ALGEBRAIC HYPERSTRUCTURES and APPLICATIONS

Proceedings of the sixth International Congress
Prague, Czech Republic, September 1-9, 1996

Publisher: Democritus University of Thrace, Greece

SIXTH INT. CONGRESS ON AHA (1996) 89-101
DEMOCRITUS UNIV. OF THRACE PRESS

ON THE RESULT OF THE DIFFERENCE OF A SUBGROUP OF THE MULTIPLICATIVE GROUP OF A FIELD FROM ITSELF

by

CHRISTOS G. MASSOUROS
(54, Klious st., 155 61 Cholargos, Athens, GREECE)

ABSTRACT This paper deals with the problem of finding which fields can be written as a difference of a subgroup of their multiplicative group from itself and which are these subgroups. It describes the genesis of this problem, it explains its hypercompositional origin, it exhibits the hitherto partial solutions and it proceeds to the next step, which is the solution for the case of subgroups of index 4 and 5 of the multiplicative group of a field. The theorems that are being proved give a clue about what can be expected to hold for greater indexes.

AMS-Classification number: 12E20, 12K99, 20N20

1. QUOTIENT AND NON QUOTIENT HYPERFIELDS

In 1956 M. Krasner introduced the notion of the **hyperfield** in order to define a certain approximation of a complete valued field by sequences of such fields [1]. The hyperfields which were used for this purpose were named **residual hyperfields**. Next M. Krasner constructed a larger class of hyperfields, the **quotient hyperfields**, a part of which are the residual ones [2]. The construction of the quotient hyperfields is as follows:

We consider a field F and a subgroup G of its multiplicative group. In the set of the classes F/G we define the following hypercomposition and composition, which make the structure $(F/G, +, \cdot)$ a hyperfield:

$$xG + yG = \{(xp+yq)G \mid p, q \in G\}$$
$$xG \cdot yG = xyG$$

In the same paper [1], where M. Krasner introduced the notion of the hyperfield, he also introduced the notion of the valued hyperfield, where he was lead, starting from a valued field. In fact, M. Krasner has used these notions in order to achieve the pursued approximation without proceeding to any deep study of these structures. He has proved though that every hyperfield which is isomorphic to a hyperfield that derives as a quotient from a valued field by a multiplicative equivalence is valued itself.

After that, I. Mittas in a long list of papers has firstly presented the study of the hyperfield's additive part, i.e. the **canonical hypergroup**, as he has named it, and next the study of the hyperfield itself (e.g. see [10], [11], [12], [13], [14]). Thus he has studied the **valuation** of the canonical hypergroups and then he generalized this theory by introducing and studying the **simply** and **strictly hypervalued** canonical hypergroups. This study has led to the introduction of the **strongly** and the **superiorly canonical hypergroups** as well as to the introduction of the **strongly** and the **superiorly canonical hyperfields**. Among the other properties which he has presented, he has proved that every simply hypervalued canonical hypergroup is strongly canonical and every strictly hypervalued canonical hypergroup is superiorly canonical. Also he has proved that the converse is true, i.e. every strongly canonical hypergroup is hypervaluable and every superiorly canonical is strictly hypervaluable. For all these structures which he has introduced, I. Mittas has proceeded to the constructions of many examples. Thus, those hyperfields by Mittas which are not strongly canonical, and consequently not hypervaluable, are not isomorphic to residual hyperfields of a valued field by a multiplicative equivalence (see also [9]). For instance, the Theorem holds:

Theorem *(Mittas): Let $(H,\cdot)$ be a totally ordered multiplicative almost-group with 0 being its minimum element. If in H the hypercomposition:*

$$x+y = \max\{x, y\} \text{ if } x \neq y \text{ and } x+x = \{z \in H \mid z \leq x\} = [0, x]$$

is introduced, then $(H,+)$ is a canonical, but not superiorly canonical hypergroup, and $(H,+,\cdot)$ is a hyperfield non isomorphic to a residual hyperfield of a valued field with a multiplicative equivalence.

Moreover the research which has been carried out in the beginning of the 80's by the author and A. Nakassis has resulted to the proof of the existence of classes of non quotient hyperfields. A. Nakassis has worked with hyperfields in which the hypersum of two different to each other and non opposite elements does not contain the two addends [15]. More precisely he started his construction with a multiplicative group T^* which has more than three elements and he considered one more element 0 which is multiplicatively absorbing in $T = T^* \cup \{0\}$, i.e. $a \cdot 0 = 0 \cdot a = 0$ for every $a \in T$. Next he endowed T with a hyperfield structure introducing the hypercomposition:

$a+0 = 0+a = a$, for every $a \in T$

$a+a = \{0, a\}$, for every $a \in T^*$

$a+b = b+a = T\setminus\{0, a, b\}$, for every $a, b \in T^*$, with $a \neq b$

In [3] and [7] it has been proved that in the hyperfields in which the hypersum of two different to each other and non opposite elements does not contain these elements, the following equality is valid:

$$x-x = \{-x, 0, x\}$$

Examples of such hyperfields from the class of the quotient hyperfields can be found in [3], [7], [15]. Indeed the quotient C/R^+, where C is the

field of the complex numbers and R^+ is the set of the positive real numbers, or the quotient $GF[7^2]/\{1,2,4\}$ are such hyperfields. Moreover such hyperfields, but with selfopposite elements (i.e. $x+x = \{0, x\}$) are the C/R^*, where R^* is the multiplicative group of the real numbers and the $GF[p^n]/G$, where $p>2$ is a prime number, $n>2$ is a natural number and G is the multiplicative group of the prime subfield of $GF[p^n]$. In these hyperfields the differences x-x have certain, interesting properties. Thus, for every element x of the hyperfield H, it is card (x-x) = 3, if H does not consist of self opposite elements and card (x-x) = 2, if H consists of selfopposite elements. Also $(x-x) \cap (y-y) = \{0\}$, if $y \neq -x$, x and $\bigcup_{x \in H}(x-x) = H$. A. Nakassis, having worked with such properties, has proved that one can choose either the cardinality or the structure of the group T^* of his construction in such a way that $(T,+,\cdot)$ is not isomorphic to a quotient hyperfield. For this proof he has used the following very important Proposition, which allowed him to calculate the number of the elements which are contained in the result of the hypersum of two elements.

Proposition *(Nakassis): Let R be a ring and P an equivalence relation that induces a hyperring structure in R/P with P(0) = {0}. Assume that a hyperring H is embeddable in the partition hyperring R/P and assume that there exist two elements a and b in H, such that [c+(-c)] ∩ [b+(-b)] = {0} for every c in a+b. Then the cardinality of the isomorphic image of b (viewed as a subset of R) cannot exceed the cardinality of a+b.*

Contrarily to Nakassis' hyperfields, the author has used hyperfields in which the hypersum of two elements contains the two addends and he has proved that certain classes of such hyperfields contain elements that are not quotient hyperfields [3], [4], [5]. The construction of Massouros' hyperfields starts with a multiplicative group, which is then equipped with a multiplicatively absorbing element and a hypercomposition. For instance, if Θ is a multiplicative group with more than two elements and if 0 is a bilaterally multiplicatively absorbing element, then the set $H = \Theta \cup \{0\}$ becomes a hyperfield when we define a hypercomposition as follows:

$x+0 = 0+x = x$, 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 $x \neq y$

It has been proved [4], [6], [8] that if Θ is periodic, then the hyperfield $(H,+,\cdot)$ is not a quotient hyperfield. Corresponding result has been proved in [5] for hyperfields with no selfopposite elements. The research which has been carried out by the author has led to the introduction of hyperfields which have the property that for each one of their non zero elements, the difference x-x gives the entire hyperfield. Due to this property, the above hyperfields were named monogene. A. Nakassis,

having worked on these hyperfields, has proved that there exist monogene hyperfields which are quotient hyperfields [3], [7]. Moreover, the study of the isomorphism of the monogene hyperfields to the quotient ones has led the author to a problem in the theory of the fields, which he firstly presented in the early 80's. In the following paragraphs there will appear the problem and its hitherto partial solutions.

2. The Isomorphism of Monogene Hyperfields to the Quotient Hyperfields and the Genesis of a Problem in the Theory of Fields.

As it has been proved in [3], [7] and [8], if a monogene hyperfield is isomorphic to a quotient hyperfield F/G, then for every non zero element xG of F/G it will hold xG - xG = F/G and consequently for G and F it will be G-G = F. Thus the author raised the question:

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

The first attempts to solve this problem appear in [3], where the solution is connected with the characteristic of the field F. So it is being proved that in the finite fields, the multiplicative subgroups of index 3 which do not contain the multiplicative group of the prime subfield of F, satisfy the equality G-G = F, provided that char F > 13. Corresponding property is proved for the multiplicative subgroups of index 2 in fields with char F > 5.

The final solution of this problem though, for multiplicative subgroups of index 2 and 3, is given in [8], where the following two theorems are being proved:

Theorem 2.1. *If F is a finite field and G a subgroup of the multiplicative group of F which has index 2 and card G > 2, then G-G = F.*

Theorem 2.2. *If F is a finite field and G a subgroup of the multiplicative group of F which has index 3 and card G > 5, then G-G = F*

After the proof of these theorems, it is beyond any doubt that the validity of the equality G-G = F depends only on the cardinality of G. Of course this does not mean that every subset S of F with the same cardinality as G has the property S-S = F. Indeed let $F = Z_{19}$. Then if we consider the multiplicative subgroup of index 3 which is $G = \{1, 7, 8, 11, 12, 18\}$, we have G-G = F, while if we consider the set $S = \{1, 6, 8, 11, 13, 17\}$ which has the same number of elements with G, we have $S-S \neq F$. It must be mentioned though that the classes $\xi^i G$ which are defined in F^* by G, are sets with the same cardinality as G that satisfy the equality $\xi^i G - \xi^i G = F$, when of course this is satisfied by G.

3. The solution of this problem for Multiplicative Subgroups of Index 4 and 5.

We have already described the problem and its hitherto solution for multiplicative subgroups of index 2 and 3. Here we will proceed with the solution for multiplicative subgroups of index 4 and 5.

So, firstly, let's consider that the index of the multiplicative subgroup G is 4. In this case it is possible for -1 either to belong or not to belong in G. Thus we start with the assumption that -1 is an element of G. Then the characteristic of the field F can not be equal to 2. Indeed, if card $F = 2^k$, then card $F^* = 2^k-1$ and therefore card F^* is an odd number which implies that there can not exist a multiplicative subgroup of index 4.

As G is a subgroup of index 4, it creates a partition in F which consists of five classes and thus:

$$F = G \cup \xi G \cup \xi^2 G \cup \xi^3 G \cup \{0\}$$

Moreover, since F is a field, it holds that F-1 = F and so:

$$F = (G-1) \cup (\xi G-1) \cup (\xi^2 G-1) \cup (\xi^3 G-1) \cup (\{0\}-1)$$

Obviously, the above differences consist of elements from the five classes that have been defined by G. Thus, if $\gamma_i \in G$, i=1, 2 and $\xi^4 = \gamma \in G$, then we have:

$\gamma_1 - 1 = \xi\gamma_2 \Leftrightarrow \xi(-\gamma_2) - 1 = -\gamma_1$

$\gamma_1 - 1 = \xi\gamma_2 \Leftrightarrow \xi^3\gamma_1 - \xi^3 = \xi^4\gamma_2 \Leftrightarrow \xi^3\gamma_1 - \gamma\gamma_2 = \xi^3 \Leftrightarrow \xi^3\gamma_1(\gamma\gamma_2)^{-1} - 1 = \xi^3(\gamma\gamma_2)^{-1}$

Consequently, if λ elements from ξG belong to G-1, then λ elements from G belong to ξG-1 and λ elements from $\xi^3 G$ belong to $\xi^3 G$-1. Working in a similar way we reach the following Lemma:

Lemma 3.1. *The following equalities are valid:*

- $card [\xi G \cap (G-1)] = card [G \cap (\xi G-1)] = card [\xi^3 G \cap (\xi^3 G-1)] = \lambda$
- $card [\xi^2 G \cap (G-1)] = card [\xi^2 G \cap (\xi^2 G-1)] = card [G \cap (\xi^2 G-1)] = \mu$
- $card [\xi^3 G \cap (G-1)] = card [\xi G \cap (\xi G-1)] = card [G \cap (\xi^3 G-1)] = \nu$
- $card [\xi^2 G \cap (\xi G-1)] = card [\xi^3 G \cap (G-1)] = card [\xi G \cap (\xi^2 G-1)] =$
  $= card [\xi^3 G \cap (\xi^2 G-1)] = card [\xi G \cap (\xi^3 G-1)] = card [\xi^2 G \cap (\xi^3 G-1)] = \tau$
- $card [G \cap (G-1)] = \kappa$

and for the $\kappa, \lambda, \mu, \nu$ *holds:*

i. $\kappa+\lambda+\mu+\nu+1 = card\ G$
ii. $\lambda+\nu+2\tau = card\ G$
iii. $2\mu+2\tau = card\ G$

This Lemma is very significant for the rest, since it determines the restrictions for the cardinality of G, so that the equality G-G = F is being verified.

Lemma 3.2. *a) If $\lambda=0$, $v\neq 0$ and $\kappa\geq 4$, then $v>3$.*
b) If $v=0$, $\lambda\neq 0$ and $\kappa\geq 4$, then $\lambda>3$.

P r o o f. From the equations

$$\lambda+v+2\tau = \text{card } G \quad \text{and} \quad 2\mu+2\tau = \text{card } G$$

and the suppositions for λ and v we have that $v=2\mu$, which implies that $v\neq 1$. Assume that $v=2$. Then $\mu=1$. So $G \cap (\xi^2 G-1)$ contains only one element. Let's suppose that this element is $\xi^2\gamma_1-1$. We shall look in the differences $\xi^i G-1$ to find which one of them contains the inverse of this element.

If $(\xi^2\gamma_1-1)^{-1} = \gamma_2-1 \in G-1$, then $(\xi^2\gamma_1-1)(\gamma_2-1) = 1 \Leftrightarrow \xi^2\gamma_1 = \gamma_2(\gamma_2-1)^{-1} \in G$, thus $\xi^2\gamma_1 \in G$ which is absurd.

If $(\xi^2\gamma_1-1)^{-1} = \xi^3\gamma_2-1 \in \xi^3 G-1$, then $(\xi^2\gamma_1-1)(\xi^3\gamma_2-1) = 1 \Leftrightarrow \xi\gamma_2 = \gamma_1(\xi^3\gamma_2-1) \in G$, thus $\xi\gamma_2 \in G$, which is absurd.

Lastly, since $\lambda=0$, $(\xi^2\gamma_1-1)^{-1}$ does not belong to $\xi G-1$, and so we have to assume that $(\xi^2\gamma_1-1)^{-1} = \xi^2\gamma_1-1$, since there does not exist any other element of G in the set $\xi^2 G-1$. Then

$$(\xi^2\gamma_1-1)^2 = 1 \Rightarrow \xi^4\gamma_1^2 - 2\xi^2\gamma_1 = 0 \Rightarrow \xi^2\gamma_1 - 2 = 0 \Rightarrow \xi^2\gamma_1 = 2$$

Thus $2 \in \xi^2 G$, and so 1 is the only element of G which belongs to $\xi^2 G-1$, while $-1-1 = -2$ is the only element of $G-1$ which belongs to $\xi^2 G$.

Next let's assume that $\kappa\geq 4$. Then there exists an element of G which belongs to G-1 along with its opposite. That is:

$$(\gamma_1-1) + (\gamma_2-1) = 0 \Rightarrow \gamma_1+\gamma_2 = 2 \Rightarrow -\gamma_1\gamma_2^{-1} - 1 = -2\gamma_2^{-1}$$

Since -2 is the only element of $\xi^2 G$ which belongs to the set G-1, it derives that $\gamma_2=1$. But this is absurd and therefore $v>2$.

Moreover, due to the equations (ii) and (iii) of Lemma 3.1, if $v=3$, then $2\mu=3$, which is absurd. Thus $v>3$.

Part (b) can be proved in a similar way and so the Lemma.

Lemma 3.3. *a) If $r \in G \cap (\xi^3 G-1)$, $r^2=-1$, $\lambda = 0$ and $\kappa\geq 4$, then $v>4$.*
b) If $r \in G \cap (\xi G-1)$, $r^2=-1$, $v = 0$ and $\kappa\geq 4$, then $\lambda>4$.

P r o o f. Because of Lemma 3.2, $v>3$. Also, because of the equations (ii) and (iii) of Lemma 3.1, if $v = 4$, then $\mu = 2$. Let $r = \xi^3\gamma_1-1$ and $\xi^4 = \gamma$. Thus:

$$(\xi^3\gamma_1-1)^2 = -1 \Rightarrow \xi^2\gamma\gamma_1^2 - 2\xi^3\gamma_1+1 = -1 \Rightarrow \xi^2\gamma\gamma_1^2 = 2\xi^3\gamma_1-2 \Rightarrow \xi^2\gamma\gamma_1^2 = 2(\xi^3\gamma_1-1)$$

Consequently $2 \in \xi^2 G$. Since $1 = 2-1 \in \xi^2 G-1$, then one more element of G, different than 1, must belong to $\xi^2 G-1$. Let this element be $\xi^2\gamma_2-1$. As it derives from the proof of Lemma 3.2, this element must be self-inverse. So:

$$(\xi^2\gamma_2-1)^2 = 1 \Rightarrow \xi^4\gamma_2^2 - 2\xi^2\gamma_2+1 = 1 \Rightarrow \xi^2\gamma_2(\xi^2\gamma_2-2) = 0 \Rightarrow \xi^2\gamma_2 = 2$$

Therefore $\xi^2\gamma_2-1 = 2-1 = 1$, absurd.

Part (b) can be proved in a similar way and so the Lemma.

Lemma 3.4. *If* $G - G = G \cup \xi^2 G \cup \xi^3 G \cup \{0\}$, *then* $2 \notin \xi^3 G$.

P r o o f. Because $G - G = G \cup \xi^2 G \cup \xi^3 G \cup \{0\}$ we have

$$\xi G - \xi G = \xi G \cup \xi^3 G \cup G \cup \{0\}$$
$$\xi^2 G - \xi^2 G = \xi^2 G \cup G \cup \xi G \cup \{0\}$$
$$\xi^3 G - \xi^3 G = \xi^3 G \cup \xi G \cup \xi^2 G \cup \{0\}$$

Let $2 \in \xi^3 G$. Then $4 \in \xi^2 G$ and $8 \in \xi G$. Now, for 3 we have:
$3 = 2+1 \in \xi^3 G + G$, thus $3 \neq 0$
$1 = 3-2$ so $3 \notin \xi^3 G$, because otherwise $G \cap (\xi^3 G - \xi^3 G) \neq \varnothing$, absurd.
If $3 \in G$ or $3 \in \xi^2 G$, then $9 \in G$, and since $8 = 9-1$ we will have $\xi G \cap (G - G) \neq \varnothing$, absurd.
If $3 \in \xi G$, then $6 \in G$, $9 \in \xi^2 G$, $12 \in \xi^3 G$ and $5, 7, 11 \neq 0$, because
$5 = 4+1 \in \xi^2 G - G$, $7 = 4+3 \in \xi^2 G - \xi G$, $11 = 9+2 \in \xi^2 G - \xi^3 G$
Now, for 5 we have:
$5 = 6-1 \in G - G$ thus $5 \notin \xi G$
$5 = 9-4 \in \xi^2 G - \xi^2 G$ thus $5 \notin \xi^3 G$
$5 = 8-3 \in \xi G - \xi G$ thus $5 \notin \xi^2 G$
If $5 \in G$, then for 7 we have
$7 \notin G$ because $8 = 7+1$ and $\xi G \cap (G - G) = \varnothing$
$7 \notin \xi G$ because $7 = 6+1$ and $\xi G \cap (G - G) = \varnothing$
$7 \notin \xi^2 G$ because $2 = 9-7$ and $\xi^3 G \cap (\xi^2 G - \xi^2 G) = \varnothing$
$7 \notin \xi^3 G$ because $5 = 12-7$ and $G \cap (\xi^3 G - \xi^3 G) = \varnothing$
Consequently the initial assumption for 2 has led into a contradiction and thus the Lemma.

Analogously we can prove the next Lemmas:

Lemma 3.5. *If* $G - G = G \cup \xi G \cup \xi^2 G \cup \{0\}$, *then* $2 \notin \xi G$.

Lemma 3.6. *If* $G - G = G \cup \xi G \cup \xi^2 G \cup \{0\}$, *then* $2 \in G$.

Proposition 3.1. *If* $G \cup \xi^2 G \cup \xi^3 G \cup \{0\} \subseteq G - G$ *and card* $G > 11$, *then* $F = G - G$

P r o o f. Let $\xi G \cap (G - G) = \varnothing$. We consider an element r of G such that $r^2 \neq -1$, $r^3 \neq 1$ and $r-1 \in \xi^3 G$. According to the preceding Lemmas 3.2. and 3.3., such an element r exists in G when card G>11. Then

i. $r+1 \neq 0$, because $r+1 = (r-1) + 2$ and $r-1 \in \xi^3 G$ while, because of Lemma 3.4, 2 does not belong to $\xi^3 G$.
ii. $r+1 \notin \xi G$, because $r+1 \in G + G$

iii. $r+1 \notin \xi^2G$, because on the contrary case we would have
$r^2-1 = (r-1)(r+1) \in \xi G$, which is absurd.
iv. Let $r+1 \in \xi^3G$, then $r^2-1 \in \xi^2G$ and
$2 = r+1 - (r-1) \in \xi^3G - \xi^3G$, so $2 \notin G$
$2 = 1+1 \in G + G$ so $2 \notin \xi G$
$2 \notin \xi^3G$, because of Lemma 3.4. Therefore $2 \in \xi^2G$
For r^2+1 now, we have
$r^2+1 \in G + G$ thus $r^2+1 \notin \xi G$
$r^2+1 \notin \xi^3G$ because on the contrary case we would have
$r^4-1 = (r^2-1)(r^2+1) \in \xi G$, which is absurd.
Consequently we have the following two cases for r^2+1 :
α) Let $r^2+1 \in \xi^2G$, then $r^4-1 \in G$ and for r^3-1 and r^3+1 we have
$r^3+1 \neq 0$, because $r^3+1 = r(r^2+1) - (r-1) \in \xi^2G - \xi^3G$
$r^3-1 \notin \xi G$ and $r^3+1 \notin \xi G$, because r^3-1, $r^3+1 \in G + G$
$r^3-1 \notin \xi^2G$, because on the contrary case we would have:
$$\xi^3G \ni r^2(r+1) = (r^3-1) + (r^2+1) \in \xi^2G + \xi^2G, \text{ absurd.}$$
$r^3+1 \notin \xi^2G$, because on the contrary case we would have:
$$\xi^3G \ni r^2(r-1) = (r^3+1) - (r^2+1) \in \xi^2G + \xi^2G, \text{ absurd.}$$
$r^3+1 \notin \xi^3G$, because on the contrary case we would have:
$$G \ni r^4-1 = r(r^3+1) - (r+1) \in \xi^3G + \xi^3G, \text{ absurd.}$$
$r^3-1 \notin \xi^3G$ because if $r^3-1 \in \xi^3G$, then $r^2+r+1 \in G$, and
$$\xi G \ni (r+1)(r^2+1) = r(r^2+r+1) + 1 \in G + G, \text{ absurd.}$$
Finally if $r^3-1 \in G$ and $r^3+1 \in G$, then $r^2+r+1 \in \xi G$ and $r^2-r+1 \in \xi G$
and therefore $\xi^2G \ni 2r = (r^2+r+1) - (r^2-r+1) \in \xi G - \xi G$, which is absurd.
β) Let $r^2+1 \in G$, then $r^4-1 \in \xi^2G$ and so for r^3+1 we will have:
$r^3+1 \neq 0$, because $r^3+1 = r(r^2+1) - (r-1) \in G - \xi^3G$
$r^3+1 \notin \xi G$, because $r^3+1 \in G + G$
$r^3+1 \notin \xi^2G$, because, otherwise we would have:
$$\xi^3G \ni r^2(r+1) = (r^3+1) + (r^2-1) \in \xi^2G + \xi^2G, \text{ absurd.}$$
$r^3+1 \notin \xi^3G$, because, otherwise we would have:
$$G \ni r(r^2+1) = (r^3+1) + (r-1) \in \xi^3G + \xi^3G, \text{ absurd.}$$
$r^3+1 \notin G$, because, otherwise we would have $r^2-r+1 \in \xi G$ and
$$\xi G \ni r^2-r+1 = (r^2+1) - r \in G + G, \text{ which is absurd.}$$
iv. Let $r+1 \in G$, then $r^2-1 \in \xi^3G$ and for r^2+1 we have
$r^2+1 \notin \xi G$, because $r^2+1 \in G + G$
$r^2+1 \notin \xi^2G$, because on the contrary case we would have:
$$r^4-1 = (r^2-1)(r^2+1) \in \xi G, \text{ absurd.}$$
$r^2+1 \notin \xi^3G$, because on the contrary case we would have:
$$G \ni r(r+1) = (r^2+1) + (r-1) \in \xi^3G + \xi^3G, \text{ absurd.}$$
Thus let $r^2+1 \in G$. Then $r^4-1 \in \xi^3G$ and
$r^4+1 \neq 0$, because $r^4+1 = r^2(r^2+1) - (r^2-1) \in G - \xi G$

$r^4+1 \notin \xi G$, because $r^4+1 \in G + G$
$r^4+1 \notin \xi^2 G$, because $r^3-1 \in G + G$
$r^4+1 \notin \xi^3 G$, because otherwise we would have:

$$G \ni r^2(r^2+1) = (r^4+1) + (r^2-1) \in \xi^3 G + \xi^3 G, \text{ absurd.}$$

Therefore $r^4+1 \in G$. Now for r^3-1 it holds:
$r^3-1 \notin G$ because otherwise it would be:

$$G \ni r(r^3-1) = (r^4-1) - (r-1) \in \xi^3 G - \xi^3 G, \text{ absurd.}$$

$r^3-1 \notin \xi G$, because $r^3-1 \in G + G$
$r^3-1 \notin \xi^2 G$, because otherwise it would be:

$$\xi G \ni (r^3-1)(r-1) = (r^4+1) - r(r^2+1) \in G + G, \text{ absurd.}$$

Thus $r^3-1 \in \xi^3 G$. Then for $r^3 + 1$ it holds:
$r^3+1 \neq 0$, because $r^3+1 = r(r^2-1) + (r+1) \in \xi G + G$
$r^3+1 \notin \xi G$, since $r^3+1 \in G + G$
$r^3+1 \notin \xi^2 G$, because $r^6-1 \in G + G$
$r^3+1 \notin \xi^3 G$, because otherwise it would be:

$$G \ni r^3(r+1) = (r^4-1) + (r^3+1) \in \xi^3 G + \xi^3 G, \text{ absurd}$$

Consequently $r^3+1 \in G$.
Next let's consider the $r-1$, r^2-1, r^3-1 which belong to $\xi^3 G$. Then:

$$(r-1)(r^2-1)(r^3-1) \in \xi G \Rightarrow r^4(r^2-r-1) + (r^2+r-1) \in \xi G$$

We will see where do r^2-r-1 and r^2+r-1 belong. Firstly
$r^2-r-1 \notin \xi G$, because $r^2-r-1 = r^2 - (r+1) \in G - G$
$r^2+r-1 \notin \xi G$, because $r^2+r-1 = r(r+1) - 1 \in G - G$
$r^2-r-1 \notin \xi^3 G$, because on the contrary case it would be:

$$G \ni -1 = (r^2-r-1) - r(r-1) \in \xi^3 G - \xi^3 G, \text{ absurd.}$$

$r^2+r-1 \notin \xi^3 G$, because on the contrary case it would be:

$$G \ni r^2 = (r^2+r-1) - (r-1) \in \xi^3 G - \xi^3 G, \text{ absurd.}$$

Next let $r^2-r-1 \in \xi^2 G$. Then

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

and since $r^3+1 \in G$, it derives that $2 \notin G$. Therefore we have that $2 \in \xi^2 G$
Also from $r^2-r-1 \in \xi^2 G$ and $r+1 \in G$, it derives

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

Then

$$\xi^3 G \ni r^3-1 = (r^3-2r-1) + 2r \in \xi^2 G + \xi^2 G, \text{ absurd}$$

So $r^2-r-1 \in G$.
Now let $r^2+r-1 \in \xi^2 G$. Then

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

and so

$$\xi^3 G \ni r^3-1 = (r^3+2r^2-1) - 2r^2 \in \xi^2 G - \xi^2 G, \text{ which is absurd}$$

Therefore $r^2+r-1 \in G$, which implies that

$$\xi G \ni r^4(r^2-r-1) + (r^2+r-1) \in G + G$$

which is a contradiction, and thus the Proposition.

Analogously to Proposition 3.1 we can prove the next Proposition:

Proposition 3.2. *If $G \cup \xi G \cup \xi^2 G \cup \{0\} \subseteq G - G$ and card $G > 11$, then $F = G - G$*

Proposition 3.3. *If $G \cup \xi G \cup \xi^3 G \cup \{0\} \subseteq G - G$ and card $G > 5$, then $F = G - G$.*

P r o o f. Suppose that $\xi^2 G \cap (G-G) = \varnothing$. Then because of Lemma 3.6, $2 \in G$. We consider an element r of G such that $r-1 \in \xi G$. Then $r \neq -1$, since $-2 \notin \xi G$, and

i. $r+1 \notin \xi^2 G$, because $r+1 \in G + G$

ii. $r+1 \notin \xi G$, because, on the contrary case we would have:
$$r^2-1 = (r-1)(r+1) \in \xi^2 G$$
which is absurd.

iii. $r+1 \notin \xi^3 G$, because, otherwise we would have:
$$G \ni 4r = (r+1)^2 - (r-1)^2 \in \xi^2 G - \xi^2 G$$
which is absurd.

iv. Lastly, let $r+1 \in G$. Then $r^2-1 \in \xi G$, $r^2 \neq -1$ and for the same reasons as above (i)-(iii) $r^2+1 \in G$. But then:
$$\xi^2 G \ni (r-1)^2 = (r^2+1) - 2r \in G - G$$
which contradicts the supposition, and so the Proposition.

Lemma 3.7. *If $G - G = G \cup \xi G \cup \{0\}$, then $2 \in G$, $i = 1, 3$.*

P r o o f. Let $G - G = G \cup \xi^3 G \cup \{0\}$ and let $2 \in \xi^3 G$. Then $4 \in \xi^2 G$ and $8 \in \xi G$. Since $3 = 4-1$ and $\xi^2 G \neq G$ it is $3 \neq 0$. Also $3 \notin G$ because $4 = 3+1$ and $\xi^2 G \cap (G - G) = \varnothing$. Similarly, from $7 = 8-1$ it derives that $7 \neq 0$ and $7 \notin G$.

If $3 \in \xi G$, then $6 \in G$, $9 \in \xi^2 G$, and
$$5 = 2+3 \in \xi^3 G + \xi G, \text{ thus } 5 \neq 0 \qquad (1)$$
$$5 = 6-1 \in G \cup \xi^3 G \qquad (2)$$
Now $7 \in \xi^3 G$, because $7 = 6+1 \in G + G$ and $7 \neq 0$, $7 \notin G$. Then, additionally to the above (1) and (2), for 5 we also have the relations:
$$5 = 7-2 \in \xi^3 G - \xi^3 G = \xi^3 G \cup \xi^2 G \cup \{0\} \qquad (3)$$
$$5 = 9-4 \in \xi^2 G - \xi^2 G = \xi^2 G \cup \xi G \cup \{0\} \qquad (4)$$
From (1), (2), (3) and (4) it derives that we are led into a contradiction.

If $3 \in \xi^2 G$, then $6 \in \xi G$. But
$$2 = 8-6 \Rightarrow \xi^3 G \subseteq \xi G - \xi G \Rightarrow \xi^2 G \subseteq G - G, \text{ absurd.}$$
If $3 \in \xi^3 G$, then $6 \in \xi^2 G$. But
$$2 = 6-4 \Rightarrow \xi^3 G \subseteq \xi^2 G - \xi^2 G \Rightarrow \xi G \subseteq G - G, \text{ absurd.}$$
In an analogous way as above one can prove the Lemma for $i=1$.

Proposition 3.4. *If card G > 2, then* $G - G \neq G \cup \xi^i G \cup \{0\}$, $i = 1, 2, 3$.

P r o o f. *α)* Let $G - G = G \cup \xi^3 G \cup \{0\}$. We consider $r \in G$, such that $r-1 \in \xi^3 G$.
If $r+1 = 0$, then $r = -1$ and so $2 \in \xi^3 G$, which is absurd, because of Lemma 3.7 If $r+1 \in \xi^3 G$, then $r^2-1 \in \xi^2 G$. But $r^2-1 \in G - G$ and so $\xi^2 G \cap (G - G) \neq \varnothing$, absurd.
If $r+1 \in G$, then $r^2-1 \in \xi^3 G$.
For similar reasons as above, $r^2+1 \neq 0$ and $r^2+1 \notin \xi^3 G$. Thus $r^2+1 \in G$. But then we have:

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

Because of Lemma 3.7, we have that $2 \in G$. But then $(G - G) \cap \xi^2 G \neq \varnothing$, which is a contradiction.
Analogous is the proof of the Proposition for i=1.
β) Suppose that $G - G = G \cup \xi^2 G \cup \{0\}$. If $\xi^2\gamma_1 - 1 \in \xi G$ and $\xi^2\gamma_2 - 1 \in \xi G$, then

$$\xi G - \xi G \ni (\xi^2\gamma_1 - 1) - (\xi^2\gamma_2 - 1) = \xi^2\gamma_1 - \xi^2\gamma_2 \in \xi^2 G - \xi^2 G$$

But $(\xi G - \xi G) \cap (\xi^2 G - \xi^2 G) = \{0\}$, thus $\gamma_1 = \gamma_2$. Therefore it will be $\lambda=0$, $v=0$ and $\tau=0$ or $\tau=1$.
If $\tau=0$, then the set $K = G \cup \xi^2 G \cup \{0\}$ must be a subfield of F.
Let p be the characteristic of F, then $|F| = p^k$ and $p^k = 4|G| + 1$ as well as $|K| = p^\lambda$ and $p^\lambda = 2|G| + 1$ with $\lambda<k$. Let $k = \lambda+t$. Then

$$p^k = 4|G| + 1 \Rightarrow p^{\lambda+t} = 2|G| + 2|G| + 1 \Rightarrow p^\lambda p^t = 2|G| + 2|G| + 1 \Rightarrow$$

$$\Rightarrow (2|G| + 1)p^t = 2|G| + 2|G| + 1 \Rightarrow 1 < p^t = \frac{2|G|}{2|G|+1} + 1 < 2, \text{ absurd.}$$

If $\tau=1$, then, because of the equation (ii) of Lemma 3.1. we have that card G=2, which contradicts the initial suppositions. Thus the Proposition.

With analogous procedures like the ones which have been developed above, and especially similar to the ones of the Proposition 3.1., it can be proved that:

Proposition 3.5. *If card G > 10, then* $G \subseteq G - G$

and so we have the Theorem:

Theorem 3.1. *If* $-1 \in G$ *and card G > 11, then:*

$$G - G = F$$

Theorem 3.2. *If* $-1 \notin G$ *and card G > 3, then:*

$$G - G = F$$

P r o o f. Since $-1 \notin G$, it derives that one of the following three cases may hold:

(i) $G - G = G \cup (-G) \cup \{0\}$
(ii) $G - G = \xi G \cup (-\xi G) \cup \{0\}$
(iii) $G - G = G \cup (-G) \cup \xi G \cup (-\xi G) \cup \{0\}$

Let's suppose that (i) is valid. Then we have the cases:

i.α) If $\aleph = G \cup (-G) \cup \{0\}$ is a subfield of F, then with corresponding reasoning as the one of the second part of the proof of Proposition 3.4. we are led into a contradiction.

i.β) If K is not a subfield of F, then there exists $r \in G$ such that $r-1 \in G$ and $r+1 \in \xi G$. But then $r^2-1 \in \xi G$, which contradicts our initial supposition (i).

Next let's suppose that (ii) is valid. We consider an element $r \in G$ such that $r-1 \in \xi G$ and $r^3 \neq 1$. We observe that $r+1 \neq 0$, since $-1 \notin G$. So we have the cases:

ii.α) If $r^2-1 \in \xi G$, then $r+1 \in G$, thus

$$G \ni r = (r+1) - 1 \in G - G, \text{ absurd}$$

ii.β) If $r^2-1 \in -\xi G$, then $r+1 \in -G$.

ii.β_1) Let $r^3-1 \in \xi G$. Since $r^3-1 = (r-1)(r^2+r+1)$ and $r-1 \in \xi G$, it derives that $r^2+r+1 \in G$. But then

$$G \ni r^2+r+1 = r^2 + (r+1) \in G - G, \text{ absurd}$$

ii.β_2) Let $r^3-1 \in -\xi G$. Then $r^2+r+1 \in -G$. But $r^2 + (r+1) \in G - G$ and therefore $-G \subseteq G - G$, which is absurd.

Consequently (iii) is valid, and so the Theorem.

Lastly, through similar proving method like the one of Theorem 3.1. we can prove the Theorem:

THEOREM 3.3. *If G is a subgroup of index 5 of the multiplicative group of a finite field F and if card G > 23, then:*

$$G - G = F$$

4. BIBLIOGRAPHY

[1] **M. KRASNER** : *Approximation des corps values complets de caracteristique p≠0 par ceux 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. & Math. Sci. Vol. 6, No. 2, pp. 307-312, 1983.

[3] **C.G. MASSOUROS** : *Algebraic Structures with Hypercomposition.* Doctoral Thesis, submitted in Patras University, Greece, 1984.

[4] **C.G. MASSOUROS** : *Methods of constructing hyperfields.* Internat. J. Math. & Math. Sci. Vol. 8, No. 4, pp. 725-728, 1985.

[5] **C.G. Massouros** : *On the theory of hyperrings and hyperfields.* Algebra i Logika 24, No 6, pp. 728-742, 1985.

[6] **C.G. Massouros** : *Hypergroups and their applications.* Doctoral Thesis, Depart. of Sc. of the National Technical University of Athens, 1988.

[7] **C.G. Massouros** : *Constructions of hyperfields.* Mathematica Balkanica Vol 5, Fasc. 3, pp. 250-257, 1991.

[8] **C.G. Massouros** : *A class of hyperfields and a problem in the theory of fields.* Mathematica Montisnigri Vol 1, pp. 73-84, 1993.

[9] **C.G. Massouros** : *On the Hypercompositional Structures.* Fuzzy Systems & A.I. - Reports and Letters, Academia Romana, Vol. 3, no.3, pp. 15-27, 1994.

[10] **J. Mittas** : *Hypergroupes canoniques hypervalues.* C. R. Acad. Sci. (Paris) 271, Serie A, pp. 4-7, 1970.

[11] **J. Mittas** : *Contributions a la theorie des hypergroupes, hyperanneaux, et les hypercorps hypervalues.* C. R. Acad. Sc. Paris, t. 272, Serie A, pp. 3-6, 1971.

[12] **J. Mittas** : *Sur certains classes de structures hypercompositionnelles.* Proceedings of the Academy of Athens, Vol. 48, pp. 298 - 318, Athens 1973.

[13] **J. Mittas** : *Hypergroupes canoniques values et hypervalues. Hypergroupes fortement et superieurement canoniques.* Bull. of the Greek Math. Soc. 23, pp. 55- 88, Athens, 1982.

[14] **J. Mittas** : *Certaines remarques sur les hypergroupes canoniques hypervaluables et fortement canoniques.* Riv. Mat. Pura et Appl. N. 9 pp. 61-67, 1991.

[15] **A. Nakassis** : *Recent results in hyperring and hyperfield theory.* Internat. J. of Math. & Math. Sci. Vol. 11, no. 2, pp. 209-220, 1988.