





A note on the conjecture of the autotopism group of the Figueroa's presemifields

Una nota sobre la conjetura del grupo de autotopismos de los presemicuerpos de Figueroa

Walter Meléndez F.  and Moisés Delgado O. 

Received, Oct. 19, 2020

Accepted, Dec. 11, 2020



How to cite this article:

Meléndez FW, Delgado OM. A note on the conjecture of the autotopism group of the Figueroa's presemifields. *Selecciones Matemáticas*. 2020;7(2):267–275. <http://dx.doi.org/10.17268/sel.mat.2020.02.09>

Abstract

In [4] was stated the following conjecture: If a Figueroa's presemifield $P(K, \alpha, \beta, A, B)$ admits an autotopism of order a p -primitive prime divisor of $p^n - 1$, then its autotopism group is isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$. In [5] this conjecture was settled under an additional normality condition. In this article, we show that the assumption in the hypothesis of the conjecture is necessary in the sense that there exist a Figueroa's presemifield, that does not admit such autotopism, for which the conjecture is not met.

Keywords . finite presemifield, finite semifield, autotopism group, Cordero-Figueroa semifield, Figueroa's presemifield.

Resumen

En [4] se estableció la siguiente conjetura: Si un presemicuerpo de Figueroa $P(K, \alpha, \beta, A, B)$ admite un autotopismo de orden un divisor primo p -primitivo de $p^n - 1$, entonces su grupo autotopismo es isomorfo a un subgrupo de $\Gamma L(K) \times \Gamma L(K)$. En [5] esta conjetura se resolvió bajo una condición adicional de normalidad. En este artículo, mostramos que la suposición hecha en la hipótesis de la conjetura es necesaria en el sentido de que existe un presemicuerpo de Figueroa, que no admite tal autotopismo, para el cual la conjetura no se cumple.

Palabras clave. presemicuerpo finito, semicuerpo finito, grupo autotopismo, semicuerpo de Cordero-Figueroa, presemicuerpo de Figueroa.

1. Introduction.

Definition 1.1. A finite presemifield $(P, +, *)$ consists of an additive group $(P, +)$ and a multiplication $*$ that satisfies both distributive laws and the condition: if $x * y = 0$ then $x = 0$ or $y = 0$. A finite presemifield with multiplicative identity is called finite semifield.

Throughout this article, the term presemifield (or semifield) will always be used to refer a finite presemifield (or a finite semifield).

Definition 1.2. Two presemifields (or semifields) $(P, +, *)$ and $(P', +, \circ)$ are isotopic if there exist a triple (F, G, H) of bijective functions from P to P' which are additives and satisfy $G(x*y) = F(x) \circ H(y)$, for all $x, y \in P$. The triple (F, G, H) is called an isotopism from P to P' .

An isotopism from a presemifield (or semifield) P to itself is called an *autotopism* of P , and the set of all autotopisms of a presemifield (or semifield) P is known as the *autotopism group* of P and will be denoted by $\mathcal{A}(P)$. For more details of our concern about semifields, presemifields, autotopisms, and the autotopism group $\mathcal{A}(P)$, see [4] and [5].

*Facultad de Ciencias Físicas y Matemáticas, Universidad Nacional de Trujillo, Avenida Juan Pablo II s/n, Trujillo, Perú (wmelendez@unitru.edu.pe).

†Mathematics and Physics Department, University of Puerto Rico, Cayey Campus, 205 Calle Antonio R. Barceló, Cayey, Puerto Rico (moises.delgado@upr.edu).

In this paper, we will focus our attention on the conjecture stated in [5] about the autotopism group of the Figueroa’s presemifield of order p^n . A Figueroa’s presemifield of order p^n is defined in [4] as follows:

Definition 1.3. Let $\alpha \neq 1$ and $\beta \neq 1$, $\alpha \neq \beta$, be automorphisms of $K = GF(p^n)$, where $p \geq 3$ and $n \geq 4$, and let $A, B \in K^*$ be constants. $(K, +, *)$ is a Figueroa’s presemifield of order p^n with the product:

$$x * y = xy + Ax^\alpha y^\beta + Bx^\beta y^\alpha,$$

if α, β, A , and B are such that $x * y = 0$ implies $x = 0$ or $y = 0$. This presemifield is denoted by $P(K, \alpha, \beta, A, B)$.

In [4] we studied the autotopism group of the Cordero-Figueroa semifield of order 3^6 and we showed that its autotopism group is isomorphic to a particular subgroup of $\Gamma L(K) \times \Gamma L(K)$. There in, because of additional evidence, we also suggested that the same fact should be fulfilled for the general case (i.e. for a Figueroa’s presemifield of order p^n). Thus, in [5], we formally conjecture:

Conjecture 1 (Figueroa’s conjecture). If a Figueroa’s presemifield $P(K, \alpha, \beta, A, B)$ of order p^n admits an autotopism of order a p -primitive prime divisor, then its autotopism group is isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$.

In [5], this conjecture was proved as true under the additional condition that the subgroup generated by the autotopism $(f_0x, f_0^2y, f_0n) \in \mathcal{A}(P)$, of an appropriate order, be a normal subgroup in $\mathcal{A}(P)$.

The goal in this article is to show that the hypothesis of the Figueroa’s conjecture is necessary in the sense that there exist an example where the hypothesis is not satisfied and the conjecture for this example is not met.

2. Resolved cases. In this section, we review the main results obtained in [4] and [5] that contribute to the proof of the stated conjecture.

2.1. The autotopism group of the Cordero-Figueroa semifield of order 3^6 . In [4], we determine that the full autotopism group of the Cordero-Figueroa semifield of order 3^6 is isomorphic to a particular subgroup of $\Gamma L(K) \times \Gamma L(K)$, where $K = GF(3^6)$. To be more specific:

Theorem 2.1. Let $P = P(K, \alpha, \beta, A, B)$ be the Cordero-Figueroa semifield of order 3^6 . The full autotopism group $\mathcal{A}(P)$ is isomorphic to the subgroup of $\Gamma L(K) \times \Gamma L(K)$:

$$\langle (\gamma^{13}x, \gamma^{26}y) \rangle \times \langle (\gamma x^3, \gamma y^3) \rangle,$$

where $\langle (\gamma^{13}x, \gamma^{26}y) \rangle$ is normal in the group $\langle (\gamma^{13}x, \gamma^{26}y) \rangle \langle (\gamma x^3, \gamma y^3) \rangle$. Furthermore, the order of $\mathcal{A}(P)$ is 672.

Since the Cordero-Figueroa semifield of order 3^6 is a semifield that admits an autotopism of order a 3–primitive prime divisor of $3^6 - 1$, it is a presemifield (see [1]), or more properly speaking, it is a Figueroa’s presemifield of order 3^6 .

2.2. The autotopism group of the Figueroa’s presemifield of order p^n . In [5], in order to prove the Figueroa’s conjecture, we provided a characterization for a Figueroa’s presemifield of order p^n to admit a certain autotopism of order a p -primitive prime divisor of $p^n - 1$, as follows:

Theorem 2.2. Let $P = P(K, \alpha, \beta, A, B)$ be a Figueroa’s presemifield of order p^n . Assume that $p^n - 1$ has a p -primitive prime divisor s and $\alpha^3 \neq 1$ if $\alpha\beta = 1$. Then $\mathcal{A}(P)$ admits the autotopism (f_0x, f_0^2y, f_0n) of order s , with $f_0 \in K^*$, if and only if s divides $(\beta - 1) + (\alpha - 1)$.

This characterization allowed us to demonstrate the Figueroa’s conjecture in Theorem 2.3, under the assumption that the subgroup generated by the autotopism $(f_0x, f_0^2y, f_0n) \in \mathcal{A}(P)$ is a normal subgroup in $\mathcal{A}(P)$.

Theorem 2.3. Let $P = P(K, \alpha, \beta, A, B)$ be a Figueroa’s presemifield of order p^n . Assume that $\mathcal{A}(P)$ admits the autotopism of order s (as referred in Theorem 2.2). If the subgroup generated by this autotopism is normal in $\mathcal{A}(P)$, then

$$\mathcal{A}(P) = \{(ux^\phi, uv y^\phi, vn^\phi) : u, v \in K^*, \phi \in \text{Aut}(K)\},$$

and hence, it is isomorphic to a subgroup of $\Gamma L(K) \times \Gamma L(K)$.

3. On the sufficient condition of the Figueroa’s conjecture. As mentioned at the end of section 1, in this section we provide a Figueroa presemifield of order 3^4 and find its autotopism group. We show that the assumption on the existence of an autotopism of order a p -primitive prime divisor of $p^n - 1$, in the hypothesis of Figueroa’s conjecture, is required.

Theorem 3.1. Let $K = GF(3^4)$ and consider $\alpha = 3^1, \beta = 3^3, A = \gamma^0 = 1$ and $B = \gamma^{13}$, with $\gamma \in K$ a primitive element such that $\gamma^4 = 1 + \gamma$. Let $P = P(K, \alpha, \beta, A, B)$ be the Figueroa’s presemifield defined by the product

$$x \circ y = xy + Ax^{3^1}y^{3^3} + Bx^{3^3}y^{3^1},$$

for all $x, y \in K$. Then, P does not admit an autotopism of order a 3-primitive prime divisor of $3^4 - 1$ and $\mathcal{A}(P)$ is not isomorphic to any subgroup of $\Gamma L(K) \times \Gamma L(K)$.

Proof: Let $(f, g, h) \in \mathcal{A}(P)$ be any element. Since f, g and h are additive functions,

$$f(x) = \sum_{k=0}^3 f_k x^{3^k}, \quad g(y) = \sum_{k=0}^3 g_k y^{3^k}, \quad h(n) = \sum_{k=0}^3 h_k n^{3^k}.$$

Let $m = h(n)$. Then, the condition $g(x \circ n) = f(x) \circ m$ yields the following equations:

$$(3.1) \quad g_0 n + (g_3 + g_1 B^3)n^{3^2} = f_0 m + f_3^{3^1} m^{3^3} + B f_1^{3^3} m^{3^1},$$

$$(3.2) \quad g_1 n^{3^1} + (g_0 + g_2 B)n^{3^3} = f_1 m + f_0^{3^1} m^{3^3} + B f_2^{3^3} m^{3^1},$$

$$(3.3) \quad (g_1 + g_3 B^3)n + g_2 n^{3^2} = f_2 m + f_1^{3^1} m^{3^3} + B f_3^{3^3} m^{3^1},$$

$$(3.4) \quad (g_2 + g_0 B)n^{3^1} + g_3 n^{3^3} = f_3 m + f_2^{3^1} m^{3^3} + B f_0^{3^3} m^{3^1}.$$

Since the multiplicative group of the middle nucleus of P :

$$N_m^* = \{(f, g, h) \in \mathcal{A}(P) : f(x) = cx, g(y) = y, h(n) = c^{-1}n\},$$

is normal in $\mathcal{A}(P)$ (see [4]), we have that for all $(f, g, h) \in \mathcal{A}(P)$ and any $(f_0, i, h_0) \in N_m^*$, where i is the identity function from P to P , there exists $(\tilde{f}_0, i, \tilde{h}_0) \in N_m^*$ such that

$$(f, g, h)^{-1} \circ (f_0, i, h_0) \circ (f, g, h) = (\tilde{f}_0, i, \tilde{h}_0).$$

Then, for all $x \in K$,

$$(3.5) \quad f_0(f(x)) = f(\tilde{f}_0(x)).$$

Let $f_0(x) = c_0 x$ and $\tilde{f}_0(x) = \tilde{c}_0 x$. Since $|N_m^*| = 3^{(4 \cdot 3 - 1)} - 1 = 8$, we get that $\tilde{c}_0 \in GF^*(3^2)$ (see Lemma 1 in [4]). Then, from (3.5),

$$(3.6) \quad c_0 f_0 = f_0 \tilde{c}_0,$$

$$(3.7) \quad c_0 f_1 = f_1 \tilde{c}_0^3,$$

$$(3.8) \quad c_0 f_2 = f_2 \tilde{c}_0,$$

$$(3.9) \quad c_0 f_3 = f_3 \tilde{c}_0^3.$$

Since $f(x) \neq 0$, $f(x)$ has at least one nonzero coefficient. Suppose that $f_0 \neq 0$. Then, from (3.6), $c_0 = \tilde{c}_0$. Hence, (3.7) and (3.9) imply that $f_1 = f_3 = 0$. In the same way, if $f_2 \neq 0$ then $f_1 = f_3 = 0$, and if $f_1 \neq 0$ or $f_3 \neq 0$ then $f_0 = f_2 = 0$. Therefore, $f(x)$ has at least one nonzero coefficient and at most two nonzero coefficients (f_0 and f_2 , or f_1 and f_3). We now analyze each case in order to determine the full autotopism group of P .

CASE 1: *Two coefficients of $f(x)$ are nonzero.* For this case, we have the following subcases:

(a) $f_0 \neq 0, f_2 \neq 0, f_1 = 0, f_3 = 0$.

(b) $f_1 \neq 0, f_3 \neq 0, f_2 = 0, f_4 = 0$.

If (a) occurs, then (3.1) - (3.4) imply that

$$(3.10) \quad m = \frac{g_0}{f_0} n + \left(\frac{g_3}{f_0} + \frac{g_1}{f_0} B^3\right) n^9,$$

$$(3.11) \quad f_0^9 m + B^3 f_2 m^9 = (g_0^3 + g_2^3 B^3) n + g_1^3 n^9,$$

$$(3.12) \quad m = \left(\frac{g_1}{f_2} + \frac{g_3}{f_2} B^3\right) n + \frac{g_2}{f_2} n^9,$$

$$(3.13) \quad f_2^9 m + B^3 f_0 m^9 = g_3^3 n + (g_2^3 + g_0^3 B^3) n^9.$$

From (3.10) and (3.12), we get

$$(3.14) \quad \frac{g_0}{f_0} = \frac{g_1}{f_2} + \frac{g_3}{f_2} B^3,$$

$$(3.15) \quad \frac{g_2}{f_2} = \frac{g_3}{f_0} + \frac{g_1}{f_0} B^3.$$

Let $P = \frac{g_2}{f_2}$ and $Q = \frac{g_0}{f_0}$. Then, from equations (3.14) and (3.15) we obtain

$$\begin{aligned} f_2 Q &= g_1 + g_3 B^3, \\ f_0 P &= g_3 + g_1 B^3. \end{aligned}$$

Hence

$$(3.16) \quad g_1 = -(f_0 P + f_2 Q B),$$

$$(3.17) \quad g_3 = -(f_2 Q + f_0 P B).$$

On the other hand, from (3.10) and (3.15) we conclude that

$$m = \frac{g_0}{f_0} n + \frac{g_2}{f_2} n^3,$$

or

$$(3.18) \quad m = Qn + Pn^9.$$

Substituting this into equation (3.11) we obtain

$$f_0^9(Qn + Pn^9) + B^3 f_2(Q^9 n^9 + P^9 n) = (g_0^3 + g_2^3 B^3)n + g_1^3 n^9,$$

which is equivalent to

$$(f_0^9 Q + B^3 f_2 P^9)n + (f_0^9 P + B^3 f_2 Q^9)n^9 = (g_0^3 + g_2^3 B^3)n + g_1^3 n^9,$$

a polynomial identity in n . Therefore

$$(3.19) \quad f_0^9 Q + B^3 f_2 P^9 = g_0^3 + g_2^3 B^3,$$

$$(3.20) \quad f_0^9 P + B^3 f_2 Q^9 = g_1^3.$$

Since $g_0 = f_0 Q$ and $g_2 = f_2 P$, the equations (3.19), (3.20) and (3.16) imply that

$$(3.21) \quad f_0^9 Q + B^3 f_2 P^9 = f_0^3 Q^3 + f_2^3 P^3 B^3,$$

$$(3.22) \quad f_0^9 P + B^3 f_2 Q^9 = -(f_0^3 P^3 + f_2^3 Q^3 B^3).$$

Notice that $B^4 = -1$. Then, multiplying (3.21) and (3.22) by B , and rearranging the resultant equations, we get

$$(3.23) \quad (f_0^9 Q - f_0^3 Q^3)B = f_2 P^9 - f_2^3 P^3,$$

$$(3.24) \quad (f_0^9 P + f_0^3 P^3)B = f_2 Q^9 + f_2^3 Q^3.$$

Similarly, replacing the expression obtained for m (see equation (3.18)) into equation (3.13), we obtain that

$$(3.25) \quad (f_2^9 Q + f_2^3 Q^3)B = f_0 P^9 + f_0^3 P^3,$$

$$(3.26) \quad (f_2^9 P - f_2^3 P^3)B = f_0 Q^9 - f_0^3 Q^3.$$

Now, adding and subtracting side to side (3.23) and (3.24) we find, respectively, that

$$(3.27) \quad f_0^9 B(P + Q) + f_0^3 B(P - Q)^3 = f_2(P + Q)^9 + f_2^3(Q - P)^3,$$

$$(3.28) \quad f_0^9 B(P - Q) + f_0^3 B(P + Q)^3 = f_2(Q - P)^9 + f_2^3(P + Q)^3.$$

Analogously, from (3.25) and (3.26), we get

$$(3.29) \quad f_2^9 B(P + Q) + f_2^3 B(Q - P)^3 = f_0(P + Q)^9 + f_0^3(P - Q)^3,$$

$$(3.30) \quad f_2^9 B(Q - P) + f_2^3 B(P + Q)^3 = f_0(P - Q)^9 + f_0^3(P + Q)^3.$$

Let $R = P + Q$ and $S = P - Q$. Then, from (3.27) - (3.30),

$$\begin{aligned} f_0^9 BR + f_0^3 BS^3 &= f_2 R^9 - f_2^3 S^3, \\ f_0^9 BS + f_0^3 BR^3 &= -f_2 S^9 + f_2^3 R^3, \\ f_2^9 BR - f_2^3 BS^3 &= f_0 R^9 + f_0^3 S^3, \\ -f_2^9 BS + f_2^3 BR^3 &= f_0 S^9 + f_0^3 R^3. \end{aligned}$$

Rearranging terms in each one of these equations, we obtain

$$(3.31) \quad (f_2^3 + f_0^3 B)S^3 = f_2 R^9 - f_0^9 BR,$$

$$(3.32) \quad (f_2^3 - f_0^3 B)R^3 = f_2 S^9 + f_0^9 BS,$$

$$(3.33) \quad (f_0^3 + f_2^3 B)S^3 = f_2^9 BR - f_0 R^9,$$

$$(3.34) \quad (f_2^3 B - f_0^3)R^3 = f_0 S^9 + f_2^9 BS.$$

Multiplying (3.31) by f_0 and (3.33) by f_2 , and adding side to side the resulting equations, we get

$$(3.35) \quad [(f_2^3 + f_0^3 B)f_0 + (f_0^3 + f_2^3 B)f_2]S^3 = (f_2^{10} - f_0^{10})BR.$$

In the same way, multiplying (3.31) by f_2^9 and (3.33) by f_0^9 , and adding side to side the resulting equations, we obtain that

$$(3.36) \quad [(f_2^3 + f_0^3 B)f_2^9 + (f_0^3 + f_2^3 B)f_0^9]S^3 = (f_2^{10} - f_0^{10})R^9.$$

Similarly, with (3.32) and (3.34), we have

$$(3.37) \quad [(f_2^3 - f_0^3 B)f_0 - (f_2^3 B - f_0^3)f_2]R^3 = (f_0^{10} - f_2^{10})BS,$$

$$(3.38) \quad [(f_2^3 - f_0^3 B)f_2^9 - (f_2^3 B - f_0^3)f_0^9]R^3 = (f_2^{10} - f_0^{10})S^9.$$

Rearranging terms in (3.35) - (3.38), we obtain

$$(3.39) \quad [f_0 f_2 (f_2^2 + f_0^2) + (f_0^4 + f_2^4)B]S^3 = (f_2^{10} - f_0^{10})BR,$$

$$(3.40) \quad [(f_2^4 + f_0^4)^3 + f_0^3 f_2^3 (f_2^6 + f_0^6)B]S^3 = (f_2^{10} - f_0^{10})R^9,$$

$$(3.41) \quad [(f_2^4 + f_0^4)B - f_0 f_2 (f_2^2 + f_0^2)]R^3 = (f_2^{10} - f_0^{10})BS,$$

$$(3.42) \quad [(f_2^4 + f_0^4)^3 - f_0^3 f_2^3 (f_2^6 + f_0^6)B]R^3 = (f_2^{10} - f_0^{10})S^9.$$

Let $V = f_0 f_2 (f_2^2 + f_0^2)$, $W = f_0^4 + f_2^4$ and $D = f_2^{10} - f_0^{10}$. We note that, since $f(x)$ is bijective, $f_0^{10} \neq f_2^{10}$. Hence, $D \neq 0$. Furthermore, since $D^9 = f_2^{90} - f_0^{90} = f_2^{10} - f_0^{10} = D$, we get $D^8 = 1$. Replacing the expressions V , W and D in (3.39) - (3.42), we obtain

$$(3.43) \quad (V + WB)S^3 = DBR,$$

$$(3.44) \quad (W^3 + V^3 B)S^3 = DR^9,$$

$$(3.45) \quad (WB - V)R^3 = DBS,$$

$$(3.46) \quad (W^3 - V^3 B)R^3 = DS^9.$$

From (3.43), if $S = 0$ then $R = 0$. Since $R = P + Q$ and $S = P - Q$, we conclude that $P = 0$ and $Q = 0$. Therefore, equation (3.18) implies that $m = 0$, which is a contradiction. Analogously, from (3.45), if $R = 0$ then $S = 0$. Therefore, $m = 0$. Hence $R \neq 0$ and $S \neq 0$.

Solving (3.43) for R and replacing it in (3.44) - (3.46), we obtain the following equations

$$(3.47) \quad B(W^3 + V^3 B) = (V^9 + W^9 B)S^{24},$$

$$(3.48) \quad (WB - V)(V^3 + W^3 B^3)S^8 = -D^4,$$

$$(3.49) \quad (W^3 - V^3 B)(V^3 + W^3 B^3) = D^4 B^3.$$

Multiplying the equation (3.49) by B , we get

$$(3.50) \quad (W^3 - V^3 B)^2 = D^4.$$

Hence

$$(3.51) \quad W^3 - V^3 B = \epsilon D^2, \quad (\epsilon = \pm 1).$$

On the other hand, multiplying the equation (3.48) by B and using (3.51), we get

$$(WB - V)\epsilon S^8 = D^2 B.$$

Hence

$$(W^3 B^3 - V^3)\epsilon S^{24} = D^6 B^3.$$

Multiplying this equation by B , we get

$$(3.52) \quad (W^3 + V^3B)\epsilon S^{24} = D^6.$$

Solving the equation (3.52) for S^{24} and replacing into equation (3.47), we get

$$B(W^3 + V^3B)^2 = \epsilon(V^9 + W^9B)D^6.$$

Multiplying each side of this equation by B^3 , we get

$$(3.53) \quad -(W^3 + V^3B)^2 = \epsilon(V^3B - W^3)^3D^6.$$

From (3.51) and (3.53)

$$(3.54) \quad (W^3 + V^3B)^2 = D^4.$$

Thus (3.50) and (3.54) imply that

$$(W^3 + V^3B)^2 = (W^3 - V^3B)^2.$$

Then $W = 0$ or $V = 0$. Suppose that $W = 0$. Then (3.54) imply that $V^6B^2 = D^4$. So,

$$(3.55) \quad V^{12}B^4 = D^8.$$

Since $B^4 = -1$ and $D^8 = 1$, from (3.55), we have that $V^{12} = -1$, which implies that $V^4 = -1$. Remember that $W = f_0^4 + f_2^4$ and $V = f_0f_2(f_2^2 + f_0^2)$. Since $W = 0$, we have that $f_2^4 + f_0^4 = 0$. From where, $f_2^4 = -f_0^4$. Thus

$$V^2 = f_0^2f_2^2(f_2^2 + f_0^2)^2 = 2f_0^4f_2^4 = -f_0^4(-f_0^4) = f_0^8.$$

Then

$$(3.56) \quad f_0^{16} = V^4 = -1.$$

Note that (3.56) implies that $f_0^{32} = 1$. Then $f_0^{96} = 1$. Since $f_0^{80} = 1$, we get

$$f_0^{16} = 1,$$

which contradicts (3.56). Hence $W \neq 0$ and $V = 0$. Since $V = 0$, (3.50) implies

$$(3.57) \quad W^6 = D^4.$$

Then, $W^{12} = D^8 = 1$. So, $W^4 = 1$. Thus (3.57) implies $W^2 = D^4$. Therefore

$$(3.58) \quad W = \tilde{\epsilon}D^2, \quad (\tilde{\epsilon} = \pm 1).$$

Now, equations (3.51) and (3.58) imply that $W^3 = W$ or $W^3 = -W$. Thus, since $W \neq 0$, we conclude that $W^2 = 1$ or $W^2 = -1$.

Assume first that $W^2 = 1$. Since $V = 0$,

$$(3.59) \quad f_0^2 + f_2^2 = 0.$$

Then $f_2^4 = f_0^4$. Therefore

$$W = f_0^4 + f_2^4 = 2f_0^4 = -f_0^4.$$

Hence, $W^2 = f_0^8$. Thus

$$(3.60) \quad f_0^8 = 1.$$

Solving the equation (3.59) for f_2 give us

$$(3.61) \quad f_2 = jf_0,$$

where $j \in K^*$ is such that $j^2 = -1$ (then $j = \pm B^2$). Replacing f_2 in (3.23) - (3.26), we get

$$(3.62) \quad (f_0^9 Q - f_0^3 Q^3)B = j f_0 P^9 + j f_0^3 P^3,$$

$$(3.63) \quad (f_0^9 P + f_0^3 P^3)B = j f_0 Q^9 - j f_0^3 Q^3,$$

$$(3.64) \quad (j f_0^9 Q - j f_0^3 Q^3)B = f_0 P^9 + f_0^3 P^3,$$

$$(3.65) \quad (j f_0^9 P + j f_0^3 P^3)B = f_0 Q^9 - f_0^3 Q^3.$$

Multiplying the equation (3.63) by j , and using (3.65), we get

$$j f_0^9 P + j f_0^3 P^3 = -(j f_0^9 P + j f_0^3 P^3).$$

Then

$$(3.66) \quad P^2 = -f_0^6.$$

Then, since $f_0^8 = 1$, from (3.66), we get that $P^6 = -f_0^{18} = -f_0^2$. Therefore,

$$f_0 P^9 + f_0^3 P^3 = f_0 P^6 P^3 + f_0^3 P^3 = f_0 (-f_0^2) P^3 + f_0^3 P^3 = -f_0^3 P^3 + f_0^3 P^3 = 0.$$

Thus, the right hand side of (3.64) is 0. Then, since $B \neq 0$, from (3.64), we get that $j f_0^9 Q - j f_0^3 Q^3 = 0$. Hence

$$(3.67) \quad Q^2 = f_0^6.$$

Since $f_2 = j f_0$, we get $P = \frac{g_2}{f_2} = \frac{g_2}{j f_0}$. Replacing $f_2 = j f_0$, $P = \frac{g_2}{j f_0}$ and $Q = \frac{g_0}{f_0}$ in (3.16) and (3.17), we have

$$(3.68) \quad -g_1 = \frac{g_2}{j} + j B g_0,$$

$$(3.69) \quad -g_3 = j g_0 + B \frac{g_2}{j}.$$

Next, let us find the form of the autotopisms (f, g, h) of the presemifield P for this case:

FORM 1. Solving (3.60) for f_0 we obtain $f_0 = B^k$, for $k \in \mathbb{N}$, $0 \leq k \leq 7$. Since $g_0 = f_0 Q$, we get $g_0^2 = f_0^2 Q^2$. Then, using (3.67), we find $g_0^2 = f_0^2 f_0^6 = f_0^8 = 1$. Therefore, $g_0 = \pm 1$.

Similarly, since $g_2 = f_2 P$, we get that $g_2^2 = f_2^2 P^2$. Then, since $f_2 = j f_0$ (where $j^2 = -1$), using (3.66), we find that $g_2^2 = j^2 f_0^2 (-f_0^6) = f_0^8 = 1$. Therefore, $g_2 = \pm 1$.

(i) Assume that $g_0 = 1$ and $g_2 = 1$. If $j = B^2$, then from equation (3.68),

$$g_1 = -\left(\frac{1}{B^2} + B^3\right) = B^2 - B^3 = -1.$$

Similarly, from equation (3.69),

$$g_3 = -\left(B^2 + B \frac{1}{B^2}\right) = -B^2 + B^3 = 1.$$

So, we get autotopisms (f, g, h) where

$$\begin{aligned} f(x) &= B^k x + B^{k+2} x^9, \\ g(y) &= y - y^3 + y^9 + y^{27}, \\ h(n) &= B^{-k} n + B^{-k-2} n^9, \end{aligned}$$

for $0 \leq k \leq 7$.

In the same way, if $j = -B^2$ then $g_1 = 1$ and $g_3 = -1$. So, we get autotopisms (f, g, h) where

$$\begin{aligned} f(x) &= B^k x - B^{k+2} x^9, \\ g(y) &= y + y^3 + y^9 - y^{27}, \\ h(n) &= B^{-k} n - B^{-k-2} n^9, \end{aligned}$$

for $0 \leq k \leq 7$.

(ii) If $g_0 = 1$ and $g_2 = -1$, in a similar way to (i), we get autotopisms (f, g, h) where, for $0 \leq k \leq 7$,

$$\begin{aligned} f(x) &= B^k x + B^{k+2} x^9 & f(x) &= B^k x - B^{k+2} x^9, \\ g(y) &= y + y^3 - y^9 - y^{27} & \text{and} & & g(y) &= y - y^3 - y^9 - y^{27}, \\ h(n) &= B^{-k} n - B^{-k-2} n^9 & & & h(n) &= B^{-k} n + B^{-k-2} n^9. \end{aligned}$$

(iii) If $g_0 = -1$ and $g_2 = 1$, we get autotopisms (f, g, h) where, for $0 \leq k \leq 7$,

$$\begin{aligned} f(x) &= B^k x + B^{k+2} x^9 & f(x) &= B^k x - B^{k+2} x^9, \\ g(y) &= -y - y^3 + y^9 - y^{27} & \text{and} & & g(y) &= -y - y^3 + y^9 + y^{27}, \\ h(n) &= -B^{-k} n + B^{-k-2} n^9 & & & h(n) &= -B^{-k} n - B^{-k-2} n^9. \end{aligned}$$

(iv) If $g_0 = -1$ and $g_2 = -1$, we get autotopisms (f, g, h) where, for $0 \leq k \leq 7$,

$$\begin{aligned} f(x) &= B^k x + B^{k+2} x^9 & f(x) &= B^k x - B^{k+2} x^9, \\ g(y) &= -y + y^3 - y^9 - y^{27} & \text{and} & & g(y) &= -y - y^3 - y^9 + y^{27}, \\ h(n) &= -B^{-k} n - B^{-k-2} n^9 & & & h(n) &= -B^{-k} n + B^{-k-2} n^9. \end{aligned}$$

FORM 2. Assume that $W^2 = -1$. As when $W^2 = 1$ (see page 272), we get autotopisms (f, g, h) where, for $0 \leq k \leq 7$,

(i)

$$\begin{aligned} f(x) &= \gamma^5 B^k x + \gamma^5 B^{k+2} x^9 & f(x) &= \gamma^5 B^k x - \gamma^5 B^{k+2} x^9, \\ g(y) &= B^2 y - B^2 y^3 + B^2 y^9 + B^2 y^{27} & \text{and} & & g(y) &= B^2 y + B^2 y^3 + B^2 y^9 - B^2 y^{27}, \\ h(n) &= \gamma^{-5} B^{2-k} n + \gamma^{-5} B^{-k} n^9 & & & h(n) &= \gamma^{-5} B^{2-k} n - \gamma^{-5} B^{-k} n^9. \end{aligned}$$

(ii)

$$\begin{aligned} f(x) &= \gamma^5 B^k x + \gamma^5 B^{k+2} x^9 & f(x) &= \gamma^5 B^k x - \gamma^5 B^{k+2} x^9, \\ g(y) &= B^2 y - B^3 y^3 - B^2 y^9 - B^3 y^{27} & \text{and} & & g(y) &= B^2 y + B^3 y^3 - B^2 y^9 + B^3 y^{27}, \\ h(n) &= \gamma^{-5} B^{2-k} n - \gamma^{-5} B^{-k} n^9 & & & h(n) &= \gamma^{-5} B^{2-k} n + \gamma^{-5} B^{-k} n^9. \end{aligned}$$

(iii)

$$\begin{aligned} f(x) &= \gamma^5 B^k x + \gamma^5 B^{k+2} x^9 & f(x) &= \gamma^5 B^k x - \gamma^5 B^{k+2} x^9, \\ g(y) &= -B^2 y + B^3 y^3 - B^2 y^9 + B^3 y^{27} & \text{and} & & g(y) &= -B^2 y - B^3 y^3 + B^2 y^9 - B^3 y^{27}, \\ h(n) &= -\gamma^{-5} B^{2-k} n + \gamma^{-5} B^{-k} n^9 & & & h(n) &= -\gamma^{-5} B^{2-k} n - \gamma^{-5} B^{-k} n^9. \end{aligned}$$

(iv)

$$\begin{aligned} f(x) &= \gamma^5 B^k x + \gamma^5 B^{k+2} x^9 & f(x) &= \gamma^5 B^k x - \gamma^5 B^{k+2} x^9, \\ g(y) &= -B^2 y + B^2 y^3 - B^2 y^9 - B^2 y^{27} & \text{and} & & g(y) &= -B^2 y - B^2 y^3 - B^2 y^9 + B^2 y^{27}, \\ h(n) &= -\gamma^{-5} B^{2-k} n - \gamma^{-5} B^{-k} n^9 & & & h(n) &= -\gamma^{-5} B^{2-k} n + \gamma^{-5} B^{-k} n^9. \end{aligned}$$

FORM 3. If the subcase (b) of Case 1 occurs (see page 269), proceeding as in the subcase (a), we get autotopisms (f, g, h) where, for $0 \leq k, r \leq 7$,

(i)

$$\begin{aligned} f(x) &= B^k x^3 + B^{k+1} x^{27}, \\ g(y) &= -(\gamma^5 B^{k+1} + \gamma^5 B^{r+2})y + \gamma^5 B^k y^3 + (\gamma^5 B^k + \gamma^5 B^{r+3})y^9 + \gamma^5 B^r y^{27}, \\ h(n) &= \gamma^5 n^3 + \gamma^5 B^{r-k-1} n^{27}. \end{aligned}$$

(ii)

$$\begin{aligned} f(x) &= B^k x^3 - B^{k+1} x^{27}, \\ g(y) &= (\gamma^5 B^{k+1} + \gamma^5 B^{r+2})y + \gamma^5 B^k y^3 - (\gamma^5 B^k + \gamma^5 B^{r+3})y^9 + \gamma^5 B^r y^{27}, \\ h(n) &= \gamma^5 n^3 - \gamma^5 B^{r-k-1} n^{27}. \end{aligned}$$

(iii)

$$\begin{aligned} f(x) &= B^k x^3 + B^{k+3} x^{27}, \\ g(y) &= -(\gamma^5 B^{k+3} + \gamma^5 B^r)y + \gamma^5 B^k y^3 + (\gamma^5 B^{k+2} + \gamma^5 B^{r+1})y^9 + \gamma^5 B^r y^{27}, \\ h(n) &= \gamma^5 n^3 + \gamma^5 B^{r-k-3} n^{27}. \end{aligned}$$

(iv)

$$\begin{aligned} f(x) &= B^k x^3 - B^{k+3} x^{27}, \\ g(y) &= (\gamma^5 B^{k+3} + \gamma^5 B^r) y + \gamma^5 B^k y^3 - (\gamma^5 B^{k+2} + \gamma^5 B^{r+1}) y^9 + \gamma^5 B^r y^{27}, \\ h(n) &= \gamma^5 n^3 - \gamma^5 B^{r-k-3} n^{27}. \end{aligned}$$

CASE 2: *One coefficient of $f(x)$ is nonzero.* In this case, we get autotopisms (f, g, h) where, for $0 \leq k \leq 7$,

(i)

$$\begin{array}{cccc} f(x) = B^k x & f(x) = B^k x & f(x) = B^k x & f(x) = B^k x, \\ g(y) = y & g(y) = -y & g(y) = B^2 y & g(y) = -B^2 y, \\ h(n) = B^{-k} n & h(n) = -B^{-k} n & h(n) = B^{2-k} n & h(n) = -B^{2-k} n. \end{array}$$

(ii)

$$\begin{array}{cccc} f(x) = \gamma^5 B^k x & f(x) = \gamma^5 B^k x & f(x) = \gamma^5 B^k x & f(x) = \gamma^5 B^k x, \\ g(y) = y & g(y) = -y & g(y) = B^2 y & g(y) = -B^2 y, \\ h(n) = \gamma^{-5} B^{-k} n & h(n) = -\gamma^{-5} B^{-k} n & h(n) = \gamma^{-5} B^{2-k} n & h(n) = -\gamma^{-5} B^{2-k} n. \end{array}$$

(iii)

$$\begin{array}{cccc} f(x) = B^k x^9 & f(x) = B^k x^9 & f(x) = B^k x^9 & f(x) = B^k x^9, \\ g(y) = y^9 & g(y) = -y^9 & g(y) = B^2 y^9 & g(y) = -B^2 y^9, \\ h(n) = B^{-k} n^9 & h(n) = -B^{-k} n^9 & h(n) = B^{2-k} n^9 & h(n) = -B^{2-k} n^9. \end{array}$$

(iv)

$$\begin{array}{cccc} f(x) = \gamma^5 B^k x^9 & f(x) = \gamma^5 B^k x^9 & f(x) = \gamma^5 B^k x^9 & f(x) = \gamma^5 B^k x^9, \\ g(y) = y^9 & g(y) = -y^9 & g(y) = B^2 y^9 & g(y) = -B^2 y^9, \\ h(n) = \gamma^{-5} B^{-k} n^9 & h(n) = -\gamma^{-5} B^{-k} n^9 & h(n) = \gamma^{-5} B^{2-k} n^9 & h(n) = -\gamma^{-5} B^{2-k} n^9. \end{array}$$

Therefore, there exist only 512 autotopisms from P to P and so the order of $\mathcal{A}(P)$ is 512. Moreover, 5 is the only 3-primitive prime divisor of $3^4 - 1$ and no autotopism in $\mathcal{A}(P)$ has order 5.

Finally, suppose that $\mathcal{A}(P)$ is isomorphic to some subgroup N of $\Gamma L(K) \times \Gamma L(K)$. Let's denote $\mathcal{A}_f(P)$, $\mathcal{A}_g(P)$ and $\mathcal{A}_h(P)$ the groups containing the first, second and third components of $\mathcal{A}(P)$. Let's denote N_F and N_G the groups containing the first and second components of N . Then N_F and N_G are subgroups of $\Gamma L(K)$, and the linear parts of N_F and N_G are normal subgroups in $\Gamma L(K)$ (see Result 1.21 in [3]), then the linear parts of $\mathcal{A}_f(P)$, $\mathcal{A}_g(P)$ and $\mathcal{A}_h(P)$ are normal subgroups as well, which is a contradiction (see autotopisms in the Case 2, item (i) and item (ii)). Hence, $\mathcal{A}(P)$ is not isomorphic to any subgroup of $\Gamma L(K) \times \Gamma L(K)$.

4. Conclusions. Since the order of the autotopism group of the Figueroa's presemifield of order 81 give in the Theorem 3.1 is 512, we conclude that it is isomorphic to the autotopism group of the semifield plane $\mathbf{P}(\Sigma)$, where Σ belong to the Knuth class VIII (see [2]).

ORCID and License

Walter Meléndez F. <http://orcid.org/0000-0002-6253-0205>

Moisés Delgado O. <http://orcid.org/0000-0002-5267-8169>

This work is licensed under the [Creative Commons Attribution-NoComercial-ShareAlike 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/).

References

[1] Cordero M, Figueroa R. Towards a characterization of the generalized twisted field planes. *J. Geom.* 1995; 52(1-2):54-63.
 [2] Dempwolff U. Semifields Planes of Order 81. *J. Geom.* 2008; 89(1-2):1-16.
 [3] Hughes D, Piper F. *Projective Planes*. New York: Springer-Verlag; 1973.
 [4] Meléndez W, Figueroa R, Delgado M. On the autotopism group of the Cordero-Figueroa semifield of order 3^6 . *Discuss. Math. - General Algebra and Appl.* 2016; 36(1):117-126. doi:10.7151/dmgaa.1250.
 [5] Meléndez W, Delgado M. On a conjecture about the autotopism group of the Figueroa's presemifield of order p^n . *Note Mat.* 2018; 38(2):11-20. doi: 10.1285/i15900932v38n2p11