

Hyperhomographies on Krasner Hyperfields

Vahid Vahedi ¹, Morteza Jafarpour ¹ and Irina Cristea ^{2,*}

¹ Department of Mathematics, Vali-e-Asr University of Rafsanjan, 7718897111 Rafsanjan, Iran; vvahedi@yahoo.com (V.V.); m.j@vru.ac.ir (M.J.)

² Center for Information Technologies and Applied Mathematics, University of Nova Gorica, 5000 Nova Gorica, Slovenia

* Correspondence: irinacri@yahoo.co.uk

Received: 18 October 2019; Accepted: 19 November 2019; Published: 23 November 2019



Abstract: In this paper, we introduce generalized homographic transformations as hyperhomographies over Krasner hyperfields. These particular algebraic hyperstructures are quotient structures of classical fields modulo normal groups. Besides, we define some hyperoperations and investigate the properties of the derived hypergroups and H_v -groups associated with the considered hyperhomographies. They are equipped hyperhomographies obtained as quotient sets of nondegenerate hyperhomographies modulo a special equivalence. Thus the symmetrical property of the equivalence relations plays a fundamental role in this constructions.

Keywords: hypergroup; hyperring; hyperfield; (hyper)homography

MSC: 20N20; 14H52; 11G05

1. Introduction

In a recently published paper [1], the authors have initiated the study of elliptic hypercurves defined on Krasner hyperfields, generalizing the elliptic curves over fields. The main idea consists in substituting the field with a hyperfield, in particular with the associated quotient Krasner hyperfield. The power of this algebraic hyperstructure has been already used in solving different problems in affine algebraic schemes [2], theory of arithmetic functions [3], tropical geometry [4], algebraic geometry [5], etc. The quotient Krasner hyperfield is practically the quotient $\bar{F} = F/G$ of a classical field F by any normal subgroup G of the multiplicative part $(F \setminus \{0\}, \cdot)$. It was introduced by Krasner in 1983 [6] and investigated from the hyperalgebraic point of view mostly by Massouros [7] around 1985. In this new environment, the definition of an elliptic curve over a field F can be naturally extended to the definition of an elliptic hypercurve over a quotient Krasner hyperfield. Besides the group operation on the set of elliptic curves is extended to a hyperoperation on a family of elliptic hypercurves. The properties of the associated hypergroup have been investigated also in relation with the Berardi's cryptographic system [8].

The study developed in this paper goes in the same direction as our recent study. This time we extend a particular quadratic equation in two variables from a field F to a Krasner hyperfield F/G . It is well known that a conic section, which is a curve obtained as the intersection between the surface of a cone and a plane, can be algebraically represented as a quadratic equation with coefficients in a field, i.e., $g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$. If $a = c = 0$ and $b \neq 0$, the equation $g(x, y) = 0$ models a *homographic transformation*. Generally, after a suitable change of variables, a homographic transformation $y = \frac{ax+b}{cx+d}$, with $ad - bc \neq 0$, can be written in the form $(X - A)(Y - B) = 1$, where $X = x$, $Y = \frac{1}{\alpha}y$, where $\alpha = \frac{bc-ad}{c^2} \neq 0$, $A = -\frac{d}{c}$, and $B = \frac{a}{\alpha c}$ are elements in the field F . Equivalently, a homography transformation is given by a function $y = f_{a,b}(x) = b + \frac{1}{x-a}$, with a, b elements in a

field F . The aim of this paper is to generalize the homography transformation from the field F to the Krasner hyperfield \bar{F} . First, we generalize the reduced quadratic forms on Krasner hyperfields. This investigation leads us to introduce the notion of conic hypersection on a Krasner hyperfield. Secondly, using hyperconics, we define some hyperoperations and the associated hyperstructures give us the possibility of studying simultaneously some conics. As in our previous research paper [1], the results can be also applied in cryptography in relation with the Berardi’s cryptographic system [8].

2. Preliminaries

We recall here some basic notions of conics and hyperstructures theory also we fix the notations used in this paper. We assign the readers to these topics in the following fundamental books [9–11].

2.1. Conic Sections

A conic is a plane affine curve of degree 2, defined by an irreducible polynomial $g(x, y) = ax^2 + bxy + cy^2 + dx + ey + f = 0$ with coefficients in a field F . Based on the number of the points at infinity (this number can be 2, 1, or 0), the irreducible conics are divided in three categories: hyperbola, parabola and ellipse. Certain sets of points on curves can form an algebraic structure, and till now it is very well known the group structure. Generally the group law on conics is defined over a field F , following the rule illustrated in Figure 1 or Figure 2. In particular, if we take \mathcal{O} an arbitrary point on the conic, then for two arbitrary points p and q on the conic, their sum $p + q$ is obtained as the second point of the intersection with the conic of the parallel line through \mathcal{O} to the line joining p and q . In this case \mathcal{O} is the identity element of the group.

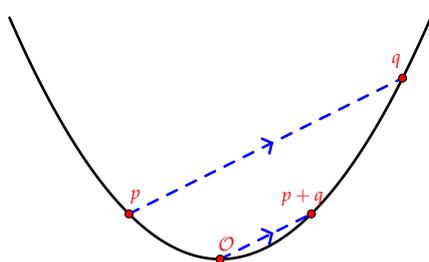


Figure 1. Addition between two points on a curve when the identity element belongs to the curve

If we consider now that the identity element \mathcal{O} is at infinity, then the sum $p + q$ of two arbitrary points p and q on the conic is the image on the conic of the point obtained as intersection with the x -axis of the line passing through p and q , as shown in Figure 2.

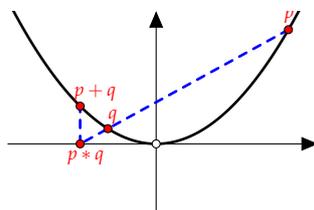


Figure 2. Addition between two points on a curve when the identity element is at infinity.

Example 1. Consider $f(x) = x^2$ over the finite field $F = \mathbb{Z}_5$. Then we have a parabola in F and the Cayley table of its points $Q_f(F) = \{\mathcal{O}, (1,1), (2,4), (3,4), (4,1)\}$ where, $\mathcal{O} = (0,0)$ is the identity element of the group, is as follows.

+	\mathcal{O}	(1,1)	(2,4)	(3,4)	(4,1)
\mathcal{O}	\mathcal{O}	(1,1)	(2,4)	(3,4)	(4,1)
(1,1)	(1,1)	(2,4)	(3,4)	(4,1)	\mathcal{O}
(2,4)	(2,4)	(3,4)	(4,1)	\mathcal{O}	(1,1)
(3,4)	(3,4)	(4,1)	\mathcal{O}	(1,1)	(2,4)
(4,1)	(4,1)	\mathcal{O}	(1,1)	(2,4)	(3,4)

If we take the identity element \mathcal{O} at infinity, then the group operation is calculated as in the following Cayley table:

+	\mathcal{O}	(1,1)	(2,4)	(3,4)	(4,1)
\mathcal{O}	\mathcal{O}	(1,1)	(2,4)	(3,4)	(4,1)
(1,1)	(1,1)	(3,4)	(4,1)	(2,4)	\mathcal{O}
(2,4)	(2,4)	(4,1)	(1,1)	\mathcal{O}	(3,4)
(3,4)	(3,4)	(2,4)	\mathcal{O}	(4,1)	(1,1)
(4,1)	(4,1)	\mathcal{O}	(3,4)	(1,1)	(2,4)

The geometrical interpretation of the associativity of the group law is equivalent with a special case of Pascal's theorem, which is a very special case of Bezout's theorem.

Theorem 1. For any conic and any six points p_1, p_2, \dots, p_6 on it, the opposite sides of the resulting hexagon, 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 (see Figure 3).

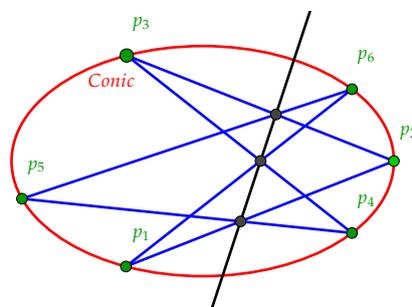


Figure 3. Pascal's theorem.

2.2. Krasner Hyperrings and Hyperfields

In this section we briefly recall the main definitions and properties of hyperrings and hyperfields, focussing on the concept of Krasner hyperfield.

Let H be a non-empty set and $\mathcal{P}^*(H)$ be the set of all non-empty subsets of H . Let \circ be a hyperoperation (or join operation) on H , that is, a function from the cartesian product $H \times H$ into $\mathcal{P}^*(H)$. The image of the pair $(a, b) \in H \times H$ under the hyperoperation \circ in $\mathcal{P}^*(H)$ is denoted by $a \circ b$. The join operation can be extended in a natural way to subsets of H as follows: for non-empty subsets A, B of H , define $A \circ B = \bigcup_{a \in A, b \in B} a \circ b$. The notation $a \circ A$ is used for $\{a\} \circ A$ and $A \circ a$ for $A \circ \{a\}$. Generally, we mean $H^k = H \times H \times \dots \times H$ (k times), for all $k \in \mathbb{N}$ and also the singleton $\{a\}$ is identified with its element a . The hyperstructure (H, \circ) is called a semihypergroup if the hyperoperation is associative, i.e., $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in H$, which means that

$$\bigcup_{u \in a \circ b} u \circ c = \bigcup_{v \in b \circ c} a \circ v.$$

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

Definition 1. Let (H, \circ) be a hypergroup and $\emptyset \neq K \subset H$. We say that (K, \circ) is a subhypergroup of H , denoted by $K \leq H$, if for all $x \in K$ we have $K \circ x = K = x \circ K$.

An element e_r (respectively e_l) of H is called a right identity (respectively left identity e_l) if for all $a \in H$, $a \in a \circ e_r$ (respectively $a \in e_l \circ a$). An element e is called a two side identity, or for simplicity an identity if, for all $a \in H$, $a \in a \circ e \cap e \circ a$. A right identity e_r (resp. left identity e_l) of H is called a scalar right identity (respectively scalar left identity) if for all $a \in H$, $a = a \circ e_r$ (respectively $a = e_l \circ a$). An element e is called a scalar identity if for all $a \in H$, $a = a \circ e = e \circ a$. An element $a' \in H$ is called a right inverse (respectively left inverse) of a in H if $e_r \in a \circ a'$, for some right identity e_r in H (respectively $e_l \in a' \circ a$, for some left identity e_l). An element $a' \in H$ is called an inverse of $a \in H$ if $e \in a' \circ a \cap a \circ a'$, for some identity e 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. In addition, if H has a scalar identity, and the inverse of $a \in H$ exists, we indicate it by a^{-1} .

Definition 2. A hypergroup H is called reversible, if the following conditions hold:

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

Definition 3. Suppose that (H, \cdot) and (K, \circ) are two hypergroups. A function $f : H \rightarrow K$ is called a homomorphism if $f(a \cdot b) \subseteq f(a) \circ f(b)$, for all a and b in H . We say that f is a good homomorphism if for all a and b in H , there is $f(a \cdot b) = f(a) \circ f(b)$. Moreover, (H, \cdot) and (K, \circ) are isomorphic, denoted by $H \cong K$, if f is a bijective good homomorphism.

An exhaustive review for the theory of hypergroups appears in [9], while the book [12] contains a wealth of applications. The more general algebraic structure that satisfies the ring-like axioms is the hyperring. There are different kinds of hyperrings. The most general one, introduced by Vougiouklis [13], has both addition and multiplication defined as hyperoperations. If only the multiplication is a hyperoperation, then we talk about multiplicative hyperrings [14,15]. If only the addition $+$ is a hyperoperation and the multiplication \cdot is a usual operation, then we say that R is an additive hyperring. A special case of this type is the hyperring introduced by Krasner [6]. An exhaustive review for the theory of hyperrings appears in [16–19].

Definition 4 ([6]). A Krasner hyperring is an algebraic structure $(R, +, \cdot)$ which satisfies the following axioms:

- (1) $(R, +)$ is a canonical hypergroup, i.e.,
 - (i) for every $x, y, z \in R$, $x + (y + z) = (x + y) + z$,
 - (ii) for every $x, y \in R$, $x + y = y + x$,
 - (iii) there exists $0 \in R$ such that $0 + x = \{x\}$ for every $x \in R$,
 - (iv) for every $x \in R$ there exists a unique element $x' \in R$ 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 that $y \in z - x$ and $x \in z - y$.
- (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 hyperring $(R, +, \cdot)$ is called commutative, if (R, \cdot) is a commutative semigroup with unit element, i.e., a monoid. A Krasner hyperring is called a Krasner hyperfield, if the multiplicative part $(R \setminus \{0\}, \cdot)$ is a group.

In the following we recall the first construction of a Krasner hyperfield, as a quotient structure of a classical field by a normal subgroup. Let $(F, +, \cdot)$ be a field and G be a normal subgroup of (F^*, \cdot) , where $F^* = F \setminus \{0\}$. Take $\frac{F}{G} = \{aG \mid a \in F\}$ with the hyperoperation and the multiplication defined by:

- (i) $aG \oplus bG = \{cG \mid c \in aG + bG\}$,
- (ii) $aG \odot bG = abG$,

for all $aG, bG \in \frac{F}{G}$. Then $(\frac{F}{G}, \oplus, \odot)$ is a hyperfield. From now on, we denote $\bar{a} = aG$, for all $aG \in \frac{F}{G}$ and the constructed hyperfield $(\frac{F}{G}, \oplus, \odot)$ by \bar{F} , and call it the Krasner hyperfield. Moreover, we denote the inverse of \bar{a} relative to \oplus by $\ominus \bar{a}$ and, for $\bar{a} \neq \bar{0}$, the multiplicative inverse \bar{a}^{-1} by $\frac{1}{\bar{a}}$. Besides, we will use the notation $\bar{S} = \{\bar{s} \mid s \in S\}$ and $\bar{T} = \{\bar{t} \mid t \in T\}$ for all $S \subseteq F, T \subseteq F^2$.

3. Hyperhomographies

In this section we define the notion of hyperhomography on a Krasner hyperfield, as a quotient structure of a classical field by a normal subgroup. Using it, we introduce some hyperoperations and investigate the properties of the associated hypergroups.

Definition 5. Let \bar{F} be the Krasner hyperfield associated with the field F and $(\bar{A}, \bar{B}) \in \bar{F}^2$. Define the generalized homography transformation on F as $\bar{1} \in (\bar{x} \ominus \bar{A}) \odot (\bar{y} \ominus \bar{B})$ on \bar{F} , and call it the hyperhomography relation. We call the set $H_{\bar{A}, \bar{B}}(\bar{F}) = \{(\bar{x}, \bar{y}) \in \bar{F}^2 \mid \bar{1} \in (\bar{x} \ominus \bar{A}) \odot (\bar{y} \ominus \bar{B})\}$ hyperhomography, while $H_{a,b}(F) = \{(x, y) \in F^2 \mid y = f_{a,b}(x) = b + \frac{1}{x-a}\}$ is a homography, for all $a \in \bar{A}$ and $b \in \bar{B}$.

Notice that the hyperhomography $H_{\bar{A}, \bar{B}}(\bar{F})$ is a generalization of a homography $H_{a,b}(F)$, because $(x, y) \in H_{a,b}(F)$ is equivalent with $y = f_{a,b}(x) = b + \frac{1}{x-a}$, i.e., $(x-a)(y-a) = 1$. The classical operations on the field F have been extended to the hyperoperation \oplus and operation \odot on \bar{F} , where by $\bar{x} \ominus \bar{A}$ we denote the hyperaddition between \bar{x} and the opposite of \bar{A} with respect to the hyperoperation \oplus . Besides, since the result of a hyperoperation is a set, the equality relation in the definition of a homography is substitute by a "belongingness" relation in the definition of a hyperhomography.

Moreover denote $H_{\bar{A}, \bar{B}}(F) = \bigcup_{a \in \bar{A}, b \in \bar{B}} H_{a,b}(F)$ and $H_{a,b}(\bar{F}) = \overline{H_{a,b}(F)} = \{(\bar{x}, \bar{y}) \mid (x, y) \in H_{a,b}(F)\}$, for all $a \in \bar{A}, b \in \bar{B}$. It follows that $\overline{H_{\bar{A}, \bar{B}}(F)} = \bigcup_{a \in \bar{A}, b \in \bar{B}} H_{a,b}(\bar{F})$.

Theorem 2. The relation between homographies and hyperhomographies is given by the following identity $H_{\bar{A}, \bar{B}}(\bar{F}) = \overline{H_{\bar{A}, \bar{B}}(F)}$.

Proof. (\Leftarrow). Let $(\bar{x}, \bar{y}) \in \overline{H_{\bar{A}, \bar{B}}(F)}$, thus there exists $(a, b) \in \bar{A} \times \bar{B}$, such that $(\bar{x}, \bar{y}) = (\bar{x}, \bar{y}) \in H_{a,b}(\bar{F})$, hence $(xg_1, yg_2) \in H_{a,b}(F)$ for some $g_1, g_2 \in G$. Then $(xg_1 - a)(yg_2 - b) = 1$ and the following implications hold:

$$\begin{aligned}
 1 = (xg_1 - a)(yg_2 - b) &\implies \begin{cases} \bar{1} = \overline{(xg_1 - a)(yg_2 - b)} \\ = \overline{(xg_1 - a)} \odot \overline{(yg_2 - b)} \\ \subseteq (\bar{x} - \bar{a}) \odot (\bar{y} - \bar{b}) \\ = (\bar{x} \ominus \bar{a}) \odot (\bar{y} \ominus \bar{b}) \end{cases} \\
 &\implies \bar{1} \in (\bar{x} \ominus \bar{A}) \odot (\bar{y} \ominus \bar{B}) \\
 &\implies (\bar{x}, \bar{y}) \in H_{\bar{A}, \bar{B}}(\bar{F}) \\
 &\implies (x, y) \in H_{\bar{A}, \bar{B}}(\bar{F}),
 \end{aligned}$$

so

$$\overline{H_{\bar{A}, \bar{B}}(\bar{F})} \subseteq H_{\bar{A}, \bar{B}}(\bar{F}).$$

(\implies). Conversely, suppose that $(\bar{x}, \bar{y}) \in H_{\bar{A}, \bar{B}}(\bar{F})$, then the following implications hold, too:

$$\begin{aligned}
 (\bar{x}, \bar{y}) \in H_{\bar{A}, \bar{B}}(\bar{F}) &\implies \bar{1} \in (\bar{x} \ominus \bar{A}) \odot (\bar{y} \ominus \bar{B}) \\
 &\implies \bar{1} \in (\bar{x} \oplus (-\bar{A})) \odot (\bar{y} \oplus (-\bar{B})) \\
 &\implies \bar{1} \in \overline{(x - \bar{A}) \odot (y - \bar{B})} \\
 &\implies \bar{1} \in \overline{(x - \bar{A})(y - \bar{B})} \\
 &\implies \bar{1} = \overline{(x - a)(y - b)}, \quad \text{for some } (a, b) \in \bar{A} \times \bar{B} \\
 &\implies \bar{1} = \overline{(x - a)} \odot \overline{(y - b)} \\
 &\implies \overline{(y - b)} = \overline{(x - a)}^{-1} \\
 &\implies \overline{(y - b)} = \overline{(x - a)}^{-1} \\
 &\implies \overline{(y - b)} = \overline{\left(\frac{1}{x - a}\right)} \\
 &\implies (y - b)g = \frac{1}{x - a} \quad \text{for some } g \in G \\
 &\implies yg = b' + \frac{1}{x - a}, \quad b' = bg \in \bar{B} \\
 &\implies (x, yg) \in H_{a, b'}(F) \\
 &\implies (\bar{x}, \bar{y}) = \overline{(x, yg)} \in \overline{H_{a, b'}(F)} = H_{a, b'}(\bar{F}) \\
 &\implies (\bar{x}, \bar{y}) \in \bigcup_{a \in \bar{A}, b \in \bar{B}} H_{a, b}(\bar{F}), \\
 &\implies (\bar{x}, \bar{y}) \in \overline{H_{\bar{A}, \bar{B}}(F)},
 \end{aligned}$$

therefore $H_{\bar{A}, \bar{B}}(\bar{F}) \subseteq \overline{H_{\bar{A}, \bar{B}}(F)}$ and consequently $H_{\bar{A}, \bar{B}}(\bar{F}) = \overline{H_{\bar{A}, \bar{B}}(F)}$. \square

Thanks to Theorem 2, we call the set $H_{\bar{A}, \bar{B}}(F)$ the hyperhomography on F , while the set $H_{a, b}(\bar{F})$ is a homography on \bar{F} .

Example 2. Let $F = \mathbb{Z}_5$ be the field of all integers modulo 5 and $G = \{1, 4\} \leq F^*$. Thus the quotient set F^*/G is $\bar{F} = \{\bar{0}, \bar{1}, \bar{2}\}$ and the hyperaddition \oplus and the multiplication \odot are defined on \bar{F} as follows:

\oplus	\parallel	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	\parallel	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	\parallel	$\bar{1}$	$\bar{0}, \bar{2}$	$\bar{1}, \bar{2}$
$\bar{2}$	\parallel	$\bar{2}$	$\bar{1}, \bar{2}$	$\bar{0}, \bar{1}$

\odot	\parallel	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	\parallel	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	\parallel	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	\parallel	$\bar{0}$	$\bar{2}$	$\bar{1}$

where $\bar{0} = \{0\}$, $\bar{1} = \{1, 4\}$ and $\bar{2} = \{2, 3\}$.

Consider now the hyperhomography

$$H_{\bar{0},\bar{1}}(\bar{F}) = \{(\bar{x}, \bar{y}) \in \bar{F}^2 \mid \bar{1} \in \bar{x} \odot (\bar{y} \ominus \bar{1})\} = \{(\bar{1}, \bar{0}), (\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})\},$$

and the homographies

$$H_{0,1}(F) = \{(x, y) \in F^2 \mid y = 1 + \frac{1}{x}\} = \{(1, 2), (2, 4), (3, 3), (4, 0)\},$$

$$H_{0,4}(F) = \{(x, y) \in F^2 \mid y = 4 + \frac{1}{x}\} = \{(1, 0), (2, 2), (3, 1), (4, 3)\}.$$

Then it follows that

$$H_{0,1}(\bar{F}) = \overline{H_{0,1}(F)} = \{(\bar{1}, \bar{0}), (\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})\} = \overline{H_{0,4}(F)} = H_{0,4}(\bar{F})$$

and therefore

$$H_{\bar{0},\bar{1}}(\bar{F}) = H_{0,1}(\bar{F}) \cup H_{0,4}(\bar{F}),$$

as stated by Theorem 2.

Definition 6. A hyperhomography $H_{A,B}(F)$ in F^2 is called nondegenerate, if the following conditions hold, respectively:

- (i) for all $a \in \bar{A}, b \in \bar{B}$, if $v = a - b^{-1} \in F$, then $(v, 0)$ can be omitted from $H_{a,b}(F)$,
- (ii) for all $a, c \in \bar{A}$ and $b, d \in \bar{B}$, there is $H_{a,b}(F) \cap H_{c,d}(F) \neq \emptyset \implies H_{a,b}(F) = H_{c,d}(F)$,
- (iii) for all $a \in \bar{A}, b \in \bar{B}$, the element (a, ∞) can be added to $H_{a,b}(F)$, where ∞ is an element outside of F .

By consequence, under the same conditions, also $H_{\bar{A},\bar{B}}(\bar{F}) = \overline{H_{A,B}(F)}$ is called a nondegenerate hyperhomography in \bar{F}^2 .

For a nondegenerate hyperhomography in F^2 , we fix some new notations: $F_\infty = F \cup \{\infty\}$, $\bar{F}_\infty = \bar{F} \cup \{\infty\}$ and $(a, \infty) = (\bar{a}, \infty)$, for any $a \in F$.

Example 3. If we go back to Example 2 and use the concepts in Definition 6, then we can omit $(4, 0)$ from $H_{0,1}(F)$ and $(1, 0)$ from $H_{0,4}(F)$, respectively, and add in both sets the element $(0, \infty)$. Then $H_{0,1}(F) = \{(0, \infty), (1, 2), (2, 4), (3, 3)\}$ and $H_{0,4}(F) = \{(0, \infty), (2, 2), (3, 1), (4, 3)\}$ are nondegenerate homographies, while $H_{\bar{0},\bar{1}}(\bar{F}) = \{(0, \infty), (\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})\}$ is a nondegenerate hyperhomography with the property $H_{\bar{0},\bar{1}}(\bar{F}) = H_{0,1}(\bar{F}) \cup H_{0,4}(\bar{F})$ where,

$$H_{0,1}(\bar{F}) = \overline{H_{0,1}(F)} = \{(\bar{0}, \infty), (\bar{1}, \bar{2}), (\bar{2}, \bar{4}), (\bar{3}, \bar{3})\} = \{(0, \infty), (\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})\},$$

$$H_{0,4}(\bar{F}) = \overline{H_{0,4}(F)} = \{(\bar{0}, \infty), (\bar{2}, \bar{2}), (\bar{3}, \bar{1}), (\bar{4}, \bar{3})\} = \{(0, \infty), (\bar{2}, \bar{2}), (\bar{2}, \bar{1}), (\bar{1}, \bar{2})\}.$$

Definition 7. Let $H_{\bar{A},\bar{B}}(F)$ be a nondegenerate hyperhomography in F^2 . Setting $f_{a,b}(a) = \infty$, we obtain that $(a, \infty) = (a, f_{a,b}(a)) \in H_{a,b}(F)$. Define

$$\mathcal{G}_{a,b}^x = \begin{cases} \{x\}, & \text{if } G = \{1\} \\ \{x, 2a - x\}, & \text{if } G \neq \{1\}, b = 0 \\ \{y \in F \mid y = x \text{ or } (x - v)(y - v) = (a - v)^2\}, & \text{if } G \neq \{1\}, b \neq 0, \end{cases}$$

for all $x \in F \setminus \{v\}$ and $(a, b) \in \bar{A} \times \bar{B}$, where $v = a - b^{-1}$.

Moreover set $\hat{X} = \{\hat{x} \mid x \in X\}$, where $\hat{x} = (x, f_{a,b}(x))$, for all $(a, b) \in \bar{A} \times \bar{B}$ and $x \in X \subseteq F$.

Corollary 1. Let $H_{\bar{A},\bar{B}}(F)$ be a nondegenerate hyperhomography in F^2 and G be a normal subgroup of F^* . If $G \neq \{1\}$ and $0 \neq b \in \bar{B}$, then $\mathcal{G}_{a,b}^x = \{x, \frac{(ab-1)x+a(2-ab)}{bx+(1-ab)}\}$.

Proof. According to Definition 7, if $G \neq \{1\}$ and $0 \neq b \in \bar{B}$, then $y = x$ or $(x - a + \frac{1}{b})(y - a + \frac{1}{b}) = \frac{1}{b^2}$. In the second case, solving the equation we get $y = \frac{(ab-1)x+a(2-ab)}{bx+(1-ab)}$. \square

In the following, for a nondegenerate hyperhomography in F^2 , we define the lines passing through two points.

Definition 8. Let $H_{\bar{A},\bar{B}}(F)$ be a nondegenerate hyperhomography in F^2 . For all $a \in \bar{A}, b \in \bar{B}$ and $\hat{x}_i, \hat{x}_j \in H_{a,b}(F)$, define $L_0 = \{(x, 0) \mid x \in F\}$ and

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

where $f'_{a,b}$ means the formal derivative of $f_{a,b}$. In addition we call $L_{a,b}(\hat{x}_i, \hat{x}_j)$ the line passing through the points \hat{x}_i and \hat{x}_j . Intuitively, for each $a \in F$, the line passing through (a, ∞) is a vertical line. In other words, (a, ∞) plays an asymptotic extension role for $f_{a,b}$.

Taking two arbitrary points \hat{x}_i, \hat{x}_j on the homography $H_{a,b}(F)$, define $x_i \bullet_{ab} x_j$ by $L_0 \cap L_{a,b}(\hat{x}_i, \hat{x}_j) = \{(x_i \bullet_{ab} x_j, 0)\}$. Using the definition of the lines $L_{a,b}(\hat{x}_i, \hat{x}_j)$ and L_0 , for $x_i \neq a \neq x_j$ we have

$$y = 0, y - f_{a,b}(x_i) = m(x - x_i) \implies x = x_i - \frac{f_{a,b}(x_i)}{m}$$

where, $m = \begin{cases} \frac{f_{a,b}(x_j) - f_{a,b}(x_i)}{x_j - x_i}, & \text{if } x_i \neq x_j \\ f'_{a,b}(x_i), & \text{if } x_i = x_j \end{cases} = \begin{cases} \frac{-1}{(x_i - a)(x_j - a)}, & \text{if } x_i \neq x_j \\ \frac{-1}{(x_i - a)^2}, & \text{if } x_i = x_j \end{cases} = \frac{-1}{(x_i - a)(x_j - a)} \in F^*$

and hence $x = x_i \bullet_{ab} x_j \in F$. If x_i or x_j are equal to a , according to Definition 8, we have

$$L_0 \cap L_{a,b}(\hat{x}_i, \hat{x}_j) = \begin{cases} \{(x_i, 0)\}, & \text{if } x_i \neq a = x_j \\ \{(x_j, 0)\}, & \text{if } x_i = a \neq x_j \\ \{(a, 0)\}, & \text{if } x_i = a = x_j \end{cases} \implies x_i \bullet_{ab} x_j = \begin{cases} x_i, & \text{if } x_i \neq a = x_j \\ x_j, & \text{if } x_i = a \neq x_j \\ a, & \text{if } x_i = a = x_j \end{cases} \implies x_i \bullet_{ab} x_j \in F.$$

Thus $|L_0 \cap L_{a,b}(\hat{x}_i, \hat{x}_j)| = 1$ and $x_i \bullet_{ab} x_j$ is well defined, therefore we have

$$\widehat{x_i \bullet_{ab} x_j} = (x_i \bullet_{ab} x_j, f_{a,b}(x_i \bullet_{ab} x_j)).$$

We will better illustrate the above defined notions in the following example.

Example 4. Consider the field $F = \mathbb{R}$ and the homography transformation $f_{0,0}(x) = \frac{1}{x}$ over F , so its graph is the hyperbola $H_{0,0}(\mathbb{R})$ represented below in Figure 4. Taking on $H_{0,0}(\mathbb{R})$ two arbitrary points $\hat{x}_i = (x_i, f_{0,0}(x_i))$ and $\hat{x}_j = (x_j, f_{0,0}(x_j))$, we draw the line $L_{0,0}(\hat{x}_i, \hat{x}_j)$ passing through \hat{x}_i and \hat{x}_j . Then $x_i \bullet_{00} x_j = L_0 \cap L_{0,0}(\hat{x}_i, \hat{x}_j)$, where L_0 is the x -axis. Then we obtain the point $\widehat{x_i \bullet_{00} x_j} = (x_i \bullet_{00} x_j, f_{0,0}(x_i \bullet_{00} x_j))$ on the hyperbola $H_{0,0}(\mathbb{R})$.

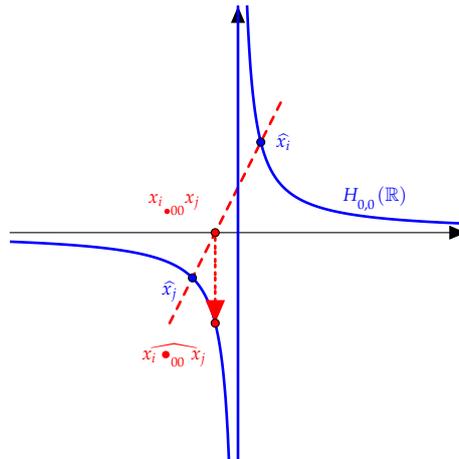


Figure 4. Hyperbola $H_{0,0}(\mathbb{R})$

Proposition 1. Let $H_{\bar{A},\bar{B}}(F)$ be a nondegenerate hyperhomography in F^2 , and $\hat{x}_i, \hat{x}_j \in H_{a,b}^2(F)$. Then, it follows that

$$x_i \bullet_{ab} x_j = bx_i x_j - (ab - 1)(x_i + x_j - a).$$

Proof. Based on Definition 8 and on the fact that $f_{a,b}(x) = b + \frac{1}{x-a}$ and $f'_{a,b}(x) = -\frac{1}{(x-a)^2}$, by simple computations, we obtain

$$\begin{aligned} x_i \bullet_{ab} x_j &= \begin{cases} \frac{x_i f_{a,b}(x_j) - x_j f_{a,b}(x_i)}{f_{a,b}(x_j) - f_{a,b}(x_i)} & x_i \neq x_j, a \notin \{x_i, x_j\}, \\ x_i - \frac{f_{a,b}(x_i)}{f'_{a,b}(x_i)} & x_i = x_j \neq a, \\ x_i & x_i \neq a = x_j, \\ x_j & x_j \neq a = x_i, \\ a & x_i = a = x_j \end{cases} \\ &= \begin{cases} x_i + (x_i - a)(x_j - a)(b + \frac{1}{x_i - a}) & x_i \neq x_j, a \notin \{x_i, x_j\} \\ x_i + (x_i - a)(x_i - a)(b + \frac{1}{x_i - a}) & x_i = x_j \neq a \\ x_i & x_i \neq a = x_j \\ x_j & x_j \neq a = x_i \\ a & x_i = a = x_j \end{cases} \\ &= \begin{cases} bx_i x_j - (ab - 1)(x_i + x_j - a) & x_i \neq x_j, a \notin \{x_i, x_j\}, \\ bx_i^2 - (ab - 1)(2x_i - a) & x_i = x_j \neq a, \\ x_i & x_i \neq a = x_j, \\ x_j & x_j \neq a = x_i, \\ a & x_i = a = x_j. \end{cases} \\ &= bx_i x_j - (ab - 1)(x_i + x_j - a). \end{aligned}$$

□

Remark 1. $(H_{a,b}(F), \bullet_{ab})$ is a homography group, for all $(a, b) \in \bar{A} \times \bar{B}$. Moreover, notice that " \bullet_{ab} " is the group operation on the homography $H_{a,b}(F)$.

On a nondegenerate hyperhomography $H_{\bar{A},\bar{B}}(F)$ in F^2 we introduce the equivalence relation “ \sim ” by considering

$$(x, y) \sim (x', y') \iff \begin{cases} x = x', \\ y = y' \notin \{\infty\}, \end{cases} \quad \text{or} \quad y, y' \in \{\infty\}$$

and denote the set of the equivalence classes of $H_{\bar{A},\bar{B}}(F)$ and $H_{a,b}(F)$ by $\mathcal{H}_{\bar{A},\bar{B}}(F)$ and $\mathcal{H}_{a,b}(F)$, respectively. It follows that $\frac{(x, y)}{\sim} = \begin{cases} (x, y), & \text{if } x \notin \bar{A} \\ (\bar{A}, \infty), & \text{if } x \in \bar{A}. \end{cases}$

Furthermore, if we introduce the notation $\mathcal{O} = \bar{A}$ and $\widehat{\mathcal{O}} = (\mathcal{O}, \infty)$. We will have $\bar{\mathcal{O}} = \mathcal{O}, \widehat{\bar{\mathcal{O}}} = \widehat{\mathcal{O}}$ and $\mathcal{H}_{\bar{A},\bar{B}}(F) = \mathcal{H}_{\bar{A},\bar{B}}(\bar{F})$.

Thus $\mathcal{H}_{\bar{A},\bar{B}}(F)$ and $\mathcal{H}_{\bar{A},\bar{B}}(\bar{F})$ are called the equipped hyperhomographies in F^2 and \bar{F}^2 , respectively. Besides, if we admit that $\bar{A} \bullet_{ab} x = x = x \bullet_{ab} \bar{A}$ for all $a \in \bar{A}, b \in \bar{B}$ and $(x, y) \in H_{a,b}(F)$, then the bijective map $\Pi : H_{a,b}(F) \rightarrow \mathcal{H}_{a,b}(F)$ defined by $\Pi(x, y) = \frac{(x, y)}{\sim}$, where $\frac{(x, y)}{\sim} = \begin{cases} (x, y), & \text{if } x \neq a \\ \mathcal{O}, & \text{if } x = a \end{cases}$ equip the quotient $\mathcal{H}_{a,b}(F)$ with a group structure and gives us a group isomorphism $(H_{a,b}(F), \bullet_{ab}) \cong (\mathcal{H}_{a,b}(F), \bullet_{ab})$.

In addition, the concepts in Definition (8) can be similarly defined on $\mathcal{H}_{a,b}(F)$, only by substituting a with \mathcal{O} .

Definition 9. Let $\mathcal{H}_{\bar{A},\bar{B}}(F)$ be an equipped hyperhomography. We define the hyperoperation “ \circ ” on $\mathcal{H}_{\bar{A},\bar{B}}(F)$ as follows.

Let $(x, y), (x', y') \in \mathcal{H}_{\bar{A},\bar{B}}(F)$. If $(x, y) \in \mathcal{H}_{a,b}(F)$ and $(x', y') \in \mathcal{H}_{a',b'}(F)$ for some $a, a' \in \bar{A}$ and $b, b' \in \bar{B}$, then

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

Theorem 3. If $\mathcal{H}_{\bar{A},\bar{B}}(\bar{F})$ is an equipped hyperhomography, then $(\mathcal{H}_{\bar{A},\bar{B}}(F), \circ)$ has a hypergroup structure.

Proof. Suppose that $\{X, Y, Z\} \subseteq \mathcal{H}_{\bar{A},\bar{B}}(F)$ such that $X = (x, y) \in \mathcal{H}_{a,b}(F), Y = (x', y') \in \mathcal{H}_{a',b'}(F)$ and $Z = (x'', y'') \in \mathcal{H}_{a'',b''}(F)$ where, $J = \{(a, b), (a', b'), (a'', b'')\} \subseteq \bar{A} \times \bar{B}$. First we notice that $(x, y) \circ (x', y') \subseteq \mathcal{P}^*(\mathcal{H}_{\bar{A},\bar{B}}(F))$, because $(x, x') \in \mathcal{G}_{a,b}^x \times \mathcal{G}_{a',b'}^{x'}$ implies that $\widehat{x \bullet_{ab} x'}$ is a non-empty set and belongs to $\mathcal{P}^*(\mathcal{H}_{\bar{A},\bar{B}}(F))$. Besides, if $(x, y) = (x_1, y_1)$ and $(x', y') = (x'_1, y'_1)$, then $x = x_1$ and $x' = x'_1$, meaning that $\mathcal{G}_{a,b}^x = \mathcal{G}_{a,b}^{x_1}$ and $\mathcal{G}_{a,b}^{x'} = \mathcal{G}_{a,b}^{x'_1}$. Hence we have $\mathcal{G}_{a,b}^x \times \mathcal{G}_{a,b}^{x'} = \mathcal{G}_{a,b}^{x_1} \times \mathcal{G}_{a,b}^{x'_1}$ and therefore $\{\widehat{z \bullet_{ab} w} | (z, w) \in \mathcal{G}_{a,b}^x \times \mathcal{G}_{a,b}^{x'}\} = \{\widehat{z \bullet_{ab} w} | (z, w) \in \mathcal{G}_{a,b}^{x_1} \times \mathcal{G}_{a,b}^{x'_1}\}$, equivalently with $(x, y) \circ (x', y') = (x_1, y_1) \circ (x'_1, y'_1)$. By consequence, the hyperoperation “ \circ ” is well defined.

If $X = (a, \infty)$ or $Y = (a, \infty)$ or $Z = (a, \infty)$, then the associativity is obvious. If not, we have the following cases.

Case 1: $|J| = 1$.

This means that $\mathcal{H}_{a,b}(F) = \mathcal{H}_{a',b'}(F) = \mathcal{H}_{a'',b''}(F)$ and we have

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

Similarly, it holds that

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

On the other hand we have

$$\begin{aligned} L_{a,b}(\widehat{x_i}, \widehat{x'_j}) \cap L_{a,b}(\widehat{x_i \bullet_{ab} x'_j}, \widehat{\mathcal{O}}) &= \{(x_i \bullet_{ab} x'_j, 0)\} \subseteq L_0, \\ L_{a,b}(\widehat{x'_j}, \widehat{x''_k}) \cap L_{a,b}(\widehat{\mathcal{O}}, \widehat{x'_j \bullet_{ab} x''_k}) &= \{(x'_j \bullet_{ab} x''_k, 0)\} \subseteq L_0. \end{aligned}$$

In other words, for the six points $p_1 = \widehat{x_i}, p_2 = \widehat{x'_j}, p_3 = \widehat{x''_k}, p_4 = \widehat{x_i \bullet_{ab} x'_j}, p_5 = \widehat{\mathcal{O}}$ and $p_6 = \widehat{x'_j \bullet_{ab} x''_k}$ on the curve we have $L_{a,b}(p_1, p_2) \cap L_{a,b}(p_4, p_5) \subseteq L_0$ and $L_{a,b}(p_2, p_3) \cap L_{a,b}(p_5, p_6) \subseteq L_0$ and therefore, by Pascal's theorem (see Theorem 1), it follows also that $L_{a,b}(p_3, p_4) \cap L_{a,b}(p_6, p_1) \subseteq L_0$, equivalently with

$$L_{a,b}(\widehat{x''_k}, \widehat{x_i \bullet_{ab} x'_j}) \cap L_{a,b}(\widehat{x'_j \bullet_{ab} x''_k}, \widehat{x_i}) \subseteq L_0.$$

By Definition 8 we know that

$$\begin{aligned} \{(x_i \bullet_{ab} x'_j) \bullet_{ab} x''_k, 0\} &= L_0 \cap L_{a,b}(\widehat{x_i \bullet_{ab} x'_j}, \widehat{x''_k}), \\ \{(x_i \bullet_{ab} (x'_j \bullet_{ab} x''_k)), 0\} &= L_0 \cap L_{a,b}(\widehat{x_i}, \widehat{x'_j \bullet_{ab} x''_k}) \end{aligned}$$

where, by the associativity of the group operation " \bullet_{ab} ", it holds $(x_i \bullet_{ab} x'_j) \bullet_{ab} x''_k = x_i \bullet_{ab} (x'_j \bullet_{ab} x''_k)$. This leads to the equality

$$L_0 \cap L_{a,b}(\widehat{x_i \bullet_{ab} x'_j}, \widehat{x''_k}) = L_{a,b}(\widehat{x''_k}, \widehat{x_i \bullet_{ab} x'_j}) \cap L_{a,b}(\widehat{x'_j \bullet_{ab} x''_k}, \widehat{x_i}) = L_0 \cap L_{a,b}(\widehat{x_i}, \widehat{x'_j \bullet_{ab} x''_k}),$$

implying that

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

Case 2: $|J| = 2$.

(i) If $\mathcal{H}_{a,b}(F) = \mathcal{H}_{a',b'}(F) \neq \mathcal{H}_{a'',b''}(F)$, then we have

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

On the other hand

$$\begin{aligned} (x, y) \circ [(x', y') \circ (x'', y'')] &= (x, y) \circ (\mathcal{H}_{a',b'}(F) \cup \mathcal{H}_{a'',b''}(F)) \\ &= (x, y) \circ \mathcal{H}_{a',b'}(F) \cup (x, y) \circ \mathcal{H}_{a'',b''}(F) \\ &= \mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a'',b''}(F). \end{aligned}$$

- (ii) If $\mathcal{H}_{a,b}(F) \neq \mathcal{H}_{a',b'}(F) = \mathcal{H}_{a'',b''}(F)$, then the associativity holds, similarly as in the case (i).
 (iii) If $\mathcal{H}_{a,b}(F) = \mathcal{H}_{a'',b''}(F) \neq \mathcal{H}_{a',b'}(F)$, then we have

$$\begin{aligned} [(x, y) \circ (x', y')] \circ (x'', y'') &= (\mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F)) \circ (x'', y'') \\ &= \mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F) \cup \mathcal{H}_{a'',b''}(F) \\ &= \mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F) \end{aligned}$$

and similarly

$$\begin{aligned} (x, y) \circ [(x', y') \circ (x'', y'')] &= (x, y) \circ (\mathcal{H}_{a',b'}(F) \cup \mathcal{H}_{a'',b''}(F)) \\ &= \mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F) \cup \mathcal{H}_{a'',b''}(F) \\ &= \mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F). \end{aligned}$$

Case 3: $|J| = 3$.

In this case we have

$$\begin{aligned} [(x, y) \circ (x', y')] \circ (x'', y'') &= (\mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F)) \circ (x'', y'') \\ &= \mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F) \cup \mathcal{H}_{a'',b''}(F). \end{aligned}$$

On the other hand

$$\begin{aligned} (x, y) \circ [(x', y') \circ (x'', y'')] &= (x, y) \circ (\mathcal{H}_{a',b'}(F) \cup \mathcal{H}_{a'',b''}(F)) \\ &= \mathcal{H}_{a,b}(F) \cup \mathcal{H}_{a',b'}(F) \cup \mathcal{H}_{a'',b''}(F). \end{aligned}$$

Therefore the hyperoperation " \circ " is associative.

In order to prove the reproduction axiom, we consider two cases as below:

Case 1. If $|\bar{A} \times \bar{B}| = 1$, then $\bar{F} = F$ and $\mathcal{H}_{\bar{A},\bar{B}}(F) = \mathcal{H}_{a,b}(F)$, where $a \in \bar{A}, b \in \bar{B}$. It follows that $(\mathcal{H}_{a,b}(F), \circ)$ is a homography group, so the reproduction axiom holds.

Case 2. If $|\bar{A} \times \bar{B}| > 1$, consider an arbitrary element $\hat{x} \in \mathcal{H}_{a,b}(F) \subseteq \mathcal{H}_{\bar{A},\bar{B}}(F)$. Then

$$\begin{aligned} \hat{x} \circ \mathcal{H}_{\bar{A},\bar{B}}(F) &= (\hat{x} \circ \bigcup_{a \neq i \in \bar{A}, b \neq j \in \bar{B}} \mathcal{H}_{i,j}(F)) \cup (\hat{x} \circ \mathcal{H}_{a,b}(F)), \\ &= (\bigcup_{a \neq i \in \bar{A}, b \neq j \in \bar{B}} \hat{x} \circ \mathcal{H}_{i,j}(F)) \cup \mathcal{H}_{a,b}(F), \\ &= (\bigcup_{i \in \bar{A}, j \in \bar{B}} \mathcal{H}_{i,j}(F)) \cup \mathcal{H}_{a,b}(F), \\ &= \mathcal{H}_{\bar{A},\bar{B}}(F). \end{aligned}$$

Similarly, $(\mathcal{H}_{\bar{A},\bar{B}}(F)) \circ \hat{x} = \mathcal{H}_{\bar{A},\bar{B}}(F)$ and thus the reproduction axiom is proved. Therefore, $(\mathcal{H}_{\bar{A},\bar{B}}(F), \circ)$ is a hypergroup. \square

Remark 2. If $G = \{1\}$, then the hyperhomography and the associated hypergroup are the classical homography and the homography group, respectively.

Example 5. Let us consider again Example 3, where we deal with the nondegenerate hyperhomography $H_{0,\bar{1}}(F)$ as a subset of F^2 , having the form $H_{0,\bar{1}}(F) = H_{0,1}(F) \cup H_{0,4}(F)$ where, $H_{0,1}(F) = \{(0, \infty), (1, 2), (2, 4), (3, 3)\}$ and $H_{0,4}(F) = \{(0, \infty), (2, 2), (3, 1), (4, 3)\}$, while the associated equipped hyperhomography is $\mathcal{H}_{0,\bar{1}}(F) = \mathcal{H}_{0,1}(F) \cup \mathcal{H}_{0,4}(F)$ where,

$$\mathcal{H}_{0,1}(F) = \{\widehat{\mathcal{O}}, (1,2), (2,4), (3,3)\}, \quad \mathcal{H}_{0,4}(F) = \{\widehat{\mathcal{O}}, (2,2), (3,1), (4,3)\},$$

for $\widehat{\mathcal{O}} = (\mathcal{O}, f_{a,b}(\mathcal{O})) = (\bar{0}, f_{a,b}(\bar{0})) = (\bar{0}, \infty) = (0, \infty)$.

Now let $T = \mathcal{H}_{0,1}(F)$ and $K = \mathcal{H}_{0,4}(F)$. Then (T, \circ) and (K, \circ) are reversible subhypergroups of $(\mathcal{H}_{\bar{0},\bar{1}}(F), \circ)$, which are defined by the following Cayley tables, respectively

(T, \circ)	(0, ∞)	(1, 2)	(2, 4)	(3, 3)
(0, ∞)	(0, ∞)	(1, 2), (2, 4)	(1, 2), (2, 4)	(3, 3)
(1, 2)	(1, 2), (2, 4)	(0, ∞), (3, 3)	(0, ∞), (3, 3)	(1, 2), (2, 4)
(2, 4)	(1, 2), (2, 4)	(0, ∞), (3, 3)	(0, ∞), (3, 3)	(1, 2), (2, 4)
(3, 3)	(3, 3)	(1, 2), (2, 4)	(1, 2), (2, 4)	(0, ∞)
(K, \circ)	(0, ∞)	(2, 2)	(3, 1)	(4, 3)
(0, ∞)	(0, ∞)	(2, 2)	(3, 1), (4, 3)	(3, 1), (4, 3)
(2, 2)	(2, 2)	(0, ∞)	(3, 1), (4, 3)	(3, 1), (4, 3)
(3, 1)	(3, 1), (4, 3)	(3, 1), (4, 3)	(0, ∞), (2, 2)	(0, ∞), (2, 2)
(4, 3)	(3, 1), (4, 3)	(3, 1), (4, 3)	(0, ∞), (2, 2)	(0, ∞), (2, 2)

For a better understanding, we will explain all details in computing, for example, in the table of T the hyperproduct $(1,2) \circ (2,4)$. For doing this, since $T = \mathcal{H}_{0,1}(F)$, we use the function $f_{0,1}(x) = 1 + \frac{1}{x}$ and the field $F = \mathbb{Z}_5$. Based on Corollary 1, we obtain

$$\mathcal{G}_{0,1}^1 = \{1, \frac{-1}{1+1}\} = \{1, -2^{-1}\} = \{1, -3\} = \{1, 2\},$$

$$\mathcal{G}_{0,1}^2 = \{2, \frac{-2}{2+1}\} = \{2, -2 \cdot 3^{-1}\} = \{2, -4\} = \{2, 1\},$$

and therefore,

$$(1,2) \circ (2,4) = \{\widehat{x_i \bullet_{01} x_j} \mid x_i \in \mathcal{G}_{0,1}^1, x_j \in \mathcal{G}_{0,1}^2\} = \{\widehat{1 \bullet_{01} 1}, \widehat{1 \bullet_{01} 2}, \widehat{2 \bullet_{01} 1}, \widehat{2 \bullet_{01} 2}\}.$$

Based on Proposition 1, we have

$$\begin{aligned} 1 \bullet_{01} 1 &= 1 \cdot 1 \cdot 1 - (-1) \cdot (1 + 1 - 0) = 3 \\ 1 \bullet_{01} 2 &= 1 \cdot 1 \cdot 2 - (-1) \cdot (1 + 2 - 0) = 5 = 0 \\ 2 \bullet_{01} 1 &= 1 \cdot 2 \cdot 1 - (-1) \cdot (2 + 1 - 0) = 5 = 0 \\ 2 \bullet_{01} 2 &= 1 \cdot 2 \cdot 2 - (-1) \cdot (2 + 2 - 0) = 8 = 3 \end{aligned}$$

which imply that

$$(1,2) \circ (2,4) = \{(3, f_{0,1}(3)), (0, f_{0,1}(0))\} = \{(3, 1 + \frac{1}{3}), (0, \infty)\} = \{(3,3), (0, \infty)\}.$$

Similarly, all the other hyperproducts in both tables can be obtained.

The next result gives a characterization of the subhypergroups of the equipped hyperhomographies in F^2 .

Theorem 4. Let H be a non-empty subset of the hypergroup $\mathcal{H}_{\bar{A},\bar{B}}(F)$. Then H is a subhypergroup of the equipped hyperhomography $\mathcal{H}_{\bar{A},\bar{B}}(F)$ if and only if it can be written as $H = \bigcup_{(i,j) \in I \subseteq \bar{A} \times \bar{B}} \mathcal{H}_{i,j}(F)$, where $I = \{(i,j) \in \bar{A} \times \bar{B} \mid H \cap \mathcal{H}_{i,j}(F) \neq \emptyset\}$, or H is a subhypergroup of $\mathcal{H}_{i,j}(F)$, for some $(i,j) \in \bar{A} \times \bar{B}$.

Proof. (\Rightarrow). Suppose that H is a subhypergroup of $\mathcal{H}_{\bar{A},\bar{B}}(F)$ and $H \not\subseteq \mathcal{H}_{i,j}(F)$, for every (i,j) in $\bar{A} \times \bar{B}$. There exist $(i',j') \neq (s',t')$ in $\bar{A} \times \bar{B}$ such that $H \cap \mathcal{H}_{i',j'}(F) \neq \emptyset \neq H \cap \mathcal{H}_{s',t'}(F)$. Now let $I = \{(i,j) \in \bar{A} \times \bar{B} \mid H \cap \mathcal{H}_{i,j}(F) \neq \emptyset\}$. Thus we have $H \subseteq \bigcup_{(i,j) \in I} \mathcal{H}_{i,j}(F) \subseteq \bigcup_{(i',j'),(s',t') \in I} (\mathcal{H}_{i',j'}(F) \cap H) \circ (\mathcal{H}_{s',t'}(F) \cap H) \subseteq H$. Hence $H = \bigcup_{(i,j) \in I} \mathcal{H}_{i,j}(F)$.

(\Leftarrow). It is obvious. \square

Theorem 5. Let H be a subhypergroup of the hypergroup $\mathcal{H}_{\bar{A},\bar{B}}(F)$. Then H is reversible if and only if H is a subhypergroup of $\mathcal{H}_{a,b}(F)$, for some $(a,b) \in \bar{A} \times \bar{B}$.

Proof. (\Leftarrow). First we prove that any subhypergroup H of $\mathcal{H}_{a,b}(F)$ is a regular reversible hypergroup, for any $(a,b) \in \bar{A} \times \bar{B}$. The regularity is clear, because \widehat{O} is an identity and each element is an inverse for itself. In order to prove the reversibility, let $\hat{x} = (x,y)$ and $\hat{x}' = (x',y')$ be arbitrary elements in $\mathcal{H}_{a,b}(F)$. We distinguish three different situations.

Case 1. If $x' \notin \mathcal{G}_{a,b}^x = \{x, \alpha\}$, where $x \bullet_{ab} \alpha = a$, then

$$\begin{aligned} \widehat{x''} = (x'', y'') \in (x, y) \circ (x', y') &\implies (x'', y'') = \widehat{z \bullet_{ab} w}, \text{ with } (z, w) \in \mathcal{G}_{a,b}^x \times \mathcal{G}_{a,b}^{x'} \\ &\implies x'' = z \bullet_{ab} w, \\ &\implies z = x'' \bullet_{ab} h, \text{ where } w \bullet_{ab} h = a, \\ &\implies (z, f_{a,b}(z)) = \widehat{x'' \bullet_{ij} h} \text{ and } h \in \mathcal{G}_{a,b}^w = \mathcal{G}_{a,b}^{x'}, z \in \mathcal{G}_{a,b}^x \\ &\implies (z, f_{a,b}(z)) \in (x'', f_{a,b}(x'')) \circ (h, f_{a,b}(h)) \\ &\implies (x, y) \in (x'', f_{a,b}(x'')) \circ (h, f_{a,b}(h)) \end{aligned}$$

Case 2. If $x' \in \mathcal{G}_{a,b}^x = \{x, \alpha\}$, then $\widehat{x''} = (x'', y'') \in (x, y) \circ (x', y') \implies (x'', y'') = \widehat{z \bullet_{ab} w}$, with $z, w \in \mathcal{G}_{a,b}^x$. Thus $(x'', y'') \in \{\widehat{x \bullet_{ab} x}, \widehat{\alpha \bullet_{ab} \alpha}, \widehat{O}\}$. It follows that $\hat{x} \in \widehat{x''} \circ \hat{\alpha}$.

Case 3. If $(x, y) = O$, then $Y \in \widehat{O} \circ X = X \circ \widehat{O}$, implying that $\widehat{O} \in Y \circ X$ and $X \in \widehat{O} \circ Y$. Notice that $\widehat{O} \in X \circ X$, for all $X \in \mathcal{H}_{i,j}(F)$ (i.e. every element is one of its inverses).

(\Rightarrow). Suppose that H is a reversible subhypergroup of $\mathcal{H}_{\bar{A},\bar{B}}(F)$ such that it is not a subhypergroup of any $\mathcal{H}_{a,b}(F)$, with $(a,b) \in \bar{A} \times \bar{B}$. Based on Theorem 4, we have $H = \bigcup_{(i,j) \in I \subseteq \bar{A} \times \bar{B}} \mathcal{H}_{i,j}(F)$, where $I = \{(i,j) \in \bar{A} \times \bar{B} \mid H \cap \mathcal{H}_{i,j}(F) \neq \emptyset\}$. Let $(x,y), (x',y')$ be arbitrary elements in $H \cap \mathcal{H}_{i,j}(F)$ and $H \cap \mathcal{H}_{s,t}(F)$, respectively, that are not equal to \widehat{O} , with $(i,j) \neq (s,t)$. If $(x'',y'') \in ((x,y) \circ (x',y')) \cap \mathcal{H}_{i,j}(F)$, then, based on the reversibility, we have $(x',y') \in (z,w) \circ (x'',y'') \subseteq \mathcal{H}_{i,j}(F)$, where $z \in \mathcal{G}_{a,b}^x$, hence $(x',y') \in \mathcal{H}_{i,j}(F) \cap \mathcal{H}_{s,t}(F) = \{\widehat{O}\}$. Thus $(x',y') = \widehat{O}$, which is in contradiction with the supposition that $(x',y') \neq \widehat{O}$. Therefore $H \leq \mathcal{H}_{i,j}(F)$, for some $(i,j) \in \bar{A} \times \bar{B}$. \square

In the following we will present two new hypergroup structures isomorphic with the equipped homography $\mathcal{H}_{a,b}(F)$ in the case when $b \neq 0$ and $b = 0$, respectively.

Theorem 6. Consider the field F and define on $F^* = F \setminus \{0\}$ the hyperoperation

$$\forall x, x' \in F^*, x \odot x' = \{xx', \frac{x}{x'}, \frac{x'}{x}, \frac{1}{xx'}\}.$$

Then, for every $b \neq 0$, there is the homomorphism $(\mathcal{H}_{a,b}(F), \circ) \cong (F^*, \odot)$.

Proof. It is easy to see that (F^*, \odot) is a hypergroup. Now, taking $v = a - b^{-1}$, consider the bijective function $\varphi : F \setminus \{v\} \rightarrow F^*$ defined by $\varphi(x) = bx + 1 - ab$ and the function $\zeta : \mathcal{H}_{a,b}(F) \rightarrow \Gamma(\varphi)$ defined by $\zeta((x, y)) = (x, \varphi(x))$, where $\Gamma(\varphi) = \{(x, \varphi(x)) \mid x \in F \setminus \{v\}\}$ and $\zeta((a, \infty)) = (a, 1) = \zeta((\bar{A}, \infty)) = \zeta(\bar{O})$. Geometrically, $\Gamma(\varphi)$ is the graph of the function φ , thus it is the line passing through the points of $(v, 0)$ and $(a, 1)$, while ζ is the map that projects the points of the hyperhomography $\mathcal{H}_{a,b}(F)$ on the above mentioned line.

Thus, using Proposition 1, for all $x_i, x_j \in F \setminus \{v\}$, we have

$$\begin{aligned} \varphi(x_i \bullet_{a,b} x_j) &= b(x_i \bullet_{a,b} x_j) + 1 - ab, \\ &= b(bx_i x_j - (ab - 1)(x_i + x_j - a)) + 1 - ab \\ &= (bx_i + 1 - ab)(bx_j + 1 - ab) \\ &= \varphi(x_i)\varphi(x_j). \end{aligned}$$

Now suppose that $(x, y), (x', y')$ are arbitrary elements in $\mathcal{H}_{a,b}(F)$. It follows that

$$\begin{aligned} \zeta((x, y) \circ (x', y')) &= \{\zeta(\widehat{x_i \bullet_{a,b} x_j}) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\} \\ &= \{(x_i \bullet_{a,b} x_j, \varphi(x_i \bullet_{a,b} x_j)) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\} \\ &= \{(x_i \bullet_{a,b} x_j, \varphi(x_i)\varphi(x_j)) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\}. \end{aligned}$$

Take now $\Pi : F \times F^* \rightarrow F^*$ with $\Pi((x, y)) = y$ as the projection map on the second component and define $\psi : \mathcal{H}_{a,b}(F) \rightarrow F^*$ by $\psi = \Pi \circ \zeta$.

We have $\psi((x, y)) = \varphi(x)$, for all $(x, y) \in \mathcal{H}_{a,b}(F)$, thus ψ is a bijective map and also a homomorphism because

$$\begin{aligned} \psi((x, y) \circ (x', y')) &= \Pi(\zeta((x, y) \circ (x', y'))) \\ &= \{\varphi(x_i)\varphi(x_j) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\} \\ &= \{\varphi(x_i)\varphi(x_j) \mid \varphi(x_i) \in \varphi(\mathcal{G}_{a,b}^x), \varphi(x_j) \in \varphi(\mathcal{G}_{a,b}^{x'})\} (\varphi \text{ is bijective map}) \\ &= \{\varphi(x_i)\varphi(x_j) \mid \varphi(x_i) \in \{\varphi(x), \frac{1}{\varphi(x)}\}, \varphi(x_j) \in \{\varphi(x'), \frac{1}{\varphi(x')}\}\} \\ &= \varphi(x) \odot \varphi(x') \\ &= \psi((x, y)) \odot \psi((x', y')). \end{aligned}$$

Therefore $(\mathcal{H}_{a,b}(F), \circ)$ is isomorphic to (F^*, \odot) . \square

Theorem 7. Consider the field F and define on $F^* = F \setminus \{0\}$ the hyperoperation

$$\forall x, x' \in F, x \odot x' = \{x + x', x - x', -x + x', -x - x'\}.$$

Then, if $b = 0$, there is the homomorphism $(\mathcal{H}_{a,b}(F), \circ) \cong (F, \otimes)$.

Proof. Clearly, (F, \otimes) is a hypergroup. Consider the bijective function $\varphi : F \rightarrow F$ defined by $\varphi(x) = x - a$ and be $\Gamma(\varphi) = \{(x, \varphi(x)) \mid x \in F\}$ its graph. Besides define $\zeta : \mathcal{H}_{a,b}(F) \rightarrow \Gamma(\varphi)$ by $\zeta((x, y)) = (x, \varphi(x))$, where $\zeta((a, \infty)) = (a, 0) = \zeta((\bar{A}, \infty))$. Therefore, for all $x_i, x_j \in F$, we have

$$\begin{aligned} \varphi(x_i \bullet_{a,b} x_j) &= (x_i \bullet_{a,b} x_j) - a, \\ &= (x_i + x_j - a) - a \\ &= (x_i - a) + (x_j - a) \\ &= \varphi(x_i) + \varphi(x_j) \end{aligned}$$

and for all $(x, y), (x', y') \in \mathcal{H}_{a,b}(F)$

$$\begin{aligned} \zeta((x, y) \circ (x', y')) &= \{\zeta(\widehat{x_i \bullet_{a,b} x_j}) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\}, \\ &= \{(x_i \bullet_{a,b} x_j, \varphi(x_i \bullet_{a,b} x_j)) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\}, \\ &= \{(x_i \bullet_{a,b} x_j, \varphi(x_i) + \varphi(x_j)) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\}. \end{aligned}$$

As in the previous theorem, let $\Pi : F \times F \rightarrow F$, $\Pi((x, y)) = y$ be the projection map on second component and define $\psi : \mathcal{H}_{a,b}(F) \rightarrow F$ by $\psi = \Pi \circ \zeta$.

Therefore, for all $(x, y) \in \mathcal{H}_{a,b}(F)$, $\psi((x, y)) = \varphi(x)$ and thus ψ is a bijective map. We claim that ψ is a homomorphism, too, because

$$\begin{aligned} \psi((x, y) \circ (x', y')) &= \Pi(\zeta((x, y) \circ (x', y'))) \\ &= \{\varphi(x_i) + \varphi(x_j) \mid x_i \in \mathcal{G}_{a,b}^x, x_j \in \mathcal{G}_{a,b}^{x'}\} \\ &= \{\varphi(x_i) + \varphi(x_j) \mid \varphi(x_i) \in \varphi(\mathcal{G}_{a,b}^x), \varphi(x_j) \in \varphi(\mathcal{G}_{a,b}^{x'})\} \text{ (}\psi \text{ is bijective map)} \\ &= \{\varphi(x_i) + \varphi(x_j) \mid \varphi(x_i) \in \{\varphi(x), -\varphi(x)\}, \varphi(x_j) \in \{\varphi(x'), -\varphi(x')\}\} \\ &= \varphi(x) \odot \varphi(x') \\ &= \psi((x, y)) \circ \psi((x', y')). \end{aligned}$$

Therefore $(\mathcal{H}_{a,b}(F), \circ)$ is isomorphic with (F^*, \otimes) . \square

4. Associated H_v -Groups

Vougiouklis [13] introduced the notion of H_v -group as a generalization of the notion of hypergroup, substituting the associativity of the hyperoperation with the weak associativity, i.e., $a \circ (b \circ c) \cap (a \circ b) \circ c \neq \emptyset$ for all $a, b, c \in H$. The motivation of introducing this hyperstructure is the following one. We know that the quotient of a group with respect to a normal subgroup is a group, while the quotient of a group with respect to any subgroup is a hypergroup. Vougiouklis stated that the quotient of a group with respect to any partition of the group is an H_v -group.

In the following we equip the hyperhomography $\mathcal{H}_{\bar{A}, \bar{B}}(\bar{F}) = \bigcup_{(a,b) \in \bar{A} \times \bar{B}} \mathcal{H}_{a,b}(\bar{F})$ as a subset of $\bar{F}^2 \cup \{\widehat{\mathcal{O}}\}$ with an H_v -group structure, by defining the following hyperoperation

$$(\bar{x}, \bar{y}) \bar{\circ} (\bar{x}', \bar{y}') = \{(\bar{u}, \bar{v}) \mid (u, v) \in (\bar{x} \times \bar{y}) \circ (\bar{x}' \times \bar{y}')\}.$$

Notice that

$$(x, y) = \widehat{\mathcal{O}} \iff (\bar{x}, \bar{y}) = \widehat{\mathcal{O}} \iff \bar{x} \times \bar{y} = \widehat{\mathcal{O}},$$

and

$$(c, d) \notin (\bar{x} \times \bar{y}) \cap \mathcal{H}_{a,b}(F) \text{ or } (c', d') \notin (\bar{x}' \times \bar{y}') \cap \mathcal{H}_{a',b'}(F) \implies (c, d) \circ (c', d') = \mathcal{O}.$$

Moreover according with Theorem 2, the hyperoperation $\bar{\circ}$ is well defined on $\mathcal{H}_{\bar{A},\bar{B}}(\bar{F})$ and in addition we have

$$\overline{(x, y) \circ (x', y')} \subseteq (\bar{x}, \bar{y}) \bar{\circ} (\bar{x}', \bar{y}').$$

Proposition 2. $(\mathcal{H}_{\bar{A},\bar{B}}(\bar{F}), \bar{\circ})$ is an H_v -group.

Proof. Let $(x, y), (x', y')$ and (x'', y'') be elements in $\mathcal{H}_{\bar{A},\bar{B}}(\bar{F})$. Then we have

$$\overline{(x, y) \circ (x', y') \circ (x'', y'')} \subseteq [(\bar{x}, \bar{y}) \bar{\circ} (\bar{x}', \bar{y}')] \bar{\circ} (\bar{x}'', \bar{y}'') \cap (\bar{x}, \bar{y}) \bar{\circ} [(\bar{x}', \bar{y}') \bar{\circ} (\bar{x}'', \bar{y}'')].$$

□

Proposition 3. Let $\psi_{\bar{A},\bar{B}} : \mathcal{H}_{\bar{A},\bar{B}}(F) \rightarrow \mathcal{H}_{\bar{A},\bar{B}}(\bar{F}), \psi_{\bar{A},\bar{B}}(x, y) = (\bar{x}, \bar{y})$. Then $\psi_{\bar{A},\bar{B}}$ is an epimorphism of H_v -groups.

Proof. Suppose that (x, y) and (x', y') belong to $\mathcal{H}_{\bar{A},\bar{B}}(F)$. We have

$$\begin{aligned} \psi_{\bar{A},\bar{B}}((x, y) \circ (x', y')) &= \{(\bar{u}, \bar{v}) \mid (u, v) \in (x, y) \circ (x', y')\} \\ &\subseteq (\bar{x}, \bar{y}) \bar{\circ} (\bar{x}', \bar{y}') \\ &= \psi_{\bar{A},\bar{B}}(x, y) \bar{\circ} \psi_{\bar{A},\bar{B}}(x', y'). \end{aligned}$$

□

Example 6. If we consider the hyperhomography $\mathcal{H}_{\bar{0},\bar{1}}(\bar{F}) = \{\widehat{\mathcal{O}}, (\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})\}$, then after long calculations similarly s those in Example 5, we get the following H_v -group table.

$\bar{\circ}$	$\widehat{\mathcal{O}}$	$(\bar{1}, \bar{2})$	$(\bar{2}, \bar{1})$	$(\bar{2}, \bar{2})$
$\widehat{\mathcal{O}}$	$\widehat{\mathcal{O}}$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1})$	$(\bar{2}, \bar{2})$
$(\bar{1}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1})$	$\mathcal{H}_{\bar{0},\bar{1}}(\bar{F})$	$\mathcal{H}_{\bar{0},\bar{1}}(\bar{F})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$
$(\bar{2}, \bar{1})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1})$	$\mathcal{H}_{\bar{0},\bar{1}}(\bar{F})$	$\mathcal{H}_{\bar{0},\bar{1}}(\bar{F})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$
$(\bar{2}, \bar{2})$	$(\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$	$(\bar{1}, \bar{2}), (\bar{2}, \bar{1}), (\bar{2}, \bar{2})$	$\mathcal{H}_{\bar{0},\bar{1}}(\bar{F})$

Proposition 4. On $\mathcal{H}_{a,a}(F)$, as a subset of $\mathcal{H}_{\bar{A},\bar{A}}(\bar{F})$, define the hyperoperation

$$(x, y) \cdot (x', y') = \begin{cases} \{\widehat{x \bullet_{aa} x'}, \widehat{y \bullet_{aa} y'}\}, & \text{if } \mathcal{O} \notin \{(x, y), (x', y')\} \\ (x, y), & \text{if } (x', y') = \mathcal{O} \\ (x', y'), & \text{if } (x, y) = \mathcal{O}. \end{cases}$$

Then $(\mathcal{H}_{a,a}(F), \cdot)$ is an H_v - group.

Proof. First we prove that, if $\mathcal{O} \neq \widehat{x}$ and $\widehat{x} \in \mathcal{H}_{a,a}(F)$, then $\widehat{f_{a,a}(x)} \in \mathcal{H}_{a,a}(F)$. To this aim, consider an arbitrary element $\widehat{x} \in \mathcal{H}_{a,a}(F)$ not equal to \mathcal{O} and notice that $f_{a,a}^2 = id_F$. Then

$$\begin{aligned}
 \hat{x} \in \mathcal{H}_{a,a}(F) &\implies (x, y) \in \mathcal{H}_{a,a}(F), y = f_{a,a}(x) \\
 &\implies f_{a,a}(y) = f_{a,a}(f_{a,a}(x)) \\
 &\implies f_{a,a}(y) = (f_{a,a} \circ f_{a,a})(x) \\
 &\implies f_{a,a}(y) = x \\
 &\implies (y, x) \in \mathcal{H}_{a,a}(F), x = f_{a,a}(y) \\
 &\implies \hat{y} \in \mathcal{H}_{a,a}(F) \\
 &\implies \widehat{f_{a,a}(x)} \in \mathcal{H}_{a,a}(F).
 \end{aligned}$$

Consequently, $(x, y) \cdot (x', y') \subseteq \mathcal{H}_{a,a}(F)$, for all $(x, y), (x', y') \in \mathcal{H}_{a,a}(F)$ and “ \cdot ” is well defined. Now, let $(x, y), (x', y'), (x'', y'')$ belong to $\mathcal{H}_{a,a}(F)$. We get

$$\{x \bullet_{aa} \widehat{x'}, y \bullet_{aa} \widehat{y''}\} \subseteq ((x, y) \cdot (x', y')) \cdot (x'', y'') \cap ((x, y) \cdot [(x', y') \cdot (x'', y'')]) \neq \emptyset,$$

thus the weak associativity condition holds. It can easily be seen that the reproduction axiom is valid, too. \square

Example 7. The Cayley table of the H_v -group $(\mathcal{H}_{0,0}(F), \cdot)$ where, $F = \mathbb{Z}_5$ is again the field of order 5, is as follows:

\cdot	$\widehat{\mathcal{O}}$	(1, 1)	(2, 3)	(3, 2)	(4, 4)
$\widehat{\mathcal{O}}$	$\widehat{\mathcal{O}}$	(1, 1)	(2, 3)	(3, 2)	(4, 4)
(1, 1)	(1, 1)	(2, 3)	(3, 2), (4, 4)	(3, 2), (4, 4)	$\widehat{\mathcal{O}}$
(2, 3)	(2, 3)	(3, 2), (4, 4)	(1, 1), (4, 4)	$\widehat{\mathcal{O}}$	(1, 1), (2, 3)
(3, 2)	(3, 2)	(3, 2), (4, 4)	$\widehat{\mathcal{O}}$	(1, 1), (4, 4)	(2, 3), (1, 1)
(4, 4)	(4, 4)	$\widehat{\mathcal{O}}$	(1, 1), (2, 3)	(1, 1), (2, 3)	(3, 2)

In this table, we have $\widehat{\mathcal{O}} \cdot (x, y) = (x, y) = (x, y) \cdot \widehat{\mathcal{O}}$, for all $(x, y) \in \mathcal{H}_{0,0}(F)$ and

$$(x, y) \cdot (x', y') = \{(x + x', (x + x')^{-1}), (y + y', (y + y')^{-1})\},$$

for all $(x, y), (x', y') \in \mathcal{H}_{0,0}(F) \setminus \{\widehat{\mathcal{O}}\}$. The hyperoperation is not associative, but only weak associative, as we can notice here below:

$$\widehat{\mathcal{O}} = [(1, 1) \cdot (1, 1)] \cdot (3, 2) \neq [(1, 1) \cdot [(1, 1) \cdot (3, 2)]] = \{\widehat{\mathcal{O}}, (3, 2), (4, 4)\}.$$

5. Conclusions

In the last few years, researchers in the hypercompositional structure theory have investigated, principally from a theoretical point of view, all types of hyperrings: general hyperrings [20], multiplicative hyperrings [15], additive hyperrings [21], superrings [22], but till now, only the Krasner hyperrings have found interesting and useful applications in number theory, algebraic geometry, scheme theory, as mentioned in the introductory part of this article. Here the authors continue the study on the research topic started in [1] about elliptic hypercurves defined on quotient Krasner hyperfield, with applications in cryptography [8]. In a similar way, the notion of a homography on a field is extended to hyperhomography over Krasner hyperfields. More exactly, considering an

arbitrary field F and a normal subgroup G of its multiplicative group, we get a Krasner hyperfield $\bar{F} = F/G$. Then the homography $H_{a,b}(F) = \{(x, y) \in F^2 \mid y = f_{a,b}(x) = b + \frac{1}{x-a}\}$, where $a, b \in F$ is naturally extended to the hyperhomography $H_{\bar{A},\bar{B}}(\bar{F}) = \{(\bar{x}, \bar{y}) \in \bar{F}^2 \mid \bar{1} \in (\bar{x} \ominus \bar{A}) \odot (\bar{y} \ominus \bar{B})\}$ over the hyperfield (\bar{F}, \oplus, \odot) . Besides, the group operation on a homography leads to a hyperoperation on the associated equipped hyperhomography $\mathcal{H}_{\bar{A},\bar{B}}(\bar{F})$, that becomes a hypergroup. Then, all reversible subhypergroups of an equipped hyperhomography are characterized. In the last part of the paper, other hyperoperations are defined on hyperhomographies and their properties are investigated in connection with weak associativity.

Author Contributions: Conceptualization, V.V., M.J. and I.C.; Funding acquisition, I.C.; Investigation, V.V. and M.J.; Methodology, I.C.; Writing—original draft, V.V. and M.J.; Writing—review & editing, I.C.

Funding: The third author acknowledges the financial support from the Slovenian Research Agency (research core funding No. P1 - 0285).

Conflicts of Interest: The authors declare no conflict of interest.

References

- Vahedi, V.; Jafarpour, M.; Aghabozorgi, H.; Cristea, I. Extension of elliptic curves on Krasner hyperfields. *Commun. Alg.* **2019**, *47*, 4806–4823. [[CrossRef](#)]
- Connes, A.; Consani, C. The hyperring of adèle classes. *J. Number Theory* **2011**, *131*, 159–194. [[CrossRef](#)]
- Al Tahan, M.; Davvaz, B. On the existence of hyperrings associated with arithmetic functions. *J. Number Theory* **2017**, *174*, 136–149. [[CrossRef](#)]
- Viro, O. On basic concepts of tropical geometry. *Proc. Steklov Inst. Math.* **2011**, *273*, 252–282. [[CrossRef](#)]
- Jun, J. Algebraic geometry over hyperrings. *Adv. Math.* **2018**, *323*, 142–192. [[CrossRef](#)]
- Krasner, M. A class of hyperrings and hyperfields. *Int. J. Math. Math. Sci.* **1983**, *6*, 307–311. [[CrossRef](#)]
- Massouros, C.G. On the theory of hyperrings and hyperfields. *Algebra i Logika* **1985**, *24*, 728–742. [[CrossRef](#)]
- Berardi, L.; Eugeni, F.; Innamorati, S. Remarks on Hypergroupoids and Cryptography. *J. Combin. Inf. Syst. Sci.* **1992**, *17*, 217–231.
- Corsini, P. *Prolegomena of Hypergroup Theory*; Aviani Editore: Tricesimo, Italy, 1993.
- Hankerson, D.; Menezes, A.; Vanstone, S.A. *Guide to Elliptic Curve Cryptography*, Springer: Berlin, Germany, 2004.
- Koblitz, N. *Introduction to Elliptic Curves and Modular Forms*; Volume 97 of Graduate Texts in Mathematics; Springer: New York, NY, USA, 1984.
- Corsini, P.; Leoreanu, V. *Applications of Hyperstructure Theory*; Kluwer Academic Publications: Dordrecht, The Netherlands, 2003.
- Vougiouklis, T. The fundamental relation in hyperrings. The general hyperfield. In Proceedings of the 4th International Congress on Algebraic Hypergroups and Applications, Xanthi, Greece, 27–30 June 1990; World Scientific: Singapore, 1991; pp. 209–217.
- Rota, R. Sugli iperanelli moltiplicativi. *Rend. Mate* **1982**, *7*, 711–724.
- Ameri, R.; Kordi, A.; Hoskova-Mayerova, S. Multiplicative hyperring of fractions and coprime hyperideals. *An. Ştiinţ. Univ. Ovidius Constanţa Ser. Mater.* **2017**, *25*, 5–23. [[CrossRef](#)]
- Davvaz, B.; Leoreanu-Fotea, V. *Hyperring Theory and Applications*; International Academic Press: Cambridge, MA, USA, 2007.
- Nakassis, A. Recent results in hyperring and hyperfield theory. *Int. J. Math. Math. Sci.* **1988**, *11*, 209–220. [[CrossRef](#)]
- Cristea, I.; Jančić-Rašović, S., Composition hyperrings. *An. Şt. Univ. Ovidius Constanţa* **2013**, *21*, 81–94. [[CrossRef](#)]
- Norouzi, M.; Cristea, I. Hyperrings with n-ary composition hyperoperation. *J. Alg. Appl.* **2018**, *17*, 1850022. [[CrossRef](#)]
- Norouzi, M.; Cristea, I. Fundamental relation on m-idempotent hyperrings. *Open Math.* **2017**, *15*, 1558–1567. [[CrossRef](#)]

21. Bordbar, H.; Cristea, I.; Novak, M. Height of hyperideals in Noetherian Krasner hyperrings. *Politehn. Univ. Bucharest Sci. Bull. Ser. A Appl. Math. Phys.* **2017**, *79*, 31–42.
22. Ameri, R.; Eyvazi, M.; Hoskova-Mayerova, S. Superring of polynomials over a hyperring. *Mathematics* **2019**, *7*, 902. [[CrossRef](#)]



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).