mathematics

MDPI

Article

Derived Hyperstructures from Hyperconics

Vahid Vahedi [1], Morteza Jafarpour [1,*,†], Sarka Hoskova-Mayerova [2], Hossein Aghabozorgi [1], Violeta Leoreanu-Fotea [3] and Svajone Bekesiene [4]

1 Department of Mathematics, Vali-e-Asr University of Rafsanjan, Rafsanjan 7718897111, Iran; v.vahedi@vru.ac.ir (V.V.); h.aghabozorgi@vru.ac.ir (H.A.)
2 Department of Mathematics and Physics, University of Defence in Brno, Kounicova 65, 662 10 Brno, Czech Republic; sarka.mayerova@unob.cz
3 Department of Mathematics, Al. I. Cuza University, 6600 Iashi, Romania; violeta.fotea@uaic.ro
4 Departament of Defence Technologies, The General Jonas Žemaitis Military Academy of Lithuania, Silo g.5, 10322 Vilnius, Lithuania; svajone.bekesiene@lka.lt
* Correspondence: m.j@vru.ac.ir
† The corresponding author in deep gratitude dedicates this work and gives special thanks to Cardiovascular Surgeon A. R. Alizadeh Ghavidel.

Received: 26 January 2020; Accepted: 11 March 2020; Published: 16 March 2020

Abstract: In this paper, we introduce generalized quadratic forms and hyperconics over quotient hyperfields as a generalization of the notion of conics on fields. Conic curves utilized in cryptosystems; in fact the public key cryptosystem is based on the digital signature schemes (DLP) in conic curve groups. We associate some hyperoperations to hyperconics and investigate their properties. At the end, a collection of canonical hypergroups connected to hyperconics is proposed.

Keywords: hypergroup; hyperring; hyperfield; (hyper)conics; quadratic forms

MSC: 20N20; 14H52; 11G05

1. Introduction

In 1934, Marty initiated the notion of hypergroups as a generalization of groups and referred to its utility in solving some problems of groups, algebraic functions and rational fractions [1]. To review this theory one can study the books of Corsini [2], Davvaz and Leoreanu-Fotea [3], Corsini and Leoreanu [4], Vougiouklis [5] and in papers of Hoskova and Chvalina [6] and Hoskova-Mayerova and Antampoufis [7]. In recent years, the connection of hyperstructures theory with various fields has been entered into a new phase. For this we advise the researchers to see the following papers. (i) For connecting it to number theory, incidence geometry, and geometry in characteristic one [8–10]. (ii) For connecting it to tropical geometry, quadratic forms [11,12] and real algebraic geometry [13,14]. (iii) For relating it to some other objects see [15–19]. M. Krasner introduced the concept of the hyperfield and hyperring in Algebra [20,21]. The theory which was developed for the hyperrings is generalizing and extending the ring theory [22–25]. There are different types of hyperrings [22,25,26]. In the most general case a triplet $(R, +, \cdot)$ is a hyperring if $(R, +)$ is a hypergroup, $(R, \cdot)$ is a semihypergroup and the multiplication is bilaterally distributive with regards to the addition [3]. If $(R, \cdot)$ is a semigroup instead of semihypergroup, then the hyperring is called additive. A special type of additive hyperring is the Krasner's hyperring and hyperfield [20,21,24,27,28]. The construction of different classes of hyperrings can be found in [29–33]. There are different kinds of curves that basically are used in cryptography [34,35]. An elliptical curve is a curve of the form $y^2 = p(x)$, where $p(x)$ is a cubic polynomial with no-repeat roots over the field F. This kind of curves are considered and extended over Krasner's hyperfields in [13]. Now let $g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f \in F[x, y]$ and

$g(x,y) = 0$ be the quadratic equation of two variables in field of F, if $a = c = 0$ and $b \neq 0$ then the equation $g(x,y) = 0$ is called homographic transformation. In [14] Vahedi et. al extended this particular quadratic equation on Krasner's quotient hyperfield $\frac{F}{G}$. The motivation of this paper goes in the same direction of [14]. If in the general form of the equation of quadratic form one suppose that $ae \neq 0$ and $b = 0$ then initiate an important quadratic equation which is called a conic. Notice that the conditions which are considered for the coefficients of the equations of a conic curve and a homographic curve are completely different. Until now the study of conic curves has been on fields. At the recent works the authors have investigated some main classes of curves; elliptic curves and homographics over Krasner's hyperfields (see [13,14]). In the present work, we study the conic curves over some quotients of Krasner's hyperfields.

2. Preliminaries

In the following, we recall some basic notions of Pell conics and hyperstructures theory that these topics can be found in the books [2,36,37]. Moreover, we fix here the notations that are used in this paper.

2.1. Conics

According to [36] a conic is a plane affine curve of degree 2. Irreducible conics C come in three types: we say that C is a hyperbola, a parabola, or an ellipse according as the number of points at infinity on (the projective closure of) C equals $2, 1$, or 0. Over an algebraically closed field, every irreducible conic is a hyperbola. Let d be a square free integer nonequal to 1 and put

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \pmod 4, \\ \\ 4d & \text{if } d \equiv 2,3 \pmod 4. \end{cases}$$

The conic $C : Q_0(x,y) = 1$ associated to the principal quadratic form of discriminant Δ,

$$Q_0(x,y) = \begin{cases} x^2 + xy + \frac{1-d}{4}y^2 & \text{if } d \equiv 1 \pmod 4, \\ \\ x^2 - dy^2 & \text{if } d \equiv 2,3 \pmod 4, \end{cases}$$

is called the *Pell conic* of discriminant. Pell conics are irreducible nonsingular affine curves with a distinguished integral point N = (1, 0). The problem corresponding to the determination of E(Q) is finding the integral points on a Pell conic. The idea that certain sets of points on curves can be given a group structure is relatively modern. For elliptic curves, the group structure became well known only in the 1920s; implicitly it can be found in the work of Clebsch, and Juel, in a rarely cited article, wrote down the group law for elliptic curves defined over $\mathbb{R}$ and $\mathbb{C}$ at the end of the 19th century. The group law on Pell conics defined over a field F. For two rational points $p, q \in Q(F)$, draw the line through $\mathcal{O}$ parallel to line p, q, and denote its second point of intersection with $p * q$ which is the sum of two p, q, where $\mathcal{O}$ is an arbitrary point in pell conic perchance in infinity, is identity element of group. In the Figure 1 the operation is picturised on the conic section $Q_{\mathbb{R}}(f_{1,1})$.

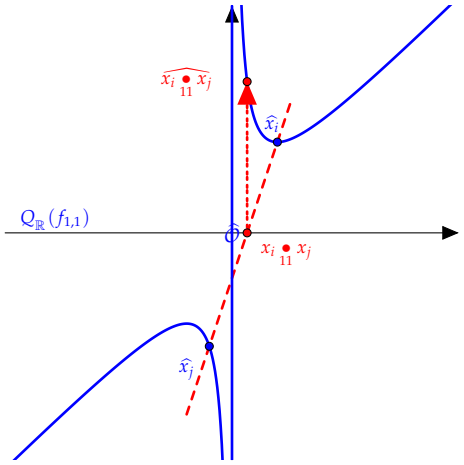

Figure 1. Conic section $Q_{\mathbb{R}}(f_{1,1})$.

Example 1. *Consider* $f_{1,1}(x) = x^{-1} + x$ *over finite field* $F = \mathbb{Z}_7$. *Then we have a Caley table of points (Table 1):*

Table 1. Conic group $(Q_{\mathbb{Z}_7}(f_{1,1}), \bullet_{a,b})$.

$\bullet_{11}$	$(0,\infty)$	$(1,2)$	$(2,-1)$	$(3,1)$	$(-3,-1)$	$(-2,1)$	$(-1,-2)$	(∞,∞)
$(0,\infty)$	$(0,\infty)$	$(1,2)$	$(2,-1)$	$(3,1)$	$(-3,-1)$	$(-2,1)$	$(-1,-2)$	(∞,∞)
$(1,2)$	$(1,2)$	$(-1,-2)$	$(-3,-1)$	$(-2,1)$	$(3,1)$	$(2,-1)$	$(0,\infty)$	(∞,∞)
$(2,-1)$	$(2,-1)$	$(-3,-1)$	$(1,2)$	$(-1,-2)$	(∞,∞)	$(0,\infty)$	$(-2,1)$	$(3,1)$
$(3,1)$	$(3,1)$	$(-2,1)$	$(-1,-2)$	$(1,2)$	$(0,\infty)$	(∞,∞)	$(-3,-1)$	$(2,-1)$
$(-3,-1)$	$(-3,-1)$	$(3,1)$	(∞,∞)	$(0,\infty)$	$(-1,-2)$	$(1,2)$	$(2,-1)$	$(-2,1)$
$(-2,1)$	$(-2,1)$	$(2,-1)$	$(0,\infty)$	(∞,∞)	$(1,2)$	$(-1,-2)$	$(3,1)$	$(-3,-1)$
$(-1,-2)$	$(-1,-2)$	$(0,\infty)$	$(-2,1)$	$(-3,-1)$	$(2,-1)$	$(3,+1)$	(∞,∞)	$(1,2)$
(∞,∞)	(∞,∞)	$(-1,-2)$	$(3,1)$	$(2,-1)$	$(-2,+1)$	$(-3,-1)$	$(1,2)$	$(0,\infty)$

The associativity of the group law is induced from a special case of Pascal's Theorem. In the following, we recall Pascal's Theorem which is a very special case of Bezout's Theorem.

Theorem 1 ([38] Pascal's Theorem). *For any conic and any six points* $p_1, p_2, ..., p_6$ *on it, the opposite sides of the resulting hexagram, extended if necessary, intersect at points lying on some straight line. More specifically, let* $L(p,q)$ *denote the line through the points* p *and* q. *Then the points* $L(p_1,p_2) \cap L(p_4,p_5)$, $L(p_2,p_3) \cap L(p_5,p_6)$, *and* $L(p_3,p_4) \cap L(p_6,p_1)$ *lie on a straight line, called the Pascal line of the hexagon Figure 2.*

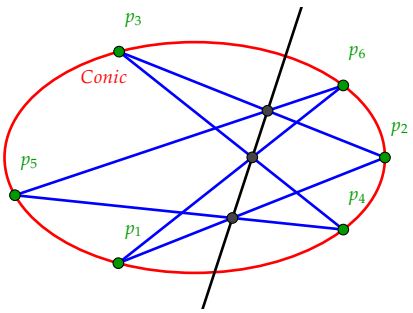

Figure 2. Pascal line of the hexagon.

2.2. *Krasner's Hyperrings and Hyperfields*

Let H be a non-empty set and $\mathcal{P}^*(H)$ denotes the set of all non-empty subsets of H. Any function $\cdot$ from the cartesian product $H \times H$ into $\mathcal{P}^*(H)$ is called a hyperoperation on H. The image of the

pair $(a, b) \in H \times H$ under the hyperoperation $\cdot$ in $\mathcal{P}^*(H)$ is denoted by $a \cdot b$. The hyperoperation can be extended in a natural way to subsets of H as follows: for non-empty subsets A, B of H, define $A \cdot B = \bigcup_{a \in A, b \in B} a \cdot b$. The notation $a \cdot A$ is applied for $\{a\} \cdot A$ and also $A \cdot a$ for $A \cdot \{a\}$. Generally, we mean $H^k = H \times H ... \times H$ (k times), for all $k \in \mathbb{N}$ and also the singleton $\{a\}$ is identified with its element a. The hyperstructure $(H, \cdot)$ is called a semihypergroup if $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in H$, which means that

$$\bigcup_{u \in x \cdot y} u \cdot z = \bigcup_{v \in y \cdot z} x \cdot v.$$

A semihypergroup $(H, \cdot)$ is called a hypergroup if the reproduction law holds: $x \cdot H = H \cdot x = H$, for all $x \in H$.

Definition 1 ([2]). *Let $(H, \cdot)$ be a hypergroup and K be a non-empty subset of H. We say that $(K, \cdot)$ is a subhypergroup of H and it denotes $K \leqslant H$, if for all $x \in K$ we have $K \cdot x = K = x \cdot K$.*

Let $(H, \cdot)$ be a hypergroup, an element e_r (resp. e_l) of H is called a right identity (resp. left identity e_l) if for all $a \in H$, $x \in a \cdot e_r$ (resp. $a \in e_l \cdot a$). An element e is called an identity if, for all $a \in H$, $a \in a \cdot e \cap e \cdot a$. A right identity e_r (resp. left identity e_l) of H is called a scalar right identity (resp. scalar left identity) if for all $a \in H$, $a = a \cdot e_r$ ($a = e_l \cdot x$). An element e is called a scalar identity if for all $a \in H$, $a = a \cdot e = e \cdot x$. An element $a' \in H$ is called a right inverse (resp. left inverse) of a in H if $e_r \in a \cdot a'$, for some right identities e_r in H ($e_l \in a' \cdot a$). An element $a' \in H$ is called an inverse of $a \in H$ if $e \in a' \cdot a \cap a \cdot a'$, for some identities in H. We denote the set of all right inverses, left inverses and inverses of $a \in H$ by $i_r(a)$, $i_l(a)$, and $i(a)$, respectively.

Definition 2 ([2]). *A hypergroup $(H, \cdot)$ is called reversible, if the following conditions hold:*

(i) *At least H has one identity e;*
(ii) *every element x of H has one inverse, that is $i(x) \neq \emptyset$;*
(iii) *$x \in y \cdot z$ implies that $y \in x \cdot z'$ and $z \in y' \cdot x$, where $z' \in i(z)$ and $y' \in i(y)$.*

Definition 3 ([2,23]). *A hypergroup $(H, +)$ is called canonical, if the following conditions hold:*

(i) *for every $x, y, z \in H, x + (y + z) = (x + y) + z$,*
(ii) *for every $x, y \in H, x + y = y + x$,*
(iii) *there exists $0 \in H$ such that $0 + x = \{x\}$ for every $x \in H$,*
(iv) *for every $x \in H$ there exists a unique element $x' \in H$ such that $0 \in x + x'$; (we shall write $-x$ for x' and we call it the opposite of x.)*
(v) *$z \in x + y$ implies $y \in z - x$ and $x \in z - y$;*

Definition 4 ([2]). *Suppose that $(H, \cdot)$ and $(K, \circ)$ are two hypergroups. A function $f : H \to K$ is called a homomorphism if $f(x \cdot y) \subseteq f(x) \circ f(y)$, for all x and y in H. We say that f is a good homomorphism if for all x and y in H, $f(x \cdot y) = f(x) \circ f(y)$.*

The more general hyperstructure that satisfies the ring-like conditions is the hyperring. The notion of the hyperring and hyperfield was introduced in Algebra by M. Krasner in 1956 [21]. According to the current terminology, these initial hypercompositional structures are additive hyperrings and hyperfields whose additive part is a canonical hypergroup. Nowadays such hypercompositional structures are called Krasner's hyperrings and hyperfields.

Definition 5 ([20]). *A Krasner's hyperring is an algebraic structure $(R, +, \cdot)$ which satisfies the following axioms:*

(1) *$(R, +)$ is a canonical hypergroup,*

(2) $(R, \cdot)$ *is a semigroup having zero as a bilaterally absorbing element, i.e.,* $x \cdot 0 = 0 \cdot x = 0$.
(3) The multiplication is distributive with respect to the hyperoperation $+$.

A Krasner's hyperring is called commutative if the multiplicative semigroup is a commutative monoid. A Krasner's hyperring is called a *Krasner's hyperfield*, if $(R - \{0\}, \cdot)$ is a commutative group. In [20] Krasner presented a class of hyperrings which is constructed from rings. He proved that if R is a ring and G is a normal subgroup of R's multiplicative semigroup, then the multiplicative classes $\bar{x} = xG, x \in R$, form a partition of R. He also proved that the product of two such classes, as subsets of R, is a class *mod* G as well, while their sum is a union of such classes. Next, he proved that the set $\bar{R} = \frac{R}{G}$ of these classes becomes a hyperring, when:

(i) $xG \oplus yG = \{zG | z \in xG + yG\}$, and
(ii) $xG \odot yG = xyG$,

Moreover, he observed that if R is a field, then $\frac{R}{G}$ is a hyperfield. Krasner named these hypercompositional structures quotient hyperring and quotient hyperfield, respectively. At the same time, he raised the question if there exist non-quotient hyperrings and hyperfields [20]. Massouros in [27] generalized Krasner's construction using not normal multiplicative subgroups, and proved the existence of non-quotient hyperrings and hyperfields. Since the paper deals only with Krasner's hyperfields we will write simply quotient hyperfields instead of Krasner's quotient hyperfields.

3. Hyperconic

The notion of hyperconics on a quotient hyperfield will be studied in this section. By the use of hyperconic $Q_{\bar{F}}(f_{\bar{A},\bar{B}})$, we present some hyperoperations as a generalization group operations on fields. We investigate some attributes of the associated hypergroups from the hyperconics and the associated H_v-groups on the hyperconics.

Let $g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f \in F[x, y]$ and $g(x, y) = 0$ be the quadratic equation of two variables in field of F. If $c = 0$ and equation $g(x, y) = 0$ still stay in quadratic and two variables or the other word $c = 0$ and $(a, b) \neq 0 \neq (e, b)$, then it can be calculated as an explicit function y in terms of x, also with a change of variables, can be expressed in the form of $Y = AX^2 + BX$ or $AX^{-1} + BX$, where $A, B \in F$.

For this purpose if $a, e \neq 0 = b$ set $x = X$ and $y = Y - fe^{-1}$ then $Y = AX^2 + BX$, where $A = -ae^{-1}, B = -de^{-1}$. If $b \neq 0 = a$ set $x = X - eb^{-1}$ and $y = Y - db^{-1}$ then $Y = AX^{-1}$, where $A = edb^{-2} - fb^{-1}$. If $b \neq 0 \neq a$ set $x = X - eb^{-1}$ and $y = Y + 2aeb^{-2}\alpha_{_F} - db^{-1}$ that

$$\alpha_{_F} = \begin{cases} 0, & \text{if } char(F) = 2 \\ 1, & \text{if } char(F) \neq 2, \end{cases}$$

then $Y = AX^{-1} + BX$, where $A = -ae^2b^{-3} + edb^{-2} - fb^{-1}$ and $B = -ab^{-1}$. Reduced quadratic equation of two variables $ax^2 + bxy + dx + ey + f = 0$ in field of F can be generalized in quotient hyperfield $\bar{F}$.

Definition 6. *Let* $\bar{F}$ *be the quotient hyperfield and* $(\bar{A}, \bar{B}) \in \bar{F}^2$ *and* $f_{\bar{A},\bar{B}}(\bar{x})$ *be equal to* $\bar{A}\bar{x}^{-1} \oplus \bar{B}\bar{x}$ *or* $\bar{A}\bar{x}^2 \oplus \bar{B}\bar{x}$. *Then the relation* $\bar{y} \in f_{\bar{A},\bar{B}}(\bar{x})$, *is called generalized reduced two variable quadratic equation in* $\bar{F}^2$. *Moreover the set* $Q(f_{\bar{A},\bar{B}}, \bar{F}) = \{(\bar{x}, \bar{y}) \in \bar{F}^2 | \bar{y} \in f_{\bar{A},\bar{B}}(\bar{x})\}$ *is called conic hypersection, and if* $\bar{A} \neq 0$, $Q(f_{\bar{A},\bar{B}}, \bar{F})$ *is named non-degenerate conic hypersection. For all* $a \in \bar{A}$ *and* $b \in \bar{B}$, $Q(f_{a,b}, F) = \{(x, y) \in F^2 | y = f_{a,b}(x)\}$ *is conic section and for* $a \neq 0$ *is non-degenerate conic section, in which* $f_{a,b}(z) = az^2 + bz$ *or* $az^{-1} + bz$ *corresponding to* $f_{\bar{A},\bar{B}}$. *It is also said to* $Q(f_{\bar{A},\bar{B}}, F) = \bigcup_{(\bar{x},\bar{y}) \in Q(f_{\bar{A},\bar{B}}, \bar{F})} \bar{x} \times \bar{y}$, *conic hypersection, as a subset of* F^2, *and* $Q(f_{a,b}, \bar{F}) = \overline{Q(f_{a,b}, F)} = \left\{ \overline{(x, y)} | (x, y) \in Q(f_{a,b}, F) \right\}$, *where*

$\overline{(x,y)} = (\bar{x},\bar{y})$ *for all* $(x,y) \in Q(f_{\bar{A},\bar{B}}, F)$.

Theorem 2. *Using the above notions we have* $Q(f_{\bar{A},\bar{B}}, F) = \bigcup\limits_{a\in\bar{A},b\in\bar{B}} Q(f_{a,b}, F)$.

Proof. Let $(x,y) \in Q(f_{\bar{A},\bar{B}}, F)$ and without losing of generality $f(x) = Ax^2 + Bx$. Then

$$\begin{aligned}
(\bar{x},\bar{y}) \in Q(f_{\bar{A},\bar{B}}, \bar{F}) &\iff \bar{y} \in \bar{A}\bar{x}^2 \oplus \bar{B}\bar{x} \\
&\iff \bar{y} \in \overline{\bar{A}x^2 + \bar{B}x} \\
&\iff \bar{y} = \overline{ax^2 + bx}, \ \ for\ some\ \ (a,b) \in \bar{A} \times \bar{B} \\
&\iff y = agx^2 + bgx \ \ for\ some\ \ g \in G \\
&\iff y = a'x^2 + b'x, \ where\ a' = ag,\ b' = bg \\
&\iff (x,y) \in Q(f_{a',b'}, F), \ \ for\ some\ \ (a',b') \in \bar{A} \times \bar{B} \\
&\iff (x,y) \in \bigcup_{a\in\bar{A},b\in\bar{B}} Q(f_{a,b}, F).
\end{aligned}$$

Consequently, $Q(f_{\bar{A},\bar{B}}, F) = \bigcup\limits_{a\in\bar{A},b\in\bar{B}} Q(f_{a,b}, F)$. □

Example 2. *Let* $F = \mathbb{Z}_5$ *be the field of order* 5 , $G = \{\pm 1\} \leqslant F^*$ *and* $f_{\bar{1},\bar{0}}(\bar{x}) = \bar{x}^2$. *Then we have* $\bar{F} = \{\bar{0},\bar{1},\bar{2}\}$, $Q(f_{\bar{1},\bar{0}}, \bar{F}) = \overline{Q(f_{1,0}, F)} \cup \overline{Q(f_{(-1),0}, F)}$, *where*

$$Q(f_{1,0}, F) = \{(0,0),(1,1),(-1,1),(2,-1),(-2,-1)\},$$

$$Q(f_{(-1),0}, F) = \{(0,0),(1,-1),(-1,-1),(2,1),(-2,1)\},$$

and $Q(f_{1,0}, \bar{F}) = \overline{Q(f_{1,0}, F)} = \{(\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{2},\bar{1})\} = \overline{Q(f_{(-1),0}, F)} = Q(f_{(-1),0}, \bar{F})$. *In this case* $Q(f_{\bar{1},\bar{0}}, \bar{F})$ *is a non-degenerate conic hypersection because* $\bar{A} = \bar{1} \neq \bar{0}$.

Definition 7. *Let* F *be a field,* $x \in F$ *and* G *be a subgroup in* F^*. *We take*

$$\mathcal{O} = \begin{cases} 0^{-1}, & if\ \ f_{a,b}(z) = az^2 + bz \\ 0, & if\ \ f_{a,b}(z) = az^{-1} + bz \end{cases}$$

$$\mathcal{G}_x(f_{a,b}) = \begin{cases} \{x\}, & if\ \ G = \{1\} \\ \{z \in F | f_{a,b}(z) = f_{a,b}(x)\}, & if\ \ G \neq \{1\}, f_{a,b}(z) = az^2 + bz \\ \{-x, x\}, & if\ \ G \neq \{1\}, f_{a,b}(z) = az^{-1} + bz. \end{cases}$$

Obviously, 0^{-1} *is an element outside of* F. *We denote* $0^{-1} = \frac{1}{0}$ *by* ∞, *where* $\infty \notin F$, *and* $\overline{\infty} = \infty$. *Suppose that* $\mathcal{G}_\infty(f_{a,b}) = \{\infty\}$, $f_{a,b}(\infty) = \infty$, $f_{a,b}(\mathcal{O}) = \infty$, *for all* $a \in \bar{A}, b \in \bar{B}$, *also* $\hat{X} = \{\hat{x} | x \in X\}$ *where* $\hat{x} = (x, f_{a,b}(x))$ *and* $X \subseteq F \cup \{\mathcal{O}\}$. *Moreover,* $\mathcal{O} \cdot \mathcal{O} = \mathcal{O} = \mathcal{O} + \mathcal{O}$, $x \cdot \mathcal{O} = \begin{cases} \mathcal{O}, & if\ x \neq 0 \\ 0, & if\ x = 0 \end{cases}$ *and* $x + \mathcal{O} = \begin{cases} \mathcal{O}, & if\ \mathcal{O} = 0^{-1} \\ x, & if\ \mathcal{O} = 0 \end{cases}$, *for all* x *in field of* $(F, +, \cdot)$.

Remark 1. *It should be noted that associativity by adding* $\mathcal{O}$ *to field of* $(F, +, \cdot)$ *for two operations of "*$+$*" and "*$\cdot$*" remains preserved.*

Definition 8. *Let $Q(f_{\bar{A},\bar{B}},\bar{F})$ be a non-degenerate conic hypersection, $F_\infty = F\cup\{\infty\}$ and*

$$Q_F(f_{a,b}) = \{\hat{x} : x\in F_\infty, \hat{x}\notin L_0\},$$

$$Q_F(f_{\bar{A},\bar{B}}) = \bigcup_{a\in\bar{A},b\in\bar{B}} Q_F(f_{a,b}),$$

where $L_0 = \{(x,0)|x\in F_{\mathcal{O}}\}$. For all $\hat{x}_i,\hat{x}_i\in Q_F(f_{a,b})$

$$\widehat{x_i\bullet_{ab}x_j} = (x_i\bullet_{ab}x_j, f_{a,b}(x_i\bullet_{ab}x_j)) \text{ in which } \{(x_i\bullet_{ab}x_j,0)\} = L_0\cap L_{a,b}(\hat{x}_i,\hat{x}_j),$$

and

$$L_{a,b}(\hat{x}_i,\hat{x}_j) = \begin{cases} \{(x,y)\in F^2|y-f_{a,b}(x_i) = \frac{f_{a,b}(x_j)-f_{a,b}(x_i)}{(x_j-x_i)}(x-x_i)\}, & x_i\neq x_j, \mathcal{O}\notin\{x_i,x_j\}\\ \{(x,y)\in F^2|y-f_{a,b}(x_i) = f'_{a,b}(x_i)(x-x_i)\}, & x_i = x_j\notin\{\mathcal{O}\}\\ \{(x,y)\in F^2|\mathcal{O}\neq x\in\{x_i,x_j\}\}\cup\{\hat{\mathcal{O}}\}, & x_i\neq x_j, \mathcal{O}\in\{x_i,x_j\}\\ \{(\mathcal{O},y)|y\in F_\infty = F\cup\{\infty\}\}, & (x_i,x_j) = (\mathcal{O},\mathcal{O}),\end{cases}$$

and $f'_{a,b}$ is meant by formal derivative $f_{a,b}$.

We denote $\overline{Q_F(f_{a,b})}$ by $Q_{\bar{F}}(f_{a,b})$ and $\overline{Q_F(f_{\bar{A},\bar{B}})}$ by $Q_{\bar{F}}(f_{\bar{A},\bar{B}})$ also take $\bar{\mathcal{O}} = \{\mathcal{O}\} = \mathcal{O}$, $\overline{f(\mathcal{O})} = \{f(\mathcal{O})\} = f(\mathcal{O})$ and, $\overline{(\mathcal{O},f(\mathcal{O}))} = (\bar{\mathcal{O}},\overline{f(\mathcal{O})}) = (\mathcal{O},f(\mathcal{O}))$. Moreover, $\mathcal{O}\odot\mathcal{O} = \mathcal{O}$ and $\mathcal{O}\oplus\mathcal{O} = \mathcal{O}$ also, for all $\bar{x}$ in hyperfield of $(\bar{F},\oplus,\odot)$, $\bar{x}\odot\mathcal{O} = \begin{cases}\mathcal{O}, & \text{if } x\neq 0\\ \bar{0}, & \text{if } x = 0\end{cases}$ $\bar{x}\oplus\mathcal{O} = \begin{cases}\mathcal{O}, & \text{if } \mathcal{O} = 0^{-1}\\ \bar{x}, & \text{if } \mathcal{O} = 0\end{cases}$ and agree to $L_o\cap L(\hat{x}_i,\hat{x}_j) = \{(\infty,0)\}$ if $f_{a,b}(x_i) = f_{a,b}(x_j)$. In addition say to $L_{a,b}(\hat{x}_i,\hat{x}_j)$ the line passing from $\hat{x}_i,\hat{x}_j$, Intuitively each line passing from $(\mathcal{O},\infty)$ is called vertical line, and every vertical line pass through $(\mathcal{O},\infty)$. $\widehat{\mathcal{O}}$ is playing an asymptotic extension role for function $f_{a,b}$

Remark 2. *By adding $\mathcal{O}$ to hyperfield of $(F,\oplus,\odot)$ associativity for two hyperoperations of "$\oplus$" and "$\odot$" remains preserved.*

Suppose that $\hat{x}\in Q(f_{a,b},F)$ and $\widetilde{x} = \begin{cases}\{x\}, & f_{a,b}(x) = ax^2+bx\\ \{x,-x\}, & f_{a,b}(x) = ax^{-1}+bx\end{cases}$ Hence, we the following proposition

Proposition 1. *if $|Q_F(\widetilde{f}_{a_1,b_1})\cap Q_F(\widetilde{f}_{a_2,b_2})|\geq 2$ then $Q(f_{a_1,b_1},F) = Q(f_{a_2,b_2},F)$.*

Proof. Let $\{\widetilde{x}_1,\widetilde{x}_2\}\subseteq Q_F(\widetilde{f}_{a_1,b_1})\cap Q_F(\widetilde{f}_{a_2,b_2})$, $\widetilde{x}_1\neq\widetilde{x}_2$ and $i,j = 1,2$. Then

$$y_i = a_jx_i^2+b_jx_i\Longrightarrow x_1\neq x_2\Longrightarrow\begin{cases}a_1 = a_2 = \dfrac{x_2y_1-x_1y_2}{x_1^2x_2-x_2^2x_1},\\ b_1 = b_2 = \dfrac{-x_2^2y_1+x_1^2y_2}{x_1^2x_2-x_2^2x_1},\end{cases}$$

$$y_i = a_jx_i^{-1}+b_jx_i\Longrightarrow x_1\neq\pm x_2\Longrightarrow\begin{cases}a_1 = a_2 = \dfrac{x_2y_1-x_1y_2}{x_2x_1^{-1}-x_1x_2^{-1}},\\ b_1 = b_2 = \dfrac{-x_2^{-1}y_1+x_1^{-1}y_2}{x_2x_1^{-1}-x_1x_2^{-1}}.\end{cases}$$

Hence $Q(f_{a_1,b_1},F) = Q(f_{a_2,b_2},F)$, as we expected. □

Definition 9. *Let $Q(f_{\bar{A},\bar{B}},\bar{F})$ be a non-degenerate conic hypersection then it is named hyperconic and denoted to $Q_{\bar{F}}(f_{\bar{A},\bar{B}})$, if the following implication for all $a,c\in\bar{A}$ and $b,d\in\bar{B}$ holds:*

$$Q_F(f_{a,b})\cap Q_F(f_{c,d})\neq\begin{cases}\{\widehat{\mathcal{O}}\}, & f_{a,b}(x)=ax^2+bx\\ \{\widehat{\mathcal{O}},\widehat{\infty}\}, & f_{a,b}(z)=ax^{-1}+bx\end{cases}\Longrightarrow Q_F(f_{a,b})=Q_F(f_{c,d}).$$

Proposition 2. *Let $\hat{x_i}=(x_i,f(x_i))$ and $\hat{x_j}=(x_j,f(x_j))$ belong to $Q_F(f_{a,b})$, then*

$$x_i\bullet_{ab}x_j=\begin{cases}\dfrac{x_if_{a,b}(x_j)-x_jf_{a,b}(x_i)}{f_{a,b}(x_j)-f_{a,b}(x_i)} & x_i\neq x_j,\mathcal{O}\notin\{x_i,x_j\},\\ x_i-\dfrac{f_{a,b}(x_i)}{f'_{a,b}(x_i)} & x_i=x_j\notin\{\mathcal{O}\},\\ x_i & x_i\neq\mathcal{O}=x_j,\\ x_j & x_j\neq\mathcal{O}=x_i,\\ \mathcal{O} & (x_i,x_j)=(\mathcal{O},\mathcal{O}).\end{cases}$$

Proof. The proof is straightforward for the first two cases. If $f_{a,b}(x_i)=f_{a,b}(x_j)$ then

$$x_i\bullet_{ab}x_j=\frac{x_if_{a,b}(x_j)-x_jf_{a,b}(x_i)}{f_{a,b}(x_j)-f_{a,b}(x_i)}=\frac{x_if_{a,b}(x_j)-x_jf_{a,b}(x_i)}{0}=\infty,$$

$$\{(x_i\bullet_{ab}x_j,0)\}=L_o\cap L(\hat{x_i},\hat{x_j})=\{(\infty,0)\}\Longrightarrow x_i\bullet_{ab}x_j=\infty.$$

Suppose that $(x_i,x_j)\in Q_{\bar{F}}^2(f_{a,b})$ by regarding Definition 8 if $x_i\neq\mathcal{O}=x_j$ then

$$\{(x_i\bullet_{ab}\mathcal{O},0)\}=L_0\cap L_{a,b}(\hat{x_i},\hat{\mathcal{O}})=\{(x_i,0)\}\Longrightarrow x_i\bullet_{ab}\mathcal{O}=x_i,$$

if $x_j\neq\mathcal{O}=x_i$ then proof is similar to previous manner, ultimately if $x_i=x_j=\mathcal{O}$ then

$$\{(\mathcal{O}\bullet_{a,b}\mathcal{O},0)\}=L_0\cap L(\hat{\mathcal{O}},\hat{\mathcal{O}})=\{(\mathcal{O},0)\}\Longrightarrow\mathcal{O}\bullet_{a,b}\mathcal{O}=\mathcal{O}.\quad\square$$

Remark 3. *$\left(Q_F(f_{a,b}),\bullet_{ab}\right)$ is a conic group, for all $(a,b)\in\bar{A}\times\bar{B}$. Notice that $\bullet_{ab}$ is the group operation on the conic $Q_F(f_{a,b})$.*

Example 3. *Let $F=\mathbb{Z}_5$ the field of order 5 , $G=\{\pm1\}\leqslant F^*$ and $f_{\bar{1},\bar{0}}(\bar{x})=\bar{x}^2$. Then we have $\bar{F}=\{\bar{0},\bar{1},\bar{2}\}$, $Q_{\bar{F}}(f_{\bar{1},\bar{0}})=\overline{Q_F(f_{1,0})}\cup\overline{Q_F(f_{(-1),0})}$, where $Q_F(f_{1,0})=\{\hat{\mathcal{O}},(1,1),(-1,1),(2,-1),(-2,-1)\}$ and $\overline{Q_F(f_{1,0})}=\{\hat{\mathcal{O}},(\bar{1},\bar{1}),(\bar{2},\bar{1})\}$, $Q_F(f_{(-1),0})=\{\hat{\mathcal{O}},(1,-1),(-1,-1),(2,1),(-2,1)\}$, and $\overline{Q_F(f_{(-1),0})}=\{\hat{\mathcal{O}},(\bar{1},\bar{1}),(\bar{2},\bar{1})\}$, in this case $Q_{\bar{F}}(f_{\bar{1},\bar{0}})$ is a hyperconic because $Q_F(f_{1,0})\cap Q_F(f_{(-1),0})=\hat{\mathcal{O}}$.*

Definition 10. *We introduce hyperoperation "$\circ$" on $Q_F(f_{\bar{A},\bar{B}})$ as follows:*
Let $(x,y),(x',y')\in Q_F(f_{\bar{A},\bar{B}})$. If $(x,y)\in Q_F(f_{a,b})$ and $(x',y')\in Q_F(f_{a',b'})$ for some $a,a'\in\bar{A}$ and $b,b'\in\bar{B}$.

$$(x,y)\circ(x',y')=\begin{cases}\{\widehat{x_i\bullet_{ab}x_j}|(x_i,x_j)\in\mathcal{G}_x(f_{a,b})\times\mathcal{G}_{x'}(f_{a',b'})\}, & \text{if } Q_F(f_{a,b})=Q_F(f_{a',b'})\\ Q_F(f_{a,b})\cup Q_F(f_{a',b'}), & \text{otherwise.}\end{cases}$$

Theorem 3. *$\left(Q_F(f_{\bar{A},\bar{B}}),\circ\right)$ is a hypergroup.*

Proof. Suppose that $\{X,Y,Z\}\subseteq Q_F(f_{\bar{A},\bar{B}})$,by Bezout's Theorem $(x,y)\circ(x',y')\subseteq P^*(Q_F(f_{a,b}))$. Now let $X=(x,y)\in Q_F(f_{a,b}),Y=(x',y')\in Q_F(f_{a',b'}),Z=(x'',y'')\in Q_F(f_{a'',b''})$, where $J=\{(a,b),(a',b'),(a'',b'')\}\subseteq\bar{A}\times\bar{B}$. If $(x,y)=(x_1,y_1)$ and $(x',y')=(x'_1,y'_1)$ then $x=x_1$

and $x' = x'_1$. Because $\mathcal{G}_x(f_{a,b}) = \mathcal{G}_{x_1}(f_{a,b})$ and $\mathcal{G}_{x'}(f_{a,b}) = \mathcal{G}_{x'_1}(f_{a,b})$ we have $\mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b}) = \mathcal{G}_{x_1}(f_{a,b}) \times \mathcal{G}_{x'_1}(f_{a,b})$ thus

$$\{\widehat{z \bullet_{ab} w} | (z,w) \in \mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b})\} = \{\widehat{z \bullet_{ab} w} | (z,w) \in \mathcal{G}_{x_1}(f_{a,b}) \times \mathcal{G}_{x'_1}(f_{a,b})\}$$

and that is $(x,y) \circ (x',y') = (x_1,y_1) \circ (x'_1,y'_1)$, consequently "$\circ$" is well defined. If $X = (\mathcal{O},\infty)$ or $Y = (\mathcal{O},\infty)$ or $Z = (\mathcal{O},\infty)$, associativity is evident. If this property is not met, the following cases may occur:

Case1. If $|J| = 1$. In this case we have $Q_F(f_{a,b}) = Q_F(f_{a',b'}) = Q_F(f_{a'',b''})$.

$$\begin{aligned}[(x,y) \circ (x',y')] \circ (x'',y'') &= \left\{(\widehat{x_i \bullet_{ab} x'_j}) | (x_i, x'_j) \in \mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b})\right\} \circ (x'',y'') \\ &= \left\{(\widehat{x_i \bullet_{ab} x'_j) \bullet_{ab}} x''_k | (x_i, x'_j, x''_k) \in \mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b}) \times \mathcal{G}_{x''}(f_{a,b})\right\}.\end{aligned}$$

Similarly

$$(x,y) \circ [(x',y') \circ (x'',y'')] = \left\{x_i \bullet_{ab} \widehat{(x'_j \bullet_{ab} x''_k)} | (x_i, x'_j, x''_k) \in \mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b}) \times \mathcal{G}_{x''}(f_{a,b})\right\}.$$

On the other hand we have

$$\begin{aligned}L(\hat{x}_i, \hat{x}'_j) \cap L(\widehat{x_i \bullet_{ab} x'_j}, \hat{\mathcal{O}}) &= \{(x_i \bullet_{ab} x_j, 0)\} \subseteq L_0, \\ L(\hat{x}'_j, \hat{x}''_k) \cap L(\hat{\mathcal{O}}, \widehat{x'_j \bullet_{ab} x''_k}) &= \{(x_j \bullet_{ab} x_k, 0)\} \subseteq L_0.\end{aligned}$$

Therefore by Pascal's Theorem we have

$$L(\hat{x''_k}, \widehat{x_i \bullet_{ab} x'_j}) \cap L(\hat{x}'_j \bullet_{ab} \hat{x''_k}, \hat{x}_i) \subseteq L_0,$$

and in addition

$$\begin{aligned}\{((x_i \bullet_{ab} x'_j) \bullet_{ab} x''_k, 0)\} &= L_0 \cap L(\widehat{x_i \bullet_{ab} x'_j}, \widehat{x''_k}), \\ \{(x_i \bullet_{ab} (x'_j \bullet_{ab} x''_k), 0)\} &= L_0 \cap L(\hat{x}_i, \widehat{x'_j \bullet_{ab} x''_k}), \\ L_0 \cap L(\widehat{x_i \bullet_{ab} x'_j}, \widehat{x''_k}) = L(\hat{x''_k}, \widehat{x_i \bullet_{ab} x'_j}) \cap L(\widehat{x'_j \bullet_{ab} x''_k}, \hat{x}_i) &= L_0 \cap L(\hat{x}_i, \widehat{x'_j \bullet_{ab} x''_k}).\end{aligned}$$

On the other word

$$(x_i \bullet_{ab} x'_j) \bullet_{ab} x''_k = x_i \bullet_{ab} (x'_j \bullet_{ab} x''_k).$$

So

$$\left((\widehat{x_i \bullet_{ab} x'_j}) \bullet_{ab} x''_k\right) = \left(x_i \bullet_{ab} \widehat{(x'_j \bullet_{ab} x''_k)}\right) \text{ for all } (x_i, x'_j, x''_k) \in \mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b}) \times \mathcal{G}_{x''}(f_{a,b})$$

Case2. If $|J| = 2$. (i) If $Q_F(f_{a,b}) = Q_F(f_{a',b'}) \neq Q_F(f_{a'',b''})$. We have

$$\begin{aligned}[(x,y) \circ (x',y')] \circ (x'',y'') &= [\{\widehat{z \bullet_{ab} w} | (z,w) \in \mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b})\}] \circ (x'',y'') \\ &= \bigcup_{(u,v) \in (x,y) \circ (x',y')} (u,v) \circ (x'',y'') \\ &= Q_F(f_{a,b}) \cup Q_F(f_{a'',b''}).\end{aligned}$$

Otherwise

$$\begin{aligned}(x,y)\circ[(x',y')\circ(x'',y'')] &= (x,y)\circ\big(Q_F(f_{a',b'})\cup Q_F(f_{a'',b''})\big)\\ &= Q_F(f_{a',b'})\cap Q_F(f_{a,b})\cup Q_F(f_{a'',b''})\\ &= Q_F(f_{a,b})\cup Q_F(f_{a'',b''}).\end{aligned}$$

(ii) If $Q_F(f_{a,b}) \neq Q_F(f_{a',b'}) = Q_F(f_{a'',b''})$. This case similar to (i).

(iii) If $Q_F(f_{a,b}) = Q_F(f_{a'',b''}) \neq Q_F(f_{a',b'})$. We have

$$\begin{aligned}[(x,y)\circ(x',y')]\circ(x'',y'') &= \big(Q_F(f_{a,b})\cup Q_F(f_{a',b'})\big)\circ(x'',y'')\\ &= Q_F(f_{a,b})\cup Q_F(f_{a',b'})\cup Q_F(f_{a'',b''})\\ &= Q_F(f_{a,b})\cup Q_F(f_{a',b'}).\end{aligned}$$

On the other hand

$$\begin{aligned}(x,y)\circ[(x',y')\circ(x'',y'')] &= (x,y)\circ(Q_F(f_{a',b'})\cup Q_F(f_{a'',b''}))\\ &= Q_F(f_{a,b})\cup Q_F(f_{a',b'})\cup Q_F(f_{a'',b''})\\ &= Q_F(f_{a,b})\cup Q_F(f_{a',b'}).\end{aligned}$$

Case3. If $|J| = 3$. In this case we have

$$\begin{aligned}[(x,y)\circ(x',y')]\circ(x'',y'') &= \big(Q_F(f_{a,b})\cup Q_F(f_{a',b'})\big)\circ(x'',y'')\\ &= Q_F(f_{a,b})\cup Q_F(f_{a',b'})\cup Q_F(f_{a'',b''}).\end{aligned}$$

On the other hand

$$\begin{aligned}(x,y)\circ[(x',y')\circ(x'',y'')] &= (x,y)\circ\big(Q_F(f_{a',b'})\cup Q_F(f_{a'',b''})\big)\\ &= Q_F(f_{a,b})\cup Q_F(f_{a',b'})\cup Q_F(f_{a'',b''}).\end{aligned}$$

To prove the validity of reproduction axiom for "$\circ$" let us consider two cases:

Case1. If $|\bar{A}\times\bar{B}| = 1$ then $\bar{F} = F$ and $Q_F(f_{\bar{A},\bar{B}}) = Q_F(f_{a,b})$, where $a\in\bar{A}, b\in\bar{B}$ also $(Q_F(f_{a,b}),\circ)$ is a conic group, hence there is nothing to prove.

Case2. If $|\bar{A}\times\bar{B}| > 1$, consider arbitrary element $\hat{x}\in Q_F(f_{a,b})\subseteq Q_F(f_{\bar{A},\bar{B}})$, then

$$\begin{aligned}\hat{x}\circ Q_F(f_{\bar{A},\bar{B}}) &= \Big(\hat{x}\circ\bigcup_{a\neq i\in\bar{A},b\neq j\in\bar{B}} Q_F(f_{i,j}))\cup(\hat{x}\circ Q_F(f_{a,b})\Big),\\ &= \Big(\bigcup_{a\neq i\in\bar{A},b\neq j\in\bar{B}}\hat{x}\circ Q_F(f_{i,j})\Big)\cup Q_F(f_{a,b}),\\ &= \Big(\bigcup_{i\in\bar{A},j\in\bar{B}} Q_F(f_{i,j})\Big)\cup Q_F(f_{a,b}),\\ &= Q_F(f_{\bar{A},\bar{B}}).\end{aligned}$$

Similarly, $Q_F(f_{\bar{A},\bar{B}})\circ\hat{x} = Q_F(f_{\bar{A},\bar{B}})$ and reproduction axiom is established. Thus, $\big(Q_F(f_{\bar{A},\bar{B}}),\circ\big)$ is a hypergroup. □

Remark 4. *The hyperconic and the associated hypergroup are conic and conic group, respectively, if* $G = \{1\}$.

Example 4. *Let $F = \mathbb{Z}_5$ be the field of order 5 and $G = \{\pm 1\} \leqslant F^*$. We have $\bar{F} = \{\bar{0}, \bar{1}, \bar{2}\}$. In addition, if we go back to Example 3 then $Q_{\bar{F}}(f_{\bar{1},\bar{0}}) = \overline{Q_F(f_{1,0})} \cup \overline{Q_F(f_{(-1),0})}$ is hyperconic, where $Q_F(f_{1,0}) = \{\hat{\mathcal{O}}, (1,1), (-1,1), (2,-1), (-2,-1)\}$*
$Q_F(f_{(-1),0}) = \{\hat{\mathcal{O}}, (1,-1), (-1,-1), (2,1), (-2,1)\}$, $Q_{\bar{F}}(f_{\bar{1},\bar{0}}) = \{\hat{\mathcal{O}}, (\bar{1},\bar{1}), (\bar{2},\bar{1})\}$. Now let $H = Q_F(f_{1,0})$ and $K = Q_F(f_{(-1),0})$. Then H and K are reversible subhypergroups of $Q_F(f_{\bar{1},\bar{0}})$, which are defined by the Caley Tables 2 and 3, respectively.

Table 2. Cayle table $(Q_{\mathbb{Z}_5}(f_{1,0}), \circ)$.

$\circ$	$\hat{\mathcal{O}}$	$(1,1)$	$(-1,1)$	$(2,-1)$	$(-2,-1)$
$\hat{\mathcal{O}}$	$\hat{\mathcal{O}}$	$(\pm 1, 1)$	$(\pm 1, 1)$	$(\pm 2, -1)$	$, (\pm 2, -1)$
$(1,1)$	$(\pm 1, 1)$	$\hat{\mathcal{O}}, (\pm 2, -1)$	$\hat{\mathcal{O}}, (\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$
$(-1,1)$	$(\pm 1, 1)$	$\hat{\mathcal{O}}, (\pm 2, -1)$	$\hat{\mathcal{O}}, (\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$
$(2,-1)$	$(\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$	$(\pm 1, 1), \hat{\mathcal{O}}$	$(\pm 1, 1), \hat{\mathcal{O}}$
$(-2,-1)$	$(\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$	$(\pm 1, 1), (\pm 2, -1)$	$(\pm 1, 1), \hat{\mathcal{O}}$	$(\pm 1, 1), \hat{\mathcal{O}}$

Table 3. Caley table $(Q_{\mathbb{Z}_5}(f_{(-1),0}), \circ)$.

$\circ$	$\hat{\mathcal{O}}$	$(1,-1)$	$(-1,-1)$	$(2,1)$	$(-2,1)$
$\hat{\mathcal{O}}$	$\hat{\mathcal{O}}$	$(\pm 1, -1)$	$(\pm 1, -1)$	$(\pm 2, 1)$	$, (\pm 2, 1)$
$(1,-1)$	$(\pm 1, -1)$	$\hat{\mathcal{O}}, (\pm 2, 1)$	$\hat{\mathcal{O}}, (\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$
$(-1,-1)$	$(\pm 1, -1)$	$\hat{\mathcal{O}}, (\pm 2, 1)$	$\hat{\mathcal{O}}, (\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$
$(2,1)$	$(\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$	$(\pm 1, -1), \hat{\mathcal{O}}$	$(\pm 1, -1), \hat{\mathcal{O}}$
$(-2,1)$	$(\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$	$(\pm 1, -1), (\pm 2, 1)$	$(\pm 1, -1), \hat{\mathcal{O}}$	$(\pm 1, -1), \hat{\mathcal{O}}$

Proposition 3. *H is subhypergroup of $Q_F(f_{\bar{A},\bar{B}})$ if and only if $H = \bigcup_{(i,j)\in I\subseteq \bar{A}\times\bar{B}} Q_F(f_{i,j})$ or $H \leqslant Q_{i,j}(F)$, for some $(i,j) \in \bar{A} \times \bar{B}$.*

Proof. $(\Rightarrow)$. Let us assume that $H \nleqslant Q_F(f_{i,j})$ for every (i,j) in $\bar{A} \times \bar{B}$. Then in $\bar{A} \times \bar{B}$ exist $(i,j) \neq (s,t)$ such that $H \cap Q_F(f_{i,j}) \neq \emptyset \neq H \cap Q_F(f_{s,t})$. Now let I=$\{(i,j) \in \bar{A} \times \bar{B} | H \cap Q_F(f_{i,j}) \neq \emptyset\}$, thus we have $H \subseteq \bigcup_{(i,j)\in I} Q_F(f_{i,j}) \subseteq \bigcup_{(s,t),(i,j)\in I} (Q_F(f_{i,j}) \cap H) \circ (Q_F(f_{s,t}) \cap H) \subseteq H$. Accordingly, $H = \bigcup_{(i,j)\in I} Q_F(f_{i,j})$.
$(\Leftarrow)$. It is obvious. □

Proposition 4. *Let H be a subhypergroup of $Q_F(f_{\bar{A},\bar{B}})$. Then H is reversible hypergroup if and only if $H \leqslant Q_F(f_{i,j})$, for some $(i,j) \in \bar{A} \times \bar{B}$.*

Proof. $(\Leftarrow)$. First we prove that $H \leqslant Q_F(f_{i,j})$ is a regular reversible hypergroup for all $(i,j) \in \bar{A} \times \bar{B}$. Let (x,y) and (x',y') are elements in $Q_F(f_{i,j})$.

Case1. If $x' \notin \mathcal{G}_x(f_{a,b})$, then

$$\begin{aligned}
(x'',y'') \in (x,y) \circ (x',y') &\Longrightarrow (x'',y'') = \widehat{z \bullet_{ij} w}, \text{for some} (z,w) \in \mathcal{G}_x(f_{a,b}) \times \mathcal{G}_{x'}(f_{a,b}) \\
&\Longrightarrow x'' = z \bullet_{ij} w, \\
&\Longrightarrow z = x'' \bullet_{ij} h \qquad \text{where, } w \bullet_{ij} h = \mathcal{O}, \\
&\Longrightarrow (z, f_{a,b}(z)) = \widehat{x'' \bullet_{ij} h} \text{ and } h \in \mathcal{G}_w(f_{a,b}) = \mathcal{G}_{x'}(f_{a,b}) \\
&\Longrightarrow (z, f_{a,b}(z)) \in (x'', f_{a,b}(x'')) \circ (x', f_{a,b}(x')).
\end{aligned}$$

Case2. If $x' \in \mathcal{G}_x(f_{a,b})$, then $z, w \in \mathcal{G}_x(f_{a,b})$ and $\hat{m} \in \hat{z} \circ \hat{w} = \{\widehat{x \bullet_{ab} x}, \widehat{n \bullet_{ab} n}, \hat{\mathcal{O}}\}$, where $x \bullet_{ab} n = \mathcal{O}$ then $\hat{z} \in \hat{m} \circ \hat{w}$ and $\hat{w} \in \hat{z} \circ \hat{m}$.

Case3. If $Y \in \infty \circ X = X \circ \infty$, then $\infty \in Y \circ X$ and $X \in \infty \circ Y$. Notice that $\infty \in X \circ X$, for all $X \in Q_F(f_{i,j})$ (i.e. every element is one of its inverses).
($\Rightarrow$). Assume that $(x, y) \in H \cap Q_F(f_{i,j})$ and $(x', y') \in H \cap Q_F(f_{s,t})$, in which $(i, j) \neq (s, t)$, $(x, y) \neq \hat{\mathcal{O}} \neq (x', y')$ and $(x'', y'') \in (x, y) \circ (x', y') \cap Q_F(f_{i,j})$. Then $(x', y') \in (z, w) \circ (x'', y'') \subseteq Q_F(f_{i,j})$, where $z \in \mathcal{G}_x(f_{a,b})$. Hence $Q_F(f_{i,j}) = Q_F(f_{s,t})$ and this means reversibility conditions do not hold. □

The class of H_v- groups is more general than the class of hypergroups which is introduced by Th. Vougiouklis [39]. The hyperstructure $(H, \circ)$ is called an H_v-group if $x \circ H = H = H \circ x$, and also the weak associativity condition holds, that is $x \circ (y \circ z) \cap (x \circ y) \circ z \neq \emptyset$ for all $x, y, z \in H$. In [13,14] the authors have investigated some hyperoperations denoted by $\bar{\circ}$ and $\diamond$ on some main classes of curves; elliptic curves and homographics over Krasner's hyperfields. In the following, we study them on hyperconic. Consider the following hyperoperation on the hyperconic; $(Q_{\bar{F}}(f_{\bar{A},\bar{B}})$:

$$(\bar{x}, \bar{y}) \bar{\circ} (\bar{x'}, \bar{y'}) = \{(\bar{v}, \bar{w}) | (v, w) \in (\bar{x} \times \bar{y}) \circ (\bar{x'} \times \bar{y'})\},$$

for all $(\bar{x}, \bar{y})$, $(\bar{x'}, \bar{y'})$ in $Q_{\bar{F}}(f_{\bar{A},\bar{B}})$.

Proposition 5. *$(Q_{\bar{F}}(f_{\bar{A},\bar{B}}), \bar{\circ})$ is an H_v-group.*

Proof. The proof is straightforward. □

Proposition 6. *If $\psi_{\bar{A},\bar{B}} : Q_F(f_{\bar{A},\bar{B}}) \longrightarrow Q_{\bar{F}}(f_{\bar{A},\bar{B}})$, $\psi_{\bar{A},\bar{B}}(x, y) = (\bar{x}, \bar{y})$, then $\psi_{\bar{A},\bar{B}}$ is an epimorphism of H_v-groups.*

Proof. The base of the proof is similar to the proof of Proposition 3 in [14]. □

Example 5. *Let $G = \{\pm 1\}$ be a subgroup of F^*, where $F = \mathbb{Z}_5$. Consider $f_{\bar{1},\bar{1}}(\bar{x}) = \bar{x}^2 \oplus \bar{x}$ on $\bar{F} = \{\bar{0}, \bar{1}, \bar{2}\}$. Consequently $Q_{\bar{F}}(f_{\bar{1},\bar{1}}) = \{\hat{\mathcal{O}}, (\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})\}$ is a hyperconic, a calculation gives us the Table 4 of H_v-group.*

Table 4. Conic H_v-group, $(Q_{\mathbb{Z}_5}(f_{\bar{1},\bar{1}}), \bar{\circ})$.

$\bar{\circ}$	$\hat{\mathcal{O}}$	$(\bar{1}, \bar{2})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{2})$
$\hat{\mathcal{O}}$	$\hat{\mathcal{O}}$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{2})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{2}), (\bar{1}, \bar{2})$
$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$
$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{1})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$	$Q_{\bar{F}}(f_{\bar{1},\bar{1}})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$
$(\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$

Let A be a finite set called *alphabet* and let K be a non-empty subset of A, called *key-set* and also let "$\cdot$" be a hyperoperation on A. In [40] Berardi et.al. utilized the hyperoperations with the following condition $k \cdot x = k \cdot y \Rightarrow x = y$, for all $(x, y) \in A^2$ and $k \in K$. Let the subhypergroup $(Q_F(f_{m,n}), \circ)$ of $(Q_F(f_{\bar{m},\bar{n}}), \circ)$ and $A = \{a_x | \hat{x} \in Q_F(f_{m,n})\}$, where $a_x = i(x)$. Notice that $i(x) = \widehat{\mathcal{G}_x(f_{a,b})}$, is the set of all inverses of $\hat{x}$, for all $\hat{x} \in Q_F(f_{m,n})$. We define the hyperoperation $\diamond$ on A as bellow:

$$a_u \diamond a_v = \{a_w | w \in u \circ v\}.$$

Theorem 4. *$(A, \diamond)$ is a canonical hypergroup which satisfies Berardi's condition.*

Proof. The proof is similar to the one of Theorem 4.1 in [13]. □

4. Conclusions

Conic curve cryptography (CCC) is rendering efficient digital signature schemes (CCDLP). They have a high level of security with small keys size. Let $g(x,y) = ax^2 + bxy + cy^2 + dx + ey + f \in F[x,y]$ and $g(x,y) = 0$ be the quadratic equation of two variables in field of F, if $a = c = 0$ and $b \neq 0$ then the equation $g(x,y) = 0$ is called homographic transformation. In [14] Vahedi et. al extended this particular quadratic equation on the quotient hyperfield $\frac{F}{G}$. Now suppose that $ae \neq 0$ and $b = 0$ in $g(x,y)$. Then the curve is called a conic. The motivation of this paper goes in the same direction of [14]. In fact, by a similar way the notion of conic on a field extended to hyperconic over a quotient hyperfield hyperfield, as picturized in Figure 3. Notice that as one can see the group structures of these two classes of curves have different applications, the associated hyperstructures can be different in applications. In the last part of the paper a canonical hypergroup which is assigned by $\left(Q_F(f_{n,m}), \diamond\right)$ is investigated.

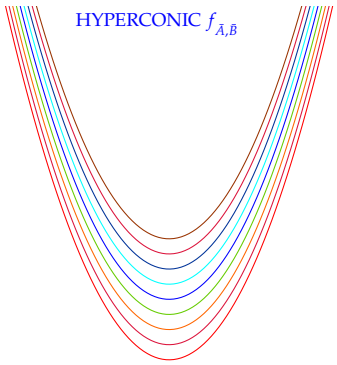

Figure 3. Hyperconic, $Q_{\mathbb{R}}(f_{\bar{A},\bar{B}})$.

Author Contributions: Conceptualization, methodology, investigation, resources, writing—original draft, writing—review and editing, all authors worked on equally; project administration and funding acquisition, S.H.-M. All authors have read and agreed to the published version of the manuscript.

Funding: Sarka Hoskova-Mayerova was supported within the project for development of basic and applied research developed in the long term by the departments of theoretical and applied bases FMT (Project code: DZRO K-217) supported by the Ministry of Defence in the Czech Republic.

Conflicts of Interest: Authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analysis, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Marty, F. Sur Une Generalization de Group. In Proceedings of the 8th Congres Des Mathematiciens Scandinaves, Stockholm, Sweden, 14–18 August 1934; pp. 45–49.
2. Corsini, P. *Prolegomena of Hypergroup Theory*; Aviani Editore: Tricesimo, Italy, 1993.
3. Davvaz, B.; Leoreanu-Fotea, V. *Hyperring Theory and Applications*; International Academic Press: Cambridge, MA, USA, 2007.
4. Corsini, P.; Leoreanu-Fotea, V. *Applications of Hyperstructure Theory*; Kluwer Academical Publications: Dordrecht, The Netherlands, 2003.
5. Vougiouklis, T. *Hyperstructures and Their Representations*; Hadronic Press: Palm Harbor, FL, USA, 1994.
6. Hoskova, S.; Chvalina, J. A survey of investigations of the Brno research group in the hyperstructure theory since the last AHA Congress. In Proceedings of the AHA 2008: 10th International Congress-Algebraic Hyperstructures and Applications, University of Defence, Brno, Czech Republic, 3–9 September 2008; pp. 71–83, ISBN 978-80-7231-688-5.

7. Antampoufis, N.; Hoskova-Mayerova, S. A Brief Survey on the two Different Approaches of Fundamental Equivalence Relations on Hyperstructures. *Ratio Math.* **2017**, *33*, 47–60. [CrossRef]
8. Connes, A.; Consani, C. From monoids to hyperstructures: In search of an absolute arithmetic. In *Casimir Force, Casimir Operators and the Riemann Hypothesis: Mathematics for Innovation in Industry and Science*; van Dijk, G., Wakayama, M., Eds.; De Gruyter: Berlin, Germany, 2010, pp. 147–198.
9. Connes, A.; Consani, C. The hyperring of adele classes. *J. Number Theory* **2011**, *131*, 159–194. [CrossRef]
10. Connes, A.; Consani, C. The universal thickening of the field of real numbers. In Proceedings of the Thirteenth Conference of the Canadian Number Theory Association, Ottawa, ON, Canada, 16–20 June 2014.
11. Viro, O. On basic concepts of tropical geometry. *Proc. Steklov Inst. Math.* **2011**, *273*, 252–282. [CrossRef]
12. Gladki, P.; Marshall, M. Orderings and signatures of higher level on multirings and hyperfields. *J.-Theory-Theory Its Appl. Algebr. Geom. Topol.* **2012**, *10*, 489–518.
13. Vahedi, V.; Jafarpour, M.; Aghabozorgi, H.; Cristea, I. Extension of elliptic curves on Krasner hyperfields. *Comm. Algebra* **2019**, *47*, 4806–4823. [CrossRef]
14. Vahedi, V.; Jafarpour, M.; Cristea, I. Hyperhomographies on Krasner Hyperfields. *Symmetry Class. Fuzzy Algebr. Hypercompos. Struct.* **2019**, *11*, 1442. [CrossRef]
15. Freni, D. Strongly Transitive Geometric Spaces: Applications to Hypergroups and Semigroups Theory. *Comm. Algebra* **2004**, *32*, 969–988. [CrossRef]
16. Izhakian, Z.; Knebusch, M.; Rowen, L. Layered tropical mathematics. *J. Algebra* **2014**, *416*, 200–273. [CrossRef]
17. Izhakian, Z.; Rowen, L. Supertropical algebra. *Adv. Math.* **2010**, *225*, 2222–2286. [CrossRef]
18. Lorscheid, O. The geometry of blueprints: Part i: Algebraic background and scheme theory. *Adv. Math.* **2012**, *229*, 1804–1846. [CrossRef]
19. Lorscheid, O. Scheme theoretic tropicalization. *arXiv* **2015**, arXiv:1508.07949.
20. Krasner, M. A class of hyperrings and hyperfields. *Int. J. Math. Math. Sci.* **1983**, *6*, 307–311. [CrossRef]
21. Krasner, M. Approximation des corps value complets de caracteristique p10 par ceux de caracteristique 0. In *Colloque d Algebre Superieure, Tenu a Bruxelles du 19 au 22 Decembre 1956*; Centre Belge de Recherches Mathematiques Etablissements Ceuterick: Louvain, Belgium; Gauthier-Villars: Paris, France, 1957; pp. 129–206.
22. Ameri, R.; Eyvazi, M.; Hoskova-Mayerova, S. Superring of Polynomials over a Hyperring. *Mathematics* **2019**, *7*, 902. [CrossRef]
23. Mittas, J.D. Hypergroupes canoniques. *Math. Balk.* **1972**, *2*, 165–179.
24. Massouros, C.G. A field theory problem relating to questions in hyperfield theory. In Proceedings of the International Conference on Numerical Analysis and Applied Mathematics, Halkidiki, Greece, 19–25 September 2011; Volume 1389, pp. 1852–1855.
25. Dakic, J.; Jancic-Rasovic, S.; Cristea, I. Weak Embeddable Hypernear-Rings. *Symmetry* **2019**, *11*, 96. [CrossRef]
26. Massouros, C.G.; Massouros, G.G. On Join Hyperrings. In Proceedings of the 10th International Congress on Algebraic Hyperstructures and Applications, University of Defence, Brno, Czech Republic, 3–9 September 2008; pp. 203–215.
27. Massouros, C.G. On the theory of hyperrings and hyperfields. *Algebra Log.* **1985**, *24*, 728–742. [CrossRef]
28. Massouros, G.G.; Massouros, C.G. Homomorphic Relations on Hyperringoids and Join Hyperrings. *Ratio Math.* **1999**, *13*, 61–70.
29. Ameri, R.; Kordi, A.; Sarka-Mayerova, S. Multiplicative hyperring of fractions and coprime hyperideals. *An. Stiintifice Univ. Ovidius Constanta Ser. Mat.* **2017**, *25*, 5–23. [CrossRef]
30. Jancic-Rasovic, S. About the hyperring of polynomials. *Ital. J. Pure Appl. Math.* **2007**, *21*, 223–234.
31. Cristea, I.; Jancic-Rasovic, S. Operations on fuzzy relations: A tool to construct new hyperrings. *J. Mult-Val. Logic Soft Comput.* **2013**, *21*, 183–200.
32. Jancic-Rasovic, S.; Dasic, V. Some new classes of (m,n)-hyperrings. *Filomat* **2012**, *26*, 585–596. [CrossRef]
33. Cristea, I. ; Jancic-Rasovic, S. Composition Hyperrings. *An. Stiintifice Univ. Ovidius Constanta Ser. Mat.* **2013**, *21*, 81–94. [CrossRef]
34. Flaut, C.; Flaut, D.; Hoskova-Mayerova, S.; Vasile, R. From Old Ciphers to Modern Communications. *Adv. Mil. Technol.* **2019**, *14*, 79–88. [CrossRef]
35. Saeid, A.B.; Flaut, C.; Hoskova-Mayerova, S. Some connections between BCK-algebras and n-ary block codes. *Soft Comput.* **2017**. [CrossRef]

36. Hankerson, D.; Menezes, A.; Vanstone, S.A. *Guide to Elliptic Curve Cryptography*; Springer: Berlin/Heidelberg, Germany, 2004.
37. Koblitz, N. Introduction to elliptic curves and modular forms. In *Volume 97 of Graduate Texts in Mathematics*; Springer: New York, NY, USA, 1984.
38. Silverman, J.H.; Tate, I.T. *Rational Points on Elliptic Curves*; Springer: New York, NY, USA, 1992; p. 289
39. Vougiouklis, T. The fundamental relation in hyperrings, The general hyperfield. In Proceedings of the 4th International Congress on AHA, Xanthi, Greece, 27–30 June 1990; World Scientific: Singapore, 1991; pp. 209–217.
40. Berardi, L.; Eugeni, F.; Innamorati, S. Remarks on Hypergroupoids and Cryptography. *J. Combin. Inform. Syst Sci.* **1992**, *17*, 217–231.