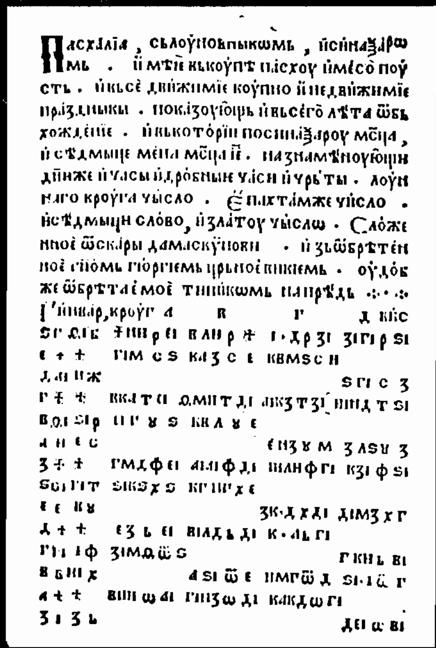

MATHEMATICA MONTISNIGRI

VOLUME I - 1993

MATHEMATICA MONTISNIGRI
Vol 1 (1993) 1-143

CONTENTS

MATHEMATICA MONTISNIGRI UDK 519.4
Vol I (1993) 73-84

A CLASS OF HYPERFIELDS AND A PROBLEM IN THE THEORY OF FIELDS

Ch. G. Massouros

Abstract

This article presents those hyperfields for which the sum of two of their elements contains the participating elements. It also exhibits the proof of two Theorems which refer to the question (deriving from the study of the isomorphism of hyperfields to the quotient ones) of whether a field can be written as a difference of one of its multiplicative subqroups, from itself. Yet, a Theorem which constructs a non quotient hyperfield from a periodical group is proved.

AMS SUBJECT CLASSIFICATION CODE. 20N20

1. Introduction

The concept of the hyperfield was introduced by M. Krasner in his study [1]. The author there uses the hyperfield as the proper algebraic tool in order to define a certain approximation of a complete valued field, by sequences of such fields. The hyperfield which appeared in this approximation was named residual hyperfield. The axioms that a hyperdield $(H, +, \cdot)$ satisfies are the following:

1. $(H, .)$ is an almost-group[1]. By 1 we shall denote its neutral element, and by 0 its absorbing element.

2. $(H, +)$ is a cononical hyperqroup[2]

3. $z \cdot (x + y) = z \cdot x + z \cdot y, \quad (x + y) \cdot z = x \cdot z + y \cdot$ (distributive axiom)

Next M. Krasner constructed a class of hyperfields, which is more general than the class of residual hyperfields. He named these new hyperfields quotient hyperfields [2] and he proved that the residual hyperfields are quotient ones. The construction of the quotient hyperfields is as follows: Let F be a field and let G be a normal subgroup of its multiplicative group. Then the multiplicative classes modulo G form a partition of F. Then F/G becomes a hyperfield if we define the product of F/G 's two elements to be their setwise product and their sum to be the set of the classes which are contained in their setwise sum.

The answer to the problem of the existence of other hyperfields, different than the quotient ones, became very crucial for the hyperfield theory. Indeed, if the quotient hyperfields were the only existing hyperfields, a large part of the hyperfield theory could have been a straightforward generalization of the theory of fields. The attempts for the solution of this problem gave birth to other types of hyperfields (see

---

[1]An almost-group is a semigroup S, which is the union $G \cup \{0\}$, where G is a group and 0 a bilaterally absorbing element of S.

[2]A non void set H, endowed with a hypercomposition "+", is called canonical hypergroup (see [7]), if it satisfies the axioms

I. $x + y = y + x$

II. $x + (y + z) = (x + y) + z$

III. There exists an element $0 \in H$, such that $x + 0 = 0 + x = x$ (in the case of the hyperfields it is easy to prove, that this element is the absorbing one).

IV. For every $x \in H$ there exists one and only one $x' \in H$ such that $0 \in x + x'$. x' is written $-x$ and it is called the opposite of x.

V. $z \in x + y \Rightarrow y \in z - x$

[4], [5], [6], [8]) proving in this way the selfsufficiency and independence of the hyperfield theory.

In the following we shall present the hyperfields which have a special property concerning the sum of any two generally non equal and non opposite elements: it contains the two participating elements. Paragraph 2 refers to the monogene hyperfields. Two Theorems are presented there, concerning a problem in the theory of fields, which was raised from the study of the isomorphism of monogene hyperfields to the quotient hyperfields. In the third paragraph a construction of a non quotient hyperfield is exhibited.

2. Monogene hyperfields and a problem in the theory of fields

A hyperfield is called monogene if it can be generated only by one element. The hyperfields in which the sum of any two elements contains these two elements are monogene hyperfields. Indeed let H be a hyperfield and $x \in x + y$ for every $x, y \in H$. Then $y \in x - x$, for every $y \in H$, so $H \subseteq x - x$. But $x - x \subseteq H$, thus $x - x = H$ (see also [3]). In [3] two methods of constructing monogene hyperfields are proved:

CONSTRUCTION I.

Let Q be a multiplicative group, and let $(H^*, \cdot)$ be its direct product with the group $\{-1, 1\}$. We consider the almost-group $(H, \cdot) = (H^* \cup \{0\}, \cdot)$ and we define a hypercomposition in H as follows:

- $(x, i) + (x, -i) = H$
- $(x, i) + 0 = 0 + (x, i) = (x, i)$
- $(x, i) + (y, j) = \{(x, i), (y, j)\}$ for every $(x, i) \neq (y, -j)$

Then $(H, +, \cdot)$ becomes a hyperfield.

CONSTRUCTION II.

Let $(H, +, \cdot)$ be a hyperfield. If we introducing in H a new hypercomposition "#", defined as follows:

- $x\#(-x) = H$
- $x\#0 = 0\#x = x$
- $x\#y = (x + y) \cup \{x, y\}$ for every $x \neq -y, 0$

then it can be proved that $(H, \#, \cdot)$ becomes a hyperfield as well.

In [3] concerning the first construction it is proved that there are quotient hyperfields in which $x + y = \{x, y\}$ for every two elements x, y with $x \neq -y$ and $x, y \neq 0$. Also concerning the second construction it is proved that if $(H, +, \cdot)$ is a quotient hyperfield, then $(H, \#, \cdot)$ is also a quotient hyperfield. In the same article it is mentioned that if $K = F/G$ is a quotient hyperfield isomorphic to such a menogene hyperfield, then G must satysfy the property $G - G = F$, and the problem is posed:

> Which fields can be written as a difference of a subgroup of their multiplicative group from itself, and furthermore which are these subgroups?

It is obvious that in ordered fields, for example, the positive elements form a multiplicative subgroup which has the above property. In the following we shall face this problem in the case of finite field, and we shall prove two Theorems for groups of index 2 and 3.

Theorem 2.1 *If F is a finite field and G a multiplicative subgroup of F^* with $|F^* : G| = 2$ and card $G > 2$, then*

$$G - G = F$$

Proof. At first we mention that a field with characteristic 2 can not have a multiplicative subgroup of order 2, since its multiplicative group has $2^n - 1$ elements, so char $F \neq 2$. G defines in F three classes. The class $\{0\}$ of the zero, and the two classes G and ξG.

If $G - G = G \cup \{0\}$, then $G \cup \{0\}$ is a subfield of F, for which is valid: 2 card $[G \cup \{0\}] - 1 =$ card F, which is absurd.

Let $G - G = \xi G \cup \{0\}$. we choose an element $r \in G$ with $r \neq \pm 1$. Then $r - 1 \in \xi G$ and $r^2 - 1 \in \xi G$. But $r^2 - 1 = (r - 1)(r + 1)$, so

$r+1 \in G$. Then we have $r=(r+1)-1 \in G-G=\xi G \cup \{0\}$. Thus $r \in \xi G$, contradiction and so the Theorem.

Now let $|F^* : G| = 3$, then G defines in F four classes. The class $\{0\}$ of the zero, and the three classes $G, \xi G, \xi^2 G$. Then the following Lemmas are valid:

Lemma 2.1 $G-G=G+G$

Proof. If char $F=2$, then $G=-G$ and so the equality. Next, let char $F \neq 2$. Since F is a finite field we have card $F=p^n$, where p is a prime number and $n \in N$. This means that F^*, has p^n-1 elements, which is an even number, because $p \neq 2$. Thus, when G exists, it contains an even number of elements and so it has one subgroup with 2 elements. But, since F^* is cyclic subgroup, it contains only one subgroup with 2 elements. This subgroup is the $\{-1,1\}$ and therefore $-1 \in G$.

Lemma 2.2 *If card $G>2$, then the difference $G-G$ can not contain only one of the classes χG, $\chi=1,\ \xi,\xi^2$.*

Proof. Let $G-G=G \cup \{0\}$. Then $G \cup \{0\}$ is a subfield of F, for which is valid: 3 card$[G \cup \{0\}]-2=$card$F$, absurd.

Let $G-G=\xi G \cup \{0\}$. We choose an element $r \in G$ with $r \neq \pm 1$. Then $r-1 \in \xi G$ and $r+1 \in \xi G$. So $r^2-1 \in \xi^2 G$, contradiction.

Similarly $G-G$ can not be equal to $\xi^2 G \cup \{0\}$.

Remark. In Z_7 the multiplicative subgroup of index 3 is $G=\{1,6\}$ and $G-G=2G \cup \{0\}$.

If card $F>16$, than the folowing Lemmas are valid.

Lemma 2.3 *If $\xi G \cup \xi^2 G \cup \{0\} \subseteq G-G$, then $G-G=F$.*

Proof. If $2 \in G$, than the Lemma is valid. Let $2 \in \xi G$. Because of our hypothesis there exists $r \in G$ such that $r-1 \in \xi G$ Assume that $r \neq -1$. If $r+1 \in G$ then the Lemma is true. Also if $r+1 \in \xi^2 G$, then $(r-1)(r+1) \in \xi G \cdot \xi^2 G \Rightarrow r^2-1 \in G$ and the Lemma is valid again. Finally, if $r+1 \in \xi G$, then $\xi G \subseteq \xi G+\xi G$, since, $r+1=(r-1)+2 \in \xi G+\xi G$ and so $G \subseteq G+G$.

Next let us suppose that the only element r with the property $r-1 \in \xi G$ is the element -1. In this case there exists an element $s \neq -1$, such that $s-1 \in \xi^2 G$. If $s+1 \in G$ then the Lemma holds and if $s+1 \in \xi G$ the Lemma is also true since $s^2-1 \in \xi G \cdot \xi^2 G = G$. If $s+1 \in \xi^2 G$, then $s^2-1 \in \xi G$. But according to our supposition, -1 is the only element with this property. Thus $s^2 = -1$ and if there does not exist any other element s with $s-1 \in \xi^2 G$, then $G = \{-1, 1, -s, s\}$. So card $G = 4$, and card $F = 3 \cdot 4 + 1 = 13$ which contradicts the hypothesis.

Similar is the proof under the assumption that $2 \in \xi^2 G$.

Now if char $F = 2$, since card $F > 16$, we have card $G > 5$, and so we choose an element $r \in G$ such that $r^5 \neq 1$. If $r+1 \in G$ then the lemma is true. Suppose that $r+1 \in \xi G$. Then $r^2+1 = (r+1)^2 \in \xi^2 G$ and $r^4+1 = (r^2+1)^2 \in \xi G$. If $r^3 = 1$, then $r^2+1 = r^2+r^3 = r^2(r+1) \in \xi G$, absurd. Thus $r^3 \neq 1$ and so:

$$(r^4+1)+(r+1) \in \xi G + \xi G \Rightarrow r^4 + r \in \xi G + \xi G \Rightarrow$$

$$\Rightarrow r(r^3+1) \in \xi G + \xi G \Rightarrow r^3 + 1 \in \xi G + \xi G$$

Therefore if r^3+1 belongs to G or to ξG the Lemma holds. Let $r^3+1 \in \xi^2 G$. Then $r^6+1 \in \xi G$. Now if $r^5+1 \in G$ the Lemma is valid. If $r^5+1 \in \xi G$, then

$$(r^6+1)+(r^5+1) \in \xi G + \xi G \Rightarrow r^5(r+1) \in \xi G + \xi G \Rightarrow$$

$$\Rightarrow \xi G \subseteq \xi G + \xi G \Rightarrow G \subseteq G + G$$

If $r^5+1 \in \xi^2 G$, then

$$(r^5+1)+(r^3+1) \in \xi^2 G + \xi^2 G \Rightarrow r^3(r^2+1) \in \xi^2 G + \xi^2 G \Rightarrow$$

$$\Rightarrow \xi^2 G \subseteq \xi^2 G + \xi^2 G \Rightarrow G \subseteq G + G$$

Finally if we suppose that $r+1 \in \xi^2 G$, we have a similar proof and therefore the Lemma is proved.

Remark. In Z_{13} the multiplicative subgroup of index 3 is $G = \{1, 12, 5, 8\}$, and $G - G = \{0\} \cup 2G \cup 4G$. Also in $GF[2^4]$, $G = \{1, x^3, x^3+x, x^3+x^2, x^3+x^2+x+1\}$ and$G - G = GF[2^4] \setminus G$[3].

[3] With $A \setminus B$ we denote the set $\{x \in A | x \notin B\}$

Lemma 2.4 *If* $G \cup \xi G \cup \{0\} \subseteq G - G$, *then* $G - G = F$.

Proof. If $2 \in \xi^2 G$, then the Lemma is valid. Let $2 \in \xi G$. Because of our hypothesis there exists $r \in G$ such that $r - 1 \in \xi G$. Assume that $r \neq -1$. If $r + 1 \in \xi^2 G$ then the Lemma is true. Next if $r + 1 \in \xi G$, then $(r-1)(r+1) \in \xi G \cdot \xi G \Rightarrow r^2 - 1 \in \xi^2 G$ and the Lemma is valid again.

Finally, if $r + 1 \in G$, then $r + 1 = (r - 1) + 2 \in \xi G + \xi G$, thus $G \subseteq \xi G + \xi G$, and so $\xi^2 G \subseteq G + G$.

Next supposing that the only element $r \in G$ with the property $r - 1 \in \xi G$ is the element -1 and that for any other element $s \in G$, we have $s - 1 \in G$. Let $t = s - 1$ (i). Then:

$$s - t = 1 \Rightarrow s^2 - 2st + t^2 = 1 \Rightarrow s^2 + t^2 - 1 = 2st \quad \text{(ii)}$$

Because of our assumption, $s^2 + t^2 \notin \xi^2 G$. If $s^2 + t^2 \in \xi G$, then $t^2(s^2/t^2 + 1) \in \xi G$, thus$s^2/t^2 = 1$, $s^2 = t^2$. So from (i) we have: If $s = t$, then $-1 = 0$, absurd. If $s = -t$, then $2s = 1$, so $2G = G$, contradiction. Now if $s^2 + t^2 \in G$, (ii) gives $s^2 + t^2 = -1$, since we have supposed that the only element $r \in G$ with the property $r - 1 \in \xi G$ is -1. So $-2 = 2st$, thus $st = -1$ (iii). Therefore, because of (i) and (iii), for every element $s \in G$, with $s \neq -1$, the equality $s^2 - s + 1 = 0$ must be valid which is absurd. So the Lemma is true if $2 \in \xi G$.

Now if $2 \in G$, then we choose an element $r \in G$, such that $r - 1 \in \xi G$. We note that $r \neq -1$ since $-2 \in G$. Also $r^2 + 1 \neq 0$, because $r - 1 \in \xi G \Rightarrow (r-1)^2 \in \xi^2 G \Rightarrow r^2 + 1 - 2r \in \xi^2 G$ and if $r^2 + 1 = 0$, then $-2r \in \xi^2 G$, which is absurd since $2 \in G$. Now we consider the $r + 1$. If $r + 1 \in \xi^2 G$, then the Lemma holds. Also if $r + 1 \in \xi G$, then $r^2 - 1 \in \xi^2 G$ and the Lemma is true. Finally if $r + 1 \in G$, then $r^2 - 1 \in \xi G$ and we consider $r^2 + 1$. If $r^2 + 1 \in G$, then $(r^2 + 1) - 2r \in G - G \Rightarrow (r-1)^2 \in G - G$. But $(r-1)^2 \in \xi^2 G$, thus $\xi^2 G \subseteq G - G$, and so the Lemma is true. The Lemma is obviously valid if $r^2 + 1$ belongs to either $\xi^2 G$ or ξG. Thus the Lemma is true when $2 \in G$.

Finally let char $F = 2$. Then from $r - 1 \in \xi G$ derives that $(r-1)^2 \in \xi^2 G$. But $(r-1)^2 = r^2 - 1 \in G - G$, so $\xi^2 G \subseteq G - G$ and the proof of the Lemma is concluded.

The following Lemma can be proved in an analogous way:

Lemma 2.5 *If $G \cup \xi^2 G \cup \{0\} \subseteq G - G$, then $G - G = F$.*

Now from the above Lemmas the following Theorem derives.

Theorem 2.2 *If F is a finite field with card $F > 16$ and G a subgroup of the multiplicative group of F with index 3, then*

$$G - G = F$$

3. A non quotient hyperfield

Let Θ be a multiplicative group, with card $\Theta > 2$. Consider the almost-group $H = \Theta \cup \{0\}$. We introduce in H a hypercomposition "#", defined as follows:

$x\#0 = 0\#x$ for every $x \in H$
$x\#x = H \setminus \{x\}$ for every $x \in \Theta$
$x\#y = y\#x = \{x, y\}$ for every $x, y \in \Theta$, with $x \neq y$

Then $H(\Theta) = (H, \#, \cdot)$ becomes a hyperfield (for the proof see [4]).

Now let us suppose that $H(\Theta)$ is isomorphic to a quotient hyperfield $(F/G, +, \cdot)$ of a field $(F, +, \cdot)$ by a subgroup G of its multiplicative group. Then:

Lemma 3.1 *If the characteristic of F is 2, then there exists an element $x \in F$ such that $x^2 \notin G$.*

Proof. Let $x \neq 0$ be en element of F such that $x + 1 \in G$. Such an element always exists, since card $(F/G) > 3$ and $xG\#G = \{xG, G\}$, when $xG \neq G$. Now we have:

$$x + 1 \in G \Rightarrow (x+1)^2 \in G \Rightarrow x^2 + 1 \in G (\text{because char } F = 2)$$

Thus for x^2 we have:

$$x^2 = (x^2 + 1) + 1 \in G + G$$

But $G + G = F \setminus G$, and so $x^2 \notin G$.

Lemma 3.2 *If the characteristic of F is p, with $p \neq 2$, then there exists an element $x \in F$ such that $x^2 \notin G$.*

Proof. At first we observe that $2 \notin G$ because:

$$2 = 1 + 1 = G + G = F \setminus G$$

Thus $2G$ is a class different from G. We choose an element $x \neq 0$ of F, such that $x \notin 2G$ and $x + 1 \in G$ (such an element exists, as we inicate in lemma 1). Then for $x - 1$ we have:

$$x - 1 \in xG + G = xG \cup G$$

and

$$x - 1 \in (x + 1) - 2 \in G + 2G = G \cup 2G$$

Thus

$$x - 1 \in (xG \cup G) \cap (G \cup 2G) = G$$

Next for $x^2 - 1$ we have:

$$x^2 - 1 = (x - 1)(x + 1) \in G \cdot G = G$$

Thus for x^2 holds:

$$x^2 = (x^2 - 1) + 1 \in G - G = F \setminus G$$

So $x^2 \notin G$.

Corollary 3.1. *For every $x \in F^* \setminus (G \cup 2G)$, such that $x + 1 \in G$, is valid:*

$$x^2 \notin G$$

Lemma 3.3 *There exists $x \in F$, such that*

$$x^n + \ldots + 1 \in G$$

for every $n \in N$.

Proof. We choose an element $x \in F^* \setminus (G \cup 2G)$ and such that $x + 1 \in G$. Then because of Corollary 3.1, is valid: $x^2 \notin G$. Also $x^2 \notin xG$, and for $x^2 + x + 1$ we have:

$$x^2 + x + 1 = x(x + 1) + 1 \in xG + G = xG \cup G$$

and

$$x^2 + x + 1 = x^2 + (x + 1) \in x^2G + G = x^2G \cup G$$

Thus x^2+x+1 belongs to G. Next let us suppose that for every $n \leq k$, the following is valid:

$$x^n + \ldots + 1 \in G$$

(this is true when $k = 2$). Then for the sum

$$x^{k+1} + x^k + \ldots + x + 1$$

we have

$$\begin{aligned} x^{k+1} + x^k + \ldots + x + 1 &= x(x^k + x^{k-1} + \ldots + 1) + 1 \in xG + G \\ &= xG \cup G \end{aligned}$$

and

$$\begin{aligned} &x^{k+1} + x^k + \ldots + x + 1 = \\ &= +x^2(x^{k-1} + x^{k-2} + \ldots + 1) + (x + 1) \in x^2G + G \\ &= x^2G \cup G \end{aligned}$$

Thus

$$x^{k+1} + x^k + \ldots + x + 1 \in (xG \cup G) \cap (x^2G \cup G) = G$$

Lemma 3.4 *The multiplicative group of hyperfield F/G is not a periodic group.*

Proof. From Carrolary 3.1 we know that there exists an element $x \in F^* \setminus (G \cup 2G)$ for which we have $x + 1 \in G$ and $x^2 \notin G$. Now let us suppose that every two elements of the set:

$$I = \{x^k \mid 0 \leq k \leq n\}$$

are different to each other, which holds for $n = 2$. Then:

$$x^{n+1} - 1 = (x - 1)(x^n + x^{n-1} + \ldots + x + 1)$$

But because of Lemma 3, $(x^n+x^{n-1}+\ldots+x+1) \in G$. Furthermore, in the proof of Lemma 2, we showed that $x - 1 \in G$, if char $K \neq 2$. Also if char $K = 2$, then $x - 1 = x + 1 \in G$. Thus we have $x^{n+1} - 1 \in G$. So for x^{n+1} holds:

$$x^{n+1} = (x^{n+1} - 1) + 1 \in G + G = F \setminus G$$

From that last relation derives that $x^{n+1} \notin G$, which means that $x^{n+1} \neq 1$. Also $x^{n+1} \neq x^k$, $1 \leq k \leq n$, and so the Lemma.

Now, using the above Lemmas, the proof of the Theorem is obvious:

Theorem 3.1 *If Θ is a periodic group, then the hyperfield $H(\Theta)$ does not belong to the class of quotient hyperfields.*

Another construction of a hyperfield which belongs to this class of hyperfields and it is not a quotient hyperfield can be found in [5].

REFERENCES

[1] M. Krasner, Approximation des corps values complets de caracteristique $p \neq 0$ par caux de caracteristique 0. Colloque d' Algebre Superieure (Bruxelles, Decembre 1956), CBRM, Bruxelles, 1957.

[2] M. Krasner, A class of hyperrings and hyperfields. Internat. J.Math. and Math. Sci. Vol. 6, No 2, 307-312, (1983).

[3] CH. G. Massouros, Construction of hyperfields. Matematica Balkanica, Vol.5, 250-257 (1991).

[4] CH. G. Massouros, Methods of constructing hyperfields. Internat. J. Math. and Math. Sci. Vol. 8, No 4, 725-728 (1985).

[5] CH. G. Massouros, On the theory of hyperrings and hyperfields. Algebra i logika 24, No 6, 728-742 (1985).

[6] J. Mittas, Certains hypercorps et hyperanneaux definis a partir de corps et anneaux ordonnes. Bull. Math. Soc. Sci. Math. de la R.S. de Roumanie t. 15 (63) nr.3, (1971).

[7] J. MMittas, Hypergroupes Canoniques. Mathematica Balkanica t. 2, 165-179 (1972).

[8] A. Nakassis, Recent results in hyperring and hyperfield theory. Internat. J.Math. and Math. Sci. (1988).

Received April 14, 1992

CH. G. MASSOUROS
54 KLIOUS ST. 155 61 CHOLARGOS
ATHENS, GREECE