A Field Theory Problem Relating to Questions in Hyperfield Theory

Ch. G. Massouros

Department of Applied Sciences, Technological Institute *of* Chalkis, Evia, GR344 00, GREECE
e-mail: masouros@teihal.gr , URL: http://www.teihal.gr/gen/profesors/massouros/index.htm

Abstract. M. Krasner introduced the notions of the hypefield and the hyperring in 1956. Much later, he constructed the quotient hyperfield/hyperrring, using a field/ring and a subgroup of its multiplicative group/semigroup. The existence of non-quotient hyperfields and hyperrings was an essential question for the self-sufficiency of the theory of hyperfields and hyperrings vis-à-vis that of fields and rings. The momogene hyperfield, which was introduced by the author, is a hyperfield H having the property $x-x=H$ for all $x \in H$ with $x \neq 0$. The existence of non-quotient monogene hyperfields is a hitherto open question. The answer to this question is directly connected with the answer to the question which fields can be expressed as a difference of a subgroup of their multiplicative group from itself and which these subgroups are. These issues, as well as some relevant theorems are presented in this paper.

Keywords: Fields, Finite Fields, Multiplicative Subgroups, Hyperfields, Hyperrings.
PACS: 02.10.De, 02.20.Bb AMS-Subject classification: 12E20, 12E99, 12K99, 20N20

INTRODUCTION

In 1934 F. Marty, in order to study problems in non-commutative algebra, such as cosets determined by non-invariant subgroups, generalized the notion of the group by defining the **hypergroup** [4, 20]. The result of the operation between two elements in a hypergroup is not a single element, but a set of elements. Thus, the notion of the **hypercomposition** was introduced. A hypercomposition "+" in a non-empty set H is a function from $H \times H$ to the powerset $\mathscr{P}(H)$ of H. In 1956, M. Krasner replaced the additive group of a field with a special hypergroup, thus introducing the **hyperfield**. He then used it as the proper algebraic tool in order to define a certain approximation of complete valued fields by sequences of such fields [2]. This additive hypergroup was later named **canonical hypergroup** by J. Mittas [21, 22]. $(H,+)$ is a canonical hypergroup, if it satisfies the following axioms:

i. $x+y=y+x$ for all $x,y \in H$,
ii. $(x+y)+z=x+(y+z)$ for all $x,y,z \in H$,
iii. there exists an element $0 \in H$, such that, for each $x \in H$, there is one and only one $x' \in H$, denoted by $-x$, such that $0 \in x+(-x)=x-x$,
iv. $z \in x+y \Rightarrow x \in z-y$ (reversibility).

Notations:

(a) If A and B are subsets of H , then $A+B$ signifies the union $\bigcup_{(a,b)\in A\times B} a+b$. $A+b$ and $a+B$ mean the same as $A+\{b\}$ and $\{a\}+B$ respectively.

(b) If A and B are subsets of H , then $A \setminus B$ signifies the set $\{x \mid x \in A \text{ and } x \notin B\}$.

Remarks:

(a) By virtue of axioms (iii) and (iv), the equality $0+x=x$ is valid for all $x \in H$. Indeed, $0 \in x-x$ and thus, $x \in x+0$ per reversibility. Next, suppose that some y different from x belongs to $x+0$. Then, $0 \in x-y$, which is absurd because of (ii). Therefore, $0+x=x$. This equality is voided if the reversibility axiom is deleted from consideration. Thus, other types of hypergroups appear, such as, for example, the fortified join hypergroup in which $0+x \subseteq \{0,x\}$ [17, 18].

Numerical Analysis and Applied Mathematics ICNAAM 2011
AIP Conf. Proc. 1389, 1852-1855 (2011); doi: 10.1063/1.3636971

(b) The collection G/Q of all double cosets of a subgroup Q of a group G is an typical example of a canonical hypergroup.

A **hyperfield** is a triplex $(H,+,\cdot)$, where:

i. $(H,+)$ is a canonical hypergroup,

ii. $(H,\cdot)$ is an almost-group (i.e. the union of a group with a bilaterally absorbing element) with the zero element (0) of the hypergroup being the absorbing element,

iii. The multiplication is distributive across the hyperaddition, i.e. $z(x+y)=zx+zy$ and $(x+y)z=xz+yz$ for all $x,y,z\in H$.

If axiom (ii) is replaced by axiom:

ii'. $(H,\cdot)$ is a semigroup in which the zero element of the hypergroup is a bilaterally absorbing element,

then, a more general structure is obtained, which was called **hyperring** by M. Krasner [3]. Among others, these structures were recently utilized by A. Connes and C. Consani in the study of the algebraic structure of the adèle class space ç$_{\text{Ê}}$=À$_{\text{Ê}}$/Ê$^{\times}$ of a global field Ê [1]. Additionally, the above structures contributed to the creation of more generalized structures, such as the hyperringoid and the join hyperring used in the theory of formal languages and automata [11, 15, 16, 19].

QUOTIENT AND NON-QUOTIENT HYPERFIELDS / HYPERRINGS

M. Krasner dealt with the question of occurrence frequency of structures such as hyperrings and hyperfields. He thus observed that the quotient R/G of any ring R by any normal subgroup G of its multiplicative semigroup is always a hyperring. This hyperring becomes a hyperfield when R is a field. Indeed, the multiplicative classes $\overline{x}=xG$, where $x\in R$, form a partition of R . The set R/G of these classes becomes a hyperring, if the product of R/G 's two elements is defined to be their setwise product and their sum to be the set of the classes contained in their setwise sum [3]. Following this observation, M. Krasner raised the question whether all hyperrings are isomorphic to subhyperring of quotient hyperrings or not. He also raised a similar question concerning hyperfields [3]. The answer to these questions was of higher importance than simply determining the number of different classes of these structures. That is, if all hyperrings could be isomorphically embedded into the type of hyperrings that Krasner exhibited, then several conclusions of their theory could be arrived at in a very straightforward manner, through the use of the ring, field and modules theories, instead of developing new techniques and proof methodologies.

The existence of non-quotient hyperfields and hyperrings was proven by the author ([6], [7]), as well as by A. Nakassis ([23]). Concerning hyperfields, A. Nakassis worked with hyperfields in which the hypersum of any two elements, different to each other, does not contain the two addends. More precisely, he started his construction with a multiplicative group T^*, which has more than three elements; he considered one more element (the 0 element), which is multiplicatively absorbing in $T=T^*\cup\{0\}$, i.e. $a\cdot 0=0\cdot a=0$ for all $a\in T$. Next, he endowed T with a hyperfield structure, through the introduction of hypercomposition $a+0=0+a=a$ for all $a\in T$, $a+a=\{0,\ a\}$ for all $a\in T^*$, $a+b=b+a=$ $=T\setminus\{0,\ a,\ b\}$ for all $a,b\in T^*$, where $a\neq b$. He then proved that choosing either the cardinality or the structure of group T^* in a suitable manner, $(T,+,\cdot)$ is not embeddable into a quotient hyperring.

Contrarily to Nakassis's methodology, the author constructed hyperfields in which the hypersum of any two elements different from each other and non-opposite contains the two addends. Construction of these hyperfields starts with a multiplicative group $(\Theta,\cdot)$, which has more than two elements. In the first construction, Θ is equipped with a multiplicatively absorbing element 0 and then the union $\mathrm{H}=\Theta\cup\{0\}$ is endowed with the following hypercomposition: $x+0=0+x=x$ for all $x\in\mathrm{H}$, $x+x=\mathrm{H}\setminus\{x\}$ for all $x\in\Theta$ and $x+y=y+x=\{x,\ y\}$ for all $x,y\in\Theta$, where $\mathrm{x}\neq\mathrm{y}$. Then, $\mathrm{H}(\Theta)=(\mathrm{H},+,\cdot)$ is a hyperfield. In the second construction, the direct product $\overline{\Theta}=\Theta\otimes\{1,-1\}$ of the multiplicative groups Θ and $\{1,-1\}$ is considered. $\overline{\Theta}$ is equipped with a multiplicatively absorbing element 0 and the union $\mathrm{K}=\overline{\Theta}\cup\{0\}$ is endowed with the following hypercomposition:

$w+0=0+w=w$ for all $w\in\mathrm{K}$,

$(x,i)+(x,i)=\mathrm{K}\setminus\{(x,i),(x,-i),0\}$, for all $(x,i)\in\bar{\Theta}$,

$(x,i)+(x,-i)=\mathrm{K}\setminus\{(x,i),(x,-i)\}$, for all $(x,i)\in\bar{\Theta}$,

$(x,i)+(y,j)=\{(x,i),\ (x,-i),\ (y,j),\ (y,-j)\}$, for all $(x,i),(y,j)\in\bar{\Theta}$ with $(y,j)\neq(x,i),\ (x,-i)$.

Then, $\mathrm{K}(\Theta)=(\mathrm{K},+,\cdot)$ is a hyperfield and the following theorem is valid:

Theorem 2.1. *If Θ is a periodic group, then hyperfields $\mathrm{H}(\Theta)$ and $\mathrm{K}(\Theta)$ do not belong to the class of quotient hyperfields* (for the proof, see [6, 7, 8, 10]).

Before hyperfields $\mathrm{H}(\Theta)$ and $\mathrm{K}(\Theta)$, the author constructed hyperfields in which the difference of each one of their non-zero elements from itself produses the entire hyperfield. Due to this property, these hyperfields were named **monogene**, since they can be generated by a single element. There are many examples of monogene hyperfields [9]. In what follows, two of them are presented.

Example 2.1. [9] Let Q be a multiplicative group and $\bar{Q}$ be the direct product of Q by $\{1,-1\}$. Consider the almost-group $M=\bar{Q}\cup\{0\}$. Then, M can be endowed with a hyperfield structure, if one defines a hyperaddition as follows: $(x,i)+(x,-i)=M$ for all $(x,i)\in M$, $(x,i)+0=0+(x,i)=(x,i)$ for all $(x,i)\in M$ and $(x,i)+(y,j)=\{(x,i),\ (y,j)\}$ for all $(x,i),(y,j)\in M$ with $(y,j)\neq(x,-i)$. A. Nakassis, having worked on these hyperfields, proved that there exist quotient hyperfields of this type [9].

Example 2.2. [9] Let $(H,+,\cdot)$ be a field or a hyperfield. If a hyperaddition «$+\!\!\!\!+$» is defined in H as follows: $x+\!\!\!\!+(-x)=H$ for all $x\in H$, where $x\neq 0$, $x+\!\!\!\!+0=0+\!\!\!\!+x=x$ for all $x\in H$ and $x+\!\!\!\!+y=$ $=(x+y)\cup\{x,\ y\}$ for all $x,y\in H$, where $y\neq -x$ and $x,y\neq 0$, then the structure $(H,+\!\!\!\!+,\cdot)$ is a hyperfield. It has been proven that, if $(H,+,\cdot)$ is a quotient hyperfield, $(H,+\!\!\!\!+,\cdot)$ is a quotient hyperfield as well.

The question that arose following the appearance of the monogene hyperfields was *whether there are monogene hyperfields that are non-quotient*. This is a hitherto unanswered question, which leads to another problem. If a monogene hyperfield is isomorphic to a quotient hyperfield F/G, then the equality $xG\text{-}xG=F/G$ must be valid for each $xG\in F/G$. Therefore, the multiplicative subgroup G of F must have the property $G-G=F$. Hence, in the early 80's, the author was led to raising the question: *when does a subgroup G of the multiplicative group of a field F posses the ability to generate F via the subtraction of G from itself?* [5, 8, 9]

Remark: Instead of defining $x-x=H$, the following was defined: $x-x=H\setminus\{-x,x\}$ or $x+x=H\setminus\{x\}$, if x is self-opposite. This subtle differentiation in definition of the hypercomposition facilitated the sidestepping of the above problems. Thus, the construction of non-quotient hyperfields was achieved.

ON THE DIFFERENCE OF A SUBGROUP OF A FIELD'S MULTIPLICATIVE GROUP FROM ITSELF

The concise answers available to us so far concerning the above problem on finite fields can be summarized in the following theorem [10, 12, 13, 14]:

Theorem 3.1. *Let F be a finite field and G be a subgroup of its multiplicative group of index n and order m. Then, G-G = F, if and only if:*

$n=2$ *and* $m>2$,
$n=3$ *and* $m>5$,
$n=4$, $-1\in G$ *and* $m>11$,
$n=4$, $-1\notin G$ *and* $m>3$,
$n=5$, $charF=2$ *and* $m>8$,
$n=5$, $charF=3$ *and* $m>9$,
$n=5$, $charF\neq 2,3$ *and* $m>23$.

From the above theorem, one can see, beyond any doubt, that the validity of equality $G-G=F$ depends only on the cardinality of G. Of course, this does not mean that any subset S of F with the same cardinality as G has the property $S-S=F$. For example, let $F=Z_{19}$. Then, if we consider the multiplicative subgroup of index 3, which is $G=\{1,7,8,11,12,18\}$, equality $G-G=F$ is true; while, if we consider the set $S=\{1,6,8,11,13,17\}$, which has the same number of elements as G, we come up with $S-S\neq F$. However, it must be mentioned that the classes $\xi^i G$, defined in F^* by G, are sets with the same cardinality as G, satisfying equality $\xi^i G-\xi^i G=F$ (when, of course, this is satisfied by G). On the other hand, what can be observed is that, when the order of G is small, there exist additional suppositions described by the above theorem, on the validity of which depends whether $G-G=F$ is true or not. Thus, for example, the index 5 subgroup in GF[3^4] numbers 16 elements and satisfies equality G – G = GF[3^4]. On the contrary, the index 5 subgroup in ñ$_{101}$ numbers 20 elements, but does not satisfy the corresponding equality, as G – G = ñ$_{101}$\ G.

REFERENCES

1. A. Connes and C. Consani, "The hyperring of adèle classes" *J. of Number Theory*, no 131, 2011, pp. 159-194.
2. M. Krasner, "Approximation des corps valués complets de caractéristique p≠0 par ceux de caractéristique 0" Colloque d' Algèbre Supérieure (Bruxelles, Decembre 1956), Centre Belge de Recherches Mathématiques, Établissements Ceuterick, Louvain, Librairie Gauthier-Villars, Paris, 1957, pp. 129-206.
3. M. Krasner, "A class of hyperrings and hyperfields" *Internat. J. Math. & Math. Sci.* vol. 6, no. 2, 1983, pp. 307-312.
4. F. Marty, "Sur un généralisation de la notion de groupe", Huitième Congrès des mathématiciens Scand., pp. 45-49, Stockholm 1934.
5. Ch. G. Massouros, "Algebraic Structures with Hypercomposition" Dissertation, submitted in Patras University, Greece, 1984.
6. Ch. G. Massouros "Methods of constructing hyperfields" *Internat. J. Math. & Math. Sci.* vol. 8, no. 4, 1985, pp. 725-728.
7. Ch. G. Massouros, "On the theory of hyperrings and hyperfields" *Algebra i Logika,* vol. 24, no. 6, 1985, pp. 728-742.
8. Ch. G. Massouros, "Hypergroups and their applications" Ph.D. Thesis, National Technical University of Athens, 1988.
9. Ch. G. Massouros, "Constructions of hyperfields" *Mathematica Balkanica* vol 5, fasc. 3, 1991, pp. 250-257.
10. Ch. G. Massouros, "A class of hyperfields and a problem in the theory of fields" *Mathematica Montisnigri* vol. 1, 1993, pp. 73-84.
11. Ch. G. Massouros, "On the hypercompositional structures" *Fuzzy Systems & A.I. - Reports and Letters*, Academia Romana, vol. 3, no.3, 1994, pp. 15-27.
12. Ch. G. Massouros, "On the result of the difference of a subgroup of the multiplicative group of a field from itself" *Proceedings of the 4th Internat. Cong. in Algebraic Hyperstructures and Applications*, Democritous Univ. of Thrace press, 1996, pp. 89-101.
13. Ch. G. Massouros, "Getting a field from differences of its multiplicative subgroups" *Bulletin of the Polytechnic Institute of Iasi, section Mathematics, Theoretical Mechanics, Physics*, tom. XLVI (L) fasc. 1-2 (2000) pp. 1-17.
14. Ch. G. Massouros, "Looking at certain Hypergroups and their properties" Proceedings of the European Conference on Intelligent Technologies 2000, Iasi 2000, Advances in Generalized Structures Approximate Reasoning and Applications, published by the cooperation of University of Teramo, Romanian Society for Fuzzy Systems and BMFSA Japan, 2001, pp. 31 – 43.
15. Ch. G. Massouros and G. G. Massouros, "On Join Hyperrings" Proceedings of the 10th Internat. Cong. on Algebraic Hyperstructures and Applications, 2008, pp. 203-216.
16. G. G. Massouros, "Automata-Languages and hypercompositional structures" Ph.D. Thesis, National Technical University of Athens, 1993.
17. G. G. Massouros, Ch. G. Massouros and J. D. Mittas, "Fortified Join Hypergroups", *Annales Matematiques Blaise Pascal*, vol 3, no 2, 1996, pp. 155-169.
18. G. G. Massouros, "The subhypergroups of the Fortified Join Hypergroup" *Italian Journal of Pure and Applied Mathematics*, no 2, 1997, pp. 51-63.
19. G. G. Massouros, "The Hyperringoid" *Multiple Valued Logic*, vol. 3, 1998, pp. 217-234.
20. G. G. Massouros, "On the Hypergroup Theory" *Fuzzy Systems & A.I. - Reports and Letters, Academia Romana*, vol. IV, no. 2/3, 1995, pp. 13-25 and *Scripta Scientiarum Mathematicarum*, tom. I, fasc. I, 1997, pp. 153-170.
21. J. Mittas, "Hypergroupes canoniques hypervalues" *C. R. Acad. Sci.* (Paris) 271, Serie A, 1970, pp. 4-7.
22. J. Mittas, "Hypergroupes canoniques", *Mathematica Balkanica*, 2, 1972, pp. 165-179.
23. A. Nakassis, "Recent results in hyperring and hyperfield theory" *Internat. J. of Math. & Math. Sci.* vol. 11, no. 2, 1988, pp. 209-220.