BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI

Publicat de
UNIVERSITATEA TEHNICĂ "GH.ASACHI", IAŞI

Tomul XLVI (L)

Fasc. 1 — 2

Secţia

MATEMATICĂ
MECANICĂ TEORETICĂ
FIZICĂ

2000

BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
BULLETIN OF THE POLYTECHNIC INSTITUTE OF JASSY
Published by
THE TECHNICAL UNIVERSITY "GH. ASACHI" OF JASSY
Tome XLVI (L), Fasc. 1–2 **2000**

Section

MATHEMATICS. THEORETICAL MECHANICS. PHYSICS

CONTENTS

BULETINUL INSTITUTULUI POLITEHNIC DIN IAŞI
Publicat de
Universitatea Tehnică "Gh. Asachi", Iaşi
Tomul XLVI (L), Fasc. 1-2, 2000
Secţia
MATEMATICĂ. MECANICĂ TEORETICĂ. FIZICĂ

D.C. 519.4

GETTING A FIELD FROM DIFFERENCES OF ITS MULTIPLICATIVE SUBGROUPS

BY

CHRISTOS G. MASSOUROS

Abstract. This paper gives the solution to the hitherto open problem regarding the finite fields which can be written as a difference of a subgroup of their multiplicative group from itself [3], [6] in the case of subgroups of index 4 and 5.

Key words: finite group, multiplicative group, subgroup.

1. Introduction

The notion of the hyperfield has been introduced by M. K r a s n e r in [1]. A hyperfield is a triplet $(H, +, \cdot)$, where $(H, +)$ is a canonical hypergroup, $(H \setminus \{0\}, \cdot)$ is a group and the multiplication is distributive both sides over addition. Also M. Krasner, in order to construct examples of hyperfields, has introduced the quotient ones, creating at the same time the problem of the existence of non quotient hyperfields [2].

The research on the existence of non quotient hyperfields, carried out in the beginning of the 80's, proved the existence of such hyperfields (and hyperrings as well) [3], [4], [5], [8] and at the same time it gave birth to the monogene hyperfields [3], [6], i.e. hyperfields $(H, +, .)$ with the property $x - x = H$ for every nonzero element x. The problem of the isomorphisms of such hyperfields to the quotient hyperfields has been studied by the author and by A. N a k a s s i s and has led the author to the hitherto open question in the theory of fields: *which fields can be written as a difference*

of a subgroup of their multiplicative group from itself and which are these subgroups? [3], [6].

In [3] there appeared theorems that show the first attempt for reaching the answer to this problem and in [7] there appear the following theorems which give the answer to the problem in the case of subgroups with index 2 or 3.

T h e o r e m 1.1. *If F is a finite field and G a subgroup of the multiplicative group of F which has index* 2 *and* card $G > 5$, *then* $G-G = F$.

T h e o r e m 1.2. *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* $G-G = F$.

This paper gives the answer to the problem for the case of subgroups which have index 4 and 5.

2. Finite Fields with Subgroup of their Multiplicative Group which has Index 4

Concerning those subgroups, we will prove two theorems. The first one gives the solution of the problem when -1 does not belong to the subgroup G and the second one solves the problem when -1 is an element of G.

T h e o r e m 2.1. *Let F be a finite field and G a subgroup of its multiplicative group, which has index* 4. *If $-1 \notin G$ and* card $G > 3$ *then* $G - G = F$.

P r o o f. Since $-1 \notin G$, it derives that there can possibly be:

(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 assume that (i) is valid. We have the cases:

α) Let $K = G \cup (-G) \cup \{0\}$ be a subfield of F. If p is the characteristic of F, then $|F| = p^\kappa$ and $p^\kappa = 4|G| + 1$. Also $|K| = p^\lambda$ and $p^\lambda = 2|G| + 1$ with $\lambda < \kappa$. Let $\kappa = \lambda + t$. Then

$$p^\kappa = 4|G| + 1 \Rightarrow p^\lambda p^t = 2|G| + 2|G| + 1 \Rightarrow (2|G| + 1)p^t =$$

$$= 2|G| + 2|G| + 1 \Rightarrow 1 < p^t = \frac{2|G|}{2|G| + 1} + 1 < 2,$$

absurd.

β) Assume that K is not a subfield of F. Then there exists $r \in G$ such that $r-1 \in G$ and $r+1 \in \xi G$. In this case $r^2-1 \in \xi G$, which contradicts the initial hypothesis (i).

Next let's assume 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 $-1 \notin G$. Thus we have the cases:

α) if $r^2-1 \in \xi G$, then $r+1 \in G$, and so $G \ni r = (r+1)-1 \in G-G$, absurd;

β) if $r^2-1 \in -\xi G$, then $r+1 \in -G$;

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 $r^2+r+1 \in G$, in which case $G \ni r^2+r+1 = r^2+(r+1) \in G-G$, absurd;

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 $-G \subseteq G-G$, absurd.

Consequently (iii) is valid and thus the Theorem.

Example 2.1. From the finite fields, $\mathbf{Z}_{29}$ is the one with the smallest cardinality which has multiplicative subgroup of index 4 that does not contain -1 and that has more than 3 elements. More precisely $G = \{1, 7, 25, 16, 20, 23, 24\}$. For this subgroup holds $G-G = \mathbf{Z}_{29}$.

In the following we assume that $-1 \in G$. Then $F = G \cup \xi G \cup \xi^2 G \cup \xi^3 G \cup \{0\}$. We observe that if $-1 \in G$, the characteristic of F can not be 2. Indeed if $|F| = 2^\kappa$, then $|F^*| = 2^\kappa - 1$. Therefore $|F^*|$ is an odd number and so there can not exist a subgroup of index 4.

P r o p o s i t i o n 2.1. *If* card $G > 10$, *then* $G \subseteq G-G$.

P r o o f. Suppose that $G \cap (G-G) = \emptyset$. Then $\xi^i G \cap (\xi^i G - \xi^i G) = \emptyset$. We consider an element r such that $r^\kappa \neq -1$, $\kappa = 1, 2, 4, 5$ and $r^5 \neq 1$. With no loss of the generality we can assume that $r-1 \in \xi G$. Then for $r+1$ we have the cases

$$\text{(I)}\ r+1 \in \xi G, \qquad \text{(II)}\ r+1 \in \xi^2 G, \qquad \text{(III)}\ r+1 \in \xi^3 G.$$

Case (III) leads directly into contradiction, while if it were valid we would have $r^2-1 \in G$, which contradicts to the hypothesis.

Case I. Let $r+1 \in \xi G$, then $r^2-1 \in \xi^2 G$. Now r^2+1 can belong to one of the three classes ξG, $\xi^2 G$ and $\xi^3 G$.

(i) Let $r^2+1 \in \xi G$; then $\xi G \ni r(r-1) = (r^2+1)-(r+1) \in \xi G - \xi G$, absurd.

(ii) Let $r^2+1 \in \xi^2 G$; then $r^4-1 \in G$, absurd.

(iii) Let $r^2+1 \in \xi^3 G$; then $r^4-1 \in \xi G$. Having made those assumptions, we will see where do r^3-1 and r^3+1 belong. Initially both r^3-1 and r^3+1 are different than zero, since

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

and

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

Also r^3-1 belongs to $\xi G - \xi G$, because $r(r^3-1) = (r^4-1)-(r-1) \in \in \xi G - \xi G$. Thus r^3-1 does not belong to ξG and therefore r^2+r+1 does not belong to G. Similarly r^3+1 does not belong to ξG, since $r(r^3+1) = = (r^4-1)+(r+1) \in \xi G - \xi G$ and so $r^2-r+1 \notin G$.

Let $r^3-1 \in \xi^2 G$. Since $r^6-1 \notin G$ we have that $r^3+1 \notin \xi^2 G$. Consequently $r^3+1 \in \xi^3 G$ and therefore $r^6-1 \in \xi G$. Then for r^5-1 we have

i) $r^5-1 \notin \xi G$ since $r(r^5-1) = (r^6-1)-(r-1) \in \xi G - \xi G$;

ii) $r^5-1 \notin \xi^2 G$ since $r^5-1 = r^2(r^3-1)-(r^2-1) \in \xi^2 G - \xi^2 G$;

iii) $r^5-1 \notin \xi^3 G$ since $r^5-1 = r^2(r^3+1)-(r^2+1) \in \xi^3 G - \xi^3 G$.

Therefore we have reached a contradiction. Lastly let $r^3-1 \in \xi^3 G$. If $r^3+1 \in \xi^3 G$, then $r^2+r+1 \in \xi^2 G$ and $r^2-r+1 \in \xi^2 G$. So we have

i) from $2 = (r+1)-(r-1) \in \xi G - \xi G$ it derives that $2 \notin \xi G$;

ii) from $2 = (r^3+1)-(r^3-1) \in \xi^3 G - \xi^3 G$ it derives that $2 \notin \xi^3 G$;

iii) from $2r = (r^2+r+1)-(r^2-r+1) \in \xi^2 G - \xi^2 G$ it derives that $2 \notin \xi^2 G$.

Consequently $r^3+1 \notin \xi^3 G$. Lastly let $r^3+1 \in \xi^2 G$. Then

i) $r^5+1 \notin \xi G$ because $r^5+1 = r^4(r+1)-(r^4-1) \in \xi G - \xi G$;

ii) $r^5+1 \notin \xi^2 G$ because $r^5+1 = r^2(r^3+1)-(r^2-1) \in \xi^2 G - \xi^2 G$;

iii) $r^5+1 \notin \xi^3 G$ because $r^5+1 = r^3(r^2+1)-(r^3-1) \in \xi^3 G - \xi^3 G$.

Therefore, Case I has led to contradiction.

Case II. Let $r+1 \in \xi^2 G$, then $r^2-1 \in \xi^3 G$. Now r^2+1 can belong to one of the three classes ξG, $\xi^2 G$ and $\xi^3 G$.

(i) Let $r^2+1 \in \xi G$; then $r^4-1 \in G$, absurd.

(ii) Let $r^2+1 \in \xi^2 G$; then $r^4-1 \in \xi G$. Having made these assumptions, we will see where do r^3-1 and r^3+1 belong. At first we observe that r^3-1 is different that 0 and it does not belong to either ξG or $\xi^2 G$, because

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

$$r^3 - 1 = (r^4 - 1) - (r-1) \in \xi G - \xi G;$$

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

So let $r^3 - 1 \in \xi^3 G$. Then $r^3+1 \neq 0$ because $r^3+1 = r(r^2+1) - (r-1) \in \in \xi^2 G - \xi G$. Also $r^3 + 1 \notin \xi G$ since $r^6 - 1 \notin G$. If $r^3 + 1 \in \xi^2 G$ then $r^6 - 1 \in \xi G$, while for $r^5 - 1$ we have

i) $r^5 - 1 \notin \xi G$ because $r(r^5 - 1) = (r^6 - 1) - (r - 1) \in \xi G - \xi G$;

ii) $r^5 - 1 \notin \xi^2 G$ because $r^5 - 1 = r^3(r^2 + 1) - (r^3 + 1) \in \xi^2 G - \xi^2 G$;

iii) $r^5 - 1 \notin \xi^3 G$ because $r^5 - 1 = r^3(r^2 - 1) - (r^2 - 1) \in \xi^3 G - \xi^3 G$.

Thus $r^3 + 1 \notin \xi^2 G$. If $r^3 + 1 \in \xi^3 G$, then $r^6 - 1 \in \xi^2 G$ and $r^6 - 1 \in \xi G$ since

i) $r^6 + 1 \neq 0$ because $r^6 + 1 = r^2(r^4 - 1) + (r^2 + 1) \in \xi G - \xi^2 G$;

ii) $r^6 + 1 \notin \xi^2 G$ because $r^{12} - 1 \notin G$;

iii) $r^6 + 1 \notin \xi^3 G$ because $r^6 + 1 = r^3(r^3 + 1) - (r^3 - 1) \in \xi^3 G - \xi^3 G$.

Then for $r^5 + 1$ we have

i) $r^5 + 1 \notin \xi G$ because $r^5 + 1 = (r^6 + 1) - r^5(r - 1) \in \xi G - \xi G$;

ii) $r^5 + 1 \notin \xi^2 G$ because $r(r^5 + 1) = (r^6 - 1) + (r + 1) \in \xi^2 G - \xi^2 G$;

iii) $r^5 + 1 \notin \xi^3 G$ because $r^5 + 1 = r^3(r^2 - 1) + (r^3 + 1) \in \xi^3 G - \xi^3 G$.

Thus $r^3 + 1 \notin \xi^3 G$ and therefore the assumption $r^2 + 1 \in \xi^2 G$ is absurd.

(iii) Let $r^2 + 1 \in \xi^3 G$; then $r^4 - 1 \in \xi^2 G$ and $r^4 + 1 \in \xi G$ since

i) $r^4 + 1 \notin \xi^2 G$ because $(r^4 - 1)(r^4 + 1) = r^8 - 1 \notin G$;

ii) $r^4 + 1 \notin \xi^3 G$ because $r^4 + 1 = r^2(r^2 + 1) - (r^2 - 1) \in \xi^3 G - \xi^3 G$.

It is again necessary to see where do the $r^3 - 1$ and $r^3 + 1$ belong, under the new assumptions. Initially $r^3 + 1$ and $r^3 - 1$ are both different than zero, since

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

and

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

Also r^3+1 does not belong to ξ^2G since $r(r^3+1)=(r^4-1)+(r+1)\in$ $\in\xi^2G-\xi^2G$. Let's suppose that $r^3-1\in\xi G$. Then r^3+1 is not an element of ξ^3G, because $(r^3-1)(r^3+1)=r^6-1\notin G$. If r^3+1 were an element of ξG then for r^4+1, we would have $r^4+1\notin\xi G$, because $r^4+1=r(r^3+1)-(r-1)\in\xi G-\xi G$. Therefore $r^3-1\notin\xi G$.

Next let's suppose that $r^3-1\in\xi^2G$. If r^3+1 belongs to ξG then for r^4+1, we will have $r^4+1\notin\xi G$ because $r^4+1=r^3(r-1)+(r^3+1)\in\xi G-\xi G$. Therefore $r^3+1\notin\xi G$.

Moreover if r^3+1 belongs to ξ^3G then for r^5+1 we have

i) $r^5+1\notin\xi G$ since $r^5+1=r(r^4+1)-(r-1)\in\xi G-\xi G$;

ii) $r^5+1\notin\xi^2G$ since $r^5+1=r^4(r+1)-(r^4-1)\in\xi^2G-\xi^2G$;

iii) $r^5+1\notin\xi^3G$ since $r^5+1=r^2(r^3+1)-(r^2-1)\in\xi^3G-\xi^3G$.

Thus $r^3+1\notin\xi^3G$ and therefore the supposition that $r^3-1\in\xi^2G$ leads to contradiction.

Lastly let $r^3-1\in\xi^3G$; then $r^3+1\notin\xi G$ since $r^6-1\notin G$. Therefore let

i) $r^3+1\in\xi^3G$; then $r^6-1\in\xi^2G$ and

ii) $r^5+1\notin\xi G$ since $r^5+1=r(r^4+1)-(r-1)\in\xi G-\xi G$;

iii) $r^5+1\notin\xi^2G$ since $r(r^5+1)=(r^6-1)+(r+1)\in\xi^2G-\xi^2G$;

iv) $r^5+1\notin\xi^3G$ since $r^5+1=r^2(r^3+1)-(r^2-1)\in\xi^3G-\xi^3G$.

Therefore the supposition $r^3-1\in\xi^3G$ is absurd. Consequently, Case II has also led to contradiction and so $G\subseteq G-G$.

Since F is a field, we have that $F-1=F$, or equivalently

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

In the following we will calculate how many elements from every class are contained in each one of the differences which form the previous union.

Let $\gamma_i\in G$, $i=1,2$ and let ξ^4, which is an element of G, be equal to γ. Then we have

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

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

Therefore if λ elements from $G-1$ belong to ξG, then λ elements from $\xi G-1$ belong to G and also λ elements from $\xi^3 G-1$ belong to $\xi^3 G$.

$$\gamma_1 - 1 = \xi^2\gamma_2 \Leftrightarrow \xi^2(-\gamma_2) - 1 = -\gamma_1 ;$$

$$\gamma_1-1=\xi^2\gamma_2 \Leftrightarrow \xi^2\gamma_1-\xi^2=\xi^4\gamma_2 \Leftrightarrow \xi^2\gamma_1-\gamma\gamma_2=\xi^2 \Leftrightarrow \xi^2\gamma_1(\gamma\gamma_2)^{-1}-1=\xi^2(\gamma\gamma_2)^{-1}.$$

Therefore if μ elements from $G-1$ belong to $\xi^2 G$, then μ elements from $\xi^2 G-1$ belong to G and also μ elements from $\xi^2 G-1$ belong to $\xi^2 G$,

$$\gamma_1 - 1 = \xi^3\gamma_2 \Leftrightarrow \xi^3(-\gamma_2) - 1 = -\gamma_1 ;$$

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

Therefore if ν elements from $G-1$ belong to $\xi^3 G$, then ν elements from $\xi^3 G-1$ belong to G and also ν elements from $\xi G-1$ belong to ξG,

$$\xi\gamma_1 - 1 = \xi^3\gamma_2 \Leftrightarrow \xi^3(-\gamma_2) - 1 = \xi(-\gamma_1) ;$$

$$\xi\gamma_1-1=\xi^3\gamma_2 \Leftrightarrow \xi^2\gamma_1-\xi=\xi^4\gamma_2 \Leftrightarrow \xi^2\gamma_1-\gamma\gamma_2=\xi \Leftrightarrow \xi^2\gamma_1(\gamma\gamma_2)^{-1}-1=$$

$$=\xi(\gamma\gamma_2)^{-1} \Leftrightarrow \xi(-\gamma\gamma_2)^{-1} - 1 = \xi^2[-\gamma_1(\gamma\gamma_2)^{-1}];$$

$$\xi\gamma_1-1=\xi^3\gamma_2 \Leftrightarrow \xi^4\gamma_1-\xi^3=\xi^2\gamma_2 \Leftrightarrow \gamma\gamma_1-\xi^3=\xi^2\gamma_2 \Leftrightarrow \xi^2\gamma_2(\gamma\gamma_1)^{-1}-1=$$

$$=\xi^3(\gamma\gamma_1)^{-1} \Leftrightarrow \xi^3(-\gamma\gamma_1)^{-1} - 1 = \xi^2[-\gamma_2(\gamma\gamma_1)^{-1}].$$

Therefore if τ elements from $\xi G-1$ belong to $\xi^3 G$, then τ elements from $\xi^2 G-1$ belong to ξG, τ elements from $\xi G-1$ belong to $\xi^2 G$ as well as τ elements from $\xi^2 G-1$ belong to $\xi^3 G$ and also τ elements from $\xi^3 G-1$ belong to $\xi^2 G$.

Lastly if κ elements from G belong to the difference $G-1$ we have the following

P r o p o s i t i o n 2.2. *For every class, the number of its elements which belong to each one of the differences* $G-1$, $\xi G-1$, $\xi^2 G-1$, $\xi^3 G-1$, $\{0\}-1$ *is given from the Table* 1

Table 1

	$G-1$	$\xi G-1$	ξ^2G-1	ξ^3G-1	0-1
G	κ	λ	μ	ν	1
ξG	λ	ν	τ	τ	0
ξ^2G	μ	τ	μ	τ	0
ξ^3G	ν	τ	τ	λ	0
0	1	0	0	0	0

and

i) $\kappa+\lambda+\mu+\nu+1=\operatorname{card} G$;

ii) $\lambda+\nu+2\tau=\operatorname{card} G$;

iii) $2\mu+2\tau=\operatorname{card} G$.

L e m m a 2.1. *If* $G-G=G\cup\xi^iG\cup\{0\}$, *then* $2\in G$, $i=1,3$.

P r o o f. Let $G-G=G\cup\xi G\cup\{0\}$, and let $2\in\xi G$. Then $4\in\xi^2G$ and $8\in\xi^3G$. Since $3=4-1\in\xi^2G-G$ it derives that $3\neq 0$. Also $3\notin G$ because if it belonged to G, then $4=3+1\in\xi^2G\cap(G-G)$, absurd since this intersection must be void. Similarly, since $7=8-1$ we have that $7\neq 0$ and $7\notin G$. If $3\in\xi G$, then $6\in\xi^2G$. But $2=6-4\Rightarrow\xi G\subseteq\subseteq\xi^2G-\xi^2G\Rightarrow G\subseteq\xi G-\xi G$, absurd. If $3\in\xi^2G$, then $6\in\xi^3G$. But $2=8-6\Rightarrow\xi G\subseteq\xi^3G-\xi^3G\Rightarrow G\subseteq\xi^2G-\xi^2G$, absurd.

If $3\in\xi^3G$, then $6\in G$, $9\in\xi^2G$, and

$$5=3+2\in\xi^3G-\xi G \qquad \text{so} \qquad 5\neq 0, \tag{1}$$

$$5=6-1\in G\cup\xi G. \tag{2}$$

Now $7\in\xi G$ because $7=6+1\in G-G$ and $7\neq 0$, $7\notin G$. Then, additionally to (1) and (2) we have for 5

$$5=7-2\in\xi G-\xi G=\xi G\cup\xi^2G\cup\{0\}, \tag{3}$$

$$5=9-4\in\xi^2G-\xi^2G=\xi^2G\cup\xi^3G\cup\{0\}. \tag{4}$$

From (1) – (4) it derives that we have a contradiction.

Similarly we can prove the Lemma for $i=3$.

P r o p o s i t i o n 2.3. *If* $\operatorname{card} G>2$, *then* $G-G\neq G\cup\xi^iG\cup\{0\}$, $i=1,2,3$.

P r o o f. α) Let $G-G=G\cup\xi G\cup\{0\}$. Consider $r\in G$, such that $r-1\in\xi G$. If $r+1=0$ then $r=-1$ and therefore $2\in\xi G$, which is absurd, because of Lemma 2.1. If $r+1\in\xi G$, then $r^2-1\in\xi^2G$. But $r^2-1\in G-G$ and so $\xi^2G\cap(G-G)\neq\emptyset$, absurd. If $r+1\in G$, then $r^2-1\in\xi G$. With similar reasoning as above, $r^2+1\neq 0$ and $r^2+1\notin\xi G$. Therefore $r^2+1\in G$ and so we have

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

But $2\in G$ (Lemma 2.1.), thus $(G-G)\cap\xi^2G\neq\emptyset$, absurd.

Analogous is the proof of the Proposition when $i=3$.

β) Let $G-G=G\cup\xi^2G\cup\{0\}$. If $\xi^2\gamma_1-1\in\xi G$, and $\xi^2\gamma_2-1=\xi G$, then

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

but $(\xi G-\xi G)\cap(\xi^2G-\xi^2G)=\{0\}$, and so $\gamma_1=\gamma_2$. Therefore in the Table 1 of Proposition 2.2 we have $\lambda=0$, $\nu=0$ and either $\tau=0$ or $\tau=1$.

If $\tau=0$, then $K=G\cup\xi^2G\cup\{0\}$ must be a subfield of F. This leads to a contradiction, through a proof similar to the proof of (α) of Theorem 2.1. If $\tau=1$, then, because of equation (ii) of Proposition 2.2 we have that card $G=2$, which contradicts the initial restrictions for G. Thus the Proposition.

From the hitherto analysis it derives that if

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

then one of the following cases is possible to hold:

(i) $G-G=G\cup\xi^2G\cup\xi^3G\cup\{0\}$;

(ii) $G-G=G\cup\xi G\cup\xi^2G\cup\{0\}$;

(iii) $G-G=G\cup\xi G\cup\xi^3G\cup\{0\}$.

L e m m a 2.2. *If* $G-G=G\cup\xi G\cup\xi^3G\cup\{0\}$, *then* $2\in G$.

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

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

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

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

Initially we observe that $2 \notin \xi^2 G$, since $2 = 1 + 1 \in G - G$. Let $2 \in \xi G$. Then $4 \in \xi^2 G$ and $8 \in \xi^3 G$. Now, for 3 and 5 we have: $3 = 2 + 1 \in \xi G - G$ thus $3 \neq 0$; $5 = 4 + 1 \in \xi^2 G - G$ thus $5 \neq 0$; $1 = 4 - 3$ and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, therefore $3 \notin \xi^2 G$; $4 = 3 + 1$ and $\xi^2 G \cap (G - G) = \emptyset$, therefore $3 \notin G$.

Let $3 \in \xi G$. Then $6, 9 \in \xi^2 G$ and for 5 we have: $5 = 9 - 4 \in \xi^2 G - \xi^2 G$, and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, therefore $5 \notin G$; $8 = 5 + 3$ and $\xi^3 G \cap (\xi G - \xi G) = \emptyset$, therefore $5 \notin \xi G$; $1 = 6 - 5$ and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, therefore $5 \notin \xi^2 G$; $5 = 3 + 2 \in \xi G - \xi G$, and $\xi^3 G \cap (\xi G - \xi G) = \emptyset$, therefore $5 \notin \xi^3 G$ and so we are led to a contradiction.

Let $3 \in \xi^3 G$. Then $6 \in G$, $9 \in \xi^2 G$ and for 5 we have: $5 = 9 - 4 \in \xi^2 G - \xi^2 G$ and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, therefore $5 \notin G$; $5 = 8 - 3 \in \xi^3 G - \xi^3 G$ and $\xi G \cap (\xi^3 G - \xi^3 G) = \emptyset$, therefore $5 \notin \xi G$; $5 = 6 - 1 \in G - G$ and $\xi^2 G \cap (G - G) = \emptyset$, therefore $5 \notin \xi^2 G$; $2 = 5 - 3$ and $\xi G \cap (\xi^3 G - \xi^3 G) = \emptyset$, therefore $5 \notin \xi^3 G$. Thus the assumption that $2 \in \xi G$, led to a contradiction.

Now let $2 \in \xi^3 G$. Then $4 \in \xi^2 G$ and $8 \in \xi G$. Again for 3 and 5 we have: $3 = 2 + 1 \in \xi^3 G - G$ so $3 \neq 0$; $5 = 4 + 1 \in \xi^2 G - G$ so $5 \neq 0$; $1 = 4 - 3$ and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, thus $3 \notin \xi^2 G$; $4 = 3 + 1$ and $\xi^2 G \cap (G - G) = \emptyset$, thus $3 \notin G$.

Let $3 \in \xi G$. Then $6 \in G$, $9 \in \xi^2 G$ and for 5 we have: $5 = 9 - 4 \in \xi^2 G - \xi^2 G$ and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, therefore $5 \notin G$; $2 = 5 - 3$ and $\xi^3 G \cap (\xi G - \xi G) = \emptyset$, therefore $5 \notin \xi G$; $5 = 6 - 1 \in G - G$ and $\xi^2 G \cap (G - G) = \emptyset$, therefore $5 \notin \xi^2 G$; $5 = 8 - 3 \in \xi G - \xi G$ and $\xi^3 G \cap (\xi G - \xi G) = \emptyset$, therefore $5 \notin \xi^3 G$. We are led thus to a contradiction.

Let $3 \in \xi^3 G$. Then $6, 9 \in \xi^2 G$ and for 5 we have: $5 = 9 - 4 \in \xi^2 G - \xi^2 G$ and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, therefore $5 \notin G$; $5 = 3 + 2 \in \xi^3 G - \xi^3 G$ and $\xi G \cap (\xi^3 G - \xi^3 G) = \emptyset$, therefore $5 \notin \xi G$; $1 = 6 - 5$ and $G \cap (\xi^2 G - \xi^2 G) = \emptyset$, therefore $5 \notin \xi^2 G$; $8 = 5 + 3$ and $\xi G \cap (\xi^3 G - \xi^3 G) = \emptyset$, therefore $5 \notin \xi^3 G$. Consequently the assumption that $2 \in \xi^3 G$, has also led to a contradiction, and so the Lemma.

The following two Lemmas are being proved in the same way:

L e m m a 2.3. *If* $G - G = G \cup \xi G \cup \xi^2 G \cup \{0\}$, *then* $2 \notin \xi G$.

L e m m a 2.4. *If* $G - G = G \cup \xi^2 G \cup \xi^3 G \cup \{0\}$, *then* $2 \notin \xi^3 G$.

P r o p o s i t i o n 2.4. *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. Let $\xi^2 G \cap (G - G) = \emptyset$. Because of Lemma 2.2, $2 \in G$. 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 in the opposite 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 in the opposite case 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 as above (i)-(iii) reasons $r^2+1 \in G$. But then we have $\xi^2 G \ni (r-1)^2 = (r^2+1) - 2r \in G-G$, which is absurd and so the Proposition.

L e m m a 2.5. *In the Table 1 of Proposition* 2.2 *if* $\nu = 0$, $\lambda \neq 0$ *and* $\kappa \geq 4$, *then* $\lambda > 2$.

P r o o f. From the last two equations of Proposition 2.2 it derives that if $\nu = 0$ and $\lambda \neq 0$, then $\lambda \neq 1$. Let $\lambda = 2$. Then from the same equations it derives that $\mu = 1$. So let $\xi^2\gamma_1 - 1$ be the element of G which belongs to the set $\xi^2 G - 1$. We will search for the set which contains its inverse. Initially let's assume that the inverse of $\xi^2\gamma_1 - 1$ belongs to the set $G-1$, and let it be the $\gamma_2 - 1$. Then

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

But $\gamma_2 - 1 \in G$, thus $\xi^2\gamma_2 \in G$, absurd.

Next let's suppose that the inverse of $\xi^2\gamma_1 - 1$ belongs to the set $\xi G - 1$, and let it be the $\xi\gamma_2 - 1$. Then

$$(\xi^2\gamma_1 - 1)(\xi\gamma_2 - 1) = 1 \Rightarrow (\xi^2\gamma_1 - 1)\xi\gamma_2 - \xi^2\gamma_1 = 0 \Rightarrow (\xi^2\gamma_1 - 1)\gamma_2 = \xi\gamma_1.$$

But $(\xi^2\gamma_1 - 1)\gamma_2 \in G$, thus $\xi\gamma_1 \in G$, absurd.

Lastly we must assume that the inverse of $\xi^2\gamma_1 - 1$ is $\xi^2\gamma_1 - 1$ itself, since there does not exist any other element of G in the set $\xi^2 G - 1$. Then

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

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

Next let's suppose that $\kappa \geq 4$. Then there exists an element of G such that both, this element and its opposite belong to $G-1$, and so we have

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

But the only element of $\xi^2 G$ which belongs to the set $G-1$ is the -2, and so $\gamma_2 = 1$. This is absurd though and therefore $\lambda > 2$.

L e m m a 2.6. *If* $r \in G \cap (\xi G - 1)$, $r^2 = -1$, $\nu = 0$ *and* $\kappa \geq 4$, *then* $\lambda > 4$.

P r o o f. Because of Lemma 2.5, $\lambda > 3$. Also, because of the equations (ii) and (iii) of Proposition 2.2, $\lambda \neq 3$. Moreover, because of the same equations, if $\lambda = 4$ then $\mu = 2$. Let $r = \xi\gamma - 1$. Then $(\xi\gamma - 1)^2 = -1 \Rightarrow \xi^2\gamma^2 - 2\xi\gamma + 1 = -1 \Rightarrow \xi^2\gamma^2 = 2\xi\gamma - 2 \Rightarrow \xi^2\gamma^2 = 2(\xi\gamma - 1)$. Consequently $2 \in \xi^2 G$. Since $1 = 2 - 1 \in \xi^2 G - 1$, it derives that there must exist another element of G in $\xi G - 1$ which is different than 1 and which, as it derives from the proof the Lemma 2.5, must be self-inverse. Let this element be $\xi\gamma - 1$. So we have

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

Thereiore $\xi^2\gamma - 1 = 2 - 1 = 1$, absurd.

P r o p o s i t i o n 2.5. *If* $G \cup \xi G \cup \xi^2 G \cup \{0\} \subseteq G - G$ *and* $\mathrm{card} G > 11$ *then* $F = G - G$.

P r o o f. Let $\xi^3 G \cap (G - G) = \emptyset$. We consider an element r from G such tat $r^2 \neq -1$, $r^3 \neq 1$ and $r - 1 \in \xi G$. According to Lemmas 2.5 and 2.6, there exists such an element. Then

(i) $r + 1 \neq 0$, because $r + 1 = (r - 1) + 2$ and $r - 1 \in \xi G$ while, because of Lemma 2.3, the 2 does not belong to ξG;

(ii) $r + 1 \notin \xi^3 G$, because $r + 1 \in G - G$;

(iii) $r + 1 \notin \xi^2 G$, because in the opposite case we would have $r^2 - 1 = (r - 1)(r + 1) \in \xi^3 G$, which is absurd;

(iv) let $r + 1 \in \xi G$, then $r^2 - 1 \in \xi^2 G$ and $2 = r + 1 - (r - 1) \in \xi G - \xi G$ so $2 \notin G$; $2 = 1 + 1 \in G + G$ so $2 \notin \xi^3 G$; $2 \notin \xi G$, because of Lemma 2.3. Therefore $2 \in \xi^2 G$.

Now, for $r^2 + 1$ we have $r^2 + 1 \in G - G$, thus $r^2 + 1 \notin \xi^3 G$; $r^2 + 1 \notin \xi G$, because if it did belong to ξG we would have $r^4 - 1 = (r^2 - 1)(r^2 + 1) \in \xi^3 G$, which is absurd. Therefore, for $r^2 + 1$ we have the following two cases:

α) Let $r^2 + 1 \in \xi^2 G$; then $r^4 - 1 \in G$ and for $r^3 - 1$ and $r^3 + 1$ we have

i) $r^3 + 1 \neq 0$, because $r^3 + 1 = r(r^2 + 1) - (r - 1) \in \xi^2 G - \xi G$;

ii) $r^3 - 1 \notin \xi^3 G$ and $r^3 + 1 \notin \xi^3 G$, because $r^3 - 1$, $r^3 + 1 \in G - G$;

iii) $r^3 - 1 \notin \xi^2 G$ because if it did belong to $\xi^2 G$ we would have $\xi G \ni r^2(r + 1) = (r^3 - 1) + (r^2 + 1) \in \xi^2 G - \xi^2 G$, absurd;

iv) $r^3 + 1 \notin \xi^2 G$ because if it did belong to $\xi^2 G$ we would have $\xi G \ni r^2(r - 1) = (r^3 + 1) - (r^2 + 1) \in \xi^2 G - \xi^2 G$, absurd;

v) $r^3 + 1 \notin \xi G$ because if it did belong to ξG we would have $G \ni r^4 - 1 = r(r^3 + 1) - (r + 1) \in \xi G - \xi G$, absurd;

vi) $r^3 - 1 \notin \xi G$ because if $r^3 - 1 \in \xi G$, then $r^2 + r + 1 \in G$, and $\xi^3 G \ni (r + 1)(r^2 + 1) = r(r^2 + r + 1) + 1 \in G - G$, absurd.

Lastly if $r^3 - 1 \in G$ and $r^3 + 1 \in G$, then $r^2 + r + 1 \in \xi^3 G$ and $r^2 - r + 1 \in \xi^3 G$ and therefore $\xi^2 G \ni 2r = (r^2 + r + 1) - (r^2 - r + 1) \in \xi^3 G - \xi^3 G$, absurd.

β) Let $r^2 + 1 \in G$, then $r^4 - 1 \in \xi^2 G$ and for $r^3 + 1$ we will have

i) $r^3 + 1 \neq 0$, because $r^3 + 1 = r(r^2 + 1) - (r - 1) \in G - \xi G$;

ii) $r^3 + 1 \notin \xi^3 G$ because $r^3 + 1 \in G - G$;

iii) $r^3 + 1 \notin \xi^2 G$ because if it did belong to $\xi^2 G$ we would have $\xi G \ni r^2(r + 1) = (r^3 + 1) + (r^2 - 1) \in \xi^2 G - \xi^2 G$, absurd;

iv) $r^3 + 1 \notin \xi G$ because in the opposite case we would have $G \ni r(r^2 + 1) = (r^3 + 1) + (r - 1) \in \xi G - \xi G$, absurd;

v) $r^3 + 1 \notin G$ because in the opposite case we would have $r^2 - r + 1 \in \xi^3 G$ and $\xi^3 G \ni r^2 - r + 1 = (r^2 + 1) - r \in G - G$, absurd.

γ) Let $r + 1 \in G$, then $r^2 - 1 \in \xi G$ and for $r^2 + 1$ we have

i) $r^2 + 1 \notin \xi^3 G$ since $r^2 + 1 \in G - G$;

ii) $r^2 + 1 \notin \xi^2 G$ because if it did belong to $\xi^2 G$ we would have $r^4 - 1 = (r^2 - 1)(r^2 + 1) \in \xi^3 G$ absurd;

iii) $r^2 + 1 \notin \xi G$ because in the opposite case we would have $G \ni r(r + 1) = (r^2 + 1) + (r - 1) \in \xi G - \xi G$, absurd.

Therefore let $r^2 + 1 \in G$; then $r^4 - 1 \in \xi G$ and

i) $r^4 + 1 \neq 0$, since $r^4 + 1 = r^2(r^2 + 1) - (r^2 - 1) \in G - \xi G$;

ii) $r^4 + 1 \notin \xi^3 G$, since $r^4 + 1 \in G - G$;

iii) $r^4 + 1 \notin \xi^2 G$, since $r^8 - 1 \in G - G$;

iv) $r^4 + 1 \notin \xi G$, because otherwise we would have $G \ni r^2(r^2 + 1) = (r^4 + 1) + (r^2 - 1) \in \xi G - \xi G$, absurd. Thus $r^4 + 1 \in G$.

Now, for $r^3 - 1$ we have

i) $r^3 - 1 \notin G$, because otherwise we would have $G \ni r(r^3 - 1) = (r^4 - 1) - (r - 1) \in \xi G - \xi G$, absurd;

ii) $r^3 - 1 \notin \xi^2 G$, because otherwise we would have $\xi^3 G \ni (r^3 - 1)(r - 1) = (r^4 + 1) - r(r^2 + 1) \in G - G$, absurd;

iii) $r^3 - 1 \notin \xi^3 G$, since $r^3 - 1 \in G - G$. Thus $r^3 - 1 \in \xi G$.

Then, for $r^3 + 1$ we have

i) $r^3 + 1 \neq 0$, because $r^3 + 1 = r(r^2 - 1) + (r + 1) \in \xi G - G$;

ii) $r^3 + 1 \notin \xi^3 G$, since $r^3 + 1 \in G - G$;

iii) $r^3 + 1 \notin \xi^2 G$, since $r^6 - 1 \in G - G$;

iv) $r^3+1 \notin \xi G$, because in the opposite case we would have $G \ni r^3(r+1) = (r^4 - 1) + (r^3 + 1) \in \xi G - \xi G$, absurd. Consequently $r^3 + 1 \in G$.

Next we consider the elements $r - 1$, $r^2 - 1$, $r^3 - 1$ which belong to ξG. Then we have

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

Now we will see where do $r^2 - r - 1$ and $r^2 + r - 1$ belong. Thus

i) $r^2 - r - 1 \notin \xi^3 G$, because $r^2 - r - 1 = r^2 - (r + 1) \in G - G$;

ii) $r^2 + r - 1 \notin \xi^3 G$, because $r^2 + r - 1 = r(r + 1) - 1 \in G - G$;

iii) $r^2-r-1 \notin \xi G$, because otherwise we would have $G \ni -1 = (r^2-r-1) - r(r - 1) \in \xi G - \xi G$, absurd;

iv) $r^2+r-1 \notin \xi G$, because if it did belong to ξG we would have $G \ni r^2 = (r^2 + r - 1) - (r - 1) \in \xi G - \xi G$, absurd.

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

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

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

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

in which case $\xi G \ni r^3 - 1 = (r^3 - 2r - 1) + 2r \in \xi^2 G - \xi^2 G$, which is absurd. Therefore $r^2 - r - 1 \in G$.

Now let $r^2 + r - 1 \in \xi^2 G$; then $(r^2 + r - 1)(r + 1) \in \xi^2 G \Rightarrow r^3 + 2r^2 - 1 \in \xi^2 G$. This implies that $\xi G \ni r^3 - 1 = (r^3 + 2r^2 - 1) - 2r^2 \in \xi^2 G - \xi^2 G$, which is absurd. Consequently $r^2 + r - 1 \in G$; then $\xi^3 G \ni r^4(r^2 - r - 1) + (r^2 + r - 1) \in G - G$, which again is absurd and thus the Proposition.

The following Proposition can be proved in a similar way.

P r o p o s i t i o n 2.6. *If* $G \cup \xi^2 G \cup \xi^3 G \cup \{0\} \subseteq G - G$ *and* card $G > 11$, *then* $F = G - G$.

Having proved all the above, we have given the proof of the

T h e o r e m 2.2. *If G is a subgroup of the finite field's F multiplicative group, which has index* 4, *with* $-1 \in G$ *and* card $G > 11$, *then*

$$G - G = F.$$

Example 2.2. α) $\mathbf{Z}_{41}$ is the finite field which has multiplicative subgroup of index 4, which contains -1 but has 10 elements. More precisely $G = \{1, 40, 4, 31, 10, 37, 16, 18, 23, 25\}$. For this subgroup $G - G \neq \mathbf{Z}_{41}$.

β) From the finite fields, $\mathbf{GF}[7^2]$ is the one with the smallest cardinality which has multiplicative subgroup of index 4 that contains -1 and that has more than 11 elements. More precisely $G = \{1, 2, 3, 4, 5, 6, \chi, 2\chi, 3\chi, 4\chi, 5\chi, 6\chi\}$. For this subgroup holds $G - G = \mathbf{GF}[7^2]$.

3. Finite Fields with Subgroup of their Multiplicative Group which has Index 5

The solution of the problem, when the subgroup is of index 5 is being reached through a similar procedure with the one that has analytically been presented in the previous paragraph. It does also involve though the case that the field is of characteristic 2, which does not appear when the subgroup is of index 4. So we first prove the following Proposition and then we have the Theorem 3.1.

P r o p o s i t i o n 3.1. *If the characteristic of F is* 2 *and if G is a multiplicative subgroup of index* 5 *which has* card $G > 8$, *then* $F = G - G$.

P r o o f. Since G is of index 5 we have that

$$F = G \cup \xi G \cup \xi^2 G \cup \xi^3 G \cup \xi^4 G \cup \{0\}.$$

Initially we observe that $G \cup \{0\}$ is not a subfield of F. Indeed, let $G \cup \{0\}$ be a subfield of F. If card $F = 2^\kappa$, then card $(G \cup \{0\}) = 2^\lambda$, or card $G = 2^\lambda - 1$, with $\lambda < \kappa$. But

$$\text{card } F = 5 \text{ card } G + 1,$$

thus $2^\kappa = 5(2^\lambda - 1) \Leftrightarrow 4 = 2^\lambda(5 - 2^{\kappa-\lambda})$, from where $\kappa = 4$ and $\lambda = 2$, which contradicts the suppositions regarding the cardinality of G. Therefore $G+G$ contains at least one class of the type $\xi^i G$, $i = 1, 2, 3, 4$. But if $\xi^i G \cap (G + G) \neq \emptyset$, then

$$\xi G \cup \xi^2 G \cup \xi^3 G \cup \xi^4 G \cup \{0\} \subseteq G - G.$$

Indeed,

i) if $r + 1 \in \xi G$, then $r^2 + 1 \in \xi^2 G$, $r^4 + 1 \in \xi^4 G$, $r^8 + 1 \in \xi^3 G$;

ii) if $r + 1 \in \xi^2 G$, then $r^2 + 1 \in \xi^4 G$, $r^4 + 1 \in \xi^3 G$, $r^8 + 1 \in \xi G$;

iii) if $r+1 \in \xi^3 G$, then $r^2+1 \in \xi G$, $r^4+1 \in \xi^2 G$, $r^8+1 \in \xi^4 G$;

iv) if $r+1 \in \xi^4 G$, then $r^2+1 \in \xi^3 G$, $r^4+1 \in \xi G$, $r^8+1 \in \xi^2 G$.

Next, let's consider the set $G+1$ and let κ of its elements belong to ξG. But if $\xi\gamma_1 = \gamma_2+1$, then $\xi^2\gamma_1^2 = \gamma_2^2+1$, and since the elements γ^2+1, $\gamma \in G$ are different to each other, it derives that in the set $G+1$ belong at least κ from the elements of $\xi^2 G$. So let $\operatorname{card}[(G+1)\cap\xi^2 G] = \kappa+\lambda$. Similarly $\operatorname{card}[(G+1)\cap\xi^4 G] = \kappa+\lambda+\nu$ and next $\operatorname{card}[(G+1)\cap\xi^3 G] = \kappa+\lambda+\nu+\mu$. But if $\xi^3\gamma_3 = \gamma_4+1$, then $\xi\gamma_3 = \gamma_4^2+1$. Consequently $\kappa+\lambda+\nu+\mu = \kappa$, so $\lambda+\nu+\mu = 0$ and therefore each one of the four classes $\xi^i G$, $i = 1,2,3,4$ contains exactly the same number of elements from the set $G+1$. Let this number be κ. If we assume that $G+1$ does not contain elements from G, then

$$\operatorname{card}(G+1) = 4\kappa+1 \Leftrightarrow \operatorname{card} G = 4\kappa+1 \Leftrightarrow \operatorname{card} F = 5(4\kappa+1)+1$$

and if $\operatorname{card} F = 2^\lambda$, then $2^\lambda = 20\kappa+6 \Leftrightarrow 2^{\lambda-1} = 2(5\kappa+1)+1$, which is absurd, and so the Proposition.

T h e o r e m 3.1. *If G is a subgroup of a finite field's F multiplicative group, having index 5 and if* $\operatorname{card} G > 23$, *then*

$$G - G = F.$$

Example 3.1. α) $\mathbf{Z}_{101}$ is the finite field that has multiplicative subgroup of index 5, which contains 20 elements. More precisely

$$G = \{1, 6, 10, 14, 17, 32, 36, 39, 41, 44, 57, 60, 62, 65, 69, 84, 87, 91, 95, 100\}.$$

For this subgroup we have $G - G \neq \mathbf{Z}_{101}$.

β) From the finite fields, $\mathbf{GF}[11^2]$ is the one with the smallest cardinality which has multiplicative subgroup of index 5 that has more than 23 elements. More precisely

$$G = \{1,\ 10,\ \chi,\ 3+\chi,\ 8+\chi,\ 1+3\chi,\ 5+3\chi,$$

$$6+3\chi,\ 10+3\chi,\ 4+4\chi,\ 7+4\chi,\ 3+5\chi,\ 8+5\chi,$$

$$3+6\chi,\ 8+6\chi,\ 4+7\chi,\ 7+7\chi,\ 1+8\chi,\ 5+8\chi,$$

$$6+8\chi,\ 10+8\chi,\ 10\chi,\ 3+10\chi,\ 8+10\chi\}.$$

For this subgroup holds $G - G = \mathbf{GF}[11^2]$.

Received October 15, 1999

University of Athens,
Athens, Greece

REFERENCES

1. K r a s n e r M., *Approximation des corps values complets de caracteristique $p \neq 0$ par ceux de caractéristique* 0. Colloque d'Algèbre Supérieure – Bruxelles, Décembre 1956; CBRM, Bruxelles, 1957.
2. K r a s n e r M., *A Class of Hyperrings and Hyperfields.* Internat. J. Math. and Math. Sci., **6**, *2*, 307-312 (1983).
3. M a s s o u r o s C. G., *Algebraic Structures with Hypercomposition.* Doctoral Thesis. submitted in Patras University, Greece, 1984.
4. M a s s o u r o s C. G., *Methods of Constructing Hyperfields.* Internat. J. Math. & Math. Sci., **8**, *4*, 725-728 (1985).
5. M a s s o u r o s C. G., *On the Theory of Hyperrings and Hyperfields.* Algebra i Logika, **24**, *6*, 728-742 (1985).
6. M a s s o u r o s C. G., *Constructions of Hyperfields.* Mathematica Balkanica, **5**, *3*, 250-257 (1991).
7. M a s s o u r o s C. G., *A Class of Hyperfields and a Problem in the Theory of Fields.* Mathematica Montisnigri, Vol. **1**, pp. 73-84, 1993.
8. N a k a s s i s A., *Recent Results in Hyperring and Hyperfield Theory.* Internat. J. Math. & Math. Sci., **11**, *2*, 209-220 (1988).

DETERMINAREA UNEI HIPERSTRUCTURI PRIN DIFERENŢA SUBGRUPURILOR SALE MULTIPLICATIVE

(Rezumat)

Se rezolvă o problemă deschisă în prezent privind hiperstructurile finite ce pot fi scrise ca diferenţe de subgrupuri ale grupului lor multiplicativ, în cazul subgrupurilor de indice 4 şi 5.