}_{m,\overline{\mathbb{K}}}$, there exist at most two such isomorphisms of $\mathbb{K}$-groups, $f, g : (\overline{C}(\mathbb{K}),\cdot) \rightrightarrows (\overline{C}\,'(\mathbb{K}),\cdot)$; if $|\overline{C}(\mathbb{K}| = |\overline{C}\,'(\mathbb{K})| \geq 3$, then there exist exactly two such isomorphisms $f \neq g$; we have $g(P) = [g(P)]^{-1}$, for each $P \in \overline{C}(\mathbb{K})$; (ii) if $(\overline{C}(\mathbb{K}),\cdot)$, $(\overline{C}\,'(\mathbb{K}),\cdot)$ are isomorphic $\mathbb{K}$-groups of type $\mathbb{G}_{a,\overline{\mathbb{K}}}$ and $A \in \overline{C}(\mathbb{K})$, $A' \in \overline{C}\,'(\mathbb{K})$ are non-neutral elements, then there exists at most one isomorphism of $\mathbb{K}$-groups, $f : (\overline{C}(\mathbb{K}),\cdot) \xrightarrow{\sim} (\overline{C}\,'(\mathbb{K}),\cdot)$ such that $f(A) = A'$; if $\mathbb{K}$ is a perfect field, there exists a unique such an isomorphism.

5 Application I: canonic $\mathbb{K}$-groups structures on subsets $U \subset \mathbb{P}^1_{\mathbb{K}}$

The following statements are extensions of Theorem 3.1 from [2] for arbitrary (not necessarily algebraically closed) base fields.

Theorem 4.1 Let $\mathbb{K}$ be an arbitrary field and $U = \mathbb{P}^1_{\mathbb{K}} \setminus \{P_1, ..., P_n\} \neq \varnothing$ a $\mathbb{K}$-open subset of $\mathbb{P}^1_{\mathbb{K}}$. Then U admits a canonic $\mathbb{K}$-group structure (i.e., as in Section 2, Example 3)) if and only if $n = 1$ or $n = 2$.

In particular, if $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed, the set U admits an algebraic $\mathbb{K}$-group structure iff $n = 1$ or $n = 2$ (cf. Section 3, Remark 1).

In Theorem 4.1 above, if $n = 1$ or $n = 2$, then the set U admits in general many canonic $\mathbb{K}$-structures, namely, for each $E \in U$ there exists a unique $\mathbb{K}$-group structure on U having the neutral element E (cf. Theorem 2.2). But all these $\mathbb{K}$-group structures are always related by automorphisms of the projective line $\mathbb{P}^1_{\mathbb{K}}$, as follows:

Proposition 4.1 Let $\mathbb{K}$ be a field and $U, U' \subset \mathbb{P}^1_{\mathbb{K}}$ some non-empty $\mathbb{K}$-open subsets. Suppose that (i) $U = \mathbb{P}^1_{\mathbb{K}} \setminus \{P_1, P_2\}$, $U' = \mathbb{P}^1_{\mathbb{K}} \setminus \{P'_1, P'_2\}$ and $(U,\cdot)$, $(U',\cdot)$ are canonic $\mathbb{K}$-groups, or (ii) $U = \mathbb{P}^1_{\mathbb{K}} \setminus \{P_1\}$, $U' = \mathbb{P}^1_{\mathbb{K}} \setminus \{P'_1\}$ and $(U,\cdot)$, $(U',\cdot)$ are canonic $\mathbb{K}$-groups. Then there exists an automorphism $\alpha : \mathbb{P}^1_{\mathbb{K}} \xrightarrow{\sim} \mathbb{P}^1_{\mathbb{K}}$ such that $\alpha(U) = U'$ and $\alpha : (U,\cdot) \xrightarrow{\sim} (U',\cdot)$ is an isomorphism of $\mathbb{K}$-groups.

In fact, let $E \in U$, $E' \in U'$ be the neutral elements of the corresponding $\mathbb{K}$-groups. In situation (i), there exists only two required automorphisms α of $\mathbb{P}^1_{\mathbb{K}}$, completely determined by the conditions

$$\alpha(P_1) = P_1', \alpha(P_2) = P_2', \alpha(E) = E'$$

or

$$\alpha(P_1) = P_2', \alpha(P_2) = P_1', \alpha(E) = E'.$$

In the situation (ii), for $P \in U$, $P \neq E$ and $P' \in U'$, $P' \neq E'$, the map α is uniquely determined by the conditions

$$\alpha(P_1) = P_1', \alpha(E) = E', \alpha(P) = P'.$$

By Definition 3.1 and Proposition 3.1,all these automorphisms α of $\mathbb{P}^1_{\mathbb{K}}$ induces maps $\alpha|_U : (U, \cdot) \xrightarrow{\sim} (U', \cdot)$ which are isomorphisms of $\mathbb{K}$-groups.

6 Application II: canonic $\mathbb{K}$-groups structures on the subset $\overline{DF}_{\mathbb{K}} \setminus \{O\}$ of the projective Descartes Folium $\overline{DF}_{\mathbb{K}}$

Let $\mathbb{K}$ be a field with char. $\mathbb{K} \neq 3$ and $\overline{\mathbb{K}} \supseteq \mathbb{K}$ an algebraic closure of $\mathbb{K}$.

Recall some facts concerning the *Descartes Folium* ([2], Sections 1 and 2).

Let $F(X, Y, Z) = X^3 + Y^3 - 3aXYZ \in \mathbb{K}[X, Y, Z]$, with $a \in \mathbb{K} \setminus \{0\}$; according to the paper [2], Prop. 1.1, F is irreducible.

The *projective Descartes Folium* (over $\mathbb{K}$) is the algebraic subset of $\mathbb{P}^2_{\mathbb{K}}$, denoted by $\overline{DF}$ or by $\overline{DF}_{\mathbb{K}}$, defined by the homogeneous equation $F(x, y, z) = 0$, where (x, y, z) are the canonic homogeneous coordinates on $\mathbb{P}^2_{\mathbb{K}}$.

If we consider the subset $\overline{DF}_{\overline{\mathbb{K}}} \subset \mathbb{P}^2_{\overline{\mathbb{K}}}$ defined by the same equation $F(x, y, z) = 0$, then $\overline{DF} = \overline{DF}_{\mathbb{K}} \subset \overline{DF}_{\overline{\mathbb{K}}}$ and $\overline{DF}_{\overline{\mathbb{K}}}$ is an (irreducible) algebraic $\overline{\mathbb{K}}$-subvariety of $\mathbb{P}^2_{\overline{\mathbb{K}}}$ defined over $\mathbb{K}$, having a unique non-smooth (non-regular) point, namely $O = (0, 0, 1)$. Concerning the subset of all $\mathbb{K}$-rational points $\overline{DF}_{\overline{\mathbb{K}}}(\mathbb{K})$ of $\overline{DF}_{\overline{\mathbb{K}}}$, we have $\overline{DF}_{\overline{\mathbb{K}}}(\mathbb{K}) = \overline{DF}_{\mathbb{K}} = \overline{DF}$ ([2], Comments 2), ii)).

There exists a natural map (parametrization of $\overline{DF} = \overline{DF}_{\mathbb{K}}$)

$$\begin{array}{cccc} \overline{DF} & (3at, 3at^2, 1+t^3) & O = (0,0,1) & (x,y,z) \in \overline{DF} \setminus \{O\} \\ p \uparrow & \uparrow & \uparrow & \downarrow \\ \mathbb{P}^1_{\mathbb{K}} = \mathbb{A}^1_{\mathbb{K}} \cup \{\infty\} & t \in \mathbb{A}^1_{\mathbb{K}} & \infty & t = \frac{y}{x} \end{array}$$

where we indicated the definition of p and of a partial inverse of p. We have $p(\infty) = p(0) = O = (0, 0, 1)$, $p(1) = (3, 3, 2) = V$ (the vertex of $\overline{DF}$) and $p(-1) = (1, -1, 0) = I$ (one of the infinity points of $\overline{DF}$).

We have a similar map p in the case of the base field $\overline{\mathbb{K}}$, as well as a commutative diagram

$$\begin{array}{ccc} \overline{DF} = \overline{DF}_{\mathbb{K}} & \hookrightarrow & \overline{DF}_{\overline{\mathbb{K}}} \\ p \uparrow & & p \uparrow \\ \mathbb{P}^1_{\mathbb{K}} & \hookrightarrow & \mathbb{P}^1_{\overline{\mathbb{K}}} \end{array}$$

where the right vertical map p is a morphism of algebraic $\overline{\mathbb{K}}$-varieties defined over $\mathbb{K}$ it is even a normalization morphism of the algebraic $\overline{\mathbb{K}}$-curve $\overline{DF}_{\overline{\mathbb{K}}}$ ([2], Section 2; hence it is uniquely determined up to an automorphism of $\mathbb{P}^1_{\overline{\mathbb{K}}}$).

For the vertical maps p, we introduce two restrictions

$$\overline{p} = p|_{\mathbb{P}^1_{\mathbb{K}}\setminus\{0,\infty\}} : \mathbb{P}^1_{\mathbb{K}} \setminus \{0,\infty\} = \mathbb{K} \setminus \{0\} \to \overline{DF} \setminus \{O\}$$

resp.

$$\overline{p} = p|_{\mathbb{P}^1_{\overline{\mathbb{K}}\setminus\{0,\infty\}}} : \mathbb{P}^1_{\overline{\mathbb{K}}} \setminus \{0,\infty\} = \overline{\mathbb{K}} \setminus \{0\} \to \overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\}.$$

From the previous diagram it follows the following commutative diagram with bijective vertical maps:

$$\begin{array}{ccc} \overline{DF} \setminus \{O\} = \overline{DF}_{\mathbb{K}} \setminus \{O\} & \hookrightarrow & \overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\} \\ \overline{p} \uparrow\sim & & \sim\uparrow \overline{p} \\ \mathbb{P}^1_{\mathbb{K}} \setminus \{0,\infty\} = \mathbb{K} \setminus \{0\} & \hookrightarrow & \mathbb{P}^1_{\overline{\mathbb{K}}} \setminus \{0,\infty\} = \overline{\mathbb{K}} \setminus \{0\} \end{array}$$

where the right vertical map $\overline{p}$ is an isomorphism of algebraic $\overline{\mathbb{K}}$-varieties defined over $\mathbb{K}$.

If we transport by the vertical bijections $\overline{p}$ the natural group multiplicative laws from $\mathbb{K}\setminus\{0\}$ and $\overline{\mathbb{K}}\setminus\{0\}$, then we obtain the group composition laws $\cdot$ on $\overline{DF}\setminus\{O\} = \overline{DF}_{\mathbb{K}} \setminus \{0\}$ and $\overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\}$, defined by

$$(3at, 3at^2, 1+t^3) \cdot (3at', 3a(t')^2, 1+(t')^3) \overset{\text{def}}{=} (3a(tt'), 3a(t')^2, 1+(tt')^3)$$

for each $t, t' \in \mathbb{K} \setminus \{0\}$, resp. $t, t' \in \overline{\mathbb{K}} \setminus \{0\}$.

We have that both vertical map $\overline{p}$ from the last diagram are group isomorphisms. Since the right vertical map $\overline{p}$ is an isomorphism of algebraic $\overline{\mathbb{K}}$-varieties defined over $\mathbb{K}$ and $(\overline{\mathbb{K}} \setminus \{0\}, \cdot) = \mathbb{G}_{m,\overline{\mathbb{K}}}$ is an algebraic $\overline{\mathbb{K}}$-group defined over $\mathbb{K}$, it follows that $(\overline{DF}_{\overline{\mathbb{K}}} \setminus \{0\}, \cdot)$ is an algebraic $\overline{\mathbb{K}}$-group defined over $\mathbb{K}$ and the right map $\overline{p}$ is an isomorphism of such algebraic $\overline{\mathbb{K}}$-groups.

We have $\overline{DF} \setminus \{O\} = (\overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\})(\mathbb{K})$ and $(\overline{DF} \setminus \{O\}, \cdot)$ is a subgroup of $(\overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\}, \cdot)$, because $(\mathbb{K} \setminus \{0\}, \cdot)$ is a subgroup of $(\overline{\mathbb{K}} \setminus \{0\}, \cdot)$.

According to the previous Definitions 2.1 and 3.1, it follows that: (i) the pair $(\overline{DF} \setminus \{O\}, \cdot)$ is a canonic $\mathbb{K}$-group (i.e., a $\mathbb{K}$-group w.r.t $\overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\}$, according to Section 2, Example 4) and (ii) the map

$$\overline{p} : \mathbb{G}_{m,\mathbb{K}} = (\mathbb{K} \setminus \{0\} \xrightarrow{\sim} (\overline{DF} \setminus \{O\}, \cdot)$$

is an isomorphism of (canonic) $\mathbb{K}$-groups (see also Section 2, Example 1).

Therefore $(\overline{DF} \setminus \{O\}, \cdot) \simeq \mathbb{G}_{m,\mathbb{K}}$ is a $\mathbb{K}$-group of type $\mathbb{G}_{m,\overline{\mathbb{K}}}$.

Now, we can recall a second group composition law $\circ$ on $\overline{DF} \setminus \{O\} = \overline{DF}_{\mathbb{K}} \setminus \{O\}$ or on $\overline{DF}_{\overline{\mathbb{K}}}\setminus\{O\}$ defined in a similar way as $\cdot$ by means of another map $p' : \mathbb{P}^1_{\mathbb{K}} \to \overline{DF}$, resp. $p' : \mathbb{P}^1_{\overline{\mathbb{K}}} \to \overline{DF}_{\overline{\mathbb{K}}}$, defined by $p'(t) = (3at^2, 3at, 1+t^3)$ for each $t \in \mathbb{K} \setminus \{0\}$, resp. $t \in \overline{\mathbb{K}} \setminus \{0\}$ and $p'(\infty) = O = (0,0,1)$.

Let us introduce two restrictions

$$\overline{\overline{p}} = p'|_{\mathbb{P}^1_{\mathbb{K}}\setminus\{0,\infty\}} : \mathbb{P}^1_{\mathbb{K}} \setminus \{0,\infty\} = \mathbb{K} \setminus \{0\} \to \overline{DF} \setminus \{O\}$$

resp.

$$\overline{\overline{p}} = p'|_{\mathbb{P}^1_{\overline{\mathbb{K}}\setminus\{0,\infty\}}} : \mathbb{P}^1_{\overline{\mathbb{K}}} \setminus \{0,\infty\} = \overline{\mathbb{K}} \setminus \{0\} \to \overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\}.$$

The second composition law $\circ$ is defined by the following formula

$$(3at^2, 3at, 1+t^3) \circ (3a(t')^2, 3a(t'), 1+(t')^3)$$

$$\stackrel{\text{def}}{=} (3a(tt')^2, 3a(tt'), 1+(tt')^3).$$

As for the previous composition law $\cdot$, it follows that: (i) the pair $(\overline{DF} \setminus \{O\}, \circ)$ is a canonic $\mathbb{K}$-group (i.e., w.r.t. $\overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\}$); (ii) the map

$$\overline{\overline{p}} : \mathbb{G}_{m,\mathbb{K}} = (\mathbb{K} \setminus \{0\}, \cdot) \xrightarrow{\sim} (\overline{DF} \setminus \{O\}, \circ)$$

is a $\mathbb{K}$-group isomorphisms.

Now we can apply Theorem 2.2: on the set $\overline{DF} \setminus \{O\}$ there exist two canonic $\mathbb{K}$-group structures, $(\overline{DF} \setminus \{O\}, \cdot)$ and $(\overline{DF} \setminus \{O\}, \circ)$, having the same neutral element $\overline{p}(1) = \overline{\overline{p}}(1) = (3, 3, 2) = V$, (the vertex of $\overline{DF}$). According to Theorem 2.2, these two groups must coincide, i.e., they have the same composition law $\cdot = \circ$.

Two results concerning $\mathbb{K}$-groups (Theorems 2.2 and 3.2. (i)) permit to describe all canonic $\mathbb{K}$-group structures on $\overline{DF} \setminus \{O\} = \overline{DF}_{\mathbb{K}} \setminus \{O\}$ (in particular all algebraic $\mathbb{K}$-groups on $\overline{DF} \setminus \{O\} = \overline{DF}_{\overline{\mathbb{K}}} \setminus \{O\}$) in the case when $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed (cf.Section 2, Remark (1)), as well as their "nice" parametrizations.

Theorem 5.1 Let $\mathbb{K}$ be an arbitrary field (not necessarily algebraically closed) with $\operatorname{char.}(\mathbb{K}) \neq 3$ and $E \in \overline{DF} \setminus \{O\} = \overline{DF}_{\mathbb{K}} \setminus \{O\}$. Then (i) there exists a unique canonic $\mathbb{K}$-group $(\overline{DF} \setminus \{O\}, \cdot_E)$ having the neutral element E; (ii) for each pair $P, Q \in \overline{DF} \setminus \{O\}$, we have $P \cdot Q = P \cdot Q \cdot E^{-1}$, with E^{-1} the symmetric/opposite of E in the group $(\overline{DF} \setminus \{O\}, \cdot)$; (iii) there exists at most two parametrizations of $\overline{DF} \setminus \{O\}$

$$\overline{p}_E, \overline{\overline{p}}_E : \mathbb{G}_{m,\mathbb{K}} \rightrightarrows (\overline{DF} \setminus \{O\}, \cdot_E)$$

which are isomorphisms of canonic $\mathbb{K}$-groups. These parametrizations are distinct iff $\mathbb{K} \neq \mathbb{Z}_2$. For each $t \in \mathbb{K} \setminus \{0\}$, we have

$$\overline{p}_E(t) = \overline{p}(t) \cdot E, \overline{\overline{p}}_E(t) = \overline{\overline{p}}(t) \cdot E$$

(with $\overline{p}, \overline{\overline{p}} : \mathbb{K} \setminus \{0\} \rightrightarrows \overline{DF} \setminus \{O\}$ previously considered).

We can obtain explicit formulae for $\cdot_E$, $\overline{p}_E$, $\overline{\overline{P}}_E$. For instance, if

$$E = (3a\lambda, 3a\lambda^2, 1+\lambda^3) = (\frac{3a}{\lambda^2}, \frac{3a}{\lambda}, \frac{1}{\lambda^3} + 1) \in \overline{DF}_{\mathbb{K}} \setminus \{O\},$$

with $\lambda \in \mathbb{K} \setminus \{0\}$ (uniquely determined), then, for each $t, t' \in \mathbb{K} \setminus \{0\}$, we have

$$(3at, 3at^2, 1+t^3) \cdot_E (3at', 3at'^2, 1+t'^3)$$

$$= \left(3a\,\frac{tt'}{\lambda}, 3a\left(\frac{tt'}{\lambda}\right)^2, 1+\left(\frac{tt'}{\lambda}\right)^3\right) = (3a\lambda^2(tt'), 3a\lambda(tt')^2, \lambda^3 + (tt')^3,$$

$$\overline{p}_E(t) = (3a\lambda t, 3a(\lambda t)^2, 1+(\lambda t)^3),$$

$$\overline{\overline{p}}_E(t) = \left(\frac{3at^2}{\lambda^2}, \frac{3at}{\lambda}, 1+\frac{t^3}{\lambda^3}\right) = (3a\lambda t^2, 3a\lambda^2 t, \lambda^3 + t^3).$$

Remarks. (1) We have $\lambda = 1$ iff $E = V = (3a, 3a, 2)$ (the "vertex" of $\overline{DF}$). Then $(\overline{DF} \setminus \{O\}, \cdot_V)$ is the previous $\mathbb{K}$-group $(\overline{DF} \setminus \{O\}, \cdot)$. (2) We have $\lambda = -1$ iff $E = I = (-1, 1, 0)$ (one of the infinity point of $\overline{DF}$). Then $(\overline{DF} \setminus \{O\}, \cdot_I)$ is the group considered in the paper [9].

Now let $P_1, ..., P_n \in \overline{DF} \setminus \{O\} = \overline{DF}_{\mathbb{K}} \setminus \{O\}$ and $Q_i = \overline{p}^{-1}(P_i) \in \mathbb{K} \setminus \{0\} \subset \mathbb{P}^2_{\mathbb{K}}$, for each $i = 1, ..., n$. For the rational $\mathbb{K}$-points subset, we have

$$(\overline{DF}_{\overline{\mathbb{K}}} \setminus \{O, P_1, ..., P_n\})(\mathbb{K}) = \overline{DF}_{\mathbb{K}} \setminus \{O, P_1, ..., P_n\}$$

and a commutative diagram

$$\begin{array}{ccc} \overline{DF}_{\mathbb{K}} \setminus \{O, P_1, ..., P_n\} & \hookrightarrow & \overline{DF}_{\overline{\mathbb{K}}} \setminus \{O, P_1, ..., P_n\} \\ \sim\uparrow \overline{p} & & \sim\uparrow \overline{p} \\ \mathbb{P}^1_{\mathbb{K}} \supset \mathbb{K} \setminus \{O, Q_1, ..., Q_n\} & \hookrightarrow & \overline{\mathbb{K}} \setminus \{O, Q_1, ..., Q_n\} \subset \mathbb{P}^1_{\overline{\mathbb{K}}} \end{array}$$

According to Theorem 4.1, the set $\mathbb{K} \setminus \{O, Q_1, ..., Q_n\}$ does not admit a $\mathbb{K}$-group structure, w.r.t. $\overline{C} = \overline{\mathbb{K}} \setminus \{O, Q_1, ..., Q_n\} = \mathbb{P}^1_{\overline{\mathbb{K}}} \setminus \{O, Q_1, ..., Q_n\}$, called *canonic* $\mathbb{K}$-*group structure*, cf. Section 2, Example (3). It follows

Proposition 5.1 Let $\mathbb{K}$ be a field with $\mathrm{char.}\,\mathbb{K} \neq 3$ and $n \in \mathbb{N} \setminus \{0\}$. Then for $P_1, ..., P_n \in \overline{DF}_{\mathbb{K}} \setminus \{0\}$, the subset $\overline{DF}_{\mathbb{K}} \setminus \{O, P_1, ..., P_n\}$ does not admit a structure of canonic $\mathbb{K}$-group (i.e., a $\mathbb{K}$-group w.r.t. the algebraic $\overline{\mathbb{K}}$-curve $\overline{C} = \overline{DF}_{\overline{\mathbb{K}}} \setminus \{O, P_1, ..., P_n\}$).

6.1 Geometric interpretations

The algebraic subset $\overline{DF} = \overline{DF}_{\mathbb{K}} \subset \mathbb{P}^2_{\mathbb{K}}$ has "few" points if the base field is "small". For instance, if $\mathbb{K} = \mathbb{Z}_2$ and $a = 1 = -1 \in \mathbb{Z}_2$, then $\overline{DF} = \{O = (0, 0, 1), I = (1, 1, 0)\}$.

However we can consider the intersections of $\overline{DF} = \overline{DF}_{\mathbb{K}} = \mathbf{V}(F)$, where $F = X^3 + Y^3 - 3aXYZ \in \mathbb{K}[X, Y, Z]$ and $a \in \mathbb{K} \setminus \{0\}$, with a straight line $\overline{d}_{\mathbb{K}} \subset \mathbb{P}^2_{\mathbb{K}}$, together their *multiplicities*. Namely, if $P \in \overline{DF}_{\mathbb{K}} \cap \overline{d}_{\mathbb{K}} \subseteq \overline{DF}_{\overline{\mathbb{K}}} \cap \overline{d}_{\overline{\mathbb{K}}}$, where $\overline{d}_{\overline{\mathbb{K}}} \subset \mathbb{P}^2_{\overline{\mathbb{K}}}$ is the projective closure of $\overline{d}_{\mathbb{K}}$ in $\mathbb{P}^2_{\overline{\mathbb{K}}}$, we define the *multiplicity* $m(P; \overline{DF}_{\mathbb{K}}, \overline{d}_{\mathbb{K}})$ of the point P in the intersection $\overline{DF}_{\mathbb{K}} \cap \overline{d}_{\mathbb{K}}$ by

$$m(P; \overline{DF}_{\mathbb{K}}, \overline{d}_{\mathbb{K}}) \stackrel{\text{def}}{=} m(P; \overline{DF}_{\overline{\mathbb{K}}}, \overline{d}_{\overline{\mathbb{K}}}),$$

where the last term is the multiplicity of P in the intersection of the *algebraic* $\overline{\mathbb{K}}$-*subvarieties* $\overline{DF}_{\overline{\mathbb{K}}}$, $\overline{d}_{\overline{\mathbb{K}}} \subset \mathbb{P}^2_{\overline{\mathbb{K}}}$.

Comment. The number $m(P; \overline{DF}_{\mathbb{K}}, \overline{d}_{\mathbb{K}})$ could be more correctly denoted by $m(P; F, \overline{d}_{\mathbb{K}})$ because it depends on the polynomial F. In fact, by definition $m(P; F, \overline{d}_{\mathbb{K}})$ depends on the subset $\overline{DF}_{\overline{\mathbb{K}}} \subset \mathbb{P}^2_{\overline{\mathbb{K}}}$ and the determination of this subset is equivalent with determination of the polynomial $F \in \overline{\mathbb{K}}[X, Y, Z]$ up to a multiplicative constant, because $\overline{\mathbb{K}}$ is algebraically closed (cf. *Hilbert Nullstellensatz*).

In the previous conditions, if $P \in \overline{DF}_{\mathbb{K}} \cap \overline{d}_{\mathbb{K}}$, we have $m(P; \overline{DF}_{\mathbb{K}}, \overline{d}_{\mathbb{K}}) \leq 3$, according to the classic multiplicity theory in $\mathbb{P}^2_{\overline{\mathbb{K}}}$. If $m(P; \overline{DF}_{\mathbb{K}}, \overline{d}_{\mathbb{K}}) \geq 2$, we will say that the straight line $d_{\mathbb{K}}$ is *tangent* to $\overline{DF}_{\mathbb{K}}$ at the point P.

The following intersection property is true.

Proposition 5.2 Let $\mathbb{K}$ be an arbitrary field (not necessarily algebraically closed) with $\mathrm{char.}\,\mathbb{K} \neq 3$. If $\ell \subset \mathbb{K}^2_{\mathbb{K}}$ is a straight line intersecting $\overline{DF}_{\mathbb{K}}$ in two points (counted with multiplicities), then ℓ intersects $\overline{DF}_{\mathbb{K}}$ in a third point (counted with multiplicity).

The intersection property permits to state the following Theorem which establishes the close relation between the canonic $\mathbb{K}$-group structures on $\overline{DF}\setminus\{O\}$ and a geometric rule of defining its composition law like the well known classic geometric rule defining the group composition laws on *elliptic curves* (see [12]).

Theorem 5.2 Let $\mathbb{K}$ be an arbitrary field with $\mathrm{char.}\,\mathbb{K} \neq 3$, a composition law $\perp$ on $\overline{DF}_{\mathbb{K}} \setminus \{O\}$ and $E \in \overline{DF}_{\mathbb{K}} \setminus \{O\}$. Then the following two assertions are equivalent: (i) the pair $(\overline{DF}_{\mathbb{K}} \setminus \{O\}, \perp)$ is a canonic $\mathbb{K}$-group and E is its neutral element; (ii) the composition law $\perp$ is defined by the following geometric rule: for each $P_1, P_2 \in \overline{DF}_{\mathbb{K}} \setminus \{O\}$ distinct (resp. not distinct) points; (ii_1) let $\ell = \overline{P_1P_2} \subset \mathbb{P}^2_{\mathbb{K}}$ be the straight line passing through P_1, P_2 (resp. tangent line to $\overline{DF}_{\mathbb{K}}$ at the point $P_1 = P_2$) and $P_3 \in \overline{DF}_{\mathbb{K}} \setminus \{O\}$ the third intersection point of ℓ with $\overline{DF}_{\mathbb{K}} \setminus \{O\}$ (counted with multiplicity); (ii_2) let $\ell' = \overline{EP_3} \subset \mathbb{P}^2_{\mathbb{K}}$ be the straight line passing through E, P_3 if $P_3 \neq E$, or tangent line to $\overline{DF}_{\mathbb{K}}$ at $P_3 = E$ if $P_3 = E$, and let P be the third intersection point of ℓ' with $\overline{DF}_{\mathbb{K}} \setminus \{O\}$; (iii_3) then $P_1 \perp P_2 = P$.

Particular cases. In Theorem 5.2 above, suppose that $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed, resp. $\mathbb{K} = \overline{\mathbb{K}} = \mathbb{C}$. Then we can replace the assertion (i) of the Theorem with "the pair $(\overline{DF}_{\mathbb{K}} \setminus \{O\}, \perp)$ is an algebraic $\mathbb{K}$-group and E is its neutral element", resp. "the pair $(\overline{DF}^{an}_{\mathbb{C}} \setminus \{O\}, \perp)$ is a Lie $\mathbb{C}$-group and E is its neutral element".

In fact, if $\mathbb{K}$ is algebraically closed, then $(\overline{DF}_{\mathbb{K}} \setminus \{O\}, \perp)$ is a canonic $\mathbb{K}$-group iff it is an algebraic $\mathbb{K}$-group (cf. Section 2, Remark 1)). If $\mathbb{K} = \mathbb{C}$, then $(\overline{DF}_{\mathbb{C}} \setminus \{O\}, \perp)$ is an algebraic $\mathbb{C}$-group iff $(\overline{DF}^{an}_{\mathbb{C}} \setminus \{O\}, \perp)$ is a Lie $\mathbb{C}$-group (cf. Corollary 2.2).

7 Comments

Group structures on Descartes Folium, invoked in this lecture, are of practical interest in Codes Theory / Cryptography. In affine coordinates, we mention that the family of generalized Hessians $H_{a,b,c} : bx^3 + y^3 + c = axy$ include both the Descartes Folium $H_{a,1,0}$, $a \neq 0$ and other cubical curves $H_{a,b,c}$, regular or not. The applications of such curves in cryptography are of recent date, but, a serious research, must involve our results published in the papers [2] [3] [9] [14], regarding the rich group structure of Descartes Folium. The unified multiplication formulas make generalized Hessian curves interesting against "side-channel attacks".

The proofs of the statements from this exposition are presented in the manuscript [3], which will appear soon in ArXiv. It is expected that some analogous results concerning "good" group composition laws on other plane projective non-smooth cubics could be establish with similar methods over an arbitrary base field $\mathbb{K}$ with $\mathrm{char.}\,\mathbb{K} \neq 3$.

Acknowledgements. This exposition is based on our invited lecture at "The 12-th International Workshop on Differential Geometry and Its Applications (DGA2015)" held at Petroleum-Gas University of Ploieşti, Romania, September 23-26, 2015. This lecture has been dedicated to the memory of *Prof. Dr. Doc. Leon Livovschi* (1921-2012)- one of the founder professors of the Petroleum-Gas Institute - Ploieşti, Romania.

References

[1] A. Borel, *Linear Algebraic Groups*, Princeton, 1969.

[2] A. Constantinescu, C. Udriste, S. Pricopie, *Classic and special Lie groups structures on some plane cubic curves with singularities. I*, ROMAI J., 10, 2 (2014), 75-88.

[3] A. Constantinescu, C. Udriste, S. Pricopie, *Genome of Descartes Folium via normalization*, manuscript, The VIII-th International Conference of Differential Geometry and Dynamical Systems (DGDS-2014), 1 - 4 September 2014 at the Callatis High-School in the city Mangalia - Romania, to appear in ArXiv.

[4] A. Grothendieck, *Elements de Geometrie Algebrique*, IHES Sci. Publ. Math., I-IV, 1960-1967 (EGA).

[5] A. Grothendieck, M. Demazure, *Schemas en Groupes*, Seminaire de Geometrie algebrique du Bois Marie 1962/1964 (SGA 3).

[6] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[7] Yu. I. Merzliakov, *Rational groups* (in Russian), Nauka, Moskow, 1980.

[8] J. S. Milne, *Algebraic Groups. An introduction to the theory of algebraic groups over fields*, Draft, September 20, 2014;
http://www.jmilne.org/math/Course Notes/iAG.pdf

[9] S. Pricopie, C. Udriste, *Multiplicative group law on the Folium of Descartes*, Balkan J. Geom. Appl., 18, 1 (2013), 57-73.

[10] N. Radu, *Local Rings. I* (in Romanian), Romanian Acad. Publ. House, 1968.

[11] I. R. Shafarevich, *Basic Algebraic Geometry*, Springer, 1977.

[12] J. H. Silverman, *Advanced Topics in the Arthmetic of Elliptic Curves*, Springer, 1994.

[13] *The Stacks Project, version* 75c3e41*, Varieties*, Columbia University, 2014;
http://stacks.math.columbia.edu/download/varieties.pdf

[14] C. Udrişte, A. Constantinescu, S. Pricopie, *Topology and differential structure on Descartes Folium*, Ann. Sofia Univ., Fac. Math. and Inf., 103 (2016), 1-9.

Authors' addresses:

Adrian Constantinescu
Institute of Mathematics "Simion Stoilov" of Romannian Academy,
Calea Grivitei 21, P.O. BOX 1-764,
Bucharest 010702, Romania.
E-mail: Adrian.Constantinescu@imar.ro

Constantin Udrişte, Steluta Pricopie
University Politehnica of Bucharest,
Faculty of Applied Sciences,
Department of Mathematics - Informatics,
Splaiul Independenţei 313, RO-060042, Bucharest, Romania.
E-mail: udriste@mathem.pub.ro ; mati_star@yahoo.com