Inner Automorphisms of Finite Semifields

G. P. Wene
Department of Mathematics,
University of Texas at San Antonio,
One UTSA Circle, San Antonio, Texas 78249.
greg.vene@utsa.edu

Abstract. Unlike finite fields, finite semifields possess inner automorphisms. A further surprise is that even noncommutative semifields possess inner automorphisms. We compute inner automorphisms and automorphism groups for semifields quadratic over the nucleus, the Hughes-Kleinfeld semifields and the Dickson commutative semifields.

Keywords: semifields, inner automorphisms.

MSC 2000 classification: primary 17A35, secondary 17A36

1 Introduction

Finite nonassociative division rings were introduced in 1905 by L. E. Dickson [7]. Current interest is driven by the fact that the finite planes of Lenz-Barlotti type V.1 (translation planes) are precisely the planes coordinizable by division rings which are not fields (see Biliotti, Jha and Johnson [2], Hughes and Piper [14]). Readers interested in the history of semifields are referred to the articles Albert [1], Knuth [18], Kleinfeld [17], Cordero and Wene [6] and Kantor [15]. We will use the term semifield to refer to a not necessarily associative division ring.

A finite semifield [18] is a finite algebraic system containing at least two distinguished elements 0 and 1. A finite semifield $\Delta$ possesses two binary operations, addition and multiplication, designated in the usual notation and satisfying the following axioms:

(i) $(\Delta,+)$ is a group with identity $0$.

(ii) If $a,b \in \Delta$ and $ab = 0$ then $a = 0$ or $b = 0$.

(iii) If $a,b,c \in \Delta$ then $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

(iv) The element 1 satisfies the relationship $1 \cdot a = a \cdot 1 = a$ for all $a \in \Delta$.

It is easily seen that there are unique solutions to the equations $ax = b$ and $xa = b$ for every nonzero $a$ and every $b$ in $\Delta$. It also follows easily that addition is commutative. In fact it can be shown that $\Delta$ is a vector space over some
prime field $GF(p)$ and that $\Delta$ has $p^n$ elements where $n$ is the dimension of $\Delta$
over $F$, see [18].

Little is known of the automorphism groups of finite semifields. Both Dickson
[8] and Menichetti [19, 20] made partial determinations of the automorphisms
group of semifield three dimensional over a finite field not of characteristic two.
Kleinfeld [16] and Knuth [18] computed the automorphism group of each of the
23 isomorphism classes of 16-element semifields; Burmester [3] showed that there
are $n$ isomorphism classes of Dickson commutative semifields of order $p^{2n}$, $p \neq 2$,
each of these semifields has $2n$ automorphisms and determines the structure
of these automorphisms; Zemmer [21] used automorphisms to determine the
existence of subsemifields.

We begin with an examination of Knuth’s System W [18].

1 Example (Knuth’s System W.). This semifield is isomorphic to Klein-
feld’s System T-35 [16]. Let $F_4$ be the four-element field with elements 0,1,$\omega$
and $\omega^2(= \omega + 1)$. The elements of System W are of the form $a + \lambda b$ where
$a,b \in F_4$. Addition and multiplication are defined in terms of the addition and
multiplication of $F_4$.

$$(x + \lambda y) + (u + \lambda v) = (x + u) + \lambda(y + v)$$
and

$$(x + \lambda y)(u + \lambda v) = (xu + \omega y^2 v) + \lambda(yu + x^2 v).$$

This system has three automorphisms. These automorphisms are all inner
and are given by $\Phi_i(x + \lambda y) = x + \lambda \omega_i y$, $i = 1, 2, 3$. There is a unique subring of
order 4 that is generated by $\omega$ and is the nucleus. Each of these automorphisms
is inner.

$$\Phi_1(x + \lambda y) = [\omega (x + \lambda y)] \omega^2 = x + \lambda \omega y$$
$$\Phi_2(x + \lambda y) = [\omega^2 (x + \lambda y)] \omega = x + \lambda \omega^2 y$$
$$\Phi_3(x + \lambda y) = [1 (x + \lambda y)] 1 = x + \lambda y$$

Knuth’s System W is quadratic over its nucleus in the sense of Hughes
and Kleinfeld [12]. We will show that all semifields quadratic over the nucleus
possess inner automorphisms and will compute the automorphism groups. The
arguments apply to a larger class of semifields that include Hughes-Kleinfeld
semifields and the Dickson commutative semifields.
We begin with some preliminaries. This is followed by a close look at the automorphisms groups of the Hughes-Kleinfeld semifields. If $\Delta$ is a Hughes-Kleinfeld semifield of order $p^4$, the automorphism group is completely determined. We construct all Dickson commutative semifields that possess inner automorphisms. The conclusion gives several directions for continued research.

2 Preliminaries

A tool used to study the associativity of finite semifields and nonassociative rings in general is the *associator of elements $a$, $b$ and $c$:* 

$$(x, y, z) = (xy)z - x(yz).$$

The three semi-nuclei of a semifield $\Delta$ are defined in terms of associators and reflect the rich structure of finite semifields. The *left nucleus* $N_l$ is the set of all elements $d$ in $\Delta$ such that $(d, x, y) = 0$ for all $x, y \in \Delta$. The *middle nucleus* $N_m$ and the *right nucleus* $N_r$ are defined analogously. The intersection of the three semi-nuclei of $\Delta$ is called the *nucleus*; the *center*, denoted by $Z$, refers to the set of all $n$ in the nucleus $N$ such that $nx = xn$ for all $x \in \Delta$. A set $W$ of elements of $A$ is called a *weak nucleus* if $(a, b, c) = 0$ whenever any two of $a, b, c$ are in $W$. The nucleus will always be a subring of the weak nucleus. If $\Delta$ is a finite semifield, any one of the above nuclei will be a field and $\Delta$ may be considered as a left vector space over $N_l$, $N_m$, $N$ and $Z$ and a right vector space over $N_m$, $N_r$, $N$ and $Z$. In a commutative semifield, the left nucleus is the right nucleus; this semi-nucleus is contained in the middle nucleus. The middle nucleus of a commutative semifield is always a weak nucleus.

If the dimension of $A$ over its weak nucleus is two, we say that $\Delta$ is *quadratic over a weak nucleus.* These semifields have been investigated by Hughes and Kleinfeld [12], Knuth [18], Cohen and Ganley [4] and Ganley [11].

An automorphism of a semifield $\Delta$ is a bijection $\Theta : \Delta \to \Delta$ such that $\Theta(x + y) = \Theta(x) + \Theta(y)$ and $\Theta(xy) = \Theta(x)\Theta(y)$ for all $a, b$ in $\Delta$. We will denote by $\text{Aut}(\Delta)$ the group of automorphisms of $\Delta$. Automorphisms of semifields will be denoted by capital Greek letters and automorphisms of fields will be denoted by lower case Greek letters. The set $S$ of all elements $s$ of $\Delta$ such that $\Theta(s) = s$ will form a subring of $\Delta$; if $\Delta$ is a finite semifield the set $S$ of elements fixed by $\Theta$ will be a semifield. If $\Theta^2 = id$, the identity automorphism, then the set $S$ will be called the *symmetric elements*; if the characteristic is not two, the set $K = \{ s \in \Delta : \Theta(x) = -x \}$ will be called the set of *skew elements."

An automorphism $\Theta$ of $\Delta$ is called an *inner automorphism* if there is an element $m \in \Delta$ with left inverse $m_l^{-1}$ ($m_l^{-1}m = 1$) such that $\Theta(x) = (m_l^{-1}x)m$ for all $x$ in $\Delta$. We will denote the inner automorphism $x \mapsto (m_l^{-1}x)m$ by $\Theta_m$. 
Clearly if \( m \) is a nonzero element of a weak nucleus then \( m^{-1} = m_{r}^{-1} = m^{-1} \) and \( \Theta_{m}(x) = (m_{l}^{-1}xm) = (m^{-1}x)m \). The elements fixed by an inner automorphism will generate a subsemifield of the semifield \( \Delta \). If \( \Theta_{m} \) is an inner automorphism of \( \Delta \) and \( \Phi \) an arbitrary automorphism of \( \Delta \), then \( \Phi^{-1} \circ \Theta_{m} \circ \Phi \) will be an inner automorphism of \( \Delta \). Since the mapping \( x \mapsto (m_{l}^{-1}x)m \) will always be an isomorphism of the additive group of \( \Delta \), we need only to determine if this mapping is an isomorphism of the multiplicative structure of \( \Delta \).

**2 Lemma.** Let \( \Delta \) denote a finite semifield with nucleus \( N \). If \( m \in N \) then the mapping \( \Theta \) defined by \( \Theta_{m}(x) = m(xm^{-1}) \) for all \( x \) in \( \Delta \) is an inner automorphism of \( \Delta \).

**Proof.** Clearly \( \Theta_{m} \) is a bijection. Let \( x, y \in \Delta \) then

\[
[(mx)m^{-1}][(my)m^{-1}] = (mx)[m^{-1}[(my)m^{-1}]] \\
= (mx)[m^{-1}(my)]m^{-1}] \\
= (mx)[ym^{-1}] = m(xym^{-1}) \\
= m([xy]m^{-1}) = [m(xy)]m^{-1}.
\]

QED

It follows immediately that if the inner automorphism group of a finite semifield \( \Delta \) is trivial then \( N \subset Z \); if the semifield \( \Delta \) has no proper subsemifields the only inner automorphism is the trivial automorphism.

**3 Theorem.** Let \( \Delta \) denote a finite semifield with nucleus \( N \). If \( \Theta_{m}(x) = (m_{l}^{-1}x)m \) defines an inner automorphism for some \( m \in \Delta \), then so does \( \Theta_{nm}(x) = [(m_{l}^{-1}n^{-1})x](nm) \) for each nonzero \( n \in N \).

**Proof.** By the previous Lemma, \( \Theta_{n} \) defines an inner automorphism for all \( n \in N \). If \( \Theta_{m}(x) = (m_{l}^{-1}x)m \) defines an automorphism then so does \( \Theta_{m} \circ \Theta_{n} \).

\[
\Theta_{m} \circ \Theta_{n}(x) = \Theta_{m}((n^{-1}x)n) \\
= \Theta_{m}(n^{-1})\Theta_{m}(x) \Theta_{m}(n) \\
= [(n^{-1}m_{l}^{-1}x)(nm)] \\
= \Theta_{nm}
\]

QED

**4 Theorem.** Let \( \Theta_{m} \) define an automorphism of the semifield \( \Delta \) and let \( a, b \) be nonzero elements of the nucleus. Then \( \Theta_{am} \) and \( \Theta_{bm} \) define the same automorphism if and only if \( ab^{-1} \in Z \).
Proof. Suppose $\Theta_{am} = \Theta_{bn}$. Then, for all $x \in \Delta$,

\[
[(m^{-1}a^{-1})a](am) = [(m^{-1}b^{-1})(x)](bm) \\
[(m^{-1}a^{-1})a] = [(m^{-1}b^{-1})(x)]b \\
[m^{-1}(a^{-1}x)]a = [m^{-1}(b^{-1}x)]b \\
m^{-1}[(a^{-1}x)a] = m^{-1}[(b^{-1}x)b] \\
(a^{-1}x)a = (b^{-1}x)b \\
xab^{-1} = ab^{-1}x
\]

QED

5 Corollary. Let $\Delta$ denote a finite semifield with nucleus $N$. The elements $m, n \in N$ define the same inner automorphism of $\Delta$ if and only if $n^{-1}m \in Z$. In this case the elements of the nucleus determine $(|N| - 1) / (|N \cap Z| - 1)$ inner automorphisms.

3 The Hughes-Kleinfeld Semifields

We begin this section a theorem of Hughes and Kleinfeld [12].

6 Theorem (Hughes and Kleinfeld [12]). Let $R$ be a not associative division ring which is a quadratic extension of a Galois field $F$, and suppose $F$ is contained in the right and middle nuclei of $R$. Then $R$ must be isomorphic to a ring $S$ constructed as follows: Let $S$ be a vector space of dimension 2 over $F$, having a basis $1, \lambda$ and multiplication defined by

\[
(x + \lambda y)(u + \lambda v) = (xu + \delta_0 y^\sigma v) + \lambda(yu + x^\sigma v + \delta_1 y^\sigma v),
\]

where $\sigma$ is an arbitrary non-identity automorphism of $F$ and $\delta_0, \delta_1$ in $F$ are subject only to the condition that

\[
w^{1+\sigma} + \delta_1 w - \delta_0 = 0
\]

have no solution for $w$ in $F$. Conversely, given $F, \sigma, \delta_0, \delta_1$, satisfying the above conditions, then $S$ will satisfy the conditions on $R$.

We will limit our discussion to those Hughes-Kleinfeld semifields for which $\delta_1 = 0$ and will write the product as

\[
(x + \lambda y)(u + \lambda v) = (xu + \delta y^\sigma v) + \lambda(yu + x^\sigma v).
\]

Clearly $(a + \lambda b) \rightarrow (a - \lambda b)$ defines an automorphism of these semifields whenever the characteristic is not two.

Motivated by example 1, we ask when does the mapping $x + \lambda y \rightarrow [f^{-1}(x + \lambda y)]f$, where $f$ is a nonzero element of $F$, define an automorphism of the semifield $\Delta$?
7 Theorem. Let \( \Delta \) be a Hughes-Kleinfeld semifield and \( \theta : \Delta \rightarrow \Delta \) be defined by \( \theta(x) = [f^{-1}x]f \), \( x \in \Delta \), where \( f \in F \). Then \( \theta \) is an automorphism if and only if \( f^{\sigma^2} = f \).

Proof. \[
\theta([x + \lambda y][u + \lambda v]) = xu + \delta y^\sigma v + \lambda(x^\sigma v + yu)(f^{-1})^\sigma f
\]
and
\[
(x + \lambda y (f^{-1})^\sigma f)(u + \lambda v (f^{-1})^\sigma f) = xu + \delta y^\sigma v [(f^{-1})^\sigma f]^\sigma (f^{-1})^\sigma f + \\
\lambda(x^\sigma v + yu)(f^{-1})^\sigma f.
\]
\[
\delta u^\sigma v = \delta v^\sigma [ (f^{-1})^\sigma f ]^\sigma (f^{-1})^\sigma f
\]
\[
1 = (f^{-1})^\sigma f
\]
\[
f^{\sigma^2} = f
\]
QED

8 Corollary. If the Hughes-Kleinfeld semifield \( \Delta \) has a subfield \( F_0 \subset F \) fixed pointwise by \( \sigma^2 \) then \( x \rightarrow [f^{-1}x]f \) defines an automorphism of \( \Delta \).

Those semifields with the largest possible nuclei are the semifields quadratic over the nucleus; Hughes and Kleinfeld [12] computed these semifields.

9 Theorem (Hughes and Kleinfeld [12]). Let \( R \) be a not associative division ring which is a quadratic extension of a Galois field \( F \), and suppose \( F \) is contained in the nucleus of \( R \). Then \( R \) must be isomorphic to one of the rings \( S \) of theorem 6 with the additional stipulation that \( \sigma^2 = I \) and \( \delta_1 = 0 \) conversely, all such \( S \) satisfy the conditions on \( R \).

10 Theorem. Let \( \Delta \) be a semifield quadratic over a nucleus isomorphic to the Galois field \( GF(q^2) \). Then the elements of the nucleus of \( \Delta \) determine \( q+1 \) inner automorphisms.

Proof. There are \( q^2 - 1 \) nonzero elements in the nucleus and \( q - 1 \) nonzero elements in \( N \cap Z \). These elements determine \( (q^2 - 1) / (q - 1) = q + 1 \) inner automorphisms.

QED

The classification of semifields of order \( p^4 \) has yet to be completed; a nice beginning is Cordero [5]. If the order of a semifield quadratic over its nucleus is \( p^4 \), for some prime \( p \neq 2 \), the automorphism group of the semifield is easily computed. The characteristic case is example 1.
11 Theorem. Let $\Delta$ be a semifield quadratic over its nucleus, of order $p^n$. If $\Phi: \Delta \to \Delta$ is an automorphism then $\Phi(x + \lambda y) = x^k + \lambda(sy^k)$ where $s$ is a nonzero element of $GF(p^2)$ and $k$ is 1 or $p$. Furthermore, $s$ is a solution of $\delta^k = \delta x^s x$.

Proof. The condition implies that $F$ is the field $GF(p^2)$. If $\Phi: \Delta \to \Delta$ is an automorphism then $\Phi: N \to N$ is a field automorphism. Since $N$ is isomorphic to the finite field $GF(p^2)$, $\Phi(n) = n^k$, where $k$ is 1 or $p$.

We must know that what $\Phi$ does to $\lambda$. Suppose that $\Phi(\lambda) = r + \lambda s$ where $s$ is a nonzero element of $GF(p^{2n})$. Let $\alpha \in GF(p^{2n})$ then

$$\Phi(\alpha \lambda) = \Phi(\alpha) \Phi(\lambda) = \alpha^k (r + \lambda s) = \alpha^k r + \lambda((\alpha^k \sigma)s) = \Phi(\alpha \alpha^\sigma) = (r + \lambda s)(\alpha^k \sigma).$$

Equating components, we find that $\alpha^k r = \alpha^k \sigma r$. If $r \neq 0$, $\sigma$ is the identity automorphism.

Hence $\Phi(\lambda) = \lambda s$,

$$\Phi(\lambda^2) = \Phi(\delta) = \delta^k = (\lambda s)(\lambda s) = [\delta s^\sigma s].$$

We must have $\delta^k = \delta s^\sigma s$.

If $k = 1$, then $\delta = \delta s^\sigma s$. Now $s^\sigma s$ must be 1. There are exactly $p^n+1$ elements $s$ such that $s^\sigma s = 1$. There are $p + 1$ automorphisms $a + \lambda b \mapsto a + \lambda sb$; these automorphisms form a subgroup isomorphic to the additive group $Z_{p+1}$.

If $k = p$ we have $\delta^p = \delta s^\sigma s$. Now $s^\sigma s$ is fixed by $\Phi$ and must be $-1$. Thus $\delta^\sigma = -\delta$ and $-1$ is a square in $GF(p)$. There are exactly $p + 1$ elements $s$ such that $s^\sigma s = -1$.

In the latter case the automorphism group is not commutative. Let $\Phi_s$ and $\Psi_t$ be automorphisms of $\Delta$ defined by $\Phi_s(a + \lambda b) = a + \lambda sb$ and $\Psi_t(a + \lambda b) = a^p + \lambda tb^p$ where $s^{p+1} = 1$ and $t^{p+1} = -1$. Then $\Psi_t(\Phi_s(a + \lambda b)) = a^p + \lambda ts^p b^p$ and $\Phi_s(\Psi_t(a + \lambda b)) = a^p + \lambda stb^p$. 

12 Lemma. Let $k$ be a nonsquare element of $GF(p^n)$ and $m$ an element of the extension field $GF(p^{2n})$ such that $m^2 = k$. Then $m$ is a nonsquare in $GF(p^{2n})$ if and only if $-1$ is a square in $GF(p^n)$. Furthermore, $m^p = -m$.

Proof. Let $k$ be a nonsquare element of $GF(p^n)$ and $m$ an element of the extension field $GF(p^{2n})$ such that $m^2 = k$. Suppose $m$ is a square in $GF(p^{2n})$ and $m = (\alpha + \beta m)^2$. Then $m = \alpha^2 + \beta^2 k + 2\alpha \beta m$. We must have $\alpha^2 + \beta^2 k = 0$.
and $2\alpha\beta m = 1$. Solving these equations for $\alpha$, we find that $4\alpha^4 = -k$. Hence if both $k$ and $-k$ are nonsquares in $GF(p)$, $m$ will be a nonsquare in $GF(p^2)$.

Since $p$ is odd, $m^p = zm$ where $z \in GF(p)$. Then $m^{p^2} = m = zm^p = z^2m$ and $z = -1$.

The above lemma tells us that we can always find a nonsquare element $m$ in $GF(p^{2n})$ such that $m^{p^n} = -m$ if $-1$ is a square in $GF(p^n)$.

13 Example. Let $F$ be the field $GF(25)$ isomorphic to $GF(5)[m]$ where $m^2 = 2$. Then $m$ is a nonsquare in $F$ such that $m^3 = -m$. We construct the semifield as before using $\delta = 1 + 2m$. Since $\delta^5 \neq -\delta$, the automorphism group consists of the six inner automorphisms generated by the automorphism

$$\Phi(a + \lambda b) = a + \lambda b(3 + 2m)$$

where $(3 + 2m)^3 = -1$.

If we use $\delta = m$, we get a 12-element automorphism group. The group is generated by the automorphisms $\Phi$ as above and the automorphism $\Psi(a + \lambda b) = a^5 + \lambda b^5(1 + m)$. The elements $\Phi$ and $\Psi$ satisfy $\Psi^2 = \Phi^3$ and $\Psi\Phi\Psi^{-1} = \Phi^5$.

14 Remark. The congruence $x^2 + 1 \equiv 0 \pmod{p}$ has a solution for the prime $p$ only if $p$ is of the form $4n + 1$ (Dickson [10]). Some primes $p$ for which $-1$ is a square in the finite field $GF(p)$ are $p = 5, 13, 17, 29, 41, 53, 61, 73, 89$ and $97$.

Let $\Delta$ be a Hughes Kleinfeld semifield that is not necessarily quadratic over its nucleus. The left inverse $\lambda^{-1}$ of the element $\lambda$ is

$$\lambda^{-1} = \lambda \left( \frac{1}{\delta} \right)^{\sigma^{-1}}$$

and

$$[(\lambda^{-1})(a + \lambda b)]\lambda = a^\sigma + \lambda b^\sigma.$$  

15 Theorem. Let $\Delta$ be a Hughes-Kleinfeld semifield and $\theta_\lambda : \Delta \rightarrow \Delta$ be defined by $\theta_\lambda(x) = [\lambda^{-1} - x]\lambda$ for $x \in \Delta$. Then $\theta_\lambda$ is an automorphism if and only if $\delta^\sigma = \delta$. In particular, $\Delta$ is not quadratic over its nucleus.

Proof.

$$\theta_\lambda([a + \lambda b][c + \lambda d]) = a^\sigma c^\sigma + \delta^\sigma b^\sigma d^\sigma + \lambda(a^\sigma d^\sigma + b^\sigma c^\sigma)$$

and

$$(a^\sigma + \lambda b^\sigma)(c^\sigma + \lambda d^\sigma) = a^\sigma c^\sigma + \delta b^\sigma d^\sigma + \lambda(a^\sigma d^\sigma + b^\sigma c^\sigma).$$

Equating components yields $\delta^\sigma = \delta$. Were $\Delta$ to be quadratic over its nucleus, this would force $\delta$ to be a square in the field $F$. \qed
**16 Example.** Let $F$ be the field $GF(5^3)$. Since 2 is a nonsquare in $GF(5)$, it remains a nonsquare in $GF(5^3)$. Construct the Hughes-Kleinfeld semifield with product

$$(x + \lambda y)(u + \lambda v) = (xu + 2y^5v) + \lambda(yu + x^5v).$$

The automorphism $\theta_\lambda(x + \lambda y) \to x^5 + \lambda y^5$ generates a cyclic subgroup of three automorphisms. If $\Phi : \Delta \to \Delta$ is the automorphism $(x + \lambda y) \to x - \lambda y$ then $\Phi \circ \theta_\lambda$ generates a cyclic subgroup of order six.

**4 The Dickson Commutative Semifields**

The Dickson commutative [9] semifields are the only commutative semifields quadratic over a weak nucleus. The definitive study of the Dickson commutative semifields is the paper by Burmester [3].

Surprisingly, the Dickson commutative semifields possess inner automorphisms. The only inner automorphisms of a finite field is the trivial automorphism. The real quaternions are an infinite, associative, noncommutative division ring that permits inner automorphisms. We will construct a subclass of the Dickson commutative semifields that have nontrivial inner automorphisms.

**17 Example.** Let $F$ be the field $GF(p^n)$, $p \neq 2$ and $n \geq 2$. The elements of $\Delta$ are of the form $a + \lambda b$ where $a, b \in F$. Addition and multiplication are defined in terms of the addition and multiplication of $F$, an automorphism $\sigma$ of $F$ and an element $\delta \in F$ that is a nonsquare in $F$. The addition is given by

$$(a + \lambda b) + (c + \lambda d) = (a + c) + \lambda(b + d)$$

and the multiplication by

$$(a + \lambda b)(c + \lambda d) = ac + \delta(bd)^\sigma + \lambda(ad + bc).$$

Burmester [3] showed that the automorphisms of $\Delta$ are given by

$$\Phi_{ij}(a + \lambda b) = a^{\sigma^i} + \lambda(s_{ij}b^{\sigma^j}), i = 0, 1, \ldots, n - 1 \text{ and } j = 1, 2$$

where $s_{ij}$ is one solution of $\delta^{\sigma^i} = \delta(x^2)^\sigma$.

He shows that there are $n$ isomorphism classes of Dickson commutative semifields of order $p^{2n}$, $p \neq 2$; each of these semifields has $2n$ automorphisms.

We now derive an alternative description, in terms of inner automorphisms, for some of these automorphism groups.

An obvious automorphism is the mapping $(a + \lambda b) \mapsto (a - \lambda b)$. 
18 Theorem. Let $\Delta$ be a Dickson commutative semifield, $F$ the field $GF(p^n)$, $p \neq 2$ and $n \geq 2$ and $\delta$ a nonsquare element of $F$. Then $\Phi(a + \lambda b) = [\lambda^{-1}_i(a + \lambda b)] \lambda = a^\sigma + \lambda b^\sigma$ defines an automorphism of $\Delta$ if and only if $\delta^\sigma = \delta$.

**Proof.**

$$\lambda^{-1}_i = \lambda \frac{1}{\delta}$$

then

$$[\lambda^{-1}_i(a + \lambda b)] \lambda = a^\sigma + \lambda b^\sigma$$

The multiplication property of the automorphism:

$$\Phi \left[(a + \lambda b)(c + \lambda d)\right] = \Phi (ac + \delta(bd)) + \lambda(ad + bc))$$

$$= (ac)^\sigma + \delta^\sigma (bd)^{\sigma^2} + \lambda(ad + bc)^\sigma$$

$$(a^\sigma + \lambda b^\sigma)(c^\sigma + \lambda d^\sigma) = (ac)^\sigma + \delta (bd)^{\sigma^2} + \lambda(ad + bc)^\sigma$$

Equating components gives $\delta^\sigma = \delta$. 

**QED**

19 Example. Let $\Delta$ be a Dickson commutative semifield, $F$ the field $GF(5^5)$, and $\delta = 2$. Since 2 is a nonsquare in $GF(5)$ it remains a nonsquare in $GF(5^5)$. The cyclic automorphism group is generated $\Phi \circ \Psi$ where $\Phi(a + \lambda b) = a^5 + \lambda b^5 = [\lambda^{-1}_i(a + \lambda b)] \lambda$ and $\Psi(a + \lambda b) = a - \lambda b$. The elements of $\Delta$ fixed by the automorphism $\Phi$ is the 25 element field $GF(5)[\lambda]$. There will be ten automorphisms.

5 Conclusion And Further Directions

We have seen that all semifields $\Delta$ quadratic over the nucleus have (nontrivial) inner automorphisms: if $|\Delta| = p^4$ for some prime $p$, the automorphism group can be completely determined. Any Hughes-Kleinfeld semifield in which there is a subfield fixed pointwise by the automorphism $\sigma$ has an inner automorphism as does any Hughes-Kleinfeld semifield in which $\delta^\sigma = \delta$. Our results can be used to produce many examples.

We determined a sufficient condition that a Dickson commutative semifield have a (nontrivial) inner automorphism.

Much work remains to be done. The automorphism groups of the Hughes-Kleinfeld semifields need to be computed. We need to find additional examples of semifields with inner automorphisms.

Dickson [8] discovered a certain family of three-dimensional commutative nonassociative division algebras. Let $F$ be any field of characteristic $\neq 2$. Let
B, β, b be elements of F such that \(x^3 - Bx^2 - \beta x - b\) is irreducible over F. Define an algebra with basis 1, i, j by

\[
\begin{align*}
i^2 &= j \\
i j &= ji = b + \beta i + Bj \\
j^2 &= 4bB - \beta^2 - 8bi - 2\beta j.
\end{align*}
\]

There has yet to emerge a comprehensive description of the automorphism of either the commutative or noncommutative semifields 3-dimensional over a finite field. Complete the work started by Dickson and Menichetti.

We will use \(\Delta \otimes_F K\) to denote the algebra that results from extending the base field F to the field K and are interested in the case where \(\Delta \otimes_F K\) is a semifield. What are the automorphism groups of the resulting semifields \(\Delta \otimes_F K\)? Does the obvious extension of the automorphism group always work?

The polynomial \(x^3 - Bx^2 - \beta x - b\) will continue to be irreducible in all field extensions K of degree prime to 3 and can be used to construct a commutative semifield \(\Delta\). If \(\theta : \Delta \to \Delta\) is an automorphism and \(\sigma : K \to K\) an automorphism of the field K then \(\sigma \circ \theta : \Delta \otimes_F K \to \Delta \otimes_F K\) will be an automorphism. Clearly the polynomial \(w^{1+p^k} + \delta_1 w - \delta_0\) used to construct the Hughes-Kleinfeld semifield will remain irreducible in all field extensions K of degree prime to \(p^k + 1\); does the obvious extension of the automorphism group give the automorphisms group of \(\Delta \otimes_F K\)?

Knowing that the automorphism group has an element of order 2 immediately provides some knowledge of the multiplication of the algebra. What other interesting conditions can we impose on the automorphism group?

There is much to do.

References


